GROUPES ET GÉOMÉTRIE

GROUPES ET GÉOMÉTRIE

TABLE DES MATIÈRES

..... vii
Premiers exemples vii
Les groupes et les équations ix
Les actions de groupe arrivent naturellement x

1. Lois, groupes : généralités et exemples 1
1.1. Relations d'équivalence et ensemble quotient 1
1.2. Groupes 12
1.3. Premiers exemples 15
1.4. Sous-groupes 22
1.5. Ordre d'un groupe, ordre d'un élément sous-groupe engendré par un élément 26
1.6. Classes et théorème de Lagrange 38
1.7. Générateurs d'un groupe 50

2. 55
2.1. Morphismes de groupes 55
2.2. Isomorphismes 65
2.3. Produits directs 79
2.4. Application 83

3. 85
3.1. Conjugaison dans un groupe 85
3.2. Sous-groupes distingués 96
3.3. Groupes quotients 101
3.4. Ordres des éléments dans un groupe quotient 107
3.5. Théorème de factorisation, isomorphismes 110
3.6. Produits semi-directs 113
3.7. Le Théorème de Cauchy et ses conséquences 132

4. Groupes abéliens infinis, finis, de type fini, de torsion 143
4.1. Étude du groupe $\mathbb{Z}$: premières propriétés 145

4.2. Propriété universelle de $\mathbb{Z}/d\mathbb{Z}$ 149
4.3. Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ 151
4.4. Exposant d'un groupe abélien fini 155
4.5. Classification des groupes abéliens finis 156
4.6. Groupes abéliens de type fini 165
4.7. Groupes abéliens de torsion 171
4.8. Classification des matrices équivalentes à coefficients entiers, facteurs invariants de matrices 172

5. Deux exemples de groupes non abéliens 177
5.1. Les groupes symétriques et alternés 178
5.2. Le groupe diédral 210

6. Actions de groupes 243
6.1. Une illustration, une définition, les premiers exemples 243
6.2. Actions transitives, actions fidèles, orbites, stabilisateurs 249
6.3. Quelques propriétés des actions de groupes 261
6.4. Actions transitives 271

7. Actions de groupes, applications 281
7.1. Deux applications aux groupes infinis 281
7.2. Le théorème de Cauchy 282
7.3. Applications aux p-groupes 284
7.4. Applications au groupe de permutations et au groupe alterné 290
7.5. Théorème de Wedderburn 297
7.6. Automorphismes de $\mathbb{Z}/n\mathbb{Z}$ 300
7.7. Isomorphismes « exceptionnels » 305
7.8. Étude du groupe $\mathrm{O}(p,q)$ 316
7.9. Sous-groupes de $\mathrm{GL}(n,\mathbb{C})$ 320
7.10. Dénombrement des colorations du cube 325
7.11. Le théorème de Noether 327
7.12. Simplicité du groupe spécial linéaire $\mathrm{PSL}(n,\Bbbk)$ 329

8. Groupes libres ; groupes définis par générateurs et relations 335
8.1. Groupes libres 335
8.2. Ubiquité des groupes libres dans les groupes linéaires 340
8.3. Groupes définis par générateurs et relations 342
8.4. Le groupe $\mathrm{SL}(2,\mathbb{Z})$ 347

9. Actions de groupes et algèbre linéaire 371
9.1. Action par translation du groupe linéaire : pivot de Gauss 372
9.2. Action par translation des groupes orthogonal et unitaire 372
9.3. Actions de Steinitz : matrices équivalentes 372
9.4. Action de $\mathrm{GL}(n,\mathbb{C})$ par conjugaison 385
9.5. Exemples d'actions classiques de groupes classiques 403

10. Théorèmes de Sylow 409
10.1. Les Théorèmes de Sylow et leurs premières conséquences 411
10.2. Théorèmes de Sylow et sous-groupes distingués 419
10.3. Description des Sylow de certains groupes « classiques » 423
10.4. Propriétés de commutativité 431
10.5. Le groupe $\mathcal{A}_n$ est simple dès que $n \geq 5$, version ? ? ? 435
10.6. Automorphismes extérieurs de $\mathfrak{S}_6$, version 2 439
10.7. Classification des groupes d'ordre 12 441
10.8. Extension des théorèmes de Sylow 446

11. Représentations des groupes 451
11.1. Représentations 451
11.2. Caractères 463
11.3. Table des caractères 473
11.4. Groupes abéliens finis et représentations linéaires des groupes finis 494
11.5. Applications 496

12. Géométrie 507
12.1. Géométrie euclidienne 510
12.2. Simplicité du groupe des rotations de $\mathbb{R}^3$ 516
12.3. Solides platoniciens 520
12.4. Les sous-groupes finis de $\mathrm{SO}(3, \mathbb{R})$ 525
12.5. Géométrie affine 528

Index 537

Bibliographie 541

Historiquement, les groupes sont d'abord apparus comme « groupes de transformations » *i.e.* comme sous-groupes de certains groupes de bijections. On a ensuite progressivement compris l'intérêt d'axiomatiser la notion, ce qui a conduit à la notion de « groupe abstrait », celle que nous connaissons aujourd'hui. Néanmoins l'expérience montre que pour comprendre un groupe abstrait, il peut être utile de le voir, éventuellement de plusieurs façons différentes, comme un groupe de transformations.

Premiers exemples

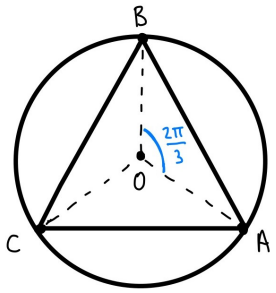
Aujourd'hui on introduit la notion de « groupe » comme un ensemble d'éléments sur lesquels on peut effectuer une opération. Par exemple un ensemble de nombres avec, comme opération, l'addition (ou encore la multiplication) ou encore un ensemble de fonctions pour lequel l'opération serait la composition.

Nous allons « détailler » chacun de ces exemples.

- ◇ Dans le premier cas considérons par exemple l'ensemble des entiers relatifs avec l'addition comme opération. C'est un groupe car il vérifie les quatre propriétés qui définissent un groupe.
  - — On doit rester dans l'ensemble quand on effectue l'opération ; autrement dit lorsqu'on opère sur plusieurs éléments de l'ensemble le résultat appartient encore à l'ensemble. Quand on ajoutons plusieurs entiers, nous obtenons un entier.
  - — On peut lorsqu'on doit opérer sur plus de trois éléments travailler de proche en proche comme on le souhaite du moment qu'on ne modifie pas l'ordre des éléments. Cela revient à mettre des parenthèses comme on veut quand on effectue l'opération. Dans le cas des entiers cela se traduit par le fait que l'on trouve bien le même résultat si on effectue $2 + (3 + 4)$ et $(2 + 3) + 4$.
  - — L'un des éléments du groupe n'a aucun effet pour cette opération, on l'appelle l'élément neutre. Dans le cas des entiers relatifs muni de l'addition 0 est un élément neutre.

— On doit toujours pouvoir faire marche arrière. Autrement dit en partant d'un objet du groupe on peut toujours en trouver un autre de sorte qu'on obtient l'élément neutre lorsqu'on effectue l'opération entre les deux. Lorsqu'on considère l'ensemble des entiers relatifs muni de l'addition il suffit de faire la somme de n'importe quel entier relatif et de son opposé pour trouver 0.

◇ Dans le second cas considérons les isométries du plan qui laissent invariant un triangle équilatéral.



Sur cette figure il s'agit des rotations r_1, r_2 et r_3 de centre O et d'angle $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ et 2π et des symétries s_1, s_2 et s_3 d'axes (OA), (OB) et (OC).

L'élément neutre est ici la transformation géométrique qui ne modifie aucun point de la figure c'est-à-dire r_3.

On peut vérifier que l'ensemble des isométries du plan qui laissent invariant un triangle équilatéral muni de la composition satisfait les trois autres règles évoquées précédemment et forme un groupe. À noter que ce groupe est formé de 6 éléments.

Remarquons que nous pourrions également adopter un autre point de vue sur cette situation en oubliant la géométrie et en considérant simplement que chacune des lettres A, B et C doit être transformée en A, B ou C. On trouve six possibilités :

— A devient A, B devient B, C devient C ;
— A devient A, B devient C, C devient B ;
— A devient B, B devient A, C devient C ;
— A devient C, B devient B, C devient A ;
— A devient B, B devient C, C devient A ;
— A devient C, B devient A, C devient B.

Ou encore imaginons que l'on place trois jetons numérotés 1, 2 et 3 côte à côte comme sur la première ligne des tableaux ci-dessous et que sur la seconde ligne on essaie de trouver toutes les dispositions différentes possibles. On appelle *substitutions* toute opération qui consiste à passer d'une disposition à une autre. On obtient six substitutions qui sont

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Il suffit de changer les nombres 1, 2 et 3 en A, B et C pour retrouver ce qui précède. Et si on revient à la situation géométrique on s'aperçoit que le premier bloc correspond à r_3, le second à s_1, le troisième à s_3, le quatrième à s_2, le cinquième à r_1 et le dernier à r_2. L'ensemble de ces six substitutions muni de la composition forme donc un groupe à six éléments.

Les nombres rationnels non nuls $\mathbb{Q}^*$ muni de la multiplication forment un groupe. De même l'ensemble des nombres réels (resp. complexes) privé de 0 muni de la multiplication forme un groupe. En revanche l'ensemble des entiers relatifs non nuls $\mathbb{Z}^*$ muni de la multiplication n'est pas un groupe. En effet prenons le nombre 3 il faudrait le multiplier par $\frac{1}{3}$ pour retrouver l'élément neutre de la multiplication qui est 1. Mais $\frac{1}{3}$ n'est pas un entier donc $\mathbb{Z}^*$ muni de la multiplication n'est pas un groupe.

Les groupes et les équations

Nous avons vu que les substitutions étaient "liées" au groupe des isométries planes laissant un triangle équilatéral invariant. Citons une autre situation dans laquelle elles interviennent. Au début du 19ième siècle on connaissait des formules pour résoudre des équations comme $ax^2 + bx + c = 0$. Voici une telle formule

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Pour une équation du troisième degré on dispose aussi des formules de Cardan. Par exemple

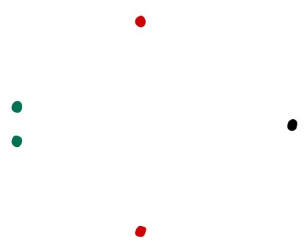
$$x = \left(\sqrt{q^2 + p^3} - q\right)^{1/3} + \left(\sqrt{q^2 + p^3} + q\right)^{1/3}$$

est une solution de $x^3 + 3px + 2q = 0$; les deux autres solutions sont données par des formules analogues. Il existe aussi une méthode avec des formules, due à Ferrarri, pour résoudre des équations de degré 4.

La question posée depuis au moins Lagrange est : y a-t-il toujours des formules pour résoudre des équations algébriques ? Il se trouve que certaines opérations algébriques liées à l'équation permutent les solutions de l'équation entre elles. En général si on prend une équation de degré 5 on associe par cette méthode le groupe des permutations des cinq solutions de l'équation

$$X^5 - X - 1 = 0.$$

Voici dessinées les solutions complexes de cette équation



Pour cette équation permuter les solutions revient à considérer le groupe qui lui est associé. Ce procédé est même très complet ; il faut y penser comme à un dictionnaire, certes un peu difficile à établir explicitement, mais un dictionnaire quand même, entre les équations d'une part et les groupes d'autre part. Le fait de savoir résoudre une équation peut se lire sur ce groupe, cet ensemble abstrait associé à l'équation, sans qu'on ait besoin de calculer explicitement les formules donnant les solutions. Si l'équation est résoluble par des formules, alors le groupe qui lui est associé dans le dictionnaire vérifie une propriété algébrique, concrète : "être résoluble". Ainsi quand on prend une équation il suffit en théorie de consulter le dictionnaire pour savoir si on peut résoudre cette équation par des formules algébriques à condition qu'on sache à quel type de groupe on a affaire, résoluble ou pas.

Prenons une équation de degré 2 qui a deux solutions distinctes ; le groupe qui lui est associé est l'ensemble des permutations des deux solutions x_1 et x_2. Ce groupe a deux éléments, la permutation identité et celle qui échange x_1 et x_2. Ce groupe à deux éléments est résoluble, c'est la raison pour laquelle on dispose d'une formule pour résoudre les équations de degré 2. Revenons à notre équation de degré 5

$$X^5 - X - 1 = 0.$$

Le groupe qui lui est associé dans le dictionnaire est le groupe des permutations à cinq éléments. Galois a démontré que ce groupe n'est pas résoluble de sorte qu'on ne peut pas résoudre cette équation par des formules.

Les actions de groupe arrivent naturellement...

Les actions de groupes sur des espaces de matrices illustrent une méthode uniforme pour des problèmes de classification que l'on rencontre en mathématiques. En effet en agissant un groupe partitionne en orbites l'ensemble sur lequel il agit avec, dans le cas des espaces de matrices, une possibilité d'avoir des actions linéaires. La nature de la classification dépendra alors du groupe agissant :

- ◇ groupe linéaire pour des classifications linéaires ;
- ◇ groupe affine pour des classifications affines ;
- ◇ groupe orthogonal pour des classifications euclidiennes ;
- ◇ et enfin le groupe projectif pour des classifications projectives.

Chaque orbite se voit munie d'un classifiant (invariant total) et souvent d'une matrice de forme normale.

Dans les espaces de matrices le problème de classification provient principalement du problème de changement de base. En effet, on se sert des matrices pour coder des objets (applications linéaires, endomorphismes, formes quadratiques, représentations) mais ce codage dépend de façon drastique d'une base. Il faut alors gérer le problème de changement de bases.

Dans un premier temps, les problématiques sont les suivantes : décrire les actions, décrire les classificants, trouver des algorithmes pour calculer les classificants, déterminer les formes normales. Dans un second temps nous pouvons si le corps est $\mathbb{R}$ ou $\mathbb{C}$ mettre une topologie sur l'espace des matrices puis chercher les cardinaux de chaque orbite. Enfin dans un troisième

temps nous pouvous nous intéresser à des problèmes de descente, *i.e.* nous demander comment passer de la classification sur un corps $\Bbbk$ à un sous-corps de $\Bbbk$.

Le premier exemple édifiant est l'action de Steinitz. Une même application linéaire est codée dans deux paires de bases distinctes $(\underline{e}, \underline{f})$ et $(\underline{e}', \underline{f}')$ et les matrices respectives vont vérifier $A' = P^{-1}AQ$ où P désigne la matrice de passage de $\underline{f}$ à $\underline{f}'$ et Q désigne la matrice de passage de $\underline{e}$ à $\underline{e}'$. On dit alors que les matrices A et A' appartiennent à la même orbite. Le classificant est le rang [1] qui se calcule grâce au pivot de Gauss sur les lignes (à gauche) et sur les colonnes (à droite). On vérifie que deux matrices A et A' appartiennent à la même orbite si et seulement si elles ont le même rang . En particulier on distingue la matrice de forme normale de rang r qui est la matrice avec r "1" sur sa diagonale et des zéros ailleurs. Il n'y a ici pas d'obstruction de descente puisque le rang est indépendant du corps de base ; par suite deux matrices sur $\Bbbk$ sont équivalentes sur $\Bbbh$, sous-corps de $\Bbbk$, si et seulement si elles le sont sur $\Bbbk$. De plus si $\mathcal{O}_r$ est l'orbite des matrices de rang r sur $\mathbb{R}$ ou $\mathbb{C}$ alors son adhérence est donnée par la réunion des $\mathcal{O}_{r'}$, $0 \leq r' \leq r$. Pour calculer le cardinal d'une orbite sur un corps fini on utilise le cardinal du groupe linéaire et le cardinal d'un stabilisateur.

Nous pouvons considérer le cas de l'action par conjugaison de $\mathrm{GL}(n, \mathbb{C})$ sur les matrices diagonalisables sur $\mathbb{C}$ et même sur les matrices nilpotentes. Le premier cas a sa petite spécificité : les orbites sont toutes fermées et cela constitue une caractéristation des matrices diagonalisables. Dans le second cas nous tombons, pour les formes normales, sur les réduites de Jordan. Dans toutes les éventualités nous n'avons pas d'obstruction de descente : deux matrices carrées sur $\Bbbk$ sont $\Bbbh$-semblables si et seulement si elles sont $\Bbbk$-semblables.

Nous pouvons aussi traiter le cas de l'action de $\mathrm{GL}(n, \Bbbk)$ par congruence sur l'espace $\mathrm{Sym}(n, \Bbbk)$ des matrices symétriques. Les choses dépendent drastiquement du corps de base :

- ⋄ $\mathbb{C}$, invariant = rang ;
- ⋄ $\mathbb{R}$, invariant = signature par le théorème de Sylvester ;
- ⋄ et $\mathbb{F}_q$, invariant = discriminant.

L'algorithme dominant est la méthode de Gauss.

Il y a aussi l'action à gauche $P \cdot A = PA$ de $\mathrm{GL}(n, \Bbbk)$ sur l'espace $\mathrm{M}_{n,m}(\Bbbk)$. En effet lorsque nous souhaitons résoudre le système linéaire $AX = Y$ nous intervenons par combinaisons linéaires sur les lignes et donc uniquement à gauche sur $A \in \mathrm{M}_{n,m}(\Bbbk)$. Nous effectuons un algorithme de pivot, mais uniquement à gauche [2]. Les formes normales sont alors les matrices échelonnées réduites : pour tout A il existe une unique matrice échelonnée réduite E telle que $PA = E$ pour un P dans $\mathrm{GL}(n, \Bbbk)$.

Se donner une représentation complexe d'un groupe fini G d'ordre n revient à se donner n matrices $A_g \in \mathrm{M}(m, \mathbb{C})$, $g \in \mathrm{G}$, qui vérifient les mêmes relations que dans le groupe : $gh = k$ implique $A_g A_h = A_k$. On peut se demander s'il existe une matrice de passage P telle que les PA_gP^{-1} soient réelles pour tout g. Une réponse est donnée dans le cas d'une représentation irréductible par l'indicatrice de Frobenius-Schur.

1. Rappelons que le rang est égal à la taille du plus grand mineur non nul.
2. Le pivot à droite correspondrait à des changements de variables

CHAPITRE 1

LOIS, GROUPES : GÉNÉRALITÉS ET EXEMPLES

1.1. Relations d'équivalence et ensemble quotient

Nous sommes souvent amenés à partager les éléments d'un ensemble en différentes classes, c'est-à-dire à définir une partition de cet ensemble. Il devient alors possible de raisonner et de calculer sur les classes : c'est un procédé algébrique puissant.

1.1.1. Partition et relation d'équivalence. —

1.1.1.1. *Partition d'un ensemble.* —

Définition 1.1.1

Soit E un ensemble. Une *partition* de E est la donnée de parties C_i de E, non vides, deux à deux disjointes et dont la réunion est E. On dit que les parties C_i, $i \in I$ I ensemble quelconque non vide appelé ensemble des indices), sont des *classes*.

On peut évidemment définir des partitions de manière totalement arbitraire, par exemple $\mathbb{N} = \{1, 2, 3, 4\} \cup \{0\} \cup \{n \in \mathbb{N} \mid n \geq 5\}$, ou bien réunir les éléments qui partagent une propriété commune :

Exemple 1.1.1. — Pour tout entier naturel n notons C_n l'ensemble des entiers relatifs qui sont divisibles par 2^n mais pas par 2^{n+1}. On a ainsi C_0 qui est l'ensemble des entiers impairs, C_1 l'ensemble des entiers multiples de 2 mais pas de 4.

Les parties $(C_n)_{n\in\mathbb{N}}$ et $\{0\}$ forment une partition de $\mathbb{Z}$.

On peut aussi utiliser une fonction intermédiaire :

Exemple 1.1.2. — Soit $f\colon E \to F$ une application surjective entre deux ensembles.

Rappelons que pour tout élément $b \in F$, la partie de E définie par

$$f^{-1}(\{b\}) = \{x \in E \mid f(x) = b\}$$

s'appelle *l'image réciproque de b par f*. Par abus de notations nous écrirons $f^{-1}(b)$.

- ◇ Puisque f est surjective, $f^{-1}(b)$ est non vide.
- ◇ Les parties $C_b = f^{-1}(b)$ sont deux à deux disjointes car s'il existe x appartenant à $C_b \cap C_{b'}$, alors $b = f(x) = b'$.
- ◇ De plus leur réunion est E, car pour tout $x \in E$ nous avons $x \in f^{-1}(f(x))$ donc x appartient à $C_{f(x)}$. Par suite les parties C_b, $b \in F$, forment une partition de E.

Exemple 1.1.3. — Soit $f\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ l'application définie par $f(x,y) = 2x+3y$. L'application f est surjective car pour tout entier $k \in \mathbb{Z}$, nous avons $f(-k,k) = -2k+3k = k$. Ainsi par exemple les parties

$$C_0 = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} \,|\, 2x+3y = 0\} \qquad \text{et} \qquad C_5 = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} \,|\, 2x+3y = 5\}$$

sont des classes de la partition de $\mathbb{Z}\times\mathbb{Z}$ définie par f (droites parallèles à $2x+3y = 0$ intersectées avec $\mathbb{Z}\times\mathbb{Z}$).

En toute généralité, si E est un ensemble et si $\mathcal{P} = \{C_i\}_{i\in I}$ est une partition de E, on peut dire de deux éléments de E qu'ils sont « reliés » par la partition $\mathcal{P}$ s'ils appartiennent au même ensemble C_i. En particulier on constate alors que tout $x \in E$ est relié à lui-même, que si $x \in E$ est relié à $y \in E$ alors y est relié à x et enfin que si x est relié à y et y à z alors x est relié à z. Une telle relation entre les éléments d'un même ensemble est une *relation d'équivalence*. Il s'agit d'un moyen qui peut s'avérer extrêmement fin pour obtenir des informations sur un ensemble, notamment sur les groupes. Dans le paragraphe qui suit nous introduisons plus précisément cette notion.

1.1.1.2. *Relation d'équivalence.* —

Définition 1.1.2

Soit E un ensemble. On a défini une *relation* $\mathcal{R}$ sur l'ensemble E si on s'est donné un ensemble $\Gamma \subset E \times E$ appelé *graphe de la relation*.

Cette définition revient à dire que pour définir une relation, on se donne l'ensemble des couples (x,y) d'éléments de E qui vérifient la relation, *i.e.* $(x,y) \in \Gamma$. Nous avons ici le même mode de définition que pour une application, qui est un cas particulier de relation. Au lieu de noter $(x,y) \in \Gamma$ nous noterons $x\mathcal{R}y$.

Définitions 1.1.1

Une relation $\mathcal{R}$ sur un ensemble E est une *relation d'équivalence* si elle est

(i) réflexive : $\forall\, a \in E,\ a\mathcal{R}a$;

(ii) symétrique : $\forall\, a,\ b \in E,\ a\mathcal{R}b \Rightarrow b\mathcal{R}a$;

(iii) transitive : $\forall\, a,\ b,\ c \in E\ (a\mathcal{R}b \text{ et } b\mathcal{R}c) \Rightarrow a\mathcal{R}c$;

Pour tout $a \in E$, l'ensemble

$$\overline{a} = \{x \in E \,|\, x\mathcal{R}a\}$$

s'appelle la *classe* (*d'équivalence*) *de* a.

Exemple 1.1.4. — Sur tout ensemble E, l'égalité de deux éléments est une relation d'équivalence. En effet définissons sur E la relation $\mathcal{R}$ par : soient $x,\ y \in E$ alors $x\mathcal{R}y$ si et seulement si $x = y$. La relation $\mathcal{R}$ est :

- ◇ réflexive : pour tout x dans E, nous avons $x = x$, *i.e.* $x\mathcal{R}x$;
- ◇ symétrique : soient x et y dans E tels que $x\mathcal{R}y$, c'est-à-dire $x = y$; mais $x = y$ si et seulement si $y = x$, autrement dit $y\mathcal{R}x$;
- ◇ transitive : soient x, y et z dans E tels que $x\mathcal{R}y$ et $y\mathcal{R}z$; alors d'une part $x = y$ et d'autre part $y = z$ ce qui conduit à $x = z$, *i.e.* $x\mathcal{R}z$.

Pour tout x dans E, $\overline{x} = \{x\}$.

Comme on peut s'en douter, ce premier exemple correspond à la relation d'équivalence « triviale ». Les classes d'équivalence y étant réduites à un élément elle n'a concrètement pas une grande utilité. Elle indique cependant que les relations d'équivalence sont en quelque sorte des généralisations de la relation d'égalité.

Exemple 1.1.5. — Sur l'ensemble des droites (du plan ou de l'espace), la relation « droites parallèles ou confondues » est une relation d'équivalence. Si d est une droite, sa classe d'équivalence $\overline{d}$ est par définition la direction de d.

Exemple 1.1.6. — Pour les angles du plan, la relation de congruence modulo 2π est une relation d'équivalence. La classe d'équivalence d'un angle ϑ par la relation de congruence modulo 2π est l'angle lui-même modulo 2π : $C_\vartheta = \{\vartheta + 2k\pi \,|\, k \in \mathbb{Z}\}$.

Exemple 1.1.7. — Dans $\mathbb{Z}$, la relation $x \equiv y \bmod (n)$, que nous noterons aussi $x \equiv_n y$, si $x - y$ est divisible par l'entier n est une relation d'équivalence $\mathcal{R}$. En effet, $\mathcal{R}$ est

- ◇ réflexive : pour tout $x \in \mathbb{Z}$ nous avons $x - x = 0$ est divisible par n, *i.e.* $x\mathcal{R}x$;
- ◇ symétrique : soient x et y dans $\mathbb{Z}$ tels que $x\mathcal{R}y$, c'est-à-dire tels que $x - y = nu$ pour un certain $u \in \mathbb{Z}$, alors $y - x = n(-u)$ et $y\mathcal{R}x$;

- ◇ transitive : soient x, y et z dans $\mathbb{Z}$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors d'une part $x-y=nu$ pour un certain $u\in\mathbb{Z}$ et $y-z=nv$ pour un certain $v\in\mathbb{Z}$. Nous en déduisons que
$$x-z=(x-y)+(y-z)=nu+nv=n\underbrace{(u+v)}_{\in\mathbb{Z}}$$
soit $x\mathcal{R}z$.

Les classes d'équivalence sont les $\overline{y}=\{x\in\mathbb{Z}\,|\,\exists\,k\in\mathbb{Z},x-y=kn\}$ pour $y\in\{0,1,2,\ldots,n-1\}$, ce qui correspond à l'ensemble des restes possibles de la division euclidienne par n. En effet, par définition
$$\overline{y}=\{x\in\mathbb{Z}\,|\,x\mathcal{R}y\}=\{x\in\mathbb{Z}\,|\,x-y\text{ est divisible par }n\}=\{x\in\mathbb{Z}\,|\,\exists k\in\mathbb{Z}\,x-y=kn\}$$
Alors, pour tout $x\in\mathbb{Z}$, si on désigne par q le quotient et par r le reste de la division euclidienne de x par n, on a $x=qn+r$ et donc $\overline{x}=\overline{r}$. Il y a donc au plus autant de classes d'équivalence que de restes possibles dans la division euclidienne par n. C'est-à-dire n. On constate maintenant que si $0\leq r<r'\leq n-1$ sont deux restes possibles de la division euclidienne par n alors $0<r'-r\leq n-1$, ce qui prouve l'impossibilité de trouver $k\in\mathbb{Z}$ tel que $r'-r=kn$, et montre que $\overline{r'}\neq\overline{r}$. Il y a donc autant de classes d'équivalence que de restes possibles dans la division euclidienne par n. L'ensemble de ces classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$. On a donc $\mathbb{Z}/n\mathbb{Z}=\{\overline{r}\,|\,r\in[\![0,n-1]\!]\}$.

Considérons par exemple le cas où $n=3$. L'ensemble $\mathbb{Z}/3\mathbb{Z}$ compte trois éléments, à savoir $\overline{0}$, $\overline{1}$ et $\overline{2}$. Si a est un entier quelconque, pour savoir auquel de ces trois éléments la classe $\overline{a}$ est égale, on calcule le reste de la division euclidienne de a par 3. Par exemple, $581=3\times193+2$, et donc $\overline{581}=\overline{2}$; et $(-47)=3\times(-16)+1$, d'où l'égalité $\overline{(-47)}=\overline{1}$.

Nous munirons $\mathbb{Z}/n\mathbb{Z}$ d'une addition dans l'Exemple 1.1.17, puis nous verrons Exemple 1.3.11 que $\mathbb{Z}/n\mathbb{Z}$ muni de cette addition est un groupe, enfin nous l'étudierons en détails dans le Chapitre 4.

Exemple 1.1.8. — Notons $\mathcal{S}$ l'ensemble des suites de nombres complexes. On dit que $(x_n)\in\mathcal{S}$ est équivalente à $(y_n)\in\mathcal{S}$ s'il existe $(r_n)\in\mathcal{S}$ qui converge vers 1, et $N\in\mathbb{N}$ tels que pour tout entier $n\geq N$ on ait $x_n=r_ny_n$. Il s'agit d'une relation d'équivalence. En effet, elle est

- ◇ réflexive : avec $r_n=1$ pour tout n on a $x_n=r_nx_n$.
- ◇ symétrique : soient $N\in\mathbb{N}$ et (r_n) convergeant vers 1 tels que pour tout $n\geq N$ on a $x_n=r_ny_n$. Puisque (r_n) converge vers 1, la suite $\left(\dfrac{1}{r_n}\right)=(q_n)$ est bien définie à partir d'un certain rang N_1 et elle converge vers 1. Pour $n\geq\max(N,N_1)$ on a : $y_n=q_nx_n$, ce qui nous indique que (y_n) est équivalente à (x_n).
- ◇ transitive : soient (x_n) une suite équivalente à (y_n) elle-même équivalente à (z_n). Il existe $(N_1,N_2)\in\mathbb{N}\times\mathbb{N}$ et $(r_n)\in\mathcal{S}$ et $(s_n)\in\mathcal{S}$, toutes deux convergeant vers 1, tels que pour $n\geq\max(N_1,N_2):=N$ on a $x_n=r_ny_n$ et $y_n=s_nz_n$. On a alors, pour $n\geq N$,

$x_n = r_n s_n z_n$. La suite $(r_n s_n)$ converge vers 1 ce qui permet de conclure que (x_n) est équivalente à (z_n).

Exemple 1.1.9. — Étant donnés deux ensembles E_1 et E_2 munis respectivement des relations d'équivalence $\mathcal{R}_1$ et $\mathcal{R}_2$, on définit sur le produit cartésien $E_1 \times E_2$ une relation d'équivalence $\mathcal{R}$ en posant pour $(x, y) \in E_1 \times E_2$ et $(x', y') \in E_1 \times E_2$:

$$(x, y)\mathcal{R}(x', y') \Longleftrightarrow x\mathcal{R}_1 x' \quad \text{et} \quad y\mathcal{R}_2 y'.$$

On peut vérifier que $\overline{(x, y)} = \overline{x} \times \overline{y}$.

Exemple 1.1.10. — Dans $E = \mathbb{N} \times \mathbb{N}$, $(a, b)\mathcal{R}(a', b') \Longleftrightarrow a + b' = a' + b$ est une relation d'équivalence. En effet, la relation $\mathcal{R}$ est

- ◇ réflexive : pour tout (a, b) dans E, nous avons $a + b = a + b$, *i.e.* $(a, b)\mathcal{R}(a, b)$;
- ◇ symétrique : soient (a, b) et (a', b') dans E tels que $(a, b)\mathcal{R}(a', b')$, c'est-à-dire tels que $a + b' = a' + b$. Or $a + b' = a' + b$ se réécrit $a' + b = a + b'$ donc $(a', b')\mathcal{R}(a, b)$.
- ◇ transitive : soient (a, b), (a', b') et (a'', b'') dans E tels que $(a, b)\mathcal{R}(a', b')$ et $(a', b')\mathcal{R}(a'', b'')$. Alors d'une part $a + b' = b + a'$ et d'autre part $a' + b'' = a'' + b'$; nous en déduisons que

$$a + b'' = \underbrace{a + b'}_{b+a'} - b' + b'' = b + a' - b' + b'' = b - b' + \underbrace{a' + b''}_{a''+b'} = b - b' + a'' + b' = a'' + b$$

c'est-à-dire que $(a, b)\mathcal{R}(a'', b'')$.

La classe $\overline{(a, b)}$ de (a, b) est par définition le nombre relatif $a - b$. En effet, par définition

$$\begin{aligned} \overline{(a, b)} &= \{(a', b') \in E \,|\, (a', b')\mathcal{R}(a, b)\} = \{(a', b') \in E \,|\, a' + b = a + b'\} \\ &= \{(a', b') \in E \,|\, a' - b' = a - b\} \end{aligned}$$

Lorsque l'on construit les ensembles de nombres, cette manière de « symétriser » l'addition de $\mathbb{N}$ permet, partant de $\mathbb{N}$, de construire l'ensemble $\mathbb{Z}$. On a en effet très envie d'identifier la classe de (a, b) avec l'entier relatif $a - b$. On fait en réalité le contraire en définissant $(a - b)$ comme la classe de (a, b). Il faut alors définir une addition naturelle sur l'ensemble des classes d'équivalence, ce que l'on détaillera plus tard.

Ne pas oublier de compléter après l'introduction de l'ensemble quotient...

Exemple 1.1.11. — Dans $E = \mathbb{Z} \times \mathbb{Z}^*$, $(p, q)\mathcal{R}(p', q') \Longleftrightarrow pq' = p'q$ est une relation d'équivalence. On vérifie en effet qu'elle est :

- ◇ réflexive : pour tout (p, q) dans E, nous avons $pq = pq$, *i.e.* $(p, q)\mathcal{R}(p, q)$;
- ◇ symétrique : soient (p, q) et (p', q') dans E tels que $(p, q)\mathcal{R}(p', q')$. C'est-à-dire tels que $pq' = p'q$. Cela se réécrit $p'q = pq'$ donc $(p', q')\mathcal{R}(p, q)$.
- ◇ transitive : soient (p, q), (p', q') et (p'', q'') dans E tels que $(p, q)\mathcal{R}(p', q')$ et $(p', q')\mathcal{R}(p'', q'')$. Alors d'une part $pq' = p'q$ et d'autre part $p'q'' = p''q'$; nous en déduisons que

$$\underbrace{pq'}_{p'q} q'' = p'qq'' = q\underbrace{p'q''}_{p''q'} = qp''q' = p''qq'$$

soit $pq'' = p''q$ (car q' appartient à $\mathbb{Z}^*$), *i.e.* $(p,q)\mathcal{R}(p'',q'')$.

La classe $\overline{(p,q)}$ de (p,q) est par définition le nombre rationnel $\frac{p}{q}$. En effet, par définition

$$\begin{aligned}\overline{(p,q)} &= \{(p',q') \in E \,|\, (p',q')\mathcal{R}(p,q)\} = \{(p',q') \in E \,|\, pq' = p'q\} \\ &= \left\{(p',q') \in E \,|\, \frac{p'}{q'} = \frac{p}{q}\right\}\end{aligned}$$

C'est la multiplication sur $\mathbb{Z}$ que l'on « symétrise » cette fois et partant de $\mathbb{Z}$ on construit l'ensemble $\mathbb{Q}$ en définissant $\frac{p}{q}$ comme la classe de (p,q). Il convient ensuite de munir l'ensemble des classes d'équivalence d'une addition et d'une multiplication.

Ces deux derniers exemples illustrent la puissance des relations d'équivalence qui permettent de formaliser certaines idées de manière très efficace.

Proposition 1.1.1

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Alors

- ◇ pour tout $a \in E$, $a \in \overline{a}$;
- ◇ pour tous a, $b \in E$ nous avons l'équivalence : $a\mathcal{R}b \Longleftrightarrow \overline{a} = \overline{b}$;
- ◇ pour tous a, $b \in E$, si $\overline{a} \neq \overline{b}$, alors $\overline{a} \cap \overline{b} = \emptyset$.

Démonstration. — Soient a, b dans E.

- ◇ Puisque d'après (i) nous avons $a\mathcal{R}a$, nous obtenons : $a \in \overline{a}$.
- ◇ Supposons que $a\mathcal{R}b$. Pour tout $z \in \overline{a}$ nous avons $z\mathcal{R}a$; puisque par hypothèse $a\mathcal{R}b$, nous obtenons par transitivité $z\mathcal{R}b$. En particulier z appartient à $\overline{b}$. Ceci montre que $\overline{a} \subset \overline{b}$. Comme $a\mathcal{R}b$ nous avons par symétrie $b\mathcal{R}a$; de la même façon que précédemment nous obtenons que $\overline{b} \subset \overline{a}$. Ainsi $\overline{a} = \overline{b}$.

  Réciproquement, si $\overline{a} = \overline{b}$, alors a qui appartient à $\overline{a}$ appartient aussi à $\overline{b}$ et donc $a\mathcal{R}b$.
- ◇ Montrons la dernière assertion en raisonnant par contraposée. Supposons que $\overline{a} \cap \overline{b} \neq \emptyset$. Soit donc z dans $\overline{a} \cap \overline{b}$. Puisque z appartient à $\overline{a}$ (resp. $\overline{b}$), $z\mathcal{R}a$ (resp. $z\mathcal{R}b$). Par symétrie $a\mathcal{R}z$. Par transitivité $a\mathcal{R}z$ et $z\mathcal{R}b$ conduisent à $a\mathcal{R}b$, soit $\overline{a} = \overline{b}$.

□

Remarquons que E est la réunion des classes d'équivalence car tout élément a de E appartient à $\overline{a}$. Nous en déduisons l'énoncé suivant :

Proposition 1.1.2

Étant donnée une relation d'équivalence sur E, les classes d'équivalence forment une partition de E.

Réciproquement, et comme nous l'avons déjà indiqué à la fin du paragraphe sur les partitions (§1.1.1.1), si on se donne une partition $(C_i)_{i\in I}$ de E, alors la relation définie par $a\mathcal{R}b \iff (\exists\, i \in I$ tel que $a,\, b \in C_i)$ est une relation d'équivalence dont les classes sont les C_i. Ainsi relation d'équivalence et partition sont deux points de vue différents d'un même concept.

1.1.1.3. *Relation d'équivalence définie par une application.* — Soit $f\colon E \to F$ une application entre deux ensembles. Définissons une relation $\mathcal{R}_f$ sur E en posant

$$\forall\, x,\, y \in E,\ x\mathcal{R}_f y \iff f(x) = f(y).$$

Cette relation est réflexive, symétrique et transitive. En effet

- ◇ si $x \in E$, alors $f(x) = f(x)$, c'est-à-dire $x\mathcal{R}x$;
- ◇ si x, y sont deux éléments de E tels que $x\mathcal{R}y$, alors $f(x) = f(y)$ d'où $f(y) = f(x)$ et $y\mathcal{R}x$;
- ◇ si x, y et z sont des éléments de E tels que $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $f(x) = f(y)$ et $f(y) = f(z)$; nous en déduisons que $f(x) = f(z)$, c'est-à-dire $x\mathcal{R}z$.

Définition 1.1.3

Soit $f\colon E \to F$ une application. La relation d'équivalence $\mathcal{R}_f$ définie par

$$\forall\, x,\, y \in E,\ x\mathcal{R}_f\, y \iff f(x) = f(y)$$

s'appelle la *relation d'équivalence définie par* f.

Pour tout $a \in E$, la classe de a est $\overline{a} = \{x \in E \mid f(x) = f(a)\} = f^{-1}(f(a))$.

Exemple 1.1.12. — Soit O un point du plan euclidien E et soit $f\colon E \to \mathbb{R}$, la fonction qui à M associe la distance OM de O à M. La relation d'équivalence associée à f est

$$\forall\, M,\, M' \in E,\ M\mathcal{R}_f M' \iff OM = OM'.$$

La classe d'équivalence d'un point $A \in E$ est formée des points M qui sont à la même distance de O que A :

$$\overline{A} = \{M \in E \mid M\mathcal{R}_f\} = \{M \in E \mid OM = OA\}$$

Ainsi :

- ◇ si $A \neq O$, alors $\overline{A}$ est le cercle de centre O passant par A,
- ◇ $\overline{O} = \{O\}$.

Exemple 1.1.13. — Soient E et F deux espaces vectoriels et $f\colon E \to F$ une application linéaire. Si x et y sont dans E, alors

$$x\mathcal{R}_f\, y \iff f(x) = f(y) \iff f(x) - f(y) = 0_F \iff f(x - y) = 0_F.$$

Autrement dit on a $x\mathcal{R}_f\, y \iff (x - y) \in \ker f$.

1.1.2. Ensemble quotient. —

Définitions 1.1.2

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E.

- ◇ L'ensemble des classes d'équivalence s'appelle l'*ensemble quotient* de E par $\mathcal{R}$ et se note $E/\mathcal{R}$.
- ◇ L'application $p\colon E \to E/\mathcal{R}$ définie par $p(x) = \overline{x}$ s'appelle la *projection canonique*.
- ◇ Étant donnée une classe d'équivalence $\overline{a}$ tout élément $x \in \overline{a}$ s'appelle un *représentant* de cette classe.

Proposition 1.1.3

- ◇ L'application p est surjective : $\forall\, \alpha \in E/\mathcal{R}$, $\exists\, a \in E$, $\alpha = p(a)$.
- ◇ La relation $\mathcal{R}$ est la relation d'équivalence définie par p :

$$\forall\, x,\, y \in E,\ p(x) = p(y) \Leftrightarrow x\mathcal{R}y.$$

Démonstration. —

- ◇ Toute classe $\alpha \in E/\mathcal{R}$ est la classe d'au moins un élément $a \in E$: $\alpha = \overline{a}$, donc $\alpha = p(a)$.
- ◇ Pour tous x, $y \in E$, nous avons $x\mathcal{R}y \iff \overline{x} = \overline{y} \iff p(x) = p(y)$ donc $\mathcal{R}$ est la relation d'équivalence définie par l'application p.

□

Toute relation d'équivalence sur E est donc définie par une application : la projection canonique $E \to E/\mathcal{R}$.

Exemple 1.1.14. — Considérons la relation sur $\mathbb{R}^*$ définie par $x\mathcal{R}y \iff xy > 0$: C'est une relation d'équivalence car :

- elle est réflexive : pour tout x dans $\mathbb{R}^*$ on a $x^2 > 0$, *i.e.* $xx > 0$, c'est-à-dire $x\mathcal{R}x$;
- elle est symétrique : pour tous x, y dans $\mathbb{R}^*$ tels que $x\mathcal{R}y$, *i.e.* tels que $xy > 0$, alors $yx > 0$, c'est-à-dire $y\mathcal{R}x$;
- elle est transitive : pour tous x, y, z dans $\mathbb{R}^*$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$, *i.e.* tels que $xy > 0$ et $yz > 0$, alors $xy^2z > 0$ et comme $y^2 > 0$, $xz > 0$, c'est-à-dire $x\mathcal{R}z$.

La relation $\mathcal{R}$ est la relation d'équivalence définie par l'application $\mathrm{sgn}\colon \mathbb{R}^\times \to \{1, -1\}$ qui à tout $x \in \mathbb{R}^\times$ associe son signe (avec l'abus de notation 1 pour $\overline{1}$ et -1 pour $\overline{-1}$).

Il y a deux classes : $\overline{1} = \mathbb{R}^{\times +}$ et $\overline{-1} = \mathbb{R}^{\times -}$. L'ensemble quotient $\mathbb{R}^\times/\mathcal{R}$ est donc formé de deux éléments : $\mathbb{R}^\times/\mathcal{R} = \{\overline{-1}, \overline{1}\}$.

1.1.3. Passage au quotient d'une application (**). — Comme nous l'avons vu

- ◇ la notion de relation d'équivalence sur un ensemble X est l'outil qui permet en pratique d'identifier les éléments de X partageant une certaine propriété (les rendant « équivalents ») ;
- ◇ la donnée d'une telle relation sur X définit une partition naturelle de X en classes d'équivalence ;
- ◇ l'ensemble de ces classes, un sous-ensemble de l'ensemble de toutes les parties de X, est appelé ensemble quotient de X par $\mathcal{R}$, et il est noté $X/\mathcal{R}$.

Sa propriété principale (dite « universelle ») est qu'une application $f\colon X \to Y$ constante sur les classes d'équivalence de $\mathcal{R}$ se factorise canoniquement en une application $\widetilde{f}\colon X/\mathcal{R} \to Y$, appelée passage au quotient de f (*voir* Théorème 1.1.1).

Exemple 1.1.15. — Pour comprendre les enjeux du problème considérons un premier exemple.

Soit $n > 0$ un entier quelconque. Soit E un ensemble. Soit f une application de $\mathbb{Z}$ dans E. Peut-on définir une application de $\mathbb{Z}/n\mathbb{Z}$ dans E par la formule $\overline{a} \mapsto f(a)$? La réponse est non en général. Donnons deux exemples :

- ◇ Considérons l'application $\sin\colon \mathbb{Z} \to \mathbb{R}$. Elle ne passe pas au quotient modulo 2. En effet $\overline{0} = \overline{2}$ mais $\sin(0) \neq \sin(2)$. Nous ne pouvons donc pas définir d'application de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{R}$ par la formule $\overline{a} \mapsto \sin(a)$ (si elle existait une telle application devrait envoyer $\overline{0} = \overline{2}$ à la fois sur $\sin 0$ et $\sin 2$ ce qui est impossible puisque $\sin 0 \neq \sin 2$).
- ◇ Considérons l'application $f\colon \mathbb{Z} \to \mathbb{R}$, $a \mapsto (-1)^a$. Elle passe au quotient modulo 2. En effet si a et b sont deux entiers tels que $b-a$ soit pair, alors $(-1)^a = (-1)^{a+(b-a)} = (-1)^b$. Par suite f induit une application de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{R}$ donnée par la formule $\overline{a} \mapsto (-1)^a$. Cette application envoie $\overline{0}$ sur $(-1)^0$ et $\overline{1}$ sur $(-1)^1 = -1$.

Le souci survient dès qu'il existe deux éléments distincts a et b de $\mathbb{Z}$ tels que $\overline{a} = \overline{b}$ et $f(a) \neq f(b)$. Si cette situation ne se présente pas, c'est-à-dire si $f(a) = f(b)$ dès que $\overline{a} = \overline{b}$, on dit que f *passe au quotient modulo* n. Si f passe au quotient, alors la formule $\overline{a} \mapsto f(a)$ définit bien une application de $\mathbb{Z}/n\mathbb{Z}$ dans E que nous qualifierons d'application *induite* par f.

Exemple 1.1.16. — Reprenons la relation de l'Exemple 1.1.6 de congruence modulo 2π. Étant donné $\vartheta \in [0, 2\pi[$ on note $\overline{\vartheta} := \{\vartheta + 2n\pi,\ n \in \mathbb{Z}\}$ sa classe d'équivalence. On a alors $E/\mathcal{R} = \bigcup_{\vartheta \in \mathbb{R}} \overline{\vartheta}$. Considérons les fonctions $f\colon x \mapsto \cos(x)$ et $g\colon x \mapsto x+1$. Il est très tentant de définir « naïvement » $\overline{f}\colon E/\mathcal{R} \to \mathbb{R}$ et $\overline{g}\colon E/\mathcal{R} \to \mathbb{R}$ en posant tout simplement $\overline{f}(\overline{\vartheta}) = f(\vartheta)$ et $\overline{g}(\overline{\vartheta}) = g(\vartheta)$. Mais si cela a du sens pour $\overline{f}$, cela n'en a aucun pour $\overline{g}$. En effet, pour tout $k \in \mathbb{Z}$ on a $\overline{\vartheta} = \overline{\vartheta + 2k\pi}$ alors $f(\vartheta) = \cos(\vartheta) = \cos(\vartheta + 2k\pi) = f(\vartheta + 2k\pi)$, par contre, si $k \neq 0$, $g(\vartheta) = \vartheta + 1 \neq \vartheta + 2k\pi + 1 = g(\vartheta + 2k\pi)$. La définition « naturelle » a donc un sens pour f, qui est constante sur les classes d'équivalence, mais aucun pour g, qui ne l'est pas.

L'énoncé suivant permet de définir des applications sur un ensemble quotient :

Théorème 1.1.1: (Factorisation canonique d'une application)

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Soit $p\colon E \to {}^{E}\!/_{\mathcal{R}}$ la projection canonique. Soit $f\colon E \to F$ une application entre deux ensembles.
Pour qu'il existe une application $\widetilde{f}\colon {}^{E}\!/_{\mathcal{R}} \to F$ telle que $\widetilde{f} \circ p = f$ il faut et il suffit que $\forall\, x,\, y \in E,\ x\mathcal{R}y \Longrightarrow f(x) = f(y)$.
Dans ce cas

- $\widetilde{f}$ est unique et pour toute classe $\alpha \in {}^{E}\!/_{\mathcal{R}}$ nous avons $\widetilde{f}(\alpha) = f(a)$ pour tout représentant a de α ;
- $\widetilde{f}$ est injective si et seulement si $\forall\, x,\, y \in E,\ x\mathcal{R}y \Longleftrightarrow f(x) = f(y)$;
- les applications f et $\widetilde{f}$ ont la même image.

Si l'application $\widetilde{f}$ existe, nous disons que f *passe au quotient modulo* $\mathcal{R}$ et $\widetilde{f}$ s'appelle la *factorisation* de f par ${}^{E}\!/_{\mathcal{R}}$:

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[d, "p"'] & F \\ {}^{E}\!/_{\mathcal{R}} \arrow[ur, "\widetilde{f}"'] & \end{tikzcd}$$

Démonstration. —

- Supposons qu'il existe $\widetilde{f}\colon {}^{E}\!/_{\mathcal{R}} \to F$ telle que $f = \widetilde{f} \circ p$. Si $x,\, y \in E$ sont tels que $x\mathcal{R}y$, alors $p(x) = p(y)$, donc $f(x) = \widetilde{f}(p(x)) = \widetilde{f}(p(y)) = f(y)$.

  Réciproquement supposons que pour tous $x,\, y \in E$, nous ayons la propriété : $x\mathcal{R}y \Longrightarrow f(x) = f(y)$. Si $\alpha \in {}^{E}\!/_{\mathcal{R}}$, alors pour tous représentants $a,\, a'$ de α nous avons $a'\mathcal{R}a$ donc $f(a) = f(a')$: l'application f prend la même valeur sur tous les représentants de α. Nous pouvons donc poser $\widetilde{f}(\alpha) = f(a)$ où a est un représentant quelconque de α. Nous définissons ainsi une application $\widetilde{f}\colon {}^{E}\!/_{\mathcal{R}} \to F$ telle que $\widetilde{f}(p(a)) = f(a)$ quel que soit $a \in E$.

- Supposons que $\widetilde{f}$ soit injective. Soient $x,\, y \in E$ tels que $f(x) = f(y)$. Alors $\widetilde{f}(p(x)) = \widetilde{f}(p(y))$ donc $p(x) = p(y)$ et par suite $x\mathcal{R}y$.

  Réciproquement, supposons que pour tous $x,\, y \in E$ nous avons $x\mathcal{R}y \Longleftrightarrow f(x) = f(y)$. Soient α et β des éléments de ${}^{E}\!/_{\mathcal{R}}$ tels que $\widetilde{f}(\alpha) = \widetilde{f}(\beta)$. Puisque p est surjective il existe $a,\, b$ dans E tels que $\alpha = p(a)$ et $\beta = p(b)$; alors $\widetilde{f}(\alpha) = \widetilde{f}(\beta)$ se réécrit $\widetilde{f}(p(a)) = \widetilde{f}(p(b))$ et $f(a) = f(b)$. Par conséquent $a\mathcal{R}b$ et $\alpha = \beta$: l'application $\widetilde{f}$ est donc injective.

- Puisque $f = \widetilde{f} \circ p$ nous avons $f(E) = \widetilde{f}(p(E)) = \widetilde{f}\left({}^{E}\!/_{\mathcal{R}}\right)$ car p est surjective.

$\square$

Exemple 1.1.17. — Appliquons ce résultat pour définir, comme annoncé dans l'Exemple 1.1.7, une addition sur $\mathbb{Z}/n\mathbb{Z}$. On considère donc l'ensemble $\mathbb{Z}\times\mathbb{Z}$ que l'on munit de la relation de congruence modulo n sur le produit cartésien comme dans l'Exemple 1.1.9 : $(x,y)\mathcal{R}(x',y')$ si et seulement si $x\equiv_n x'$ et $y\equiv_n y'$. Nous avons vu dans l'Exemple 1.1.9 que l'ensemble quotient $\mathbb{Z}\times\mathbb{Z}/\mathcal{R}$ était le produit cartésien des ensembles quotients, en l'occurence : $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$.

Considérons à présent l'addition modulo n, notée f, définie pour $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ par $f(x,y)=\overline{x+y}$, où $\overline{z}$ désigne la classe de z dans $\mathbb{Z}/n\mathbb{Z}$.

Montrons que cette application passe au quotient. Soient $(x,y)\mathcal{R}(x',y')$ deux éléments de $\mathbb{Z}\times\mathbb{Z}$ en relation pour $\mathcal{R}$. On a donc $x\equiv_n x'$ et $y\equiv_n y'$. Autrement dit, il existe k et p dans $\mathbb{Z}$ tels que $x-x'=kn$ et $y-y'=pn$. On a donc $(x+y)-(x'+y')=(k+p)n$. Soit $\overline{x+y}=\overline{x'+y'}$, ou encore $f(x,y)=f(x',y')$. L'application f passe au quotient, elle possède donc une factorisation $\tilde{f}$ définie pour $(\overline{x},\overline{y})\in\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ par : $\tilde{f}(\overline{x},\overline{y})=\overline{x+y}$. Ce qui peut se réécrire : $\overline{x}+\overline{y}=\overline{x+y}$.

En appliquant le Théorème 1.1.1 à la relation $\mathcal{R}_f$ définie par f, nous obtenons l'énoncé très utile suivant.

Corollaire 1.1.1: (Factorisation canonique d'une application)

Soit $f\colon E\to F$. Notons $\mathcal{R}_f$ la relation d'équivalence et $p\colon E\to E/\mathcal{R}_f$ la projection canonique asociées.

- ◇ Il existe une unique application $\widetilde{f}\colon E/\mathcal{R}_f\to F$ telle que $\widetilde{f}\circ p=f$.
- ◇ L'application $\widetilde{f}$ est injective.
- ◇ L'application $\widetilde{f}$ est bijective si et seulement si l'application f est surjective.

Démonstration. — Dans le Théorème 1.1.1, prenons $\mathcal{R}_f$ comme relation d'équivalence sur E. Pour tous x, $y\in E$ nous avons alors les deux implications

$$x\mathcal{R}_f y\Longrightarrow f(x)=f(y)\qquad\qquad f(x)=f(y)\Longrightarrow x\mathcal{R}_f y$$

donc f passe au quotient modulo $\mathcal{R}_f$ et l'application $\widetilde{f}$ est injective. Par suite l'application $\widetilde{f}$ est bijective si et seulement si elle est surjective, c'est-à-dire si et seulement si f est surjective car f et $\widetilde{f}$ ont même image. □

Exemple 1.1.18. — Reprenons un exemple introduit précédemment. Soit O un point du plan euclidien E et soit $f\colon E\to\mathbb{R}$, la fonction qui à M associe OM. La relation d'équivalence associée à f est

$$\forall\, M,\, M'\in E,\ M\mathcal{R}_f M'\Longleftrightarrow OM=OM'.$$

L'ensemble quotient $E/\mathcal{R}_f$ est l'ensemble des cercles de centre O. L'application $\widetilde{f}\colon E/\mathcal{R}_f\to\mathbb{R}$ est définie comme suit : pour tout cercle $C\in E/\mathcal{R}_f$ $\widetilde{f}(C)=OM$ où M est un point quelconque

de C. Autrement dit, pour tout cercle C de centre O, $\widetilde{f}(C)$ est le rayon de C. Cette application est bien injective.

Pour qu'une application $g\colon E \to \mathbb{R}$ passe au quotient il faut et il suffit que pour tous M, $M' \in E$ nous ayons la propriété suivante : $OM = OM' \Rightarrow g(M) = g(M')$: cette propriété signifie que pour tout $M \in E$, $g(M)$ ne dépend que de la distance OM.

Exemple 1.1.19. — Dans l'ensemble $E = \mathbb{Z} \times \mathbb{N}^*$ définissons la relation

$$\forall\,(x,y),\ (x',y') \in E,\ (x,y)\mathcal{R}(x',y') \Longleftrightarrow xy' - x'y = 0.$$

C'est une relation d'équivalence (à vérifier en exercice [1]).

Soit $f\colon E \to \mathbb{Q}$ l'application définie par $f(x,y) = \frac{x}{y}$. Pour tous (x,y), (x',y') dans E nous avons

$$(x,y)\mathcal{R}(x',y') \Longleftrightarrow xy' = x'y \Longleftrightarrow \frac{x}{y} = \frac{x'}{y'} \Longleftrightarrow f(x,y) = f(x',y').$$

Ainsi $\mathcal{R}$ est la relation définie par f.

En appelant $p\colon E \to {}^{E}\!/_{\mathcal{R}}$ la projection canonique, il existe donc une application injective $\widetilde{f}\colon E \to {}^{E}\!/_{\mathcal{R}} \to \mathbb{Q}$ telle que $\widetilde{f} \circ p = f$. L'application f est surjective car tout nombre rationnel s'écrit $\frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ et $f(a,b) = \frac{a}{b}$. Par conséquent l'application $\widetilde{f}$ est bijective.

L'ensemble quotient ${}^{E}\!/_{\mathcal{R}}$ est une construction de $\mathbb{Q}$ à partir des ensembles $\mathbb{N}$ et $\mathbb{Z}$.

1.2. Groupes

Définition 1.2.1

Soit E un ensemble. Une *loi de composition interne* dans E est une application $\mu\colon E \times E \to E$. Notons cette loi $*$; on a $\mu(a,b) = a * b$.

Une loi peut vérifier certaines des propriétés suivantes :

- associativité : on a
$$\forall\, a,\ b,\ c \in E \qquad a * (b * c) = (a * b) * c;$$
- commutativité : on a
$$\forall\, a,\ b \in E \qquad a * b = b * a.$$
- existence d'un *élément neutre à droite*, *à gauche*, d'un *élément neutre* : l'élément $e \in E$ est neutre à droite si $x * e = x$ pour tout $x \in E$, neutre à gauche si $e * x = x$ pour tout $x \in E$, neutre si $x * e = e * x = x$ pour tout $x \in E$. Lorsque la loi admet un élément neutre on dit qu'elle est *unitaire*.

1. On peut ensuite relire l'Exemple 1.1.11...

- ⋄ lorsqu'il y a un élément neutre il existe des symétriques à droite et à gauche. L'élément $a' \in E$ est *symétrique* de a à *droite* si $a * a' = e$. L'élément $a' \in E$ est *symétrique* de a à *gauche* si $a' * a = e$. L'élément $a' \in E$ est *symétrique* de a si $a * a' = a' * a = e$.

Si une loi admet un élément neutre, il est unique. Si une loi admet un élément neutre à droite et un élément neutre à gauche, ces deux éléments neutres sont égaux et la loi est unitaire.

Si une loi est associative et unitaire, si a' est symétrique à droite de $a \in E$ et si a'' est symétrique à gauche de ce même élément a, alors $a' = a''$. En particulier si la loi est associative et unitaire on peut parler, lorsqu'il existe, du symétrique de $a \in E$.

Un élément a de E est dit *régulier à gauche* pour la loi $*$ si pour tout x et tout y dans E on a

$$a * x = a * y \quad \Longleftrightarrow x = y.$$

Un élément a de E est dit *régulier à droite* pour la loi $*$ si pour tout x et tout y dans E on a

$$x * a = y * a \quad \Longleftrightarrow x = y.$$

Exemple 1.2.1. — L'addition sur $\mathbb{Z}$ est une loi de composition interne : $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(x, y) \mapsto x + y$. Elle est associative, commutative, admet 0 pour élément neutre et tout élément k de $\mathbb{Z}$ admet $-k$ pour symétrique.

Exemple 1.2.2. — La soustraction sur $\mathbb{Z}$ est une loi de composition interne : $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(x, y) \mapsto x - y$. Elle est associative, commutative, admet 0 pour élément neutre et tout élément k de $\mathbb{Z}$ admet k pour symétrique.

Exemple 1.2.3. — La soustraction sur $\mathbb{N}$ n'est pas une loi de composition interne : alors que 2 et 5 appartiennent à $\mathbb{N}$, $2 - 5$ n'appartient pas à $\mathbb{N}$.

Exemple 1.2.4. — La multiplication sur $\mathbb{R}$ est une loi de composition interne : $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(x, y) \mapsto xy$. Elle est associative, commutative, admet 1 pour élément neutre et tout élément x de $\mathbb{R}^\times$ admet $\frac{1}{x}$ pour symétrique.

Exemple 1.2.5. — Soit X un ensemble. Sur $\mathcal{P}(X)$ la réunion $\mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$, $(A, B) \mapsto A \cup B$ est une loi de composition interne qui est associative et commutative. Elle admet $\emptyset$ comme élément neutre et le seul élément ayant un symétrique est $\emptyset$ (son symétrique est $\emptyset$).

Exemple 1.2.6. — Soit X un ensemble. Sur $\mathcal{P}(X)$ l'intersection $\mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$, $(A, B) \mapsto A \cap B$ est une loi de composition interne qui est associative et commutative. Elle admet X comme élément neutre et le seul élément ayant un symétrique est X (son symétrique est X).

Exemple 1.2.7. — Soit X un ensemble. Sur $\mathcal{P}(X)$ la différence symétrique $\mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$, $(A, B) \mapsto A \Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) = (A \cap B^c) \cup (B \cap A^c)$ est une loi de composition interne.

Elle possède $\emptyset$ comme élément neutre et tout élément $A \subset X$ admet A^c comme symétrique.

Exemple 1.2.8. — Soit X un ensemble. Soit $E = \mathcal{F}(X)$ l'ensemble des applications de X dans X. La composition des applications $E \times E \to E$, $(f, g) \mapsto f \circ g$ est une loi de composition interne.

La fonction identité est l'élément neutre. Seules les bijections admettent un symétrique qui est la bijection réciproque.

Exemple 1.2.9. — L'addition sur $\mathbb{R}^2$: $\mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$, $\big((x, y), (x', y')\big) \mapsto \big((x + x', y + y')\big)$ est une loi de composition interne.

Son élément neutre est $(0, 0)$, le symétrique de (x, y) est $(-x, -y)$.

Exemple 1.2.10. — La multiplication par un scalaire $\mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2$, $\big(\lambda, (x, y)\big) \mapsto \big(\lambda x, \lambda y\big)$ n'est pas une loi de composition interne.

Définitions 1.2.1

Étant donnés un ensemble G avec une loi de composition interne $*$, le couple $(\mathrm{G}, *)$ est un *groupe* si $*$ est associative, si elle possède un élément neutre e et si chaque élément de G possède un symétrique.
Si la loi $*$ est commutative, alors G est un groupe *commutatif* ou *abélien*.
Si le groupe G est réduit à son élément neutre, c'est-à-dire si $\mathrm{G} = \{e\}$, on dit que le groupe est *trivial*.

Le terme abélien fait référence au mathématicien norvégien Niels Henrik Abel (1802-1829).

Remarque 1.2.1. — En toute rigueur, nous devrions donc écrire « soit $(\mathrm{G}, *)$ un groupe » et non « soit G un groupe ». Respecter ce principe conduirait à alourdir la rédaction, et nous nous en affranchissons donc le plus souvent ; mais il faut garder en tête que nous commettons un petit abus, pour les rares cas où il pourrait y avoir une ambiguïté sur la loi de groupe.

Lorsque $(\mathrm{G}, \cdot)$ est un groupe fini, il est possible de créer un tableau qui présente, pour tous les éléments g et h de G, les résultats obtenus par cette loi : à l'intersection de la ligne représentant g et de la colonne représentant h se trouve $g \cdot h$. Le tableau à double entrée ainsi construit est appelé *table de Cayley* (voir 1.3.13 pour le premier exemple). Ces tableaux sont nommés ainsi en l'honneur du mathématicien Arthur Cayley. La donnée d'une telle table équivaut à celle de la structure du groupe qu'elle représente. Tous les éléments d'une ligne ou d'une colonne donnée dans la table de Cayley d'un groupe fini sont représentés exactement une fois. La table donne bien évidemment l'inverse de chaque élément : si $g \cdot h = e$ alors h est l'inverse de g pour la loi $\cdot$. À noter qu'un groupe fini est abélien si et seulement si sa table de Cayley est symétrique par rapport à la diagonale principale.

On adopte pour la loi du groupe considéré soit une notation *additive* ($x*y = x+y$), soit une notation *multiplicative* ($x*y = xy$). Lorsque le groupe n'est pas abélien on utilise uniquement la notation multiplicative.

Notation additive : l'élément neutre est noté 0, l'élément symétrique de g s'appelle son opposé et est noté $-g$, la « somme »

$$\underbrace{g+g+\ldots+g}_{n \text{ fois}}$$

est notée ng. Pour $n \in \mathbb{Z} \smallsetminus \mathbb{N}$ on a $ng = (-n)(-g)$.

Notation multiplicative : l'élément neutre est noté 1, l'élément symétrique de g s'appelle son inverse et est noté g^{-1}, le « produit »

$$\underbrace{g \cdot g \cdot \ldots \cdot g}_{n \text{ fois}}$$

est noté g^n. Pour $n \in \mathbb{Z} \smallsetminus \mathbb{N}$ on a $g^n = (g^{-1})^{-n}$.

1.3. Premiers exemples

***Exemple 1.3.1* (Le groupe $\mathbb{Z}$).** — L'ensemble $\mathbb{Z}$ des entiers relatifs, muni de l'addition, est un groupe abélien. L'élément neutre est 0 et le symétrique d'un élément est son opposé.

Lorsque nous parlerons du groupe $\mathbb{Z}$, il sera désormais toujours sous-entendu que sa loi de composition interne est l'addition.

***Exemple 1.3.2* (Les groupes $\mathbb{R}$ et $\mathbb{C}$).** — L'ensemble $\mathbb{R}$ (respectivement $\mathbb{C}$) muni de l'addition est un groupe dont l'élément neutre est 0 et l'inverse de x est $-x$.

Exemple 1.3.3. — L'ensemble $\mathbb{N}$ muni de l'addition n'est pas un groupe : 1 n'a pas d'inverse pour la loi + dans $\mathbb{N}$.

Exemple 1.3.4. — Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la multiplication ne sont pas des groupes. L'élément neutre pour la multiplication est 1, la multiplication est associative, mais 0 n'a pas de symétrique puisque l'équation $x \times 0 = 1$ n'a pas de solution.

C'est le seul élément des ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ qui ne possède pas de symétrique pour la multiplication. Par contre aucun élément de $\mathbb{Z}$, hormis 1, ne possède de symétrique pour la multiplication.

***Exemple 1.3.5* (Les groupes $\mathbb{Q}^\times$, $\mathbb{R}^\times$ et $\mathbb{C}^\times$).** — L'ensemble $\mathbb{Q}^\times$ (respectivement $\mathbb{R}^\times$, $\mathbb{C}^\times$) des nombres rationnels (respectivement réels, complexes) non nuls, muni de la multiplication, est un groupe abélien. L'élément neutre est 1 et le symétrique d'un élément est son inverse.

Lorsque nous parlerons du groupe $\mathbb{Q}^\times$ (respectivement $\mathbb{R}^\times$, $\mathbb{C}^\times$), il sera désormais toujours sous-entendu que sa loi de composition interne est la multiplication.

Remarquons que l'on peut définir $\mathbb{Z}^\times$. C'est le groupe trivial puisque seul 1 admet un symétrique dans $\mathbb{Z}$.

Exemple 1.3.6. — Le cercle unité dans $\mathbb{C}$, $\mathbb{S}^1 = \{z \in \mathbb{C},\ |z| = 1\}$, muni de la multiplication est un groupe.

***Exemple 1.3.7* (Le groupe des racines de l'unité).** — Soit $n \geq 1$, on note μ_n l'ensemble des racines complexes de l'équation $X^n = 1$, on parle des *racines $n^{\text{ième}}$ de l'unité*. On note aussi $\mathscr{R} = \bigcup_{n\geq 1} \mu_n$. Munis de la multiplication il s'agit de groupes abéliens. Ils contiennent 1 puisque $1^n = 1$. Si z_1 et z_2 sont dans $\mathscr{R}$, ou dans μ_n, il existe n tel que $z_1^n = 1$ et m tel que $z_2^m = 1$, avec $n = m$ s'ils sont dans μ_n. Si $p = \operatorname{ppcm}(n, m)$ (on a $p = n$ si $n = m$) alors $(z_1 z_2^{-1})^p = z_1^p z_2^{-p} = 1(z_2^p)^{-1} = 1$ ce qui prouve que $\mathscr{R}$, ainsi que μ_n, sont des groupes.

Remarque 1.3.1. — On attire l'attention du lecteur sur le fait qu'une réunion de groupes munis d'une même loi est rarement un groupe.

***Exemple 1.3.8* (Le groupe affine de $\mathbb{R}$).** — On note $\operatorname{Aff}(\mathbb{R}) = \{x \mapsto ax + b\,,\ (a, b) \in \mathbb{R}^* \times \mathbb{R}\}$ que l'on munit de la composition. C'est une loi interne puisque si $\varphi\colon x \mapsto ax + b$ et $\psi\colon x \mapsto \alpha x + \beta$, alors $\varphi \circ \psi\colon x \mapsto a\alpha x + (a\beta + b)$. L'élément neutre est l'identité et l'inverse de $x \mapsto ax + b$ est $x \mapsto \frac{1}{a}x - \frac{b}{a}$.

***Exemple 1.3.9* (Le groupe $\mathrm{GL}(n, \mathbb{R})$).** — Soit $n \geq 2$ un entier. Soit $\mathrm{GL}(n, \mathbb{R})$ l'ensemble des matrices de taille $n \times n$ à coefficients réels qui sont inversibles. Si $\times$ désigne la multiplication matricielle alors $(\mathrm{GL}(n, \mathbb{R}), \times)$ est un groupe non abélien. Son élément neutre est la matrice identité de taille $n \times n$ et si $A \in \mathrm{GL}(n, \mathbb{R})$ alors son inverse est simplement l'inverse A^{-1} au sens matriciel.

Par contre $(\mathrm{GL}(n, \Bbbk), +)$ n'est pas un groupe car la somme de deux matrices inversibles n'est généralement pas inversible (la loi $+$ n'est donc pas interne).

Exemple 1.3.10. — Soit $\mathrm{M}(n, \Bbbk)$ l'ensemble des matrices carrées de taille n à coefficients dans un corps $\Bbbk$. Alors $(\mathrm{M}(n, \Bbbk), +)$, où $+$ désigne l'addition des matrices, est un groupe abélien. Cependant $(\mathrm{M}(n, \Bbbk), \cdot)$ n'est pas un groupe : la matrice nulle, par exemple, n'est pas inversible.

***Exemple 1.3.11* (Le groupe $\mathbb{Z}/n\mathbb{Z}$).** — On a introduit Exemple 1.1.7 l'ensemble $\mathbb{Z}/n\mathbb{Z}$, ensemble quotient de $\mathbb{Z}$ pour la relation d'équivalence d'égalité modulo n. On a ensuite défini une addition sur cet ensemble en posant, pour $\overline{a}$ et $\overline{b}$ dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{a} + \overline{b} = \overline{a + b}$ (Exemple 1.1.17). Rappelons qu'il y a des précautions à prendre pour justifier la légitimité de cette définition, se référer aux Exemples 1.1.15 et 1.1.16.

Vérifions maintenant que $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est un groupe.

Montrons que cette loi est associative. Soient $\overline{a}$, $\overline{b}$ et $\overline{c}$ trois éléments de $\mathbb{Z}/n\mathbb{Z}$. Nous avons

$$\begin{aligned}
\overline{a}+(\overline{b}+\overline{c}) &= \overline{a}+\overline{b+c} && (1.3.1)\\
&= \overline{a+(b+c)} && (1.3.2)\\
&= \overline{(a+b)+c} && (1.3.3)\\
&= \overline{a+b}+\overline{c} && (1.3.4)\\
&= (\overline{a}+\overline{b})+\overline{c} && (1.3.5)
\end{aligned}$$

Remarquons que les égalités (1.1.1), (1.1.2), (1.1.4) et (1.1.5) proviennent de la formule qui définit la loi interne + de $\mathbb{Z}/n\mathbb{Z}$ et que (1.1.3) provient de l'associativité de l'addition de $\mathbb{Z}$.

Montrons que l'élément $\overline{0}$ est neutre pour la loi +. En effet soit $\overline{a}$ un élément de $\mathbb{Z}/n\mathbb{Z}$; nous avons

$$\overline{a}+\overline{0}=\overline{a+0}=\overline{a}.$$

La première égalité provient de la formule qui définit la loi interne + de $\mathbb{Z}/n\mathbb{Z}$ et la seconde du fait que 0 est neutre pour l'addition dans $\mathbb{Z}$. De même nous pouvons montrer que $\overline{0}+\overline{a}=\overline{a}$.

Montrons que tout élément de $\mathbb{Z}/n\mathbb{Z}$ possède un symétrique pour la loi +. Soit $\overline{a}$ un élément de $\mathbb{Z}/n\mathbb{Z}$. Nous avons $\overline{a}+\overline{(-a)}=\overline{a+(-a)}=\overline{0}$ (la première égalité provient de la formule qui définit la loi interne + de $\mathbb{Z}/n\mathbb{Z}$ et la seconde du fait que $a+(-a)=0$ dans $\mathbb{Z}$). De même $\overline{(-a)}+\overline{a}=0$. Par conséquent $\overline{(-a)}$ est le symétrique de $\overline{a}$ pour la loi +. On dit aussi que c'est l'opposé de $\overline{a}$ et nous le notons souvent $-\overline{a}$. Nous écrivons $\overline{a}-\overline{b}$ plutôt que $\overline{a}+\overline{-b}$.

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition définie précédemment est un groupe. Désormais lorsque nous parlons de $\mathbb{Z}/n\mathbb{Z}$ il est sous-entendu que sa loi de composition interne est l'addition telle que définie ci-dessus.

Le groupe $\mathbb{Z}/n\mathbb{Z}$ est abélien. En effet soient $\overline{a}$ et $\overline{b}$ deux éléments de $\mathbb{Z}/n\mathbb{Z}$; nous avons

$$\begin{aligned}
\overline{a}+\overline{b} &= \overline{a+b} && (1.3.6)\\
&= \overline{b+a} && (1.3.7)\\
&= \overline{b}+\overline{a} && (1.3.8)
\end{aligned}$$

Notons que (1.1.6) et (1.1.8) proviennent de la définition de la loi interne + de $\mathbb{Z}/n\mathbb{Z}$ et (1.1.7) provient du fait que $\mathbb{Z}$ est un groupe abélien.

Exemple 1.3.12 **(Multiplication modulo n, le groupe $\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$)**

On fixe un entier $n \geq 1$.

On a vu que la présence d'éléments non inversibles nécessitait de prendre des précautions pour trouver une structure de groupe multiplicatif sur $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$.

La multiplication dans $\mathbb{Z}$ étant compatible avec la relation d'équivalence modulo n, il y a sur $\mathbb{Z}/n\mathbb{Z}$ une multiplication « naturelle » qui est associative avec pour élément neutre $1 \mod n$.

Quels sont les éléments inversibles pour cette multiplication ?

Dans $\mathbb{Z}/5\mathbb{Z}$ on constate que $2 \times 3 \equiv_5 1$, donc $2 \mod 5$ et $3 \mod 5$ sont inverses l'un de l'autre, que $4 \times 4 \equiv_5 1$, et donc $4 \mod 5$ est son propre inverse. Ainsi, à part $0 \mod 5$, tous les éléments de $\mathbb{Z}/5\mathbb{Z}$ admettent un inverse pour la multiplication et on a

$$\left(\mathbb{Z}/5\mathbb{Z}\right)^\times := \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}.$$

Dans $\mathbb{Z}/6\mathbb{Z}$ on a $5 \times 5 \equiv_6 1$ donc $5 \mod 6$ est son propre inverse. Mais on a aussi $2 \times 3 \equiv_6 0$ et $4 \times 3 \equiv_6 0$. Si $2 \mod 6$ possédait un inverse, disons $k \mod 6$, on aurait alors $k \times (2 \times 3) \equiv_6 k \times 0 \equiv 0$ et, par associativité, $k \times (2 \times 3) \equiv_6 (k \times 2) \times 3 \equiv_6 1 \times 3 \equiv_6 3$. Ceci impliquerait $0 \equiv_6 3$. C'est absurde, donc $2 \mod 6$ n'est pas inversible pour la multiplication dans $\mathbb{Z}/6\mathbb{Z}$. Pour les mêmes raisons $3 \mod 6$ et $4 \mod 6$ ne sont pas inversibles, ainsi on a :

$$\left(\mathbb{Z}/6\mathbb{Z}\right)^\times := \{\bar{1}, \bar{5}\}.$$

Plus généralement, $k \mod n$ possède un inverse pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si il existe $\ell \in \mathbb{Z}$ tel que $k \times \ell \equiv_n 1$. Ce qui est équivalent à l'existence d'un entier $a \in \mathbb{Z}$ tel que $k\ell = an + 1$ soit encore $k\ell - an = 1$. C'est une égalité de Bézout dont on sait qu'elle est équivalente au fait que k et n sont premiers entre eux. On a donc

Proposition 1.3.1

Soient $n \geq 2$ un entier et $k \in \mathbb{Z}$. L'élément $k \mod n$ possède un inverse pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si il est premier avec n.
Ainsi on a : $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \{k \mod n \mid k \in \mathbb{Z} \text{ est premier avec } n\}$.

Définition 1.3.1

Pour tout entier positif n on note $\phi(n)$ le nombre d'entiers positifs inférieurs ou égaux à n qui sont premiers avec n. Il s'agit de l'*indicatrice d'Euler* de n.

Corollaire 1.3.1

Le cardinal de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ est $\phi(n)$.

***Exemple 1.3.13* (Le groupe de Klein).** — Le *groupe de Klein* (ou Vierergruppe), du nom de Felix Klein, est le plus petit groupe non trivial qui ne soit pas cyclique [2]. On le note $\mathcal{K}$.

Ce groupe compte quatre éléments. Pour tout élément $g \in \mathcal{K} \setminus \{e\}$ nous avons : $g \neq e$ et $g^2 = e$; on dit que g est d'ordre 2 (nous reviendrons ultérieurement sur cette notion, Définitions 1.5.2). Le produit de deux éléments distincts d'ordre 2 est égal au troisième élément d'ordre 2.

2. La notion de groupe cyclique sera définie avec précision Définition 1.5.3 page 26.

La table de Cayley de $\mathcal{K} := \{e, a, b, c\}$ est :

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

L'ensemble $\mathcal{K}$ muni de $\star$ est une présentation [3] possible du groupe de Klein.

Nous verrons par la suite que $(\mathcal{K}, \star)$ est isomorphe à $\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +\right)$, c'est-à-dire que ces deux groupes ont exactement la même structure.

***Exemple 1.3.14* (Le groupe des quaternions).** — Soit $\mathbb{H}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ le groupe des quaternions. La multiplication est définie par la règle des signes et les formules

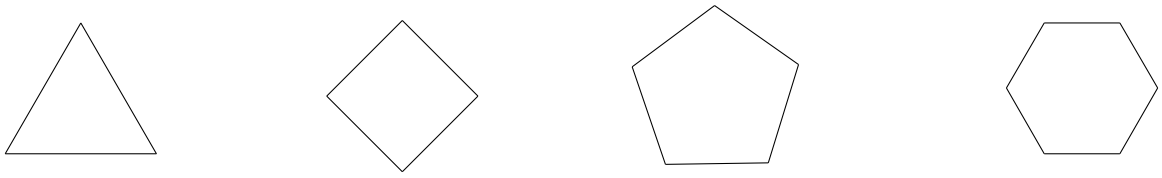
$$i^2 = j^2 = k^2 = -1 \qquad ij = -ji = k \qquad jk = -kj = i \qquad ki = -ik = j$$

Le groupe ainsi obtenu est non abélien : $ij = -ji$. Plus précisément le groupe des quaternions est l'un des deux groupes non abéliens comptant huit éléments, on dit qu'il est d'ordre 8 (cf. Définition 1.5.1, Chapitre 1). La table de Cayley du groupe des quaternions est

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

***Exemple 1.3.15* (Le groupe diédral).** — Soit $n \geq 3$. Le *groupe diédral* D_{2n} est l'ensemble des isométries préservant un polygone régulier à n côtés, l'opération étant la composition. Ces polygones pour $n = 3$, 4, 5 et 6 sont

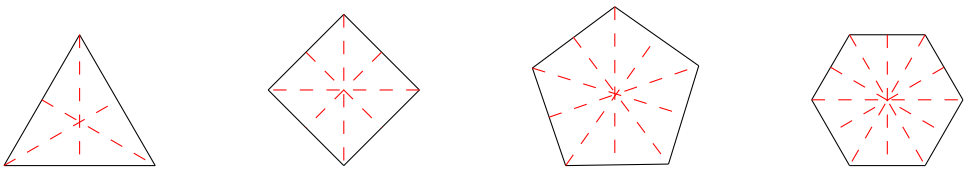
3. En théorie des groupes, un groupe peut se définir par une présentation, autrement dit par la donnée d'un ensemble de générateurs et d'un ensemble de relations que ceux-ci vérifient. Voir Définition 8.3.1, Chapitre 8.



Triangle équilatéral Carré Pentagone régulier Hexagone régulier

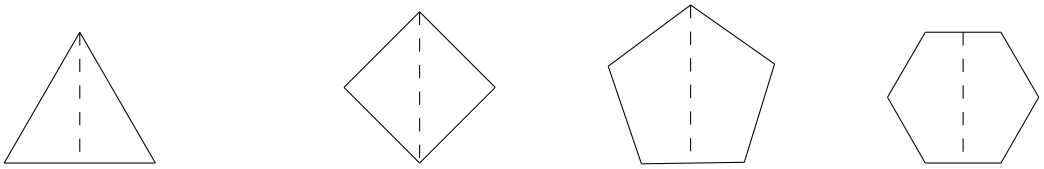
Polygones réguliers à n côtés pour $n = 3, 4, 5, 6$

Les réflexions d'axe les lignes pointillées rouges appartiennent à D_6, D_8, D_{10} et D_{12} :



La rotation d'angle un multiple de $\frac{2\pi}{n}$ de centre le centre du polygone est une isométrie qui préserve le polygone ; D_{2n} contient donc quelques rotations.

Soit s une réflexion d'axe une droite passant par un sommet du polygone. Voir les exemples dans la figure ci-dessous.[4] Une réflexion est d'ordre 2, donc $s^2 = \mathrm{id}$ et $s^{-1} = s$.



s s s s

Dans le Chapitre 5 nous étudierons plus en détails ce groupe, nous démontrerons en particulier l'énoncé suivant (Théorème 5.2.4) : Le groupe D_{2n} compte $2n$ éléments :

$$\mathrm{D}_{2n} = \{\mathrm{id},\, r,\, r^2,\, \ldots,\, r^{n-1},\, s,\, rs,\, \ldots,\, r^{n-1}s\}.$$

La table de Cayley de D_6 est :

4. La convention ici que s désigne une réflexion d'axe une droite passant par un sommet du polygone n'a d'importance que pour n pair, cas où l'axe de certaines réflexions ne passe pas par un sommet. Lorsque n est impair, l'axe de toutes les réflexions passe par un sommet, et n'importe laquelle d'entre elles peut être utilisée comme s.

	id	r	r^2	s	rs	r^2s
id	id	r	r^2	s	rs	r^2s
r	r	r^2	id	rs	r^2s	s
r^2	r^2	id	r	r^2s	s	rs
s	s	r^2s	rs	id	r^2	r
rs	rs	s	r^2s	r	id	r^2
r^2s	r^2s	rs	s	r^2	r	id

Exemple 1.3.16 **(Le groupe des permutations ou groupe symétrique)**

Soit E un ensemble et soit $\mathfrak{S}_E$ l'ensemble des bijections de E dans E, appelé également les *permutations* de E. Si σ et τ sont deux permutations de E, leur composée est une permutation de E. La formule $(\sigma, \tau) \mapsto \sigma \circ \tau$ définit donc une loi de composition interne sur $\mathfrak{S}_E$. Cette loi est associative et id_E en est un élément neutre. Si $\sigma \in \mathfrak{S}_E$, la bijection réciproque σ^{-1} est un symétrique de σ pour la loi $\circ$. L'ensemble $\mathfrak{S}_E$ muni de la composition des permutations est donc un groupe.

Lorsque nous parlerons du groupe $\mathfrak{S}_E$, il sera désormais toujours sous-entendu que sa loi de composition interne est la composition des permutations. Lorsque cela ne prêtera pas à confusion, nous nous permettrons d'écrire $\sigma\tau$ plutôt que $\sigma \circ \tau$. Nous écrirons aussi parfois simplement id au lieu de id_E s'il n'y a pas d'ambiguïté sur E.

Donnons quelques exemples de groupes de permutations :

1. Le cas de l'ensemble vide. L'ensemble vide possède une seule permutation, à savoir l'identité. Le groupe $\mathfrak{S}_\emptyset$ est donc égal à $\{\mathrm{id}\}$, il est trivial.

2. Le cas d'un singleton. Un singleton $\{g\}$ possède une seule permutation, à savoir l'identité (une application de $\{g\}$ dans lui-même envoie en effet nécessairement g sur g). Le groupe $\mathfrak{S}_{\{g\}}$ est par conséquent égal à $\{\mathrm{id}\}$ et est donc là encore trivial.

3. Le cas où E possède deux éléments distincts. Supposons que $E = \{a, b\}$ avec $a \neq b$. Le groupe $\mathfrak{S}_E$ compte alors deux éléments : l'identité et la permutation τ qui échange a et b. Le groupe $\mathfrak{S}_E$ n'est donc pas trivial : il est égal à $\{\mathrm{id}, \tau\}$. Notons que $\tau^2 = \mathrm{id}$, τ est donc son propre inverse. Le groupe $\mathfrak{S}_E$ est abélien.

4. Le cas où E possède au moins trois éléments distincts. Choisissons trois éléments distincts a, b et c dans E. Soit τ la permutation de E qui échange a et b et fixe tous les autres éléments de E (y compris c). Soit σ la permutation de E qui échange a et c et fixe tous les autres éléments de E (y compris b).

   D'une part
$$(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(b) = b$$

et d'autre part

$$(\tau \circ \sigma)(a) = \tau(\sigma(a)) = \tau(c) = c.$$

Ainsi $\sigma \circ \tau \neq \tau \circ \sigma$. En particulier le groupe $\mathfrak{S}_E$ n'est pas abélien.

Nous nous focalisons maintenant sur les groupes de permutations $\mathfrak{S}_{\{1,\dots,n\}}$; pour alléger un peu les notations, nous écrirons $\mathfrak{S}_n$ au lieu de $\mathfrak{S}_{\{1,\dots,n\}}$; notons que $\mathfrak{S}_0 = \mathfrak{S}_\emptyset$.

Pour décrire un élément de $\mathfrak{S}_n$, nous le présentons sous forme d'un tableau : la première ligne comporte tous les entiers compris entre 1 et n, et sous chacun d'eux nous écrivons son image :

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Par exemple

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

désigne l'élément de $\mathfrak{S}_3$ qui envoie 1 sur 2, 2 sur 3 et 3 sur 1.

Notons aussi que

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

est l'identité de $\mathfrak{S}_3$.

1.4. Sous-groupes

Définition 1.4.1

Soit $(\mathrm{G}, *)$ un groupe. Un sous-ensemble non vide H de G est un *sous-groupe* de G si la restriction de la loi $*$ à $\mathrm{H} \times \mathrm{H}$ munit H d'une structure de groupe.

Une condition nécessaire et suffisante pour que H soit un sous-groupe de G est que H soit stable pour $*$, que $e \in \mathrm{H}$ et que le symétrique de tout élément de H pour $*$ soit dans H.

Une autre condition nécessaire et suffisante pour que H soit un sous-groupe de G est

$$\mathrm{H} \neq \emptyset \qquad\qquad \forall\, g,\, h \in \mathrm{H} \qquad g * h^{-1} \in \mathrm{H}.$$

Exemple 1.4.1. — Si G est un groupe, alors G et $\{e\}$ sont des sous-groupes de G.

Exemple 1.4.2. — Pour tout $k \in \mathbb{N}$, l'ensemble $k\mathbb{Z} := \{kn \mid n \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.

Exemple 1.4.3. — Le sous-ensemble $\mathbb{R}^\times$ est un sous-groupe de $\mathbb{C}^\times$.

Exemple 1.4.4. — Le sous-ensemble $\{-1, 1\}$ de $\mathbb{R}^\times$ en est un sous-groupe.

Exemple 1.4.5. — Le groupe $\mathrm{O}(n,\mathbb{R})$ des matrices orthogonales réelles (ce sont les matrices M qui vérifient ${}^{\mathrm{t}}MM = \mathrm{id}$) est un sous-groupe de $\mathrm{GL}(n,\mathbb{R})$; le groupe $\mathrm{U}(n,\mathbb{C})$ des matrices unitaires complexes (constitué des matrices M qui vérifient ${}^{\mathrm{t}}\overline{M}M = \mathrm{id}$) est un sous-groupe de $\mathrm{GL}(n,\mathbb{C})$.

Exemple 1.4.6. — Soit K le sous-ensemble $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ de $\mathfrak{S}_4$. Il contient l'identité, il est stable par inversion (chacun de ses éléments est égal à son propre inverse), et par produit $((1\ 2)(3\ 4)(1\ 3)(2\ 4) = (1\ 4)(2\ 3)$ etc). C'est donc un sous-groupe de $\mathfrak{S}_4$. Il est isomorphe à $\mathcal{K}$.

Exemple 1.4.7. — Soit G un groupe. Soit H un sous-groupe de G et soit H′ un sous-ensemble de H. L'ensemble H′ est un sous-groupe de H si et seulement si c'est un sous-groupe de G. En effet, les trois conditions que doit vérifier H′ pour être un sous-groupe de H sont les mêmes que celles qu'il doit satisfaire pour être un sous-groupe de G.

Exemple 1.4.8. — Soit G un groupe. Soit $(\mathrm{H}_i)_{i\in I}$ une famille de sous-groupes de G indexée par un certain ensemble d'indices I. L'intersection des H_i est un sous-groupe de G :

- ◇ Comme chacun des H_i est un sous-groupe de G, on a $e \in \mathrm{H}_i$ pour tout $i \in I$ et donc $e \in \bigcap_{i\in I} \mathrm{H}_i$.
- ◇ Soit $h \in \bigcap_{i\in I} \mathrm{H}_i$. Pour tout i, l'élément h de G appartient à H_i ce qui entraîne que $h^{-1} \in \mathrm{H}_i$ puisque H_i est un sous-groupe de G ; comme ceci vaut quel que soit i, on a $h^{-1} \in \bigcap_{i\in I} \mathrm{H}_i$.
- ◇ Soient h et h' deux éléments de $\bigcap_{i\in I} \mathrm{H}_i$. Pour tout i, les éléments h et h' de G appartiennent à H_i ce qui entraîne que $hh' \in \mathrm{H}_i$ puisque H_i est un sous-groupe de G ; comme ceci vaut quel que soit i, on a $hh' \in \bigcap_{i\in I} \mathrm{H}_i$.

Ainsi $\bigcap_{i\in I} \mathrm{H}_i$ est donc bien un sous-groupe de G.

Définition 1.4.2

Un sous-groupe *propre* de G est un sous-groupe de G distinct de $\{e\}$ et de G.

Exemple 1.4.9. — Supposons que $\mathrm{G} = \mathbb{Z}$. L'ensemble des entiers de la forme $ng = gn$ avec $n \in \mathbb{Z}$, *i.e.* l'ensemble des multiples de g, est noté en général $g\mathbb{Z}$.

Ainsi le sous-groupe de $\mathbb{Z}$ engendré par 2 est l'ensemble $2\mathbb{Z}$ des entiers pairs, celui engendré par 3 est l'ensemble $3\mathbb{Z}$ des multiples de 3, etc.

En fait tous les sous-groupes de $\mathbb{Z}$ s'obtiennent ainsi :

Théorème 1.4.1

Soit G un sous-groupe de $\mathbb{Z}$. Il existe un unique entier $d \geq 0$ tel que $\mathrm{G} = d\mathbb{Z}$.

Démonstration. — ◇ Montrons tout d'abord l'existence.

Si $\mathrm{G} = \{0\}$, alors $\mathrm{G} = 0\mathbb{Z}$.

Supposons maintenant le groupe G non trivial ; G possède alors un élément g non nul. Il possède même un élément strictement positif ; en effet c'est clair si $g > 0$ et si $g < 0$ il suffit de prendre l'inverse $(-g)$ de g. L'ensemble des éléments strictement positifs de G étant non vide, il possède un plus petit élément d. Nous allons montrer que $\mathrm{G} = d\mathbb{Z}$. Puisque G est un sous-groupe de $\mathbb{Z}$ contenant d, il contient le sous-groupe de $\mathbb{Z}$ engendré par d, c'est-à-dire $d\mathbb{Z}$.

Reste à montrer l'inclusion réciproque $\mathrm{G} \subset d\mathbb{Z}$. Soit $g \in \mathrm{G}$. Puisque $d > 0$ on peut effectuer la division euclidienne de g par d. Elle fournit un couple (q, r) d'entiers avec $0 \leq r < d$ tels que $g = dq + r$. Ainsi $r = g - dq$. Comme $d\mathbb{Z} \subset \mathrm{G}$, nous avons : $-dq \in \mathrm{G}$. Puisque G est un groupe $g - dq$ appartient à G, *i.e.* r appartient à G. Puisque $0 \leq r < d$ et puisque d est le plus petit élément strictement positif de G, nous avons $r = 0$ et $g = dq$. En particulier, g appartient à $d\mathbb{Z}$ et $\mathrm{G} \subset d\mathbb{Z}$.

◇ Il reste à s'assurer de l'unicité de d. Soit $\delta > 0$ un entier tel que $\mathrm{G} = d\mathbb{Z} = \delta\mathbb{Z}$.

Si $d = 0$, alors $\mathrm{G} = 0\mathbb{Z} = \{0\}$ et δ est donc nul puisque δ appartient à $\mathrm{G} = \delta\mathbb{Z}$.

Supposons $d \neq 0$. Comme d appartient à $\mathrm{G} = \delta\mathbb{Z}$ il existe $a \in \mathbb{Z}$ tel que $d = a\delta$; de même il existe $b \in \mathbb{Z}$ tel que $\delta = bd$. Ainsi $d = a\delta = abd$ soit $d(1 - ab) = 0$. Par hypothèse d est non nul donc $1 - ab = 0$ soit $ab = 1$. Puisque a et b sont entiers ils sont ou bien tous deux égaux à 1 ou bien tous deux égaux à -1. Si a et b étaient tous deux égaux à -1, on aurait $\delta = bd = -d$ ce qui est impossible car d et δ sont positifs. Par suite $a = b = 1$ et $\delta = bd = d$.

□

Définition 1.4.3

Soit G un groupe.
Le *centre* de G est l'ensemble $Z(\mathrm{G})$ des éléments de G qui commutent avec tous les éléments de G c'est-à-dire

$$Z(\mathrm{G}) = \{x \in \mathrm{G} \,|\, \forall\, g \in \mathrm{G},\ gx = xg\}.$$

Le *centralisateur* Z_g d'un élément g de G est l'ensemble des éléments qui commutent à g :

$$Z_g = \{h \in \mathrm{G} \,|\, hg = gh\}$$

Ces deux notions sont reliées par : $Z(\mathrm{G}) = \bigcap_{g \in \mathrm{G}} Z_g$.

La notation Z vient de l'allemand : le centre est « Zentrum » et le centralisateur est « Zentralisator ».

Proposition 1.4.1

Soit G un groupe. Son centre $Z(\mathrm{G})$ est un sous-groupe abélien de G.
Le centralisateur Z_g de tout élément g de G est un sous-groupe de G.

Démonstration. — Par définition l'élément neutre e_{G} commute à tout élément de G. C'est donc un élément du centralisateur, Z_g, de tout élément g de G.

Soient h_1 et h_2 deux éléments de Z_g, où g un élément de G. Par associativité de la loi on a $(h_1h_2)g = h_1(h_2g)$ et, puisque h_2 est dans Z_g, $h_2g = gh_2$. Ce qui mène à $(h_1h_2)g = h_1(gh_2)$. En appliquant le même raisonnement on obtient $h_1(gh_2) = (h_1g)h_2 = (gh_1)h_2 = g(h_1h_2)$. Ce qui montre que $(h_1h_2)g = g(h_1h_2)$ et donc h_1h_2 est un élément du centralisateur de g.

Soient h un élément de Z_{g}. Alors $hg = gh$ d'où $g^{-1}hg = g^{-1}gh$, soit $g^{-1}hg = h$ et $g^{-1}h = hg^{-1}$ ce qu'on peut aussi réécrire $(hg^{-1})^{-1} = (g^{-1}h)^{-1}$, c'est-à-dire $gh^{-1} = h^{-1}g$. Ainsi h^{-1} est un élément de Z_{g}.

Nous avons ainsi prouvé que Z_{g} est un sous-groupe de G.

Puisque les éléments de $Z(\mathrm{G})$ commutent avec tous les éléments de G ils sont dans le centralisateur de tout $g \in \mathrm{G}$ et on a $Z(\mathrm{G}) \subset \bigcap_{g\in\mathrm{G}} Z_g$. Réciproquement, un élément dans l'intersection de tous les centralisateurs commute avec tous les éléments de G et donc $\bigcap_{g\in\mathrm{G}} Z_g \subset Z(\mathrm{G})$. Ce qui prouve que $\bigcap_{g\in\mathrm{G}} Z_g = Z(\mathrm{G})$. On peut alors déduire de l'Exemple 1.4.8 que $Z(\mathrm{G})$ est un sous-groupe de G. Il est abélien puisque par définition ses éléments commutent à tout élément de G et donc, en particulier, entre eux. □

Exemple 1.4.10. — Si G est abélien, alors $Z(\mathrm{G})$ et G coïncident.

Exemple 1.4.11. — Le centre du groupe des quaternions $\mathbb{H}_8$ est non trivial : $Z(\mathbb{H}_8) = \{1, -1\}$.

Exemple 1.4.12. — Notons que $\mathfrak{S}_1 = \{\mathrm{id}\}$ donc $Z(\mathfrak{S}_1) = \{\mathrm{id}\}$.

On a $\mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ donc $\mathfrak{S}_2$ est abélien et $Z(\mathfrak{S}_2) = \mathfrak{S}_2$.

Soit $n \geq 3$. Le centre de $\mathfrak{S}_n$ est réduit à $\{\mathrm{id}\}$.

Si $n \geq 3$, si a, b appartiennent à $\{1, 2, \ldots, n\}$ et si σ appartient à $\mathfrak{S}_n$, alors

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b)) \tag{1.4.1}$$

Soit σ un élément du centre de $\mathfrak{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite (1.4.1) entraîne

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement, id commute avec toutes les permutations.

1.5. Ordre d'un groupe, ordre d'un élément sous-groupe engendré par un élément

Un cas particulièrement important de groupes est le cas où l'ensemble G est fini. Rappelons que si E est un ensemble fini, le cardinal de E est simplement le nombre d'éléments de E. On le note $\mathrm{Card}(E)$ ou $|E|$.

Définitions 1.5.1

Un groupe G est dit *fini* si l'ensemble G est fini.
Le cardinal d'un groupe fini G s'appelle *l'ordre* de G.

Exemple 1.5.1. — Le groupe symétrique $\mathfrak{S}_n$ est un groupe fini d'ordre $n!$.

Exemple 1.5.2. — Soit $n \geq 2$ un entier. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est un groupe fini d'ordre n.

Définitions 1.5.2

Soit g un élément du groupe G. On note $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.
C'est le *sous-groupe engendré par* g.
S'il est fini, son ordre est l'*ordre de* g. Sinon, on dit que g est *d'ordre infini*.

Définition 1.5.1

Soient G un groupe et $g \in \mathrm{G}$. On dit que g est de *n-torsion* si $g^n = e_{\mathrm{G}}$.
On dit que g est de *torsion* s'il existe $n \in \mathbb{N}$ tel que g est de n-torsion.

Définitions 1.5.3

Le groupe G est *monogène* s'il existe $g \in \mathrm{G}$ tel que $\langle g \rangle = \mathrm{G}$.
On dit alors que g est un *générateur* de G.
Un groupe monogène et fini est un groupe *cyclique*.

Exemple 1.5.3. — Soit G un groupe, pour tout entier $n \in \mathbb{Z}$ on a $e_{\mathrm{G}}^n = e_{\mathrm{G}}$, et donc $\langle e_{\mathrm{G}} \rangle = \{e_{\mathrm{G}}\}$. Par conséquent, dans tout groupe e_{G} est d'ordre 1 et c'est l'unique élément d'ordre 1.

Exemple 1.5.4. — Considérons le sous-groupe de $(\mathbb{C}^\times, \cdot)$ engendré par $\mathbf{i}$:

$$\langle \mathbf{i} \rangle = \{\mathbf{i}^k \,|\, k \in \mathbb{Z}\} = \{\mathbf{i},\, -1,\, -\mathbf{i},\, 1\};$$

nous avons : $\langle\rangle$ est d'ordre 4 et $\mathbf{i}$ est d'ordre 4.

Exemple 1.5.5. — Dans $\mathbb{Z}/4\mathbb{Z}$ on a $< \bar{1} >= \{\bar{1}, \bar{2}, \bar{3}, \bar{0}\}$ et donc $\bar{1}$ est d'ordre 4 dans $\mathbb{Z}/4\mathbb{Z}$.
On a aussi $< \bar{2} >= \{\bar{2}, \bar{0}\}$ et $\bar{2}$ est d'ordre 2 dans $\mathbb{Z}/4\mathbb{Z}$.
On a enfin $< \bar{3} >= \{\bar{3}, \bar{2}, \bar{5}, \bar{0}\}$ ce qui fait de $\bar{3}$ un élément d'ordre 4 dans $\mathbb{Z}/4\mathbb{Z}$.

Exemple 1.5.6. — Les trois éléments i, j et k du groupe des quaternions $\mathbb{H}_8$ sont d'ordre 4 dans $\mathbb{H}_8$ et deux quelconques d'entre eux engendrent le groupe entier.

Commençons par énoncer une propriété immédiate :

Lemme 1.5.1

Soit G un groupe. Les éléments g et g^{-1} de G ont même ordre.

Démonstration. — L'énoncé est une conséquence directe de :

$$\langle g \rangle = \{g^k \,|\, k \in \mathbb{Z}\} = \{g^{-\ell} \,|\, -\ell \in \mathbb{Z}\} = \{g^{-\ell} \,|\, \ell \in \mathbb{Z}\} = \{(g^{-1})^\ell \,|\, \ell \in \mathbb{Z}\} = \langle g^{-1} \rangle.$$

□

Nous pouvons nous poser les trois questions suivantes à propos des éléments d'ordre fini : soit G un groupe,

1. si g est d'ordre fini, existe-t-il un critère permettant d'affirmer quand $g^k = g^\ell$?
2. si g est d'ordre fini, peut-on relier l'ordre de g^k à l'ordre de g ?
3. si g_1 et g_2 sont d'ordre fini, peut-on déterminer l'ordre de $g_1 g_2$ en fonction de l'ordre de g_1 et l'ordre de g_2 ?

Nous allons essentiellement donner des réponses complètes aux deux premières questions et une réponse partielle à la troisième question.

Proposition 1.5.1

Soit g un élément du groupe G.

- Le sous-groupe engendré par g est un sous-groupe abélien de G.
- Si g est d'ordre fini n on a $g^n = e_{\mathrm{G}}$. En outre, si $k \neq \ell$ sont deux éléments de $[\![0, n-1]\!]$, on a $g^k \neq g^\ell$. En particulier, on a $n = \min\{k \in \mathbb{N}^* \,|\, g^k = e_{\mathrm{G}}\}$ et $\langle g \rangle = \{g^k \,|\, k \in [\![0, n-1]\!]\}$.
- Si G est d'ordre fini, alors l'ordre de g divise l'ordre de G.

Corollaire 1.5.1

Dans un groupe fini d'ordre n tout élément est de n-torsion.

Remarque 1.5.1. — Nous attirons l'attention sur la troisième assertion de la Proposition 1.5.1 et plus précisément sur sa démonstration. C'est une des premières fois où nous utilisons les éléments du groupe pour construire des objets, d'abord une fonction puis une relation d'équivalence afin d'étudier le groupe lui-même. La première fois où nous « faisons agir » le groupe, en l'occurence sur lui-même. Étudier l'action d'un groupe sur un ensemble est une idée extrêmement puissante qui sera utilisée de nombreuses fois et développée plus en détails aux Chapitres 6 et 7.

Démonstration. —

- On a par convention $g^0 = e_{\mathrm{G}} \in \langle g \rangle$.

  Soient g^n et g^p deux éléments de $\langle g \rangle$. On a, c'est la définition de g^n, $g^n g^p = g^{n+p} \in \langle g \rangle$.

  Le sous-groupe engendré par g est bien un sous-groupe de G.

- Notons $M := \{k \in \mathbb{Z} \,|\, g^k = e_{\mathrm{G}}\}$. C'est un sous-ensemble non-vide de $\mathbb{Z}$ puisqu'il contient 0. D'autre part, si k et k' sont deux éléments de M, alors $g^k = g^{k'} = e_{\mathrm{G}}$, et donc $g^{k+k'} = g^k g^{k'} = e_{\mathrm{G}}$. C'est-à-dire que $(k + k') \in M$. Enfin, pour $k \in M$, on a par définition, $g^{-k} = (g^k)^{-1} = e_{\mathrm{G}}$, ce qui nous indique que $-k \in M$. L'ensemble M est donc un sous-groupe de $\mathbb{Z}$. D'après le Théorème 1.4.1 il existe $d > 0$ tel que $M = d\mathbb{Z}$. On a en particulier $d \in M$ et donc $g^d = e_{\mathrm{G}}$, ainsi que $d = \min\{k \in \mathbb{N}^* \,|\, g^k = e_{\mathbb{G}}\}$.

  Soit $k \in \mathbb{Z}$. La division euclidienne de k par d donne $q \in \mathbb{Z}$ et $r \in [\![0, d-1]\!]$ tels que $k = qd + r$. On a alors $g^k = g^{qd+r} = g^{qd} g^r = (g^d)^q g^r = (e_{\mathrm{G}})^q g^r = g^r$.

  Par suite $g^k = g^{k'}$ si $k \equiv_d k'$. D'autre part, si $g^k = g^{k'}$ alors $g^{k-k'} = e_{\mathrm{G}}$ et donc $k - k' \in M$ c'est-à-dire $k \equiv_d k'$. On peut alors conclure que $g^k = g^{k'}$ si et seulement si $k \equiv_d k'$ et donc que
  $$\langle g \rangle = \{g^k \,|\, k \in [\![0, d-1]\!]\}\cdot$$
  On a donc $|\langle g \rangle| = d = \min\{k \in \mathbb{N}^* \,|\, g^k = e_{\mathbb{G}}\}$.

- Soit g un élément de G d'ordre n. On définit sur G la relation $x \,\mathcal{R}\, y$ s'il existe $k \in [\![0, n-1]\!]$ tel que $x = g^k y$. C'est une relation d'équivalence :

  - elle est réflexive puisque $x = g^0 x$,
  - elle est symétrique puisque si $x = g^\ell y$ avec $\ell \in [\![0, n-1]\!]$, alors $y = x$ si $\ell = 0$, et $y = g^{n-\ell} x$ sinon, et on a $n - \ell \in [\![0, n-1]\!]$ dans ce cas,
  - elle est transitive, si $x = g^k y$, $y = g^\ell z$, alors $x = g^{k+\ell} z = g^p z$, avec p le reste de la division euclidienne de $k + \ell$ par n.

  La classe de x est l'ensemble $\bar{x} := \{g^k x \,|\, k \in [\![0, n-1]\!]\}$. On constate qu'elle contient n éléments et ce indépendamment de $x \in \mathrm{G}$ puisque pour $k \neq \ell$ dans $[\![0, n-1]\!]$ on a $g^k \neq g^\ell$.

Si p désigne le nombre de classes d'équivalence, comme elles forment une partition de G et qu'elles ont toutes le même cardinal, on a : $|\mathrm{G}| = pn$, ce qui prouve que n divise $|\mathrm{G}|$. □

Dans la démonstration de la Proposition 1.5.1 nous avons établi l'énoncé suivant qui répond à la question 1. :

Proposition 1.5.2

Soit G un groupe. Soit g un élément d'ordre n. Pour tous $k, \ell \in \mathbb{Z}$ $g^k = g^\ell$ si et seulement si $k \equiv_n \ell$.

Exemple 1.5.7. — Considérons le groupe $\mathbb{C}^\times$; les nombres complexes -1 et $\mathbf{i}$ sont d'ordre 2 et 4 respectivement alors que 3 est d'ordre infini. Le groupe $\mathbb{C}^\times$ admet des éléments de tout ordre : si $n \geq 0$ est un entier alors $\cos\left(\frac{2\pi}{n}\right) + \mathbf{i}\sin\left(\frac{2\pi}{n}\right)$ est d'ordre n.

Exemple 1.5.8. — Désignons par σ la permutation de $\mathfrak{S}_5$ suivante : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$. Nous avons

k	1	2	3	4	5
$\sigma(k)$	3	5	1	2	4
$\sigma^2(k)$	1	4	3	5	2
$\sigma^3(k)$	3	2	1	4	5
$\sigma^4(k)$	1	5	3	2	4
$\sigma^5(k)$	3	4	1	5	2
$\sigma^6(k)$	1	2	3	4	5

Par conséquent σ est d'ordre 6.

Exemple 1.5.9. — Un entier modulo m appartient à $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ s'il est relativement premier à n ce qui peut être déterminé efficacement à l'aide de l'algorithme d'Euclide. Dire que a mod m est d'ordre n dans $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ signifie que $a^n \equiv_m 1$ et $a^j \not\equiv_m 1$ pour tout $1 \leq j < n$.

Il n'existe pas de formule simple qui donne l'ordre d'un élément de $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$. Par exemple $2 \not\equiv_7 1$, $2^2 \not\equiv_7 1$, $2^3 \equiv_7 1$, *i.e.* 2 est d'ordre 3 dans $\left(\mathbb{Z}/7\mathbb{Z}\right)^\times$. À partir de $2^{11} \equiv_{23} 1$ et $2^j \not\equiv_{23} 1$ pour tout $1 \leq j < 11$ nous obtenons que 2 est d'ordre 11 dans $\left(\mathbb{Z}/23\mathbb{Z}\right)^\times$. Pour $m \geq 3$, -1 est d'ordre 2 dans $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ car $(-1)^2 \equiv_m 1$ et $-1 \not\equiv 1_m$. Reste le cas $m = 2$: comme $-1 \equiv_2 1$ nous avons : -1 est d'ordre 1 dans $\left(\mathbb{Z}/2\mathbb{Z}\right)^\times$ (le groupe $\left(\mathbb{Z}/2\mathbb{Z}\right)^\times$ est réduit à un élément !)

Exemple 1.5.10. — Considérons dans $\mathfrak{S}_n$ le r-cycle $\sigma = (a_1\ a_2\ \dots\ a_r)$. L'itéré $k$ième de σ décale chaque a_i de k termes. Ainsi le plus petit entier k tel que $\sigma^k = \mathrm{id}$ est $k = r$. Autrement dit, un r-cycle est d'ordre r. En particulier, une transposition est d'ordre 2.

Cette information sur l'ordre des r-cycles combinée au fait que toute permutation s'écrit comme un produit de cycles disjoints permettra de déterminer l'ordre d'une permutation quelconque de $\mathfrak{S}_n$.

L'indicatrice d'Euler de n, $\phi(n)$, a été introduite Définition 1.3.1, elle désigne le nombre d'entiers compris entre 1 et n qui sont premiers avec n.

Corollaire 1.5.2: (Théorème d'Euler)

Soit $n \geq 1$ un entier et a un entier premier avec n, alors $a^{\phi(n)} \equiv_n 1$.

Démonstration. — Comme a est premier avec n, sa classe modulo n est un élément de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. D'après le Corollaire 1.3.1 c'est un groupe d'ordre $\phi(n)$, et d'après le Corollaire 1.5.1 tous ses éléments sont de $\phi(n)$-torsion. On en déduit l'égalité : $a^{\phi(n)} \equiv_n 1$. □

Le théorème d'Euler a pour cas particulier le petit théorème de Fermat. Si n est un entier premier, alors $\phi(n) = n - 1$. On a donc

Corollaire 1.5.3: (Petit Théorème de Fermat)

Si $p \geq 2$ est un entier premier et si a est un entier non divisible par p, alors $a^{p-1} \equiv_p 1$.

Remarque 1.5.2. — Si G est un groupe fini, la Proposition 1.5.1 nous indique que tous ses éléments sont d'ordre fini.

La réciproque est fausse : il existe des groupes infinis dont tous les éléments sont d'ordre fini, par exemple le groupe des racines de l'unité dans $\mathbb{C}^\times$ introduit dans l'Exemple 1.3.7.

Corollaire 1.5.4

Si G est un groupe fini et si k est un entier premier à $|\mathrm{G}|$, alors la fonction $f\colon \mathrm{G} \to \mathrm{G}$, $g \mapsto g^k$ est bijective.

Démonstration. — Puisque $\mathrm{pgcd}(k, |\mathrm{G}|) = 1$ le théorème de Bezout assure l'existence d'entiers ℓ et m tels que $k\ell + |\mathrm{G}|m = 1$. Alors

$$g = g^1 = g^{k\ell}\left(g^{|\mathrm{G}|}\right)^m = g^{k\ell}e^m = g^{k\ell}.$$

Soit ℓ un entier tel que $k\ell \equiv_{|\mathrm{G}|} 1$ et soit $F\colon \mathrm{G} \to \mathrm{G}$, $g \mapsto g^\ell$. Alors $F(f(g)) = F(g^k) = g^{k\ell} = g$ et $f(F(g)) = f(g^\ell) = g^{k\ell} = g$: autrement dit la fonction f est inversible d'inverse F. □

Exemple 1.5.11. — Considérons le groupe diédral D_{10} d'ordre 10. Soit $f\colon \mathrm{D}_{10} \to \mathrm{D}_{10}$, $g \mapsto g^3$

g	1	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
$f(g)$	1	r^3	r	r^4	r^2	s	rs	r^2s	r^3s	r^4s

Comme $3 \times 7 = 21 \equiv_{10} 1$ f est inversible d'inverse $\mathrm{D}_{10} \to \mathrm{D}_{10}$, $g \mapsto g^7$. Par exemple $f(r^4) = r^{12} = r^2$ et $F(r^2) = r^{14} = r^4$ donc $F(f(r^4)) = r^4$.

Corollaire 1.5.5

Tout groupe G d'ordre premier est cyclique ; plus précisément, tout élément de $\mathrm{G} \smallsetminus \{e\}$ est un générateur de G.

Démonstration. — Soit G un groupe. Soit $g \in \mathrm{G} \smallsetminus \{e\}$. La Proposition 1.5.1 assure que l'ordre de g divise $|\mathrm{G}|$; comme g appartient à $\mathrm{G} \smallsetminus \{e\}$ l'ordre de g est > 1. Il en résulte que g est d'ordre $|\mathrm{G}|$. Ainsi $\langle g \rangle$ est un sous-groupe de G de même ordre que G, *i.e.* $\mathrm{G} = \langle g \rangle$. □

Théorème 1.5.1

Soit G un groupe. Soit g un élément de G d'ordre n. Alors $g^k = e$ si et seulement si n divise k.

Démonstration. — Soit g un élément d'ordre n. Lors de la démonstration de la Proposition 1.5.1 nous avons montré que l'ensemble $M = \{k \in \mathbb{Z} \,|\, g^k = e_{\mathrm{G}}\}$ était égal à $n\mathbb{Z}$ ce qui prouve le résultat. □

Exemple 1.5.12. — Dans $\mathbb{R}^\times$ -1 est d'ordre 2 et $(-1)^k = 1$ si et seulement si k est pair autrement dit si et seulement si 2 divise k.

Nous allons donner une application du Théorème 1.5.1 : une formule pour l'ordre d'une permutation quelconque.

Théorème 1.5.2

Soit σ une permutation de $\mathfrak{S}_n$. Décomposons σ en produit de cycles disjoints : $\sigma = \sigma_1\sigma_2 \dots \sigma_\ell$ où σ_i désigne un r_i-cycle. L'ordre de σ est $\mathrm{ppcm}(r_1, r_2, \dots, r_\ell)$.

Nous utilisons dans cet énoncé le Théorème 5.1.1 qui assure l'existence d'une telle décomposition, ainsi que le fait que des permutations à support disjoints commutent, ce qui est vu au §5.1.2.

Démonstration. — Comme les cycles disjoints commutent nous avons pour tout k

$$\sigma^k = \sigma_1^k \sigma_2^k \dots \sigma_\ell^k.$$

Puisque les σ_i permutent des éléments contenus dans des ensembles disjoints $\sigma^k = \mathrm{id}$ si et seulement si $\sigma_i^k = \mathrm{id}$ pour tout $1 \leq i \leq \ell$. Rappelons que σ_i est d'ordre r_i (Exemple 1.5.10) ;

par suite le Théorème 1.5.1 assure que $\sigma_i^k = \mathrm{id}$ si et seulement si r_i divise k. Par suite $\sigma^k = \mathrm{id}$ si et seulement si r_i divise k pour tout $1 \leq i \leq \ell$. Or r_i divise k pour tout $1 \leq i \leq \ell$ si et seulement si $\mathrm{ppcm}(r_1, r_2, \ldots, r_\ell)$ divise k donc $\sigma^k = \mathrm{id}$ si et seulement si $\mathrm{ppcm}(r_1, r_2, \ldots, r_\ell)$ divise k. Finalement σ est d'ordre $\mathrm{ppcm}(r_1, r_2, \ldots, r_\ell)$. □

Théorème 1.5.3

Soit G un groupe qui contient les éléments g_1, $g_2, \cdots$, g_n d'ordre fini égaux respectivement à r_1, $r_2, \cdots$, r_n. Si ces éléments commutent deux à deux, c'est-à-dire si $g_k g_\ell = g_\ell g_k$ pour tout k et tout ℓ dans $[\![1, n]\!]$, alors $\prod_{k=1}^{n} g_k$ est d'ordre fini égal à $\mathrm{ppcm}(r_1, r_2, \cdots, r_\ell)$.

Exemple 1.5.13. — Considérons $\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8\ 9\ 10)$; les cycles apparaissant dans la définition de σ sont à supports disjoints, le Théorème 1.5.2 assure donc que σ est d'ordre $\mathrm{ppcm}(4, 6) = 12$.

Exemple 1.5.14. — Nous avons vu (Exemple 1.5.8) que $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$ est d'ordre 6.

La décomposition de σ en produit de cycles disjoints est $(1\ 3)(2\ 4\ 5)$ et $\mathrm{ppcm}(2, 3) = 6$.

Exemple 1.5.15. — Considérons $\sigma = (1\ 2\ 3)(2\ 4\ 1)$. Cet élément de $\mathfrak{S}_4$ s'écrit comme un produit de deux 3-cycles mais il n'est pas d'ordre $\mathrm{ppcm}(3, 3) = 3$; en effet

k	1	2	3	4
$\sigma(k)$	3	4	1	2
$\sigma^2(k)$	1	2	3	4

i.e. $\sigma^2 = \mathrm{id}$ et σ est d'ordre 2. Remarquons que $(1\ 2\ 3)$ et $(2\ 4\ 1)$ ne sont pas à supports disjoints, c'est pour cette raison que nous ne pouvons pas appliquer le Théorème 1.5.2. On peut réécrire σ comme $(1\ 3)(2\ 4)$ et appliquer le Théorème 1.5.2 ; on retrouve que σ est d'ordre $\mathrm{ppcm}(2, 2) = 2$.

Corollaire 1.5.6

Une permutation σ de $\mathfrak{S}_n$ est d'ordre premier p si et seulement si σ est un produit de p-cycles disjoints.

Remarque 1.5.3. — Cet énoncé ne dit pas que tout élément d'ordre premier p est un p-cycle mais que c'est un produit de p-cycles disjoints. Par exemple $(1\ 2)(3\ 4)(5\ 6)$ est d'ordre 2 et $(1\ 2\ 3)(4\ 5\ 6)$ est d'ordre 3.

Démonstration. — Écrivons σ comme un produit de cycles disjoints non triviaux $\sigma = \sigma_1\sigma_2\ldots\sigma_\ell$. Désignons par r_i l'ordre de σ_i. Le Théorème 1.5.2 assure que σ est d'ordre $p = \text{ppcm}(r_1, r_2, \ldots, r_\ell)$. Chaque r_i est donc un facteur de p et est plus grand que 1 (par hypothèse les r_i sont non triviaux) ; il en résulte que $r_i = p$.

Réciproquement, supposons que $r_i = p$ pour tout $1 \leq i \leq \ell$; d'une part $\text{ppcm}(r_1, r_2, \ldots, r_\ell) = \text{ppcm}(p, p, \ldots, p) = p$ et d'autre part σ est d'ordre $\text{ppcm}(r_1, r_2, \ldots, r_\ell)$ (Théorème 1.5.2). Par conséquent, σ est d'ordre p. □

Soit G un groupe. Soit $g \in$ G d'ordre fini n. Comme $(g^k)^n = (g^n)^k = e$ le Théorème 1.5.1 assure que l'ordre de g^k divise n. Quel facteur de n est-ce ?

Exemple 1.5.16. — Supposons que g soit d'ordre 12 ; alors l'ordre de chaque puissance de g est un facteur de 12. Par définition de l'ordre g^2 est d'ordre $6 = \frac{12}{2}$. Par contre il est absurde de dire que g^8 est d'ordre $\frac{12}{8} = \frac{3}{2}$ car $\frac{3}{2}$ n'est pas un entier. Remarquons que

$$g^8 \neq e, \qquad (g^8)^2 = g^{16} = g^4 \neq e, \qquad (g^8)^3 = g^{24} = (g^{12})^2 = e^2 = e;$$

nous en déduisons que g^8 est d'ordre $3 = \frac{12}{4} = \frac{12}{\text{pgcd}(12,8)}$.

Théorème 1.5.4

Soit G un groupe. Soit g un élément d'ordre n de G. Soit $k > 0$ un entier.

- ◇ Si k divise n, alors g^k est d'ordre $\frac{n}{k}$.
- ◇ Si $\text{pgcd}(k, n) = 1$, alors g^k est d'ordre n (comme g).
- ◇ L'élément g^k est d'ordre $\frac{n}{\text{pgcd}(k,n)}$.

Remarque 1.5.4. — La troisième assertion contient les deux premières ; si nous avons choisi d'énoncer le théorème de cette façon c'est parce que les deux premières assertions peuvent se montrer indépendamment de la troisième et c'est ce que nous allons faire.

Démonstration. — Désignons par t l'ordre de g^k ; alors $(g^k)^t = e$ et t est le plus petit entier qui satisfait cette équation.

- ◇ Supposons que k divise n. La condition $(g^k)^t = e$ est équivalente à $g^{kt} = e$ donc n divise kt d'après le Théorème 1.5.1. Ainsi $n \leq kt$ et $\frac{n}{k} \leq t$.

  À partir de $(g^k)^{\frac{n}{k}} = g^{k\frac{n}{k}} = g^n = e$ nous obtenons que $t \leq \frac{n}{k}$ (il suffit de revenir à la définition de période). Finalement $t = \frac{n}{k}$.
- ◇ Nous avons $(g^k)^t = e$ si et seulement si $g^{kt} = e$; le Théorème 1.5.1 assure que n divise kt. Puisque $\text{pgcd}(k, n) = 1$, n divise kt se réécrit n divise t. En particulier $n \leq t$. Puisque $(g^k)^n = g^{kn} = (g^n)^k = e^k = e$ la définition d'ordre conduit à $t \leq n$. Finalement $t = n$.

◇ L'équation $(g^k)^t = e$ se réécrit $g^{kt} = e$ d'où (Théorème 1.5.1) n divise kt c'est-à-dire $nm = kt$ pour un certain $m \in \mathbb{Z}$. Nous pouvons réécrire n sous la forme $\mathrm{pgcd}(n,k)n'$ et k sous la forme $\mathrm{pgcd}(n,k)k'$; bien sûr $\mathrm{pcgd}(n',k') = 1$. Remarquons que $kt = nm$ se réécrit $\mathrm{pgcd}(n,k)k't = \mathrm{pgcd}(n,k)n'm =$ d'où n' divise $k't$. Puisque n' et k' sont premiers entre eux n' divise $k't$ conduit à n' divise t. En particulier $n' \leq t$. À partir de

$$(g^k)^{n'} = g^{kn'} = g^{k\frac{n}{\mathrm{pgcd}(k,n)}} = g^{n\frac{k}{\mathrm{pgcd}(k,n)}} = g^{nk'} = (g^n)^{k'} = e^{k'} = e$$

nous obtenons l'inégalité $t \leq n'$. Finalement $t = n'$, *i.e.* $t = \frac{n}{\mathrm{pgcd}(n,k)}$.

□

On peut utiliser ce résultat pour décrire complètement l'ensemble des sous-groupes d'un groupe cyclique.

Théorème 1.5.5

Soit G un groupe cyclique d'ordre n dont g est un générateur.
Pour tout diviseur d de n, $\mathrm{H}_d = \langle g^{\frac{n}{d}} \rangle$ est l'unique sous-groupe de G d'ordre d.

Démonstration. — Soit H un sous-groupe de G d'ordre d.

Notons $\ell = \min\{i \in [\![1,n]\!] \mid g^i \in \mathrm{H}\}$. Le groupe engendré par g^ℓ est un sous-groupe de H.

Soit g^k un autre élément de H. La division euclidienne de k par ℓ assure l'existence de $q \in \mathbb{N}$ et $r \in [\![0, \ell-1]\!]$ tel que $k = q\ell + r$. Ainsi on a $g^k = g^{q\ell+r} \in \mathrm{H}$ et $g^{q\ell} = \left(g^\ell\right)^q \in \mathrm{H}$. On en déduit que $g^{-q\ell}g^{q\ell+r} = g^r \in \mathrm{H}$. Comme $r < \ell$ cela entraîne, par minimalité de ℓ, que $r = 0$. Ainsi $k = q\ell$ et $g^k \in \langle g^\ell \rangle$.

On en déduit que $\mathrm{H} \subset \langle g^\ell \rangle$ puis que $\mathrm{H} = \langle g^\ell \rangle$.

On effectue maintenant la division euclidienne de n par ℓ. On obtient $u \in \mathbb{N}$ et $s \in [\![0, \ell-1]\!]$ tels que $n = u\ell + s$. On a d'après la Proposition 1.5.1, $e_{\mathrm{G}} = g^n = g^{u\ell+s}$. On en déduit que $g^s = g^{-u\ell} = \left(g^\ell\right)^{-u}$ est un élément de H. On utilise une nouvelle fois la minimalité de ℓ pour conclure que $s = 0$. Alors $n = u\ell$ et le Théorème 1.5.4 nous indique que g^ℓ est d'ordre u. On a donc $u = d$ et $\ell d = n$, soit $\ell = \frac{n}{d}$ comme annoncé. □

Remarque 1.5.5. — Les seconde et troisième assertions du Théorème 1.5.4 sont encore vraies si $k < 0$ car g^k et g^{-k} sont de même ordre.

La première assertion du Théorème 1.5.4 est encore vraie si $k < 0$ à condition de remplacer $\frac{n}{k}$ par $\frac{n}{|k|}$.

Exemple 1.5.17. — Nous retrouvons le fait que g et g^{-1} sont de même ordre. En effet, si g est d'ordre n, alors comme $\mathrm{pgcd}(n,-1) = 1$ l'élément g^{-1} est aussi d'ordre n.

Exemple 1.5.18. — Si g est d'ordre 12, alors l'ordre de g^k est $\frac{12}{\mathrm{pgcd}(12,k)}$:

k	1	2	3	4	5	6	7	8	9	10	11	12
ordre de g^k	12	6	4	3	12	2	12	3	4	6	12	1

Exemple 1.5.19. — Si g est d'ordre 12, alors g^k est d'ordre 12 lorsque $\mathrm{pgcd}(k, 12) = 1$. En regardant la table ci-dessus nous obtenons que g^k est d'ordre 12 lorsque k appartient à $\{1, 5, 7, 11\}$, *i.e.* lorsque k est premier à 12.

Comment l'ordre de $g_1 g_2$ est-il relié à l'ordre de g_1 et l'ordre de g_2 ?

Exemple 1.5.20. — Nous avons vu dans l'Exemple 1.5.19 que les éléments (1 2 3) et (2 4 1) de $\mathfrak{S}_4$ sont tous deux d'ordre 3 alors que leur produit $(1\ 2\ 3)(2\ 4\ 1) = (1\ 3)(2\ 4)$ est d'ordre 2.

Exemple 1.5.21. — Soit G un groupe contenant un élément d'ordre 5. Alors g^{-1} est d'ordre 5 (Lemme 1.5.1) et g^2 est d'ordre 5 (Théorème 1.5.4). Mais le produit $gg^{-1} = e$ est d'ordre 1 alors que $gg^2 = g^3$ est d'ordre 5 (Théorème 1.5.4).

Exemple 1.5.22. — Considérons dans $\mathrm{GL}(2, \mathbb{R})$ les deux matrices $A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. On peut vérifier que $A^2 = B^2 = \mathrm{id}$, ainsi A et B sont d'ordre 2. Néanmoins $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini ; en effet $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ donc $(AB)^n = \mathrm{id}$ si et seulement si $n = 0$.

Le produit $BA = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = (AB)^{-1}$ est aussi d'ordre infini (Lemme 1.5.1). Il en résulte que deux éléments peuvent être d'ordre fini et leur produit d'ordre infini.

Exemple 1.5.23. — Donnons des exemples de groupe fini contenant deux éléments d'ordre 2 dont le produit est d'ordre n quelconque. Considérons dans $\mathrm{GL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$ les matrices A et B données par

$$A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

(ce sont les mêmes matrices que dans l'Exemple précédent mais vues cette fois dans $\mathrm{GL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$. Puisque $1 \not\equiv_n -1$ les matrices A et B sont d'ordre 2 et leur produit AB est d'ordre n dans $\mathrm{GL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$.

Les deux derniers Exemples montrent qu'on ne peut rien dire en général sur l'ordre du produit de deux éléments d'ordre fini.

Néanmoins si les deux éléments considérés commutent, on peut utiliser le Théorème 1.5.3 qui nous indique que l'ordre du produit est, dans ce cas, égal au ppcm des deux ordres. En particulier, si ces deux ordres sont premiers entre eux, alors l'ordre du produit est le produit des deux ordres.

On a donc le résultat suivant :

Théorème 1.5.6

Soit G un groupe. Soient g_1 un élément de G d'ordre n_1 et g_2 un élément de G d'ordre n_2. Supposons que g_1 et g_2 commutent. Si $\mathrm{pgcd}(n_1, n_2) = 1$, alors $g_1 g_2$ est d'ordre $n_1 n_2$.

Démonstration. — Désignons par n_1 l'ordre de g_1 et par n_2 celui de g_2. Comme $g_1 g_2 = g_2 g_1$, le Théorème 1.5.3 nous indique que l'ordre de $g_1 g_2$ est égal à $\mathrm{ppcm}(n_1, n_2)$, et puisque que $\mathrm{pgcd}(n_1, n_2) = 1$, on a $\mathrm{ppcm}(n_1, n_2) = n_1 n_2$. On a utilisé la relation, vraie pour tout couple d'entier (n, k) : $nk = \mathrm{pgcd}(n, k)\mathrm{ppcm}(n, k)$. □

Exemple 1.5.24. — Dans $\left(\mathbb{Z}/21\mathbb{Z}\right)^\times$ -1 est d'ordre 2 et 4 est d'ordre 3. Par suite $-1 \times 4 = -4 \equiv_{21} 17$ est d'ordre 6.

Exemple 1.5.25. — Soit G un groupe. Si $g_1 \in \mathrm{G}$ est d'ordre 5, $g_2 \in \mathrm{G}$ est d'ordre 8 et si de plus g_1 et g_2 commutent, alors $g_1 g_2$ est d'ordre 40.

Exemple 1.5.26. — Dans $\mathfrak{S}_5$ la permutation $(1\ 2\ 3)$ est d'ordre 3, $(1\ 5\ 3\ 4\ 2)$ est d'ordre 5 mais $(1\ 2\ 3)(1\ 5\ 3\ 4\ 2) = (1\ 5)(3\ 4)$ est d'ordre 2 et pas d'ordre $3 \times 5 = 15$. Remarquons que $(1\ 2\ 3)$ et $(1\ 5\ 3\ 4\ 2)$, c'est pour cette raison que nous ne pouvons pas appliquer le Théorème 1.5.6. Autrement dit le Théorème 1.5.6 n'est plus vrai si on enlève l'hypothèse « g_1 et g_2 commutent ».

Le ppcm de n_1 et n_2 n'est pas seulement une borne supérieure pour l'ordre de $g_1 g_2$ mais peut aussi être réalisé comme l'ordre de $g_1^{a_1} g_2^{a_2}$ pour a_1, a_2 bien choisis :

Corollaire 1.5.7

Soit G un groupe. Soient g_1 un élément de G d'ordre n_1 et g_2 un élément de G d'ordre n_2. Supposons que g_1 et g_2 commutent. Il existe des entiers a_1 et a_2 tels que $g_1^{a_1} g_2^{a_2}$ est d'ordre $\mathrm{ppcm}(n_1, n_2)$.

Démonstration. — Écrivons la décomposition en facteurs premiers de n_1 et n_2

$$n_1 = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} \qquad\qquad n_2 = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$$

les e_i et f_i pouvant être nuls. Rappelons que $\mathrm{ppcm}(n_1, n_2) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \dots p_r^{\max(e_r,f_r)}$. Posons $k_1 = \prod_{e_i \geq f_i} p_i^{e_i}$ et $k_2 = \prod_{e_i < f_i} p_i^{f_i}$. Alors $\mathrm{ppcm}(n_1, n_2) = k_1 k_2$ et $\mathrm{pgcd}(k_1, k_2) = 1$ (en effet, k_1 et k_2 n'ont pas de facteur premier en commun). Par définition k_1 divise n_1 et k_2 divise n_2. Alors $g_1^{n_1/k_1}$ est d'ordre k_1 et $g_2^{n_2/k_2}$ est d'ordre k_2. Comme $g_1^{n_1/k_1} g_2^{n_2/k_2} = g_2^{n_2/k_2} g_1^{n_1/k_1}$ et $\mathrm{pgcd}\left(\frac{n_1}{k_1}, \frac{n_2}{k_2}\right) = 1$ le Théorème 1.5.6 assure que $g_1^{n_1/k_1} g_2^{n_2/k_2}$ est d'ordre $k_1 k_2 = \mathrm{ppcm}(n_1, n_2)$. □

Exemple 1.5.27. — Supposons que g_1 soit d'ordre $n_1 = 60 = 2^2 \times 3 \times 5$ et que g_2 soit d'ordre $n_2 = 630 = 2 \times 3^2 \times 5 \times 7$; alors $\mathrm{ppcm}(n_1, n_2) = 2^2 \times 3^2 \times 5 \times 7$. Posons $k_1 = 2^2 \times 5$ et $k_2 = 3^2 \times 7$; nous avons : $\mathrm{ppcm}(n_1, n_2) = k_1 k_2$ et $\mathrm{pgcd}(k_1, k_2) = 1$. Alors g_1^3 est d'ordre $2^2 \times 5$ et g_2^{10} est d'ordre $3^2 \times 7$. Étant donnés que $\mathrm{pgcd}(2^2 \times 5, 3^2 \times 7) = 1$ et que g_1^3 et g_2^{10} commutent le Corollaire 1.5.7 assure que $g_1^3 g_2^{10}$ est d'ordre $\mathrm{ppcm}(n_1, n_2) = 2^2 \times 3^2 \times 5 \times 7$.

Remarque 1.5.6. — Les entiers a_1 et a_2 ne sont pas uniques. Reprenons l'Exemple 1.5.27. Puisque 5 apparaît à la fois dans la décomposition de n_1 en facteurs premiers et dans la décomposition de n_2 en facteurs premiers nous pouvons décomposer $\mathrm{ppcm}(n_1, n_2)$ comme suit : $\mathrm{ppcm}(n_1, n_2) = \underbrace{2^2}_{k_1'} \underbrace{3^2 \times 5 \times 7}_{k_2'}$. Alors g_1^{15} est d'ordre k_1', g_2^2 est d'ordre k_2 et $\mathrm{pgcd}(k_1', k_2') = 1$; de plus g_1^{15} et g_2^2 commutent. Ainsi d'après le Corollaire 1.5.7 l'élément $g_1^{15} g_2^2$ est d'ordre $\mathrm{ppcm}(n_1, n_2) = 2^2 \times 3^2 \times 5 \times 7$.

Alors que le Théorème 1.5.6 donne une formule pour l'ordre d'un produit d'éléments d'ordre premier entre eux qui commutent on peut se demander si on peut écrire tout élément $g \in \mathrm{G}$ d'ordre $n = n_1 n_2$ avec $\mathrm{pgcd}(n_1, n_2) = 1$ sous la forme $g = g_1 g_2$ avec g_i élément d'ordre n_i. Si oui ces deux éléments g_1 et g_2 sont-ils uniques ? La réponse à ces deux questions est oui. Autrement dit le Théorème 1.5.6 admet une « réciproque » :

Théorème 1.5.7

Soit G un groupe. Soit g un élément de G d'ordre n. Supposons que n s'écrive $n_1 n_2$ avec $\mathrm{pgcd}(n_1, n_2) = 1$. Il existe g_1 et g_2 dans G tels que

- $g = g_1 g_2$,
- g_i est d'ordre n_i,
- $g_1 g_2 = g_2 g_1$.

De plus, g_1 et g_2 sont uniques dans le groupe G.

Exemple 1.5.28. — Soit G un groupe. Soit g un élément de G d'ordre $40 = 5 \times 8$. Posons $g_1 = g^{16}$ et $g_2 = g^{-15}$. D'une part g_1 et g_2 sont d'ordre 5 et 8 respectivement (Théorème 1.5.4), d'autre part g_1 et g_2 commutent (ce sont des puissances de g). De plus $g = g_1 g_2$.

Remarque 1.5.7. — Nous n'avons pas supposé que G est abélien dans le Théorème 1.5.7 et il peut ne pas l'être.

Démonstration du Théorème 1.5.7. — Puisque $\mathrm{pgcd}(n_1, n_2) = 1$ il existe des entiers p et q tels que $n_1 p + n_2 q = 1$. Alors $g = g^1 = g^{n_1 p + n_2 q} = g^{n_1 p} g^{n_2 q}$. Le Théorème 1.5.4 assure que g^{n_1} est d'ordre $\frac{n}{n_1} = n_2$. L'égalité $n_1 p + n_2 q = 1$ implique que $\mathrm{pgcd}(p, n_2) = 1$; par conséquent $(g^{n_1})^p = g^{n_1 p}$ est d'odre n_2 (Théorème 1.5.4). De même $g^{n_2 q}$ est d'ordre n_1. Posons $g_1 = g^{n_2 q}$

et $g_2 = g^{n_1 p}$. En particulier, g_1 et g_2 étant des puissances de g, ils commutent. Finalement, g_1 et g_2 satisfont les conclusions de l'énoncé.

Montrons maintenant que g_1 et g_2 sont uniques. Raisonnons par l'absurde : supposons qu'il existe g_1, g_2, g_1' et g_2' dans G tels que

- ◇ g_1 et g_1' sont d'ordre n_1 ;
- ◇ g_2 et g_2' sont d'ordre n_2 ;
- ◇ $g_1 g_2 = g_2 g_1$ et $g_1' g_2' = g_2' g_1'$;
- ◇ $g = g_1 g_2 = g_1' g_2'$.

On a $n_1 p + n_2 q = 1$ d'où $g_2 = g_2^{n_1 p + n_2 q} = (g_2^{n_1})^p (g_2^{n_2})^q$.

D'une part $g_2^{n_2} = e = (g_2')^{n_2}$ et donc $g_2 = (g_2^{n_1})^p (g_2^{n_2})^q$ se réécrit $g_2 = (g_2^{n_1})^p$. D'autre part l'identité $g_1 g_2 = g_1' g_2'$ conduit à $(g_1 g_2)^{n_1} = (g_1' g_2')^{n_1}$ soit encore, puisque les facteurs dans les produits commutent entre eux, $g_1^{n_1} g_2^{n_1} = (g_1')^{n_1} (g_2')^{n_1}$, c'est-à-dire $g_2^{n_1} = (g_2')^{n_1}$.

Alors

$$g_2 = (g_2^{n_1})^p (g_2^{n_2})^q = ((g_2')^{n_1})^p ((g_2')^{n_2})^q = (g_2')^{n_1 p + n_2 q} = g_2';$$

ainsi $g_2 = g_2'$ et l'égalité $g_1 g_2 = g_1' g_2'$ implique $g_1 = g_1'$. □

Le fait que dans le Théorème 1.5.7 les éléments g_1 et g_2 commutent est crucial pour démontrer que g_1 et g_2 sont uniques. Si on ne suppose plus que g_1 et g_2 commutent, alors ils ne sont plus nécessairement uniques. Considérons dans $\mathfrak{S}_9$ l'élément $\sigma = (1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9)$. Les cycles apparaissant dans l'écriture de σ sont à support disjoints ; il s'en suit que σ est d'ordre $\mathrm{ppcm}(3, 2, 4) = 12$ (Théorème 1.5.2). Nous pouvons écrire 12 comme 3×4 et il y a deux décompositions $\sigma = g_1 g_2$ avec g_1 d'ordre 3 et g_2 d'ordre 4 possibles

$$(g_1, g_2) = \big((1\ 2\ 3), (4\ 5)(6\ 7\ 8\ 9)\big), \qquad (g_1, g_2) = \big((1\ 2\ 4), (2\ 3\ 4\ 5)(6\ 7\ 8\ 9)\big);$$

dans le premier cas g_1 et g_2 commutent alors que dans le second non.

1.6. Classes et théorème de Lagrange

Nous avons déjà remarqué (Remarque 1.5.1) l'efficacité d'utiliser les interactions des éléments du groupe entre eux pour étudier le groupe. Nous voyons dans ce paragraphe une nouvelle illustration de ce principe.

Relations à droite et à gauche.

Soit G un groupe dont la loi sera notée multiplicativement. Soit H un sous-groupe de G. On a deux relations d'équivalence associées à ce sous-groupe :

- ◇ *équivalence à gauche modulo* H :

$$g\mathcal{R}h \iff \exists\, x \in \mathrm{H},\ h = gx \iff g^{-1}h \in \mathrm{H}$$

- ◇ *équivalence à droite modulo* H :

$$g\mathcal{R}'h \iff \exists\, x \in \mathrm{H},\ h = xg \iff hg^{-1} \in \mathrm{H}$$

On note $g\mathrm{H}$ la *classe d'équivalence à gauche modulo* H de $g \in \mathrm{G}$ et ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ est l'*ensemble des classes à gauche modulo* H.

On note $\mathrm{H}g$ la *classe d'équivalence à droite* modulo H de $g \in \mathrm{G}$ et ${}_{\mathrm{H}}\!\backslash^{\mathrm{G}}$ est l'*ensemble des classes à droite modulo* H.

On a

$$g\mathrm{H} = \{gh \mid h \in \mathrm{H}\} \qquad\qquad \mathrm{H}g = \{hg \mid h \in \mathrm{H}\}$$

Par définition nous avons

Lemme 1.6.1

Soit G un groupe. Soit H un sous-groupe de G. Alors

- ◇ les classes d'équivalence à gauche (resp. à droite) modulo H forment une partition de G ; en particulier elles sont disjointes.
- ◇ Nous avons $g\mathrm{H} = \mathrm{H}$ si et seulement si $g \in \mathrm{H}$.
- ◇ L'ensemble $g\mathrm{H}$ est un sous-groupe de G si et seulement si $g \in \mathrm{H}$.

Remarque 1.6.1. — Notons que g appartient à la fois à $g\mathrm{H}$ et à $\mathrm{H}g$ puisque $g = ge = eg$. En général $g\mathrm{H} \neq \mathrm{H}g$. Néanmoins lorsque G est abélien les classes à gauche et à droite coïncident, *i.e.* $g + \mathrm{H} = \mathrm{H} + g$ pour tous $g \in \mathrm{G}$ et $\mathrm{H} \subset \mathrm{G}$.

Remarque 1.6.2. — Un sous-groupe H est une classe à gauche (resp. à droite) modulo H : $\mathrm{H}e = e\mathrm{H} = \mathrm{H}$.

Théorème 1.6.1

Soit G un groupe. Soit H un sous-groupe de G. Toute classe à gauche (resp. à droite) modulo H est en bijection avec H.
En particulier, lorsque H est fini, toute classe à gauche (resp. à droite) a même cardinal que H, *i.e.* $\#g\mathrm{H} = |\mathrm{H}|$ pour tout $g \in \mathrm{H}$.

Démonstration. — Soit $g\mathrm{H}$ une classe à gauche. On peut passer de $g\mathrm{H}$ à H en multipliant à gauche par g^{-1} : $g^{-1}(gh) = h \in \mathrm{H}$.

Réciproquement, on peut passer de H à $g\mathrm{H}$ en multipliant à gauche par g.

Ces deux opérations étant inverses l'une de l'autre nous obtenons que $g\mathrm{H}$ et H sont en bijection. □

Les ensembles $g\mathrm{H}$ et $\mathrm{H}g$ sont en bijection mais il n'y a aucune raison pour qu'ils soient égaux. Il existe néanmoins des sous-groupes qui ont la particularité d'avoir leurs classes à droite et à gauche égales, des sous-groupes pour lesquels pour tout $g \in \mathrm{G}$ on a $g\mathrm{H} = \mathrm{H}g$. Ces sous-groupes joueront un rôle capital par la suite.

Définition 1.6.1

Un sous-groupe H d'un groupe G est *distingué* si $g\mathrm{H} = \mathrm{H}g$ pour tout $g \in \mathrm{G}$.
On note $\mathrm{H} \triangleleft \mathrm{G}$.

Exemple 1.6.1. — Considérons le sous-groupe $\mathrm{H} = \{\pm 1\}$ de $\mathbb{R}^\times$; la classe de x modulo H est $x\mathrm{H} = \{x, -x\}$.

Exemple 1.6.2. — Considérons le sous-groupe $\mathrm{H} = \{\mathrm{id}, (1\ 2)\}$ de $\mathfrak{S}_3$. Les classes à gauche et à droite de g suivant H sont données par

g	$g\mathrm{H}$	$\mathrm{H}g$
id	$\{\mathrm{id}, (1\ 2)\}$	$\{\mathrm{id}, (1\ 2)\}$
$(1\ 2)$	$\{\mathrm{id}, (1\ 2)\}$	$\{\mathrm{id}, (1\ 2)\}$
$(1\ 3)$	$\{(1\ 3), (1\ 2\ 3)\}$	$\{(1\ 3), (1\ 3\ 2)\}$
$(2\ 3)$	$\{(2\ 3), (1\ 3\ 2)\}$	$\{(2\ 3), (1\ 2\ 3)\}$
$(1\ 2\ 3)$	$\{(1\ 3), (1\ 2\ 3)\}$	$\{(2\ 3), (1\ 2\ 3)\}$
$(1\ 3\ 2)$	$\{(2\ 3), (1\ 3\ 2)\}$	$\{(1\ 3), (1\ 3\ 2)\}$

Si $g = (1\ 3)$, alors $g\mathrm{H} = \{(1\ 3), (1\ 2\ 3)\}$ ne contient pas id, *i.e.* une classe n'est pas un groupe.

Notons par exemple que si $g = (2\ 3)$ alors $g\mathrm{H} \neq \mathrm{H}g$.

Remarquons que $\mathrm{H}(1\ 3) = \mathrm{H}(1\ 3\ 2)$: deux éléments distincts peuvent avoir la même classe suivant H.

Le tableau précédent nous permet d'illustrer le Lemme 1.6.1 :

$$\mathfrak{S}_3 = \mathrm{H} \cup (1\ 3)\mathrm{H} \cup (2\ 3)\mathrm{H}.$$

On constate que l'ensemble des classes à gauche modulo H est

$$\mathfrak{S}_3/\mathrm{H} = \{\mathrm{H}, (1\ 3)\mathrm{H},\ (2\ 3)\mathrm{H}\} = \{\{\mathrm{id}, (1\ 2)\}, \{(1\ 3), (1\ 2\ 3), \{(2\ 3), (1\ 3\ 2)\}\}.$$

Exemple 1.6.3. — Soit $\mathrm{G} = \mathbb{Z}$; considérons $\mathrm{H} = n\mathbb{Z}$ pour $n > 0$, c'est un sous-groupe de G.

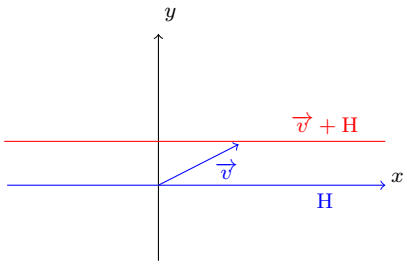
Les classes modulo H sont les $k + n\mathbb{Z}$, $k \in \mathbb{Z}$. Remarquons qu'il s'agit aussi de la classe de k modulo n.

La décomposition de G en classes à gauche modulo H correspond à la décomposition de $\mathbb{Z}$ en classes de congruence modulo n :

$$\mathbb{Z} = n\mathbb{Z} \cup (1 + n\mathbb{Z}) \cup (2 + n\mathbb{Z}) \cup \ldots \cup (n - 1 + n\mathbb{Z}).$$

Exemple 1.6.4. — Soient $\mathrm{G} = \mathbb{R}^2$ et $\mathrm{H} = \mathbb{R}e_1$ l'axe des abscisses. La classe à gauche du vecteur $v \in \mathbb{R}^2$ modulo H est

$$v + \mathrm{H} = v + \mathbb{R}e_1 = \{v + ce_1 \mid c \in \mathbb{R}\} :$$



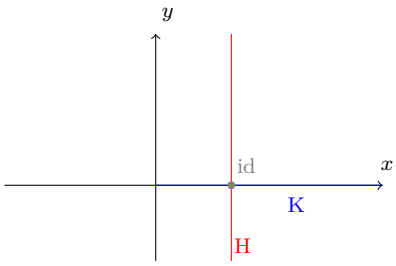
En général, les classes modulo H sont des droites parallèles à H. Deux droites parallèles sont ou bien égales, ou bien disjointes donc deux classes modulo H sont ou bien égales, ou bien disjointes.

Exemple 1.6.5. — Soit $\mathrm{G} = \mathrm{Aff}^+(\mathbb{R})$ le groupe constitué des matrices de la forme $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ avec $x > 0$. On peut identifier les éléments de G avec les points du plan (x, y) tels que $x > 0$; ces points forment un demi-plan :

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \leftrightarrow (x, y) \in \mathbb{R}_{>0} \times \mathbb{R}$$

Par exemple la matrice id correspond au point $(1, 0)$. Tout élément $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ de $\mathrm{Aff}^+(\mathbb{R})$ s'écrit sous la forme $\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$; on introduit alors les groupes

$$\mathrm{H} = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \mid y \in \mathbb{R} \right\} \qquad \& \qquad \mathrm{K} = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \mid x > 0 \right\}$$



Soit $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ dans $\mathrm{Aff}^+(\mathbb{R})$; déterminons sa classe à gauche (resp. à droite) modulo H, *i.e.* déterminons $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\mathrm{H}$ (resp. $\mathrm{H}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$). Soit $\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ dans H ; alors d'une part

$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ay+b \\ 0 & 1 \end{pmatrix}$, d'autre part $\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & y+b \\ 0 & 1 \end{pmatrix}$. Rappelons qu'ici a et b sont fixés alors que y parcourt $\mathbb{R}$; ainsi $ay+b$ parcourt $\mathbb{R}$ et $b+y$ aussi. Il en résulte que la classe à gauche de $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ modulo H coïncide avec la classe à droite de $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ modulo H et

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\mathrm{H} = \mathrm{H}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \left\{\begin{pmatrix} a & t \\ 0 & 1 \end{pmatrix} \mid t \in \mathbb{R}\right\}.$$

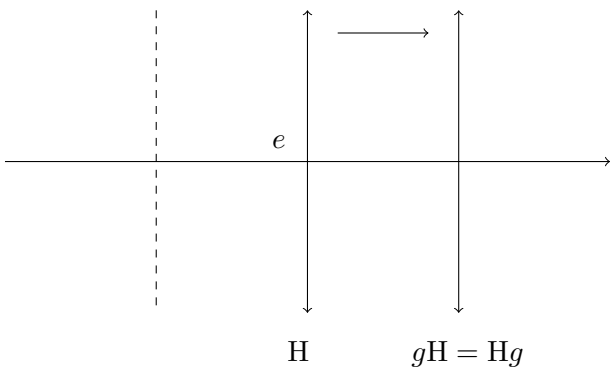
Déterminons la classe de $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ modulo K ; si $x > 0$, alors

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ax & b \\ 0 & 1 \end{pmatrix}$$

Lorsque x parcourt $\mathbb{R}^{+\times}$, $\begin{pmatrix} ax & b \\ 0 & 1 \end{pmatrix}$ est une matrice de la forme $\begin{pmatrix} t & b \\ 0 & 1 \end{pmatrix}$ avec t qui parcourt $\mathbb{R}^{+\times}$. Par suite

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\mathrm{K} = \left\{\begin{pmatrix} t & b \\ 0 & 1 \end{pmatrix} \mid t > 0\right\};$$

en particulier la classe à gauche de $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ modulo K est indépendante du choix de a : $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\mathrm{K} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\mathrm{K}$. C'est la droite horizontale passant par (a, b) :



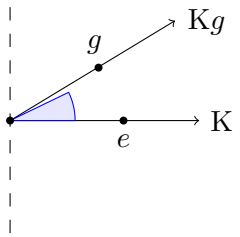
Déterminons désormais la classe à droite de $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ modulo K :

$$\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ax & bx \\ 0 & 1 \end{pmatrix}$$

D'une part lorsque x varie dans $\mathbb{R}^{+\times}$ ax aussi ; d'autre part si on désigne ax par u et xb par v alors $x = \frac{u}{a}$ et $v = xb = \frac{u}{a}b$. Finalement

$$\mathrm{K}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} u & \frac{ub}{a} \\ 0 & 1 \end{pmatrix} \mid u > 0 \right\}$$

C'est une demi-droite « d'extrémité » l'origine et de pente $\frac{b}{a}$:



En particulier, les classes à gauche et à droite de $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ suivant K ne sont pas les mêmes dès que $b \neq 0$. Nous retrouvons la propriété évoquée dans le Lemme 1.6.1 : les classes à gauche (resp. à droite) de K forment une partition de $\mathrm{Aff}^+(\mathbb{R})$:

$$\mathrm{Aff}^+(\mathbb{R}) = \bigcup_{b\in\mathbb{R}} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mathrm{K}.$$

Remarquons que

$$\mathrm{Aff}^+(\mathbb{R})/\mathrm{K} = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$$

Dans la suite nous allons énoncer des propriétés sur les classes à gauche ; elles sont bien entendu valables pour les classes à droite. Soit G un groupe. Soit H un sous-groupe de G ; bien sûr $\mathrm{H} = e\mathrm{H} = \mathrm{H}e$. Il est possible d'avoir $g\mathrm{H} = \mathrm{H}$ même lorsque $g \neq e$. Par exemple si $\mathrm{G} = \mathbb{Z}$ et $\mathrm{H} = 5\mathbb{Z}$ nous avons $10 + 5\mathbb{Z} = 5\mathbb{Z}$; plus généralement, si a est un multiple de 5, *i.e.* si a appartient à $5\mathbb{Z}$, alors $a + 5\mathbb{Z} = 5\mathbb{Z}$. L'énoncé qui suit répond à la question : quand a-t-on $g\mathrm{H} = \mathrm{H}$?

Théorème 1.6.2

Soit G un groupe. Soit H un sous-groupe de G. Soit $g \in \mathrm{G}$. Alors $g\mathrm{H} = \mathrm{H}$ si et seulement si $g \in \mathrm{H}$.

Démonstration. — Soit $g \in \mathrm{G}$. Alors $g\mathrm{H} = \mathrm{H}$ si et seulement si $g \in \mathrm{H}$. Puisque $g = ge$ appartient à $g\mathrm{H}$, avoir $g\mathrm{H} = \mathrm{H}$ nécessite d'avoir $g \in \mathrm{H}$.

Réciproquement, soit g un élément de H. Comme H est un sous-groupe de G pour tout $h \in \mathrm{H}$ nous avons $gh \in \mathrm{H}$; autrement dit $g\mathrm{H} \subset \mathrm{H}$. Remarquons que tout $h \in \mathrm{H}$ s'écrit $g(g^{-1}h)$, que $g^{-1}h$ appartient à H et h à $g\mathrm{H}$, *i.e.* $\mathrm{H} \subset g\mathrm{H}$. Finalement si g appartient à H, alors $\mathrm{H} = g\mathrm{H}$. □

Exemple 1.6.6. — Considérons le sous-groupe $\mathrm{H} = \{\mathrm{id}, s\}$ de D_8. Les éléments r et r^2 appartiennent à $\mathrm{D}_8 \smallsetminus \mathrm{H}$ et leur classe à gauche modulo H n'est pas égal à H :

$$r\mathrm{H} = \{r, rs\}, \qquad r^2\mathrm{H} = \{r^2, r^2s\}.$$

Pour tout entier $n \neq 0$ le nombre de classes à gauche $n\mathbb{Z}$ dans $\mathbb{Z}$ est $|n|$. Nous pouvons passer de $\mathbb{Z}$ à un groupe général et compter le nombre de classes à gauche :

Définition 1.6.2

Soit G un groupe. Soit H un sous-groupe de G. L'*indice* de H dans G est le nombre de classes à gauche modulo H dans G ; autrement dit l'indice de H dans G est le cardinal de G/H. Ce nombre qui est un entier positif ou $+\infty$ est noté $[\mathrm{G} : \mathrm{H}]$.

Le terme indice est dû à Cauchy. Concrètement l'indice d'un sous-groupe nous indique combien de fois nous devons translater H pour recouvrir G.

Exemple 1.6.7. — Reprenons l'Exemple 1.6.2. Puisque $\mathrm{H} = \{\mathrm{id}, (1\ 2)\}$ a trois classes à gauche dans $\mathfrak{S}_3$ nous obtenons $[\mathfrak{S}_3 : \mathrm{H}] = 3$.

Exemple 1.6.8. — Le sous-groupe $\mathrm{H} = \{\mathrm{id}, s\}$ de D_8 a quatre classes à gauche :

$$\mathrm{H}, \qquad r\mathrm{H} = \{r, rs\}, \qquad r^2\mathrm{H} = \{r^2, r^2s\}, \qquad r^3\mathrm{H} = \{r^3, r^3s\}.$$

L'indice de H dans D_8 est donc 4.

Exemple 1.6.9. — Déterminons l'indice de $15\mathbb{Z}$ dans $3\mathbb{Z}$, *i.e.* $[3\mathbb{Z} : 15\mathbb{Z}]$. Modulo 15 un multiple de 3 est congru à 0, 3, 6, 9 ou 12 ; autrement dit nous avons

$$3\mathbb{Z} = 15\mathbb{Z} \cup (3 + 15\mathbb{Z}) \cup (6 + 15\mathbb{Z}) \cup (9 + 15\mathbb{Z}) \cup (12 + 15\mathbb{Z})$$

et cette union est disjointe. Il en résulte que $[3\mathbb{Z} : 15\mathbb{Z}] = 5$.

Exemple 1.6.10. — L'indice de $\mathbb{Z}$ dans $\mathbb{R}$ est infini, *i.e.* $[\mathbb{R} : \mathbb{Z}]$ est infini. Tout nombre réel modulo l'addition d'un entier est un nombre appartenant à $[0, 1)$. Soit x un élément de $[0, 1)$; il n'est pas le $\mathbb{Z}$-translaté d'un autre élément de $[0, 1)$ d'où

$$\mathbb{R} = \bigcup_{0 \leq x < 1} (x + \mathbb{Z})$$

et cette union est disjointe. En particulier, il y a une infinité de classes modulo $\mathbb{Z}$ dans $\mathbb{R}$, c'est-à-dire $[\mathbb{R} : \mathbb{Z}] = \infty$.

Pouvons-nous faire de G/H un groupe en utilisant la loi de G comme nous l'avons fait avec $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}$? L'idée « naturelle » serait de définir sur G/H la loi

$$\mathrm{G}/\mathrm{H} \times \mathrm{G}/\mathrm{H} \to \mathrm{G}/\mathrm{H}, \qquad (g_1\mathrm{H}, g_2\mathrm{H}) \mapsto g_1\mathrm{H} \cdot g_2\mathrm{H} = (g_1g_2)\mathrm{H}. \tag{1.6.1}$$

Malheureusement une telle opération n'a pas toujours un sens. Le membre de droite $(g_1g_2)\mathrm{H}$ peut changer si nous modifions les représentants g_1 et g_2 sans que les classes $g_1\mathrm{H}$ et $g_2\mathrm{H}$ ne soient changées.

Exemple 1.6.11. — Considérons le sous-groupe $\mathrm{H} = \{\mathrm{id}, (1\ 2)\}$ de $\mathfrak{S}_3$. Soient $g_1 = (1\ 3)$, $g_2 = (2\ 3)$, $g_1' = (1\ 2\ 3)$ et $g_2' = (1\ 3\ 2)$. Alors

- $g_1\mathrm{H} = g_1'\mathrm{H} = \{(1\ 3), (1\ 2\ 3)\}$,
- $g_2\mathrm{H} = g_2'\mathrm{H} = \{(2\ 3), (1\ 3\ 2)\}$,
- $g_1\mathrm{H} \cdot g_2\mathrm{H} = (g_1g_2)\mathrm{H} = (132)\mathrm{H} \neq \mathrm{H} = (g_1'g_2')\mathrm{H} = g_1'\mathrm{H} \cdot g_2'\mathrm{H}$.

Si G est abélien, le problème illustré dans l'exemple précédent n'existe pas : si $g_1\mathrm{H} = g_1'\mathrm{H}$ et $g_2\mathrm{H} = g_2'\mathrm{H}$, alors $g_1g_2\mathrm{H} = g_1'g_2'\mathrm{H}$. Il en résulte que G/H muni de la loi (1.6.1) est un groupe.

Si G n'est pas abélien, alors il peut exister des sous-groupes H de G, appelés sous-groupes distingués (cette notion sera reprise au Chapitre 6, §**??**), pour lesquels si $g_1\mathrm{H} = g_1'\mathrm{H}$ et $g_2\mathrm{H} = g_2'\mathrm{H}$, alors $g_1g_2\mathrm{H} = g_1'g_2'\mathrm{H}$ auquel cas G/H muni de la loi (1.6.1) est un groupe.

Il y a plusieurs raisons à notre volonté d'obtenir un groupe quotient G/H et non pas seulement un ensemble :

- l'utilité de l'arithmétique modulaire dans $\mathbb{Z}/n\mathbb{Z}$ (en théorie des nombres, cryptographie...) suggère qu'une construction analogue pour d'autres groupes mérite considération ;
- cela permet de construire un nouveau groupe à partir de G et de H ;
- lorsque G est fini et H est un sous-groupe non trivial de G, alors H et G/H sont deux groupes d'ordre inférieur à $|\mathrm{G}|$ ce qui peut s'avérer utile pour démontrer des théorèmes sur les groupes finis par récurrence sur l'ordre du groupe.

Les classes d'équivalence forment une partition du groupe. Si le groupe est fini, le théorème 1.6.1 nous indique que ces classes ont toutes le même nombre d'éléments. Nous en déduisons les deux résultats suivants :

Théorème 1.6.3

Soit G un groupe fini. Soit H un sous-groupe de G. L'ordre de G et l'ordre de H sont reliés à l'indice de H dans G par la formule :

$$|\mathrm{G}| = |\mathrm{H}| \cdot \#\mathrm{G}/\mathrm{H} = |\mathrm{H}| \cdot [\mathrm{G} : \mathrm{H}].$$

Théorème 1.6.4: (Théorème de Lagrange)

Soit G un groupe fini. Soit H un sous-groupe de G. L'ordre de H divise l'ordre de G.

Exemple 1.6.12. — Déterminons les sous-groupes du groupe des quaternions

$$\mathbb{H}_8 = \{1,\, -1,\, i,\, -i,\, j,\, -j,\, k,\, -k\}.$$

Soit G un sous-groupe de $\mathbb{H}_8$. D'après le Théorème de Lagrange l'ordre de G divise $|\mathbb{H}_8| = 8$, autrement dit $|\mathrm{G}| \in \{1,\, 2,\, 4,\, 8\}$.

- ◇ Si $|\mathrm{G}| = 1$, alors comme $1 \in \mathrm{G}$ nous avons $\mathrm{G} = \{e\}$.
- ◇ Si $|\mathrm{G}| = 8$, alors puisque $\mathrm{G} \subset \mathbb{H}_8$ nous avons $\mathrm{G} = \mathbb{H}_8$.
- ◇ Si $|\mathrm{G}| = 2$, alors G est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (Corollaire 2.2.1) ; en particulier G est engendré par un élément d'ordre 2. Or -1 est l'unique élément d'ordre 2 de $\mathbb{H}_8$ donc $\mathrm{G} = \langle -1 \rangle$.
- ◇ Si $|\mathrm{G}| = 2$, alors G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/4\mathbb{Z}$ (Théorème 2.2.7). Étant donné que $\mathbb{H}_8$ contient un unique élément d'ordre 2 le groupe G ne peut pas être isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si G est isomorphe à $\mathbb{Z}/4\mathbb{Z}$, alors G est engendré par un élément d'ordre 4. Le groupe $\mathbb{H}_8$ contient six éléments d'ordre 4 qui engendrent trois sous-groupes d'ordre 4 distincts

$$\langle i \rangle = \langle -i \rangle, \qquad \langle j \rangle = \langle -j \rangle, \qquad \langle k \rangle = \langle -k \rangle.$$

Finalement les sous-groupes de $\mathbb{H}_8$ sont

$$\{\mathrm{id}\}, \qquad \langle -1 \rangle, \qquad \langle i \rangle, \qquad \langle j \rangle, \qquad \langle k \rangle, \qquad \mathbb{H}_8.$$

Nous verrons plus tard d'autres applications du Théorème de Lagrange. La réciproque du Théorème de Lagrange :

« si d est un diviseur de l'ordre de G alors il existe un sous-groupe d'ordre d »

est vraie pour certains groupes (tous les groupes cycliques) mais fausse en général comme nous allons le voir dans les exemples qui suivent.

Exemple 1.6.13. — Le plus petit contre-exemple à la réciproque du Théorème de Lagrange est le sous-groupe $\mathcal{A}_4$ [5] de $\mathfrak{S}_4$ défini par

$$\mathcal{A}_4 = \{\mathrm{id},\, (2\ 3\ 4),\, (2\ 4\ 3),\, (1\ 2)(3\ 4),\, (1\ 2\ 3),\, (1\ 2\ 4),\, (1\ 3\ 2),\, (1\ 3\ 4),\, (1\ 3)(2\ 4),\, (1\ 4\ 2),\, (1\ 4\ 3),\, (1\ 4)(2\ 3)\}$$

On remarque que $\mathcal{A}_4$ est d'ordre 12. Alors que $\mathcal{A}_4$ possède des sous-groupes d'ordre 1, 2, 3, 4 et 12 il n'en possède pas d'ordre 6. En effet, raisonnons par l'absurde : supposons que $\mathcal{A}_4$ possède un sous-groupe H d'ordre 6. Alors $[\mathcal{A}_4 : \mathrm{H}] = 2$, *i.e.* il y a deux classes modulo H dans $\mathcal{A}_4$.

Montrons que pour tout $g \in \mathcal{A}_4$ alors g^2 appartient à H. Soit g un élément de $\mathcal{A}_4$.

- ◇ Si g appartient à H, alors g^2 appartient à H.

5. Pour une définition de $\mathcal{A}_n$, $n \geq 2$, on renvoie au Chapitre 5, §5.1.

◇ Si g n'appartient pas à H, alors $g\mathrm{H} \neq \mathrm{H}$ (Théorème 1.6.2). Puisque $[\mathcal{A}_4 : \mathrm{H}] = 2$, H et $g\mathrm{H}$ sont les deux seules classes modulo H. Laquelle est $g^2\mathrm{H}$? Si $g^2\mathrm{H} = g\mathrm{H}$, alors g^2 appartient à $g\mathrm{H}$ (Théorème 1.6.2), c'est-à-dire g^2 s'écrit gh pour un certain $h \in \mathrm{H}$; nous en déduisons après multiplication à gauche par g^{-1} que $g = h$. En particulier puisque h appartient à H, nous obtenons que g appartient à H : contradiction. Il en résulte que $g^2\mathrm{H} = \mathrm{H}$; le Théorème 1.6.2 assure alors que g^2 appartient à H.

Finalement si g est un élément de $\mathcal{A}_4$, alors g^2 est un élément de H.

Si $(a\ b\ c)$ est un 3-cycle de $\mathcal{A}_4$, alors $(a\ b\ c) = (a\ b\ c)^4 = \left((a\ b\ c)^2\right)^2$; ainsi tout 3-cycle de $\mathcal{A}_4$ est le carré d'un 3-cycle de $\mathcal{A}_4$. Il s'en suit que H contient tous les 3-cycles de $\mathcal{A}_4$; or $\mathcal{A}_4$ compte huit 3-cycles

$$(1\ 2\ 3),\quad (1\ 3\ 2),\quad (1\ 2\ 4),\quad (1\ 4\ 2),\quad (1\ 3\ 4),\quad (1\ 4\ 3),\quad (2\ 3\ 4),\quad (2\ 4\ 3)$$

d'où $|\mathrm{H}| \geq 8$: contradiction avec $|\mathrm{H}| = 6$.

Exemple 1.6.14. — Un second contre-exemple à la réciproque du Théorème de Lagrange est $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$. Ce groupe est d'ordre 24 ; il possède des sous-groupes d'ordre 1, 2, 3, 4, 6, 8 et 24 mais pas 12.

Raisonnons par l'absurde : supposons que $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ possède un sous-groupe d'ordre 12. Alors H est d'indice 2 dans $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$; comme dans l'Exemple 1.6.13 si g désigne un élément de $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$, alors g^2 appartient à H. On peut vérifier qu'il y a dix carrés $M_1, M_2, \ldots, M_{10}$ dans $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$; ainsi H contient id, $M_1, M_2, \ldots, M_{10}$. Quitte à réindicer les M_i nous pouvons supposer que $M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^2$ et $M_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^2$. Nous en déduisons que $M_1M_2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ et $M_2M_1 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ appartiennent à H. On peut vérifier que M_1M_2 et M_2M_1 ne sont pas des carrés ; en particulier, $M_1M_2 \neq M_i$ pour tout $1 \leq i \leq 10$ et $M_2M_1 \neq M_i$ pour tout $1 \leq i \leq 10$. Il en résulte que H contient les treize éléments distincts suivants : id, $M_1, M_2, \ldots, M_{10}, M_1M_2, M_2M_1$: contradiction avec $|\mathrm{H}| = 12$.

Remarque 1.6.3. — Il n'y a pas de critère simple pour déterminer si un groupe fini satisfait la réciproque du Théorème de Lagrange. Les groupes abéliens, les groupes diédraux, les groupes d'ordre p^k avec p premier satisfont la réciproque du Théorème de Lagrange.

Donnons maintenant quelques applications du Théorème de Lagrange. Pour montrer que a divise b on peut trouver un groupe d'ordre b qui contient un sous-groupe d'ordre a :

Corollaire 1.6.1

Les coefficients binomiaux sont des entiers : soient $n \geq 1$ et $0 \leq m \leq n$ le quotient $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ est un entier.

Démonstration. — Considérons l'ensemble H des permutations de $\mathfrak{S}_n$ qui induisent une permutation de $\{1, 2, \ldots, m\}$ et une permutation de $\{m+1, m+2, \ldots, n\}$.

On peut vérifier que d'une part H est un sous-groupe de $\mathfrak{S}_n$, d'autre part $|\mathrm{H}| = m!(n-m)!$ Le Théorème de Lagrange (Théorème 1.6.4) assure que $|\mathrm{H}|$ divise $\mathfrak{S}_n$ c'est-à-dire que $m!(n-m)!$ divise $n!$ □

Corollaire 1.6.2

Soit $n \geq 3$. L'ordre $\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right|$ du groupe des inversibles modulo n est pair. C'est-à-dire que l'indicatrice d'Euler $\phi(n)$ est paire.

Démonstration. — Puisque $\{\pm 1\}$ est un sous-groupe de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$, le théorème de Lagrange assure que $|\{\pm 1\}|$ divise $\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right|$, *i.e.* 2 divise $\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right|$. □

Corollaire 1.6.3

Soit G un groupe fini. Soient H et K deux sous-groupes de G d'ordre premier entre eux. Alors $\mathrm{H} \cap \mathrm{K} = \{e\}$.

Démonstration. — Notons que $\mathrm{H} \cap \mathrm{K}$ est un sous-groupe à la fois de H et de K. D'après le Théorème de Lagrange (Théorème 1.6.4) d'une part $|\mathrm{H} \cap \mathrm{K}|$ divise $|\mathrm{H}|$, d'autre part $|\mathrm{H} \cap \mathrm{K}|$ divise $|\mathrm{K}|$. Comme $|\mathrm{H}|$ et $|\mathrm{K}|$ sont premiers entre eux, $|\mathrm{H} \cap \mathrm{K}| = 1$, c'est-à-dire $\mathrm{H} \cap \mathrm{K} = \{e\}$. □

Corollaire 1.6.4

Soient p et q deux nombres premiers. Tout sous-groupe propre d'un groupe d'ordre pq est cyclique.

Démonstration. — Soit G un groupe d'ordre pq avec p, q premiers. Soit H un sous-groupe propre de G ; alors $|\mathrm{H}|$ divise pq (Théorème de Lagrange, Théorème 1.6.4). Comme p et q sont premiers, $|\mathrm{H}|$ divise p ou $|\mathrm{H}|$ divise q. Dans chacun de ces cas $|\mathrm{H}|$ est premier et H est cyclique d'après le Corollaire 1.5.5. □

Par exemple si G est un groupe d'ordre 6 (ou 15, ou 21 ou ...), alors l'ensemble des sous-groupes de G est

$$\{\langle g \rangle \mid g \in \mathrm{G} \smallsetminus \{e\}\} \cup \{e\} \cup \mathrm{G}.$$

Voici une application du Théorème de Lagrange qui permet de caractériser les groupes cycliques à partir d'informations combinatoires sur leurs sous-groupes :

Théorème 1.6.5

Un groupe fini qui possède au plus un sous-groupe de chaque ordre possible est cyclique.

Démonstration. — Soit G un groupe d'ordre n, on note $\mathcal{C}$ l'ensemble de ses sous-groupes cycliques. On définit $\Psi\colon \mathrm{G} \to \mathcal{C}$, $g \mapsto \langle g \rangle$. Il s'agit d'une application surjective et le Théorème de factorisation (Corollaire 1.1.1) nous permet de conclure que sa projection, $\bar{\Psi}\colon {}^{\mathrm{G}}\!/_{\mathcal{R}_\Psi} \to \mathcal{C}$, $\bar{g} \mapsto \langle g \rangle$, est une application bijective.

Soit $g \in \mathrm{G}$, on note d son ordre. Étant donné $h \in \mathrm{G}$, d'après le Théorème 1.5.4 on a $\bar{h} = \bar{g}$ si et seulement si il existe k, premier avec d, tel que $h = g^k$. On en déduit que le cardinal de $\bar{g}$ est le nombre d'entiers dans $[\![1, d]\!]$ qui sont premiers avec d. On reconnaît l'indicatrice d'Euler de d, introduite dans la Définition 1.3.1, et notée $\phi(d)$.

On a donc montré que si g est d'ordre d alors : $\#\bar{g} = \phi(d)$.

Soit $\mathcal{G}_d$ l'ensemble des éléments $\bar{g}$ de ${}^{\mathrm{G}}\!/_{\mathcal{R}_\Psi}$ tels que $|g| = d$. On a

$$\bar{\Psi}(\mathcal{G}_d) = \{\mathrm{H} \subset \mathrm{G} \,|\, \mathrm{H} \text{ sous-groupe cyclique d'ordre } d\}\cdot$$

L'application $\bar{\Psi}$ étant une bijection ces deux ensembles ont le même cardinal noté α_d. Puisque les classes d'équivalence fournissent une partition de G, on a :

$$\begin{aligned} |\mathrm{G}| &= \sum_{\bar{g} \in {}^{\mathrm{G}}\!/_{\mathcal{R}_\Psi}} \#\bar{g} = \sum_{d|n} \sum_{\bar{g} \in \mathcal{G}_d} \#\bar{g} = \sum_{d|n} \phi(d)\alpha_d \\ &= \sum_{d|n} \phi(d)\, \#\{\mathrm{H} \subset \mathrm{G} \,|\, \mathrm{H} \text{ sous-groupe cyclique d'ordre } d\}\cdot \end{aligned}$$

Cette relation est vraie pour tout groupe G d'ordre fini. Elle l'est donc en particulier pour ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. Le Théorème 1.5.5 fournit une description complète des sous-groupes de tout groupe cyclique. Pour chaque diviseur d de n il existe un unique groupe d'ordre d. Autrement dit, dans ce cas, on a $\alpha_d = 1$ et la relation s'écrit alors

$$n = \sum_{d|n} \phi(d)\cdot$$

Revenons maintenant au cas d'un groupe G qui possède au plus un sous-groupe de chaque ordre. C'est-à-dire un groupe pour lequel on a $\alpha_d \leq 1$ pour tout d divisant n. On a

$$n = \sum_{d|n} \phi(d) = \sum_{d|n} \phi(d)\alpha_d \quad \text{soit} \quad \sum_{d|n} \phi(d)(1 - \alpha_d) = 0.$$

Comme $\phi(d) > 0$ et $(1 - \alpha_d) \geq 0$, cette égalité nous permet de conclure que pour tout diviseur d de n on a $(1 - \alpha_d) = 0$. On a en particulier $\alpha_n = 1$. Il existe donc un sous-groupe d'ordre n qui est cyclique. C'est nécessairement G puisqu'il est son unique sous-groupe d'ordre n.

□

Corollaire 1.6.5

Soit G un groupe fini tel que pour tout diviseur d de G l'équation $x^d = 1$ a au plus d solutions dans G. Alors G est cyclique.

Démonstration. — Nous allons montrer que G a au plus un sous-groupe de chaque ordre. Si H est un sous-groupe de G d'ordre d, alors tout élément de H satisfait l'équation $x^d = 1$ et, par hypothèse, H coïncide avec l'ensemble des solutions dans G de l'équation $x^d = 1$. Ceci montre qu'il y a au plus un sous-groupe d'ordre d ; en effet, si H et H′ sont tous deux égaux à $\{g \in \mathrm{G} \mid g^d = 1\}$, alors $\mathrm{H} = \mathrm{H}'$. □

1.7. Générateurs d'un groupe

1.7.1. Définitions, exemples et propriétés. — Dans $\mathbb{R}^n$ tout vecteur s'écrit comme une unique combinaison linéaire des vecteurs $e_1, e_2, \ldots, e_n$ de la base canonique. Une notion un peu plus « faible » que la notion de base est la notion de système de générateurs : les vecteurs v_1, $v_2, \ldots, v_k$ de $\mathbb{R}^n$ sont un système de générateurs de $\mathbb{R}^n$ si l'ensemble des combinaisons linéaires des v_i coïncide avec $\mathbb{R}^n$:

$$\left\{\sum_{i=1}^{k} \lambda_i v_i \,|\, \lambda_i \in \mathbb{R}\right\} = \mathbb{R}^n.$$

La différence entre une base de $\mathbb{R}^n$ et un système de générateurs de $\mathbb{R}^n$ est que le second « peut contenir plus de vecteurs que nécessaire ». Par exemple $((1,0), (2,1), (3,1))$ est un système de générateurs de $\mathbb{R}^2$ mais n'est pas une base de $\mathbb{R}^2$; par contre les vecteurs $(1,0)$ et $(2,1)$ (respectivement $(1,0)$ et $(3,1)$, respectivement $(2,1)$ et $(3,1)$) forment une base de $\mathbb{R}^2$. Une base est un système de générateurs minimal.

En théorie des groupes il existe aussi une notion de système de générateurs :

Définitions 1.7.1

Soit G un groupe. Les éléments $g_1, g_2, \ldots, g_n$ de G forment un *système de générateurs* ou plus simplement sont des *générateurs* si tout élément $g \in \mathrm{G}$ s'écrit

$$g = g_1^{m_1} g_2^{m_2} \ldots g_n^{m_n}$$

où les m_i désignent des éléments de $\mathbb{Z}$.
On dit aussi que $g_1, g_2, \ldots, g_n$ *engendrent* G.
On écrit $\mathrm{G} = \langle g_1, g_2, \ldots, g_n \rangle$.
Si G admet un système de générateurs fini, on dit que G est *finiment engendré* ou que G est *de type fini*.

Remarque 1.7.1. — Une définition analogue est la suivante. Soit G un groupe. Les éléments g_1, g_2, …, g_n de G forment un système de générateurs si tout élément $g \in \mathrm{G}$ s'écrit

$$g = g_1^{m_1} g_2^{m_2} \dots g_r^{m_r}$$

où les m_i appartiennent à $\{1, -1\}$; autrement dit au lieu d'écrire $g_1^3 g_2^{-2}$ nous écrivons $g_1 g_1 g_1 g_2^{-1} g_2^{-1}$.

Remarque 1.7.2. — Le sous-groupe engendré par une partie P de G est le plus petit sous-groupe de G contenant P. C'est aussi l'intersection de tous les sous-groupes de G qui contiennent P.

Exemple 1.7.1. — Supposons que $\mathrm{G} = \mathfrak{S}_4$ et $g = (1\ 2)$. On a $g^2 = \mathrm{id}$ et donc $g^{2n} = \mathrm{id}$ pour tout n et $g^{2n+1} = g$ pour tout n. Ainsi $\langle g \rangle$ est simplement l'ensemble à deux éléments $\{\mathrm{id}, g\} = \{\mathrm{id}, (1, 2)\}$.

Exemple 1.7.2. — Supposons que $\mathrm{G} = \mathfrak{S}_4$ et $g = (1\ 2\ 3\ 4)$. Remarquons que $g^4 = \mathrm{id}$. Soit n un entier relatif. Effectuons la division euclidienne de n par 4. Elle fournit une écriture $n = 4q + r$ avec $0 \leq r \leq 3$. On a alors $g^n = g^{4q+r} = (g^4)^q g^r = e^q g^r = g^r$. Ainsi $\langle g \rangle$ est simplement $\{\mathrm{id}, g, g^2, g^3\}$. Comme $3 = 4 - 1$ nous avons $g^3 = g^{-1} = (1\ 4\ 3\ 2)$. Un calcul montre que $g^2 = (1\ 3)(2\ 4)$. Ainsi $\langle h \rangle = \{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$.

Exemple 1.7.3. — Toute permutation de $\mathfrak{S}_n$ est un produit de cycles (Théorème 5.1.1) ; par suite l'ensemble des cycles de $\mathfrak{S}_n$ est un système de générateurs de $\mathfrak{S}_n$.

Exemple 1.7.4. — Le groupe $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est engendré par $(\overline{1}, \overline{0})$ et $(\overline{0}, \overline{1})$; en effet tout élément $(\overline{a}, \overline{b})$ de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ s'écrit $a(\overline{1}, \overline{0}) + b(\overline{0}, \overline{1})$.

Exemple 1.7.5. — Un groupe possédant un ensemble de générateurs réduit à un élément est cyclique. Par exemple $\{1\}$ (respectivement $\{-1\}$) est un système de générateurs de $\mathbb{Z}$.

Exemple 1.7.6. — Les groupes diédraux ont pour système de générateurs $\{r, s\}$.

Exemple 1.7.7. —

Définition 1.7.1

Le *groupe dérivé* de G noté $D(\mathrm{G})$ est le sous-groupe engendré par les *commutateurs* de G, *i.e.* les éléments du type $ghg^{-1}h^{-1}$ avec g, $h \in \mathrm{G}$.

Le commutateur de g et h est appelé ainsi car il vaut 1 si et seulement si g et h commutent.

Notons que $\mathrm{G}/D(\mathrm{G})$ est abélien. C'est même le plus grand quotient abélien de G, et ceci caractérise $D(\mathrm{G})$.

- ◇ Si G est abélien, alors $D(\mathrm{G}) = \{e_{\mathrm{G}}\}$.
- ◇ Le groupe dérivé du groupe linéaire $\mathrm{GL}(n, \Bbbk)$ est $\mathrm{SL}(n, \Bbbk)$ sauf si $n = 2$ et $\Bbbk = \mathbb{Z}/2\mathbb{Z}$.

◇ Le groupe dérivé du groupe des quaternions $\mathbb{H}_8$ est $\{1, -1\}$.

◇ Le groupe dérivé du groupe $\{x \mapsto ax+b \,|\, a \in \mathbb{C}^*,\, b \in \mathbb{C}\}$ est le groupe $\{x \mapsto x+b \,|\, b \in \mathbb{C}\}$.

◇ Si $\sigma = (1\ 2\ 3)$, alors $D(\mathfrak{S}_3) = \{\mathrm{id},\, \sigma,\, \sigma^2\}$.

Exemple 1.7.8. — Le groupe infini non abélien $\mathrm{G} = \left\{ \begin{pmatrix} a & k \\ 0 & 1 \end{pmatrix} \,|\, a \in \{1, -1\},\, k \in \mathbb{Z} \right\}$ est de type fini. À partir de

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k \qquad \text{et} \qquad \begin{pmatrix} -1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

nous obtenons $\mathrm{G} = \langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$.

Exemple 1.7.9. — Le groupe $\mathbb{Q}$ n'est pas de type fini. Raisonnons par l'absurde : supposons que $\mathbb{Q} = \langle q_1,\, q_2,\, \ldots, q_\ell \rangle$. Soit N le dénominateur commun des rationnels $q_1,\, q_2,\, \ldots,\, q_\ell$. Le dénominateur d'un élément de $\langle q_1,\, q_2,\, \ldots, q_\ell \rangle$ divise N. Ainsi $\frac{1}{N+1}$ n'appartient pas à $\langle q_1,\, q_2,\, \ldots, q_\ell \rangle$ alors que $\frac{1}{N+1}$ appartient à $\mathbb{Q}$: contradiction.

Exemple 1.7.10. — Un groupe de type fini est nécessaire dénombrable. Autrement dit tout groupe non dénombrable n'est pas de type fini.

Certains groupes « classiques » ont un système de générateurs (on renvoie au Chapitre 5, §5.1 pour les groupes $\mathfrak{S}_n$ et $\mathcal{A}_n$, au Chapitre 8.4 pour le groupe $\mathrm{SL}(2, \mathbb{Z})$) :

groupe	système de générateurs	taille
$\mathfrak{S}_n$, $n \geq 2$	$(i\ j)$	$\frac{n(n-1)}{2}$
	$(1\ 2)$, $(1\ 3)$, …, $(1\ n)$	$n-1$
	$(1\ 2)$, $(2\ 3)$, …, $(n-1\ n)$	$n-1$
	$(1\ 2)$, $(1\ 2\ \ldots n)$ si $n \geq 3$	2
	$(1\ 2)$, $(2\ 3\ \ldots n)$ si $n \geq 3$	2
	$(a\ b)$, $(1\ 2\ \ldots n)$ si $\mathrm{pgcd}(b-a, n) = 1$	2
$\mathcal{A}_n$, $n \geq 3$	3-cycles	$\frac{n(n-1)(n-2)}{3}$
	$(1\ i\ j)$	$(n-1)(n-2)$
	$(1\ 2\ i)$	$n-2$
	$(i\ i+1\ i+2)$	$n-2$
	$(1\ 2\ 3)$, $(1\ 2\ \ldots\ n)$ si $n \geq 4$ pair	2
	$(1\ 2\ 3)$, $(1\ 2\ \ldots\ n)$ si $n \geq 4$ impair	2
$\mathrm{SL}(2, \mathbb{Z})$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	2
$\mathrm{GL}(n, \mathbb{R})$	matrices élémentaires	infini
$\mathrm{SL}(n, \mathbb{R})$	matrices élémentaires	infini

Proposition-Définition 1.7.1

Soient G un groupe et $A \subset \mathrm{G}$ une partie de G. Il existe un plus petit sous-groupe H de G contenant A. On dit que H est le *sous-groupe engendré par* A ou encore que les éléments de A sont des *générateurs* de H. Nous notons $\mathrm{H} = \langle A \rangle$.

Démonstration. — L'existence de H peut se voir de deux manières distinctes :

1. ou bien nous considérons tous les sous-groupes de G contenant A (il y a au moins G tout entier) et leur intersection convient ;
2. ou bien nous supposons A non vide (sinon $\mathrm{H} = \{1\}$) et nous posons
$$A^{-1} = \{x \in \mathrm{G} \,|\, x^{-1} \in A\}$$
puis
$$\mathrm{H} = \{a_1 a_2 \ldots a_n \,|\, n \in \mathbb{N},\ a_i \in A \cup A^{-1}\}.$$
Alors H est un groupe, contient A et est évidemment le plus petit possible.

□

1.7.2. Des systèmes de générateurs de $\mathrm{GL}(n, \mathbb{R})$ et $\mathrm{SL}(n, \mathbb{R})$. —

CHAPITRE 2

2.1. Morphismes de groupes

En théorie des groupes les fonctions les plus importantes entre deux groupes sont celles qui « préservent » les lois des deux groupes :

Définition 2.1.1

Soient $(\mathrm{G}, \cdot)$ et $(\mathrm{H}, *)$ deux groupes. Un *morphisme de groupes* (on dit aussi un *homomorphisme de groupes*) entre G et H est une application $\varphi\colon \mathrm{G} \to \mathrm{H}$ telle que

$$\forall\, g,\, h \in \mathrm{G} \qquad \varphi(g \cdot h) = \varphi(g) * \varphi(h)$$

Ici $g \cdot h$ appartient à G et $\varphi(g) * \varphi(h)$ appartient à H ; un morphisme de groupes est donc une fonction qui « transforme » la loi de groupe $\cdot$ de G en celle $*$ de H. Par exemple un morphisme de groupes de $\varphi\colon \mathbb{R} \to \mathbb{R}^*$ satisfait $\varphi(x+y) = \varphi(x)\varphi(y)$ pour tous x, y dans $\mathbb{R}$ alors qu'un morphisme de groupes $\varphi\colon \mathbb{R}^* \to \mathbb{R}$ satisfait $\varphi(xy) = \varphi(x) + \varphi(y)$ pour tous x, y dans $\mathbb{R}^*$.

2.1.1. Premiers exemples. —

Exemple 2.1.1. — Soit c un réel. L'égalité $c(x+y) = cx + cy$ satisfaite pour tous x, y dans $\mathbb{R}$ assure que la fonction

$$M_c\colon \mathbb{R} \to \mathbb{R}, \qquad x \mapsto cx$$

est un morphisme de groupes.

Exemple 2.1.2. — Pour tous nombres réels x et y nous avons $|xy| = |x|\,|y|$. Il en résulte que

$$\varphi\colon \mathbb{R}^* \to \mathbb{R}^{+*}, \qquad x \mapsto |x|$$

est un morphisme de groupes. Notons que nous excluons 0 même si la formule est valable afin que le domaine de définition de φ soit un groupe.

Exemple 2.1.3. — Considérons la « fonction signe »

$$s\colon \mathbb{R}^* \to \{-1, 1\}, \qquad x \mapsto \begin{cases} 1 \text{ si } x > 0 \\ -1 \text{ si } x < 0 \end{cases}$$

Pour tous x, y dans $\mathbb{R}^*$ nous avons $s(xy) = s(x)s(y)$. Par conséquent $s\colon \mathbb{R}^* \to \{-1, 1\}$ est un morphisme de groupes.

Exemple 2.1.4. — Pour tous nombres réels x et y nous avons $(xy)^2 = x^2y^2$; il s'en suit que la « fonction carrée »

$$f\colon \mathbb{R}^* \to \mathbb{R}^* \qquad x \mapsto x^2$$

est un morphisme de groupes (notons que là encore nous excluons 0 même si $(xy)^2 = x^2y^2$ est encore valable si $x = 0$ ou $y = 0$ afin que le domaine de définition de f soit un groupe). Remarquons que la « fonction carrée » est aussi un morphisme de $\mathbb{R}^*$ dans $\mathbb{R}^{+*}$, de $\mathbb{R}^{+*}$ dans $\mathbb{R}^*$ et de $\mathbb{R}^{+*}$ dans $\mathbb{R}^{+*}$. Attention une fonction n'est pas complètement déterminée par sa formule mais aussi par ses ensembles de départ et d'arrivée. Ainsi les quatre façons de décrire la « fonction carrée » que nous venons de donner sont quatre fonctions différentes et par suite quatre morphismes de groupes différents ;

- ◇ la « fonction carrée » $\mathbb{R}^* \to \mathbb{R}^*$ n'est ni injective, ni surjective ;
- ◇ la « fonction carrée » $\mathbb{R}^* \to \mathbb{R}^{+*}$ est surjective mais pas injective ;
- ◇ la « fonction carrée » $\mathbb{R}^{+*} \to \mathbb{R}^*$ est injective mais pas surjective ;
- ◇ la « fonction carrée » $\mathbb{R}^{*+} \to \mathbb{R}^*$ est injective et surjective.

Exemple 2.1.5. — Considérons un entier n. Pour tous nombres réels x et y nous avons $(xy)^n = x^ny^n$. Par suite $f\colon \mathbb{R}^* \to \mathbb{R}^*$, $x \mapsto x^n$ est un morphisme de groupes.

Exemple 2.1.6. — Pour tous réels positifs x et y l'égalité $\sqrt{xy} = \sqrt{x}\sqrt{y}$ est satisfaite. Ainsi la fonction racine carrée

$$f\colon \mathbb{R}^{+*} \to \mathbb{R}^{+*}, \qquad x \mapsto \sqrt{x}$$

est un morphisme de groupes.

Exemple 2.1.7. — Soit a un réel non nul. Puisque $a^{m+n} = a^ma^n$ pour tous entiers n et m la fonction

$$f\colon \mathbb{Z} \to \mathbb{R}^*, \qquad n \mapsto a^n$$

satisfait $f(m+n) = f(m)f(n)$ pour tous entiers n et m. Autrement dit f est un morphisme du groupe additif $\mathbb{Z}$ dans le groupe multiplicatif $\mathbb{R}^*$.

Exemple 2.1.8. — Considérons deux réels a et b non nuls et $f\colon \mathbb{Z}^2 \to \mathbb{R}^*$, $(m,n) \mapsto a^m b^n$.

Pour tous couples d'entiers (m,n) et (m',n') nous avons

$$\begin{aligned} f((m,n)+(m',n')) &= f(m+m',n+n') \\ &= a^{m+m'}b^{n+n'} \\ &= a^m a^{m'} b^n b^{n'} \\ &= a^m b^n a^{m'} b^{n'} \\ &= f(m,n)f(m',n')\cdot \end{aligned}$$

On a donc $f((m,n)+(m',n') = f(m,n)f(m',n')$, ce qui fait que f est un morphisme du groupe additif $\mathbb{Z}^2$ dans le groupe multiplicatif $\mathbb{R}^*$.

Cette construction se généralise bien entendu comme suit : si $a_1, a_2, \cdots, a_k$ désignent k réels non nuls, nous obtenons un morphisme de groupes en définissant $f\colon \mathbb{Z}^k \to \mathbb{R}^*$, $(m_1, m_2, \cdots, m_k) \mapsto a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}$.

Exemple 2.1.9. — Soit a un réel strictement positif. L'égalité $a^{x+y} = a^x a^y$, valable pour tous réels x et y, assure que $f : \mathbb{R} \to \mathbb{R}^*$, $x \mapsto a^x$ est un morphisme de groupes. Remarquons que f est injectif et surjectif pour $a \neq 1$. La fonction f est à valeurs dans $\mathbb{R}^*$ et c'est un morphisme de groupes bijectif (on dit que c'est un *isomorphisme de groupes*) si $a \neq 1$.

Exemple 2.1.10. — Soit c un réel. Pour tous x, y dans $\mathbb{R}^{+*}$ nous avons $(xy)^c = x^c y^c$; il en résulte que $f\colon \mathbb{R}^{+*} \to \mathbb{R}^{+*}$, $x \mapsto x^c$ est un morphisme de groupes.

Exemple 2.1.11. — Soit a un réel strictement positif et distinct de 1. Pour tous réels strictement positifs x et y nous avons $\log_a(xy) = \log_a(x) + \log_a(y)$; par suite la fonction logarithme de base a $\log_a : \mathbb{R}^{+*} \to \mathbb{R}$ est un morphisme de groupes.

Exemple 2.1.12. — Pour tous z, w dans $\mathbb{C}$ nous avons $\overline{z+w} = \overline{z} + \overline{w}$ et $\overline{zw} = \overline{z}\,\overline{w}$. Ainsi la conjugaison complexe définit deux morphismes de groupes, l'un de $(\mathbb{C},+)$ dans lui-même et l'autre de $(\mathbb{C}^*,\times)$ dans lui même.

Exemple 2.1.13. — Pour tous z, w dans $\mathbb{C}$ nous avons $|zw| = |z|\,|w|$. Par conséquent l'application $|\cdot|\colon \mathbb{C}^* \to \mathbb{R}^{+*}$, $z \mapsto |z|$ est un morphisme de groupes. Notons que nous excluons 0 même si la formule est valable afin que le domaine de définition de f soit un groupe.

Exemple 2.1.14. — Rappelons les deux formules suivantes valables pour tous x, y réels

$$\circledast \quad \left\{ \begin{array}{rcl} \sin(x+y) &=& \sin(x)\cos(y) + \cos(x)\sin(y) \\ \cos(x+y) &=& \cos(x)\cos(y) - \sin(x)\sin(y) \end{array} \right.$$

Considérons $\mathcal{E}\colon \mathbb{R} \to \mathbb{C}^*$, $x \mapsto \cos(x) + \mathbf{i}\sin(y)$. Alors

$$\circledast \quad \Longleftrightarrow \quad \mathcal{E}(x+y) = \mathcal{E}(x)\mathcal{E}(y)$$

et $\mathcal{E}$ est un morphisme de groupes de $\mathbb{R}$ dans $\mathbb{C}^*$.

2.1.2. Exemples en algèbre linéaire et arithmétique. —

Exemple 2.1.15. — Soit A une matrice $m\times n$. Considérons la fonction $f\colon \mathbb{R}^n \to \mathbb{R}^m$, $x \mapsto Ax$. Notons que $\mathbb{R}^n$ et $\mathbb{R}^m$ sont deux groupes additifs et que la formule $A(x+y) = Ax + Ay$ assure que f est un morphisme de groupes.

Plus généralement, les espaces vectoriels sont des groupes additifs et les applications linéaires sont des morphismes de groupes.

Exemple 2.1.16. — L'application $\det\colon \mathrm{GL}(n,\mathbb{C}) \to \mathbb{C}^*$ est un morphisme de groupes. En effet pour toutes matrices $n\times n$ à coefficients complexes A et B nous avons $\det(AB) = \det(A)\det(B)$.

Exemple 2.1.17. — Considérons le groupe $\mathrm{Aff}(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in \mathbb{R}^*,\, b \in \mathbb{R} \right\}$ muni de la multiplication matricielle. Remarquons que

$$\circledast \qquad \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a\alpha & a\beta + b \\ 0 & 1 \end{pmatrix}.$$

Soit $f\colon \mathrm{Aff}(\mathbb{R}) \to \mathbb{R}^*$, $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto a$. D'après $\circledast$ nous avons

$$f\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}\right) = f\left(\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\right) f\left(\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}\right),$$

autrement dit f est un morphisme de groupes.

Nous aurions aussi pu remarquer que $f = \det_{|\mathrm{Aff}(\mathbb{R})}$ et conclure en utilisant l'Exemple 2.1.16.

Exemple 2.1.18. — Soient m dans $\mathbb{N}^*$ et c dans $\mathbb{Z}$.

Considérons l'application $\mathrm{M}_c\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $x \mod m \mapsto cx \mod m$. L'égalité $c(x+y) \equiv_m cx + cy$ valable pour tous x, y dans $\mathbb{Z}$ implique que M_c est un morphisme de groupes de $\mathbb{Z}/m\mathbb{Z}$ dans lui-même.

Exemple 2.1.19. — Considérons deux entiers positifs n et m. L'égalité $(xy)^n \equiv x^n y^n \mod m$ entraîne que $\Psi_n\colon \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \to \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$, $x \mapsto x^n$ est un morphisme de groupes.

Par exemple pour $n = 3$ et $m = 15$ on a

$x \mod 15$	1	2	4	7	8	11	13	14
$x^3 \mod 15$	1	8	4	13	2	11	7	14

et pour $n = 3$ et $m = 21$ on a

$x \mod 15$	1	2	4	5	8	10	11	13	16	17	19	20
$x^3 \mod 15$	1	8	1	20	8	13	8	13	1	20	13	20

Remarque 2.1.1. — Alors que Ψ_3 permute les éléments de $\left(\mathbb{Z}/15\mathbb{Z}\right)^\times$, l'image de $\left(\mathbb{Z}/21\mathbb{Z}\right)^\times$ par Ψ_3 est un sous-groupe d'ordre 4 de $\left(\mathbb{Z}/21\mathbb{Z}\right)^\times$.

Exemple 2.1.20. — Soit $m \geq 1$ un entier. On définit l'addition sur $\mathbb{Z}/m\mathbb{Z}$ par la formule $\overline{x} + \overline{y} = \overline{x+y}$. Le morphisme de réduction modulo m, $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $x \mapsto \overline{x}$ est un morphisme de groupes.

Exemple 2.1.21. — Généralisons l'exemple précédent. Soient m et d deux entiers positifs. On peut considérer, si d divise m, le *morphisme de réduction* $r\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$, $x \mod m \mapsto x \mod d$; en effet si $a \equiv b \mod m$, alors m divise $a - b$ et donc d aussi, *i.e.* $a \equiv b \mod d$.

L'application r est un morphisme de groupes ; en effet

$$\begin{aligned} r(x \mod m + y \mod m) &= r(x + y \mod m) \\ &= x + y \mod d \\ &= x \mod d + y \mod d \\ &= r(x \mod d) + r(y \mod d) \end{aligned}$$

2.1.3. Autres exemples. —

Exemple 2.1.22. — Soit G un groupe. L'identité $\mathrm{id}\colon \mathrm{G} \to \mathrm{G}$, $g \mapsto g$ est un morphisme.

Exemple 2.1.23. — Soit G un groupe. Pour tout sous-groupe H de G l'inclustion $\mathrm{H} \hookrightarrow \mathrm{G}$ est un morphisme.

Exemple 2.1.24. — Pour tous groupes G et H de neutre e_G, respectivement e_H, il existe un morphisme appelé *morphisme trivial* : $f : \mathrm{G} \to \mathrm{H}$, $x \mapsto e_\mathrm{H}$.

Pour tous x, y dans G nous avons d'une part $f(xy) = f(e_\mathrm{G}) = e_\mathrm{H}$ et d'autre part $f(x)f(y) = e_\mathrm{H}e_\mathrm{H} = e_\mathrm{H}$. En particulier $f(xy) = f(x)f(y)$ pour tous x, y dans G.

Le morphisme trivial est parfois l'unique morphisme entre deux groupes, c'est par exemple le cas entre $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/5\mathbb{Z}$.

Exemple 2.1.25. — Soit G un groupe abélien. Soit n un entier supérieur à 1. L'égalité $(gh)^n = g^n h^n$ valable pour tous g, h dans G assure que $f\colon \mathrm{G} \to \mathrm{G}$, $g \mapsto g^n$ est un morphisme de groupes.

Attention ceci n'est plus vrai si G n'est pas abélien. Considérons par exemple le groupe diédral D_8 et l'application $f\colon \mathrm{D}_8 \to \mathrm{D}_8$, $g \mapsto g^3$. Notons comme d'habitude r et s les générateurs de D_8. Nous avons $f(rs) = (rs)^3 = rs$ alors que $f(r)f(s) = r^3s^3 = r^3s$. Mais $r \neq r^3$ donc $rs \neq r^3s$, *i.e.* $f(rs) \neq f(r)f(s)$. Autrement dit $f\colon \mathrm{D}_8 \to \mathrm{D}_8$, $g \mapsto g^3$ n'est pas un morphisme.

Exemple 2.1.26. — Soit G un groupe dont g est un élément. La *conjugaison* par g est la fonction $\gamma_g\colon \mathrm{G} \to \mathrm{G}$, $h \mapsto ghg^{-1}$.

Notons que tous x, y dans G nous avons

$$\gamma_g(x)\gamma_g(y) = (gxg^{-1})(gyg^{-1}) = gxg^{-1}gyg^{-1} = gxyg^{-1} = \gamma_g(xy)$$

et γ_g est un morphisme de groupes.

2.1.4. Exemples de fonctions qui ne sont pas des morphismes de groupes. —

Exemple 2.1.27. — Considérons la fonction

$$f\colon \mathrm{GL}(2,\mathbb{R}) \to \mathrm{GL}(2,\mathbb{R}), \qquad A \mapsto A^2.$$

Désignons par A la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et par B la matrice $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Alors d'une part

$$f(A)f(B) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$$

et d'autre part

$$f(AB) = \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right)^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$$

En particulier $f(A)f(B) \neq f(AB)$ et f n'est pas un morphisme de groupes.

Exemple 2.1.28. — Alors que $\det(AB) = \det(A)\det(B)$ pour toutes matrices A, B de taille 2×2 à coefficients réels, le déterminant $\det\colon M(2,\mathbb{R}) \to \mathbb{R}$, $M \mapsto \det(M)$ n'est pas un morphisme de groupes car $M(2,\mathbb{R})$ et $\mathbb{R}$ ne sont pas des groupes pour leur multiplication respective.

Exemple 2.1.29. — Soit A une matrice 2×2 à coefficients réels ; son exponentielle est définie par

$$\exp(A) = \sum_{n\geq 0} \frac{A^n}{n!} = \mathrm{Id} + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \cdots$$

Nous avons $\exp(A)\exp(-A) = \mathrm{Id}$; par suite $\exp(A)$ appartient à $\mathrm{GL}(2,\mathbb{R})$. Ainsi $\exp\colon M(2,\mathbb{R}) \to \mathrm{GL}(2,\mathbb{R})$ est une fonction du groupe additif $M(2,\mathbb{R})$ dans le groupe multiplicatif $\mathrm{GL}(2,\mathbb{R})$. C'est un analogue de la fonction exponentielle classique $\exp\colon \mathbb{R} \to \mathbb{R}^*$. Cependant $\exp\colon M(2,\mathbb{R}) \to \mathrm{GL}(2,\mathbb{R})$ n'est pas un morphisme de groupes : si $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

alors d'une part $\exp(A)\exp(B) = \begin{pmatrix} e & e \\ 0 & e \end{pmatrix}\begin{pmatrix} e & 0 \\ e & e \end{pmatrix} = \begin{pmatrix} 2e^2 & e^2 \\ e^2 & e^2 \end{pmatrix}$ et d'autre part $\exp(A+B) = \begin{pmatrix} \frac{e^3+e}{2} & \frac{e^3-e}{2} \\ \frac{e^3-e}{2} & \frac{e^3+e}{2} \end{pmatrix}$; en particulier $\exp(A+B) \neq \exp(A)\exp(B)$.

2.1.5. Quelques résultats sur les morphismes de groupes. —

Théorème 2.1.1

Soit $\varphi\colon \mathrm{G} \to \mathrm{H}$ un morphisme de groupes de G dans H. Désignons par e_{G} (resp. e_{H}) l'élément neutre de G (resp. H). Nous avons

1. $\varphi(e_{\mathrm{G}}) = e_{\mathrm{H}}$;
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$ pour tout $g \in \mathrm{G}$;
3. $\varphi(g^n) = \varphi(g)^n$ pour tout $g \in \mathrm{G}$, pour tout $n \in \mathbb{Z}$.

Démonstration. —

1. À partir de $e_{\mathrm{G}}e_{\mathrm{G}} = e_{\mathrm{G}}$ nous obtenons $\varphi(e_{\mathrm{G}}e_{\mathrm{G}}) = \varphi(e_{\mathrm{G}})$ qui se réécrit $\varphi(e_{\mathrm{G}})\varphi(e_{\mathrm{G}}) = \varphi(e_{\mathrm{G}})$ ou encore $\varphi(e_{\mathrm{G}})\varphi(e_{\mathrm{G}}) = \varphi(e_{\mathrm{G}})e_{\mathrm{H}}$ d'où en multipliant cette égalité à gauche par le symétrique de $\varphi(e_{\mathrm{G}})$, $\varphi(e_{\mathrm{G}}) = e_{\mathrm{H}}$.
2. L'égalité $gg^{-1} = e_{\mathrm{G}}$ conduit à $\varphi(gg^{-1}) = \varphi(e_{\mathrm{G}})$ d'où $\varphi(g)\varphi(g^{-1}) = e_{\mathrm{H}}$. Autrement dit $\varphi(g^{-1})$ est l'inverse de $\varphi(g)$ est l'inverse de $\varphi(g^{-1})$, *i.e.* $(\varphi(g))^{-1} = \varphi(g^{-1})$.
3. Raisonnons par récurrence pour $n \geq 0$. L'initialisation se fait avec la convention $g^0 = e_{\mathrm{G}}$ qui nous donne : $\varphi(g^0) = \varphi(e_{\mathrm{G}}) = e_{\mathrm{H}} = \varphi(g)^0$.

   Supposons que la relation $\varphi(g^n) = \varphi(g)^n$ soit vérifiée pour un certain $n \geq 0$. Alors
$$\varphi(g^{n+1}) = \varphi(gg^n) = \varphi(g)\varphi(g^n) \overset{\text{hyp. réc.}}{=} \varphi(g)\varphi(g)^n = \varphi(g)^{n+1}.$$
   Ainsi la relation $\varphi(g^n) = \varphi(g)^n$ est vérifiée pour tout entier $n \geq 0$.

   Enfin pour $n < 0$ on écrit $N = -n \geq 1$ et on a
$$\varphi(g^n) = \varphi(g^{-N}) = \varphi((g^N)^{-1}) \overset{\text{cf. 2.}}{=} \varphi(g^N)^{-1} \overset{\text{car } N \geq 0}{=} (\varphi(g)^N)^{-1} = \varphi(g)^{-N} = \varphi(g)^n.$$
   Finalement $\varphi(g^n) = \varphi(g)^n$ pour tout $n \in \mathbb{Z}$.

□

Corollaire 2.1.1

Soit $\varphi\colon \mathrm{G} \to \mathrm{H}$ un morphisme de groupes.
Si $g \in \mathrm{G}$ est d'ordre n, alors l'ordre de $\varphi(g)$ divise n.

Démonstration. — Puisque g est d'ordre n, $g^n = e_{\mathrm{G}}$. Par suite $\varphi(g^n) = \varphi(e_{\mathrm{G}})$ et le Théorème 2.1.1 donne $\varphi(g^n) = \varphi(g)^n = e_{\mathrm{H}} = \varphi(e_{\mathrm{G}})$. L'ordre de $\varphi(g)$ est un diviseur de n. □

Exemple 2.1.30. — Reprenons l'Exemple 2.1.21 du morphisme de réduction avec $n = 21$ et $d = 7$, $r\colon {}^{\mathbb{Z}}\!/_{21\mathbb{Z}}{}^{\times} \to {}^{\mathbb{Z}}\!/_{7\mathbb{Z}}{}^{\times}$.

- ◇ On a $11 \equiv_{21} -10$ d'où $11^2 \equiv_{21} 100 = 5\times 21 - 5 \equiv_{21} -5$, donc $11^3 \equiv_{21} -50 = -2\times 21 - 8 \equiv_{21} -8$, $11^4 \equiv_{21}= (-5)^2 \equiv_{21} 4$, $11^5 \equiv_{21} 44 \equiv_{21} 2$ et $11^6 \equiv_{21} 22 \equiv_{21} 1$. Ainsi $11 \mod 21$ est d'ordre 6.

  On a $r(11) = 11 \mod 7 = 4 \mod 7$, d'où $r(11)^2 \equiv_7 16 \equiv_7 2$ et $r(11)^3 \equiv_7 2 \times 4 \equiv_7 1$. Ainsi $r(11)$ est d'ordre 3.
- ◇ On vérifie de même que $8 \mod 21$ est d'ordre 2 quand $8 \mod 7 = 1 \mod 7$ est d'ordre 1.

Théorème 2.1.2

La composée de deux morphismes de groupes est un morphisme de groupes : si $\varphi_1\colon \mathrm{G}_1 \to \mathrm{G}_2$ et $\varphi_2\colon \mathrm{G}_2 \to \mathrm{G}_3$ sont deux morphismes de groupes, alors $\varphi_2 \circ \varphi_1\colon \mathrm{G}_1 \to \mathrm{G}_3$ est un morphisme de groupes.

Démonstration. — Soient x et y dans G_1 ; alors
$(\varphi_2 \circ \varphi_1)(xy) = \varphi_2(\varphi_1(xy)) = \varphi_2(\varphi_1(x)\varphi_1(y)) = \varphi_2(\varphi_1(x))\varphi_2(\varphi_1(y)) = (\varphi_2 \circ \varphi_1)(x)(\varphi_2 \circ \varphi_1)(y)$. □

Exemple 2.1.31. — La fonction $\varphi\colon \mathrm{GL}(2,\mathbb{R}) \to \mathbb{R}^{+*}$, $A \mapsto |\det(A)|$ est la composée de $\det\colon \mathrm{GL}(2,\mathbb{R}) \to \mathbb{R}^*$, qui est un morphisme de groupes, et de $|\ |\colon \mathbb{R}^* \to \mathbb{R}^{+*}$, qui est aussi un morphisme de groupes, c'est donc un morphisme de groupes.

On rappelle qu'étant donnée une application f définie sur un ensemble X et à valeurs dans un ensemble Y, on associe à toute partie A de X son *image* par f : $f(A) = \{f(a) \mid a \in A\}$. Et on associe à toute partie B de Y son *image réciproque* par f : $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$.

Lorsque $A = X$, on dit que $f(A) = f(X)$ est l'image de f et on écrit indifféremment $\mathrm{Im}(f)$ et $f(X)$.

Exemple 2.1.32. — Considérons la fonction $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2 + 1$.

Alors $f(\{2, 10\}) = \{5, 101\}$, $f^{-1}(\{10\}) = \{3, -3\}$, $f([1, 4]) = [2, 17]$, $f^{-1}([2, 17]) = [-4, -1] \cup [1, 4]$ et $f^{-1}\left(\left\{\frac{1}{8}\right\}\right) = \emptyset$.

Théorème 2.1.3

Soit $\varphi\colon \mathrm{G} \to \mathrm{H}$ un morphisme de groupes.

1. L'image d'un sous-groupe de G est un sous-groupe de H. En particulier $\mathrm{Im}(\varphi)$ est un sous-groupe de H.
2. L'image réciproque par φ d'un sous-groupe de H est un sous-groupe de G.

Démonstration. — 1. Soit K un sous-groupe de G.

- ◇ $e_{\mathrm{H}} \in \varphi(K)$ puisque $e_{\mathrm{H}} = \varphi(e_{\mathrm{G}})$ et $e_{\mathrm{G}} \in \mathrm{K}$.
- ◇ Considérons deux éléments de $\varphi(\mathrm{K})$. Par définition ils sont de la forme $\varphi(k)$ et $\varphi(k')$, avec k et k' deux éléments de K. Puisque φ est un morphisme de groupes nous avons $\varphi(k)\varphi(k') = \varphi(kk')$. Comme K est un groupe, $kk' \in \mathrm{K}$ et donc $\varphi(k)\varphi(k') \in \varphi(\mathrm{K})$.
- ◇ Considérons un élément de $\varphi(\mathrm{K})$; il s'écrit $f(k)$ pour un certain $k \in \mathrm{K}$. D'une part le Théorème 2.1.1 assure que $(f(k))^{-1} = f(k^{-1})$, d'autre part k^{-1} appartient à K car K est un groupe. En conséquence $\varphi(k)^{-1}$ est un élément de $\varphi(\mathrm{K})$.

2. Soit L un sous-groupe de H.
   - ◇ À partir de $f(e_{\mathrm{G}}) = e_{\mathrm{H}} \in \mathrm{L}$ nous obtenons $e_{\mathrm{G}} \in f^{-1}(\mathrm{L})$.
   - ◇ Soient x et y deux éléments de $\varphi^{-1}(\mathrm{L})$; par définition $\varphi(x)$ et $\varphi(y)$ appartiennent à L. Comme L est un groupe $\varphi(x)\varphi(y)$ est dans L. Mais φ est un morphisme de groupes donc $\varphi(x)\varphi(y) = \varphi(xy)$. Ainsi $\varphi(xy)$ appartient à L et $xy \in \varphi^{-1}(\mathrm{L})$.
   - ◇ Soit $x \in \varphi^{-1}(\mathrm{L})$; par définition $\varphi(x) \in \mathrm{L}$ et $\varphi(x)^{-1} \in \mathrm{L}$ puisque L est un groupe. Mais d'après le Théorème 2.1.1 on a $\varphi(x)^{-1} = \varphi(x^{-1})$, alors $\varphi(x^{-1}) \in \mathrm{L}$ et $x^{-1} \in \varphi^{-1}(\mathrm{L})$.

□

Exemple 2.1.33. — Reprenons l'Exemple 2.1.19, $\psi_3 \colon \left(\mathbb{Z}/21\mathbb{Z}\right)^\times \to \left(\mathbb{Z}/21\mathbb{Z}\right)^\times$, $x \mapsto x^3$. On a $\psi_3\left(\mathbb{Z}/21\mathbb{Z}^\times\right) = \{1, 8, 13, 30 \mod 21\}$ qui est un sous-groupe de $\left(\mathbb{Z}/21\mathbb{Z}\right)^\times$.

Dans $\left(\mathbb{Z}/21\mathbb{Z}\right)^\times$ le sous-groupe engendré par $2 \mod 21$ est $\langle 2 \mod 21\rangle = \{1, 2, 4, 6, 8, 11, 16 \mod 21\}$. Son image par ψ_3 est le sous-groupe $\{1, 8 \mod 21\}$.

Dans $\left(\mathbb{Z}/21\mathbb{Z}\right)^\times$ le sous-groupe engendré par $20 \equiv_2 1 - 1$ est $\langle 20 \mod 21\rangle = \{1, 20\}$. Son image réciproque par ψ_3 est un sous-groupe de $\left(\mathbb{Z}/21\mathbb{Z}\right)^\times$. On a $\psi_3^{-1}(\langle 20 \mod 21\rangle) = \{x \in \left(\mathbb{Z}/21\mathbb{Z}\right)^\times \mid x^3 = 1 \text{ ou } x^3 = 20 \mod 21\} = \{1, 4, 5, 16, 17, 20 \mod 21\} = \langle 5 \mod 21\rangle$.

Il n'existe pas de critère « simple » pour déterminer si un morphisme de groupes est surjectif mais il en existe un pour déterminer si un morphisme est injectif.

Théorème 2.1.4

Un morphisme de groupes $\varphi \colon \mathrm{G} \to \mathrm{H}$ est injectif si et seulement si $\varphi(x) = e_{\mathrm{H}}$ admet une unique solution $x = e_{\mathrm{G}}$.

Démonstration. — L'égalité $\varphi(x) = e_{\mathrm{H}}$ se réécrit $\varphi(x) = \varphi(e_{\mathrm{G}})$ et si φ est injective cela implique que $x = e_{\mathrm{G}}$.

Réciproquement supposons que l'unique solution de $\varphi(x) = e_{\mathrm{H}}$ est $x = e_{\mathrm{G}}$. Soient g et g' dans G tels que $\varphi(g) = \varphi(g')$ alors $\varphi(g)^{-1}\varphi(g') = e_{\mathrm{H}}$. Le Théorème 2.1.1 assure que $\varphi(g)^{-1}\varphi(g')^{-1} =$

e_{H} se réécrit $\varphi(g^{-1})\varphi(g') = e_{\mathrm{H}}$, et commme φ est un morphisme de groupes on en déduit que $\varphi(g^{-1}g') = e_{\mathrm{H}}$. D'après notre hypothèse cela implique que $g^{-1}g' = e_{\mathrm{G}}$ et donc que $g = g'$. □

Exemple 2.1.34. — Reprenons une nouvelle fois l'Exemple 2.1.19.

Le morphisme $\psi_3\colon \left(\mathbb{Z}/15\mathbb{Z}\right)^{\times} \to \left(\mathbb{Z}/15\mathbb{Z}\right)^{\times}$ est injectif car $\psi_3(x) = 1$ si et seulement si $x = 1 \mod 15$.

Le morphisme $\psi_3\colon \left(\mathbb{Z}/21\mathbb{Z}\right)^{\times} \to \left(\mathbb{Z}/21\mathbb{Z}\right)^{\times}$ n'est pas injectif en effet $\psi_3(1) = \psi_3(4) = \psi_3(16) = 1$.

Ainsi si $\varphi\colon \mathrm{G} \to \mathrm{H}$ est un morphisme de groupes, savoir combien d'éléments de G satisfont $\varphi(g) = e_{\mathrm{H}}$ est important d'où la notion de noyau d'un morphisme de groupes.

Définition 2.1.2

Soit $\varphi\colon \mathrm{G} \to \mathrm{H}$ un morphisme de groupes. Le *noyau* de φ est défini par

$$\ker\varphi = \{g \in \mathrm{G} \mid \varphi(g) = e_{\mathrm{H}}\}.$$

Proposition 2.1.1

Le noyau du morphisme de groupes $\varphi\colon \mathrm{G} \to \mathrm{H}$ est un sous-groupe de G.

Démonstration. — *Première rédation possible.* Étant donné que $\varphi(e_{\mathrm{G}}) = e_{\mathrm{H}}$, e_{G} appartient à $\ker\varphi$. Soient x et y dans $\ker\varphi$. D'une part, φ est un morphisme de groupes donc $\varphi(xy) = \varphi(x)\varphi(y)$, d'autre part x et y appartiennent à $\ker\varphi$ d'où $\varphi(x) = \varphi(y) = e_{\mathrm{H}}$. Ainsi $\varphi(xy) = e_{\mathrm{H}}$ c'est-à-dire xy appartient à $\ker\varphi$. Soit x dans $\ker\varphi$. D'une part $(\varphi(x))^{-1} = \varphi(x^{-1})$ (Théorème 2.1.1), d'autre part $\varphi(x) = e_{\mathrm{H}}$. Par conséquent

$$\varphi(x^{-1}) = (\varphi(x))^{-1} = e_{\mathrm{H}}^{-1} = e_{\mathrm{H}};$$

autrement dit x^{-1} appartient à $\ker\varphi$.

Seconde rédaction possible. Puisque $\ker\varphi = \{x \in \mathrm{G} \mid \varphi(x) = e_{\mathrm{H}}\} = \varphi^{-1}(\{e_{\mathrm{H}}\})$ est l'image réciproque du groupe trivial $\{e_{\mathrm{H}}\}$ le Théorème 2.1.3 assure que $\ker\varphi$ est un sous-groupe de G. □

Exemple 2.1.35. — Le morphisme $f = \mathrm{Aff}(\mathbb{R}) \to \mathbb{R}^*$, $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto a$ de l'Exemple 2.1.17 a pour noyau $\ker f = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$.

Exemple 2.1.36. — Le morphisme de groupes $\mathbb{R}^* \to \mathbb{R}^*$, $x \mapsto x^2$ a pour noyau $\{-1, 1\}$.

Exemple 2.1.37. — Le noyau du morphisme $\mathcal{E}\colon \mathbb{R} \to \mathbb{C}^*$, $x \mapsto \cos x + \mathbf{i} \sin x$ considéré dans l'Exemple 2.1.14 est

$$\ker \mathcal{E} = \{x \in \mathbb{R} \mid \cos x + \mathbf{i} \sin x = 1\} = \{x \in \mathbb{R} \mid \cos x = 1 \text{ et } \sin x = 0\} = \{2\pi k \mid k \in \mathbb{Z}\} = 2\pi\mathbb{Z}.$$

Exemple 2.1.38. — Le noyau du morphisme $\det\colon \mathrm{GL}(n, \mathbb{C}) \to \mathbb{C}^*$ considéré dans l'Exemple 2.1.16 est le groupe spécial linéaire $\mathrm{SL}(n, \mathbb{C})$.

Pour finir donnons une caractérisation des éléments d'un groupe qui ont même image par un morphisme de groupes :

Théorème 2.1.5

Soit $\varphi\colon \mathrm{G} \to \mathrm{H}$ un morphisme de groupes.
Alors $\varphi(g) = \varphi(h)$ si et seulement si $h = gk$ pour un certain $k \in \ker \varphi$.

Démonstration. — Soient g et h dans $\ker \varphi$ tels que $\varphi(g) = \varphi(h)$. Alors

$$\varphi(g^{-1}h) = \varphi(g^{-1})\varphi(h) = (\varphi(g))^{-1}\varphi(h) = e_{\mathrm{H}}.$$

Réciproquement, supposons que $h \in \mathrm{H}$ s'écrive gk avec k dans $\ker \varphi$. Alors $\varphi(h) = \varphi(gk) = \varphi(g)\varphi(k) = \varphi(g)e_{\mathrm{H}} = \varphi(g)$. □

2.2. Isomorphismes

Deux groupes qui ne sont pas littéralement les mêmes peuvent être structurellement les mêmes. Un exemple de cette idée est la relation entre la multiplication et l'addition via l'exponentielle :

$$\circledast \quad e^x e^y = e^{x+y}.$$

Tout nombre de $\mathbb{R}^{+*}$ est de la forme e^x pour un unique x dans $\mathbb{R}$. Quand nous écrivons les éléments de $\mathbb{R}^{+*}$ sous la forme e^x, la relation $\circledast$ nous indique que multiplier dans $\mathbb{R}^{+*}$ revient à additionner les exposants dans $\mathbb{R}$.

Réciproquement tout nombre réel est de la forme $\ln x$ pour un unique $x > 0$ et le lien entre l'addition dans $\mathbb{R}$ et la multiplication dans $\mathbb{R}^{+*}$ est le suivant

$$\ln(x) + \ln(y) = \ln(xy)\cdot$$

Les fonctions $\exp\colon \mathbb{R} \to \mathbb{R}^{+*}$ et $\ln\colon \mathbb{R}^{+*} \to \mathbb{R}$ donnent aux groupes $\mathbb{R}$ et $\mathbb{R}^{+*}$ la même apparence : il y a une bijection permettant de passer de l'un à l'autre qui transforme l'opération d'un des groupes en l'opération de l'autre groupe.

On peut aussi faire le même type de construction pour les groupes finis $\mathcal{A}_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$, rencontré dans l'Exemple **??**, et $\mathbb{Z}/3\mathbb{Z}$. Si nous posons $\varphi(0) = \mathrm{id}$, $\varphi(1) = (1\ 2\ 3)$ et $\varphi(2) = (1\ 3\ 2)$, nous définissons un morphisme de groupes. On vérifie par exemple que $\varphi(1 + 2) = \varphi(0) = \mathrm{id} = (1\ 2\ 3)(1\ 3\ 2)$.

Ce morphisme est une bijection puisque son noyau est évidemment réduit à $\{0\}$.

Ces deux groupes pourtant différents sont indiscernables l'un de l'autre si on se limite aux propriétés liées à leur structure de groupes.

Définition 2.2.1

Deux groupes G_1 et G_2 sont *isomorphes* s'il existe un morphisme bijectif $\varphi\colon \mathrm{G}_1 \to \mathrm{G}_2$ entre G_1 et G_2.

Un isomorphisme entre deux groupes est un dictionnaire qui permet de traduire les éléments et opération d'un groupe à l'autre sans perdre les informations essentielles. Par exemple nous verrons que tous les groupes cycliques de même ordre sont isomorphes ; ainsi, si nous comprenons un groupe cyclique G, nous pouvons transférer via l'isomorphisme $f\colon \mathrm{G} \to \mathrm{H}$ toutes les propriétés de G à H. Les isomorphismes sont le moyen d'exprimer comment deux groupes différents sont néanmoins structurellement les mêmes.

2.2.1. Exemples. —

Exemple 2.2.1. — La fonction $\exp\colon \mathbb{R} \to \mathbb{R}^{+*}$, $x \mapsto \exp x$ est un isomorphime :

- ◇ c'est un morphisme de groupes car pour tous x, y dans $\mathbb{R}$ nous avons $\exp(x+y) = \exp(x)\exp(y)$;
- ◇ c'est une bijection, la fonction inverse étant la fonction logarithme.

Plus généralement pour tout $b > 0$ avec $b \neq 1$, la fonction

$$f\colon \mathbb{R} \to \mathbb{R}^{+*}$$

est un isomorphime :

- ◇ c'est un morphisme de groupes car pour tous réels x et y nous avons $f(x+y) = b^{x+y} = b^x b^y = f(x)f(y)$;
- ◇ c'est une bijection, la fonction inverse étant la fonction $x \mapsto \log_b x$.

Notons que $\log_b\colon \mathbb{R}^{+*} \to \mathbb{R}$ est un isomorphisme : d'une part c'est un morphisme de groupes et d'autre part c'est une bijection (l'inverse étant $\mathbb{R} \to \mathbb{R}^{+*}$, $x \mapsto b^x$).

***Exemple 2.2.2* (groupe affine).** — On reprend l'Exemple 1.3.8, avec $\mathrm{Aff}(\mathbb{R}) = \{x \mapsto ax+b\,;\ (a,b) \in \mathbb{R}^* \times \mathbb{R}\}$. On considère l'ensemble $A = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},\ (a,b) \in \mathbb{R}^* \times \mathbb{R} \right\}$. Il s'agit d'un sous-groupe de $\mathrm{GL}(2,\mathbb{R})$. L'application $\Psi\colon \mathrm{Aff}(\mathbb{R}) \to A$, $(x \mapsto ax+b) \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ est un isomorphisme de groupes.

Dans la suite nous identifierons $\mathrm{Aff}(\mathbb{R})$, $\mathrm{Aff}(\mathbb{Z})$, $\mathrm{Aff}\left(\mathbb{Z}/n\mathbb{Z}\right)$, ... avec le groupe de matrices 2×2 donné par cet isomorphisme.

Exemple 2.2.3. — La fonction $f\colon \mathbb{Z}/4\mathbb{Z} \to \left(\mathbb{Z}/5\mathbb{Z}\right)^\times$, $a \mod 4 \mapsto 2^a \mod 5$ est un isomorphisme entre $\mathbb{Z}/4\mathbb{Z}$ et $\left(\mathbb{Z}/5\mathbb{Z}\right)^\times$. Commençons par remarquer que f est bien définie : l'égalité $2^4 \equiv 1 \mod 5$ implique $2^{a+4k} = 2^a 2^{4k} \equiv 2^a \mod 5$. De plus, f est un morphisme de groupes ; en effet, d'une part

$$f(a \bmod 4)f(b \bmod 4) = (2^a \bmod 5)(2^b \bmod 5) = 2^{a+b} \bmod 5$$

et d'autre part

$$f(a \bmod 4 + b \bmod 4) = f((a+b) \bmod 4) = 2^{a+b} \bmod 5$$

d'où $f(a \bmod 4)f(a \bmod 4) = f(a \bmod 4 + b \bmod 4)$. Par ailleurs f est une bijection puisque

$$f(0) = 1, \qquad f(1) = 2, \qquad f(2) = 4, \qquad f(3) = 3.$$

Exemple 2.2.4. — La fonction $f\colon \mathbb{Z}/4\mathbb{Z} \to \left(\mathbb{Z}/5\mathbb{Z}\right)^\times$, $a \bmod 4 \mapsto 4^a \bmod 5$ n'est pas un isomorphisme de groupes. En effet, nous pouvons vérifier comme précédemment que f est bien définie et est un morphisme de groupes. Par contre f n'est pas injective ; en effet, $f(0) = f(2) = 1$. En particulier, f n'est pas bijective.

Exemple 2.2.5. — Les groupes D_6 et $\mathfrak{S}_3$ sont isomorphes. À première vue ces deux groupes se ressemblent : ils sont tous les deux d'ordre 6 et possèdent tous les deux

- ◇ un élément d'ordre 1, l'identité ;
- ◇ trois éléments d'ordre 2 ;
- ◇ deux éléments d'ordre 3.

Considérons un triangle équilatéral $\mathcal{T}$ dont les sommets sont désignés par 1, 2 et 3 de sorte que les éléments de D_6 permutent les sommets et peuvent donc être vus comme des éléments de $\mathfrak{S}_3$.

Soient O le centre de gravité de $\mathcal{T}$ et M le milieu du segment $[2\,3]$. Désignons par s la réflexion d'axe OM et par r la rotation de centre O qui envoie 1 sur 2, 2 sur 3 et 3 sur 1. Notons N le milieu de $[1\,2]$ et P celui de $[1\,3]$. Alors rs est la réflexion d'axe ON et r^2s celle d'axe OP. Nous avons la correspondance suivante entre les éléments de D_6 et ceux de $\mathfrak{S}_3$:

D_6	id	r	r^2	s	rs	r^2s
$\mathfrak{S}_3$	id	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$

Cette correspondance est compatible avec les lois de groupes de D_6 et $\mathfrak{S}_3$:

- ◇ r est d'ordre 3 et $(1\ 2\ 3)$ est d'ordre 3 ;
- ◇ s est d'ordre 2 et $(2\ 3)$ est d'ordre 2 ;
- ◇ $sr = r^{-1}s$ et $(2\ 3)(1\ 2\ 3) = (1\ 2\ 3)^{-1}(2\ 3)$

Si nous notons $f\colon \mathrm{D}_6 \to \mathfrak{S}_3$ la correspondance donnée par le tableau précédent, nous constatons que c'est une bijection et nous pouvons vérifier que c'est un morphisme de groupes. Ainsi f réalise un isomorphisme entre le groupe diédral D_6 et le groupe symétrique $\mathfrak{S}_3$.

Exemple 2.2.6. — Les groupes $\mathrm{Aff}\left(\mathbb{Z}/4\mathbb{Z}\right)$ et D_8 sont isomorphes. Remarquons que toute matrice de $\mathrm{Aff}\left(\mathbb{Z}/4\mathbb{Z}\right)$ s'écrit $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ avec $a \in \{\pm 1 \bmod 4\}$ et $b \in \mathbb{Z}/4\mathbb{Z}$ et que toute telle matrice peut se décomposer comme suit

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}.$$

Notons de plus que $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre 4 dans $\mathrm{Aff}\left(\mathbb{Z}/4\mathbb{Z}\right)$, $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre 2 dans $\mathrm{Aff}\left(\mathbb{Z}/4\mathbb{Z}\right)$ et

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

qui ressemble à la relation $sr = r^{-1}s$ dans D_8. Ceci amène à considérer la fonction

$$f\colon \mathrm{D}_8 \to \mathrm{Aff}\left(\mathbb{Z}/4\mathbb{Z}\right), \qquad r^k s^\ell \mapsto \begin{pmatrix} (-1)^\ell & k \\ 0 & 1 \end{pmatrix} \bmod 4$$

ce qui a un sens puisque

- ⋄ dans l'expression $r^k s^\ell$ l'exposant k « compte modulo 4 » et l'exposant s modulo 2 ;
- ⋄ dans l'expression $\begin{pmatrix} (-1)^\ell & k \\ 0 & 1 \end{pmatrix} \bmod 4$ les entiers ℓ et k « comptent modulo 4 ».

Par ailleurs f est un morphisme de groupes ; en effet, d'une part

$$f(r^k s^\ell) f(r' s^{\ell'}) = \begin{pmatrix} (-1)^\ell & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} (-1)^{\ell'} & k' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} (-1)^{\ell+\ell'} & (-1)^\ell k' + k \\ 0 & 1 \end{pmatrix}$$

et d'autre part

$$f\big((r^k s^\ell)(r^{k'} s^{\ell'})\big) = f\big(r^k \underbrace{(s^\ell r^{k'})}_{r^{(-1)^\ell k'} s^\ell} s^{\ell'}\big) = f\big(r^{k+(-1)^\ell k'} s^{\ell+\ell'}\big) = \begin{pmatrix} (-1)^{\ell+\ell'} & (-1)^\ell k' + k \\ 0 & 1 \end{pmatrix}.$$

En outre

$$\begin{aligned}
\ker f &= \{r^k s^\ell \mid f(r^k s^\ell) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 4\} \\
&= \{r^k s^\ell \mid \begin{pmatrix} (-1)^\ell & k \\ 0 & 1 \end{pmatrix} \bmod 4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 4\} \\
&= \{r^k s^\ell \mid \ell \equiv 0 \bmod 2 \text{ et } k \equiv 0 \bmod\} \\
&= \{\mathrm{id}\}
\end{aligned}$$

autrement dit f est un morphisme de groupes injectif. Comme les groupes D_8 et $\mathrm{Aff}\left(\mathbb{Z}/4\mathbb{Z}\right)$ sont tous deux d'ordre 8, le morphisme f est surjectif. Finalement f réalise un isomorphisme entre D_8 et $\mathrm{Aff}\left(\mathbb{Z}/4\mathbb{Z}\right)$.

Exemple 2.2.7. — Soient G un groupe et $h \in \mathrm{G}$; on peut considérer le morphisme $\gamma_h \colon \mathrm{G} \to \mathrm{G}$, $g \mapsto hgh^{-1}$. Il est bijectif d'inverse $\gamma_{h^{-1}}$. Nous retrouvons ces isomorphismes plusieurs fois, en particulier dans Chapitre 3, §3.1 mais aussi dans Chapitre 6, §6.1.3.2.

Exemple 2.2.8. — Les groupes $\mathbb{S}^1$, $\mathbb{R}/\mathbb{Z}$ et $\mathbb{R}^{+*}/2^{\mathbb{Z}}$ sont isomorphes. On rappelle que $\mathbb{S}^1$ est le cercle unité dans $\mathbb{C}$ (voir Exemple 1.3.6), que $\mathbb{R}/\mathbb{Z}$ est l'ensemble des nombres réels modulo 1 et enfin que $\mathbb{R}^{+*}/2^{\mathbb{Z}}$ représente les classes d'équivalence dans $\mathbb{R}^{+*}$ pour la relation $x \equiv y$ s'il existe $n \in \mathbb{Z}$ tel que $x = 2^n y$.

Soit $\varphi_1 \colon \mathbb{R}/\mathbb{Z} \to \mathbb{S}^1$, $\bar{x} \mapsto e^{2\mathbf{i}\pi x}$. C'est une application bien définie puisque si $\bar{x} = \bar{y}$, alors $(x - y) \in \mathbb{Z}$ et $e^{2\mathbf{i}\pi(x-y)} = 1$, d'où $\varphi_2(\bar{x}) = \varphi_2(\bar{y})$.

Soit $\varphi_2 \colon \mathbb{S}^1 \to \mathbb{R}^{+*}/2^{\mathbb{Z}}$, $z = e^{\mathbf{i}\theta} \mapsto \widetilde{2^\theta}$, où θ est un argument de z (*i.e.* $z = e^{\mathbf{i}\theta}$) et $\widetilde{a}$ est la classe de a dans $\mathbb{R}^{+*}/2^{\mathbb{Z}}$.

Et enfin soit $\varphi_3 \colon \mathbb{R}^{+*}/2^{\mathbb{Z}} \to \mathbb{R}/\mathbb{Z}$, $\widetilde{x} \mapsto \overline{\log_2(x)}$. Il convient de s'assurer que φ_3 est bien définie. Si $\widetilde{x} = \widetilde{y}$ il existe $n \in \mathbb{Z}$ tel que $x = 2^n y$. On a donc $\log_2(x) = n + \log_2(y)$. Soit $\overline{\log_2(x)} = \overline{\log_2(y)}$. Ce qui assure que φ_3 est convenablement définie.

Ces trois applications sont bijectives. On vérifie par exemple que φ_2 et $\varphi_1 \circ \varphi_3$ sont inverses l'une de l'autre. Soit $z = e^{2\mathbf{i}\pi\theta}$, on a $\varphi_2(z) = \widetilde{2^\theta}$, $\varphi_3 \circ \varphi_2(z) = \bar{\theta}$ et $\varphi_1 \circ \varphi_3 \circ \varphi_2(z) = e^{2\mathbf{i}\pi\theta}$. Soit $\widetilde{y} \in \mathbb{R}^{+*}/2^{\mathbb{Z}}$. On a $\varphi_3(\widetilde{y}) = \overline{\log_2(y)}$, $\varphi_1 \circ \varphi_3(\widetilde{y}) = e^{2\mathbf{i}\pi \log_2(y)}$ et $\varphi_2 \circ \varphi_1 \circ \varphi_3(\widetilde{y}) = \widetilde{2^{\log_2(y)}} = \widetilde{y}$.

Vérifions pour finir qu'il s'agit de morphismes de groupes.

◇ Soient $\bar{x}$ et $\bar{y}$ deux éléments de $\mathbb{R}/\mathbb{Z}$ on a

$$\varphi_1(\overline{x+y}) = e^{2i\pi(x+y)} = e^{2i\pi x} e^{2i\pi y} = \varphi_1(\overline{x})\varphi_1(\overline{y}).$$

◇ Soient $z = e^{2i\pi\theta}$ et $z' = e^{2i\pi\theta'}$ deux éléments de $\mathbb{S}^1$ on a

$$\varphi_2(zz') = \varphi_2(e^{2i\pi(\theta+\theta')}) = \widetilde{2^{(\theta+\theta')}} = \widetilde{2^\theta}\widetilde{2^{\theta'}} = \varphi_2(z)\varphi_2(z').$$

◇ Soient $\widetilde{2^x}$ et $\widetilde{2^y}$ deux éléments de ${\mathbb{R}^{+*}}/{2^{\mathbb{Z}}}$. On a

$$\varphi_3(\widetilde{2^x}\widetilde{2^y}) = \varphi_3(\widetilde{2^{(x+y)}}) = \overline{x+y} = \bar{x} + \bar{y} = \varphi_3(\widetilde{2^x})\varphi_3(\widetilde{2^y}).$$

Bien qu'il existe une infinité de sous-groupes cycliques de même ordre distincts, ils sont tous isomorphes entre eux ; c'est l'objet des deux résultats suivants.

Théorème 2.2.1

Un groupe monogène infini est isomorphe à $\mathbb{Z}$.

Démonstration. — Soit $\mathrm{G} = \langle g \rangle$ un groupe cyclique infini de générateur g.

Étant donné que $g^k g^{k'} = g^{k+k'}$ pour tous entiers k et k' la fonction $f\colon \mathbb{Z} \to \mathrm{G}$, $k \mapsto g^k$ est un morphisme de groupes.

De plus, ce morphisme est

◇ injectif ; en effet, raisonnons par l'absurde : supposons que $g^n = g^{n'}$ avec $n \neq n'$. Nous pouvons par exemple supposer que $n' < n$. Alors $g^{n-n'} = e_{\mathrm{G}}$ et $n - n' > 0$; par suite g est d'ordre fini (d'ordre divisant $n - n'$) : contradiction avec le fait que $\langle g \rangle$ soit infini.

◇ surjectif car $\mathrm{G} = \langle g \rangle$, *i.e.* tout élément de G s'écrit $f(n)$ pour un certain n.

Finalement f réalise un isomorphisme de groupes entre G et $\mathbb{Z}$. □

Exemple 2.2.9. — Le sous-groupe $\langle 2 \rangle = \{2^n \,|\, n \in \mathbb{Z}\}$ de $\mathbb{Q}^\times$ est mogonène et infini de générateur 2 ; il est donc isomorphe à $\mathbb{Z}$ via le morphisme $f\colon \mathbb{Z} \to \langle 2 \rangle$, $n \mapsto 2^n$.

Théorème 2.2.2

Tout groupe cyclique d'ordre m est isomorphe à ${\mathbb{Z}}/{m\mathbb{Z}}$.

Démonstration. — Soit G un groupe cyclique d'ordre m et de générateur g. Puisque l'ordre de $\langle g \rangle$ et l'ordre de g coïncident, g est d'ordre m. Considérons

$$f\colon {\mathbb{Z}}/{m\mathbb{Z}} \to \mathrm{G}, \qquad a \bmod m \mapsto g^a.$$

Remarquons que f est bien défini, *i.e.* que si $a \equiv a' \bmod m$, alors $g^a = g^{a'}$: si $a \equiv a' \bmod m$, c'est-à-dire si $a = a' + mk$ pour un certain $k \in \mathbb{Z}$, alors

$$g^a = g^{a'+mk} = g^{a'} g^{mk} = g^{a'} (g^m)^k = g^{a'} e_{\mathrm{G}}^k = g^{a'}.$$

La fonction f est un morphisme de groupes car

$$f(a \bmod m) f(b \bmod m) = g^a g^b = g^{a+b} = f((a+b) \bmod m) = f(a \bmod m + b \bmod m).$$

Puisque G est un groupe cyclique de générateur g tout élément de G s'écrit sous la forme g^k avec $k \in \mathbb{Z}$; autrement dit tout élément de G s'écrit $f(k \bmod m)$. Le morphisme de groupes f est donc surjectif. Étant donné que G et ${\mathbb{Z}}/{m\mathbb{Z}}$ sont tous deux d'ordre m, le morphisme

$f\colon \mathbb{Z}/m\mathbb{Z} \to \mathrm{G}$ est surjectif si et seulement s'il est bijectif. Ainsi f réalise un isomorphisme entre G et $\mathbb{Z}/m\mathbb{Z}$. □

La construction de l'isomorphisme f entre $\mathbb{Z}$ (ou $\mathbb{Z}/m\mathbb{Z}$) et un groupe cyclique G dépend du choix d'un générateur puisque $f(1) = g$. Si nous utilisons un autre générateur de G, nous obtiendrons un autre isomorphisme.

Exemple 2.2.10. — Le groupe des racines 5ième de l'unité $\mu_5 = \{z \in \mathbb{C}^* \mid z^5 = 1\}$ est cyclique de générateur $e^{2\mathbf{i}\pi/5}$; il est isomorphe à $\mathbb{Z}/5\mathbb{Z}$ via $f\colon \mathbb{Z}/5\mathbb{Z} \to \mu_5$, $k \bmod 5 \mapsto e^{2\mathbf{i}k\pi/5}$.

Exemple 2.2.11. — Considérons encore le groupe $\mu_5 = \{z \in \mathbb{C}^* \mid z^5 = 1\}$ des racines 5ième de l'unité. Remarquons que $e^{2\mathbf{i}\pi/5}$ et $e^{4\mathbf{i}\pi/5}$ sont deux générateurs distincts de μ_5 :

$$\mu_5 = \langle e^{2\mathbf{i}\pi/5} \rangle = \langle e^{4\mathbf{i}\pi/5} \rangle.$$

Le générateur $e^{2\mathbf{i}\pi/5}$ fournit l'isomorphisme $f\colon \mathbb{Z}/5\mathbb{Z} \to \mu_5$, $k \bmod 5 \mapsto e^{2\mathbf{i}k\pi/5}$ alors que $e^{4\mathbf{i}\pi/5}$ fournit l'isomorphisme $F\colon \mathbb{Z}/5\mathbb{Z} \to \mu_5$, $k \bmod 5 \mapsto e^{4\mathbf{i}k\pi/5}$. Ces deux morphismes sont distincts car ils ne prennent pas les mêmes valeurs :

$k \bmod 5$	0	1	2	3	4
$f(k \bmod 5)$	1	$e^{2\mathbf{i}\pi/5}$	$e^{4\mathbf{i}\pi/5}$	$e^{6\mathbf{i}\pi/5}$	$e^{8\mathbf{i}\pi/5}$
$F(k \bmod 5)$	1	$e^{4\mathbf{i}\pi/5}$	$e^{8\mathbf{i}\pi/5}$	$e^{2\mathbf{i}\pi/5}$	$e^{6,\mathbf{i}\pi/5}$

Corollaire 2.2.1

Tout groupe d'ordre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Démonstration. — Soit p un nombre premier. Soit G un groupe d'ordre p. Considérons un élément g de $\mathrm{G} \smallsetminus \{e_{\mathrm{G}}\}$. L'ordre de $\langle g \rangle$ divise $|\mathrm{G}| = p$ (Théorème de Lagrange, Théorème 1.6.4) et est distinct de 1 (car $g \neq e_{\mathrm{G}}$) ; il en résulte que $\langle g \rangle$ est d'ordre p. À partir de $|\langle g \rangle| = |\mathrm{G}|$ et $\langle g \rangle \subset \mathrm{G}$ nous obtenons $\langle g \rangle = \mathrm{G}$: le groupe G est cyclique. Le Théorème 2.2.2 assure que G et $\mathbb{Z}/p\mathbb{Z}$ sont isomorphes via $\mathbb{Z}/p\mathbb{Z} \to \mathrm{G}$, $a \bmod p \mapsto g^a$. □

Théorème 2.2.3

Si $\varphi\colon \mathrm{G} \to \widetilde{\mathrm{G}}$ est un isomorphisme de groupes, alors $\varphi^{-1}\colon \widetilde{\mathrm{G}} \to \mathrm{G}$ est aussi un isomorphisme de groupes.

Démonstration. — Commençons par montrer que φ^{-1} est un morphisme de groupes. Soient y et y' deux éléments de $\widetilde{\mathrm{G}}$; ils s'écrivent $y = \varphi(x)$ et $y' = \varphi(x')$ avec x et x' dans G. Remarquons

que x et x' sont uniques (φ est un isomorphisme de groupes). Alors $yy' = \varphi(x)\varphi(x') = f(xx')$ d'où

$$\varphi^{-1}(yy') = xx' = \varphi^{-1}(y)\varphi^{-1}(y').$$

Montrons que φ^{-1} est surjective. Soit x un élément de G. Posons $y = \varphi(x) \in \widetilde{\mathrm{G}}$. Alors $\varphi^{-1}(y) = x$; autrement dit tout élément de G est l'image par φ^{-1} d'un élément de $\widetilde{\mathrm{G}}$.

Pour finir montrons que φ^{-1} est injective. Comme φ^{-1} est un morphisme de groupes montrer que φ^{-1} est injective est équivalent à montrer que $\ker\varphi^{-1}$ est trivial. Soit $y \in \ker\varphi^{-1}$, alors $\varphi^{-1}(y) = e_{\mathrm{G}}$ ce qui conduit à $y = \varphi(e_{\mathrm{G}})$. Mais f étant un morphisme de groupes, $\varphi(e_{\mathrm{G}}) = e_{\widetilde{\mathrm{G}}})$ (Théorème 2.1.1). Ainsi $y = e_{\widetilde{\mathrm{G}}}$ et $\ker\varphi^{-1} = \{e_{\widetilde{\mathrm{G}}}\}$. □

Remarque 2.2.1. — On aurait bien évidemment pu se passer de la démonstration du fait que φ^{-1} était bijective. Une application $\varphi\colon E \to F$ étant bijective si et seulement si elle possède une application réciproque $\varphi^{-1}\colon F \to E$. Mais alors φ est la réciproque de φ^{-1} qui est donc elle aussi bijective.

Mais nous avons pris prétexte de ce résultat pour retravailler les propriétés des morphismes de groupes.

Théorème 2.2.4

La composée de deux isomorphismes de groupes est un isomorphisme de groupes.

Démonstration. — Soient $\varphi_1\colon \mathrm{G}_1 \to \mathrm{G}_2$ et $\varphi_2\colon \mathrm{G}_2 \to \mathrm{G}_3$ deux isomorphismes de groupes.

D'une part $\varphi_2 \circ \varphi_1$ est un morphisme de groupes (Théorème 2.1.2).

D'autre part $\varphi_2 \circ \varphi_1$ est bijective (exercice).

Finalement $\varphi_2 \circ \varphi_1$ réalise un isomorphisme entre G_1 et G_3. □

Exemple 2.2.12. — Soient $\mathrm{G} = \langle g \rangle$ et $\widetilde{\mathrm{G}} = \langle \widetilde{g} \rangle$ deux groupes cycliques de même ordre (fini ou infini). Chacun de ces groupes est isomorphe à un certain $\mathbb{Z}/m\mathbb{Z}$ ou à $\mathbb{Z}$ d'où (Théorème 2.2.4) l'existence d'un isomorphisme $\mathrm{G} \to \widetilde{\mathrm{G}}$, $g^k \mapsto \widetilde{g}^k$ entre G et $\widetilde{\mathrm{G}}$.

Considérons la relation $\mathcal{R}$ définie par : le groupe G est en relation avec le groupe H, *i.e.* $\mathrm{G}\mathcal{R}\mathrm{H}$, si et seulement si G et H sont isomorphes. La relation $\mathcal{R}$ est

- ◇ réflexive (pour tout groupe G la fonction $\mathrm{id}\colon \mathrm{G} \to \mathrm{G}$, $g \mapsto g$ est un isomorphisme de groupes) ;
- ◇ symétrique (Théorème 2.2.3) ;
- ◇ transitive (Théorème 2.2.4).

Nous pouvons donc énoncer le

Corollaire 2.2.2

Considérons la relation $\mathcal{R}$ définie par : le groupe G est en relation avec le groupe H, *i.e.* G$\mathcal{R}$H, si et seulement si G et H sont isomorphes. La relation $\mathcal{R}$ est une relation d'équivalence.

Les propriétés des groupes qui sont décrites uniquement en termes d'opération de groupe se transportent d'un groupe à un groupe isomorphe. Donnons deux exemples :

Théorème 2.2.5

Soient G et H deux groupes. Soit $\varphi\colon \mathrm{G} \to \mathrm{H}$ un isomorphisme de groupes. Soit g un élément de G. Alors g est d'ordre k si et seulement si $\varphi(g)$ est d'ordre k.
En particulier, deux groupes isomorphes ont le même nombre d'éléments d'ordre d.

Démonstration. — Il suffit d'appliquer le Corollaire 2.1.1 à φ puis à φ^{-1}. □

Exemple 2.2.13. — Les groupes D_8 et $\mathbb{H}_8$ ne sont pas isomorphes : D_8 compte cinq éléments d'ordre 2 et $\mathbb{H}_8$ n'en compte qu'un.

Remarque 2.2.2. — Deux groupes de même ordre n qui comptent le même nombre d'éléments d'ordre d pour tout diviseur d de n ne sont pas nécessairement isomorphes.

Les groupes $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{H}_8 \times \mathbb{Z}/2\mathbb{Z}$ sont d'ordre 16 et comptent tous deux :

- ◇ un élément d'ordre 1 ;
- ◇ trois éléments d'ordre 2 ;
- ◇ douze éléments d'ordre 4.

Le groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est abélien et $\mathbb{H}_8 \times \mathbb{Z}/2\mathbb{Z}$ ne l'est pas ; en particulier $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{H}_8 \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes.

Théorème 2.2.6

Soient G et $\widetilde{\mathrm{G}}$ deux groupes isomorphes.
Les centres de ces deux groupes sont isomorphes. En particulier le groupe G est abélien si et seulement si $\widetilde{\mathrm{G}}$ l'est.
Le groupe G est cyclique si et seulement si $\widetilde{\mathrm{G}}$ l'est.

Démonstration. — Soit $\varphi\colon \mathrm{G} \to \widetilde{\mathrm{G}}$ un isomorphisme de groupes.

Soient $g \in Z(\mathrm{G})$ et $\widetilde{h} \in \widetilde{\mathrm{G}}$. Puisque g est dans le centre de G, on a $g\varphi^{-1}(\widetilde{h}) = \varphi^{-1}(\widetilde{h})g$ et donc aussi $\varphi\left(g\varphi^{-1}(\widetilde{h})\right) = \varphi\left(\varphi^{-1}(\widetilde{h})g\right)$, soit $\varphi(g)\widetilde{h} = \widetilde{h}\varphi(g)$ et $\varphi(g) \in Z(\widetilde{\mathrm{G}})$. On vient de vérifier que $\varphi(Z(\mathrm{G})) \subset Z(\widetilde{\mathrm{G}})$. Pour les mêmes raisons on a $\varphi^{-1}(Z(\widetilde{\mathrm{G}})) \subset Z(\mathrm{G})$ ce qui, après composition

par φ, donne $Z(\widetilde{\mathrm{G}}) \subset \varphi(Z(\mathrm{G}))$. Inclusion qui permet de conclure que $\varphi(Z(\mathrm{G})) = Z(\widetilde{\mathrm{G}})$: les centres de G et $\widetilde{\mathrm{G}}$ sont isomorphes.

Si G est abélien alors $Z(\mathrm{G}) = G$ et on a $\widetilde{\mathrm{G}} = \varphi(\mathrm{G}) = \varphi(Z(\mathrm{G})) = Z(\widetilde{\mathrm{G}})$. On a donc $\widetilde{\mathrm{G}} = Z(\widetilde{\mathrm{G}})$ et $\widetilde{\mathrm{G}}$ est abélien.

Supposons que G soit abélien. Pour tous x, x' dans G nous avons :

$$xx' = x'x \Longrightarrow \varphi(xx') = \varphi(x'x) \Longrightarrow \varphi(x)\varphi(x') = \varphi(x')\varphi(x).$$

Puisque φ est surjectif, tout élément de $\widetilde{\mathrm{G}}$ est une valeur de φ ; ainsi tous les couples d'éléments de $\widetilde{\mathrm{G}}$ commutent et $\widetilde{\mathrm{G}}$ est abélien.

Réciproquement, si $\widetilde{\mathrm{G}}$ est abélien, alors pour tous x, x' dans G nous avons $\varphi(x)\varphi(x') = \varphi(x')\varphi(x)$ qui se réécrit $\varphi(xx') = \varphi(x'x)$. Comme φ est injective nous en déduisons que $xx' = x'x$: le groupe G est donc abélien.

Supposons désormais que G soit cyclique. Soit g un générateur de G, c'est-à-dire $\mathrm{G} = \langle g \rangle = \{g^a \mid a \in \mathbb{Z}\}$. Tout élément y de $\widetilde{\mathrm{G}}$ s'écrit $\varphi(x)$ pour un certain x dans G et x est de la forme g^a, $a \in \mathbb{Z}$, car $\mathrm{G} = \langle g \rangle$. Il en résulte que $y = \varphi(g^a) = (\varphi(g))^a$ (Théorème 2.1.1). En particulier, tout élément de $\widetilde{\mathrm{G}}$ est de la forme $\varphi(g)^k$, $k \in \mathbb{Z}$, *i.e.* $\widetilde{\mathrm{G}} = \langle \varphi(g) \rangle$: le groupe $\widetilde{\mathrm{G}}$ est cyclique.

Réciproquement, supposons que $\widetilde{\mathrm{G}}$ soit cyclique. Soit $\widetilde{g}$ un générateur de $\widetilde{\mathrm{G}}$. Le morphisme φ étant surjectif il existe $g \in \mathrm{G}$ tel que $\widetilde{g} = \varphi(g)$. Pour tout $x \in \mathrm{G}$ il existe un entier n tel que $\varphi(x) = \widetilde{g}^n$; ainsi pour tout $x \in \mathrm{G}$ il existe un entier n tel que $\varphi(x) = \varphi(g)^n$ ou encore tel que $\varphi(x) = \varphi(g^n)$ (Théorème 2.1.1). Le morphisme φ étant injectif $\varphi(x) = \varphi(g^n)$. Le morphisme φ étant injectif $\varphi(x) = \varphi(g^n)$ conduit à $x = g^n$. Autrement dit tout élément de G s'écrit comme une puissance de g et $\mathrm{G} = \langle g \rangle$ est cyclique. □

Remarque 2.2.3. — Mentionnons une autre façon de démontrer que si $\widetilde{\mathrm{G}}$ est abélien alors G est abélien. En utilisant l'isomorphisme inverse dont l'existence est assurée par le Théorème 2.2.3 nous pouvons utiliser un raisonnement analogue à celui utiliser pour montrer que « G abélien implique $\widetilde{\mathrm{G}}$ abélien »pour établir la réciproque.

Nous pouvons bien sûr utiliser cet argument pour démontrer la seconde assertion du Théorème 2.2.6.

Lorsque nous classifions les groupes ayant une propriété particulière nous ne faisons pas de distinction entre les groupes isomorphes car un groupe possède la propriété si et seulement si l'autre l'a. Par exemple le Corollaire 2.2.1 assure que tous les groupes d'ordre premier p sont isomorphes à $\mathbb{Z}/p\mathbb{Z}$ et donc que tous les groupes d'ordre premier p sont isomorphes entre eux ; on dit qu'ils sont « les mêmes à isomorphisme près ». Lorsque nous abordons des problèmes de classification en théorie des groupes, nous ne nous préoccupons pas de lister tous les groupes ayant une propriété donnée mais de lister tous les groupes à isomorphisme près ayant une propriété donnée. Avant de donner un exemple introduisons la notation suivante. Étant donné un entier $n > 0$ nous désignons par $\mathrm{U}(n)$ l'ensemble des entiers positifs inférieurs à n et relativement premier à n ; cet ensemble muni de la multiplication modulo n forme un groupe.

Par exemple

$$\mathrm{U}(7) = \{1, 2, 3, 4, 5, 6\} = \langle 3 \rangle, \qquad \mathrm{U}(9) = \{1, 2, 4, 5, 7, 8\} = \langle 2 \rangle.$$

Considérons par exemple le problème qui consiste à classifier les groupes d'un ordre donné n.

Le Corollaire 2.2.1 assure qu'un groupe

- ◇ d'ordre 2 est isomorphe à $\mathbb{Z}/2\mathbb{Z}$;
- ◇ d'ordre 3 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

Les groupes

$$\mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathrm{U}(5),\ \mathrm{U}(8),\ \mathrm{U}(10),\ \mathrm{U}(12),\ \langle \mathbf{i} \rangle,\ \{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4),\ (2\ 3)\}$$

sont d'ordre 4 ; il y a encore beaucoup d'autres groupes d'ordre 4. Remarquons que

$$\mathbb{Z}/4\mathbb{Z} \simeq \mathrm{U}(5) \simeq \mathrm{U}(10) \simeq \langle \mathbf{i} \rangle$$

et

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{U}(8) \simeq \mathrm{U}(12) \simeq \{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

De plus, $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes (première justification possible : $\mathbb{Z}/4\mathbb{Z}$ est cyclique alors que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne l'est pas, Théorème 2.2.6 ; seconde justification possible : $\mathbb{Z}/4\mathbb{Z}$ contient un élément d'ordre 4 alors que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'en contient pas, Corollaire 2.1.1). On peut montrer qu'à isomorphisme près il y a deux groupes d'ordre 4 :

Théorème 2.2.7

Un groupe G d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On constate en particulier qu'un groupe d'ordre 4 est nécessairement abélien.

On en déduit aussi que le groupe de Klein de l'Exemple 1.3.13, le plus petit groupe à ne pas être cyclique, est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. — Soit $\mathrm{G} = \{e_{\mathrm{G}}, a, b, c\}$ un groupe d'ordre 4.

S'il possède un élément d'ordre 4 alors il est cyclique et donc isomorphe à $\mathbb{Z}/4\mathbb{Z}$ d'après le Théorème 2.2.2.

Sinon a, b et c sont d'ordre 2. En effet, leur ordre doit diviser celui du groupe d'après le théorème de Lagrange (Théorème 1.6.4). Il ne vaut pas 1 puisque seul e_{G} est d'ordre 1, et il ne peut pas valoir 4 puisque le groupe n'est pas cyclique.

Par unicité de l'inverse on a $ab \neq e_{\mathrm{G}}$ et $ba \neq e_{\mathrm{G}}$. Supposons que $ab = a$ (respectivement $ba = a$). Comme a est d'ordre 2, en multipliant cette égalité à gauche (resp. à droite) par a on aboutirait à $a^2 b = a^2$ (resp. $ba^2 = a^2$). C'est-à-dire, puisque $a^2 = e_{\mathrm{G}}$, $b = e_{\mathrm{G}}$, qui est faux. On en déduit que $ab \neq a$ et $ba \neq a$. On montrerait de la même manière que $ab \neq b$ et $ba \neq b$. Alors $ab = ba = c$ et un raisonnement similaire montre que $ac = ca = b$ et $bc = cb = a$.

Nous définissons alors $\varphi\colon \mathrm{G} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ en posant $\varphi(e_{\mathrm{G}}) = (\bar{0}, \bar{0})$, $\varphi(a) = (\bar{1}, \bar{0})$, $\varphi(b) = (\bar{0}, \bar{1})$ et $\varphi(c) = (\bar{1}, \bar{1})$. C'est évidemment une application bijective ; les relations obtenues précédemment permettent de vérifier qu'il s'agit d'un morphisme de groupes. Le groupe G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

Les groupes

$$\mathbb{Z}/6\mathbb{Z},\ \mathfrak{S}_3,\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\ \mathrm{U}(7),\ \mathrm{U}(9),\ \mathrm{U}(14),\ \mathrm{U}(18),\ \mathrm{D}_6,\ \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right),\ \mathrm{Aff}\left(\mathbb{Z}/3\mathbb{Z}\right)$$

sont d'ordre 6 ; cette liste n'est pas exhaustive. On peut vérifier que

$$\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathrm{U}(7) \simeq \mathrm{U}(9) \simeq \mathrm{U}(14) \simeq \mathrm{U}(18)$$

et

$$\mathfrak{S}_3 \simeq \mathrm{D}_6 \simeq \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right) \simeq \mathrm{Aff}\left(\mathbb{Z}/3\mathbb{Z}\right)$$

Remarquons que $\mathbb{Z}/6\mathbb{Z}$ et $\mathfrak{S}_3$ ne sont pas isomorphes (première justification possible : $\mathbb{Z}/6\mathbb{Z}$ est abélien alors que $\mathfrak{S}_3$ ne l'est pas, Théorème 2.2.6 ; seconde justification possible : $\mathbb{Z}/6\mathbb{Z}$ contient un élément d'ordre 6 alors que $\mathfrak{S}_3$ n'en contient pas, Corollaire 2.1.1).

En fait pour les groupes d'ordre 6 on a

Théorème 2.2.8

Un groupe G d'ordre 6 est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ou $\mathfrak{S}_3$.

Démonstration. — Puisque G est d'ordre 6, le neutre est d'ordre 1 et les autres éléments sont d'ordre 2, 3, ou 6.

Si G ne possède que des éléments d'ordre 2 il est abélien d'après le Lemme 2.2.1.

Soient e_{G}, a et b trois éléments distincts de G, alors $ab = ba$ est un quatrième élément. En effet, a et b ne sont pas inverses l'un de l'autre donc $ab \neq e_{\mathrm{G}}$ et $ab = a$ entraînerait, par multiplication à droite par b, $a = e_{\mathrm{G}}$, ce qui est faux. Soit c un cinquième élément de G. Que vaut ac ? Il ne peut pas être égal à e_{G}, a et c n'étant pas inverses l'un de l'autre. Il ne peut pas être égal à a ni à c. Il ne peut pas être égal à ab, l'égalité $ac = ab$ mènerait à $c = b$ qui est fausse. Si $ac = b$, alors en multipliant à gauche par a on aboutirait à $ab = c$ qui est fausse. Donc ac est le sixième et dernier élément de G. On a donc :

$$\mathrm{G} = \{e_{\mathrm{G}}, a, b, c, ab, ac\}.$$

Comme il s'agit d'un groupe, on a $bc \in \mathrm{G}$. Mais comme nous l'avons déjà vu précédemment on a $bc \neq e_{\mathrm{G}}$, $bc \neq b$, $bc \neq c$, $bc \neq ab$ et $bc \neq ac$. C'est-à-dire $bc \notin \mathrm{G}$! C'est absurde, notre hypothèse initiale est fausse et G contient au moins un élément d'ordre 6, auquel cas en vertu du Théorème 2.2.2, il est isomorphe à $\mathbb{Z}/6\mathbb{Z}$, ou un élément d'ordre 3, et donc 2, puisque l'inverse d'un élément d'ordre 3 est aussi d'ordre 3.

D'autre part, d'après le Lemme 2.2.2, il y a au moins un élément d'ordre 2 dans G puisque son ordre égal à 6 est pair.

Soient alors a un élément d'ordre 3 et b un élément d'ordre 2. Si a et b commutent alors ab est d'ordre 6, le groupe est cyclique isomorphe à $\mathbb{Z}/6\mathbb{Z}$. Sinon, $ab \neq ba$ et on a

$$\mathrm{G} = \{e_{\mathrm{G}}, a, a^2, b, ab, ba\}.$$

Quel est l'ordre de ab, celui de ba ?

On a $(ab)(ba) = ab^2a = a^2 \neq e_{\mathrm{G}}$, ce qui indique que ab et ba ne sont pas inverses l'un de l'autre. Comme ni a, ni a^2 et ni b ne peuvent être leur inverse, ils sont donc tous les deux d'ordre 2. On a donc $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^2$ et $ba = (ba)^{-1} = a^{-1}b^{-1} = a^2b$.

On a alors :

$\times$	e_{G}	a	a^2	b	ab	ba
e_{G}	e_{G}	a	a^2	b	ab	ba
a	a	a^2	e_{G}	ab	ba	b
a^2	a^2	e_{G}	a	ba	b	ab
b	b	ba	ab	e_{G}	a^2	a
ab	ab	b	ba	a	e_{G}	a^2
ba	ba	ab	b	a^2	a	e_{G}

$\times$	id	$(1\,2\,3)$	$(1\,3\,2)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$
id	id	$(1\,2\,3)$	$(1\,3\,2)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$
$(1\,2\,3)$	$(1\,2\,3)$	$(1\,3\,2)$	id	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$
$(1\,3\,2)$	$(1\,3\,2)$	id	$(1\,2\,3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$
$(1\ 2)$	$(1\ 2)$	$(2\ 3)$	$(1\ 3)$	id	$(1\,3\,2)$	$(1\,2\,3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 2)$	$(2\ 3)$	$(1\,2\,3)$	id	$(1\,3\,2)$
$(2\ 3)$	$(2\ 3)$	$(1\ 3)$	$(1\ 2)$	$(1\,3\,2)$	$(1\,2\,3)$	id

À gauche la table de Cayley de G, à droite celle de $\mathfrak{S}_3$

En suivant les couleurs des deux tableaux et en s'assurant qu'elles respectent la loi des deux groupes, par exemple $(1\ 2\ 3)^2 = (1\ 3\ 2)$, ou encore $(1\ 2\ 3)(1\ 2) = (1\ 3)$, on définit maintenant $\varphi\colon \mathrm{G} \to \mathfrak{S}_3$ en posant $\varphi(e_{\mathrm{G}}) = \mathrm{id}$, $\varphi(a) = (1\ 2\ 3)$, $\varphi(b) = (1\ 2)$ et en prolongeant afin de définir un morphisme de groupes. C'est un isomorphisme de groupes. □

Lemme 2.2.1

Un groupe dont tous les éléments non triviaux sont d'ordre 2 est abélien.

Démonstration. — Dans un tel groupe G on a $g^{-1} = g$ pour tout $g \in \mathrm{G}$.

Soient a et b deux éléments de G alors $ab \in \mathrm{G}$ et on a : $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

Le groupe G est abélien. □

Lemme 2.2.2

Un groupe d'ordre pair possède un élément d'ordre 2.

Démonstration. — Soient G un tel groupe et g un de ses éléments. L'ensemble $\{g, g^{-1}\}$ contient deux éléments sauf si $g = e_{\mathrm{G}}$ ou si $g = g^{-1}$ auquel cas c'est un singleton. Posons $\mathrm{E}_1 = \{g \in \mathrm{G} \,|\, g \neq g^{-1}\}$ et $\mathrm{E}_2 = \{g \in \mathrm{G} \,|\, g = g^{-1}\}$.

Il s'agit d'une partition de G ; par suite $|\mathrm{G}| = \#\mathrm{E}_1 + \#\mathrm{E}_2$. Le groupe étant d'ordre pair cela donne :

$$0 \equiv_2 \#\mathrm{E}_1 + \#\mathrm{E}_2\cdot$$

Comme $\mathrm{E}_1 = \bigcup_{g \neq g^{-1}} \{g, g^{-1}\}$, c'est un ensemble dont le cardinal est pair et on a donc :

$$0 \equiv_2 \#\mathrm{E}_2\cdot$$

Enfin, puisque $e_{\mathrm{G}} \in \mathrm{E}_2$, on a $\#\mathrm{E}_2 \geq 1$. Ainsi $\#\mathrm{E}_2$ est un nombre pair supérieur à 1, c'est donc au moins 2. L'ensemble E_2 possède au moins deux éléments ce qui signifie qu'il existe au moins un élément d'ordre 2. □

Autre démonstration du Théorème 2.2.8. — ◇ Montrons qu'un groupe abélien d'ordre 6 est isomorphe à $\mathbb{Z}/6\mathbb{Z}$.

Soit G un groupe abélien d'ordre 6. D'après le Lemme 2.2.2 le groupe G contient un élément g d'ordre 2. D'après le Théorème de Lagrange (Théorème 1.6.4) tout élément de $\mathrm{G} \smallsetminus \{e\}$ est d'ordre 2, 3 ou 6. Supposons que tous les éléments de $\mathrm{G} \smallsetminus \{e\}$ soient d'ordre 2. Soit h dans $\mathrm{G} \smallsetminus \{e, g\}$. Puisque G est abélien $\{e, g, h, gh\}$ est un sous-groupe d'ordre 4 de G ce qui contredit le Théorème de Lagrange (Théorème 1.6.4). Par suite G contient un élément d'ordre 3 ou 6.

- Si G contient un élément d'ordre 6, alors G est cyclique et $\mathrm{G} \simeq \mathbb{Z}/6\mathbb{Z}$.
- Si $k \in \mathrm{G}$ est un élément d'ordre 3 de G, alors gk est d'ordre 6. En effet

$$(gk)^2)g^2k^2 = k^2 \neq e, \qquad (gk)^3 = g^3k^3 = g^3 = g \neq e, \qquad (gk)^6 = g^6k^6 = e.$$

Dans ce cas aussi G est cyclique et $\mathrm{G} \simeq \mathbb{Z}/6\mathbb{Z}$.

◇ Montrons qu'un groupe non abélien d'ordre 6 est isomorphe à $\mathfrak{S}_3$.

Le groupe G ne contient pas d'élément d'ordre 6. Ainsi le Théorème de Lagrange assure que les éléments de G sont d'ordre 1, 2 ou 3. D'après le Lemme 2.2.1 le groupe G contient nécessairement un élément d'ordre 3.

Soient x un élément d'ordre 2 de G et y un élément d'ordre 3 de G. Posons $\mathrm{H} = \langle x \rangle = \{e, x\}$ Il y a trois classes à gauche qui sont H, $y\mathrm{H}$, $y^2\mathrm{H}$ puisque y n'appartient pas à H. Pour tout $g \in \mathrm{G}$ nous définissons

$$\ell_g \colon \{\mathrm{H}, y\mathrm{H}, y^2\mathrm{H}\} \to \{\mathrm{H}, y\mathrm{H}, y^2\mathrm{H}\}, \qquad c\mathrm{H} \mapsto gc\mathrm{H}.$$

Remarquons que ℓ_g est inversible d'inverse $\ell_{g^{-1}}$; ainsi ℓ_g est une permutation de $\mathfrak{S}_3$. La fonction $\varphi \colon \mathrm{G} \to \mathfrak{S}_3$, $g \mapsto \ell_g$ est un morphisme de groupes ; en effet, pour tout $c\mathrm{H}$ nous avons

$$(\ell_g \circ \ell_h)(c\mathrm{H}) = \ell_g(\ell_h(c\mathrm{H})) = \ell_g(hc\mathrm{H}) = g(hc\mathrm{H}) = (gh)c\mathrm{H} = \ell_{gh}(c\mathrm{H})$$

Montrons que φ est injective. Soit $g \in \ker\varphi$. On a alors $g\mathrm{H} = \mathrm{H}$, $gy\mathrm{H} = y\mathrm{H}$ et $gy^2\mathrm{H} = y^2\mathrm{H}$. De $g\mathrm{H} = \mathrm{H}$ on tire $g \in \mathrm{H}$, soit $g = e$ ou $g = x$. Montrons que $g = x$ n'est pas

possible. Si tel était le cas on aurait donc $xy\mathrm{H} = gy\mathrm{H} = y\mathrm{H}$, d'où on déduit $y \in xy\mathrm{H}$, soit $y = xy$ ou $y = xyx$. Mais $y = xy$ implique $x = e$, ce qui est faux puisque x est d'ordre 2, donc $y = xyx$ ce qui implique $xy = yx$ et donc que x et y commutent. L'ordre de xy est alors égal au plus petit commun multiple des ordres de x et y, soit 6 ; le groupe est alors cyclique, donc abélien, ce qui met notre hypothèse sur G à défaut. Donc $g = e$ et φ est injective. [1] Comme $|\mathrm{G}| = |\mathfrak{S}_3|$ le morphisme de groupes φ est un isomorphisme.

□

2.3. Produits directs

Pour deux groupes H et K, la construction la plus élémentaire d'un groupe contenant des copies de H et K en tant que sous-groupes est le produit direct $\mathrm{H} \times \mathrm{K}$, où la loi de groupe est : $(h, k)(h', k') = (hh', kk')$. Puisque $(h, 1)(h', 1) = (hh', 1)$ et $(1, k)(1, k') = (1, kk')$, on peut plonger H et K dans $\mathrm{H} \times \mathrm{K}$ « via » $h \mapsto (h, 1)$ et $k \mapsto (1, k)$ pour $h \in \mathrm{H}$ et $k \in \mathrm{K}$. Cela nous permet de considérer $\mathrm{H} \times \mathrm{K}$ comme un groupe engendré par des sous-groupes isomorphes à H et K. Certains groupes peuvent se décomposer en un produit direct de groupes plus petits, cela facilite leur étude ; par exemple, tout groupe abélien fini est isomorphe au produit direct de ses sous-groupes de Sylow. Néanmoins tous les groupes ne sont pas isomorphes à un produit direct de groupes plus petits : $\mathfrak{S}_n$ pour $n \geq 3$ ne l'est pas.

À partir de deux groupes H et K nous pouvons faire une construction un peu plus « subtile » que $\mathrm{H} \times \mathrm{K}$ qu'on appelle produit semi-direct qui a d'autres avantages comme par exemple :

(i) un produit semi-direct peut être non-abélien même si H et K sont abéliens (alors que $\mathrm{H} \times \mathrm{K}$ est abélien si et seulement si H et K sont abéliens)

(ii) à partir de H et K nous pouvons obtenir plusieurs produits semi-directs non isomorphes.

Lorsque H et K sont plongés dans $\mathrm{H} \times \mathrm{K}$ de manière canonique, les images de H et K à l'intérieur de $\mathrm{H} \times \mathrm{K}$ vérifient les propriétés suivantes :

- ◇ elles engendrent $\mathrm{H} \times \mathrm{K}$: $(h, k) = (h, 1)(1, k)$,
- ◇ elles s'intersectent trivialement : $(h, e) = (e, k) \Rightarrow h = e,\ k = e$,
- ◇ elles commutent : $(h, e)(e, k) = (e, k)(h, e)$.

---

1. On aurait aussi pu montrer que φ est surjective. La permutation ℓ_y est un 3-cycle : $\ell_y(\mathrm{H}) = y\mathrm{H}$, $\ell_y(y\mathrm{H}) = y^2\mathrm{H}$ et $\ell_y(y^2\mathrm{H}) = \mathrm{H}$; autrement dit l'image de φ contient un 3-cycle. Remarquons que x appartenant à H nous avons $\ell_x(\mathrm{H}) = x\mathrm{H} = \mathrm{H}$. Étant donné que ℓ_x est une permutation, si $\ell_x(y\mathrm{H}) \neq y^2\mathrm{H}$, alors $\ell_x(y\mathrm{H}) = y\mathrm{H}$ c'est-à-dire $xy\mathrm{H} = y\mathrm{H}$ ou encore $\{xy, xyx\} = \{y, yx\}$. En particulier, xy est y ou yx.

- Si $xy = y$, alors $x = e$ ce qui contredit le fait que x est d'ordre 2.
- Si $xy = yx$, alors x et y commutent donc xy est d'ordre 6 ce qui contredit le fait que G n'est pas abélien.

Il en résulte que $\ell_x(y\mathrm{H}) = y^2\mathrm{H}$ et $\ell_x(y^2\mathrm{H}) = y\mathrm{H}$. La permutation ℓ_x est donc une transposition de $\mathfrak{S}_3$. L'image de φ est donc un sous-groupe de $\mathfrak{S}_3$ qui contient une transposition et un 3-cycle ; le Théorème de Lagrange (Théorème 1.6.4) assure que $\operatorname{im}\varphi$ est d'ordre 6, *i.e.* φ est surjective.

L'énoncé suivant donne une caractérisation des groupes isomorphes à un produit direct :

Théorème 2.3.1

Le groupe G est isomorphe à un produit direct si et seulement si il possède deux sous-groupes distingués H et K tels que $\mathrm{H} \cap \mathrm{K} = \{e\}$ et $\mathrm{HK} = \mathrm{G}$. On a alors $\mathrm{G} \simeq \mathrm{H} \times \mathrm{G}$. Il est possible de remplacer l'hypothèse « H et K sont distingués » par « $hk = kh$ pour tout $(h, k) \in \mathrm{H} \times \mathrm{K}$. ».

Démonstration. — Soit $f\colon \widetilde{\mathrm{H}} \times \widetilde{\mathrm{K}} \to \mathrm{G}$ un isomorphisme de groupes. Les ensembles $\widetilde{\mathrm{H}} \times \{e_{\widetilde{\mathrm{K}}}\}$ et $\{e_{\widetilde{\mathrm{H}}}\} \times \widetilde{\mathrm{K}}$ sont deux sous-groupes du produit cartésien $\widetilde{\mathrm{H}} \times \widetilde{\mathrm{K}}$. Leur image par f, que l'on note respectivement H et K, sont donc deux sous-groupes de G.

Si (h, k) est un élément de $\widetilde{\mathrm{H}} \times \widetilde{\mathrm{K}}$, alors : $(h, k) = (h, e_{\widetilde{\mathrm{K}}})(e_{\widetilde{\mathrm{H}}}, k)$ et donc $f(h, k) = f\left[(h, e_{\widetilde{\mathrm{K}}})(e_{\widetilde{\mathrm{H}}}, k)\right] = f(h, e_{\widetilde{\mathrm{K}}})f(e_{\widetilde{\mathrm{H}}}, k)$, car f est un morphisme de groupes. Or $f(h, e_{\widetilde{\mathrm{K}}}) \in \mathrm{H}$ et $f(e_{\widetilde{\mathrm{H}}}, k) \in \mathrm{K}$ donc $f(h, k) \in \mathrm{HK}$. Comme f est surjectif, tout élément g de G s'écrit sous la forme $f(h, k)$ et donc tout élément de G est dans HK. C'est-à-dire $\mathrm{G} \subset \mathrm{HK}$. L'inclusion réciproque ne fait pas de doute et on a $\mathrm{HK} = \mathrm{G}$.

Soit $g \in \mathrm{H} \cap \mathrm{K}$. Il existe $(h, k) \in \widetilde{\mathrm{H}} \times \widetilde{\mathrm{K}}$ tel que $g = f(h, e_{\widetilde{\mathrm{K}}})$ et $g = f(e_{\widetilde{\mathrm{H}}}, k)$. Mais f est surjectif, donc $(h, e_{\widetilde{\mathrm{K}}}) = (e_{\widetilde{\mathrm{H}}}, k)$. Soient $h = e_{\widetilde{\mathrm{H}}}$ et $k = e_{\widetilde{\mathrm{K}}}$; alors $g = f(e_{\widetilde{\mathrm{H}}}, e_{\widetilde{\mathrm{K}}}) = e$ et $\mathrm{H} \cap \mathrm{K} = \{e\}$.

Montrons que H et K sont distingués dans G. Nous faisons la démonstration pour H, celle pour K s'en déduisant. On doit vérifier que pour tout $g \in \mathrm{G}$ on a $g\mathrm{H} = \mathrm{H}g$. Soient $g \in \mathrm{G}$ et $\ell \in \mathrm{H}$. il existe donc $(h, k) \in \widetilde{\mathrm{H}} \times \widetilde{\mathrm{K}}$ tel que $g = f(h, k)$ et $h' \in \widetilde{\mathrm{H}}$ tel que $\ell = f(h', e_{\widetilde{\mathrm{K}}})$. On a

$$(h, k)(h', e_{\widetilde{\mathrm{K}}}) = (hh', k) = (hh'h^{-1}h, k) = (hh'h^{-1}, e_{\widetilde{\mathrm{K}}})(h, k)\cdot$$

Posons $\tilde{h} = hh'h^{-1}$. C'est un élément de H. En appliquant f, qui est un morphisme de groupes, on aboutit à

$$g\ell = f(h, k)f((h', e_{\widetilde{\mathrm{K}}}) = f(hh', k) = f\left[(\tilde{h}, e_{\widetilde{\mathrm{K}}})(h, k)\right] = f(\tilde{h}, e_{\widetilde{\mathrm{K}}})g \in \mathrm{H}g\cdot$$

Par conséquent $g\mathrm{H} \subset \mathrm{H}g$.

Réciproquement on a

$$(h', e_{\widetilde{\mathrm{K}}})(h, k) = (h, k)(h^{-1}h'h, e_{\widetilde{\mathrm{K}}})\cdot$$

On en déduit :

$$f(h', e_{\widetilde{\mathrm{K}}})f(h, k) = f(h, k)f(h^{-1}h'h, e_{\widetilde{\mathrm{K}}})\cdot$$

Ce qui permet de montrer que $\mathrm{H}g \subset g\mathrm{H}$.

Vérifions que dans ces conditions G est isomorphe à $\mathrm{H} \times \mathrm{K}$.

L'application $f\colon \mathrm{H} \times \mathrm{K} \to \mathrm{G}$, $(h, k) \mapsto hk$ est un morphisme :

$$f((h, k)(h', k')) = f(hh', kk') = hh'kk' \overset{\star}{=} h(kh')k' = (hk)(h'k') = f(h, k)f(h', k')$$

où $\overset{\star}{=}$ est une utilisation de l'hypothèse $hk = kh$.

Soit $(h,k) \in \mathrm{H} \times \mathrm{K}$ tel que $f(h,k) = e$ alors $hk = e$ et $h = k^{-1}$ appartient à $\mathrm{H} \cap \mathrm{K}$. Comme $\mathrm{H} \cap \mathrm{K} = \{e\}$; il en résulte que $h = e$ et $k = e$. Finalement f est injectif. Il est aussi surjectif puisque $\mathrm{HK} = \mathrm{G}$.

Nous montrons pour finir l'équivalence des hypothèses « H et K sont distingués » et « $hk = kh$ pour tout $(h,k) \in \mathrm{H} \times \mathrm{K}$ ».

Supposons « $hk = kh$ pour tout $(h,k) \in \mathrm{H} \times \mathrm{K}$ ». Soient $g \in \mathrm{G}$ et $h' \in \mathrm{H}$. Puisque $\mathrm{HK} = \mathrm{G}$, il existe $(h,k) \in \mathrm{H} \times \mathrm{K}$ tel que $g = hk$. On a $gh' = hkh' = hh'k = hh'h^{-1}hk = hh'h^{-1}g$ et $h'g = h'hk = khh^{-1}h'h$ ce qui montre que $g\mathrm{H} = \mathrm{H}g$, *i.e.* H est distingué dans G. On montre de même que K est distingué dans G.

Supposons que H et K sont distingués dans G. Soit $(h,k) \in \mathrm{H} \times \mathrm{K}$; nous avons $k^{-1}hkh^{-1} = (k^{-1}hk)h^{-1}$. Or $hk \in \mathrm{H}k = k\mathrm{H}$, alors $k^{-1}hk \in \mathrm{H}$ et donc $k^{-1}hkh^{-1} \in \mathrm{H}$. Mais on a aussi : $k^{-1}hkh^{-1} = k^{-1}(hkh^{-1})$. Comme K est distingué dans G, on déduit comme précédemment que $hkh^{-1} \in \mathrm{K}$ et que $k^{-1}hkh^{-1} \in \mathrm{K}$. Alors $k^{-1}hkh^{-1}$ appartient à $\mathrm{H} \cap \mathrm{K} = \{e_{\mathrm{G}}\}$. Par suite nous avons $k^{-1}hkh^{-1} = e_{\mathrm{G}}$, soit $hk = kh$. □

Un exemple classique de produit direct est donné par le lemme chinois : *si p et q sont premiers entre eux, alors*

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

On a par exemple :

$$\mathbb{Z}/30\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}.$$

ce qui permet de constater que la décomposition en produit direct n'est pas unique.

Il existe de nombreux groupes qui se décomposent en un produit de deux sous-groupes H et K tels que $\mathrm{HK} = \mathrm{G}$, $\mathrm{H} \cap \mathrm{K} = \{e\}$ sans que les deux sous-groupes soient distingués. La structure est alors celle de produit semi-direct. Elle est abordée en détail au §3.6 et voici quelques exemples :

Exemple 2.3.1. — Considérons le groupe $\mathrm{G} = \mathrm{Aff}(\mathbb{R})$. Il contient les sous-groupes

$$\mathrm{H} = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \mid y \in \mathbb{R} \right\} \simeq \mathbb{R}, \qquad \mathrm{K} = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \,\middle|\, x \in \mathbb{R}^\times \right\} \simeq \mathbb{R}^\times.$$

Puisque

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}}_{\in \mathrm{H}} \underbrace{\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}}_{\in \mathrm{K}}$$

nous avons $\mathrm{G} = \mathrm{HK}$. On peut vérifier que $\mathrm{H} \cap \mathrm{K} = \mathrm{id}$. Néanmoins d'une part $\mathrm{H} \times \mathrm{K}$ est abélien (H et K sont abéliens), d'autre part G n'est pas abélien. En particulier G et $\mathrm{H} \times \mathrm{K}$ ne sont pas isomorphes. Les éléments des deux sous-groupes ne commutent pas :

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 2 & 4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

Exemple 2.3.2. — Considérons le groupe $\mathrm{G} = \mathrm{GL}(2,\mathbb{R})$ et les sous-groupes H et K de G définis par

$$\mathrm{H} = \mathrm{SL}(2,\mathbb{R}), \qquad \mathrm{K} = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R}^\times \right\}.$$

Soit $g \in \mathrm{G}$; alors $\Delta = \det g$ est non nul et la matrice $\begin{pmatrix} \Delta & 0 \\ 0 & 1 \end{pmatrix}$ a un déterminant Δ donc

$$g = \underbrace{g \begin{pmatrix} \Delta & 0 \\ 0 & 1 \end{pmatrix}^{-1}}_{\in \mathrm{H}} \underbrace{\begin{pmatrix} \Delta & 0 \\ 0 & 1 \end{pmatrix}}_{\in \mathrm{K}}.$$

Ainsi $\mathrm{GL}(2,\mathbb{R}) = \mathrm{HK}$. On peut aussi vérifier que $\mathrm{H} \cap \mathrm{K} = \{\mathrm{Id}\}$.

Il s'avère que $\mathrm{GL}(2,\mathbb{R}) \not\simeq \mathrm{SL}(2,\mathbb{R}) \times \mathbb{R}^\times$. En effet, $\mathrm{GL}(2,\mathbb{R})$ possède une infinité d'éléments d'ordre 2 (les réflexions par rapport à n'importe quelle droite de $\mathbb{R}^2$ passant par l'origine), alors que $\mathrm{SL}(2,\mathbb{R})$ et $\mathbb{R}^\times$ possèdent un unique élément d'ordre 2 (la matrice $-\mathrm{Id}$ et -1 respectivement) donc $\mathrm{SL}(2,\mathbb{R}) \times \mathbb{R}^\times$ a trois éléments d'ordre 2. À nouveau les éléments des deux sous-groupes ne commutent pas :

$$\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix} \neq \begin{pmatrix} 2 & 2 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}.$$

Exemple 2.3.3. — Pour cet exemple nous renvoyons au paragraphe 5.1 page 178 pour les définitions précises des groupes symétrique et alterné.

Soit $n \geq 3$ un entier. Considérons le groupe $\mathrm{G} = \mathfrak{S}_n$ et ses deux sous-groupes H et K donnés par

$$\mathrm{H} = \mathcal{A}_n, \qquad \mathrm{K} = \langle (1\ 2) \rangle = \{\mathrm{id}, (1\ 2)\}.$$

Soit σ dans G.

- ⋄ Si $\sigma \in \mathrm{H}$ alors $\sigma = \sigma \mathrm{id}$ appartient à HK,
- ⋄ tandis que si $\sigma \notin \mathrm{H}$ alors $\sigma = \underbrace{\sigma(1\ 2)}_{\in \mathrm{H}} \underbrace{(1\ 2)}_{\in \mathrm{K}}$.

Ainsi $\mathrm{G} = \mathrm{HK}$. De plus $\mathrm{H} \cap \mathrm{K} = \{\mathrm{id}\}$. Cependant, $\mathfrak{S}_n \not\simeq \mathrm{H} \times \mathrm{K}$; en effet le centre de G est trivial tandis que le centre de $\mathrm{H} \times \mathrm{K}$ n'est pas trivial, le centre de K ne l'étant pas puisque ce groupe est cyclique donc abélien. Les centres n'étant pas isomorphes, le Théorème 2.2.6 permet de conclure que les groupes ne le sont pas plus.

Exemple 2.3.4. — Considérons le groupe $\mathrm{G} = \mathfrak{S}_4$. Soit H un 2-Sylow (nous renvoyons au Chapitre 10 pour une définition des p-Sylow) de G et K un 3-Sylow de G ; le groupe K est donc cyclique d'ordre 3.

D'après les théorèmes de Sylow $n_2 = 3$ et $n_3 = 4$; en particulier H et K ne sont pas distingués dans $\mathfrak{S}_4$. L'ensemble HK peut s'écrire à l'aide des classes à gauche Hk mais aussi à l'aide des classes à gauche hK. Il en résulte que $|\mathrm{HK}|$ est divisible par $|\mathrm{H}| = 8$ et par $|\mathrm{K}| = 3$; par suite $|\mathrm{HK}| \geq 24$. De plus $\mathrm{HK} \subset \mathfrak{S}_4$ et $|\mathfrak{S}_4| = 24$ d'où $|\mathrm{HK}| = 24$ et $\mathfrak{S}_4 = \mathrm{HK}$.

Les sous-groupes H et K s'intersectent trivialement.

Néanmoins $\mathfrak{S}_4 \not\simeq \mathrm{H} \times \mathrm{K}$. En effet le centre de $\mathrm{H} \times \mathbb{Z}/3\mathbb{Z}$ est non trivial ($\mathbb{Z}/3\mathbb{Z}$ a un centre non trivial) tandis que le centre de $\mathfrak{S}_4$ est trivial ; le Théorème 2.2.6 permet de conclure.

Alors que dans les Exemples 2.3.1, 2.3.2 et 2.3.3 le sous-groupe H est distingué dans G, dans l'Exemple 2.3.4 ni H, ni K ne sont distingués dans G. En raison de cette différence, le produit semi-direct que nous définissons au §3.6 inclut les Exemples 2.3.1, 2.3.2, 2.3.3 comme cas particuliers mais n'inclut pas l'Exemple 2.3.4.

2.4. Application

Donnons une application des §2.2 et §2.3.

CHAPITRE 3

3.1. Conjugaison dans un groupe

3.1.1. Classes de conjugaison : définition et exemples. —

Soient $\mathcal{D}$ et $\mathcal{D}'$ deux droites du plan euclidien ; la réflexion par rapport à $\mathcal{D}$ ne coïncide pas avec la réflexion par rapport à $\mathcal{D}'$ mais a « le même type d'effet ». De même, deux transpositions distinctes de $\mathfrak{S}_n$ ne sont pas égales mais se ressemblent au sens où elles échangent deux éléments et laissent les autres inchangés. Le concept qui donne naissance à la notion de « différent mais de même type d'effet » précise est appelé conjugaison.

Définition 3.1.1

Soit G un groupe. Deux éléments g et h de G sont *conjugués* lorsque $h = xgx^{-1}$ pour un certain $x \in \mathrm{G}$.
Cette relation est symétrique, puisque $g = yhy^{-1}$ avec $y = x^{-1}$.
Lorsque $h = xgx^{-1}$ ou $h = x^{-1}gx$, on dit que x *conjugue* g à h.

Dans §3.1.4, nous démontrons que les réflexions par rapport à une droite du plan sont conjuguées dans le groupe de toutes les isométries du plan.

Exemple 3.1.1. — Le tableau ci-dessous répertorie tous les conjugués de (1 2) dans $\mathfrak{S}_3$:

σ	(id)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
$\sigma(1\ 2)\sigma^{-1}$	(1 2)	(1 2)	(2 3)	(1 3)	(2 3)	(1 3)

Les conjugués de (1 2) sont donc : (1 2), (1 3) et (2 3). Ainsi toutes les transpositions dans $\mathfrak{S}_3$ sont conjuguées. Nous verrons que toutes les transpositions de $\mathfrak{S}_n$ sont conjuguées les uns aux autres (Théorème 5.1.4).

Il est utile de rassembler les éléments conjugués dans un groupe, ils forment un ensemble appelé classe de conjugaison ; nous donnerons des exemples de classe de conjugaison au §3.1.1. Nous démontrerons quelques résultats sur les éléments conjugués au §3.1.2. Nous étudierons

les classes de conjugaison dans D_{2n} au §5.2.3 et les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathcal{A}_n$ au §5.1.4. Au §3.1.3 nous démontrerons certains théorèmes sur les p-groupes finis, comme la classification des groupes d'ordre p^2 et l'existence d'un sous-groupe distingué de chaque ordre divisant l'ordre d'un p-groupe.

Définition 3.1.2

Soit G un groupe. Soit g un élément de G. La *classe de conjugaison* de g est l'ensemble des éléments qui lui sont conjugués :

$$\{hgh^{-1} \mid h \in \mathrm{G}\}.$$

Exemple 3.1.2. — Si G est abélien, alors $hgh^{-1} = g$ pour tous h, $g \in \mathrm{G}$: chaque g est sa propre classe de conjugaison. Cela caractérise les groupes abéliens : chaque $g \in \mathrm{G}$ est sa propre classe de conjugaison si et seulement si $hgh^{-1} = g$ pour tous h et g dans G si et seulement $hg = gh$ pour tous h et g, donc G est abélien.

Exemple 3.1.3. — Dans $\mathfrak{S}_3$,

- ◇ la classe de conjugaison de $(1\ 2)$ dans $\mathfrak{S}_3$ est $\{(1\ 2), (1\ 3), (2\ 3)\}$ (Exemple 3.1.1) ;
- ◇ la classe de conjugaison de $(1\ 2\ 3)$ est $\{(1\ 2\ 3), (1\ 3\ 2)\}$;
- ◇ la classe de conjugaison de id est simplement $\{\mathrm{id}\}$.

Ainsi $\mathfrak{S}_3$ a trois classes de conjugaison : $\{\mathrm{id}\}$, $\{(1\ 2), (1\ 3), (2\ 3)\}$, $\{(1\ 2\ 3), (1\ 3\ 2)\}$.

Exemple 3.1.4. — Dans $\mathrm{D}_8 = \langle r\, s \mid r^4 = e,\, s^2 = e,\, rsrs = e\rangle$, il existe cinq classes de conjugaison : $\{\mathrm{id}\}$, $\{r^2\}$, $\{s,\, r^2 s\}$, $\{r,\, r^3\}$, $\{rs,\, r^3 s\}$. Les membres d'une classe de conjugaison de D_8 sont différents mais ont le même type d'effet sur un carré :

- ◇ r et r^3 sont des rotations de $\pm\frac{\pi}{2}$,
- ◇ s et $r^2 s$ sont des réflexions par rapport à une diagonale,
- ◇ et rs et $r^3 s$ sont des réflexions.

Exemple 3.1.5. — Il existe cinq classes de conjugaison dans $\mathbb{H}_8$:

$$\{1\},\ \{-1\},\ \{i,\, -i\},\ \{j,\, -j\},\ \{k, -k\}.$$

Exemple 3.1.6. — On compte quatre classes de conjugaison dans $\mathcal{A}_4$:

$$\begin{array}{ll} \{\mathrm{id}\}, & \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}, \\ \{(1\ 2\ 3), (2\ 4\ 3), (1\ 3\ 4), (1\ 4\ 2)\}, & \{(1\ 3\ 2), (2\ 3\ 4), (1\ 4\ 3), (1\ 2\ 4)\}. \end{array}$$

Tous les 3-cycles de $\mathcal{A}_4$ sont conjugués dans $\mathfrak{S}_4$, par exemple $(1\ 3\ 2) = (2\ 3)(1\ 2\ 3)(2\ 3)^{-1}$ et la permutation de conjugaison $(2\ 3)$ n'est pas dans $\mathcal{A}_4$. Les 3-cycles $(1\ 2\ 3)$ et $(1\ 3\ 2)$ ne sont pas conjugués dans $\mathcal{A}_4$.

Dans ces exemples, les différentes classes de conjugaison d'un groupe sont disjointes : elles ne s'intersectent pas. Cela sera démontré en général dans §3.1.2. De plus, les cardinaux des différentes classes de conjugaison ne sont pas tous les mêmes, mais ces cardinaux divisent tous l'ordre du groupe (§3.1.3). La conjugaison peut s'appliquer non seulement aux éléments, mais aussi aux sous-groupes : si $\mathrm{H} \subset \mathrm{G}$ est un sous-groupe de G et $g \in \mathrm{G}$, l'ensemble $g\mathrm{H}g^{-1} = \{ghg^{-1} \mid h \in \mathrm{H}\}$ est un sous-groupe de G, appelé *sous-groupe conjugué* à H. C'est un sous-groupe ; en effet,

- ⋄ il contient l'identité ($e = geg^{-1}$),
- ⋄ il est stable par multiplication et passage à l'inverse : $(ghg^{-1})(gh'g^{-1}) = g(hh')g^{-1}$ et $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$.

Contrairement aux différentes classes de conjugaison, les différents sous-groupes conjugués ne sont pas disjoints : ils contiennent tous l'identité.

Exemple 3.1.7. — Alors que D_8 possède 5 classes de conjugaison d'éléments (Exemple 3.1.4), il possède 8 classes de conjugaison de sous-groupes. Le groupe D_8 compte 10 sous-groupes :

$$\begin{array}{lll} \langle \mathrm{id} \rangle = \{\mathrm{id}\}, & \langle s \rangle = \{\mathrm{id},\, s\}, & \langle rs \rangle = \{\mathrm{id},\, rs\}, \\ \langle r^2 s \rangle = \{\mathrm{id},\, r^2 s\}, & \langle r^3 s \rangle = \{\mathrm{id},\, r^3 s\}, & \langle r \rangle = \{\mathrm{id},\, r,\, r^2,\, r^3\}, \\ \langle r^2 \rangle = \{\mathrm{id},\, r^2\}, & \langle r^2, s \rangle = \{\mathrm{id},\, r^2,\, s,\, r^2 s\}, & \langle r^2,\, rs \rangle = \{\mathrm{id},\, r^2,\, rs,\, r^3 s\}, \qquad \mathrm{D}_8. \end{array}$$

Les sous-groupes $\langle s \rangle$ et $\langle r^2 s \rangle$ de cette liste sont conjugués, tout comme $\langle rs \rangle$ et $\langle r^3 s \rangle$; en effet, $r\langle s \rangle r^{-1} = \langle r^2 s \rangle$ et $r\langle rs \rangle r^{-1} = \langle r^3 s \rangle$. Les six autres sous-groupes de D_8 sont conjugués uniquement à eux-mêmes.

Nous abordons peu les sous-groupes conjugués dans ce paragraphe néanmoins le concept est important. Par exemple, un sous-groupe est conjugué uniquement à lui-même précisément lorsqu'il est distingué.

3.1.2. Quelques propriétés des classes de conjugaison. —

Lemme 3.1.1

Soit G un groupe. Soient h, g deux éléments de G. Nous avons : $(hgh^{-1})^n = hg^n h^{-1}$ pour tout $n \in \mathrm{Z}$.

Démonstration. — L'énoncé se montre par récurrence. L'équation est en fait vraie pour tout $n \in \mathbb{Z}$. □

Théorème 3.1.1

Les éléments d'une classe de conjugaison ont le même ordre.

Démonstration. — Soit G un groupe. Soient h, g deux éléments de G. D'après le Lemme 3.1.1, nous avons $(hgh^{-1})^n = hg^nh^{-1}$ pour tout $n \in \mathbb{N}$. Par suite si $g^n = e$, alors $(hgh^{-1})^n = hg^nh^{-1} = hh^{-1} = e$, et si $(hgh^{-1})^n = e$ alors $hg^nh^{-1} = e$ et $g^n = h^{-1}x = e$. Ainsi $(hgh^{-1})^n = e$ si et seulement si $g^n = e$, donc g et hgh^{-1} ont le même ordre. □

La réciproque du Théorème 3.1.1 est fausse : deux éléments de même ordre dans un groupe ne sont pas nécessairement conjugués dans ce groupe. En effet, dans un groupe abélien deux éléments distincts ne sont jamais conjugués mais peuvent être de même ordre. En regardant les exemples non abéliens de §3.1.1, on remarque qu'il y a dans D_8 cinq éléments d'ordre 2 répartis dans trois classes de conjugaison. De même, il existe des éléments non conjugués de même ordre dans $\mathbb{H}_8$ et $\mathcal{A}_4$. Mais dans $\mathfrak{S}_3$, deux éléments de même ordre sont conjugués. C'est le plus « grand » exemple de groupe fini ayant cette propriété : à isomorphisme près les seuls groupes finis non triviaux où tous les éléments de même ordre sont conjugués sont $\mathbb{Z}/2\mathbb{Z}$ et $\mathfrak{S}_3$.

Vérifions l'observation du §3.1.1 selon laquelle les différentes classes de conjugaison sont disjointes.

Théorème 3.1.2

Soit G un groupe. Soient g et h deux éléments de G. Si les classes de conjugaison de g et h s'intersectent, alors les classes de conjugaison de g et h sont égales.

Démonstration. — Nous devons montrer que tout élément conjugué à g est également conjugué à h, et réciproquement.

Puisque les classes de conjugaison s'intersectent, il existe x et y dans G tels que $xgx^{-1} = yhy^{-1}$. Par suite $g = x^{-1}yhy^{-1}x = (x^{-1}y)h(x^{-1}y)^{-1}$, autrement dit g est conjugué à h. Un élément conjugué à g s'écrit zgz^{-1} pour un certain $z \in \mathrm{G}$; on remarque que

$$zgz^{-1} = z(x^{-1}y)h(x^{-1}y)^{-1}z^{-1} = (zx^{-1}y)h(zx^{-1}y)^{-1}.$$

Ainsi chaque élément de G conjugué à g est également conjugué à h.

L'implication réciproque se montre de la même façon à partir de $xgx^{-1} = yhy^{-1}$ et $h = (y^{-1}x)g(y^{-1}x)^{-1}$. □

Le Théorème 3.1.2 assure que chaque élément d'un groupe appartient à une seule classe de conjugaison. Un élément d'une classe de conjugaison est un *représentant* de cette classe.

Une classe de conjugaison comprend tous les hgh^{-1} pour g fixé et h qui varie. Nous pouvons aussi examiner tous les hgh^{-1} pour h fixé et g qui varie. Autrement dit, au lieu de regarder tous les éléments conjugués à g, nous examinons toutes les façons dont h peut conjuguer les éléments du groupe. Cette fonction « conjugaison par h » est notée γ_h, *i.e.* $\gamma_h \colon \mathrm{G} \to \mathrm{G}$, $g \mapsto hgh^{-1}$.

Théorème 3.1.3

Chaque fonction de conjugaison $\gamma_h \colon \mathrm{G} \to \mathrm{G}$ est un automorphisme de G.

Démonstration. — Pour tous g et h dans G, nous avons

$$\gamma_x(g)\gamma_x(h) = xgx^{-1}xhx^{-1} = xghx^{-1} = \gamma_x(gh);$$

par suite γ_x est un morphisme de G dans lui-même. Puisque $h = xgx^{-1}$ si et seulement si $g = x^{-1}hx$, la fonction γ_x a pour inverse $\gamma_{x^{-1}}$, donc γ_x est un automorphisme de G. □

Le Théorème 3.1.3 explique en quoi deux éléments conjugués d'un groupe G sont « proches » : ils sont liés par un automorphisme de G, plus précisément par un γ_x. Cela signifie qu'un élément de G et ses conjugués dans G partagent les mêmes propriétés algébriques : avoir le même ordre, être une puissance n-ième, appartenir au centre, être un commutateur... De même, un sous-groupe H et ses conjugués $g\mathrm{H}g^{-1}$ ont les mêmes propriétés algébriques.

Les automorphismes de G de la forme γ_x sont appelés *automorphismes intérieurs*. Il existe des groupes G ayant la propriété suivante : tout automorphisme de G est un automorphisme intérieur ; c'est par exemple le cas pour les groupes $\mathfrak{S}_n$ lorsque $n \neq 6$. Il existe des automorphismes de $\mathrm{GL}(n, \mathbb{R})$ qui ne sont pas intérieurs lorsque $n \geq 2$: puisque ${}^{\mathrm{t}}(AB) = {}^{\mathrm{t}}B{}^{\mathrm{t}}A$ et $(AB)^{-1} = B^{-1}A^{-1}$, l'involution $\iota(A) = {}^{\mathrm{t}}A^{-1}$ sur $\mathrm{GL}(n, \mathbb{R})$ est un automorphisme qui n'est pas intérieur ; cette involution est appelée *contragrédiente*.

Voici un résultat où les automorphismes intérieurs nous renseignent sur tous les automorphismes d'un groupe.

Théorème 3.1.4

Soit G un groupe. Si le centre de G est trivial, alors le centre de Aut(G) est trivial.

Démonstration. — Soit ϕ un élément de $Z(\mathrm{Aut(G)})$. Écrivons que ϕ commute avec γ_x, avec x dans G : soit $g \in \mathrm{G}$,

- ◇ d'une part $(\phi \circ \gamma_x)(g) = \phi(\gamma_x(g)) = \phi(xgx^{-1}) = \phi(x)\phi(g)\phi(x)^{-1}$,
- ◇ et d'autre part $(\gamma_x \circ \phi)(g) = \gamma_x(\phi(g)) = x\phi(g)x^{-1}$.

Ainsi $\phi\gamma_x = \gamma_x\phi$ si et seulement si $\phi(x)\phi(g)\phi(x)^{-1} = x\phi(g)x^{-1}$ pour tout $g \in \mathrm{G}$ si et seulement si $x^{-1}\phi(x)\phi(g) = \phi(g)x^{-1}\phi(x)$. Comme ϕ est surjective, $x^{-1}\phi(x)$ appartient à $Z(\mathrm{G})$; or par hypothèse $Z(\mathrm{G}) = \{\mathrm{id}\}$ donc $\phi(x) = x$. Ceci étant valable pour tout $x \in \mathrm{G}$, nous obtenons que $\phi = \mathrm{id}$: le centre de Aut(G) est trivial. □

3.1.3. Centralisateurs et équation aux classes. — Le Théorème 3.1.2 assure que deux classes de conjugaison distinctes ne s'intersectent pas. Elles fournissent donc un moyen de recouvrir le groupe par des ensembles disjoints. Ceci est analogue aux classes à gauche d'un sous-groupe qui forment une partition du groupe. Pour $g \in \mathrm{G}$, notons C_g sa classe de conjugaison dans G :

$$C_g = \{xgx^{-1} \mid x \in \mathrm{G}\}.$$

Si les différentes classes de conjugaison sont C_{g_1}, C_{g_2}, …, C_{g_r}, alors

$$|\mathrm{G}| = \#C_{g_1} + \#C_{g_2} + \ldots + \#C_{g_r}. \tag{3.1.1}$$

L'équation (3.1.1) joue un rôle analogue à la formule $|\mathrm{G}| = |\mathrm{H}|\,[\mathrm{G} : \mathrm{H}]$.

Voyons ce que dit (3.1.1) pour certains groupes du §3.1.2.

Exemple 3.1.8. — Lorsque $\mathrm{G} = \mathfrak{S}_3$, (3.1.1) se réécrit $6 = 1 + 2 + 3$.

Exemple 3.1.9. — Lorsque $\mathrm{G} = \mathrm{D}_8$, (3.1.1) se réécrit $8 = 1 + 1 + 2 + 2 + 2$.

Exemple 3.1.10. — Lorsque $\mathrm{G} = \mathbb{H}_8$, (3.1.1) se réécrit $8 = 1 + 1 + 2 + 2 + 2$.

Exemple 3.1.11. — Lorsque $\mathrm{G} = \mathcal{A}_4$, (3.1.1) se réécrit $12 = 1 + 3 + 4 + 4$.

La raison pour laquelle (3.1.1) est importante est que $\#C_{g_i}$ divise l'ordre du groupe. Nous l'avons vu précédemment dans des exemples. Nous allons maintenant le prouver de manière générale.

Théorème 3.1.5

Soit G un groupe fini. Le cardinal de chaque classe de conjugaison dans G divise $|\mathrm{G}|$.

Le Théorème 3.1.5 n'est pas une conséquence immédiate du Théorème de Lagrange, car les classes de conjugaison ne sont pas des sous-groupes. Par exemple, aucune classe de conjugaison ne contient l'élément neutre, à l'exception de la classe de conjugaison de l'élément neutre qui est réduite à l'élément neutre. Néanmoins, même si une classe de conjugaison n'est pas un sous-groupe, son cardinal est égal à l'indice d'un sous-groupe, ce qui expliquera pourquoi son cardinal divise l'ordre du groupe.

Théorème 3.1.6

Soit G un groupe fini. Soit g un élément de G. Le cardinal de la classe de conjugaison de g coïncide avec l'indice du centralisateur de g, c'est-à-dire $\#\{xgx^{-1} \mid x \in \mathrm{G}\} = [\mathrm{G} : Z_g]$.

Démonstration. — Considérons la fonction $f\colon \mathrm{G} \to C_g$, $x \mapsto xgx^{-1}$. Cette fonction est surjective : par définition tout élément de C_g s'écrit xgx^{-1} pour un certain $x \in \mathrm{G}$.

Soient x et x' dans G ; nous avons $f(x) = f(x')$ si et seulement si $xgx^{-1} = x'g(x')^{-1}$ si et seulement si $gx^{-1}x' = x^{-1}x'g$ si et seulement si $x^{-1}x'$ commute avec g si et seulement si $x^{-1}x'$ appartient à Z_g et x' appartient à xZ_g. Ainsi :

$$f(x) = f(x') \Rightarrow xZ_g = x'Z_g. \tag{3.1.2}$$

Réciproquement supposons que $xZ_g = x'Z_g$. Alors $x = x'z$ pour un certain $z \in Z_g$ (*i.e.* $zg = gz$). Ainsi

$$f(x) = xgx^{-1} = (x'z)g(x'z)^{-1} = x'zgz^{-1}(x')^{-1} = x'gzz^{-1}(x')^{-1} = x'g(x')^{-1} = f(x').$$

Finalement la fonction $f\colon \mathrm{G} \to C_g$ prend la même valeur en deux éléments précisément lorsqu'ils sont dans la même classe à gauche modulo Z_g dans G. Par conséquent, le nombre de

valeurs différentes prises par f est le nombre de classes à gauche modulo Z_g dans G, c'est-à-dire $[\mathrm{G} : Z_g]$.

Puisque f est surjectif, nous obtenons, par application du Corollaire 1.1.1, que $\#C_g = [\mathrm{G} : Z_g]$. □

Démonstration du Théorème 3.1.5. — D'après le Théorème 3.1.6, le cardinal de la classe de conjugaison de g coïncide avec l'indice $[\mathrm{G} : Z_g]$ qui divise $|\mathrm{G}|$. □

On peut réécrire (3.1.1) sous la forme

$$|\mathrm{G}| = \sum_{i=1}^{r} [\mathrm{G} : Z_{g_i}] = \sum_{i=1}^{r} \frac{|\mathrm{G}|}{|Z_{g_i}|}. \tag{3.1.3}$$

Les classes de conjugaison de cardinal 1 sont exactement celles contenant des éléments du centre de G (c'est-à-dire celles g_i telles que $Z_{g_i} = \mathrm{G}$). En combinant tous ces 1 en un seul terme, nous obtenons

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i'} \frac{|\mathrm{G}|}{|Z_{g_{i'}}|}, \tag{3.1.4}$$

où la somme porte désormais uniquement sur les classes de conjugaison $C_{g_{i'}}$ contenant strictement plus d'un élément. Aux termes de cette somme, $|Z_{g_{i'}}| < |\mathrm{G}|$. L'équation (3.1.3) est appelée *l'équation aux classes*. La différence entre l'équation de classe et (3.1.1) est que nous avons combiné les termes contribuant au centre de G en un seul terme.

Voici une application de l'équation aux classes.

Définition 3.1.3

Un groupe G est un *p-groupe* si tout élément de G a pour ordre une puissance de p.

Théorème 3.1.7

Le centre d'un p-groupe fini non trivial est non trivial.

Démonstration. — Soit G un p-groupe. Écrivons $|\mathrm{G}|$ sous la forme p^n avec $n > 0$. Considérons un terme $[\mathrm{G} : Z_{g_{i'}}]$ dans l'équation aux classes avec $g_{i'} \notin Z(\mathrm{G})$. Alors $Z_{g_{i'}} \neq \mathrm{G}$, ainsi l'indice $[\mathrm{G} : Z_{g_{i'}}]$ est un facteur de $|\mathrm{G}|$ distinct de 1. C'est donc l'un des $\{p, p^2, \ldots, p^n\}$; autrement dit $[\mathrm{G} : Z_{g_{i'}}]$ est divisible par p. Dans (3.1.4) tous les termes de la somme sur i' sont des multiples de p. De plus, le membre de gauche de (3.1.4) est un multiple de p, puisque $|\mathrm{G}| = p^n$. Par conséquent p divise $|Z(\mathrm{G})|$. Puisque $Z(\mathrm{G})$ contient e, $|Z(\mathrm{G})| \geq 1$; de plus $|Z(\mathrm{G})|$ est divisible par p ; il s'en suit que $|Z(\mathrm{G})| \geq p$. En particulier $Z(\mathrm{G})$ n'est pas réduit à $\{e\}$. □

Corollaire 3.1.1

Pour tout nombre premier p, tout groupe d'ordre p^2 est abélien. Plus précisément, un groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Démonstration. — Soit G un groupe d'ordre p^2, p premier. L'ordre d'un élément de $\mathrm{G} \smallsetminus \{e\}$ est p ou p^2 (Théorème de Lagrange).

S'il existe un élément de G d'ordre p^2, alors G est cyclique et donc isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$.

Supposons désormais que G n'a aucun élément d'ordre p^2, *i.e.* que chaque élément de $\mathrm{G} \smallsetminus \{e\}$ est d'ordre p. Le Théorème 3.1.7 assure l'existence d'un élément a appartenant à $Z(\mathrm{G}) \smallsetminus \{e\}$. Puisque a est d'ordre p, $\langle a \rangle$ est un sous-groupe propre de G. Soit b un élément de $\mathrm{G} \smallsetminus \langle a \rangle$; par hypothèse b est aussi d'ordre p. On a $\langle a \rangle \cap \langle b \rangle = \{\mathrm{e}\}$. Pour tout $(i, j) \in [\![1, p]\!]^2$ on a $a^i b^j = b^j a^i$, car $a \in Z(\mathrm{G})$. C'est-à-dire que les éléments de $\langle a \rangle$ et de $\langle b \rangle$ commutent. Enfin, $\#(\langle a \rangle \langle b \rangle) = p^2$ et donc $\langle a \rangle \langle b \rangle = \mathrm{G}$. D'après le Théorème 2.3.1 le groupe G est isomorphe à $\langle a \rangle \times \langle b \rangle$ et donc à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. □

3.1.4. Conjugaison en géométrie plane. — Nous allons montrer que les réflexions dans $\mathbb{R}^2$ sont conjuguées à la réflexion par rapport à l'axe des x dans un groupe approprié de transformations du plan.

Définition 3.1.4

Une *isométrie de* $\mathbb{R}^2$ est une fonction $f : \mathbb{R}^2 \to \mathbb{R}^2$ qui préserve les distances : pour tous les points P et Q de $\mathbb{R}^2$, la distance entre $f(P)$ et $f(Q)$ est la même que la distance entre P et Q.

Les les translations, les rotations et les réflexions sont des isométries de $\mathbb{R}^2$. Ces trois types d'isométries sont inversibles (l'inverse de la translation par le vecteur v est la translation par le vecteur $-v$, l'inverse de la rotation d'angle ϑ est la rotation d'angle $-\vartheta$, une réflexion est sa propre inverse). Les isométries sont inversibles (cela nécessite une preuve), et la composition de deux isométries de $\mathbb{R}^2$ est une isométrie de $\mathbb{R}^2$. Les isométries de $\mathbb{R}^2$ forment donc un groupe.

Il existe deux manières de décrire algébriquement des points du plan, en utilisant des vecteurs ou des nombres complexes. Nous allons utiliser ce second point de vue. Le point (a, b) est considéré comme le nombre complexe $a + b\mathbf{i}$. On mesure la distance de 0 à $a + b\mathbf{i}$ grâce au module : $|a + b\mathbf{i}| = \sqrt{a^2 + b^2}$; de plus, la distance entre $a + b\mathbf{i}$ et $c + d\mathbf{i}$ est : $|(a + b\mathbf{i}) - (c + d\mathbf{i})| = \sqrt{(a - c)^2 + (b - d)^2}$. À chaque nombre complexe $z = a + b\mathbf{i}$, on peut associer son conjugué $\overline{z} = a - b\mathbf{i}$. Un calcul explicite conduit à :

$$\overline{z + z'} = \overline{z} + \overline{z'}, \qquad \overline{zz'} = \overline{z}\,\overline{z'}.$$

Deux propriétés algébriques importantes du module sont les suivantes :

$$|zz'| = |z||z'|, \qquad\qquad |\overline{z}| = |z|.$$

En particulier, si $|w| = 1$ alors $|wz| = |z|$.

Un exemple de réflexion par rapport à une droite dans le plan est la conjugaison complexe : $s(z) = \overline{z}$. Cette réflexion préserve les distances :

$$s(z) - s(z') = |\overline{z} - \overline{z'}| = |\overline{z - z'}| = |z - z'|.$$

Nous allons comparer cette réflexion avec la réflexion par rapport à une autre droite : dans un premier temps cette autre droite sera une droite passant par l'origine, puis elle sera quelconque.

Choisissons une droite passant par l'origine qui fait un angle ϑ par rapport à $\Delta = \{(x, 0) \mid x > 0\}$. Une rotation centrée en l'origine, en termes de nombres complexes, est une multiplication par le nombre $\cos\vartheta + \mathbf{i}\sin\vartheta$, qui est de module 1. Notons r_ϑ la rotation dans le sens antihoraire autour de l'origine par ϑ

$$r_\vartheta(z) = (\cos\vartheta + \mathbf{i}\sin\vartheta)z, \qquad\qquad |\cos\vartheta + \mathbf{i}\sin\vartheta| = 1.$$

Chaque rotation r_ϑ préserve les distances :

$$|r_\vartheta(z) - r_\vartheta(z')| = |(\cos\vartheta + \mathbf{i}\sin\vartheta)(z - z')| = |\cos\vartheta + \mathbf{i}\sin\vartheta|\,|z - z'| = |z - z'|.$$

Composer des rotations centrées en l'origine revient à additionner des angles : $r_\vartheta \circ r_\varphi = r_{\vartheta+\varphi}$. En particulier, $r_\vartheta^{-1} = r_{-\vartheta}$ puisque $r_\vartheta \circ r_{-\vartheta} = r_0$, qui est l'identité : $r_0(z) = z$.

Soit s_ϑ la réflexion par rapport à l'axe des abscisses ; en particulier, la conjugaison complexe est s_0. La réflexion s_ϑ est le composition de

- ⋄ rotation centrée en l'origine d'angle $-\vartheta$ pour ramener la droite de réflexion sur l'axe des x,
- ⋄ réflexion par rapport à l'axe des x,
- ⋄ rotation centrée en l'origine d'angle ϑ pour ramener la droite à sa position d'origine.

Autrement dit

$$s_\vartheta = r_\vartheta s r_{-\vartheta} = r_\vartheta s r_\vartheta^{-1}. \tag{3.1.5}$$

Ainsi une réflexion par rapport à une droite passant par l'origine est conjuguée, dans le groupe des isométries du plan, à une réflexion par rapport à l'axe des x.

La translation dans le plan par le vecteur w peut être vue comme une addition : $t_w(z) = z + w$ pour tout z dans $\mathbb{C}$; c'est une isométrie puisque

$$|t_w(z) - t_w(z')| = |(z + w) - (z' + w)| = |z - z'|.$$

Remarquons que $t_w \circ t_{w'} = t_{w+w'}$, et l'inverse de t_w est t_{-w} : $t_w^{-1} = t_{-w}$.

Se donner une droite $\mathcal{D}$ du plan revient à se donner un point w de $\mathcal{D}$ et l'angle ϑ entre $\mathcal{D}$ et Δ ; on la notera $\mathcal{D}_{w,\vartheta}$. Nous pouvons décrire la réflexion par rapport à $\mathcal{D}_{w,\vartheta}$ à l'aide de translations de vecteurs w et $-w$ et de la réflexion par rapport à $\mathcal{D}_{0,\vartheta}$:

- ⋄ faire une translation par $-w$ pour envoyer $\mathcal{D}_{w,\vartheta}$ sur $\mathcal{D}_{0,\vartheta}$ (c'est-à-dire appliquer t_{-w}) ;

◇ faire une réflexion d'axe $\mathcal{D}_{0,\vartheta}$ (c'est-à-dire appliquer s_ϑ),

◇ faire une translation par w pour ramener $\mathcal{D}_{0,\vartheta}$ sur $\mathcal{D}_{w,\vartheta}$ (appliquer t_w).

En combinant ces trois étapes avec (3.1.5), nous obtenons que la réflexion d'axe $\mathcal{D}_{w,\vartheta}$ s'écrit aussi

$$t_w s_\vartheta t_{-w} = t_w(r_\vartheta s r_\vartheta^{-1})t_x^{-1} = t_w r_\vartheta s(t_w r_\vartheta)^{-1}.$$

Il s'agit d'un conjugué de conjugaisons complexes dans le groupe des isométries du plan.

Théorème 3.1.8

La réflexion par rapport à une droite est conjuguée dans le groupe des isométries du plan à la réflexion par rapport à l'axe des abscisses.

Exemple 3.1.12. — La réflexion par rapport à la droite $y = b$ correspond à $\vartheta = 0$ et $w = b\mathbf{i}$. Autrement dit, cette réflexion est $t_{b\mathbf{i}} s t_{-b\mathbf{i}}$: on commence par translater par $-b$, on fait la réflexion par rapport à l'axe des x puis on translate par b.

3.1.5. Borner l'ordre d'un groupe par le nombre de classes de conjugaison. — Il est clair qu'il existe, à isomorphisme près, un nombre fini de groupes d'ordre donné. Ce qui pourrait être plus surprenant est qu'il existe, à isomorphisme près, un nombre fini de groupes finis avec un nombre donné de classes de conjugaison. L'énoncé suivant est une application de l'équation aux classes ([**Lan03**]) :

Théorème 3.1.9

Si G est un groupe fini dont on connaît le nombre de classes de conjugaison, alors on peut borner $|\mathrm{G}|$.

Démonstration. — Lorsqu'il n'y a qu'une seule classe de conjugaison, le groupe est trivial. Fixons maintenant un entier positif $k > 1$. Soit G un groupe fini ayant k classes de conjugaison représentées par g_1, g_2, …, g_k. L'équation aux classes s'écrit

$$|\mathrm{G}| = \sum_{i=1}^{k} \frac{|\mathrm{G}|}{|Z_{g_i}|}. \tag{3.1.6}$$

ou encore quitte à diviser par $|\mathrm{G}|$:

$$1 = \frac{1}{n_1} + \frac{1}{n_2} + \ldots + \frac{1}{n_k} \tag{3.1.7}$$

où $n_i = |Z_{g_i}|$. Notons que si G n'est pas trivial, nous avons $n_i > 1$ pour tout $1 \leq i \leq k$. Quitte à réindicer les n_i nous pouvons supposer que $n_1 \leq n_2 \leq \ldots \leq n_k$ (il peut y avoir des répétitions).

Puisque $n_i \geq 1$ pour tout $1 \leq i \leq k$ l'équation (3.1.7) implique l'inégalité $1 \leq \frac{k}{n_1}$ soit

$$n_1 \leq k. \tag{3.1.8}$$

Comme $n_i \geq n_2$ pour tout $i \geq 2$ nous obtenons

$$1 \leq \frac{1}{n_1} + \frac{k-1}{n_2}.$$

Il en résulte que $1 - \frac{1}{n_1} \leq \frac{k-1}{n_2}$ et donc que

$$n_2 \leq \frac{k-1}{1 - \frac{1}{n_1}}$$

Par récurrence il vient pour tout $m \geq 2$ l'inégalité

$$n_m \leq \frac{k+1-m}{1 - \left(\frac{1}{n_1} + \frac{1}{n_2} + \ldots + \frac{1}{n_{m-1}}\right)}. \tag{3.1.9}$$

Puisque les n_i sont bornés supérieurement (*voir* (3.1.8) et (3.1.9)), il n'y a qu'un nombre fini de k-uplets $(n_1, n_2, \ldots, n_k)$. On peut donc lister les k-uplets qui satisfont (3.1.7). La plus grande valeur de n_k est $|\mathrm{G}|$ (le centralisateur de e est G). □

L'élément neutre est sa propre classe de conjugaison, donc le seul groupe fini avec une seule classe de conjugaison est le groupe trivial. Burnside et Miller ont indépendamment déterminé, à isomorphisme près, les groupes finis possédant 2, resp. 3, resp. 4, resp. 5 classes de conjugaison ([**Bur11, Mil10**]). Poland a déterminé, à isomorphisme près, les groupes ayant 6, resp. 7 classes de conjugaison ([**Pol68**]). Cette classication est poursuivie dans [**VLS07**].

Un groupe d'ordre n a au plus n classes de conjugaison, et il y a n classes de conjugaison si et seulement si le groupe est abélien. En particulier, une liste de groupes finis avec k classes de conjugaison contient tous les groupes abéliens d'ordre k.

Pour tout entier $k \geq 3$ il existe un groupe non abélien possédant k classes de conjugaison. En effet lorsque $n = 2m+1$ est impair et supérieur ou égal à 3, le groupe diédral D_{2n} a $m+2$ classes de conjugaison (Proposition 5.2.1). Lorsque $k = m+3$, nous avons $2m+1 = 2k-5$; ainsi pour tout entier $k \geq 3$ le groupe $\mathrm{D}_{2(2k-3)}$ contient k classes de conjugaison.

Exemple 3.1.13. — Un groupe fini avec exactement deux classes de conjugaison est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Exemple 3.1.14. — Les groupes finis possédant exactement trois classes de conjugaison sont $\mathfrak{S}_3 \simeq \mathrm{D}_6$ (qui est d'ordre 6) et $\mathbb{Z}/3\mathbb{Z}$ (qui est d'ordre 3).

Exemple 3.1.15. — Les groupes finis possédant quatre classes de conjugaison sont $\mathbb{Z}/4\mathbb{Z}$, $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$, D_{10} et $\mathcal{A}_4$. Le plus grand groupe fini de ce type est d'ordre 12.

Exemple 3.1.16. — Les groupes finis possédant cinq classes de conjugaison sont $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{H}_8$, D_8, D_{14}, $\mathrm{Aff}\left(\mathbb{Z}/5\mathbb{Z}\right)$, $\mathfrak{S}_4$, $\mathcal{A}_5$ et le groupe non abélien d'ordre 21 [1]. Le plus grand groupe fini de ce type est le groupe $\mathcal{A}_5$ (qui est d'ordre 60).

1. Le plus petit groupe non abélien d'ordre impair est le groupe de Frobenius F_{21}, d'ordre 21.

Exemple 3.1.17. — Les groupes finis possédant six classes de conjugaison sont $\mathbb{Z}/6\mathbb{Z}$, D_{12}, D_{18}, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathfrak{S}_3$, $\mathrm{Aff}(\mathbb{F}_9)$, $\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, a,\, b \in \mathbb{F}_9,\, a^4 = 1 \right\}$ et $\mathrm{PSL}\left(2, \mathbb{Z}/7\mathbb{Z}\right)$. Le groupe fini de ce type est le groupe $\mathrm{PSL}\left(2, \mathbb{Z}/7\mathbb{Z}\right)$ (qui est d'ordre 168).

Exemple 3.1.18. — Les groupes finis possédant sept classes de conjugaison sont

$$\mathbb{Z}/7\mathbb{Z}, \qquad \mathrm{D}_{16}, \qquad \mathrm{D}_{22}, \qquad \mathfrak{S}_5, \qquad \mathcal{A}_6, \qquad \mathrm{Aff}\left(\mathbb{Z}/7\mathbb{Z}\right), \qquad \mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right),$$

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, a,\, b \in \mathbb{Z}/13\mathbb{Z},\, a^3 = 1 \right\}, \qquad \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, a,\, b \in \mathbb{Z}/13\mathbb{Z},\, a^4 = 1 \right\},$$

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, a,\, b \in \mathbb{Z}/11\mathbb{Z},\, a^5 = 1 \right\},$$

le sous-groupe d'ordre 16 dans $\mathrm{GL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ et le groupe des quaternions généralisé d'ordre 16

$$\langle g,\, h \,|\, g^8 = e,\, g^4 = h^2,\, hgh^{-1} = g^{-1} \rangle.$$

Le plus grand groupe de ce type est $\mathcal{A}_6$ (d'ordre 360).

3.2. Sous-groupes distingués

Nous allons essayer de généraliser la construction de $\mathbb{Z}/n\mathbb{Z}$ à partir du groupe $\mathbb{Z}$ et de son sous-groupe $n\mathbb{Z}$ au cas d'un groupe quelconque G. Nous allons voir que dans le cas général les analogues à $n\mathbb{Z}$ ne sont pas des sous-groupes quelconques mais sont des sous-groupes distingués de G. Un groupe modulo un sous-groupe distingué est un groupe de quotient ; nous examinerons quelques exemples et propriétés de groupes de quotient.

Les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont des classes d'équivalence et une classe d'équivalence est une « double progression arithmétique » :

$$a + n\mathbb{Z} = \{\ldots,\, a - 2n,\, a - n,\, a,\, a + n,\, a + 2n,\, \ldots\}.$$

On ajoute deux éléments de $\mathbb{Z}/n\mathbb{Z}$ comme suit

$$\overline{a} + \overline{b} = \overline{a + b},$$

Le point important dans cette formule est que l'addition est indépendante du choix des représentants utilisés parmi les deux classes d'équivalence : si $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$ alors $\overline{a} + \overline{b} = \overline{a'} + \overline{b'}$. Autrement dit si $a \equiv_n a'$ et $b \equiv_n b'$ alors $a + b \equiv_n a' + b'$. Puisque $a + n\mathbb{Z}$ est une classe à gauche de $n\mathbb{Z}$ dans $\mathbb{Z}$, on souhaite étendre la notion d'addition d'entiers modulo n à une multiplication de classes à gauche (ou à droite) d'un sous-groupe d'un groupe : si G est un groupe et H est un sous-groupe de G, pouvons-nous définir le produit de deux classes à gauche de H comme étant une classe à gauche de H via la formule $g_1\mathrm{H} \cdot g_2\mathrm{H} = g_1 g_2 \mathrm{H}$? Malheureusement cela n'a

parfois aucun sens : ce produit peut dépendre du choix des représentants des classes à gauche comme nous allons le voir dans l'exemple suivant.

Exemple 3.2.1. — Considérons le groupe $\mathrm{G} = \mathrm{D}_6$ et le sous-groupe H de G défini par $\mathrm{H} = \langle s \rangle = \{\mathrm{id},\, s\}$. Alors

$$r\mathrm{H} = \{r,\, rs\} = rs\mathrm{H}, \qquad\qquad r^2\mathrm{H} = \{r^2,\, r^2 s\} = r^2 s\mathrm{H}.$$

Cependant $r \cdot r^2\mathrm{H} = \mathrm{H}$ tandis que $rs \cdot r^2 s\mathrm{H} = rr^{-2}ss\mathrm{H} = r^{-1}\mathrm{H} \neq \mathrm{H}$. Ainsi, même si r et rs sont dans la même classe à gauche et si r^2 et $r^2 s$ sont dans la même classe à gauche, $r \cdot r^2$ et $rs \cdot r^2 s$ ne sont pas dans la même classe à gauche.

Un problème similaire se produit si on considère les classes à droite : $\mathrm{H}r = \mathrm{H}r^2 s$ et $\mathrm{H}r^2 = \mathrm{H}rs$, mais $\mathrm{H}r \cdot r^2 = \mathrm{H}$ tandis que $\mathrm{H}r^2 s \cdot rs = \mathrm{H}r \neq \mathrm{H}$.

Il s'avère que

$$g_1\mathrm{H} \cdot g_2\mathrm{H} = g_1 g_2\mathrm{H} \tag{3.2.1}$$

a un sens en tant qu'opération sur les classes à gauche de H si H satisfait la propriété suivante : $g\mathrm{H} = \mathrm{H}g$ pour tout $g \in \mathrm{G}$.

Définition 3.2.1

Un sous-groupe H d'un groupe G est *distingué* si $g\mathrm{H} = \mathrm{H}g$ pour tout $g \in \mathrm{G}$.
De manière équivalente, H est distingué si $g\mathrm{H}g^{-1} = \mathrm{H}$ pour tout $g \in \mathrm{G}$.
Une autre formulation possible est la suivante : H est *distingué* dans G s'il est invariant par automorphisme intérieur.

La condition $g\mathrm{H} = \mathrm{H}g$ ne signifie pas $gh = hg$ pour tout $h \in \mathrm{H}$, mais signifie que pour tout $h \in \mathrm{H}$ il existe $h' \in \mathrm{H}$ tel que $gh = h'g$.

Exemple 3.2.2. — Soit G un groupe. Alors G et $\{e\}$ sont des sous-groupes distingués de G.

Exemple 3.2.3. — Si G est un groupe abélien alors tout sous-groupe de G est un sous-groupe distingué de G ; en effet comme G est abélien $gh = hg$ pour tous $g \in \mathrm{G}$ et $h \in \mathrm{H}$ d'où $g\mathrm{H} = \mathrm{H}g$.

La réciproque est fausse puisque tous les sous-groupes du groupe des quaternions $\mathbb{H}_8$ sont distingués mais $\mathbb{H}_8$ n'est pas abélien.

Exemple 3.2.4. — Le centre $Z(\mathrm{G})$ d'un groupe G est un sous-groupe distingué puisque chaque élément de $Z(\mathrm{G})$ commute avec G : $gz = zg$ pour tous $g \in \mathrm{G}$ et $z \in Z(\mathrm{G})$, donc $gZ(\mathrm{G}) = Z(\mathrm{G})g$.

Un raisonnement analogue conduit à : tout sous-groupe du centre de G est un sous-groupe distingué de G.

Remarque 3.2.1. — Les sous-groupes abéliens d'un groupe G ne sont pas en général des sous-groupes distingués de G. Par exemple, $\langle s \rangle = \{\mathrm{id},\, s\}$ est un sous-groupe abélien (et même cyclique) de D_{2n} pour $n \geq 3$ mais il n'est pas distingué dans D_{2n}. En effet, $r\{\mathrm{id},\, s\} =$

$\{r,\, rs\}, \{\mathrm{id},\, s\}r = \{r,\, sr\}$ et $rs \neq sr$ (car $sr = r^{-1}s = r^{n-1}s \neq rs$ puisque r est d'ordre n et $n > 2$). Ainsi $r\{\mathrm{id},\, s\} \neq \{\mathrm{id},\, s\}r$.

Exemple 3.2.5. — Le groupe dérivé d'un groupe G est un sous-groupe distingué de G.

Exemple 3.2.6. — Montrons que le sous-groupe $\mathrm{H} = \langle r \rangle$ de D_{2n} est distingué dans D_{2n}. Cela revient à montrer que $g\mathrm{H} = \mathrm{H}g$ pour tout $g \in \mathrm{D}_{2n}$.

Si $g \in \mathrm{H}$ puisque alors $g\mathrm{H} = \mathrm{H}$ et $\mathrm{H}g = \mathrm{H}$.

Si g n'appartient à H alors g n'est pas une rotation donc c'est une réflexion, *i.e.* $g = r^i s$ pour un certain i. Alors $g\mathrm{H} = r^i s\mathrm{H} = sr^{-i}\mathrm{H} = s\mathrm{H}$ car $r^{-i} \in \mathrm{H}$ et $\mathrm{H}g = \mathrm{H}r^i s = \mathrm{H}s$ car $r^i \in \mathrm{H}$, nous sommes donc ramenés à vérifier que $s\mathrm{H} = \mathrm{H}s$. Or d'une part

$$s\mathrm{H} = \{s,\, sr,\, sr^2,\, \ldots,\, sr^{n-1}\} = \{s,\, r^{-1}s,\, r^{-2}s,\, \ldots,\, r^{-(n-1)}s\}.$$

et d'autre part

$$\mathrm{H}s = \{s,\, rs,\, r^2 s,\, \ldots,\, r^{n-1}s\};$$

ainsi $s\mathrm{H} = \mathrm{H}s$ (rappelons que $r^{-i} = r^{n-i}$).

Cet exemple est en fait un cas particulier de l'énoncé suivant.

Théorème 3.2.1

Soit G un groupe. Un sous-groupe d'indice 2 de G est distingué dans G.

Démonstration. — Soit H un sous-groupe d'indice 2 de G. Nous voulons montrer $g\mathrm{H} = \mathrm{H}g$ pour tout $g \in \mathrm{G}$.

Si g appartient à H, alors $g\mathrm{H} = \mathrm{H}$ et $\mathrm{H}g = \mathrm{H}$ d'où $g\mathrm{H} = \mathrm{H}g$.

Si g n'appartient pas à H alors $g\mathrm{H} \neq \mathrm{H}$; puisque H est d'indice 2 dans G, la classe à gauche $g\mathrm{H}$ est la classe de H distincte de H, c'est-à-dire $g\mathrm{H} = \mathrm{G} \smallsetminus \mathrm{H}$. De même nous avons $\mathrm{H}g \neq \mathrm{H}$ donc $\mathrm{H}g = \mathrm{G} \smallsetminus \mathrm{H}$. Ainsi $g\mathrm{H} = \mathrm{G} \smallsetminus \mathrm{H} = \mathrm{H}g$. □

Exemple 3.2.7. — Puisque $[\mathfrak{S}_n : \mathcal{A}_n] = 2$, le groupe $\mathcal{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$.

La notation standard pour indiquer qu'un sous-groupe H d'un groupe G est distingué dans G est : $\mathrm{H} \triangleleft \mathrm{G}$. Par exemple :

$$m\mathbb{Z} \triangleleft \mathbb{Z}, \qquad \langle r \rangle \triangleleft \mathrm{D}_{2n}, \qquad \mathcal{A}_n \triangleleft \mathfrak{S}_n;$$

en effet $\mathbb{Z}$ est abélien, $\langle r \rangle$ (resp. $\mathcal{A}_n$) est un sous-groupe d'indice 2 de D_{2n} (resp. $\mathfrak{S}_n$).

Montrons que la multiplication des classes à gauche (à droite) d'un sous-groupe distingué via $g_1\mathrm{H} \cdot g_2\mathrm{H} = g_1 g_2\mathrm{H}$ est bien définie, c'est-à-dire indépendante du choix du représentant.

Théorème 3.2.2

Soit G un groupe. Soit $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. S'il existe $g_1,\, g_1',\, g_2,\, g_2'$ dans G tels que $g_1\mathrm{N} = g_1'\mathrm{N}$ et $g_2\mathrm{N} = g_2'\mathrm{N}$, alors $g_1 g_2\mathrm{N} = g_1' g_2'\mathrm{N}$.

Démonstration. — Puisque $g_1\mathrm{N} = g_1'\mathrm{N}$ et $g_2\mathrm{N} = g_2'\mathrm{N}$, il existe n_1, $n_2 \in \mathrm{N}$ tels que $g_1 = g_1'n_1$ et $g_2 = g_2'n_2$. Alors $g_1g_2 = g_1'n_1g_2'n_2 = g_1'(n_1g_2')n_2$. Comme N est un sous-groupe distingué de G, n_1g_2' s'écrit aussi $g_2'n_1'$ pour un certain $n_1' \in \mathrm{N}$. Alors $g_1g_2 = g_1'(g_2'n_1')n_2 = g_1'g_2'(n_1'n_2)$, et $n_1'n_2 \in \mathrm{N}$ d'où $g_1g_2\mathrm{N} = g_1'g_2'\mathrm{N}$. □

Pour vérifier qu'un sous-groupe H d'un groupe G est un sous-groupe distingué de G, on peut réécrire la condition $g\mathrm{H} = \mathrm{H}g$ sous la forme $g\mathrm{H}g^{-1} = \mathrm{H}$. De plus, il s'avère que pour vérifier $g\mathrm{H}g^{-1} = \mathrm{H}$ pour tout $g \in \mathrm{G}$, il suffit de vérifier l'inclusion $g\mathrm{H}g^{-1} \subset \mathrm{H}$ pour tout g :

Théorème 3.2.3

Un sous-groupe H d'un groupe G est distingué dans G si et seulement si $g\mathrm{H}g^{-1} \subset \mathrm{H}$ pour tout $g \in \mathrm{G}$. Autrement dit $g\mathrm{H}g^{-1} = \mathrm{H}$ pour tout $g \in \mathrm{G}$ si et seulement si $g\mathrm{H}g^{-1} \subset \mathrm{H}$ pour tout $g \in \mathrm{G}$.

Démonstration. — Si $g\mathrm{H}g^{-1} = \mathrm{H}$ pour tout $g \in \mathrm{G}$ alors évidemment $g\mathrm{H}g^{-1} \subset \mathrm{H}$ pour tout $g \in \mathrm{G}$.

Réciproquement supposons que $g\mathrm{H}g^{-1} \subset \mathrm{H}$ pour tout $g \in \mathrm{G}$. Quitte à remplacer g par g^{-1} nous obtenons $g^{-1}\mathrm{H}g \subset \mathrm{H}$ pour tout g aussi. En multipliant la relation $g\mathrm{H}g^{-1} \subset \mathrm{H}$ à droite par g nous obtenons $g\mathrm{H} \subset \mathrm{H}g$; de plus multiplier la relation $g^{-1}\mathrm{H}g \subset \mathrm{H}$ à gauche par g conduit à $\mathrm{H}g \subset g\mathrm{H}$. Les inclusions $g\mathrm{H} \subset \mathrm{H}g$ et $\mathrm{H}g \subset g\mathrm{H}$ entraînent $g\mathrm{H} = \mathrm{H}g$. □

Exemple 3.2.8. — Le groupe $\mathrm{SL}(2,\mathbb{R})$ est un sous-groupe distingué de $\mathrm{GL}(2,\mathbb{R})$. D'après le Théorème 3.2.3, il suffit de montrer $A\mathrm{SL}(2,\mathbb{R})A^{-1} \subset \mathrm{SL}(2,\mathbb{R})$ pour tout $A \in \mathrm{GL}(2,\mathbb{R})$. Soit B un élément de $\mathrm{SL}(2,\mathbb{R})$, alors

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(A)\det(B)\frac{1}{\det A} = \det B = 1,$$

donc ABA^{-1} appartient à $\mathrm{SL}(2,\mathbb{R})$.

Exemple 3.2.9. — Le sous-groupe $\langle r\rangle$ de D_{2n} est distingué dans D_{2n} puisqu'il est d'indice 2 (Théorème 3.2.1). Par contre $\langle s\rangle = \{\mathrm{id},\, s\}$ n'est pas un sous-groupe distingué de D_{2n} puisque $r\langle s\rangle r^{-1} \not\subset \langle s\rangle$ (en effet, nous avons en particulier $rsr^{-1} = rrs = r^2s \notin \langle s\rangle$).

Exemple 3.2.10. — L'ensemble $\mathrm{Aut}(\mathrm{G})$ des automorphismes d'un groupe G forme un groupe pour la composition des applications. C'est un sous-groupe du groupe $\mathfrak{S}_{\mathrm{G}}$ des permutations des éléments de G. Si G est un groupe fini d'ordre b, alors $\mathrm{Aut}(\mathrm{G})$ est d'ordre au plus $(n-1)!$.

Pour tout $g \in \mathrm{G}$ la conjugaison par g

$$\gamma_g \colon \mathrm{G} \to \mathrm{G}, \qquad h \mapsto ghg^{-1}$$

introduite dans l'Exemple 2.1.26 est un automorphisme de G. L'ensemble $\mathrm{Int}(\mathrm{G}) = \{\gamma_g \mid g \in \mathrm{G}\}$ est un sous-groupe distingué de $\mathrm{Aut}(\mathrm{G})$ appelé *groupe des automorphismes intérieurs* de G.

En effet soit $\gamma_g \in \mathrm{Int(G)}$ et soit $\varphi \in \mathrm{Aut(G)}$; pour tout $h \in \mathrm{G}$ nous avons

$$\varphi\gamma_g\varphi^{-1}(h) = \varphi(g\varphi^{-1}(h)g^{-1}) = \varphi(g)h\varphi(g)^{-1} = \gamma_{\varphi(g)}(h) \in \mathrm{Int(G)}.$$

Pour montrer qu'un sous-groupe H d'un groupe G n'est pas distingué dans G, il suffit de montrer $g\mathrm{H}g^{-1}$ n'est pas contenu dans H pour un certain $g \in \mathrm{G}$, autrement dit que $ghg^{-1} \notin \mathrm{H}$ pour un $g \in \mathrm{G}$ et un $h \in \mathrm{H}$.

Exemple 3.2.11. — Le sous-groupe $\mathrm{Aff}(\mathbb{R})$ de $\mathrm{GL}(2,\mathbb{R})$ n'est pas distingué dans $\mathrm{GL}(2,\mathbb{R})$. En effet, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ appartient à $\mathrm{GL}(2,\mathbb{R})$ et

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

n'appartient pas à $\mathrm{Aff}(\mathbb{R})$.

Le Théorème 3.2.3 nous permet de montrer une réciproque du Théorème 3.2.2 : si le produit (3.2.1) est bien défini alors H doit être un sous-groupe distingué de G. En effet, pour $g \in \mathrm{G}$ et $h \in \mathrm{H}$, $h\mathrm{H} = \mathrm{H} = e\mathrm{H}$ et $g\mathrm{H} = g\mathrm{H}$, donc pour que (3.2.1) soit bien défini il faut que $hg\mathrm{H} = eg\mathrm{H}$, *i.e.* que hg appartienne à $g\mathrm{H}$. Ainsi $g^{-1}hg$ appartient à H pour tous $h \in \mathrm{H}$ et $g \in \mathrm{G}$. Cela étant censé être vrai pour tout g, nous pouvons remplacer g par g^{-1} pour obtenir $ghg^{-1} \in \mathrm{H}$ pour tout $h \in \mathrm{H}$, donc $g\mathrm{H}g^{-1} \subset \mathrm{H}$ pour tout $g \in \mathrm{G}$. Par conséquent $\mathrm{H} \triangleleft \mathrm{G}$ (Théorème 3.2.3).

Remarque 3.2.2. — Il est crucial dans le Théorème 3.2.3 que la quantification s'étende à tout $g \in \mathrm{G}$, puisque pour certains H et $g \in \mathrm{G}$ il peut arriver que $g\mathrm{H}g^{-1} \subset \mathrm{H}$ sans que $g\mathrm{H}g^{-1} = \mathrm{H}$. Par exemple, soit $\mathrm{G} = \mathrm{GL}(2,\mathbb{R})$ (ou $\mathrm{G} = \mathrm{GL}(2,\mathbb{Q})$). Soit H le sous-groupe de G défini par $\mathrm{H} = \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \mid m \in \mathbb{Z} \right\}$. Considérons l'élément g de G défini par $g = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. D'une part

$$\begin{aligned} g\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}g^{-1} &= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 2m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2m \\ 0 & 1 \end{pmatrix} \in \mathrm{H} \end{aligned}$$

pour tout $m \in \mathbb{Z}$, donc $g\mathrm{H}g^{-1} \subset \mathrm{H}$. D'autre part

$$g^{-1}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}g = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{m}{a} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{m}{2} \\ 0 & 1 \end{pmatrix}$$

n'appartient pas à H si $m = 1$; il en résulte que $g^{-1}\mathrm{H}g \not\subset \mathrm{H}$. Par suite $g\mathrm{H}g^{-1} \neq \mathrm{H}$: le sous-groupe H de G n'est pas un sous-groupe distingué de G.

Remarque 3.2.3. — Soient G un groupe et $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. Il est important de bien réaliser que si K est un sous-groupe de N, cela n'implique pas que K soit distingué dans G. Par exemple considérons le sous-groupe K de $\mathcal{A}_4$ défini par :

$$\mathrm{K} = \{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

On peut vérifier que K, qui est isomorphe au groupe de Klein $\mathcal{K}$, est un sous-groupe distingué de $\mathcal{A}_4$. Les trois sous-groupes d'ordre 2 de K sont distingués dans K mais sont conjugués dans $\mathcal{A}_4$, donc, en particulier, non distingués dans $\mathcal{A}_4$.

Proposition 3.2.1

Si $\varphi\colon \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes, alors $\ker\varphi$ est un sous-groupe distingué de G.

Démonstration. — En effet, soient g dans G et h dans $\ker\varphi$; comme φ est un morphisme de groupes nous avons $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1})$. Étant donné que h appartient à $\ker\varphi$, $\varphi(h) = e_{\mathrm{G}'}$. Ainsi $\varphi(ghg^{-1}) = \varphi(g)\varphi(g^{-1})$. Puisque φ est un morphisme de groupes $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_{\mathrm{G}}) = e_{\mathrm{G}'}$. Finalement $\varphi(ghg^{-1}) = e_{\mathrm{G}'}$, autrement dit ghg^{-1} appartient à $\ker\varphi$. □

Exemple 3.2.12. — Le groupe spécial linéaire $\mathrm{SL}(n, \mathbb{C})$ est un sous-groupe distingué de $\mathrm{GL}(n, \mathbb{C})$ (prendre $\varphi = \det$).

Exemple 3.2.13. — Le groupe $\mathcal{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$ (prendre $\varphi = \mathrm{sgn}$).

Exemple 3.2.14. — Soit G un groupe. L'application

$$\varphi\colon \mathrm{G} \to \mathrm{Int}(\mathrm{G}), \qquad g \mapsto \gamma_g$$

est un morphisme de groupes de noyau $Z(\mathrm{G})$. En particulier $Z(\mathrm{G})$ est un sous-groupe distingué de G.

3.3. Groupes quotients

Le Théorème 3.2.2 assure que la multiplication des classes à gauche d'un sous-groupe distingué N d'un groupe G est bien définie :

Définition 3.3.1

Soit G un groupe. Si $\mathrm{N} \triangleleft \mathrm{G}$ est un sous-groupe distingué de G, le produit de deux classes à gauche $g_1\mathrm{N}$ et $g_2\mathrm{N}$, g_1, $g_2 \in \mathrm{G}$, est : $g_1\mathrm{N} \cdot g_2\mathrm{N} = g_1g_2\mathrm{N}$.

Nous pourrions de manière équivalente utiliser les classes à droite de N car N étant distingué dans G nous avons $g\mathrm{N} = \mathrm{N}g$ pour tout $g \in \mathrm{G}$.

Théorème 3.3.1

Soient G un groupe et $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. L'ensemble des classes à gauche de N dans G muni de la loi

$$(g_1\mathrm{N}, g_2\mathrm{N}) \mapsto g_1\mathrm{N} \cdot g_2\mathrm{N} = g_1g_2\mathrm{N}$$

est un groupe.

Démonstration. — L'élément neutre pour cette opération sur les classes à gauche de N est N :

$$\mathrm{N} \cdot g\mathrm{N} = e\mathrm{N} \cdot g\mathrm{N} = eg\mathrm{N} = g\mathrm{N}, \qquad g\mathrm{N} \cdot \mathrm{N} = g\mathrm{N} \cdot e\mathrm{N} = ge\mathrm{N} = g\mathrm{N}.$$

L'inverse de $g\mathrm{N}$ est $g^{-1}\mathrm{N}$; en effet

$$gN \cdot g^{-1}\mathrm{N} = gg^{-1}\mathrm{N} = e\mathrm{N} = \mathrm{N}, \qquad g^{-1}N \cdot g\mathrm{N} = g^{-1}g\mathrm{N} = e\mathrm{N} = \mathrm{N}.$$

L'associativité de cette loi sur les classes à gauche découle de l'associativité de la loi de groupe dans G : d'une part

$$(g\mathrm{N} \cdot h\mathrm{N}) \cdot k\mathrm{N} = gh\mathrm{N} \cdot k\mathrm{N} = (gh)k\mathrm{N}, \qquad g\mathrm{N} \cdot (h\mathrm{N} \cdot k\mathrm{N}) = g\mathrm{N} \cdot hk\mathrm{N} = g(hk)\mathrm{N},$$

d'autre part $(gh)k = g(hk)$. Par suite nous obtenons $(gh)k\mathrm{N} = g(hk)\mathrm{N}$. □

Exemple 3.3.1. — Soit G un groupe. Le sous-groupe $\mathrm{N} = \{e\}$ est distingué dans G. Le groupe quotient $\mathrm{G}/\mathrm{N} = \mathrm{G}/\{e\}$ est

$$\{g\mathrm{N} \,|\, g \in \mathrm{G}\} = \{g\{e\} \,|\, g \in \mathrm{G}\} = \mathrm{G}.$$

Exemple 3.3.2. — Soit G un groupe. Le sous-groupe $\mathrm{N} = \mathrm{G}$ est distingué dans G. Le groupe quotient $\mathrm{G}/\mathrm{N} = \mathrm{G}/\mathrm{G}$ est

$$\{g\mathrm{N} \,|\, g \in \mathrm{G}\} = \{g\mathrm{G} \,|\, g \in \mathrm{G}\} = \mathrm{G} = \mathrm{N} = \{e_{\mathrm{G}/\mathrm{N}}\}.$$

Exemple 3.3.3. — Considérons le groupe $\mathbb{H}_8$. Rappelons que $\langle -1 \rangle$ est un sous-groupe distingué de $\mathbb{H}_8$; l'ensemble quotient $\mathbb{H}_8/\langle -1 \rangle$ est donc un groupe. Donnons une description de $\mathbb{H}_8/\langle -1 \rangle$. Par définition

$$\mathbb{H}_8/\langle -1 \rangle = \{g\langle -1 \rangle \,|\, g \in \mathbb{H}_8\}.$$

Nous avons

$$\begin{aligned}
\overline{1} &= 1\langle -1 \rangle = \langle -1 \rangle, & -1\langle -1 \rangle &= \langle -1 \rangle = \overline{1},\\
\overline{i} &= i\langle -1 \rangle = \{i, -i\}, & -i\langle -1 \rangle &= \{-i, i\} = \overline{i},\\
\overline{j} &= j\langle -1 \rangle = \{j, -j\}, & -j\langle -1 \rangle &= \{-j, j\} = \overline{j},\\
\overline{k} &= k\langle -1 \rangle = \{k, -k\}, & -k\langle -1 \rangle &= \{-k, k\} = \overline{k}.
\end{aligned}$$

Ainsi ${}^{\mathrm{G}}\!/_{\mathrm{H}} = \{\overline{1}, \overline{i}, \overline{j}, \overline{k}\}$.

Exemple 3.3.4. — Considérons le groupe diédral

$$\mathrm{D}_{2n} = \{\mathrm{id}, r, r^2, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}.$$

Rappelons que $\langle r\rangle$ est un sous-groupe distingué de D_{2n} (en effet $[\mathrm{D}_{2n} : \langle r\rangle] = 2$). L'ensemble quotient ${}^{\mathrm{D}_{2n}}\!/_{\langle r\rangle}$ est donc un groupe. Donnons une description de celui-ci. Par définition

$${}^{\mathrm{D}_{2n}}\!/_{\langle r\rangle} = \{g\langle r\rangle \mid g \in \mathrm{D}_{2n}\}.$$

Nous avons

- ◇ si $g \in \mathrm{D}_{2n}$ est une rotation c'est-à-dire $g = r^k$ avec $0 \leq k \leq n-1$, alors
$$g\langle r\rangle = r^k\langle r\rangle = \{r^k r^i \mid 0 \leq i \leq n-1\} = \{r^j \mid 0 \leq j \leq n-1\} = \langle r\rangle = \overline{\mathrm{id}}.$$
- ◇ si $g \in \mathrm{D}_{2n}$ n'est pas une rotation, c'est-à-dire $g = r^k s$ avec $0 \leq k \leq n-1$, alors
$$g\langle r\rangle = \{r^k s r^i \mid 0 \leq i \leq n-1\}$$
Comme $sr^\ell = r^{-\ell}s$ pour tout $0 \leq \ell \leq n-1$ nous obtenons
$$g\langle r\rangle = \{sr^{k-1}r^i \mid 0 \leq i \leq n-1\} = s\{r^j \mid 0 \leq j \leq n-1\} = s\langle r\rangle = \overline{s}.$$

Finalement nous obtenons que ${}^{\mathrm{D}_{2n}}\!/_{\langle r\rangle} = \{\overline{\mathrm{id}}, \overline{s}\}$.

L'énoncé suivant assure que l'ordre de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$ peut être déterminé à partir des ordres de G et N.

Théorème 3.3.2

Soient G un groupe. Soit $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. Si G est fini, alors $\left|{}^{\mathrm{G}}\!/_{\mathrm{N}}\right| = \frac{|\mathrm{G}|}{|\mathrm{N}|}$.

Démonstration. — L'ordre de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$ est le nombre de classes à gauche de N dans G (gauche ou droite n'a pas d'importance puisque $g\mathrm{N} = \mathrm{N}g$). D'après le théorème de Lagrange (Théorème 1.6.4), si N possède ν classes à gauche dans G alors $\nu|\mathrm{N}| = |\mathrm{G}|$, d'où $\left|{}^{\mathrm{G}}\!/_{\mathrm{N}}\right| = \nu = \frac{|\mathrm{G}|}{|\mathrm{N}|}$. □

Comme dans ${}^{\mathbb{Z}}\!/_{m\mathbb{Z}}$, où $\overline{a}$ désigne la classe de congruence $a + m\mathbb{Z}$, on désigne parfois $g\mathrm{N}$ par $\overline{g}$ dans ${}^{\mathrm{G}}\!/_{\mathrm{N}}$. On appelle $\overline{g}$ la *réduction de g modulo* N. Avec cette notation, la loi de groupe de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$ se réécrit $\overline{g_1}\,\overline{g_2} = \overline{g_1 g_2}$, l'élément neutre est $\overline{e}$ et $\overline{g}^{-1} = \overline{g^{-1}}$. Si la loi est additive, nous avons $\overline{g_1} + \overline{g_2} = \overline{g_1 + g_2}$, l'élément neutre est $\overline{0}$ et $-\overline{g} = \overline{-g}$.

Théorème 3.3.3

Soient G un groupe et $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. Considérons un élément g de G ; pour tout $k \in \mathbb{Z}$ nous avons $\overline{g}^k = \overline{g^k}$.

Démonstration. — Le cas $k = 0$ est trivial.

Le cas $k \geq 1$ s'obtient par récurrence.

Supposons $k < 0$. Posons $k = -\ell$ alors $\ell \geq 1$. D'après ce qui précède $\overline{g}^\ell = \overline{g^\ell}$. Alors

$$\overline{g}^k = \overline{g}^{-\ell} = (\overline{g}^\ell)^{-1} = \overline{g^\ell}^{-1} = \overline{(g^\ell)^{-1}} = \overline{g^{-\ell}} = \overline{g^k}.$$

□

Corollaire 3.3.1

Soient G un groupe fini et $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. Soit g un élément de G. Alors $g^{|\mathrm{G}|/|\mathrm{N}|}$ appartient à N.

Démonstration. — Posons $\nu = \frac{|\mathrm{G}|}{|\mathrm{N}|}$. Le groupe G/N est donc d'ordre ν. Considérons un élément g de G. Nous avons $\overline{g}^\nu = \overline{e}$ dans G/N. Ainsi, d'après le Théorème 3.3.3, nous obtenons $\overline{g^\nu} = \overline{e}$; il en résulte que g^ν appartient à N. □

Exemple 3.3.5. — Si $\mathrm{G} = \mathfrak{S}_n$ et $\mathrm{N} = \mathcal{A}_n$, alors $\frac{|\mathrm{G}|}{|\mathrm{N}|} = 2$. Soit g dans $\mathfrak{S}_n$. D'après le Corollaire 3.3.1 l'élément g^2 appartient à $\mathcal{A}_n$.

Si N n'est pas distingué dans G, il peut y avoir contre-exemples : si $\mathrm{G} = \mathfrak{S}_3$ et $\mathrm{H} = \{\mathrm{id}, (1\ 2)\}$, alors H n'est pas un sous-groupe distingué de G et $\frac{|\mathrm{G}|}{|\mathrm{H}|} = 3$. Si $g = (1\ 3)$ (resp. $(2\ 3)$), alors g^3 n'appartient pas à H.

Néanmoins si $|\mathrm{G}|$ est une puissance d'un nombre premier, alors pour tout sous-groupe H de G, pour tout élément g de G l'élément $g^{|\mathrm{G}|/|\mathrm{H}|}$ appartient à H que H soit distingué ou non.

Théorème 3.3.4

Soient G un groupe et $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de G.

1. Si G est abélien alors G/N est abélien.
2. Si G est cyclique alors G/N est cyclique.

Démonstration. — 1. Supposons que G soit abélien. Considérons deux eléments $\overline{g}$ et $\overline{g'}$ de G/N. Alors $\overline{g}\overline{g'} = \overline{gg'}$ et $\overline{g'}\overline{g} = \overline{g'g}$. Puisque G est abélien, $gg' = g'g$ dans G. Il en résulte que $\overline{gg'} = \overline{g'g}$ dans G/N. Ainsi $\overline{g}\overline{g'} = \overline{g'}\overline{g}$.

2. Supposons que G soit cyclique. Soit x un générateur de G. Chaque élément de G s'écrit donc x^k pour un certain $k \in \mathbb{Z}$. Ainsi tout élément de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$ est de la forme $\overline{x^k}$ pour un certain $k \in \mathbb{Z}$, et $\overline{x^k} = \overline{x}^k$ (Théorème 3.3.3). Il en résulte que $\overline{x}$ est un générateur de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$. $\square$

***Exemple 3.3.6* (Le groupe quotient ${}^{\mathbb{Z}}\!/_{m\mathbb{Z}}$).** — Considérons l'ensemble $\mathbb{Z}$ des entiers relatifs et le sous-groupe $2\mathbb{Z}$ constitué des entiers pairs. Alors le groupe quotient ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ est constitué de deux éléments (pour la relation de congruence), représentant la classe des nombres pairs et la classe des nombres impairs.

De manière plus générale on construit à partir de l'ensemble $\mathbb{Z}$ des entiers relatifs et du sous-groupe $m\mathbb{Z}$ constitué des entiers multiples de m le groupe quotient ${}^{\mathbb{Z}}\!/_{m\mathbb{Z}}$, *i.e.* l'ensemble des entiers modulo m muni de l'addition.

***Exemple 3.3.7* (Le groupe quotient ${}^{\mathbb{R}^\times}\!/_{\{\pm 1\}}$).** — Si $\mathrm{G} = \mathbb{R}^\times$ et $\mathrm{H} = \{\pm 1\}$, le groupe quotient est ${}^{\mathbb{R}^\times}\!/_{\{\pm 1\}}$, cela consiste à travailler sur les réels sans se soucier du signe des nombres qu'on manipule.

***Exemple 3.3.8* (Le groupe quotient ${}^{\mathbb{R}}\!/_{2\pi\mathbb{Z}}$).** — L'ensemble $\mathbb{R}$ des nombres réels, considéré comme groupe additif, et son sous-groupe $2\pi\mathbb{Z}$ permettent de définir un groupe quotient ${}^{\mathbb{R}}\!/_{2\pi\mathbb{Z}}$ utilisé pour la mesure des angles orientés.

Jusqu'à présent, nos exemples ont été des groupes quotients de groupes abéliens, où chaque sous-groupe est distingué. Donnons désormais des exemples un peu différents.

***Exemple 3.3.9* (Le groupe quotient $\mathfrak{S}_n/\mathcal{A}_n$).** — On compte deux classes de $\mathcal{A}_n$ dans $\mathfrak{S}_n$

- $\overline{\mathrm{id}} = \mathrm{id}\mathcal{A}_n = \mathcal{A}_n$ (les permutations paires)
- $\overline{(1\ 2)} = (1\ 2)\mathcal{A}_n$ (les permutations impaires).

Par conséquent ${}^{\mathfrak{S}_n}\!/_{\mathcal{A}_n} = \{\overline{\mathrm{id}}, \overline{(1\ 2)}\}$. Notons que $\overline{(1\ 2)(1\ 2)} = \overline{(1\ 2)(1\ 2)} = \overline{\mathrm{id}}$. Le groupe ${}^{\mathfrak{S}_n}\!/_{\mathcal{A}_n}$ est donc cyclique d'ordre 2.

***Exemple 3.3.10* (Le groupe quotient ${}^{\mathrm{D}_{16}}\!/_{Z(\mathrm{D}_{16})}$).** — Les 16 éléments de D_{16} sont

$$\mathrm{id},\ r,\ r^2,\ \ldots,\ r^7,\ s,\ rs,\ r^2s,\ \ldots,\ r^7s$$

et le centre $Z(\mathrm{D}_{16})$ de D_{16} est $\{\mathrm{id},\ r^4\}$ (rappelons que $r^{-4} = r^4$). Si g désigne un élément de D_{16} alors $\overline{g} = gZ(\mathrm{D}_{16}) = \{g,\ gr^4\}$. Le groupe quotient ${}^{\mathrm{D}_{16}}\!/_{Z(\mathrm{D}_{16})}$ est d'ordre $\frac{16}{2} = 8$, les classes à gauche dans $\mathrm{D}_{16}/Z(\mathrm{D}_{16})$ sont

$$\overline{\mathrm{id}} = \{\mathrm{id},\ r^4\}, \qquad \overline{r} = \{r,\ r^5\}, \qquad \overline{r^2} = \{r^2,\ r^6\}, \qquad \overline{r^3} = \{r^3,\ r^7\},$$

$$\begin{aligned}
\overline{s} &= \{s,\, sr^4\} = \{s,\, r^{-4}s\} = \{s,\, r^4 s\} = \overline{r^4 s},\\
\overline{rs} &= \{rs,\, rsr^4\} = \{rs,\, r^{-3}s\} = \{rs,\, r^5 s\} = \overline{r^5 s},\\
\overline{r^2 s} &= \{r^2 s,\, r^2 sr^4\} = \{r^2 s,\, r^{-2}s\} = \{r^2 s,\, r^6 s\} = \overline{r^6 s},\\
\overline{r^3 s} &= \{r^3 s,\, r^3 sr^4\} = \{r^3 s,\, r^{-1}s\} = \{r^3 s,\, r^7 s\} = \overline{r^7 s}.
\end{aligned}$$

Nous pouvons nous demander à quoi ressemble le groupe $\mathrm{D}_{16}/Z(\mathrm{D}_{16})$? Puisque $\overline{r}^4 = \overline{r^4} = \overline{\mathrm{id}}$ et $\overline{r}^k = \overline{r^k} \neq \overline{\mathrm{id}}$ pour $1 \leq k \leq 3$, $\overline{r}$ est d'ordre 4 dans ${}^{\mathrm{D}_{16}}\!/_{Z(\mathrm{D}_{16})}$. La classe $\overline{s}$ n'est pas l'identité puisque s n'appartient pas à $Z(\mathrm{D}_{16})$ et $\overline{s}^2 = \overline{s^2} = \overline{\mathrm{id}}$; il en résulte que $\overline{s}$ est d'ordre 2. Puisque $rs = sr^{-1}$ dans D_{16}, nous avons dans ${}^{\mathrm{D}_{16}}\!/_{Z(\mathrm{D}_{16})}$

$$\overline{rs} = \overline{r}\,\overline{s} = \overline{sr^{-1}} = \overline{s}\,\overline{r^{-1}} = \overline{s}\,\overline{r}^{-1};$$

ainsi les relations entre r et s font « ressembler » ${}^{\mathrm{D}_{16}}\!/_{Z(\mathrm{D}_{16})}$ au groupe D_8.

Exemple 3.3.11 **(Le groupe quotient ${}^{\mathrm{GL}(2,\mathbb{R})}\!/_{\mathrm{SL}(2,\mathbb{R})}$).** — Nous allons d'abord montrer que chaque classe a un unique représentant de la forme $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$ avec $\delta \in \mathbb{R}^\times$. Soit $A \in \mathrm{GL}(2,\mathbb{R})$; alors $\overline{A} = A\mathrm{SL}(2,\mathbb{R}) = \{AB \mid B \in \mathrm{SL}(2,\mathbb{R})\}$. Posons $\delta = \det A$. Alors $\det \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix} = \delta$ et $\det \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}^{-1} A = \frac{1}{\delta}\delta = 1$. Autrement dit $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}^{-1} A$ appartient à $\mathrm{SL}(2,\mathbb{R})$ et A à $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}\mathrm{SL}(2,\mathbb{R})$. Cela montre que $\overline{A} = \begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$. Par conséquent tout élément de ${}^{\mathrm{GL}(2,\mathbb{R})}\!/_{\mathrm{SL}(2,\mathbb{R})}$ est représenté par une matrice de la forme $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$.

Remarquons que δ est unique : si

$$\overline{\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}} = \overline{\begin{pmatrix} \delta' & 0 \\ 0 & 1 \end{pmatrix}}$$

alors $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \delta' & 0 \\ 0 & 1 \end{pmatrix} B$; en prenant les déterminants des deux côtés nous obtenons $\delta = \delta' \det B = \delta'$.

La formule $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \delta' & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \delta\delta' & 0 \\ 0 & 1 \end{pmatrix}$ pour les matrices implique la formule $\overline{\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}} \cdot \overline{\begin{pmatrix} \delta' & 0 \\ 0 & 1 \end{pmatrix}} = \overline{\begin{pmatrix} \delta\delta' & 0 \\ 0 & 1 \end{pmatrix}}$ pour les classes à gauche. Le groupe quotient $\mathrm{GL}(2,\mathbb{R})/\mathrm{SL}(2,\mathbb{R})$ « ressemble » donc au groupe $(\mathbb{R}^\times, \cdot)$.

Exemple 3.3.12 **(Le groupe quotient $\mathrm{GL}\left(2, \mathbb{Z}/m\mathbb{Z}\right)/\mathrm{SL}\left(2, \mathbb{Z}/m\mathbb{Z}\right)$)**

Si nous raisonnons comme dans l'exemple précédent en remplaçant $\mathbb{R}$ par $\mathbb{Z}/m\mathbb{Z}$, chaque élément de $\mathrm{GL}\left(2, \mathbb{Z}/m\mathbb{Z}\right)/\mathrm{SL}\left(2, \mathbb{Z}/m\mathbb{Z}\right)$ a un représentant unique de la forme $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}$ avec $\delta \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$. Le groupe quotient $\mathrm{GL}\left(2, \mathbb{Z}/m\mathbb{Z}\right)/\mathrm{SL}\left(2, \mathbb{Z}/m\mathbb{Z}\right)$ « ressemble » à $\left(\left(\mathbb{Z}/m\mathbb{Z}\right)^\times, \cdot\right)$.

Ne confondez pas groupes et sous-groupes de quotients ! Même si les éléments de $\mathbb{Z}/m\mathbb{Z}$ ont des représentants $(\{0, 1, \ldots, m-1\})$ dans $\mathbb{Z}$, le groupe $\mathbb{Z}/m\mathbb{Z}$ n'est pas un sous-groupe de $\mathbb{Z}$: les éléments de $\mathbb{Z}/m\mathbb{Z}$ sont d'ordre fini, contrairement aux éléments non nuls de $\mathbb{Z}$.

3.4. Ordres des éléments dans un groupe quotient

Comparons l'ordre d'un élément de G à son ordre dans G/N. Dire que $\overline{g} \in \mathrm{G}/\mathrm{N}$ est d'ordre k signifie $\overline{g}^k = \overline{e}$ et que $\overline{g}^\ell \neq \overline{e}$ pour tout $1 \leq \ell < k$. Cela revient à dire que g^k appartient à N et que g^ℓ n'appartient à N pour tout $1 \leq \ell < k$. En passant de G à G/N, l'ordre d'un élément peut chuter : de l'infini à fini ou d'une valeur finie k à une valeur finie $\ell < k$.

Exemple 3.4.1. — Dans le groupe additif $\mathbb{Z}$, 1 est d'ordre infini tandis que dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{1} = 1 + 6\mathbb{Z}$ est d'ordre 6.

Exemple 3.4.2. — Dans le groupe de quaternions $\mathbb{H}_8$, le sous-groupe $\{\pm 1\}$ est distingué dans $\mathbb{H}_8$ (c'est le centre de $\mathbb{H}_8$). L'ordre de i dans $\mathbb{H}_8$ est 4 alors que l'ordre de i dans $\mathbb{H}_8/\{\pm 1\}$ est 2 puisque $\overline{i}^2 = \overline{-1} = \overline{1}$ et $\overline{i} \neq \overline{1}$.

Exemple 3.4.3. — Soit $n \geq 3$. Le n-cycle $(1\ 2\ \ldots\ n)$ est d'ordre n dans $\mathfrak{S}_n$, tandis que sa réduction dans $\mathfrak{S}_n/\mathcal{A}_n$ est d'ordre 1 ou 2 puisque $\mathfrak{S}_n/\mathcal{A}_n$ est un groupe d'ordre 2. Plus précisément, si $\sigma \in \mathfrak{S}_n$ la réduction $\overline{\sigma} = \sigma\mathcal{A}_n$ d'une permutation dans $\mathfrak{S}_n/\mathcal{A}_n$ est

- ⋄ triviale lorsque σ est pair,

◇ non triviale lorsque σ est impair ;

Ainsi σ est d'ordre

◇ 1 si σ est pair,

◇ 2 si σ est impair.

Exemple 3.4.4. — Soient $\mathrm{G} = \mathbb{Z}/20\mathbb{Z}$ et $\mathrm{N} = 10\mathbb{Z}/20\mathbb{Z}$. Alors G est cyclique d'ordre 20 et $\mathrm{N} = \{0, 10 \bmod 20\}$ est un sous-groupe distingué d'ordre 2 (tous les sous-groupes d'un groupe cyclique sont distingués). Le groupe quotient G/N est un groupe cyclique d'ordre $\frac{20}{2} = 10$ (Théorème 3.3.4) et la démonstration de cet énoncé montre que la réduction de chaque générateur de G dans G/N est un générateur de G/N. Par exemple, 1 mod 20 est d'ordre 20 dans G et $\overline{1 \bmod 20}$ est d'ordre 10 dans dans G/N. L'élément 5 mod 20 de G est d'ordre 4 et $\overline{5 \bmod 20} \in \mathrm{G}/\mathrm{N}$ est d'ordre 2. Par contre 4 mod 20 $\in$ G et $\overline{4 \bmod 20} \in \mathrm{G}/\mathrm{N}$ sont tous deux d'ordre 5.

Théorème 3.4.1

Soient G un groupe et $\mathrm{N} \triangleleft \mathrm{H}$ un sous-groupe distingué de G. Si $g \in \mathrm{G}$ est d'ordre fini m, alors l'ordre de $\overline{g}$ dans G/N divise m.

Démonstration. — Dans G nous avons $g^m = e$; dans G/N nous avons donc $\overline{g}^m = (g\mathrm{N})^m = g^m\mathrm{N} = \mathrm{N} = \overline{e}$. Par conséquent l'ordre de $\overline{g}$ divise m. □

Si $\overline{g} \in \mathrm{G}/\mathrm{N}$ est d'ordre fini k, alors le Théorème 3.4.1 assure que l'ordre de chaque représentant de $\overline{g}$ dans G est un multiple de k (si le représentant est d'ordre fini, par exemple si G est fini). Il peut ou non y avoir un représentant de g d'ordre k.

Exemple 3.4.5. — Soient $\mathrm{G} = \mathbb{Z}/12\mathbb{Z} = \{0, 1, \ldots, 11 \bmod 12\}$ et

$$\mathrm{N} = 2\mathbb{Z}/12\mathbb{Z} = \{0, 2, 4, 6, 8, 10 \bmod 12\}.$$

L'élément $\overline{1 \bmod 12} \in \mathrm{G}/\mathrm{N}$ est d'ordre 2 et ses représentants dans G sont $\{1, 3, 5, 7, 9, 11 \bmod 12\}$. Chacun d'eux est respectivement d'ordre 12, 4, 12, 12, 4 et 12 ; en particulier, aucun représentant n'est d'ordre 2.

Exemple 3.4.6. — Considérons le groupe quotient $\mathbb{H}_8/\{\pm 1\}$. L'élément $\overline{i}$ est d'ordre 2 et ses représentants dans $\mathbb{H}_8$ sont $\pm i$, qui sont tous deux d'ordre 4.

Corollaire 3.4.1

Soient G un groupe fini et $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de N. Supposons que l'ordre $|\mathrm{N}|$ de N et l'indice $[\mathrm{G} : \mathrm{N}]$ de N dans G soient premiers entre eux. Alors N est le seul sous-groupe de G d'ordre $|\mathrm{N}|$. Autrement dit si H est un sous-groupe de G tel que $|\mathrm{H}| = |\mathrm{N}|$, alors $\mathrm{H} = \mathrm{N}$.

Démonstration. — Posons $|\mathrm{N}| = n$. Soit $h \in \mathrm{H}$. Puisque $|\mathrm{H}| = n$, nous avons $h^n = e$. Dans le groupe quotient G/N nous obtenons $\overline{h}^n = \overline{e}$. Ainsi l'ordre de $\overline{h}$ divise n. De plus, l'ordre de $\overline{h}$ divise $\left|\mathrm{G}/\mathrm{N}\right|$; étant donné que $|\mathrm{N}|$ et $\left|\mathrm{G}/\mathrm{N}\right|$ sont premiers entre eux, nous obtenons $\overline{h} = \overline{e}$. Par suite h appartient à N. Finalement $\mathrm{H} \subset \mathrm{N}$ et $\mathrm{H} = \mathrm{N}$ (car $|\mathrm{H}| = |\mathrm{N}|$). □

Remarque 3.4.1. — L'hypothèse « N distingué dans G » est indispensable. Considérons le groupe $\mathfrak{S}_3$. Le sous-groupe $\mathcal{A}_3$ de $\mathfrak{S}_3$ est distingué dans $\mathfrak{S}_3$; il est d'ordre 3 et d'indice 2. Il est l'unique sous-groupe d'ordre 3 de $\mathfrak{S}_3$ (Corollaire 3.4.1). Le groupe $\{\mathrm{id}, (1\ 2)\}$ est d'ordre 2, d'indice 3 dans $\mathfrak{S}_3$; il n'est pas distingué dans $\mathfrak{S}_3$ et n'est pas l'unique sous-groupe d'ordre 2 dans $\mathfrak{S}_3$ (il y a par exemple $\{\mathrm{id}, (1\ 3)\}$).

Théorème 3.4.2

Soit G un groupe fini. Soit $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. Si $\overline{g} \in \mathrm{G}/\mathrm{N}$ est d'ordre p^k avec p premier, alors un des représentants de $\overline{g}$ est d'ordre p^ℓ.

Démonstration. — Désignons par p^r l'ordre de $\overline{g} \in \mathrm{G}/\mathrm{N}$ et par m l'ordre d'un représentant $g \in \mathrm{G}$ de $\overline{g}$. Le Théorème 3.4.1 assure que p^r divise m. Écrivons m sous la forme $p^s n$ où p ne divise pas n ; ainsi $r \leq s$.

Montrons que $g = ab$ où a et b sont des puissances de g telles que

- $a^{p^s} = 1$
- et b appartient à N et satisfait $b^n = e$

auquel cas $\overline{g} = \overline{a}$ et l'ordre de a est une puissance de p.

Puisque p^s et n sont premiers entre eux, il existe des entiers u et v tels que $1 = p^s u + nv$. Alors

$$g = g^1 = g^{p^s u} g^{nv} = \underbrace{g^{nv}}_{a} \underbrace{g^{p^s u}}_{b}$$

où

- $a = g^{nv}$ satisfait $a^{p^s} = g^{p^s nv} = g^{mv} = e$, en particulier l'ordre de a divise p^s et est donc une puissance de p ;
- $b = g^{p^s u}$ satisfait $b^n = g^{p^s nu} = g^{mu} = e$. À partir de $r \leq s$ et $\overline{g}^{p^r} = \overline{e}$, nous obtenons $\overline{g}^{p^s} = \overline{e}$; ainsi g^{p^s} appartient à N. Par conséquent $b = g^{p^s u}$ appartient à N.

□

Remarque 3.4.2. — Il s'avère que a est d'ordre p^s et b d'ordre n. En effet, le Théorème 1.5.6 assure que a et b sont les uniques éléments de G d'ordre p^s et n qui commutent et dont le produit est g.

Exemple 3.4.7. — Soient $\mathrm{G} = \mathbb{Z}/90\mathbb{Z}$ et $\mathrm{N} = 15\mathbb{Z}/90\mathbb{Z}$. Alors $\mathrm{G}/\mathrm{N} \simeq \mathbb{Z}/15\mathbb{Z}$.

- ◇ Dans G/N, 5 est d'ordre 3 tandis que dans G, 5 est d'ordre 18 mais $5 = 20$ dans G/N et 20 en G est d'ordre 9.
- ◇ Dans G/N, 6 est d'ordre 5 tandis que dans G, 6 est d'ordre 30 mais $6 = 36$ dans G/N et 36 en G est d'ordre 5.

3.5. Théorème de factorisation, isomorphismes

Soient G un groupe et $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. L'application $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{N}$, $g \mapsto \overline{g} = g\mathrm{N}$ est un morphisme de groupes surjectif de noyau N. En effet,

- ◇ soient g et g' dans G, alors
$$\pi(gg') = (gg')\mathrm{N} = g\mathrm{N} \cdot g'\mathrm{N} = \pi(g) \cdot \pi(g').$$
- ◇ Tout $g\mathrm{N}$ dans G/N s'écrit $\pi(g)$.
- ◇ Soit g appartenant à $\ker \pi$; alors $\pi(g) = \mathrm{N}$, *i.e.* $g\mathrm{N} = \mathrm{N}$. Or le Théorème 1.6.2 assure que $g\mathrm{N} = \mathrm{N}$ si et seulement si g appartient à N. Par suite g est un élément de N et $\ker \pi \subset \mathrm{N}$.

  Soit g un élément de N, alors $g\mathrm{N} = \mathrm{N}$ (Théorème 1.6.2) c'est-à-dire $\pi(g) = \mathrm{N}$ ou encore g appartient à $\ker \pi$. Il en résulte que $\mathrm{N} \subset \ker \pi$.

Ainsi, la structure de groupe sur G se projette sur G/N. Si $\varphi\colon \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes, la question se pose de savoir s'il se factorise en une application $\bar{\varphi}\colon \mathrm{G}/\mathrm{N} \to \mathrm{G}'$? Si oui, cette application est-elle un morphisme de groupes ?

Si on interprète le théorème de factorisation (Théorème 1.1.1) dans notre situation, on comprend que φ se factorise si et seulement si : $g' \mathcal{R} g \Longrightarrow \varphi(g) = \varphi(g')$. Ce qui dans notre cas se réécrit $g'g^{-1} \in \mathrm{N} \Longrightarrow \varphi(g'g^{-1}) = e_{\mathrm{G}}$, soit encore $g'g^{-1} \in \mathrm{N} \Longrightarrow g'g^{-1} \in \ker \varphi$. Condition réalisée si et seulement si $\mathrm{N} \subset \ker \varphi$.

Sous cette condition le morphisme φ se factorise en $\bar{\varphi}\colon \mathrm{G}/\mathrm{N} \to \mathrm{G}'$ avec $\bar{\varphi}(g\mathrm{N}) = \varphi(g)$. De plus nous avons
$$\bar{\varphi}(g\mathrm{N} \cdot g'\mathrm{N}) = \bar{\varphi}(gg'\mathrm{N}) = \varphi(gg') = \varphi(g)\varphi(g') = \bar{\varphi}(g\mathrm{N})\bar{\varphi}(g'\mathrm{N});$$
i.e. $\bar{\varphi}$ est un morphisme de groupes. Ainsi nous pouvons énoncer

Théorème 3.5.1: Théorème de factorisation

Soient G et G′ deux groupes. Soit $\varphi\colon \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes. Soit $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. Supposons que $\mathrm{N} \subset \ker\varphi$. Nous pouvons définir un morphisme $\overline{\varphi}\colon {}^{\mathrm{G}}\!/_{\mathrm{N}} \to \mathrm{G}'$ tel que $\overline{\varphi} \circ \pi = \varphi$ où π est la projection de G sur ${}^{\mathrm{G}}\!/_{\mathrm{N}}$. De plus, nous avons l'égalité : $\operatorname{im}\varphi = \operatorname{im}\overline{\varphi}$. Nous disons que φ *passe au quotient*.
Cet énoncé se symbolise par le schéma commutatif suivant :

$$\begin{tikzcd} \mathrm{G} \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \mathrm{G}' \\ {}^{\mathrm{G}}\!/_{\mathrm{N}} \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

Théorème 3.5.2: Premier théorème d'isomorphisme

Soient G et G′ deux groupes. Soit $\varphi\colon \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes. Alors ${}^{\mathrm{G}}\!/_{\ker\varphi}$ et $\operatorname{im}\varphi$ sont isomorphes.

Démonstration du Théorème 3.5.2. — Il suffit d'appliquer le théorème de factorisation au cas où $\mathrm{N} = \ker\varphi$ et de restreindre l'ensemble d'arrivée. □

Exemple 3.5.1. — Considérons la fonction $f\colon \mathbb{Z} \to \mathbb{C}^*$, $n \mapsto \mathbf{i}^n$. La formule $\mathbf{i}^{n+n'} = \mathbf{i}^n\mathbf{i}^{n'}$ valable pour tous n, n' dans $\mathbb{Z}$ assure que f est un morphisme de groupes. L'image de f est le groupe $\{1, \mathbf{i}, -1, -\mathbf{i}\} = \langle \mathbf{i} \rangle$; le noyau de f est

$$\ker f = \{n \in \mathbb{Z} \mid f(n) = 1\} = \{n \in \mathbb{Z} \mid \mathbf{i}^n = 1\} = \{n \in \mathbb{Z} \mid n = 4k,\ k \in \mathbb{Z}\} = 4\mathbb{Z}.$$

Le premier théorème d'isomorphisme (Théorème 3.5.2) assure que ${}^{\mathbb{Z}}\!/_{4\mathbb{Z}} \simeq \langle \mathbf{i} \rangle$ (via $a \bmod 4 \mapsto \mathbf{i}^a$).

Exemple 3.5.2. — Considérons la fonction

$$f\colon \mathbb{Z} \to \mathrm{U}(7), \qquad n \mapsto 2^n \bmod 7.$$

Puisque $2^{n+n'} = 2^n 2^{n'}$ pour tous n, n' dans $\mathbb{Z}$, f est un morphisme de groupes. L'image de f est $\{1, 2 \bmod 7, 4 \bmod 7\} = \langle 2 \bmod 7 \rangle$ car $2 \bmod 7$ est d'ordre 3. Le noyau de f est

$$\ker f = \{n \in \mathbb{Z} \mid f(n) = 1\} = 3\mathbb{Z}$$

car $2 \bmod 7$ est d'ordre 3. Le premier théorème d'isomorphisme (Théorème 3.5.2) assure que ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$ et $\langle 2 \bmod 7 \rangle$ sont isomorphes (via $a \bmod 3 \mapsto 2^a \bmod 7$).

Exemple 3.5.3. — Considérons la fonction

$$f\colon \mathbb{Z} \to \mathrm{U}(7), \qquad n \mapsto 3^n \bmod 7.$$

Comme $3^{n+n'} \equiv 3^n 3^{n'} \bmod 7$ pour tous n, n' dans $\mathbb{Z}$, f est un morphisme de groupes. L'image de f est $\mathrm{U}(7)$ car $\mathrm{U}(7) = \langle 3 \bmod 7 \rangle$. Le noyau de f est $6\mathbb{Z}$ car $3 \bmod 7$ est d'ordre 6 dans $\mathrm{U}(7)$. Le premier théorème d'isomorphisme (Théorème 3.5.2) assure que $\mathbb{Z}/6\mathbb{Z} \simeq \mathrm{U}(7)$ (via $a \bmod 6 \mapsto 3^a \bmod 7$).

Exemple 3.5.4. — La fonction $\det\colon \mathrm{GL}(n,\mathbb{R}) \to \mathbb{R}^*$, $A \mapsto \det A$ est un morphisme de groupes. D'une part $\ker\det = \{A \in \mathrm{GL}(n,\mathbb{R}) \mid \det A = 1\} = \mathrm{SL}(n,\mathbb{R})$, d'autre part det est surjective : soit λ un réel non nul, alors $\det \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ 0 & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix} = \lambda$. Le théorème de factorisation assure donc que $\mathrm{GL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{R}) \simeq \mathbb{R}^*$.

Le premier théorème d'isomorphisme (Théorème 3.5.2) assure que $\mathrm{GL}(n,\mathbb{R})/\mathrm{SL}(n,\mathbb{R}) \simeq \mathbb{R}^*$ via $A\mathrm{SL}(n,\mathbb{R}) \mapsto \det A$.

De manière analogue nous obtenons que $\mathrm{GL}\left(2, \mathbb{Z}/m\mathbb{Z}\right)/\mathrm{SL}\left(2, \mathbb{Z}/m\mathbb{Z}\right)$ et $\mathrm{U}(m)$ sont isomorphes.

Exemple 3.5.5. — La fonction

$$f\colon \mathbb{R} \to \mathbb{S}^1, \qquad x \mapsto \cos(x) + \mathbf{i}\sin(x)$$

est un morphisme de groupes surjectif (*i.e.* $\operatorname{im} f = \mathbb{S}^1$) et $\ker f = 2\pi\mathbb{Z}$. Le premier théorème d'isomorphisme (Théorème 3.5.2) assure que $\mathbb{R}/2\pi\mathbb{Z}$ et $\mathbb{S}^1$ sont isomorphes.

Voici deux façons d'interpréter le premier théorème d'isomorphisme (Théorème 3.5.2) :

- ◇ le quotient de G par le noyau d'un morphisme de groupes $f\colon \mathrm{G} \to \mathrm{H}$ est isomorphe à l'image de f : $\mathrm{G}/\ker f \simeq \operatorname{im} f$;
- ◇ montrer qu'un groupe quotient G/N est isomorphe à un groupe $\widetilde{\mathrm{G}}$ revient à déterminer un morphisme de groupes $f\colon \mathrm{G} \to \widetilde{\mathrm{G}}$ tel que $\begin{cases} f \text{ soit surjectif} \\ \ker f = \mathrm{N} \end{cases}$

Enfin nous définissons une suite exacte

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1;$$

dans cette écriture N, G et H sont des groupes, i, p des morphismes et $\begin{cases} i \text{ est injectif} \\ p \text{ est surjectif} \\ \operatorname{im} i = \ker p \end{cases}$

Dans ces conditions on a $i(\mathrm{N})$ qui est isomorphe à N et qui est un sous-groupe distingué de G, en outre ${}^{\mathrm{G}}\!/_{i(\mathrm{N})}$ est isomorphe à H.

Lorsque les groupes sont abéliens et notés additivement nous écrivons les suites exactes comme suit :

$$0 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 0.$$

Exemple 3.5.6. — Étudions le groupe $\mathfrak{S}_3$ qui compte six éléments

$$\mathrm{id}, \qquad \tau_c = (a\ \ b), \qquad \tau_b = (a\ \ c), \qquad \tau_a = (b\ \ c), \qquad \sigma = (a\ \ b\ \ c), \qquad \sigma^2 = \sigma^{-1} = (a\ \ c\ \ b).$$

Le groupe $\mathfrak{S}_3$ contient un sous-groupe distingué d'ordre 3, $\langle\sigma\rangle = \{\mathrm{id}, \sigma, \sigma^2\} = \mathcal{A}_3$ isomorphe à ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$ et nous avons une suite exacte

$$1 \longrightarrow \mathcal{A}_3 \simeq {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \xrightarrow{i} \mathfrak{S}_3 \xrightarrow{p} {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} = \{-1, 1\} \longrightarrow 1.$$

où

- $i\colon {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \simeq \mathcal{A}_3 \to \mathfrak{S}_3$ désigne l'inclusion,
- $\varepsilon\colon \mathfrak{S}_3 \to {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} = \{-1, 1\}$ désigne la signature.

Le groupe $\mathcal{A}_3$ est un sous-groupe distingué de $\mathfrak{S}_3$ et ${}^{\mathfrak{S}_3}\!/_{\mathcal{A}_3} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.

Définition 3.5.1

Un groupe $\mathrm{G} \neq \{e\}$ est *simple* si ses seuls sous-groupes distingués sont $\{e\}$ et G.

Exemples 3.5.7. — 1. Le groupe ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ est simple si et seulement si p est premier.

2. Le groupe alterné $\mathcal{A}_n$ est simple dès que $n \geq 5$.

L'intérêt des sous-groupes distingués est de permettre le « dévissage » des groupes : si G est un groupe et si $\mathrm{H} \triangleleft \mathrm{G}$ est un sous-groupe distingué de G, nous pouvons essayer de ramener l'étude de G à l'étude de H et ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ (si G est fini, les groupes H et ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ sont d'ordre plus petit que G). Les groupes simples sont eux indévissables d'où l'intérêt particulier qu'on leur porte : la classification des groupes finis simples a été achevée en 1981 !

Les groupes classiques fourniront beaucoup d'exemples de groupes simples.

3.6. Produits semi-directs

3.6.1. Produits semi-directs. — Lorsque H et K sont des sous-groupes d'un groupe G, le produit HK peut ne pas être un sous-groupe de G. Par exemple, si on considère les deux sous-groupes $\mathrm{H} = \langle(1\ 2)\rangle$ et $\mathrm{K} = \langle(1\ 3)\rangle$ de $\mathfrak{S}_3$, alors $\mathrm{HK} = \big\{\mathrm{id}, (1\ 2), (1\ 3), (1\ 3\ 2)\big\}$ a pour cardinal 4 et 4 ne divise pas $|\mathfrak{S}_3| = 6$.

Néanmoins, si H ou K est un sous-groupe distingué de G, alors HK est un sous-groupe de G. On rappelle, voir Définition 1.6.1, que H est distingué dans G si pour tout $g \in \mathrm{G}$ on a $g\mathrm{H} = \mathrm{H}g$

Supposons par exemple que H soit distingué dans G, alors

$$(hk)(h'k') = (hkh'k^{-1})(kk') \in \mathrm{HK}, \qquad (hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1} \in \mathrm{HK} \tag{3.6.1}$$

puisque $kh'k^{-1} \in \mathrm{H}$ et $k^{-1}hk \in \mathrm{H}$. Ceci inclut les Exemples 2.3.1, 2.3.2 et 2.3.3 Remarquons que dans $\mathrm{H} \times \mathrm{K}$, les copies standards de H et K sont toutes deux des sous-groupes distingués de $\mathrm{H} \times \mathrm{K}$; en effet H (resp. K) est le noyau du morphisme de projection $\mathrm{H} \times \mathrm{K} \to \mathrm{K}$ (resp. $\mathrm{H} \times \mathrm{K} \to \mathrm{H}$), et on verra que le noyau d'un morphisme est toujours distingué (Proposition 3.2.1).

Considérons maintenant deux groupes arbitraires H et K qui ne sont a priori pas des sous-groupes d'un groupe G. Supposons que nous ayons un morphisme $\varphi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$. Désignons par φ_k l'automorphisme de H associé à k ; alors $\varphi_k\colon \mathrm{H} \to \mathrm{H}$ est une bijection et $\varphi_k(hh') = \varphi_k(h)\varphi_k(h')$ pour tous h, $h' \in \mathrm{H}$. Le fait que φ soit un morphisme de K dans Aut(H) signifie

$$\varphi_{k_1} \circ \varphi_{k_2} = \varphi_{k_1k_2}, \qquad \varphi_e = \mathrm{id}_{\mathrm{H}}X$$

pour tous k_1, $k_2 \in \mathrm{K}$. En particulier, $\varphi_k \circ \varphi_{k^{-1}} = \varphi_e = \mathrm{id}_{\mathrm{H}}$, donc

$$\varphi_k^{-1} = \varphi_{k^{-1}}. \tag{3.6.2}$$

Autrement dit, l'inverse de $\varphi_k \in \mathrm{Aut}(\mathrm{H})$ est $\varphi_{k^{-1}}$. On peut par exemple prendre $\varphi_k = \mathrm{id}_{\mathrm{H}}$ pour tout $k \in \mathrm{K}$. Mais nous sommes davantage intéressés par des cas où le morphisme $\varphi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$ n'est pas trivial ; néanmoins il arrive que ce soit le seul choix, par exemple si H et K sont finis avec $\mathrm{pgcd}(|\mathrm{K}|, |\mathrm{Aut}(\mathrm{H})|) = 1$.

Dans les Exemples 2.3.1, 2.3.2, 2.3.3, on peut pour tout $k \in \mathrm{K}$ considérer $\varphi_k\colon h \mapsto khk^{-1}$, qui est un automorphisme de H puisque dans ces cas K est un sous-groupe distingué de G.

Définition 3.6.1

Soient H et K deux groupes. Soit $\varphi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$ un morphisme de groupes (une action de K sur H par automorphismes), le produit semi-direct correspondant $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est défini comme suit :

- ◇ en tant qu'ensemble c'est $\mathrm{H} \times \mathrm{K} = \{(h,k) \mid h \in \mathrm{H},\ k \in \mathrm{K}\}$;
- ◇ la loi de groupe sur $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est

$$(h,k)(h',k') = (h\varphi_k(h'), kk').$$

Cette opération de groupe s'inspire de la première formule de (3.6.1), $\varphi_k(h')$ étant une version abstraite de $kh'k^{-1}$. Dans notre notation de produit semi-direct, $\mathrm{H} \rtimes_\varphi \mathrm{K}$, le groupe sur lequel on agit est toujours en premier et le groupe qui agit est en second.

Il faut vérifier que la Définition 3.6.1 a un sens : $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est vraiment un groupe. L'élément neutre est (e,e) :

$$(h,k)(e,e) = (h\varphi_k(e), ke) = (h,k), \qquad (e,e)(h,k) = (e\varphi_e(h), ek) = (h,k)$$

où $\varphi_k(e) = e$ et $\varphi_e = \mathrm{id}_{\mathrm{H}}$ puisque les morphismes préservent les éléments neutres. Soit (h, k) dans $\mathrm{H} \rtimes_\varphi \mathrm{K}$; alors $(\varphi_{k^{-1}}(h^{-1}), k^{-1})$ est son inverse. En effet, d'une part

$$(h,k)\big((\varphi_{k^{-1}}(h))^{-1}, k^{-1}\big) = (h\varphi_k(\varphi_{k^{-1}}(h^{-1})), kk^{-1}) = (hh^{-1}, e) = (e, e)$$

d'autre part

$$(\varphi_{k^{-1}}(h^{-1}), k^{-1})(h,k) = (\varphi_{k^{-1}}(h^{-1})\varphi_{k^{-1}}(h), k^{-1}k) = (\varphi_{k^{-1}}(hh^{-1}), e) = (\varphi_{k^{-1}}(e), e) = (e, e).$$

Enfin on peut vérifier que cette opération est associative.

Exemple 3.6.1. — Si $\varphi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$ est le morphisme trivial, alors $\varphi_k = \mathrm{id}_{\mathrm{H}}$ pour tout $k \in \mathrm{K}$ et la loi de groupe sur $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est le produit direct : $(h,k)(h',k') = (h\varphi_k(h'), kk') = (hh', kk')$. Nous verrons qu'un produit semi-direct est un produit direct (de manière naturelle) seulement lorsque φ est l'action triviale de K sur H (Théorème 3.6.2).

Exemple 3.6.2. — Considérons les groupes $\mathrm{H} = \mathbb{R}$, $\mathrm{K} = \mathbb{R}^\times$ et le morphisme $\varphi\colon \mathbb{R}^\times \to \mathrm{Aut}(\mathbb{R})$ défini par : $\varphi_x\colon \mathbb{R},\ y \mapsto xy$. Notons que

- ◇ φ_x est un automorphisme de $\mathbb{R}$ en tant que groupe additif
- ◇ et $\varphi_x \circ \varphi_{x'} = \varphi_{xx'}$ puisque $x(x'y) = (xx')y$ pour tout $y \in \mathbb{R}$.

L'opération du groupe $\mathbb{R} \rtimes_\varphi \mathbb{R}^\times$ est

$$(a,b)(a',b') = (a + \varphi_b(a'), bb') = (a + ba', bb').$$

Cette opération ressemble à la multiplication dans $\mathrm{Aff}(\mathbb{R})$:

$$\begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} b' & a' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} bb' & ba' + a \\ 0 & 1 \end{pmatrix}.$$

Les groupes $\mathbb{R} \rtimes_\varphi \mathbb{R}^\times$ et $\mathrm{Aff}(\mathbb{R})$ sont isomorphes via

$$\mathbb{R} \rtimes_\varphi \mathbb{R}^\times \to \mathrm{Aff}(\mathbb{R}), \qquad (a,b) \mapsto \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}.$$

Exemple 3.6.3. — Reprenons l'exemple précédent en remplaçant $\mathbb{R}$ par $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{R}^\times$ par $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times$. Les automorphismes du groupe additif $\mathbb{Z}/m\mathbb{Z}$ sont les applications $\varphi_a\colon x \bmod m \mapsto ax \bmod m$ pour $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Par suite $\mathrm{Aut}\left(\mathbb{Z}/m\mathbb{Z}\right) \simeq \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$. Considérons $\varphi\colon \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \to \mathrm{Aut}\left(\mathbb{Z}/m\mathbb{Z}\right)$ défini par

$$a \mapsto \varphi_a\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \qquad x \bmod m \mapsto ax \bmod m.$$

La loi du produit semi-direct $\mathbb{Z}/m\mathbb{Z} \rtimes_\varphi \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ est

$$(a,b)(a',b') = (a + ba', b + b').$$

Le produit semi-direct $\mathbb{Z}/m\mathbb{Z} \rtimes_\varphi \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ est isomorphe à $\mathrm{Aff}\left(\mathbb{Z}/m\mathbb{Z}\right)$ via

$$\mathbb{Z}/m\mathbb{Z} \rtimes_\varphi \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \to \mathrm{Aff}\left(\mathbb{Z}/m\mathbb{Z}\right), \qquad (a,b) \bmod m \mapsto \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} \bmod m.$$

Exemple 3.6.4. — Le morphisme $\mathbb{Z} \to \{\pm 1\}$ donné par $n \mapsto (-1)^n$ conduit au produit semi-direct $\mathbb{Z} \rtimes_\varphi \mathbb{R}$, la loi étant

$$(m,n)(m',n') = (m + (-1)^n m', n + n').$$

Montrons, comme annoncé dans l'Exemple 3.6.1 que $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est un produit direct seulement lorsque φ est l'action triviale de K sur H (Théorème 3.6.2) :

Théorème 3.6.1

Le groupe G est isomorphe à un produit semi-direct si et seulement si il possède deux sous-groupes H et K tels que H est distingué dans G, $\mathrm{HK} = \mathrm{G}$ et $\mathrm{H} \cap \mathrm{K} = \{e\}$. On a alors $\mathrm{G} \simeq \mathrm{H} \rtimes_\varphi \mathrm{K}$ avec $\varphi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$, $k \mapsto \varphi_k$ où φ_k est l'automorphisme intérieur associé à k.
Le produit semi-direct $\widetilde{\mathrm{H}} \rtimes_\varphi \widetilde{\mathrm{K}}$ est direct si et seulement si $\varphi\colon \widetilde{\mathrm{K}} \to \mathrm{Aut}(\widetilde{\mathrm{H}})$ est trivial, c'est-à-dire $\varphi_k = \mathrm{id}_{\widetilde{\mathrm{H}}}$ pour tout $k \in \widetilde{\mathrm{K}}$.
En particulier, si G est abélien alors φ est trivial.

Remarque 3.6.1. — Si on considère le produit semi-direct $\mathrm{H} \rtimes_\varphi \mathrm{K}$, pour tout sous-groupe K' de K, alors l'application restreinte $\varphi\colon \mathrm{K}' \to \mathrm{Aut}(\mathrm{H})$ reste un morphisme de groupes ; on peut donc considérer le produit semi-direct $\mathrm{H} \rtimes_\varphi \mathrm{K}'$ qui est un sous-groupe de $\mathrm{H} \rtimes_\varphi \mathrm{K}$.

Par contre, si H' est un sous-groupe de H, le produit semi-direct $\cancel{\mathrm{H}' \rtimes_\varphi \mathrm{K}}$ n'est pas forcément défini.

Il n'est défini que si $\varphi(\mathrm{K}) \subset \mathrm{Aut}(\mathrm{H}')$. C'est le cas par exemple si $\mathrm{H}' = \{e_\mathrm{H}\}$.

Démonstration. — Comme dans la démonstration du Théorème 2.3.1 on définit $\mathrm{H} = f(\widetilde{\mathrm{H}} \rtimes_\psi \{e_{\widetilde{\mathrm{K}}}\})$ et $\mathrm{K} = f(\{e_{\widetilde{\mathrm{H}}}\} \rtimes_\psi \widetilde{\mathrm{K}})$ où $f\colon \widetilde{\mathrm{H}} \rtimes_\psi \widetilde{\mathrm{K}} \to \mathrm{G}$ désigne un isomorphisme. D'après la Remarque 3.6.1, $\widetilde{\mathrm{H}} \rtimes_\psi \{e_{\widetilde{\mathrm{K}}}\}$ et $\{e_{\widetilde{\mathrm{H}}}\} \rtimes_\psi \widetilde{\mathrm{K}}$ sont deux sous-groupes de $\widetilde{\mathrm{H}} \rtimes_\psi \widetilde{\mathrm{K}}$, leurs images par le morphisme f sont donc deux sous-groupes de G.

Soit $g \in \widetilde{\mathrm{H}} \cap \widetilde{\mathrm{K}}$; il existe h dans $\widetilde{\mathrm{H}}$ et k dans $\widetilde{\mathrm{K}}$ tels que $g = f(h, e_{\widetilde{\mathrm{K}}}) = f(e_{\widetilde{\mathrm{H}}}, k)$. Comme f est un isomoprhisme on a $h = e_{\widetilde{\mathrm{H}}}$ et $g = f(e_{\widetilde{\mathrm{H}}}, e_{\widetilde{\mathrm{K}}}) = e_\mathrm{G}$. L'intersection est donc bien réduite à l'élément neutre.

Étant donné $g \in \mathrm{G}$, il existe $(h,k) \in \widetilde{\mathrm{H}} \times \widetilde{\mathrm{K}}$ tels que $g = f(h,k)$. On a

$$(h, e_\mathrm{K})(e_\mathrm{H}, k) = (h\psi_{e_\mathrm{K}}(e_\mathrm{H}), k) = (h, k)\,;$$

ainsi $g = f(h,k) = f\left[(h, e_\mathrm{K})(e_\mathrm{H}, k)\right] = f(h, e_\mathrm{K}) f(e_\mathrm{H}, k) \in \mathrm{HK}$. On en déduit que $\mathrm{G} \subset \mathrm{HK}$. L'inclusion inverse étant naturellement vérifiée, on conclut que $\mathrm{G} = \mathrm{HK}$.

Montrons que H est distingué dans G. Soient $g \in \mathrm{G}$ et $\ell \in \mathrm{H}$, il existe $(h,k) \in \widetilde{\mathrm{H}} \times \widetilde{\mathrm{K}}$ et $h' \in \widetilde{\mathrm{H}}$ tels que $g = f(h,k)$ et $\ell = f(h', e_{\widetilde{\mathrm{K}}})$. On rappelle que $(h,k)^{-1} = (\psi_k^{-1}(h^{-1}), k^{-1})$. On a :

$$\begin{aligned}
(h,k)(h', e_{\widetilde{\mathrm{K}}})(h,k)^{-1} &= (h,k)(h', e_{\widetilde{\mathrm{K}}})(\psi_k^{-1}(h^{-1}), k^{-1}) \\
&= (h,k)(h'\psi_k^{-1}(h^{-1}), k^{-1}) \\
&= (h\psi_k(h'\psi_k^{-1}(h^{-1})), e_{\widetilde{\mathrm{K}}}) \\
&= (h\psi_k(h')h^{-1}, e_{\widetilde{\mathrm{K}}})
\end{aligned}$$

Comme $\psi_k \in \mathrm{Aut}(\widetilde{\mathrm{H}})$, on a $\psi_k(h') \in \widetilde{\mathrm{H}}$ et $h\psi_k(h')h^{-1} \in \widetilde{\mathrm{H}}$, alors $(h\psi_k(h')h^{-1}, e_{\widetilde{\mathrm{K}}}) \in \widetilde{\mathrm{H}} \times \{e_{\widetilde{\mathrm{K}}}\}$.

On en déduit que

$$g\ell g^{-1} = f(h,k)f(h', e_{\widetilde{\mathrm{K}}})f(h,k)^{-1} = f\left[(h,k)(h', e_{\widetilde{\mathrm{K}}})(h,k)^{-1}\right] = f\left[h\psi_k(h')h^{-1}, e_{\widetilde{\mathrm{K}}}\right] \in \mathrm{H}.$$

Le sous-groupe H est distingué dans G.

Vérifions que G est isomorphe au produit semi-direct $\mathrm{H} \rtimes_\varphi \mathrm{K}$ où, pour tout $k \in \mathrm{K}$, φ_k désigne l'automorphisme intérieur associé à k.

Comme H est distingué dans G, pour tout $k \in \mathrm{K}$ l'automophisme intérieur $\varphi_k : h \mapsto khk^{-1}$ est un élément de $\mathrm{Aut}(\mathrm{H})$; il en résulte que le produit direct $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est bien défini. Considérons l'application $f\colon \mathrm{H} \rtimes_\varphi \mathrm{K} \to \mathrm{G}$, $(h,k) \mapsto hk$.

On a

$$f\left[(h,k)(h',k')\right] = f\left[(hkh'k^{-1}, kk')\right] = hkh'k^{-1}kk' = hkh'k' = f(h,k)f(h',k');$$

autrement dit f est un morphisme de groupes.

Si $(h,k) \in \ker f$ alors $f(h,k) = hk = e$. Ainsi $h = k^{-1}$ est un élément de $\mathrm{H} \cap \mathrm{K}$; or $\mathrm{H} \cap \mathrm{K} = \{e\}$ donc $h = k = e$ et f est injective.

Enfin, puisque $\mathrm{HK} = \mathrm{G}$, le morphisme f est surjectif ; finalement f est un isomorphisme.

Il reste à montrer que le produit semi-direct $\widetilde{\mathrm{H}} \rtimes_\varphi \widetilde{\mathrm{K}}$ est direct si et seulement si le morphisme φ est trivial. Si le morphisme est trivial alors pour (h,k) et (h',k') dans $\widetilde{\mathrm{H}} \rtimes_\varphi \widetilde{\mathrm{K}}$ on a

$$(h,k)(h',k') = (h\varphi_k(h'), kk') = (hh', kk')$$

ce qui correspond bien au produit direct.

Supposons que le produit soit direct. Alors pour tout (h,k) et (h',k') nous avons d'une part $(h,k)(h'k') = (hh', kk')$ par produit direct et d'autre part $(h,k)(h',k') = (h\varphi_k(h'), kk')$ par produit semi-direct. Nous avons donc $hh' = h\varphi_k(h')$ et $h' = \varphi_k(h')$. Ceci étant vrai pour tout h', on obtient que $\varphi_k = \mathrm{id}$, et comme c'est aussi vrai pour tout k, on déduit que φ est trivial.

Vérifions que $\widetilde{\mathrm{H}}$ est distingué dans G, c'est-à-dire que $g\widetilde{\mathrm{H}} = \widetilde{\mathrm{H}}g$ pour tout $g \in \mathrm{G}$. Soient $f(h', e_{\mathrm{K}}) \in \widetilde{\mathrm{H}}$ et $f(h,k) \in \mathrm{G}$. On a

$$\begin{aligned} f(h,k)f(h',e_{\mathrm{K}}) &= f\left[(h,k)(h',e_{\mathrm{K}})\right] \\ &= f(h\varphi_k(h'),k) \\ &= f(h\varphi_k(h')h^{-1}h,k) \\ &= f\left[(h\varphi_k(h')h^{-1},e_{\mathrm{K}})(h,k)\right] \\ &= f(h\varphi_k(h')h^{-1},e_{\mathrm{K}})f(h,k)\cdot \end{aligned}$$

Or $\varphi_k(h') \in \mathrm{H}$ car $\varphi_k \in \mathrm{Aut(H)}$ donc $h\varphi_k(h')h^{-1} \in \mathrm{H}$ et $f(h\varphi_k(h')h^{-1}, e_{\mathrm{K}}) \in \widetilde{\mathrm{H}}$. On en déduit que $f(h\varphi_k(h')h^{-1}, e_{\mathrm{K}})f(h,k) = f(h\varphi_k(h')h^{-1}, e_{\mathrm{K}})g \in \widetilde{\mathrm{H}}g$. Ainsi $g\widetilde{\mathrm{H}} \subset \widetilde{\mathrm{H}}g$. On montre l'inclusion inverse de même, ce qui prouve l'égalité entre les deux ensembles et le caractère distingué de $\widetilde{\mathrm{H}}$.

Réciproquement, supposons que $\widetilde{\mathrm{H}}$ est distingué dans $\widetilde{\mathrm{G}}$, que $\widetilde{\mathrm{H}}\widetilde{\mathrm{K}} = \widetilde{\mathrm{G}}$ et que $\widetilde{\mathrm{H}} \cap \widetilde{\mathrm{K}} = \{e_{\mathrm{G}}\}$. Soit $k \in \widetilde{\mathrm{K}}$, on note $\varphi_k \colon \widetilde{\mathrm{H}} \to \widetilde{\mathrm{H}}$, $h \mapsto k^{-1}hk$. C'est un automorphisme intérieur qui laisse $\widetilde{\mathrm{H}}$ invariant puisque ce sous-groupe est distingué dans G.

Vérifions que $f \colon \widetilde{\mathrm{H}} \rtimes_{\varphi} \widetilde{\mathrm{K}} \to \widetilde{\mathrm{G}}$, $(h,k) \mapsto hk$ est un isomorphisme de groupes. Soient (h,k) et (h',k') deux éléments de $\widetilde{\mathrm{H}} \rtimes_{\varphi} \widetilde{\mathrm{K}}$ on a :

$$f(h,k)f(h',k') = hkh'k' = hkh'k^{-1}kk' = h\varphi_k(h')kk' = f((h,k)(h',k'))\cdot$$

Ce morphisme est surjectif puisque $\widetilde{\mathrm{H}}\widetilde{\mathrm{K}} = \mathrm{G}$. Il reste à prouver qu'il est injectif, *i.e.* que son noyau est réduit à e_{G}.

Si $f(h,k) = e_{\mathrm{G}}$ alors $hk = e_{\mathrm{G}}$ et $h = k^{-1}$; par suite $h \in \widetilde{\mathrm{H}} \cap \widetilde{\mathrm{K}}$. Comme cette intersection est réduite à l'élément neutre, on obtient que $h = k = e_{\mathrm{G}}$ et donc que f est injectif. Si le produit

est direct alors $\widetilde{\mathrm{K}}$ est lui-aussi distingué dans G et d'après le Théorème 3.6.2 on a $hk = kh$ pour tout $(h,k) \in \widetilde{\mathrm{H}} \times \widetilde{\mathrm{K}}$. Par conséquent l'automorphisme intérieur est trivial.

Réciproquement, si l'automorphisme intérieur φ_k est trivial pour tout $k \in \widetilde{\mathrm{K}}$ cela signifie que $khk^{-1} = h$ pour tout $(h,k) \in \widetilde{\mathrm{H}} \times \widetilde{\mathrm{K}}$, c'est-à-dire que $kh = hk$. Le Théorème 3.6.2 assure alors que le produit est direct. $\square$

Théorème 3.6.2

Dans le produit semi-direct $\mathrm{G} = \mathrm{H} \rtimes_\varphi \mathrm{K}$, nous considérons $\widetilde{\mathrm{H}} = \{(h,e) \,|\, h \in \mathrm{H}\}$ et $\widetilde{\mathrm{K}} = \{(e,k) \,|\, k \in \mathrm{K}\}$. Nous avons

$$\mathrm{H} \simeq \widetilde{\mathrm{H}} \text{ via } h \mapsto (h,e), \qquad \mathrm{K} \simeq \widetilde{\mathrm{K}} \text{ via } k \mapsto (e,k),$$

L'ensemble $\widetilde{\mathrm{H}}$ est un sous-groupe distingué dans G.
Le produit est direct si et seulement si $\varphi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$ est trivial, c'est-à-dire $\varphi_k = \mathrm{id}_\mathrm{H}$ pour tout $k \in \mathrm{K}$.
En particulier, si G est abélien alors φ est trivial.

La formule $(h,k) = (h,e)(e,k) = (e,k)(\varphi_k^{-1}(h),e)$ dans l'énoncé semble moins « étrange » si H et K sont des sous-groupes d'un même groupe : nous pouvons alors écrire $hk = k(k^{-1}hk)$. Le terme $k^{-1}hk$ entre parenthèses est l'action par conjugaison de k^{-1} sur h et correspond à $(\varphi_{k^{-1}}(h),e) = (\varphi_k^{-1}(h),e)$.

Ainsi $\mathrm{H} \rtimes_\varphi \mathrm{K}$ n'est pas abélien si φ n'est pas trivial. En particulier, même si H et K sont tous deux abéliens et $\varphi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$ non trivial, alors $\mathrm{H} \rtimes_\varphi \mathrm{K}$ n'est pas un groupe abélien.

Démonstration. — Les applications

$$\mathrm{H} \to \mathrm{H} \rtimes_\varphi \mathrm{K},\ \ h \mapsto (h,e) \qquad \text{et} \qquad \mathrm{K} \to \mathrm{H} \rtimes_\varphi \mathrm{K},\ \ k \mapsto (e,k)$$

sont des morphismes de groupes. On a en effet

$$(h,e)(h',e) = (h\varphi_e(h'),e) = (hh',e) \qquad \text{et} \qquad (e,k)(e,k') = (e\varphi_k(e),kk') = (e,kk')\cdot$$

Tous deux sont injectifs puisque d'après :

$$(h,e) = (e,e) \iff h = e \qquad \text{et} \qquad (e,k) = (e,e) \iff k = e,$$

leurs noyaux sont réduits à l'élément neutre. On en déduit que $\widetilde{\mathrm{H}} \simeq \mathrm{H}$ et $\widetilde{\mathrm{K}} \simeq \mathrm{K}$.

Soit $(h,k) \in \mathrm{H} \rtimes_\varphi \mathrm{K}$, nous avons

$$(h,e)(e,k) = (h\varphi_e(e), e\cdot k) = (h,k)$$

et

$$(e,k)(\varphi_k(h),e) = (e\cdot\varphi_k(\varphi_k^{-1}(h)), k\cdot e) = (h,k).$$

Puisque

- ◇ chaque élément de $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est construit à partir de $\widetilde{\mathrm{H}}$ et $\widetilde{\mathrm{K}}$ (c'est-à-dire $(h,k) = (h,e)(e,k)$) ;
- ◇ l'action par conjugaison de $\widetilde{\mathrm{H}}$ laisse $\widetilde{\mathrm{H}}$ invariant.

pour montrer que $\widetilde{\mathrm{H}}$ est un sous-groupe distingué de $\mathrm{H} \rtimes_\varphi \mathrm{K}$, il suffit de montrer que l'action par conjugaison de $\widetilde{\mathrm{K}}$ laisse $\widetilde{\mathrm{H}}$ invariant, Soient $(e,k) \in \widetilde{\mathrm{K}}$ et $(h,e) \in \widetilde{\mathrm{H}}$; alors

$$\begin{aligned}
(e,k)(h,e)(e,k)^{-1} &= (e,k)(h,e)(e,k^{-1}) \\
&= (e \cdot \varphi_k(h), k \cdot e)(e,k^{-1}) \\
&= (\varphi_k(h),k)(e,k^{-1}) \\
&= (\varphi_k(h) \cdot \varphi_k(e), kk^{-1}) \\
&= (\varphi_k(h), e).
\end{aligned}$$

Ainsi $\widetilde{\mathrm{H}}$ est distingué dans $\mathrm{H} \rtimes_\varphi \mathrm{K}$.

On a $\widetilde{\mathrm{H}}\widetilde{\mathrm{H}} = \mathrm{H} \rtimes_\varphi \mathrm{K}$, $\widetilde{\mathrm{H}} \cap \widetilde{\mathrm{K}} = \{(e,e)\}$. D'après le Théorème **??** Soient $h \in \mathrm{H}$ et $k \in \mathrm{K}$; alors

$$(h,e)(e,k) = (e,k)(h,e) \iff (h,k) = (e \cdot \varphi_k(h), k \cdot e) \iff (h,k) = (\varphi_k(h),k).$$

Par conséquent (e,k) et (h,e) commutent si et seulement si pour tous $h \in \mathrm{H}$ et tout $k \in \mathrm{K}$ nous avons $\varphi_k(h) = h$, *i.e.* si et seulement si $\ker \varphi = \mathrm{K}$. Mais $\ker \varphi = \mathrm{K}$ si et seulement si l'action $\varphi \colon \mathrm{H} \to \mathrm{Aut}(\mathrm{K})$ est triviale d'où le résultat. □

Exemple 3.6.5. — Dans l'Exemple 3.6.4, nous nous sommes intéressés au produit semi-direct non trivial $\mathbb{Z} \rtimes \mathbb{Z}$ muni de la loi $(m,n)(m',n') = (m + (-1)^n m', n + n')$. Dans ce groupe,

$$(m,n) = (m,0)(0,n) = (1,0)^m (0,1)^n,$$

donc $\mathbb{Z} \rtimes \mathbb{Z}$ est engendré par $(1,0)$ et $(0,1)$ où

$$(0,1)(1,0)(0,1)^{-1} = (-1,0) = (1,0)^{-1}.$$

Autrement dit si $x = (1,0)$ et $y = (0,1)$, le groupe $\mathbb{Z} \rtimes \mathbb{Z}$ est engendré par x et y soumis à la relation $yxy^{-1} = x^{-1}$.

***Exemple 3.6.6* (Le groupe cyclique $\mathbb{Z}/8\mathbb{Z}$).** — Le groupe cyclique $\mathbb{Z}/8\mathbb{Z}$ n'est pas de la forme $\mathrm{N} \rtimes \mathrm{H}$. En effet comme $\mathbb{Z}/8\mathbb{Z}$ est abélien, le produit serait direct. Or $\mathbb{Z}/8\mathbb{Z}$ n'est isomorphe ni à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ni à $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$ qui sont les seuls possibles.

***Exemple 3.6.7* (Le groupe diédral).** — Soit n un entier supérieur ou égal à 3. Rappelons que le groupe diédral D_{2n} d'ordre $2n$ est le sous-groupe de $\mathrm{O}(2,\mathbb{R})$ engendré par la rotation r d'angle $\frac{2\pi}{n}$ et la symétrie s autour de l'axe des abscisses dans $\mathbb{R}^2$. Autrement dit il s'agit du groupe engendré par les matrices

$$r = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} \qquad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

La rotation r engendre le groupe des rotations d'angle $\frac{2k\pi}{n}$ avec $0 \leq k \leq n-1$ et donc $\langle r \rangle \simeq \mathbb{Z}/n\mathbb{Z}$. De plus $s^2 = \mathrm{id}$ ainsi $\langle s \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

Un calcul montre que

$$srs^{-1} = srs = r^{-1}$$

et par récurrence nous obtenons

$$sr^k s^{-1} = r^{-k}.$$

Cette relation implique que tous les éléments de $\langle r,\, s\rangle$ sont de la forme r^k ou $r^k s$ (Corollaire 5.2.1). Par conséquent

$$\mathrm{D}_{2n} = \{r^k,\, r^k s \,|\, 0 \leq k \leq n-1\}.$$

ce groupe se décompose en produit semi-direct

$$\mathrm{D}_{2n} \simeq \langle r\rangle \rtimes \langle s\rangle.$$

En effet

- ◇ $\langle r\rangle \cap \langle s\rangle = \{\mathrm{id}\}$,
- ◇ tout élément de D_{2n} est le produit d'un élément de $\langle r\rangle$ par un élément de $\langle s\rangle$
- ◇ comme $sr^k s^{-1} = r^{-k}$ le sous-groupe $\langle r\rangle$ est distingué.

Nous pouvons penser à ce produit semi-direct comme suit : puisque $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien, $(gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1}$, *i.e.* l'application $g \mapsto g^{-1}$ est un isomorphisme de groupes. Ainsi l'application

$$\varphi\colon \left(\mathbb{Z}/2\mathbb{Z}, +\right) \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}, +\right)$$

donnée par

$$\varphi(0) = \mathrm{id} \qquad\qquad \varphi(1)\colon m \mapsto -m$$

est un morphisme de groupes et la description précédente montre que

$$\mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}.$$

***Exemple 3.6.8* (Le groupe diédral infini).** — Remplaçons les sommets d'un polyèdre régulier par les entiers sur l'axe réel. Pour $n \in \mathbb{Z}$ notons τ_n la translation de n ;

$$\tau_n\colon \mathbb{Z} \to \mathbb{Z}, \qquad\qquad m \mapsto m+n.$$

Pour simplifier posons $r = \tau_1$ et notons s la symétrie en 0, c'est-à-dire $s(m) = -m$. Le *groupe diédral infini* D_∞ est le sous-groupe $\langle r,\, s\rangle$ des bijections de $\mathbb{Z}$ dans lui-même.

Remarquons que $s^2 = \mathrm{id}$ et $s\tau_m s = \tau_{-m}$. Comme pour le groupe diédral nous pouvons montrer que

$$\mathrm{D}_\infty \simeq \langle r\rangle \rtimes \langle s\rangle.$$

En identifiant $\langle r\rangle$ à $(\mathbb{Z}, +)$ via l'isomorphisme $n \mapsto \tau_n = r^n$ et $\langle s\rangle$ à $\mathbb{Z}/2\mathbb{Z}$ via $i \mapsto s^i$ nous obtenons la décomposition en produit semi-direct

$$\mathrm{D}_\infty \simeq \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Exemple 3.6.9. — Soient p et q des nombres premiers avec $p < q$.

Les groupes d'ordre pq sont tous cycliques si p ne divise pas $q-1$ (c'est une application classique des théorèmes de Sylow).

Si par contre p divise $q-1$ nous avons un produit semi-direct non commutatif $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ via le fait qu'il y a des morphismes non triviaux $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}\big(\mathbb{Z}/q\mathbb{Z}\big) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.

Exemple 3.6.10. — Soit H un groupe abélien écrit additivement, donc $\mathrm{neg}\colon h \mapsto -h$ est un automorphisme d'ordre 2. Soit $\varphi\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathrm{H})$ défini par

$$\varphi_0 = \mathrm{id}_{\mathrm{H}}, \qquad\qquad \varphi_1\colon \mathrm{H} \to \mathrm{H},\ h \mapsto -h.$$

Alors φ est un morphisme [2]. L'opération de $\mathrm{H} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ est

$$(h, a \bmod 2)(h', a' \bmod 2) = (h + (-1)^a h', a + a' \bmod 2). \tag{3.6.3}$$

Alors

$$(h,0)(0,1) = (h,1) \qquad \text{et} \qquad (0,1)(h,0) = (0 + \mathrm{neg}(h), 1+0) = (-h, 1).$$

Ainsi $(h,0)$ et $(0,1)$ commutent dans $\mathrm{H} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ si et seulement si $h = -h$. Si tous les éléments de $\mathrm{H} \smallsetminus \{e\}$ sont d'ordre 2 (donc la négation sur H est l'identité) alors $\mathrm{H} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z} = \mathrm{H} \times \mathbb{Z}/2\mathbb{Z}$. Si $\mathrm{H} \smallsetminus \{e\}$ contient un élément d'ordre 2 alors $\mathrm{H} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ n'est pas abélien.

Lorsque nous considérons le cas particulier $\mathrm{H} = \mathbb{Z}/n\mathbb{Z}$, $n \geq 3$ nous retrouvons l'Exemple 3.6.7.

Théorème 3.6.3

Le sous-groupe $\{e\} \times \mathrm{K}$ du produit semi-direct $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est distingué si et seulement si $\varphi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$ est trivial, autrement dit si et seulement si $\mathrm{H} \rtimes_\varphi \mathrm{K} = \mathrm{H} \times \mathrm{K}$.

Démonstration. — Puisque $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est engendré par les sous-groupes $\mathrm{H} \times \{e\}$ et $\{e\} \times \mathrm{K}$, $\{e\} \times \mathrm{K}$ est un sous-groupe distingué de $\mathrm{H} \rtimes_\varphi \mathrm{K}$ si et seulement si $(h,e)(e,k)(h,e)^{-1} \in \{e\} \times \mathrm{K}$ pour tous $h \in \mathrm{H}$ et $k \in \mathrm{K}$. On a

$$(h,e)(e,k)(h,e)^{-1} = (h,k)(h^{-1},e) = (h\varphi_k(h^{-1}), k \cdot e) = (h\varphi_k(h)^{-1}, k),$$

qui est dans $\{e\} \times \mathrm{K}$ si et seulement si $\varphi_k(h) = h$. Donc $\{e\} \times \mathrm{K}$ est distingué dans $\mathrm{H} \rtimes_\varphi \mathrm{K}$ si et seulement si chaque φ_k est l'application d'identité sur H, ce qui signifie que φ est trivial. □

2. Lorsqu'un groupe G contient un élément g d'ordre m, l'application $\mathbb{Z}/m\mathbb{Z} \to \mathrm{G}$, $a \bmod m \mapsto g^a$; et ici nous utilisons le cas particulier $\mathrm{G} = \mathrm{Aut}(\mathrm{H})$ et g est l'inversion sur H.

Théorème 3.6.4

Le sous-groupe $\{e\} \times \mathrm{K}$ du produit semi-direct $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est distingué si et seulement si $\varphi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$ est trivial, autrement dit si et seulement si $\mathrm{H} \rtimes_\varphi \mathrm{K} = \mathrm{H} \times \mathrm{K}$.

Démonstration. — Puisque $\mathrm{H} \rtimes_\varphi \mathrm{K}$ est engendré par les sous-groupes $\mathrm{H} \times \{e\}$ et $\{e\} \times \mathrm{K}$, $\{e\} \times \mathrm{K}$ est un sous-groupe distingué de $\mathrm{H} \rtimes_\varphi \mathrm{K}$ si et seulement si $(h,e)(e,k)(h,e)^{-1}$ appartient à $\{e\} \times \mathrm{K}$ pour tous $h \in \mathrm{H}$ et $k \in \mathrm{K}$. On a $(h,e)(e,k)(h,e)^{-1} = (h,k)(h^{-1},e) = (h\varphi_k(h^{-1}), k \cdot e) = (h\varphi_k(h)^{-1}, k)$, qui est dans $\{e\} \times \mathrm{K}$ si et seulement si $\varphi_k(h) = h$. Donc $\{e\} \times \mathrm{K}$ est distingué dans $\mathrm{H} \rtimes_\varphi \mathrm{K}$ si et seulement si chaque φ_k est l'application d'identité sur H, ce qui signifie que φ est trivial. □

3.6.2. Reconnaître les produits semi-directs. — Le Théorème **??** nous indique quand un groupe est isomorphe au produit direct de deux sous-groupes. On peut se poser la question : quand un groupe est-il isomorphe à un produit semi-direct de deux sous-groupes ?

Dans $\mathrm{H} \rtimes_\varphi \mathrm{K}$ les sous-groupes $\mathrm{H} \times \{e\}$ et $\{e\} \times \mathrm{K}$ satisfont les propriétés suivantes :

- ils engendrent $\mathrm{H} \rtimes_\varphi \mathrm{K}$: $(h,k) = (h,e)(e,k)$;
- ils s'intersectent trivialement : $(h,e) = (e,k)$ implique $h = e$ et ke ;
- les éléments de $\{e\} \times \mathrm{K}$ conjuguent $\mathrm{H} \times \{e\}$ par φ : $(e,k)(h,e)(e,k)^{-1} = (\varphi_k(h), e)$.

Ces propriétés peuvent être résumées dans l'énoncé suivant :

Théorème 3.6.5

Soit G un groupe ; soient H et K deux sous-groupes de G. Supposons que

1. $\mathrm{G} = \mathrm{HK}$,
2. $\mathrm{H} \cap \mathrm{K} = \{e\}$,
3. $\mathrm{H} \triangleleft \mathrm{G}$.

Soit $\varphi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$ l'application définie par $\varphi_k(h) = khk^{-1}$ pour tout $k \in \mathrm{K}$.
Alors φ est un morphisme de groupes et l'application $f\colon \mathrm{H} \rtimes_\varphi \mathrm{K} \to \mathrm{G}$, $(h,k) \mapsto hk$ est un isomorphisme.

Démonstration. — Le fait que φ ait un sens est dû à 3.

On peut vérifier que $\varphi_k \circ \varphi_{k'} = \varphi_{kk'}$, *i.e.* que φ est un morphisme de groupes.

La fonction

$$f\colon \mathrm{H} \rtimes_\varphi \mathrm{K} \to \mathrm{G}, \qquad (h,k) \mapsto hk$$

est surjective par 1. et est injective par 2. en utilisant le même argument que dans la démonstration du Théorème **??**.

Soient (h,k) et (h',k') dans $\mathrm{H} \rtimes_\varphi \mathrm{K}$; nous avons

$$\begin{aligned} f((h,k)(h',k')) &= f(h\varphi_k(h'), kk') \\ &= h\varphi_k(h')kk' \\ &= hkh'k^{-1}kk' \\ &= hk, h'k' \\ &= f(h,k)f(h',k'). \end{aligned}$$

Finalement f est un isomorphisme. □

Exemple 3.6.11. — Soit $\tau \in \mathfrak{S}_n$ une transposition. D'après le Théorème 3.6.5 nous acons $\mathfrak{S}_n \simeq \mathcal{A}_n \rtimes \langle \tau \rangle$ le morphisme associé au produit semi-direct étant la conjugaison.

Nous avons aussi

$$\mathrm{D}_{2n} \simeq \langle r \rangle \rtimes \langle s \rangle, \qquad \mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right) \simeq \mathrm{P} \rtimes \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$$

où P est le 2-Sylow (distingué) de $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$.

Enfin, $\mathrm{GL}(2,\mathbb{R}) \simeq \mathrm{SL}(2,\mathbb{R}) \rtimes \mathrm{K}$ où K est l'ensemble des matrices diagonales $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ pour $a \in \mathbb{R}^\times$ (nous avons rencontré cette décomposition dans l'Exemple 2.3.2).

Remarque 3.6.2. — Nous pouvons décomposer un groupe de deux manières distinctes. Nous allons montrer pour $n > 1$ impair que le produit direct $\mathrm{SL}(n,\mathbb{R}) \times \mathbb{R}^\times$ est isomorphe à un produit semi-direct non trivial $\mathrm{SL}(n,\mathbb{R}) \rtimes \mathbb{R}^\times$.

Soient $\mathrm{H} = \mathrm{SL}(n,\mathbb{R})$ et K le sous-groupe des matrices diagonales $\mathrm{diag}(a,1,1,\ldots,1)$, $a \in \mathbb{R}^\times$, donc $\mathrm{K} \simeq \mathbb{R}^\times$. Alors $\mathrm{G} = \mathrm{HK}$ avec $\mathrm{H} \subset \mathrm{G}$ et $\mathrm{H} \cap \mathrm{K} = \{\mathrm{Id}\}$ (le cas $n = 2$ est traité dans l'Exemple 2.3.2). Lorsque $n > 1$, la conjugaison l'action de K sur H n'est pas triviale ; par conséquent $\mathrm{GL}(n,\mathbb{R})$ est isomorphe à un produit semi-direct non trivial $\mathrm{SL}(n,\mathbb{R}) \times \mathrm{H} \simeq \mathrm{SL}(n,\mathbb{R}) \rtimes \mathbb{R}^\times$.

Le centre de G est $Z(\mathrm{G}) = \{\lambda \mathrm{Id} \,|\, \lambda \in \mathbb{R}^\times\}$; il est isomorphe à $\mathbb{R}^\times$ et

- ◇ $\mathrm{H} \cap Z(\mathrm{G}) = \{\mathrm{Id}\}$ si n est impair ;
- ◇ $\mathrm{H} \cap Z(\mathrm{G}) = \{\pm \mathrm{Id}\}$ si n est pair.

Pour n impair nous avons $\mathrm{G} = \mathrm{H}Z(\mathrm{G})$: si g désigne G et Δ désigne $\det g$, alors $g = hz$ où $h = g(\sqrt[n]{\Delta}\mathrm{Id})^{-1}$ et $z = \sqrt[n]{\Delta}\mathrm{Id}$. L'action part conjugaison de $Z(\mathrm{G})$ sur H est trivial ; ainsi $\mathrm{GL}(n,\mathbb{R})$ est isomorphe au produit direct $\mathrm{SL}(n,\mathbb{R}) \times Z(\mathrm{G}) \simeq \mathrm{SL}(n,\mathbb{R}) \times \mathbb{R}^\times$.

Exemples 3.6.12. — Nous avons rencontré plusieurs exemples de groupes isomorphes à un produit semi-direct de deux groupes :

- ◇ $\mathrm{Aff}(\mathbb{R}) \simeq \mathbb{R} \rtimes \mathbb{R}^\times$;
- ◇ $\mathfrak{S}_n \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$;

◇ $\mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$;

◇ $\mathrm{GL}(2,\mathbb{R}) \simeq \mathrm{SL}(2,\mathbb{R}) \rtimes \mathbb{R}^\times$.

Dans ces groupes respectifs,

◇ $\mathbb{R}^\times$ agit sur $\mathbb{R}$ par les applications de multiplication $\varphi_x \colon y \mapsto xy$ pour $x \in \mathbb{R}^\times$;

◇ $\mathbb{Z}/2\mathbb{Z}$ s'identifie à $\{\mathrm{id}, \tau\}$ pour toute transposition τ dans $\mathfrak{S}_n$;

◇ $\mathbb{Z}/n\mathbb{Z}$ s'identifie à $\langle r \rangle$ et $\mathbb{Z}/2\mathbb{Z}$ s'identifie à $\{\mathrm{id}, s\}$ dans D_{2n} ;

◇ $\mathbb{R}^\times$ s'identifie au groupe des matrices $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$.

« Comprendre » les produits semi-directs donnés dans tous ces exemples revient à comprendre

◇ comment un groupe se décompose en un produit HK de deux sous-groupes H et K d'intersection triviale ;

◇ le morphisme de K dans Aut(H).

3.6.3. Construire des produits semi-directs. — Jusqu'à présent, nous n'avons pas utilisé de produits semi-directs pour créer de nouveaux groupes. Pour construire de nouveaux groupes, nous commençons par considérer deux groupes H et K et nous cherchons des morphismes $\varphi \colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$ non triviaux (si φ est trivial, le produit obtenu est direct).

Exemple 3.6.13. — Déterminons un produit semi-direct $\mathbb{Z}/25\mathbb{Z} \rtimes \mathbb{Z}/15\mathbb{Z}$ qui ne soit pas un produit direct. Puisque $\mathrm{Aut}\left(\mathbb{Z}/25\mathbb{Z}\right) = \left(\mathbb{Z}/25\mathbb{Z}\right)^\times$ est d'ordre 20 et $\mathrm{pgcd}(20,15) \neq 1$, un tel produit semi-direct existe.

Soit $\varphi \colon \mathbb{Z}/15\mathbb{Z} \to \left(\mathbb{Z}/25\mathbb{Z}\right)^\times$ un morphisme non trivial. Posons $g = \varphi(1)$; nous avons $g^{15} = 1$. Si $g^{15} \equiv_{25} 1$, alors $g^{15} \equiv_5 1$ et $g \equiv_5 1$. Par g appartient à $\{1, 6, 11, 16, 21\}$.

Choisissons par exemple $g = 6$. On peut vérifier que $6^{15} \equiv_{25} 1$ (en fait, si $a \equiv_5 1$, alors $a^5 \equiv_{25} 1$ et $a^{15} \equiv_{25} 1$). Considérons $\varphi \colon \mathbb{Z}/15\mathbb{Z} \to \left(\mathbb{Z}/25\mathbb{Z}\right)^\times$ défini par $\varphi(1) = 6$. Ceci implique que $\varphi(k \bmod 25) = 6^k \bmod 25$; par exemple $\varphi(2) = \varphi(1+1) = \varphi(1)\varphi(1) = 6^2$. Nous obtenons donc un produit semi-direct $\mathbb{Z}/25\mathbb{Z} \rtimes_\varphi \mathbb{Z}/15\mathbb{Z}$ non trivial dont la loi est

$$(a,b)(c,d) = (a + \varphi_b(c), b + d) = (a + 6^b c, b + d)$$

C'est un groupe non abélien d'ordre $15 \times 25 = 375$ construit à partir de deux groupes cycliques d'ordre 15 et 25.

Exemple 3.6.14. — Existe-t-il un produit semi-direct non trivial construit à partir des groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$?

Puisque $\mathrm{Aut}\left(\mathbb{Z}/4\mathbb{Z}\right) = \{x \mapsto x,\, x \mapsto -x\} \simeq \{\pm 1 \bmod 4\} = \left(\mathbb{Z}/4\mathbb{Z}\right)^{\times}$, il existe un morphisme $\varphi\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/4\mathbb{Z}\right)$ donné par $\varphi(k \bmod 2) = x \mapsto (-1)^k x$. La loi de $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ est donc donnée par

$$(a,b)(c,d) = (a + (-1)^b c, b + d).$$

Le produit $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ ainsi construit est un groupe d'ordre 8 construit à partir des deux sous-groupes $\mathrm{H} = \mathbb{Z}/4\mathbb{Z}$ et $\mathrm{K} = \mathbb{Z}/2\mathbb{Z}$. Il est isomorphe à D_8 via

$$f\colon \mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z} \to \mathrm{D}_8 = h, \qquad f(a,b) = r^a s^b.$$

Exemple 3.6.15. — Soit H un groupe possédant un automorphisme ψ d'ordre 2. Nous pouvons construire le produit semi-direct $\mathrm{H} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ muni de la loi

$$(h,k)(h',k') = (h \cdot \psi^k(h'), k + k').$$

Ici φ est le morphisme

$$\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathrm{H}), \qquad k \mapsto \varphi_k\colon h \mapsto \varphi_k(h) = \psi^k(h) = \underbrace{\psi \circ \psi \circ \ldots \circ \psi}_{k \text{ times}}(h),\ k > 0.$$

Un exemple est donné par $\mathrm{H} = \mathrm{GL}(2,\mathbb{R})$ et $\psi\colon A \mapsto ({}^{\mathrm{t}}A)^{-1}$.

De même, si un groupe H possède un automorphisme ψ tel que $\psi^n = \mathrm{id}_{\mathrm{H}}$, alors nous obtenons un produit semi-direct $\mathrm{H} \rtimes_\varphi \mathbb{Z}/n\mathbb{Z}$ muni de la loi

$$(h,k)(h',k') = (h \cdot \psi^k(h'), k + k').$$

Exemple 3.6.16. — Un produit semi-direct $\mathbb{Z}/8\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ est d'ordre 16 et provient d'un morphisme $\varphi\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/8\mathbb{Z}\right)$. Il existe quatre automorphismes de de $\mathbb{Z}/8\mathbb{Z}$ qui sont

$$x \mapsto x, \qquad x \mapsto 3x, \qquad x \mapsto 5x, \qquad x \mapsto 7x.$$

Cela conduit à quatre produits semi-directs $\mathbb{Z}/8\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, avec les différentes lois de groupe suivantes : (a, b)(c, d) = (a+ c, b + d),

$$(a,b)(c,d) = (a + 3^b c, b + d), \tag{3.6.4}$$

$$(a,b)(c,d) = (a + 5^b c, b + d), \tag{3.6.5}$$

$$(a,b)(c,d) = (a + 7^b c, b + d). \tag{3.6.6}$$

Ce n'est pas parce que les formules de deux lois de groupe semblent différentes que les groupes obtenus à partir de ces deux lois ne sont pas isomorphes. Nous allons montrer que les quatre groupes évoqués ci-dessus bien ne sont pas isomorphes. Le premier est abélien et les autres

ne sont pas abéliens (produits semi-directs non triviaux). Une façon de distinguer les groupes qui ne sont pas abéliens est de montrer qu'ils n'ont pas le même nombre d'éléments d'ordre 2 (Théorème 2.2.5).

- ◇ Le groupe (3.6.4). Ici $(a,b)^2 = (a(1+3^b),0)$; nous voulons donc les compter (a,b) avec $a \in \mathbb{Z}/8\mathbb{Z}$ et $b \in \mathbb{Z}/2\mathbb{Z}$ tels que $a(1+3^b) \equiv_8 0$. Si $b=0$ dans $\mathbb{Z}/2\mathbb{Z}$ alors $(2a,0)=(0,0)$, donc $a=0$, 4 dans $\mathbb{Z}/8\mathbb{Z}$. Si au contraire $b=1$ dans $\mathbb{Z}/2\mathbb{Z}$ alors $4a \equiv_8 0$, donc a est même. Il existe quatre valeurs de a, donc le nombre de solutions de $(a,b)^2=(0,0)$ est $2+4=6$. Nous en déduisons qu'il y a cinq éléments d'ordre 2.
- ◇ Le groupe (3.6.5). Ici $(a,b)^2 = (a(1+5^b),0)$; nous sommes donc ramener à déterminer tous les $(a,b) in \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ tels que $a(1+5^b) \equiv_8 0$. Si $b=0$ alors $(2a,0)=(0,0)$, donc $a=0$, 4 dans $\mathbb{Z}/8\mathbb{Z}$. Si $b=1$ alors $6a \equiv_8 0$, donc $2a \equiv_8 0$. Il y a deux valeurs de a, donc le nombre de solutions de $(a,b)^2=(0,0) est 2+2=4$. Par conséquent il y a trois éléments d'ordre 2.
- ◇ Le groupe (3.6.6). Ici $(a,b)^2 = (a(1+7^b),0)$. Lorsque $b=0$ il y a deux valeurs de a (comme dans les autres cas), tandis que lorsque $b=1$ nous avons $a(1+7^b)=0$ dans $\mathbb{Z}/8\mathbb{Z}$ pour tout a. Le nombre de solutions de $(a,b)^2=(0,0)$ est $2+8=10$. Il en résulte qu'il y a neuf éléments d'ordre 2.

3.6.4. Sous-groupes complémentaires. — La caractérisation des groupes isomorphes à un produit semi-direct (Théorème 3.6.5) conduit à la notion et la question qui suivent. Si un groupe G contient des sous-groupes H et K tels que $G = HK$ et $H \cap K = \{e\}$, alors H et K sont appelés *sous-groupes complémentaires*. Soit $H \triangleleft G$ un sous-groupe distingué de G ; existe-t-il un sous-groupe complémentaire K de H dans G auquel cas $G \simeq H \rtimes_\varphi K$? La réponse est non !

Exemple 3.6.17. — Soit G un groupe fini cyclique d'ordre $> p$ dont tout élément a pour ordre une puissance de p. Tout sous-groupe de G est distingué dans G. Soit $H \subset G$ un sous-groupe de G tel que $1 < |H| < |G|$. Supposons que $G = HK$; alors $|K| > 1$. Le théorème de Cauchy assure que H et K possèdent des sous-groupes d'ordre p. Le groupe cyclique G a au plus un sous-groupe par « ordre possible ». Les sous-groupes d'ordre p dans H et K sont donc identiques ; en particulier $H \cap K \neq \{e\}$. Il en résulte que G n'est pas un produit semi-direct de deux sous-groupes propres.

Exemple 3.6.18. — Considérons le groupe des quaternions $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Il n'existe qu'un seul sous-groupe d'ordre 2, le groupe $\{\pm 1\}$. Les sous-groupes de $\mathbb{H}_8$ sont tous distingués dans $\mathbb{H}_8$. Soit $H \subset \mathbb{H}_8$ un sous-groupe propre de $\mathbb{H}_8$. Si $\mathbb{H}_8 = HK$, alors puisque $1 < |K| < 8$ nous avons $K \neq \{e\}$. Par le même argument que dans l'exemple précédent $H \cap K \neq \{e\}$. En particulier, $\mathbb{H}_8$ n'est pas un produit semi-direct de deux sous-groupes propres.

Exemple 3.6.19. — Considérons le groupe diédral $\mathrm{D}_{2n} = \langle r, s\rangle$ pour $n \geq 6$ pair.

Pour tout $n \geq 6$ pair, $\langle r^2, s\rangle$ et $\langle rs\rangle$ sont des sous-groupes complémentaires. Il en résulte que

$$\mathrm{D}_{2n} = \langle r^2,\, s\rangle\langle rs\rangle \simeq \mathrm{D}_n \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Le centre de D_{2n} est $\mathrm{Z} = \{\mathrm{id},\, r^{n/2}\}$.

- ◇ Lorsque $\frac{n}{2}$ est impair, le sous-groupe $\mathrm{K} = \langle r^2,\, s\rangle$ de D_{2n} est d'ordre n et d'intersection triviale avec Z. Ainsi

$$\mathrm{D}_{2n} = \mathrm{ZK} \simeq \mathrm{Z} \times \mathrm{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_n.$$

- ◇ Lorsque $\frac{n}{2}$ est pair, $\mathrm{D}_{2n} \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_n$ puisque D_{2n} a un centre d'ordre 2 et $\mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_n$ a un centre d'ordre 4.

Remarquons que lorsque $\mathrm{G} = \mathrm{HK}$ avec $\mathrm{H} \subset \mathrm{G}$ et $\mathrm{H} \cap \mathrm{K} = \{e\}$, le groupe K n'est pas nécessairement unique.

Exemple 3.6.20. — Soit $n \geq 3$ un entier. Pour toute transposition τ de $\mathfrak{S}_n$ nous avons $\mathfrak{S}_n = \mathcal{A}_n \langle\tau\rangle$.

Exemple 3.6.21. — Soit $n \geq 3$ un entier. Pour tout $0 \leq i \leq n-1$ nous avons $\mathrm{D}_{2n} = \langle r\rangle\,\langle r^i s\rangle$ (notons que pour tout $0 \leq i \leq n-1$ l'élément $r^i s$ de D_{2n} est une réflexion).

On peut se demander à quelle(s) condition(s) un sous-groupe distingué possède un complémentaire. Si G est un groupe fini, alors tout sous-groupe distingué admet un complémentaire, (c'est une condition suffisante mais pas nécessaire). Le Théorème de Schur-Zassenhaus que nous verrons au Chapitre 3, §3.6 apporte une réponse partielle à cette question.

3.6.5. Suites exactes. — Nous avons introduit au Chapitre 2, §2.3 la notion de produit semi-direct. Nous allons donner ici un autre point de vue de cette notion.

Soient N et H deux groupes. Le produit direct $\mathrm{G} = \mathrm{N} \times \mathrm{H}$ est le produit cartésien de N et H muni de la loi produit :

$$(n, h)(n', h') = (nn', hh').$$

La projection $p\colon \mathrm{G} \to \mathrm{H}$ définie par $p(n, h) = h$ est un morphisme de groupes surjectif de noyau le sous-groupe distingué

$$\overline{\mathrm{N}} = \{(n, 1) \mid n \in \mathrm{N}\}.$$

Nous avons la suite exacte

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{N} \times \mathrm{H} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

où $i\colon \mathrm{N} \to \mathrm{N} \times \mathrm{H}$, $n \mapsto (n, 1)$. Notons que les groupes N et H jouent des rôles symétriques. Le sous-groupe

$$\overline{\mathrm{H}} = \{(1, h) \mid h \in \mathrm{H}\}$$

noyau de la projection sur N est tel que

- ◇ la restriction de la projection $p_{|\overline{\mathrm{H}}} \colon \overline{\mathrm{H}} \to \mathrm{H}$ est un isomorphisme,
- ◇ $\overline{\mathrm{H}}$ est un sous-groupe distingué de $\mathrm{N} \times \mathrm{H}$.

Le produit semi-direct est une variante « affaiblie » du produit direct :

Proposition 3.6.1

Considérons une suite exacte

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1.$$

Supposons que p possède une *section*, *i.e.* qu'il existe un morphisme $s \colon \mathrm{H} \to \mathrm{G}$ tel que $p \circ s = \mathrm{id}_{\mathrm{H}}$.
Alors G est isomorphe à $\mathrm{N} \rtimes \mathrm{H}$.

Démonstration. — Posons $\mathrm{N}' = i(\mathrm{N})$ et $\mathrm{H}' = s(\mathrm{H})$. Nous avons les trois propriétés suivantes :

- ◇ Le groupe N' est distingué dans G car $\mathrm{N}' = \ker p$.
- ◇ Soit $g \in \mathrm{G}$. Posons $h = s(p(g)) \in \mathrm{H}'$. Alors
$$p(h) = p(s(p(g))) = p(g)$$
donc $n = gh^{-1}$ appartient à $\ker p = \mathrm{N}'$. Finalement nous avons bien $\underbrace{g}_{\in \mathrm{G}} = \underbrace{n}_{\in \mathrm{N}'} \underbrace{h}_{\in \mathrm{H}'}$ ce qui assure que $\mathrm{G} = \mathrm{N}'\mathrm{H}'$.
- ◇ Soit $g \in \mathrm{N}' \cap \mathrm{H}'$. Puisque $g \in \mathrm{H}'$ il existe $h \in \mathrm{H}$ tel que $g = s(h)$. Comme $g \in \mathrm{N}'$ nous avons $p(g) = e$. Par suite $p(s(h)) = e$, *i.e.* $h = e$, donc $g = s(e) = e$. Il s'en suit que $\mathrm{N}' \cap \mathrm{H}' = \{e\}$.

Le Théorème 3.6.5 permet de conclure. □

Exemple 3.6.22. — Soient $\mathrm{G} = \mathrm{GL}(2, \mathbb{R})$ et $\mathrm{H} = \mathrm{SL}(2, \mathbb{R})$. Rappelons que $\det \colon \mathrm{GL}(2, \mathbb{R}) \to \mathbb{R}^\times$, $M \mapsto \det M$ est un morphisme de groupes. Remarquons que $\mathrm{H} = \ker \det$; en particulier G/H a une structure de groupes et $\mathrm{G}/\mathrm{H} \simeq \mathbb{R}^\times$. De plus

$$s \colon \mathbb{R}^\times \to \mathrm{GL}(2, \mathbb{R}), \qquad c \mapsto \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}$$

est une section de det : pour tout $c \in \mathbb{R}^\times$ nous avons $\det(s(c)) = c$.

Soient G un groupe et N un sous-groupe distingué de G ; peut-on reconstruire G à partir de N et G/N ? En général, non. Par exemple,

- ◇ les groupes $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (pour p premier) ne sont pas isomorphes, mais chacun d'eux possède un sous-groupe cyclique d'ordre p et le quotient par celui-ci est également d'ordre p ;

- ⋄ les groupes non isomorphes $\mathbb{Z}/2p\mathbb{Z}$ et D_{2p} (pour p premier impair) possèdent un sous-groupe distingué cyclique d'ordre p et le quotient de $\mathbb{Z}/2p\mathbb{Z}$ (resp. D_{2p}) par ce groupe est cyclique d'ordre 2

Si nous imposons que $|N|$ et $\left|G/N\right|$ sont premiers entre eux, alors G est le produit semi-direct de N et G/N. C'est le Théorème de Schur-Zassenhaus dont nous discuterons ci-dessous. Attention cela ne détermine pas G de manière unique : par exemple, si $N \simeq \mathbb{Z}/p\mathbb{Z}$ pour p premier impair et $G/N \simeq \mathbb{Z}/2\mathbb{Z}$ alors G est un produit semi-direct de la forme $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, *i.e.*

- ⋄ ou bien le produit est direct et G est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$;
- ⋄ ou bien le produit semi-direct est non trivial et G est isomorphe à D_{2p}.

Énonçons maintenant le Théorème de Schur-Zassenhaus évoqué ci-dessus et au Chapitre 2, §2.3.

Théorème 3.6.6: (Schur-Zassenhaus)

Soit G un groupe fini. Écrivons $|G|$ sous la forme ab avec $\mathrm{pgcd}(a,b) = 1$. Si G possède un sous-groupe distingué d'ordre a, alors il possède un sous-groupe d'ordre b.
De plus, les sous-groupes de G d'ordre b sont conjugués entre eux.

La démonstration du Théorème de Schur-Zassenhaus dans le cas général nécessite des outils élaborés que nous n'allons pas introduire ici, nous pouvons la trouver par exemple dans [**Rob96**]. Néanmoins nous donnerons la démonstration de cet énoncé dans deux cas particuliers (Exemple 3.6.23 et Exemple 3.6.23).

Corollaire 3.6.1

Soit G un groupe fini d'ordre ab avec $\mathrm{pgcd}(a,b) = 1$. Soient N un sous-groupe distingué d'ordre a de G et H un sous-groupe d'ordre b de G. Alors G est un produit semi-direct de N et H.

Démonstration. — Remarquons que $N \cap H$ est trivial puisque $\mathrm{pgcd}(a,b) = 1$. Il en résulte que $G = NH \simeq N \rtimes H$ où H agit sur N par conjugaison. □

Dans les deux exemples qui suivent nous donnons deux cas où la démonstration du théorème de Schur-Zassenhaus est assez directe.

Exemple 3.6.23. — Soit G un groupe abélien. Soit $f\colon G \to G$ défini par $f(g) = g^b$. Puisque $\mathrm{pgcd}(b, |N|) = 1$, la restriction $f_{|N}$ de f à N est un isomorphisme ; en particulier, $N \subset f(G)$. Comme $(g^b)^a = g^{ab} = 1$ pour tout $g \in G$, l'ordre de tout élément de $f(G)$ divise a ; par suite $\mathrm{pgcd}(a,b) = 1$ implique $\mathrm{pgcd}(|f(G)|, b) = 1$ (Théorème de Cauchy). Puisque $|f(G)|$ divise $|G|$, nous obtenons $|f(G)|$ divise a. De plus, a divise $|f(G)|$ puisque $N = f(N)$ est un sous-groupe

de $f(\mathrm{G})$. Ainsi $|f(\mathrm{G})| = a$, donc $f(\mathrm{G}) = \mathrm{N}$. Soit $\mathrm{H} = \ker f$, alors ${}^{\mathrm{G}}\!/_{\mathrm{H}} \simeq f(\mathrm{G}) = \mathrm{N}$, donc $|\mathrm{H}| = \frac{|\mathrm{G}|}{|\mathrm{N}|} = b$.

Exemple 3.6.24. — Si ${}^{\mathrm{G}}\!/_{\mathrm{N}}$ est cyclique (par exemple, si l'indice de N dans G est premier), alors on peut démontrer le théorème de Schur-Zassenhaus comme suit. Posons $|\mathrm{N}| = a$, $[\mathrm{G} : \mathrm{N}] = b$ et ${}^{\mathrm{G}}\!/_{\mathrm{N}} = \langle g \rangle$. Étant donnés que a et b sont premiers entre eux et que $\left|{}^{\mathrm{G}}\!/_{\mathrm{N}}\right| = b$, nous avons ${}^{\mathrm{G}}\!/_{\mathrm{N}} = \langle ga \rangle$. Par ailleurs, $|\mathrm{G}| = ab$ d'où : $e = g^{ab} = (g^a)^b$. Posons $x = g^a$; alors $x^b = e$ et ${}^{\mathrm{G}}\!/_{\mathrm{N}} = \langle x \rangle$. Il en résulte que chaque élément de G est de la forme $x^i n$ pour certains $i \in \mathbb{Z}$ et $n \in \mathbb{N}$. L'ordre de $\langle x \rangle$ divise b, qui est premier avec $a = |\mathrm{N}|$; par suite $|\langle x \rangle| \cap \mathrm{N} = \{e\}$. Ainsi $\mathrm{G} = \mathrm{N}\langle x \rangle$. Par conséquent $ab = |\mathrm{G}| = |\mathrm{N}|\,|\langle x \rangle| = a\,|\langle x \rangle|$, donc $|\langle x \rangle| = b$: x engendre un sous-groupe de G d'ordre b.

Corollaire 3.6.2

Soit p un nombre premier. Soit G un groupe fini d'ordre divisible par p.
Les assertions suivantes sont équivalentes :

- $|\mathrm{Aut}(\mathrm{G})|$ n'est pas divisible par p ;
- G est isomorphe à ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \times \mathrm{H}$ où $|\mathrm{H}|$ et $|\mathrm{Aut}(\mathrm{H})|$ ne sont pas divisibles par p.

En particulier, si p^2 divise $|\mathrm{G}|$, alors p divise $|\mathrm{Aut}(\mathrm{G})|$.

Démonstration. — Montrons que la seconde assertion implique la première. Nous avons

$$\mathrm{Aut}\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \times \mathrm{H}\right) \simeq \mathrm{Aut}\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right) \times \mathrm{Aut}(\mathrm{H}) \simeq \left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)^{\times} \times \mathrm{Aut}(\mathrm{H});$$

puisque $|\mathrm{Aut}(\mathrm{H})|$ n'est pas divisible par p, $\left|\mathrm{Aut}\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \times \mathrm{H}\right)\right|$ n'est pas divisible par p.

Montrons que la première assertion implique la seconde. Soit P un p-Sylow de G. Montrons que $\mathrm{G} \simeq \mathrm{P} \times \mathrm{H}$ et $\mathrm{P} \simeq {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. Pour tout $x \in \mathrm{P}$ désignons par γ_x l'automorphisme de G défini par $\gamma_x(g) = xgx^{-1}$. Puisque x est d'ordre une puissance de p, γ_x aussi (rappelons que $\gamma_x^n = \gamma_{x^n}$ pour tout n). Par hypothèse $|\mathrm{Aut}(\mathrm{G})|$ n'est pas divisible par p, donc le seul élément d'ordre une puissance de p dans $\mathrm{Aut}(\mathrm{G})$ est l'identité. Ainsi $\gamma_x = \mathrm{id}_{\mathrm{G}}$ pour tout $x \in \mathrm{P}$, ce qui signifie $\mathrm{P} \subset Z(\mathrm{G})$. En particulier, P est un sous-groupe distingué de G (Théorème 10.1.2) et P est abélien. Par conséquent, le théorème de Schur-Zassenhaus assure que $\mathrm{G} \simeq \mathrm{PH}$ pour un sous-groupe H d'ordre non divisible par p. Comme $\mathrm{P} \subset Z(\mathrm{G})$, nous avons $\mathrm{G} \simeq \mathrm{P} \times \mathrm{H}$. Étant donnés que $|\mathrm{P}|$ et $|\mathrm{H}|$ sont premiers entre eux et que P et H commutent nous avons : $\mathrm{Aut}(\mathrm{G}) \simeq \mathrm{Aut}(\mathrm{P}) \times \mathrm{Aut}(\mathrm{H})$. Ainsi ou bien p ne divise pas $|\mathrm{Aut}(\mathrm{P})|$ ou bien p ne divise pas $|\mathrm{Aut}(\mathrm{H})|$.

Quels sont les p-groupes abéliens finis P tels que $|\mathrm{Aut}(\mathrm{P})|$ n'est pas divisible par p ? Écrivons P comme un produit direct de groupes cycliques

$$\mathrm{P} = {}^{\mathbb{Z}}\!/_{p^{r_1}\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{p^{r_2}\mathbb{Z}} \times \ldots \times {}^{\mathbb{Z}}\!/_{p^{r_k}\mathbb{Z}}.$$

Puisque $\mathrm{Aut}\left(\mathbb{Z}/p^r\mathbb{Z}\right) \simeq \left(\mathbb{Z}/p^r\mathbb{Z}\right)^\times$ est d'ordre $p^{r-1}(p-1)$, on constate que si certains $r_i > 1$ alors que $\mathbb{Z}/p^{r_i}\mathbb{Z}$ possède un automorphisme d'ordre p, donc P aussi (sur le $i$ème facteur agit l'automorphisme choisi et sur les autres facteurs agit l'identité). Ainsi, si $|\mathrm{Aut(P)}|$ n'est pas divisible par p nous devons avoir $r_i = 1$ pour tout i, donc $\mathrm{P} \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^k$ est une somme directe de copies de $\mathbb{Z}/p\mathbb{Z}$. Il en résulte que $\mathrm{Aut(P)} \simeq \mathrm{GL}\left(k, \mathbb{Z}/p\mathbb{Z}\right)$, dont l'ordre est divisible par $p^{k(k-1)/2}$, et donc divisible par p sauf si $k = 1$. Par conséquent P est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. □

Exemple 3.6.25. — Si $|\mathrm{G}|$ est pair et $|\mathrm{Aut(G)}|$ est impair, alors G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathrm{H}$ où H désigne un groupe d'ordre impair et où Aut(H) est aussi d'ordre impair. Le plus petit (au sens de l'inclusion) H non trivial possible est d'ordre $3^6 = 729$ avec un groupe d'automorphismes d'ordre $3^9 = 19683$.

Lorsque p divise $|\mathrm{Aut(G)}|$, une façon de rechercher des éléments d'ordre p dans Aut(G) est la suivante : si $g \in \mathrm{G}$ est d'ordre p et g n'appartient pas au centre de G, alors la conjugaison par g est un automorphisme (dit automorphisme intérieur) de G d'ordre p. On peut se demander quand il existe des automorphismes d'ordre p qui ne sont pas intérieurs. Il existe une réponse complète à cette question pour les p-groupes :

- si G est un p-groupe abélien fini, il possède un automorphisme d'ordre p tant que $\mathrm{G} \not\simeq \mathbb{Z}/p\mathbb{Z}$ et cet automorphisme n'est pas intérieur puisque G est abélien ;
- lorsque G est un p-groupe non-abélien fini, il existe un automorphisme d'ordre p qui n'est pas intérieur, la démonstration utilise des outils sophistiqués, on renvoie à [**Gas66**].

3.7. Le Théorème de Cauchy et ses conséquences

3.7.1. Énoncé et preuve du théorème de Cauchy. —

La réciproque du théorème de Lagrange est fausse en général : si G est un groupe fini et si d divise $|\mathrm{G}|$, alors G ne contient pas nécessairement un sous-groupe d'ordre d. Par exemple $\mathcal{A}_4$ est un groupe d'ordre 12 qui ne contient pas de sous-groupe d'ordre 6. La réciproque du théorème de Lagrange n'est donc pas vraie en toute généralité ; par contre elle l'est si on suppose que d est premier ; ce résultat est dû à Cauchy (1844) :

Théorème 3.7.1: (Théorème de Cauchy)

Soit G un groupe fini. Soit p un facteur premier de $|\mathrm{G}|$. Alors G contient un élément d'ordre p ; autrement dit, G contient un sous-groupe d'ordre p.

Remarque 3.7.1. — Cauchy a énoncé son résultat pour les groupes de permutations, c'est-à-dire les sous-groupes de $\mathfrak{S}_n$, et non pour les groupes finis abstraits ; le concept de groupe fini abstrait n'existait pas encore.

Démonstration. — Nous allons raisonner par récurrence sur $|\mathrm{G}|$. Posons $n = |\mathrm{G}|$. Notons que comme p divise n, nous avons l'inégalité $n \geq p$.

Commençons donc par étudier le cas $n = p$. Lorsque $|\mathrm{G}| = p$, chaque élément de $\mathrm{G} \smallsetminus \{e\}$ a un ordre p puisque p est premier.

Supposons que $n > p$, que $p \mid n$ et que l'énoncé est vrai pour tous les groupes d'ordre inférieur à n divisible par p. Nous traitons d'abord le cas G abélien puis le cas G non abélien par deux méthodes différentes.

- ◇ Cas 1 : G est abélien. Supposons qu'aucun élément de G soit d'ordre p. Alors aucun élément est d'ordre divisible par p. En effet, si $g \in \mathrm{G}$ est d'ordre r et $p \mid r$ alors $g^{\frac{r}{p}}$ est un élément de G d'ordre p : contradiction. Désignons par $g_1, g_2, \ldots, g_n$ les éléments de G, *i.e.* $\mathrm{G} = \{g_1, g_2, \ldots, g_n\}$. Notons m_i l'ordre de g_i ; par hypothèse, m_i, $1 \leq i \leq n$ n'est pas divisible par p. Posons $m = \mathrm{ppcm}(m_1, m_2, \ldots, m_n)$; d'une part m n'est pas divisible par p, d'autre part $g_i^m = e$ pour tout $1 \leq i \leq n$. Le groupe G étant abélien, la fonction $f\colon \left(\mathbb{Z}/m\mathbb{Z}\right)^n \to \mathrm{G}$ donnée par $f(a_1, a_2, \ldots, a_n) = g_1^{a_1} g_2^{a_2} \ldots g_n^{a_n}$ est un morphisme (cette fonction est bien définie car $g_i^m = e$ pour tout i, donc $g_i^{a+mk} = g_i^a$ pour tout $k \in \mathbb{Z}$). Ce morphisme est surjectif ($\mathrm{G} = \{g_1, g_2, \ldots, g_n\}$ et si $a_i = 1$ et $a_j = 0$ pour tout $j \neq i$ alors $f(a_1, a_2, \ldots, a_n) = g_i$). Par suite le premier théorème d'isomorphisme (Théorème 3.5.2) assure que $\left(\mathbb{Z}/m\mathbb{Z}\right)^n / \ker f \simeq \mathrm{G}$. Il en résulte que

$$|\mathrm{G}| = \frac{\left|\left(\mathbb{Z}/m\mathbb{Z}\right)^n\right|}{|\ker f|} = \frac{m^n}{|\ker f|},$$

  et $|\mathrm{G}|\,|\ker f| = m^n$. Par conséquent $|\mathrm{G}|$ est un facteur de m^n, mais p divise $|\mathrm{G}|$ et m^n n'est pas divisible par p : contradiction.

- ◇ Cas 2 : G n'est pas abélien. Supposons qu'aucun élément de G ne soit d'ordre p. Soit H un sous-groupe propre de G (abélien ou non) ; il ne possède pas d'élément d'ordre p. Par récurrence $|\mathrm{H}|$ n'est pas divisible par p. Par ailleurs $|\mathrm{G}| = |\mathrm{H}|[\mathrm{G} : \mathrm{H}]$; comme $|\mathrm{H}|$ n'est pas divisible par p alors que $|\mathrm{G}|$ est divisible par p, l'indice $[\mathrm{G} : \mathrm{H}]$ est divisible par p.

  Le groupe G n'étant pas abélien, il possède des classes de conjugaison de cardinal supérieur à 1. Supposons que ces classes soient représentées par $g_1, g_2, \ldots, g_k$. Les classes de conjugaison dans G de cardinal 1 sont les éléments de $Z(\mathrm{G})$. Puisque les classes de conjugaison dans G forment une partition de G nous avons

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{k} \#C_{g_i} = |Z(\mathrm{G})| + \sum_{i=1}^{k} [\mathrm{G} : Z_{g_i}], \tag{3.7.1}$$

  où C_{g_i} désigne la classe de conjugaison de g_i et Z_{g_i} est le centralisateur de g_i (pour tout $g \in \mathrm{G}$, nous avons $\#C_g = [\mathrm{G} : Z_g]$). Comme $\#C_{g_i} > 1$, nous avons $[\mathrm{G} : Z_{g_i}] > 1$, donc $Z_{g_i} \neq \mathrm{G}$ pour tout i. Finalement p divise $[\mathrm{G} : Z_{g_i}]$. Ainsi $|\mathrm{G}|$ et $[\mathrm{G} : Z_{g_i}]$ sont divisibles par

p donc d'après (3.7.1) l'entier $|Z(\mathrm{G})|$ est divisible par p. Mais aucun sous-groupe propre de G n'est d'ordre divisible par p d'où $Z(\mathrm{G}) = \mathrm{G}$, *i.e.* G est abélien : contradiction.

□

3.7.2. Premières conséquences. —

Théorème 3.7.2

Soit G un groupe fini. Soit p un nombre premier. L'ordre de G est une puissance de p si et seulement si tous les éléments de G sont d'ordre p^k pour un certain $k \in \mathbb{N}$.

Démonstration. — Supposons que $|\mathrm{G}|$ est une puissance de p. D'après le théorème de Lagrange (Théorème 1.6.4) l'ordre de $g \in \mathrm{G}$ divise $|\mathrm{G}|$ donc l'ordre de g est une puissance de p.

Réciproquement, supposons que tous les éléments de G sont d'ordre une puissance de p. Pour Raisonnons par l'absurde : supposons que $|\mathrm{G}|$ est divisible par un nombre premier $q \neq p$. Alors, d'après le théorème de Cauchy (Théorème 3.7.1), le groupe G contient un élément d'ordre q : contradiction. □

Théorème 3.7.3

Si tous les éléments de $\mathrm{G} \smallsetminus \{e\}$ sont de même ordre, cet ordre est premier p et $|\mathrm{G}|$ est une puissance de p.

Démonstration. — Si $|\mathrm{G}|$ a deux facteurs premiers, disons p et q, alors G contient des éléments d'ordres p et q (Théorème de Cauchy, Théorème 3.7.1) : contradiction. Ainsi $|\mathrm{G}|$ n'a qu'un seul facteur premier p, autrement dit $|\mathrm{G}| = p^m$. Si g appartient à $\mathrm{G} \smallsetminus \{e\}$, alors le Théorème de Lagrange (Théorème 1.6.4 assure que l'ordre de g appartient à $\{p, p^2, \ldots, p^m\}$. Cependant le Théorème de Cauchy (Théorème 3.7.1) assure l'existence d'au moins un élément d'ordre p ; par hypothèse tous les éléments de $\mathrm{G} \smallsetminus \{e\}$ sont d'ordre p. □

Exemple 3.7.1. — Les groupes abéliens correspondant à l'hypothèse du Théorème 3.7.3 sont faciles à décrire, ce sont les $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$ où p est premier ; tout élément non nul est d'ordre p. Un exemple non abélien est le groupe d'Heisenberg sur $\mathbb{Z}/p\mathbb{Z}$ lorsque p est un nombre premier impair ; tout élément non trivial est d'ordre p.

Corollaire 3.7.1

Le cardinal de tout corps fini est une puissance première.

Démonstration. — Soit $\Bbbk$ un corps fini. Il est de cardinal ≥ 2 (puisque $1 \neq 0$ dans $\Bbbk$). Nous allons regarder $\Bbbk$ comme un groupe additif. Chaque paire d'éléments non nuls a et b dans $\Bbbk$ (éventuellement égaux) a le même ordre (pour la loi $+$), puisque la fonction $f(x) = (b/a)x$

est additive, inversible, et envoie a sur fb. Ainsi $\#\Bbbk$ est une puissance première d'après le Théorème 3.7.3. □

Théorème 3.7.4

Soient G un groupe fini et $k \in \mathbb{Z}$. La fonction $f(x) = x^k$ sur G est une bijection si et seulement si $\mathrm{pgcd}(k, |\mathrm{G}|) = 1$.

Lorsque G n'est pas abélien, l'application $x \mapsto x^k$ n'est pas un morphisme en général. Néanmoins, on peut se demander s'il s'agit d'une bijection ou non.

Démonstration. — Posons $n = |\mathrm{G}|$.

Supposons dans un premier temps que $\mathrm{pgcd}(k, n) = 1$. Il existe alors ℓ et m tels que $k\ell = 1 + nm$. Ainsi tout $x \in \mathrm{G}$ satisfait $x^{k\ell} = xx^{nm} = x$. Ceci montre que $\mathrm{G} \to \mathrm{G}$, $x \mapsto x^k$ a une fonction inverse $x \mapsto x^\ell$ puisque $(x^k)^\ell = x$ et $(x^\ell)^k = x$ pour tout $x \in \mathrm{G}$. En particulier, $\mathrm{G} \to \mathrm{G}$, $x \mapsto x^k$ est une bijection.

Supposons désormais que $\mathrm{pgcd}(k, n) > 1$. Nous allons montrer que $\mathrm{G} \to \mathrm{G}$, $x \mapsto x^k$ n'est pas une bijection. Comme k et n ont un facteur commun non trivial, ils ont un facteur premier commun p. Étant donné que p divise n, le théorème de Cauchy (Théorème 3.7.1) assure que G contient un élément g d'ordre p. Alors, puisque p divise k, nous avons : $g^k = (g^p)^{k/p} = e^{k/p} = e$. Ainsi, $\mathrm{G} \to \mathrm{G}$, $x \mapsto x^k$ n'est pas injective : $g \neq e$ et $g^k = e^k = e$; en particulier ce n'est pas une bijection. □

3.7.3. Décomposition des groupes abéliens. — Le théorème de Cauchy nous permet de décrire comment décomposer un groupe abélien fini en sous-groupes d'ordre p^k, p premier.

Théorème 3.7.5

Soit G un abélien fini d'ordre ab avec $\mathrm{pgcd}(a, b) = 1$. Alors G est isomorphe à un produit direct $\mathrm{A} \times \mathrm{B}$ où $|\mathrm{A}| = a$ et $|\mathrm{B}| = b$.

Démonstration. — Si a ou b vaut 1, le résultat est clair : on prend $\mathrm{A} = \{e\}$ ou $\mathrm{B} = \{e\}$.

Puisque $|\mathrm{G}| = ab$, nous avons $g^{ab} = e$ pour tout $g \in \mathrm{G}$. Pour tout $m \geq 1$ les éléments g de G tels que $g^m = e$ forment un sous-groupe de G puisque G est abélien. Considérons les deux sous-groupes de G définis par

$$\mathrm{A} = \{g \in \mathrm{G} \mid g^a = e\}, \qquad \mathrm{B} = \{g \in \mathrm{G} \mid g^b = e\}.$$

Montrons que $\mathrm{G} = \mathrm{AB}$, c'est-à-dire que tout élément de G est le produit d'un élément de A et d'un élément de B. Par Bézout, il existe r et s dans $\mathbb{Z}$ tels que $1 = ar + bs$. Par conséquent chaque $g \in \mathrm{G}$ peut s'écrire $g = g^{ar+bs} = (g^r)^a(g^s)^b$. Remarquez $(g^r)^a$ appartient à B puisque $((g^r)^a)^b = (g^r)^{ab} = e$; de même $(g^s)^b$ appartient à A. Par suite tout élément g de G s'écrit sous la forme $g = (g^s)^b(g^r)^a$, *i.e.* comme le produit d'un élément de A et d'un élément de B, donc $\mathrm{G} = \mathrm{AB}$.

Montrons maintenant que G est isomorphe au produit direct $\mathrm{A} \times \mathrm{B}$. Soit $f\colon \mathrm{A} \times \mathrm{B} \to \mathrm{G}$ défini par : $f(x, y) = xy$. Étant donné que G est abélien, f est un morphisme de groupes :

$$f((x, y)(x', y')) = f(xx', yy') = xx'yy' = (xy)(x'y') = f(x, y)f(x', y').$$

Comme $\mathrm{G} = \mathrm{AB}$, f est surjective. Montrons que f est injective. Soit $(x, y) \in \mathrm{A} \times \mathrm{B}$ tel que $f(x, y) = e$. Alors $xy = e$, donc $x = y^{-1}$. Cette équation montre que x et y appartiennent à $\mathrm{A} \cap \mathrm{B}$. Puisque chaque élément de A a un ordre divisant a, chaque élément de B a un ordre divisant b, et $\operatorname{pgcd}(a, b) = 1$, l'intersection $\mathrm{A} \cap \mathrm{B}$ est triviale. Ainsi $x = e$ et $y = e$, donc $(x, y) = (e, e)$ est l'élément d'identité de $\mathrm{A} \times \mathrm{B}$; autrement dit $\ker f = \{(e, e)\}$.

Montrons que $|\mathrm{A}| = a$ et que $|\mathrm{B}| = b$. Puisque f est une bijection, $|\mathrm{A} \times \mathrm{B}| = |\mathrm{G}|$; il en résulte

$$|\mathrm{A}|\,|\mathrm{B}| = ab. \tag{3.7.2}$$

Montrons maintenant $(|\mathrm{A}|, b) = 1$. Si $(|\mathrm{A}|, b) \neq 1$, alors il existe un nombre premier p qui divise b et $|\mathrm{A}|$. Le Théorème de Cauchy assure l'existence d'un élément d'ordre p dans A. Mais chaque élément de A a un ordre divisant a, et p ne divise pas a (puisque p divise b et $\operatorname{pgcd}(a, b) = 1$). Ainsi $(|\mathrm{A}|, b) = 1$. De même, $(|\mathrm{B}|, a) = 1$. D'après (3.7.2), nous avons $|\mathrm{A}|$ divise ab donc $|\mathrm{A}|$ divise a. De même $|\mathrm{B}|$ divise b. Finalement (3.7.2) assure que $|\mathrm{A}| = a$ et que $|\mathrm{B}| = b$. □

Corollaire 3.7.2

Tout groupe abélien fini est isomorphe à un produit direct de groupes abéliens finis dont l'ordre est une puissance d'un entier.

Démonstration. — Soit G un groupe abélien fini, d'ordre $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. On peut supposer que $n > 1$ et que chaque e_i est non nul. Si $a = p_1^{e_1}$ et $b = \frac{n}{a}$, alors $\operatorname{pgcd}(a, b) = 1$. Le Théorème 3.7.5 assure que G est isomorphe à un produit direct $\mathrm{A} \times \mathrm{B}$ avec $|\mathrm{A}| = a = p_1^{e_1}$ et $|\mathrm{B}| = b = \frac{n}{a}$. Puisque $a > 1$, par récurrence sur l'ordre nous obtenons que B est isomorphe à un produit direct de groupes d'ordre $p_2^{e_2}$, $p_3^{e_3}$, …, $p_r^{e_r}$. □

3.7.4. Groupes d'ordre pq. — Nous allons donner une classification, à isomorphisme près, des groupes d'ordre pq, où p et q désignent des nombres premiers distincts.

Théorème 3.7.6

Soient p et q des nombres premiers distincts, avec $p < q$.
Si $q \not\equiv_p 1$, alors tous les groupes d'ordre pq sont cycliques. En particulier, tous les groupes d'ordre pq sont isomorphes.
Si $q \equiv_p 1$, alors il existe à isomorphisme près deux groupes d'ordre pq : l'un est cyclique et l'autre non abélien.

Exemple 3.7.2. — Chaque groupe d'ordre 15 est cyclique. En effet $15 = 3 \times 5$ et $5 \not\equiv_3 1$.

Exemple 3.7.3. — On connaît déjà deux groupes non isomorphes d'ordre 6 ($p = 2$, $q = 3$) : $\mathbb{Z}/6\mathbb{Z}$ et $\mathfrak{S}_3$. Le premier est cyclique et le second ne l'est pas (il est non abélien). Le Théorème 3.7.6 assure que chaque groupe d'ordre 6 est isomorphe à l'un d'entre eux. Voici un tableau répertoriant des exemples de groupes abéliens et non abéliens d'ordre 6.

groupes abéliens	groupes non abéliens
$\mathbb{Z}/6\mathbb{Z}$	$\mathfrak{S}_3$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	D_6
$\left(\mathbb{Z}/9\mathbb{Z}\right)^\times$	$\mathrm{Aff}\left(\mathbb{Z}/3\mathbb{Z}\right)$
μ_6	$\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$

Les groupes de chaque colonne sont isomorphes.

La démonstration du Théorème 3.7.6 utilise l'énoncé suivant.

Lemme 3.7.1

Soit G un groupe d'ordre pq, où p et q désignent des nombres premiers tels que $p < q$. Le groupe G possède un seul sous-groupe d'ordre q.

Remarque 3.7.2. — Les hypothèses ne sont pas symétriques en p et q ; le lemme concerne les sous-groupes avec l'ordre premier le plus grand.

Démonstration. — Le théorème de Cauchy assure l'existence d'un sous-groupe de G d'ordre q. Comme q est premier, ce sous-groupe est cyclique ; écrivons-le sous la forme $\langle g \rangle$. Afin de montrer que $\langle g \rangle$ est le seul sous-groupe d'ordre q, nous allons raisonner par l'absurde : supposons qu'il existe $h \in \mathrm{G}$ d'ordre q tel que $h \notin \langle g \rangle$. Alors $\langle h \rangle \cap \langle g \rangle$ est trivial : cette intersection est un sous-groupe de $\langle h \rangle$ qui ne peut pas être $\langle h \rangle$ (car $h \notin \langle g \rangle$), il doit donc être trivial car le seul sous-groupe propre de $\langle h \rangle$ est trivial. Considérons les classes à gauche de $\langle g \rangle$ représentées par des puissances de h :

$$\langle g \rangle,\ h\langle g \rangle,\ h^2\langle g \rangle,\ \ldots,\ h^{q-1}\langle g \rangle; \tag{3.7.3}$$

il y a q classes à gauche dans cette liste. Le nombre de classes à gauche distinctes de $\langle g \rangle$ est $[\mathrm{G} : \langle g \rangle] = \frac{pq}{q} = p$. Puisque $p < q$, deux des classes de (3.7.3) doivent être égales, par exemple $h^i\langle g \rangle = h^{i'}\langle g \rangle$ avec $0 \leq i < i' \leq q-1$. Alors $h^{i'-i}$ appartient à $\langle g \rangle$ et est une puissance de h distincte de l'identité et égale à une puissance de g : contradiction. Autrement dit, chaque élément de G d'ordre q appartient à $\langle g \rangle$; il en résulte que $\langle g \rangle$ est l'unique sous-groupe d'ordre q. □

Exemple 3.7.4. — Considérons le groupe D_{10} d'ordre 10. Ici $q = 5$. Il existe un sous-groupe d'ordre 5, celui des rotations.

Nous sommes maintenant prêts à démontrer une partie du Théorème 3.7.6 :

Théorème 3.7.7

Soient p, q des nombres premiers tels que $p < q$. Chaque groupe abélien d'ordre pq est cyclique. Si $q \not\equiv_p 1$, alors chaque groupe d'ordre pq est cyclique.

Les exemples satisfaisant la condition $q \not\equiv_p 1$ sont $15 = 3 \times 5$, $35 = 5 \times 7$, 33, 65, 77 et 95. Chaque groupe de cet ordre est cyclique.

Démonstration. — Soit G un groupe fini d'ordre pq. D'après le théorème de Cauchy, le groupe G possède un élément a d'ordre p et un élément b d'ordre q. Si G est abélien alors ab est d'ordre pq, donc G est cyclique.

Le reste de la démonstration est consacré à montrer que, lorsque $q \not\equiv_p 1$, a et b doivent commuter, même si le groupe G n'est pas supposé abélien, auquel cas nous obtenons une nouvelle fois que ab est d'ordre pq et G est cyclique. Comme aba^{-1} est un conjugué de b, il est d'ordre q. Le Lemme 3.7.1 assure que aba^{-1} est une puissance de b, c'est-à-dire $aba^{-1} = b^k$ pour un entier k. Par récurrence, $a^m b a^{-m} = b^{km}$ pour tout $m \geq 1$. Pour $m = p$ nous obtenons $b = b^{kp}$. Comme b est d'ordre q, cette égalité implique $kp \equiv_q 1$, donc k est ordre soit 1, soit p dans le groupe $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ qui est d'ordre $q-1$. Si k est d'ordre p, alors p divise $(q-1)$ donc $q \equiv_p 1$: contradiction. Ainsi l'ordre de k dans $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ est 1, donc $k \equiv_q 1$ et $aba^{-1} = b^k = b^1 = b$, ce qui se réécrit $ab = ba$. □

Jusqu'à présent, nous avons démontré le Théorème 3.7.6 si $q \not\equiv_p 1$ et partiellement (c'est-à-dire pour les groupes abéliens) si $q \equiv_p 1$. Qu'en est-il des groupes non abéliens d'ordre pq pour les nombres premiers $p < q$ si $q \equiv_p 1$? Il existe toujours un groupe non abélien d'ordre pq lorsque $q \equiv_p 1$. En voici un, construit en tant que sous-groupe du groupe affine $\mathrm{Aff}\left(\mathbb{Z}/q\mathbb{Z}\right)$:

$$\mathrm{A}_{p,q} = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}\left(\mathbb{Z}/q\mathbb{Z}\right) \mid x^p = 1 \text{ dans } \mathbb{Z}/q\mathbb{Z} \right\}. \tag{3.7.4}$$

On peut vérifier qu'il s'agit d'un sous-groupe de $\mathrm{Aff}\left(\mathbb{Z}/q\mathbb{Z}\right)$. Pour déterminer son ordre notons qu'il y a q choix pour y, puisque nous n'avons pas imposé de contrainte sur y. Déterminons maintenant les choix possibiles pour x. Puisque x appartient à $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ et $p|(q-1)$ par hypothèse, le théorème de Cauchy assure l'existence d'un élément d'ordre p dans $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$, et donc ses puissances donnent au moins p solutions à $x^p = 1$ dans $\mathbb{Z}/q\mathbb{Z}$. Il ne peut y avoir plus de p solutions (voir Théorème 3.7.9) ; il y a donc exactement p solutions. Ainsi les solutions de $x^p = 1$ dans $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ forment un groupe cyclique d'ordre p. Par suite $|\mathrm{A}_{p,q}| = pq$. Le

groupe $\mathrm{A}_{p,q}$ n'est pas abélien, puisque les matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ ne commutent pas (x désigne ici un élément d'ordre p dans $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$.

Exemple 3.7.5. — Lorsque $p = 3$ et $q = 7$, alors $q \equiv_p 1$. Les solutions de $x^3 \equiv_7 1$ sont 1, 2 et 4, donc un groupe non abélien d'ordre 21 est

$$\mathrm{A}_{3,7} = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \middle| x,\, y \in \mathbb{Z}/7\mathbb{Z}, x \equiv_7 1,\, y \equiv_7 2,\, Z \equiv_7 4 \right\}.$$

Nous sommes maintenant prêts à compléter la démonstration du Théorème 3.7.6 avec le cas non abélien, $q \equiv_p 1$.

Théorème 3.7.8

Soient p et q des nombres premiers tels que $p < q$ et $q \equiv_p 1$. Le groupe $\mathrm{A}_{p,q}$ défini dans (3.7.4) est, à isomorphisme près, l'unique groupe non abélien d'ordre pq.

Démonstration. — Soit G un groupe non abélien d'ordre pq. Le Théorème de Cauchy assure que G contient un élément a d'ordre p et un élément b d'ordre q. Si a et b commutent, alors ab est d'ordre pq et G est cyclique ; mais G n'est pas abélien, donc a et b ne commutent pas. Puisque $\langle a,\, b\rangle$ contient des sous-groupes d'ordre p et q, $|\langle a,\, b\rangle|$ est divisible par pq, donc $\langle a,\, b\rangle = \mathrm{G}$.

D'après le Lemme 3.7.1 (nous utilisons ici la condition $p < q$), tous les éléments de G d'ordre q sont des puissances de b, donc $aba^{-1} = b^t$ pour un certain t. Nécessairement $t \not\equiv_q 1$, sinon nous aurions $aba^{-1} = b$, ce qui impliquerait $ab = ba$, mais a et b ne commutent pas.

La relation $aba^{-1} = b^t$ entraîne pour tout $k \geq 0$

$$a^k b a^{-k} = b^{tk}. \tag{3.7.5}$$

En prenant $k = p$, nous avons $b = b^{tp}$ d'où $t^p \equiv_q 1$. Ainsi t est d'ordre p dans $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$.

De plus, élever (3.7.5) à une puissance entière arbitraire conduit à $a^k b^\ell a^{-k} = b^{t^k}$. Ainsi

$$a^k b^\ell = b^{\ell t^k} a^k \tag{3.7.6}$$

et

$$\mathrm{G} = \langle a,\, b\rangle = \{b^n a^m \,|\, m,\, n \geq 0\}. \tag{3.7.7}$$

Étudions maintenant le groupe $\mathrm{A}_{p,q}$. Le premier coefficient d'une matrice de ce groupe est un élément de $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ d'ordre divisant p. Parce que les solutions de $x^p = 1$ dans $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ forment un sous-groupe d'ordre p et t est d'ordre p dans $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$, ces solutions sont exactement

les puissances de t. Chaque matrice de $\mathrm{A}_{p,q}$ a donc la forme suivante, où m, $n \geq 0$:

$$\begin{pmatrix} t^m & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t^m & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}^m.$$

Cela suggère que puisque $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre q (comme b) et $\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}$ est d'ordre p (comme a), de considérer la fonction $f\colon \mathrm{A}_{p,q} \to \mathrm{G}$ définie par :

$$f\begin{pmatrix} t^m & n \\ 0 & 1 \end{pmatrix} = b^n a^m.$$

Cette fonction f est bien définie, puisque m intervient seulement modulo p et n seulement modulo q.

Soient $A = \begin{pmatrix} t^m & n \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} t^{m'} & n' \\ 0 & 1 \end{pmatrix}$ dans $\mathrm{A}_{p,q}$. Alors

$$\begin{aligned} f(AB) &= f\left(\begin{pmatrix} t^m & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} t^{m'} & n' \\ 0 & 1 \end{pmatrix}\right) \\ &= f\begin{pmatrix} t^{m+m'} & t^m n' + n \\ 0 & 1 \end{pmatrix} \\ &= b^{t^m n' + n} a^{m+m'} \\ &= b^n b^{t^m n'} a^m a^{m'} \\ &= b^n a^m b^{n'} a^{m'} \text{ d'après (3.7.7)} \\ &= f(A)f(B). \end{aligned}$$

La surjectivité de f est assurée par (3.7.7), qui montre que chaque élément de G est une valeur de f.

Puisque $f\colon \mathrm{A}_{p,q} \to \mathrm{G}$ est surjectif et $|\mathrm{A}_{p,q}| = |\mathrm{G}|$, le morphisme f est bijectif. □

Corollaire 3.7.3

Soit q un nombre premier. Un groupe d'ordre $2q$ est soit cyclique, soit diédral ; autrement dit un groupe d'ordre $2q$ est isomorphe à $\mathbb{Z}/2q\mathbb{Z}$ ou à D_{2q}.

Démonstration. — Supposons dans un premier temps que $q \geq 3$. Prenons $p = 2$ dans le Théorème 3.7.8 ; on constate que $\mathrm{A}_{2,q}$ de $\mathrm{Aff}\left(\mathbb{Z}/q\mathbb{Z}\right)$ est l'un des « modèles matriciels » de D_{2q}.

Pour finir supposons que $q = 2$. Rappelons que d'une part $\mathrm{D}_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, d'autre part qu'un groupe d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (Théorème 2.2.7) ; l'énoncé est donc aussi vrai pour $q = 2$. □

Remarque 3.7.3. — Lorsque $p = q$, les groupes d'ordre $pq = p^2$ peuvent être classés à isomorphisme près. Comme dans le Théorème 3.7.6, il existe deux de ces groupes, mais tous deux sont abéliens : l'un est cyclique et l'autre est $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

3.7.5. Décompte des racines. — Nous démontrons ici un résultat sur les polynômes utilisé pour déterminer $|\mathrm{A}_{p,q}|$ dans §3.7.4.

Théorème 3.7.9

Soit P un polynôme non constant à coefficients en $\mathbb{Z}/p\mathbb{Z}$, de degré d. Alors P a au plus d racines dans $\mathbb{Z}/p\mathbb{Z}$.

Lemme 3.7.2

Soit P un polynôme non constant à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Soit a dans $\mathbb{Z}/p\mathbb{Z}$, nous avons : $P(a) = 0$ si et seulement si $X - a$ est un facteur de P.

Exemple 3.7.6. — Lorsque les coefficients sont $\mathbb{Z}/5\mathbb{Z}$ le polynôme $P = X^3 - 2$ est tel que $P(3) = 0$ et $P = (X - 3)(X^2 + 3X - 1)$.

Démonstration du Lemme 3.7.2. — Si $X - a$ est un facteur de P, alors $P(X) = (X - a)Q(X)$ et $P(a) = (a - a)Q(a) = 0$.

Réciproquement supposons que $P(a) = 0$. Écrivons le polynôme sous la forme

$$P(x) = c_n X^n + c_{n-1} X^{n-1} + \ldots + c_1 X + c_0, \tag{3.7.8}$$

avec $c_j \in \mathbb{Z}/p\mathbb{Z}$ et $c_n \neq 0$. Alors

$$0 = c_n a^n + c_{n-1} a^{n-1} + \ldots + c_1 a + c_0. \tag{3.7.9}$$

En soustrayant (3.7.9) à (3.7.8), nous obtenons

$$P = c_n(X^n - a^n) + c_{n-1}(X^{n-1} - a^{n-1}) + \ldots + c_1(X - a).$$

Puisque

$$X^j - a^j = (X - a)(X^{j-1} + aX^{j-2} + \ldots + a^i X^{j-1-i} + \ldots + a^{j-2}X + a^{j-1}),$$

chaque $c_i(X^i - a^i)$ se factorise par $X - a$; par suite il existe un polynôme Q à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ tel que $P(X) = (X - a)Q(X)$. □

Démonstration du Théorème 3.7.9. — On raisonne par récurrence sur le degré $d \geq 1$ de P.

Un polynôme de degré 1 est de la forme $P = aX + b$, avec a, b dans $\mathbb{Z}/p\mathbb{Z}$ et $a \neq 0$. Celui-ci a exactement une racine $(-\frac{b}{a})$ dans $\mathbb{Z}/p\mathbb{Z}$ et donc au plus une racine dans $\mathbb{Z}/p\mathbb{Z}$.

Supposons maintenant que le théorème soit vrai pour tous les polynômes de degré d à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. On cherche alors à établir le résultat pour tous les polynômes de degré $d+1$ à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Un polynôme de degré $d+1$ s'écrit sous la forme

$$P = c_{d+1}X^{d+1} + c_dX^d + \ldots + c_1X + c_0,$$

avec $c_j \in \mathbb{Z}/p\mathbb{Z}$ et $c_{d+1} \neq 0$. Si P n'a pas de racines dans $\mathbb{Z}/p\mathbb{Z}$, alors l'énoncé est vrai $(0 \leq d+1)$. Si P a une racine dans $\mathbb{Z}/p\mathbb{Z}$, disons r, alors le Lemme 3.7.2 assure que $P = (X - r)Q$, où Q désigne un polynôme de degré d à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. On peut appliquer l'hypothèse de récurrence à Q : le polynôme Q a au plus d racines dans $\mathbb{Z}/p\mathbb{Z}$. Puisque $P(a) = (a - r)Q(a)$ pour tout $a \in \mathbb{Z}/p\mathbb{Z}$ et puisqu'un produit dans $\mathbb{Z}/p\mathbb{Z}$ vaut 0 seulement quand un des facteurs est 0, on obtient : une racine de P dans $\mathbb{Z}/p\mathbb{Z}$ est soit r, soit une racine de Q. Ainsi, P a au plus $d+1$ racines dans $\mathbb{Z}/p\mathbb{Z}$. $\square$

CHAPITRE 4

GROUPES ABÉLIENS INFINIS, FINIS, DE TYPE FINI, DE TORSION

4.0.1. Brefs rappels sur les anneaux. — Commençons ce paragraphe par quelques rappels en théorie des anneaux commutatifs, sans démonstration. Soit A un anneau commutatif (unitaire) et soit $\mathcal{I}$ un idéal de A ; c'est en particulier un sous-groupe additif de A.

4.0.1.1. *Structure d'anneau sur* $A/\mathcal{I}$. — Si x et y sont deux éléments de A, la classe modulo $\mathcal{I}$ de xy ne dépend que des classes de x et y modulo $\mathcal{I}$. La multiplication de A induit donc une loi interne supplémentaire sur le groupe abélien $\left(A/\mathcal{I}, +\right)$, qui fait de celui-ci un anneau commutatif.

4.0.1.2. *Propriété universelle du quotient.* — Le morphisme quotient $\pi\colon A \to A/\mathcal{I}$ est alors un morphisme d'anneaux de noyau $\mathcal{I}$, et il satisfait la propriété universelle suivante : pour tout anneau commutatif B, la formule $\psi \mapsto \psi \circ \pi$ établit une bijection entre l'ensemble des morphismes d'anneaux de $A/\mathcal{I}$ vers B et l'ensemble des morphismes de A vers B dont le noyau contient $\mathcal{I}$. Elle caractérise le morphisme $A \to A/\mathcal{I}$ à unique isomorphisme près.

4.0.1.3. *Quotient par un sous-ensemble.* — Si E désigne un ensemble de générateurs de l'idéal $\mathcal{I}$, la formule $\psi \mapsto \psi \circ \pi$ établit également une bijection entre l'ensemble des morphismes d'anneaux de $A/\mathcal{I}$ vers B et l'ensemble des morphismes de A vers B dont le noyau contient E.

Remarque 4.0.1. — On se retrouve avec un phénomène analogue à ceux constatés en théorie des ensembles et en théorie des groupes : $A/\mathcal{I}$ apparaît à la fois comme l'anneau commutatif le plus général construit à partir de A en décrétant que les éléments de $\mathcal{I}$ sont nuls, et comme l'anneau commutatif le plus général construit à partir de A en se contentant de décréter que les éléments de E sont nuls. Attention quand on force les éléments de E à être triviaux, on trivialise du même coup tous les éléments de $\mathcal{I}$ (mais les dégâts s'arrêtent là, le noyau de $A \to A/\mathcal{I}$ étant précisément $\mathcal{I}$).

4.0.1.4. *Idéaux de* A/I. — Les formules $J \mapsto \varphi(K)$ et $K \mapsto \varphi^{-1}(K)$ établissent une bijection entre l'ensemble des idéaux de A contenant $\mathcal{I}$ et l'ensemble des idéaux de $A/\mathcal{I}$.

4.0.1.5. *L'isomorphisme fondamental.* — Soit $f\colon A \to B$ un morphisme d'anneaux commutatifs. Il induit un isomorphisme d'anneaux entre $A/\ker f$ et $\operatorname{im} f$.

4.0.2. Sommes et sommes directes internes dans les groupes abéliens. — Soit G un groupe abélien noté additivement et soit (G_i) une famille de sous-groupes de G.

D'après la Remarque **??** le sous-groupe de G engendré par les G_i est l'ensemble des éléments de G de la forme $\sum g_i$ où (g_i) est une famille d'éléments de G presque tous nuls (en algèbre *on fait uniquement des sommes finies*) tels que $g_i \in \mathrm{G}_i$ pour tout i. Ce sous-groupe est la *somme des* G_i ; il est noté $\sum \mathrm{G}_i$. Les G_i sont en *somme directe* si tout élément de $\sum \mathrm{G}_i$ a une unique écriture sous la forme $\sum g_i$ comme ci-dessus ; on écrit alors $\sum \mathrm{G}_i = \oplus \mathrm{G}_i$.

4.0.2.1. *Propriétés élémentaires.* — Nous allons énoncer des faits sans les démontrer (les démonstrations étant analogues à celles rencontrées dans le cadre de l'algèbre linéaire).

Pour que $\sum \mathrm{G}_i = \oplus \mathrm{G}_i$ il suffit de vérifier que

$$\sum g_i = 0 \quad \Rightarrow \quad \forall\, i \quad g_i = 0$$

pour toute famille (g_i) comme ci-dessus.

Si G_1 et G_2 sont deux sous-groupes de G, alors $\mathrm{G}_1 + \mathrm{G}_2 = \mathrm{G}_1 \oplus \mathrm{G}_2$ si et seulement si $\mathrm{G}_1 \cap \mathrm{G}_2 = \{0\}$.

4.0.2.2. *Somme d'idéaux.* — Soit A un anneau commutatif. Soit $(\mathcal{J}_i)_{i\in I}$ une famille d'idéaux de A. La somme $\sum \mathcal{J}_i$ est encore un idéal de A.

4.0.3. Somme directe externe de groupes abéliens. — Définissons désormais une notion de somme directe qui diffère de la précédente. Cette dernière était interne : elle portait sur les sous-groupes d'un groupe donné. Celle que nous allons présenter maintenant est externe : elle porte sur une famille de groupes qui ne sont pas a priori plongés dans un même groupe.

4.0.3.1. *La somme directe externe : construction.* — Soit (G_i) une famille de groupes abéliens notés additivement. Soit H le sous-ensemble de $\prod_i \mathrm{G}_i$ formé des éléments (g_i) tels que le g_i soient presque tous nuls ; c'est un sous-groupe de $\prod_i \mathrm{G}_i$. Pour tout j, notons h_j l'application de G_j dans $\prod_i \mathrm{G}_i$ qui envoie un élément γ sur la famille (g_i) telle que

$$\begin{cases} g_j = \gamma \\ g_i = 0 \text{ si } i \neq j \end{cases}$$

L'application h_j est un morphisme injectif de groupes.

Il résulte immédiatement de sa définition que le groupe H ci-dessus est la somme directe des $h_i(\mathrm{G}_i)$. Comme h_i induit pour tout i un isomorphisme entre G_i et $h_i(\mathrm{G}_i)$, on se permet de dire que le groupe H est la *somme directe externe* des G_i, et d'écrire $\mathrm{H} = \sum_i \mathrm{G}_i$. Cette construction force en quelque sorte les G_i à être contenus dans un même groupe H, et à être en somme directe dans ce dernier.

Remarque 4.0.2. — Rien n'interdit à plusieurs des G_i d'être égaux à un même groupe G. Ils seront néanmoins considérés comme des sommandes distincts de la somme directe externe $\oplus\mathrm{G}_i$; pour cette raison, on décrira parfois ces sommandes comme des copies de G.

Supposons donné pour tout i un sous-groupe H_i de G_i. La somme directe $\oplus\mathrm{H}_i$ s'identifie à un sous-groupe de $\oplus\mathrm{G}_i$ et on a un isomorphisme naturel entre ${}^{\oplus\mathrm{G}_i}\!/_{\oplus\mathrm{H}_i}$ et $\oplus{}^{\mathrm{G}_i}\!/_{\mathrm{H}_i}$.

Remarque 4.0.3. — Lorsque la famille (G_i) est finie, la somme directe $\oplus\mathrm{G}_i$ coïncide avec le produit $\prod \mathrm{G}_i$. Suivant le contexte on préfèrera l'une ou l'autre des notations. Ici nous utiliserons la notion produit.

4.1. Étude du groupe $\mathbb{Z}$: premières propriétés

Entamons l'étude du groupe abélien $\mathbb{Z}$ et établissons quelques unes de ses propriétés qui sont à la base de l'arithmétique.

Remarque 4.1.1. — Soit G un groupe abélien noté additivement. Soit g un élément de G. Soit n un entier. L'élément ng de G est alors par définition

- ◇ la somme de n termes égaux à g si $n \geq 0$,
- ◇ et la somme de $-n$ termes égaux à $-g$ sinon.

Mais lorsque G est lui-même égal à $\mathbb{Z}$ cet élément coïncide avec le produit de n et g au sens de la multiplication de $\mathbb{Z}$. En particulier, tout sous-groupe de $(\mathbb{Z}, +)$ est automatiquement stable par multiplication externe par les éléments de $\mathbb{Z}$ et est donc un idéal de $\mathbb{Z}$.

Soit $d \in \mathbb{Z}$. Le sous-groupe de $\mathbb{Z}$ engendré par d (qui est aussi en vertu de ce qui précède l'idéal principal de $\mathbb{Z}$ engendré par d) n'est autre que $d\mathbb{Z} = \{dn \,|\, n \in \mathbb{Z}\}$. Soit $d' \in \mathbb{Z}$; les équivalences suivantes sont immédiates

$$d\mathbb{Z} \subset d'\mathbb{Z} \quad \Longleftrightarrow \quad d' \,|\, d$$

et

$$(d\mathbb{Z} = d'\mathbb{Z}) \quad \Longleftrightarrow \quad (d' \,|\, d \text{ et } d \,|\, d') \quad \Longleftrightarrow \quad \exists\, \varepsilon \in \{-1,\, 1\},\, d' = \varepsilon d.$$

Par suite le générateur d'un idéal principal de $\mathbb{Z}$ est uniquement déterminé au signe près [1]. Il peut donc toujours être choisi dans $\mathbb{N}$ et est alors unique.

Rappelons que tout sous-groupe de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$ pour un unique $d \in \mathbb{N}$ (Théorème **??**). Cet énoncé assure en particulier que tout idéal de l'anneau commutatif intègre $\mathbb{Z}$ est principal ; l'anneau $\mathbb{Z}$ est donc ce qu'on appelle un *anneau principal*.

Les propriétés que nous allons maintenant énoncer et démontrer pour $\mathbb{Z}$ valent en fait pour tout anneau principal, avec essentiellement les mêmes démonstrations.

1. Ce fait s'étend à tout anneau commutatif intègre à condition de remplacer « au signe près » par « à un inversible près ».

4.1.1. Le pcgd. — Soit $(a_i)_{i\in I}$ une famille d'éléments de $\mathbb{Z}$. Soit n un élément de $\mathbb{Z}$. L'élément n divise chacun des a_i si et seulement si $a_i \in n\mathbb{Z}$ pour tout i. Cela revient à demander que $n\mathbb{Z}$ contienne l'idéal $\sum_i a_i\mathbb{Z}$ engendré par les a_i. Ce dernier est de la forme $d\mathbb{Z}$ pour un entier $d \in \mathbb{Z}$ uniquement déterminé au signe près. Par conséquent, n divise chacun des a_i si et seulement si $d\mathbb{Z} \subset n\mathbb{Z}$, c'est-à-dire si et seulement si n divise d. L'entier d est appelé le *plus grand commun diviseur* (pgcd) des a_i.

Remarquons que pour que le pgcd d des a_i soit non nul, il faut et il suffit que $\sum a_i\mathbb{Z}$ soit non nul, *i.e.* qu'il existe i tel que $a_i \neq 0$. Si c'est le cas, l'égalité $\sum a_i\mathbb{Z} = d\mathbb{Z}$ implique que $\sum(a_i/d)\mathbb{Z} = \mathbb{Z}$; le pgcd des (a_i/d) vaut donc 1.

Si a et b sont deux éléments de $\mathbb{Z}$ et si d désigne leur pgcd, on a par définition l'égalité $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$; il s'ensuit qu'il existe u et v dans $\mathbb{Z}$ tels que $au + bv = d$ (relation de Bezout). Les entiers a et b sont *premiers entre eux* si $d = 1$. Cela revient à demander que $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$; il suffit pour cela que $a\mathbb{Z} + b\mathbb{Z}$ contienne 1, *i.e.* qu'il existe u et v dans $\mathbb{Z}$ tels que $au + bv = 1$.

4.1.2. Le ppcm. — Soit $(a_i)_{i\in I}$ une famille d'éléments de $\mathbb{Z}$. Soit n un élément de $\mathbb{Z}$. L'élément n est multiple de chacun des a_i si et seulement si n appartient à $a_i\mathbb{Z}$ pour tout i. Cela revient à demander que $n\mathbb{Z}$ soit contenu dans $\bigcap_i a_i\mathbb{Z}$; ce dernier est de la forme $d\mathbb{Z}$ pour un entier $d \in \mathbb{Z}$ uniquement déterminé au signe près. Par suite n est multiple de chacun des a_i si et seulement si $n\mathbb{Z}$ est contenu dans $d\mathbb{Z}$, *i.e.* si et seulement si n est multiple de d. L'entier d est appelé le *plus petit multiple commun* des a_i.

Remarque 4.1.2. — Si l'un des a_i est nul, le ppcm des a_i est nul. La réciproque est fausse ; en effet par exemple le ppcm de tous les entiers strictement positifs est multiple de tout entier > 0 donc est nul. Par contre si la famille (a_i) est finie et si le ppcm des a_i est nul le produit des a_i est nul (car il est multiple de leur ppcm) si bien que l'un des a_i au moins est nul.

Lemme 4.1.1: (Lemme de Gauss)

Soient a, b et c trois éléments de $\mathbb{Z}$. Si a divise bc et si a est premier avec b, alors a divise c.

Démonstration. — Soit n un entier tel que $bc = an$. Choissisons une relation de Bezout $au + bv = 1$. Nous avons alors

$$c = c(au + bv) = aux + bcv = auc + anv = a(uc + nv).$$

□

Corollaire 4.1.1

Soient a_1, a_2, ..., a_r et b des éléments de $\mathbb{Z}$. Supposons que b soit premier avec chacun des a_i, alors il est premier avec $a_1 a_2 \dots a_r$.

Démonstration. — Nous raisonnons par récurrence sur r.

Si $r = 0$, alors b est premier avec $a_1 a_2 \dots a_r$ car ce dernier est égal à 1 et l'énoncé est vrai.

Supposons que $r > 0$ et que l'énoncé soit vrai pour les entiers $< r$. Désignons par d le pgcd de b et de $a_1 a_2 \dots a_r$. Par définition d divise $a_1 a_2 \dots a_r$. Par ailleurs tout diviseur commun de d et de l'un des a_j est un diviseur commun de b et a_j, et vaut donc 1 ou -1. Il en résulte que d est premier avec chacun des a_j. Puisque d est premier avec a_1 et divise $a_1 a_2 \dots a_r$ le lemme de Gauss assure que d divise $a_2 a_3 \dots a_r$. Comme d est premier avec chacun des a_j l'hypothèse de récurrence assure que d est premier avec $a_2 a_3 \dots a_r$; étant donné que d divise $a_2 a_3 \dots a_r$ et est premier avec $a_2 a_3 \dots a_r$, d vaut 1 ou -1. □

Définition 4.1.1

Un *nombre premier* est un élément p de $\mathbb{N}$ qui est > 1 et qui admet pour seuls diviseurs 1 et lui-même.

Théorème 4.1.1: (Écriture comme produit de nombres premiers)

Tout élément non nul n de $\mathbb{Z}$ possède une écriture sous la forme $\varepsilon \prod_{i=1}^{n} p_i^{n_i}$ où $\varepsilon \in \{1, -1\}$, où les p_i sont des nombres premiers deux à deux distincts et où les n_i sont des entiers > 1.
Une telle écriture est unique à permutation près des p_i.

Démonstration. — **Existence**. Montrons d'abord l'existence d'une telle écriture par récurrence sur $|n|$.

Si $|n| = 1$, alors $n = 1$ ou $n = -1$; dans ces deux cas $\varepsilon = n$ et la famille des p_i est vide. L'énoncé est donc vrai.

Supposons $|n| > 1$ et le théorème vrai pour les entiers de valeur absolue $< |n|$. Posons $\varepsilon = 1$ si n est positif et $\varepsilon = -1$ sinon. Si $|n|$ est premier, alors l'écriture $n = \varepsilon|n|$ est du type souhaité. Sinon nous pouvons écrire $|n| = m\ell$ où m et ℓ sont deux entiers strictement compris entre 1 et $|n|$. En vertu de l'hypothèse de récurrence m et ℓ sont tous deux produits d'un nombre fini de nombres premiers et $n = \varepsilon|n| = \varepsilon m\ell$ possède donc une écriture de la forme requise.

Unicité. Montrons maintenant l'unicité. Celle de ε est claire : c'est le signe de n. Reste à s'assurer que si $p_1 p_2 \dots p_m = q_1 q_2 \dots q_s$, où les p_i et q_j sont des nombres premiers (pas forcément deux à deux distincts) alors $m = s$ et il existe une permutation σ de $\{1, \dots, m\}$

telle que $q_i = p_{\sigma(i)}$ pour tout i. Procédons par récurrence sur m. Si $m = 0$, alors la famille des p_i est vide et $q_1 q_2 \dots q_s = 1$. Comme un nombre premier est par définition strictement supérieur à 1, cette dernière égalité force s à être nul et la famille des q_j à être vide ce qu'il fallait établir. Supposons désormais que $m > 0$ et que l'assertion est vraie pour $m - 1$. L'entier p_1 divise $q_1 q_2 \dots q_s$. Il est alors égal à l'un des q_j ; en effet dans le cas contraire p_1 serait premier à chacun des q_j et donc premier à $q_1 q_2 \dots q_s$ (Corollaire 4.1.1). On divise alors par p_1 les deux membres de l'égalité et on conclut en appliquant l'hypothèse de récurrence. □

Remarque 4.1.3. — La démonstration de l'existence de la décomposition en produit de facteurs premiers est élémentaire et n'utilise pas le fait que $\mathbb{Z}$ soit principal. Cette existence n'a en fait rien de particulièrement remarquable : on peut démontrer plus généralement que dans n'importe quel anneau commutatif intègre noethérien tout élément non nul est produit d'une famille finie d'éléments irréductibles.

C'est l'unicité de la décomposition qui fait sa force. Sa démonstration repose sur le lemme de Gauss, c'est-à-dire sur les relations de Bezout et donc la principalité de $\mathbb{Z}$.

Lemme 4.1.2

Soient a et b deux entiers. Au signe près nous avons l'égalité

$$ab = \operatorname{pgcd}(a, b) \cdot \operatorname{ppcm}(a, b).$$

Démonstration. — Soit d le pgcd de a et b ; soit m leur ppcm. Choisissons une relation de Bezout $au + bv = 1$.

- ◇ Si a et b sont nuls, alors $d = m = 0$ et le lemme est clair.
- ◇ Supposons que a et b ne soient pas tous deux nuls. Dans ce cas $d \neq 0$. Posons $\alpha = \frac{a}{d}$ et $\beta = \frac{b}{d}$. Montrons que le ppcm de (a, b) est égal au signe près à $d\alpha\beta$ ce qui permettra de conclure car $ab = d^2\alpha\beta$. Puisque $d\alpha = a$ et $d\beta = b$, le produit $d\alpha\beta$ est à la fois multiple de a et de b et est donc multiple de m. Il suffit dès lors de prouver que m est multiple de a et de b (et *a fortiori* de d). Écrivons $m = xa = yb$ avec x, y dans $\mathbb{Z}$. Alors

$$m = d\frac{m}{d} = (au + bv)\frac{m}{d} = \underbrace{yu\frac{ab}{d}}_{\text{car } m = yb} + \underbrace{xv\frac{ab}{d}}_{\text{car } m = xa} = (yu + xv)d\alpha\beta.$$

□

Soient a_1, a_2, …, a_m des éléments de $\mathbb{Z}$. La famille des réductions modulo les différents a_i définit un morphisme d'anneaux

$$\mathbb{Z} \to \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \dots \times \mathbb{Z}/a_m\mathbb{Z}.$$

Puisque son noyau contient visiblement $a_1 a_2 \dots a_m\mathbb{Z}$, il induit un morphisme d'anneaux

$$\mathbb{Z}/a_1 a_2 \dots a_m\mathbb{Z} \to \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \dots \times \mathbb{Z}/a_m\mathbb{Z}.$$

Lemme 4.1.3

Soit $(a_1, a_2, \ldots, a_m)$ une famille d'éléments de $\mathbb{Z}$ deux à deux premiers entre eux. Le morphisme d'anneaux naturel

$$\mathbb{Z}/a_1a_2\ldots a_m\mathbb{Z} \to \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_m\mathbb{Z}$$

est un isomorphisme.

Démonstration. — On procède par récurrence sur m.

Le cas $m = 0$ est trivial : nous avons l'anneau nul des deux côtés.

Supposons que $m \geq 1$ et que le résultat soit vrai pour les entiers strictement inférieurs à m. Posons $b = a_2a_3\ldots a_m$. L'hypothèse de récurrence assure que le morphisme naturel

$$\mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/a_2\mathbb{Z} \times \mathbb{Z}/a_3\mathbb{Z} \times \ldots \times \mathbb{Z}/a_m\mathbb{Z}$$

est un isomorphisme. Il suffit donc de motnrer que le morphisme naturel

$$\pi\colon \mathbb{Z}/(a_1b)\mathbb{Z} \to \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

est un isomorphisme.

Comme a_1 est premier avec les a_j pour $j > 1$, il est premier avec b (Corollaire 4.1.1). Choisissons une relation de Bezout $a_1u + bv = 1$.

Injectivité de π. Soit n un entier. L'image de n dans $\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est nulle si et seulement si n est à la fois multiple de a_1 et de b, donc si et seulement si n est multiple du ppcm de a_1 et b. Mais comme a_1 et b sont premiers entre eux ce ppcm vaut a_1b d'après le Lemme 4.1.2. Le noyau de $\mathbb{Z} \to \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est donc égal à $a_1b\mathbb{Z}$; il en résulte l'injectivité de π.

Surjectivité de π. Soient x et y deux éléments de $\mathbb{Z}$. Posons $z = ya_1u + xbv$. En écrivant $bv = 1 - a_1u$ on voit que z est égal à x modulo a_1. En écrivant $a_1u = 1 - bv$ on voit que z est égal à y modulo b. Par conséquent π est surjective. □

4.2. Propriété universelle de $\mathbb{Z}/d\mathbb{Z}$

Le but de ce qui suit est de décrire les morphismes de $\mathbb{Z}/d\mathbb{Z}$ vers un groupe donné G en commençant par le cas où $d = 0$, c'est-à-dire par les morphismes de $\mathbb{Z}$ dans G.

Définition 4.2.1

Soit G un groupe. Soit g un élément de G. On dit que g est de *n-torsion* s'il existe $n \in \mathbb{Z}$ tel que $g^n = e$.

4.2.1. Le cas abélien. — Soit G un groupe abélien noté additivement. Soit $n \in \mathbb{Z}$. L'application $g \mapsto ng$ de multiplication par n est alors un endomorphisme de G. Son image est notée nG et son noyau est précisément l'ensemble des éléments de n-torsion de G. Ce dernier est donc un sous-groupe de G.

Remarque 4.2.1. — Attention si G n'est pas abélien, les éléments de n-torsion de G ne forment pas un sous-groupe en général. Par exemple les éléments

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

de $\mathrm{GL}(2, \mathbb{R})$ sont de 2-torsion mais le produit AB n'est pas de 2-torsion.

4.2.2. La propriété universelle de $\mathbb{Z}$. — Soit G un groupe. Soit f un morphisme de $\mathbb{Z}$ dans G. Soit g l'image de 1. Pour tout $n \in \mathbb{Z}$ nous avons alors nécessairement

$$f(n) = f(n \cdot 1) = g^n.$$

Réciproquement $f \mapsto f(1)$ établit une bijection entre l'ensemble des morphismes de groupes de $\mathbb{Z}$ dans G et l'ensemble des éléments de G. La bijection réciproque associe à un élément g de G le morphisme $n \mapsto g^n$.

Si G est abélien, alors cette bijection est un morphisme de groupes.

4.2.3. La propriété universelle de $\mathbb{Z}/d\mathbb{Z}$. — Soit $d \in \mathbb{Z}$ et soit G un groupe. Comme $\mathbb{Z}$ est abélien, $d\mathbb{Z}$ est le plus petit sous-groupe distingué de $\mathbb{Z}$ contenant d [2]. L'application $\psi \mapsto (n \mapsto \psi(\overline{n})$ établit une bijection entre l'ensemble des morphismes de $\mathbb{Z}/d\mathbb{Z}$ dans G et l'ensemble des morphismes de $\mathbb{Z}$ dans G s'annulant sur d.

On déduit à l'aide de §4.2.2 que $f \mapsto f(\overline{1})$ établit une bijection entre l'ensemble de morphismes de $\mathbb{Z}/d\mathbb{Z}$ dans G et l'ensemble des éléments g de d-torsion. La bijection réciproque envoie un élément g tel que $g^d = e$ sur le morphisme $\overline{n} \mapsto g^n$ (comme $g^d = e$, l'élément g^n de G ne dépend bien que de la classe de n modulo d).

---

2. *Intersection de sous-groupes distingués.*

Soit G un groupe et soit $(\mathrm{H}_i)_i$ une famille de sous-groupes distingués de G. Le sous-groupe $\cap_i \mathrm{H}_i$ de G est distingué dans G.

Si E est un sous-ensemble de G, l'intersection des sous-groupes distingués de G contenant E est donc un sous-groupe distingué H de G qui est le plus petit sous-groupe distingué de G contenant E. On peut vérifier que H est le sous-groupe de G engendré par $\left\{gxg^{-1}\right\}_{g \in \mathrm{G},\, x \in E}$.

Soit H le plus petit sous-groupe distingué de G contenant E. Soit π le morphisme quotient $\mathrm{G} \to \mathrm{G}/\mathrm{H}$. Si φ est un morphisme de groupes de source G, son noyau $\ker \pi$ est un sous-groupe distingué de G si bien que $E \subset \ker \pi$ si et seulement si $\mathrm{H} \subset \ker \pi$. La propriété universelle du morphisme π peut alors se réécrire en disant que $\psi \mapsto \psi \circ \pi$ établit une bijection entre $\mathrm{Hom}\left(\mathrm{G}/\mathrm{H}, \mathrm{G}'\right)$ et l'ensemble des φ appartenant à $\mathrm{Hom}(\mathrm{G}, \mathrm{G}')$ tels que $E \subset \ker \varphi$; c'est précisément la propriété universelle cherchée. En termes un peu plus informels se donner un morphisme de G/H vers un groupe G' c'est se donner un morphisme de G vers G' qui est trivial sur E.

Si G est abélien, on vérifie que cette bijection est un morphisme de groupes.

4.2.4. Énoncés informels. — Les propriétés universelles énoncées aux §4.2.2 et §4.2.3 peuvent se résumer peu ou prou par :

- ◇ *se donner un morphisme de* $\mathbb{Z}$ *dans* G *c'est choisir un élément de* G *– l'image de* 1 ;
- ◇ *se donner un morphisme de* $\mathbb{Z}/d\mathbb{Z}$ *dans* G *c'est choisir un élément de d-torsion de* G *– l'image de* $\overline{1}$.

4.2.5. Endomorphismes de $\mathbb{Z}$. — Il résulte de §4.2.2, appliqué à $\mathrm{G} = \mathbb{Z}$, que $a \mapsto h_a$, où h_a désigne l'endomorphisme $x \mapsto ax$ (l'homothétie de rapport a), établit un isomorphisme de groupes entre $\mathbb{Z}$ et $\operatorname{End}\mathbb{Z}$.

On vérifie que cet isomorphisme de groupes est même un isomorphisme d'anneaux. Le groupe $\operatorname{Aut}\mathbb{Z}$ s'identifie donc, via $a \mapsto h_a$, à $\mathbb{Z}^\times = \{-1, 1\}$.

4.2.6. Endomorphismes de $\mathbb{Z}/d\mathbb{Z}$. — Il résulte de §4.2.3, appliqué à $\mathrm{G} = \mathbb{Z}/p\mathbb{Z}$ que $a \mapsto h_a$, où h_a désigne l'endomorphisme $x \mapsto ax$ (l'homothétie de rapport a), établit une bijection entre $\mathbb{Z}/d\mathbb{Z}$ et $\operatorname{End}\mathbb{Z}/d\mathbb{Z}$.

On vérifie que cet isomorphisme de groupes est même un isomorphisme d'anneaux. Le groupe $\operatorname{Aut}\left(\mathbb{Z}/d\mathbb{Z}\right)$ s'identifie donc, via $a \mapsto h_a$, à $\left(\mathbb{Z}/d\mathbb{Z}\right)^\times$.

4.3. Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geq 1$ un entier. Nous allons faire une étude détaillée des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ et de l'ordre de ses éléments. Rappelons que si a et b sont deux éléments de $\mathbb{Z}$ nous avons les égalités suivantes dans $\mathbb{Z}/n\mathbb{Z}$

$$a\overline{b} = \overline{ab} = \overline{a}\,\overline{b}.$$

Précisons que la notation $a\overline{b}$ est ici une simple occurence de la notation ag qui a un sens pour tout élément g d'un groupe abélien noté additivement et que $\overline{a}\,\overline{b}$ désigne le produit de $\overline{a}$ et $\overline{b}$ dans l'anneau $\mathbb{Z}/n\mathbb{Z}$. L'égalité $a\overline{b} = \overline{ab}$ vient du fait que la réduction modulo b est un morphisme entre groupes abéliens notés additivement et commute à la multiplication par a. La seconde égalité provient du fait que la réduction modulo n est un morphisme d'anneaux. Par ailleurs nous avons implicitement utilisé la double interprétation du produit ab (Remarque 4.1.1).

4.3.1. Rappels. — Avant d'entrer dans le vif du sujet établissons deux résultats dont nous aurons besoin par la suite.

Lemme 4.3.1

Soit G un groupe. Soit H un sous-groupe distingué de G. Soit $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ le morphisme quotient. Nous avons les deux assertions suivantes :

- Soit Γ un sous-groupe de G. Alors $\mathrm{H} \cap \Gamma$ est un sous-groupe distingué de Γ et $\pi(\Gamma)$ est isomorphe à ${}^{\Gamma}\!/_{\mathrm{H} \cap \Gamma}$.
- Les formules $\Gamma \mapsto \pi(\Gamma)$ et $\Delta \mapsto \pi^{-1}(\Delta)$ établissent une bijection croissante (pour l'inclusion) entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Démonstration. — Puisque $\mathrm{H} = \ker \pi$, le noyau de $\pi_{|\Gamma}$ est égal à $\mathrm{H} \cap \Gamma$. Ce dernier est donc distingué dans Γ et $\pi(\Gamma) \simeq {}^{\Gamma}\!/_{\mathrm{H} \cap \Gamma}$.

Montrons maintenant la seconde assertion. Soit Γ un sous-groupe de G contenant H. Montrons que $\pi^{-1}(\pi(\Gamma)) = \Gamma$. Nous avons l'inclusion $\Gamma \subset \pi^{-1}(\pi(\Gamma))$. Réciproquement soit $g \in \mathrm{G}$ tel que $\pi(g) \in \pi(\Gamma)$. Il existe alors $\gamma \in \Gamma$ tel que $\pi(g) = \pi(\gamma)$, c'est-à-dire que $\pi(g\gamma^{-1}) = e$. Ainsi $g\gamma^{-1}$ appartient à $\ker \pi = \mathrm{H} \subset \Gamma$. Puisque $g = (g\gamma^{-1})\gamma$ nous avons $g \in \Gamma$.

La surjectivité de π implique par ailleurs que $\pi(\pi^{-1}(\Delta)) = \Delta$ pour toute partie Δ de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$; c'est en particulier le cas lorsque Δ est un sous-groupe de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

Ainsi les formules données établissent bien une bijection entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$. Par ailleurs elles définissent des applications croissantes. □

Lemme 4.3.2

Soit G un groupe. Soit H un sous-groupe distingué de G. Soit π le morphisme quotient de G dans ${}^{\mathrm{G}}\!/_{\mathrm{H}}$. Soit Γ un sous-groupe de G.

- Si Γ est un sous-groupe distingué de G, alors $\pi(\Gamma)$ est un sous-groupe distingué de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.
- Si $\pi(\Gamma)$ est un sous-groupe distingué de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ et si de plus $\mathrm{H} \subset \Gamma$, alors Γ est un sous-groupe distingué de G et le morphisme composé
$$\mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{{}^{\mathrm{G}}\!/_{\mathrm{H}}}\!/_{\pi(\Gamma)}$$
induit un isomorphisme ${}^{\mathrm{G}}\!/_{\Gamma} \simeq {}^{{}^{\mathrm{G}}\!/_{\mathrm{H}}}\!/_{\pi(\Gamma)}$.

Démonstration. — Supposons que Γ soit distingué dans G. Soit h dans $\pi(\Gamma)$ et soit x dans G/H. Écrivons $h = \pi(\gamma)$ avec $\gamma \in \Gamma$ et $x = \pi(g)$ avec $g \in \mathrm{G}$. Nous avons

$$xhx^{-1} = \pi(g)\pi(\gamma)\pi(g^{-1}) = \pi(g\gamma g^{-1}).$$

Or Γ est distingué dans G donc $g\gamma g^{-1}$ appartient à Γ. Ainsi xhx^{-1} appartient à $\pi(\Gamma)$ et $\pi(\Gamma)$ est un sous-groupe distingué de G/H.

Supposons désormais que $\pi(\Gamma)$ soit un sous-groupe distingué de G/H et que Γ contienne H. Le morphisme

$$\mathrm{G} \to \mathrm{G}/\mathrm{H} \to \mathrm{G}/\mathrm{H}/\pi(\Gamma)$$

est surjectif comme composé de surjections. Son noyau est égal à $\pi^{-1}(\pi)$, c'est-à-dire Γ d'après le Lemme 4.3.1. Ce dernier est donc distingué dans G et le morphisme

$$\mathrm{G} \to \mathrm{G}/\mathrm{H} \to \mathrm{G}/\mathrm{H}/\pi(\Gamma)$$

induit l'isomorphisme $\mathrm{G}/\Gamma \simeq \mathrm{G}/\mathrm{H}/\pi(\Gamma)$. □

4.3.2. — Soit G un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ et soit Γ son image réciproque dans $\mathbb{Z}$. On peut écrire $\Gamma = a\mathbb{Z}$ pour un unique $a \in \mathbb{N}$. Le groupe G étant égal à l'image de Γ, il vient $\mathrm{G} = \langle \overline{a} \rangle$ (Lemme 4.3.1).

4.3.3. — Soit $a \in \mathbb{Z}$. Soit $r \in \mathbb{N}$ le pgcd de a et n. L'image réciproque de $\langle \overline{a} \rangle$ dans $\mathbb{Z}$ est égale à $a\mathbb{Z} + n\mathbb{Z} = r\mathbb{Z}$. Le Lemme 4.3.1 assure que le groupe $\langle \overline{a} \rangle$ coïncide avec l'image de $r\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire $\langle \overline{r} \rangle$. Le quotient $\mathbb{Z}/n\mathbb{Z}/\langle \overline{a} \rangle$ s'identifie canoniquement à $\mathbb{Z}/r\mathbb{Z}$.

L'intérêt de cette remarque est le suivant. Comme r divise n, l'ordre de $\overline{r}$ dans $\mathbb{Z}/n\mathbb{Z}$ est très facile à calculer. En effet si m est un entier, nous avons les équivalences suivantes

$$m\overline{r} = \overline{0} \quad \Longleftrightarrow \quad n \text{ divise } mr \quad \Longleftrightarrow \quad \frac{n}{r} \text{ divise } m.$$

L'ordre de $\overline{r}$ dans $\mathbb{Z}/n\mathbb{Z}$ est donc égal à $\frac{n}{r}$.

4.3.4. Description des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$. — Il résulte de ce qui précède que pour tout diviseur d de n il existe un et un seul sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. Il est cyclique, engendré par $\overline{\frac{n}{d}}$. Le quotient correspondant de $\mathbb{Z}/n\mathbb{Z}$ s'identifie canoniquement à $\mathbb{Z}/\frac{n}{d}\mathbb{Z}$.

4.3.5. Relations d'inclusion entre les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$. — Soient d et d' deux diviseurs de n. Soit G_d (resp. $\mathrm{G}_{d'}$) l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d (resp. d'). Nous avons : $\mathrm{G}_d \subset \mathrm{G}_{d'}$ si et seulement si d divise d'.

En effet G_d est engendré par $\overline{\frac{n}{d}}$. Son image réciproque Γ_d dans $\mathbb{Z}$ est donc égale à

$$\frac{n}{d}\mathbb{Z} + n\mathbb{Z} = \frac{n}{d}\mathbb{Z}$$

(car $n\mathbb{Z} \subset \frac{n}{d}\mathbb{Z}$). De même l'image réciproque $\Gamma_{d'}$ de $\mathrm{G}_{d'}$ dans $\mathbb{Z}$ est égale à $\frac{n}{d'}\mathbb{Z}$.

Le Lemme 4.3.1 assure que $\mathrm{G}_d \subset \mathrm{G}_{d'}$ si et seulement si $\Gamma_d \subset \Gamma_{d'}$, c'est-à-dire si et seulement si $\frac{n}{d}\mathbb{Z} \subset \frac{n}{d'}\mathbb{Z}$. Mais ceci revient à demander que $\frac{n}{d'}$ divise $\frac{n}{d}$, *i.e.* à demander que d divise d'.

4.3.6. Sous-groupes de r-torsion de $\mathbb{Z}/n\mathbb{Z}$. — Soit r un entier. Soit d le pgcd de n et r ; Posons $\nu = \frac{n}{d}$ et $\rho = \frac{r}{d}$ (notons que d est non nul car n est non nul). Les entiers ν et ρ sont premiers entre eux.

Soit T le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ formé des éléments de r-torsion. Son image réciproque Θ dans $\mathbb{Z}$ est l'ensemble des entiers relatifs m tels que n divise rm, c'est-à-dire encore tels que ν divise ρm. Puisque ν est premier avec ρ nous pouvons, d'après le Lemme de Gauss, décrire également Θ comme l'ensemble des éléments m de $\mathbb{Z}$ tels que ν divise m. Nous avons donc $\Theta = \nu\mathbb{Z} = \frac{n}{d}\mathbb{Z}$. Nous déduisons alors du Lemme 4.3.1 que T est le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\overline{\frac{n}{d}}$, *i.e.* l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d.

4.3.7. Générateurs de $\mathbb{Z}/n\mathbb{Z}$. — Soit $a \in \mathbb{Z}$. On déduit de §4.3.3 que $\overline{a}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a est premier avec n, c'est-à-dire encore si et seulement s'il existe u et v dans $\mathbb{Z}$ tels que $au + nv = 1$; autrement dit c'est le cas si et seulement si $\overline{a}$ est inversible modulo n.

Le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$ est donc égal au nombre d'entiers compris entre 0 et $n-1$ qui sont premiers à n, ou encore inversibles modulo n. Nous noterons ce nombre $\Phi(n)$; la fonction Φ est appelée *l'indicateur d'Euler*.

Si n est de la forme p^m avec p premier et $m \geq 1$ un calcul direct [3] montre que $\Phi(n) = p^{m-1}(p-1)$. Écrivons n sous la forme $\prod p_i^{m_i}$ avec les p_i premiers et deux à deux distincts et les $m_i \geq 1$. Le Lemme chinois assure que les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\prod \mathbb{Z}/p_i^{m_i}\mathbb{Z}$ sont isomorphes. L'interprétation de $\Phi(n)$ en termes d'éléments inversibles assure alors que

$$\Phi(n) = \prod_i \Phi(p_i^{m_i}) = \prod_i p_i^{m_i-1}(p_i - 1).$$

4.3.8. — Soit d un diviseur de n. Un élément de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre d si et seulement s'il engendre un sous-groupe d'ordre d donc si et seulement s'il engendre l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d à savoir $\langle \overline{\frac{n}{d}} \rangle$. Les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ sont donc exactement les générateurs du groupe cyclique $\langle \overline{\frac{n}{d}} \rangle$ qui est isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Il y en a donc exactement $\Phi(d)$.

Puisque tout élément de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre divisant n il vient

$$\sum_{d|n} \Phi(d) = n.$$

3. fondé sur le fait qu'un entier est premier avec p^m si et seulement s'il n'est pas multiple de p

4.4. Exposant d'un groupe abélien fini

Abordons désormais l'étude générale des groupes abéliens finis. Commençons par l'étude d'un invariant important d'un tel groupe, son exposant.

Définition 4.4.1

Soit G un groupe abélien fini noté additivement. Soit I l'ensemble des entiers d tels que $dg = 0$ pour tout g dans G. C'est un idéal de $\mathbb{Z}$. Soit e l'entier ≥ 0 tel que $I = e\mathbb{Z}$. L'entier e est appelé *exposant* de G.

4.4.1. Exposant et cardinal. — Soit G un groupe fini noté additivement. Soit n son ordre. Comme $ng = 0$ pour tout g dans G l'entier e divise n. Cette relation de divisibilité peut être stricte : par exemple si $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, nous avons $e = 2$ et $n = 4$.

4.4.2. Autre expression de l'exposant. — Pour tout $g \in \mathrm{G}$, soit I_g l'ensemble des entiers d tels que $dg = 0$. C'est un idéal de $\mathbb{Z}$ dont le générateur positif est l'ordre de g (*voir* §**??**). Puisque I est l'intersection des I_g pour g parcourant G, l'exposant de G est le ppcm des ordres des éléments de G.

Lemme 4.4.1

Soit G un groupe abélien noté additivement. Soient g et h deux éléments de G dont les ordres respectifs a et b sont finis et premiers entre eux. L'ordre de $g + h$ est alors égal à ab.

Démonstration. — Soit d l'ordre de $g + h$. Nous avons

$$ab(g + h) = bag + abh = 0.$$

Par conséquent d divise ab.

Pour conclure il suffit de montrer que ab divise d. Par définition de d nous avons $d(g+h) = 0$, c'est-à-dire $dg = -dh$. L'élément $dg = -dh$ de G appartient donc au sous-groupe $\mathrm{H} = \langle g \rangle \cap \langle h \rangle$ de G. Puisque H est contenu à la fois dans $\langle g \rangle$ et dans $\langle h \rangle$ son ordre divise a et b. Comme a et b sont premiers entre eux, $|\mathrm{H}| = 1$ et $\mathrm{H} = \{0\}$. Ainsi $dg = 0$ et $-dh = 0$. Ceci entraîne que a divise d et b divise d. Par conséquent d est multiple du ppcm de a et b qui n'est autre que ab puisque a et b sont premiers entre eux. □

Lemme 4.4.2

Soit G un groupe abélien fini et soit e son exposant. Il existe un élément de G d'ordre exactement e.

Démonstration. — Notons le groupe G additivement. Comme e est non nul (il divise $|\mathrm{G}|$) on peut le décomposer en produit de facteurs premiers ; écrivons $e = \prod p_i^{n_i}$ (les p_i désignant des nombres premiers distincts). Puisque e est le ppcm des ordres des éléments de G il existe pour tout i un élément g_i de G dont l'ordre est divisible par $p_i^{n_i}$, disons égal à $p_i^{n_i} m_i$ pour un certain $m_i > 0$. Alors $m_i g_i$ est d'ordre $p_i^{n_i}$.

Une application répétée du Lemme 4.4.1 assure alors que la somme $\sum_i m_i g_i$ est d'ordre $\prod p_i^{n_i} = e$ ce qui termine la démonstration. □

Corollaire 4.4.1

Soit $\Bbbk$ un corps commutatif et soit G un sous-groupe fini de $\Bbbk^\times$. Le groupe G est cyclique.

Démonstration. — Soit e l'exposant de G. Nous avons $g^e = 1$ pour tout g dans G. Par suite le polynôme $X^e - 1 \in \Bbbk[X]$ a au moins $|\mathrm{G}|$ racines distinctes dans $\Bbbk$ ce qui implique que $|\mathrm{G}| \leq e$. Par ailleurs G possède un élément g d'ordre e (Lemme 4.4.2). Le sous-groupe $\langle g \rangle$ de G a alors pour ordre e. Puisque $|\mathrm{G}| \leq e$ nous obtenons que $|\mathrm{G}| = e$ et $\mathrm{G} = \langle g \rangle$. □

Remarque 4.4.1. — Il résulte de l'énoncé précédent que $\Bbbk^\times$ est cyclique pour tout corps fini $\Bbbk$. En particulier si p est un nombre premier le groupe $\mathbb{F}_p^\times$ est cyclique. Il existe donc un entier n dont la classe $\overline{n}$ modulo p engendre $\mathbb{F}_p^\times$. Attention ce résultat n'est pas effectif : le Corollaire 4.4.1 repose en effet sur le Lemme 4.4.2 et si celui-ci affirme que l'exposant d'un groupe abélien fini G est l'ordre d'un certain élément g de G sa démonstration ne fournit pas de méthode pratique pour exhiber un tel g.

4.5. Classification des groupes abéliens finis

Nous terminons cette section par un théorème de classification de tous les groupes abéliens finis à isomorphisme près. Commençons par quelques lemmes techniques qui peuvent avoir leur intérêt propre et qui sont essentiellement des énoncés de prolongements de morphismes. Le premier d'entre eux, ci-dessous, est essentiellement formel.

Lemme 4.5.1

Soient G et H deux groupes abéliens notés additivement. Soient G_1 et G_2 deux sous-groupes de G tels que $\mathrm{G} = \mathrm{G}_1 \times \mathrm{G}_2$. Soit $\varphi_1 \colon \mathrm{G}_1 \to \mathrm{H}$ (resp. $\varphi_2 \colon \mathrm{G}_2 \to \mathrm{H}$) un morphisme de G_1 (resp. G_2) dans H. Supposons que φ_1 et φ_2 coïncident sur $\mathrm{G}_1 \cap \mathrm{G}_2$. Il existe alors un unique morphisme $\varphi \colon \mathrm{G} \to \mathrm{H}$ tel que $\varphi_{|\mathrm{G}_1} = \varphi_1$ et $\varphi_{|\mathrm{G}_2} = \varphi_2$.

Démonstration. — **Unicité**. L'unicité est claire : si φ est un morphisme comme ci-dessus et si g appartient à G, on écrit $g = g_1 + g_2$ avec $g_1 \in \mathrm{G}_1$ et $g_2 \in \mathrm{G}_2$, et on a nécessairement

$$\varphi(g) = \varphi(g_1) + \varphi(g_2) = \varphi_1(g_1) + \varphi_2(g_2).$$

Existence. Soit $g \in \mathrm{G}$. Écrivons $g = g_1 + g_2$ avec $g_1 \in \mathrm{G}_1$ et $g_2 \in \mathrm{G}_2$. Vérifions tout d'abord que l'élément $\varphi_1(g_1) + \varphi_2(g_2)$ de H ne dépend que de g et pas de la décomposition choisie. Écrivons donc $g = g_1' + g_2'$ avec $g_1' \in \mathrm{G}_1$ et $g_2' \in \mathrm{G}_2$. L'égalité $g_1 + g_2 = g_1' + g_2'$ peut se réécrire

$$\underbrace{g_1 - g_1'}_{\in \mathrm{G}_1} = \underbrace{g_2' - g_2}_{\in \mathrm{G}_2}$$

Puisque φ_1 et φ_2 coïncident sur $\mathrm{G}_1 \cap \mathrm{G}_2$ nous obtenons $\varphi_1(g_1 - g_1') = \varphi_2(g_2' - g_2)$, soit $\varphi_1(g_1) - \varphi_1(g_1') = \varphi_2(g_2') - \varphi_2(g_2)$ et finalement

$$\varphi_1(g_1) + \varphi_2(g_2) = \varphi_1(g_1') + \varphi_2(g_2')$$

comme annoncé. Il est donc licite de poser $\varphi(g) = \varphi(g_1) + \varphi(g_2)$. En particulier

- $\varphi(g) = \varphi(g + 0) = \varphi_1(g)$ si g appartient à G_1,
- $\varphi(g) = \varphi(g + 0) = \varphi_2(g)$ si g appartient à G_2.

Soient g et γ dans G. Écrivons $g = g_1 + g_2$ et $\gamma = \gamma_1 + \gamma_2$ où g_1 et γ_1 appartiennent à G_1 et g_2 et γ_2 appartiennent à G_2. Nous avons alors

$$g + \gamma = g_1 + \gamma_1 + g_2 + \gamma_2.$$

Comme $g_1 + \gamma_1$ (resp. $g_2 + \gamma_2$) appartient à G_1 (resp. G_2), il résulte de la définition de φ que

$$\begin{aligned} \varphi(g + \gamma) &= \varphi_1(g_1 + \gamma_1) + \varphi_2(g_2 + \gamma_2) \\ &= \varphi_1(g_1) + \varphi_1(\gamma_1) + \varphi_2(g_2) + \varphi_2(\gamma_2) \\ &= \varphi(g) + \varphi(\gamma) \end{aligned}$$

et φ est un morphisme de groupes. □

Lemme 4.5.2

Soient $d \geq 1$ un entier et n un mutiple de d. Soit G un sous-groupe de $\mathbb{Z}/d\mathbb{Z}$. Soit ψ un morphisme de G dans $\mathbb{Z}/n\mathbb{Z}$. Le morphisme ψ s'étend en un morphisme de $\mathbb{Z}/d\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. — Il existe un diviseur a de d tel que $\mathrm{G} = \langle \overline{a} \rangle$. Écrivons $d = ab$ et $n = dm$ avec a et m dans $\mathbb{N}$. Puisque l'élément $\overline{a}$ de $\mathbb{Z}/d\mathbb{Z}$ est de b-torsion, l'élément $\psi(\overline{a})$ de $\mathbb{Z}/n\mathbb{Z}$ est de b-torsion. Comme $n = abm$ cela signifie que $\psi(\overline{a})$ est égal à $\overline{ram}$ pour un certain entier r

(*voir* §4.3.6). L'élément $\overline{rm}$ de $\mathbb{Z}/n\mathbb{Z}$ est de d-torsion (car $n = dm$) ; il existe donc un (unique) morphisme χ de $\mathbb{Z}/d\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ envoyant $\overline{1}$ sur $\overline{rm}$. On a alors

$$\underbrace{\chi(\overline{a}) = \chi(a\overline{1})}_{\text{les classes sont prises modulo } d} \quad = \quad \underbrace{a\overline{rm} = \overline{arm}}_{\text{les classes sont prises modulo } n}$$

Ainsi $\chi(\overline{a}) = \psi(\overline{a})$. Étant donné que $\overline{a}$ engendre G la restriction de χ à G est égale à ψ. □

Lemme 4.5.3

Soit G un groupe abélien fini. Soit $n > 0$ un entier tel que $ng = 0$ pour tout $g \in$ G. Soit H un sous-groupe de G. Soit φ un morphisme de H dans $\mathbb{Z}/n\mathbb{Z}$.
Le morphisme φ s'étend alors en un morphisme de G dans $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. — On procède par récurrence sur l'indice [G : H].

- Si [G : H] = 1, alors H = G et il n'y a rien à démontrer.
- Supposons donc que [G : H] > 1 et que l'énoncé soit vrai pour les sous-groupes K de G tels que [G : K] < [G : H].

  Comme [G : H] > 1, il existe un élément g de G qui n'appartient pas à H. Puisque $ng = 0$, l'ordre d de g est un diviseur de n. Le groupe $\langle g\rangle$ étant isomorphe à $\mathbb{Z}/d\mathbb{Z}$ il découle du Lemme 4.5.2 que $\varphi_{|\mathrm{H}\cap\langle g\rangle}$ se prolonge en un morphisme θ de $\langle g\rangle$ vers $\mathbb{Z}/n\mathbb{Z}$. Par construction φ et θ coïncident sur $\mathrm{H}\cap\langle g\rangle$. D'après le Lemme 4.5.1 il existe alors un (unique) morphisme Φ de $\mathrm{H}\times\langle g\rangle$ dans $\mathbb{Z}/n\mathbb{Z}$ dont la restriction à H est égale à φ et dont la restriction à $\langle g\rangle$ est égale à θ. Puisque $\mathrm{H}\times\langle g\rangle$ contient strictement H (car g n'appartient pas à H) son indice dans G est strictement inférieur à [G : H]. L'hypothèse de récurrence assure alors l'existence d'un morphisme de G dans $\mathbb{Z}/n\mathbb{Z}$ qui prolonge Φ, et a fortiori φ.

□

Nous pouvons maintenant énoncer le théorème de classification des groupes abéliens finis.

Théorème-Définition 4.5.1

Soit G un groupe abélien fini. Il existe une unique famille finie $(d_1, d_2, \ldots, d_n)$ d'entiers > 1 tels que

- $d_1 \mid d_2 \mid \ldots \mid d_n$
- et $\mathrm{G} \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}$.

Les d_i sont appelés les *facteurs invariants* du groupe G.
Écrivons d_i sous la forme $d_i = p_1^{\alpha_{i,1}} p_2^{\alpha_{i,2}} \ldots p_r^{\alpha_{i,r}}$ avec p_i premier et $\alpha_{1,j} \leq \alpha_{2,j} \leq \ldots \leq \alpha_{\ell,j}$; les $p_i^{\alpha_{i,j}}$ sont appelés les *diviseurs élémentaires* du groupe G.

Exemple 4.5.1. — Soit G le groupe abélien fini dont les facteurs invariants sont $d_4 = 30$, $d_3 = 15$, $d_2 = 3$ et $d_1 = 3$.

Notons que $d_4 = 5 \times 3 \times 2$ et $d_3 = 5 \times 3$. Par suite les diviseurs élémentaires sont 5, 5, 3, 3, 3, 3 et 2.

Exemple 4.5.2. — Soit G un groupe abélien fini dont les diviseurs élémentaires sont 2^5, 2^3, 2, 2, 3^3, 3 et 5.

Les facteurs invariants de G sont donc

$$d_4 = 2^5 \times 3^3 \times 5 = 4320, \qquad d_3 = 2^3 \times 3 = 24, \qquad d_2 = 2 \qquad d_1 = 2.$$

Il en résulte que

$$\mathrm{G} \simeq \mathbb{Z}/_{4320\mathbb{Z}} \times \mathbb{Z}/_{24\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}.$$

Exemple 4.5.3. — Soit G le groupe abélien défini par

$$\mathrm{G} = \mathbb{Z}/_{162\mathbb{Z}} \times \mathbb{Z}/_{21\mathbb{Z}}.$$

Notons que $162 = 3^4 \times 2$ et $21 = 7 \times 3$. Par conséquent

$$\mathbb{Z}/_{162\mathbb{Z}} \simeq \mathbb{Z}/_{3^4\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}} \qquad\qquad \mathbb{Z}/_{21\mathbb{Z}} \simeq \mathbb{Z}/_{7\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}.$$

Ainsi

$$\mathrm{G} \simeq \mathbb{Z}/_{3^4\mathbb{Z}} \times \mathbb{Z}/_{7\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}.$$

Les diviseurs élémentaires de G sont 3^4, 7, 2 et 3 et les facteurs invariants de G sont $d_2 = 3^4 \times 7 \times 2 = 1134$ et $d_1 = 3$. Il s'en suit que

$$\mathrm{G} \simeq \mathbb{Z}/_{1134\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}.$$

Exemple 4.5.4. — Soit G le groupe donné par

$$\left(\mathbb{Z}/_{2\mathbb{Z}}\right)^2 \times \mathbb{Z}/_{2^2\mathbb{Z}} \times \mathbb{Z}/_{2^3\mathbb{Z}} \times \left(\mathbb{Z}/_{3\mathbb{Z}}\right)^3 \times \mathbb{Z}/_{5\mathbb{Z}} \times \mathbb{Z}/_{5^2\mathbb{Z}}.$$

Les diviseurs élémentaires de G sont 2, 2, 2^2, 2^3, 3, 3, 3, 5 et 5^2. Les facteurs invariants de G sont donc $2^3 \times 3 \times 5^2 = 600$, $2^2 \times 3 \times 5 = 60$, $2 \times 3 = 6$ et 2.

Exemple 4.5.5. — Déterminons les facteurs invariants du groupe $\mathrm{G} = \mathbb{Z}/_{54\mathbb{Z}} \times \mathbb{Z}/_{360\mathbb{Z}}$.

D'une part $54 = 2 \times 3^3$, d'autre part $360 = 2^3 \times 5 \times 3^2$. Il en résulte que les diviseurs élémentaires de G sont 2, 2^3, 3^2, 3^3 et 5. Les facteurs invariants de G sont donc $2 \times 3^2 = 18$ et $2^3 \times 3^3 \times 5 = 1080$.

Exemple 4.5.6. — Classifions à isomorphisme près les groupes abéliens d'ordre 360.

D'après le théorème de structure des groupes abéliens de type fini il suffit de déterminer toutes les possibilités pour les diviseurs élémentaires de $\mathbb{Z}/_{360\mathbb{Z}}$.

D'une part

$$360 = 2^3 \times 3^2 \times 5$$

et d'autre part

◇ un groupe abélien d'ordre 8 est, à isomorphisme près, de la forme

$$\mathbb{Z}/8\mathbb{Z} \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z};$$

◇ et un groupe abélien d'ordre 9 est, à isomorphisme près, de la forme

$$\mathbb{Z}/9\mathbb{Z} \qquad \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Par conséquent tout groupe abélien d'ordre 360 est isomorphe à l'un des groupes suivants :

$$\begin{array}{l}
\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\
\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}
\end{array}$$

Démonstration. — La démonstration comporte deux parties, nous traitons d'abord l'existence des d_i puis leur unicité.

Existence de $(d_1, d_2, \ldots, d_n)$. On procède par récurrence sur $|\mathrm{G}|$.

- Si $|\mathrm{G}| = 1$ le groupe G est trivial et la famille vide d'entiers convient.
- Supposons maintenant que $|\mathrm{G}| > 1$ et que l'existence a été établie pour tout groupe abélien de cardinal strictement inférieur à celui de $|\mathrm{G}|$. notons que comme il existe un élément non nul dans G, l'exposant e de G est > 1. Le Lemme 4.4.2 assure qu'il existe un élément $g \in \mathrm{G}$ dont l'ordre est égal à e. Il existe alors un isomorphisme $\varphi\colon \langle g \rangle \to \mathbb{Z}/e\mathbb{Z}$. En vertu du Lemme 4.5.3, l'isomorphisme φ se prolonge en un morphisme Φ de G dans $\mathbb{Z}/e\mathbb{Z}$. Soit H le noyau de Φ. Comme φ est surjectif, Φ l'est a fortiori et on a donc $e|\mathrm{H}| = |\mathrm{G}|$. Par ailleurs l'injectivité de φ assure que $\mathrm{H} \cap \langle g \rangle = \{0\}$. Les sous-groupes H et $\langle g \rangle$ de G sont donc en somme directe, et le sous-groupe $\mathrm{H} \times \langle g \rangle$ est d'ordre $e|\mathrm{H}|$. Puisque $e|\mathrm{H}| = |\mathrm{G}|$ nous avons $\mathrm{G} = \mathrm{H} \times \langle g \rangle \simeq \mathrm{H} \times \mathbb{Z}/e\mathbb{Z}$.

  Comme $e > 1$ l'ordre de H est strictement inférieur à celui de G. D'après l'hypothèse de récurrence il existe alors une famille finie $(d_1, d_2, \ldots, d_r)$ d'entiers > 1 tels que $d_1|d_2|\ldots|d_r$ et tels que H soit isomorphe à

  $$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}.$$

  Puisque e est l'exposant de G tous les éléments de H sont de e-torsion ; ceci entraîne notamment que d_r divise e si $r > 0$ (considérer l'élément $(0, 0, \ldots, 0, 1)$ de $\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$). Posons $n = r + 1$ et $d_n = e$. La famille $(d_1, d_2, \ldots, d_n)$ satisfait alors les conditions de l'énoncé.

Unicité de $(d_1, d_2, \ldots, d_n)$. Pour montrer que $(d_1, d_2, \ldots, d_n)$ est unique, nous allons montrer qu'elle peut être reconstituée à partir des propriétés intrinsèques du groupe G.

Lemme 4.5.4

Pour connaître $(d_1, d_2, \ldots, d_n)$ il suffit de connaître pour tout nombre premier p et tout entier $m > 0$ le cardinal $\ell(p, m)$ de l'ensemble des indices i tels que p^m divise d_i.

Démonstration. — Compte tenu du fait que si p^m divise d_i il divise aussi d_j pour tout $j > i$ on peut vérifier [4] que la famille $(d_1, d_2, \ldots, d_n)$ s'obtient à partir des $\ell(p, m)$ par l'algorithme récursif suivant :

- ◇ si $\ell(p, m) = 0$ pour tout p et tout $m > 0$ la famille $(d_1, d_2, \ldots, d_n)$ est vide ;
- ◇ sinon considérons P est l'ensemble des nombres premiers p tels que l'ensemble

$$E_p = \{m > 0 \,|\, \ell(p, m) \neq 0\}$$

soit non vide, n_p le plus grand élément de E_p et posons $d_n = \prod_{p \in P} p^{n_p}$. On remplace alors pour tout $p \in P$ et tout $m \in E_p$ l'entier $\ell(p, m)$ par $\ell(p, m) - 1$ puis on détermine $(d_1, d_2, \ldots, d_{n-1})$ en appliquant l'algorithme à la nouvelle liste des $\ell(p, m)$.

□

Il suffit donc maintenant d'expliquer comment calculer les $\ell(p, m)$ à partir de G. Fixons un nombre premier p et un entier $m > 0$.

Soit $1 \leq i \leq n$. Soit e_i l'exposant de p dans la décomposition de d_i en produit de facteurs premiers. Le pgcd de d_i et p^m est alors égal à $p^{\min(m, e_i)}$. Le sous-groupe $p^m\left(\mathbb{Z}/d_i\mathbb{Z}\right)$ de $\mathbb{Z}/d_i\mathbb{Z}$ est aussi son sous-groupe engendré par $\overline{p^m}$; c'est donc l'unique sous-groupe de $\mathbb{Z}/d_i\mathbb{Z}$

4. Si cela vous paraît abstrait prenez un cas concret, par exemple la famille $(2, 2, 2, 6, 12, 24, 120, 240, 240)$. Comme $6 = 2 \times 3$, $12 = 2^2 \times 3$, $24 = 2^3 \times 3$, $120 = 2^3 \times 3 \times 5$, $240 = 2^4 \times 3 \times 5$ nous avons $\ell(2, 1) = 9$, $\ell(2, 2) = 5$, $\ell(2, 3) = 4$, $\ell(2, 4) = 2$, $\ell(3, 1) = 6$, $\ell(5, 1) = 3$.

Première étape de l'algorithme : $E_2 = \{1, 2, 3, 4\}$ et $n_2 = 4$, $E_3 = \{1\}$ et $n_3 = 1$, $E_5 = \{1\}$ et $n_5 = 1$ donc $P = \{2, 3, 5\}$ et $d_9 = 2^4 \times 3 \times 5 = 240$. Alors les $\ell(p, m)$ deviennent : $\ell(2, 1) = 8$, $\ell(2, 2) = 4$, $\ell(2, 3) = 3$, $\ell(2, 4) = 1$, $\ell(3, 1) = 5$, $\ell(5, 1) = 2$.

Deuxième étape de l'algorithme : $E_2 = \{1, 2, 3, 4\}$ et $n_2 = 4$, $E_3 = \{1\}$ et $n_3 = 1$, $E_5 = \{1\}$ et $n_5 = 1$ donc $P = \{2, 3, 5\}$ et $d_8 = 2^4 \times 3 \times 5 = 240$. Alors les $\ell(p, m)$ deviennent : $\ell(2, 1) = 7$, $\ell(2, 2) = 3$, $\ell(2, 3) = 2$, $\ell(3, 1) = 4$, $\ell(5, 1) = 1$.

Troisième étape de l'algorithme : $E_2 = \{1, 2, 3\}$ et $n_2 = 3$, $E_3 = \{1\}$ et $n_3 = 1$, $E_5 = \{1\}$ et $n_5 = 1$ donc $P = \{2, 3, 5\}$ et $d_7 = 2^3 \times 3 \times 5 = 120$. Alors les $\ell(p, m)$ deviennent : $\ell(2, 1) = 6$, $\ell(2, 2) = 2$, $\ell(2, 3) = 1$, $\ell(3, 1) = 3$.

Quatrième étape de l'algorithme : $E_2 = \{1, 2, 3\}$ et $n_2 = 3$, $E_3 = \{1\}$ et $n_3 = 1$ donc $P = \{2, 3\}$ et $d_6 = 2^3 \times 3 = 24$. Alors les $\ell(p, m)$ deviennent : $\ell(2, 1) = 5$, $\ell(2, 2) = 1$, $\ell(3, 1) = 2$.

En itérant le procédé on trouve $d_5 = 12$, $d_4 = 6$, $d_3 = d_2 = d_1 = 2$.

d'ordre $\frac{d_i}{p^{\min(m,e_i)}}$ (*voir* §4.3.3). De même $p^{m-1}\left(\mathbb{Z}/d_i\mathbb{Z}\right)$ est l'unique sous-groupe de $\mathbb{Z}/d_i\mathbb{Z}$ d'ordre $\frac{d_i}{p^{\min(m-1,e_i)}}$ et il vient

$$\left|\frac{p^{m-1}\left(\mathbb{Z}/d_i\mathbb{Z}\right)}{p^m\left(\mathbb{Z}/d_i\mathbb{Z}\right)}\right| = \frac{p^{\min(m,e_i)}}{p^{\min(m-1,e_i)}}.$$

Le terme de droite vaut p si $m \leq e_i$, c'est-à-dire si p^m divise d_i ; il vaut 1 si $m > e_i$.

En appliquant ce qui précède sommande par sommande, on en déduit que le quotient $p^{m-1}\mathrm{G}/p^m\mathrm{G}$ est d'ordre $p^{\ell(p,m)}$. L'entier $\ell(p,m)$ peut donc bien se décrire en termes des propriétés intrinsèques du groupe G. □

Exemple 4.5.7. — Soit n un entier naturel. Considérons le groupe $\mathrm{G} = \mathbb{Z}/p^n\mathbb{Z}$. Si $0 \leq k \leq n$, alors nous désignons par G_k l'ensemble des éléments de G divisibles par p^k dans G. Soit u le morphisme de multiplication par p de G dans lui-même. Alors

1. G_k est l'image du morphisme u^k ;
2. G_k est le sous-groupe des éléments d'ordre au plus p^{n-k} ;
3. G_k est le noyau du morphisme u^{n-k}.
4. $\mathrm{G}_n = \{0\}$;
5. $\mathrm{G}_0 = \mathrm{G}$.

À la multiplication par p agissant sur $\mathbb{Z}/p^n\mathbb{Z}$ nous associons un schema

$$\mathrm{G}_n = \{0\} \longleftarrow \mathrm{G}_{n-1} \longleftarrow \ldots \longleftarrow \mathrm{G}_1 \longleftarrow \mathrm{G}_0 = \mathrm{G}$$

où les flèches représentent l'action de la multiplication par p. Nous résumons cette information dans un petit tableau formé d'une seule ligne et de n-colonnes

□ □ ... □ □

en omettant $\{0\}$ et en convenant que l'action est le décalage vers la gauche : le carré le plus à gauche représente le noyau de la multiplication par p sur G.

Théorème 4.5.1

Soient p un nombre premier, n un entier et G un groupe abélien fini d'ordre p^n. Il existe une unique partition de n en $N_1 + N_2 + \ldots + N_s$, $N_1 \geq N_2 \geq \ldots \geq N_s$ telle que

$$\mathrm{G} \simeq \mathbb{Z}/p^{N_1}\mathbb{Z} \times \mathbb{Z}/p^{N_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{N_s}\mathbb{Z}.$$

En particulier la classe d'isomorphisme d'un groupe abélien d'ordre p^n est donnée par la *partition* de n en $(\beta_1, \beta_2, \ldots, \beta_t)$ où les β_i sont des nombres entiers positifs tels que

$$\begin{cases} \beta_i \geq \beta_{i+1} & \forall\, 1 \leq i \leq t-1 \\ \beta_1 + \beta_2 + \ldots + \beta_t = n \end{cases}$$

Exemple 4.5.8. — Les partitions possibles de 5 sont (5), $(4,1)$, $(3,2)$, $(3,1,1)$, $(2,2,1)$, $(2,1,1,1)$ et $(1,1,1,1,1)$. Par suite à isomorphisme près il y a exactement sept groupes abéliens d'ordre p^5 pour tout nombre premier p.

Pour démontrer le Théorème 4.5.1 nous aurons besoin de l'énoncé suivant :

Lemme 4.5.5

Soient p un nombre premier, n un entier et G un groupe abélien fini d'ordre p^n.
Considérons un élément $x \in \mathrm{G}$ d'ordre maximum p^r et le sous-groupe cyclique H engendré par x.
Étant donné un élément y d'ordre p^m dans G/H il existe un élément $\widetilde{y}$ de G dont la classe modulo H est y et de même ordre que y.

Démonstration. — Soit z dans G dont la classe modulo H est y. Puisque $p^m y$ est nul dans G/H, $p^m z$ appartient à H. Par conséquent $p^m z$ s'écrit ℓx avec ℓ entier inférieur ou égal à p^r. Écrivons ℓ sous la forme $p^s q$ avec $s \leq r$ et q non divisible par p. Autrement dit $p^m z = p^s q x$. L'élément $p^s q x$ est d'ordre p^{r-s} et z est d'ordre p^{m+r-s}. Comme p^r est l'ordre maximum d'un élément de G nous avons l'inégalité $m + r - s \leq r$ d'où $m \leq s$. Il en résulte que

$$\widetilde{y} = z - p^{s-m} x$$

est annulé par p^m. Ainsi l'ordre de $\widetilde{y}$ est p^m ; en effet si l'ordre de $\widetilde{y}$ était inférieur à p^m, sa classe y serait annulée par un entier inférieur à p^m. □

Démonstration du Théorème 4.5.1. — Nous allons séparer la preuve en deux parties : nous allons d'abord montrer l'existence, puis l'unicité.

Existence. La démonstration se fait par récurrence sur n.

Pour $n = 0$, le groupe G est réduit à l'élément neutre, il n'y a donc rien à démontrer.

Supposons désormais que $n > 0$. Dans le groupe G d'ordre p^n l'ordre de tout élément est une puissance de p. Soit x un élément de G d'ordre maximum p^r ; soit H le sous-groupe cyclique engendré par x. Le quotient G/H est d'ordre p^{n-r}. L'hypothèse de récurrence assure qu'il existe une unique partition de $n - r$ en $N_2 + N_3 + \ldots + N_s$, $N_2 \geq N_3 \geq \ldots \geq N_s$ telle que

$$\mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/p^{N_2}\mathbb{Z} \times \mathbb{Z}/p^{N_3}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{N_s}\mathbb{Z}.$$

En particulier il existe un morphisme surjectif

$$\pi \colon \mathrm{G} \to \mathbb{Z}/p^{N_2}\mathbb{Z} \times \mathbb{Z}/p^{N_3}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{N_s}\mathbb{Z}$$

dont le noyau est H.

Nous allons maintenant construire un isomorphisme entre G et $\mathbb{Z}/p^{N_1}\mathbb{Z} \times \mathbb{Z}/p^{N_2}\mathbb{Z} \times \mathbb{Z}/p^{N_3}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{N_s}\mathbb{Z}$. Comme p^{N_1} est l'ordre maximal d'un élément de G, nous avons l'inégalité $N_1 \geq N_2$.

Pour tout $2 \leq j \leq s$, le Lemme 4.5.5 assure l'existence d'un élément y_j de G d'ordre p^{N_j} dont l'image par π a pour i-ème composante 1 si $i = j$ et 0 sinon. Notons que le morphisme

$$\sigma\colon \mathbb{Z}/p^{N_2}\mathbb{Z} \times \mathbb{Z}/p^{N_3}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{N_s}\mathbb{Z} \to \mathrm{G} \qquad (a_2,\, a_3,\, \ldots,\, a_s) \mapsto a_2y_2 + a_3y_3 + \ldots + a_sy_s$$

est injectif ; sa composée avec le morphisme quotient $\mathrm{G} \to \mathrm{G}/\mathrm{H}$ est un isomorphisme.

L'isomorphisme recherché ϕ entre $\mathbb{Z}/p^{N_1}\mathbb{Z} \times \mathbb{Z}/p^{N_2}\mathbb{Z} \times \mathbb{Z}/p^{N_3}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{N_s}\mathbb{Z}$ et G est alors donné par

$$\phi(b,\, a_2,\, \ldots,\, a_s) = bx + \sigma(a_2,\, \ldots,\, a_s).$$

On peut en effet vérifier que

- ◇ ϕ est surjectif en utilisant que sa composée avec la surjection canonique $\mathrm{G} \to \mathrm{G}/\mathrm{H}$ est surjective ;
- ◇ ϕ est injectif en étudiant l'intersection de H avec le sous-groupe de G engendré par $(y_2,\, y_3,\, \ldots,\, y_s)$ (*i.e.* l'image de σ).

Unicité.

Lemme 4.5.6

Soit p un nombre premier. Si

$$\begin{aligned} \mathrm{G} &\simeq \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p^{\alpha_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\alpha_s}\mathbb{Z} \\ &\simeq \mathbb{Z}/p^{\beta_1}\mathbb{Z} \times \mathbb{Z}/p^{\beta_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\beta_t}\mathbb{Z} \end{aligned}$$

avec $\alpha_1 \geq \alpha_2 \geq \ldots \alpha_s \geq 1$, $\beta_1 \geq \beta_2 \geq \ldots \beta_t \geq 1$.
Alors $s = t$ et $\alpha_i = \beta_i$ pour tout $1 \leq i \leq s$.

Démonstration par récurrence sur l'ordre de G. — ◇ Si $|\mathrm{G}| = p$, alors $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z}$.

- ◇ Soit G un groupe abélien fini d'ordre p^k, $k \in \mathbb{N}^*$. Supposons que l'énoncé soit vrai pour tout groupe abélien H d'ordre p^ℓ avec $0 \leq \ell \leq k$. Si $\mathrm{G} \simeq \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p^{\alpha_2}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\alpha_s}\mathbb{Z}$, alors

$$\begin{aligned} p\mathrm{G} &\simeq p\,\mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times p\,\mathbb{Z}/p^{\alpha_2}\mathbb{Z} \times \ldots \times p\,\mathbb{Z}/p^{\alpha_s}\mathbb{Z} \\ &\simeq \mathbb{Z}/p^{\alpha_1-1}\mathbb{Z} \times \mathbb{Z}/p^{\alpha_2-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\alpha_s-1}\mathbb{Z}; \end{aligned}$$

de même

$$p\mathrm{G} \simeq \mathbb{Z}/p^{\beta_1-1}\mathbb{Z} \times \mathbb{Z}/p^{\beta_2-1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{\beta_t-1}\mathbb{Z}.$$

Alors $|p\mathrm{G}| = \frac{|\mathrm{G}|}{p^s} = \frac{|\mathrm{G}|}{p^t}$. Ainsi $s = t$ et l'hypothèse de récurrence assure que

$$\alpha_1 - 1 = \beta_1 - 1, \qquad \alpha_2 - 1 = \beta_2 - 1, \qquad \ldots, \qquad \alpha_s - 1 = \beta_s - 1.$$

Par conséquent $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$, …, $\alpha_s = \beta_s$.

□

Ceci termine la démonstration du théorème. □

4.6. Groupes abéliens de type fini

Rappelons qu'un groupe abélien G est *de type fini* s'il existe une famille génératrice finie de G, *i.e.* un entier k et une famille $(a_1, a_2, \ldots, a_k)$ d'éléments de G tels que tout élément de G est une combinaison linéaire à coefficients entiers d'éléments du système $(a_1, a_2, \ldots, a_k)$.

Précisément pour tout g dans G il existe des entiers $n_1, n_2, \ldots, n_k$ tels que $g = \sum_{i=1}^{k} n_i a_i$. Notons qu'une telle écriture n'a aucune raison d'être unique.

Nous pouvons traduire ce qui précède comme suit : le groupe G est engendré par $(a_1, a_2, \ldots, a_k)$ si et seulement si le morphisme de groupes

$$\mathbb{Z}^k \to \mathrm{G} \qquad\qquad (n_1, n_2, \ldots, n_k) \mapsto \sum_{i=1}^{k} n_i a_i$$

est surjectif. En d'autres termes : *le groupe* G *est un groupe abélien de type fini si et seulement si il existe un entier k et un morphisme surjectif de $\mathbb{Z}^k$ sur* G.

Exemple 4.6.1. — Un groupe engendré par un élément est

- ◇ soit réduit à l'élément neutre,
- ◇ soit isomorphe à $\mathbb{Z}$,
- ◇ soit cyclique et fini.

Convention : le système vide engendre le groupe réduit à l'élément neutre.

Exemple 4.6.2. — L'ensemble

$$\mathrm{G} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

est un sous-groupe de $\mathbb{R}$, engendré par le système $(1, \sqrt{2})$ et ne peut pas être engendré par un seul élément de G.

L'application

$$\mathbb{Z}^2 \to \mathrm{G}, \qquad\qquad (a, b) \mapsto a + b\sqrt{2}$$

est un isomorphisme de groupes.

Définition 4.6.1

Un groupe abélien G est *libre de type fini* s'il existe un entier naturel r tel que G soit isomorphe à $\mathbb{Z}^r$.

***Exemple 4.6.3* (Le groupe $\mathbb{Z}^r$).** — Pour $1 \leq j \leq r$ nous notons e_j l'élément dont la j-ème coordonnée vaut 1 et les autres 0. Tout élément x de $\mathbb{Z}^r$ a une unique écriture

$$x = \sum_{i=1}^{r} x_i e_i.$$

Le système $(e_1, e_2, \ldots, e_r)$ est donc un système générateur. Il est aussi $\mathbb{Z}$-*libre* : si $0 = \sum_{i=1}^{r} x_i e_i$, alors tous les x_i sont nuls. Il est appelé $\mathbb{Z}$-*base canonique* de $\mathbb{Z}^r$.

Un morphisme de groupes de $\mathbb{Z}^r$ dans $\mathbb{Z}^s$ est $\mathbb{Z}$-linéaire. Il est déterminé par sa matrice (à coefficients entiers) dans les bases canoniques de $\mathbb{Z}^r$ et $\mathbb{Z}^s$.

Exemple 4.6.4. — Le sous-ensemble de $\mathbb{R}$ défini par

$$A = \{a + b\sqrt{2} + c\sqrt{3} \mid a,\, b,\, c \in \mathbb{Z}\}$$

est un groupe libre. En effet l'application

$$\mathbb{Z}^3 \to \mathrm{G}, \qquad (a, b, c) \mapsto a + b\sqrt{2} + c\sqrt{3}$$

est un isomorphisme de groupes.

Exemple 4.6.5. — Le sous-ensemble de $\mathbb{C}$ appelé aussi entiers de Gauss

$$\mathbb{Z}[\mathbf{i}] = \{a + \mathbf{i}b \mid a,\, b \in \mathbb{Z}\}$$

est un groupe libre. En effet l'application

$$\mathbb{Z}^2 \to \mathrm{G}, \qquad (a, b) \mapsto a + \mathbf{i}b$$

est un isomorphisme de groupes.

Proposition 4.6.1

Soient s et r deux entiers naturels. Les deux groupes $\mathbb{Z}^r$ et $\mathbb{Z}^s$ sont isomorphes si et seulement si $r = s$.

Démonstration. — Supposons qu'il existe un morphisme injectif de groupes

$$\varphi \colon \mathbb{Z}^r \to \mathbb{Z}^s$$

que nous pouvons prolonger en un morphisme injectif, noté $\widetilde{\varphi}$, de $\mathbb{Z}^r$ dans $\mathbb{Q}^s$. Considérons dans l'espace vectoriel $\mathbb{Q}^s$ une relation linéaire à coefficients rationnels

$$\sum_{j=1}^{r} \lambda_j \widetilde{\varphi}(e_j) = 0$$

entre les images $\widetilde{\varphi}(e_1)$, $\widetilde{\varphi}(e_2)$, $\ldots$, $\widetilde{\varphi}(e_r)$ des éléments de la $\mathbb{Z}$-base canonique de $\mathbb{Z}^r$.

Multiplions les rationnels λ_j par un dénominateur commun d ; nous obtenons un élément $\sum_{j=1}^{r} d\lambda_j e_j$ de $\mathbb{Z}^r$ dont l'image par $\widetilde{\varphi}$, et donc par φ, est nulle. Puisque φ est injective, $\sum_{j=1}^{r} d\lambda_j e_j$ est nul dans $\mathbb{Z}^r$. Par suite tous les $d\lambda_j$, $1 \leq j \leq r$, sont nuls.

La famille $(\widetilde{\varphi}(e_1), \widetilde{\varphi}(e_2), \ldots, \widetilde{\varphi}(e_r))$ est libre dans $\mathbb{Q}^s$; il en résulte que $r \leq s$.

Si $\mathbb{Z}^r$ et $\mathbb{Z}^s$ sont isomorphes, nous avons donc $r = s$. □

Corollaire-Définition 4.6.1

Si G est un groupe abélien libre de type fini, il existe un unique entier naturel r tel que G est isomorphe à $\mathbb{Z}^r$.
Cet entier r est appelé *rang* de G.
Un système de générateurs de G composé de r éléments est appelé une $\mathbb{Z}$-base de G.

Attention la notion de $\mathbb{Z}$-base n'a de sens que pour un groupe libre.

Un produit de deux groupes libres de rangs respectifs r et s est libre de rang $r + s$.

Théorème 4.6.1

Un sous-groupe d'un groupe libre de rang r est libre. Son rang s est au plus égal à r.

Exemple 4.6.6. — Les sous-groupes de $\mathbb{Z}$ sont les ensembles $n\mathbb{Z}$, $n \in \mathbb{N}$. Ils sont de rang 1 excepté 0 qui est de rang 0. Ainsi il peut exister un sous-groupe, distinct du groupe, de même rang que le groupe (comparer avec les espaces vectoriels et leur dimension : l'analogie avec les notions correspondantes de la catégorie des espaces vectoriels a ses limites...)

Démonstration. — Considérons un groupe libre L de rang r, une $\mathbb{Z}$-base $\mathcal{B} = (e_1, e_2, \ldots, e_r)$ de L et un sous-groupe M de L. Pour $1 \leq j \leq r$ nous désignons par L_j le sous-groupe libre de L engendré par $(e_1, e_2, \ldots, e_j)$ et par M_j le sous-groupe de L_j donné par $\mathrm{M}_j = \mathrm{M} \cap \mathrm{L}_j$.

La démonstration se fait par récurrence sur r.

Lorsque $r = 0$ il n'y a rien à prouver.

Lorsque $r = 1$ le groupe L est isomorphe à $\mathbb{Z}$. Les sous-groupes de $\mathbb{Z}$ sont engendrés par un élément donc libres de rang 0 ou 1 (Exemple 4.6.6).

Supposons désormais que $r \geq 1$. Par hypothèse de récurrence M_{r-1} est libre de rang $\leq r-1$. Tout élément x de M se décompose de manière unique comme suit sur la $\mathbb{Z}$-base $\mathcal{B}$:

$$x = x_1 e_1 + x_2 e_2 + \ldots + x_r e_r.$$

Considérons l'application

$$\mathrm{M} \to \mathbb{Z}, \qquad x \mapsto x_r.$$

Notons que son noyau est le sous-groupe M_{r-1}. De plus son image est un sous-groupe de $\mathbb{Z}$ qui est donc engendré par un entier a_r.

- ◇ Si $a_r = 0$, alors $\mathrm{M} = \mathrm{M}_{r-1}$ et M est libre de rang $\leq r-1$.
- ◇ Si $a_r \neq 0$, nous choisissons un élément z de M tel que $z_r = a_r$ (par hypothèse il y en a au moins un). Nous considérons le produit $\mathrm{M}_{r-1} \times \mathbb{Z}$ et le morphisme

$$\mathrm{M}_{r-1} \times \mathbb{Z} \to \mathrm{M}, \qquad (x, n) \mapsto x + nz$$

dont on peut vérifier qu'il est injectif et surjectif. Le groupe M est isomorphe à $\mathrm{M}_{r-1} \times \mathbb{Z}$ libre de rang $\leq r$.

□

Soit G un groupe abélien de type fini. Ainsi il existe un morphisme surjectif $\pi\colon \mathbb{Z}^r \to \mathrm{G}$. Le noyau K de ce morphisme est un groupe libre de type fini de rang $s \leq r$. Les éléments de K sont associés aux relations entre les généateurs de G. Précisément pour toute relation

$$\sum_{i=1}^{r} \lambda_i a_i = 0$$

entre les générateurs de G le vecteur $(\lambda_1, \lambda_2, \ldots, \lambda_r)$ se décompose de manière unique sur la $\mathbb{Z}$-base de K.

Soit H un sous-groupe de G ; alors $\mathrm{L} = \pi^{-1}(\mathrm{H})$ est un sous-groupe de $\mathbb{Z}^r$ donc libre de rang $r' \leq r$. La restriction de π à L est un morphisme surjectif de L sur H qui est donc de type fini.

Exemple 4.6.7. — Considérons dans $\mathbb{Z}^4$ le sous-ensemble G suivant

$$\mathrm{G} = \{x \in \mathbb{Z}^4 \mid x_1 + 2x_2 + 3x_3 = 0,\ 2x_2 + x_4 = 0\};$$

c'est un groupe libre de rang 2. L'application

$$\varphi\colon \mathbb{Z}^2 \to \mathrm{G}, \qquad (x_2, x_3) \mapsto (-2x_2 - 3x_3, x_2, x_3, -2x_2)$$

est un isomorphisme de groupes.

Précisons le Théorème 4.6.1 :

Théorème 4.6.2

Soit L un groupe abélien libre de rang r. Soit M un sous-groupe non réduit à $\{0\}$. Il existe une $\mathbb{Z}$-base $\mathcal{B}$ de L, des éléments $e_1, e_2, \ldots, e_s$ de $\mathcal{B}$ et des entiers $a_1, a_2, \ldots, a_s$ non nuls tels que

1. les éléments $a_1e_1, a_2e_2, \ldots, a_se_s$ forment une $\mathbb{Z}$-base de M ;
2. les a_i sont ordonnés pour la relation de divisibilité $a_1|a_2|\ldots|a_s$;
3. les entiers $a_1, a_2, \ldots, a_s$ ne dépendent que de la donnée de M dans L. Ils sont appelés *facteurs invariants* de M dans L.

Le quotient L/M est isomorphe au produit

$$\mathbb{Z}^{r-s} \times \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_s\mathbb{Z}$$

Soit G un groupe abélien de type fini engendré par une famille finie $(g_1, g_2, \ldots, g_r)$. Il existe un morphisme surjectif

$$\mathbb{Z}^r \to \mathrm{G}, \qquad (n_1, n_2, \ldots, n_r) \mapsto \sum_{i=1}^{r} n_i g_i.$$

Le noyau de ce morphisme est un sous-groupe (distingué) M de $\mathbb{Z}^r$; il est donc libre. Le quotient $\mathbb{Z}^r/\mathrm{M}$ est isomorphe à G. Soient $a_1, a_2, \ldots, a_s$ les facteurs invariants de M. Le Théorème 4.6.2 assure que le groupe G est isomorphe à

$$\mathbb{Z}^{r-s} \times \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_s\mathbb{Z}.$$

Exemple 4.6.8. — Soit G un groupe abélien de type fini de rang 13 dont les diviseurs élémentaires sont 2^5, 2^3, 2, 2, 3^3, 3 et 5.

Les facteurs invariants de G sont donc

$$2^5 \times 3^3 \times 5 = 4320, \qquad 2^3 \times 3 = 24, \qquad 2 \qquad 2.$$

Il en résulte que

$$\mathrm{G} \simeq \mathbb{Z}^{13} \times \mathbb{Z}/4320\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Exemple 4.6.9. — Soit G le groupe abélien défini par

$$\mathrm{G} = \mathbb{Z}^2 \times \mathbb{Z}/162\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}.$$

Notons que $162 = 3^4 \times 2$ et $21 = 7 \times 3$. Par conséquent

$$\mathbb{Z}/162\mathbb{Z} \simeq \mathbb{Z}/3^4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \mathbb{Z}/21\mathbb{Z} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

Ainsi

$$\mathrm{G} \simeq \mathbb{Z}^2 \times \mathbb{Z}/3^4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Les diviseurs élémentaires de G sont 3^4, 7, 2 et 3 et les facteurs invariants de G sont $3^4 \times 7 \times 2 = 1134$ et 3. Il s'en suit que

$$\mathrm{G} \simeq \mathbb{Z}^2 \times \mathbb{Z}/1134\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Démonstration du Théorème 4.6.2. — La démonstration se fait par récurrence sur le rang de M.

Existence. Soit L′ l'ensemble des formes $\mathbb{Z}$-linéaires sur L. Notons que par restriction toute forme f induit une forme de M dans $\mathbb{Z}$. L'image $f(\mathrm{M})$ est aussi un idéal, contenu dans $f(\mathrm{L})$. Parmi tous les éléments de L′ il en existe dont la restriction à M n'est pas identiquement nulle. Choisissons une forme f telle que l'idéal $f(M)$ soit engendré par un élément positif non nul a_1 le plus petit possible (un tel entier existe puisqu'un ensemble d'entiers naturels non vide a un plus petit élément). Choisissons également un élément x_1 de M tel que $f(x_1) = a_1$. Soit $\mathcal{B}_0$ une $\mathbb{Z}$-base de L. Toute forme $\mathbb{Z}$-linéaire prend sur x_1 une valeur qui est un multiple de a_1 sinon nous pourrions en trouver une qui prend une valeur non nulle inférieure. En particulier les formes coordonnées pour une $\mathbb{Z}$-base $\mathcal{B}_0$ ont cette propriété ; ceci montre que les coordonnées

de x_1 dans la $\mathbb{Z}$-base $\mathcal{B}_0$ sont divisibles par a_1. Par suite il existe un élément e_1 de L tel que $x_1 = a_1 e_1$ et $f(e_1) = 1$. Montrons que $\mathrm{L} \simeq \mathbb{Z} \times \ker f$. Considérons le morphisme

$$\phi\colon \mathbb{Z} \times \ker f \to \mathrm{L} \qquad\qquad (a, x) \mapsto a e_1 + x.$$

Soit y dans L. L'équation $f(y - \alpha e_1) = 0$ a pour unique solution $\alpha = f(y)$. Il s'en suit que ϕ est bijectif.

Notons que $\ker f$ est un groupe libre de rang $\operatorname{rg} \mathrm{L} - 1$. Le morphisme

$$\varphi\colon \mathbb{Z} \times (\mathrm{M} \cap \ker f) \to \mathrm{M} \qquad\qquad (a, x) \mapsto a x_1 + x$$

est aussi un isomorphisme et $\mathrm{M} \cap \ker f$ est un sous-groupe libre de $\ker f$ de rang $s - 1$. Si $s = 1$ la démonstration est terminée. Sinon par hypothèse de récurrence il existe une $\mathbb{Z}$-base de $\ker f$, une partie $(e_2, e_3, \ldots, e_s)$ de $\mathcal{B}_1$ et des entiers $a_2, a_3, \ldots, a_s$ tels que $(a_2 e_2, a_3 e_3, \ldots, a_s e_s)$ soit une $\mathbb{Z}$-base de $\mathrm{M} \cap \ker f$. Nous terminons la preuve en prenant pour $\mathcal{B}$ la $\mathbb{Z}$-base obtenue en adjoignant e_1 à $\mathcal{B}_1$.

Unicité. Le sous-groupe M est donc libre de type fini. Se donner un tel groupe revient à se donner une famille génératrice $\mathcal{V}$ de t éléments de L. Leurs coordonnées dans une base $\mathcal{B}_0$ de L sont les colonnes d'une matrice A de $M_{r,t}(\mathbb{Z})$.

L'existence d'une base $\mathcal{B}$ de L avec les propriétés de l'énoncé équivaut à l'existence

1. d'une matrice P inversible dans $M_r(\mathbb{Z})$ (la matrice de passage de la base $\mathcal{B}$ à la base $\mathcal{B}_0$) ;
2. d'une matrice Q de $M_{t,s}(\mathbb{Z})$ (la matrice des coordonnées des vecteurs de la famille $(a_1 e_1, a_2 e_2, \ldots, a_s e_s)$ dans la famille génératrice $\mathcal{V}$) ;
3. d'une matrice R de $M_{t,s}(\mathbb{Z})$ (la matrice des coordonnées des vecteurs de la famille $\mathcal{V}$ dans la base $(a_1 e_1, a_2 e_2, \ldots, a_s e_s)$)

telles que

$$PAQ = \begin{pmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & & a_s \\ 0 & 0 & \ldots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}$$

Le pgcd des coefficients de A divise le pgcd des coefficients de PA ; nous en déduisons qu'ils sont égaux. Notons qu'il y a une propriété analogue pour A et AQ (remarquer que si $AQ = A'$ alors $A'R = A$). Il en résulte que le plus petits des invariants de A est le pgcd de ses coefficients.

Plus généralement soit $n \leq s$ un entier, soit I un sous-ensemble de n éléments extraits de $\{1, 2, \ldots, r\}$ et J un sous-ensemble de n éléments extraits de $\{1, 2, \ldots, s\}$. Notons A_I la matrice de taille $n \times s$ extraite de A et formée des lignes de A dont l'indice appartient à I.

Désignons par Q_J la matrice de taille $s \times n$ extraite de Q et formée des colonnes de Q dont l'indice appartient à J. Considérons alors le produit $B_{IJ} = A_I Q_J$ dans $M(n, \mathbb{Z})$. Notons que toute colonne du produit B_{IJ} est combinaison linéaire des colonnes de A_I. Par conséquent le déterminant $\det B_{IJ}$ appartient à l'idéal engendré par les mineurs de A_I de taille $n \times n$ donc à l'idéal engendré par les mineurs $n \times n$ de A. L'idéal de $\mathbb{Z}$ engendré par les mineurs $n \times n$ de A est égal à l'idéal engendré par les $n \times n$ mineurs de AQ.

Nous avons une propriété analogue pour A et PA lorsque P est dans $\mathrm{GL}(s, \mathbb{Z})$. Il en résulte que le $n$ième en invariant de A est le pgcd de ses $b \times n$ mineurs. □

4.7. Groupes abéliens de torsion

Un élément d'un groupe abélien est de *torsion* s'il est d'ordre fini. Autrement dit un élément g d'un groupe abélien est de torsion s'il engendre un sous-groupe cyclique fini ou encore s'il existe un entier non nul n tel que $ng = 0$.

Un groupe abélien est de *torsion* si tous ses éléments sont de torsion.

Proposition 4.7.1

Un groupe abélien est de type fini et de torsion si et seulement s'il est fini.

Démonstration. — Soit G un groupe abélien fini. Il est de type fini et chacun de ses éléments est d'ordre fini donc de torsion. Il existe un entier (le ppcm des ordres des éléments de G convient mais aussi l'ordre de G) qui annule tous les éléments de G.

Réciproquement montrons qu'un groupe abélien de type fini et de torsion est fini. Soit G un groupe abélien de type fini. Le Théorème 4.6.2 assure que

$$\mathrm{G} \simeq \mathbb{Z}^r \times \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_s\mathbb{Z}$$

où $r \geq 0$, $a_j \geq 0$ pour tout $1 \leq j \leq s$ et a_i divise a_{i+1} pour tout $1 \leq i \leq s-1$. De plus G est de torsion, *i.e.* tout élément est d'ordre fini. Il en résulte que $r = 0$, c'est-à-dire que

$$\mathrm{G} \simeq \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_s\mathbb{Z}.$$

En particulier $|\mathrm{G}| = a_1 a_2 \ldots a_s < \infty$. □

Théorème 4.7.1

Un groupe abélien de type fini est isomorphe au produit de son sous-groupe de torsion (fini) par un groupe libre.
En particulier un groupe abélien de type fini sans torsion est libre.

Démonstration. — Soit G un groupe engendré par un système fini de générateurs $(g_1, g_2, \ldots, g_r)$. Considérons un sous-système $\mathbb{Z}$-libre maximal. Quitte à réindicer les générateurs nous pouvons supposer que le système $(g_1, g_2, \ldots, g_s)$, $s \leq r$, est $\mathbb{Z}$-libre, ce qui revient à dire que le

sous-groupe L engendré par $(g_1, g_2, \ldots, g_s)$ est libre de rang s. Pour tout $s+1 \leq j \leq r$ il existe un entier non nul a_j tel que $a_j g_j$ appartient à L. Désignons par a le ppcm (non nul) des entiers $a_{s+1}, a_{s+2}, \ldots, a_r$. L'application

$$\mathrm{G} \to \mathrm{L}, \qquad x \mapsto ax$$

est surjective ; son noyau est le sous-groupe T des éléments de torsion de G. En effet si ax est nul, c'est que x est de torsion. Réciproquement si x est de torsion, ax appartient à $\mathrm{L} \cap \mathrm{T} = \{0\}$ donc ax est nul. L'application

$$\mathrm{G}/\mathrm{T} \to \mathrm{L}, \qquad \overline{x} \mapsto ax$$

est bien définie et injective. Le groupe G/T s'identifie à un sous-groupe de L qui est libre (Théorème 4.6.1). Or nous avons aussi un morphisme injectif de L dans G/T induit par l'application quotient. D'après la Proposition 4.6.1 les groupes L et G/T sont libres et de même rang. Soient $x_1, x_2, \ldots, x_s$ des éléments de G dont les classes $\overline{x_1}, \overline{x_2}, \ldots, \overline{x}_s$ forment une $\mathbb{Z}$-base de G/T. Considérons le morphisme

$$\phi\colon \mathrm{T} \times \mathbb{Z}^s \to \mathrm{G}, \qquad (x, n_1, n_2, \ldots, n_s) \mapsto x + \sum_{i=1}^{s} n_i x_i.$$

Remarquons que si $x + \sum_{i=1}^{s} n_i x_i = y$ est vraie dans G, alors $\sum_{i=1}^{s} n_i \overline{x}_i = \overline{y}$ est vraie dans G/T. Il s'en suit que ϕ est bijectif. □

4.8. Classification des matrices équivalentes à coefficients entiers, facteurs invariants de matrices

Rappelons que le groupe $\mathrm{GL}(n, \mathbb{Z})$ est composé des matrices carrées de taille $n \times n$ à coefficients dans $\mathbb{Z}$ inversibles dont l'inverse est aussi à coefficients dans $\mathbb{Z}$; il est équivalent de dire que le déterminant vaut ± 1.

Lemme 4.8.1

Soit A un matrice de taille $m \times n$ à coefficients dans $\mathbb{Z}$. Il existe $P \in \mathrm{GL}(m, \mathbb{Z})$ et $Q \in \mathrm{GL}(n, \mathbb{Z})$ tels que

$$PAQ = \begin{pmatrix} d_1 & & & & & & \\ & \ddots & & & & & \\ & & d_s & & & & \\ & & & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 \cdots & 0 \end{pmatrix}$$

où d_1, d_2, …, d_s sont des entiers positifs satisfaisant $d_1|d_2|\dots|d_s$ appelés *facteurs invariants de la matrice* A. Ils sont entièrement déterminés par A.

Cet énoncé assure qu'une matrice à coefficients entiers est déterminée, à équivalence près, non seulement par son rang s (le seul invariant pour les matrices à coefficients dans un corps) mais aussi par ses facteurs invariants d_1, d_2, …, d_s.

Démonstration. — **Unicité**.

Commençons par l'unicité des d_i. Remarquons que d_1 est le pgcd (positif) de tous les coefficients de A ; en effet le pgcd des coefficients de A divise tous les coefficients de PAQ et inversement le pgcd des coefficients de PAQ divise tous les coefficients de $A = P^{-1}(PAQ)Q^{-1}$. En particulier d_1 est unique.

Étendons cette observation de la manière suivante. Désignons par $m_k(A)$ le pgcd des mineurs d'ordre k de A. Notons que pour $k = 1$ on retrouve le pgcd des coefficients de A. Le point crucial est l'invariance par équivalence

$$\forall\, P \in \mathrm{GL}(m, \mathbb{Z}) \qquad \forall\, Q \in \mathrm{GL}(n, \mathbb{Z}) \qquad m_k(PAQ) = m_k(A). \tag{4.8.1}$$

Par suite $m_k(A) = d_1 d_2 \dots d_k$; les d_i sont donc entièrement déterminés par A.

Remarquons que pour démontrer (4.8.1) il suffit de montrer que pour toute matrice P à coefficients entiers nous avons

$$m_k(A) \,|\, m_k(PA). \tag{4.8.2}$$

En effet si P est inversible cela implique

$$m_k(A) \,|\, m_k(PA) \,|\, m_k(P^{-1}PA) = m_k(A)$$

donc $m_k(PA) = m_k(A)$. Par passage à la transposée cela fournit aussi $m_k(AQ) = m_k(A)$ et donc (4.8.1).

Reste à montrer (4.8.2) : cette relation se montre directement en exprimant les mineurs de PA comme combinaisons linéaires à coefficients entiers des mineurs de A (les détails sont laissés en exercice).

Existence de P et Q.

Comme pour la classification à équivalence près des matrices à coefficients dans un corps, on effectue des opérations élémentaires, qui peuvent s'interpréter comme la multiplication à droite ou à gauche par certaines matrices, dont des matrices carrées dites *élémentaires* qui ne diffèrent de la matrice identité que par un seul coefficient, situé hors de la diagonale. **La différence avec le cas d'un corps est qu'on ne peut pas diviser**.

Plus précisément notons E_{ij} la matrice dont tous les coefficients sont nuls, sauf celui situé sur la $i$ème ligne et la $j$ème colonne qui vaut 1.

Les opérations autorisées sont les suivantes :

- ◇ la multiplication à gauche par la matrice $\mathrm{id} + \alpha E_{ij}$ qui permet d'ajouter à la $i$ème ligne α fois la $j$ème ligne ;
- ◇ la multiplication à droite par la matrice $\mathrm{id} + \alpha E_{ij}$ qui permet d'ajouter à la $j$ème colonne α fois la $i$ème colonne.

Remarquons que grâce à ses opérations on peut changer deux lignes ou deux colonnes quitte à changer le signe d'une d'elles :

$$\begin{pmatrix} L_i \\ L_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} L_i \\ L_i + L_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} -L_j \\ L_i + L_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} -L_j \\ L_i \end{pmatrix} \tag{4.8.3}$$

Nous allons montrer que partant de A, à l'aide de ces seules opérations élémentaires, on peut arriver à une matrice du type voulu à ceci près : d_s ne sera pas nécessairement positif.

Nous allons raisonner par récurrence sur la taille de la matrice :

- ◇ Si A est une matrice 1×1 à coefficients dans $\mathbb{Z}$ l'énoncé est immédiat.
- ◇ Supposons désormais que l'énoncé soit vrai pour toute matrice B de taille $k \times \ell$ à coefficients dans $\mathbb{Z}$ où $k < m$ et $\ell < n$.

  Soit λ_1 le pgcd (positif) des coefficients de la première colonne. Appliquons des opérations élémentaires sur les lignes pour obtenir une première colonne dont tous les coefficients sont nuls, sauf le coefficient a_{11} qui sera égal à $\pm\lambda_1$. Quitte à échanger les deux premières lignes on peut supposer $|a_{11}| \geq |a_{21}|$. Si $a_{21} = 0$, alors il n'y a rien à faire sinon effectuons la division euclidienne $a_{11} = ba_{21} + c$ avec $0 \leq c < |a_{21}|$. En effectuant la transformation élémentaire dans laquelle la seconde ligne, multipliée par b, est soustraite à la première, les coefficients (a_{11}, a_{21}) sont transformés en (c, a_{21}) avec $|a_{21}| + |c| < |a_{11}| + |a_{21}|$. En itérant, l'algorithme d'Euclide nous indique qu'on finit par arriver au couple $(\mathrm{pgcd}(a_{11}, a_{21}), 0)$. En répétant ce procédé sur chaque ligne on arrive à

la première colonne souhaitée

$$\begin{pmatrix} \pm\lambda_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

La même méthode peut alors être appliquée à la première ligne, en utilisant des opérations élémentaires sur les colonnes, pour obtenir une matrice dont la première ligne a la forme $(\pm\lambda_2, 0, 0, \ldots, 0)$ où λ_2 est le pgcd des coefficients de la première ligne. Malheureusement nous avons ainsi modifié la première colonne donc les coefficients ne sont donc peut-être plus nuls. Néanmoins nous avons gagné quelque chose : $0 \leq \lambda_2 \leq \lambda_1$ puisque c'est le pgcd de λ_1 et des autres coefficients. Nous itérons donc la construction en mettant alternativement des 0 sur la première colonne et la première ligne : les coefficients à la place $(1, 1)$, positifs, décroissent : $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \ldots \geq 0$. Cette suite se stabilise donc : on obtient par exemple une première ligne $(\delta_1\ 0\ 0\ \ldots\ 0)$ où δ_1 est aussi un pgcd des coefficients de la première colonne donc divise tous ces coefficients. Il suffit alors de retrancher à chaque ligne un multiple adéquat de la première pour arriver à une matrice du type

$$\begin{pmatrix} \delta_1 & 0 & \cdots & 0 \\ 0 & & & \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}.$$

On applique alors l'hypothèse de récurrence à B pour parvenir à une matrice

$$\begin{pmatrix} \delta_1 & & & & & \\ & \delta_2 & & & & \\ & & \ddots & & & \\ & & & \delta_s & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

où $\delta_2 \,|\, \delta_3 \,|\, \ldots \,|\, \delta_s$.

Il n'y a, a priori, pas de raison pour que δ_1 divise δ_2. Mais nous pouvons remplacer le couple (δ_1, δ_2) par (d_1, m_2) où d_1 et m_2 sont des pgcd et ppcm de δ_1 et δ_2. En effet par

l'application d'une transformation élémentaire puis du procédé précédent nous obtenons successivement en n'écrivant que les deux premières lignes et colonnes, sur lesquelles les opérations ont lieu :

$$\begin{pmatrix} \delta_1 & 0 \\ 0 & \delta_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} \delta_1 & 0 \\ \delta_2 & \delta_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} d_1 & d'_1 \\ 0 & m'_2 \end{pmatrix}$$

où nous avons en fait $m'_2 = m_2$ puisque le déterminant de la matrice reste inchangé : $d_1 m_2 = \delta_1\delta_2 = d_1 m'_2$. De plus le pgcd des coefficients, à savoir d_1, reste aussi inchangé, donc d_1 divise d'_1. Une dernière opération élémentaire nous permet d'arriver à la forme voulue $\begin{pmatrix} d_1 & 0 \\ 0 & m_2 \end{pmatrix}$.

Appliquant le même procédé au couple (m_2, δ_3) on peut le remplacer par le couple $(\mathrm{pgcd}(m_2, \delta_3), \mathrm{ppcm}(m_2, \delta_3))$. Puisque $d_1 = \mathrm{pgcd}(\delta_1\delta_2)$ et $\delta_2 \,|\, \delta_3$, d divise $d_2 = \mathrm{pgcd}(m_2, \delta_3)$. En itérant le procédé on remplace les coefficients $(\delta_1, \delta_2, \ldots, \delta_r)$ par $(d_1, d_2, \ldots, d_r)$ avec $d_1 \,|\, d_2 \,|\, \ldots \,|\, d_r$.

Reste enfin à régler la question des signes : en se restreignant toujours aux opérations élémentaires on peut changer les signes deux par deux en faisant deux fois les opérations décrites en (4.8.3) :

$$\begin{pmatrix} L_i \\ L_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} -L_j \\ L_i \end{pmatrix} \rightsquigarrow \begin{pmatrix} -L_i \\ -L_j \end{pmatrix}$$

Cela termine la récurrence : seul d_s peut encore être négatif (et uniquement si $n = m = s$). Pour finir de démontrer le Lemme il suffit si $d_s < 0$ de multiplier à droite par $\mathrm{id} - 2E_{ss}$ (à noter que c'est l'unique fois que l'on multiplie par une matrice de déterminant -1).

□

CHAPITRE 5

DEUX EXEMPLES DE GROUPES NON ABÉLIENS

La classification des groupes simples finis est un ensemble de travaux, principalement publiés entre environ 1955 et 1983, qui a pour but de classer tous les groupes finis simples. En tout, cet ensemble comprend des dizaines de milliers de pages publiées dans 500 articles par plus de 100 auteurs. Il est à noter qu'une partie « combinatoire » de la démonstration nécessite l'utilisation de l'ordinateur. Dans le tableau qui suit :

- ◇ la première colonne indique le nombre d'éléments du groupe,
- ◇ la seconde indique le nombre de structures de groupes (on dira de groupes non isomorphes) ayant ce nombre d'éléments
- ◇ et la troisième colonne fournit la liste de ces groupes.

$\lvert G\rvert$	#	liste des groupes à isomorphisme près
4	2	$\mathbb{Z}/4\mathbb{Z}$, $D_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
6	2	$\mathbb{Z}/6\mathbb{Z}$, D_6
8	5	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{H}_8$, D_8
9	2	$\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
10	2	$\mathbb{Z}/10\mathbb{Z}$, D_{10}
12	5	$\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathcal{A}_4 \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, D_{12}
14	2	$\mathbb{Z}/14\mathbb{Z}$, D_{14}
15	1	$\mathbb{Z}/15\mathbb{Z}$
16	14	...
18	5	$\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathfrak{S}_3$, $\left(\mathbb{Z}/3\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/2\mathbb{Z}$, D_{18}
20	5	$\mathbb{Z}/20\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \rtimes_{\varphi_1} \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \rtimes_{\varphi_2} \mathbb{Z}/4\mathbb{Z}$, D_{20}
21	2	$\mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$
22	2	$\mathbb{Z}/22\mathbb{Z}$, D_{22}
24	15	...
25	2	$\mathbb{Z}/25\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$
26	2	$\mathbb{Z}/26\mathbb{Z}$, D_{26}

Rappelons que

- le sous-groupe cyclique de D_{2n} engendré par la rotation r est isomorphe à $\mathbb{Z}/n\mathbb{Z}$;
- tout groupe d'ordre p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, c'est pourquoi les groupes d'ordres premiers ne figurent pas dans le tableau.

Ce tableau justifie en partie pourquoi nous détaillons les propriétés des groupes diédraux et symétriques.

5.1. Les groupes symétriques et alternés

Lemme 5.1.1

Soit $n \geq 0$ un entier. Soient X et Y deux ensembles de cardinal n.
L'ensemble des bijections de X sur Y a pour cardinal $n!$.
En particulier (cas où $Y = X$) le groupe $\mathfrak{S}_X$ compte $n!$ éléments.

Démonstration par récurrence sur n. — Si $n = 0$, alors $X = Y = \emptyset$. Or si i est une application de l'ensemble vide dans lui-même, $i = \mathrm{id}$. Il y a donc une unique bijection de X sur Y (à savoir l'identité), et la propriété requise est démontrée puisque $0! = 1$.

Supposons $n > 0$ et la propriété vraie aux rangs $< n$. Comme $n > 0$ l'ensemble X est non vide ; on choisit $x \in X$. Pour tout y dans Y, on note B_y l'ensemble des bijections de X vers Y qui envoient x sur y. Le cardinal de B est alors égal à $\sum_{y \in Y} \mathrm{card}(B_y)$. Soit $y \in Y$. Se donner une bijection de X sur Y qui envoie x sur y revient à se donner une bijection de $X \smallsetminus \{x\}$ sur $Y \smallsetminus \{y\}$: une fois qu'on a imposé que l'image de x doit être égale à y, il reste à déterminer les images des autres éléments de X, nécessairement différentes de y. Comme $X \smallsetminus \{x\}$ et $Y \smallsetminus \{y\}$ sont de cardinal $n-1$, l'hypothèse de récurrence assure qu'il y a $(n-1)!$ bijections de $X \smallsetminus \{x\}$ sur $Y \smallsetminus \{y\}$; le cardinal de B_y est par conséquent égal à $(n-1)!$. Il vient

$$\mathrm{card}(B) = \sum_{y \in Y} \mathrm{card}(B_y) = \sum_{y \in Y} (n-1)! = \mathrm{card}(Y)(n-1)! = n \times (n-1)! = n!$$

□

Donnons la liste explicite de tous les éléments de $\mathfrak{S}_n$ pour les petites valeurs de n :

- $\mathfrak{S}_0 = \{\mathrm{id}\}$;
- $\mathfrak{S}_1 = \{\mathrm{id}\}$;
- $\mathfrak{S}_2$ compte $2 = 2!$ (Lemme 5.1.1) éléments qui sont

$$\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

◇ $\mathfrak{S}_3$ compte $6 = 3!$ (Lemme 5.1.1) éléments qui sont

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \sigma^2 \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Ce qui permet de dresser la table de Cayley $\mathfrak{S}_3$:

	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	e	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	e	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	e	σ^2	σ
$\sigma\tau$	$\sigma\tau$	s	$\sigma^2\tau$	σ	e	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	e

On constate que les tables de Cayley du groupe symétrique $\mathfrak{S}_3$ et du groupe diédral D_6 sont les mêmes. Ces deux groupes ont exactement la même structure, on dit qu'ils sont *isomorphes* (Définition 2.2.1).

◇ $\mathfrak{S}_4$ compte $24 = 4!$ (Lemme 5.1.1) éléments qui sont

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

5.1.1. Support d'une permutation. — Soit E un ensemble. Soit σ un élément de $\mathfrak{S}_E$. Un *point fixe* de σ est un élément x de E tel que $\sigma(x) = x$. Notons $\mathrm{Fix}(\sigma)$ l'ensemble des points fixes de σ. L'ensemble des éléments x de E tels que $\sigma(x) \neq x$ est appelé *support de* σ. Notons $\mathrm{Supp}(\sigma)$ le support de σ. Par construction

$$E = \mathrm{Fix}(\sigma) \bigsqcup \mathrm{Supp}(\sigma)$$

Remarque 5.1.1. — Nous avons l'équivalence : $\mathrm{Supp}(\sigma) = \emptyset$ si et seulement si $\mathrm{Fix}(\sigma) = E$, *i.e.* si et seulement si $\sigma(x) = x$ pour tout $x \in E$ donc si et seulement si $\sigma = \mathrm{id}$.

Remarque 5.1.2. — Pour tout $x \in E$ nous avons $\sigma(x) = x$ si et seulement si x est son propre antécédent par σ, *i.e.* si et seulement si $\sigma^{-1}(x) = x$. Il s'en suit que $\mathrm{Fix}(\sigma) = \mathrm{Fix}(\sigma^{-1})$ puis, par passage au complémentaire, que $\mathrm{Supp}(\sigma^{-1}) = \mathrm{Supp}(\sigma)$.

Exemple 5.1.1. — Supposons que $E = \{1, 2, 3, 4, 5\}$ et que

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$$

Alors $\mathrm{Fix}(\sigma) = \{3, 4\}$ et $\mathrm{Supp}(\sigma) = \{1, 2, 5\}$.

Comme σ est injective, $\sigma(\sigma(x)) = \sigma(x)$ si et seulement si $\sigma(x) = x$. Autrement dit $\sigma(x) \in \mathrm{Fix}(\sigma)$ si et seulement si $x \in \mathrm{Fix}(\sigma)$. Par passage au complémentaire $\sigma(x) \in \mathrm{Supp}(\sigma)$ si et seulement si $x \in \mathrm{Supp}(\sigma)$.

Par suite l'image et l'antécédent par σ d'un élément de $\mathrm{Supp}(\sigma)$ appartiennent à $\mathrm{Supp}(\sigma)$; par récurrence $\sigma^k(x)$ appartient à $\mathrm{Supp}(\sigma)$ pour tout $k \in \mathbb{Z}$ et tout $x \in \mathrm{Supp}(\sigma)$. Par conséquent σ induit une bijection de $\mathrm{Supp}(\sigma)$ dans lui-même qui n'a pas de point fixe (rappelons que par définition $\mathrm{Supp}(\sigma)$ ne contient aucun point fixe de σ). De même σ induit une bijection de $\mathrm{Fix}(\sigma)$ dans lui-même qui, par définition de $\mathrm{Fix}(\sigma)$, est l'identité.

Exemple 5.1.2. — Si $E = \{1, 2, 3, 4, 5\}$ et

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix},$$

alors σ induit l'identité de $\mathrm{Fix}(\sigma) = \{3, 4\}$ dans lui-même. Notons que σ induit aussi la bijection

$$1 \mapsto 2, \qquad 2 \mapsto 5, \qquad 5 \mapsto 1$$

de $\mathrm{Supp}(\sigma) = \{1, 2, 5\}$ dans lui-même.

Soient σ_1, σ_2, ..., σ_n des permutations de E. Si $\sigma_k(x) = x$ pour tout k, nous avons $(\sigma_1\sigma_2\dots\sigma_n)(x) = x$; il en résulte que $\bigcap_\ell \mathrm{Fix}(\sigma_\ell) \subset \mathrm{Fix}(\sigma_1\sigma_2\dots\sigma_n)$. Par passage au complémentaire $\mathrm{Supp}(\sigma_1\sigma_2\dots\sigma_n) \subset \bigcup_\ell \mathrm{Supp}(\sigma_\ell)$. En d'autres termes le support du produit est contenu dans la réunion des supports.

En particulier $\mathrm{Supp}(\sigma^\ell) \subset \mathrm{Supp}(\sigma)$ pour toute permutation σ de E et pour tout $\ell \in \mathbb{N}$. De plus $\mathrm{Supp}(\sigma) = \mathrm{Supp}(\sigma^{-1})$ donc $\mathrm{Supp}(\sigma^k) \subset \mathrm{Supp}(\sigma)$ pour toute permutation σ de E et pour tout $k \in \mathbb{Z}$.

Remarque 5.1.3. — Le support du produit est en général strictement contenu dans la réunion des supports. Considérons par exemple une permutation non triviale de E, alors $\mathrm{Supp}(\sigma) = \mathrm{Supp}(\sigma^{-1}) \neq \emptyset$ mais $\mathrm{Supp}(\sigma\sigma^{-1}) = \mathrm{Supp}(\mathrm{id}) = \emptyset$; en particulier $\mathrm{Supp}(\sigma\sigma^{-1}) \subsetneq \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\sigma^{-1})$.

5.1.2. Produit de permutations à supports disjoints. — Soit E un ensemble. Soient σ_1, σ_2, ..., σ_n des permutations de E à supports deux à deux disjoints. Soient S_1, S_2, ..., S_n des sous-ensembles deux à deux disjoints de E tels que $\mathrm{Supp}(\sigma_i) \subset S_i$ pour tout i (de tels S_i existent, on peut par exemple prendre $S_i = \mathrm{Supp}(\sigma_i)$).

Soit x dans S_i, alors $\sigma(x)$ appartient à S_i. En effet, si x est un point fixe de σ_i, alors $\sigma_i(x) = x$ et en particulier $\sigma_i(x)$ appartient à S_i. Si x appartient au support de σ_i alors $\sigma_i(x)$ appartient au support de σ_i qui est contenu dans S_i.

Soit x un élément de E. Nous avons l'alternative x appartient à aucun des S_i et il existe i tel que x appartient à S_i.

- ◇ Supposons que x n'appartienne à aucun des S_i ; il est alors fixe par tous les σ_i. Par conséquent $(\sigma_1\sigma_2\dots\sigma_n)(x) = x$.
- ◇ S'il existe un entier i tel que x appartient à S_i. Notons que cet entier est unique car les S_i sont deux à deux disjoints. Si $j > i$ alors x n'appartient pas à S_j et donc $\sigma_j(x) = x$. Il s'en suit que $(\sigma_{i+1}\dots\sigma_n)(x) = x$ et $(\sigma_i\sigma_{i+1}\dots\sigma_n)(x) = \sigma_i(x)$. L'image $\sigma_i(x)$ appartient à S_i ; elle n'appartient donc pas à S_j dès que $j < i$. Il s'en suit que

$$(\sigma_1\sigma_2\dots\sigma_n)(x) = (\sigma_1\sigma_2\dots\sigma_{i-1})(\sigma_i\sigma_{i+1}\dots\sigma_n)(x) = (\sigma_1\sigma_2\dots\sigma_{i-1})(\sigma_i(x)) = \sigma_i(x).$$

Autrement dit pour tout $x \in E$

- ◇ si x n'appartient à aucun des S_i, alors $(\sigma_1\sigma_2\dots\sigma_n)(x) = x$;
- ◇ sinon x appartient à S_i pour un unique i et $(\sigma_1\sigma_2\dots\sigma_n)(x) = \sigma_i(x)$.

En particulier le produit $\sigma_1\sigma_2\dots\sigma_n$ ne change pas si nous changeons l'ordre des σ_i : *le produit de permutations à supports deux à deux disjoints est commutatif.*

Puisque $\sigma_i(x) \neq x$ dès que $x \in \mathrm{Supp}(\sigma_i)$ ce qui précède entraîne que $(\sigma_1\sigma_2\dots\sigma_n)(x) = x$ si et seulement si x n'appartient à aucun des $\mathrm{Supp}(\sigma_i)$. Ainsi

$$\mathrm{Supp}(\sigma_1\sigma_2\dots\sigma_n) = \bigsqcup \mathrm{Supp}(\sigma_i).$$

Mais $\sigma_1\sigma_2\ldots\sigma_n = \mathrm{id}$ si et seulement si son support est vide ; ainsi $\sigma_1\sigma_2\ldots\sigma_n = \mathrm{id}$ si et seulement si $\mathrm{Supp}(\sigma_i)$ est vide pour tout i soit si et seulement si $\sigma_i = \mathrm{id}$ pour tout i.

5.1.3. Cycles. — Soit E un ensemble.

Soient $a_1, a_2, \ldots, a_\ell$ des éléments deux à deux distincts de E avec ℓ entier au moins égal à 2. Désignons par $(a_1\ a_2\ \ldots\ a_\ell)$ la permutation de E définie par

- ◇ si $x \notin \{a_1, a_2, \ldots, a_\ell\}$ alors $\sigma(x) = x$;
- ◇ $\sigma(a_i) = a_{i+1}$ pour tout $1 \leq i \leq \ell - 1$;
- ◇ $\sigma(a_\ell) = a_1$.

Une telle permutation est appelée un *ℓ-cycle*, ou *cycle de longueur ℓ*.

Exemple 5.1.3. — Supposons que $E = \{1, 2, 3, 4\}$. Le 3-cycle $(1\ 2\ 4)$ est la permutation qui fixe 3, envoie 1 sur 2, envoie 2 sur 4 et envoie 4 sur 1. En d'autres termes c'est la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Un 2-cycle de E est également appelé une *transposition*. Autrement dit si a_1 et a_2 sont deux éléments distincts de E, la transposition $(a_1\ a_2)$ est la permutation qui échange a_1 et a_2 et qui fixe tous les autres éléments de E.

Soit $\ell \geq 2$ un entier. Soient $a_1, a_2, \ldots, a_\ell$ des éléments de E deux à deux distincts. Soit σ le ℓ-cycle $(a_1\ a_2\ \ldots\ a_\ell)$. Par définition $\mathrm{Supp}(\sigma) = \{a_1, a_2, \ldots, a_\ell\}$. L'écriture de σ sous la forme $(a_1\ a_2\ \ldots\ a_\ell)$ n'est pas unique. En effet $\sigma = (a_2\ a_3\ \ldots a_\ell\ a_1)$ et plus généralement $\sigma = (a_i\ a_{i+1}\ \ldots\ a_\ell\ a_1\ a_2\ \ldots\ a_{i-1})$ pour tout $1 \leq i \leq \ell$.

Exemple 5.1.4. — Si $E = \{1, 2, 3, 4, 5\}$ et $\sigma = (1\ 5\ 4\ 2)$ alors σ s'écrit aussi $(5\ 4\ 2\ 1)$ mais aussi $(4\ 2\ 1\ 5)$ ou encore $(2\ 1\ 5\ 4)$.

La bijection réciproque σ^{-1} de $\sigma = (a_1\ a_2\ \ldots\ a_\ell)$ envoie a_ℓ sur $a_{\ell-1}$, $a_{\ell-1}$ sur $a_{\ell-2}, \ldots, a_3$ sur a_2, a_2 sur a_1, a_1 sur a_ℓ. Autrement dit σ^{-1} est le ℓ-cycle $(a_\ell\ a_{\ell-1}\ \ldots\ a_3\ a_2\ a_1)$. En d'autres termes l'inverse d'un cycle est un cycle obtenu par renversement de l'ordre des termes.

Exemple 5.1.5. — Si $E = \{1, 2, 3, 4, 5\}$ et $\sigma = (1\ 5\ 4\ 2)$ alors $\sigma^{-1} = (2\ 4\ 5\ 1)$.

Notons que l'itéré $k$ième d'un cycle n'est pas nécessairement un cycle. Considérons par exemple le 4-cycle $\sigma = (1\ 2\ 3\ 4)$ de $\mathfrak{S}_4$, alors $\sigma^2 = (1\ 3)(2\ 4)$.

Considérons un élément c de $\mathbb{Z}/\ell\mathbb{Z}$. Il existe un unique entier $n \in \{1, 2, \ldots, \ell\}$ tel que $c = \overline{n}$; posons $a_c = a_n$. Par exemple $a_{\overline{1}} = a_1$, $a_{\overline{0}} = a_{\overline{\ell}} = a_\ell$. Cette notation est très pratique pour décrire l'action de σ sur $\{a_1, a_2, \ldots, a_\ell\}$. En effet $\sigma(a_n) = a_{n+1}$ pour tout $1 \leq n \leq \ell - 1$ et $\sigma(a_\ell) = a_1$. Mais $\overline{1} = \overline{\ell} + \overline{1}$, nous pouvons donc écrire pour tout n

$$\sigma(a_{\overline{n}}) = a_{\overline{n}+\overline{1}} \qquad\qquad \sigma^{-1}(a_{\overline{n}}) = a_{\overline{n}-\overline{1}}$$

Il en résulte que pour tout $d \in \mathbb{Z}$ et tout n

$$\sigma^d(a_{\overline{n}}) = a_{\overline{n}+\overline{d}}.$$

Exemple 5.1.6. — Supposons que $E = \{1, 2, 3, 4, 5\}$, $\ell = 5$ et

$$\sigma = (a_1\ a_2\ a_3\ a_4\ a_5) = (2\ 4\ 1\ 5\ 3).$$

Calculons $\sigma^{-121}(1)$. D'une part $\sigma^{-121}(1) = \sigma^{-121}(a_3) = \sigma^{-121}(a_{\overline{3}}) = a_{\overline{3}-\overline{121}}$. D'autre part $\overline{121} = \overline{120} + \overline{1} = \overline{5 \times 24} + \overline{1} = \overline{0} + \overline{1}$. Par conséquent $\sigma^{-121}(1) = a_{\overline{3}-\overline{1}} = a_{\overline{2}} = a_2 = 4$.

Soit x un élément de $\mathrm{Supp}(\sigma)$. Alors $\sigma^d(x)$ appartient à $\mathrm{Supp}(\sigma)$ pour tout d dans $\mathbb{Z}$. Réciproquement tout élément y du support de σ est de la forme $\sigma^d(x)$ pour un certain $0 \leq d \leq \ell - 1$. En effet choisissons i et j tels que $x = a_{\overline{i}}$ et $y = a_{\overline{j}}$. Il existe un unique entier $0 \leq d \leq \ell - 1$ tel que $\overline{d} = \overline{j} - \overline{i}$ et

$$\sigma^d(x) = \sigma^d(a_{\overline{i}}) = a_{\overline{i}+\overline{d}} = a_{\overline{j}} = y.$$

Par suite $\mathrm{Supp}(\sigma) = \{\sigma^d(x)\}_{d \in \mathbb{Z}}$.

Le théorème qui suit joue un rôle central dans la théorie des permutations des ensembles finis. Il permet dans de nombreux cas de ramener l'étude d'une permutation quelconque à celle de permutations circulaires qui sont plus faciles à manipuler.

Théorème 5.1.1

Soit E un ensemble fini. Soit σ une permutation de E.
Il existe une famille finie $C_1, C_2, \ldots, C_r$ de cycles sur E à supports deux à deux disjoints tels que $\sigma = C_1 C_2 \ldots C_r$.
De plus cette écriture est « unique à permutation près des C_i ». En d'autres termes si $D_1 D_2 \ldots D_s$ est une autre écriture de σ comme produit de cycles à supports deux à deux disjoints, alors

- ◇ $r = s$,
- ◇ et il existe une permutation τ de $\{1, 2, \ldots, r\}$ telle que $D_i = C_{\tau(i)}$ pour tout i.

Exemple 5.1.7. — Soit E un ensemble fini. L'écriture de id comme produit de cycles à supports deux à deux disjoints est simplement son écriture comme produit vide de tels cycles.

Exemple 5.1.8. — Soit C un cycle de E. L'écriture de C comme produit de cycles à supports deux à deux disjoints est simplement l'écriture $C = C$. Il y a donc un seul cycle dans la décomposition de C à savoir C lui-même.

Exemple 5.1.9. — Soit σ la permutation de $\{1, 2, \ldots, 10\}$ donnée par

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 2 & 4 & 7 & 9 & 8 & 5 & 6 & 1 \end{pmatrix}$$

Nous avons

$$\sigma = (1\ 3\ 2\ 10)(5\ 7\ 8)(6\ 9)$$

Démonstration du Théorème 5.1.1. — ◇ Construction de cycles.

Soit x un élément de $\mathrm{Supp}(\sigma)$. Montrons qu'il existe $d > 0$ tel que $\sigma^d(x) = x$. Notons tout d'abord que comme E est fini, l'ensemble $\{\sigma^i(x)\}_{i\in\mathbb{N}}$ est fini. Par suite il existe deux entiers distincts $i > j$ tels que $\sigma^i(x) = \sigma^j(x)$ ou encore $x = \sigma^{j-i}(x)$; autrement dit il suffit de prendre $d = j - i$.

Ainsi l'ensemble $\{d > 0 \,|\, \sigma^d(x) = x\}$ est non vide ; il possède donc un plus petit élément ℓ. Puisque x appartient au support de σ, $\sigma(x) \neq x$ et $\ell \geq 2$. Les éléments x, $\sigma(x)$, $\sigma^2(x)$, $\ldots$, $\sigma^{\ell-1}(x)$ sont deux à deux distincts. En effet, raisonnons par l'absurde *i.e.* supposons qu'il existe deux entiers $0 < j < i < \ell$ tels que $\sigma^i(x) = \sigma^j(x)$. Alors $\sigma^{i-j}(x) = x$ mais $0 < i - j < \ell$: contradiction avec la définition de ℓ.

Considérons le ℓ-cycle $C_x = (x\ \sigma(x)\ \sigma^2(x)\ \ldots\ \sigma^{\ell-1}(x))$. Soit y un élément du support de C_x. Par définition de C_x nous avons $C_x(y) = \sigma(y)$ et $C_x^{-1}(y) = \sigma^{-1}(y)$. Par récurrence nous obtenons que $C_x^d(y) = \sigma^d(y)$ pour tout $d \in \mathbb{Z}$. La formule $\mathrm{Supp}(C_x) = \{C_x^d(y)\}_{d\in\mathbb{Z}}$ établie précédemment se réécrit

$$\mathrm{Supp}(C_x) = \{\sigma^d(y)\}_{d\in\mathbb{Z}}.$$

Soient x et z deux éléments du support de σ tels que

$$\mathrm{Supp}(C_x) \cap \mathrm{Supp}(C_z) \neq \emptyset.$$

Alors $C_x = C_z$. En effet soit $y \in \mathrm{Supp}(C_x) \cap \mathrm{Supp}(C_z)$. D'après ce qui précède

$$\mathrm{Supp}(C_x) = \{\sigma^d(y)\}_{d\in\mathbb{Z}} = \mathrm{Supp}(C_z)$$

et $C_x(w) = \sigma(w) = C_z(w)$ pour tout $w \in \mathrm{Supp}(C_x) = \mathrm{Supp}(C_z)$. Les permutations C_x et C_z ont donc même support et coïncident sur ce support commun. Il en résulte qu'elles sont égales.

◇ Existence de la décomposition.

Nous venons d'expliquer comment associer à chaque élément x de $\mathrm{Supp}(\sigma)$ un cycle C_x. Désignons par $\mathcal{C}$ l'ensemble des cycles de la forme C_x pour $x \in \mathrm{Supp}(\sigma)$. Notons r le cardinal de $\mathcal{C}$ et C_1, C_2, $\ldots$, C_r les éléments de $\mathcal{C}$. Nous avons pour tout i et tout $x \in \mathrm{Supp}(C_i)$

$$C_i(x) = \sigma(x)$$

et d'après ce qui précède les supports des C_i sont deux à deux disjoints.

Soit $x \in E$. Supposons dans un premier temps que x n'appartienne à aucun des $\mathrm{Supp}(C_i)$. Alors x n'appartient pas au support de σ. En effet, raisonnons par l'absurde : supposons que x appartienne au support de σ. Alors x appartient au support de C_x qui est l'un des C_i. Il s'en suit que $\sigma(x) = x$. Supposons maintenant que x appartient à $\mathrm{Supp}(C_i)$ pour un cerain i (nécessairement unique) ; alors $\sigma(x) = C_i(x)$.

Autrement dit

- ◇ les C_i sont des cycles à supports deux à deux disjoints.
- ◇ si x n'appartient à aucun des supports des C_i, alors $\sigma(x) = x$;
- ◇ si x appartient à $\mathrm{Supp}(C_i)$ pour un certain i, alors $\sigma(x) = C_i(x)$.

Ainsi d'après ce qui précède $\sigma = C_1 C_2 \dots C_r$.

◇ Unicité de la décomposition.

Supposons que σ s'écrive $D_1 D_2 \dots D_s$, les D_i désignant des cycles à supports deux à deux disjoints. Le support de σ est alors la réunion disjointe des supports des D_i.

Fixons $1 \leq i \leq s$. Puisque $\sigma = D_1 D_2 \dots D_s$ nous avons pour tout y dans $\mathrm{Supp}(D_i)$

$$\sigma^d(y) = D_i^d(y).$$

Si x appartient à $\mathrm{Supp}(D_i)$, alors

$$\mathrm{Supp}(D_i) = \{D_i^d(x)\}_{d\in\mathbb{Z}} = \{\sigma^d(x)\}_{d\in\mathbb{Z}} = \mathrm{Supp}(C_x).$$

Par ailleurs pour tout $y \in \mathrm{Supp}(D_i) = \mathrm{Supp}(C_x)$ nous avons $D_i(y) = \sigma(y) = C_x(y)$. Il en résulte que les permutations D_i et C_x ont même support et coïncident sur ce support commun. Elles sont donc égales.

D'après ce qui précède $\{D_1, D_2, \dots, D_s\}$ est l'ensemble des cycles de la forme C_x, $x \in \mathrm{Supp}(\sigma)$. Autrement dit $\{D_1, D_2, \dots, D_s\} = \{C_1, C_2, \dots, C_r\}$.

□

Grâce à cette démonstration nous pouvons donner l'algorithme permettant d'écrire une permutation quelconque d'un ensemble fini E comme produit de cycles à supports deux à deux disjoints. Soit E un ensemble fini. Soit σ une permutation quelconque de E. Le cœur de cet algorithme consiste à associer à un élément x de $\mathrm{Supp}(\sigma)$ un cycle C_x. Il découle de la définition de ce dernier qu'il s'écrit $(x_1\ x_2\ \dots\ x_\ell)$ où (x_i) est la suite construite récursivement par le procédé suivant :

- ◇ $x_1 = x$;
- ◇ si $\sigma(x_i) = x$ on s'arrête, sinon on pose $x_{i+1} = \sigma(x_i)$.

La décomposition de σ s'obtient alors comme suit. Si $\sigma = \mathrm{id}$, il y a rien à faire. Sinon on construit une suite $y_1, y_2, \dots, y_s$ d'éléments de $\mathrm{Supp}(\sigma)$ comme suit :

- ◇ on prend pour y_i n'importe quel élément de $\mathrm{Supp}(\sigma)$;
- ◇ si la réunion des supports des cycles $C_{y_1}, C_{y_2}, \dots, C_{y_i}$ est égale au support de σ on arrête, sinon on prend pour y_{i+1} n'importe quel élément de

$$\mathrm{Supp}(\sigma) \smallsetminus \Big(\mathrm{Supp}(C_{y_1}) \bigsqcup \mathrm{Supp}(C_{y_2}) \bigsqcup \dots \bigsqcup \mathrm{Supp}(C_{y_i})\Big).$$

L'écriture cherchée est alors $\sigma = C_{y_1} C_{y_2} \dots C_{y_s}$ (les cycles C_{y_i} sont eux-mêmes construits par le procédé décrit précédemment).

Voyons ce que cela donne sur un exemple concret :

Exemple 5.1.10. — Reprenons la permutation σ de $\{1, 2, \ldots, 10\}$ donnée par

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 2 & 4 & 7 & 9 & 8 & 5 & 6 & 1 \end{pmatrix}$$

Nous avons $\sigma(1) = 3$, $\sigma(3) = 2$, $\sigma(2) = 10$ et $\sigma(10) = 1$. Le cycle C_1 est donc égal à $(1\ 3\ 2\ 10)$. Son support est $\{1, 2, 3, 10\}$. Il y a des éléments de $\mathrm{Supp}(\sigma)$ qui n'appartiennent pas à $\mathrm{Supp}(C_1)$, par exemple 4. Nous avons $\sigma(4) = 4$. Le cycle C_2 est donc égal à (4), son support est $\{4\}$. La réunion des supports de C_1 et C_2 est $\{1, 2, 3, 4, 10\}$. Il y a des éléments de $\mathrm{Supp}(\sigma)$ qui n'appartiennent pas à $\{1, 2\,3, 4, 10\}$, par exemple 5. Nous avons $\sigma(5) = 7$, $\sigma(7) = 8$, $\sigma(8) = 5$. Le cycle C_3 est donc égal à $(5\ 7\ 8)$. Son support est $\{5, 7, 8\}$. La réunion des supports de C_1, C_2 et C_3 est $\{1, 2, 3, 4, 5, 7, 8, 10\}$. Il y a des éléments de $\mathrm{Supp}(\sigma)$ qui n'appartiennent pas à $\{1, 2, 3, 4, 5, 7, 8, 10\}$, par exemple 6. Nous avons $\sigma(6) = 9$ et $\sigma(9) = 6$. Le cycle C_4 est donc égal à $(6\ 9)$. Son support est $\{6, 9\}$. La réunion des supports de C_1, C_2, C_3 et C_4 est $\mathrm{Supp}(\sigma) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. D'où la décomposition

$$\sigma = (1\ 3\ 2\ 10)(4)(5\ 7\ 8)(6\ 9)$$

Remarque 5.1.4. — Nous avons précédemment donné la liste des éléments de $\mathfrak{S}_4$. Le « type »d'une décomposition est le nombre de cycles de chaque longueur qu'elle met en jeu. La liste des éléments de $\mathfrak{S}_4$ en considérant les différents types possibles de décomposition en produit de cycles à supports deux à deux disjoints est :

- ◇ aucun cycle : id ;
- ◇ une transposition : $(1\ 2)$, $(1\ 3)$, $(1\ 4)$, $(2\ 3)$, $(2\ 4)$, $(3\ 4)$;
- ◇ un 3-cycle : $(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$, $(1\ 4\ 3)$, $(1\ 3\ 4)$, $(2\ 3\ 4)$, $(2\ 4\ 3)$;
- ◇ un 4-cycle : $(1\ 2\ 3\ 4)$, $(1\ 2\ 4\ 3)$, $(1\ 3\ 2\ 4)$, $(1\ 3\ 4\ 2)$, $(1\ 4\ 2\ 3)$, $(1\ 4\ 3\ 2)$;
- ◇ deux transpositions : $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$.

Lemme 5.1.2

Un cycle de longueur ℓ peut s'écrire comme le produit de $\ell - 1$ transpositions.

Démonstration. — Soit E un ensemble et soient a_1, a_2, …, a_ℓ des éléments deux à deux distincts de E.

Nous avons

$$(a_1\ a_2\ \ldots\ a_\ell) = (a_1\ a_2)(a_2\ a_3)\ldots(a_{\ell-1}\ a_\ell). \tag{5.1.1}$$

□

Si E est fini, toute permutation de E peut s'écrire comme un produit de cycles à supports deux à deux disjoints (Théorème 5.1.1). Puisque tout cycle sur E est produit de transpositions (5.1.1) nous pouvons énoncer le :

Théorème 5.1.2

Toute permutation de E est un produit de transpositions.

Soit $n \geq 0$ un entier et soit σ un élément de $\mathfrak{S}_n$. Désignons par $\mathcal{P}$ l'ensemble des parties de $\{1, 2, \ldots, n\}$ de cardinal 2. Si $A = \{i, j\}$ est un élément de $\mathcal{P}$, son image $\sigma(A) = \{\sigma(i), \sigma(j)\}$ est encore un élément de $\mathcal{P}$. En effet comme σ est injective, $\sigma(i) \neq \sigma(j)$ donc $\sigma(A)$ est de cardinal 2. Si $A = \{u, v\}$ appartient à $\mathcal{P}$, alors $\sigma(\{\sigma^{-1}(u), \sigma^{-1}(v)\}) = A$. Ainsi $\mathcal{P} \to \mathcal{P}$, $A \mapsto \sigma(A)$ est une bijection de $\mathcal{P}$ dans lui-même.

Définition 5.1.1

Soit $n \geq 0$ un entier et soit σ un élément de $\mathfrak{S}_n$. Soit $\mathcal{P}$ l'ensemble des parties de $\{1, 2, \ldots, n\}$ de cardinal 2.
Un élément $A = \{i, j\}$ de $\mathcal{P}$ est une *inversion* de σ si $j - i$ et $\sigma(j) - \sigma(i)$ sont de signes opposés.
Notons $\mathrm{I}(\sigma)$ le nombre d'inversions de σ.

Exemple 5.1.11. — Soit σ la permutation de $\mathfrak{S}_4$ définie par

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Les inversions de σ sont

$$\{1, 4\} \qquad \{2, 4\} \qquad \{3, 4\};$$

en particulier $\mathrm{I}(\sigma) = 3$.

Théorème 5.1.3

Soit n un entier. Soient σ et τ deux permutations de $\{1, 2 \ldots, n\}$.
L'entier $\mathrm{I}(\sigma) + \mathrm{I}(\tau) - \mathrm{I}(\sigma\tau)$ est pair.

Démonstration. — Soit $\mathcal{P}$ l'ensemble des parties de $\{1, 2, \ldots, n\}$ de cardinal 2. Soit E^+ le sous-ensemble de $\mathcal{P}$ constitué des parties A telles que τ ne renverse pas l'ordre des éléments de A. Soit E^- le sous-ensemble de $\mathcal{P}$ constitué des parties A telles que τ renverse l'ordre des éléments de A ; autrement dit E^- est l'ensemble des inversions de τ. Soit F^+ le sous-ensemble de $\mathcal{P}$ constitué des parties A telles que σ ne renverse pas l'ordre des éléments de A. Soit F^- le sous-ensemble de $\mathcal{P}$ telles que σ renverse l'ordre des éléments de A ; autrement dit E^- est l'ensemble des inversions de σ.

Considérons un élément A de $\mathcal{P}$. La permutation $\sigma\tau$ renverse l'ordre des éléments de A si et seulement si nous sommes dans l'une des situations suivantes :

- ◇ τ ne renverse pas l'ordre des éléments de A et σ renverse l'ordre des éléments de $\tau(A)$, *i.e.* $A \in E^+$ et $\tau(A) \in F^-$.
- ◇ τ renverse l'ordre des éléments de A et σ ne renverse pas l'ordre des éléments de $\tau(A)$, *i.e.* $A \in E^+$ et $\tau(A) \in F^-$.

Soit G^- le sous-ensemble de $\mathcal{P}$ constitué des parties A dont l'image par τ appartient à F^-. Puisque $A \mapsto \sigma(A)$ définit une bijection de $\mathcal{P}$ dans lui-même le cardinal de G^- coïncide avec celui de F^-, *i.e.* coïncide avec $\mathrm{I}(\sigma)$. La permutation $\sigma\tau$ renverse l'ordre des éléments de A si et seulement si A appartient à E^- et pas à G^- ou A appartient à G^- et pas à E^-. Ainsi

$$\begin{aligned}\mathrm{I}(\sigma\tau) &= \mathrm{Card}(E^-) - \mathrm{Card}(E^- \cap G^-) + \mathrm{Card}(G^-) - \mathrm{Card}(E^- \cap G^-)\\ &= \mathrm{Card}(E^-) + \mathrm{Card}(G^-) - 2 \times \mathrm{Card}(E^- \cap G^-)\\ &= \mathrm{I}(\tau) + \mathrm{I}(\sigma) - 2 \times \mathrm{Card}(E^- \cap G^-)\end{aligned}$$

Ainsi

$$\mathrm{I}(\sigma) + \mathrm{I}(\tau) - \mathrm{I}(\sigma\tau) = 2 \times \mathrm{Card}(E^- \cap G^-)$$

est bien pair. □

Définitions 5.1.1

Soit n un entier. Soit $\sigma \in \mathfrak{S}_n$. La *signature*, notée $\mathrm{sgn}(\sigma)$, est $(-1)^{\mathrm{I}(\sigma)} \in \{-1, 1\}$.
La permutation σ est *paire* si $\mathrm{sgn}(\sigma) = 1$.
La permutation σ est *impaire* si $\mathrm{sgn}(\sigma) = -1$.

Exemple 5.1.12. — La permutation identité est paire.

Exemple 5.1.13. — Soit σ la permutation de $\mathfrak{S}_4$ définie par

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Nous avons vu que $\mathrm{I}(\sigma) = 3$; en particulier σ est impaire.

Soit n un entier et soient σ, τ deux éléments de $\mathfrak{S}_n$. Par définition $\mathrm{sgn}(\sigma\tau) = (-1)^{\mathrm{I}(\sigma\tau)}$. Le théorème 5.1.3 assure que $(-1)^{\mathrm{I}(\sigma\tau)} = (-1)^{\mathrm{I}(\sigma)+\mathrm{I}(\tau)}$. Or $(-1)^{\mathrm{I}(\sigma)+\mathrm{I}(\tau)} = (-1)^{\mathrm{I}(\sigma)}(-1)^{\mathrm{I}(\tau)}$ et $(-1)^{\mathrm{I}(\sigma)}(-1)^{\mathrm{I}(\tau)} = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$ donc

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau).$$

Pour tout σ dans $\mathfrak{S}_n$ nous avons donc

$$1 = \mathrm{sgn}(\mathrm{id}) = \mathrm{sgn}(\sigma\sigma^{-1}) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\sigma^{-1})$$

d'où $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma^{-1})^{-1} = \mathrm{sgn}(\sigma^{-1})$ (un élément de $\{-1, 1\}$ est égal à sont propre inverse pour la multiplication).

Exemple 5.1.14. — Soit n un entier. Soit $\tau = (a\ b)$ une transposition de $\mathfrak{S}_n$. Notons que $(a\ b) = (b\ a)$, nous pouvons donc toujours supposer que $a < b$.

Soient $i < j$ deux entiers. La description de τ assure que $\tau(i) > \tau(j)$ si et seulement si nous sommes dans l'un des deux cas suivants :

- ◇ $i = a$ et $a < j \leq b$;
- ◇ $a \leq i < b$ et $j = b$.

On compte $b - a$ couples (i, j) qui satisfont la première condition et $b - a$ couples (i, j) qui satisfont la seconde. Par ailleurs il y a exactement un couple qui satisfait les deux, le couple (a, b). Ainsi

$$\mathrm{I}(\tau) = b - a + b - a - 1 = 2(b - a) - 1;$$

en particulier $\mathrm{I}(\tau)$ est impair. Nous en déduisons que $\mathrm{sgn}(\tau) = -1$; autrement dit une transposition est impaire.

Exemple 5.1.15. — Soit n un entier. Soit $2 \leq \ell \leq n$ et soit c un ℓ-cycle de $\mathfrak{S}_n$. Nous avons vu que c est le produit de $\ell - 1$ transpositions. La signature d'une transposition étant -1 nous obtenons que $\mathrm{sgn}(c) = (-1)^{\ell-1}$. Autrement dit la parité d'un cycle est opposée à celle de sa longueur.

Exemple 5.1.16. — Soit n un entier. Soit σ une permutation de $\{1, 2 \ldots, n\}$. Pour calculer $\mathrm{sgn}(\sigma)$ nous pouvons calculer la décomposition de σ en produit de cycles à supports deux à deux disjoints puis d'appliquer la multiplicativité de sgn et l'Exemple 5.1.15.

Exemple 5.1.17. — Soit n un entier. Soit σ un élément de $\mathfrak{S}_n$. Nous avons vu que σ peut s'écrire comme un produit de transpositions $\tau_1\tau_2 \ldots \tau_r$.

Cette écriture et l'entier r ne sont pas uniques ; en effet

$$(1\ 2\ 3) = (3\ 1)(1\ 2) = (1\ 2)(2\ 3) = (3\ 2)(2\ 1)(3\ 2)(2\ 1)$$

Par contre la parité de r est bien déterminée. La signature d'une transposition étant égale à -1 nous avons $\mathrm{sg}(\sigma) = (-1)^r$. Autrement dit ou bien r et σ sont pairs, ou bien r et σ sont impairs.

5.1.4. Classes de conjugaison dans $\mathfrak{S}_n$ et $\mathcal{A}_n$. — Les tableaux suivants répertorient un représentant de chaque classe de conjugaison dans $\mathfrak{S}_n$ et $\mathcal{A}_n$ pour $3 \leq n \leq 6$, ainsi que le cardinal des classes de conjugaison. Les différentes classes de conjugaison ne s'intersectent pas (Théorème 3.1.2) ; par suite la somme des cardinaux des classes de conjugaison dans $\mathfrak{S}_n$ (resp. $\mathcal{A}_n$) vaut $n!$ (resp. $\frac{n!}{2}$).

$\mathfrak{S}_3$			
représentant	(id)	(1 2 3)	(1 2)
cardinal	1	2	3

$\mathfrak{S}_4$					
représentant	(id)	(1 2)(3 4)	(1 2)	(1 2 3 4)	(1 2 3)
cardinal	1	3	6	6	8

$\mathfrak{S}_5$							
représentant	(id)	(1 2)	(1 2)(3 4)	(1 2 3)	(1 2)(3 4 5)	(1 2 3 4 5)	(1 2 3 4)
cardinal	1	10	15	20	20	24	30

$\mathfrak{S}_6$						
représentant	(id)	(1 2)	(1 2)(3 4)(5 6)	(1 2 3)	(1 2 3)(4 5 6)	(1 2)(3 4)
cardinal	1	15	15	40	40	45
représentant	(1 2 3 4)	(1 2)(3 4 5 6)	(1 2 3 4 5 6)	(1 2)(3 4 5)	(1 2 3 4 5)	
cardinal	90	90	120	120	144	

$\mathcal{A}_3$			
représentant	(id)	(1 2 3)	(1 3 2)
cardinal	1	1	1

$\mathcal{A}_4$				
représentant	(id)	(1 2)(3 4)	(1 2 3)	(1 3 2)
cardinal	1	3	4	4

$\mathcal{A}_5$					
représentant	(id)	(1 2 3 4 5)	(2 1 3 4 5)	(1 2)(3 4)	(1 2 3)
cardinal	1	12	12	15	20

$\mathcal{A}_6$							
représentant	(id)	(1 2 3)	(1 2 3)(4 5 6)	(1 2)(3 4)	(1 2 3 4 5)	(2 3 4 5 6)	(1 2 3 4)(5 6)
cardinal	1	40	40	45	72	72	90

Considérons la permutation de $\mathfrak{S}_5$ donnée par $\sigma = (1\ 3)(2\ 4\ 5)$. Alors

$$\sigma(1\ 4\ 3\ 2)\sigma = (1\ 5\ 3\ 2) \qquad \text{et} \qquad (\sigma(1)\ \sigma(4)\ \sigma(3)\ \sigma(2)) = (3\ 2\ 1\ 5)$$

d'où $\sigma(1\ 4\ 3\ 2)\sigma = (\sigma(1)\ \sigma(4)\ \sigma(3)\ \sigma(2))$.

Considérons la permutation de $\mathfrak{S}_7$ donnée par $\sigma = (1\ 3)(2\ 6\ 5)$. Alors

$$\sigma(7\ 3\ 5\ 2\ 1)\sigma = (1\ 2\ 6\ 3\ 7) \qquad \text{et} \qquad (\sigma(7)\ \sigma(3)\ \sigma(5)\ \sigma(2)\ \sigma(1)) = (1\ 2\ 6\ 3\ 7)$$

d'où $\sigma(7\ 3\ 5\ 2\ 1)\sigma = (\sigma(7)\ \sigma(3)\ \sigma(5)\ \sigma(2)\ \sigma(1))$.

Plus généralement, nous avons la :

Proposition 5.1.1

Si $\sigma = (a_1\ a_2\ \dots\ a_k) \in \mathfrak{S}_n$ est un k-cycle et τ un élément de $\mathfrak{S}_n$, nous avons

$$\tau\sigma\tau^{-1} = \big(\tau(a_1)\ \tau(a_2)\ \dots\ \tau(a_k)\big). \tag{5.1.2}$$

Démonstration. — Si x n'appartient pas à $\{\tau(a_1), \tau(a_2), \dots, \tau(a_k)\}$, alors $\tau^{-1}(x)$ n'appartient pas à $\{a_1, a_2, \dots, a_k\}$ donc $\tau\sigma\tau^{-1}(x) = x$. Si en revanche $x = \tau(a_i)$, alors $\tau\sigma\tau^{-1}(x) = \tau\sigma(a_i) = \tau(a_{i+1})$. D'où l'égalité (5.1.2). □

Nous savons maintenant que tout conjugué d'un cycle est un cycle de même longueur. La réciproque est-elle vraie ? L'énoncé qui suit répond positivement à cette question.

Théorème 5.1.4

Tous les k-cycles sont conjugués dans $\mathfrak{S}_n$; autrement dit, tous les cycles de $\mathfrak{S}_n$ de même ordre sont conjugués.

Démonstration. — Considérons les deux k-cycles suivants

$$(a_1\ a_2\ \dots\ a_k) \qquad\qquad (b_1\ b_2\ \dots b_k).$$

Soit $\sigma \in \mathfrak{S}_n$ tel que

- ◇ $\sigma(a_1) = b_1$, $\sigma(a_2) = b_2$, …, $\sigma(a_k) = b_k$;
- ◇ et σ réalise une bijection arbitraire entre le complément de $\{a_1, a_2, \dots, a_k\}$ et le complément de $\{b_1, b_2, \dots, b_k\}$. La Proposition 5.1.1 assure que la conjugaison par σ envoie le premier k-cycle sur le second.

□

Par exemple, les transpositions dans $\mathfrak{S}_n$ forment une seule classe de conjugaison.

Considérons maintenant la classe de conjugaison d'une permutation quelconque de $\mathfrak{S}_n$, pas nécessairement un cycle. En écrivant une permutation comme un produit de cycles disjoints, organisons les cycles par longueur croissante, y compris les cycles de longueur 1 s'il y a des points fixes. Ces longueurs sont appelées *le type* de la permutation. Par exemple, dans $\mathfrak{S}_7$, le type de la permutation $(1\ 2)(3\ 4)(5\ 6\ 7)$ est $(2, 2, 3)$; dans $\mathfrak{S}_5$ le type de $(1\ 2)(3\ 5)$ dans $\mathfrak{S}_5$ est $(1, 2, 2)$ car $(1\ 2)(3\ 5) = (4)(1\ 2)(3\ 5)$.

Le type d'une permutation dans $\mathfrak{S}_n$ est un ensemble d'entiers positifs dont la somme vaut n, appelé partition de n. Il y a sept partitions de 5 :

$$5, \quad 1+4, \quad 2+3, \quad 1+1+3, \quad 1+2+2, \quad 1+1+1+2, \quad 1+1+1+1+1.$$

Ainsi, il y a sept types de permutations dans $\mathfrak{S}_5$. Connaître le type d'une permutation nous donne des renseignements sur sa structure en produit de cycles à supports disjoints, mais sans dire la façon dont les nombres sont répartis dans les cycles. Par exemple, les permutations $(1)(23)(45)$, $(2)(35)(14)$ de $\mathfrak{S}_5$ ont le même type : $(1, 2, 2)$. On peut se demander quand deux permutations ont le même type : deux permutations de $\mathfrak{S}_n$ sont conjuguées si et seulement si elles ont le même type. Regardons ce qu'il se passe sur un exemple.

Exemple 5.1.18. — Considérons les deux permutations de $\mathfrak{S}_5$ de type $(2, 3)$:

$$\pi_1 = (2\ 4)(1\ 5\ 3), \qquad \pi_2 = (1\ 3)(4\ 2\ 5).$$

Soit $\sigma \in \mathfrak{S}_5$ la permutation qui envoie les termes apparaissant dans π_1 sur les termes apparaissant dans π_2 (exactement dans le même ordre) :

$$\sigma = \begin{pmatrix} 4 & 2 & 5 & 3 & 1 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} = (1\ 2\ 3\ 4).$$

Alors

$$\sigma\pi_1\sigma^{-1} = \sigma(2\ 4)(1\ 5\ 3)\sigma^{-1} = \underbrace{\sigma(2\ 4)\sigma^{-1}}_{\left(\sigma(2)\ \sigma(4)\right)}\ \underbrace{\sigma(1\ 5\ 3)\sigma^{-1}}_{\left(\sigma(1)\ \sigma(5)\ \sigma(3)\right)} = (1\ 3)(4\ 2\ 5),$$

autrement dit $\sigma\pi_1\sigma^{-1} = \pi_2$.

Lemme 5.1.3

Si π_1 et π_2 sont deux permutations de $\mathfrak{S}_n$ à supports disjoints, alors pour tout $\sigma \in \mathfrak{S}_n$ les permutations $\sigma\pi_1\sigma^{-1}$ et $\sigma\pi_2\sigma^{-1}$ sont à supports disjoints.

Démonstration. — Être à supports disjoints signifie qu'aucun nombre n'est déplacé à la fois par π_1 et π_2. Si $\sigma\pi_1\sigma^{-1}$ et $\sigma\pi_2\sigma^{-1}$ ne sont pas à supports disjoints, alors ils déplacent tous les deux un certain nombre, disons j. Alors $\sigma^{-1}(j)$ est déplacé à la fois par π_1 et π_2 : contradiction. □

Théorème 5.1.5

Deux permutations de $\mathfrak{S}_n$ sont conjuguéés si et seulement si elles ont le même type. Autrement dit, les classes de conjugaison de $\mathfrak{S}_n$ sont en bijection avec les partitions de n :

$$n = k_1 + k_2 + \ldots + k_r, \quad r \in \mathbb{N}, \quad 1 \leq k_1 \leq k_2 \leq \ldots \leq k_r.$$

Le nombre de classes de conjugaison est donc égal au nombre de « partages » $p(n)$ de l'entier n, et si la décomposition d'une permutation contient k_1 1-cycles (les points fixes), k_2 2-cycles, …, k_m m-cycles, alors le nombre de ses conjugués vaut :

$$\frac{n!}{1^{k_1}k_1!\,2^{k_2}k_2!\,\ldots\,m^{k_m}k_m!}.$$

Démonstration. — Soit π un élément de $\mathfrak{S}_n$. Écrivons sa décomposition en cycles à supports disjoints $c_1 c_2 \dots c_\ell$. D'après le Théorème 3.1.3 et le Lemme 5.1.3 la permutation $\sigma\pi\sigma^{-1}$ s'écrit $(\sigma c_1 \sigma^{-1})(\sigma c_2 \sigma^{-1}) \dots (\sigma c_\ell \sigma^{-1})$. Notons que les $\pi c_i \pi^{-1}$ sont d'une part à supports disjoints et d'autre part de même longueur que les c_i. Il en résulte que $\sigma\pi\sigma^{-1}$ et π ont le même type.

Réciproquement expliquons pourquoi deux permutations π_1 et π_2 ayant le même type sont conjuguées. Supposons que π_1 et π_2 soient de type $(m_1, m_2, \dots)$. Alors

$$\pi_1 = \underbrace{(a_1\ a_2\ \dots a_{m_1})}_{m_1 \text{ termes}} \underbrace{(a_{m_1+1}\ a_{m_1+2}\ \dots\ a_{m_1+m_2})}_{m_2 \text{ termes}} \dots$$

et

$$\pi_2 = \underbrace{(b_1\ b_2\ \dots b_{m_1})}_{m_1 \text{ termes}} \underbrace{(b_{m_1+1}\ b_{m_1+2}\ \dots\ b_{m_1+m_2})}_{m_2 \text{ termes}} \dots$$

où les cycles ici sont disjoints. Considérons la permutation $\sigma \in \mathfrak{S}_n$ définie par $\sigma(a_i) = b_i$ pour tout i. D'après les Théorèmes 3.1.3 et 5.1.4 nous avons $\sigma\pi_1\sigma^{-1} = \pi_2$ (c'est exactement la méthode utilisée pour trouver σ dans l'Exemple 5.1.18). Supposons que π_1 et π_2 soient de type $(m_1, m_2, \dots)$. Alors

$$\pi_1 = \underbrace{(a_1\ a_2\ \dots a_{m_1})}_{m_1 \text{ termes}} \underbrace{(a_{m_1+1}\ a_{m_1+2}\ \dots\ a_{m_1+m_2})}_{m_2 \text{ termes}} \dots$$

et

$$\pi_2 = \underbrace{(b_1\ b_2\ \dots b_{m_1})}_{m_1 \text{ termes}} \underbrace{(b_{m_1+1}\ b_{m_1+2}\ \dots\ b_{m_1+m_2})}_{m_2 \text{ termes}} \dots$$

où les cycles ici sont disjoints. Considérons la permutation $\sigma \in \mathfrak{S}_n$ définie par $\sigma(a_i) = b_i$ pour tout i. Les Théorèmes 3.1.3 et 5.1.4 assurent que $\sigma\pi_1\sigma^{-1} = \pi_2$ (c'est exactement la méthode utilisée pour trouver σ dans l'Exemple 5.1.18).

□

On peut vérifier que

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$p(n)$	1	2	3	5	7	11	15	22	30	42	56	77	101	135

Notons que la fonction $p(n)$ croît très rapidement ; par exemple $p(100) > 190000000$. On peut vérifier que les $p(n)$, $n \geq 6$, coïncident avec le nombre de classes de conjugaison donné au début du paragraphe.

Exemples 5.1.19. —

1. Les deux partitions de 2 sont $1+1$ et $0+2$. Les classes de conjugaison correspondantes dans $\mathfrak{S}_2$ sont $\{\mathrm{id}\}$ et $\{(1\ 2)\}$.
2. Les trois partitions de 3 sont $1+1+1$, $1+2$ et $3+0$. Les classes de conjugaison correspondantes dans $\mathfrak{S}_3$ sont $\{\mathrm{id}\}$, $\{(1\ 2), (1\ 3), (2\ 3)\}$ et $\{(1\ 2\ 3), (1\ 3\ 2)\}$.

3. Les cinq partitions de 4 sont $1+1+1+1$, $1+1+2$, $2+2$, $1+3$ et 4. Les classes de conjugaison correspondantes dans $\mathfrak{S}_4$ sont $\{\mathrm{id}\}$, les six transpositions, les trois doubles transpositions, les huit 3-cycles et les six 4-cycles.

En utilisant le Théorème 5.1.5, on peut démontrer une « réciproque » du Théorème 3.1.1 : les éléments de même ordre d'un groupe ne sont a priori pas conjugués, néanmoins ils le deviennent si on travaille dans un groupe plus grand :

Corollaire 5.1.1

Soit G un groupe fini. Il peut être plongé dans un groupe d'ordre plus grand dans lequel les éléments de même ordre de G sont conjugués.

Démonstration. — Le Théorème de Cayley (Théorème 6.1.1) assure qu'on peut plonger G dans un $\mathfrak{S}_n$ pour un certain entier n en associant à chaque g la permutation $\ell_g\colon \mathrm{G} \to \mathrm{G}$, $x \mapsto gx$. En désignant par $g_1, g_2, \ldots, g_n$ les éléments de G nous obtenons que chaque permutation de G « ressemble » à une permutation de $\{1, \ldots, n\}$; ainsi l'application qui à g associe ℓ_g est un morphisme de groupes injectif de G dans $\mathfrak{S}_n$ où $n = |\mathrm{G}|$.

Soit $g \in \mathrm{G}$ un élément d'ordre m ; alors m divise n. La multiplication à gauche par g sur G, vue comme permutation de G, est un produit de m-cycles disjoints $(x\ gx\ g^2x\ \ldots\ g^{m-1}x)$. La décomposition de ℓ_g en cycles compte $\frac{|\mathrm{G}|}{m}$ m-cycles disjoints. Ainsi le type de la permutation ℓ_g dans $\mathfrak{S}_n$ dépend uniquement de l'ordre m de g. Soit g' un élément de G d'ordre m distinct de g ; $\ell_{g'}$ vue comme permutation de G et ℓ_g ont le même type. Le Théorème 5.1.5 assure que ℓ_g et $\ell_{g'}$ sont conjuguées. □

Exemple 5.1.20. — Considérons le groupe $\mathrm{G} = \mathbb{Z}/10\mathbb{Z}$. Les éléments $\overline{2}$ et $\overline{4}$ sont d'ordre 5 et ne sont pas conjugués dans G puisque G est abélien. D'après le Théorème de Cayley (Théorème 6.1.1) on peut voir G comme un sous-groupe de $\mathfrak{S}_{10}$ et

$$\ell_2 = (0\ 2\ 4\ 6\ 8)(1\ 3\ 5\ 7\ 9), \qquad \ell_4 = (0\ 4\ 8\ 2\ 6)(1\ 5\ 9\ 3\ 7).$$

Les permutations ℓ_2 et ℓ_4 sont conjuguées dans $\mathfrak{S}_{10}$: si

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 1 & 4 & 5 & 8 & 9 & 2 & 3 & 6 & 7 \end{pmatrix} = (2\ 4\ 8\ 6)(3\ 5\ 9\ 7),$$

alors $\ell_4 = \sigma\ell_2\sigma^{-1}$.

Le Corollaire 5.1.1 reste vrai pour des groupes infinis quitte à considérer des groupes de permutations infinis dans la démonstration.

Nous nous intéressons désormais aux classes de conjugaison dans $\mathcal{A}_n$. Si π est une permutation paire, alors $\sigma\pi\sigma^{-1}$ est également paire. Par suite une classe de conjugaison dans $\mathfrak{S}_n$ qui contient une permutation paire ne contient que des permutations paires. Cependant, deux

permutations π_1 et π_2 dans $\mathcal{A}_n$ peuvent avoir le même type et donc être conjuguées dans $\mathfrak{S}_n$ tout en n'étant pas conjuguées dans $\mathcal{A}_n$.

Exemple 5.1.21. — Les 3-cycles (1 2 3) et (1 3 2) sont conjugués dans $\mathfrak{S}_3$:

$$(2\ 3)(1\ 2\ 3)(2\ 3)^{-1} = (1\ 3\ 2).$$

Cependant (1 2 3) et (1 3 2) ne sont pas conjugués dans $\mathcal{A}_3$ car $\mathcal{A}_3$ est abélien.

Exemple 5.1.22. — Les 3-cycles (1 2 3) et (1 3 2) sont conjugués dans $\mathfrak{S}_4$ (via (2 3)) mais ils ne le sont pas dans $\mathcal{A}_4$. En effet, déterminons les $\sigma \in \mathfrak{S}_4$ qui conjuguent (1 2 3) à (1 3 2). Pour $\sigma \in \mathfrak{S}_4$, la condition $\sigma(1\ 2\ 3)\sigma^{-1} = (1\ 3\ 2)$ est la même que $(\sigma(1)\ \sigma(2)\ \sigma(3)) = (1\ 3\ 2)$. Il y a trois possibilités :

- ◇ si $\sigma(1) = 1$, alors $\sigma(2) = 3$ et $\sigma(3) = 2$, (nécessairement $\sigma(4) = 4$). Ainsi $\sigma = (2\ 3)$.
- ◇ si $\sigma(1) = 3$, alors $\sigma(2) = 2$ et $\sigma(3) = 1$, (nécessairement $\sigma(4) = 4$). Par conséquent $\sigma = (1\ 3)$.
- ◇ si $\sigma(1) = 2$, alors $\sigma(2) = 1$ et $\sigma(3) = 3$, (nécessairement $\sigma(4) = 4$). Par suite $\sigma = (1\ 2)$.

Les seuls σ possibles sont donc les transpositions ; elles n'appartiennent pas à $\mathcal{A}_4$.

Soit σ une permutation paire de $\mathfrak{S}_n$. Sa classe de conjugaison dans $\mathfrak{S}_n$ ne coïncide pas nécessairement avec sa classe de conjugaison dans $\mathcal{A}_n$. Par exemple, en observant les tables du début du §5.1.4 nous constatons que :

- ◇ il existe une classe de huit 3-cycles dans $\mathfrak{S}_4$, mais deux classes de quatre 3-cycles dans $\mathcal{A}_4$,
- ◇ il existe une classe de vingt-quatre 5-cycles dans $\mathfrak{S}_5$, mais deux classes de douze 5-cycles dans $\mathcal{A}_5$,
- ◇ il existe une classe de cent quarante quatre 5-cycles dans $\mathfrak{S}_6$, mais deux classes de soixante douze 5-cycles dans $\mathcal{A}_6$.

Détaillons le cas de $\mathcal{A}_5$:

***Exemple 5.1.23* (Classes de conjugaison de $\mathcal{A}_5$).** — Le groupe $\mathcal{A}_5$ a cinq classes de conjugaison :

- ◇ la classe C_1 de l'élément neutre, de cardinal 1 ;
- ◇ la classe C_3 des 3-cycles (d'ordre 3), de cardinal 20 ;
- ◇ la classe $C_{2,2}$ des produits de deux transpositions de supports disjoints (d'ordre 2), de cardinal 15 ;
- ◇ deux classes C_5 et C_5' de cardinal 12 dont la réunion est l'ensemble des 5-cycles (d'ordre 5). De plus, si σ est un 5-cycle, alors σ et σ^2 ne sont pas dans la même classe. Désignons par exemple par C_5 la classe de $\sigma_0 = (1\ 2\ 3\ 4\ 5)$ et par C_5' la classe de $\sigma_0^2 = (1\ 3\ 5\ 2\ 4)$.

En effet les classes de conjugaison de $\mathcal{A}_5$ peuvent se déduire de celles de $\mathfrak{S}_5$. Rappelons que si G est un groupe, si g est un élément de G et si Z_g est le centralisateur de g (c'est-à-dire l'ensemble des éléments de G qui commutent à g), alors la classe de conjugaison de g est isomorphe à ${}^{\mathrm{G}}\!/_{Z_g}$ via $h \mapsto hgh^{-1}$; en particulier elle est de cardinal $\frac{|\mathrm{G}|}{|Z_g|}$. Ainsi comprendre ce que devient une classe de conjugaison de $\mathfrak{S}_5$ dans $\mathcal{A}_5$ revient à comprendre le lien du centralisateur Z_g de g dans $\mathfrak{S}_5$ avec son centralisateur $Z_g \cap \mathcal{A}_5$ dans $\mathcal{A}_5$.

Rappelons que $\mathcal{A}_5$ est le noyau du morphisme

$$\mathrm{sgn}\colon \mathfrak{S}_5 \to \{1, -1\}.$$

Par suite si H est un sous-groupe de $\mathfrak{S}_5$, alors ou bien H est contenu dans $\mathcal{A}_5$, ou bien $\mathrm{sgn}_{|\mathrm{H}}\colon \mathrm{H} \to \{1, -1\}$ est surjective et donc $\mathrm{H} \cap \mathcal{A}_5$ qui en est le noyau est de cardinal $\frac{|\mathrm{H}|}{2}$.

Soit C une classe de conjugaison de $\mathfrak{S}_5$. Si $C \cap \mathcal{A}_5 \neq \emptyset$, alors le caractère χ_{sgn} de $\mathfrak{S}_5$ prend la valeur 1 sur un élément de C donc sur C tout entier ; autrement dit $C \subset \mathcal{A}_5$. Si g appartient à C, la classe de conjugaison C_g de g dans $\mathcal{A}_5$ est incluse dans C et si Z_g est son centralisateur dans $\mathfrak{S}_5$, alors nous avons l'alternative suivante

- ou bien $Z_g \subset \mathcal{A}_5$ et alors

$$|C_g| = \frac{|\mathcal{A}_5|}{|Z_g|} = \frac{1}{2}\frac{|\mathfrak{S}_5|}{|Z_g|} = \frac{1}{2}|C|$$

  et C se scinde en deux classes de conjugaison dans $\mathcal{A}_5$;

- Z_g contient un élément de signature -1 et alors $|Z_g \cap \mathcal{A}_5| = \frac{1}{2}|Z_g|$ donc

$$|C_g| = \frac{|\mathcal{A}_5|}{|Z_g \cap \mathcal{A}_5|} = \frac{\frac{|\mathfrak{S}_5|}{2}}{\frac{|Z_g|}{2}} = \frac{|\mathfrak{S}_5|}{|Z_g|} = |C|$$

  et $C = C_g$; en particulier C reste une classe de conjugaison dans $\mathcal{A}_5$.

Puisque (4 5) commute à (1 2 3) la classe des 3-cycles reste une classe de conjugaison de $\mathcal{A}_5$.

De même la transposition (1 2) commute à la double transposition (1 2)(3 4) donc $C_{2,2}$ est une classe de conjugaison de $\mathcal{A}_5$.

Intéressons-nous maintenant aux 5-cycles. Ils sont au nombre de 24 ; comme 24 ne divise pas $|\mathcal{A}_5| = 60$ la classe des 5-cycles se scinde nécessairement en deux dans $\mathcal{A}_5$. Considérons le 4-cycle $\sigma = (2\ 3\ 5\ 4) \in \mathfrak{S}_5 \smallsetminus \mathcal{A}_5$. À partir de

$$\sigma_0^2 = \sigma\sigma_0\sigma^{-1}$$

nous obtenons que σ_0 et σ_0^2 ne sont pas dans la même classe de conjugaison de $\mathcal{A}_5$. Puisque les 5-cycles sont toujours conjugués dans $\mathfrak{S}_5$ pour tout 5-cycle σ, les 5-cycles σ et σ^2 ne sont pas dans la même classe.

Plus généralement,

Théorème 5.1.6

Soit $\sigma \in \mathcal{A}_n$ une permutation paire. Soit C_σ la classe de conjugaison dans $\mathfrak{S}_n$. Ou bien C_σ est la classe de conjugaison de σ dans $\mathcal{A}_n$, ou bien C_σ se scinde en deux classes de conjugaison dans $\mathcal{A}_n$ de même cardinal.
La classe de conjugaison C_σ se scinde si et seulement si les longueurs du type de σ sont des nombres impairs distincts.

Voici un tableau précisant les types de permutations de $\mathcal{A}_n$ qui se répartissent en deux classes de conjugaison pour $4 \leq n \leq 14$. Par exemple, les permutations dans $\mathcal{A}_6$ de type $(1,5)$ se scindent en deux classes de conjugaison, par contre celles de type $(3,3)$ non ; les permutations dans $\mathcal{A}_8$ de type $(1,7)$ et $(3,5)$ se scindent en deux classes de conjugaison.

n	4	5	6	7	8	9	10	11	12	13	14
type dans $\mathcal{A}_n$	$(1,3)$	(5)	$(1,5)$	(7)	$(1,7)$ $(3,5)$	(9) $(1,3,5)$	$(1,9)$ $(3,7)$	(11) $(1,3,7)$	$(1,11)$ $(3,9)$ $(5,7)$	(13) $(1,3,9)$ $(1,5,7)$	$(1,13)$ $(3,11)$ $(5,9)$

Le tableau suivant répertorie le nombre $\gamma(n)$ de classes de conjugaison dans $\mathcal{A}_n$ pour $n \leq 14$:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\gamma(n)$	1	1	3	4	5	7	9	14	18	24	31	43	55	72

Proposition 5.1.2

Si $n \geq 5$, alors les cycles d'ordre 3 sont conjugués dans $\mathcal{A}_n$.

Démonstration. — Soient $\sigma = (a_1\ a_2\ a_3)$ et $\tau = (b_1\ b_2\ b_3)$; soit $g \in \mathcal{A}_n$, $n \geq 5$, tel que $g(a_i) = b_i$ pour tout $1 \leq i \leq 3$ (un tel g existe puisque $\mathcal{A}_n$ est $n-2$ fois transitif sur $\{1, 2, \ldots, n\}$) ; alors $\tau = g\sigma g^{-1}$. □

Remarque 5.1.5. — Si $n = 3$ ou $n = 4$, la Proposition 5.1.2 est fausse. En effet, pour $n = 3$ le groupe $\mathcal{A}_3$ est abélien donc la conjugaison y est triviale ; pour $n = 4$ il y a huit cycles d'ordre 3 qui ne peuvent être conjugués dans $\mathcal{A}_4$ sinon ils formeraient une orbite dont le cardinal devrait diviser $|\mathcal{A}_4| = 12$ en vertu de la Proposition 6.3.1.

5.1.5. Une autre définition de la signature. — Donnons une seconde définition de la *signature*.

Soit n un entier. Pour tout $\sigma \in \mathfrak{S}_n$ il existe un unique morphisme d'anneaux de $\mathbb{Z}[X_1, X_2, \ldots, X_n]$ dans lui-même qui envoie X_i sur $X_{\sigma(i)}$ pour tout i ; nous le notons

$P \mapsto \sigma \cdot P$. On peut immédiatement vérifier que

$$\mathrm{id} \cdot P = P \qquad \forall\, P \qquad\qquad \sigma \cdot (\tau \cdot P) = (\sigma\tau) \cdot P \qquad \forall\, (\sigma,\, \tau,\, P).$$

Nous avons ainsi défini une opération de $\mathfrak{S}_n$ sur $\mathbb{Z}[X_1,\, X_2,\, \ldots,\, X_n]$ par automorphismes d'anneaux.

Soit Δ l'élément $\prod_{i<j}(X_i - X_j)$ de $\mathbb{Z}[X_1,\, X_2,\, \ldots,\, X_n]$. Nous avons

$$\Delta^2 = \prod_{i<j}(X_j - X_i)^2 = \prod_{i<j}(-1)(X_j - X_i)(X_i - X_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(X_i - X_j).$$

Cette dernière écriture montre que Δ^2 est invariant par permutation des indéterminées, *i.e.* $\sigma \cdot (\Delta^2) = \Delta^2$ pour tout $\sigma \in \mathfrak{S}_n$.

Si σ un élément de $\mathfrak{S}_n$, alors

$$\Delta^2 = \sigma \cdot (\Delta)^2 = (\sigma \cdot \Delta)^2.$$

Puisque $\mathbb{Z}[X_1,\, X_2,\, \ldots,\, X_n]$ est intègre, il existe $\mathrm{sgn}(\sigma) \in \{-1,\, 1\}$ tel que $\sigma \cdot \Delta = \mathrm{sgn}(\sigma)\Delta$.

Soient σ et τ deux éléments de $\mathfrak{S}_n$; nous avons

$$\begin{aligned}
\mathrm{sgn}(\sigma\tau)\Delta &= (\sigma\tau) \cdot \Delta \\
&= \sigma \cdot (\tau \cdot \Delta) \\
&= \sigma \cdot (\mathrm{sgn}(\tau)\Delta) \\
&= \mathrm{sgn}(\tau)\sigma \cdot \Delta \\
&= \mathrm{sgn}(\tau)\mathrm{sgn}(\sigma)\Delta
\end{aligned}$$

Mais $\mathbb{Z}[X_1,\, X_2,\, \ldots,\, X_n]$ est intègre et $\{-1,\, 1\}$ est abélien donc $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$. Par conséquent sgn est un morphisme de groupes de $\mathfrak{S}_n$ dans $\{-1,\, 1\}$, appelé *signature*.

Proposition-Définition 5.1.1

Soit E un ensemble fini de cardinal n. Soit Φ une bijection de E sur $\{1,\, 2,\, \ldots,\, n\}$. Le morphisme de groupes

$$\mathfrak{S}_E \to \{-1,\, 1\} \qquad\qquad \sigma \mapsto \mathrm{sgn}(\Phi \circ \sigma \circ \Phi^{-1})$$

ne dépend pas de Φ. On le note encore sgn et on l'appelle encore la signature.

Démonstration. — Soit Ψ une (autre) bijection de E sur $\{1,\, 2,\, \ldots,\, n\}$. Soit σ un élément de $\mathfrak{S}_E$. Nous avons

$$\Psi \circ \sigma \circ \Psi^{-1} = (\Psi \circ \Phi^{-1}) \circ (\Phi \circ \sigma \circ \Phi^{-1}) \circ (\Phi \circ \Psi^{-1}) = (\Psi \circ \Phi^{-1}) \circ (\Phi \circ \sigma \circ \Phi^{-1}) \circ (\Psi \circ \Phi^{-1})^{-1}.$$

Or $\Psi \circ \Phi^{-1}$ est une bijection de $\{1, 2, \ldots, n\}$ sur lui-même donc les permutations $\Phi \circ \sigma \circ \Phi^{-1}$ et $\Psi \circ \sigma \circ \Psi^{-1}$ sont conjuguées dans $\mathfrak{S}_n$. Par suite leurs images par le morphisme sgn sont conjuguées dans $\{-1, 1\}$ et sont finalement égales puisque $\{-1, 1\}$ est abélien [1]. $\square$

***Exemple 5.1.24* (Signature d'une transposition).** — Soit E un ensemble fini et soit $\tau = (a\ b)$ une transposition de E.

Soit Φ une bijection de E sur $\{1, 2, \ldots, n\}$ qui envoie a sur 1 et b sur 2. Nous avons

$$\mathrm{sgn}(\tau) = \mathrm{sgn}(\Phi \circ (a\ b) \circ \Phi^{-1}) = \mathrm{sgn}((1\ 2)).$$

Il reste à calculer ce dernier terme. Nous avons

$$\begin{aligned} \Delta &= \prod_{i<j}(X_j - X_i) \\ &= (X_2 - X_1)\prod_{j>2}(X_j - X_1)\prod_{j>2}(X_j - X_2)\prod_{j>i>2}(X_j - X_i) \end{aligned}$$

La transposition $(1\ 2)$ remplace $(X_2 - X_1)$ par $(X_1 - X_2)$, échange les deux facteurs $\prod_{j>2}(X_j - X_1)$ et $\prod_{j>2}(X_j - X_2)$ et laisse invariant le produit $\prod_{j>i>2}(X_j - X_i)$. Il s'ensuit que $(1\ 2) \cdot \Delta = -\Delta$ et donc que $\mathrm{sgn}((1\ 2)) = -1$. Finalement $\mathrm{sgn}(\tau) = -1$.

Soit E un ensemble fini. Une permutation σ de E ; elle s'écrit comme un produit $\tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$ de r transpositions. Il résulte alors de l'Exemple 5.1.24 que $\mathrm{sgn}(\sigma) = (-1)^r$. En particulier la classe de r modulo 2 ne dépend pas de l'écriture $\tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$ choisie.

La permutation σ est dite *paire* (respectivement impaire) si sa signature est 1 (respectivement -1). D'après ce qui précède σ est paire (respectivement impaire) si et seulement si elle s'écrit comme le produit d'un nombre pair (respectivement impair) de transpositions.

Calculons la signature dans le cas général. Soit E un ensemble fini. Soit C un ℓ-cycle de $\mathfrak{S}_E$. Puisque C s'écrit comme un produit de $\ell - 1$ transpositions (Lemme 5.1.2) nous avons $\mathrm{sgn}(C) = (-1)^{\ell-1}$. Considérons maintenant une permutation quelconque de $\mathfrak{S}_E$. Soit $C_1 C_2 \ldots C_s$ la décomposition de σ en cycles. Pour tout i désignons par ℓ_i la longueur de C_i. D'après ce qui précède nous avons

$$\mathrm{sgn}(\sigma) = \prod_i (-1)^{\ell_i - 1} = (-1)^{\sum_i \ell_i - r}.$$

En pratique nous calculons le plus souvent la signature d'une permutation en effectuant sa décomposition en cycles et en appliquant la formule ci-dessus.

1. Soient h et h' deux éléments conjugués de G ; soit $g \in$ G tel que $ghg^{-1} = h'$. Soit φ un morphisme de G vers un groupe G$'$. Alors $\varphi(h') = \varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}$. Ainsi $\varphi(h)$ et $\varphi(h')$ sont eux aussi conjugués. Si de plus G$'$ est abélien, alors $\varphi(h') = \varphi(h)$.

5.1.6. Générateurs de $\mathfrak{S}_n$. —

Comme nous l'avons montré au §5.1.3 :

Théorème 5.1.7

Le groupe $\mathfrak{S}_n$ est engendré par les transpositions.

Le nombre total de transpositions dans $\mathfrak{S}_n$ est $\binom{n}{2} = \frac{n(n-1)}{2}$. Le Théorème 5.1.7 fournit donc pour $\mathfrak{S}_n$ un système d'environ $\frac{n^2}{2}$ générateurs. Ce n'est pas le système minimal ; l'énoncé suivant assure l'existence d'un système de $(n-1)$ générateurs :

Théorème 5.1.8

Dès que $n \geq 2$ le groupe $\mathfrak{S}_n$ est engendré par les $n-1$ transpositions

$$(1\ 2),\ (1\ 3),\ \ldots,\ (1\ n).$$

Démonstration. — L'énoncé est vrai pour $n = 2$!

Supposons $n \geq 3$. D'après le Théorème 5.1.7 il suffit de montrer que toute transposition $(a\ b)$, $2 \leq a,\ b \leq n$ de $\mathfrak{S}_n$ s'écrit comme un produit de transpositions de la forme $(1\ i)$. C'est le cas puisque

$$(a\ b) = (1\ a)(1\ b)(1\ a)$$

d'où le résultat. □

Le groupe $\mathfrak{S}_n$ admet un autre système de $n-1$ générateurs :

Théorème 5.1.9

Dès que $n \geq 2$ le groupe $\mathfrak{S}_n$ est engendré par les $n-1$ transpositions

$$(1\ 2),\ (2\ 3),\ \ldots,\ (n-1\ n).$$

Démonstration. — D'après le Théorème 5.1.7 il suffit de montrer que toute transposition $(a\ b)$ de $\mathfrak{S}_n$ s'écrit comme un produit de transpositions de la forme $(i\ i+1)$ avec $i < n$. Puisque $(a\ b) = (b\ a)$ nous pouvons supposer que $a < b$. Nous allons raisonner par récurrence sur $b - a$ pour montrer que $(a\ b)$ s'écrit comme un produit de transpositions de la forme $(i\ i+1)$:

- ◇ si $b - a = 1$, alors $b = a + 1$ et $(a\ b) = (a\ a+1)$;
- ◇ supposons que toute transposition $(a\ b)$ avec $1 < b - a < k$ s'écrive comme un produit de transpositions de la forme $(i\ i+1)$. Soit $(a\ b)$ une transposition telle que $b - a = k$. Remarquons que

  $$(a\ b) = (a\ a+1)(a+1\ b)(a\ a+1).$$

  La transposition $(a\ a+1)$ est de la forme voulue. Remarquons que $b-(a+1) = k-1 < k$ donc $(a+1\ b)$ s'écrit par hypothèse de récurrence comme un produit de transpositions de

la forme $(i\ i+1)$. Finalement $(a\ b)$ s'écrit par hypothèse de récurrence comme un produit de transpositions de la forme $(i\ i+1)$.

□

Théorème 5.1.10

Dès que $n \geq 2$ le groupe $\mathfrak{S}_n$ est engendré par la transposition $(1\ 2)$ et le n-cycle $(1\ 2\ \dots\ n)$.

Démonstration. — D'après le Théorème 5.1.9 il suffit de montrer qu'à partir de la transposition $(1\ 2)$ et le n-cycle $(1\ 2\ \dots\ n)$ nous obtenons toutes les transpositions de la forme $(i\ i+1)$. C'est clair si $n = 2$. Supposons donc que $n \geq 3$. Soit $\sigma = (1\ 2\ \dots\ n)$; alors d'une part $\sigma(1\ 2) = (1\ 2\ \dots\ n)(1\ 2) = (1\ 3\ 4\ \dots\ n)$, d'autre part $(2\ 3)\sigma = (2\ 3)(1\ 2\ \dots\ n) = (1\ 3\ 4\ \dots\ n)$, *i.e.* $\sigma(1\ 2) = (2\ 3)\sigma$ ou encore

$$\sigma(1\ 2)\sigma^{-1} = (2\ 3).$$

Plus généralement

$$\sigma^k(1\ 2)\sigma^{-k} = (k+1\ k+2).$$

En particulier, nous pouvons écrire toutes les transpositions du type $(i\ i+1)$ à l'aide de la transposition $(1\ 2)$ et du cycle $\sigma = (1\ 2\ \dots\ n)$. □

Corollaire 5.1.2

Dès que $n \geq 3$ le groupe $\mathfrak{S}_n$ est engendré par $(1\ 2)$ et le $(n-1)$-cycle $(2\ 3\ \dots\ n)$.

Démonstration. — Le Théorème 5.1.10 et l'égalité $(1\ 2\ \dots\ n) = (1\ 2)(2\ 3\ \dots\ n)$ impliquent que $\mathfrak{S}_n$ est engendré par $(1\ 2)$ et $(2\ 3\ \dots\ n)$ dès que $n \geq 3$. □

Théorème 5.1.11

La transposition $(a\ b)$, $1 \leq a, b \leq n$, et le n-cycle $(1\ 2\ \dots\ n)$ engendrent $\mathfrak{S}_n$ si et seulement si $\operatorname{pgcd}(b-a, n) = 1$.

Démonstration. — Posons $d = \operatorname{pgcd}(b-a, n)$. Montrons que pour tout élément σ de $\langle (a\ b)\,(1\ 2\ \dots\ n)\rangle$ nous avons

$$i \equiv_d j \Longrightarrow \sigma(i) \equiv_d \sigma(j). \tag{5.1.3}$$

Il suffit de le vérifier pour $\sigma = (a\ b)$ et $\sigma = (1\ 2\ \dots\ n)$. Nous avons

$$\begin{cases} (a\ b)(i) = i \text{ pour tout } i \notin \{a, b\} \\ (a\ b)(i) = (a\ b)(a) = b \equiv_d a \\ (a\ b)(i) = (a\ b)(b) = a \equiv_d b \end{cases}$$

ainsi $(a\ b)(i) \equiv_d i$ pour tout i et (5.1.3) est vraie pour $\sigma = (a\ b)$.

Par ailleurs $(1\ 2\ \dots\ n)(i) \equiv_n i+1$ $(1\ 2\ \dots\ n)(i) \equiv_d i+1$ car d divise n. Par suite si $\sigma = (1\ 2\ \dots\ n)$ alors $i \equiv_d j \Longrightarrow i+1 \equiv_d j+1$ se réécrit

$$i \equiv_d j \Longrightarrow \sigma(i) \equiv_d \sigma(j)$$

et (5.1.3) est satisfaite pour $\sigma = (1\ 2\ \dots\ n)$.

Supposons $d > 1$. Comme $d = \mathrm{pgcd}(b-a, n)$ et comme $b - a < n$, on a $d + 1 \leq n$. Posons $g = (1\ d)$. On remarque que $1 \equiv_d d+1$ et $g(d+1) - g(1) = d + 1 - d = 1 \not\equiv_d 0$. Ainsi, g ne satisfaisant pas (5.1.3), n'est pas un élément du groupe engendré par σ et $(a\,b)$. Par contraposée on a donc montré que si $\langle \sigma, (a\,b)\rangle = \mathfrak{S}_n$ alors $\mathrm{pgcd}(b-a, n) = 1$.

Réciproquement, supposons que $\mathrm{pgcd}(b-a, n) = 1$. Pour tout $1 \leq i < n$ on a $\sigma(i) = i+1$ et donc $\sigma^{b-a}(a) = b$. Comme $\mathrm{pgcd}(b-a, n) = 1$, $\langle\sigma\rangle = \langle\sigma^{b-a}\rangle$ (Théorème 1.5.4) et σ^{b-a} est un n-cycle qui envoie a sur b. Nous pouvons écrire σ^{b-a} sous la forme $(a\ b\ i_3\ i_4\ \dots\ i_n)$ avec $i_3, i_4, \dots, i_n \in \{1, 2, \dots, n\} \smallsetminus \{a, b\}$. Définissons τ en posant $\tau(a) = 1$, $\tau(b) = 2$ et pour tout $k \in [\![3, n]\!]$, $\tau(i_k) = k$. On vérifie que $\tau(a\ b)\tau^{-1} = (1\ 2)$ et que $\tau\sigma^{b-a}\tau^{-1} = \sigma$.

Or $\langle(1\ 2), (1\ 2\ \dots\ n)\rangle = \mathfrak{S}_n$ (Théorème 5.1.10) donc $\langle(a\ b), \sigma\rangle = \langle(a\ b), \sigma^{b-a}\rangle = \mathfrak{S}_n$. □

Corollaire 5.1.3

Soient $\tau = (a\ b)$ une transposition de $\mathfrak{S}_n$ et σ un n-cycle de $\mathfrak{S}_n$. Nous avons $\langle\tau, \sigma\rangle = \mathfrak{S}_n$ si et seulement si $\mathrm{pgcd}(k, n) = 1$ où $\sigma^k(a) = b$.

Corollaire 5.1.4

Soit p un nombre premier. Le groupe $\mathfrak{S}_p$ est engendré par une transposition arbitraire et un p-cycle.

Une réflexion par rapport à une droite du plan est, d'un point de vue géométrique, identique à une réflexion par rapport à une autre droite du plan. Autrement dit, même si les réflexions sur deux droites différentes du plan ne sont pas strictement identiques, elles ont le même type d'effet. De même, deux transpositions différentes dans $\mathfrak{S}_n$ ne sont pas la même permutation mais ont le même type d'effet : échanger deux éléments et laisser tout le reste inchangé. Le concept qui précise la notion « d'effet différent mais de même type » est appelé conjugaison. Dans un groupe G, deux éléments g et h sont dits *conjugués* lorsque $h = xgx^{-1}$ pour certains $x \in \mathrm{G}$. Cette relation est symétrique, puisque $g = yhy^{-1}$ avec $y = x^{-1}$. Lorsque $h = xgx^{-1}$, on dit que x conjugue g à h. (Attention : lorsque certaines personnes disent « x conjugue g à h », elles peuvent vouloir dire $h = x^{-1}gx$ au lieu de $h = xgx^{-1}$).

Démonstration. — À conjugaison près $\sigma = (1\ 2\ \dots\ p)$. Pour toute transposition $(a\ b)$, $1 \leq a < b \leq p$, de $\mathfrak{S}_p$ nous avons $\mathrm{pgcd}(b-a, p) = 1$ (rappelons que par hypothèse p est premier). Le Théorème 5.1.10 assure que $\langle(a\ b), (1\ 2\ \dots\ p)\rangle = \mathfrak{S}_p$. □

5.1.7. Générateurs de $\mathcal{A}_n$. —

5.1.8. Simplicité du groupe alterné, version 1. —

Théorème 5.1.12

Le groupe $\mathcal{A}_n$ est simple dès que $n \geq 5$.

Rappelons que nous avons dj́à donné une démonstration de ce résultat dans §7.4.4 ; nous allons en donner deux autres.

5.1.8.1. *Le groupe $\mathcal{A}_n$ est simple dès que $n \geq 5$, version 1.* —

Corollaire 5.1.5

Dès que $n \geq 5$, on a $D(\mathcal{A}_n) = \mathcal{A}_n$.
Dès que $n \geq 2$, on a $D(\mathfrak{S}_n) = \mathcal{A}_n$.

Remarque 5.1.6. — Le Corollaire est une conséquence évidente du Théorème 5.1.12 mais il peut se montrer directement. Donnons quelques détails. On a les inclusions suivantes :

$$D(\mathcal{A}_n) \subset D(\mathfrak{S}_n) \subset \mathcal{A}_n$$

Lemme 5.1.4

Soit $n \geq 5$.

1. Le groupe $\mathcal{A}_n$ est $(n-2)$ fois transitif sur $\{1, 2, \ldots, n\}$; autrement dit si a_1, a_2, $\ldots$, a_{n-2} sont des éléments distincts de $\{1, 2, \ldots, n\}$, si b_1, b_2, $\ldots$, b_{n-2} sont des éléments distincts de $\{1, 2, \ldots, n\}$, alors il existe $\sigma \in \mathcal{A}_n$ tel que $\sigma(a_i) = b_i$.
2. Les 3-cycles sont conjugués dans $\mathcal{A}_n$.

Démonstration. — 1. Nous écrivons

$$\{1, 2, \ldots, n\} = \{a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, b_2, \ldots, b_{n-2}, b_{n-1}, b_n\}$$

et considérons $\rho \in \mathfrak{S}_n$ telle que $\rho(a_i) = b_i$ pour tout $i = 1, \ldots, n$. Si σ est paire, alors $\sigma = \rho$ convient. Si σ est impaire, alors $\rho = \sigma(a_{n-1}\ a_n)$ convient.

2. Soient $\sigma = (a_1\ a_2\ a_3)$ et $\tau = (b_1\ b_2\ b_3)$ deux 3-cycles dans $\mathfrak{S}_n$. Comme d'après ce qui précède $\mathcal{A}_n$ est $(n-2)$ transitif il existe g dans $\mathcal{A}_n$ tel que $g(a_i) = b_i$ pour tout $i = 1, 2, 3$. De plus $\tau = g\sigma g^{-1}$.

□

Lemme 5.1.5

Dès que $n \geq 3$ les 3-cycles engendrent $\mathcal{A}_n$.

Démonstration. — Puisque le groupe $\mathfrak{S}_n$ est engendré par les produits de transpositions, le groupe $\mathcal{A}_n$ est engendré par les produits pairs de transpositions et on a

$$(a\ b)(b\ c) = (a\ b\ c)$$

$$(a\ b)(a\ c) = (a\ c\ b)$$

(notons au passage que tous les 3-cycles sont dans $\mathcal{A}_n$) et

$$(a\ b)(c\ d) = (a\ b)(a\ c)(a\ c)(c\ d) = (a\ c\ b)(a\ c\ d)$$

□

Il suffit donc de montrer que tout 3-cycle est dans $\mathcal{A}_n$ un commutateur. Soit $\sigma = (a\ b\ c)$ un 3-cycle, $\sigma^2 = (a\ c\ b)$ en est un autre donc σ et σ^2 sont conjugués dans $\mathcal{A}_n$ (Lemme 5.1.4) : il existe τ dans $\mathcal{A}_n$ tel que $\sigma^2 = \tau^{-1}\sigma\tau$ d'où $\sigma = \sigma^{-1}\tau^{-1}\sigma\tau = [\sigma^{-1}, \tau^{-1}]$.

On montre de manière "analogue" que $D(\mathfrak{S}_n) = \mathcal{A}_n$ dès que $n \geq 2$.

Remarques 5.1.7. — Soit H un sous-groupe distingué de G.

- ◇ La classe de conjugaison d'un élément $h \in \mathrm{H}$ est contenue dans H, c'est-à-dire

$$\forall\, g \in \mathrm{G} \qquad ghg^{-1} \in \mathrm{H}$$

- ◇ Si $h \in \mathrm{H}$ et $g \in \mathrm{G}$ le commutateur $ghg^{-1}h^{-1} = (ghg^{-1})h^{-1}$ appartient à H et n'est pas, en général, un conjugué de h ; on obtient donc une nouvelle classe de conjugaison, le but étant de montrer qu'un système générateur de G est tout entier dans H.

Démonstration du Théorème 5.1.12 pour $n = 5$. — Le groupe $\mathcal{A}_5$ a 60 éléments :

- ◇ le neutre ;
- ◇ 15 éléments d'ordre 2 (produit de deux transpositions disjointes) ;
- ◇ 20 éléments d'ordre 3 (3-cycles) ;
- ◇ 24 éléments d'ordre 5 (5-cycles).

Les 3-cycles sont conjugués dans $\mathcal{A}_5$ (Lemme 5.1.4). Les éléments d'ordre 2 le sont aussi : si $\tau = (a\ b)(c\ d)(e)$ et $\tau' = (a'\ b')(c'\ d')(e')$ on définit $\sigma \in \mathcal{A}_n$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$ alors $\sigma\tau\sigma^{-1} = \tau'$.

Soit H un sous-groupe distingué non trivial de $\mathcal{A}_5$. Si H contient un élément d'ordre 3 (respectivement 2), alors il les contient tous d'après ce qui précède. Si H contient un élément d'ordre 5, il contient le 5-Sylow engendré par cet élément donc tous les 5-sous-groupes de Sylow puisqu'ils sont conjugués ainsi tous les éléments d'ordre 5.

Le groupe H ne peut pas contenir un seul des trois types d'éléments précédents en plus du neutre car ni $25 = 24 + 1$, ni $21 = 20 + 1$, ni $16 = 15 + 1$ ne divisent 60 (rappel : $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$). Par conséquent H contient au moins deux des trois types d'où

$$|\mathrm{H}| \geq 15 + 20 + 1 = 36.$$

Comme $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$ on obtient $|\mathrm{H}| = 60$ et $\mathrm{H} = \mathcal{A}_5$. □

Remarque 5.1.8. — Les 25 éléments d'ordre 5 de $\mathcal{A}_5$ ne sont pas conjugués dans $\mathcal{A}_5$ sinon ils formeraient une orbite et 24 diviserait 60. Nous pouvons cependant éviter le recours à Sylow dans la démonstration précédente en remarquant que si a et b sont d'ordre 5, alors b est conjugué à a ou a^2 dans $\mathfrak{S}_5$.

Démonstration du théorème 5.1.12 pour $n > 5$. — Posons $E = \{1, 2, \ldots, n\}$. Soit $\{\mathrm{id}\} \neq \mathrm{H} \triangleleft \mathcal{A}_n$. Soit $\sigma \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$. On se ramène au cas $n = 5$; pour ce faire on va fabriquer à partir de σ un élément non trivial de H qui n'agit que sur un ensemble à 5 éléments donc qui a $n - 5$ points fixes.

Comme $\sigma \neq \mathrm{id}$ il existe $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \in E$ tel que $c \notin \{a, b, \sigma(b)\}$ (un tel c existe puisque $n \geq 5$). Soit τ le 3-cycle donné par $\tau = (a\ c\ b)$. Alors $\tau^{-1} = (a\ b\ c)$. Considérons ρ défini par

$$\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (a\ c\ b)(\sigma(a)\ \sigma(b)\ \sigma(c)).$$

Comme $b = \sigma(a)$ l'ensemble $F = \{a, b, \sigma(a), \sigma(b), \sigma(c)\}$ a au plus 5 éléments et $\rho(F) = F$, $\rho_{|E\smallsetminus F} = \mathrm{id}_{|E\smallsetminus F}$. Quitte à ajouter au besoin des éléments à F on peut supposer que $|F| = 5$. Notons que $\rho(b) = \tau(\sigma(b)) \neq b$ (en effet $\sigma(b) \neq \tau^{-1}(b) = c$) donc $\rho \neq \mathrm{id}$.

Considérons $\mathcal{A}(F)$ l'ensemble des permutations paires de F. Il satisfait les deux propriétés suivantes

- ◇ $\mathcal{A}(F)$ est isomorphe à $\mathcal{A}_5$;
- ◇ $\mathcal{A}(F)$ se plonge dans $\mathcal{A}_n$ via $u \mapsto \overline{u}$ où

$$\begin{cases} \overline{u}_{|F} = u \\ \overline{u}_{|E\smallsetminus F} = \mathrm{id}_{|E\smallsetminus F} \end{cases}$$

Soit $\mathrm{H}_0 = \{u \in \mathcal{A}(F) \,|\, \overline{u} \in \mathrm{H}\} = \mathrm{H} \cap \mathcal{A}(F)$. Alors

- ◇ $\mathrm{H}_0 \triangleleft \mathcal{A}(F)$;
- ◇ $\rho_{|F} \in \mathrm{H}_0$;
- ◇ $\rho_{|F} \neq \mathrm{id}_F$.

Comme $\mathcal{A}(F) \not\simeq \mathcal{A}_5$ est simple on a $\mathrm{H}_0 = \mathcal{A}(F)$. Soit alors $u \in \mathcal{A}(F)$ un 3-cycle. Il appartient à H_0 donc $\overline{u}$ qui est encore un 3-cycle appartient à H. Mais comme les 3-cycles sont tous conjugués dans $\mathcal{A}_n$ (Lemme 5.1.4) ils appartiennent tous à H et puisqu'ils engendrent $\mathcal{A}_n$ (Lemme 5.1.5) on a $\mathrm{H} = \mathcal{A}_n$. □

Remarque 5.1.9. — Le groupe $\mathcal{A}_4$ n'est pas simple car

$$\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

est un sous-groupe distingué de $\mathcal{A}_4$ d'ordre 4.

Corollaire 5.1.6

Dès que $n \geq 5$ les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathfrak{S}_n$.

Avant de démontrer ce résultat donnons quelques résultats intermédiaires.

Lemme 5.1.6

Soit $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathfrak{S}_n$. Alors

$$\sigma(a\ b)\sigma^{-1} = (\sigma(a)\ \sigma(b)).$$

Lemme 5.1.7

Soit $n \geq 3$. Le centre de $\mathfrak{S}_n$ est réduit à $\{\mathrm{id}\}$.

Démonstration. — Soit σ un élément du centre de $\mathfrak{S}_n$. En particulier $\sigma(1\ 2) = (1\ 2)\sigma$, *i.e.* $\sigma(1\ 2)\sigma^{-1} = (1\ 2)$. Par suite (Lemme 5.1.6)

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma(1\ 3) = (1\ 3)\sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations. □

Démonstration du Corollaire 5.1.6. — Soit $\mathrm{H} \triangleleft \mathfrak{S}_n$. Alors $\mathrm{H} \cap \mathcal{A}_n \triangleleft \mathcal{A}_n$ donc $\mathrm{H} \cap \mathcal{A}_n \in \{\mathrm{id}, \mathcal{A}_n\}$.

Si $\mathrm{H} \cap \mathcal{A}_n = \mathcal{A}_n$, alors $\mathrm{H} = \mathcal{A}_n$ ou $\mathrm{H} = \mathfrak{S}_n$.

Si $\mathrm{H} \cap \mathcal{A}_n = \{\mathrm{id}\}$, alors la signature ε induit un isomorphisme de H sur $\varepsilon(\mathrm{H}) \subset \{1, -1\}$. Par suite $|\mathrm{H}| \leq 2$. Si $|\mathrm{H}| = 2$, alors $\mathrm{H} = \{\mathrm{id}, \sigma\}$. Mais si $\tau \in \mathfrak{S}_n$ comme $\tau\sigma\tau^{-1}$ appartient à H et $\tau\sigma\tau^{-1} \neq \mathrm{id}$ on a $\tau\sigma\tau^{-1} = \sigma$. Autrement dit σ appartient au centre de $\mathfrak{S}_n$ d'où $\sigma = \mathrm{id}$ (Lemme 5.1.7) : contradiction. Il en résulte que $\mathrm{H} = \{\mathrm{id}\}$. □

5.1.9. Les automorphismes du groupe symétrique. — Puisque $n \geq 3$ le centre $Z(\mathfrak{S}_n)$ de $\mathfrak{S}_n$ est réduit à $\{\mathrm{id}\}$ (Lemme 5.1.9). Par suite $\mathfrak{S}_n$ agit fidèlement sur lui-même par conjugaison. Autrement dit le groupe $\mathrm{Int}(\mathfrak{S}_n)$ des automorphismes intérieurs de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_n$.

L'énoncé suivant assure que sauf dans le cas exceptionnel $n = 6$ les automorphismes intérieurs sont les seuls automorphismes.

On donne ensuite un automorphisme non intérieur de $\mathfrak{S}_6$.

5.1.9.1. *Automorphismes de $\mathfrak{S}_n$, $n \neq 6$.* —

Lemme 5.1.8

Soit $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathfrak{S}_n$. Alors

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$$

Lemme 5.1.9

Soit $n \geq 3$. Le centre de $\mathfrak{S}_n$ est réduit à $\{\mathrm{id}\}$.

Démonstration. — Soit σ un élément du centre de $\mathfrak{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite (Lemme 5.1.8)

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations. □

Théorème 5.1.13

Soit $n \geq 3$. Supposons que $n \neq 6$; alors

$$\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n) \simeq \mathfrak{S}_n.$$

Lemme 5.1.10

Soit φ un automorphisme de $\mathfrak{S}_n$ qui envoie transpositions sur transpositions. Alors φ appartient à $\mathrm{Int}(\mathfrak{S}_n)$.

Démonstration. — Les transpositions de la forme $(1\ i)$ où $2 \leq i \leq n$ engendrent $\mathfrak{S}_n$. Posons $\tau_i = \varphi(1\ i)$. Remarquons que pour i et j distincts τ_i et τ_j ne commutent pas car $(1\ i)$ et $(1\ j)$ ne commutent pas. Il en résulte que les transpositions τ_i et τ_j ont exactement un élément en commun dans leur support. On peut donc écrire τ_2 et τ_3 sous la forme

$$\tau_2 = (\alpha_1\ \alpha_2) \qquad \tau_3 = (\alpha_1\ \alpha_3)$$

avec $\alpha_2 \neq \alpha_3$. Montrons que pour tout $k \geq 4$ on a $\tau_k = (\alpha_1\ \alpha_k)$ pour un certain $\alpha_k \in \{1, 2, \ldots, n\}$. En effet si α_1 n'était pas dans le support de τ_k on aurait $\tau_k = (\alpha_2\ \alpha_3)$ et

$$\tau_2 \circ \tau_k = (\alpha_1\ \alpha_2\ \alpha_3) \qquad \tau_3 \circ \tau_k = (\alpha_1\ \alpha_3\ \alpha_2)$$

seraient inverses l'un de l'autre. Mais

$$(1\ 2)(1\ k) = (2\ 1\ k)$$

n'est pas l'inverse de

$$(1\ 3)(1\ k) = (3\ 1\ k)$$

contradiction.

Notons que $\alpha\colon k \mapsto \alpha_k$ est un élément de $\mathfrak{S}_n$.

L'automorphisme φ et la conjugaison par α coïncident sur les générateurs $(1\ j)$ de $\mathfrak{S}_n$; ils coïncident donc sur $\mathfrak{S}_n$ tout entier. □

Démonstration du Théorème 5.1.13. — Soit φ un automorphisme non intérieur de $\mathfrak{S}_n$. Montrons que $n = 6$.

D'après le Lemme 5.1.10 il existe une transposition τ telle que $\varphi(\tau)$ ne soit pas une transposition. Puisque $(\varphi(\tau))^2 = \mathrm{id}$, $\varphi(\tau)$ est un produit de $k \geq 2$ transpositions à supports disjoints. Désignons par $\mathrm{C}(\tau)$ le centralisateur de τ

$$\mathrm{C}(\tau) = \{f \in \mathfrak{S}_n \mid f \circ \tau = \tau \circ f\}.$$

On a

$$\mathrm{C}(\tau) = \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{engendré par } \tau} \times \underbrace{\mathfrak{S}_{n-2}}_{\text{permutations de support disjoint de celui de } \tau}$$

En particulier on a un morphisme surjectif

$$\psi\colon \mathrm{C}(\tau) \to \mathfrak{S}_{n-2}$$

de noyau $\mathbb{Z}/2\mathbb{Z}$.

Posons $\mathrm{H} = \mathrm{C}(\varphi(\tau)) = \{f \in \mathfrak{S}_n \mid f \circ \varphi(\tau) = \varphi(\tau) \circ f\}$. Les groupes H et $\mathrm{C}(\tau)$ sont isomorphes via φ. Chacune des transpositions de la décomposition de $\varphi(\tau)$ commute avec $\varphi(\tau)$ donc H contient un sous-groupe N isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^k$. De plus N est le noyau du morphisme

$$\begin{array}{rcl} \mathrm{H} & \to & \mathfrak{S}_k \\ h & \mapsto & \text{permutation induite sur les } k \text{ transpositions de la décomposition de } \varphi(\tau) \end{array}$$

donc $\mathrm{N} \lhd \mathrm{H}$.

Ainsi comme $\mathrm{C}(\tau) \simeq \mathrm{H}$, $\mathrm{C}(\tau)$ contient un sous-groupe N' avec les deux propriétés suivantes :

$$\begin{cases} \mathrm{N}' \lhd \mathrm{C}(\tau) \\ \mathrm{N}' \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^k \end{cases}$$

Via ψ on obtient que $\mathfrak{S}_{n-2}$ contient un sous-groupe distingué isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^k$ ou $\left(\mathbb{Z}/2\mathbb{Z}\right)^{k-1}$ suivant que $\tau \in \mathrm{N}'$ ou $\tau \notin \mathrm{N}'$.

Or les sous-groupes distingués de $\mathfrak{S}_n$ sont

- $\diamond$ $\{\mathrm{id}\}$, $\mathcal{A}_n$, $\mathfrak{S}_n$ si $n \neq 4$;

◇ $\{\mathrm{id}\}$, $\mathcal{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathcal{A}_4$, $\mathfrak{S}_4$.

On en déduit les deux possibilités suivantes

◇ $n = 4$ car $\mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ peut alors correspondre à $\left(\mathbb{Z}/2\mathbb{Z}\right)^{k-1}$ avec $k = 2$;

◇ $n = 6$ car $\mathfrak{S}_4$ contient $\mathcal{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Supposons que $n = 4$. Le centralisateur d'une transposition dans $\mathfrak{S}_4$ est de cardinal 4 (c'est le groupe $\mathcal{K}$) alors que le centralisateur d'une double transposition est de cardinal 8 (en effet il divise strictement 24, est multiple strict de 4 car contient $\mathcal{K}$ mais aussi au moins un 4-cycle) : contradiction.

Ainsi $n = 6$. □

5.1.10. Les morphismes de $\mathfrak{S}_4$ vers $\mathfrak{S}_3$. — Désignons par V_4 le sous-groupe de $\mathfrak{S}_4$ engendré par les doubles transpositions ; notons que V_4 est isomorphe au groupe de Klein $\mathcal{K}$.

Lemme 5.1.11

Les sous-groupes distingués de $\mathcal{S}_4$ sont : $\{\mathrm{id}\}$, V_4, $\mathcal{A}_4$ et $\mathfrak{S}_4$.

Démonstration. — D'une part, l'ordre d'un sous-groupe de $\mathcal{S}_4$ divise 24 (Théorème de Lagrange, Théorème 1.6.4). D'autre part un sous-groupe distingué de $\mathcal{S}_4$ est une union de classe de conjugaison. De plus les diverses classes de conjugaison de $\mathfrak{S}_4$ sont constituées des éléments ayant le même type et

◇ le cardinal de la classe de conjugaison $C_{1,1,1,1}$ de l'identité est 1 ;

◇ le cardinal de la classe de conjugaison $C_{2,1,1}$ des transpositions est 6 ;

◇ le cardinal de la classe de conjugaison $C_{2,2}$ des double transpositions est 3 ;

◇ le cardinal de la classe de conjugaison $C_{3,1}$ des 3-cycles est 8 ;

◇ le cardinal de la classe de conjugaison C_4 des 4-cycles est 6.

On en déduit que

◇ $C_{1,1,1,1} = \{\mathrm{id}\}$ est un sous-groupe distingué de $\mathfrak{S}_4$;

◇ $C_{1,1,1,1} \cup C_{2,2} = \mathrm{V}_4$ est un sous-groupe distingué de $\mathfrak{S}_4$;

◇ $C_{1,1,1,1} \cup C_{2,2} \cup C_{3,1} = \mathcal{A}_4$ est un sous-groupe distingué de $\mathfrak{S}_4$;

◇ $C_{1,1,1,1} \cup C_{2,1,1} \cup C_{2,2} \cup C_{3,1} \cup C_4 = \mathfrak{S}_4$ est un sous-groupe distingué de $\mathfrak{S}_4$.

□

Théorème 5.1.14

Il y a exactement dix morphismes de $\mathfrak{S}_4$ dans $\mathfrak{S}_3$.

Démonstration. — Considérons un morphisme $\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_3$.

D'une part $\ker\varphi$ est un sous-groupe distingué de $\mathfrak{S}_4$, d'autre part φ ne peut être injectif (en effet, $|\mathfrak{S}_4| > |\mathfrak{S}_3|$). Par conséquent $\ker\varphi \in \{\mathfrak{S}_4, \mathcal{A}_4, \mathrm{V}_4\}$.

Si $\ker\varphi = \mathfrak{S}_4$, alors φ est le morphisme trivial ; autrement dit il y a un seul morphisme $\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_3$ de noyau $\mathfrak{S}_4$.

Supposons que $\ker\varphi = \mathcal{A}_4$. Par le Théorème 3.5.1 il existe un unique morphisme $\widetilde{\varphi}\colon {}^{\mathfrak{S}_4}\!/_{\mathcal{A}_4} \to \mathfrak{S}_3$ tel que $\widetilde{\varphi}\circ\pi = \varphi$ où $\pi\colon \mathfrak{S}_4 \to {}^{\mathfrak{S}_4}\!/_{\mathcal{A}_4}$ désigne la projection canonique ; de plus, $\widetilde{\varphi}$ est injectif. Réciproquement, un morphisme injectif $\psi\colon {}^{\mathfrak{S}_4}\!/_{\mathcal{A}_4} \to \mathfrak{S}_3$ détermine un morphisme $\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_3$ tel que $\ker\varphi = \mathcal{A}_4$ par la formule $\varphi = \psi\circ\pi$. En outre ψ est déterminé par un élément d'ordre 2 de $\mathfrak{S}_4$, en l'occurence $\psi(g)$ où g est l'unique élément non trivial de ${}^{\mathfrak{S}_4}\!/_{\mathrm{V}_4} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. Il y a donc autant de morphismes $\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_3$ de noyau $\mathcal{A}_4$ que d'éléments d'ordre 2 dans $\mathfrak{S}_3$, c'est-à-dire trois.

Soit $\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_3$ un morphisme de noyau V_4. D'après le Théorème 3.5.1 les groupes $\operatorname{im}\varphi$ et ${}^{\mathfrak{S}_4}\!/_{\ker\varphi} = {}^{\mathfrak{S}_4}\!/_{\mathrm{V}_4}$ sont isomorphes. En particulier $|\mathrm{im}\varphi| = \frac{|\mathfrak{S}_4|}{|\ker\varphi|} = \frac{24}{4} = 6$. Le Théorème 2.2.8 assure que $\mathrm{im}\varphi$ est isomorphe à ${}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$ ou à $\mathfrak{S}_3$. Supposons que ${}^{\mathfrak{S}_4}\!/_{\mathrm{V}_4}$ soit isomorphe à ${}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$. Comme ${}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$ est abélien, ceci implique que $D(\mathfrak{S}_4) \subset \mathrm{V}_4$: contradiction avec le fait que $D(\mathfrak{S}_4) = \mathcal{A}_4$ est d'ordre $12 > |\mathrm{V}_4| = 4$. Il s'en suit que ${}^{\mathfrak{S}_4}\!/_{\mathrm{V}_4}$ est isomorphe à $\mathfrak{S}_3$; notons α cet isomorphisme. Désignons par $\psi\colon \mathfrak{S}_4 \to {}^{\mathfrak{S}_4}\!/_{\mathrm{V}_4} \simeq \mathfrak{S}_3$ le morphisme quotient. Nous avons $\psi = \alpha\circ\pi$. D'après le Théorème 3.5.1 il existe un unique morphisme $\widetilde{\varphi}\colon {}^{\mathfrak{S}_4}\!/_{\mathrm{V}_4} \to \mathfrak{S}_3$ tel que $\widetilde{\varphi}\circ\pi = \varphi$. De plus, $\widetilde{\varphi}$ est un isomorphisme entre ${}^{\mathfrak{S}_4}\!/_{\mathrm{V}_4}$ et $\operatorname{im}\varphi = \operatorname{im}\widetilde{\varphi} = \mathfrak{S}_3$ d'après ce qui précède. Par suite si f est l'automorphisme de $\mathfrak{S}_3$ défini par $f = \widetilde{\varphi}\circ\alpha^{-1}$, alors $\varphi = f\circ\psi$. Autrement dit pour tout morphisme $\varphi\colon \mathfrak{S}_4 \to \mathfrak{S}_3$ tel que $\ker\varphi = \mathrm{V}_4$, il existe un unique automorphisme f de $\mathfrak{S}_3$ tel que $\varphi = f\circ\psi$. Réciproquement si f est un automrphisme de $\mathfrak{S}_3$, alors $f\circ\psi$ est un morphisme de $\mathfrak{S}_4$ dans $\mathfrak{S}_3$ de noyau V_4. Par suite il y a $|\mathrm{Aut}(\mathfrak{S}_3)|$ morphismes de $\mathfrak{S}_4$ dans $\mathfrak{S}_3$ de noyau V_4. Puisque $\mathrm{Aut}(\mathfrak{S}_3) \simeq \mathfrak{S}_3$ (Théorème 5.1.13), il y a $|\mathrm{Aut}(\mathfrak{S}_3)| = 6$ morphismes de $\mathfrak{S}_4$ dans $\mathfrak{S}_3$ de noyau V_4.

Finalement on compte $1 + 3 + 6 = 10$ morphismes de $\mathfrak{S}_4$ dans $\mathfrak{S}_3$.

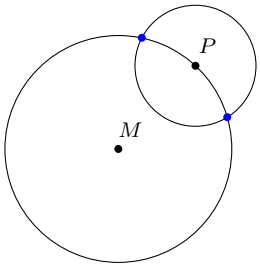
□

5.2. Le groupe diédral

Description des éléments de D_{2n}. — Soient M, P deux points du plan. Les points du plan situés à une distance donnée de M forment un cercle. Par suite les points situés à une distance donnée de M et à une distance donnée de P sont l'intersection de deux cercles, c'est-à-dire

- ◇ soit deux points (cercles non tangents),
- ◇ soit un point (cercles tangents).

Par exemple, sur la figure ci-dessous les points bleus sont à la même distance de chacun des deux points noirs (centres des cercles). Par conséquent étant donnés deux points distincts M et P (les points noirs), il y a au plus deux points dans le plan (les points bleus) qui peuvent être à distance donnée de M, resp. P.



Les points équidistants des deux points bleus se trouvent sur la droite passant par M et P. Ainsi, si nous choisissons un troisième point non colinéaire à P et M, alors ses distances aux deux points bleus sont différentes. Autrement dit, un point du plan est caractérisé de manière unique par ses distances à trois points non colinéaires. Sur un polygone régulier, nous avons le résultat suivant :

Lemme 5.2.1

Chaque point d'un polygone régulier est déterminé, parmi les points du polygone, par ses distances à deux sommets adjacents du polygone régulier.

Démonstration. — Soit $\mathcal{P}$ un polygone régulier. Nous désignons par $d(M, N)$ la distance entre deux points M et N de $\mathcal{P}$. Soient A et B deux sommets adjacents de $\mathcal{P}$; le segment $[AB]$ est donc un bord de $\mathcal{P}$. Soient P et Q deux points distincts de $\mathcal{P}$. Nous voulons montrer qu'on ne peut pas avoir $d(A, P) = d(A, Q)$ et $d(B, P) = d(B, Q)$. Raisonnons par l'absurde, *i.e.* supposons que $d(A, P) = d(A, Q)$ et $d(B, P) = d(B, Q)$. Alors P et Q se trouvent sur deux cercles $\mathcal{C}_A$ et $\mathcal{C}_B$ centré respectivement en A et B. Puisque $\#\mathcal{C}_A \cap \mathcal{C}_B \leq 2$ et puisque P et Q appartiennent à $\mathcal{C}_A \cap \mathcal{C}_B$, nous obtenons que $\mathcal{C}_A \cap \mathcal{C}_B = \{A, B\}$. Cela place P et Q « de part et d'autre » de $[AB]$ ce qui est impossible : un polygone régulier est toujours « d'un côté » de la droite passant par une arête. Par conséquent chaque point M de $\mathcal{P}$ est déterminé par $d(A, M)$ et $d(B, M)$. □

Théorème 5.2.1

Le groupe D_{2n} est d'ordre $2n$.

Démonstration. — Soit $\mathcal{P}$ un polygone régulier à n côtés.

Nous allons d'abord démontrer que $|\mathrm{D}_{2n}| \leq 2n$ puis exhiber $2n$ éléments distincts de D_{2n}.

- Dans un premier temps montrons que $|\mathrm{D}_{2n}| \leq 2n$. Soient A et B deux sommets adjacents d'un polygone régulier à n côtés. Un élément g de D_{2n} est une isométrie préservant $\mathcal{P}$;

comme g préserve les distances, g préserve d'une part les sommets de $\mathcal{P}$ et d'autre part la contiguïté des sommets. Ainsi $g(A)$ et $g(B)$ sont des sommets adjacents de $\mathcal{P}$.

Soit P un point du polygone $\mathcal{P}$. L'image de P par g est, d'après le Lemme 5.2.1, entièrement déterminée par la distance de $g(P)$ à $g(A)$ et la distance de $g(P)$ à $g(B)$. Autrement dit l'isométrie g est déterminée par $g(A)$ et $g(B)$. Ainsi pour borner $|\mathrm{D}_{2n}|$, il suffit de borner le nombre de possibilités pour $g(A)$ et $g(B)$. Puisque g(A) et g(B) sont des sommets adjacents, nous avons n possibilités pour $g(A)$ (le polygone compte n sommets) et pour chaque choix de $g(A)$, il y a deux choix possibles pour $g(B)$ (en effet, $g(B)$ est l'un des deux sommets adjacents à $g(A)$). Il en résulte qu'il y a au plus $n \times 2 = 2n$ possibilités pour $(g(A), g(B))$. Par conséquent $|\mathrm{D}_{2n}| \leq 2n$.

◇ Montrons que $|\mathrm{D}_{2n}| = 2n$.

Le polygone $\mathcal{P}$ peut pivoter autour de son centre de n manières différentes pour revenir sur lui-même. Plus précisément, le groupe diédral contient les rotations autour du centre d'angle $\frac{2k\pi}{n}$ avec $k = 0, 1, \ldots, n-1$; en particulier D_{2n} contient n rotations.

Décrivons les réflexions qui préservent $\mathcal{P}$.

- Si n est impair, il y a une réflexion d'axe la droite reliant chaque sommet au milieu du côté opposé. Cela représente un total de n réflexions (une par sommet) ; elles sont distinctes car chacune fixe un sommet différent.
- Si n est pair, il y a une réflexion d'axe la droite reliant chaque couple de sommets opposés ($\frac{n}{2}$ réflexions) et une réflexion d'axe la droite reliant les milieux des côtés opposés (encore $\frac{n}{2}$ réflexions). Le nombre de ces réflexions est $\frac{n}{2} + \frac{n}{2} = n$. Elles sont distinctes car ont différents types de points fixes sur le polygone : des paires de sommets opposés ou des paires de milieux de côtés opposés.

Les rotations et réflexions sont distinctes ; en effet, une rotation non triviale ne fixe aucun point de $\mathcal{P}$, la rotation triviale fixe $\mathcal{P}$ point par point et une réflexion fixe deux points de $\mathcal{P}$.

□

On note généralement $r \in \mathrm{D}_{2n}$ la rotation dans le sens inverse des aiguilles d'une montre de $\frac{2\pi}{n}$. Remarquons que cette rotation dépend de n : $r \in \mathrm{D}_6$ désigne une roration différente de $r \in \mathrm{D}_8$. Néanmoins tant que nous avons affaire à une seule valeur de n, il n'y a pas de confusion.

Théorème 5.2.2

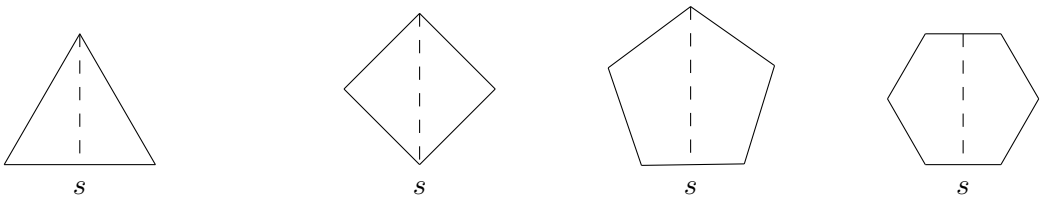
Les n rotations de D_{2n} sont id, r, r^2, ... , r^{n-1}.

Démonstration. — Les rotations id, r, r^2, ..., r^{n-1} sont distinctes puisque r est d'ordre n. □

Théorème 5.2.3

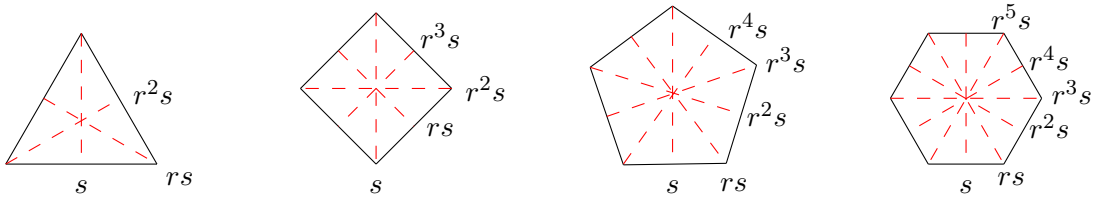
Les n réflexions de D_{2n} sont s, rs, r^2s, …, $r^{n-1}s$.

Soit s une réflexion d'axe une droite passant par un sommet du polygone. Voir les exemples dans la figure ci-dessous. [2] Une réflexion est d'ordre 2, donc $s^2 = \mathrm{id}$ et $s^{-1} = s$.



Démonstration. — Les isométries s, rs, r^2s, …, $r^{n-1}s$ sont distinctes puisque les rotations id, r, r^2, …, r^{n-1} le sont et que nous les composons simplement toutes à droite par s. Aucun des r^ks n'est une rotation. En effet si r^ks était une rotation, alors nous aurions $r^ks = r^\ell$ pour un certain ℓ, soit $s = r^{\ell-k}$; en particulier s serait une rotation ! Comme D_{2n} compte n rotations et n réflexions, et qu'aucun r^ks n'est une rotation, chaque r^ks est une réflexion. □

Les éléments de D_{2n} sont des rotations ou des réflexions : la composée d'une rotation r^i et d'une réflexion r^js (dans les deux sens) est une réflexion. L'interprétation géométrique des réflexions s, rs, r^2s, etc est la suivante : en traçant les axes de toutes les réflexions de D_{2n} et en se déplaçant dans le sens des aiguilles d'une montre autour du polygone à partir d'un sommet fixé par s, on rencontre successivement les axes de rs, r^2s, … , $r^{n-1}s$:



Résumons ce qui précède :

Théorème 5.2.4

Le groupe D_{2n} compte $2n$ éléments :

$$\mathrm{D}_{2n} = \{\mathrm{id},\, r,\, r^2,\, \ldots,\, r^{n-1},\, s,\, rs,\, \ldots,\, r^{n-1}s\}.$$

En particulier, les éléments de D_{2n} d'ordre supérieur à 2 sont des puissances de r.

2. La convention ici que s désigne une réflexion d'axe une droite passant par un sommet du polygone n'a d'importance que pour n pair, cas où l'axe de certaines réflexions ne passe pas par un sommet. Lorsque n est impair, l'axe de toutes les réflexions passe par un sommet, et n'importe laquelle d'entre elles peut être utilisée comme s.

Remarque 5.2.1. — Bien que chaque élément de D_{2n} d'ordre supérieur à 2 doive être une puissance de r il est faux en général que les seuls éléments d'ordre 2 soient des réflexions. Lorsque n est pair, la rotation d'angle $r^{\frac{n}{2}}$ est une rotation d'ordre 2. De toute évidence, une rotation d'angle π est la seule rotation d'ordre 2, et elle est contenue dans D_{2n} seulement lorsque n est pair.

Relations entre les rotations et les réflexions. — Les isométries r et s ne commutent pas. Leur relation de commutation est une formule fondamentale pour les calculs dans D_{2n} :

Théorème 5.2.5

Nous avons dans D_{2n} la relation :

$$srs^{-1} = r^{-1}. \tag{5.2.1}$$

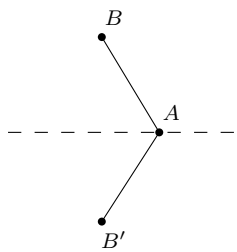
Démonstration. — Une démonstration directe vient du fait que rs est une réflexion :

$$(rs)^2 = \mathrm{id} \Longrightarrow rsrs = \mathrm{id} \Longrightarrow srs = r^{-1}$$

et $s = s^{-1}$ puisque s est d'ordre 2.

Nous voulons maintenant démontrer (5.2.1) de manière moins directe en utilisant une interprétation géométrique de srs^{-1}. Puisque toute isométrie d'un polygone régulier à n côtés est déterminé par son action sur deux sommets adjacents, pour démontrer $srs^{-1} = r^{-1}$ dans D_{2n} il suffit de vérifier que srs^{-1} et r^{-1} ont les mêmes valeurs sur une paire de sommets adjacents.

Rappelons que s est une réflexion fixant un sommet du polygone. Soit A un sommet fixé par s et notons ses sommets adjacents B et B' :



où la ligne pointillée passant par A est fixée par s. Nous avons $r(A) = B$, $r^{-1}(A) = B'$, $s(A) = A$ et $s(B) = B'$.

Les valeurs de srs^{-1} et r^{-1} en A sont

$$(srs^{-1})(A) = (srs)(A) = sr(s(A)) = sr(A) = s(B) = B' \qquad r^{-1}(A) = B',$$

tandis que leurs valeurs en B sont

$$(srs^{-1})(B) = (srs)(B) = sr(s(B)) = sr(B') = s(A) = A \qquad r^{-1}(B) = A.$$

Puisque srs^{-1} et r^{-1} prennent les mêmes valeurs en A et en B, elles prennent les mêmes valeurs sur le polygone et $srs^{-1} = r^{-1}$. □

Puisque $s^{-1} = s$ la relation $srs^{-1} = r^{-1}$ s'écrit aussi

$$sr = r^{-1}s, \qquad rs = sr^{-1}. \tag{5.2.2}$$

Par récurrence nous obtenons à partir de (5.2.1) pour tout entier k la relation

$$sr^k = r^{-k}s, \qquad r^k s = sr^{-k}. \tag{5.2.3}$$

Cela découle également du fait que $r^k s$ est une réflexion :

$$\mathrm{id} = (r^k s)^2 = r^k s r^k s \Longrightarrow sr^k = r^{-k}s^{-1} = r^{-k}s.$$

Exemple 5.2.1. — Dans D_{14}, en utilisant (5.2.3) nous obtenons

$$r^2 sr^6 sr^3 = r^2(sr^6)sr^3 = r^2(r^{-6}s)sr^3 = r^2 r^{-6} ssr^3 = r^{-4}r^3 = r^{-1} = r^6$$

et

$$sr^4 sr^3 sr^2 = s(r^4 s)r^3(sr^2) = s(sr^{-4})r^3(r^{-2}s) = ssr^{-4}r^3 r^{-2}s = r^{-3}s = r^4 s.$$

La relation (5.2.2) concerne une rotation particulière et une réflexion particulière de D_{2n}. Dans (5.2.3), nous avons étendu (5.2.2) à toute rotation et réflexion particulière dans D_{2n}. On peut étendre (5.2.3) à toute rotation et toute réflexion dans D_{2n} : une réflexion générale de D_{2n} est $r^i s$, donc par (5.2.3)

$$(r^i s)r^j = r^i r^{-j} s = r^{-j} r^i s = r^{-j}(r^i s).$$

Par ailleurs

$$r^j(r^i s) = r^i r^j s = r^i s r^{-j} = (r^i s)r^{-j}.$$

Puisque τ est d'ordre n la relation 5.2.1 se réécrit $srs^{-1} = r^{n-1}$ qui implique pour tout entier ℓ

$$sr^\ell s^{-1} = r^{\ell(n-1)}. \tag{5.2.4}$$

La relation (5.2.4) permet de retrouver le Théorème 5.2.4 :

Corollaire 5.2.1

Le groupe D_{2n} compte $2n$ éléments :

$$\mathrm{D}_{2n} = \{\mathrm{id},\, r,\, r^2,\, \ldots,\, r^{n-1},\, s,\, rs,\, \ldots,\, r^{n-1}s\}.$$

Démonstration. — Le groupe D_{2n} étant engendré par r et s, un élément de D_{2n} est de la forme

$$s^{\ell_1} r^{i_1} s^{\ell_2} r^{i_2} s^{\ell_3} \ldots s^{\ell_k} r^{i_k} \tag{5.2.5}$$

avec ℓ_j, i_j dans $\mathbb{Z}$.

Remarquons que pour tout $i_j \in \mathbb{Z}$ il existe $0 \leq \gamma_j \leq n-1$ tel que

$$r^{i_j} = r^{\gamma_j}. \tag{5.2.6}$$

En effet écrivons la division euclidienne de $i_j \in \mathbb{Z}$ par n : $i_j = nq_j + \gamma_j$, $0 \leq \gamma_j \leq n-1$; alors

$$r^{i_j} = r^{nq_j + \gamma_j} = r^{nq_j} r^{\gamma_j} = (r^n)^{q_j} r^{\gamma_j} = (\mathrm{id})^{q_j} r^{\gamma_j} = r^{\gamma_j}.$$

Remarquons que pour tout $\ell_j \in \mathbb{Z}$ il existe $0 \leq \delta_j \leq 1$ tel que

$$s^{\ell_j} = s^{\delta_j}. \tag{5.2.7}$$

En effet écrivons la division euclidienne de $\ell_j \in \mathbb{Z}$ par 2 : $\ell_j = 2Q_j + \delta_j$, $0 \leq \delta_j \leq 1$; alors

$$s^{\ell_j} = s^{2Q_j+\delta_j} = s^{2Q_j}s^{\delta_j} = (s^2)^{Q_j}s^{\delta_j} = (\mathrm{id})^{Q_j}s^{\delta_j} = s^{\delta_j}.$$

En utilisant (5.2.6) et (5.2.7) on remarque qu'un élément de la forme (5.2.5) s'écrit aussi

$$s^{\ell_1}r^{i_1}s^{\ell_2}r^{i_2}s^{\ell_3}\dots s^{\ell_k}r^{i_k}$$

avec $0 \leq \ell_j \leq 1$, $0 \leq i_j \leq n-1$.

Remarquons que si $\ell_j = 0$ alors $r^{i_{j-1}}s^{\ell_j}r^{i_j} = r^{\beta_j}$.

Par conséquent un élément de D_{2n} s'écrit

$$s^{\alpha_1}r^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k}s^{\alpha_2}$$

avec $0 \leq \alpha_1$, $\alpha_2 \leq 1$, $0 \leq \beta_j \leq n-1$.

a) Commençons par considérer le cas $\alpha_1 = 1$ et $\alpha_2 = 0$, autrement dit par considérer un élément de la forme $sr^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k}$. Montrons par récurrence sur $k \geq 2$ qu'il s'écrit aussi r^κ pour un certain κ.

   ◇ C'est vrai pour $k = 2$, en effet la relation (5.2.4) assure que

$$\underbrace{sr^{\beta_1}}_{r^{\beta_1(n-1)}s}\ sr^{\beta_2} = r^{\beta_1(n-1)}ssr^{\beta_2} = r^{\beta_1(n-1)}r^{\beta_2} = r^{\beta_1(n-1)+\beta_2}$$

   ◇ Supposons que la propriété soit vraie pour tout $j \leq k$ et montrons qu'alors elle est vraie pour $k+1$:

$$\underbrace{sr^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_{k-1}}}_{r^{\kappa_1}}\underbrace{sr^{\beta_k}sr^{\beta_{k+1}}}_{r^{\kappa_2}} = r^{\kappa_1}r^{\kappa_2} = r^{\kappa_1+\kappa_2}.$$

La propriété est donc vraie pour tout $k \geq 2$.

b) considérons le cas $\alpha_1 = \alpha_2 = 0$, autrement dit considérons un élément de la forme $r^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k}$ avec $k \geq 2$, alors il s'écrit $r^\ell s$ pour un certain ℓ ; en effet d'après a)

$$r^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k} = \underbrace{ss}_{\mathrm{id}}r^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k} = s\underbrace{sr^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k}}_{r^\kappa} = sr^\kappa = r^{\kappa(n-1)}s.$$

c) Considérons le cas $\alpha_1 = 0$ et $\alpha_2 = 1$, c'est-à-dire un élément de la forme $r^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k}s$ avec $k \geq 2$; d'après b) il s'écrit $\tau^\kappa s$ pour un certain κ :

$$r^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k}s = \underbrace{r^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k}}_{r^\kappa s}s = r^\kappa ss = r^\kappa\underbrace{ss}_{\mathrm{id}} = r^\kappa.$$

d) Finalement considérons le cas $\alpha_1 = \alpha_2 = 1$, soit un élément de la forme $sr^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k}s$ avec $k \geq 2$; d'après a) il s'écrit $r^\kappa s$ pour un certain κ :

$$sr^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k}s = \underbrace{sr^{\beta_1}sr^{\beta_2}s\dots sr^{\beta_k}}_{r^\kappa}s = r^\kappa s.$$

□

5.2.1. Centre. — Connaître le comportement des rotations et des réflexions lorsqu'on les compose nous permet de calculer le centre de D_{2n}. La réponse dépend de / la parité de n :

Théorème 5.2.6

Soit $n \geq 3$ un entier.
Si n est impair, alors le centre de D_{2n} est trivial.
Si n est pair, alors le centre de D_{2n} est $\{\mathrm{id}, r^{n/2}\}$.

Démonstration. — Aucune réflexion n'appartient à $Z(\mathrm{D}_{2n})$. En effet si les réflexions appartenaient à $Z(\mathrm{D}_{2n})$, alors elles commuteraient avec r, c'est-à-dire nous aurions

$$(r^i s)r = r(r^i s) \iff r^i(sr) = r^{i+1}s \iff r^i r^{-1}s = r^{i+1}s \iff r^{i-1}s = r^{i+1}s \iff r^{i-1} = r^{i+1}.$$

Or $r^{i-1} = r^{i+1}$ entraîne $r^2 = \mathrm{id}$: contradiction avec le fait que r est d'ordre $n \geq 3$.

Supposons qu'une rotation r^j appartienne au centre de D_{2n} ; notons que nous pouvons supposer que $0 \leq j < n$. Alors en particulier $r^j s = sr^j$, ce qui équivaut à $r^j s = r^{-j}s$ et à $r^j = r^{-j}$; ainsi $r^{2j} = \mathrm{id}$. Puisque r est d'ordre n la relation $r^{2j} = \mathrm{id}$ implique n divise $2j$; de plus, $0 \leq 2j < 2n$. Les seuls multiples de n dans $\{0, 1, \ldots, 2n-1\}$ sont 0 et n ; il s'en suit que $2j = 0$ ou $2j = n$. Si $2j = 0$, alors $j = 0$ et $r^j = \mathrm{id}$. Si $2j = n$, alors n est pair et $j = \frac{n}{2}$, donc $r^j = r^{\frac{n}{2}}$.

Si n est impair, alors $j = 0$ et $r^j = \mathrm{id}$. Évidemment id appartient à $Z(\mathrm{D}_{2n})$ donc $Z(\mathrm{D}_{2n}) = \{\mathrm{id}\}$.

Si n est pair, alors r^j coïncide avec id ou $r^{\frac{n}{2}}$. Évidemment id appartient à $Z(\mathrm{D}_{2n})$. Reste à déterminer si $r^{\frac{n}{2}}$ appartient à $Z(\mathrm{D}_{2n})$. Clairement $r^{\frac{n}{2}}$ commute à chaque r^i ; de plus, nous avons :

$$r^{\frac{n}{2}}(r^i s) = r^{\frac{n}{2}+i}s, \qquad (r^i s)r^{\frac{n}{2}} = r^i r^{-\frac{n}{2}}s = r^i r^{\frac{n}{2}}s = r^{i+\frac{n}{2}}s = r^{\frac{n}{2}+i}s,$$

(nous avons utilisé la relation $r^{\frac{n}{2}} = r^{-\frac{n}{2}}$ qui découle de $r^n = \mathrm{id}$). Finalement $r^{\frac{n}{2}}$ commute à toutes les rotations et réflexions de D_{2n} donc appartient au centre de D_{2n}. □

Exemple 5.2.2. — Le centre du groupe D_6 est trivial. Le centre du groupe D_8 est $\{\mathrm{id}, r^2\}$.

Pour n pair, la rotation $r^{\frac{n}{2}}$ est une rotation d'angle π. Le Théorème 5.2.6 assure que pour n pair cette rotation est la seule isométrie non triviale qui préserve le polygone régulier à n côtés et qui commute aux autres isométries préservant le polygone régulier. Notons que lorsque n est impair, une rotation d'angle π ne préserve pas le polygone régulier à n côtés.

5.2.2. Le groupe dérivé. —

Théorème 5.2.7

Soit $n \geq 3$ un entier. Le groupe dérivé de D_{2n} est

$$D(\mathrm{D}_{2n}) = \begin{cases} \langle r \rangle \text{ si } n \text{ est impair} \\ \langle r^2 \rangle \text{ si } n \text{ est pair} \end{cases}$$

Démonstration. — Le groupe D_{2n} n'est pas abélien ; en effet d'une part $sr = r^{n-1}s$ et d'autre part $r^{n-1}s \neq rs$ (car $n \neq 2$). Par conséquent $D(\mathrm{D}_{2n}) \neq \{\mathrm{id}\}$.

L'égalité $[\mathrm{D}_{2n} : \langle r \rangle] = 2$ assure que $\langle r \rangle$ est un sous-groupe distingué d'ordre n de D_{2n} (Théorème 3.2.1). Ainsi $\mathrm{D}_{2n}/\langle r \rangle$ est un groupe d'ordre 2 donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$; en particulier le quotient $\mathrm{D}_{2n}/\langle r \rangle$ est abélien. Puisque $\mathrm{D}_{2n}/D(\mathrm{D}_{2n})$ est le plus grand quotient abélien de D_{2n} nous avons l'inclusion : $D(\mathrm{D}_{2n}) \subset \langle r \rangle$.

Étant donné que

$$[s, r] = srs^{-1}r^{-1} = r^{-1}r^{-1} = r^{-2}$$

l'élément r^{-2} appartient à $D(\mathrm{D}_{2n})$ et r^2 aussi. Finalement $\langle r^2 \rangle \subset D(\mathrm{D}_{2n})$. Nous avons donc les inclusions

$$\langle r^2 \rangle \subset D(\mathrm{D}_{2n}) \subset \langle r \rangle.$$

- Si n est impair, alors n est premier avec 2 et l'ordre de r^2 est $\frac{n}{\mathrm{pgcd}(2,n)} = n$ donc $\langle r^2 \rangle = \langle r \rangle$ et $D(\mathrm{D}_{2n}) = \langle r \rangle$.
- Si $n = 2m$ est pair, montrons que

$$D(\mathrm{D}_{2n}) = \langle r^2 \rangle = \{\mathrm{id}, r^2, r^4, \ldots, r^{n-2}\} = \{\mathrm{id}, r^2, r^4, \ldots, r^{2(m-1)}\}.$$

Nous avons vu que $\langle r^2 \rangle \subset D(\mathrm{D}_{2n})$. Montrons que $\langle r^2 \rangle \lhd \mathrm{D}_{2n}$. Soit $y = r^{2a} \in \langle r^2 \rangle$ et $x \in \mathrm{D}_{2n}$; nous avons $x = r^k$ ou $x = r^k s$. Dans le premier cas nous obtenons

$$xyx^{-1} = r^k r^{2a} r^{-k} = r^{k+2a-k} = r^{2a} = y \in \langle r^2 \rangle.$$

et dans le second cas

$$\begin{aligned} xyx^{-1} &= r^k s r^{2a} (r^k s)^{-1} = r^k \underbrace{s r^{2a}}_{r^{2a(n-1)}s} s^{-1} r^{-k} \\ &= r^k r^{2a(n-1)} s s^{-1} r^{-k} = r^k r^{2a(n-1)} r^{-k} \\ &= r^{k+2a(n-1)-k} = r^{2a(n-1)} \in \langle r^2 \rangle \end{aligned}$$

Ainsi $\langle r^2 \rangle \lhd \mathrm{D}_{2n}$.

De plus r^2 est d'ordre $\frac{n}{\mathrm{pgcd}(2,n)} = \frac{n}{2} = m$ donc $|\langle r^2 \rangle| = m$. Ainsi le quotient $\mathrm{D}_{2n}/\langle r^2 \rangle$ est d'ordre $\frac{2n}{m} = 4$. Mais un groupe d'ordre 4 est abélien car isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il s'en suit que $\mathrm{D}_{2n}/\langle r^2 \rangle$ est abélien. Comme $\mathrm{D}_{2n}/D(\mathrm{D}_{2n})$ est le plus grand

quotient abélien de D_{2n} nous avons l'inclusion $\mathrm{D}_{2n}/\langle r^2\rangle \subset \mathrm{D}_{2n}/D(\mathrm{D}_{2n})$ et l'inclusion $D(\mathrm{D}_{2n}) \subset \langle r^2\rangle$. Finalement $D(\mathrm{D}_{2n}) = \langle r^2\rangle$.

□

5.2.3. Classes de conjugaison dans D_{2n}. —

Les réflexions de D_{2n} se répartissent en une ou deux classes de conjugaison suivant la parité de n qui prescrit la nature géométrique de celles-ci. Si n est impair, alors les réflexions de D_{2n} se « ressemblent toutes » : ce sont des réflexions par rapport à une droite passant par un sommet et le milieu du côté opposé :

D_6 D_{10}

Par contre si n est pair, alors les réflexions sont de deux types : les réflexions par rapport à une droite passant par deux sommets opposés et les réflexions par rapport à une droite passant par les milieux des deux côtés opposés

D_8 D_{12}

Proposition 5.2.1

Considérons le groupe diédral D_{2n} des isométries du plan euclidien conservant le polygone régulier à n côtés centré en l'origine de $\mathbb{R}^2$. Désignons par $r \in \mathrm{D}_{2n}$ la rotation d'angle $\frac{2\pi}{n}$ et par $s \in \mathrm{D}_{2n}$ la réflexion par rapport à l'axe des abscisses.
Si n est pair, *i.e.* $n = 2m$, alors

- ◇ on compte deux classes de conjugaison de cardinal 1 : $\{\mathrm{id}\}$ et $\{-\mathrm{id}\} = \{r^m\}$,
- ◇ il y a $m-1$ classes de conjugaison de cardinal 2 : $\{r, r^{-1}\}$, $\{r^2, r^{-2}\}$, ..., $\{r^{m-1}, r^{-m+1}\}$,
- ◇ les réflexions se répartissent en deux classes de conjugaison de cardinal m : $\{s, r^2s, r^4s, \ldots, r^{2m-2}s\}$ et $\{rs, r^3s, \ldots, r^{2m-1}s\}$.

En particulier, D_{2n} compte $3 + \frac{n}{2}$ classes de conjugaison.
Si n est impair, *i.e.* $n = 2m+1$,

- ◇ alors il y a une classe de conjugaison de cardinal 1 : $\{\mathrm{id}\}$,
- ◇ on compte m classes de conjugaison de cardinal 2 : $\{r, r^{-1}\}$, $\{r^2, r^{-2}\}$, ..., $\{r^m, r^{-m}\}$,
- ◇ les réflexions forment une classe de conjugaison de cardinal n : $\{s, rs, r^2s, \ldots, r^{n-1}s\}$.

En particulier, D_{2n} compte $\frac{3+n}{2}$ classes de conjugaison.

Démonstration. — Si σ est une réflexion de D_{2n}, alors pour toute rotation R de D_{2n} nous avons

$$\sigma R = R^{-1}\sigma \tag{5.2.8}$$

(en effet $R\sigma$ est une réflexion donc $(R\sigma)^2 = \mathrm{id}$, *i.e.* $R\sigma R\sigma = \mathrm{id}$ et $\sigma R = R^{-1}\sigma^{-1} = R^{-1}\sigma$).

Remarquons qu'une rotation et une réflexion ne peuvent pas être conjuguées car leurs déterminants sont distincts.

Soient R une rotation de D_{2n} et g un élément de D_{2n}.

- ◇ Si g est une rotation, alors $gRg^{-1} = R$ car le groupe des rotations de $\mathbb{R}^2$ est abélien.
- ◇ Si g est une réflexion, alors en vertu de (5.2.8) nous avons $gRg^{-1} = R^{-1}$.

Il s'en suit que deux rotations de D_{2n} sont conjuguées si et seulement si elles sont égales ou inverses l'une de l'autre. Remarquons que si R est une rotation de D_{2n} distincte de id et telle que $R = R^{-1}$, alors $R = -\mathrm{id}$ et comme $R^{2n} = \mathrm{id}$ alors n est pair.

Intéressons-nous maintenant aux conjugués d'une réflexion de D_{2n}. Soient $k \in \mathbb{Z}$ et $g = r^k$ ou $g = r^k s$. Alors en vertu de (5.2.8) nous avons

$$gsg^{-1} = r^k s r^{-k} = (r^k s)s(sr^{-k}) = r^{2k}s. \tag{5.2.9}$$

Nous sommes amenés à distinguer deux cas selon la parité de n.

i) Considérons d'abord le cas n pair, *i.e.* $n = 2m$. La relation (5.2.9) montre que la classe de conjugaison de s est exactement formée des $r^{2k}s$ avec $0 \leq k \leq m-1$. Cherchons la classe de conjugaison de rs. Si $g = r^k$ pour un certain k dans $\mathbb{Z}$, alors

$$grsg^{-1} = r^k rsr^{-k} = r^{2k+1}s.$$

Ainsi la classe de conjugaison de rs est formée des $r^{2k-1}s$ avec $1 \leq k \leq m$. Il en résulte que les classes de conjugaison de D_{2n} sont

- ◇ $\{\mathrm{id}\}$,
- ◇ $\{-\mathrm{id}\}$,
- ◇ $\{r, r^{-1}\}, \{r^2, r^{-2}\}, \ldots, \{r^{m-1}, r^{-m+1}\}$,
- ◇ $\{s, r^2s, r^4s, \ldots, r^{2m-2}s\}$,
- ◇ $\{rs, r^3s, \ldots, r^{2m-1}s\}$

Géométriquement il est clair qu'il existe deux classes de conjugaison de réflexions dans D_{2n}, n pair : les premières ont un axe passant par deux sommets opposés du polygone tandis que l'axe des autres passe par le milieu de deux sommets consécutifs du polygone.

ii) Considérons maintenant le cas n impair, *i.e.* $n = 2m+1$. Dans ce cas r^2 est d'ordre n d'où $\{r^{2k} \,|\, k \in \mathbb{Z}\} = \{r^k \,|\, k \in \mathbb{Z}\}$ et (5.2.9) montre que la classe de conjugaison de s est $\{r^k s \,|\, k \in \mathbb{Z}\}$, *i.e.* que les réflexions de D_{2n} sont conjuguées. Ainsi les classes de conjugaison de D_{2n} sont

- ◇ $\{\mathrm{id}\}$,
- ◇ $\{r, r^{-1}\}, \{r^2, r^{-2}\}, \ldots, \{r^m, r^{-m}\}$,
- ◇ $\{s, rs, r^2s, \ldots, r^{n-1}s\}$.

□

5.2.4. Centralisateurs. — Soit $Z_g = \{h \in \mathrm{D}_{2n} \,|\, gh = hg\}$ le centralisateur de $g \in \mathrm{D}_{2n}$. Rappelons que $|Z_g| = \frac{|\mathrm{D}_{2n}|}{|C_g|}$ où C_g désigne la classe de conjugaison de $g \in \mathrm{D}_{2n}$.

- ◇ Supposons dans un premier temps que n est impair. Soit $1 \leq k \leq n-1$ un entier. D'une part $|Z_{r^k}| = \frac{|\mathrm{D}_{2n}|}{|C_{r^k}|}$, d'autre part $\langle r \rangle \subseteq Z_{r^k}$. Par conséquent $Z_{r^k} = \langle r \rangle$.

  De même si σ est une réflexion, *i.e.* $\sigma = r^k s$ pour un certain k, alors $Z_\sigma = \langle \sigma \rangle$.

- ◇ Supposons désormais que n soit pair. Écrivons n sous la forme $2m$. Soit $1 \leq |k| \leq m-1$. Comme précédemment nous obtenons que $Z_{r^k} = \langle r \rangle$. Si σ est une réflexion, alors $|Z_\sigma| = \frac{|\mathrm{D}_{2n}|}{|C_\sigma|} = \frac{4m}{m} = 4$. Il en résulte que $Z_\sigma = \{\mathrm{id}, -\mathrm{id}, \sigma, -\sigma\}$ et Z_σ est isomorphe au groupe de Klein. Enfin $Z_{-\mathrm{id}} = \mathrm{D}_{2n}$.

Résumons les propriétés établies dans ces derniers paragraphes :

D_{2n}, $n = 2m+1$			
élément	ordre	classe de conjugaison	centralisateur
id	1	$\{\mathrm{id}\}$	D_{2n}
r^k, $k \in \{-m, \ldots, m\} \smallsetminus \{0\}$	$\frac{n}{\mathrm{pgcd}(k,n)}$	$\{r^k, r^{-k}\}$	$\langle r \rangle$
$r^k s$, $0 \leq k \leq n-1$	2	$\{r^i s \mid 0 \leq i \leq n-1\}$	$\langle r^k s \rangle$

D_{2n}, $n = 2m$			
élément	ordre	classe de conjugaison	centralisateur
id	1	$\{\mathrm{id}\}$	D_{2n}
$-\mathrm{id}$	2	$\{-\mathrm{id}\}$	D_{2n}
r^k, $0 \leq \lvert k \leq \lvert m-1$	$\frac{n}{\mathrm{pgcd}(k,n)}$	$\{r^k, r^{-k}\}$	$\langle r \rangle$
$r^{2k} s$, $0 \leq k \leq n-1$	2	$\{r^{2i-1} s \mid 1 \leq i \leq m\}$	$\langle r^{2k-1} s, -\mathrm{id} \rangle$

5.2.5. Caractérisation abstraite. — Le groupe D_{2n} possède deux générateurs r et s respectivement d'ordre n et 2 tels que $srs^{-1} = r^{-1}$. Nous allons montrer que tout groupe G ayant deux générateurs avec des propriétés similaires à r et s satisfait les propriétés suivantes :

Théorème 5.2.8

Soit G un groupe engendré par deux éléments x et y satisfaisant les propriétés suivantes : $x^n = e$ pour un certain $n \geq 3$, $y^2 = e$ et $yxy^{-1} = x^{-1}$. Alors il existe un morphisme surjectif de D_{2n} dans G. Si, de plus, G est d'ordre $2n$, alors ce morphisme est un isomorphisme.

Les hypothèses $x^n = e$ et $y^2 = e$ ne signifient pas que x est d'ordre n et y est d'ordre 2, mais seulement que l'ordre de x divise n et l'ordre de y divise 2. Par exemple, le groupe trivial est de la forme $\langle x, y \rangle$ avec $x^n = e$, $y^2 = e$ et $yxy^{-1} = x^{-1}$: il suffit de prendre $x = y = e$.

Démonstration. — La relation $yxy^{-1} = x^{-1}$ implique $yx^jy^{-1} = x^{-j}$ pour tout $j \in \mathbb{Z}$. Puisque $y^2 = e$, on a pour tout $k \in \mathbb{Z}$ la relation $y^k x^j y^{-k} = x^{(-1)^k j}$. Ainsi pour tous j, $k \in \mathbb{Z}$,

$$y^k x^j = x^{(-1)^k j} y^k. \tag{5.2.10}$$

Cela montre que chaque produit faisant intervenir x et y (comme par exemple $y^7x^{-5}y^2x^3y^{-1}x^{13}$) s'écrit aussi sous la forme $x^a y^b$. Étant donnés que $x^n = e$ et $y^2 = e$, nous avons

$$\mathrm{G} = \langle x, y \rangle = \{x^j, x^j y \mid j \in \mathbb{Z}\} = \{e, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y\}.$$

Ainsi G est un groupe fini d'ordre $2n$. Les relations $x^n = e$, $y^2 = e$ et $yxy^{-1} = x^{-1}$ suggèrent que pour définir un morphisme de D_{2n} dans G nous devons envoyer r sur x et s sur y ; autrement

dit que $\varphi\colon \mathrm{D}_{2n} \to \mathrm{G}$ est défini par $\varphi(r^j s^k) = x^j y^k$. Cette formule définit φ sur D_{2n} puisque tous les éléments de D_{2n} sont de la forme $r^j s^k$ pour certains entiers j, k (Théorème 5.2.4). Mais cette écriture n'est pas unique (par exemple $r^j s^k = r^{j+n} s^{k+2}$), vérifions donc que φ est bien défini, c'est-à-dire que si $r^j s^k = r^{j'} s^{k'}$, alors $\varphi(r^j s^k) = \varphi(r^{j'} s^{k'})$. Si $r^j s^k = r^{j'} s^{k'}$, alors $r^{j-j'} = s^{k'-k}$; en particulier $r^{j-j'} = s^{k'-k}$ appartient à $\langle r\rangle \cap \langle s\rangle = \{\mathrm{id}\}$. Par suite $j' \equiv_n j$ et $k' \equiv_2 k$; comme $x^n = e$ et $y^2 = 1$ nous obtenons que $x^j y^k = x^{j'} y^{k'}$, autrement dit que $\varphi(r^j s^k) = \varphi(r^{j'} s^{k'})$.

Pour vérifier que φ est un morphisme, on utilise (5.2.10) : d'une part

$$\varphi(r^j s^k)\varphi(r^{j'} s^{k'}) = x^j y^k x^{j'} y^{k'} = x^j x^{(-1)^k j'} y^k y^{k'} = x^{j+(-1)^k j'} y^{k+k'}$$

et d'autre part

$$\varphi\big((r^j s^k)(r^{j'} s^{k'})\big) = \varphi(r^j r^{(-1)^k j'} s^k s^{k'}) = \varphi(r^{j+(-1)^k j'} s^{k+k'}) = x^{j+(-1)^k j'} y^{k+k'}.$$

Il en résulte que φ est un morphisme de D_{2n} dans G. La surjectivité découle du fait que tout élément de G est de la forme $x^j y^k$.

Si $|\mathrm{G}| = 2n$ alors la surjectivité de φ entraîne l'injectivité de φ, *i.e.* φ est un isomorphisme. □

Remarque 5.2.2. — Le morphisme $\varphi\colon \mathrm{D}_{2n} \to \mathrm{G}$ construit dans la démonstration est l'unique morphisme tel que $\varphi(r) = x$ et $\varphi(s) = y$. Une formulation plus précise du Théorème 5.2.8 est donc la suivante : pour chaque groupe $\mathrm{G} = \langle x, y\rangle$ tel que $x^n = e$ pour un certain $n \geq 3$, $y^2 = e$ et $yxy^{-1} = x^{-1}$, il existe un unique morphisme de D_{2n} dans G qui envoie r sur x et s sur y.

Une conséquence du Théorème 5.2.8 est la suivante : lorsque $n \geq 3$, le groupe D_{2n} est isomorphe à un groupe de matrices défini sur $\mathbb{Z}/n\mathbb{Z}$. Considérons le sous-groupe de $\mathrm{GL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$ défini par

$$\widetilde{\mathrm{D}_{2n}} = \left\{ \begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix} \mid k \in \mathbb{Z}/n\mathbb{Z} \right\}. \tag{5.2.11}$$

Le groupe $\widetilde{\mathrm{D}_{2n}}$ est d'ordre $2n$ (puisque $1 \not\equiv_n -1$ pour $n \geq 3$). Les éléments $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de $\widetilde{\mathrm{D}_{2n}}$ sont d'ordre 2, respectivement n. Un élément générique de $\widetilde{\mathrm{D}_{2n}}$ est de la forme $\begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix}$ et

$$\begin{pmatrix} \pm 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \pm 1 & 1 \\ 0 & 1 \end{pmatrix}^k \begin{pmatrix} \pm 1 & 0 \\ 0 & 1 \end{pmatrix}$$

donc $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ engendre $\widetilde{\mathrm{D}_{2n}}$. De plus, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}$ sont conjugués par $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$:

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}$$

Ainsi $\widetilde{\mathrm{D}_{2n}}$ est isomorphe à D_{2n} avec $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dans le rôle de r et $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ dans le rôle de s (Théorème 5.2.8).

Cette réalisation de D_{2n} comme sous-groupe de de $\mathrm{GL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$ ne doit pas être confondue avec la réalisation de D_{2n} comme sous-groupe de $\mathrm{GL}(2, \mathbb{R})$ obtenue en utilisant les matrices :

$$r = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \qquad s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Corollaire 5.2.2

Lorsque $n \geq 3$ est impair, nous avons l'isomorphisme : $\mathrm{D}_{2n} \simeq \mathrm{D}_n \times \mathbb{Z}/2\mathbb{Z}$.

Par exemple, $\mathrm{D}_6 \simeq \mathrm{D}_3 \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{D}_{10} \simeq \mathrm{D}_5 \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. — Soit $\mathrm{H} = \langle r^2, s\rangle$ où r et s désignent les générateurs de D_{2n}. Alors $(r^2)n = \mathrm{id}$, $s^2 = \mathrm{id}$, et $sr^2s^{-1} = r^{-2}$; par suite il existe un morphisme surjectif de D_{2n} dans H (Théorème 5.2.8). Puisque r^2 est d'ordre n, $|\mathrm{H}| = 2n = |\mathrm{D}_{2n}|$; par conséquent $\mathrm{D}_{2n} \simeq \mathrm{H}$. Considérons $Z(\mathrm{D}_{2n}) = \{\mathrm{id}, r^n\}$ le centre de D_{2n}. Les éléments de H commutent avec les éléments de $Z(\mathrm{D}_{2n})$; ainsi la fonction $\varphi\colon \mathrm{H} \times Z(\mathrm{D}_{2n}) \to \mathrm{D}_{2n}$ définie par $\varphi(h, z) = hz$ est un morphisme. Puisque $n = 2\ell+1$ pour un certain entier ℓ, nous obtenons que $\varphi((r^2)^{-\ell}, r^n) = r^{n-2\ell} = r$ et $\varphi(s, 1) = s$; l'image de f contient donc $\langle r, s\rangle = \mathrm{D}_{2n}$. Il en résulte que φ est surjectif. L'égalité $|\mathrm{H}\times Z(\mathrm{D}_{2n})| = |\mathrm{D}_{2n}|$ assure que φ est également injectif et est donc un isomorphisme. □

La figure ci-dessous est une interprétation géométrique de l'isomorphisme $\mathrm{D}_6 \simeq \mathrm{D}_3 \times \mathbb{Z}/2\mathbb{Z}$:

Toute isométrie préservant le triangle bleu préserve également le triangle rouge et l'hexagone, et c'est ainsi que D_3 s'intègre naturellement dans D_6. Le groupe quotient $\mathrm{D}_6/\mathrm{D}_3$ est d'ordre 2 et il est représenté par l'élément non trivial de $\mathbb{Z}/2\mathbb{Z}$, qui correspond à l'élément non trivial du centre de D_6. Il s'agit d'une rotation d'angle π autour de l'origine, et les triangles équilatéraux bleu et rouge sont liés l'un à l'autre par une rotation d'angle π.

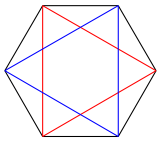


FIGURE 1. Deux triangles équilatéraux dans un hexagone régulier

Lorsque $2n \geq 6$ est divisible par 4, la conclusion du Corollaire 5.2.2 est fausse : $\mathrm{D}_{2n} \simeq \mathrm{D}_n \times \mathbb{Z}/2\mathbb{Z}$. En effet, puisque $2n$ et n sont pairs, le centre de D_{2n} est d'ordre 2 tandis que le centre de $\mathrm{D}_n \times \mathbb{Z}/2\mathbb{Z}$ est d'ordre $2 \times 2 = 4$. Puisque les groupes $Z(\mathrm{D}_{2n})$ et $Z(\mathrm{D}_n \times \mathbb{Z}/2\mathbb{Z})$ sont non isomorphes, les groupes sont non isomorphes.

Comme conséquence du Théorème 5.2.8 et de la Remarque 5.2.2, nous obtenons la description du groupe des automorphismes de D_{2n} comme groupe matriciel :

Théorème 5.2.9

Lorsque $n \geq 3$, nous avons l'isomorphisme

$$\mathrm{Aut}(\mathrm{D}_{2n}) \simeq \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times, b \in \mathbb{Z}/n\mathbb{Z} \right\}.$$

En particulier, l'ordre de $\mathrm{Aut}(\mathrm{D}_{2n})$ est $n\phi(n)$.

Démonstration. — Chaque automorphisme φ de D_{2n} est déterminé par les images de r et s. Puisque $\varphi(r)$ est d'ordre n et que tous les éléments de $\mathrm{D}_{2n} \smallsetminus \langle r \rangle$ sont d'ordre $2 < n$ nous avons nécessairement $\varphi(r) = r^a$ avec $\mathrm{pgcd}(a, n) = 1$; par suite $\varphi(\langle r \rangle) = \langle r \rangle$. En particulier, $\varphi(s)$ n'appartient pas à $\langle r \rangle$; autrement dit $\varphi(r) = r^a$, $\varphi(s) = r^b s$ pour un certain $a \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ et un certain $b \in \mathbb{Z}/n\mathbb{Z}$.

Réciproquement soient (a, b) un élément de $\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^\times, \mathbb{Z}/n\mathbb{Z}\right)$. D'après le Théorème 5.2.8 et la Remarque 5.2.2, pour montrer qu'il existe un unique automorphisme de D_{2n} qui envoie r sur r^a et s à $r^b s$ il suffit de montrer que

- $(r^a)^n = 1$,
- $(r^b)^2 = 1$,
- $(r^b s)(r^a)(r^b s)^{-1} = r^{-a}$.

La relation $(r^a)^n = 1$ découle de $r^n = 1$. La relation $(r^b s)^2 = 1$ découle du fait que tous les éléments de $\mathrm{D}_{2n} \smallsetminus \langle r \rangle$ sont d'ordre 2. La troisième relation découle de

$$(r^b s)(r^a)(r^b s)^{-1} = r^b \underbrace{s r^a}_{r^{-a} s} s^{-1} r^{-b} = r^b r^{-a} s s^{-1} r^{-b} = r^b r^{-a} r^{-b} = r^{-a}.$$

Le groupe $\mathrm{Aut}(\mathrm{D}_{2n})$ est donc paramétré par les couples (a,b) de $\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^\times, \mathbb{Z}/n\mathbb{Z}\right)$: pour tout $(a,b) \in \left(\left(\mathbb{Z}/n\mathbb{Z}\right)^\times, \mathbb{Z}/n\mathbb{Z}\right)$, il existe un unique $\varphi_{a,b} \in \mathrm{Aut}(\mathrm{D}_{2n})$ déterminé par les conditions $\varphi_{a,b}(r) = r^a$ et $\varphi_{a,b}(s) = r^b s$. Si $\varphi_{a,b}$ et $\varphi_{c,d}$ sont deux automorphismes de D_{2n} alors d'une part

$$(\varphi_{a,b} \circ \varphi_{c,d})(r) = \varphi_{a,b}(r^c) = (\varphi_{a,b(r)})^c = (r^a)^c = r^{ac}$$

et d'autre part

$$(\varphi_{a,b} \circ \varphi_{c,d})(s) = \varphi_{a,b}(r^d s) = (\varphi_{a,b}(r))^d \varphi_{a,b}(s) = r^{ad}(r^b s) = r^{ad+b} s;$$

ainsi $\varphi_{a,b} \circ \varphi_{c,d} = \varphi_{ac,ad+b}$. Puisque $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix}$, l'application

$$\mathrm{Aut}(\mathrm{D}_{2n}) \to \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times, b \in \mathbb{Z}/n\mathbb{Z} \right\}, \qquad \varphi_{a,b} \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

est un isomorphisme. □

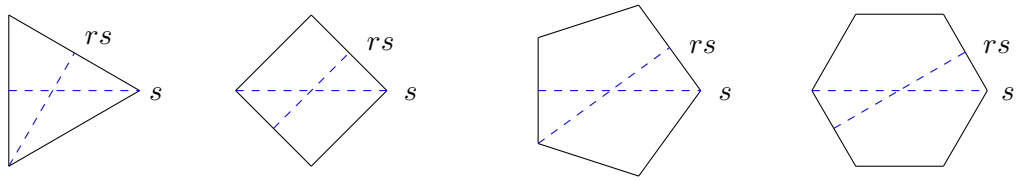
Corollaire 5.2.3

Pour chaque couple d'éléments g et h dans $\mathrm{D}_{2n} \smallsetminus \langle r \rangle$, il existe un unique automorphisme φ de D_{2n} tel que φ fixe $\langle r \rangle$ et envoie g sur h (*i.e.* $\varphi(g) = h$).

Démonstration. — Nous reprenons les notations de la démonstration du Théorème 5.2.9.

Chaque $\varphi \in \mathrm{Aut}(\mathrm{D}_{2n})$ est déterminé par $\varphi(r) = r^a$ et $\varphi(s) = r^b s$ où $a \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ et $b \in \mathbb{Z}/n\mathbb{Z}$. Remarquons que φ fixe $\langle r \rangle$ signifie $a \equiv_n 1$. Comment pouvons-nous obtenir $\varphi(g) = h$? Écrivons g sous la forme $r^i s$ et h sous la forme $r^j s$ pour certains i et j (uniques modulo n). Alors $\varphi(g) = \varphi(r)^i \varphi(s) = r^i r^b s = r^{i+b} s$, donc $\varphi(g) = h$ si et seulement si $r^{i+b} s = r^j s$, ou de manière équivalente $b \equiv_n j - i$. Par conséquent $\varphi_{1,j-i}$ fixe $\langle r \rangle$, envoie g sur h, et est le seul automorphisme de D_{2n} de ce type. □

5.2.6. Groupe diédral et sous-groupe engendré par des éléments d'ordre 2. — Puisque $\mathrm{D}_{2n} = \langle r, s \rangle = \langle rs, s \rangle$, le groupe D_{2n} est non seulement engendré par r et s mais aussi par les deux réflexions s et rs. Les réflexions s et rs fixent des droites séparées par un angle $\frac{2\pi}{2n}$, comme on peut le voir sur la figure suivante pour $3 \leq n \leq 6$:



Quels groupes finis distincts de D_{2n}, pour $2n \geq 3$, peuvent être engendrés par deux éléments d'ordre 2 ? Supposons $\mathrm{G} = \langle x, y\rangle$ avec $x^2 = e$ et $y^2 = e$. Si x et y commutent, alors $\mathrm{G} = \{e, x, y, xy\}$. Si x et y sont distincts, alors G est d'ordre 4 et G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (l'élément x correspond à $(1,0)$ et l'élément y à $(0,1)$). Si $x = y$, alors $\mathrm{G} = \{e, x\} = \langle x\rangle$ est cyclique d'ordre 2, *i.e.* isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Si x et y ne commutent pas, alors G est isomorphe à un groupe diédral :

Théorème 5.2.10

Soit G un groupe non abélien fini engendré par deux éléments d'ordre 2. Alors G est isomorphe à un groupe diédral.

Démonstration. — Notons x et y deux générateurs d'ordre 2 de G. Puisque G n'est pas abélien et que x et y engendrent G, x et y ne commutent pas, *i.e.* $xy \neq yx$.

Puisque G est d'ordre fini, xy est d'ordre fini. Notons n l'ordre de xy. Posons $a = xy$ et $b = y$. Alors $\mathrm{G} = \langle x, y\rangle = \langle xy, y\rangle$ est engendré par a et b, où $a^n = e$ et $b^2 = e$. Comme a est d'ordre n, n divise $|\mathrm{G}|$. Étant donné que b n'appartient pas à $\langle a\rangle$, nous avons $|\mathrm{G}| > n$ d'où $|\mathrm{G}| \geq 2n$.

Si $n \leq 2$ alors $a^2 = e$, donc $xyxy = e$; puisque x et y sont d'ordre 2, on obtient $xy = y^{-1}x^{-1} = yx$: contradiction avec le fait que x et y ne commutent pas. Par conséquent $n \geq 3$. À partir de (on rappelle que x et y sont d'ordre 2)

$$bab^{-1} = yxyy = yx, \qquad a^{-1} = y^{-1}x^{-1} = yx,$$

nous obtenons la relation : $bab^{-1} = a^{-1}$. Le Théorème 5.2.8 assure l'existence d'un morphisme surjectif de D_{2n} dans G ; il en résulte que $|\mathrm{G}| \leq 2n$.

Les inégalités $|\mathrm{G}| \geq 2n$ et $|\mathrm{G}| \leq 2n$ impliquent $|\mathrm{G}| = 2n$; finalement G est isomorphe à D_{2n}. □

Nous connaissons les groupes finis non abéliens engendrés par deux éléments d'ordre 2 (Théorème 5.2.10). Qu'en est-il des groupes abéliens finis engendrés par deux éléments d'ordre 2 ? Comme nous l'avons vu, un tel groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou (dans le cas dégénéré où les deux générateurs sont le même élément) à $\mathbb{Z}/2\mathbb{Z}$. On peut donc définir de nouveaux groupes diédraux d'ordre 2 et 4 : $\mathrm{D}_2 := \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{D}_4 := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En termes de générateurs, D_2 et D_4 sont définis comme suit : $\mathrm{D}_2 = \langle r, s\rangle$ où $r = e$ et s sont d'ordre 2 et $\mathrm{D}_4 = \langle r, s\rangle$ où r et s sont d'ordre 2 et commutent. Avec ces définitions,

- $|\mathrm{D}_{2n}| = 2n$ pour tout $n \geq 1$,
- les groupes diédraux sont précisément les groupes finis engendrés par deux éléments d'ordre 2,
- la description des commutateurs dans D_{2n} pour $n > 2$ est vraie pour $n \geq 1$

- ◇ si $n \geq 1$ est pair, le Corollaire 5.2.2 est vrai lorsque n est le double d'un nombre impair (ceci inclut le cas $n = 2$) et faux lorsque n est un multiple de 4,
- ◇ le modèle de D_{2n} en tant que sous-groupe de $\mathrm{GL}(2, \mathbb{R})$ lorsque $n \geq 3$ est valable pour tout $n \geq 1$.

Cependant, D_2 et D_4 ne satisfont pas toutes les propriétés de D_{2n} lorsque $n > 2$. Par exemple,

- ◇ D_{2n} n'est pas abélien pour $n > 2$ mais est abélien pour $n \leq 2$,
- ◇ la description de $Z(\mathrm{D}_{2n})$ lorsque $n > 2$ (trivial pour n impair et d'ordre 2 pour n pair) n'est pas valable lorsque $n \leq 2$; en effet $Z(\mathrm{D}_{2n}) = \mathrm{D}_{2n}$ est d'ordre 2 pour $n = 1$ et d'ordre 4 pour $n = 2$,
- ◇ le modèle matriciel de D_{2n} sur $\mathbb{Z}/n\mathbb{Z}$ dans (5.2.11) n'est pas valable lorsque $n \leq 2$,
- ◇ le modèle matriciel de $\mathrm{Aut}(\mathrm{D}_{2n})$ sur $\mathbb{Z}/n\mathbb{Z}$ du Théorème 5.2.9 n'est pas valable lorsque $n = 2$: $\mathrm{Aut}(\mathrm{D}_4) = \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est d'ordre $6 \neq 2\phi(2)$.

Remarque 5.2.3. — Ce qui précède ne se généralise pas : il n'existe pas de description élémentaire de tous les groupes finis engendrés par deux éléments d'ordre égal > 2 ou de tous les groupes finis engendrés par deux éléments d'ordre 2 et $n \geq 3$. De tels groupes peuvent être compliqués : la plupart des groupes simples finis sont engendrés par un couple d'éléments d'ordre 2 et 3.

Théorème 5.2.11

Les quotients non triviaux des groupes diédraux sont isomorphes aux groupes diédraux : si N est un sous-groupe distingué de D_{2n} d'indice $k > 1$, alors k est pair et $\mathrm{D}_{2n}/\mathrm{N} \simeq \mathrm{D}_k$.

Démonstration. — Le groupe $\mathrm{D}_{2n}/\mathrm{N}$ est engendré par $\overline{rs}$ et $\overline{s}$ qui sont donc d'ordre 1 ou 2. Notons qu'ils ne sont pas tous les deux triviaux puisque $\mathrm{D}_{2n}/\mathrm{N}$ est par hypothèse non trivial. Ainsi $\left|\mathrm{D}_{2n}/\mathrm{N}\right|$ est pair et k est pair.

Si $\overline{rs}$ et $\overline{s}$ sont tous deux d'ordre 2 alors $\mathrm{D}_{2n}/\mathrm{N}$ est isomorphe à

- ◇ D_k si $\mathrm{D}_{2n}/\mathrm{N}$ est non abélien (Théorème 5.2.10),
- ◇ $\mathbb{Z}/2\mathbb{Z} = \mathrm{D}_2$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \mathrm{D}_4$ si $\mathrm{D}_{2n}/\mathrm{N}$ est abélien.

Si $\overline{rs}$ ou $\overline{s}$ sont d'ordre 1 alors un seul d'entre eux est d'ordre 1 et $\mathrm{D}_{2n}/\mathrm{N}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} = \mathrm{D}_2$. □

Exemple 5.2.3. — Pour $n \geq 3$ pair, $Z(\mathrm{D}_{2n}) = \{\mathrm{id}, r^{n/2}\}$, donc $\mathrm{D}_{2n}/Z(\mathrm{D}_{2n})$ est d'ordre $\frac{2n}{2} = n = 2\,\frac{n}{2}$ et est engendré par les images $\overline{r}$ (d'ordre $\frac{n}{2}$ dans $\mathrm{D}_{2n}/Z(\mathrm{D}_{2n})$) et $\overline{s}$ (d'ordre 2), soumis à la relation $\overline{srs}^{-1} = \overline{r}^{-1}$. Nous en déduisons que $\mathrm{D}_{2n}/Z(\mathrm{D}_{2n})$ est isomorphe à D_n.

Lorsque $n \geq 3$ est impair, $Z(\mathrm{D}_{2n}) = \{\mathrm{id}\}$ donc l'isomorphisme ci-dessus se réécrit $\mathrm{D}_{2n}/Z(\mathrm{D}_{2n}) = \mathrm{D}_{2n}$.

Exemple 5.2.4. — Soit $n \geq 3$. Le groupe $[\mathrm{D}_{2n}, \mathrm{D}_{2n}]$ est $\langle r^2 \rangle$. Nous avons l'alternative suivante

- $[\mathrm{D}_{2n}, \mathrm{D}_{2n}] = \langle r \rangle$ si n est impair (car $\langle r^2 \rangle = \langle r \rangle$ si n est impair). Ainsi $\mathrm{D}_{2n}/[\mathrm{D}_{2n}, \mathrm{D}_{2n}]$ est d'ordre $\frac{2n}{n} = 2$ si n est impair ;
- $[\mathrm{D}_{2n}, \mathrm{D}_{2n}] = \langle r^2 \rangle \subsetneq \langle r \rangle$ si n est pair (car $\langle r^2 \rangle$ est un sous-groupe propre de $\langle r \rangle$ si n est pair). Ainsi $\mathrm{D}_{2n}/[\mathrm{D}_{2n}, \mathrm{D}_{2n}]$ est d'ordre $\frac{2n}{\frac{n}{2}} = 4$ pour n pair

Le groupe $\mathrm{D}_{2n}/[\mathrm{D}_{2n}, \mathrm{D}_{2n}]$ est abélien et engendré par $\overline{r}$ et l'élément $\overline{s}$ d'ordre 2. De plus

- si n est impair, $\overline{r}$ est trivial donc $\mathrm{D}_{2n}/[\mathrm{D}_{2n}, \mathrm{D}_{2n}] = \langle \overline{s} \rangle \simeq \mathbb{Z}/2\mathbb{Z} = \mathrm{D}_2$;
- si n est pair, $\overline{r}$ est d'ordre 2 et n'est pas égal à $\overline{s}$, donc $\mathrm{D}_{2n}/[\mathrm{D}_{2n}, \mathrm{D}_{2n}] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \mathrm{D}_4$.

5.2.7. Sous-groupes des groupes diédraux. — Nous allons déterminer les sous-groupes de D_{2n}. Nos résultats seront aussi valables pour $n = 1$ et $n = 2$. Rappelons que

- $\mathrm{D}_2 = \langle r, s \rangle$ où $r = \mathrm{id}$ et s est d'ordre 2,
- et $\mathrm{D}_4 = \langle r, s \rangle$ où r et s sont d'ordre 2 et commutent.

Théorème 5.2.12

Chaque sous-groupe de D_{2n} est cyclique ou diédral. Plus précisément, un sous-groupe de D_{2n} est de l'une des formes suivantes :

1. $\langle r^d \rangle$, avec $d \mid n$, d'indice $2d$,
2. $\langle r^d, r^i s \rangle$, avec $d \mid n$ et $0 \leq i \leq d-1$, d'indice d.

Chaque sous-groupe de D_{2n} apparaît exactement une fois dans cette liste.

Dans ce résultat, les sous-groupes du premier type sont cycliques et les sous-groupes du deuxième type sont diédraux : $\langle r^d \rangle \simeq \mathbb{Z}/(n/d)\mathbb{Z}$ et $\langle r^d, r^i s \rangle \simeq \mathrm{D}_{2n/d}$.

Démonstration. — Supposons $n \geq 3$ (les cas $n = 1$ et $n = 2$ sont laissés au lecteur). Soit H un sous-groupe de D_{2n}. Puisque $\langle r \rangle$ est cyclique d'ordre n, si H est contenu dans $\langle r \rangle$, alors $\mathrm{H} = \langle r^d \rangle$ où d désigne un diviseur (strictement positif) de n. Le sous-groupe $\langle r^d \rangle$ est d'ordre $\frac{n}{d}$ et d'indice $\frac{2n}{\frac{n}{d}} = 2d$. Supposons désormais que H n'est pas contenu dans $\langle r \rangle$. Il s'en suit que H contient un élément de la forme $z^i s$. L'intersection $\mathrm{H} \cap \langle r \rangle$ est un sous-groupe de $\langle r \rangle$; ainsi $\mathrm{H} \cap \langle r \rangle = \langle r^d \rangle$ pour un certain diviseur d (strictement positif) de n.

- Considérons le cas $s \in \mathrm{H}$. Montrons qu'alors $\mathrm{H} = \langle r^d, s \rangle$. Comme r^d et s appartiennent à h, $\langle r^d, s \rangle$ est contenu dans H. Soit h un élément de H. Si h appartient à $\langle r \rangle$, alors h appartient à $\mathrm{H} \cap \langle r \rangle = \langle r^d \rangle \subset \langle r^d, s \rangle$. Si h n'appartient pas à $\langle r \rangle$, alors h est de la forme $r^i s$

pour un certain i. Puisque s est un élément de H nous obtenons que $hs^{-1} = r^i \in \mathrm{H} \cap \langle r \rangle$. Autrement dit $r^i = r^{dk}$ pour un certain k. Il en résulte que

$$h = r^i s = r^{dk} s = (r^d)^k s$$

appartient à $\langle r^d, s \rangle$. Finalement $\mathrm{H} \subset \langle r^d, s \rangle$.

- ◇ Le groupe H contient un élément de la forme $r^i s$. Puisque s et $r^i s$ ne sont pas des éléments de $\langle r \rangle$ il existe d'après le Corollaire 5.2.3 un automorphisme φ de D_{2n} tel que $\varphi(r) = r$ et $\varphi(r^i s) = s$. Il s'en suit que $\varphi(\mathrm{H})$ est un sous-groupe de D_{2n} qui contient s. D'après ce qui précède $\varphi(\mathrm{H}) = \langle r^d, s \rangle$ pour un certain diviseur (strictement positif) d de n. Par conséquent $\mathrm{H} = \varphi^{-1}(\langle r^d, s \rangle) = \langle \varphi^{-1}(r^d), \varphi^{-1}(s) \rangle = \langle r^d, r^i s \rangle$. Comme $\langle r^d, r^i s \rangle = \langle r^d, r^j s \rangle$ lorsque $j \equiv_d i$ on peut ajuster i mod d sans affecter $\langle r^d, r^i s \rangle$ de sorte que $h = \langle r^d, r^i s \rangle$ avec $0 \leq i \leq d-1$.

Quel est l'indice de $\langle r^d, r^i s \rangle$ dans D_{2n} (où d désigne un diviseur strictement positif de n) ? Puisque $r^i s$ est d'ordre 2 et puisque $(r^i s) r^k = r^{-k}(r^i s)$ tous les éléments de $\langle r^d, r^i s \rangle$ qui ne sont pas des puissances de r sont de la forme $(r^d)^\ell (r^i s) = r^{d\ell} r^i s$. Par suite $\mathrm{H} = \langle r^d, r^i s \rangle = \langle r^d \rangle \sqcup \langle r^d \rangle r^i s$; nous en déduisons que $|\mathrm{H}| = 2|\langle r^d \rangle| = 2\frac{n}{d}$. Ainsi $[\mathrm{D}_{2n} : \mathrm{H}] = \frac{2n}{2\frac{n}{d}} = d$.

Il reste à montrer que la liste de l'énoncé n'est pas redondante. Commençons par montrer que la liste des groupes apparaissant dans 1. est disjointe de la liste des groupes apparaissant dans 2. Tout élément de $\langle r^d \rangle$ commute avec r alors que le groupe $\langle r^d, r^i s \rangle$ contient $r^i s$ qui ne commute pas avec r. Il en résulte que la liste des groupes apparaissant dans 1. est disjointe de la liste des groupes apparaissant dans 2.

La liste des groupes apparaissant dans 1. n'est pas redondante car $\langle r^d \rangle$ est caractérisé par d (diviseur strictement positif de n) ; en effet $\langle r^d \rangle$ est d'indice $2d$ dans D_{2n}.

Montrons que la liste des groupes apparaissant dans 2. n'est pas redondante. Si deux groupes apparaissant dans 2. sont égaux, alors ils sont de même indice d dans D_{2n} ; autrement dit ils sont de la forme $\langle r^d, r^i s \rangle$ et $\langle r^d, r^j s \rangle$ avec $0 \leq i, j \leq d-1$. En particulier $r^j s$ appartient à $\langle r^d, r^i s \rangle = \langle r^d \rangle \sqcup \langle r^d \rangle r^i s$ et $r^j s$ s'écrit $r^{dk+i} s$ pour un certain $k \in \mathbb{Z}$. Par conséquent $j \equiv_n dk+i$. Puisque d divise n nous nous ramenons à $j \equiv_n i$. Il en résulte que $j = 1$ puisque $0 \leq i, j \leq d-1$. □

Corollaire 5.2.4

1. Supposons que n soit impair et que k divise $2n$.
   Si k est impair, alors D_{2n} contient k sous-groupes d'indice k.
   Si k est pair, alors D_{2n} contient un sous-groupe d'indice k.
2. Supposons que n soit pair et que k divise $2n$.
   - ⋄ Si k est impair, alors D_{2n} contient m sous-groupes d'indice k.
   - ⋄ Si k est pair et k ne divise pas n alors D_{2n} contient un sous-groupe d'indice k.
   - ⋄ Si k est pair et k divise n, alors D_{2n} contient $k+1$ sous-groupes d'indice k.

Démonstration. — Supposons $n \geq 3$ (les cas $n = 1$ et $n = 2$ sont laissés au lecteur).

1. Si n est impair, alors les diviseurs impairs de $2n$ sont les diviseurs de n et les diviseurs pairs de $2n$ sont de la forme $2d$ avec $d \,|\, n$. Le Théorème 5.2.12 assure que chaque sous-groupe de D_{2n} d'indice impair est diédral et chaque sous-groupe de D_{2n} d'indice pair est contenu dans $\langle r \rangle$. Un sous-groupe d'indice impair k est de la forme $\langle r^k, r^i s \rangle$ pour un unique $0 \leq i \leq k-1$; il y a k tels groupes. Un sous-groupe d'indice pair k est $\langle r^{k/\ell} \rangle$ d'après le Théorème 5.2.12.

2. Si n est pair et k est un diviseur impair de $2n$, alors k divise n et les sous-groupes de D_{2n} d'indice k sont les $\langle r^k, r^i s \rangle$ avec $0 \leq i \leq k-1$.

   Si n est pair et k un diviseur pair de $2n$, alors $\frac{k}{2}$ divise n et $\langle r^{k/2} \rangle$ est un sous-groupe d'indice k de D_{2n}. Si k ne divise pas n, c'est l'unique sous-groupe d'indice k de D_{2n} ; si k divise n, les autres sous-groupes d'indice k sont du type $\langle r^k, r^i s \rangle$ avec $0 \leq i \leq m-1$.

□

Théorème 5.2.13

1. Supposons que n soit impair et que k divise $2n$.

   Si k est impair, alors les k sous-groupes de D_{2n} d'indice k sont conjugués à $\langle r^k,\, s\rangle$.

   Si k est pair, alors l'unique sous-groupe de D_{2n} d'indice k est $\langle r^{k/2}\rangle$.

   En particulier, tous les sous-groupes de D_{2n} ayant le même indice sont conjugués les uns aux autres.

2. Supposons que n soit pair et que k divise $2n$.

   Si k est impair alors les k sous-groupes de D_{2n} d'indice k sont conjugués à $\langle r^k,\, s\rangle$.

   Si k est pair et k ne divise pas n alors l'unique sous-groupe de D_{2n} d'indice k est $\langle r^{k/2}\rangle$.

   Si k est pair et k divise n, alors tout sous-groupe de D_{2n} d'indice k est $\langle r^{k/2}\rangle$ ou est conjugué à exactement l'un de $\langle r^k,\, s\rangle$ ou $\langle r^k,\, rs\rangle$.

   En particulier, le nombre de classes de conjugaison des sous-groupes de D_{2n} d'indice k est 1 lorsque m est impair, 1 lorsque k est pair et k ne divise pas n, et 3 lorsque k est pair et k divise n.

Démonstration. — Supposons que $n \geq 3$ (les cas $n = 1$ et $n = 2$ sont laissés au lecteur).

- Si n et k sont impairs, alors k divise n et un sous-groupe de D_{2n} d'indice k est de la forme $\langle r^k,\, r^i s\rangle$. Puisque n est impair, $r^i s$ est conjugué à s dans D_{2n}. Les seuls conjugués de r^m dans D_{2n} sont r^m et r^{-m}. De plus, une conjugaison qui envoie s sur $r^i s$ envoie $\langle r^m,\, s\rangle$ sur $\langle r^{\pm m},\, r^i s\rangle = \langle r^m,\, r^i s\rangle$.
- Si n est impair et m pair, alors le Théorème 5.2.12 assure que l'unique sous-groupe d'indice pair m est $\langle r^{m/2}\rangle$.
- Si n est pair et m un diviseur impair de $2n$, alors m divise n et un sous-groupe de D_{2n} d'indice m est de la forme $\langle r^m,\, r^i s\rangle$ avec $0 \leq i \leq m-1$. Comme $r^i s$ est conjugué à rs ou s (suivant la parité de i) et les seuls conjugués de r^m sont r^m et r^{-m}, le groupe $\langle r^m,\, r^i s\rangle$ est conjugué à $\langle r^m,\, s\rangle$ ou $\langle r^m, rs\rangle$.
- Si m est un diviseur pair de $2n$, alors $\frac{m}{2}$ divise n. D'après le Théorème 5.2.12 le groupe $\langle r^{m/2}\rangle$ est d'indice m dans D_{2n}. Tout autre sous-groupe d'indice m est $\langle r^m,\, r^i s\rangle$ pour un certain i ; ceci n'arrive que si m divise n auquel cas $\langle r^m,\, r^i s\rangle$ est conjugué à $\langle r^m,\, s\rangle$ ou à $\langle r^m,\, rs\rangle$. Il reste à montrer que $\langle r^m,\, s\rangle$ et $\langle r^m,\, rs\rangle$ ne sont pas conjugués dans D_{2n}. Comme m est pair les réflexions de $\langle r^m,\, s\rangle$ sont de la forme $r^i s$ avec i pair alors que les réflexions de $\langle r^m,\, rs\rangle$ sont de la forme $r^i s$ avec i impair. Ainsi les conjugués des réflexions de $\langle r^m,\, s\rangle$ n'appartiennent pas à $\langle r^m,\, rs\rangle$. En particulier, $\langle r^m,\, s\rangle$ et $\langle r^m,\, rs\rangle$ ne sont pas conjugués dans D_{2n}

□

Exemple 5.2.5. — Les sous-groupes d'indice 2 de D_{12} sont $\langle r\rangle$, $\langle r^2,\, s\rangle$ et $\langle r^2,\, rs\rangle$; ils ne sont pas conjugués.

À conjugaison près D_{12} compte un seul sous-groupe d'indice 3, le groupe $\langle r^3,\, s\rangle$.

Le groupe D_{12} compte un seul sous-groupe d'indice 4, le groupe $\langle r^2\rangle$.

Soit G un sous-groupe d'indice 6 de D_{12} ; alors $G = \langle r^3\rangle$ ou G coïncide, à conjugaison près, avec $\langle s\rangle$ ou $\langle rs\rangle$; ils ne sont pas conjugués.

Exemple 5.2.6. — Les sous-groupes d'indice 2 de D_{20} sont $\langle r\rangle$, $\langle r^2,\, s\rangle$ et $\langle r^2, rs\rangle$, qui sont non conjugués.

L'unique sous-groupe de D_{20} d'indice 4 est $\langle r^2\rangle$.

Les cinq sous-groupes d'indice 5 sont conjugués à $\langle r^5,\, s\rangle$.

Soit G un sous-groupe d'indice 10 de D_{20}. Alors $G = \langle r^5\rangle$ ou G est conjugué à l'un des deux groupes suivants : $\langle r^{10},\, s\rangle$, $\langle r^{10},\, rs\rangle$.

Exemple 5.2.7. — Soit $k \geq 3$ un entier. Le groupe diédral $D_{2^{k+1}}$ possède trois classes de conjugaison de sous-groupes d'indice 2, resp. 4, ..., resp. $2k-1$.

Nous classifions maintenant les sous-groupes distingués de D_{2n} (nous n'utilisons pas notre liste de sous-groupes de D_{2n}, ni notre liste de classes de conjugaison de sous-groupes de D_{2n}).

Théorème 5.2.14

Tout sous-groupe de $\langle r\rangle$ est un sous-groupe distingué de D_{2n}. Ce sont les $\langle r^d\rangle$ pour $d|n$; ils sont d'indice $2d$.
Si n est impair, les sous-groupes distingués propres de D_{2n} sont les $\langle r^d\rangle$ pour $d|n$.
Si n est pair, les sous-groupes distingués propres de D_{2n} sont les

- ◇ $\langle r^d\rangle$ pour $d|n$;
- ◇ $\langle r^2,\, s\rangle$ et $\langle r^2,\, rs\rangle$ d'indice 2.

En particulier, il y a au plus un sous-groupe distingué par indice $d \neq 2$ dans D_{2n} sauf trois sous-groupes distingués $\langle r\rangle$, $\langle r^2,\, s\rangle$ et $\langle r^2,\, rs\rangle$ d'indice 2.

Démonstration. — Supposons que $n \geq 3$ (les cas $n = 1$ et $n = 2$ sont laissés au lecteur).

- ◇ Puisque $\langle r\rangle$ est un sous-groupe cyclique distingué de D_{2n}
  - d'une part tous les sous-groupes de $\langle r\rangle$ sont distingués dans D_{2n},
  - d'autre part tous les sous-groupes de $\langle r\rangle$ sont de la forme $\langle r^d\rangle$ avec $d\ vert\, n$.
- ◇ Intéressons-nous désormais aux sous-groupes distingués propres de D_{2n} qui ne sont pas contenus dans D_{2n} ; ils contiennent nécessairement une réflexion.

- Supposons dans un premier temps que n est impair. Toutes les réflexions de D_{2n} sont conjuguées ; par conséquent un sous-groupe distingué G de D_{2n} contenant une réflexion les contient toutes. En particulier $|\mathrm{G}| \geq \frac{|\mathrm{D}_{2n}|}{2}$. De plus G contient id. Par suite $|\mathrm{G}| \geq \frac{|\mathrm{D}_{2n}|}{2} + 1$; il en résulte que $\mathrm{G} = \mathrm{D}_{2n}$. Ainsi tout sous-groupe distingué propre de D_{2n} est contenu dans $\langle r \rangle$ lorsque n est impair.
- Supposons maintenant que n est pair. Les réflexions de D_{2n} sont réparties en deux classes de conjugaison d'ordre $\frac{n}{2}$ représentées par r et rs. Ainsi un sous-groupe distingué propre G de D_{2n} qui contient une réflexion contient ou bien $\frac{n}{2}$ réflexions, ou bien toutes les réflexions. Comme on vient de le voir si G contient toutes les réflexions, alors $\mathrm{G} = \mathrm{D}_{2n}$: contradiction avec le fait que G soit propre. Donc G contient $\frac{n}{2}$ réflexions. Étant donné que G contient aussi e, nous avons $|\mathrm{G}| > \frac{n}{2}$ et $[\mathrm{D}_{2n} : \mathrm{G}] < \frac{2n}{\frac{n}{2}} = 4$. De plus une réflexion de $\mathrm{D}_{2n} \smallsetminus \mathrm{G}$ est d'ordre 2 dans $\mathrm{D}_{2n}/\mathrm{G}$ d'où $[\mathrm{D}_{2n} : \mathrm{G}]$ est pair. Il s'en suit que $[\mathrm{D}_{2n} : \mathrm{G}] = 2$.

  Réciproquement tout sous-groupe de D_{2n} d'indice 2 est distingué dans D_{2n}. Puisque $\left|\mathrm{D}_{2n}/\mathrm{G}\right| = 2$, nous avons : $r^2 \in \mathrm{G}$. Le sous-groupe $\langle r^2 \rangle$ de D_{2n} est d'indice 4 et distingué dans D_{2n}. Par conséquent les sous-groupes d'indice 2 de D_{2n} sont obtenus en prenant l'image réciproque dans D_{2n} des sous-groupes d'indice 2 dans $\mathrm{D}_{2n}/\langle r^2 \rangle = \{\overline{id}, \overline{r}, \overline{s}, \overline{rs}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$:
  - — l'image réciproque de $\{\overline{\mathrm{id}}, \overline{r}\}$ est $\langle r \rangle$;
  - — l'image réciproque de $\{\overline{\mathrm{id}}, \overline{s}\}$ est $\langle r^2, s \rangle$;
  - — l'image réciproque de $\{\overline{\mathrm{id}}, \overline{rs}\}$ est $\langle r^2, rs \rangle$.

□

Exemple 5.2.8. — Soit p un premier impair. L'unique sous-groupe distingué propre non trivial de D_{2p} est $\langle r \rangle$ qui est d'indice 2.

Exemple 5.2.9. — Les sous-groupes distingués d'indice 2 de D_{12} sont $\langle r \rangle$, $\langle r^2, s \rangle$ et $\langle r^2, s \rangle$ et $\langle r^2, rs \rangle$. L'unique sous-groupe distingué d'indice 4 de D_{12} est $\langle r^2 \rangle$. L'unique sous-groupe distingué d'indice 6 de D_{12} est $\langle r^3 \rangle$. Il n'existe pas de sous-groupe distingué d'indice 3 dans D_{10}.

Exemple 5.2.10. — Les sous-groupes distingués d'indice 2 de D_{20} sont : $\langle r \rangle$, $\langle r^2, s \rangle$ et $\langle r^2, rs \rangle$.

L'unique sous-groupe distingué d'indice 4 de D_{20} est $\langle r^2 \rangle$. L'unique sous-groupe distingué d'indice 10 de D_{20} est $\langle r^5 \rangle$.

Enfin, il n'existe pas de sous-groupe distingué d'indice 5 de D_{20}.

Exemple 5.2.11. — Lorsque $k \geq 3$, le groupe diédral D_{4k} possède

- ◇ trois sous-groupes distingués d'indice 2,
- ◇ un sous-groupe distingué de chaque indice d distinct de 2.

Les sous-groupes distingués « exceptionnels » $\langle r^2, s\rangle$ et $\langle r^2, rs\rangle$ dans D_{2n} pour $n \geq 4$ pair peuvent être réalisés comme noyaux de morphismes explicites $\mathrm{D}_{2n} \to \mathbb{Z}/2\mathbb{Z}$. Dans $\mathrm{D}_{2n}/\langle r^2, s\rangle$ nous avons $r^2 = e$ et $s = e$, donc $r^a s^b = r^a$ et notons que seul a modulo 2 importe. Dans $\mathrm{D}_{2n}/\langle r^2, rs\rangle$ nous avons $r^2 = e$ et $s = r^{-1} = r$, donc $r^a s^b = r^{a+b}$ et notons que seul $a + b$ modulo 2 importe. Considérons donc les deux morphismes

$$\mathrm{D}_{2n} \to \mathbb{Z}/2\mathbb{Z}, \quad r^a s^b \mapsto a \bmod 2 \qquad\qquad \mathrm{D}_{2n} \to \mathbb{Z}/2\mathbb{Z}, \quad r^a s^b \mapsto a + b \bmod 2$$

Ces fonctions sont bien définis puisque n est pair et leurs noyaux respectifs sont $\langle r^2, s\rangle$ et $\langle r^2, rs\rangle$.

5.2.8. Classes de conjugaison et normalisateurs des sous-groupes de D_{2n}. —

5.2.8.1. *Classes de conjugaison des sous-groupes de* D_{2n}. — Les classes de conjugaison des sous-groupes de $\langle r\rangle$ sont des singletons puisque ces sous-groupes sont distingués dans D_{2n}. Intéressons-nous désormais aux classes des sous-groupes de D_{2n} contenant une réflexion. Pour tous diviseur d de n et entier $0 \leq k \leq d-1$ posons $\mathrm{H}_{d,k} = \langle r^d, r^k s\rangle$. Les $\mathrm{H}_{d,k}$ sont les sous-groupes de D_{2n} contenant une réflexion. Si deux groupes $\mathrm{H}_{d,j}$ et $\mathrm{H}_{d',k}$ sont conjugués alors $|\mathrm{H}_{d,j}| = |\mathrm{H}_{d',k}|$, soit $\frac{2n}{d} = \frac{2n}{d'}$ et $d = d'$.

- ◇ Supposons dans un premier temps que n soit impair. Puisque d'une part deux réflexions quelconques sont conjuguées dans D_{2n} et d'autre part si f appartient à D_{2n} alors
$$f r^d f^{-1} \in \{r^d, r^{-d}\}$$
les groupes $\mathrm{H}_{d,j} = \langle r^d, r^j s\rangle$ et $\mathrm{H}_{d,k} = \langle r^d, r^k s\rangle$ sont conjugués.
- ◇ Supposons dans un second temps que n soit pair.
  - — Si j et k ont même parité alors comme dans le cas précédent $\mathrm{H}_{d,j}$ et $\mathrm{H}_{d,k}$ sont conjugués.
  - — Supposons finalement que k et j soient de parités différentes. Les groupes $\mathrm{H}_{d,j}$ et $\mathrm{H}_{d,k}$ sont conjugués si et seulement si $r^j s$ est le conjugué d'une réflexion de $\mathrm{H}_{d,k}$, autrement dit si et seulement s'il existe $g \in \mathrm{D}_{2n}$ et $m \in \mathbb{Z}$ tels que
$$r^j s = g(r^{md} r^k s)g^{-1}$$
c'est-à-dire si et seulement s'il existe $m \in \mathbb{Z}$ tel que j et $md + k$ ont même parité. Si d est pair, alors c'est impossible. Si d est impair, alors $r^j s$ et $r^{k+d} s$ sont conjugués et $\mathrm{H}_{d,j}$ et $\mathrm{H}_{d,k}$ sont conjugués.

5.2.8.2. *Normalisateurs des sous-groupes de* D_{2n}. — Si H est un sous-groupe de $\langle r\rangle$, alors H est un sous-groupe distingué de D_{2n} et donc $\mathrm{N}_{\mathrm{D}_{2n}}(\mathrm{H}) = \mathrm{D}_{2n}$.

Supposons que H soit un sous-groupe de D_{2n} non contenu dans $\langle r\rangle$; alors H contient une réflexion et

$$\mathrm{H} = \mathrm{H}_{d,k} = \langle r^d, r^k s\rangle$$

où d désigne un diviseur de n et $0 \leq k \leq d-1$. Si C_{H} désigne l'ensemble des conjugués de H, alors $|\mathrm{N}_{\mathrm{D}_{2n}}(\mathrm{H})| = \frac{|\mathrm{D}_{2n}|}{|C_{\mathrm{H}}|}$.

- ◇ Supposons dans un premier temps que n soit impair. Nous avons vu que les d sous-groupes $\mathrm{H}_{d,i}$, où $0 \leq i \leq d-1$, forment une classe de conjugaison de sous-groupes de D_{2n} de sorte que $|\mathrm{N}_{\mathrm{D}_{2n}}(\mathrm{H})| = \frac{|\mathrm{D}_{2n}|}{|C_{\mathrm{H}}|} = \frac{2n}{d}$. Étant donnés que $|\mathrm{H}| = \frac{2n}{d}$ et que $\mathrm{H} \subseteq \mathrm{N}_{\mathrm{D}_{2n}}(\mathrm{H})$ nous avons $\mathrm{N}_{\mathrm{D}_{2n}}(\mathrm{H}) = \mathrm{H}$.

- ◇ Supposons pour finir que n soit pair.

  - Si d est impair, alors un raisonnement analogue au précédent assure que $\mathrm{N}_{\mathrm{D}_{2n}}(\mathrm{H}) = \mathrm{H}$.

  - Si d est pair, alors écrivons-le sous la forme 2δ. Les sous-groupes $\mathrm{H}_{d,i}$ où i parcourt $\{0, 1, \ldots, d-1\}$ forment deux classes de conjugaison :

    $$\{\mathrm{H}_{d,0}, \mathrm{H}_{d,2}, \ldots, \mathrm{H}_{d,2(\delta-1)}\}, \qquad \{\mathrm{H}_{d,1}, \mathrm{H}_{d,3}, \ldots, \mathrm{H}_{d,2\delta-1}\}.$$

    Ainsi $|\mathrm{N}_{\mathrm{D}_{2n}}(\mathrm{H})| = \frac{|\mathrm{D}_{2n}|}{|C_{\mathrm{H}}|} = \frac{2n}{d/2} = \frac{4n}{d}$. Puisque $\mathrm{N}_{\mathrm{D}_{2n}}(\mathrm{H})$ contient la réflexion $r^k s$ de H le sous-groupe $\mathrm{N}_{\mathrm{D}_{2n}}(\mathrm{H})$ est un groupe diédral $\mathrm{D}_{2n/\delta}$; il contient une rotation d'ordre $\frac{n}{\delta}$, par exemple r^δ. Il en résulte que

    $$\mathrm{N}_{\mathrm{D}_{2n}}(\mathrm{H}) = \langle r^\delta, r^k s\rangle = N_{\delta,k}.$$

    Nous retrouvons en particulier que

    $$\mathrm{H}_{d,k} \lhd \mathrm{D}_{2n} \Longleftrightarrow 4\frac{n}{d} = 2n \Longleftrightarrow d = 2 \text{ et } 0 \leq k \leq 1.$$

Résumons les résultats précédents :

D_{2n}, $n = 2m+1$				
sous-groupe	ordre	quotient si distingué	classe de conjugaison	normalisateur
$\langle r^d\rangle$, $d \mid n$	$\frac{n}{d}$	$\mathrm{D}_{2\delta}$	$\langle r^d\rangle$	D_{2n}
$\langle r^d, r^k s\rangle$, $d \mid n$ $d > 1$, $0 \leq k \leq d-1$	$\frac{2n}{d}$		$\langle r^d, r^i s\rangle$ $0 \leq i \leq d-1$	$\langle r^d, r^k s\rangle$
$\mathrm{G} = \langle r, s\rangle$	$2n$	$\{\mathrm{id}\}$	D_{2n}	D_{2n}

D_{2n}, $n = 2m$				
sous-groupe	ordre	quotient si distingué	classe de conjugaison	normalisateur
$\langle r^d \rangle$, $d \mid n$	$\frac{n}{d}$	$\mathrm{D}_{2\delta}$	$\langle r^d \rangle$	D_{2n}
$\langle r^2, s \rangle$	n	$\mathbb{Z}/2\mathbb{Z}$	$\langle r^2, s \rangle$	D_{2n}
$\langle r^2, rs \rangle$	n	$\mathbb{Z}/2\mathbb{Z}$	$\langle r^2, rs \rangle$	D_{2n}
$\langle r^d, r^k s \rangle$, $d \mid n$ $d > 2$ pair, $0 \leq k \leq d-1$	$\frac{2n}{d}$		$\langle r^d, r^i s \rangle$ $0 \leq i \leq d-1$, $i \equiv_2 k$	$\langle r^{d/2}, r^k s \rangle$
$\langle r^d, r^k s \rangle$, $d \mid n$ $d > 1$ impair, $0 \leq k \leq d-1$	$\frac{2n}{d}$		$\langle r^d, r^i s \rangle$ $0 \leq i \leq d-1$	$\langle r^d, r^k s \rangle$
$\mathrm{G} = \langle r, s \rangle$	$2n$	$\{\mathrm{id}\}$	D_{2n}	D_{2n}

5.2.9. Un groupe diédral infini. — Dans le Théorème 5.2.10, le groupe est supposé fini ; cette hypothèse est utilisée dans la démonstration pour s'assurer que xy est d'ordre fini. Il est raisonnable de se demander si l'hypothèse de finitude peut être supprimée : un groupe non abélien engendré par deux éléments d'ordre 2 pourrait-il vraiment être infini ? Oui ! Dans ce paragraphe d'une part nous construisons un tel groupe et d'autre part nous montrons qu'il n'existe un unique groupe à isomorphisme près.

Considérons l'ensemble $\mathrm{Aff}(\mathbb{Z}) = \{x \mapsto ax + b \,|\, a \in \{-1, 1\},\, b \in \mathbb{Z}\}$; muni de la composition c'est un groupe appelé *groupe affine sur* $\mathbb{Z}$. Par exemple, l'inverse de $-x$ est lui-même et l'inverse de $x + 7$ est $x - 7$. Ce groupe est appelé groupe affine sur $\mathbb{Z}$ et est noté $\mathrm{Aff}(\mathbb{Z})$.

Puisque les fonctions de la forme $ax + b$ se composent de la même manière que les matrices de la forme $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ se multiplient ; nous pouvons donc considérer de telles matrices, avec $a = \pm 1$ et $b \in \mathbb{Z}$, comme un autre modèle pour le groupe $\mathrm{Aff}(\mathbb{Z})$.

Nous adopterons ce modèle matriciel pour la raison pratique suivante : il est plus simple d'écrire des produits et des puissances de matrices que des compositions de fonctions.

Théorème 5.2.15

Le groupe $\mathrm{Aff}(\mathbb{Z})$ est engendré par $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Autrement dit le groupe $\mathrm{Aff}(\mathbb{Z})$ est engendré par $x \mapsto -x$ et $x \mapsto x + 1$.

Démonstration. — Les éléments de $\mathrm{Aff}(\mathbb{Z})$ sont de la forme

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k$$

ou encore

$$\begin{pmatrix} -1 & \ell \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \ell \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\ell}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

□

Alors que $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ est d'ordre 2, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini. Néanmoins le groupe $\mathrm{Aff}(\mathbb{Z})$ est aussi engendré par deux éléments d'ordre 2 :

Corollaire 5.2.5

Le groupe $\mathrm{Aff}(\mathbb{Z})$ est engendré par $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$, qui sont chacun d'ordre 2.

Démonstration. — On peut vérifier que $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$ est d'ordre 2. D'après le Théorème 5.2.15, il suffit maintenant de montrer $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ s'écrit à l'aide de $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$. Cela découle du fait que : $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. □

Corollaire 5.2.6

Les matrices $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$ ne sont pas conjuguées dans $\mathrm{Aff}(\mathbb{Z})$.

Les matrices $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$ ne commutent pas avec un élément commun d'ordre 2 dans $\mathrm{Aff}(\mathbb{Z})$.

Démonstration. — Tout conjugué de $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ dans $\mathrm{Aff}(\mathbb{Z})$ est de la forme $\begin{pmatrix} -1 & 2b \\ 0 & 1 \end{pmatrix}$ pour $b \in \mathbb{Z}$ et $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$ n'est pas de cette forme. Les matrices $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$

ne sont donc pas conjuguées. Le centralisateur de $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ dans $\mathrm{Aff}(\mathbb{Z})$ est $\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \rangle = \left\{ \mathrm{id}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. □

Le Corollaire 5.2.5 montre que $\mathrm{Aff}(\mathbb{Z})$ est un exemple de groupe infini engendré par deux éléments d'ordre 2. Existe-t-il d'autres groupes de ce type, non isomorphes à $\mathrm{Aff}(\mathbb{Z})$? L'énoncé suivant fournit la réponse à cette question :

Théorème 5.2.16

Tout groupe infini engendré par deux éléments d'ordre 2 est isomorphe à $\mathrm{Aff}(\mathbb{Z})$.

Démonstration. — Notons G un tel groupe et x, y ses deux générateurs d'ordre 2. Puisque G est infini, x et y ne commutent pas (en effet, si x et y commutent, alors $\mathrm{G} = \langle x, y \rangle = \{e, x, y, xy\}$ est d'ordre 4). Puisque $x^{-1} = x$ et $y^{-1} = y$, nous avons : $x^n = y^n = e$ si n est pair et $x^n = x$, $y^n = y$ si n est impair. Les éléments de G sont donc des mots en x et y, telles que $xyyxxyxyxyxyxyxxy$. Les relations $x^2 = e$ et $y^2 = e$ impliquent que $xyyxxyxyxyxyxyxxy$ peut être simplifié en $xyxyxyxyx = (xy)^4x$. De plus, l'inverse d'un tel mot est à nouveau un mot en x et y.

Il existe donc quatre types d'éléments dans G :

$$(xy)^k, \quad (yx)^k, \quad (xy)^k x, \quad (yx)^k y, \tag{5.2.12}$$

où k désigne un entier non négatif.

Avant d'examiner plus en détail ces produits, indiquons comment va s'effectuer la correspondance entre G et $\mathrm{Aff}(\mathbb{Z})$. Nous aimerions identifier x avec $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et y avec $\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$. Le produit xy correspondrait donc à $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Notons qu'il n'y a pas de contradiction au niveau de l'ordre. D'une part $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini. D'autre part xy est lui d'ordre infini ; en effet, si xy est d'ordre fini, alors d'après la démontration du Théorème 5.2.10 le groupe $\mathrm{G} = \langle x, y \rangle$ est fini.

Un élément de $\mathrm{Aff}(\mathbb{Z})$ est de la forme $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k$ ou $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ avec $k \in \mathbb{Z}$ (Théorème 5.2.15). Cela suggère que chaque élément de G a la forme $(xy)^k$ ou $(xy)^k x$. C'est ce que nous allons démontrer. Soit $z = xy$; alors $z^{-1} = y^{-1}x^{-1} = yx$ et $xzx^{-1} = yx$, d'où

$$xzx^{-1} = z^{-1}. \tag{5.2.13}$$

De plus $z^{-k}y = z^{-k}yxx = z^{-k-1}x$ les éléments de (5.2.12) sont donc de la forme z^k ou z^kx avec $k \in \mathbb{Z}$.

Considérons donc $\varphi\colon \mathrm{Aff}(\mathbb{Z}) \to \mathrm{G}$ défini par

$$\varphi\left(\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\right) = z^k, \qquad \varphi\left(\begin{pmatrix} -1 & \ell \\ 0 & 1 \end{pmatrix}\right) = z^\ell x.$$

La fonction φ est surjective car tout élément de G est de la forme z^k ou z^kx. La fonction φ est injective ; en effet, z étant d'ordre infini, aucune puissance de z n'est égale à x, qui est d'ordre 2. On peut de plus vérifier que $\varphi(AB) = \varphi(A)\varphi(B)$ pour tous A et B dans $\mathrm{Aff}(\mathbb{Z})$ (ceci nécessite la relation $xz^n = z^{-n}x$ qui s'obtient en élevant (5.2.13) à la puissance n). □

Remarque 5.2.4. — Le groupe abstrait $\langle x, y\rangle$ de la démonstration qui précède est l'ensemble de tous les mots en x et y (comme $xyxyx$) soumis uniquement à la relation suivante : toutes les paires de x adjacents ou de y adjacents peuvent être annulées (par exemple, $xyxxxy = xyxy$). En effet la seule relation imposée (en plus des axiomes de groupe) est : $x^2 = y^2 = e$, ce groupe est appelé *groupe libre* à deux générateurs d'ordre 2.

Corollaire 5.2.7

Tout groupe quotient non trivial de $\mathrm{Aff}(\mathbb{Z})$ est isomorphe à $\mathrm{Aff}(\mathbb{Z})$ ou à D_{2n} pour un certain $n \geq 1$.

Démonstration. — Le groupe $\mathrm{Aff}(\mathbb{Z})$ étant engendré par deux éléments d'ordre 2, un groupe quotient non trivial de $\mathrm{Aff}(\mathbb{Z})$ est engendré par deux éléments d'ordre 1 ou 2, l'un au moins étant d'ordre 2.

- ◇ Si l'un des générateurs est d'ordre 1 alors le groupe quotient est isomorphe à $\mathbb{Z}/2\mathbb{Z} = \mathrm{D}_2$.
- ◇ Si les deux générateurs sont d'ordre 2 alors le groupe quotient est isomorphe
  - à $\mathrm{Aff}(\mathbb{Z})$ s'il est infini (Théorème 5.2.16),
  - à un groupe diédral s'il est fini (Théorème 5.2.10).

□

Remarque 5.2.5. — Chaque groupe diédral apparaît comme un quotient de $\mathrm{Aff}(\mathbb{Z})$. Pour $n \geq 3$, la réduction modulo n donne un morphisme de $\mathrm{Aff}(\mathbb{Z})$ dans $\mathrm{GL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$ dont l'image est $\widetilde{\mathrm{D}_{2n}}$ (*voir* (5.2.11)) qui est isomorphe à D_{2n}. Par ailleurs

- ◇ l'application $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto (a, b \bmod 2)$ est un morphisme de $\mathrm{Aff}(\mathbb{Z})$ dans $\{\pm 1\} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{D}_4$;
- ◇ et l'application $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto a$ est un morphisme de $\mathrm{Aff}(\mathbb{Z})$ sur $\{\pm 1\} \simeq \mathrm{D}_2$.

L'étude des noyaux de ces morphismes (pour $n \geq 3$, $n = 2$, et $n = 1$) révèle que pour tout $n \geq 1$, $\langle \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \rangle$ est un sous-groupe distingué de $\mathrm{Aff}(\mathbb{Z})$ et $\mathrm{Aff}(\mathbb{Z}) \big/ \langle \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \rangle \simeq \mathrm{D}_{2n}$. Ce modèle commun est une autre justification de la définition des groupes diédraux D_2 et D_4.

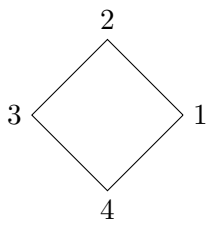
CHAPITRE 6

ACTIONS DE GROUPES

6.1. Une illustration, une définition, les premiers exemples

6.1.1. L'illustration. — Nous motivons l'introduction de la notion d'action de groupes par le Théorème de Cayley qui affirme que tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Les groupes diédraux D_{2n} sont les groupes d'isométries du plan euclidien préservant un polygone régulier à n côtés. Ils peuvent aussi être considérés comme un groupe de permutations des n sommets du polygone régulier invariant. Précisons cela par exemple pour $n = 4$. Considérons le groupe D_8 des isométries du plan euclidien préservant un carré



La numérotation des sommets choisie nous permet d'identifier

- ⋄ la rotation r d'angle $\frac{\pi}{2}$ dans D_8 avec le 4-cycle $(1\ 2\ 3\ 4)$.
- ⋄ la réflexion s d'axe horizontal coupant le carré en deux avec la transposition $(2\ 4)$.

En fait, les éléments de D_8 s'identifient à ceux de $\mathfrak{S}_4$ comme suit :

id	r	r^2	r^3	s	rs	r^2s	r^3s
id	$(1\ 2\ 3\ 4)$	$(1\ 3)(2\ 4)$	$(1\ 4\ 3\ 2)$	$(2\ 4)$	$(1\ 2)(3\ 4)$	$(1\ 3)$	$(1\ 4)(2\ 3)$

Cette identification signifie que l'unique morphisme de groupes $\varphi\colon \mathrm{D}_8 \to \mathfrak{S}_4$, caractérisé par la donnée de $\varphi(r) = (1\ 2\ 3\ 4)$ et par celle de $\varphi(s) = (2\ 4)$, est un isomorphisme de D_8 sur $\{\mathrm{id}, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (2\ 4), (1\ 2)(3\ 4), (1\ 3), (1\ 4)(2\ 3)\}$.

Si nous changeons la numérotation des sommets, alors nous identifions D_8 avec un autre sous-groupe de $\mathfrak{S}_4$.

Cette construction n'est pas propre au groupe D_8 :

Théorème 6.1.1: (Théorème de Cayley)

Si G est fini d'ordre n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Démonstration. — À $g \in \mathrm{G}$ nous associons la fonction $\pi_g \colon \mathrm{G} \to \mathrm{G}$, $x \mapsto gx$. Tout π_g est une permutation de G, vu comme un ensemble, d'inverse $\pi_{g^{-1}}$. Par suite π_g appartient à $\mathfrak{S}_\mathrm{G}$. Puisque $\pi_{g_1} \circ \pi_{g_2} = \pi_{g_1 g_2}$

$$\pi \colon \mathrm{G} \to \mathfrak{S}_\mathrm{G}, \qquad g \mapsto \ell_g$$

est un morphisme de groupes. Ce morphisme est injectif : en effet, si $\pi_g = \mathrm{id}_{\mathfrak{S}_\mathrm{G}}$, c'est-à-dire si pour tout $x \in \mathrm{G}$ on a $gx = x$ alors, en particulier, $g = ge = e$. $\pi_g = \mathrm{id}_{\mathfrak{S}_\mathrm{G}}$, alors $g = e$. □

6.1.2. La définition. — Permettre à un groupe G de se comporter comme un groupe de permutations d'un ensemble X comme dans la démonstration du Théorème de Cayley (Théorème 6.1.1) est une idée très utile ; lorsque c'est le cas nous dirons que *le groupe* G *agit sur l'ensemble* X. Une action d'un groupe G sur un ensemble X est le choix pour tout $g \in \mathrm{G}$ d'une permutation $\pi_g \colon X \to X$ telle que

- $\pi_{g_1} \circ \pi_{g_2} = \pi_{g_1 g_2}$ pour tous g_1, g_2 dans G ;
- π_e est l'identité : $\pi_e(x) = x$ pour tout $x \in X$.

En pratique nous n'utilisons pas la notation π_g et remplaçons $\pi_g(x)$ par $g \cdot x$. Attention cela ne signifie pas qu'on peut multiplier un élément de G et un élément de X, cela symbolise l'action de g sur x. La définition d'action de groupe se réécrit alors :

Définition 6.1.1

Soient G un groupe et X un ensemble. On dit que G *agit* sur X si on s'est donné une application

$$\mathrm{G} \times X \to X, \qquad (g, x) \mapsto g \cdot x$$

vérifiant les axiomes suivants :

- $\forall\, g,\, g' \in \mathrm{G},\ \forall\, x \in X,\ g \cdot (g' \cdot x) = (gg') \cdot x$;
- $\forall\, x \in X,\ e \cdot x = x$.

C'est une notion essentielle ; au delà de l'intérêt de l'opération pour l'étude de l'ensemble X, elle permet souvent en retour d'obtenir des renseignements sur le groupe G comme nous le verrons dans la suite.

6.1.3. Les premiers exemples. — Une manière fondamentale d'utiliser les actions de groupes pour mieux comprendre ces derniers est de faire agir le groupe sur lui-même, sur l'ensemble de ses sous-parties, ou sur un sous-ensemble de ses parties. Les deux exemples qui suivent joueront un rôle capital dans la suite et nous reviendrons régulièrement dessus.

6.1.3.1. *Actions par translation à gauche.* — Soit G un groupe.

Exemple 6.1.1. — Comme nous l'avons vu dans la démonstration du Théorème 6.1.1 le groupe G agit sur lui-même (le groupe G est alors vu comme un groupe et comme un ensemble) : $\pi_g \colon \mathrm{G} \to \mathrm{G}$, $h \mapsto gh$. Alors les conditions pour être une action de groupes sont

- ⋄ $g_1(g_2h) = (g_1g_2)h$ pour tous g_1, g_2, h dans G ;
- ⋄ $eh = h$ pour tout $h \in \mathrm{G}$.

Celles-ci sont satisfaites car la loi de composition interne de G est associative et e est l'élément de G.

Il s'agit de l'action de G sur lui-même par *multiplication à gauche*, ou encore par *translation à gauche*.

En faisant agir un espace vectoriel E sur lui-même par translation, c'est un groupe abélien pour son addition, on retrouve l'aspect géométrique que suggère l'usage de ce terme. Pour tous v et w dans E, on a $v \cdot w = v + w$.

Exemple 6.1.2. — Le groupe G peut aussi agir par translation à gauche sur l'ensemble de ses sous-ensembles : soit A un sous-ensemble de G et soit g un élément de G, alors $g \cdot A = gA = \{ga \mid a \in A\}$.

Considérons par exemple l'action de $\mathfrak{S}_4$ sur l'ensemble des couples de $\{1, 2, 3, 4\}$ définie par $(\sigma, \{a, b\}) \mapsto \sigma \cdot \{a, b\} = \{\sigma(a), \sigma(b)\}$. Les couples de $\{1, 2, 3, 4\}$ sont

$$x_1 = \{1, 2\}, \quad x_2 = \{1, 3\}, \quad x_3 = \{1, 4\}, \quad x_4 = \{2, 3\}, \quad x_5 = \{2, 4\}, \quad x_6 = \{3, 4\}$$

L'action de $(1\ 2)$ sur l'ensemble des couples de $\{1, 2, 3, 4\}$ est

$$(1\ 2)x_1 = x_1, \quad (1\ 2)x_2 = x_4, \quad (1\ 2)x_3 = x_5, \quad (1\ 2)x_4 = x_2, \quad (1\ 2)x_5 = x_3, \quad (1\ 2)x_6 = x_6.$$

Autrement dit, vue comme une permutation de l'ensemble $\{x_1, x_2, x_3, x_4, x_5, x_6\}$, $(1\ 2)$ agit comme $(x_2\ x_4)(x_3\ x_5)$. Nous pouvons ainsi construire un plongement de $\mathfrak{S}_4$ dans $\mathcal{A}_6$.

Exemple 6.1.3. — Soit H un sous-groupe de G, pas nécessairement distingué. Soit G/H l'ensemble des classes à gauche modulo H, *i.e.* l'ensemble des parties $a\mathrm{H}$ pour $a \in \mathrm{G}$. Alors G *agit sur* G/H *par translation à gauche* en posant :

$$\mathrm{G} \times \mathrm{G}/\mathrm{H} \to \mathrm{G}/\mathrm{H}, \qquad (g, a\mathrm{H}) \mapsto g \cdot (a\mathrm{H}) = (ga)\mathrm{H}.$$

En effet

- ⋄ pour tous g, g' dans G, pour tout $a\mathrm{H} \in \mathrm{G}/\mathrm{H}$ nous avons

$$g \cdot (g' \cdot (a\mathrm{H})) = g \cdot ((g'a)\mathrm{H}) = (gg'a)\mathrm{H} = (gg') \cdot a\mathrm{H};$$

◇ $\forall\, a\mathrm{H} \in {}^{\mathrm{G}}\!/_{\mathrm{H}}$, $e \cdot a\mathrm{H} = (e\,a)\mathrm{H} = a\mathrm{H}$.

Exemple 6.1.4. — Si, comme nous venons de le voir dans l'Exemple 6.1.2, le groupe G agit par translation à gauche sur l'ensemble des sous-ensembles de G, il n'agit pas de cette façon sur l'ensemble de ses sous-groupes. En effet, lorsque H est un sous-groupe de G, $g\mathrm{H}$ n'est généralement pas un sous-groupe de G ! Considérons par exemple le sous-groupe $\mathrm{H} = \langle(1\ 2)\rangle$ de $\mathfrak{S}_3$ et l'élément $g = (1\ 3)$ de $\mathfrak{S}_3$. Alors $g\mathrm{H} = \{(1\ 3), (1\ 2\ 3)\}$ n'est pas un sous-groupe de $\mathfrak{S}_3$ (il ne contient pas id !)

6.1.3.2. *Actions par conjugaison.* —

Exemple 6.1.5. — Le groupe G *agit sur lui-même par conjugaison*, ou par *automorphisme intérieur*

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, a) \mapsto g \cdot a = gag^{-1}.$$

En effet

◇ $\forall\, g,\, h \in \mathrm{G}$, $\forall\, a \in \mathrm{G}$, nous avons

$$g \cdot (h \cdot a) = g \cdot (hah^{-1}) = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1} = (gh) \cdot a;$$

◇ $\forall\, a \in \mathrm{G}$, $e \cdot a = eae^{-1} = a$.

Exemple 6.1.6. — Notons X l'ensemble des sous-groupes de G. Considérons

$$\mathrm{G} \times X \to X, \qquad (g, \mathrm{H}) \mapsto g \cdot \mathrm{H} = g\mathrm{H}g^{-1}.$$

C'est une action de groupe ; en effet

◇ $\forall\, g,\, h \in \mathrm{G}$, $\forall\, \mathrm{H} \in X$, nous avons

$$g \cdot (h \cdot \mathrm{H}) = g \cdot (h\mathrm{H}h^{-1}) = g(h\mathrm{H}h^{-1})g^{-1} = (gh)\mathrm{H}(h^{-1}g^{-1}) = (gh)\mathrm{H}(gh)^{-1} = (gh) \cdot \mathrm{H};$$

◇ $\forall\, \mathrm{H} \in X$, $e \cdot \mathrm{H} = e\mathrm{H}e^{-1}$.

On dit que H et $g\mathrm{H}g^{-1}$ sont *conjugués*.

6.1.3.3. *Autres actions.* —

Exemple 6.1.7. — Le groupe $\mathfrak{S}_n$ agit sur $X = \{1, 2, \ldots, n\}$ comme suit :

$$\mathfrak{S}_n \times X \to X, \qquad (\sigma, i) \mapsto \sigma \cdot i = \sigma(i).$$

En effet, pour tout $i \in X$, d'une part $\mathrm{id} \cdot i = \mathrm{id}(i) = i$, d'autre part,

$$\sigma \cdot (\sigma' \cdot i) = \sigma \cdot (\sigma'(i)) = \sigma(\sigma'(i)) = (\sigma\sigma')(i) = (\sigma\sigma') \cdot i.$$

Exemple 6.1.8. — Signalons les exemples géométriques, d'autres exemples seront détaillés plus tard. Soit E un espace euclidien, nous pouvons faire opérer sur E tous les groupes de transformations classiques : groupes des translations, rotations, homothéties, etc.

Exemple 6.1.9. — Le groupe $\mathrm{GL}(n,\mathbb{R})$ agit sur les vecteurs dans $\mathbb{R}^n$ de la manière habituelle : $f\colon \mathrm{GL}(n,\mathbb{R})\times\mathbb{R}^n \to \mathbb{R}^n$, $(A,v)\mapsto A\cdot v = Av$. Dans cette action, l'origine 0 est fixée par chaque $A \in \mathrm{GL}(n,\mathbb{R})$ tandis que les autres vecteurs sont déplacés (lorsque A varie). Les axiomes d'une action de groupe sont des propriétés de la multiplication matrice-vecteur : $\mathrm{Id}v = v$ et $A(Bv) = (AB)v$.

Exemple 6.1.10. — Le groupe $\mathrm{GL}(n,\Bbbk)$ agit sur $\mathrm{M}(n,\Bbbk)$ par conjugaison

$$\mathrm{GL}(n,\Bbbk)\times\mathrm{M}(n,\Bbbk)\to\mathrm{M}(n,\Bbbk), \qquad (P,M)\mapsto P\cdot M = PMP^{-1}.$$

Exemple 6.1.11. — Le groupe $\mathrm{GL}(n,\Bbbk)$ agit sur $\mathrm{M}(n,\Bbbk)$ par congruence

$$\mathrm{GL}(n,\Bbbk)\times\mathrm{M}(n,\Bbbk)\to\mathrm{M}(n,\Bbbk), \qquad (P,M)\mapsto P\cdot M = PM{}^{\mathrm{t}}P.$$

Deux matrices $M_1 = S_1 + A_1$ et $M_2 = S_2 + A_2$ sont congruentes si et seulement si leurs parties symétriques et antisymétriques le sont simultanément. Le problème de classification des formes quadratiques et des formes bilinéaires alternées sur le corps $\Bbbk$ est un cas particulier.

Exemple 6.1.12. — Considérons

$$\mathrm{GL}(n,\Bbbk)\times\mathrm{GL}(n,\Bbbk)\times\mathrm{M}(n,\Bbbk)\to\mathrm{M}(n,\Bbbk), \qquad \big((P,Q),M\big)\mapsto (P,Q)\cdot M = PMQ^{-1};$$

on peut vérifier que c'est une action de $\mathrm{GL}(n,\Bbbk)\times\mathrm{GL}(n,\Bbbk)$ sur $\mathrm{M}(n,\Bbbk)$. Cette action est appelée *action de Steinitz* ; deux matrices conjuguées sous cette action sont dites *r-équivalentes*. La « r-équivalence » des matrices est à la base de la notion de rang d'une matrice.

Exemple 6.1.13. — Le groupe $\mathrm{GL}(n,\Bbbk)$ agit sur les quadruplets de droites de $\Bbbk^n$

$$\mathrm{GL}(n,\Bbbk)\times\Bbbk^n\to\Bbbk^n \quad \big(g,(\mathcal{D}_1,\mathcal{D}_2,\mathcal{D}_3,\mathcal{D}_4)\big)\mapsto g\cdot(\mathcal{D}_1,\mathcal{D}_2,\mathcal{D}_3,\mathcal{D}_4) = \big(g(\mathcal{D}_1),g(\mathcal{D}_2),g(\mathcal{D}_3),g(\mathcal{D}_4)\big)$$

L'étude de cette opération lorsque $n = 2$ est à la base de la notion de birapport de quatre points de la droite projective.

Exemple 6.1.14. — Soit G un groupe fini d'ordre $p^\alpha m$ où le nombre premier p ne divise pas l'entier m. Alors le groupe G agit sur les p-Sylow c'est-à-dire sur les sous-groupes de G d'ordre p^α. Nous verrons au Chapitre 10 que de tels groupes existent toujours.

Exemple 6.1.15. — Le groupe $\mathfrak{S}_n$ agit sur les polynômes $P(X_1,X_2,\dots,X_n)$ en permutant les variables :

$$(\sigma\cdot P)(X_1,X_2,\dots,X_n) = P(X_{\sigma(1)},X_{\sigma(2)},\dots,X_{\sigma(n)}).$$

Il s'agit de remplacer X_i par $X_{\sigma(i)}$ dans $P(X_1,X_2,\dots,X_n)$. Il est clair que $(\mathrm{id})\cdot P = P$.

On a par exemple $(1\ 2)(2\ 3) = (1\ 2\ 3)$ dans $\mathfrak{S}_3$ et

- ⋄ d'une part $(1\ 2)\cdot\big((2\ 3)\cdot(X_2+X_3^2)\big) = (1\ 2)\cdot(X_3+X_2^2) = X_3+X_1^2$
- ⋄ d'autre part $(1\ 2\ 3)\cdot(X_2+X_3^2) = X_3+X_1^2$.

Plus généralement soient σ et σ' dans $\mathfrak{S}_n$; alors d'une part

$$\begin{aligned}\sigma\cdot(\sigma'\cdot P)(X_1,X_2,\dots,X_n) &= \sigma\cdot(X_{\sigma'(1)},X_{\sigma'(2)},\dots,X_{\sigma'(n)})\\ &= (X_{\sigma(\sigma'(1))},X_{\sigma(\sigma'(2))},\dots,X_{\sigma(\sigma'(n))})\\ &= (X_{\sigma\sigma'(1))},X_{\sigma\sigma'(2))},\dots,X_{\sigma\sigma'(n))})\end{aligned}$$

et d'autre part

$$(\sigma\sigma')\cdot P(X_1,X_2,\dots,X_n) = (X_{\sigma\sigma'(1))},X_{\sigma\sigma'(2))},\dots,X_{\sigma\sigma'(n))}).$$

Autrement dit pour tous σ, σ' dans $\mathfrak{S}_n$ nous avons $\sigma\cdot(\sigma'\cdot P) = (\sigma\sigma')\cdot P$.

Exemple 6.1.16. — Soit G le groupe du Rubik's cube : toutes les suites de mouvements sur le cube (en gardant les couleurs centrales à des emplacements fixes). Ce groupe agit sur deux ensembles différents : les douze « petits cubes » d'arête et les huit « petits cubes » d'angle.

Exemple 6.1.17. — Considérons

$$\mathfrak{S}_n\times\mathbb{R}^n\to\mathbb{R}^n,\qquad (\sigma,v=(v_1,v_2,\dots,v_n))\mapsto\sigma\cdot v=(v_{\sigma^{-1}(1)},v_{\sigma^{-1}(2)},\dots,v_{\sigma^{-1}(n)})\cdot$$

C'est une action de groupes. En effet, $\mathrm{id}\cdot v = v$ et si σ et σ' désignent deux éléments de $\mathfrak{S}_n$ alors $\sigma\cdot(\sigma'\cdot v) = (\sigma\sigma')\cdot v$.

Par contre

$$\mathfrak{S}_n\times\mathbb{R}^n\to\mathbb{R}^n,\qquad (\sigma,v=(v_1,v_2,\dots,v_n))\mapsto\sigma\cdot v=(v_{\sigma(1)},v_{\sigma(2)},\dots,v_{\sigma(n)})$$

n'est pas une action de groupes. En effet, supposons par exemple que $n = 3$, $\sigma = (1\ 2)$, $\sigma' = (2\ 3)$ et $v = (5,7,9)$. D'une part

$$\sigma\cdot(\sigma'\cdot v) = \sigma\cdot(5,9,7) = (9,5,7)$$

et d'autre part

$$(\sigma\sigma')\cdot v = (1,2,3)\cdot v = (7,9,5)$$

En particulier, $\sigma\cdot(\sigma'\cdot v)\neq(\sigma\sigma')\cdot v$.

Exemple 6.1.18. — On peut généraliser l'exemple et le contre-exemple précédents comme suit.

Soit G un groupe agissant sur un ensemble X. Soit S un ensemble. Désignons par $\mathcal{F}(X,S)$ l'ensemble des fonctions $\mathfrak{f}\colon X\to S$. Considérons

$$\mathrm{G}\times\mathcal{F}(X,S)\to\mathcal{F}(X,S),\qquad (g,\mathfrak{f})\mapsto g*\mathfrak{f}\colon x\mapsto\mathfrak{f}(g^{-1}\cdot x).$$

C'est une action de groupe puisque pour tous g, h dans G et tout $\mathfrak{f}\in\mathcal{F}(X,S)$ nous avons

$$(g*(h*\mathfrak{f}))(x) = (h*\mathfrak{f})(g^{-1}\cdot x) = \mathfrak{f}(h^{-1}\cdot(g^{-1}\cdot x)) = \mathfrak{f}((gh)^{-1}\cdot x) = ((gh)*\mathfrak{f})(x)$$

d'où $g*(h*\mathfrak{f}) = (gh)*\mathfrak{f}$.

Par contre

$$\mathrm{G}\times\mathcal{F}(X,S)\to\mathcal{F}(X,S),\qquad (g,\mathfrak{f})\mapsto g\star\mathfrak{f}\colon x\mapsto\mathfrak{f}(g\cdot x);$$

n'est pas une action de groupe. En effet,

$$(g \star (h \star \mathfrak{f}))(x) = (h \star \mathfrak{f})(g \cdot x) = \mathfrak{f}(h \cdot (g \cdot x)) = \mathfrak{f}(hg \cdot x) = ((hg) \star \mathfrak{f})(x),$$

qui n'a aucune raison d'être égal à $((gh) \star \mathfrak{f})(x)$.
On retrouve la situation de l'exemple 6.1.17. En effet, si $S = \mathbb{R}$ et $X = \{1, \ldots, n\}$, alors $\mathcal{F}(X, S)$ s'identifie naturellement à $\mathbb{R}^n$ en associant à $\mathfrak{f} \in \mathcal{F}(X, \mathbb{R})$ le vecteur $(\mathfrak{f}(1), \cdots, \mathfrak{f}(n))$. On a alors, pour $\sigma \in \mathfrak{S}_n$, $\sigma * \mathfrak{f}(i) = \mathfrak{f}(\sigma^{-1}(i))$ qui correspond au vecteur $(\mathfrak{f}(\sigma^{-1}(1)), \cdots, \mathfrak{f}(\sigma^{-1}(n)))$, et $\sigma \star \mathfrak{f}(i) = \mathfrak{f}(\sigma(i))$ qui correspond au vecteur $(\mathfrak{f}(\sigma(1)), \cdots, \mathfrak{f}(\sigma(n)))$.

6.2. Actions transitives, actions fidèles, orbites, stabilisateurs

Nous commençons ce paragraphe avec un résultat qui donne un point de vue différent sur les actions de groupes.

Théorème 6.2.1

Se donner une action d'un groupe G sur un ensemble X

$$\mathrm{G} \times X \to X, \qquad (g, x) \mapsto g \cdot x$$

revient à se donner un morphisme de groupes de G dans $\mathfrak{S}_X$

$$\mathrm{G} \to \mathfrak{S}_X, \qquad g \mapsto \pi_g \colon X \to X, \quad x \mapsto g \cdot x$$

Démonstration. — Supposons que nous ayons une action de G sur X. On peut voir $g \cdot x$ comme une fonction de x : pour tout $g \in \mathrm{G}$ on définit la fonction $\pi_g \colon X \to X$, $x \mapsto \pi_g(x) = g \cdot x$. L'axiome $e \cdot x = x$ traduit le fait que π_e est la fonction identité sur X. L'axiome $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ assure que $\pi_{g_1} \circ \pi_{g_2} = \pi_{g_1 g_2}$. De plus, π_g est inversible d'inverse $\pi_{g^{-1}}$. Par conséquent π_g appartient à $\mathfrak{S}_X$ et $g \mapsto \pi_g$ est un morphisme de groupes de G dans $\mathfrak{S}_X$.

Réciproquement, supposons que $f \colon \mathrm{G} \to \mathfrak{S}_X$ soit un morphisme de groupes. Pour tout $g \in \mathrm{G}$, $f(g)$ est une permutation de X et f étant un morphisme $f(g_1 g_2) = f(g_1) \circ f(g_2)$. Posons $g \cdot x = f(g)(x)$; le fait que f soit un morphisme de groupes entraîne les propriétés requises pour avoir une action de groupes. □

De ce point de vue l'ensemble des $g \in \mathrm{G}$ qui agissent trivialement ($g \cdot x = x$ pour tout $x \in X$) est le noyau du morphisme $\mathrm{G} \to \mathfrak{S}_X$ associé à l'action :

Proposition 6.2.1

Soit G un groupe agissant sur un ensemble X. L'ensemble des $g \in \mathrm{G}$ qui agissent trivialement ($g \cdot x = x$ pour tout $x \in X$) est le noyau du morphisme $\mathrm{G} \to \mathfrak{S}_X$ associé à l'action.

Définitions 6.2.1

a) Le groupe G *agit transitivement* sur l'ensemble X si

$$\forall\, x \in X,\ \forall\, y \in X,\ \exists\, g \in \mathrm{G},\ g \cdot x = y.$$

On dit que l'action est *simplement transitive* si pour tous x et y dans X il existe un unique $g \in \mathrm{G}$ tel que $g \cdot x = y$.

b) Le groupe G *agit fidèlement* sur l'ensemble X si le morphisme $\pi\colon \mathrm{G} \to \mathfrak{S}_X$, $g \mapsto \pi_g$ est injectif, soit si son noyau est réduit à l'élément neutre, c'est-à-dire si $g \cdot x = x$ pour tout $x \in X$ implique $g = e$.

Remarque 6.2.1. — Si G est un groupe abélien qui agit fidèlement et transitivement sur un ensemble X, alors G agit simplement transitivement sur X.

En effet, soit x dans X et soient g, h dans G tels que $g \cdot x = h \cdot x$. L'action de G sur X étant transitive pour tout $y \in X$ il existe $k \in \mathrm{G}$ tel que $y = k \cdot x$. Il en résulte que

$$g \cdot y = g \cdot (k \cdot x) = (gk) \cdot x \underbrace{=}_{\text{G abélien}} (kg) \cdot x = k \cdot (g \cdot x) = k \cdot (h \cdot x) = (kh) \cdot x \underbrace{=}_{\text{G abélien}} (hk) \cdot x = h \cdot y;$$

puisque l'action est fidèle on en déduit : $g = h$.

Exemple 6.2.1. — Soit G un groupe fini d'ordre $p^\alpha m$ où le nombre premier p ne divise pas m. Alors le groupe G agit transitivement sur les p-Sylow, *i.e.* sur les sous-groupes de G d'ordre p^α.

Exemple 6.2.2. — Le groupe $\mathrm{GL}(2, \Bbbk)$ agit transitivement sur les triplets de droites deux à deux distinctes de $\Bbbk^2$. En effet soient $(\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3)$ un triplet de droites distinctes : il existe v_1, v_2, v_3 non nuls tels que $v_3 = v_1 + v_2$ et $v_i \in \mathcal{D}_i$ pour $1 \leq i \leq 3$. Les vecteurs v_1 et v_2 qui forment une base de $\Bbbk^2$ peuvent être envoyés par une application linéaire sur deux vecteurs w_1 et w_2 libres fixés et v_3 s'envoie sur $w_3 = w_1 + w_2$.

Exemple 6.2.3. — Le groupe projectif $\mathrm{PGL}(2, \Bbbk) = \mathrm{GL}(2, \Bbbk)/Z(\mathrm{GL}(2, \Bbbk)) = \mathrm{GL}(2, \Bbbk)/\Bbbk^\times$ sur les triplets de droites deux à deux distinctes de $\Bbbk^2$ est simplement transitive c'est-à-dire qu'il existe un unique $\overline{g}$ envoyant un triplet sur un autre. Ceci équivaut à dire que le stabilisateur d'un tel triplet pour l'action de $\mathrm{GL}(2, \Bbbk)$ est réduit à $\Bbbk^\times$; en effet, un élément du stabilisateur a trois directions propres, il est donc scalaire.

Proposition 6.2.2

Toute action simplement transitive est fidèle.

Démonstration. — Soit une action simplement transitive du groupe G sur l'ensemble X. Pour tout $x \in X$ on a $e \cdot x = x$. L'action étant simplement transitive, e est l'unique élément de G vérifiant cette égalité. L'action est donc fidèle. □

Exemple 6.2.4. — L'action de G sur lui-même par translation à gauche est simplement transitive. En effet si x et y sont deux éléments de G, on a alors, pour $g \in \mathrm{G}$, $g \cdot x = y$ si et seulement si $gx = y$, soit si et seulement si $g = yx^{-1}$. D'où l'existence et l'unicité de $g \in \mathrm{G}$ qui permet de "passer" de x à y par translation à gauche.
En vertu de la Proposition 6.2.2, cette action est aussi fidèle.

Exemple 6.2.5. — L'action de G sur lui-même par conjugaison est fidèle si et seulement si $Z(\mathrm{G}) = \{e\}$ (en effet $g \cdot x = x$ pour tout $x \in \mathrm{G}$ si et seulement si $gxg^{-1} = x$ pour tout $x \in \mathrm{G}$ si et seulement si $gx = xg$ pour tout $x \in \mathrm{G}$ si et seulement si g appartient à $Z(\mathrm{G})$).
Cette action n'est en général pas transitive puisque la conjugaison préserve les propriétés algébriques, tel l'ordre. Par exemple un élément d'ordre 3 ne peut pas être envoyé par conjugaison sur un élément d'ordre 2.
En fait cette action n'est transitive que dans le cas $\mathrm{G} = \{e\}$. En effet si l'action est transitive, pour tout $x \in \mathrm{G}$ il existe $g \in \mathrm{G}$ tels que $gxg^{-1} = e$. Ce qui implique $x = e$.

Exemple 6.2.6. — Soit $A = (a_{i,j})$ dans $\mathrm{GL}(2, \mathbb{R})$ tel que $A \cdot v = v$ pour tout $v \in \mathbb{R}^2$. En particulier

- ◇ d'une part $A \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ qui conduit à $a_{1,1} = 1$ et $a_{2,1} = 0$;
- ◇ d'autre part $A \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ qui donne $a_{1,2} = 0$ et $a_{2,2} = 1$.

Il en résulte que $A = \mathrm{id}$. Ainsi l'action de $\mathrm{GL}(2, \mathbb{R})$ sur $\mathbb{R}^2$ est fidèle.

Pour tout élément $A \in \mathrm{GL}(2, \mathbb{R})$ on a $A \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. En particulier il n'existe pas matrice $A \in \mathrm{GL}(2, \mathbb{R})$ telle que $A \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. L'action n'est pas transitive.

Exemple 6.2.7. — Soit G un groupe. Soit H un sous-groupe de G. Supposons que G agisse sur G/H par multiplication à gauche. L'action de G est fidèle si le noyau de π est réduit à l'élément neutre. Soit g' un élément de ce noyau, alors pour tout $g \in \mathrm{G}$ on a $g' \cdot g\mathrm{H} = g'g\mathrm{H} = g\mathrm{H}$. Ce qui signifie que $g' \in g\mathrm{H}g^{-1}$ et l'action est fidèle si et seulement si $\{e\} = \bigcap_{g \in \mathrm{G}} g\mathrm{H}g^{-1}$.
Cette action est transitive puisque si $x\mathrm{H}$ et $y\mathrm{H}$ sont deux éléments de G/H et si $g = yx^{-1}$, alors on a $g \cdot x\mathrm{H} = y\mathrm{H}$.

Exemple 6.2.8. — Soit G un groupe agissant sur un ensemble X et $\pi \colon \mathrm{G} \to \mathfrak{S}_X$ introduit dans le Théorème 6.2.1. Le groupe $\mathrm{G}/\ker \pi$ ($\ker \pi$ est distingué) agit fidèlement sur X puisque le théorème de factorisation (Théorème 3.5.2) assure que π induit un morphisme injectif de $\mathrm{G}/\ker \pi$ dans $\mathfrak{S}_X$. Le Théorème 6.2.1 permet de conclure.

Exemples 6.2.9. — ◇ Soit E un ensemble ; $\mathfrak{S}(E)$ agit transitivement sur E.

En effet, si x et y sont deux éléments de E et si $\tau = (x\ y)$ désigne la transposition de ces deux éléments, c'est un élément de $\mathfrak{S}(E)$, on a $\tau \cdot x = \tau(x) = y$ et l'action est transitive.
L'action est fidèle puisque si on a $\sigma \cdot x = x$ pour tout $x \in E$, alors $\sigma(x) = x$ pour tout $x \in E$, et donc $\sigma = \mathrm{id}$.

◇ Soit E un ensemble fini. Si σ désigne un élément de $\mathfrak{S}(E)$, on peut considérer l'action sur E du groupe cyclique engendré par σ. L'action sur E de ce sous-groupe de $\mathfrak{S}(E)$ est à nouveau fidèle. Mais elle est transitive si et seulement si σ est un cycle de longueur $n = \#E$ (σ est alors appelée permutation circulaire).

Soit $\mathrm{G} = \langle \sigma \rangle$ et soit x un élément de E. On note n le cardinal de E.

Si σ est un cycle de longueur n alors $\{\sigma^k(x) \,|\, k \in \mathbb{N}\}$ est un sous-ensemble de E de cardinal n. C'est donc E tout entier et pour tout $y \in E$ il existe $k \in \mathbb{N}$ tel que $y = \sigma^k(x)$. C'est-à-dire $\sigma^k.x = y$ et le groupe G agit transitivement sur E.

Supposons que G agit transitivement sur E, alors pour tout $y \in E$ il existe $k \in \mathbb{N}$ tel que $\sigma^k \cdot x = \sigma^k(x) = y$. La transitivité de l'action se réécrit alors $E = \{\sigma^k(x) \,|\, k \in \mathbb{N}\}$. Comme E est fini, il existe nécessairement deux entiers $0 \leq i$ et $0 < j$ tels que $\sigma^i(x) = \sigma^{i+j}(x)$ ce qui implique que $x = \sigma^j(x)$. Si nous notons $\ell = \min\{k > 0 \,|\, \sigma^k(x) = x\}$ nous avons alors $\sigma^i(x) \neq \sigma^j(x)$ pour tous $i \neq j$ dans $[\![0, \ell - 1]\!]$ et $\sigma^\ell(x) = x$. Ainsi l'ensemble $\{\sigma^k(x) \,|\, k \in [\![0, \ell - 1]\!]\}$ a ℓ éléments et il est égal à E, cela implique $\ell = n$. De plus, on constate que σ est la permutation circulaire qui envoie $\sigma^{k-1}(x)$ sur $\sigma^k(x)$, pour $1 \leq k < n$, et $\sigma^{n-1}(x)$ sur x.

Proposition-Définition 6.2.1: Orbite d'un point

Soit X un ensemble sur lequel agit le groupe G. On définit sur X la relation $\mathcal{R}$ par :

$$\forall\, x,\, y \in X \quad x\mathcal{R}y \Longleftrightarrow \exists\, g \in \mathrm{G},\, g \cdot x = y.$$

Il s'agit d'une relation d'équivalence.
La classe de $x \in X$ est son *orbite* sous l'action de G, on la note $\mathcal{O}_x$ et on a donc $\mathcal{O}_x = \{g \cdot x \,|\, g \in \mathrm{G}\}$.
Les orbites forment une partition de X et G agit transitivement sur chacune d'entre elles.

Démonstration. — Soient x, y et z trois éléments de X.

◇ On a $e \cdot x = x$. C'est-à-dire $x\mathcal{R}x$ et la relation est réflexive.

◇ Si $x\mathcal{R}y$ alors il existe $g \in \mathrm{G}$ tel que $g \cdot x = y$. En faisant agir g^{-1} sur y on a donc : $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = g^{-1}g \cdot x = e_{\mathrm{G}} \cdot x = x$. C'est-à-dire que $y\mathcal{R}x$ et la relation est symétrique.

◇ Si $x\mathcal{R}y$ et $y\mathcal{R}z$, il existe g et h dans G tels que $g \cdot x = y$ et $h \cdot y = z$. On a alors : $h \cdot y = h \cdot (g \cdot x) = hg \cdot x$, donc $x\mathcal{R}z$ et la relation est transitive.

On a vérifié que $\mathcal{R}$ est une relation d'équivalence. □

Cette relation mesure le défaut de transitivité. Si l'action est transitive alors il y a une unique orbite qui est X en entier.

Définition 6.2.1

Soit G un groupe agissant sur un ensemble X.
On dit que $x \in X$ est *un point fixe* de $g \in \mathrm{G}$ si $g \cdot x = x$. On note $\mathtt{fixe}_X(g)$ l'ensemble des points fixes de g.
On dit que $x \in X$ est *un point fixe* de l'action de G sur X s'il est laissé fixe par tous les éléments de G. C'est-à-dire si $\mathcal{O}_x = \{x\}$.
On note $\mathtt{fixe}_X(\mathrm{G})$ l'ensemble des points fixes de l'action.
On a : $\mathtt{fixe}_X(\mathrm{G}) = \bigcap_{g \in \mathrm{G}} \mathtt{fixe}_X(g)$.

Exemple 6.2.10. — Les orbites de $\mathbb{R}^n$ sous l'action du groupe orthogonal $\mathrm{O}(n, \mathbb{R})$ sont les sphères euclidiennes de centre l'origine.

On peut commencer par remarquer que l'orbite de 0 est réduite à 0.

Soit $x \in \mathbb{R}^n$ et $y \in \mathcal{O}_x$. Il existe donc $M \in \mathrm{O}(n, \mathbb{R})$ tel que $Mx = y$. On a alors $||y|| = ||Mx|| = ||x||$ puisque $M \in \mathrm{O}(n, \mathbb{R})$.

Réciproquement, si $x \neq 0$ et y sont deux éléments de $\mathrm{O}(n, \mathbb{R})$ tels que $||x|| = ||y|| = r \neq 0$. Le procédé de Gram-Schmidt permet de compléter $x_1 = \frac{x}{r}$ en une base orthonormée $\mathcal{B} = \{x_1, \cdots, x_n\}$, ainsi que $y_1 = \frac{y}{r}$ en une base orthonormée $\mathcal{B}' = \{y_1, \cdots, y_n\}$. L'endomorphisme $\varphi \colon \mathbb{R}^n \to, \mathbb{R}^n$ défini par $\varphi(x_i) = y_i$ est orthogonal, sa matrice dans la base canonique, M, est orthogonale et vérifie $m \cdot x = Mx = y$.

Exemple 6.2.11. — Rappelons que le groupe $\mathrm{GL}(n, \Bbbk) \times \mathrm{GL}(p, \Bbbk)$ agit sur $\mathrm{M}((n, p), \Bbbk)$

$$\mathrm{GL}(n, \Bbbk) \times \mathrm{GL}(p, \Bbbk) \times \mathrm{M}((n, p), \Bbbk) \to \mathrm{M}(n, \Bbbk), \qquad ((P, Q), M) \mapsto PMQ^{-1}$$

et que deux matrices conjuguées sous cette action sont dites r-équivalentes. Deux matrices sont r-équivalentes si et seulement si elles ont même rang. Il s'ensuit que pour l'action de Steinitz le nombre d'orbites est égal à $\min(n+1, p+1)$. C'est un résultat qui sera détaillé au paragraphe 9.3 page 372.

Exemple 6.2.12. — Soit $\Bbbk$ un corps de caractéristique différente de 2. Considérons l'action par congruence de $\mathrm{GL}(n, \Bbbk)$ sur l'espace vectoriel des matrices symétriques $\mathrm{S}(n, \Bbbk)$

$$\mathrm{GL}(n, \Bbbk) \times \mathrm{S}(n, \Bbbk) \to \mathrm{S}(n, \Bbbk), \qquad (P, M) \mapsto P \cdot M = PM{}^{\mathrm{t}}P$$

L'orbite de tout élément contient une matrice diagonale. En effet, soit f la forme bilinéaire symétrique définie dans la base canonique de $\Bbbk^n$ par la matrice symétrique S. Comme $\Bbbk$ n'est

pas de caractéristique 2, la forme f possède une base orthogonale, *i.e.* une base dans laquelle la matrice de f, qui sera notée D, est diagonale. Si P désigne la matrice de changement de base, nous avons $S = PD{}^{\mathrm{t}}P$; autrement dit D appartient à $\mathcal{O}_S$.

Exemple 6.2.13 **(Décomposition d'une permutation en produit de cycles disjoints)**

On peut reprendre la partie existence du Théorème 5.1.1 en utilisant une action de groupe de la manière suivante.
Le groupe $\mathfrak{S}_n$ agit sur $X = \{1, 2, \ldots, n\}$ par $\sigma \cdot x = \sigma(x)$. Soit $\sigma \in \mathfrak{S}_n$ et soit $\langle\sigma\rangle$ le groupe cyclique engendré par σ qui agit aussi sur X. Soient $F_1, F_2, \ldots, F_r$ les orbites de X sous l'action de $\langle\sigma\rangle$. Alors les permutations σ_i définies par

$$\sigma_i(x) = \begin{cases} x \text{ si } x \notin F_i \\ \sigma(x) \text{ si } x \in F_i \end{cases}$$

sont des cycles, d'ordre $\#F_i$, deux à deux permutables, puisque leurs supports sont disjoints, et nous avons $\sigma = \sigma_1\sigma_2 \ldots \sigma_r$.

En particulier, si $X = \{1, 2, \ldots, 8\}$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix}$, alors

$$F_1 = \mathcal{O}_1 = \{g(1) \,|\, g \in \langle\sigma\rangle\} = \{\sigma^k(1) \,|\, k \in \mathbb{Z}\} = \{1, 3, 4, 5\},$$

$$F_2 = \mathcal{O}_2 = \{g(2) \,|\, g \in \langle\sigma\rangle\} = \{\sigma^k(2) \,|\, k \in \mathbb{Z}\} = \{2, 6, 8\}$$

et $\sigma = (1\ 3\ 4\ 5)(2\ 6\ 8)$.

Proposition-Définitions 6.2.1: Stabilisateur-Fixateur-Point Fixe

Soient G un groupe agissant sur un ensemble X et A une partie X. Le *stabilisateur* de A sous l'action de G est

$$\mathrm{St}_{\mathrm{G}}(A) = \{g \in \mathrm{G} \,|\, \forall\, a \in A \quad g \cdot a \in A\}.$$

Il s'agit d'un sous-groupe de G si A est fini mais pas en général.
Si $A = \{x\}$ est un singleton, on note

$$\mathrm{St}_{\mathrm{G}}(x) = \mathrm{St}_{\mathrm{G}}(\{x\}) = \{g \in \mathrm{G} \,|\, g \cdot x = x\};$$

le *stabilisateur* (ou encore *fixateur*) de x.
Un élément x de X est *point fixe* de l'action de G si pour tout g dans G on a $g \cdot x = x$. Autrement dit si $\mathrm{St}_{\mathrm{G}}(x) = \mathrm{G}$.
Enfin, le *fixateur* de A sous l'action de G est le sous-groupe de G

$$\mathrm{Fix}_{\mathrm{G}}(A) = \{g \in \mathrm{G} \,|\, \forall\, a \in A \quad g \cdot a = a\} = \bigcap_{a \in A} \mathrm{St}_{\mathrm{G}}(a).$$

Remarque 6.2.2. — Soit G un groupe agissant sur un ensemble X.

Il existe un lien évident entre ces nouvelles notions et celle de point fixe (Définition 6.2.1). On a $\mathrm{St}_{\mathrm{G}}(x) = \{g \in \mathrm{G} \,|\, x \in \mathtt{fixe}_X(g)\}$ et aussi $\mathrm{Fix}_{\mathrm{G}}(A) = \{g \in \mathrm{G} \,|\, A \subset \mathtt{fixe}_X(g)\}$.

D'autre part pour $x \in X$, on a

$$x \text{ est un point fixe de l'action} \iff \mathrm{St}_{\mathrm{G}}(x) = \mathrm{G} \iff \mathcal{O}_x = \{x\}.$$

On constate que pour une orbite de taille minimale on a un stabilisateur de taille maximale. Ce lien entre la taille de l'orbite et celle du stabilisateur sera explicité dans la Proposition 6.3.1.

Démonstration. — Soient $A \subset X$, g et g' deux éléments de $\mathrm{St}_{\mathrm{G}}(A)$. Pour tout élément $a \in A$ on a :

$$(gg') \cdot a = g \cdot (g' \cdot a) \in A \qquad \text{car } g' \cdot a = b \in A \text{ et donc } g \cdot b \in A.$$

Pour vérifier la stabilité par passage à l'inverse on suppose que **A est fini** et on considère $\varphi \colon A \to A$, $a \mapsto g \cdot a$. Si $\varphi(a) = \varphi(b)$, soit si $g \cdot a = g \cdot b$, alors $g^{-1} \cdot (g \cdot a) = g^{-1} \cdot (g \cdot a)$, c'est-à-dire $a = b$. Ainsi φ est injective, et donc bijective puisque A est fini. En particulier, étant donné $a \in A$ il existe $b \in A$ tel que $g \cdot b = a$. On a donc $g^{-1} \cdot a = b \in A$. Ce qui prouve la stabilité par passage à l'inverse.

Ainsi, si A est fini alors $\mathrm{St}_{\mathrm{G}}(A)$ est un sous-groupe de G. En particulier $\mathrm{St}_{\mathrm{G}}(x)$ est un sous-groupe de G.

Une intersection quelconque de sous-groupes étant un sous-groupe, on conclut que $\mathrm{Fix}_{\mathrm{G}}(A)$ est un sous-groupe de G. □

Remarque 6.2.3. — Comme nous l'avons mentionné précédemment, si A n'est pas fini alors $\mathrm{St}_{\mathrm{G}}(A)$ n'est pas nécessairement un sous-groupe de G.

Considérons par exemple l'action de $\mathbb{Z}$ sur lui-même par translation : $g \cdot n = g + n$. Prenons $A = \mathbb{N}$. On a $g \in \mathrm{St}_{\mathrm{G}}(A)$ si et seulement si pour tout $a \in \mathbb{N}$, $g + a \in \mathbb{N}$. C'est-à-dire si et seulement si $g \in \mathbb{N}$, alors $\mathrm{St}_{\mathrm{G}}(A) = \mathbb{N}$ qui n'est pas un sous-groupe de $\mathbb{Z}$.

Si on souhaite que le stabilisateur de A soit un sous-groupe de G il suffit de prendre comme définition

$$\mathrm{St}_{\mathrm{G}}(A) = \{g \in \mathrm{G} \,|\, \forall\, a \in A \quad g \cdot a \in A,\, g^{-1} \cdot a \in A\}.$$

Remarque 6.2.4. — Si G agit sur X et si $\pi \colon \mathrm{G} \to \mathfrak{S}_X$ est le morphisme associé à cette action, alors $\ker \pi = \bigcap_{x \in X} \mathrm{St}_{\mathrm{G}}(x) = \mathrm{Fix}_{\mathrm{G}}(X)$. En effet

$$\ker \pi = \{g \in \mathrm{G} \,|\, \pi(g) = \mathrm{id}_X\} = \{g \in \mathrm{G} \,|\, g \cdot x = x \quad \forall\, x \in X\} = \mathrm{Fix}_{\mathrm{G}}(X) = \bigcap_{x \in X} \mathrm{St}_{\mathrm{G}}(x).$$

La Remarque 6.2.4 et la Définition 6.2.1 d'une action fidèle conduisent à

Proposition 6.2.3

L'action du groupe G sur l'ensemble X est fidèle si et seulement si $\mathrm{Fix}_{\mathrm{G}}(X) = \{e\}$.

Exemple 6.2.14. — Considérons l'action de $\mathfrak{S}_n$ sur $X = \{1, 2, \ldots, n\}$; le stabilisateur d'un point $k \in X$ sous cette action est isomorphe à $\mathfrak{S}_{n-1}$: le stabilisateur d'un point k est

$$\begin{aligned}\{\sigma \in \mathfrak{S}_n \,|\, \sigma \cdot k = k\} &= \{\sigma \in \mathfrak{S}_n \,|\, \sigma(k) = k\} \\ &= \{\sigma \in \mathfrak{S}(\{1, 2, \ldots, k-1, k+1, k+2, \ldots, n\})\} \\ &\simeq \mathfrak{S}_{n-1}.\end{aligned}$$

Exemple 6.2.15. — Considérons l'action $\mathcal{A}_n$ sur $X = \{1, 2, \ldots, n\}$. Le stabilisateur d'un point $k \in X$ sous cette action est isomorphe à $\mathcal{A}_{n-1}$: le stabilisateur d'un point k est

$$\begin{aligned}\{\sigma \in \mathcal{A}_n \,|\, \sigma \cdot k = k\} &= \{\sigma \in \mathcal{A}_n \,|\, \sigma(k) = k\} \\ &= \{\sigma \in \mathfrak{S}(\{1, 2, \ldots, k-1, k+1, k+2, \ldots, n\}) \,|\, \mathrm{sgn}(\sigma) = 1\} \\ &\simeq \mathcal{A}_{n-1}.\end{aligned}$$

Exemple 6.2.16. — Considérons l'action de $\mathrm{GL}(2, \mathbb{R})$ sur $\mathbb{R}^2$.

L'orbite du vecteur nul $\mathbf{0}$ est $\{\mathbf{0}\}$ car $A \cdot \mathbf{0} = \mathbf{0}$ pour tout $A \in \mathrm{GL}(2, \mathbb{R})$. Le stabilisateur de $\mathbf{0}$ est $\mathrm{GL}(2, \mathbb{R})$.

L'orbite de $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ est $\mathbb{R}^2 \smallsetminus \{\mathbf{0}\}$. Autrement dit tout vecteur non nul peut s'écrire $A \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ pour un $A \in \mathrm{GL}(2, \mathbb{R})$ bien choisi. En effet, soit $\begin{pmatrix} a \\ b \end{pmatrix} \neq \mathbf{0}$, alors

- ⋄ ou bien $b \neq 0$ et $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a & 1 \\ b & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathcal{O}_{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}$;
- ⋄ ou bien $a \neq 0$ et $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathcal{O}_{\begin{pmatrix} 1 \\ 0 \end{pmatrix}}$.

Par suite $\begin{pmatrix} a \\ b \end{pmatrix} \neq \mathbf{0}$ est dans la $\mathrm{GL}(2, \mathbb{R})$-orbite de $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. L'action de $\mathrm{GL}(2, \mathbb{R})$ sur $\mathbb{R}^2$ possède donc deux orbites : celle du vecteur nul qui est réduite au vecteur nul, et une seconde qui contient tous les autres vecteurs.

Soit $\begin{pmatrix} a & x \\ b & y \end{pmatrix} \in \mathrm{GL}(2, \mathbb{R})$ dans le stabilisateur de $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. On a alors $\begin{pmatrix} a & x \\ b & y \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ si et seulement si $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, autrement dit si et seulement si $a = 1$ et $b = 0$, et on

peut conclure que le stabilisateur de $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ est $\left\{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \mid y \neq 0 \right\} \subset \mathrm{GL}(2, \mathbb{R})$. Remarquons que le stabilisateur de $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ est isomorphe à $\mathrm{Aff}(\mathbb{R})$ via $\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \mapsto \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}^{-1}$.

Exemple 6.2.17. — Considérons l'action de $\mathrm{GL}(2, \mathbb{Z})$ sur $\mathbb{Z}^2$. Malgré les similitudes formelles évidentes avec l'exemple précédent, nous allons voir que la situation est beaucoup plus compliquée.

L'orbite du vecteur nul $\mathbf{0}$ est $\{\mathbf{0}\}$ et le stabilisateur de $\mathbf{0}$ est $\mathrm{GL}(2, \mathbb{Z})$.

Soit $\gamma \in \mathbb{Z}^*$, si $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ appartient à l'orbite de $\begin{pmatrix} \gamma \\ 0 \end{pmatrix}$ il existe alors une matrice $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z})$ telle que $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} \gamma \\ 0 \end{pmatrix} = \begin{pmatrix} \gamma a \\ \gamma b \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ et on a $\alpha = \gamma a$ et $\beta = \gamma b$. Comme $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z})$ on a $ad - bc = \pm 1$, ce qui implique en particulier que a et b sont premiers entre eux et donc que l'on a $\mathrm{pgcd}(\alpha, \beta) = \mathrm{pgcd}(\gamma a, \gamma b) = \gamma \mathrm{pgcd}(a, b) = \gamma$.

Réciproquement, si $\mathrm{pgcd}(\alpha, \beta) = \gamma$, il existe a et b premiers entre eux tels que $\gamma a = \alpha$ et $\gamma b = \beta$. Le théorème de Bézout nous indique qu'il existe $-c$ et d tels que $ad - bc = 1$. On a alors $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z})$ et $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} \gamma \\ 0 \end{pmatrix} = \begin{pmatrix} \gamma a \\ \gamma b \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$.

On déduit de ces observations que $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ appartient à la même orbite que $\begin{pmatrix} \gamma \\ 0 \end{pmatrix}$ si et seulement si $\mathrm{pgcd}(\alpha, \beta) = \gamma$. On peut donc décrire l'ensemble des orbites comme : $\left\{ \mathcal{O}_{\mathbf{v}} \mid \mathbf{v} = \begin{pmatrix} \gamma \\ 0 \end{pmatrix} \gamma \in \mathbb{N} \right\}$, avec pour $\mathbf{v} = \begin{pmatrix} \gamma \\ 0 \end{pmatrix}$, $\mathcal{O}_{\mathbf{v}} = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \mid \mathrm{pgcd}(a, b) = \gamma \right\}$.

Le stabilisateur de $\begin{pmatrix} d \\ 0 \end{pmatrix}$ pour $d > 0$ est $\left\{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \mid y = \pm 1 \right\} \subset \mathrm{GL}(2, \mathbb{Z})$.

Exemple 6.2.18. — Quitte à identifier $\mathbb{Z}/2\mathbb{Z}$ au sous-groupe $\{\mathrm{id}, -\mathrm{id}\}$ de $\mathrm{GL}(n, \mathbb{R})$ nous obtenons une action de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{R}^n$ où 0 agit comme l'identité et 1 agit comme « prendre l'opposé ». Nous pouvons restreindre cette action à la sphère unitaire de $\mathbb{R}^n$; l'action obtenue s'appelle alors l'action antipodale puisque ses orbites sont des paires de points opposés sur la sphère.

6.2.1. Quelques exemples d'actions. —

6.2.1.1. *Exemple fondamental : action par translation.* — On reprend l'exemple fondamental 6.1.3.1 de l'action par translation à gauche.

Exemple 6.2.19. — L'action de G sur lui-même par translation à gauche

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, x) \mapsto g \cdot x = gx$$

est simplement transitive (Exemple 6.2.4), donc fidèle. Puisqu'elle est transitive elle possède une unique orbite.

Pour tout $a \in \mathrm{G}$ et tout $g \in \mathrm{G}$ on a $g \cdot a = a$ si et seulement si $ga = a$, si et seulement si $gaa^{-1} = aa^{-1}$ si et seulement si $g = e$. Ainsi le stabilisateur de tout point est réduit à l'élément neutre.

Cette constatation et la Remarque 6.2.2 permettent de conclure qu'à part dans le cas trivial $\mathrm{G} = \{e\}$ l'action ne possède pas de point fixe.

Exemple 6.2.20. — Soit H un sous-groupe de G, pas nécessairement distingué. On a vu Exemple 6.1.3 que

$$\mathrm{G} \times {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}, \qquad (g, a\mathrm{H}) \mapsto g \cdot (a\mathrm{H}) = (ga)\mathrm{H}.$$

définissait une action de groupe.

Cette action possède les propriétés suivantes :

- ⋄ il y a une seule orbite, c'est-à-dire $\mathcal{O}_{\mathrm{H}} = {}^{\mathrm{G}}\!/_{\mathrm{H}}$; en effet pour tout élément $g\mathrm{H}$ de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ nous avons $g\mathrm{H} = g \cdot \mathrm{H}$, *i.e.* $g\mathrm{H}$ appartient à $\mathcal{O}_{\mathrm{H}}$.
- ⋄ le stabilisateur de $a\mathrm{H}$ est

$$\mathrm{St}(a\mathrm{H}) = \{g \in \mathrm{G} \mid g \cdot a\mathrm{H} = a\mathrm{H}\} = \{g \in \mathrm{G} \mid a^{-1}ga\mathrm{H} = \mathrm{H}\} = \{g \in \mathrm{G} \mid a^{-1}ga \in \mathrm{H}\} = a\mathrm{H}a^{-1}.$$

- ⋄ il n'y a pas de point fixe dès que $\mathrm{H} \neq \mathrm{G}$.

Cette opération est transitive : pour a, $b \in \mathrm{G}$, nous avons $(ba^{-1})a\mathrm{H} = b\mathrm{H}$.

Cette action n'est pas fidèle en général : si $\varphi \colon \mathrm{G} \to \mathfrak{S}_{\mathrm{G}/\mathrm{H}}$ est le morphisme associé, alors

$$\ker \varphi = \bigcap_{a \in \mathrm{G}} a\mathrm{H}a^{-1}.$$

C'est en fait l'exemple « générique » d'une action transitive comme le montrera le Théorème 6.4.3.

Exemple 6.2.21. — On peut faire agir $\mathbb{R}^n$ sur lui-même par translation : soit $v \in \mathbb{R}^n$, considérons $T_v \colon \mathbb{R}^n \to \mathbb{R}^n$, $w \mapsto w + v$. D'une part $w + 0 = w$ se réecrit $T_0(w) = w$; d'autre part $(w + v_2) + v_1 = w + (v_1 + v_2)$ se réecrit $T_{v_1}(T_{v_2}(w)) = T_{v_1+v_2}(w)$.

Exemple 6.2.22. — Considérons l'action de $\mathrm{G} = {}^{\mathbb{Z}}\!/_{4\mathbb{Z}}$ sur lui-même ($X = \mathrm{G}$) par addition. Par exemple, l'action de l'addition par 1 a pour effet $0 \mapsto 1$, $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 0$. Ainsi l'action de l'addition par 1 sur ${}^{\mathbb{Z}}\!/_{4\mathbb{Z}}$ coïncide avec l'action du 4-cycle $(0\ 1\ 2\ 3)$. L'action de l'addition par 2 a pour effet $0 \mapsto 2$, $1 \mapsto 3$, $2 \mapsto 0$, $3 \mapsto 1$. Par suite l'action de l'addition par 2

sur $\mathbb{Z}/4\mathbb{Z}$ coïncide avec l'action du produit de 2-cycles $(0\ 2)(1\ 3)$. La composition de ces deux permutations est $(0\ 1\ 2\ 3)(0\ 2)(1\ 3) = (0\ 3\ 2\ 1)$; l'action de l'addition par 3 coïncide donc avec l'action du 4-cycle $(0\ 3\ 2\ 1)$.

6.2.1.2. *Exemple fondamental : action par conjugaison.* — On reprend l'Exemple 6.1.3.2.

Exemple 6.2.23. — On considère l'action de G sur lui-même par conjugaison : pour tous g et x dans G, $g \cdot x = gxg^{-1}$. On a vu Exemple 6.2.5 que cette action est fidèle si et seulement si Z(G), son centre, est réduit à l'élément neutre et qu'elle est transitive si et seulement si $\mathrm{G} = \{e\}$.
Nous avons les propriétés suivantes :

- ◇ l'orbite de a est $\mathcal{O}_a = \{g \cdot a \mid g \in \mathrm{G}\} = \{gag^{-1} \mid g \in \mathrm{G}\}$, *i.e.* l'orbite de a est la classe de conjugaison de a ;
- ◇ le stabilisateur de a dans G est le centralisateur de a dans G ; en effet

$$\mathrm{St}(a) = \{g \in \mathrm{G} \mid g \cdot a = a\} = \{g \in \mathrm{G} \mid gag^{-1} = a\} = \{g \in \mathrm{G} \mid ga = ag\} = Z_a;$$

- ◇ un point fixe sous l'action de G commute à tous les éléments de G, *i.e.* appartient au centre de G. En effet, $x \in X$ est fixe sous l'action de G si pour tout $g \in \mathrm{G}$ $g \cdot x = x$, *i.e.* si pour tout $g \in \mathrm{G}$ $gxg^{-1} = x$ ou encore si pour tout $g \in \mathrm{G}$ $gx = xg$.

Exemple 6.2.24. — Notons X l'ensemble des sous-groupes de G. On a vu Exemple 6.1.6 que le groupe G agissait sur X par automorphisme intérieur : $g \cdot \mathrm{H} = g\mathrm{H}g^{-1}$.

On dit que H et $g\mathrm{H}g^{-1}$ sont *conjugués*.
Nous avons les propriétés suivantes :

- ◇ $\mathrm{St}_{\mathrm{G}}(\mathrm{H}) = \{g \in \mathrm{G} \mid g\mathrm{H}g^{-1} = \mathrm{H}\} = \mathrm{N}_{\mathrm{G}}(\mathrm{H}) =$ le normalisateur de H ;
- ◇ un point fixe de l'action est un sous-groupe distingué de G.

Par exemple dans $\mathfrak{S}_3$ considérons les trois sous-groupes à deux éléments :

$$\mathrm{H}_3 = \{\mathrm{id}, (1\ \ 2)\}, \qquad \mathrm{H}_2 = \{\mathrm{id}, (1\ \ 3)\}, \qquad \mathrm{H}_1 = \{\mathrm{id}, (2\ \ 3)\}$$

Pour tout $i \neq j$ on a

$$(i\ \ j)\mathrm{H}_{\mathrm{k}}(i\ \ j) = \mathrm{H}_k \quad \text{si } k \notin \{i, j\} \quad \text{et} \quad (i\ \ j)\mathrm{H}_{\mathrm{k}}(i\ \ j) = \mathrm{H}_i \quad \text{si } k = i$$

Ainsi ces trois groupes sont conjugués et ils sont leur propre normalisateur.

Proposition-Définition 6.2.2

Soit H un sous-groupe d'un groupe G. Le *normalisateur* de H dans G est

$$\mathrm{N_G(H)} = \{g \in \mathrm{G} \mid g\mathrm{H}g^{-1} = \mathrm{H}\};$$

Il s'agit du stabilisateur de H par l'action par conjugaison de G sur l'ensemble de ses sous-groupes.
On a $\mathrm{H} \triangleleft \mathrm{N_G(H)}$ et $\mathrm{N_G(H)}$ est le plus grand sous-groupe de G ayant cette propriété.

Démonstration. — Le fait que H soit distingué dans $\mathrm{N_G(H)}$ est tautologique.

Soit K un sous-groupe de G tel que $\mathrm{H} \triangleleft \mathrm{K}$. Comme H est distingué dans K, pour tout $g \in \mathrm{K}$ on a $g\mathrm{H}g^{-1} = \mathrm{H}$. C'est-à-dire $g \in \mathrm{N_G(H)}$. On en déduit que $\mathrm{K} \subset \mathrm{N_G(H)}$. □

Les deux énoncés qui suivent témoignent à nouveau du rôle capital de la notion de conjugaison. Le premier affirme que les stabilisateurs sur une même orbite sont conjugués.

Proposition 6.2.4

Soit G agissant sur l'ensemble X.
Pour tout $g \in \mathrm{G}$ et tout $x \in X$ on a

$$\mathrm{St_G}(g \cdot x) = g\,\mathrm{St_G}(x)\,g^{-1}.$$

Démonstration. — Soit $g' \in \mathrm{St_G}(g \cdot x)$. On a alors $g' \cdot (g \cdot x) = g \cdot x$. Ce qui implique $(g^{-1}g'g) \cdot x = x$. Ainsi $(g^{-1}g'g) \in \mathrm{St_G}(x)$ et le résultat en découle. □

Remarque 6.2.5. — Si deux points sur une même orbite ont des stabilisateurs conjugués, la réciproque n'est pas vraie en général : les points avec des stabilisateurs conjugués n'appartiennent pas nécessairement à la même orbite. Même des points ayant un même stabilisateur n'appartiennent pas nécessairement à la même orbite. Par exemple, si $\mathcal{A}_4$ agit sur lui-même par conjugaison, alors $(1\ 2\ 3)$ et $(1\ 3\ 2)$ appartiennent à des orbites différentes (ils ne sont pas conjugués dans $\mathcal{A}_4$) mais $\mathrm{St}_{\mathcal{A}_4}((1\ 2\ 3)) = \mathrm{St}_{\mathcal{A}_4}((1\ 3\ 2)) = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$.

Le second énoncé fait le lien entre point fixe et sous-groupes conjugués dans le cas de l'action par translation à gauche.

Proposition 6.2.5

Soient G un groupe, H et K deux de ses sous-groupes. On considère l'action de K sur G/H par translation à gauche.
Alors $a\mathrm{H}$ est un point fixe de cette action si et seulement si $\mathrm{K} \subset a\mathrm{H}a^{-1}$.

Démonstration. — On a : $a\mathrm{H}$ point fixe de cette action si et seulement si pour tout $k \in \mathrm{K}$ on a $k \cdot a\mathrm{H} = ka\mathrm{H} = a\mathrm{H}$. Ainsi pour tout $k \in \mathrm{K}$ et tout $h \in \mathrm{H}$ il existe $h' \in \mathrm{H}$ tel que $kah = ah'$.

On a donc $k = ah'h^{-1}a^{-1} \in a\mathrm{H}a^{-1}$. Ce qui permet de conclure que $\mathrm{K} \subset a\mathrm{H}a^{-1}$.
Réciproquement, si $\mathrm{K} \subset a\mathrm{H}a^{-1}$ alors pour tout $k \in \mathrm{K}$ on a $h \in \mathrm{H}$ tel que $k = aha^{-1}$. Ainsi $k \cdot a\mathrm{H} = aha^{-1}a\mathrm{H} = ah\mathrm{H} = a\mathrm{H}$. Tout élément de K est un point fixe de l'action.

□

Exemple 6.2.25. — Soit $\Bbbk$ un corps commutatif, soit $\mathrm{G} = \mathrm{GL}(n, \Bbbk)$ le groupe des matrices carrées d'ordre n inversibles à coefficients dans $\Bbbk$. Considérons l'action de G sur lui-même par conjugaison. Les classes de conjugaison regroupent les matrices semblables ; en effet, l'orbite de $A \in \mathrm{GL}(n, \Bbbk)$ qui est aussi la classe de conjugaison de A est donnée par

$$\mathcal{O}_A = \{g \cdot A \,|\, g \in \mathrm{GL}(n, \Bbbk)\} = \{gAg^{-1} \,|\, g \in \mathrm{GL}(n, \Bbbk)\} = \{ \text{ matrices semblables à } A \}$$

Exemple 6.2.26. — Le groupe $\mathrm{GL}(n, \Bbbk) \times \mathrm{GL}(n, \Bbbk)$ agit sur $M(n, \Bbbk)$ par $(A, B) \cdot M = AMB^{-1}$. Les orbites regroupent les matrices de même rang (voir Chapitre 9).

6.3. Quelques propriétés des actions de groupes

Orbites et stabilisateurs sont liés par l'énoncé suivant dans lequel sont reprises les notations du Corollaire 1.1.1 du Chapitre 1 :

Proposition 6.3.1

Soit G un groupe agissant sur un ensemble X.
Soit $x \in X$ on note $f \colon \mathrm{G} \to \mathcal{O}_x$, $g \mapsto g \cdot x$.
On a $f(g) = f(g')$ si est seulement si $g\mathrm{St}_\mathrm{G}(x) = g'\mathrm{St}_\mathrm{G}(x)$. De plus l'application

$$\widetilde{f} \colon \mathrm{G}/\mathrm{St}_\mathrm{G}(x) \to \mathcal{O}_x, \qquad \overline{g} \mapsto g \cdot x$$

est bien définie et c'est une bijection.
Lorsque G est fini, nous avons donc $\#\mathcal{O}_x = \frac{|\mathrm{G}|}{|\mathrm{St}_\mathrm{G}(x)|}$.

Démonstration. — Soit $x \in X$. L'application $f \colon \mathrm{G} \to \mathcal{O}_x$, $g \mapsto g \cdot x$ est bien définie et c'est une surjection.
Soient g et g' dans G ; on a $f(g) = f(g')$ si et seulement si $g \cdot x = g' \cdot x$, ce qui équivaut aussi à $(g'g^{-1}) \cdot x = x$. Cette dernière égalité signifiant que $g'g^{-1} \in \mathrm{St}_\mathrm{G}(x)$, ou encore que $g\mathrm{St}_\mathrm{G}(x) = g'\mathrm{St}_\mathrm{G}(x)$.
Ainsi on a $\mathrm{G}/\mathrm{St}_\mathrm{G}(x) = \mathrm{G}/\mathcal{R}_f$.
Puisque f est surjective, le Corollaire 1.1.1 nous permet de conclure que l'application $\widetilde{f} \colon \mathrm{G}/\mathrm{St}_\mathrm{G}(x) \to \mathcal{O}_x$ est une bijection.
Si G est fini, tous les ensembles le sont et la bijection nous indique que $\mathrm{G}/\mathrm{St}_\mathrm{G}(x)$ et $\mathcal{O}_x$ ont le même nombre d'éléments. Alors $\#\mathcal{O}_x = \dfrac{|\mathrm{G}|}{|\mathrm{St}_\mathrm{G}(x)|}$ (Théorème 1.6.3).

□

Exemple 6.3.1. — Soient $n \geq 1$ et $k \in \{1, 2, \ldots, n-1\}$; le groupe $\mathrm{G} = \mathfrak{S}_n$ agit sur les sous-ensembles de $\{1, 2, \ldots, n\}$ de cardinal k comme suit :

$$\sigma(\{i_1, i_2, \ldots, i_k\}) = \{\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k)\}.$$

Cette action de groupe a une orbite car $\{i_1, i_2, \ldots, i_k\} = \sigma(\{1, 2, \ldots, k\})$ où σ est la permutation $\begin{pmatrix} 1 & 2 & \ldots & k \\ i_1 & i_2 & \ldots & i_k \end{pmatrix}$.

Le nombre de sous-ensembles de $\{1, 2, \ldots, n\}$ de cardinal k est $\binom{n}{k}$. La Proposition 6.3.1 assure que

$$\binom{n}{k} = \frac{|\mathfrak{S}_n|}{|\mathrm{St}_{\mathfrak{S}_n}(\{1, 2, \ldots, k\})|}.$$

Un élément de $\mathrm{St}_{\mathfrak{S}_n}(\{1, 2, \ldots, k\})$ est une permutation σ de $\mathfrak{S}_n$ telle que

$$\{\sigma(1), \sigma(2), \ldots, \sigma(k)\} = \{1, 2, \ldots, k\},$$

c'est-à-dire une permutation de $\mathfrak{S}_n$ qui induit une permutation de $\mathfrak{S}_k$ et une permutation de $\mathfrak{S}_{n-k}$. Ainsi $\mathrm{St}_{\mathfrak{S}_n}(\{1, 2, \ldots, k\}) \simeq \mathfrak{S}_k \times \mathfrak{S}_{n-k}$; en particulier, $|\mathrm{St}_{\mathfrak{S}_n}(\{1, 2, \ldots, k\})| = k!(n-k)!$. Finalement $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Exemple 6.3.2. — Soit G un groupe fini. Soient H et K des sous-groupes de G. Nous allons justifier la relation : $\#\mathrm{HK} = \frac{|\mathrm{H}|\,|\mathrm{K}|}{|\mathrm{H} \cap \mathrm{K}|}$. Ici $\mathrm{HK} = \{hk \mid h \in \mathrm{H},\, k \in \mathrm{K}\}$ est l'ensemble des produits, qui n'est généralement qu'un sous-ensemble (pas un sous-groupe) de G. Considérons l'action du groupe $\mathrm{H} \times \mathrm{K}$ sur G définie par :

$$(\mathrm{H} \times \mathrm{K}) \times \mathrm{G}, \qquad\qquad ((h, k), g) \mapsto (h, k) \cdot g = hgk^{-1}$$

Vérifier que c'est bien une action de groupe (le groupe est $\mathrm{H} \times \mathrm{K}$ et l'ensemble est G). Remarquons que HK est l'orbite de e. Par suite nous avons d'après la Proposition 6.3.1

$$\#\mathrm{HK} = \frac{|\mathrm{H} \times \mathrm{K}|}{|\mathrm{St}_{\mathrm{H} \times \mathrm{K}}(e)|}$$

Mais (h, k) appartient à $\mathrm{St}_{\mathrm{H} \times \mathrm{K}}(e)$ si et seulement si $(h, k) \cdot e = e$, *i.e.* si et seulement si $hk^{-1} = e$, donc $\mathrm{St}_{\mathrm{H} \times \mathrm{K}}(e) = \{(h, h) \mid h \in \mathrm{H} \cap \mathrm{K}\}$ ensemble qui a le même cardinal que $\mathrm{H} \cap \mathrm{K}$. Finalement, nous avons : $\#\mathrm{HK} = \frac{|\mathrm{H} \times \mathrm{K}|}{|\mathrm{H} \cap \mathrm{K}|}$.

Corollaire 6.3.1

Soit G un groupe fini qui agit sur un ensemble X.

- ◇ Soit x dans X. Le cardinal de $\mathcal{O}_x$ divise $|\mathrm{G}|$.
- ◇ Deux points d'une même orbite ont des stabilisateurs conjugués ; en particulier, l'ordre des stabilisateurs des points d'une même orbite est le même.

Démonstration. —

- ◇ Ceci découle directement de l'égalité $\#\mathcal{O}_x\,|\mathrm{St}_{\mathrm{G}}(x)| = |\mathrm{G}|$ (Proposition 6.3.1).
- ◇ Il s'agit d'appliquer la Proposition 6.2.4 dans le cas d'un groupe fini.

□

Exemple 6.3.3. — Considérons le groupe $\mathrm{G} = \mathrm{GL}(2, \mathbb{R})$. Les matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{G}$ telles que $a + c = b + d = 1$ forment un sous-groupe H. On peut le voir en observant que les sommes des colonnes sont les entrées du produit vectoriel-matrice $\begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$; les éléments de H sont les matrices qui satisfont $\begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \end{pmatrix}$. Ainsi H est le stabilisateur de $\begin{pmatrix} 1 & 1 \end{pmatrix}$ dans l'action (à droite !) de G sur $\mathbb{R}^2$ – vu comme vecteurs lignes – par $\mathbf{v} \cdot A = \mathbf{v}A$. Ainsi H est un sous-groupe de G puisque les stabilisateurs d'un point sont toujours un sous-groupe. De plus, comme $\begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \end{pmatrix}$, les sous-groupes $\mathrm{St}_{\mathrm{G}}(\begin{pmatrix} 1 & 1 \end{pmatrix})$ et $\mathrm{St}_{\mathrm{G}}(\begin{pmatrix} 0 & 1 \end{pmatrix})$ sont conjugués dans G (Corollaire 6.3.1). Puisque $\mathrm{St}_{\mathrm{G}}(\begin{pmatrix} 0 & 1 \end{pmatrix}) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{G} \right\} = \mathrm{Aff}(\mathbb{R})$, nous avons

$$\mathrm{H} = \mathrm{St}_{\mathrm{G}}(\begin{pmatrix} 1 & 1 \end{pmatrix}) = \mathrm{St}_{\mathrm{G}}\left(\begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \right) = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{-1} \mathrm{Aff}(\mathbb{R}) \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

La *formule des classes* n'est que la reformulation du fait qu'un ensemble sur lequel un groupe G agit est réunion disjointe des orbites. Son intérêt provient du fait que lorsque G est fini, le cardinal de chaque orbite divise $|\mathrm{G}|$.

Proposition 6.3.2: Formule des classes

Soit G un groupe fini agissant sur un ensemble fini X. Supposons que les différentes orbites de X soient représentées par x_1, x_2, …, x_ℓ. Alors

$$\#X = \sum_{i=1}^{\ell} \#\mathcal{O}_{x_i} = \sum_{i=1}^{\ell} \frac{|\mathrm{G}|}{|\mathrm{St}_{\mathrm{G}}(x_i)|}.$$

Démonstration. — L'ensemble X peut s'écrire comme l'union de ses orbites, deux à deux disjointes. La Proposition 6.3.1 permet de conclure. □

Exemple 6.3.4. — Considérons l'action de G sur lui-même par conjugaison

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, h) \mapsto g \cdot h = ghg^{-1}.$$

L'orbite d'un élément h de G est égale à $\{h\}$ si et seulement si h appartient à $Z(\mathrm{G})$ (*voir* §6.2.23). De plus si h appartient à G, alors $\mathrm{St}(h) = Z_h$ où Z_h désigne le centralisateur de h (*voir* §6.2.23). Si G est fini, si $\mathcal{O}_{g_1}$, $\mathcal{O}_{g_2}$, …, $\mathcal{O}_{g_q}$ sont les orbites de G qui contiennent plus d'un élément, la formule des classes se réécrit

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{q} \#\mathcal{O}_{g_i} = |Z(\mathrm{G})| + \sum_{i=1}^{q} \frac{|\mathrm{G}|}{Z_{g_i}}.$$

Exemple 6.3.5. — Dans un groupe fini G, le cardinal de chaque classe de conjugaison divise $|\mathrm{G}|$ puisque les classes de conjugaison sont des orbites pour l'action par conjugaison de G sur lui-même.

Par exemple, les classes de conjugaisons de $\mathrm{G} = \mathfrak{S}_3$ sont $\{\mathrm{id}\}$, $\{(1\ 2\ 3), (1\ 3\ 2)\}$ et $\{(1\ 2), (1\ 3), (2\ 3)\}$ (Exemples 5.1.19). Elles sont de cardinal 1, 2 et 3 ; tous ces nombres sont des diviseurs de 6. La Proposition 6.3.2 permet de retrouver que $6 = 1 + 2 + 3$. Les classes de conjugaison de $\mathrm{G} = \mathfrak{S}_4$ sont $\{\mathrm{id}\}$, les six transpositions, les trois doubles transpositions, les huit 3-cycles et les six 4-cycles (Exemples 5.1.19). Elles sont de cardinal 1, 6, 3, 8 et 6 ; tous ces nombres sont des diviseurs de 24 et la Proposition 6.3.2 permet de retrouver que $24 = 1 + 6 + 3 + 8 + 6$.

Exemple 6.3.6. — Quels éléments de D_{12} commutent avec la réflexion s ? Autrement dit peut-on décrire $Z_s = \{g \in \mathrm{D}_{12} \mid gs = sg\}$? Les éléments id, s et r^3 appartiennent à Z_s.

Remarquons que $gs = sg$ se réécrit $gsg^{-1} = s$: il s'agit donc de déterminer le stabilisateur de s lorsque D_{12} agit sur lui-même par conjugaison. Déterminons d'abord l'orbite de g : combien y a-t-il d'éléments gsg^{-1} distincts lorsque g parcourt D_{12} ? Les éléments de D_{12} sont les r^k (rotations) et $r^k s$ (réflexions, donc égales à leurs inverses). À partir de

$$r^k s r^{-k} = r^{2k} s \qquad (r^k s) s (r^k s)^{-1} = r^k s s r^k s = r^k r^k s = r^{2k} s$$

nous obtenons que $\{gsg^{-1} \mid g \in \mathrm{D}_{12}\} = \{r^{2p} s\} = \{s, r^2 s, r^4 s\}$. Puisque le cardinal de l'orbite de s est 3, l'ordre du stabilisateur de s est $\frac{|\mathrm{D}_{12}|}{3} = \frac{12}{3} = 4$. Les éléments id, s et r^3 appartiennent

au stabilisateur de s ; ce dernier étant un groupe, il contient aussi r^3s. Nous avons donc les quatre éléments de $\mathrm{St}_{\mathrm{D}_{12}}(s)$. Finalement $Z_s = \{\mathrm{id},\, s,\, r^3,\, r^3s\}$.

Lorsque l'on considère une action de groupe, le cardinal d'une orbite divise $|\mathrm{G}|$, mais le nombre d'orbites ne divise généralement pas $|\mathrm{G}|$. Par exemple, les groupes D_8 et $\mathbb{H}_8$ ont chacun 5 classes de conjugaison, et 5 ne divise pas 8. Mais il existe une relation intéressante entre le nombre d'orbites et l'action de groupe :

Théorème 6.3.1

Soit G un groupe fini agissant sur un ensemble fini X avec r orbites. Alors r est le nombre moyen de points fixes des éléments du groupe :

$$r = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \#\mathtt{fixe}_X(g)$$

où on rappelle que $\mathtt{fixe}_X(g) = \{x \in X \mid g \cdot x = x\}$ est l'ensemble des éléments de X fixés par g.

Remarque 6.3.1. — Lorsque l'action est transitive, le nombre d'orbites vaut 1 donc le nombre moyen de points fixes des éléments du groupe est 1.

Par exemple si $\mathrm{G} = \mathfrak{S}_n$ agit sur $X = \{1,\, 2,\, \ldots,\, n\}$, alors le nombre moyen de points fixes d'une permutation est exactement 1.

Démonstration. — Nous allons déterminer le cardinal de $\{(g, x) \in \mathrm{G} \times X \mid g \cdot x = x\}$ de deux manières distinctes.

- ◇ D'une part
$$\#\{(g, x) \in \mathrm{G} \times X \mid g \cdot x = x\} = \sum_{g \in \mathrm{G}} \#\mathtt{fixe}_X(g).$$
- ◇ D'autre part
$$\#\{(g, x) \in \mathrm{G} \times X \mid g \cdot x = x\} = \sum_{x \in X} |\mathrm{St}_{\mathrm{G}}(x))|.$$

Nous en déduisons que

$$\sum_{g \in \mathrm{G}} \#\mathtt{fixe}_X(g) = \sum_{x \in X} |\mathrm{St}_{\mathrm{G}}(x)|.$$

La Proposition 6.3.1 assure que

$$\sum_{g \in \mathrm{G}} \#\mathtt{fixe}_X(g) = \sum_{x \in X} \frac{|\mathrm{G}|}{\#\mathcal{O}_x}$$

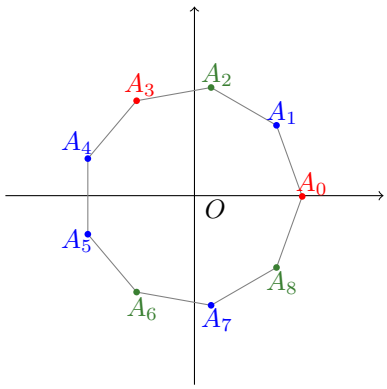
d'où

$$\frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \#\mathtt{fixe}_X(g) = \sum_{x \in X} \frac{1}{\#\mathcal{O}_x}$$

Considérons la somme $\sum_{x\in X} \frac{1}{\#\mathcal{O}_x}$. Si $\mathcal{O}_x$ compte n points, alors la somme des points de cette orbite est une somme de $\frac{1}{n}$ pour n termes, c'est-à-dire 1. Ainsi, la partie de la somme sur les points d'une orbite est 1, ce qui implique que $\sum_{x\in X} \frac{1}{\#\mathcal{O}_x}$ est égale au nombre d'orbites, qui est r. □

Exemple 6.3.7. — On considère les colliers de 9 perles que l'on peut faire avec 4 perles bleues, 3 perles vertes et 2 perles rouges.

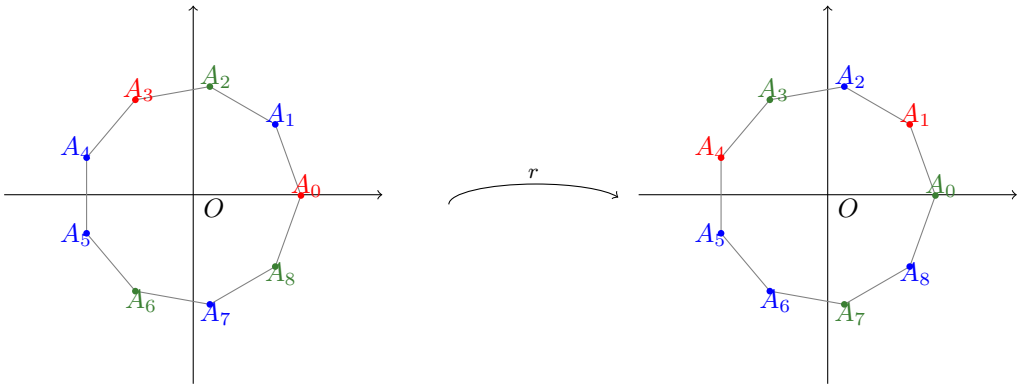
On représente un collier par un cercle du plan euclidien orienté $\mathbb{R}^2$ (de centre O et de rayon 1) muni de neuf points A_0, A_1, …, A_8 disposés à intervalles réguliers. Pour fixer les idées, on peut poser A_k comme étant le point d'affixe $e^{\mathbf{i}\frac{2k\pi}{9}}$. Ces neuf points sont les sommets d'un ennéagone, polygone régulier à neuf côtés, et un collier correspond à l'ornement de chacun de ses sommets avec une des perles colorées. Avant de réaliser un collier on fait son patron en choisissant la couleur de la perle qui sera fixée sur chacun des sommets.



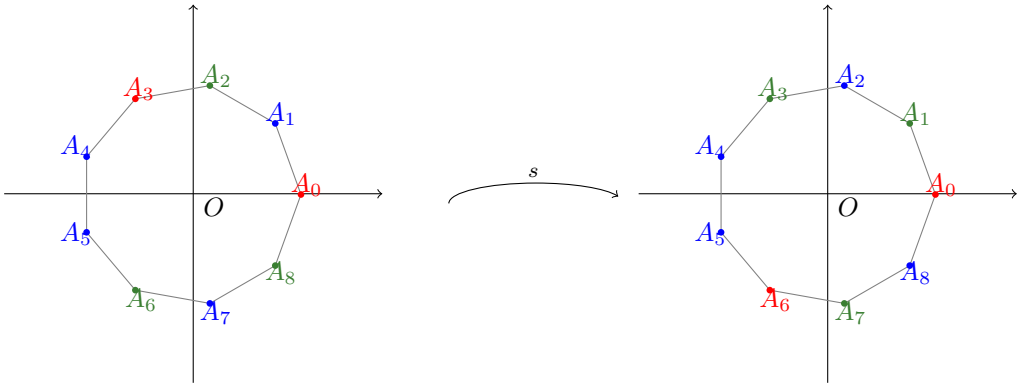
Deux patrons sont dits équivalents si après confection ils mènent à la fabrication du même collier. Un collier est inchangé par rotation plane, ou s'il est retourné « comme une crêpe »dans l'espace de dimension 3.

Combien de colliers différents peut-on faire ?

Les colliers, inchangés par rotation, font que deux patrons obtenus par rotation l'un de l'autre sont équivalents. C'est en particuler le cas sous l'effet de la rotation d'angle $\frac{2\pi}{9}$. On la note r. Autrement dit, si l'on fait « tourner d'un cran » les couleurs, pour $0 \leq i \leq 7$ la couleur en A_i se fixe en A_{i+1}, celle de A_8 venant se poser en A_0, on n'obtient un patron équivalent.



Quant à l'invariance par « retournement comme une crêpe » elle affirme par exemple qu'un patron et son image obtenue par la rotation de l'espace d'angle π autour de l'axe $\Delta = (OA_0)$ sont équivalents. Cette rotation a sur les couleurs des sommets le même effet que la symétrie orthogonale d'axe $\Delta = (OA_0)$ que l'on note s. C'est-à-dire que A_0 ne change pas de couleur quand, pour tout $k \in [\![1, 4]\!]$, celles sur A_k et sur A_{9-k} sont permutées.



Autrement dit, le groupe diédral $\mathrm{G} = \mathrm{D}_{18} = \langle r, s \rangle$ des isométries d'un polygône régulier à neuf côtés agit sur l'ensemble X des patrons. Le groupe G est un sous-groupe de $\mathrm{SO}(2, \mathbb{R})$ d'ordre 18 ; ses éléments sont les suivants

$$\mathrm{id},\ r,\ r^2,\ r^3,\ r^4,\ r^5,\ r^6,\ r^7,\ r^8,\ s,\ rs,\ r^2s,\ r^3s,\ r^4s,\ r^5s,\ r^6s,\ r^7s,\ r^8s$$

où on rappelle que r est la rotation de centre O et d'angle $\frac{2\pi}{9}$ et s est la symétrie orthogonale d'axe $\Delta = (OA_0)$. En particulier, G contient neuf rotations et neuf symétries orthogonales.

Désignons par $\Omega = \{\mathcal{O}_x \mid x \in X\}$ l'ensemble des orbites de l'action de G sur X.

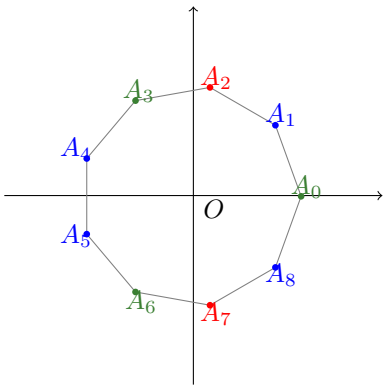
Le nombre de colliers est exactement le nombre d'orbites dans l'action de G sur X, *i.e.* $\#\Omega$. On calcule ce nombre à l'aide du Théorème 6.3.1 :

$$\#\Omega = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \#\mathtt{fixe}_X(g).$$

Remarquons qu'un point fixe est un patron qui est inchangé par l'action de g.

Déterminons $\mathtt{fixe}_X(g)$ pour tout g dans G. Soit $g \in \mathrm{G}$.

- Si $g = \mathrm{id}$, alors $\mathtt{fixe}_X(g) = X$.
- Si $g \in \{r, r^2, r^4, r^5, r^7, r^8\}$, alors le sous-groupe de G engendré par g est constitué des neuf rotations (r^k engendre ce groupe si et seulement si k est premier avec 9). Donc un patron fixe par g est fixe par r ce qui implique que toutes les perles sont de la même couleur. Ceci n'est pas possible. Par suite $\mathtt{fixe}_X(g) = \emptyset$.
- Si $g \in \{r^3, r^6\}$, alors dans un patron fixe par g le nombre de perles d'une couleur donnée doit être un multiple de 3. En effet les couleurs des sommets indexés par i, $i+3$ et $i+6$ modulo 9 doivent avoir la même couleur. Nos patrons ayant seulement deux sommets en rouge on a $\mathtt{fixe}_X(g) = \emptyset$.
- Si g est une symétrie, nous pouvons supposer que $g = s$, les autres cas étant identiques. Puisque l'axe Δ de g ne contient que la perle A_0, dans un patron fixe par g, les perles A_i, $i \neq 1$, vont par paire de même couleur. Cela assure que la perle A_0 est nécessairement verte. Se donner un patron fixe par g revient alors à se donner les couleurs des perles A_1, A_2, A_3, A_4 de sorte que 2 soient bleues, 1 verte et 1 rouge.



Il est clair que le nombre de tels patrons vaut

$$\mathtt{fixe}_X(g) = \binom{4}{2}\binom{2}{1} = 6 \times 2 = 12.$$

Enfin le cardinal de X est

$$\#X = \binom{9}{4}\binom{5}{3} = 126 \times 10 = 1260.$$

On en déduit que

$$\#\Omega = \frac{1}{18}\Big(1260 + 9 \times 12\Big) = 76.$$

Les 1260 patrons différents permettent donc de confectionner 76 colliers différents.

Il y a donc 76 colliers distincts satisfaisant les contraintes de l'énoncé.

Exemple 6.3.8. — Nous utiliserons un cas particulier du Théorème 6.3.1 pour montrer que pour tout entier relatif a et pour tout entier naturel m nous avons

$$\sum_{k=1}^{m} a^{\mathrm{pgcd}(k,m)} \equiv_m 0. \tag{6.3.1}$$

Lorsque $m = p$ est un nombre premier, le membre de gauche de (6.3.1) est $(p-1)a + ap = (ap - a) + pa$, donc (6.3.1) se réécrit $ap \equiv_p a$, qui est le petit théorème de Fermat (Corollaire 1.5.3). Ainsi (6.3.1) peut être considéré comme une généralisation du petit théorème de Fermat qui est essentiellement différente de la généralisation appelée théorème d'Euler (Corollaire 1.5.2), qui dit que $a^{\phi(m)} \equiv_m 1$ si $\mathrm{pgcd}(a, m) = 1$: l'équation (6.3.1) est vraie pour tout $a \in \mathbb{Z}$.

Soit G un groupe fini. Pour tout entier positif a, le groupe G agit sur l'ensemble $\mathcal{F}$ des fonctions définies sur G et à valeurs dans $\{1, 2, \ldots, a\}$) par $(g \cdot \mathfrak{f})(h) = \mathfrak{f}(g^{-1}h)$ pour g, $h \in \mathrm{G}$ (c'est un cas particulier de l'Exemple 6.1.18). Afin d'appliquer le Théorème 6.3.1 à cette action, nous devons donc comprendre les points fixes de chaque $g \in \mathrm{G}$. Nous avons $g \cdot \mathfrak{f} = \mathfrak{f}$ si et seulement si $\mathfrak{f}(g^{-1}h) = \mathfrak{f}(h)$ pour tout $h \in \mathrm{G}$, ce qui revient à dire que $\mathfrak{f}$ est constante sur chaque classe à droite $\langle g \rangle h$ dans G. En effet, si $\mathfrak{f}(g^{-1}h) = \mathfrak{f}(h)$ alors pour tout entier n on a $\mathfrak{f}(g^{-n}h) = \mathfrak{f}(h)$, ce qui implique que $\mathfrak{f}$ est constante sur $\langle g \rangle h$, puisque chaque élément de $|g|$ est de la forme g^{-n} pour un certain entier n. Réciproquement, si pour tout $g \in \mathrm{G}$ et tout $h \in \mathrm{G}$ $\mathfrak{f}$ est constante sur $\langle g \rangle h$, alors pour tout $g \in \mathrm{G}$ et tout $h \in \mathrm{G}$ on a $h \in \langle g \rangle h$ et $g^{-1}h \in \langle g \rangle h$, donc $\mathfrak{f}(g^{-1}h) = \mathfrak{f}(h)$. Ce qui prouve que $\mathfrak{f} \in \mathtt{fixe}_{\mathcal{F}}(\mathrm{G})$.

Le nombre de classes à droite de $\langle g \rangle$ dans G est $[\mathrm{G} : \langle g \rangle] = \frac{m}{|\langle g \rangle|}$ (Théorème 1.6.3), où $m = |\mathrm{G}|$. Ainsi le nombre de fonctions fixées par g est $a^{\frac{m}{|\langle g \rangle|}}$, puisque la valeur de la fonction sur chaque classe à gauche peut être choisie arbitrairement dans $\{1, \ldots, a\}$. D'après le Théorème 6.3.1 la quantité $\frac{1}{m} \sum_{g \in \mathrm{G}} a^{\frac{m}{|\langle g \rangle|}}$ est un entier positif. Il en résulte que

$$\sum_{g \in \mathrm{G}} a^{\frac{m}{|\langle g \rangle|}} \equiv_m 0. \tag{6.3.2}$$

Puisque (6.3.2) dépend de a uniquement par la valeur de a modulo m, l'égalité est valable pour tout $a \in \mathbb{Z}$, pas seulement pour $a > 0$.
Ainsi on a montré

Proposition 6.3.3

Soit G un groupe fini d'ordre m. Pour tout entier $a \in \mathbb{Z}$ on a

$$\sum_{g \in \mathrm{G}} a^{\frac{m}{|\langle g \rangle|}} \equiv_m 0\cdot$$

Si $\mathrm{G} = \mathbb{Z}/m\mathbb{Z}$, alors tout élément $k \in \mathrm{G}$ est d'ordre $\frac{m}{\mathrm{pgcd}(k,m)}$; ainsi (6.3.2) devient

$$\sum_{k=1}^{m} a^{\mathrm{pgcd}(k,m)} \equiv_m 0.$$

Corollaire 6.3.2

Soit G un groupe fini non trivial agissant sur un ensemble fini X. Supposons d'une part que $\#X > 1$ et d'autre part que l'action est transitive (*i.e.* qu'il n'y a qu'une seule orbite). Alors G contient au moins un élément sans point fixe.

Démonstration. — Rappelons que $\mathtt{fixe}_X(g)$ désigne $\{x \in X \mid g \cdot x = x\}$. Le Théorème 6.3.1 assure que

$$1 = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \#\mathtt{fixe}_X(g) = \frac{1}{|\mathrm{G}|} \left(\#X + \sum_{g \neq e} \#\mathtt{fixe}_X(g) \right)$$

Raisonnons par l'absurde : supposons que tout élément g de G a au moins un point fixe. Alors

$$1 \geq \frac{1}{|\mathrm{G}|} \Big(\#X + |\mathrm{G}| - 1 \Big) = 1 + \frac{\#X - 1}{|\mathrm{G}|}.$$

Par conséquent $\#X - 1 \leq 0$ et $\#X = 1$: contradiction. □

Corollaire 6.3.3

Soit G un groupe fini. Soit H un sous-groupe propre de G. Alors $\mathrm{G} \neq \bigcup_{a \in \mathrm{G}} a\mathrm{H}a^{-1}$.

Remarque 6.3.2. — L'hypothèse « G fini » est indispensable dans le Corollaire 6.3.3. Par exemple, considérons le groupe $\mathrm{G} = \mathrm{GL}(2, \mathbb{C})$. Chaque élément de G a un vecteur propre ; on peut donc conjuguer chaque matrice de G à une matrice de la forme $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Alors $\mathrm{G} = \bigcup_{g \in \mathrm{G}} g\mathrm{H}g^{-1}$, où H désigne le sous-groupe propre des matrices triangulaires supérieures.

Démonstration. — Considérons l'action de G sur G/H par translation à gauche. Étant donné $g \in \mathrm{G}$, l'élément $a\mathrm{H} \in \mathrm{G}/\mathrm{H}$ est un point fixe de g pour l'action considérée si $g \cdot a\mathrm{H} = ga\mathrm{H} = a\mathrm{H}$. Ce qui est équivalent à $g \in a\mathrm{H}a^{-1}$. Comme cela est montré dans l'Exemple 6.2.5 l'action est transitive, alors le Corollaire 6.3.2 nous indique l'existence de $g \in \mathrm{G}$ sans point fixe. Ainsi, pour tout $a \in \mathrm{G}$, on a $g \notin a\mathrm{H}a^{-1}$. Ce qui exprime bien que l'on a $\bigcup_{a \in \mathrm{G}} a\mathrm{H}a^{-1} \subsetneq \mathrm{G}$. □

On en déduit l'énoncé :

Corollaire 6.3.4

Soit G un groupe fini. Si H est un sous-groupe propre de G, alors il existe une classe de conjugaison dans G distincte de H et de ses sous-groupes conjugués.

Démonstration. — Soient G un groupe fini et H un de ses sous-groupes propres. D'après le Corollaire 6.3.3 il existe $g \in \mathrm{G}$ tel que $g \notin \bigcup_{a \in \mathrm{G}} a\mathrm{H}a^{-1}$.
Pour tous a et b dans G on a donc $bgb^{-1} \notin a\mathrm{H}a^{-1}$. Le contraire mènerait à $g \in (b^{-1}a)\mathrm{H}(b^{-1}a)^{-1}$ qui est faux.
Alors on a : $\left\{bgb^{-1} \,|\, b \in \mathrm{G}\right\} \cap \bigcup_{a \in \mathrm{G}} a\mathrm{H}a^{-1} = \emptyset$. □

6.4. Actions transitives

Soit G un groupe agissant sur un ensemble X. Rappelons que G agit transitivement sur X si

$$\forall\, x \in X,\ \forall\, y \in X,\ \exists\, g \in \mathrm{G},\ g \cdot x = y$$

autrement dit s'il existe $x \in X$ tel que $\mathcal{O}_x = X$.

Exemple 6.4.1. — Soit $n \geq 1$ un entier. L'action usuelle de $\mathfrak{S}_n$ sur $\{1, 2, \ldots, n\}$

$$\mathfrak{S}_n \times \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}, \qquad (\sigma, k) \mapsto \sigma \cdot k = \sigma(k)$$

est transitive : soit $1 \leq p \leq n$, alors la transposition $(1\ p)$ envoie 1 sur p ; autrement dit l'orbite de 1 est $\{1, 2, \ldots, n\}$.

Exemple 6.4.2. — Soit $n \geq 3$ un entier. L'action de $\mathcal{A}_n$ sur $\{1, 2, \ldots, n\}$

$$\mathcal{A}_n \times \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}, \qquad (\sigma, k) \mapsto \sigma \cdot k = \sigma(k)$$

est transitive ; en effet, pour tout $1 \leq k \leq n$ le 3-cycle $(1\ k\ n)$ envoie 1 sur k. L'orbite de 1 est donc $\{1, 2, \ldots, n\}$.

Remarquons que l'hypothèse $n \geq 3$ est indispensable : $\mathcal{A}_2$ n'agit pas de manière transitive sur l'ensemble $\{1, 2\}$ puisque $\mathcal{A}_2$ est trivial.

Exemple 6.4.3. — Soit $n \geq 3$ un entier. L'action de $\mathrm{D}_{2n} = \langle r, s \,|\, r^n = e,\ s^2 = e,\ rsrs = e\rangle$ sur l'ensemble des sommets $\{A_1, A_2, \ldots, A_n\}$ d'un polygone régulier à n côtés

$$\mathrm{D}_{2n} \times \{A_1, A_2, \ldots, A_n\} \to \{A_1, A_2, \ldots, A_n\}, \qquad (g, A_i) \mapsto g \cdot A_i = g(A_i)$$

est transitive. En effet, pour tout $0 \leq k \leq n-1$, nous avons $A_{k+1} = r^k(A_1)$; autrement dit $\mathcal{O}_{A_1} = \{A_1, A_2, \ldots, A_n\}$.

Exemple 6.4.4. — Rappelons que le groupe orthogonal $\mathrm{O}(n,\mathbb{R})$ est défini par

$$\mathrm{O}(n,\mathbb{R}) = \{A \in \mathrm{GL}(n,\mathbb{R}) \mid A^{\mathrm{t}}A = {}^{\mathrm{t}}AA = \mathrm{id}\}.$$

Nous avons vu Exemple 6.2.10 que les orbites de l'action de $\mathrm{O}(n,\mathbb{R})$ sur $\mathbb{R}^n$, $(A,\mathbf{v}) \mapsto A{\cdot}\mathbf{v} = A\mathbf{v}$, étaient les sphères euclidiennes centrées en $\mathbf{0}$: $\mathbb{S}_n(r) = \{\mathbf{v} \in \mathbb{R}^n \mid ||\mathbf{v}|| = r\}$. Cette action n'est donc pas transitive.
Par contre la Proposition 6.2.1 nous indique que l'action de $\mathrm{O}(n,\mathbb{R})$ sur $\mathbb{S}_n(r)$ est transitive puisqu'il s'agit de l'action sur une de ses orbites.

Exemple 6.4.5. — Considérons l'action de $\mathfrak{S}_n$ sur $\{1, 2, \ldots, n\}$; elle est transitive. Le stabilisateur de n s'identifie naturellement à $\mathfrak{S}_{n-1} \subset \mathfrak{S}_n$ (Exemple 6.2.14). Tous les éléments d'une classe à gauche $\sigma\mathfrak{S}_{n-1}$ dans $\mathfrak{S}_n$ prennent la même valeur en n puisque $\mathfrak{S}_{n-1}$ fixe n. Autrement dit, pour tout $\tau \in \mathfrak{S}_{n-1}$ nous avons $(\sigma\tau)(n) = \sigma(n)$. Réciproquement si $\sigma(n) = \tau(n)$ alors $\sigma^{-1}\tau(n) = n$, donc $\sigma^{-1}\tau$ appartient à $\mathfrak{S}_{n-1}$. Ainsi $\sigma\mathfrak{S}_{n-1} = \tau\mathfrak{S}_{n-1}$. Associer chaque classe à gauche de $\mathfrak{S}_{n-1}$ dans $\mathfrak{S}_n$ à la valeur commune de ses éléments en n « envoie » l'action de $\mathfrak{S}_n$ sur ${}^{\mathfrak{S}_n}\!/_{\mathfrak{S}_{n-1}}$ sur l'action de $\mathfrak{S}_n$ sur $\{1, 2, \ldots, n\}$.

Proposition 6.4.1

Soit G un groupe d'ordre $p^\alpha r$, avec p premier ne divisant pas r. On note X l'ensemble de ses sous-groupes d'ordre p^α et on suppose qu'il est non vide.
L'action de G sur X par conjugaison est transitive. Autrement dit les sous-groupes d'ordre p^α sont conjugués.

Remarque 6.4.1. — L'hypothèse « X est non vide » est inutile comme on le verra dans le premier théorème de Sylow (Théorème 10.1.1).

Démonstration. — Comme X est supposé non-vide, on considère un de ses éléments H.

Prenons alors un élément quelconque de X, K, que l'on fait agir sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ par translation à gauche. La Proposition 6.2.5 nous indique que si $a\mathrm{H}$ est un point fixe de cette action alors $\mathrm{K} \subset a\mathrm{H}a^{-1}$. Ici K et $a\mathrm{H}a^{-1}$ sont des sous-groupes de G d'indice p^α, cette inclusion est donc en fait une égalité et elle prouve que tous les éléments de X sont conjugués à H ce qui est le résultat.
Montrons à présent que l'action possède un point fixe. Il s'agit ici de l'action de K, qui est d'ordre p^α, sur l'ensemble ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ qui est de cardinal r.
Si $a\mathrm{H}$ est dans ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ son orbite a comme cardinal $[\mathrm{K} : \mathrm{St}(a\mathrm{H})]$. Il s'agit d'un diviseur de l'ordre de K. C'est donc une puissance de p puisque K est d'ordre p^α. Autrement dit, si $a\mathrm{H}$ n'est pas un point fixe, son orbite a un cardinal qui vaut 0 modulo p. Soit n_f le nombre de points fixes, c'est-à-dire $n_f = \#\mathtt{fixe}_{{}^{\mathrm{G}}\!/_{\mathrm{H}}}(\mathrm{K})$. Si nous désignons par $(a_i\mathrm{H})_{1\leq i\leq \ell}$ des représentants de chacune

des orbites non réduites à un point, l'équation aux classes (Proposition 6.3.2) s'écrit

$$r = n_f + \sum_{i=1}^{\ell} \#\mathcal{O}_{a_i\mathrm{H}}.$$

Puisque p est premier avec r on a $r \not\equiv_p 0$. Ainsi l'équation aux classes modulo p mène à $n_f \equiv_p r \not\equiv_p 0$. Ce qui nous indique que n_f est non nul. Il y a donc au moins un point fixe. □

Exemple 6.4.6. — Soit G un groupe. Soit X_d l'ensemble des sous-groupes de G d'ordre d. L'action

$$\mathrm{G} \times X_d \to X_d, \qquad (g, \mathrm{H}) \mapsto g \cdot \mathrm{H} = g\mathrm{H}g^{-1}.$$

Si d est une puissance première maximale divisant $|\mathrm{G}|$, cette action est transitive.

Théorème 6.4.1

Soit G un groupe agissant transitivement sur X. Alors $\#X$ divise $|\mathrm{G}|$.

Démonstration. — L'action étant transitive pour tout $x \in X$ nous avons $X = \mathcal{O}_x$. La Proposition 6.3.1 assure que $\#\mathrm{O}_x = \left|\mathrm{G}/\mathrm{St}_{\mathrm{G}}(x)\right|$ qui se réécrit $\#\mathrm{O}_x\,|\mathrm{St}_{\mathrm{G}}(x)| = |\mathrm{G}|$. Finalement $\#X\,|\mathrm{St}_{\mathrm{G}}(x)| = |\mathrm{G}|$ et $\#X$ divise $|\mathrm{G}|$. □

Exemple 6.4.7. — Soit p un nombre premier. Si G est un sous-groupe de $\mathfrak{S}_p$ et si l'action de G sur $\{1, 2, \ldots, p\}$ est transitive alors p divise $|\mathrm{G}|$ (Théorème 6.4.1). Le Théorème de Cauchy (Théorème 3.7.1) assure que G contient un élément d'ordre p. Les seuls éléments d'ordre p dans $\mathfrak{S}_p$ sont les p-cycles. Finalement tout sous-groupe de $\mathfrak{S}_p$ dont l'action sur $\{1, 2, \ldots, p\}$ est transitive contient un p-cycle.

Théorème 6.4.2

Soit G un groupe agissant sur deux ensembles finis X et Y. Supposons qu'il existe une fonction $f\colon X \to Y$ qui respecte les actions de G, c'est-à-dire $f(g \cdot x) = g \cdot f(x)$ pour tout $g \in \mathrm{G}$ et pour tout $x \in X$.
Si l'action de G sur Y est transitive, alors $\#Y$ divise $\#X$.

Nous verrons une application de ce résultat au Chapitre 10 (Corollaire 10.1.3).

Démonstration. — Nous avons la décomposition suivante de X :

$$X = \bigsqcup_{y \in Y} f^{-1}(y),$$

les ensembles $f^{-1}(y)$ étant disjoints on a : $\#X = \sum_{y \in Y} f^{-1}(y)$.

Soient y et y' deux éléments de Y. L'action de G sur Y étant transitive il existe g dans G tel que $y' = g \cdot y$. Les applications

$$f^{-1}(y) \to f^{-1}(y'),\ x \mapsto g \cdot x \qquad \text{et} \qquad f^{-1}(y') \to f^{-1}(y),\ x' \mapsto g^{-1} \cdot x'$$

sont inverses l'une de l'autre d'où $\#f^{-1}(y) = \#f^{-1}(y')$.
Posons $n = \#f^{-1}(y)$; alors $\#X = \sum_{y \in Y} f^{-1}(y) = n\#Y$ conduit à $\#X = n\#Y$. □

L'énoncé qui suit sur les actions transitives est fondamental. Il dit que toute action transitive peut être vue comme une action par translation à gauche. Avant de démontrer ce résultat précisons ce qu'on entend par « peut être vue ». Soit G un groupe agissant sur un ensemble X et sur un ensemble Y. Ces deux actions sont *équivalentes* s'il existe une bijection $f\colon X \to Y$ telle que $f(g \cdot x) = g \cdot (f(x))$ pour tout $g \in \mathrm{G}$ et pour tout $x \in X$. Lorsque $f\colon X \to Y$ est une équivalence d'actions de groupe sur X et Y, alors $g \cdot x = x$ si et seulement si $g \cdot f(x) = f(x)$, les stablisateurs de $x \in X$ et $f(x) \in Y$ sont donc les mêmes.

Exemple 6.4.8. — Soit $\mathcal{B}$ l'ensemble des bases ordonnées (e_1, e_2) de $\mathbb{R}^2$. Considérons l'action naturelle de $\mathrm{GL}(2, \mathbb{R})$ sur $\mathcal{B}$:

$$\mathrm{GL}(2, \mathbb{R}) \times \mathcal{B} \to \mathcal{B}, \qquad (A, (e_1, e_2)) \mapsto A \cdot (e_1, e_2) = (Ae_1, Ae_2).$$

Considérons l'action de $\mathrm{GL}(2, \mathbb{R})$ sur lui-même par translation à gauche. Considérons l'application

$$f\colon \mathcal{B} \to \mathrm{GL}(2, \mathbb{R}), \qquad \left(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix} \right) \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix};$$

c'est une bijection. De plus, pour tout $A \in \mathrm{GL}(2, \mathbb{R})$, pour tout $(e_1, e_2) \in \mathcal{B}$ nous avons $f(A \cdot (e_1, e_2)) = A \cdot f(e_1, e_2)$. Autrement dit l'action naturelle de $\mathrm{GL}(2, \mathbb{R})$ sur $\mathcal{B}$ est équivalente à l'action de $\mathrm{GL}(2, \mathbb{R})$ sur lui-même par translation à gauche.

Théorème 6.4.3

Une action transitive d'un groupe G sur un ensemble X est équivalente à une action de G par translation à gauche sur un quotient ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ de G.

Démonstration. — Soit x_0 un élément de X. Posons $\mathrm{H} = \mathrm{St}(x_0)$. Puisque l'action est transitive, $\mathcal{O}_{x_0} = X$ et l'application

$${}^{\mathrm{G}}\!/_{\mathrm{H}} \to \mathcal{O}_{x_0} = X, \qquad g\mathrm{H} \mapsto g \cdot x_0$$

est une bijection (Proposition 6.3.1).

Montrons que cette bijection respecte l'action de G de chaque côté. Soit $x \in X$ et soit $g \in \mathrm{G}$. Écrivons x sous la forme $g_0 \cdot x_0$; la classe à gauche correspondant à x est $g_0\mathrm{H}$. De même, puisque $y = g \cdot (g_0 \cdot x_0) = (gg_0) \cdot x_0$ nous obtenons que la classe à gauche correspondant à y est

$(gg_0)\mathrm{H} = gg_0\mathrm{H}$. Ainsi quand $x \rightsquigarrow g_0\mathrm{H}$, on a $gx \rightsquigarrow gg_0\mathrm{H}$: la bijection entre ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ et X préserve les actions de G sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ et X. □

Exemple 6.4.9. — Considérons l'action naturelle de $\mathrm{GL}(2,\mathbb{R})$ sur $\mathbb{R}^2 \smallsetminus \{0\}$ par multiplication matrice-vecteur :

$$\mathrm{GL}(2,\mathbb{R}) \times (\mathbb{R}^2 \smallsetminus \{0\}) \to (\mathbb{R}^2 \smallsetminus \{0\}), \qquad (A, v) \mapsto A \cdot v = Av.$$

Nous avons vu dans l'Exemple 6.2.16 que l'orbite de $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ est $\mathbb{R}^2 \smallsetminus \{\mathbf{0}\}$; l'action est donc bien transitive.

En suivant l'idée de la démonstration du Théorème 6.4.3, nous allons montrer que cette action de $\mathrm{GL}(2,\mathbb{R})$ sur $\mathbb{R}^2 \smallsetminus \{0\}$ est équivalente à une action par translation à gauche de $\mathrm{GL}(2,\mathbb{R})$ sur un certain espace quotient ${}^{\mathrm{GL}(2,\mathbb{R})}\!/_{\mathrm{H}}$.

Le stabilisateur de $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ est (Exemple 6.2.16)

$$\mathrm{H} = \mathrm{St}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \left\{\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \mid y \neq 0\right\} \subset \mathrm{GL}(2,\mathbb{R}).$$

Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de $\mathrm{GL}(2,\mathbb{R})$; alors

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\mathrm{H} = \left\{\begin{pmatrix} a & r \\ c & s \end{pmatrix} \mid r,\, s \in \mathbb{R},\, as - cr \neq 0\right\}.$$

Soit $\left\{\begin{pmatrix} \alpha & r \\ \beta & s \end{pmatrix} \mid r,\, s \in \mathbb{R},\, \alpha x - \beta r \neq 0\right\}$ un élément de ${}^{\mathrm{GL}(2,\mathbb{R})}\!/_{\mathrm{H}}$. La matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ agit par translation à gauche sur $\begin{pmatrix} \alpha & r \\ \beta & s \end{pmatrix}$ comme suit

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & r \\ \beta & s \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta & ar + bs \\ c\alpha + d\beta & cr + ds \end{pmatrix}. \tag{6.4.1}$$

Considérons le vecteur $v = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$. Pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathrm{GL}(2,\mathbb{R})$ nous avons $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot v = \begin{pmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{pmatrix}$: on retrouve la première colonne de (6.4.1). Les deux actions sont donc équivalentes.

Mentionnons un cas particulier du Théorème 6.4.3 : *une action de* G *sur un ensemble* X *est équivalente à l'action par multiplication à gauche de* G *sur lui-même si et seulement si l'action a une orbite et les stabilisateurs sont triviaux.*

Définition 6.4.1

Soit G un groupe agissant sur un ensemble X. L'action de G sur X est dite *libre* lorsque tout point de X a un stabilisateur trivial.

Exemple 6.4.10. — L'action par multiplication à gauche d'un groupe sur lui-même

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, x) \mapsto g \cdot x$$

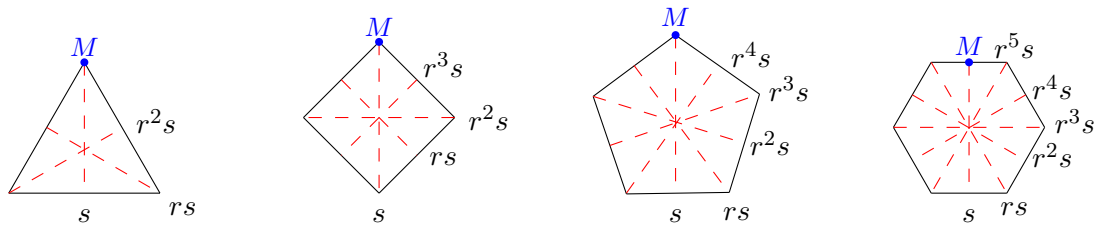
est libre et ne possède qu'une seule orbite ($g = g \cdot e \in \mathcal{O}_e$).

On trouve beaucoup d'actions libres en topologie. En particulier :

Exemple 6.4.11. — Identifions $\mathbb{Z}/2\mathbb{Z}$ avec le sous-groupe $\{\mathrm{Id}, -\mathrm{Id}\}$ de $\mathrm{GL}(n, \mathbb{R})$; le groupe $\mathbb{Z}/2\mathbb{Z}$ agit sur $\mathbb{R}^n$ comme suit : 0 agit comme l'identité et 1 agit comme $v \mapsto -v$. Nous pouvons restreindre cette action de $\mathbb{Z}/2\mathbb{Z}$ sur la sphère unitaire de $\mathbb{R}^n$; on l'appelle l'action antipodale puisque ses orbites sont des paires de points opposés (appelés points antipodaux) sur la sphère. Cette action est une action libre. Il y a un nombre non dénombrable d'orbites.

Exemple 6.4.12. — Pour un entier $n \geq 2$, désignons par μ_n l'ensemble des racines de l'unité d'ordre n dans $\mathbb{C}^\times$ (par exemple, $\mu_4 = \{\mathbf{i}, -\mathbf{i}\}$) ; ainsi $\#\mu_n = \phi(n)$. Le groupe $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ agit sur μ_n comme suit : si a appartient à $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ et ξ à μ_n, on pose $a \cdot \xi = \xi^a$ (cette action est bien définie puisque $a \equiv_n b \Rightarrow \xi^a = \xi^b$). Puisque chaque élément de μ_n est une puissance de tout autre élément de μ_n en utilisant des exposants relativement premiers à n, cette action est transitive. Comme $\xi^a = \xi$ seulement si $a \equiv_n 1$ (ξ est d'ordre n), tous les stabilisateurs sont triviaux. Ainsi l'action de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ sur μ_n est équivalente à l'action de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ sur lui-même par multiplication.

Exemple 6.4.13. — L'action du groupe D_{2n} sur l'ensemble des sommets du polygone préservé est transitive mais pas libre.



Le stabilisateur du sommet M est $\{\mathrm{id}, s\}$.

Comparons les notions « action fidèle » et « action libre ». Une action est fidèle si pour tous g_1 et g_2 distincts dans G, on a $g_1 \cdot x \neq g_2 \cdot x$ pour certains $x \in X$; une action est libre si pour tous g_1 et g_2 distincts dans G, alors $g_1 \cdot x \neq g_2 \cdot x$ pour tout $x \in X$. Ainsi

toutes les actions libres sont fidèles.

Puisque $g_1 \cdot x = g_2 \cdot x$ si et seulement si $g_2^{-1} g_1 \cdot x = x$, nous pouvons décrire des actions fidèles et libres en termes de points fixes : une action est fidèle lorsque pour tout $g \neq e$ on a $\mathrm{Fix}_g(X) \neq X$ alors qu'une action est libre lorsque pour tout $g \neq e$ on a $\mathrm{Fix}_g(X) = \emptyset$.

Théorème 6.4.4

Soit G un groupe agissant transitivement sur un ensemble X. Soit N un sous-groupe distingué de G. Toutes les orbites de N sur X ont le même cardinal.

Démonstration. — Soient x et y dans X. Puisque G agit transitivement sur X il existe $g \in \mathrm{G}$ tel que $y = g \cdot x$. Notons que

$$\mathrm{N}x \mapsto \mathrm{N}y = \mathrm{N}gx = g\mathrm{N}x, \qquad t \mapsto g \cdot t$$

est une bijection (qui dépend du choix de g tel que $y = g \cdot x$). □

Exemple 6.4.14. — Considérons l'action du groupe diédral D_8 sur l'ensemble S des quatre sommets d'un carré.

- ◇ Les orbites de S sous l'action de $Z(\mathrm{G})$ sont des orbites de longueur 2, elles sont constituées des paires de sommets opposés.
- ◇ Considérons l'action de $\langle s \rangle = \{\mathrm{id}, s\}$ où s désigne la réflexion par rapport à une diagonale du carré sur S. Le groupe $\langle s \rangle$ n'est pas distingué dans D_8 et les orbites de S sous l'action de $\langle s \rangle$ n'ont pas toutes le même cardinal : il existe deux orbites de longueur 1 et une orbite de longueur 2.

Exemple 6.4.15. — Soit p un nombre premier. Si G est un sous-groupe de $\mathfrak{S}_p$ et si l'action de G sur $\{1, 2, \ldots, p\}$ est transitive, alors l'action d'un sous-groupe distingué non trivial N de G sur $\{1, 2, \ldots, p\}$ est également transitive. D'après le Théorème 6.4.4 les N-orbites sur $\{1, 2, \ldots, p\}$ ont toutes le même cardinal m. Puisque N n'est pas un sous-groupe trivial, une N-orbite n'est pas un point et $m > 1$. Étant donné que $\{1, 2, \ldots, p\}$ coïncide avec la réunion (disjointe) des orbites nous obtenons $p = m\,\#\{\text{N-orbites}\}$. À partir de $m > 1$, $p = m\,\#\{\text{N-orbites}\}$ et p premier nous obtenons $m = p$ et donc $\#\{\text{N-orbites}\} = 1$.

Théorème 6.4.5

Soit G un groupe agissant sur un ensemble X. Soit H un sous-groupe de G. Les assertions suivantes sont équivalentes :

1. H agit transitivement sur X,
2. G agit transitivement sur X et $\mathrm{G} = \mathrm{HSt}_{\mathrm{G}}(x)$ pour un certain $x \in X$.

Lorsque cela se produit, $\mathrm{G} = \mathrm{HSt}_{\mathrm{G}}(x)$ pour tout $x \in X$.

Nous donnerons une application de cet énoncé au Chapitre 10.

Démonstration. — Supposons que H agisse transitivement sur l'ensemble X. Alors G agit transitivement sur X. Soit x un élément de X. Pour tout $g \in \mathrm{G}$ il existe $h \in \mathrm{H}$ tel que $g \cdot x = h \cdot x$ autrement dit tel que $(h^{-1}g) \cdot x = x$ ce qui revient à dire que $h^{-1}g$ appartient à $\mathrm{St}_{\mathrm{G}}(x)$. Ainsi g appartient à $\mathrm{HSt}_{\mathrm{G}}(x)$ et $\mathrm{G} = \mathrm{HSt}_{\mathrm{G}}(x)$.

Réciproquement, si G agit transitivement sur X et $\mathrm{G} = \mathrm{HSt}(x)$ pour un certain $x \in X$ alors $X = \mathrm{G} \cdot x = \mathrm{HSt}_{\mathrm{G}}(x) \cdot x = \mathrm{H} \cdot x$, donc H agit transitivement sur X. □

Corollaire 6.4.1

Soit G un groupe agissant sur un ensemble X. Si H est un sous-groupe de G tel que

- ⋄ H agit transitivement sur X et
- ⋄ $\mathrm{St}_{\mathrm{G}}(x)$ est contenu dans H pour un certain $x \in X$,

alors $\mathrm{H} = \mathrm{G}$.

Démonstration. — D'après le Théorème 6.4.5 nous avons $\mathrm{G} = \mathrm{HSt}_{\mathrm{G}}(y)$ pour tout $y \in X$; c'est en particulier le cas pour $y = x$. Nous avons donc d'une part $\mathrm{G} = \mathrm{HSt}_{\mathrm{G}}(x)$ et d'autre part $\mathrm{St}_{\mathrm{G}}(x) \subset \mathrm{H}$. Il en résulte que $\mathrm{G} = \mathrm{H}$. □

Soit G un groupe. Considérons l'action naturelle du groupe Aut(G) sur G :

$$\mathrm{Aut}(\mathrm{G}) \times \mathrm{G} \to \mathrm{G}, \qquad (\phi, g) \mapsto \phi(g)$$

Remarquons que pour tout automorphisme ϕ de G nous avons $\phi(e) = e$, *i.e.* e est un point fixe. L'action de Aut(G) sur $\mathrm{G} \smallsetminus \{e\}$ peut-elle être transitive ? C'est le cas lorsque $\mathrm{G} = \left(\mathbb{Z}/p\mathbb{Z}\right)^n$: Aut(G) est égal à $\mathrm{GL}\left(n, \mathbb{Z}/p\mathbb{Z}\right)$ et la transitivité de $\mathrm{GL}\left(n, \mathbb{Z}/p\mathbb{Z}\right)$ sur $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$ découle du faire que tout vecteur non nul de $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$ peut être complété en une base de $\mathrm{GL}\left(n, \mathbb{Z}/p\mathbb{Z}\right)$. Nous montrons maintenant que c'est la seule situation où Aut(G) agit transitivement sur $\mathrm{G} \smallsetminus \{e\}$ lorsque G est fini :

Théorème 6.4.6

Soit G un groupe fini d'ordre > 1. Si $\mathrm{Aut}(\mathrm{G})$ agit transitivement sur $\mathrm{G} \smallsetminus \{e\}$, alors $\mathrm{G} \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^n$ pour un certain p premier et un certain entier n.

Démonstration. — Si g est un élément de G et ϕ un automorphisme de G, alors $\phi(g)$ et g sont de même ordre. Puisque $\mathrm{Aut}(\mathrm{G})$ agit transitivement sur $\mathrm{G} \smallsetminus \{e\}$ il en résulte que tous les élements de $\mathrm{G} \smallsetminus \{e\}$ sont de même ordre. Soit p un facteur premier de $|\mathrm{G}|$. Le théorème de Cauchy (Théorème 3.7.1) assure l'existence d'un élément d'ordre p ; par conséquent tout élément de $\mathrm{G} \smallsetminus \{e\}$ est d'ordre p. Ainsi $|\mathrm{G}| = p^k$ pour un certain entier k. Comme G est un p-groupe non trivial, il possède un centre non trivial (Corollaire 7.3.2). Soit $g \in \mathrm{G} \smallsetminus \{e\}$. Ou bien g et $\phi(g)$ appartiennent à $Z(\mathrm{G})$, ou bien g et $\phi(g)$ n'appartiennent pas à $Z(\mathrm{G})$. Par hypothèse tout élément non trivial de G appartient donc au centre et G est abélien. Puisque chaque élément non nul est d'ordre p, nous pouvons considérer G comme un espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$, nécessairement de dimension finie puisque G est fini. Il s'en suit que G est isomorphe à $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$ pour un certain p premier et un certain entier n. $\square$

CHAPITRE 7

ACTIONS DE GROUPES, APPLICATIONS

7.1. Deux applications aux groupes infinis

Théorème 7.1.1

Un groupe de type fini possède un nombre fini de sous-groupes d'indice n pour chaque entier $n \geq 1$.

Démonstration. — Soit G un groupe de type fini. Soit H un sous-groupe de G d'indice fini n. Considérons l'action de G sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ par translation à gauche :

$$\mathrm{G} \times {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}, \qquad (g, a\mathrm{H}) \mapsto g \cdot (a\mathrm{H}) = (ga)\mathrm{H};$$

Comme $g\mathrm{H} = \mathrm{H}$ si et seulement si g appartient à H (Théorème 1.6.2) le stabilisateur de H est H. Notons $\varphi\colon \mathrm{G} \to \mathfrak{S}_{\mathrm{G}/\mathrm{H}}$ le morphisme associé à cette action. On peut numéroter les $n = [\mathrm{G} : \mathrm{H}]$ classes à gauche dans ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ de sorte que la classe à gauche de H corresponde à 1. Ainsi à isomorphisme près $\varphi\colon \mathrm{G} \to \mathfrak{S}_n$ et $\mathrm{H} = \mathrm{St}(1)$. Autrement dit pour tout sous-groupe H de G d'indice n on peut construire une action de G sur $\{1, 2, \ldots, n\}$ telle que $\mathrm{H} = \mathrm{St}(1)$. Le nombre de sous-groupes de G d'indice n est donc borné par le nombre de morphismes de G dans $\mathfrak{S}_n$. Comme G est de type fini, il y a un nombre fini de morphismes de G dans le groupe fini $\mathfrak{S}_n$ d'où le résultat. □

Modulo la bijection ${}^{\mathrm{G}}\!/_{\mathrm{St}_{\mathrm{G}}(x)} \xrightarrow{\sim} \mathcal{O}_x$ (Proposition 6.3.1) l'action de G sur $\mathcal{O}_x$ n'est autre que l'action naturelle de G sur ${}^{\mathrm{G}}\!/_{\mathrm{St}_{\mathrm{G}}(x)}$. Un exemple d'utilisation de cette action est le suivant :

Proposition 7.1.1

Soit G un groupe infini. Si G contient un sous-groupe H, distinct de G et d'indice fini dans G, alors G n'est pas simple.

Démonstration. — Désignons par n l'indice de H dans G ; par hypothèse $n = [\mathrm{G} : \mathrm{H}] > 1$. Le groupe G agit par translation sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$

$$\mathrm{G} \times {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}, \qquad (g, a\mathrm{H}) \mapsto g \cdot (a\mathrm{H}) = (ga)\mathrm{H};$$

autrement dit il existe un morphisme de groupes

$$\varphi \colon \mathrm{G} \to \mathfrak{S}_{{}^{\mathrm{G}}\!/_{\mathrm{H}}} \simeq \mathfrak{S}_n.$$

Le noyau $\ker \varphi$ de φ satisfait les propriétés suivantes :

- ◇ $\ker \varphi$ est un sous-groupe distingué de G ;
- ◇ $\ker \varphi$ est distinct de $\{e\}$ car G est infini ;
- ◇ $\ker \varphi$ est distinct de G parce que $[\mathrm{G} : \mathrm{H}] > 1$.

□

7.2. Le théorème de Cauchy

Nous retrouvons l'énoncé suivant (Théorème 3.7.1) :

Théorème 7.2.1: (Théorème de Cauchy)

Soit G un groupe fini. Soit p un facteur premier de $|\mathrm{G}|$. Alors G contient un élément d'ordre p ; autrement dit G contient un sous-groupe d'ordre p.

Démonstration. — Soit p un facteur premier de $|\mathrm{G}|$.

On considère l'ensemble $X = \{(g_1, \ldots, g_p) \in \mathrm{G}^p \mid g_1 \ldots g_p = e_{\mathrm{G}}\}$.

L'application $\varphi \colon \mathrm{G}^{p-1} \to X$, $(g_1, \ldots, g_{p-1}) \mapsto (g_1, \ldots, g_{p-1}, (g_1 \ldots g_{p-1})^{-1})$ est une bijection. Ainsi on a $\#X = |\mathrm{G}|^{p-1}$ et en particulier $\#X \equiv_p 0$.

On fait agir ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ sur X par permutations circulaires des coordonnées de la manière suivante :

$${}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \times X \to X, \qquad (\bar{k}, (g_1, \ldots, g_p)) \mapsto \bar{k}.(g_1, \ldots, g_p) = (g_{1+k \bmod p}, \ldots, g_{p+k \bmod p}).$$

Le cardinal de chaque orbite étant un diviseur de l'ordre de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ (Corollaire 6.3.1), il vaut donc 1 ou p.

L'orbite de $\mathcal{G} = (g_1, \ldots, g_p) \in X$ sous cette action est réduite à un point si et seulement si pour tous i et k dans $[\![1, p]\!]$ on a $g_{i+k \bmod p} = g_i$. C'est-à-dire si tous les g_i sont égaux, donc si $\mathcal{G} = (g, \ldots, g)$. De plus, puisque $\mathcal{G} \in X$ nous avons $g^p = e_{\mathrm{G}}$.

Notons alors r le nombre d'orbites réduites à un point. Remarquons que $r \geq 1$ puisque $(e_{\mathrm{G}}, \ldots, e_{\mathrm{G}}) \in X$ a son orbite réduite à lui-même. Notons $\mathcal{G}_1, \cdots, \mathcal{G}_r$ les r-éléments de X qui

ont une orbite réduite à un point, et $\mathcal{G}_{r+1}, \cdots, \mathcal{G}_{r+N}$ des représentants de chacune des orbites ayant p éléments. La formule des classes (Proposition 6.3.2) s'écrit alors

$$\#X = \sum_{k=1}^{r} \#\mathcal{O}_{\mathcal{G}_i} + \sum_{k=r+1}^{r+N} \#\mathcal{O}_{\mathcal{G}_i} = r + Np\,;$$

modulo p cette égalité se réécrit $0 \equiv_p r$ (on rappelle que $\#X \equiv_p 0$). Ainsi $r \geq 1$ est un multiple de p. En particulier $r \geq p$. On en déduit qu'outre $(e_{\mathrm{G}}, \ldots, e_{\mathrm{G}})$ il y a au moins $p-1$ éléments dont l'orbite est réduite à un point, c'est-à-dire au moins $p-1$ éléments g dans $\mathrm{G} \smallsetminus \{e\}$ tels que $g^p = e_{\mathrm{G}}$. □

Corollaire 7.2.1

Soit H un groupe fini d'ordre n. Soit $m \in \mathbb{N}^*$ tel que pour tout $g \in \mathrm{H}$ on ait $g^m = e$. Alors n divise une puissance de m.

Démonstration. — Il suffit de montrer que tous les facteurs premiers de n sont des facteurs premiers de m. Soit p un premier divisant n. Le Théorème de Cauchy (Théorème 3.7.1) garantit l'existence d'un élément $h \in \mathrm{H}$ d'ordre p. Or par hypothèse $h^m = e$ donc p divise m. □

Dans le Théorème 6.1.1, nous avons vu que se donner une action de groupe de G sur un ensemble X est équivalent à se donner un morphisme de groupes de G sur $\mathfrak{S}_{\mathrm{G}}$. Nous allons maintenant mettre cette idée à profit :

Théorème 7.2.2

Tout groupe non abélien d'ordre 6 est isomorphe à $\mathfrak{S}_3$.

Démonstration. — Soit G un groupe non abélien d'ordre 6. Le Théorème de Cauchy (Théorème 3.7.1) assure que G possède un élément a d'ordre 2 et un élément b d'ordre 3. Si a et b commutaient, alors ab serait d'ordre 6 et G serait cyclique : impossible. Ainsi a et b ne commutent pas ; par suite bab^{-1} n'est ni e, ni a. Considérons le groupe $\mathrm{H} = \langle a \rangle = \{e, a\}$; remarquons que H n'est pas un sous-groupe distingué de G puisque bab^{-1} n'appartient pas à H. Il y a trois classes à gauche modulo H dans G qui sont H, $b\mathrm{H}$ et $b^2\mathrm{H}$.

Considérons l'action de G sur les classes à gauche modulo H par multiplication à gauche

$$\mathrm{G} \times {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}, \qquad (g, h\mathrm{H}) \mapsto g \cdot h\mathrm{H} = (gh)\mathrm{H}.$$

Soit $\varphi\colon \mathrm{G} \to \mathfrak{S}_{\mathrm{G}/\mathrm{H}} \simeq \mathfrak{S}_3$ le morphisme associé

$$\varphi\colon \mathrm{G} \to \mathfrak{S}_{\mathrm{G}/\mathrm{H}},\ g \mapsto \varphi(g)\colon {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$$
$$h\mathrm{H} \mapsto \varphi(g)(h\mathrm{H}) = g \cdot h\mathrm{H} = (gh)\mathrm{H}.$$

Si g appartient à $\ker\varphi$, *i.e.* si $\varphi(g) = \mathrm{id}$, alors $g\mathrm{H} = \mathrm{H}$ et g appartient à H ; autrement dit $\ker\varphi \subset \mathrm{H}$. Par suite ou bien $\ker\varphi = \{e\}$, ou bien $\ker\varphi = \mathrm{H}$. Puisque H n'est pas un sous-groupe distingué de G, nous avons $\ker\varphi \neq \mathrm{H}$ et $\ker\varphi = \{e\}$. Autrement dit φ est injectif. Mais $|\mathrm{G}| = |\mathfrak{S}_3| = 6$ donc φ est un isomorphisme. □

7.3. Applications aux p-groupes

Un groupe G d'ordre p^k avec p premier et $k \in \mathbb{N} \smallsetminus \{0\}$ est appelé *p-groupe*. Par exemple, $\left(\mathbb{Z}/5\mathbb{Z}\right)^* = \{1,\ 2,\ 3,\ 4\}$ et D_8 sont des 2-groupes. L'action d'un p-groupe présente des propriétés particulières. Comme tous les sous-groupes d'un p-groupe ont un indice de puissance p, le cardinal d'une orbite sous l'action d'un p-groupe est divisible par p sauf si le point est un point fixe auquel cas son orbite est réduite à lui-même. Cela conduit à l'énoncé suivant :

Proposition 7.3.1

Soit G un p-groupe agissant sur un ensemble X. Soit X^{G} l'ensemble des points fixes de X sous l'action de G, *i.e.*

$$X^{\mathrm{G}} = \{x \in X \mid \forall\, g \in \mathrm{G},\ g \cdot x = x\}.$$

Alors $\#X \equiv_p \#X^{\mathrm{G}}$.

Remarque 7.3.1. — Attention la Proposition 7.3.1 n'est valable que pour les actions de p-groupes. Lorsqu'un groupe d'ordre $9 = 3^2$ agit, nous obtenons $\#X \equiv_3 \#X^{\mathrm{G}}$, mais lorsqu'un groupe d'ordre $6 = 2 \times 3$ agit, nous n'obtenons ni $\#X \equiv_2 \#X^{\mathrm{G}}$, ni $\#X \equiv_3 \#X^{\mathrm{G}}$.

La Proposition 7.3.1 peut être utilisée pour démontrer des théorèmes d'existence sur des groupes finis (de manière non constructive) si on peut interpréter un problème en termes de points fixes. Par exemple, un élément d'un groupe G appartient au centre de G précisément lorsqu'il est un point fixe pour l'action de G sur lui-même par conjugaison. Donc, si nous voulons montrer qu'une classe de groupes a des centres non triviaux, nous pouvons essayer de montrer qu'il existe des points fixes pour l'action de G par conjugaison sur lui-même distinct de l'identité.

Démonstration. — Écrivons X comme réunion disjointe de ses orbites sous G en remarquant que $x \in X^{\mathrm{G}} \Leftrightarrow \mathcal{O}_x = \{x\}$:

$$X = \bigcup_{x \in X^{\mathrm{G}}} \mathcal{O}_x \cup \bigcup_{x \notin X^{\mathrm{G}}} \mathcal{O}_x = X^{\mathrm{G}} \cup \bigcup_{x \notin X^{\mathrm{G}}} \mathcal{O}_x.$$

Si x n'appartient pas à X^{G}, nous avons $\#\mathcal{O}_x > 1$ et comme $\#\mathcal{O}_x$ divise $|\mathrm{G}| = p^n$ nous obtenons : p divise $\#\mathcal{O}_x$. Le résultat provient alors de l'égalité

$$\#X = \#X^{\mathrm{G}} + \underbrace{\sum_{x \notin X^{\mathrm{G}}} \underbrace{\#\mathcal{O}_x}_{\text{divisible par } p}}_{\text{divisible par } p}$$

□

Corollaire 7.3.1: (Wilson)

Soit p un nombre premier. Alors $(p-1)! \equiv_p -1$.

Démonstration. — Considérons l'ensemble $X = \{(\sigma_1, \sigma_2, \ldots, \sigma_p) \,|\, \sigma_i \in \mathfrak{S}_p,\ \sigma_1\sigma_2\ldots\sigma_p = \mathrm{id}\}$. L'équation $\sigma_1\sigma_2\ldots\sigma_p = \mathrm{id}$ se réécrit $\sigma_p = (\sigma_1\sigma_2\ldots\sigma_{p-1})^{-1}$; par conséquent $\#X = |\mathfrak{S}_p|^{p-1}$. Remarquons que si $(\sigma_1, \sigma_2, \ldots, \sigma_p)$ appartient à X, alors $(\sigma_2, \sigma_3, \ldots, \sigma_p, \sigma_1)$ aussi. Le décalage des coordonnées dans une solution peut être interprété comme une action du groupe $\mathbb{Z}/p\mathbb{Z}$ sur X :

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} \times X &\to X \\ (j, (\sigma_1, \sigma_2, \ldots, \sigma_p)) &\mapsto j \cdot (\sigma_1, \sigma_2, \ldots, \sigma_p) = (\sigma_{1+j \bmod p}, \sigma_{2+j \bmod p}, \ldots, \sigma_{p+j \bmod p}) \end{aligned}$$

Comme $\mathbb{Z}/p\mathbb{Z}$ est un p-groupe la Proposition 7.3.1 assure que $\#X \equiv_p \#X^{\mathbb{Z}/p\mathbb{Z}}$. Mais

$$X^{\mathbb{Z}/p\mathbb{Z}} = \{(\sigma, \sigma, \ldots, \sigma) \,|\, \sigma \in \mathfrak{S}_p,\ \sigma^p = \mathrm{id}\};$$

ainsi $\#X \equiv_p \#X^{\mathbb{Z}/p\mathbb{Z}}$ se récrit

$$\#X \equiv_p \#\{\sigma \in \mathfrak{S}_p \,|\, \sigma^p = \mathrm{id}\}.$$

De plus $\#X = |\mathfrak{S}_p|^{p-1}$ et $|\mathfrak{S}_p|^{p-1} \equiv_p 0$ donc

$$0 \equiv_p \#\{\sigma \in \mathfrak{S}_p \,|\, \sigma^p = \mathrm{id}\}.$$

Un élément de σ de $\mathfrak{S}_p$ satisfait $\sigma^p = \mathrm{id}$ si et seulement si $\sigma = \mathrm{id}$ ou σ est un p-cycle. Comme le nombre de p-cycles dans $\mathfrak{S}_p$ est $(p-1)!$ nous avons $\#\{\sigma \in \mathfrak{S}_p \,|\, \sigma^p = \mathrm{id}\} = (p-1)! + 1$ et

$$0 \equiv_p (p-1)! + 1.$$

□

Corollaire 7.3.2

Le centre d'un p-groupe distinct de $\{e\}$ n'est pas réduit à $\{e\}$.

Démonstration. — Le groupe G agit sur lui-même par conjugaison

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g, a) \mapsto g \cdot a = gag^{-1}.$$

L'ensemble des points fixes de l'action de G sur lui-même par conjugaison coïncide avec le centre de G :

$$\begin{aligned} \mathrm{G}^{\mathrm{G}} &= \{x \in \mathrm{G} \,|\, \forall\, g \in \mathrm{G},\, g \cdot x = x\} = \{x \in \mathrm{G} \,|\, \forall\, g \in \mathrm{G},\, gxg^{-1} = x\} \\ &= \{x \in \mathrm{G} \,|\, \forall\, g \in \mathrm{G},\, gx = xg\} = Z(\mathrm{G}). \end{aligned}$$

La Proposition 7.3.1 assure alors que $|\mathrm{G}| \equiv_p |Z(\mathrm{G})|$. Puisque e appartient à $Z(\mathrm{G})$ nécessairement $|Z(\mathrm{G})| \geq p$ d'où le résultat. □

Corollaire 7.3.3

Soit G un p-groupe fini agissant sur un ensemble fini X.
Si $\#X$ n'est pas divisible par p, alors il y a au moins un point fixe dans X.
Si $\#X$ est divisible par p, alors le nombre de points fixes est divisible par p (éventuellement 0).

Démonstration. — Si $\#X$ n'est divisible par p, alors le nombre de points fixes n'est pas divisible par p (Proposition 7.3.1). Par suite le nombre de points fixes ne peut être nul (p divise 0), il est donc ≥ 1.

Lorsque $\#X$ est divisible par p, d'après la Proposition 7.3.1 le nombre de points fixes est nul modulo p, c'est donc un multiple de p. □

Exemple 7.3.1. — Soit G un p-groupe de $\mathrm{GL}\left(n, \mathbb{Z}/p\mathbb{Z}\right)$ où $n \geq 1$. Le groupe G agit sur $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$:

$$\mathrm{GL}\left(n, \mathbb{Z}/p\mathbb{Z}\right) \times \left(\mathbb{Z}/p\mathbb{Z}\right)^n \to \left(\mathbb{Z}/p\mathbb{Z}\right)^n, \qquad (A, v) \mapsto A \cdot v = Av.$$

En effet,

- ◇ pour tout v dans $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$ nous avons $\mathrm{id} \cdot v = v$;
- ◇ pour tous A, B dans $\mathrm{GL}\left(n, \mathbb{Z}/p\mathbb{Z}\right)$, pour tout v dans $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$ nous avons $A \cdot (B \cdot v) = ABv = (AB) \cdot v$.

L'ensemble $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$ est de cardinal p^n ; par conséquent le nombre de points fixes est divisible par p (Corollaire **??**). Par ailleurs le vecteur nul est un point fixe, donc le nombre de points fixes est supérieur ou égal à 1. Il en résulte que le nombre de points fixes est supérieur ou égal à p.

Un point fixe non nul pour un groupe de matrices peut être interprété comme un "vecteur propre simultané" de valeur propre 1. Ce sont les seuls "vecteurs propres simultanés" possibles

pour G dans $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$ puisque l'ordre de chaque élément de G est une puissance de p et l'unique élément dont l'ordre est une puissance de p dans $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ est 1.

Corollaire 7.3.4

Soit p un nombre premier. Tout groupe d'ordre p^2 est abélien.

Démonstration. — Soit G un groupe d'ordre p^2. Un élément de $\mathrm{G} \smallsetminus \{e\}$ est d'ordre p ou p^2 (Théorème 1.6.4).

- Si G possède un élément d'ordre p^2, alors G est cyclique, donc abélien.
- Supposons que G ne possède pas d'élément d'ordre p^2 ; les éléments de $\mathrm{G} \smallsetminus \{e\}$ sont donc d'ordre p. Le Corollaire 7.3.2 assure l'existence d'un élément $g \in Z(\mathrm{G}) \smallsetminus \{e\}$; en particulier g est d'ordre p. Soit h un élément de $\mathrm{G} \smallsetminus \langle g \rangle$. Comme g appartient au centre de G les éléments g^i et h^j commutent pour tous i, j dans $\mathbb{Z}$. Il en résulte que $\mathrm{H} = \{g^i h^j \mid i,\, j \in \mathbb{Z}\}$ est un sous-groupe abélien de G. Puisque H contient g, nous avons l'inclusion $\langle g \rangle \subsetneq \mathrm{H}$. Ainsi d'une part $p = |\langle g \rangle| < |\mathrm{H}|$, d'autre part $|\mathrm{H}|$ divise p^2 (en effet H est un sous-groupe de G). Nous en déduisons que $|\mathrm{H}| = p^2$ et $\mathrm{H} = \mathrm{G}$. En particulier G est abélien.

□

Théorème 7.3.1

Soit G un p-groupe non trivial. Soit N un sous-groupe distingué non trivial de G. Alors $\mathrm{N} \cap Z(\mathrm{G}) \neq \{e\}$.

Démonstration. — Considérons l'action de G sur N par conjugaison (cette action est bien définie, c'est-à-dire ghg^{-1} appartient à N pour tout $g \in \mathrm{G}$ et tout $h \in \mathrm{N}$ car $\mathrm{N} \triangleleft \mathrm{G}$)

$$\mathrm{G} \times \mathrm{N} \to \mathrm{N}, \qquad (g, h) \mapsto ghg^{-1}$$

et comptons les points fixes. Puisque N est un p-groupe non trivial, le Corollaire 7.3.2 assure que $|\mathrm{N} \cap Z(\mathrm{G})|$ est un multiple de p. Ainsi $\mathrm{N} \cap Z(\mathrm{G})$ est non trivial. □

Théorème 7.3.2

Soit G un groupe fini. Soit H un p-sous-groupe de G tel que p divise $[\mathrm{G} : \mathrm{H}]$. Alors p divise $[N_{\mathrm{G}}(\mathrm{H}) : \mathrm{H}]$. En particulier, $N_{\mathrm{G}}(\mathrm{H}) \neq \mathrm{H}$.

Démonstration. — Considérons l'action de H sur G/H par translation à gauche :

$$\mathrm{H} \times \mathrm{G}/\mathrm{H} \to \mathrm{G}/\mathrm{H}, \qquad (g, a\mathrm{H}) \mapsto g \cdot (a\mathrm{H}) = (ga)\mathrm{H};$$

Puisque H est un p-groupe la Proposition 7.3.1 assure que $[\mathrm{G}:\mathrm{H}] \equiv_p \#{}^{\mathrm{G}}\!/_{\mathrm{H}}{}^{\mathrm{H}}$. Un point fixe est une classe à gauche $g\mathrm{H}$ telle que $h \cdot g\mathrm{H} = g\mathrm{H}$ pour tout $h \in \mathrm{H}$, *i.e.* telle que $hg\mathrm{H} = g\mathrm{H}$ pour tout $h \in \mathrm{H}$. Cela signifie que hg appartient à $g\mathrm{H}$ pour tout $h \in \mathrm{H}$, *i.e.* $g^{-1}\mathrm{H}g = \mathrm{H}$. Autrement dit g appartient à $N_{\mathrm{G}}(\mathrm{H})$. Ainsi les points fixes sont les classes à gauche $g\mathrm{H}$ avec $g \in N_{\mathrm{G}}(\mathrm{H})$ et $[\mathrm{G}:\mathrm{H}] \equiv_p \#{}^{\mathrm{G}}\!/_{\mathrm{H}}{}^{\mathrm{H}}$ se réécrit $[\mathrm{G}:\mathrm{H}] \equiv_p [N_{\mathrm{G}}(\mathrm{H}):\mathrm{H}]$. Si p divise $[\mathrm{G}:\mathrm{H}]$, alors $[\mathrm{G}:\mathrm{H}] \equiv_p 0$ et $[N_{\mathrm{G}}(\mathrm{H}):\mathrm{H}] \equiv_p 0$; en particulier, $[N_{\mathrm{G}}(\mathrm{H}):\mathrm{H}] \neq 1$ et $N_{\mathrm{G}}(\mathrm{H}) \neq \mathrm{H}$. □

Exemple 7.3.2. — Considérons le groupe $\mathrm{G} = \mathcal{A}_4$ et le sous-groupe $\mathrm{H} = \{\mathrm{id}, (1\ 2)(3\ 4)\}$. Remarquons que 2 divise $[\mathrm{G}:\mathrm{H}]$; nous avons $N_{\mathrm{G}}(\mathrm{H}) \neq \mathrm{H}$ (Théorème 7.3.2). On peut en effet vérifier que $N_{\mathrm{G}}(\mathrm{H}) = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Corollaire 7.3.5

Soit G un p-groupe. Tout sous-groupe de G d'indice p est un sous-groupe distingué de G.

Démonstration. — Soit H un sous-groupe de G d'indice p. Considérons l'action de G sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ par translation à gauche

$$\mathrm{G} \times {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}, \qquad (g, a\mathrm{H}) \mapsto g \cdot (a\mathrm{H}) = (ga)\mathrm{H}.$$

Soit $\varphi\colon \mathrm{G} \to \mathfrak{S}_{{}^{\mathrm{G}}\!/_{\mathrm{H}}} \simeq \mathfrak{S}_p$ le morphisme associé à cette action. Notons K le noyau de φ ; c'est un sous-groupe distingué de G.

- ◇ D'une part ${}^{\mathrm{G}}\!/_{\mathrm{K}}$ se plonge dans $\mathfrak{S}_p$; par suite $\left|{}^{\mathrm{G}}\!/_{\mathrm{K}}\right|$ divise $p!$. Puisque $\left|{}^{\mathrm{G}}\!/_{\mathrm{K}}\right|$ est une puissance de p, nous avons l'alternative : $\left|{}^{\mathrm{G}}\!/_{\mathrm{K}}\right| = 1$ ou $\left|{}^{\mathrm{G}}\!/_{\mathrm{K}}\right| = p$.
- ◇ D'autre part pour tout $g \in \mathrm{K}$ nous avons $g\mathrm{H} = \mathrm{H}$ ce qui entraîne g appartient à H (Théorème 1.6.2). Autrement dit $\mathrm{K} \subset \mathrm{H}$ d'où $[\mathrm{G}:\mathrm{K}] > 1$.

Finalement $\left|{}^{\mathrm{G}}\!/_{\mathrm{K}}\right| = p$. Il en résulte que $\#{}^{\mathrm{H}}\!/_{\mathrm{K}} = \frac{\left|{}^{\mathrm{G}}\!/_{\mathrm{K}}\right|}{\#{}^{\mathrm{G}}\!/_{\mathrm{H}}} = 1$, c'est-à-dire $\mathrm{H} = \mathrm{K} \triangleleft \mathrm{G}$. □

Nous avons un résultat un peu plus géneéral :

Théorème 7.3.3

Soit G un p-groupe fini non trivial d'ordre p^n. Le groupe G contient un sous-groupe distingué d'ordre p^j pour tout $0 \leq j \leq n$.

Démonstration. — Nous raisonnons par récurrence sur n.

Le résultat est vrai si $n = 1$. En effet, d'après le Corollaire 7.3.2, le centre $Z(\mathrm{G})$ de G est un p-groupe non trivial. Soit $g \in Z(\mathrm{G}) \smallsetminus \{e\}$. Le Théorème de Lagrange assure que g est d'ordre p^r pour un certain $r \geq 1$. Ainsi $g^{p^{r-1}}$ est d'ordre p ; en particulier, $Z(\mathrm{G})$ contient un sous-groupe d'ordre p, qui est distingué dans G puisque tout sous-groupe de $Z(\mathrm{G})$ est un sous-groupe distingué de G.

Supposons $n \geq 2$ et l'énoncé vrai pour les p-groupes d'ordre p^{n-1}. Si $|\mathrm{G}| = p^n$, alors il a un sous-groupe distingué N d'ordre p par l'argument précédent. Alors $\left|{}^{\mathrm{G}}\!/_{\mathrm{N}}\right| = p^{n-1}$, donc pour $0 \leq j \leq n-1$ il existe un sous-groupe distingué de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$ d'ordre p^j. La préimage de ce groupe par la projection canonique $\mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{N}}$ est un sous-groupe distingué de G d'ordre $p^j\,|\mathrm{N}| = p^{j+1}$. □

Exemple 7.3.3. — Les sous-groupes d'ordre 2 de D_8 sont $\langle s\rangle$, $\langle rs\rangle$, $\langle r^2 s\rangle$, $\langle r^3 s\rangle$ et $\langle r^2\rangle$. Le dernier est distingué. Les sous-groupes d'ordre 4 de D_8 sont $\langle r\rangle$ et $\langle r^2, s\rangle$; tous deux sont distingués. Enfin $\{\mathrm{id}\}$ et D_8 sont deux groupes distingués dans D_8. Ainsi D_8 contient un sous-groupe distingué d'ordre 2^j pour tout $0 \leq j \leq 3$.

Théorème 7.3.4

Soit G un groupe fini non trivial. Soit p le plus petit facteur premier de $|\mathrm{G}|$. Tout sous-groupe de G d'indice p est un sous-groupe distingué de G.

Démonstration. — Considérons l'action de G sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ par translation à gauche. Soit

$$\varphi\colon \mathrm{G} \to \mathfrak{S}_{{}^{\mathrm{G}}/_{\mathrm{H}}} \simeq \mathfrak{S}_p, \qquad g \mapsto \varphi(g)\colon {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}, \quad x\mathrm{H} \mapsto gx\mathrm{H}$$

le morphisme associé. Désignons par K le noyau de φ ; c'est un sous-groupe distingué de G. Le groupe quotient ${}^{\mathrm{G}}\!/_{\mathrm{K}}$ se plonge dans $\mathfrak{S}_p$; il en résulte que $[\mathrm{G} : \mathrm{K}]$ divise $p!$. Puisque $[\mathrm{G} : \mathrm{K}]$ divise $|\mathrm{G}|$ dont le plus petit facteur premier est p, le pgcd de $|\mathrm{G}|$ et $p!$ est p. Ainsi ou bien $[\mathrm{G} : \mathrm{K}] = 1$, ou bien $[\mathrm{G} : \mathrm{K}] = p$. Remarquons que pour tout g dans K nous avons $g\mathrm{H} = \mathrm{H}$; ainsi le Théorème 1.6.2 assure que g appartient à H. Par conséquent $\mathrm{K} \subset \mathrm{H}$ et

$$[\mathrm{G} : \mathrm{K}] = [\mathrm{G} : \mathrm{H}][\mathrm{H} : \mathrm{K}] = p[\mathrm{H} : \mathrm{K}].$$

Il en résulte que $[\mathrm{G} : \mathrm{K}] = p$ et $[\mathrm{H} : \mathrm{K}] = 1$ d'où $\mathrm{H} = \mathrm{K} \triangleleft \mathrm{G}$. □

Corollaire 7.3.6

Soit G un groupe fini.

- Si H est un sous-groupe de G d'indice 2, alors H est un sous-groupe distingué de G.
- Si G est un p-groupe et H est un sous-groupe de G d'indice p, alors H est un sous-groupe distingué de G.
- Si $|\mathrm{G}| = pq$ où $p < q$ sont des nombres premiers distincts, alors chaque sous-groupe de G d'ordre q est un sous-groupe distingué de G.

7.4. Applications au groupe de permutations et au groupe alterné

7.4.1. Automorphismes extérieurs de $\mathfrak{S}_6$, version 1. —

Lemme 7.4.1

Soit $n \geq 5$. Soit H un sous-groupe de $\mathfrak{S}_n$ d'indice n. Si H agit transitivement sur $\{1, 2, \ldots, n\}$, alors le morphisme associé à l'action de $\mathfrak{S}_n$ sur ${}^{\mathfrak{S}_n}\!/_{\mathrm{H}}$ est un automorphisme extérieur.

Démonstration. — Considérons l'action

$$\mathfrak{S}_n \times {}^{\mathfrak{S}_n}\!/_{\mathrm{H}} \to {}^{\mathfrak{S}_n}\!/_{\mathrm{H}} \qquad (g, h\mathrm{H}) \mapsto g \cdot (h\mathrm{H}) = (gh)\mathrm{H}.$$

Soit $\varphi\colon \mathfrak{S}_n \to {}^{\mathfrak{S}_n}\!/_{\mathrm{H}}$ le morphisme de groupes associé à cette action :

$$\varphi\colon \mathfrak{S}_n \to \mathfrak{S}_{{}^{\mathfrak{S}_n}\!/_{\mathrm{H}}}, \qquad g \mapsto \varphi(g)\colon {}^{\mathfrak{S}_n}\!/_{\mathrm{H}} \to {}^{\mathfrak{S}_n}\!/_{\mathrm{H}}$$
$$h\mathrm{H} \mapsto \varphi(g)(h\mathrm{H}) = g \cdot h\mathrm{H} = (gh)\mathrm{H}$$

Notons que ${}^{\mathfrak{S}_n}\!/_{\mathrm{H}}$ étant de cardinal n, les groupes $\mathfrak{S}_{{}^{\mathfrak{S}_n}\!/_{\mathrm{H}}}$ et $\mathfrak{S}_n$ sont isomorphes. Posons ${}^{\mathfrak{S}_n}\!/_{\mathrm{H}} = \{h_1\mathrm{H}, h_2\mathrm{H}, \ldots, h_n\mathrm{H}\}$. Se donner φ est équivalent à se donner

$$\widetilde{\varphi}\colon \mathfrak{S}_n \to \mathfrak{S}_{{}^{\mathfrak{S}_n}\!/_{\mathrm{H}}}, \qquad g \mapsto \widetilde{\varphi}(g)\colon \mathfrak{S}_n \to \mathfrak{S}_n$$
$$i \mapsto j \text{ tel que } \varphi(g)(h_i\mathrm{H}) = h_j\mathrm{H}$$

Les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ ou $\mathfrak{S}_n$. Si $\ker\widetilde{\varphi}$ contient $\mathcal{A}_n$, alors $\operatorname{im}\widetilde{\varphi}$ est d'ordre ≤ 2 et les orbites de ${}^{\mathfrak{S}_n}\!/_{\mathrm{H}}$ sous l'action de $\mathfrak{S}_n$ sont de cardinal ≤ 2 : contradiction avec le fait que H agit transitivement sur $\{1, 2, \ldots, n\}$. Il en résulte que $\ker\widetilde{\varphi} = \{\mathrm{id}\}$. Finalement $\widetilde{\varphi}$ est un automorphisme de $\mathfrak{S}_n$.

Supposons que $\widetilde{\varphi}$ soit un automorphisme intérieur de $\mathfrak{S}_n$, *i.e.* supposons qu'il existe $a \in \mathfrak{S}_n$ tel que $\widetilde{\varphi}(\mathrm{H}) = a\mathrm{H}a^{-1}$. Puisque H agit transitivement sur $\{1, 2, \ldots, n\}$, pour tout $1 \leq i, j \leq n$ il existe h dans H tel que $h(a^{-1}(i)) = a^{-1}(j)$. On remarque alors que $aha^{-1} \in a\mathrm{H}a^{-1} = \widetilde{\varphi}(\mathrm{H})$ envoie i sur j ; autrement dit $\widetilde{\varphi}(\mathrm{H})$ agit transitivement sur $\{1, 2, \ldots, n\}$. Néanmoins si $g_k\mathrm{H} = \mathrm{H}$ est la classe de l'élément neutre modulo H et si $h \in \mathrm{H}$, alors

$$hg_k\mathrm{H} = h\mathrm{H} = \mathrm{H} = g_k\mathrm{H}$$

c'est-à-dire $\widetilde{\varphi}(\mathrm{H})$ fixe k : contradiction avec le fait que $\widetilde{\varphi}(\mathrm{H})$ agit transitivement sur $\{1, 2, \ldots, n\}$. Il s'en suit que $\widetilde{\varphi}$ n'est pas un morphisme intérieur de $\mathfrak{S}_n$. □

Proposition 7.4.1

Il existe un sous-groupe H de $\mathfrak{S}_6$ d'indice 6 qui agit transitivement sur $\{1, 2, 3, 4, 5, 6\}$.

Démonstration. — Soit X l'ensemble des six droites du plan $(\mathbb{F}_5)^2$:

$$X = \{\mathcal{D}_1,\, \mathcal{D}_2,\, \mathcal{D}_3,\, \mathcal{D}_4,\, \mathcal{D}_5,\, \mathcal{D}_6\}, \qquad \mathcal{D}_k = \langle (1,k)\rangle,\ k \in \mathbb{F}_5,\ \mathcal{D}_0 = \langle (0,1)\rangle$$

Considérons l'action de $\mathrm{GL}(2,\mathbb{F}_5)$ sur X

$$\mathrm{GL}(2,\mathbb{F}_5) \times X \to X, \qquad (A,\mathcal{D}) \mapsto A\cdot\mathcal{D} = A(\mathcal{D}).$$

Elle est transitive. Notons φ le morphisme de $\mathrm{GL}(2,\mathbb{F}_5)$ dans $\mathfrak{S}_X \simeq \mathfrak{S}_6$ induit par cette action. L'action de $\mathrm{GL}(2,\mathbb{F}_5)$ sur X devient fidèle après avoir quotienté par le sous-groupe $\ker\varphi$ des homothéties qui est d'ordre 4 $(= \#\mathbb{F}_5 - 1)$; autrement dit φ induit un morphisme injectif $\widetilde{\varphi}$ de $\mathrm{PGL}(2,\mathbb{F}_5)$ dans $\mathfrak{S}_6$. D'une part $\operatorname{im}\widetilde{\varphi}$ agit transitivement sur $\{1,\,2,\,3,\,4,\,5,\,6\}$, d'autre part

$$|\operatorname{im}\widetilde{\varphi}| = |\mathrm{PGL}(2,\mathbb{F}_5)| = \left|\mathrm{GL}(2,\mathbb{F}_5)\big/\ker\varphi\right| = \frac{(5^2-1)(5^2-5)}{4} = 5!$$

Ainsi $\operatorname{im}\widetilde{\varphi}$ est un sous-groupe d'indice 6 de $\mathfrak{S}_6$. □

Le Lemme 7.4.1 et la Proposition 7.4.1 conduisent à l'énoncé suivant.

Théorème 7.4.1

L'inclusion $\mathrm{Int}(\mathfrak{S}_6) \subsetneq \mathrm{Aut}(\mathfrak{S}_6)$ est stricte ; autrement dit il existe un automorphisme de $\mathfrak{S}_6$ qui n'est pas intérieur.

7.4.2. Décomposition d'une permutation en transpositions. —

Théorème 7.4.2

Toute permutation est un produit de transpositions.

Démonstration du Théorème 7.4.2. — D'après le Théorème 5.1.1 il suffit de montrer que tout cycle $(i_1\ i_2\ \dots\ i_p)$ est un produit de transpositions. Montrons par récurrence sur la longueur p du cycle que

$$(i_1\ i_2\ \dots\ i_p) = (i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_p).$$

La formule est vraie pour $p = 2$.

Supposons que $p > 2$ et que la formule soit vraie pour $p-1$, *i.e.*

$$(i_1\ i_2\ \dots\ i_{p-1}) = (i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_{p-1});$$

alors

$$(i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_p) = (i_1\ i_2\ \dots\ i_{p-2})(i_{p-1}\ i_p) = (i_1\ i_2\ \dots\ i_p).$$

□

Corollaire 7.4.1

Les double-transpositions de $\mathfrak{S}_n$ engendrent $\mathcal{A}_n$.

Démonstration. — Soit σ dans $\mathcal{A}_n \subset \mathfrak{S}_n$. D'après le Théorème 7.4.2 il existe $\ell \in \mathbb{N}$ et τ_1, τ_2, …, τ_ℓ des transpositions tels que $\sigma = \tau_1\tau_2\dots\tau_\ell$. Or d'une part $1 = \operatorname{sgn}(\sigma)$ et d'autre part $\operatorname{sgn}(\sigma) = \prod_{i=1}^{n} \operatorname{sgn}(\tau_i) = (-1)^\ell$ donc ℓ est pair. □

7.4.3. Indice des sous-groupes du groupe alterné. — Le contre-exemple standard à la réciproque du Théorème de Lagrange (Théorème 1.6.4) est $\mathcal{A}_4$; en effet $\mathcal{A}_4$ est un groupe d'ordre 12 qui ne contient pas de sous-groupe d'ordre 6, autrement dit $\mathcal{A}_4$ est un groupe d'ordre 12 qui ne contient pas de sous-groupe d'indice 2.

Dès que $n \geq 5$, les groupes $\mathcal{A}_n$ n'ont pas non plus de sous-groupe d'indice 2 ; en effet, si $\mathcal{A}_n$ contenait un sous-groupe d'indice 2, alors $\mathcal{A}_n$ contiendrait un sous-groupe distingué : contradiction avec le fait que dès que $n \geq 5$ le groupe $\mathcal{A}_n$ est simple (Théorème 5.1.12).

Nous avons en fait un résultat plus précis :

Corollaire 7.4.2

Soit n un entier ≥ 5. Un sous-groupe propre de $\mathcal{A}_n$ est d'indice au moins n.

Remarque 7.4.1. — La borne inférieure du Corollaire 7.4.2 est réalisée : $[\mathcal{A}_n : \mathcal{A}_{n-1}] = n$.

Remarque 7.4.2. — Le Corollaire 7.4.2 est faux pour $n = 4$: le groupe $\mathcal{A}_4$ contient un sous-groupe d'indice 3.

Démonstration. — Soit H un sous-groupe propre de $\mathcal{A}_n$ d'indice $m > 1$. Le groupe $\mathcal{A}_n$ agit par translation à gauche sur $\mathcal{A}_n/\mathrm{H}$

$$\mathcal{A}_n \times \mathcal{A}_n/\mathrm{H} \to \mathcal{A}_n/\mathrm{H}, \qquad (a, g\mathrm{H}) \mapsto a \cdot g\mathrm{H} = (ag)\mathrm{H}.$$

Notons

$$\varphi\colon \mathcal{A}_n \to \mathfrak{S}_{\mathcal{A}_n/\mathrm{H}} \simeq \mathfrak{S}_m$$

le morphisme de groupes associé à cette action. Désignons par K le noyau de φ ; c'est un sous-groupe distingué de $\mathcal{A}_n$. Étant donné que $\mathcal{A}_n$ est simple, ou bien $\mathrm{K} = \{\mathrm{id}\}$, ou bien $\mathrm{K} = \mathcal{A}_n$. Les inclusions $\mathrm{K} \subset \mathrm{H}$ et $\mathrm{H} \subsetneq \mathcal{A}_n$ entraînent $\mathrm{K} = \{\mathrm{id}\}$. Ainsi le groupe $\mathcal{A}_n$ s'injecte dans $\mathfrak{S}_m$; en particulier $\frac{n!}{2}$ divise $m!$ d'où l'inégalité $n \leq m$. □

Remarque 7.4.3. — La démonstration du Corollaire 7.4.2 montre que si G est un groupe fini simple et H est un sous-groupe d'indice $m > 1$, alors il y a un plongement de G dans $\mathfrak{S}_m$ et $|\mathrm{G}|$ divise $m!$; ceci produit une borne inférieure pour l'indice d'un sous-groupe propre de G.

7.4.4. Simplicité de $\mathcal{A}_n$. — En utilisant l'action « hautement » transitive de $\mathcal{A}_{n-1}$ sur $\{1, 2, \dots, n-1\}$, nous allons démontrer que le groupe $\mathcal{A}_n$ est simple dès que $n \geq 5$.

Certaines actions de groupe ne se contentent pas d'envoyer un élément sur un autre mais peuvent le faire par paire. Dans ce paragraphe quand nous parlons de paire il s'agit de *paire ordonnée*.

Définition 7.4.1

Soit X un ensemble de cardinal supérieur ou égal à 2. Soit G un groupe agissant sur X. Le groupe G agit 2-*transitivement* si pour toutes paires d'éléments distincts (x, x') et (y, y') dans X il existe $g \in \mathrm{G}$ tel que $y = g \cdot x$ et $y' = g \cdot x'$.

Remarque 7.4.4. — La Définition 7.4.1 n'exclut pas la possibilité $x = y$ (ou $x = y'$) ou $x' = y'$ (ou $x' = y$).

Remarque 7.4.5. — Toute action 2-transitive est transitive. En effet, si $\#X = 2$, c'est immédiat, supposons donc que $\#X \geq 3$. Soit G un groupe agissant 2-transitivement sur X. Soient x, y et z trois éléments distincts de X. Alors (x, y) et (x, z) sont des paires d'éléments distincts dans X ; par hypothèse il existe $g \in \mathrm{G}$ tel que $g \cdot x = x$ et $g \cdot y = z$. En particulier l'action de G sur X est transitive.

Exemple 7.4.1. — Le groupe $\mathcal{A}_n$, $n \geq 4$, agit 2-transitivement sur $\{1, 2, \ldots, n\}$. En effet, si les deux paires de nombres distincts n'ont aucun élément en commun alors on peut supposer que ce sont $(1, 2)$ et $(3, 4)$. On remarque alors que la permutation paire $(1\ 3)(2\ 4)$ envoie la première paire sur la seconde. Si les paires ont un élément en commun on peut supposer qu'elles sont $(1, 2)$ et $(1, 3)$; le 3-cycle $(2\ 3\ 4)$ envoie $(1, 2)$ sur $(1, 3)$.

L'hypothèse « $n \geq 4$ » est indispensable :

- $\mathcal{A}_2$ (qui est trivial !) n'agit pas 2-transitivement sur $\{1, 2\}$.
- Remarquons que $\mathcal{A}_3$ n'agit pas 2-transitivement sur $\{1, 2, 3\}$: il n'existe pas de permutation $\sigma \in \mathcal{A}_3$ pouvant envoyer $(1, 2)$ sur $(2, 1)$.

Le Théorème 6.4.4 indique que les orbites d'un sous-groupe distingué d'un groupe agissant transitivement sur un ensemble ont le même cardinal. Nous pouvons en dire plus sur les orbites d'un sous-groupe distingué lorsque l'action du groupe est 2-transitive :

Théorème 7.4.3

Soit G un groupe agissant 2-transitivement sur un ensemble X. Un sous-groupe distingué de G agit sur X ou bien de manière triviale, ou bien de manière transitive.

Démonstration. — Soit N un sous-groupe distingué de G. Supposons que N n'agisse pas de manière triviale : $n \cdot x \neq x$ pour un certain $x \in X$ et un certain $n \in \mathrm{N} \smallsetminus \{e\}$. Soient y et y' deux éléments distincts de X. Puisque G agit 2-transitivement sur X il existe $g \in \mathrm{G}$ tel que $y = g \cdot x$ et $y' = g \cdot (nx)$. D'une part $y' = (gn) \cdot x = (gng^{-1}g) \cdot x = (gng^{-1})(gx) = (gng^{-1})(y)$ et d'autre part gng^{-1} appartient à N. Il en résulte que N agit transitivement sur X. $\square$

Exemple 7.4.2. — Le groupe $\mathcal{A}_4$ agit 2-transitivement sur l'ensemble $\{1, 2, 3, 4\}$; le Théorème 7.4.3 assure que le sous-groupe distingué $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ de $\mathcal{A}_4$ agit transitivement sur $\{1, 2, 3, 4\}$.

Dans la Remarque 7.4.5, nous avons observé qu'une action 2-transitive sur un ensemble X avec $\#X \geq 3$ doit être capable de fixer un élément arbitraire x tout en envoyant chaque élément distinct de x sur un élément distinct de x. Cela reflète le caractère transitif de l'action du stabilisateur de x sur l'ensemble $X \smallsetminus \{x\}$ (pour tout $g \in \mathrm{St}_{\mathrm{G}}(x)$, pour tout $y \in X \smallsetminus \{x\}$, si x est distinct de y, alors $g \cdot y$ est distinct de $g \cdot x = x$; par suite $\mathrm{St}_{\mathrm{G}}(x)$ agit sur $X \smallsetminus \{x\}$). Le fait que l'action de $\mathrm{St}_{\mathrm{G}}(x)$ sur $X \smallsetminus \{x\}$ soit transitive équivaut au fait que l'action de G sur X est 2-transitive :

Théorème 7.4.4

Soit X un ensemble de cardinal ≥ 3.
Soit G un groupe agissant sur un ensemble X.
Cette action est 2-transitive si et seulement si pour tout $x \in X$ le groupe $\mathrm{St}_{\mathrm{G}}(x)$ agit transitivement sur $X \smallsetminus \{x\}$.

L'hypothèse « $\#X \geq 3$ » est cruciale : si $\#X = 2$ et G agit trivialement sur X : l'action n'est pas 2-transitive mais $\mathrm{St}_{\mathrm{G}}(x)$ agit transitivement sur $X \smallsetminus \{x\}$.

Démonstration. — Si G agit 2-transitivement sur X et si x désigne un élément de X, alors $\mathrm{St}_{\mathrm{G}}(x)$ agit transitivement sur $X \smallsetminus \{x\}$ (Remarque 7.4.5).

Réciproquement, supposons que pour tout $x \in X$ l'action de $\mathrm{St}_{\mathrm{G}}(x)$ sur $X \smallsetminus \{x\}$ est transitive. Considérons deux paires (x_1, x_2) et (y_1, y_2) de $X \times X$, avec $x_1 \neq x_2$ et $y_1 \neq y_2$.

- Supposons que $x_1 \neq y_2$. Il existe g dans $\mathrm{St}_{\mathrm{G}}(x_1)$ tel que $g \cdot x_2 = y_2$ (rappelons que l'action de $\mathrm{St}_{\mathrm{G}}(x_1)$ sur $X \smallsetminus \{x_1\}$ est transitive ; notons que comme $x_1 \neq y_2$ nous avons $y_2 \in X \smallsetminus \{x_1\}$). De même il existe h dans $\mathrm{St}_{\mathrm{G}}(y_2)$ tel que $h \cdot x_1 = y_1$. Finalement $(hg) \cdot x_1 = y_1$ et $(hg) \cdot x_2 = y_2$.
- Supposons que $x_1 = y_2$. Soit z dans $X \smallsetminus \{x_1, y_1\}$ (l'existence d'un tel élément z est assurée par l'hypothèse $\#X \geq 3$). Il existe g dans $\mathrm{St}_{\mathrm{G}}(x_1)$ tel que $g \cdot x_2 = z$. Il existe h dans $\mathrm{St}_{\mathrm{G}}(z)$ tel que $g \cdot x_1 = y_1$. Il existe k dans $\mathrm{St}_{\mathrm{G}}(y_1)$ tel que $k \cdot z = y_2$. Alors $(hgk) \cdot x_1 = y_1$ et $(hgk) \cdot x_2 = y_2$.

□

Une conséquence de cet énoncé est la suivante :

Corollaire 7.4.3

Soit G un groupe agissant sur un ensemble X de cardinal ≥ 2. Soit $x_0 \in X$. L'action est 2-transitive si et seulement si elle est transitive et $\mathrm{St}_{\mathrm{G}}(x_0)$ agit transitivement sur $X \smallsetminus \{x_0\}$.

Démonstration. — Le résultat est clair lorsque $\#X = 2$; supposons donc désormais que $\#X \geq 3$. L'implication « si l'action est 2-transitive, alors elle est transitive et $\mathrm{St}_{\mathrm{G}}(x_0)$ agit transitivement sur $X \smallsetminus \{x_0\}$ » découle du Théorème 7.4.4.

Réciproquement, supposons que l'action est transitive et que $\mathrm{St}_{\mathrm{G}}(x_0)$ agit transitivement sur $X \smallsetminus \{x_0\}$. Montrons que pour tout $y \in X$ le groupe $\mathrm{St}_{\mathrm{G}}(y)$ agit transitivement sur $X \smallsetminus \{y\}$; alors le Théorème 7.4.4 assure que G agit 2-transitivement sur X. Soit y dans X. Puisque l'action est transitive il existe $g \in \mathrm{G}$ tel que $y = g \cdot x_0$. Alors $\mathrm{St}_{\mathrm{G}}(y) = g\mathrm{St}_{\mathrm{G}}(x_0)g^{-1}$. Soient z_1, z_2 dans $\mathrm{X} \smallsetminus \{y\}$; alors $g^{-1} \cdot z_1 \neq g^{-1} \cdot y = x_0$ et $g^{-1} \cdot z_2 \neq g^{-1} \cdot y = x_0$. Comme $\mathrm{St}_{\mathrm{G}}(x_0)$ agit transitivement sur $X \smallsetminus \{x_0\}$ il existe $h \in \mathrm{St}_{\mathrm{G}}(x_0)$ tel que $h \cdot g^{-1}z_1 = g^{-1}z_2$, *i.e.* tel que $(ghg^{-1}) \cdot z_1 = z_2$. Puisque ghg^{-1} appartient à $g\mathrm{St}_{\mathrm{G}}(x_0)g^{-1} = \mathrm{St}_{\mathrm{G}}(y)$, le groupe $\mathrm{St}_{\mathrm{G}}(y)$ agit transitivement sur $X \smallsetminus \{y\}$. □

Rappelons qu'un *sous-groupe maximal* est un sous-groupe propre contenu dans aucun autre sous-groupe propre.

Théorème 7.4.5

Soit G un groupe agissant 2-transitivement sur un ensemble X. Alors le stabilisateur de chaque point de X est un sous-groupe maximal de G.

Démonstration. — Soit $x_0 \in X$; posons $\mathrm{H} = \mathrm{St}_{\mathrm{G}}(x_0)$. Supposons que K soit un sous-groupe de G contenant strictement H. Le Corollaire 7.4.3 assure que $\mathrm{G} = \mathrm{H} \cup \mathrm{H}g\mathrm{H}$ pour tout $g \notin \mathrm{H}$. Soit g un élément de $\mathrm{K} \smallsetminus \mathrm{H}$. Alors $\mathrm{G} = \mathrm{H} \cup \mathrm{H}g\mathrm{H} \subset \mathrm{K}$ et donc $\mathrm{K} = \mathrm{G}$. □

Une action de groupe est dite *régulière* lorsque l'action est équivalente à l'action du groupe sur lui-même par multiplication à gauche.

Lemme 7.4.2

Soit G un groupe agissant sur un ensemble X. Si l'action est 2-transitive et fidèle et si $\mathrm{St}(x)$ est un groupe simple pour certains $x \in X$ alors tout sous-groupe distingué propre non trivial de G agit régulièrement sur X.

Démonstration. — Pour tout $x \in X$ posons $\mathrm{H}_x = \mathrm{St}(x)$. Les H_x sont conjugués (donc isomorphes) les uns aux autres et sont donc des groupes simples par hypothèse. Puisque G agit 2-transitivement sur X, le Théorème 7.4.5 assure que H_x est un sous-groupe maximal de G.

Supposons qu'il existe un sous-groupe distingué propre N de G. Puisque N n'est pas trivial et que l'action de G sur X est fidèle, N n'agit pas de manière triviale sur X. Donc N agit de manière transitive sur X (Théorème 7.4.3). Soit $x \in X$. À partir de $\mathrm{N} \subset \mathrm{G}$, nous obtenons l'inclusion $\mathrm{N} \cap \mathrm{H}_x \subset \mathrm{H}_x$. Puisque H_x est un groupe simple, $\mathrm{N} \cap \mathrm{H}_x = \{e\}$ ou $\mathrm{N} \cap \mathrm{H}_x = \mathrm{H}_x$.

Si $\mathrm{N} \cap \mathrm{H}_x = \mathrm{H}_x$ pour un certain $x \in X$ alors $\mathrm{H}_x \subset \mathrm{N}$, donc $\mathrm{N} = \mathrm{H}_x$ ou $\mathrm{N} = \mathrm{G}$ car H_x est un sous-groupe maximal de G. Comme $\mathrm{N} \neq \mathrm{G}$ nous obtenons $\mathrm{N} = \mathrm{H}_x$, mais alors N n'agit pas de manière transitive : contradiction. Par conséquent $\mathrm{N} \cap \mathrm{H}_x = \{e\}$ pour chaque x. Le groupe N

agissant de manière transitive sur X avec des stabilisateurs triviaux, N agit régulièrement sur X. □

Théorème 7.4.6

Soit G un groupe agissant sur un ensemble fini X. Supposons que $\mathrm{St}(x)$ est un groupe simple pour certains $x \in X$.
Si l'action est 3-transitive, alors G est simple ou $\#X$ appartient à $\{3, 2^n \mid n \in \mathbb{N}\}$.
Si l'action est 4-transitive, alors G est simple.

Avant de démontrer le Théorème 7.4.6, énonçons et démontrons sa principale conséquence.

Corollaire 7.4.4

Dès que $n \geq 5$, le groupe $\mathcal{A}_n$ est simple.

Démonstration. — Nous raisonnons par récurrence sur n. Pour le cas $n = 5$ on renvoie à la démonstration du Théorème 5.1.12 pour $n = 5$.

Supposons que $n \geq 6$ et que $\mathcal{A}_{n-1}$ est simple. Considérons l'action naturelle de $\mathcal{A}_n$ sur $X = \{1, 2, \ldots, n\}$. L'action est fidèle et $(n-2)$-transitive, donc fidèle et 4-transitive puisque $n \geq 6$. D'après le Théorème 7.4.6 le groupe $\mathcal{A}_n$ est simple. □

Démonstration du Théorème 7.4.6. — Soit $n = \#X \geq 3$. Supposons que G n'est pas simple et que N est un sous-groupe distingué propre de G. D'après le Lemme 7.4.2, le groupe N agit régulièrement sur X, donc $|\mathrm{N}| = n$.

Considérons $x_0 \in X$. Soit $\mathrm{H} = \mathrm{St}(x_0) \subset \mathrm{G}$. Alors $|\mathrm{G}| = |\mathrm{H}|\, n = |\mathrm{H}|\,|\mathrm{N}|$. Le sous-groupe H agit sur $X \smallsetminus \{x_0\}$. On peut aussi faire agir H sur N par conjugaison. Les conjugaisons sur N fixent l'identité, nous pouvons donc considérer l'action par conjugaison de H sur l'ensemble $\mathrm{N} \smallsetminus \{e\}$.

Puisque N agit régulièrement sur X, pour chaque $x \in X$ (même $x = x_0$) il existe un unique $g \in \mathrm{N}$ tel que $g \cdot x_0 = x$. Posons $\phi(x) = g$. Alors $\phi(x_0) = e$ et $\phi\colon X \smallsetminus \{x_0\} \to \mathrm{N} \smallsetminus \{e\}$ est une bijection. Soit $h \in \mathrm{H}$; alors

$$h \cdot \phi(x) = h\phi(x)h^{-1}.$$

Cet élément de $\mathrm{N} \smallsetminus \{e\}$ envoie x_0 sur

$$(h\phi(x)h^{-1})(x_0) = h(\phi(x)(h^{-1}(x_0))) = h(\phi(x)(x_0)) = h(x),$$

donc $\phi(h(x)) = h \cdot \phi(x)$ par la définition de ϕ. Ainsi ϕ respecte les H-actions sur $X \smallsetminus \{x_0\}$ et sur $\mathrm{N} \smallsetminus \{e\}$. L'action naturelle de H sur $X \smallsetminus \{x_0\}$ et l'action de H sur $\mathrm{N} \smallsetminus \{e\}$ par conjugaison sont donc équivalentes.

Supposons que G agit 3-transitivement sur X, alors H agit 2-transitivement sur $X \smallsetminus \{x_0\}$ et par suite son action sur $\mathrm{N} \smallsetminus \{e\}$ est 2-transitive. L'action (par conjugaison) de H sur N induit

un morphisme $\mathrm{H} \to \mathrm{Aut}(\mathrm{N})$, donc $\mathrm{Aut}(\mathrm{N})$ agit 2-transitivement sur $\mathrm{N} \smallsetminus \{e\}$. Le Théorème **??** assure que $\mathrm{N} \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^m$ ou $\mathrm{N} \simeq \mathbb{Z}/3\mathbb{Z}$. Ainsi $\#X = |\mathrm{N}| = 2m$ ou 3.

Supposons que G agit 4-transitivement sur X. Alors l'action de H sur $X \smallsetminus \{x_0\}$ est 3-transitive ; par conséquent l'action par conjugaison de H sur $\mathrm{N} \smallsetminus \{e\}$ est 3-transitive. Ainsi $\mathrm{Aut}(\mathrm{N})$ agit 3-transitivement sur $\mathrm{N} \smallsetminus \{e\}$ et $\mathrm{N} \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^2$ d'après le Corollaire **??**. Comme H est simple et agit de manière non triviale sur N, le morphisme

$$\mathrm{H} \to \mathrm{Aut}(\mathrm{N}) \simeq \mathrm{GL}\left(\mathbb{Z}/2\mathbb{Z}\right) \simeq \mathfrak{S}_3$$

est injectif. Il en résulte que $\mathrm{H} \simeq \mathbb{Z}/2\mathbb{Z}$ ou $\mathrm{H} \simeq \mathbb{Z}/3\mathbb{Z}$; en particulier $|\mathrm{G}| = |\mathrm{H}| \times 4 = 8$ ou 12. Puisque H est un sous-groupe maximal de G, la possibilité $|\mathrm{H}| = 2$ (et $|\mathrm{G}| = 8$) est exclue. Ainsi $|\mathrm{H}| = 3$ et $|\mathrm{G}| = 12$. À isomorphisme près il y a cinq groupes d'ordre 12. Dans tous ces groupes excepté $\mathcal{A}_4$, le sous-groupe d'ordre 3 est un sous-groupe distingué. Un sous-groupe distingué d'ordre 3 et un élément d'ordre 2 engendrent un sous-groupe d'ordre 6. Ainsi, puisque H est maximal dans G, le groupe G est isomorphe à $\mathcal{A}_4$. Une étude des sous-groupes d'ordre 3 de $\mathcal{A}_4$ montre que l'action de G sur G/H est équivalente à l'action naturelle de $\mathcal{A}_4$, qui n'est pas 4-transitive : contradiction. □

7.5. Théorème de Wedderburn

Théorème 7.5.1

Tout corps fini est commutatif.

Soit $\Bbbk$ un corps et soit $n \in \mathbb{N}^*$. Supposons que n est premier à la caractéristique de $\Bbbk$. L'ensemble des racines n-ièmes de l'unité dans $\Bbbk$ est noté $\mu_n(\Bbbk)$

$$\mu_n(\Bbbk) = \{\zeta \in \Bbbk \mid \zeta^n = 1\}.$$

C'est un sous-groupe de $\Bbbk^*$, de cardinal $\leq n$, donc cyclique.

Notons K_n le corps de décomposition de $P_n = X^n - 1$ sur $\Bbbk$. Alors $|\mu_n(K_n)| = n$ et $\mu_n(K_n) \simeq \mathbb{Z}/n\mathbb{Z}$. De plus comme $\mu_n(\Bbbk)$ est inclus dans $\mu_n(K_n)$, on a $\mu_n(\Bbbk) \simeq \mathbb{Z}/d\mathbb{Z}$ pour un certain diviseur d de n.

Une racine n-ième primitive de 1 est un élément ζ de K_n tel que $\zeta^n = 1$ et $\zeta^d \neq 1$ pour $d < n$. Autrement dit ζ est un générateur du groupe $\mu_n(K_n)$ de sorte qu'il y a $\varphi(n)$ racines primitives de 1. Leur ensemble est noté $\mu_n^*(K_n)$.

Le n-ième polynôme cyclotomique $\phi_{n,\Bbbk} \in K_n[X]$ est donné par la formule

$$\phi_{n,\Bbbk}(X) = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta).$$

Remarques 7.5.1. — ◇ Si ζ est une racine n-ième primitive de l'unité, les autres sont les ζ^m avec $\mathrm{pgcd}(n, m) = 1$.

◇ Le polynôme $\phi_{n,\Bbbk}$ est unitaire, de degré $\varphi(n)$.

Proposition 7.5.1

On a la formule
$$X^n - 1 = \prod_{d|n} \phi_{d,\Bbbk}(X).$$

Démonstration. — Cela résulte de l'égalité
$$\mu_n(K_n) = \bigcup_{d|n} \mu_d^*(K_n)$$
(l'union est ici disjointe) qui dit que si ζ est une racine n-ième de 1, l'ordre de ζ est un diviseur de n. □

Remarque 7.5.2. — En comparant les degrés des polynômes on retrouve la formule
$$n = \sum_{d|n} \varphi(d).$$

Démonstration du Théorème 7.5.1. — Considérons un corps fini $\Bbbk$. Notons $Z(\Bbbk)$ le centre de $\Bbbk$:
$$Z(\Bbbk) = \{a \in \Bbbk \,|\, \forall\, x \in \Bbbk,\, xa = ax\}$$
$Z(\Bbbk)$ est un sous-corps commutatif de $\Bbbk$ de cardinal $q \geq 2$. Puisque $\Bbbk$ est un $Z(\Bbbk)$-espace vectoriel on a $|\Bbbk| = q^n$ (le $Z(\Bbbk)$-espace vectoriel $\Bbbk$ est isomorphe à $Z(\Bbbk)^n$ où n est la dimension du $Z(\Bbbk)$-espace vectoriel $\Bbbk$).

Si $\Bbbk$ est commutatif la démonstration est terminée. Supposons donc $\Bbbk$ non commutatif. En particulier $n > 1$. Alors $\Bbbk^*$ agit sur lui-même par automorphismes intérieurs
$$\iota_g \colon \Bbbk^* \to \Bbbk^*, \qquad x \mapsto gxg^{-1}.$$
Considérons cette action. Soit $g \in \Bbbk^*$. Nous noterons $\mathcal{O}_g$ l'orbite de g et $\mathrm{St}(g)$ son stabilisateur. Notons que $\mathrm{St}(g) \cup \{0\}$ est un sur-corps de $Z(\Bbbk)$; nous en déduisons donc comme précédemment qu'il existe $d \in \mathbb{N}^*$ tel que $|\mathrm{St}(g)| = q^d - 1$. Comme $\mathrm{St}(g) \subset \Bbbk^*$ le théorème de Lagrange assure que $q^d - 1$ divise $q^n - 1$. Alors d divise n [1]. Finalement
$$\#\mathcal{O}_g = \frac{|\Bbbk^*|}{|\Bbbk_g^*|} = \frac{q^n - 1}{q^d - 1}.$$

1. En effet écrivons la division euclidienne de n par d : il existe $q \in \mathbb{N} \smallsetminus \{0\}$ et $r \in \mathbb{N}$ tels que $n = dq + r$ et $r < d$. Alors
$$q^n - 1 = (q^d - 1)(q^{n-d} + q^{n-2d} + \ldots + q^{n-qd}) + (q^r - 1).$$
Puisque $n - qd = r < d$ cela constitue la division euclidienne de $q^n - 1$ par $q^d - 1$. Comme $q^d - 1$ divise $q^n - 1$ nous en déduisons que $q^r - 1 = 0$ d'où $r = 0$ et d divise n.

En utilisant les formules

$$q^n - 1 = \prod_{m|n} \phi_m(q), \qquad\qquad q^d - 1 = \prod_{m|d} \phi_m(q).$$

nous en déduisons que si $d < n$ alors $\phi_n(q)$ divise

$$\#\mathcal{O}_g = \frac{q^n - 1}{q^d - 1} = \prod_{\substack{m|n \\ m\nmid d}} \phi_m(q).$$

Considérons $\{x_1, x_2, \ldots, x_r\} \subset \Bbbk^*$ un système de représentants des orbites non triviales. D'après l'équation aux classes

$$|\Bbbk^*| = |Z(\Bbbk)^*| + \sum_{i=1}^{r} \#\mathcal{O}_{x_i}$$

soit d'après ce qui précède

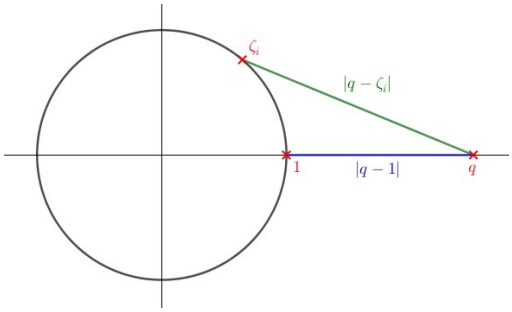
$$q^n - 1 = (q-1) + \sum_{i=1}^{r} \#\mathcal{O}_{x_i}.$$

Par suite $\phi_n(q)$ divise $q - 1$. En particulier $|\phi_n(q)| \leq q - 1$.

Notons $\zeta_1, \ldots, \zeta_\ell$ les racines primitives $n$ièmes de 1 ; elles vérifient

$$\begin{cases} |\zeta_i| = 1 \\ \zeta_i \neq 1 \text{ (car } n \neq 1) \end{cases}$$

On a $\phi_n(q) = (q - \zeta_1)(q - \zeta_2) \ldots (q - \zeta_\ell)$. Pour tout i on a $|q - \zeta_i| > q - 1$:



Ainsi

$$|\phi_n(q)| > (q-1)^\ell \geq q - 1$$

contradiction. □

7.6. Automorphismes de $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier ≥ 2. Si s désigne un élément de $\mathbb{Z}$, nous notons $\overline{s}$ son image dans $\mathbb{Z}/n\mathbb{Z}$.

Proposition 7.6.1

Soit $s \in \mathbb{Z}$. Les propriétés suivantes sont équivalentes :

- s et n sont premiers entre eux ;
- $\overline{s}$ est un générateur du groupe $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$;
- $\overline{s}$ appartient au groupe $\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$ des éléments inversibles pour la multiplication de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. — D'après Bezout nous avons

$$\begin{aligned} s \text{ et } n \text{ sont premiers entre eux} &\iff \text{il existe } \lambda,\, \mu \in \mathbb{Z} \text{ tels que } \lambda s + \mu n = 1 \\ &\iff \text{il existe } \lambda \in \mathbb{Z} \text{ tel que } \overline{\lambda}\overline{s} = \overline{1} \text{ dans } \mathbb{Z}/n\mathbb{Z} \\ &\iff \overline{s} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^{\times} \end{aligned}$$

D'autre part si λ appartient à $\mathbb{Z}$, alors

$$\begin{aligned} \overline{\lambda}\overline{s} = \overline{1} &\iff \lambda\overline{s} = \overline{1} \\ &\iff \underbrace{\overline{s} + \overline{s} + \ldots + \overline{s}}_{\lambda \text{ fois}} = \overline{1} \\ &\iff \overline{1} \in \langle \overline{s} \rangle \\ &\iff \langle \overline{s} \rangle = \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

□

Définition 7.6.1

On appelle fonction d'Euler et on note $\varphi(n)$ le nombre d'entiers m tels que

$$\begin{cases} 1 \leq m \leq n \\ m \text{ premier avec } n \end{cases}$$

D'après la Proposition 7.6.1 nous avons l'égalité

$$\varphi(n) = \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}\right|$$

Par ailleurs si p est premier il est clair que

$$\begin{cases} \varphi(p) = p - 1 \\ \varphi(p^\alpha) = p^{\alpha-1}(p-1) \text{ pour un certain } \alpha \in \mathbb{N}^* \end{cases}$$

Proposition 7.6.2

Les groupes $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ et $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ sont isomorphes

$$\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$$

En particulier $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ est un groupe abélien de cardinal $\varphi(n)$.

Démonstration. — Soit ψ un élément de $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$. Alors $\psi(1)$ est un générateur de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ donc $\psi(1)$ appartient à $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ (Proposition 7.6.1). On peut donc considérer

$$\tau \colon \varphi \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) \mapsto \varphi(\overline{1}) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$$

Montrons que τ est un morphisme de groupes : soient φ et ψ deux automorphismes de $\mathbb{Z}/n\mathbb{Z}$, alors

$$\tau(\varphi + \psi) = (\varphi + \psi)(\overline{1}) = \varphi(\overline{1}) + \psi(\overline{1}) = \tau(\varphi) + \tau(\psi).$$

Soit σ défini sur $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ par $\sigma(s)x = sx$. Comme $s(x+y) = sx + sy$ on a : $\sigma(s)$ est un endomorphisme de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$. C'est un automorphisme puisque, s étant inversible, $sx = 0$ entraîne $x = 0$.

On peut vérifier que σ et τ sont réciproques l'un de l'autre. □

Précisons maintenant la structure de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ suivant la décomposition en facteurs premiers de n. Pour ce faire rappelons le Lemme chinois (Lemme 4.1.3) :

Lemme 7.6.1: (Lemme chinois)

Si p et q sont premiers entre eux, alors

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Proposition 7.6.3

Soit n un entier. Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ où les p_i désignent des entiers premiers distincts et les α_i des éléments de $\mathbb{N}^*$, alors on a

- ◇ un isomorphisme d'anneaux
$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$
- ◇ un isomorphisme de groupes
$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \simeq \prod_{i=1}^{r} \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)^\times$$
- ◇ et
$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Démonstration. — La première assertion résulte du Lemme chinois.

En passant aux éléments inversibles on obtient la seconde assertion.

Il en résulte la troisième assertion. □

Reste à déterminer la structure des $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$ pour p premier. Commençons par l'énoncé suivant :

Lemme 7.6.2

Si p est un nombre premier, alors
$$\left(\mathbb{Z}/p\mathbb{Z}\right)^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

Remarque 7.6.1. — Si d divise n, désignons par C_d l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. Soit Φ_d l'ensemble des générateurs de C_d. Comme tout élément de $\mathbb{Z}/n\mathbb{Z}$ engendre l'un des C_d le groupe $\mathbb{Z}/n\mathbb{Z}$ est réunion disjointe des Φ_d et
$$n = \#\left(\mathbb{Z}/n\mathbb{Z}\right) = \sum_{d|n} \#\Phi_d = \sum_{d|n} \varphi(d).$$

Lemme 7.6.3

Soit H un sous-groupe d'ordre fini n. Supposons que pour tout diviseur d de n
$$\#\{g \in \mathrm{H} \mid g^d = 1\} \leq d.$$
Alors H est cyclique.

Démonstration. — Soit d un diviseur de n. S'il existe $g \in \mathrm{H}$ d'ordre d, alors le sous-groupe $\langle g \rangle = \{1, g, g^2, \ldots, g^{d-1}\}$ engendré par g est cyclique d'ordre d. Étant donnée l'hypothèse tout élément h de H tel que $h^d = 1$ appartient à $\langle h \rangle$. En particulier les seuls éléments de H d'ordre d sont les générateurs de $\langle g \rangle$ et il y en a $\varphi(d)$. Ainsi le nombre d'éléments de H d'ordre d est 0 ou $\varphi(d)$. Si c'était 0 pour une valeur de d, alors $n = \sum_{d|n} \varphi(d)$ impliquerait $|\mathrm{H}| < n$: contradiction. En particulier il existe g dans H d'ordre n et $\mathrm{H} = \langle g \rangle$. □

Démonstration du Lemme 7.6.2. — On applique le Lemme 7.6.3 à $\mathrm{H} = \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ et $n = p-1$. Il est en effet clair que l'équation $x^d = 1$ qui est de degré d a au plus d solutions dans $\mathbb{Z}/p\mathbb{Z}$. □

Il faut ensuite distinguer les cas $p = 2$ et p impair.

Proposition 7.6.4

Si p est un nombre premier ≥ 3 et α un entier ≥ 2, alors

$$\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^\alpha(p-1)\mathbb{Z}.$$

Lemme 7.6.4

Si k appartient à $\mathbb{N}^*$, alors $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ pour un certain $\lambda \in \mathbb{N}^*$ premier à p.

Démonstration. — Si $k = 1$, alors

$$(1+p)^p = 1 + \binom{p}{1}p + \ldots + \binom{p}{i}p^i + \ldots + p^p$$

et pour $1 \leq i < p$, p divise $\binom{p}{i}$ donc pour $i \geq 2$ et $i < p$ p^3 divise $\binom{p}{i}p^i$ et comme $p \geq 3$ p^3 divise aussi p^p de sorte que

$$(1+p)^p = 1 + p^2 + up^3 = 1 + p^2(1+up)$$

et $\lambda = 1 + up$ est bien premier à p.

Supposons que $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ avec λ premier à p, alors

$$(1+p)^{p^{k+1}} = (1+\lambda p^{k+1})^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} \lambda^i p^{(k+1)i} + \lambda^p p^{(k+1)p}.$$

Si $i = 1$, alors λp^{k+2} et pour $i \geq 2$ nous remarquons que p^{k+3} est en facteur donc

$$(1+p)^{p^{k+1}} = 1 + p^{k+2}(\lambda + up).$$

□

Démonstration de la Proposition 7.6.4. — D'après le Lemme 7.6.4 $1+p$ est un élément d'ordre $p^{\alpha-1}$ de $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$. En effet

$$(1+p)^{p^{\alpha-1}} = 1 + \lambda p^\alpha \equiv_{p^\alpha} 1$$

et

$$(1+p)^{p^{\alpha-2}} = 1 + \lambda p^{\alpha-1}$$

avec $p \not| \lambda$ donc $(1+p)^{p^{\alpha-2}} \neq 1$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$.

Considérons l'homomorphisme surjectif naturel induit par l'identité de $\mathbb{Z}$:

$$\psi\colon \left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times \to \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$$

Soit g un élément de $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$ qui engendre $\mathbb{Z}/(p-1)\mathbb{Z}$ (Lemme 7.6.2). L'ordre de g est un multiple de $p-1$ et donc dans le groupe $\langle g\rangle$ il y a un élément h d'ordre $p-1$. Mais comme $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$ est abélien, $h(1+p)$ est d'ordre $p^{\alpha-1}(p-1)$ en vertu du Lemme 7.6.4 et le groupe est cyclique. □

Il reste à traiter le cas $p = 2$:

Proposition 7.6.5

Nous avons

$$\begin{cases} \left(\mathbb{Z}/2\mathbb{Z}\right)^\times = \{1\} \\ \left(\mathbb{Z}/4\mathbb{Z}\right)^\times = \{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z} \\ \left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \text{ pour } \alpha \geq 3 \end{cases}$$

Remarque 7.6.2. — Le groupe $\left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times$ n'est donc pas cyclique dès que $\alpha \geq 3$.

Lemme 7.6.5

Si k désigne un élément de $\mathbb{N}^*$, alors $5^{2^k} = 1 + \lambda\, 2^{k+2}$ pour un certain λ impair.

Démonstration. — Pour $k = 1$, nous avons d'une part $5^2 = 25$ et d'autre part $1 + 3 \times 2^3 = 25$.

Suppsons que $(5)^{2^k} = 1 + \lambda\, 2^{k+2}$. Alors

$$(5)^{2^{k+1}} = (1 + \lambda\, 2^{k+2})^2 = 1 + \lambda\, 2^{k+3} + \lambda^2\, 2^{2k+4} = 1 + \lambda(2 + \lambda\, 2^{k+2})\, 2^{k+2}.$$

□

Démonstration de la Proposition 7.6.5. — Les cas 2 et 4 sont triviaux.

Traitons les autres, *i.e.* supposons que $\alpha \geq 3$. Considérons l'homomorphisme surjectif

$$\psi\colon \left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times \to \left(\mathbb{Z}/4\mathbb{Z}\right)^\times = \{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

Posons $\mathrm{H} = \ker \psi$. Alors $|\mathrm{H}| = 2^{\alpha-2}$ et $5 \in \mathrm{H}$ est d'ordre $2^{\alpha-2}$ (Lemme 7.6.5). Par suite H est cyclique et nous avons la suite exacte

$$1 \longrightarrow \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \longrightarrow \left(\mathbb{Z}/2^{\alpha}\mathbb{Z}\right)^{\times} \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

D'autre part comme 1 et -1 ne sont pas égaux modulo 4, le sous-groupe $\{1, -1\}$ de $\left(\mathbb{Z}/2^{\alpha}\mathbb{Z}\right)^{\times}$ fournit un relèvement de $\mathbb{Z}/2\mathbb{Z}$ de sorte que l'extension est scindée. Mais comme $\left(\mathbb{Z}/2^{\alpha}\mathbb{Z}\right)^{\times}$ est abélien nous avons un produit direct :

$$\left(\mathbb{Z}/2^{\alpha}\mathbb{Z}\right)^{\times} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$

□

7.7. Isomorphismes « exceptionnels »

7.7.1. Les groupes $\mathrm{SU}(2,\mathbb{C})/\{\pm\mathrm{id}\}$ et $\mathrm{SO}(3,\mathbb{R})$ sont isomorphes. —

7.7.1.1. *Groupes de matrices.* — Soit $E = \mathbb{R}^n$ et soit q la forme quadratique canonique $q(x_1, x_2, \ldots, x_n) = \sum_{k=1}^{n} x_k^2$. L'ensemble des éléments f du groupe linéaire $\mathrm{GL}(\mathbb{R}^n)$ tels que $q(f(x)) = q(x)$ pour tout $x \in E$ est un groupe appelé groupe orthogonal standard. Il s'identifie canoniquement au groupe des matrices orthogonales $n \times n$

$$\mathrm{O}(n,\mathbb{R}) = \{A \in \mathrm{GL}(n,\mathbb{R}) \mid {}^{\mathrm{t}}AA = A{}^{\mathrm{t}}A = \mathrm{Id}\}$$

où ${}^{\mathrm{t}}A$ est la matrice transposée de A. Le déterminant d'un élément de $\mathrm{O}(n,\mathbb{R})$ appartient à $\{1, -1\}$. Le sous-groupe $\mathrm{SO}(n,\mathbb{R}) = \mathrm{O}(n,\mathbb{R}) \cap \mathrm{SL}(n,\mathbb{R})$ des éléments de $\mathrm{O}(n,\mathbb{R})$ dont le déterminant est 1 est un sous-groupe de $\mathrm{O}(n,\mathbb{R})$.

Rappelons que le groupe unitaire est

$$\mathrm{U}(n,\mathbb{C}) = \{A \in \mathrm{GL}(n,\mathbb{C}) \mid A^*A = AA^* = \mathrm{Id}\}$$

où la matrice ajdointe de A est notée A^* (*i.e.* $A^* = {}^{\mathrm{t}}\overline{A}$). Le groupe spécial unitaire est par définition $\mathrm{SU}(n,\mathbb{C}) = \mathrm{U}(n,\mathbb{C}) \cap \mathrm{SL}(n,\mathbb{C})$; il est formé des matrices unitaires de déterminant 1. Pour $n = 2$ on a

$$\mathrm{SU}(2,\mathbb{C}) = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in \mathrm{M}(2,\mathbb{C}) \mid |a|^2 + |b|^2 = 1 \right\}.$$

Rappelons que le groupe $\mathrm{SU}(2,\mathbb{C})$ est difféomorphe à la sphère $\mathbb{S}^3 \subset \mathbb{R}^4$ via

$$\varphi\colon \mathbb{S}^3 \subset \mathbb{R}^4 \to \mathrm{SU}(2,\mathbb{C}), \qquad (\alpha,\beta,\gamma,\delta) \mapsto \begin{pmatrix} \alpha + \mathbf{i}\beta & -\gamma + \mathbf{i}\delta \\ \gamma + \mathbf{i}\delta & \alpha - \mathbf{i}\beta \end{pmatrix}.$$

7.7.1.2. *Définition des quaternions.* — On appelle *corps des quaternions* l'algèbre $\mathbb{H}$ de dimension 4 sur le corps des réels ayant pour base (1, i, j, k) dans laquelle la multiplication est définie par

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1, \qquad \mathrm{ijk} = -1.$$

L'élément 1 est neutre et la dernière relation signifie

$$\mathrm{ij} = \mathrm{k} = -\mathrm{ji}, \qquad \mathrm{jk} = \mathrm{i} = -\mathrm{kj}, \qquad \mathrm{ki} = \mathrm{j} = -\mathrm{ik}.$$

Remarque 7.7.1. — Il n'est pas clair que l'algèbre $\mathbb{H}$ est un corps, ni même une algèbre associative. Nous allons le démontrer (Lemme 7.7.1 et Corollaire 7.7.1) ; à noter que nous pouvons aussi nous en convaincre à l'aide de la représentation matricielle des quaternions.

Nous identifions $\mathbb{R}$ à la sous-algèbre de $\mathbb{H}$ engendrée par 1. Nous notons $\mathbb{I}$ le sous-espace de $\mathbb{H}$ suivant

$$\mathbb{I} = \mathbb{R}\mathrm{i} \oplus \mathbb{R}\mathrm{j} \oplus \mathbb{R}\mathrm{k};$$

ses éléments sont appelés *imaginaires* ou *imaginaires quaternioniques*.

Pour $(x, y, z, t) \in \mathbb{R}^4$ et $h = x + y\mathrm{i} + z\mathrm{j} + t\mathrm{k} \in \mathbb{H}$ nous appelons *conjugué* de h le quaternion

$$\overline{h} = x - y\mathrm{i} - z\mathrm{j} - t\mathrm{k}$$

Nous appelons *norme* de h le quaternion

$$N(h) = h\overline{h}.$$

Lemme 7.7.1

Soient h, h', h'' dans $\mathbb{H}$. Nous avons :

(i) $(hh')h'' = h(h'h'')$;

(ii) $h \in \mathbb{R}$ si et seulement si $\overline{h} = h$;

(iii) $h \in \mathbb{I}$ si et seulement si $h^2 \in \mathbb{R}^-$ si et seulement si $\overline{h} = -h$;

(iv) si $h = x + y\mathrm{i} + z\mathrm{j} + t\mathrm{k}$, alors $N(h) = h\overline{h} = \overline{h}h = x^2 + y^2 + z^2 + t^2 \in \mathbb{R}$;

(v) $N(hh') = N(h)N(h')$.

Remarque 7.7.2. — La démonstration est laissée en exercice (il s'agit uniquement de calculs directs). À noter que l'égalité $N(hh') = N(h)N(h')$ prend un relief nouveau une fois vue la réalisation matricielles des quaternions : la norme, dans cette réalisation, n'est autre que le déterminant.

Notons que $q \mapsto N(q)$ est une forme quadratique euclidienne sur $\mathbb{H}$ de forme polaire $\varphi(q_1, q_2) = \frac{1}{2}(q_1\overline{q_2} + q_2\overline{q_1})$. La base (1, i, j, k) est orthonormée relativement à N et la conjugaison est une symétrie orthogonale, d'espaces propres $\mathbb{R}$ et $\mathbb{I}$.

Corollaire 7.7.1

L'algèbre $\mathbb{H}$ est un corps non commutatif.

Démonstration. — L'associativité a été « vue » dans le Lemme 7.7.1.

Reste a vérifier que tout élément non nul a un inverse : si $h = x + y\mathrm{i} + z\mathrm{j} + t\mathrm{k} \in \mathbb{H} \smallsetminus \{0\}$, alors

$$h^{-1} = \frac{1}{N(h)}\overline{h}.$$

□

La non-commutativité de l'algèbre des quaternions fait que nous nous intéressons en premier à son centre. Puisque 1 est central dans $\mathbb{H}$, il en est de même de la sous-algèbtre $\mathbb{R}$. En fait la réciproque est vraie.

Proposition 7.7.1

Le centre de $\mathbb{H}$ est réduit à $\mathbb{R}$.

Démonstration. — D'apès l'assertion qui précède il suffit de montrer une seule inclusion.

Soit h dans le centre de $\mathbb{H}$. Montrons que h est réel. Posons $h = x + y\mathrm{i} + z\mathrm{j} + t\mathrm{k}$ avec x, y, z et t dans $\mathbb{R}$. Alors les égalités $h\mathrm{i} = \mathrm{i}h$, $h\mathrm{j} = \mathrm{j}h$ et $h\mathrm{k} = \mathrm{k}h$ donnent par identification $y = -y$, $z = -z$ et $t = -t$. Ainsi $h = x$ est réel. □

Donnons maintenant la réalisation matricielle complexe des quaternions. Considérons dans $\mathrm{GL}(2, \mathbb{C})$ les sous-groupes $\mathbb{R}^{+*} = \mathbb{R}^{+*}\mathrm{Id}$ et $\mathrm{SU}(2, \mathbb{C})$:

$$\mathrm{SU}(2, \mathbb{C}) = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in \mathrm{M}(2, \mathbb{C}) \,|\, |a|^2 + |b|^2 = 1 \right\}.$$

Leur intersection est triviale et ils commutent entre eux. Le groupe engendré par ces deux sous-groupes de $\mathrm{GL}(2, \mathbb{C})$ est isomorphe à leur produit direct topologique

$$H^* \simeq \mathbb{R}^{+*} \times \mathrm{SU}(2, \mathbb{C}).$$

Nous définissons alors $H = H^* \cup \{0\}$ de sorte que

$$H = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in \mathrm{M}(2, \mathbb{C}) \,|\, a,\, b \in \mathbb{C} \right\}$$

En tant qu'espace vectoriel réel H est de dimension 4 et admet pour base

$$\mathrm{id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad I = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix} \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad K = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$$

Ainsi si x, y, z, $t \in \mathbb{R}$ et si $a = x + \mathbf{i}y$ et $b = -z + \mathbf{i}t$, alors un élément typique de H s'écrit

$$h = x\mathrm{id} + yI + zJ + tK = \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}$$

Nous pouvons vérifier que H est un corps non commutatif isomorphe à $\mathbb{H}$. Dans cette réalisation l'anti-automorphisme de conjugaison $\overline{} : h \mapsto h^*$ s'identifie à l'adjoinction des matrices et la norme multiplicative d'un élément h est

$$N(h) = h\overline{h} = \overline{h}h = |a|^2 + |b|^2 = \det h.$$

7.7.1.3. *L'isomorphisme.* —

Théorème 7.7.1

Les groupes ${\mathrm{SU}(2,\mathbb{C})}/{\{\pm\mathrm{id}\}}$ et $\mathrm{SO}(3,\mathbb{R})$ sont isomorphes :

$$\mathrm{SU}(2,\mathbb{C})/\{\pm\mathrm{id}\} \simeq \mathrm{SO}(3,\mathbb{R})$$

Lemme 7.7.2

Les retournements, *i.e.* les rotations d'angle π, engendrent $\mathrm{SO}(3,\mathbb{R})$.

Démonstration. — Tout élément de $\mathrm{SO}(3,\mathbb{R})$ est la composition d'un nombre pair de réflexions. Il suffit donc de montrer que la composée de deux réflexions est une composée de deux retournements.

Soient x et y deux points de $\mathbb{R}^3 \smallsetminus \{0\}$. On désigne par τ_x et τ_y les réflexions respectives par rapport à $x^\perp$ et $y^\perp$. On a

$$\tau_x \circ \tau_y = (-\tau_x) \circ (-\tau_y)$$

et $-\tau_x$ et $-\tau_y$ sont des retournements. □

Démonstration du Théorème 7.7.1. — Rappelons que

$$\mathbb{H} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in M(2,\mathbb{C}) \,|\, a,\, b \in \mathbb{C} \right\}.$$

est un $\mathbb{R}$-espace vectoriel de dimension 4 dont la base canonique est $\{\mathrm{id},\, I,\, J,\, K\}$ où

$$I = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad K = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}.$$

Le déterminant correspond à la norme au carrée $N\colon h \mapsto h\overline{h}$ donc au produit scalaire standard sur $\mathbb{R}^4$; du point de vue matriciel $\overline{h}$ correspond à la transposée conjuguée.

Le sous-espace

$$\mathbb{I} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in M(2,\mathbb{C}) \,|\, a \in \mathbf{i}\mathbb{R},\, b \in \mathbb{C} \right\}$$

des quaternions imaginaires purs est l'orthogonale de $\mathbb{R} = \mathbb{R}\mathrm{id}$; il s'identifie à $\mathbb{R}^3$.

Notons que $\mathrm{SU}(2,\mathbb{C}) \simeq \mathbb{S}^3$ agit sur $\mathbb{H}$ par automorphismes d'algèbres

$$\begin{aligned} \varphi\colon \mathrm{SU}(2,\mathbb{C}) &\to \mathrm{Aut}(\mathbb{H}) \\ h \mapsto \varphi_h\colon \mathbb{H} &\to \mathbb{H} \\ u &\mapsto huh^{-1} \end{aligned}$$

L'application φ_h est linéaire et respecte la norme de $\mathbb{H}$ car $N(huh^{-1}) = N(u)$. Comme id est central dans $\mathbb{H}$ l'action de $\mathrm{SU}(2,\mathbb{C})$ préserve $\mathbb{R}$ et donc préserve son orthogonal $\mathbb{I}$. On peut alors considérer

$$\begin{aligned} \varphi\colon \mathrm{SU}(2,\mathbb{C}) &\to \mathrm{O}(\mathbb{I}) \\ h \mapsto \varphi_h\colon \mathbb{I} &\to \mathbb{I} \\ u &\mapsto huh^{-1} \end{aligned}$$

Via le choix d'une base on a un isomorphisme entre les isométries de $\mathbb{I}$ et le groupe orthogonal $\mathrm{O}(3,\mathbb{R})$. On peut donc définir un morphisme encore noté $\varphi\colon \mathrm{SU}(2,\mathbb{C}) \to \mathrm{O}(3,\mathbb{R})$.

Remarquons qu'en fait φ est à valeurs dans $\mathrm{SO}(3,\mathbb{R})$; en effet $\mathrm{SU}(2,\mathbb{C})$ est connexe donc $\varphi(\mathrm{SU}(2,\mathbb{C}))$ est contenu dans la composante connexe de l'identité de $\mathrm{O}(3,\mathbb{R})$, à savoir $\mathrm{SO}(3,\mathbb{R})$.

Déterminons $\ker\varphi$. Par définition

$$\ker\varphi = \{M \in \mathrm{SU}(2,\mathbb{C}) \,|\, M \text{ commute avec } I,\, J \text{ et } K\}.$$

Ainsi $\ker\varphi$ correspond à l'intersection du centre de $\mathbb{H}$ (*i.e.* les quaternions réels) avec la sphère unité. Par suite $\ker\varphi = \{\pm\mathrm{id}\}$.

Montrons que φ est surjective. D'après le Lemme 7.7.2 il suffit de montrer que tout retournement est dans l'image de φ. Soit h un élément de $\mathbb{S}^3 \cap \mathbb{I} \simeq \mathbb{S}^2$. Considérons

- ◇ d'une part le retournement r_h de $\mathbb{I} \simeq \mathbb{R}^3$ d'axe $\mathbb{R}h$,
- ◇ d'autre part la rotation φ_h.

Montrons que $\varphi_h = r_h$:

- ◇ on a $\varphi_h(h) = hhh^{-1} = h$;
- ◇ soit $u \in h^\perp$, *i.e.* u tel que $u\overline{h} + h\overline{u} = 0$ car la forme bilinéaire symétrique associée à la norme $N(h) = h\overline{h}$ est
$$\langle h, h' \rangle = \frac{1}{2}\Big(h\overline{h'} + h'\overline{h}\Big).$$
Puisque u et h appartiennent à $\mathbb{I}$ l'égalité $u\overline{h} + h\overline{u} = 0$ se réécrit $-uh - hu = 0$ ou encore $huh^{-1} = -u$ soit $\varphi_h(u) = -u$.

□

7.7.2. Groupes linéaires. — *Quelques rappels*

Certaines des notions évoquées dans ce paragraphe seront reprises dans §?? pour E de dimension quelconque.

Définitions 7.7.1

Soit E un plan vectoriel (*i.e.* un espace vectoriel de dimension 2) sur $\Bbbk$.
On appelle *droite projective associée à* E l'ensemble des droites vectorielles de E. Cet ensemble est noté $\mathbb{P}(E)$.
On appelle *droite projective* tout ensemble de la forme $\mathbb{P}(E)$ (pour un certain plan vectoriel E).
La droite projective associée au plan $\Bbbk^2$ est notée $\mathbb{P}^1(\Bbbk)$; elle est appelée *droite projective standard sur* $\Bbbk$.

Soit E un plan vectoriel. A tout vecteur $x \in E \smallsetminus \{0\}$ associons la droite vectorielle $\Bbbk x$. On définit ainsi une application canonique

$$p\colon E \smallsetminus \{0\} \to \mathbb{P}(E) \qquad\qquad x \mapsto [x].$$

Elle est surjective : si D est une droite vectorielle de E et x un vecteur non nul de D, nous avons $D = \Bbbk x = [x]$. La relation d'équivalence $\mathcal{R}$ sur $E \smallsetminus \{0\}$ associée à p est la *relation de colinéarité* : si x et y appartiennent à $E \smallsetminus \{0\}$, alors $x\mathcal{R}y$ équivaut à $\Bbbk x = \Bbbk y$. Les classes modulo $\mathcal{R}$ sont donc les $D \smallsetminus \{0\}$ où D appartient à $\mathbb{P}(E)$. Nous identifions donc, via p, l'ensemble $\mathbb{P}(E)$ à l'ensemble quotient $E \smallsetminus \{0\}/_{\mathcal{R}}$.

Bien que les éléments de $\mathbb{P}(E)$ soient des droites vectorielles de E nous les appelons aussi des points de la droite projective $\mathbb{P}(E)$.

Définition 7.7.1

Soient E et E' deux plans vectoriels. Soit u un isomorphisme linéaire de E sur E'. Notons $[u]$ la bijection de $\mathbb{P}(E)$ sur $\mathbb{P}(E')$ définie ainsi : si D appartient à $\mathbb{P}(E)$, alors $[u](D)$ est la droite vectorielle $u(D)$ de E'.
On appelle *homographie* de $\mathbb{P}(E)$ sur $\mathbb{P}(E')$ toute bijection de $\mathbb{P}(E)$ sur $\mathbb{P}(E')$ de la forme $[u]$ pour un certain isomorphisme u de E sur E'.

Lemme 7.7.3

Soient E et E' deux plans vectoriels. Soient u et v deux isomorphismes de E sur E'. Pour que les homographies $[u]$ et $[v]$ soient égales il faut et il suffit que u et v soient colinéaires.

Démonstration. — Si $v = \lambda u$ pour un certain $\lambda \in \Bbbk^*$, alors $v(D) = \lambda(u(D)) = u(D)$ pour toute droite vectorielle D de E donc $[v] = [u]$.

Réciproquement supposons que $[v] = [u]$. Pour tout $x \in E$ non nul il existe alors un scalaire $\lambda_x \in \Bbbk^*$ tel que $v(x) = \lambda_x u(x)$. Montrons que l'application

$$E \smallsetminus \{0\} \to \Bbbk^*, \qquad x \mapsto \lambda_x$$

est constante. Soient donc x, y dans $E \smallsetminus \{0\}$. Supposons d'abord que x et y soient linéairement indépendants. Nous avons

$$\lambda_{x+y}u(x) + \lambda_{x+y}u(y) = \lambda_{x+y}u(x+y) = v(x+y) = v(x) + v(y) = \lambda_x u(x) + \lambda_y u(y).$$

Puisque $(u(x), u(y))$ est une famille libre de E' nous obtenons que $\lambda_x = \lambda_{x+y} = \lambda_y$. Si x et y sont liés, considérons un vecteur $z \in E \smallsetminus \Bbbk x$; alors les familles (x, z) et (y, z) sont libres donc d'après ce qui précède $\lambda_x = \lambda_z = \lambda_y$. □

Voici un énoncé essentiel sur les homographies.

Théorème 7.7.2

Soient Δ et Δ' deux droites projectives et t_1, t_2, t_3 (respectivement t'_1, t'_2, t'_3) trois points de Δ (respectivement Δ') distincts. Il existe une unique homographie h de Δ sur Δ' telle que $h(t_i) = t'_i$ pour $i = 1, 2, 3$.

Démonstration. — Il existe deux plans vectoriels E et E' tels que $\Delta = \mathbb{P}(E)$ et $\Delta' = \mathbb{P}(E')$. Pour $i = 1, 2, 3$ le point t_i de Δ est une droite vectorielle D_i de E_i de même le point t'_i de Δ' est une droite vectorielle D'_i de E'. Pour tout i choisissons un vecteur non nul x_i de D_i (respectivement x'_i de D'_i).

Puisque $D_1 \neq D_2$, (x_1, x_2) est une base de E. Il existe donc des scalaires α_1 et $\alpha_2 \in \Bbbk$ uniques tels que $x_3 = \alpha_1 x_1 + \alpha_2 x_2$. En outre D_3 étant distincte de D_1 et D_2, α_1 et α_2 sont non nuls. De même (x'_1, x'_2) est une base de E' et il existe α'_1, $\alpha'_2 \in \Bbbk^*$ tels que $x'_3 = \alpha'_1 x'_1 + \alpha'_2 x'_2$. Posons $\lambda_1 = \frac{\alpha'_1}{\alpha_1}$ et $\lambda_2 = \frac{\alpha'_2}{\alpha_2}$. Soit $u\colon E \to E'$ l'isomorphisme linéaire appliquant x_1 sur $\lambda_1 x'_1$ et x_2 sur $\lambda_2 x'_2$. Ainsi $u(D_i) = D'_i$ pour $i = 1, 2$. De plus

$$u(x_3) = u(\alpha_1 x_2 + \alpha_2 x_2) = \alpha_1\lambda_1 x'_1 + \alpha_2\lambda_2 x'_2 = \alpha'_1 x'_1 + \alpha'_2 x'_2 = x'_3$$

d'où $u(D_3) = D'_3$. L'homographie $[u]$ de Δ sur Δ' envoie bien t_i sur t'_i pour $i = 1, 2, 3$.

Soit v un isomorphisme de E sur E' distinct de u et tel que $v(D_i) = D'_i$ pour $i = 1, 2, 3$. Il existe donc β_1, β_2, $\beta_3 \in \Bbbk^*$ tels que $v(x_i) = \beta_i x'_i$ pour $i = 1, 2, 3$. Alors

$$\beta_3(\alpha'_1 x'_1 + \alpha'_2 x'_2) = \beta_3 x'_3 = v(x_3) = v(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1\beta_1 x'_1 + \alpha_2\beta_2 x'_2$$

d'où $\beta_3\alpha'_1 = \alpha_1\beta_1$ et $\beta_3\alpha'_2 = \alpha_2\beta_2$. Ainsi $\beta_1 = \lambda_1\beta_3$ et $\beta_2 = \lambda_2\beta_3$. Par conséquent $v = \beta_3 u$ car nous avons pour $i = 1, 2$

$$v(x_i) = \beta_i x'_i = \lambda_i\beta_3 x'_i = \beta_3 u(x_i).$$

Il en résulte que $[v] = [u]$. □

Remarque 7.7.3. — Soit E un plan vectoriel. Si u appartient à $\mathrm{GL}(E)$, l'homographie $[u]$ est en particulier une permutation de $\mathbb{P}(E)$. De plus $u \mapsto [u]$ est un morphisme de $\mathrm{GL}(E)$ dans le groupe $\mathfrak{S}_{\mathbb{P}(E)}$ des permutations de $\mathbb{P}(E)$.

Proposition 7.7.2

Soit E un plan vectoriel.

1. L'ensemble des homographies de la droite projective $\mathbb{P}(E)$ sur elle-même est un sous-groupe de $\mathfrak{S}_{\mathbb{P}(E)}$, nous le notons $\mathrm{PGL}(E)$. Lorsque $E = \Bbbk^2$, le groupe $\mathrm{PGL}(\Bbbk^2)$ est aussi noté $\mathrm{PGL}(2, \Bbbk)$.
2. L'application
$$\mathrm{GL}(E) \to \mathrm{PGL}(E) \qquad\qquad u \mapsto [u]$$
est un morphisme surjectif dont le noyau est le groupe des homothéties $\{\lambda \mathrm{id}_E \mid \lambda \in \Bbbk^*\}$.

Démonstration. — La première assertion résulte de la définition d'une homographie et de la Remarque 7.7.3.

Concernant la seconde assertion : la surjectivité résulte de la définition d'une homographie et la description du noyau du Lemme 7.7.3 □

Rappelons qu'une action d'un groupe G sur un ensemble E est *simplement transitive* si elle est à la fois transitive et libre, *i.e.* si pour tous x, y dans E il existe un unique $g \in \mathrm{G}$ tel que $gx = y$.

Une action d'un groupe G sur un ensemble E (d'au moins n éléments) est dite *n-transitive* si l'action correspondante sur l'ensemble des n-uplets d'éléments distincts est transitive, *i.e.* si pour n points distincts $x_1, x_2, \ldots, x_n$ et n points distincts $y_1, y_2, \ldots, y_n$ quelconques dans E, il existe toujours au moins un élément g de G tel que $g \cdot x_1 = y_1$, $g \cdot x_2 = y_2$, $\ldots$, $g \cdot x_n = y_n$. L'énoncé suivant est une simple traduction du Théorème 7.7.2 lorsque $E = E'$:

Théorème 7.7.3

Soit E un plan vectoriel. L'action naturelle de $\mathrm{PGL}(E)$, qui est un sous-groupe de $\mathfrak{S}_{\mathbb{P}(E)}$, sur $\mathbb{P}(E)$ est simplement 3 fois transitif. Autrement dit étant donnés trois points distincts t_1, t_2, t_3 (respectivement t'_1, t'_2, t'_3) de $\mathbb{P}(E)$, il existe une unique homographie h de $\mathrm{PGL}(E)$ telle que $h(t_i) = t'_i$ pour $i = 1, 2, 3$.

Donnons une interprétation de la droite projective standard $\mathbb{P}^1(\Bbbk)$ et du groupe $\mathrm{PGL}(2, \Bbbk)$ des homographies de cette droite projective. Considérons l'ensemble $\widehat{\Bbbk} = \Bbbk \cup \{\infty\}$ où ∞ est un symbole arbitraire n'appartenant pas à $\Bbbk$.

Lemme 7.7.4

Considérons l'application

$$\phi\colon \Bbbk^2 \smallsetminus \{0\} \to \widehat{\Bbbk} \qquad (x,y) \mapsto \begin{cases} \frac{x}{y} \text{ si } y \neq 0 \\ \infty \text{ si } y = 0 \end{cases}$$

Alors ϕ induit une bijection Φ de $\mathbb{P}^1(\Bbbk) = {(\Bbbk^2 \smallsetminus \{0\})}/{\mathcal{R}}$ sur $\widehat{\Bbbk}$.

Démonstration. — Tout d'abord ϕ est surjective. En effet $\infty = \phi((1,0))$ et $t = \phi((t,1))$ pour tout $t \in \Bbbk$.

Soient (x,y) et (x',y') deux éléments de $\Bbbk^2 \smallsetminus \{0\}$. Ces deux couples ont même image par ϕ si et seulement si $y = y' = 0$ ou $y \neq 0$, $y' \neq 0$ et $\frac{x}{y} = \frac{x'}{y'}$ ce qui équivaut à dire que (x,y) et (x',y') sont colinéaires. La relation d'équivalence associée à l'application ϕ est donc $\mathcal{R}$ d'où la conclusion par passage au quotient. □

Identifions le groupe $\mathrm{GL}(\Bbbk^2)$ au groupe $\mathrm{GL}(2,\Bbbk)$ des matrices carrées inversibles 2×2 à coefficients dans $\Bbbk$: toute transformation linéaire u de $\Bbbk^2$ est identifiée à sa matrice dans la base canonique de $\Bbbk^2$.

Proposition 7.7.3

Soient $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\Bbbk)$ et h l'homographie de $\mathbb{P}^1(\Bbbk)$ associée à M. La permutation $\widetilde{h} = \Phi \circ h \circ \Phi^{-1}$ de $\widehat{\Bbbk}$ s'obtient ainsi :

$$\widetilde{h}(z) = \begin{cases} \frac{az+b}{cz+d} \text{ si } z \in \Bbbk \text{ et } cz+d \neq 0 \\ \infty \text{ si } c \neq 0 \text{ et } z = -\frac{d}{c} \end{cases} \qquad \widetilde{h}(\infty) = \begin{cases} \infty \text{ si } c = 0 \\ \frac{a}{c} \text{ si } c \neq 0 \end{cases}$$

Démonstration. — Soient $z \in \widehat{\Bbbk}$ et $(x,y) \in \Bbbk^2 \smallsetminus \{0\}$ tels que $z = \phi((x,y))$ de sorte que $\Phi^{-1}(z)$ est la droite vectorielle $\Bbbk(x,y)$. L'image (x',y') de (x,y) par M est donnée par

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Par définition $\widetilde{h}(z) = \phi((x',y'))$ c'est-à-dire

$$\widetilde{h}(z) = \phi((ax+by, cx+dy)).$$

1. Supposons dans un premier temps que $z \neq \infty$, soit $y \neq 0$. Dans ce cas $z = \frac{x}{y}$ donc $x = zy$ d'où
$$\widetilde{h}(z) = \phi(y(az+b, cz+d)) = \phi((az+b, cz+d)).$$

- ◇ Si $cz+d \neq 0$, alors $\widetilde{h}(z) \in \Bbbk$ est donnée par la formule
$$\widetilde{h}(z) = \frac{az+b}{cz+d}.$$
- ◇ Supposons que $cz+d=0$. Comme $(c,d) \neq (0,0)$ nous avons $c \neq 0$ et $z = -\frac{d}{c}$. Alors $\widetilde{h}(z) = \phi((az+b,0)) = \infty$.

2. Supposons que $z=\infty$, *i.e.* que $y=0$. Alors $x \neq 0$ et
$$\widetilde{h}(\infty) = \phi(x(a,c)) = \phi((a,c)).$$
Nous en déduisons que
$$\widetilde{h}(\infty) = \begin{cases} \infty \text{ si } c=0 \\ \frac{a}{c} \text{ si } c \neq 0 \end{cases}$$

□

Désormais nous identifions via la bijection Φ définie dans le Lemme 7.7.4 la droite projective $\mathbb{P}^1(\Bbbk)$ et $\widehat{\Bbbk}$. Cette identification étant faite le groupe $\mathrm{PGL}(2,\Bbbk)$ apparaît comme sous-groupe de $\mathfrak{S}_{\widehat{\Bbbk}}$. Plus précisément $\mathrm{PGL}(2,\Bbbk)$ est formé des *transformations homographiques* de $\widehat{\Bbbk}$, *i.e.* des transformations de
$$[M]\colon z \mapsto \frac{az+b}{cz+d} \qquad\qquad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\Bbbk)$$
avec les trois conventions particulières concernant ∞ données par la Proposition 7.7.3. Rappelons que
$$\mathrm{GL}(2,\Bbbk) \to \mathrm{PGL}(2,\Bbbk) \qquad\qquad M \mapsto [M]$$
est un morphisme surjectif dont le noyau est $\{\lambda \mathrm{id} \,|\, \lambda \in \Bbbk^*\}$. Par ailleurs l'action naturelle de $\mathrm{PGL}(2,\Bbbk)$ sur $\widehat{\Bbbk}$ est simplement 3 fois transitive comme dans le Théorème 7.7.3. L'énoncé suivant donne la description du stabilisateur de ∞ :

Lemme 7.7.5

Le stabilisateur de ∞ dans l'action naturelle de $\mathrm{PGL}(2,\Bbbk)$ sur $\widehat{\Bbbk}$ est formé des transformations affines de la droite affine $\Bbbk$, *i.e.* des transformations $f\colon z \mapsto az+b$ où $a \in \Bbbk^*$ et $b \in \Bbbk$, f étant prolongée par $f(\infty)=\infty$.

Démonstration. — La Proposition 7.7.3 assure que ce stabilisateur est formé des transformations $[M]$ où $M \in \mathrm{GL}(2,\Bbbk)$ est du type $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ avec a, $d \in \Bbbk^*$ et $b \in \Bbbk$. Si M est de ce type,

alors $M = dN$ donc $[M] = [N]$ en posant

$$N = \begin{pmatrix} \frac{a}{d} & \frac{b}{d} \\ 0 & 1 \end{pmatrix}$$

d'où l'énoncé. □

***Remarque 7.7.4* (Le cas d'un corps de base fini).** — Supposons que $\Bbbk$ soit un corps fini à q éléments. Nous écrivons aussi $\Bbbk = \mathbb{F}_q$ en désignant par $\mathbb{F}_q$ un corps à q éléments fixé (un tel corps existe et est unique à isomorphisme près). Observons que la droite projective standard $\mathbb{P}^1(\Bbbk)$, identifiée à $\widehat{\Bbbk}$, est de cardinal $q+1$. Il en résulte que toute droite projective $\mathbb{P}(E)$ est de cardinal $q+1$ (considérer une homographie de $\mathbb{P}(E)$ sur $\widehat{\Bbbk}$). Le Théorème **??** assure que $\mathrm{PGL}(E)$ agit simplement 3 fois transitivement sur $\mathbb{P}(E)$, *i.e.* il agit transitivement sur l'ensemble des triplets injectifs (a, b, c) de points de $\mathbb{P}(E)$. Il est clair que cet ensemble est de cardinal $(q+1)q(q-1) = q(q^2-1)$. Il en résulte que

$$|\mathrm{PGL}(E)| = q(q^2-1).$$

À l'action naturelle et fidèle de $\mathrm{PGL}(E)$ sur $\mathbb{P}(E)$ est associé un morphisme injectif de $\mathrm{PGL}(E)$ dans $\mathfrak{S}_{\mathbb{P}(E)}$. En numérotant les points de $\mathbb{P}(E)$ on obtient donc un morphisme injectif de $\mathrm{PGL}(E)$ dans $\mathfrak{S}_{q+1}$, *i.e.* $\mathrm{PGL}(E)$ est isomorphe à un sous-groupe de $\mathfrak{S}_{q+1}$.

Théorème 7.7.4

On a les isomorphismes suivants

1. $\mathrm{GL}(2, \mathbb{F}_2) = \mathrm{SL}(2, \mathbb{F}_2) = \mathrm{PSL}(2, \mathbb{F}_2) \simeq \mathfrak{S}_3$;
2. $\mathrm{PGL}(2, \mathbb{F}_3) \simeq \mathfrak{S}_4$ et $\mathrm{PSL}(2, \mathbb{F}_3) \simeq \mathcal{A}_4$;
3. $\mathrm{PGL}(2, \mathbb{F}_4) = \mathrm{PSL}(2, \mathbb{F}_4) \simeq \mathcal{A}_5$;
4. $\mathrm{PGL}(2, \mathbb{F}_5) \simeq \mathfrak{S}_5$ et $\mathrm{PSL}(2, \mathbb{F}_5) \simeq \mathcal{A}_5$.

Lemme 7.7.6

Tout sous-groupe d'indice n dans $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

Démonstration. — Soit H un sous-groupe d'indice n dans $\mathfrak{S}_n$.

Si $n \leq 3$, on vérifie l'énoncé directement.

Si $n = 4$, alors : si $\mathrm{H} \not\simeq \mathfrak{S}_3$, alors H est cyclique (rappel : si p, q sont des nombres premiers tels que $p < q$ et p ne divise pas $q-1$ alors tout groupe d'ordre pq est cyclique) : contradiction avec le fait que $\mathfrak{S}_4$ ne contient pas d'élément d'ordre 6.

Supposons $n \geq 5$. Le groupe $\mathfrak{S}_n$, et donc aussi H, agit par translation à gauche sur $E = {}^{\mathfrak{S}_n}\!/_{\mathrm{H}}$ d'où un homomorphisme

$$\phi \colon \mathfrak{S}_n \to \mathfrak{S}_E \simeq \mathfrak{S}_n.$$

Puisque $\ker\phi = \bigcap_{a\in\mathfrak{S}_n} a\mathrm{H}a^{-1}$, $\ker\phi$ est distingué dans $\mathfrak{S}_n$ et $\ker\phi \subset \mathrm{H}$ on a $\ker\phi = \{\mathrm{id}\}$ (rappel : pour $n \geq 5$ les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathfrak{S}_n$). Pour des raisons de cardinalité ($|\mathfrak{S}_n| = |\mathfrak{S}_E \simeq \mathfrak{S}_n|$), ϕ est un isomorphisme.

Comme H est le stabilisateur de la classe de idH on a : $\phi(\mathrm{H}) \subset \mathfrak{S}_n$ est le stabilisateur d'un point et c'est donc un sous-groupe isomorphe à $\mathfrak{S}_{n-1}$. □

Démonstration du Théorème 7.7.4. — Soit E un $\Bbbk$-espace vectoriel. On introduit l'espace projectif $\mathbb{P}(E)$ associé à E ; c'est l'ensemble des droites vectorielles de E. Le groupe $\mathrm{GL}(E)$ agit sur $\mathbb{P}(E)$ et les homothéties opérant trivialement $\mathrm{PGL}(E)$ agit aussi sur $\mathbb{P}(E)$. De plus $\mathrm{PGL}(E)$ agit fidèlement sur $\mathbb{P}(E)$.

Nous faisons agir $\mathrm{PGL}(2,\mathbb{F}_q)$ sur les droites vectorielles de $(\mathbb{F}_q)^2$. Il y a $q+1$ telles droites de sorte que l'on a un morphisme injectif

$$\phi\colon \mathrm{PGL}(2,\mathbb{F}_q) \hookrightarrow \mathfrak{S}_{q+1}.$$

Par ailleurs le cardinal de $\mathrm{PGL}(2,\mathbb{F}_q)$ est $\frac{(q^2-1)(q^2-q)}{q-1} = q(q^2-1)$; c'est aussi le cardinal de $\mathrm{SL}(2,\mathbb{F}_q)$. Notons aussi que si la caractéristique de $\mathbb{F}_q$ n'est pas 2, alors $\mathrm{PSL}(2,\mathbb{F}_q)$ est d'indice 2 dans $\mathrm{PGL}(2,\mathbb{F}_q)$.

1. On a $\mathrm{PGL}(2,\mathbb{F}_2) = \mathrm{GL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2) = \mathrm{PSL}(2,\mathbb{F}_2)$.
2. Comme $|\mathrm{PGL}(2,\mathbb{F}_3)| = 24$, on a $\mathrm{PGL}(2,\mathbb{F}_3) \simeq \mathfrak{S}_4$. Puisque $\mathcal{A}_4$ est le seul sous-groupe d'indice 2 dans $\mathfrak{S}_4$ on a $\mathrm{PSL}(2,\mathbb{F}_3) \simeq \mathcal{A}_4$.
3. On a $|\mathrm{PGL}(2,\mathbb{F}_4)| = |\mathrm{PSL}(2,\mathbb{F}_4)| = 60$. Puisque $\mathcal{A}_5$ est l'unique sous-groupe d'indice 2 dans $\mathfrak{S}_5$ on a $\mathrm{PGL}(2,\mathbb{F}_4) \simeq \mathcal{A}_5$.
4. On a $|\mathrm{PGL}(2,\mathbb{F}_5)| = 120$ donc $\mathrm{PGL}(2,\mathbb{F}_5)$ s'identifie à un sous-groupe d'indice 6 de $\mathfrak{S}_6$. Ainsi, d'après le Lemme 7.7.6, le groupe $\mathrm{PGL}(2,\mathbb{F}_5)$ est isomorphe à $\mathfrak{S}_5$. Il en résulte que
$$\mathrm{PSL}(2,\mathbb{F}_5) \simeq \mathcal{A}_5.$$

□

7.8. Étude du groupe $\mathrm{O}(p,q)$

Soit n un entier naturel. L'ensemble des matrices symétriques définies positives de taille $n\times n$ est

$$\begin{aligned}\mathrm{S}^{++}(n,\mathbb{R}) &= \left\{ S \in \mathrm{GL}(n,\mathbb{R}) \,\middle|\, \begin{cases} {}^{\mathrm{t}}S = S \\ \forall\, x \in \mathbb{R}^n \smallsetminus \{0\} \quad {}^{\mathrm{t}}xSx > 0 \end{cases} \right\} \\ &= \{ P\,{}^{\mathrm{t}}P \in \mathrm{M}(n,\mathbb{R}) \,|\, P \in \mathrm{GL}(n,\mathbb{R}) \}\end{aligned}$$

Remarque 7.8.1. — L'ensemble des matrices symétriques définies positives forme un système homogène (*i.e.* un espace sur lequel un groupe agit de façon transitive).

Théorème 7.8.1: (Théorème de décomposition polaire)

La multiplication matricielle induit l'homéomorphisme

$$\mathrm{O}(n,\mathbb{R}) \times \mathrm{S}^{++}(n,\mathbb{R}) \xrightarrow{\sim} \mathrm{GL}(n,\mathbb{R}), \qquad (O,S) \mapsto OS$$

Soient p et q deux entiers naturels. On désigne par $\mathrm{O}(p,q)$ le sous-groupe de $\mathrm{GL}(p+q,\mathbb{R})$ formé des isométries de la forme quadratique standard sur $\mathbb{R}^{p+q}$ de signature (p,q) c'est-à-dire

$$x_1^2 + x_2^2 + \ldots + x_p^2 - x_{p+1}^2 - x_{p+2}^2 - \ldots - x_{p+q}^2$$

dont la matrice dans la base canonique est

$$I_{p,q} = \left(\begin{array}{cccc|cccc} 1 & 0 & \ldots & 0 & & & & \\ 0 & \ddots & \ddots & \vdots & & & 0 & \\ \vdots & \ddots & \ddots & 0 & & & & \\ 0 & \ldots & 0 & 1 & & & & \\ \hline & & & & -1 & 0 & \ldots & 0 \\ & & 0 & & 0 & \ddots & \ddots & \vdots \\ & & & & \vdots & \ddots & \ddots & 0 \\ & & & & 0 & \ldots & 0 & -1 \end{array}\right)$$

Proposition 7.8.1

Soient p et q deux entiers naturels distincts. Le groupe $\mathrm{O}(p,q)$ est homéomorphe à $\mathrm{O}(p) \times \mathrm{O}(q) \times \mathbb{R}^{pq}$.

Démonstration. — Soit $M \in \mathrm{O}(p,q) \subset \mathrm{GL}(n,\mathbb{R})$ avec $n = p+q$. La décomposition polaire assure l'existence de deux matrices $O \in \mathrm{O}(n,\mathbb{R})$ et $S \in \mathrm{S}^{++}(n,\mathbb{R})$ telles que $M = OS$.

Montrons que O et S appartiennent à $\mathrm{O}(p,q)$. Remarquons que pour cela il suffit de montrer que S appartient à $\mathrm{O}(p,q)$.

Posons $T = {}^{\mathrm{t}}MM$. On peut vérifier que $S^2 = T$. Montrons que $\mathrm{O}(p,q)$ est stable par transposition :

$$\begin{aligned} M \in \mathrm{O}(p,q) \quad &\Rightarrow \quad M I_{p,q} {}^{\mathrm{t}}M = I_{p,q} \\ &\Rightarrow \quad {}^{\mathrm{t}}M^{-1} I_{p,q} M^{-1} = I_{p,q} \\ &\Rightarrow \quad {}^{\mathrm{t}}M^{-1} \in \mathrm{O}(p,q) \\ &\Rightarrow \quad {}^{\mathrm{t}}M \in \mathrm{O}(p,q) \end{aligned}$$

On en déduit que $T = {}^{\mathrm{t}}MM \in \mathrm{O}(p,q)$ et donc que $S^2 \in \mathrm{O}(p,q)$. Puisque T est, comme S, définie positive, on peut écrire $T = \exp U$ pour $U \in \mathrm{S}(n,\mathbb{R})$ bien choisie. On a alors

$$\begin{aligned}
T \in \mathrm{O}(p,q) \quad &\Leftrightarrow \quad T I_{p,q} {}^{\mathrm{t}}T = I_{p,q} \\
&\Leftrightarrow \quad {}^{\mathrm{t}}T = I_{p,q} T^{-1} I_{p,q}^{-1} \\
&\Leftrightarrow \quad {}^{\mathrm{t}}\exp(U) = I_{p,q} (\exp U)^{-1} I_{p,q}^{-1} \\
&\Leftrightarrow \quad \exp({}^{\mathrm{t}}U) = I_{p,q} \exp(-U) I_{p,q}^{-1} \\
&\Leftrightarrow \quad \exp({}^{\mathrm{t}}U) = \exp(-I_{p,q} U I_{p,q}^{-1}) \\
&\Leftrightarrow \quad {}^{\mathrm{t}}U = U = -I_{p,q} U I_{p,q}^{-1} \quad (\exp\colon \mathrm{S}(n,\mathbb{R}) \to \mathrm{S}^{++}(n,\mathbb{R}) \text{ est bijective}) \\
&\Leftrightarrow \quad U I_{p,q} + I_{p,q} U = 0 \\
&\Leftrightarrow \quad \frac{U}{2} I_{p,q} + I_{p,q} \frac{U}{2} = 0 \\
&\Leftrightarrow \quad \frac{{}^{\mathrm{t}}U}{2} = -I_{p,q} \frac{U}{2} I_{p,q}^{-1}
\end{aligned}$$

$$\begin{aligned}
T \in \mathrm{O}(p,q) \quad &\Leftrightarrow \quad \exp\left(\frac{{}^{\mathrm{t}}U}{2}\right) = \exp\left(-I_{p,q} \frac{U}{2} I_{p,q}^{-1}\right) \\
&\Leftrightarrow \quad {}^{\mathrm{t}}\exp\left(\frac{{}^{\mathrm{t}}U}{2}\right) = I_{p,q} \exp\left(\frac{U}{2}\right)^{-1} I_{p,q}^{-1}
\end{aligned}$$

Or $\exp\left(\frac{U}{2}\right)$ appartient à $\mathrm{S}(n,\mathbb{R})$ et $\exp^2\left(\frac{U}{2}\right) = \exp U = T$. Par suite $\exp\left(\frac{U}{2}\right) = S$ et $S I_{p,q} {}^{\mathrm{t}}S = I_{p,q}$, *i.e.* S appartient à $\mathrm{O}(p,q)$. Enfin $O \in \mathrm{O}(p,q)$. Ainsi la décomposition polaire $M = OS \mapsto (O,S)$ induit une bijection continue

$$\mathrm{O}(p,q) \simeq \big(\mathrm{O}(p,q) \cap \mathrm{O}(n)\big) \times \big(\mathrm{O}(p,q) \cap \mathrm{S}^{++}(n,\mathbb{R})\big).$$

« Étude »de $\mathrm{O}(p,q) \cap \mathrm{O}(n)$: soit $O \in \mathrm{O}(p,q) \cap \mathrm{O}(n)$; on découpe O en blocs

$$0 = \left(\begin{array}{c|c} A & C \\ \hline B & D \end{array}\right) \in \mathrm{O}(p,q) \Leftrightarrow \begin{cases} {}^{\mathrm{t}}AA - {}^{\mathrm{t}}BB = I_p \\ {}^{\mathrm{t}}AC - {}^{\mathrm{t}}BD = 0 \\ {}^{\mathrm{t}}CA - {}^{\mathrm{t}}DB = 0 \\ {}^{\mathrm{t}}CC - {}^{\mathrm{t}}DD = -I_q \end{cases}$$

En effet

$$\begin{aligned}\begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix} &= \begin{pmatrix} {}^tA & {}^tB \\ {}^tC & {}^tD \end{pmatrix}\begin{pmatrix} I_p & 0 \\ 0 & I_q \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} \\ &= \begin{pmatrix} {}^tA & {}^tB \\ {}^tC & {}^tD \end{pmatrix}\begin{pmatrix} A & C \\ -B & -D \end{pmatrix} \\ &= \begin{pmatrix} {}^tAA - {}^tBB & {}^tAC - {}^tBD \\ {}^tCA - {}^tDB & {}^tCC - {}^tDD \end{pmatrix}\end{aligned}$$

D'autre part nous avons

$$O \in \mathrm{O}(n) \Longleftrightarrow \begin{cases} {}^tAA + {}^tBB = I_p \\ {}^tAC + {}^tBD = 0 \\ {}^tCA + {}^tDB = 0 \\ {}^tCC + {}^tDD = I_q \end{cases}$$

car

$$\begin{aligned}\begin{pmatrix} I_p & 0 \\ 0 & I_q \end{pmatrix} &= \begin{pmatrix} {}^tA & {}^tB \\ {}^tC & {}^tD \end{pmatrix}\begin{pmatrix} A & C \\ B & D \end{pmatrix} \\ &= \begin{pmatrix} {}^tAA + {}^tBB & {}^tAC + {}^tBD \\ {}^tCA + {}^tDB & {}^tCC + {}^tDD \end{pmatrix}\end{aligned}$$

À partir de ${}^tBB = 0$ nous obtenons $\mathrm{Tr}\,{}^tBB = 0$. Si on écrit B sous la forme $B = (b_{ij})$ il vient $\sum_{i,j} b_{i,j}^2 = 0$ puis $B = 0$. De même $C = 0$. Par conséquent $A \in \mathrm{O}(p)$ et $D \in \mathrm{O}(q)$. Ainsi

$$\mathrm{O}(p,q) \cap \mathrm{O}(n) = \left\{ \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \mid A \in \mathrm{O}(p),\, D \in \mathrm{O}(q) \right\} \simeq \mathrm{O}(p) \times \mathrm{O}(q).$$

Pour la seconde intersection on utilise que

- ⋄ $\exp\colon \mathrm{S}(n,\mathbb{R}) \to \mathrm{S}^{++}(n,\mathbb{R})$ est un homéomorphisme
- ⋄ $\exp\colon L = \{U \in \mathrm{M}(n,\mathbb{R}) \mid UI_{p,q} + I_{p,q}U = 0\} \to \mathrm{O}(p,q)$

Nous en déduisons l'homéomorphisme

$$\mathrm{S}(n,\mathbb{R}) \cap L \simeq \mathrm{S}^{++}(n,\mathbb{R}) \cap \mathrm{O}(p,q).$$

Or $\mathrm{S}(n,\mathbb{R})$ est un espace vectoriel de dimension $\frac{n(n+1)}{2}$ et on peut vérifier que

$$\dim\left(\mathrm{S}(n,\mathbb{R}) \cap L\right) = pq$$

d'où $\mathrm{O}(p,q) \cap \mathrm{S}^{++}(n,\mathbb{R}) \simeq \mathbb{R}^{pq}$.

Finalement nous avons l'homéomorphisme

$$\mathrm{O}(p,q) \simeq \mathrm{O}(p) \times \mathrm{O}(q) \times \mathbb{R}^{pq}.$$

□

7.9. Sous-groupes de $\mathrm{GL}(n,\mathbb{C})$

7.9.1. Un théorème de Burnside. —

Lemme 7.9.1

Soit A un élément de $M(n,\mathbb{C})$ telle que $\mathrm{Tr}(A^k) = 0$ pour tout k dans $\mathbb{N}^*$. Alors A est nilpotente, *i.e.* il existe un entier ℓ tel que $A^\ell = 0$.

Démonstration. — Le polynôme caractéristique de A est scindé sur $\mathbb{C}$. Raisonnons par l'absurde et supposons A non nilpotente. Alors A possède des valeurs propres complexes non nulles. Notons λ_1, λ_2, …, λ_r ces valeurs propres non nulles de A (noter que $r \geq 1$) ; désignons par n_1, n_2, …, n_r leurs multiplicités respectives. La matrice A est semblable à une matrice triangulaire avec sur la diagonale les valeurs propres apparaissant autant de fois que leur multiplicité. En élevant à la puissance $k$ième cette matrice triangulaire supérieure on obtient une matrice triangulaire semblable à A^k si bien que pour tout $k \geq 1$ on a

$$\mathrm{Tr}(A^k) = n_1\lambda_1^k + n_2\lambda_2^k + \ldots + n_r\lambda_r^k = 0.$$

Si on écrit ces relations pour $1 \leq k \leq r$ on obtient que $(n_1, n_2, \ldots, n_r)$ est solution du système linéaire

$$\begin{pmatrix} \lambda_1 & \lambda_r \\ \lambda_1^2 & \lambda_r^2 \\ \vdots & \vdots \\ \lambda_1^r & \lambda_r^r \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} = 0$$

Or ce système est de Cramer puisque le déterminant de la matrice du système vaut

$$\lambda_1\lambda_2\ldots\lambda_r \prod_{1\leq i<j\leq r} (\lambda_j - \lambda_i) \neq 0.$$

Nécessairement $n_1 = n_2 = \ldots = n_r = 0$ ce qui est exclu. □

Lemme 7.9.2

Soit G un sous-groupe de $\mathrm{GL}(n,\mathbb{C})$. Soit $(M_i)_{1\leq i\leq m} \in \mathrm{G}^m$ une base de $\mathrm{Vect}(\mathrm{G})$. Considérons l'application

$$f\colon \mathrm{G} \to \mathbb{C}^m, \qquad A \mapsto (\mathrm{Tr}(AM_i))_{1\leq i\leq m}$$

Si $f(A) = f(B)$, alors $AB^{-1} - I_n$ est nilpotente.

Démonstration. — Soient A et B dans G tels que $f(A) = f(B)$. La trace étant linéaire on a $\mathrm{Tr}(AM) = \mathrm{Tr}(BM)$ pour toute matrice $M \in \mathrm{Vect}(\mathrm{G})$. En particulier $\mathrm{Tr}(AM) = \mathrm{Tr}(BM)$ pour toute matrice M de G. Posons $D = AB^{-1}$. La matrice D appartient à G donc pour tout $k \in \mathbb{N}^*$

$$\mathrm{Tr}(D^k) = \mathrm{Tr}(AB^{-1}D^{k-1}) = \mathrm{Tr}(A(B^{-1}D^{k-1})) = \mathrm{Tr}(B(B^{-1}D^{k-1})) = \mathrm{Tr}(D^{k-1}).$$

Par conséquent pour tout k dans $\mathbb{N}$ on a $\mathrm{Tr}(D^k) = \mathrm{Tr}(I_n) = n$. Ainsi pour tout k in $\mathbb{N}^*$

$$\mathrm{Tr}(D - I_n)^k = \mathrm{Tr}\Big(\sum_{j=0}^{k} \binom{k}{j} (-1)^j D^{k-j}\Big) = n \sum_{j=0}^{k} \binom{k}{j} (-1)^j = n(1-1)^k = 0$$

D'après le Lemme 7.9.1 la matrice $D - I_n$ est nilpotente. □

Lemme 7.9.3

Soit G un sous-groupe de $\mathrm{GL}(n,\mathbb{C})$. Soit $(M_i)_{1\leq i\leq m} \in \mathrm{G}^m$ une base de $\mathrm{Vect}(\mathrm{G})$. Considérons l'application

$$f\colon \mathrm{G} \to \mathbb{C}^m, \qquad A \mapsto (\mathrm{Tr}(AM_i))_{1\leq i\leq m}$$

Supposons que toutes les matrices de G soient diagonalisables. Alors f est injective.

Démonstration. — Soient A, B deux éléments de G tels que $f(A) = f(B)$. La matrice $D = AB^{-1}$ appartient à G. Elle est donc diagonalisable. Par suite $D - I_n$ est aussi diagonalisable. De plus $D - I_n$ est nilpotente (Lemme 7.9.2). Ainsi $D - I_n = 0$, *i.e.* $A = B$. Il en résulte que f est injective. □

Un sous-groupe G de $\mathrm{GL}(n,\mathbb{C})$ est d'exposant fini s'il existe un entier N tel que $A^N = I_n$ pour toute matrice A de G.

Théorème 7.9.1

Un sous-groupe de $\mathrm{GL}(n,\mathbb{C})$ d'exposant fini est fini.

Démonstration. — Soit G un sous-groupe de $\mathrm{GL}(n,\mathbb{C})$ d'exposant fini N. Tout élément A de G est racine du polynôme $P(X) = X^N - 1$ qui est scindé à racines simples. Toute matrice de G est donc diagonalisable. Le Lemme 7.9.3 assure que l'application

$$f\colon \mathrm{G} \to \mathbb{C}^m \qquad\qquad A \mapsto (\mathrm{Tr}(AM_i))_{1\leq i\leq m},$$

où $(M_i)_{1\leq i\leq m} \in \mathrm{G}^m$ est une base de $\mathrm{Vect}(\mathrm{G})$, est injective. L'image de f est contenue dans X^m où

$$X = \{\mathrm{Tr}(A) \mid A \in \mathrm{G}\}$$

Pour conclure il suffit donc de montrer que X est fini. D'après ce qui précède

$$\{\text{valeurs propres de } A \mid A \in \mathrm{G}\} \subset \mu_N = \{\text{racines } N\text{ièmes de } 1\}.$$

Il en résulte que X est fini. □

7.9.2. Théorème de Lie-Kolchin. — Désignons par $D(\mathrm{G})$ le groupe dérivé d'un groupe G, *i.e.* le groupe engendré par les commutateurs $[g,h] = ghg^{-1}h^{-1}$, avec g, $h \in \mathrm{G}$, de G. Soit $D^2(\mathrm{G})$ le groupe dérivé de $D(\mathrm{G})$ et plus généralement soit $D^k(\mathrm{G})$ le groupe dérivé de $D^{k-1}(\mathrm{G})$.

Rappelons qu'un groupe G est *résoluble de longueur* ℓ si $D^\ell(\mathrm{G}) = \{\mathrm{id}\}$ pour un certain entier ℓ que l'on choisit ici minimal. On dit aussi qu'un groupe G est résoluble lorsqu'il existe une suite finie G_0, G_1, …, G_n de sous-groupes de G telle que

$$\{\mathrm{id}\} = \mathrm{G}_0 \lhd \mathrm{G}_1 \lhd \ldots \lhd \mathrm{G}_{n-1} \lhd \mathrm{G}_n = \mathrm{G}$$

où pour tout $0 \leq i \leq n-1$ le groupe G_i est un sous-groupe distingué de G_{i+1} et le groupe quotient $\mathrm{G}_{i+1}/\mathrm{G}_i$ est abélien.

Exemple 7.9.1. — Le seul groupe résoluble de longueur 0 est le groupe trivial.

Exemple 7.9.2. — Un groupe résoluble de longueur 1 est un groupe non trivial et abélien.

Exemple 7.9.3. — Un groupe résoluble de longueur 2 est un groupe non-abélien dont le sous-groupe des commutateurs est abélien. Dès que $n \geq 3$, le groupe D_{2n} est résoluble de longueur 2.

Exemple 7.9.4. — Les groupes $\mathfrak{S}_3$, $\mathcal{A}_4$ et $\mathfrak{S}_4$ sont résolubles.

Exemple 7.9.5. — Les groupes $\mathrm{Aff}(\Bbbk)$ et $\mathrm{Aff}\left(\mathbb{Z}/n\mathbb{Z}\right)$ sont résolubles.

Le théorème de Lie-Kolchin est un résultat de trigonalisabilité des sous-groupes connexes et résolubles du groupe des matrices inversibles $\mathrm{GL}(n,\Bbbk)$, où $\Bbbk$ est un corps algébriquement clos de caractéristique quelconque. Démontré en 1948, il tient son nom de son auteur, E. Kolchin, et de son analogie avec le théorème de Lie sur les algèbres de Lie résolubles (en caractéristique nulle), démontré en 1876 par S. Lie [(2)].

2. Soit $\Bbbk$ un corps algébriquement clos de caractéristique nulle. Soit V un espace vectoriel de dimension finie sur $\Bbbk$ et $\mathfrak{g}$ une sous-algèbre de Lie résoluble de $\mathfrak{gl}(V)$. Alors il existe une base de V dans laquelle tous les éléments de $\mathfrak{g}$ sont des matrices triangulaires supérieures.

Théorème 7.9.2: (Théorème de Lie-Kolchin)

Soit G un sous-groupe résoluble connexe de $\mathrm{GL}(n, \mathbb{C})$. Alors G est conjugué à un sous-groupe du groupe des matrices triangulaires de $\mathrm{GL}(n, \mathbb{C})$.

Remarque 7.9.1. — Si les groupes résolubles généralisent les groupes abéliens, alors le théorème de Lie-Kolchin généralise le fait qu'une famille de matrices qui commutent est simultanément trigonalisable à la différence près que ce théorème demande expressément d'avoir un groupe.

Notons donc G_k, $0 \leq k \leq \ell$, les sous-groupes comme ci-dessus. Supposons G non abélien ; en effet si G est abélien, on utilise le fait qu'une famille de matrices qui commutent deux à deux sont simultanément trigonalisables sur $\mathbb{C}$.

◇ Montrons que $D^k(\mathrm{G})$ est un sous-groupe distingué connexe de G et que le groupe quotient $D^{k-1}(\mathrm{G})/D^k(\mathrm{G})$ est abélien pour tout k.

Tout groupe dérivé d'un groupe donné G est distingué : par construction il est stable par tout automorphisme de G donc en particulier stable par automorphisme intérieur.

Comme G est connexe, $\mathrm{G} \times \mathrm{G}$ est également connexe. De plus la partie génératrice

$$X = \{[g, h] \mid g,\, h \in \mathrm{G}\}$$

de $D(\mathrm{G})$ qui est l'image de $\mathrm{G} \times \mathrm{G}$ par le commutateur est également connexe. D'après [**CG17**, II-F6] le groupe dérivé $D(\mathrm{G})$ est connexe. Par récurrence on obtient que $D^k(\mathrm{G})$ est connexe.

Le groupe dérivé de $D^{k-1}(\mathrm{G})$ est $D^k(\mathrm{G})$; par suite par passage au quotient le groupe dérivé de $D^{k-1}(\mathrm{G})/D^k(\mathrm{G})$ est $D^k(\mathrm{G})/D^k(\mathrm{G}) = \{\mathrm{id}\}$. Mais cela signifie que tous les commutateurs de $D^{k-1}(\mathrm{G})/D^k(\mathrm{G})$ sont triviaux, autrement dit que $D^{k-1}(\mathrm{G})/D^k(\mathrm{G})$ est abélien.

◇ Posons $\mathrm{A} = D^{\ell-1}(\mathrm{G})$. Montrons que A est abélien, non trivial puis que l'ensemble

$$V = \{v \in \mathbb{C}^n \mid \mathrm{A}v \in \mathbb{C}v\}$$

est non trivial.

Par minimalité de ℓ, le groupe A est non trivial. Puisque le groupe dérivé de A est trivial, $D^{\ell-1}(\mathrm{G})$ est abélien. Sur $\mathbb{C}$ les matrices de $D^{\ell-1}(\mathrm{G})$ sont simultanément trigonalisables. Soit $(e_1, e_2, \ldots, e_n)$ une base qui les trigonalise toutes. Nous avons alors : e_1 appartient à V.

◇ Soit v non nul dans V. Pour $a \in$ A posons $\chi_v(a)$ le complexe tel que $a(v) = \chi_v(a)v$. Montrons que pour tout g dans G, $g(v)$ est encore dans V et que $\chi_{g(v)}(a) = \chi_v(g^{-1}ag)$ pour tout a dans A.

Nous avons

$$a(g(v)) = g\big((g^{-1}ag)(v)\big) = g\big(\chi_v(gag^{-1})v\big) = \chi_v(gag^{-1})g(v)$$

d'où l'assertion.

◇ En utilisant la connexité de G montrer que si v est un vecteur propre de a pour la valeur propre λ, alors $g(v)$ est un vecteur propre de a pour la valeur propre λ.

Notons que comme v est non nul, $g(v)$ est également non nul. Nous avons vu que $g(v)$ est vecteur propre pour tout élément a de A. L'application de G dans $\mathbb{C}^*$ qui envoie g sur $\chi_v(g^{-1}ag)$ est continue ; en effet elle est la composée de $g \mapsto gag^{-1}$ qui est continue avec l'application χ_v qui est continue sur le stabilisateur de la droite $\mathbb{C}v$.

Ainsi l'image de G est un connexe. Comme $\chi_{g(v)}(a) = \chi_v(g^{-1}ag)$ cette image est dans l'ensemble discret des valeurs propres de a. Par conséquent $\chi_{g(v)}(a)$ n'a qu'une valeur quand g varie, celle atteinte pour $g = e$, c'est-à-dire λ.

◇ Soit v non nul dans V et soit W le sous-espace engendré par les $g(v)$, $g \in$ G. Montrons que W est un sous-espace G-stable de dimension $0 < \dim W < n$.

Le sous-espace W est défini par un système de générateurs G-stable, il est donc G-stable. Par ailleurs il contient v qui est non nul ; ainsi W est non nul.

Reste à montrer que $W \neq \mathbb{C}^n$. Soit a quelconque dans A. Alors pour tout g dans G $g(v)$ est un vecteur propre pour a pour la même valeur propre. Il s'en suit que W est un sous-espace propre pour a. Raisonnons par l'absurde, *i.e.* supposons que $W = \mathbb{C}^n$. Alors tout a est un homothétie et A est un sous-groupe constitué d'homothéties. Puisque G est non abélien, $\ell > 1$ et A est le groupe dérivé d'un groupe, en l'occurence le groupe d'érivé de $D^{\ell-2}$(G). Ainsi le déterminant d'un élément de A est 1. Comme toutes les matrices de A sont scalaires ces scalaires sont forcément des racines de l'unité. Or comme nous l'avons vu A est connexe donc A est trivial : contradiction avec la minimalité de ℓ.

◇ Montrons en utilisant une récurrence sur n qu'il existe une base de trigonalisation commune à tous les g de G.

Pour $n = 1$ c'est clair.

Pour n quelconque nous avons obtenu un sous-espace W de dimension k, $1 \leq k \leq n-1$. Soit W' un supplémentaire de W dans $\mathbb{C}^n$. En choisissant une base adaptée à la décomposition $\mathbb{C}^n = W \oplus W'$ nous constatons que g est semblable à une matrice de la forme $\begin{pmatrix} \rho(g) & \zeta(g) \\ 0 & \rho'(g) \end{pmatrix}$. De plus vue comme fonction ρ (resp. ρ') est un morphisme

continu de G dans $\mathrm{GL}(W)$ (resp. $\mathrm{GL}(W')$). Par récurrence il existe une base de W et une base de W' qui trigonalisent simultanément les $\rho(g)$ et $\rho'(g)$. Nous obtenons une base qui trigonalise tous les g de G en concaténant ces deux bases.

7.10. Dénombrement des colorations du cube

Considérons l'espace euclidien $\mathbb{R}^n$ muni du produit scalaire $\langle\,,\,\rangle$ qui donne la norme euclidienne $||v|| = \sqrt{\langle v,\, v\rangle}$. La distance associée est donnée par $d(x, y) = ||x - y||$.

Définition 7.10.1

Une *isométrie euclidienne* f est une application bijective de $\mathbb{R}^n$ qui préserve la norme euclidienne, *i.e.* qui vérifie

$$\forall\, x,\, y \in \mathbb{R}^n \qquad d(f(x), f(y)) = d(x, y).$$

Le *groupe des isométries euclidiennes* est $\mathrm{Isom}(\mathbb{R}^n, d)$.

Les translations et les éléments du groupe orthogonal $\mathrm{O}(n, \mathbb{R})$ sont des isométries euclidiennes. L'énoncé suivant donne toutes ces isométries :

Théorème 7.10.1

Toute isométrie de $(\mathbb{R}^n, d)$ est une application affine.
Toute isométrie de $(\mathbb{R}^n, d)$ qui fixe l'origine est donnée par un élément de $\mathrm{O}(n, \mathbb{R})$.
Le groupe $\mathrm{Isom}(\mathbb{R}^n)$ se décompose en un produit semi-direct de la façon suivante :

$$\mathrm{Isom}(\mathbb{R}^n) = \mathrm{O}(n, \mathbb{R}) \ltimes (\mathbb{R}^n, +)$$

où $(\mathbb{R}^n, +)$ est identifié au groupe des translations de $\mathbb{R}^n$.

Rappelons qu'une application $f\colon \mathbb{R}^n \to \mathbb{R}^n$ est *affine* s'il existe une application linéaire $A\colon \mathbb{R}^n \to \mathbb{R}^n$ et un élément b de $\mathbb{R}^n$ tels que pour tout $x \in \mathbb{R}^n$ on ait $f(x) = Ax + b$. Remarquons que le couple (A, b) est unique. En effet $b = f(0)$ et A est l'application linéaire $x \mapsto f(x) - f(0)$.

Pour $x \in \mathbb{R}^n$ nous notons τ_x la translation de vecteur x ; autrement dit $\tau_x(y) = y + x$ pour tout $y \in \mathbb{R}^n$.

Attardons-nous un instant sur la dimension trois. Avant d'énoncer la classification des isométries en dimension trois rappelons qu'un *vissage* (ou *rotation glissée*) est un déplacement dans un espace affine euclidien qui est la composée commutative d'une rotation et d'une translation selon un vecteur dirigeant l'axe de rotation (si la rotation n'est pas l'identité). Une *anti-rotation* est un type particulier d'antidéplacement (*i.e.* d'isométrie qui renverse l'orientation) de l'espace euclidien de dimension 3 (espace affine euclidien ou espace vectoriel euclidien, suivant le contexte) : c'est la composée commutative d'une rotation d'angle ϑ autour d'un axe Δ et d'une réflexion par rapport à un plan perpendiculaire à Δ.

Théorème 7.10.2

Les éléments de $\mathrm{Isom}(\mathbb{R}^3)$ sont :

- ◇ les translations,
- ◇ les rotations,
- ◇ les rotations glissées,
- ◇ les symétries orthogonales par rapport à un plan,
- ◇ les symétries glissées,
- ◇ les anti-rotations.

Pour une preuve on renvoie à [**Aud06**].

Proposition 7.10.1

Le groupe d'isométries directes du cube est isomorphe à $\mathfrak{S}_4$.

Démonstration. — Notons C_6 le cube. Désignons par $\mathrm{Isom}(C_6)$ les isométries du cube et par $\mathrm{Isom}^+(C_6)$ les isométries directes du cube. Soit $\mathcal{D} = \{D_1, D_2, D_3, D_4\}$ l'ensemble des grandes diagonales du cube (elles sont préservées par les isométries de C_6 car ce sont les plus grandes longueurs que l'on peut trouver dans le cube).

Ainsi

$$\phi\colon \mathrm{Isom}^+(C_6) \to \mathfrak{S}_4 \qquad\qquad g \mapsto g_{|\mathcal{D}}$$

Notons $D_i = A_iG_i$ les diagonales de C_6. Désignons par s_0 la symétrie centrale en 0. Si $\phi(g) = \mathrm{id}_{\mathcal{D}}$, alors

- ◇ ou bien $\begin{cases} g(A_1) = A_1 \\ g(G_1) = G_1 \end{cases}$ et dans ce cas en utilisant le fait que g fixe toutes les diagonales et les deux points opposés A_1 et G_1 nous obtenons que g fixe tous les sommets. Il en résulte que $g = \mathrm{id}_{\mathbb{R}^3}$.
- ◇ ou bien $\begin{cases} g(A_1) = G_1 \\ g(G_1) = A_1 \end{cases}$ et $s_0 g = \mathrm{id}$ d'après ce qui précède. Il s'en suit que g est la symétrie centrale s_0 en 0 : contradiction avec $g \in \mathrm{Isom}^+(C_6)$.

Ainsi $\ker \phi = \{\mathrm{id}_{\mathbb{R}^3}\}$ et nous avons l'inclusion $\mathrm{Isom}^+(C_6) \subset \mathfrak{S}_4$.

Les transpositions sont toutes réalisées grâce à des retournements d'axes reliant les milieux des arêtes joignant les diagonales).

Par suite $\mathrm{Isom}^+(C_6) \simeq \mathfrak{S}_4$. □

Par coloriage d'un cube on entend le choix d'une couleur pour chaque face et deux cubes coloriés sont considérés comme identiques s'ils diffèrent par une rotation.

Théorème 7.10.3

Le nombre de façons de colorier un cube avec au plus c couleurs est :

$$\frac{c^6 + 3c^4 + 12c^3 + 8c^2}{24}$$

Démonstration. — Avant l'identification par rotation il y a c^6 coloriages possibles. On fait agir le groupe $\mathfrak{S}_4$ des rotations du cube sur l'ensemble E de ces c^6 coloriages. Il s'agit de compter le nombre n d'orbites. Le Théorème 6.3.1 assure que n est la moyenne du nombre de points fixes ;

$$n = \frac{1}{24} \sum_{g \in \mathfrak{S}_4} \#\mathrm{Fix}(g).$$

On estime $\#\mathrm{Fix}(g)$ pour chaque type de permutation :

- si g est l'identité, alors $\mathrm{Fix}(g) = E$ et $\#\mathrm{Fix}(g) = c^6$.
- si g est une rotation d'ordre 2 d'axe joignant les milieux de deux côtés, alors $\#\,\mathrm{Fix}(g) = c^3$; il y a 6 telles rotations (elles correspondent aux transpositions).
- si g est une rotation d'angle (géométrique) $\frac{2\pi}{3}$ autour de l'une des diagonales, alors $\#\,\mathrm{Fix}(g) = c^2$; il y a 8 telles rotations (elles correspondent aux 3-cycles).
- si g est une rotation d'angle $\frac{\pi}{2}$ autour d'un axe orthogonal à 2 faces du cube, alors $\#\,\mathrm{Fix}(g) = c^3$; il y a 6 telles rotations (elles correspondent aux 4-cycles).
- g est le carré de l'une des rotations d'angle $\frac{\pi}{2}$ ci-dessus, alors $\#\,\mathrm{Fix}(g) = c^4$; il y a 3 telles rotations (elles correspondent aux doubles transpositions).

Ainsi

$$n = \frac{1}{24} \sum_{g \in \mathfrak{S}_4} \#\mathrm{Fix}(g) = \frac{1}{24}\Big(c^6 + 6c^3 + 3c^2 + 6c^3 + 3c^4\Big) = \frac{c^6 + 12c^3 + 3c^2 + 3c^4}{24}$$

□

Remarque 7.10.1. — On peut vérifier que pour $c = 2$ on trouve 10 coloriages possibles que l'on peut facilement énumérer.

7.11. Le théorème de Noether

Soit G un groupe. Considérons l'action par conjugaison de G sur l'ensemble X des sous-groupes de G :

$$\mathrm{G} \times X \to X, \qquad (g, \mathrm{G}) \mapsto g \cdot \mathrm{H} = g\mathrm{H}g^{-1}.$$

Rappelons que le stabilisateur d'un sous-groupe H sous cette action est le normalisateur $\mathrm{N_G(H)}$; rappelons aussi que

- ◇ $\mathrm{N_G(H)}$ est un sous-groupe de G
- ◇ et H est un sous-groupe distingué de $\mathrm{N_G(H)}$.

Théorème 7.11.1

Soient G un groupe. Soient H et K deux sous-groupes de G tels que $\mathrm{K} \subset \mathrm{N_G(H)}$.

1. Nous avons $\mathrm{HK} = \mathrm{KH}$ et $\mathrm{HK} = \mathrm{KH}$ est le sous-groupe de G engendré par H et K.
2. $\mathrm{H} \cap \mathrm{K}$ est un sous-groupe distingué de K et H est un sous-groupe distingué de HK.
3. Les groupes ${}^{\mathrm{HK}}\!/_{\mathrm{H}}$ et ${}^{\mathrm{K}}\!/_{(\mathrm{H} \cap \mathrm{K})}$ sont isomorphes.

Démonstration. — 1. Soient $h \in \mathrm{H}$ et $k \in \mathrm{K}$. Puisque K est contenu dans $\mathrm{N_G(H)}$ le produit $hk = k(k^{-1}hk)$ appartient à KH. De même $kh = (khk^{-1})k$ appartient à KH. Nous avons donc $\mathrm{HK} = \mathrm{KH}$.

De plus, HK est un sous-groupe de G. En effet, soient h, h' dans H et k, k' dans K. Étant donné que kh' appartient à $\mathrm{KH} = \mathrm{HK}$, il existe $h'' \in \mathrm{H}$ et $k'' \in \mathrm{K}$ tels que $kh' = h''k''$. Il en résulte que

$$(hk)(h'k') = h(kh')k' = h(h''k'')k = (hh'')(k''k') \in \mathrm{HK}.$$

Par ailleurs $(hk)^{-1} = k^{-1}h^{-1} \in \mathrm{KH} = \mathrm{HK}$. Le sous-groupe HK contient à la fois H et K ; par suite $\langle \mathrm{H} \cup \mathrm{K} \rangle \subset \mathrm{HK}$. Réciproquement $\mathrm{H} \cup \mathrm{K}$ contient tous les éléments hk de HK, c'est-à-dire $\mathrm{HK} \subset \langle \mathrm{H} \cup \mathrm{K} \rangle$. Finalement $\mathrm{HK} = \langle \mathrm{H} \cup \mathrm{K} \rangle$

2. Soient $h \in \mathrm{H} \cap \mathrm{K}$ et $k \in \mathrm{K}$. D'une part K est contenu dans $\mathrm{N_G(H)}$ donc khk^{-1} appartient à H. D'autre part K est un sous-groupe de G d'où $khk^{-1} \in \mathrm{K}$. Il s'en suit que khk^{-1} appartient à $\mathrm{H} \cap \mathrm{K}$ et $\mathrm{H} \cap \mathrm{K}$ est un sous-groupe distingué de K.

   Puisque H et K sont contenus dans $\mathrm{N_G(H)}$, le produit HK est contenu dans $\mathrm{N_G(H)}$. Il en résulte que H est un sous-groupe distingué de HK.

3. Considérons la projection canonique

$$\pi \colon \mathrm{HK} \to {}^{\mathrm{HK}}\!/_{\mathrm{H}}, \qquad x \mapsto \overline{x}.$$

Désignons par $\widetilde{\pi}$ la restriction de π à K, *i.e.* $\widetilde{\pi} = \pi_{|\mathrm{K}}$. Remarquons que $\widetilde{\pi} \colon \mathrm{K} \to {}^{\mathrm{KH}}\!/_{\mathrm{H}}$ est un morphisme de groupes. Comme tout élément de ${}^{\mathrm{KH}}\!/_{\mathrm{H}}$ est de la forme $\overline{kh} = \overline{k}$, le morphisme $\widetilde{\pi}$ est surjectif. De plus, si k est un élément de K, alors

$$k \in \ker \widetilde{\pi} \iff \overline{k} = \overline{e} \iff k \in \mathrm{H} \iff k \in \mathrm{H} \cap \mathrm{K}.$$

Par conséquent $\ker f = \mathrm{H} \cap \mathrm{K}$. Le théorème de factorisation (Corollaire 1.1.1) assure que ${}^{\mathrm{K}}\!/_{(\mathrm{H} \cap \mathrm{K})}$ et ${}^{\mathrm{HK}}\!/_{\mathrm{H}}$ sont isomorphes.

□

7.12. Simplicité du groupe spécial linéaire $\mathrm{PSL}(n,\Bbbk)$

Soient $\Bbbk$ un corps et $n \geq 2$ un entier. Le groupe linéaire spécial projectif $\mathrm{PSL}(n,\Bbbk)$ est le quotient groupe de $\mathrm{SL}(n,\Bbbk)$ par son centre : $\mathrm{PSL}(n,\Bbbk) = {}^{\mathrm{SL}(n,\Bbbk)}\!/_{Z(\mathrm{SL}(n,\Bbbk))}$. En 1831, Galois annonce que $\mathrm{PSL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$ est un groupe simple pour tous les nombres premiers $p > 3$: il exclut $p = 2$ et $p = 3$ car $\mathrm{PSL}\left(2, {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}\right) \simeq \mathfrak{S}_3$ et $\mathrm{PSL}\left(2, {}^{\mathbb{Z}}\!/_{3\mathbb{Z}}\right) \simeq \mathcal{A}_4$ ne sont pas simples. Il s'avère que $\mathrm{PSL}(n,\Bbbk)$ est un groupe simple pour tout $n \geq 2$ et tous les corps $\Bbbk$ sauf lorsque $n = 2$ et $\Bbbk = {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ et ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$ (Jordan, Moore, Dickson).

7.12.1. Actions 2-transitives et critère d'Iwasawa. — Rappelons qu'un sous-groupe maximal d'un groupe G est un sous-groupe propre de G contenu dans aucun autre sous-groupe propre de G.

Théorème 7.12.1

Si G agit 2-transitivement sur X alors le stabilisateur de chaque point de X est un sous-groupe maximal de G.

Démonstration. — Soit $x \in X$.

- Montrons que pour tout $g \notin \mathrm{St}(x)$, $\mathrm{G} = \mathrm{St}(x) \cup \mathrm{St}(x)g\mathrm{St}(x)$. Soit $g' \in \mathrm{G} \smallsetminus \mathrm{St}(x)$. Par hypothèse $gx \neq x$ et $g'x \neq x$; ainsi l'action étant 2-transitive il existe $g'' \in \mathrm{G}$ tel que $g''x = x$ et $g''(gx) = g'x$. La relation $g''x = x$ assure que $g'' \in \mathrm{St}(x)$ et $g''(gx) = g'x$ implique que $g' \in h = \underbrace{g''}_{\in \mathrm{St}(x)} g\mathrm{St}(x) \subset \mathrm{St}(x)g\mathrm{St}(x)$.
- Montrons que $\mathrm{St}(x)$ est un sous-groupe maximal de G. Le groupe $\mathrm{St}(x)$ ne coïncide pas avec G, puisque d'une part $\mathrm{St}(x)$ fixe x alors que G envoie x sur tout élément de X et $\#X \geq 2$. Soit K un sous-groupe de G contenant strictement $\mathrm{St}(x)$; soit $g \in \mathrm{K} \smallsetminus \mathrm{St}(x)$. D'après ce qui précède $\mathrm{G} = \mathrm{St}(x) \cup \mathrm{St}(x)g\mathrm{St}(x)$. Or $\mathrm{St}(x)$ et $\mathrm{St}(x)g\mathrm{St}(x)$ sont tous deux dans K d'où l'inclusion $\mathrm{G} \subset \mathrm{K}$. Ainsi $\mathrm{K} = \mathrm{G}$.

□

La réciproque du Théorème 7.12.1 est fausse. Si H est un sous-groupe maximal de G, si on considère l'action de G sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ par translation à gauche, alors H est le stabilisateur de H ; néanmoins cette action n'est pas 2-transitive si G est d'ordre impair (un groupe fini agissant 2-transitivement sur un ensemble est d'ordre pair, Corollaire **??**).

L'énoncé suivant relie des groupes de quotients simples et des actions de groupe 2-transitives.

Théorème 7.12.2: (Iwasawa)

Soit G agissant 2-transitivement sur un ensemble X. Supposons que :

1. pour certains $x \in X$ le groupe $\mathrm{St}(x)$ possède un sous-groupe distingué abélien dont les conjugués engendrent G.
2. et $[\mathrm{G}, \mathrm{G}] = \mathrm{G}$.

Désignons par K est le noyau de l'action de G sur X ; le groupe G/K est simple.

Démonstration. — Pour montrer que G/K est simple, nous allons montrer les seuls sous-groupes distingués de G contenus entre K et G sont K et G. Soit N un sous-groupe de G tel que $\mathrm{K} \subset \mathrm{N} \subset \mathrm{G}$ et $\mathrm{N} \triangleleft \mathrm{G}$. Posons $\mathrm{H} = \mathrm{St}(x)$; le Théorème 7.12.1 assure que H est un sous-groupe maximal de G. Puisque N est distingué dans G, l'ensemble $\mathrm{NH} = \{nh \mid n \in \mathrm{N}, h \in \mathrm{H}\}$ est un sous-groupe de G qui contient H. Par maximalité de H nous avons l'alternative suivante : soit $\mathrm{NH} = \mathrm{H}$ soit $\mathrm{NH} = \mathrm{G}$. D'après le Théorème 7.4.3 le groupe N agit de manière triviale ou transitive sur X.

Si $\mathrm{NH} = \mathrm{H}$ alors $\mathrm{N} \subset \mathrm{H}$ et N fixe x. En particulier N n'agit pas de manière transitive sur X donc agit trivialement sur X, ce qui implique l'inclusion $\mathrm{N} \subset \mathrm{K}$. Puisque par hypothèse $\mathrm{K} \subset \mathrm{N}$, nous obtenons : $\mathrm{N} = \mathrm{K}$.

Supposons maintenant $\mathrm{NH} = \mathrm{G}$. Soit U un sous-groupe abélien et distingué de H dont les conjugués engendrent G. Puisque $\mathrm{U} \triangleleft \mathrm{H}$, nous avons $\mathrm{NU} \triangleleft \mathrm{NH} = \mathrm{G}$. Ainsi, pour $g \in \mathrm{G}$, $g\mathrm{U}g^{-1} \subset g(\mathrm{NU})g^{-1} = \mathrm{NU}$. Autrement dit NU contient tous les sous-groupes conjugués de U. Il en résulte que $\mathrm{NU} = \mathrm{G}$.

Par conséquent $\mathrm{G}/\mathrm{N} = \mathrm{NU}/\mathrm{N} \simeq \mathrm{U}/\mathrm{N} \cap \mathrm{U}$. Puisque U est abélien, l'isomorphisme nous dit que G/N est abélien, donc $[\mathrm{G}, \mathrm{G}] \subset \mathrm{N}$. Puisque $\mathrm{G} = [\mathrm{G}, \mathrm{G}]$ par hypothèse, on a $\mathrm{N} = \mathrm{G}$. □

Exemple 7.12.1. — Nous pouvons utiliser le Théorème 7.12.2 pour montrer que $\mathcal{A}_5$ est un groupe simple. Son action naturelle sur $\{1, 2, 3, 4, 5\}$ est 2-transitive. Remarquons que

$$\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

est un sous-groupe abélien distingué de $\mathrm{St}(5) \simeq \mathcal{A}_4$. Les conjugués de ce sous-groupe par $\mathcal{A}_5$ engendrent $\mathcal{A}_5$ puisque les double transpositions de $\mathcal{A}_5$ sont tous conjugués dans $\mathcal{A}_5$ et engendrent $\mathcal{A}_5$ (Corollaire 7.4.1). Le groupe dérivé $[\mathcal{A}_5, \mathcal{A}_5]$ contient toutes les double transpositions : si a, b, c, d sont distincts alors

$$(a\ b)(c\ d) = (a\ b\ c)(a\ b\ d)(a\ b\ c)^{-1}(a\ b\ d)^{-1}.$$

Il en résulte que $[\mathcal{A}_5, \mathcal{A}_5] = \mathcal{A}_5$ et donc que $\mathcal{A}_5$ est simple.

Soit $\Bbbk$ un corps. Le groupe $\mathrm{SL}(2, \Bbbk)$ agit sur $\Bbbk^2 \smallsetminus \left\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right\}$, mais cette action n'est pas 2-transitive puisque les vecteurs linéairement dépendants ne peuvent pas être envoyés sur des

vecteurs linéairement indépendants par une matrice. Les vecteurs linéairement dépendants dans $\Bbbk^2$ se trouvent le long de la même droite passant par l'origine. Considérons donc l'action de $\mathrm{SL}(2, \Bbbk)$ sur l'ensemble des droites vectorielles de $\Bbbk^2$: la matrice $A \in \mathrm{SL}(2, \Bbbk)$ envoie la droite $L = Fv$ sur la droite $A(L) = F(Av)$. (De manière équivalente $\mathrm{SL}(2, \Bbbk)$ agit sur $\mathbb{P}^1(\Bbbk)$).

Théorème 7.12.3

L'action de $\mathrm{SL}(2, \Bbbk)$ sur l'ensemble des droites vectorielles de $\Bbbk^2$ est 2-transitive.

Démonstration. — Considérons les deux droites vectorielles distinctes $\Bbbk \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\Bbbk \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ de $\Bbbk^2$. Il suffit de montrer qu'étant donnés deux droites vectorielles distinctes $\Bbbk v$ et $\Bbbk w$ de $\Bbbk^2$, il existe $A \in \mathrm{SL}(2, \Bbbk)$ qui envoie $\Bbbk \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ sur $\Bbbk v$ et $\Bbbk \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ sur $\Bbbk w$.

Écrivons v sous la forme $v = \begin{pmatrix} a \\ c \end{pmatrix}$ et w sous la forme $w = \begin{pmatrix} b \\ d \end{pmatrix}$. Puisque $\Bbbk v \neq \Bbbk w$, les vecteurs v et w sont linéairement indépendants et $\Delta = ad - bc$ est différent de zéro. Posons $A = \begin{pmatrix} a & \frac{b}{\Delta} \\ c & \frac{d}{\Delta} \end{pmatrix}$. Notons que $\det A = a\frac{d}{\Delta} - \frac{b}{\Delta}c = \frac{\Delta}{\Delta} = 1$; autrement dit la matrice A appartient à $\mathrm{SL}(2, \Bbbk)$. Puisque

$$A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} = v \qquad \text{et} \qquad A \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{b}{\Delta} \\ \frac{d}{\Delta} \end{pmatrix} = \left(\frac{1}{\Delta}\right) w$$

la matrice A envoie $\Bbbk \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ sur $\Bbbk v$ et $\Bbbk \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ sur $\Bbbk \left(\frac{1}{\Delta}\right) w = \Bbbk w$. □

Nous appliquerons le critère d'Iwasawa (Théorème 7.12.2) dans le contexte suivant : l'action de $\mathrm{SL}(2, \Bbbk)$ l'ensemble des droites vectorielles de $\Bbbk^2$. Le Théorème 7.12.3 assure que cette action est 2-transitive. Reste à vérifier

- ◇ le noyau K de cette action est le centre de $\mathrm{SL}(2, \Bbbk)$, donc $\mathrm{SL}(2, \Bbbk)/\mathrm{K} = \mathrm{PSL}(2, \Bbbk)$,
- ◇ le stabilisateur de $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ contient un sous-groupe abélien distingué dont les sous-groupes conjugés engendrent $\mathrm{SL}(2, \Bbbk)$,
- ◇ $[\mathrm{SL}(2, \Bbbk), \mathrm{SL}(2, \Bbbk)] = \mathrm{SL}(2, \Bbbk)$.

Nous aurons besoin de l'hypothèse $\#\Bbbk > 3$ uniquement pour démontrer le dernier point (les groupes $\mathrm{PSL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ et $\mathrm{PSL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ ne sont pas simples.)

Théorème 7.12.4

Le noyau de l'action du groupe $\mathrm{SL}(2,\Bbbk)$ sur l'ensemble des droites vectorielles de $\Bbbk^2$ est $Z(\mathrm{SL}(2,\Bbbk))$.

Démonstration. — Une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\Bbbk)$ est dans le noyau K de l'action lorsqu'elle fixe chaque droite vectorielle de $\Bbbk^2$. Si la matrice A fixe les droites $\Bbbk \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\Bbbk \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ alors $c = b = 0$, *i.e.* $A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. La condition $\det A = 1$ se traduit alors par $d = \frac{1}{a}$; autrement dit $A = \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$. En écrivant que A fixe $\Bbbk \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, nous obtenons que $a = \frac{1}{a}$ c'est-à-dire que $a = \pm 1$ et $A = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \pm\mathrm{id}$. Or id et $-\mathrm{id}$ agissent agissent tous deux de manière triviale sur les droites vectorielles de $\Bbbk^2$. Il en résulte que $\mathrm{K} = \langle -\mathrm{id} \rangle$.

Si une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartient à $Z(\mathrm{SL}(2,\Bbbk))$, alors en particulier elle commute avec $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ ce qui implique $a = d$ et $b = c = 0$. Par conséquent $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. Mais $\det A = 1$ donc $a^2 = 1$ et $A = \pm\mathrm{id}$. Réciproquement id et $-\mathrm{id}$ appartiennent à $Z(\mathrm{SL}(2,\Bbbk)$. $\square$

Considérons $x = \Bbbk \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Son stabilisateur dans $\mathrm{SL}(2,\Bbbk)$ est

$$\begin{aligned}
\mathrm{St}\left(\Bbbk \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) &= \left\{ A \in \mathrm{SL}(2,\Bbbk) \,\middle|\, A \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \Bbbk \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\} \\
&= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{SL}(2,\Bbbk) \right\} \\
&= \left\{ \begin{pmatrix} a & b \\ 0 & \frac{1}{a} \end{pmatrix} \,\middle|\, a \in \Bbbk^\times,\, b \in \Bbbk \right\}.
\end{aligned}$$

Ce sous-groupe contient le sous-groupe abélien distingué U donné par

$$\mathrm{U} = \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \middle| \lambda \in \Bbbk \right\}.$$

Théorème 7.12.5

Le sous-groupe U et ses conjugués engendrent $\mathrm{SL}(2, \Bbbk)$. Plus précisément, une matrice de la forme $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$ est conjuguée à une matrice de la forme $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. De plus, tout élément de $\mathrm{SL}(2, \Bbbk)$ est le produit d'au plus quatre éléments de la forme $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$ ou $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

Démonstration. — La matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ appartient à $\mathrm{SL}(2, \Bbbk)$ et

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix},$$

i.e. $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ conjugue le groupe $\mathrm{U} = \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \middle| \lambda \in \Bbbk \right\}$ au groupe des matrices triangulaires inférieures $\left\{ \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \middle| \lambda \in \Bbbk \right\}$.

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathrm{SL}(2, \Bbbk)$. Montrons que A est un produit de matrices de type $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ ou $\begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix}$. Si $b \neq 0$, alors

$$A = \begin{pmatrix} 1 & 0 \\ \frac{d-1}{b} & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \frac{a-1}{b} & 1 \end{pmatrix}.$$

Si $c \neq 0$, alors

$$A = \begin{pmatrix} 1 & \frac{a-1}{c} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{d-1}{c} \\ 0 & 1 \end{pmatrix}.$$

Si $b = 0$ et $c = 0$, alors $A = \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$ et

$$A = \begin{pmatrix} 1 & 0 \\ \frac{1-a}{a} & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\frac{1}{a} \\ 0 & 1 \end{pmatrix}.$$

□

Jusqu'à présent, $\Bbbk$ était un corps général. Nous arrivons maintenant à un résultat qui nécessite $\#\Bbbk \geq 4$.

Théorème 7.12.6

Si $\#\Bbbk \geq 4$, alors le groupe $\mathrm{SL}(2, \Bbbk)$ est parfait : $[\mathrm{SL}(2, \Bbbk), \mathrm{SL}(2, \Bbbk)] = \mathrm{SL}(2, \Bbbk)$.

Démonstration. — Soient $a \in \Bbbk^\times$ et $b \in \Bbbk$. Nous avons

$$\begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}^{-1} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & b(a^2-1) \\ 0 & 1 \end{pmatrix}.$$

Puisque $\#\Bbbk \geq 4$, le corps $\Bbbk$ contient un élément a distinct de 0, 1 et -1 ; en particulier $a^2 \neq 1$. En utilisant cette valeur de a et en laissant b parcourir $\Bbbk$ nous constatons que $[\mathrm{SL}(2, \Bbbk), \mathrm{SL}(2, \Bbbk)]$ contient U. Le groupe dérivé de $\mathrm{SL}(2, \Bbbk)$ étant distingué dans $\mathrm{SL}(2, \Bbbk)$, il contient tous les sous-groupes conjugués à U. Le Théorème 7.12.5 assure alors que $[\mathrm{SL}(2, \Bbbk), \mathrm{SL}(2, \Bbbk)] = \mathrm{SL}(2, \Bbbk)$. □

Remarque 7.12.1. — Le Théorème 7.12.6 est faux lorsque $\#\Bbbk = 2$ ou 3 ; justifions pourquoi lorsque $\#\Bbbk = 2$ (la justification dans le cas $\#\Bbbk = 3$ nécessite la notion de groupe de Sylow). Nous avons $\mathrm{SL}\left(2, \mathbb{Z}/2\mathbb{Z}\right) = \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est isomorphe à $\mathfrak{S}_3$ et $[\mathfrak{S}_3, \mathfrak{S}_3] = \mathcal{A}_3$.

Les Théorèmes 7.12.2, 7.12.3, 7.12.4, 7.12.5 et 7.12.6 assurent que :

Théorème 7.12.7

Si $\#\Bbbk \geq 4$ alors le groupe $\mathrm{PSL}(2, \Bbbk)$ est simple.

7.12.2. Simplicité de $\mathrm{PSL}(n, \Bbbk)$ pour $n > 2$. — Pour démontrer que $\mathrm{PSL}(n, \Bbbk)$ est simple pour tout $\Bbbk$ lorsque $n > 2$, nous allons étudier l'action de $\mathrm{SL}(n, \Bbbk)$ sur l'ensemble des droites vectorielles de $\Bbbk^n$, *i.e.* sur l'espace projectif $\mathbb{P}^{n-1}(\Bbbk)$.

Théorème 7.12.8

L'action de $\mathrm{SL}(n, \Bbbk)$ sur $\mathbb{P}^{n-1}(\Bbbk)$ est 2-transitive. Son noyau coïncide avec le centre de $\mathrm{SL}(n, \Bbbk)$; de plus, il existe un point dont le stabilisateur possède un sous-groupe distingué abélien.

CHAPITRE 8

GROUPES LIBRES ; GROUPES DÉFINIS PAR GÉNÉRATEURS ET RELATIONS

8.1. Groupes libres

Soit E un ensemble. Le but de ce paragraphe est de construire le « groupe libre sur l'ensemble E ». Informellement c'est le groupe le plus général que nous pouvons fabriquer à partir de E. Il est obtenu en décrétant que nous savons multiplier et inverser les éléments de E et en n'imposant à ces opérations aucune autre règle que celles données par la théorie générale des groupes.

Procédons à la construction détaillée de ce groupe.

Définition 8.1.1

Un *monoïde* est un ensemble M

- ◇ qui est muni d'une loi de composition interne associative
- ◇ qui possède un élément neutre (nécessairement unique).

Définition 8.1.2

Soit M, respectivement N, un monoïde de neutre e_M, respectivement e_N. Un *morphisme de monoïdes* de M dans N est une application f de M vers N telle que

- ◇ $f(e_M) = e_N$;
- ◇ $f(ab) = f(a)f(b)$ pour tous a et b dans M.

Exemple 8.1.1. — L'ensemble $\mathbb{N}$ muni de l'addition est un monoïde. Ce n'est pas un groupe : 1 n'a pas d'inverse.

Exemple 8.1.2. — Un groupe est un monoïde.

Plus précisément un groupe est un monoïde dans lequel tout élément a un inverse.

Exemple 8.1.3. — Si A est un anneau, alors $(A, \times)$ est un monoïde (remarquons que si $A \neq \{0\}$, alors ce n'est pas un groupe car 0 n'a alors pas d'inverse).

Remarque 8.1.1. — L'application nulle de A dans A commute au produit mais n'est pas un morphisme de monoïdes si $A \neq \{0\}$ car elle n'envoie pas 1 sur 1. Ainsi contrairement à ce qui se passe pour les groupes il est indispensable d'imposer dans la définition de morphisme de monoïdes que l'élément neutre soit envoyé sur l'élément neutre.

Définitions 8.1.1

Soit E un ensemble.
Un *mot* sur l'alphabet E est une suite finie $x_1x_2\dots x_n$ d'éléments de E. L'entier n est appelée la *longueur* du mot en question.
Il existe un et seul mot de longueur nulle sur l'alphabet E : c'est la suite vide appelée également *mot vide* et notée $\emptyset$.

Soit $\Lambda(E)$ l'ensemble des mots sur l'alphabet E. La concaténation définit une loi de composition interne sur $\Lambda(E)$; elle est associative et possède un élément neutre : le mot vide. Elle fait donc de $\Lambda(E)$ un monoïde, appelé le *monoïde libre* sur l'ensemble E.

Dans la suite nous identifions E à un sous-ensemble de $\Lambda(E)$ en voyant un élément de E comme un mot de longueur 1.

Énonçons la propriété universelle du monoïde libre :

Lemme 8.1.1

Soit E un ensemble. Soit M un monoïde. Soit $f\colon E \to M$ une application ensembliste. Il existe un unique morphisme de monoïdes de $\Lambda(E)$ dans M qui prolonge f.

Démonstration. — Un tel morphisme est nécessairement donné par la formule

$$x_1x_2\dots x_n \mapsto f(x_1)f(x_2)\dots f(x_n).$$

Réciproquement la formule ci-dessus définit un morphisme de monoïdes de $\Lambda(E)$ dans M qui prolonge f. □

Soit E un ensemble. Introduisons un ensemble E^{-1} disjoint de E et muni d'une bijection [1]

$$E \to E^{-1} \qquad\qquad x \mapsto x^{-1}.$$

Si G est un groupe, on note $h(\mathrm{G})$ l'ensemble des morphismes de monoïdes $f\colon \Lambda(E \sqcup E^{-1}) \to \mathrm{G}$ tels que $f(x^{-1}) = f(x)^{-1}$ pour tout $x \in E$. Soit $\mathcal{R}$ la relation sur $\Lambda(E \sqcup E^{-1})$ définie par : $m\mathcal{R}n$ si et seulement si pour tout groupe G et tout $f \in h(\mathrm{G})$ on a $f(m) = f(n)$. La relation $\mathcal{R}$ est une relation d'équivalence. Notons $F(E)$ le quotient $\Lambda(E \sqcup E^{-1})/\mathcal{R}$.

1. Attention E^{-1} et x^{-1} sont de simples notations.

Soient m, n, m', n' des éléments de M tels que $m\mathcal{R}n$ et $m'\mathcal{R}n'$. Soit G un groupe et soit f un élément de $h(\mathrm{G})$. Nous avons $f(m) = f(n)$ et $f(m') = f(n')$. Par suite

$$f(mm') = f(m)f(m') = f(n)f(n') = f(nn')$$

autrement dit $(mm')\mathcal{R}(nn')$. Il s'ensuit que la loi interne de $\Lambda(E \sqcup E^{-1})$ passe au quotient par $\mathcal{R}$ et induit une loi interne sur $F(E)$. On peut vérifier que celle-ci fait de $F(E)$ un monoïde et que l'application quotient $\Lambda(E \sqcup E^{-1}) \to F(E)$ est un morphisme de monoïdes.

Lemme 8.1.2

Le monoïde $F(E)$ ainsi construit est un groupe.

Démonstration. — Vérifions que chacun des éléments de $F(E)$ est inversible.

Tout élément de $F(E)$ est de la forme $\overline{x_1 x_2 \dots x_k} = \overline{x_1}\,\overline{x_2} \dots \overline{x_k}$ où les x_i appartiennent à $E \sqcup E^{-1}$. Il suffit donc de vérifier que $\overline{x}$ est inversible pour tout x dans $E \sqcup E^{-1}$. Soit E dans E, soit G un groupe et soit f un élément de $h(\mathrm{G})$. Nous avons $f(x^{-1}) = f(x)^{-1}$ donc $f(xx^{-1}) = f(x^{-1}x) = e = f(\emptyset)$. Donc $\overline{xx^{-1}} = \overline{x^{-1}x} = \overline{\emptyset}$ et $\overline{x}$ est inversible d'inverse $\overline{x^{-1}}$. □

Lemme 8.1.3: (Propriété universelle du groupe $F(E)$)

Soit E un ensemble. Soit G un groupe. Soit $f\colon E \to \mathrm{G}$ une application. Il existe un unique morphisme de groupes

$$\varphi\colon F(E) \to \mathrm{G}$$

qui envoie $\overline{x}$ sur $f(x)$ pour tout x dans E.

Démonstration. — Commençons par établir l'unicité du morphisme.

Soit φ un morphisme satisfaisant les propriétés de l'énoncé. Comme d'après ce qui précède $\overline{x}^{-1} = \overline{x^{-1}}$ pour tout x dans E et comme tout élément de $F(E)$ s'écrit $\overline{x_1 x_2 \dots x_k} = \overline{x_1}\,\overline{x_2} \dots \overline{x_k}$ avec $x_i \in E \sqcup E^{-1}$ le groupe $F(E)$ est engendré par l'ensemble des $\overline{x}$ pour $x \in E$. Il en résulte que φ est entièrement déterminé par sa restriction à cet ensemble laquelle est imposée par hypothèse ($\varphi(\overline{x}) = f(x)$ pour tout $x \in E$). Ainsi φ est unique.

Montrons maintenant l'existence de φ. Soit g l'application de $E \sqcup E^{-1}$ dans G qui envoie x sur $f(x)$ et x^{-1} sur $f(x)^{-1}$ pour tout $x \in X$. Le Lemme 8.1.1 assure que g se prolonge en un morphisme de monoïdes $\Phi\colon \Lambda(E) \to \mathrm{G}$ qui par construction appartient à $h(\mathrm{G})$. Par conséquent $\Phi(m) = \Phi(n)$ dès que $m\mathcal{R}n$ et Φ induit ainsi par passage au quotient une application $\varphi\colon F(X) \to \mathrm{G}$ qui envoie par construction $\overline{x}$ sur $f(x)$ pour tout $x \in X$. On peut vérifier qu'il s'agit d'un morphisme de groupes. □

Le groupe $F(E)$ est donc défini comme le quotient de $\Lambda(E \sqcup E^{-1})$ par une relation d'équivalence a priori peu explicite ; en effet elle est donnée par des conditions portant sur tous les

morphismes de monoïdes de source $\Lambda(E)$ dont le but est un groupe. Il est néanmoins possible de décrire $F(E)$ de manière tangible.

Définition 8.1.3

Soit E un ensemble. Un mot $m \in \Lambda(E \sqcup E^{-1})$ est dit *réduit* s'il ne contient aucune suite de deux termes consécutifs de la forme ee^{-1} ou $e^{-1}e$ avec $e \in E$.

Théorème 8.1.1

Soit E un ensemble. Soit $\mathcal{R}$ la relation sur $\Lambda(E \sqcup E^{-1})$ définie par : $m\mathcal{R}n$ si et seulement si pour tout groupe G et tout $f \in h(\mathrm{G})$ on a $f(m) = f(n)$.
Toute classe de $\mathcal{R}$ contient un unique mot réduit.

Remarque 8.1.2. — Cet énoncé signifie que le passage au quotient par $\mathcal{R}$ permet d'identifier $F(E)$ à l'ensemble des mots réduits sur l'alphabet $E \sqcup E^{-1}$ (en particulier on peut voir $E \sqcup E^{-1}$ comme un sous-ensemble de $F(E)$). Pour faire le produit de deux éléments de $F(E)$ on les concatène puis on simplifie le mot obtenu en éliminant tous les termes de la forme xx^{-1} ou $x^{-1}x$ et on recommence jusqu'à obtention d'un mot réduit.

Notations : $\underbrace{xx\dots x}_{n \text{ fois}} = x^n$ et $\underbrace{x^{-1}x^{-1}\dots x^{-1}}_{n \text{ fois}} = x^{-n}$.

Exemple 8.1.4. — Supposons que $E = \{\alpha, \beta, \gamma, \delta\}$. Considérons les deux mots réduits

$$m = \alpha^2\beta^{-1}\gamma^3\delta\alpha\delta\alpha \qquad\qquad n = \alpha^{-1}\delta^{-1}\alpha^{-1}\delta^{-1}\beta^2\gamma\alpha^4.$$

La concaténation des deux mots m et n est égale à

$$\alpha^2\beta^{-1}\gamma^3\beta^2\gamma\alpha^4$$

après élimination de $\alpha\alpha^{-1}$, puis $\delta\delta^{-1}$, puis $\alpha\alpha^{-1}$ puis $\delta\delta^{-1}$ nous obtenons le mot réduit $\alpha^2\beta^{-1}\gamma^3\beta^2\gamma\alpha^4$.

Démonstration du Théorème 8.1.1. — Commençons par démontrer l'existence. Soit m un élément de $\Lambda(E)$. Montrons par récurrence sur la longueur de m l'existence d'un mot réduit équivalent à m. Si la longueur de m est nulle, m est le mot vide et est déjà réduit. Supposons que la longueur de m est strictement positive et que l'énoncé est vrai pour les mots de longueur strictement inférieure. Si m est réduit, alors il n'y a rien à faire. Sinon m est de la forme $m'xx^{-1}m''$ ou de la forme $m'x^{-1}xm''$. Par hypothèse de récurrence $m'm''$ (dont la longueur est strictement inférieure à la longueur de m) est équivalent à un mot réduit. Il suffit maintenant de montrer que m est équivalent à $m'm''$. Supposons par exemple que $m = m'xx^{-1}m''$. Nous avons

$$\overline{m} = \overline{m'} \cdot \overline{x} \cdot \overline{x^{-1}} \cdot \overline{m''} = \overline{m'} \cdot \overline{m''} = \overline{m'm''}$$

puisque $\overline{x}$ et $\overline{x^{-1}}$ sont inverses l'un de l'autre. Par suite $m\mathcal{R}(m'm'')$. La démonstration dans le cas où $m = m'x^{-1}xm''$.

Montrons maintenant l'unicité, autrement dit montrons que deux mots réduits équivalents coïncident. Soit X l'ensemble des mots réduits. Pour tout x dans E, désignons par σ_x l'application de X dans X qui envoie un mot réduit m sur

- ⋄ xm si m n'est pas de la forme $x^{-1}m'$,
- ⋄ m' si m est de la forme $x^{-1}m'$.

Notons que les mots obtenus sont bien réduits. L'application σ_x est bien une bijection : sa réciproque envoie un mot réduit m sur

- ⋄ $x^{-1}m$ si m n'est pas de la forme xm',
- ⋄ m' si m est de la forme xm'.

Cette application ensembliste de E dans $\mathfrak{S}_X$ induit en vertu de la propriété universelle de $F(E)$ un morphisme de groupes de $F(E)$ vers $\mathfrak{S}_X$, c'est-à-dire une action de $F(E)$ sur X

$$F(E) \times X \to X, \qquad (x, m) \mapsto x \cdot m$$

Soit m un mot réduit. Montrons par récurrence sur la longueur de m que $\overline{m} \cdot \emptyset = m$. Si m est de longueur nulle, alors c'est le mot vide et $\overline{m}$ est donc l'élément neutre de $F(E)$ qui agit trivialement sur X ; l'assertion suit. Supposons que m soit de longueur strictement positive et que la propriété soit vraie pour tous les mots de longueur strictement inférieure à celle de m. Écrivons $m = xm'$ avec $x \in E \sqcup E^{-1}$. Puisque m est réduit, m' l'est aussi. Nous avons l'égalité $\overline{m} \cdot \emptyset = \overline{x} \cdot (\overline{m'} \cdot \emptyset)$. Par hypothèse de récurrence $\overline{m'} \cdot \emptyset = m'$. Si x appartient à E, alors m étant réduit m' n'est pas de la forme $x^{-1}m''$ et par conséquent

$$\overline{x} \cdot m' = \sigma_x(m') = xm' = m.$$

Si $x = y^{-1}$ pour un certain $y \in X$ alors m étant réduit m' n'est pas de la forme ym'' et par suite

$$\overline{x} \cdot m' = \sigma_y^{-1}(m') = y^{-1}m' = m.$$

Ainsi si m et n sont deux mots réduits tels que $m\mathcal{R}n$, alors $\overline{m} = \overline{n}$ et $m = \overline{m} \cdot \emptyset = \overline{n} \cdot \emptyset = n$. □

Remarque 8.1.3. — Ce n'est pas pour compliquer les choses que nous avons construit $F(E)$ comme quotient du monoïde libre $\Lambda(E \sqcup E^{-1})$ par une relation d'équivalence au lieu de le définir comme l'ensemble des mots réduits sur l'alphabet, avec la loi de concaténation-simplification comme loi interne ; cela peut être vu en essayant de démontrer directement l'associativité de cette loi...

Remarque 8.1.4. — Par abus dans la suite nous considèrerons tout mot sur l'alphabet $E \sqcup E^{-1}$ comme un élément de $F(E)$ même s'il n'est pas réduit en l'identifiant à son image par l'application quotient. En d'autres termes nous omettrons désormais la barre de réduction modulo $\mathcal{R}$.

Soit E un ensemble. Soit G un groupe. Soit $(g_x)_{x\in E}$ une famille d'éléments de G. Soit $\varphi\colon F(E) \to \mathrm{G}$ l'unique morphisme de groupes tel que $\varphi(x) = g_x$ pour tout $x \in E$. Soit m un mot sur l'alphabet $E \sqcup E^{-1}$. Nous noterons souvent $m(g_x)_x$ l'élément $\varphi(m) \in \mathrm{G}$ (ici m est vu comme appartenant à $F(E)$). Si $m = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n}$ avec $\varepsilon_i \in \{-1, 1\}$ pour tout i, alors

$$m(g_x) = g_{x_1}^{\varepsilon_1} g_{x_2}^{\varepsilon_2} \dots g_{x_n}^{\varepsilon_n}.$$

Le morphisme φ est appelé *morphisme d'évaluation en la famille* $(g_x)_{x\in E}$.

Exemple 8.1.5. — L'unique mot sur un alphabet vide est le mot vide, par suite le groupe $F(\emptyset)$ est trivial.

Exemple 8.1.6. — Soit E un singleton $\{a\}$. Un mot réduit sur $E \sqcup E^{-1}$ est de la forme a^n pour $n \in \mathbb{Z}$. Ainsi $n \mapsto a^n$ réalise un isomorphisme entre $\mathbb{Z}$ et $F(\{a\})$. Autrement dit le groupe libre sur un singleton s'identifie à $\mathbb{Z}$.

8.2. Ubiquité des groupes libres dans les groupes linéaires

Rappelons l'énoncé suivant appelé Lemme du ping-pong [2] :

Lemme 8.2.1

Soit G un groupe agissant sur un ensemble E.
Soient Γ_1 et Γ_2 deux sous-groupes de G. Désignons par Γ le sous-groupe de G engendré par Γ_1 et Γ_2. Supposons que Γ_1 soit d'ordre ≥ 3 et que Γ_2 soit d'ordre ≥ 2.
Supposons qu'il existe deux ensembles non-vides X_1 et X_2 de E tels que

$$\begin{cases} X_2 \not\subset X_1 \\ \gamma(X_2) \subset X_1 \quad \forall\, \gamma \in \Gamma_1 \smallsetminus \{e\} \\ \gamma(X_1) \subset X_2 \quad \forall\, \gamma \in \Gamma_2 \smallsetminus \{e\} \end{cases}$$

Alors Γ est isomorphe au produit libre $\Gamma_1 * \Gamma_2$.

Démonstration. — Soit w un mot réduit non vide écrit à l'aide de lettres de $(\Gamma_1 \smallsetminus \{e\}) \sqcup (\Gamma_2 \smallsetminus \{e\})$. Montrons que l'élément de Γ défini par w (encore noté w) n'est pas trivial.

2. L'argument du ping-pong remonte à la fin du XIXème siècle et est généralement attribué à Felix Klein, qui l'utilisa pour étudier les groupes Kleiniens, c'est-à-dire les sous-groupes discrets de $\mathrm{PSL}(2, \mathbb{C})$

- ◇ Si w est de la forme $a_1b_1a_2b_2\dots a_k$ avec a_1, a_2, …, a_k dans $\Gamma_1 \smallsetminus \{e\}$ et b_1, b_2, …, b_k dans $\Gamma_2 \smallsetminus \{e\}$, alors
$$\begin{aligned} w(X_2) &= a_1b_1a_2b_2\dots a_k(X_2) \subset a_1b_1a_2b_2\dots a_{k-1}b_{k-1}(X_1) \\ &\subset a_1b_1a_2b_2\dots a_{k-1}(X_2) \\ &\subset \dots \\ &\subset a_1(X_2) \\ &\subset X_1. \end{aligned}$$
Puisque $X_2 \not\subset X_1$ le mot w n'est pas trivial.
- ◇ Supposons que w soit du type $b_1a_2b_2\dots a_kb_k$ avec a_2, a_3, …, a_k dans $\Gamma_1 \smallsetminus \{e\}$ et b_1, b_2, …, b_k dans $\Gamma_2 \smallsetminus \{e\}$; considérons un élément a dans $\Gamma_1 \smallsetminus \{e\}$. L'argument précédent assure que awa^{-1} n'est pas trivial donc que w n'est pas trivial.
- ◇ Si w est de la forme $a_1b_1a_2b_2\dots a_kb_k$ avec a_1, a_2, …, a_k dans $\Gamma_1 \smallsetminus \{e\}$ et b_1, b_2, …, b_k dans $\Gamma_2 \smallsetminus \{e\}$, alors un argument analogue à celui donné plus haut implique que awa^{-1}, pour $a \in \Gamma_1 \smallsetminus \{1, a_1^{-1}\}$, n'est pas trivial et donc que w n'est pas trivial.
- ◇ Supposons que w soit du type $b_1a_2b_2\dots a_k$ avec a_2, …, a_k dans $\Gamma_1 \smallsetminus \{e\}$ et b_1, b_2, …, b_k dans $\Gamma_2 \smallsetminus \{e\}$. Un argument analogue à celui donné plus haut implique que awa^{-1}, pour $a \in \Gamma_1 \smallsetminus \{1, a_k\}$, n'est pas trivial et donc que w n'est pas trivial.

□

Corollaire 8.2.1

Le groupe $\mathrm{GL}(2,\mathbb{R})$ contient deux groupes libres à deux générateurs. En fait, il contient des groupes libres à k générateurs pour tout k.

Corollaire 8.2.2

Soit $n \geq 2$ un entier. Le groupe $\mathrm{GL}(n,\mathbb{R})$ possède des groupes libres à k générateurs pour tout k.

Soit $\mathrm{SL}(2,\mathbb{Z})$ le groupe des matrices 2×2 à coefficients dans $\mathbb{Z}$ et de déterminant 1. Le centre de $\mathrm{SL}(2,\mathbb{Z})$ est le groupe d'ordre 2 engendré par $-\mathrm{id}$:
$$Z(\mathrm{SL}(2,\mathbb{Z})) = \langle -\mathrm{id}\rangle.$$
On appelle *groupe modulaire* le groupe quotient
$$\mathrm{PSL}(2,\mathbb{Z}) = {}^{\mathrm{SL}(2,\mathbb{Z})}\!/_{\langle -\mathrm{id}\rangle}$$
il peut être identifié au groupe
$$\left\{\mathbb{C} \to \mathbb{C},\ z \mapsto \frac{az+b}{cz+d} \,\middle|\, a,\ b,\ c,\ d \in \mathbb{Z},\ ad-bc=1\right\}.$$

Corollaire 8.2.3

Le groupe $\mathrm{PSL}(2,\mathbb{Z})$ est isomorphe au produit libre $\mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$.

Démonstration. — Considérons l'action de $\mathrm{PSL}(2,\mathbb{Z})$ sur $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ par homographies

$$\mathrm{PSL}(2,\mathbb{Z}) \times \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q}), \qquad \left(g = \overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}, z\right) \mapsto g \cdot z = \frac{az+b}{cz+d}.$$

Posons

$$a = \overline{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}, \qquad b = \overline{\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}}, \qquad c = ba = \overline{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}$$

◇ Montrons que $\mathrm{PSL}(2,\mathbb{Z})$ est engendré par a et b.

Notons G le sous-groupe de $\mathrm{PSL}(2,\mathbb{Z})$ engendré par $\{a, b\}$, et supposons par l'absurde qu'il existe $g \in \mathrm{PSL}(2,\mathbb{Z}) \smallsetminus \mathrm{G}$. Supposons de plus que $g \in \mathrm{PSL}(2,\mathbb{Z}) \smallsetminus \mathrm{G}$ soit tel que $g \cdot 0 = \frac{p}{q} \in \mathbb{P}^1(\mathbb{Q})$ soit tel que $|q|$ soit minimal et non nul. Notons qu'on peut supposer $g \cdot 0 \neq \infty$ grâce à l'action de a. Nous allons montrer que $g \cdot 0 = 0$. Supposons donc que $p \neq 0$. Si $|q| > |p|$, alors $ag \cdot 0 = \frac{-q}{p}$ a un dénominateur de valeur absolue inférieure, ce qui contredit la minimalité de $|q|$. On a donc $|q| \leq |p|$.

Comme $p \neq 0$, considérons $n \in \mathbb{Z}$ tel que $|p + nq| < |q|$. Alors $ac^n g \cdot 0 = \frac{-q}{p+nq}$, ce qui contredit la minimalité de $|q|$. Ainsi $p = 0$, d'où $g \cdot 0 = 0$. Ainsi g a pour coefficients $g = \overline{\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}}$, avec $x \in \mathbb{Z}$. Or $aga = c^{-x}$, donc g appartient à G. Ceci prouve que $\mathrm{PSL}(2,\mathbb{Z}) = \mathrm{G}$ est engendré par $\{a, b\}$.

◇ Montrons que $\mathrm{PSL}(2,\mathbb{Z})$ est le produit livre des sous-groupes A et B engendrés par a et b. Notons que $a^2 = b^3 = 1$; par suite $\mathrm{A} \simeq \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{B} \simeq \mathbb{Z}/3\mathbb{Z}$.

Considérons l'ensemble $X = \mathbb{P}^1(\mathbb{Q})$, et les sous-ensembles disjoints $X_{\mathrm{A}} = \mathbb{Q} \cap]-\infty, 0[$ et $X_{\mathrm{B}} = \mathbb{Q} \cap]0, +\infty[$. Alors, pour tout $z \in X_{\mathrm{B}}$, nous avons $z > 0$ donc $a \cdot z = -\frac{1}{z} \in X_{\mathrm{A}}$. Et si z appartient à X_{A}, alors $z < 0$ donc $b \cdot z = 1 - \frac{1}{z} > 1$ donc $b \cdot z$ appartient à X_{A}. Enfin si z appartient à X_{A}, alors $z < 0$ donc $b^2 \cdot z = -\frac{1}{z-1} > 0$ donc $b^2 \cdot z$ appartient à X_{B}. Le lemme du ping-pong (Lemme 8.2.1 assure que $\mathrm{PSL}(2,\mathbb{Z}) \simeq \mathrm{A} * \mathrm{B}$.

□

8.3. Groupes définis par générateurs et relations

Soit E un ensemble. Soit R un ensemble de mots sur l'alphabet $E \sqcup E^{-1}$. Construisons le groupe le plus général fabriqué à partir de E (l'ensemble des générateurs) dans lequel les mots appartenant à R (l'ensemble des relations) sont triviaux :

Définition 8.3.1

Nous appelons *groupe défini par l'ensemble de générateurs E et l'ensemble de relations R* le quotient de $F(E)$ par le plus petit sous-groupe distingué de $F(E)$ contenant R. Nous notons ce groupe $\langle E \,|\, R\rangle$; nous dirons que $\langle E \,|\, R\rangle$ est une *présentation* de ce groupe par générateurs et relations. Si $E = \{x_1, x_2, \ldots, x_n\}$, nous écrirons souvent $\langle x_1, x_2, \ldots, x_n \,|\, R\rangle$ au lieu de $\langle \{x_1, x_2, \ldots, x_n\} \,|\, R\rangle$.

Proposition 8.3.1: Propriété universelle d'un groupe défini par générateurs et relations

Soit E un ensemble. Soit R un ensemble de mots sur l'alphabet $E \sqcup E^{-1}$ et soit p l'application composée

$$E \to F(E) \to \langle E \,|\, R\rangle.$$

Soit G un groupe et soit $(g_x)_{x\in E}$ une famille d'éléments de G telle que $m(g_x)_x = e$ pour tout $m \in R$. Il existe un unique morphisme de groupes $\varphi\colon \langle E \,|\, R\rangle \to \mathrm{G}$ tel que $\varphi(p(x)) = g_x$ pour tout $x \in E$.

Cet énoncé peut se reformuler comme suit : l'application $\varphi \mapsto (\varphi(p(x)))_{x\in E}$ établit une bijection entre l'ensemble des morphismes de groupes de $\langle E \,|\, R\rangle$ vers G et l'ensemble des familles $(g_x)_{x\in E}$ d'éléments de G telles que $m(g_x)_x = e$ pour tout $m \in R$. Autrement dit se donner un morphisme de $\langle E \,|\, R\rangle$ vers G c'est choisir une famille $(g_x)_{x\in E}$ d'éléments de G qui annulent chacune des relations appartenant à R.

Exemple 8.3.1. — Tout groupe fini est de présentation finie.

Exemple 8.3.2. — Le *groupe diédral* est défini par

$$\mathrm{D}_{2n} = \langle g, h \,|\, g^n, h^2, ghgh\rangle$$

ce que nous pouvons aussi écrire

$$\mathrm{D}_{2n} = \langle g, h \,|\, g^n = e, h^2 = e, ghgh = e\rangle$$

ou encore

$$\mathrm{D}_{2n} = \langle g, h \,|\, g^n = e, h = h^{-1}, gh = h^{-1}g^{-1}\rangle.$$

Exemple 8.3.3. — Le groupe $\mathbb{H}_8$ des quaternions admet la présentation

$$\langle x, y \,|\, x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1}\rangle$$

(prendre, par exemple, $x = i$ et $y = j$).

***Exemple 8.3.4* (Une présentation de $\mathbb{Z}/n\mathbb{Z}$ par générateurs et relations)**

Soit E un singleton $\{x\}$. Le morphisme

$$\mathbb{Z} \to F(E) \qquad\qquad n \mapsto x^n$$

est un isomorphisme.

Soit n un entier. Comme le groupe libre sur $\{a\}$ est abélien, son plus petit sous-groupe distingué contenant a^n est le groupe engendré par a^n. Il s'ensuit que $\langle a \,|\, a^n \rangle$ est une présentation de $\mathbb{Z}/n\mathbb{Z}$ par générateurs et relations.

***Exemple 8.3.5* (Une présentation de $\mathbb{Z}^2$ par générateurs et relations)**

Montrons que les groupes $\mathbb{Z}^2$ et $\langle a,\, b \,|\, aba^{-1}b^{-1} \rangle$ sont isomorphes.

Considérons l'application ensembliste de

$$\{a,\, b\} \to \mathbb{Z}^2 \qquad \begin{cases} a \mapsto (1,0) \\ b \mapsto (0,1) \end{cases}$$

Puisque

$$(1,0) + (0,1) - (1,0) - (0,1) = (0,0)$$

cette application induit un morphisme φ de $\langle a,\, b \,|\, aba^{-1}b^{-1} \rangle$ vers $\mathbb{Z}^2$.

Par ailleurs $\langle a,\, b \,|\, aba^{-1}b^{-1} \rangle$ est engendré par $\overline{a}$ et $\overline{b}$ qui commutent en vertu de la relation $aba^{-1}b^{-1}$. L'application

$$\mathbb{Z}^2 \to \langle a,\, b \,|\, aba^{-1}b^{-1} \rangle \qquad (n,m) \mapsto \overline{a}^n \overline{b}^m$$

est donc un morphisme de groupes. On peut vérifier sur les générateurs $\overline{a}$ et $\overline{b}$ d'une part, $(1,0)$ et $(0,1)$ de l'autre que $\chi \circ \psi = \mathrm{id}$ et $\psi \circ \chi = \mathrm{id}$. Par conséquent $\langle a,\, b \,|\, aba^{-1}b^{-1} \rangle$ et $\mathbb{Z}^2$ sont isomorphes.

Remarque 8.3.1. — Considérons le groupe libre sur l'alphabet $\{a,\, b\}$; notons le G. Nous pouvons décrire $\mathbb{Z}^2$ comme l'abélianisé de G. En effet considérons l'application ensembliste

$$\{a,\, b\} \to \mathbb{Z}^2 \qquad \begin{cases} a \mapsto (1,0) \\ b \mapsto (0,1) \end{cases}$$

Cette application induit un morphisme φ de G vers $\mathbb{Z}^2$. Puisque $\mathbb{Z}^2$ est abélien ce morphisme induit un morphisme ψ de $\mathrm{G}/D(\mathrm{G})$ vers $\mathbb{Z}^2$. Étant donné que $\mathrm{G}/D(\mathrm{G})$ est abélien les classes $\overline{a}$ et $\overline{b}$ de a et b modulo $D(\mathrm{G})$ commutent. L'application $\chi\colon \mathbb{Z}^2 \to \mathrm{G}/D(\mathrm{G})$ donnée par la formule $(n,m) \mapsto \overline{a}^n \overline{b}^m$ est par suite un morphisme de groupes. On peut vérifier sur les générateurs $\overline{a}$ et $\overline{b}$ d'une part, $(1,0)$ et $(0,1)$ de l'autre que $\chi \circ \psi = \mathrm{id}$ et $\psi \circ \chi = \mathrm{id}$. Ainsi $\mathrm{G}/D(\mathrm{G})$ est isomorphe à $\mathbb{Z}^2$.

***Remarque 8.3.2* (Le problème du mot).** — Soit E un ensemble. Soit R un ensemble de mots sur l'alphabet $E \sqcup E^{-1}$. Le morphisme quotient

$$F(E) \to \langle E \,|\, R \rangle \qquad m \mapsto m(\overline{x})_x$$

est surjectif. Le groupe $\langle E \,|\, R \rangle$ est donc constitué d'éléments de la forme $m(\overline{x})_x$ où m est un mot sur l'alphabet $E \sqcup E^{-1}$. Mais cette description ne précise pas à quelle condition sur les mots m et n nous avons $m(\overline{x})_x = n(\overline{x})_x$, *i.e.* à quelle condition sur un mot m nous avons $m(\overline{x})_x = e$. La réponse théorique à cette question est bien entendue : nous avons $m(\overline{x})_x = e$ si

et seulement si m appartient au plus petit sous-groupe distingué de $F(E)$ contenant R. Mais décider en pratique si c'est le cas est extrêmement difficile ; c'est même impossible en toute généralité : il n'existe pas d'algorithme permettant de résoudre le problème du mot, *i.e.* de répondre en temps fini pour n'importe quel ensemble fini E, n'importe quel ensemble fini R de mots sur l'alphabet $E \sqcup E^{-1}$ et n'importe quel mot m sur l'alphabet $E \sqcup E^{-1}$ à la question : « m appartient-il au plus petit sous-groupe distingué de $F(E)$ contenant R ? »

Les transformations de Tietze. — .

Les transformations de Tietze sont utilisées pour transformer une présentation d'un groupe donnée en une autre, souvent plus simple, du même groupe. Ces transformations portent le no du mathématicien autrichien H. Tietze qui les a introduites en 1908.

Principe. Une présentation est définie en termes de générateurs et relations. Formellement une présentation est un couple formé d'un ensemble dont les éléments sont appelés les générateurs et d'un ensemble de mots du groupe libre sur les générateurs qui sont interprétés comme relations. Les transformations de Tietze sont composées d'étapes élémentaires dont chacune séparément transforme de manière plutôt évidente la présentation en une présentation d'un groupe isomorphe.

Étapes élémentaires. Une étape élémentaire peut opérer sur les générateurs ou sur les relations. Elles sont de quatre types :

- ajouter une relation ;
- supprimer une relation ;
- ajouter un générateur ;
- supprimer un générateur.

Exemple 8.3.6. — Montrons que le groupe

$$\mathrm{G} = \langle x,\, y \,|\, x^3 = 1,\, y^2 = 1,\, (xy)^2 = 1 \rangle$$

a aussi pour présentation

$$\langle y,\, z \,|\, (zy)^3 = 1,\, y^2 = 1,\, z^2 = 1 \rangle$$

Partons de

$$\mathrm{G} = \langle x,\, y \,|\, x^3 = 1,\, y^2 = 1,\, (xy)^2 = 1 \rangle.$$

Ajoutons un générateur :

$$\mathrm{G} = \langle x,\, y,\, z \,|\, x^3 = 1,\, y^2 = 1,\, (xy)^2 = 1,\, z = xy \rangle.$$

Ajoutons $x = zy$ et supprimons $z = xy$:

$$\mathrm{G} = \langle x,\, y\,, z \,|\, x^3 = 1,\, y^2 = 1,\, (xy)^2 = 1, x = zy \rangle.$$

Supprimons x :

$$\mathrm{G} = \langle x,\, y,\, z \,|\, (zy)^3 = 1,\, y^2 = 1,\, z^2 = 1 \rangle.$$

Exemple 8.3.7. — Montrons que le groupe $\mathrm{G} = \langle a,\, b,\, c \,|\, b^2,\, (bc)^2 \rangle$ a aussi pour présentation

$$\langle x,\, y,\, z \,|\, y^2,\, z^2 \rangle.$$

Partons de $\mathrm{G} = \langle a,\, b,\, c \,|\, b^2,\, (bc)^2 \rangle$. Ajoutons un générateur (z)

$$\langle a,\, b,\, c,\, z \,|\, b^2,\, (bc)^2,\, z = bc \rangle.$$

Ajoutons $c = b^{-1}z$ et supprimons $z = bc$:

$$\langle a,\, b,\, c,\, z \,|\, b^2,\, z^2,\, c = b^{-1}z \rangle.$$

Supprimons c :

$$\langle a,\, b,\, z \,|\, b^2,\, z^2 \rangle.$$

Ajoutons deux générateurs (x et y) :

$$\langle a,\, b,\, z\, x,\, y |\, b^2,\, z^2,\, x = a,\, y = b \rangle.$$

Ajoutons $a = x$ et $b = y$ et supprimons $x = a$ et $y = b$:

$$\langle x,\, y,\, z |\, y^2,\, z^2 \rangle.$$

Exemple 8.3.8. — Considérons le groupe

$$D(\ell, m, n) = \langle x,\, y \,|\, x^\ell = y^m = (xy)^n = e \rangle.$$

Montrons que $D(\ell, m, n)$ et $D(n, m, \ell)$ ont même présentation :

$$\begin{aligned}
D(\ell, m, n) &= \langle x,\, y \,|\, x^\ell = y^m = (xy)^n = e \rangle \\
&= \langle a,\, x,\, y \,|\, a = xy,\, x^\ell = y^m = (xy)^n = e \rangle \\
&= \langle a,\, x,\, y \,|\, x = ay^{-1},\, x^\ell = y^m = (xy)^n = e \rangle \\
&= \langle a,\, y \,|\, (ay^{-1})^\ell = y^m = a^n = e \rangle \\
&= \langle a,\, y,\, b,\, |\, b = y^{-1},\, (ay^{-1})^\ell = y^m = a^n = e \rangle \\
&= \langle a,\, b,\, |\, (ab)^\ell = (b^{-1})^m = a^n = e \rangle \\
&= \langle a,\, b,\, |\, (ab)^\ell = b^{-m} = a^n = e \rangle \\
&= \langle a,\, b,\, |\, (ab)^\ell = b^m = a^n = e \rangle \\
&= D(n, m, \ell).
\end{aligned}$$

Exemple 8.3.9. — Montrons que le groupe

$$\mathrm{T} = \langle x,\, y,\, z \,|\, x = yzy^{-1},\, y = zxz^{-1},\, z = xyx^{-1} \rangle$$

a aussi pour présentation

$$\langle a,\, b \,|\, a^3 = b^2 \rangle :$$

$$\begin{aligned}
\mathrm{T} &= \langle x,\, y,\, z \,|\, x = yzy^{-1},\, y = zxz^{-1},\, z = xyx^{-1}\rangle \\
&= \langle x,\, y \,|\, x = y(xyx^{-1})y^{-1},\, y = (xyx^{-1})x(xyx^{-1})^{-1}\rangle \\
&= \langle x,\, y \,|\, xyx = yxy,\, yxy = xyx\rangle \\
&= \langle x,\, y \,|\, xyx = yxy\rangle \\
&= \langle x,\, y,\, a \,|\, xyx = yxy,\, a = xy\rangle \\
&= \langle x,\, y,\, a \,|\, xyx = yxy,\, y = x^{-1}a\rangle \\
&= \langle x,\, a \,|\, ax = x^{-1}a^2\rangle \\
&= \langle x,\, a \,|\, xax = a^2\rangle \\
&= \langle x,\, a,\, b \,|\, xax = a^2,\, b = ax\rangle \\
&= \langle x,\, a,\, b \,|\, xax = a^2,\, x = ba^{-1}\rangle \\
&= \langle x,\, a,\, b \,|\, ba^{-1}aba^{-1} = a^2,\, x = ba^{-1}\rangle \\
&= \langle\, a,\, b \,|\, b^2 = a^3\rangle
\end{aligned}$$

Exemple 8.3.10. — Le groupe des quaternions $\mathbb{H}_8$ est le sous-groupe des matrices 2×2 inversibles à coefficients complexes engendré par

$$A = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}.$$

Montrons que ce groupe admet pour présentation

$$\langle A,\, B \,|\, A^2 = B^2 = (AB)^2\rangle$$

et

$$\langle R,\, S,\, T \,|\, R^2 = S^2 = T^2 = RST\rangle.$$

Nous pouvons vérifier que $A^2 = B^2 = (AB)^2 = -\mathrm{id}$ d'où la première présentation (en effet un groupe qui a cette présentation est d'ordre 8).

De plus

$$\begin{aligned}
\langle A,\, B \,|\, A^2 = B^2 = (AB)^2\rangle &= \langle A,\, B,\, R,\, S \,|\, R = A,\, S = B,\, A^2 = B^2 = (AB)^2\rangle \\
&= \langle R,\, S \,|\, R^2 = S^2 = (RS)^2\rangle \\
&= \langle R,\, S,\, T \,|\, T = RS,\, R^2 = S^2 = T^2\rangle \\
&= \langle R,\, S,\, T \,|\, R^2 = S^2 = T^2 = RST\rangle.
\end{aligned}$$

8.4. Le groupe $\mathrm{SL}(2, \mathbb{Z})$

8.4.1. Générateurs de $\mathrm{SL}(2, \mathbb{Z})$. —

Lemme 8.4.1

Les matrices

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

engendrent $\mathrm{SL}(2, \mathbb{Z})$.

Démonstration. — Montrons que tout élément M de $\mathrm{SL}(2, \mathbb{Z})$ est un mot en $A^{\pm 1}$ et $B^{\pm 1}$. Écrivons M sous la forme $M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. On écrira parfois $\beta(M)$ (respectivement $\delta(M)$) au lieu de β (respectivement δ). Posons $T = ABA \in \mathrm{SL}(2, \mathbb{Z})$.

- ◇ Si $\beta = 0$, alors $\alpha = \delta = \pm 1$ et ou bien $M = B^{-\gamma}$ ou bien $M = -B^{\gamma} = T^2 B^{\gamma}$. Ainsi M s'exprime comme un mot en $A^{\pm 1}$ et $B^{\pm 1}$.
- ◇ Si $\delta = 0$, alors $\beta\gamma = -1$. Nous avons l'alternative $\beta = -\gamma = 1$ ou $\beta = -\gamma = -1$, *i.e.* l'alternative $M = A^{-\gamma} T$ ou $M = A^{\gamma} T^3$. Dans les deux cas M s'exprime comme un mot en $A^{\pm 1}$ et $B^{\pm 1}$.
- ◇ Supposons maintenant que $\beta\delta = \beta(M)\delta(M) \neq 0$. Notons que

$$\beta(AM) = \beta(M) + \delta(M) \qquad \text{et} \qquad \delta(AM) = \delta(M) \tag{8.4.1}$$

et

$$\beta(TM) = \delta(M) \qquad \text{et} \qquad \delta(TM) = -\beta(M). \tag{8.4.2}$$

Les égalités (8.4.1) entraînent que quitte à multiplier M à gauche par une puissance de A bien choisie nous obtenons une matrice $A^n M$ telle que

$$0 \leq |\beta(A^n M)| \leq |\delta(A^n M)|$$

Les égalités (8.4.2) impliquent qu'on peut échanger les rôles de $\pm\beta$ et $\pm\delta$ quitte à multiplier à gauche par T. Nous pouvons donc faire décroître les valeurs absolues de β et δ jusqu'à ce que l'une des deux s'annule. Autrement dit quitte à multiplier M à gauche par des puissances convenables de A et T on se ramène au cas $\beta = 0$ ou au cas $\delta = 0$, cas traités précédemment.

□

Donnons un second système de générateurs de $\mathrm{SL}(2, \mathbb{Z})$:

Théorème 8.4.1

Les matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{et} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

engendrent $\mathrm{SL}(2, \mathbb{Z})$.

Démonstration. — Désignons par G le sous-groupe de $\mathrm{SL}(2, \mathbb{Z})$ engendré par S et T, *i.e.* $\mathrm{G} = \langle S, T \rangle$.

Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est un élément quelconque de $\mathrm{SL}(2, \mathbb{Z})$, alors

$$S \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \qquad T^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + nc & b + nd \\ c & d \end{pmatrix} \tag{8.4.3}$$

Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathrm{SL}(2, \mathbb{Z})$.

- ◇ Supposons que $c = 0$. Puisque M appartient à $\mathrm{SL}(2, \mathbb{Z})$ elle est de la forme $\begin{pmatrix} \pm 1 & k \\ 0 & \pm 1 \end{pmatrix}$ pour un certain entier k et avec des entrées diagonales de même signe. Autrement dit $M = T^k$ ou $-T^{-k}$, *i.e.* il existe un élément g dans G tel que $gM = \pm T^n$ pour un certain n dans $\mathbb{Z}$. Comme T^n appartient à G et $S^2 = -\mathrm{id}$ nous obtenons que $M = \pm g^{-1} T^n$ appartient à G.
- ◇ Supposons désormais que $c \neq 0$. Si $|a| \geq |c|$, on effectue la division euclidienne de a par c : $a = cq + r$, $0 \leq r \leq |c|$. Appelons coefficient (i, j) d'une matrice le coefficient situé sur la $i$ème ligne et la $j$ième colonne de cette matrice. D'après (8.4.3) le coefficient $(1, 1)$ de $T^{-q}M$ est $a - qc = r$ qui est en valeur absolue plus petit que le coefficient $(2, 1)$ de $T^{-q}M$. Nous multiplions ensuite $T^{-q}M$ à gauche par S ce qui a pour effet d'échanger les coefficients $(1, 1)$ et $(2, 1)$ de $T^{-q}M$ modulo un signe (*cf.* (8.4.3)). Si le coefficient $(2, 1)$ de $ST^{-q}M$ est non nul nous considérons de nouveau la division euclidienne du coefficient $(1, 1)$ de $ST^{-q}M$ par le coefficient $(2, 1)$ de $ST^{-q}M$, nous multiplions par la puissance de T adéquate puis par S etc jusqu'à obtenir une matrice dont le coefficient $(2, 1)$ est nul : nous nous sommes ramenés au cas précédent.

□

Cette seconde démonstration a l'avantage d'être « constructive » comme nous pouvons le voir dans l'exemple suivant :

Exemple 8.4.1. — Écrivons $A = \begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix}$ à l'aide de S et T.

Puisque $17 = 7 \times 2 + 3$, nous allons soustraire 7×2 à 17 ;

$$T^{-2}A = \begin{pmatrix} 3 & 5 \\ 7 & 12 \end{pmatrix}.$$

Maintenant échangeons les rôles de 3 et 7 en multipliant par S :

$$ST^{-2}A = \begin{pmatrix} -7 & -12 \\ 3 & 5 \end{pmatrix}.$$

Divisons -7 par 3, nous obtenons $-7 = 3 \times (-3) + 2$; nous allons donc ajouter 3×3 à -7 en multipliant par T^3 :

$$T^3ST^{-2}A = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}.$$

Quitte à multiplier par S nous avons

$$ST^3ST^{-2}A = \begin{pmatrix} -3 & -5 \\ 2 & 3 \end{pmatrix}.$$

Comme $-3 = 2 \times (-2) + 1$ nous avons

$$T^2ST^3ST^{-2}A = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}.$$

puis

$$ST^2ST^3ST^{-2}A = \begin{pmatrix} -2 & -3 \\ 1 & 1 \end{pmatrix}.$$

Comme $-2 = 1 \times (-2) + 0$ nous obtenons

$$T^2ST^2ST^3ST^{-2}A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

et enfin

$$ST^2ST^2ST^3ST^{-2}A = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}.$$

soit $ST^2ST^2ST^3ST^{-2}A = -T = S^2T$ ou encore $A = T^2S^{-1}T^{-3}S^{-1}T^{-2}S^{-1}T^{-2}S^{-1}S^2T$. Mais $S^{-1} = -S$ donc

$$A = T^2ST^{-3}ST^{-2}ST^{-2}ST.$$

Remarque 8.4.1. — Reprenons l'exemple $\begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$. Pour obtenir une expression en termes de S et T nous regardons le ratio de la première colonne à savoir $\frac{17}{7}$:

$$\frac{17}{7} = 3 - \frac{4}{7} = 3 - \frac{1}{\frac{7}{4}} = 3 - \frac{1}{2 - \frac{1}{4}},$$

les entiers 3, 2 et 4 vont jouer un rôle crucial dans la suite. Nous avons

$$T^3 S T^2 S T^4 S = \begin{pmatrix} 17 & -5 \\ 7 & -2 \end{pmatrix}.$$

Résolvons

$$\begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix} = \begin{pmatrix} 17 & -5 \\ 7 & -2 \end{pmatrix} M$$

Nous obtenons

$$M = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = T^2$$

Ainsi

$$\begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix} = T^3 S T^2 S T^4 S T^2.$$

Notons que cette expression est différente de celle obtenue précédemment : lorsqu'on considère les fractions continues on est inéressé par les entiers les plus proches « supérieurs » ce qui n'est pas le cas lorsqu'on fait des divisions euclidiennes.

Corollaire 8.4.1

Le groupe $\mathrm{SL}(2,\mathbb{Z})$ est engendré par

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Démonstration. — Notons que T et U appartiennent à $\mathrm{SL}(2,\mathbb{Z})$; ainsi le groupe $\langle T, U\rangle$ est un sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$. Réciproquement $S = T^{-1}UT^{-1}$ donc $\langle T, U\rangle \supset \langle S, T\rangle = \mathrm{SL}(2,\mathbb{Z})$. □

Corollaire 8.4.2

Le groupe $\mathrm{SL}(2,\mathbb{Z})$ est engendré par deux matrices d'ordre fini.

Démonstration. — Nous avons vu que $\mathrm{SL}(2,\mathbb{Z}) = \langle S, T\rangle$ (Théorème 8.4.1). Par suite $\mathrm{SL}(2,\mathbb{Z}) = \langle S, ST\rangle$. Or $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est d'ordre 4 et $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ est d'ordre 6. □

Corollaire 8.4.3

L'image de tout morphisme de $\mathrm{SL}(2,\mathbb{Z})$ dans $\mathbb{C}^*$ est contenue dans le groupe des racines 12ième de l'unité.

Démonstration. — Le Corollaire 8.4.2 assure que $\mathrm{SL}(2,\mathbb{Z})$ est engendé par S qui est d'ordre 4 et ST qui est d'ordre 12. Par suite l'image d'un morphisme de $\mathrm{SL}(2,\mathbb{Z})$ dans $\mathbb{C}^*$ est contenue dans le sous-groupe engendré par μ_4 et μ_6 qui est μ_12 (en effet $12 = \mathrm{ppcm}(4,6)$). □

Exemple 8.4.2. — Considérons

$$\begin{array}{rcl} \chi\colon \mathrm{SL}(2,\mathbb{Z}) & \to & \mathbb{C}^* \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto & \exp\left(\dfrac{2\mathbf{i}\pi}{12}\Big((1-c^2)(bd+3(c-1)d+c+3)+c(a+d-3)\Big)\right). \end{array}$$

En particulier

$$\chi(S) = -\mathbf{i} = \exp\left(\frac{3\mathbf{i}\pi}{2}\right) \qquad \text{et} \qquad \chi(T) = -\mathbf{i}\left(\frac{-1+\mathbf{i}\sqrt{3}}{2}\right) = \exp\left(\frac{2\mathbf{i}\pi}{12}\right).$$

On peut vérifier que ξ est un morphisme de groupes dont l'image est le groupe des racines 12ième de l'unité tout entier.

8.4.2. Générateurs de $\mathrm{PSL}(2,\mathbb{Z})$. —

Lemme 8.4.2

Le groupe $\mathrm{PSL}(2,\mathbb{Z})$ est engendré par $\overline{S}$ et $\overline{ST}$ où

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{et} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

sont les matrices introduites au Théorème 8.4.1.

Démonstration. — Posons

$$x = \overline{S} = \overline{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}} \qquad \text{et} \qquad y = \overline{ST} = \overline{\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}}$$

Alors $x^2 = -\mathrm{id} = \mathrm{id}$ et $y^3 = -\mathrm{id} = \mathrm{id}$ dans $\mathrm{PSL}(2,\mathbb{Z})$. Puisque S et ST engendrent $\mathrm{SL}(2,\mathbb{Z})$ tout élément de $\mathrm{PSL}(2,\mathbb{Z})$ s'écrit comme un mot en les x et y. Comme x et y sont respectivement d'ordre 2 et 3 on peut écrire tout mot en les x et y sous la forme suivante

$$y^{i_0}xy^{i_1}x\dots y^{i_{n-1}}xy^{i_n} \tag{8.4.4}$$

avec

- $i_j \in \mathbb{Z}/3\mathbb{Z}$,
- $i_1 \not\equiv 0 \bmod 3$, $i_2 \not\equiv 0 \bmod 3$, …, $i_{n-1} \not\equiv 0 \bmod 3$.

□

Remarque 8.4.2. — Nous verrons que l'écriture (8.4.4) est unique au §8.4.3, autrement dit x et y engendrent librement [3] $\mathrm{PSL}(2,\mathbb{Z})$:

$$\mathrm{PSL}(2,\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$$

i.e. il n'y a pas de relations entre x et y dans le groupe $\mathrm{PSL}(2,\mathbb{Z})$ exceptées celles découlant de $x^2 = 1$ et $y^3 = 1$.

8.4.3. Présentations de $\mathrm{SL}(2,\mathbb{Z})$ et de $\mathrm{PSL}(2,\mathbb{Z})$. — Le *groupe des tresses* B_n est le groupe engendré par les $n-1$ générateurs σ_1, σ_2, …, σ_{n-1} satisfaisant les relations suivantes

$$\begin{cases} \sigma_i\sigma_j = \sigma_j\sigma_i \text{ pour tout } 1 \le i,\, j \le n-1 \text{ et } |i-j| \ge 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ pour tout } 1 \le i \le n-2 \end{cases}$$

Par définition $B_1 = \{\mathrm{id}\}$ et B_2 est le groupe cyclique infini $\langle\sigma_1\rangle$.

Considérons les trois groupes de présentation

$$\langle a,\, b \,|\, aba = bab,\, (aba)^4 = 1\rangle \tag{8.4.5}$$

$$\langle s,\, t \,|\, s^3 = t^2,\, t^4 = 1\rangle \tag{8.4.6}$$

$$\langle s,\, t \,|\, s^3 = t^2 = 1\rangle \tag{8.4.7}$$

Lemme 8.4.3

Les présentations (8.4.5) et (8.4.6) définissent le même groupe G à isomorphisme près. Le groupe G est isomorphe au quotient du groupe des tresses B_3 par le sous-groupe central engendré par $(\sigma_1\sigma_2\sigma_1)^4$.

3. Si G et H sont deux groupes, leur *produit libre* $\mathrm{G} * \mathrm{H}$ est défini comme le groupe (unique à isomorphisme près) dans lequel les groupes G et H s'injectent

$$i\colon \mathrm{G} \to \mathrm{G} * \mathrm{H} \qquad \text{et} \qquad j\colon \mathrm{H} \to \mathrm{G} * \mathrm{H}$$

avec la propriété universelle suivante : pour tout groupe K, pour tous morphismes $g\colon \mathrm{G} \to \mathrm{K}$ et $h\colon \mathrm{H} \to \mathrm{K}$ il existe un unique morphisme $f\colon \mathrm{G} * \mathrm{H} \to \mathrm{K}$ qui prolonge à la fois g et h, *i.e.* tel que $f \circ i = g$ et $f \circ j = h$.

Démonstration. — Montrons comment passer de (8.4.5) à (8.4.6). Posons $s = ab$ et $t = aba$. Alors $a = sb^{-1}$ et

$$t = aba \iff t = sb^{-1}bsb^{-1} \iff t = s^2b^{-1} \iff b = t^{-1}s^2.$$

Finalement $b = t^{-1}s^2$ et $a = sb^{-1} = ss^{-2}t = s^{-1}t$. Nous en déduisons que $aba = bab$ se réécrit

$$s^{-1}tt^{-1}s^2s^{-1}t = t^{-1}s^2s^{-1}tt^{-1}s^2 \iff s^{-1}s^2s^{-1}t = t^{-1}s^2s^{-1}s^2 \iff t = t^{-1}s^3 \iff t^2 = s^3$$

et $(aba)^4 = 1$ se réécrit $t^4 = 1$. Ainsi (8.4.5) et (8.4.6) définissent des groupes isomorphes.

En remplaçant a par σ_1 et b par σ_2 dans (8.4.5) nous constatons que G est isomorphe au quotient de B_3 par le sous-groupe normal engendré par $(\sigma_1\sigma_2\sigma_1)^4$. □

Remarque 8.4.3. — $(\sigma_1\sigma_2\sigma_1)^4 = \left((\sigma_1\sigma_2\sigma_1)^2\right)^2$ et $(\sigma_1\sigma_2\sigma_1)^2$ engendre le centre de B_3 (*voir* [**KT08**, Theorem 1.24]).

Remarque 8.4.4. — On déduit de (8.4.6) une troisième présentation de G :

$$\mathrm{G} = \langle u,\, v \mid u^2 = (uv)^3,\, u^4 = 1\rangle.$$

Lemme 8.4.4

Le groupe H défini par (8.4.7) est isomorphe au quotient de B_3 par son centre.

Démonstration. — À partir des présentations (8.4.6) et (8.4.7) il est clair que H est le quotient de G par le sous-groupe normal engendré par $s^3 = t^2 \in \mathrm{G}$. Les identifications

$$s = ab = \sigma_1\sigma_2 \qquad\qquad t = aba = \sigma_1\sigma_2\sigma_1$$

conduisent à $\mathrm{H} = {}^{B_3}\!/_{Z(B_3)}$. □

Posons

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix};$$

comme on l'a vu (Lemme 8.4.1) ces matrices engendrent $\mathrm{SL}(2,\mathbb{Z})$. Un calcul direct montre que

$$ABA = BAB \qquad \text{et} \qquad (ABA)^4 = \mathrm{id}.$$

Par conséquent il existe un morphisme de groupes $f\colon \mathrm{G} \to \mathrm{SL}(2,\mathbb{Z})$ tel que

$$f(a) = A \qquad \text{et} \qquad f(b) = B.$$

Nous constatons que

$$\begin{aligned} f(s) &= f(ab) = f(a)f(b) = AB = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \\ f(t) &= f(aba) = f(a)f(b)f(a) = ABA = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ f(t^2) &= f(tt) = f(t)f(t) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -\mathrm{id}. \end{aligned}$$

Cette dernière égalité assure que f induit un morphisme de groupes $\overline{f}\colon \mathrm{H} \to \mathrm{PSL}(2,\mathbb{Z})$.

Théorème 8.4.2

Les morphismes de groupes

$$f\colon \mathrm{G} \to \mathrm{SL}(2,\mathbb{Z})$$

et

$$\overline{f}\colon \mathrm{H} \simeq {}^{B_3}\!/_{Z(B_3)} \to \mathrm{PSL}(2,\mathbb{Z})$$

sont des isomorphismes.

Lemme 8.4.5

Le morphisme $f\colon \mathrm{G} \to \mathrm{SL}(2,\mathbb{Z})$ est injectif (respectivement surjectif) si et seulement si $\overline{f}$ est injectif (respectivement surjectif).

Démonstration. — Le morphisme f envoie le sous-groupe $\langle t^2\rangle \subset \mathrm{G}$ sur le groupe d'ordre 2 engendré par $-\mathrm{id}$. Comme $t^4 = 1$ le sous-groupe $\langle t^2\rangle$ est d'ordre au plus 2. Ainsi f induit un isomorphisme entre $\langle t^2\rangle$ et $\{\pm\mathrm{id}\}$. □

Démonstration du Théorème 8.4.2. — D'après le Lemme 8.4.5 il suffit de montrer que $f\colon \mathrm{G} \to \mathrm{SL}(2,\mathbb{Z})$ est surjective et $\overline{f}\colon \mathrm{H} \to \mathrm{PSL}(2,\mathbb{Z})$ est injective.

Le Lemme 8.4.1 assure que $A = f(a)$ et $B = f(b)$ engendrent $\mathrm{SL}(2,\mathbb{Z})$ ce qui entraîne que $f\colon \mathrm{G} \to \mathrm{SL}(2,\mathbb{Z})$ est surjective.

Montrons que $\overline{f}\colon \mathrm{H} \to \mathrm{PSL}(2,\mathbb{Z})$ est injective. Le groupe H de présentation

$$\langle s,\, t \mid s^3 = t^2 = 1\rangle$$

est le produit libre du groupe cyclique d'ordre 3 engendré par s et du groupe cyclique d'ordre 2 engendré par t. Tout élément de $\mathrm{H} \smallsetminus \{\mathrm{id}\}$ a une unique expression de l'une des formes suivantes

$$w = s^{\varepsilon_1} t s^{\varepsilon_2} t \dots t s^{\varepsilon_r}, \qquad wt, \qquad tw, \qquad twt, \qquad t$$

où $\varepsilon_i = \pm 1$ pour tout $1 \leq i \leq r$ (pour une définition des produits libres et une description des formes normales de leurs éléments voir [**LS01**, §I.11] ou [**Ser77**, §I.1.]). On est donc ramené à montrer qu'aucun de ces éléments n'appartient à $\ker \overline{f}$.

Puisque $f(t) = ABA = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, t n'appartient pas à $\ker \overline{f}$.

Comme $twt = twt^{-1}$ est un conjugué de w et comme tw est un conjugué de wt il suffit de vérifier que $\overline{f}(w) \neq 1$ et $\overline{f}(wt) \neq 1$.

Commençons par étudier $\overline{f}(wt)$. Nous avons $wt = (s^{\varepsilon_1}t)(s^{\varepsilon_2}t)\dots(s^{\varepsilon_r}t)$. Puisque $s^{-1}t = a$ et

$$st = (t^{-1}s^2)^{-1} = b^{-1} \in \mathrm{H}$$

nous avons $\overline{f}(s^{-1}t) = \overline{A}$ et $\overline{f}(st) = \overline{B}^{-1}$ où $\overline{A}$ (respectivement $\overline{B}$) désigne l'image de A (respectivement B) dans $\mathrm{PSL}(2, \mathbb{Z})$. Ainsi $\overline{f}(wt)$ est un produit non vide faisant intervenir $\overline{A}$ et $\overline{B}^{-1}$. Il suffit donc de vérifier qu'aucun produit non vide de $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ ne peut être égal à $\{\pm \mathrm{id}\}$. D'une part un tel produit n'a que des coefficients positifs ou nuls, d'autre part après chaque multiplication par A ou B^{-1} la somme des coefficients non diagonaux augmente strictement. Par suite un tel produit ne peut pas être égal à $\pm\mathrm{id}$.

Pour finir on s'intéresse à $\overline{f}(w)$. Raisonnons par l'absurde : supposons que $\overline{f}(w) = 1$. Alors

$$\overline{f}(wt) = \overline{f}(t) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

ce qui contredit le fait que $\overline{f}(wt)$ n'a que des coefficients positifs ou nuls. Il s'ensuit que $\overline{f}(w) \neq 1$. □

Donnons une autre démonstration de la présentation du groupe $\mathrm{PSL}(2, \mathbb{Z})$ (nous retrouvons le Corollaire 8.2.3) :

Théorème 8.4.3: [Alp93]

Nous avons

$$\mathrm{PSL}(2, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$$

Démonstration du Théorème 8.4.3. — Le groupe $\mathrm{SL}(2, \mathbb{Z})$ est engendré par (Théorème 8.4.1)

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

par conséquent $\overline{T}$ et $\overline{S}$ engendrent $\mathrm{PSL}(2,\mathbb{Z})$. En particulier $\mathrm{PSL}(2,\mathbb{Z})$ est engendré par

$$\mathrm{H} = \langle \overline{T} \rangle = \langle \overline{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}} \rangle \qquad \text{et} \qquad \mathrm{K} = \langle \overline{TS} \rangle = \langle \overline{\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}} \rangle;$$

Le groupe H est cyclique d'ordre 2 et le groupe K est cyclique d'ordre 3. Le groupe $\mathrm{PSL}(2,\mathbb{Z})$ agit sur $\mathbb{C}$: si $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartient à $\mathrm{SL}(2,\mathbb{Z})$, alors son action sur $\mathbb{C}$ est donnée par

$$z \mapsto \frac{az+b}{cz+d}$$

et donc sur l'ensemble des irrationnels. En particulier les générateurs agissent comme suit

$$T\colon z \mapsto -\frac{1}{z} \qquad \text{et} \qquad TS\colon z \mapsto \frac{z-1}{z}.$$

Notons que

$$T^{-1}\colon z \mapsto -\frac{1}{z} \qquad \text{et} \qquad (TS)^{-1}\colon z \mapsto \frac{1}{1-z}.$$

Désignons par $\mathcal{P}$ l'ensemble des irrationnels positifs et par $\mathcal{N}$ l'ensemble des irrationnels négatifs. Nous avons les inclusions

$$\overline{S}(\mathcal{P}) \subset \mathcal{N} \qquad \overline{TS}(\mathcal{N}) \subset \mathcal{P}.$$

Soit w un mot dont l'écriture alterne $\overline{S}$ et $\overline{TS}$.

- ◇ Supposons que w soit de longueur impaire, alors
  - — $w(\mathcal{P}) \subset \mathcal{N}$ si la lettre la plus à droite de w est $\overline{S}$,
  - — $w(\mathcal{N}) \subset \mathcal{P}$ si la lettre la plus à droite de w n'est pas $\overline{S}$.

  En particulier $w \neq \mathrm{id}$.
- ◇ Supposons que w soit de longueur paire. On peut conjuguer w par $\overline{S}$ si nécessaire afin de considérer un mot commençant par une puissance de $\overline{TS}$ et finissant par $\overline{S}$.
  - — Si $w = (\overline{TS})\ldots\overline{S}$, alors $w(\mathcal{P}) \subset \overline{TS}(\mathcal{N})$ est un ensemble d'irrationnels positifs minorés par 1.
  - — Si $w = (\overline{TS})^{-1}\ldots\overline{S}$, alors $w(\mathcal{P}) \subset \overline{TS}^{-1}(\mathcal{N})$ est un ensemble d'irrationnels positifs majorés par 1.

  En particulier il existe un irrationnel z tel que $w(z) \neq z$ et $w \neq \mathrm{id}$.

La Proposition **??** permet de conclure. □

8.4.4. Sous-groupes libres de $\mathrm{SL}(2,\mathbb{Z})$. —

Proposition 8.4.1

Les deux matrices

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

engendrent un sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$ qui est libre de rang 2.

Remarque 8.4.5. — Plus généralement

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}$$

engendrent un sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$ qui est libre de rang 2 pour tout $k \geq 2$. À noter que ce n'est pas le cas lorsque $k = 1$ vaut 1 puisque

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

est d'ordre fini.

Démonstration. — Considérons

$$\Gamma_1 = \left\{ \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \mid n \in \mathbb{Z} \right\}$$

et

$$\Gamma_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \mid n \in \mathbb{Z} \right\}.$$

Ce sont deux sous-groupes infinis cycliques de $\mathrm{SL}(2,\mathbb{Z})$ engendrés respectivement par les matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. Le groupe $\mathrm{SL}(2,\mathbb{Z})$ agit linéairement sur $\mathbb{R}^2$ comme suit

$$\mathrm{SL}(2,\mathbb{Z}) \times \mathbb{R}^2 \to \mathbb{R}^2, \qquad (M, v) \mapsto M \cdot v.$$

Posons

$$X_1 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid |x| > |y| \right\}$$

et

$$X_2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid |x| < |y| \right\}$$

Nous avons $X_2 \not\subset X_1$; en effet $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ appartient à X_2 mais pas à X_1.

Montrons que $\gamma(X_2) \subset X_1$ pour tout $\gamma \in \Gamma_1 \smallsetminus \{\mathrm{id}\}$. Soit $\gamma \in \Gamma_1 \smallsetminus \{\mathrm{id}\}$, *i.e.* $\gamma = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}$ avec $n \in \mathbb{Z}$, $n \neq 0$ et soit $\begin{pmatrix} x \\ y \end{pmatrix} \in X_2$, *i.e.* $|x| < |y|$. Nous avons

$$\gamma \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 2ny \\ y \end{pmatrix}.$$

D'une part

$$|x + 2ny| = |2ny - (-x)| > ||2ny| - |-x|| = ||2ny| - |x||$$

d'autre part $|x| < |y|$ et $2|n| > 2$ donc $2|n||y| > 2|x| > |x|$, *i.e.* $2|n||y| - |x| > 0$. Par conséquent $||2ny| - |x|| = |2ny| - |x|$ et

$$|x + 2ny| > |2ny| - |x|.$$

Par ailleurs $|x| < |y|$ d'où $-|x| > -|y|$ et

$$|2ny| - |x| > |2ny| - |y| = 2|n||y| - |y| = (2|n| - 1)|y|.$$

Or $|n| > 1$ d'où $2|n| > 2$ et $2|n| - 1 > 1$ ainsi $|2ny| - |x| > |y|$ et $|x + 2ny| > |y|$ autrement dit $\gamma \begin{pmatrix} x \\ y \end{pmatrix}$ appartient à X_1.

De même nous pouvons montrer que $\gamma(X_1) \subset X_2$ pour tout $\gamma \in \Gamma_2 \smallsetminus \{\mathrm{id}\}$.

Le Lemme du ping-pong (Lemme 8.2.1) permet de conclure. □

8.4.5. Sous-groupes de congruences. — Le groupe $\mathrm{SL}(2, \mathbb{Z})$ est un groupe discret de matrices à coefficients entiers, on parle de groupe arithmétique. Pour de tels groupes les sous-groupes les plus importants sont ceux d'indice fini. La façon la plus simple de trouver des sous-groupes d'indice fini de $\mathrm{SL}(2, \mathbb{Z})$ est de passer par les sous-groupe finis de $\mathrm{SL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$. Pour tout entier $n > 1$ le morphisme naturel de réduction

$$\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$$

est un morphisme de groupes de noyau

$$\Gamma(n) = \ker\left(\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)\right) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod n \right\}$$

(notons que cette construction est aussi possible pour $n = 1$ mais $\Gamma(1) = \mathrm{SL}(2, \mathbb{Z})$).

Comme ${\mathrm{SL}(2,\mathbb{Z})}/{\Gamma(n)}$ se plonge dans le groupe fini $\mathrm{SL}\left(2, {\mathbb{Z}}/{n\mathbb{Z}}\right)$ chaque $\Gamma(n)$ est un sous-groupe d'indice fini de $\mathrm{SL}(2,\mathbb{Z})$. Par conséquent tout sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$ contenant $\Gamma(n)$ pour un certain n est d'indice fini.

Théorème 8.4.4

Le groupe

$$\Gamma(2) = \left\{ M \in \mathrm{SL}(2,\mathbb{Z}) \mid M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod 2 \right\}$$

est engendré par les matrices

$$-\mathrm{id} \qquad T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad U^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Démonstration. — Les matrices $-\mathrm{id}$, T^2 et U^2 appartiennent à $\Gamma(2)$ donc $\langle -\mathrm{id}, T^2, U^2 \rangle \subset \Gamma(2)$.

Pour montrer l'inclusion réciproque nous allons adapter la démonstration du Théorème 8.4.1. Au lieu d'utiliser le théorème usuel de division euclidienne nous allons utiliser la version suivante modifiée : si a, b désignent deux éléments de $\mathbb{Z}$ tels que $b \neq 0$, alors $a = bq + r$ avec $|r| < \frac{|b|}{2}$ (r pouvant être négatif). Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de $\Gamma(2)$; en particulier a et d sont impairs alors que b et c sont pairs.

- Si le coefficient $(2,1)$ de M est nul, alors $M = \pm \begin{pmatrix} 1 & \ell \\ 0 & 1 \end{pmatrix}$ pour un certain $\ell \in \mathbb{Z}$. Comme de plus M appartient à $\Gamma(2)$ l'entier ℓ est pair ; on l'écrit donc sous la forme $2k$. Autrement dit $M = \pm \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix}$ et $M = \pm T^{2k} \in \langle -\mathrm{id}, T^2 \rangle$.
- Si le coefficient $(2,1)$ de M n'est pas nul, alors on multiplie M à gauche par une puissance adéquate de T^2 ou U^2 de manière à faire diminuer $\max(|a|,|c|)$. Notons que comme a est impair et c est pair nous avons $a \neq \pm c$ donc $|a| \neq |c|$ et $\max(|a|,|c|)$ vaut ou bien $|a|$, ou bien $|c|$ mais pas les deux. Nous allons distinguer les éventualités $|a| < |c|$ et $|a| > |c|$.
  - Si $|a| > |c|$ et $c \neq 0$ (le cas $c = 0$ a déjà été traité), nous écrivons $a = (2c)q + r$ avec $|r| < \frac{|2c|}{2} = |c|$. Alors

    $$T^{-2q} M = \begin{pmatrix} 1 & -2q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} r & b - 2qd \\ c & d \end{pmatrix}$$

    et $\max(|r|,|c|) = |c| < |a| = \max(|a|,|c|)$.

— Supposons pour finir que $|a| < |c|$. Comme a est impair, $a \neq 0$. Écrivons $c = (2a)q + r$ avec $|r| < \frac{|2a|}{2} = |a|$. Alors

$$U^{-2q}M = \begin{pmatrix} 1 & 0 \\ -2q & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ r & d - 2bq \end{pmatrix}$$

et $\max(|a|, |r|) = |a| < |c| = \max(|a|, |c|)$.

En appliquant, si nécessaire, ces deux étapes tour à tour nous obtenons l'existence d'un élément g de $\langle U^2, T^2 \rangle$ tel que le coefficient $(2, 1)$ de gM soit 0. Alors d'après le premier cas traité gM appartient à $\langle -\mathrm{id}, T^2 \rangle$. Il en résulte que $M = g^{-1}(gM)$ appartient à $\langle -\mathrm{id}, U^2, T^2 \rangle$.

□

Théorème 8.4.5

Le morphisme de réduction

$$\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$$

est surjectif.

Démonstration. — Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de $\mathrm{SL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$. Le théorème des restes chinois assure l'existence de b' tel que

- ◇ $b \equiv b' \bmod n$,
- ◇ a et b' sont premiers entre eux.

Comme a et b' sont premiers entre eux il existe x et y dans $\mathbb{Z}$ tels que $ax - b'y = 1$. Posons

$$c' = c + y(1 - (ad - b'c)) \qquad \text{et} \qquad d' = d + x(1 - (ad - b'c)).$$

Alors $ad' - b'c' = 1$, *i.e.* $\begin{pmatrix} a & b' \\ c' & d' \end{pmatrix}$ appartient à $\mathrm{SL}(2, \mathbb{Z})$. De plus $\begin{pmatrix} a & b' \\ c' & d' \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mod n. En effet $b' \equiv b \bmod n$ donc b' s'écrit $b + jn$ pour un certain entier j et

$$c' - c = y(1 - (ad - b'c)) = y(1 - (ad - (b + jn)c)) = y(1 - \underbrace{(ad - bc)}_{1} + jnc)) = (yjc)n.$$

De même nous obtenons que $d' \equiv d \bmod n$. □

Exemple 8.4.3. — Soit M la matrice donnée par

$$M = \begin{pmatrix} 18 & 14 \\ 4 & 2 \end{pmatrix}.$$

Notons que $\det M = -20 \equiv 1 \bmod 21$. Déterminons une matrice de $\mathrm{SL}(2,\mathbb{Z})$ qui a pour image M par le morphisme de réduction

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}\Big(2, \mathbb{Z}/21\mathbb{Z}\Big).$$

Remarquons que 18 et 14 ne sont pas premiers entre eux mais 18 et $14+21=35$ le sont. Une solution de $18x - 35y = 1$ est $x = 2$, $y = 1$. Autrement dit en reprenant les notations de la démonstration précédente

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 18 & 14 \\ 4 & 2 \end{pmatrix}, \qquad b' = 35, \qquad x = 2, \qquad y = 1$$

d'où $c' = 109$ et $d' = 212$. Ainsi

$$\begin{pmatrix} 18 & 14 \\ 4 & 2 \end{pmatrix} \equiv \begin{pmatrix} 18 & 35 \\ 109 & 212 \end{pmatrix} \bmod 21$$

et $\begin{pmatrix} 18 & 35 \\ 109 & 212 \end{pmatrix}$ appartient à $\mathrm{SL}(2,\mathbb{Z})$.

Corollaire 8.4.4

Pour tout $n \geq 2$ nous avons

$$\mathrm{SL}(2,\mathbb{Z})/\Gamma(n) \simeq \mathrm{SL}\Big(2, \mathbb{Z}/n\mathbb{Z}\Big).$$

Démonstration. — Le morphisme de réduction

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}\Big(2, \mathbb{Z}/n\mathbb{Z}\Big)$$

est surjectif de noyau $\Gamma(n)$, le théorème d'isomorphisme permet de conclure. □

Corollaire 8.4.5

Le groupe fini $\mathrm{SL}\Big(2, \mathbb{Z}/n\mathbb{Z}\Big)$ est engendré par deux éléments d'ordre n.

Démonstration. — D'après le Corollaire 8.4.1 le groupe $\mathrm{SL}(2,\mathbb{Z})$ est engendré par

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Par conséquent $\mathrm{SL}\Big(2, \mathbb{Z}/n\mathbb{Z}\Big)$ est engendré par les réductions de T et U qui sont d'ordre n. □

Corollaire 8.4.6

Le groupe $\langle S,\, T^2\rangle$ est un sous-groupe d'indice 3 de $\mathrm{SL}(2,\mathbb{Z})$.

Démonstration. — Montrons que $\Gamma(2)$ est inclus dans $\langle S,\, T^2\rangle$. Le Théorème 8.4.4 assure qu'il suffit de montrer que les trois générateurs $-\mathrm{id}$, T^2 et U^2 de $\Gamma(2)$ appartiennent à $\langle S,\, T^2\rangle$. Or

$$-\mathrm{id} = S^2 \qquad T^2 = T^2 \qquad \text{et} \qquad U^2 = ST^{-2}S^{-1}$$

donc $\Gamma(2) \subset \langle S,\, T^2\rangle$.

Pour déterminer l'indice de $\langle S,\, T^2\rangle$ dans $\mathrm{SL}(2,\mathbb{Z})$ nous allons travailler modulo $\Gamma(2)$ et calculer l'indice du sous-groupe $\langle S,\, T^2\rangle$ dans

$$\mathrm{SL}(2,\mathbb{Z})/\Gamma(2) \simeq \mathrm{SL}\left(2, \mathbb{Z}/2\mathbb{Z}\right).$$

Puisque $T^2 \in \Gamma(2)$, $S \notin \Gamma(2)$ et $S^2 = -\mathrm{id} \in \Gamma(2)$ le groupe $\langle S,\, T^2\rangle/\Gamma(2)$ est d'ordre 2. Ainsi l'indice de $\langle S,\, T^2\rangle/\Gamma(2)$ dans $\mathrm{SL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est $\frac{6}{3} = 2$. □

Remarque 8.4.6. — Il n'y a pas d'analogue à l'énoncé précédent si on remplace $\langle S,\, T^2\rangle$ par $\langle S,\, T^m\rangle$: le groupe $\langle S,\, T^m\rangle$ n'est pas un sous-groupe d'indice fini de $\mathrm{SL}(2,\mathbb{Z})$ dès que $m > 2$.

Définition 8.4.1

Un sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$ qui contient $\Gamma(n)$ pour un certain entier n est appelé *sous-groupe de congruence* de $\mathrm{SL}(2,\mathbb{Z})$.

Cette terminologie se justifie par le fait qu'un tel sous-groupe peut être décrit par un ensemble fini de conditions de congruence.

Exemple 8.4.4. — La démonstration du Corollaire 8.4.6 assure que $\langle S,\, T^2\rangle$ est un sous-groupe de congruence puisque $\Gamma(2) \subset \langle S,\, T^2\rangle$. L'image de $\langle S,\, T^2\rangle$ dans

$$\mathrm{SL}(2,\mathbb{Z})/\Gamma(2) \simeq \mathrm{SL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$$

est $\{\overline{\mathrm{id}},\, \overline{S}\}$. Nous pouvons donc décrire $\langle S,\, T^2\rangle$ par des conditions de congruence modulo 2 :

$$\langle S,\, T^2\rangle = \left\{ M \in \mathrm{SL}(2,\mathbb{Z}) \,|\, M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \bmod 2 \right\}$$

Parmi les sous-groupes d'indice fini de $\mathrm{SL}(2,\mathbb{Z})$ les sous-groupes de congruence sont particulièrement importants en théorie des nombres : des formes modulaires leur sont associées. Par exemple la fonction L d'une courbe elliptique est une source naturelle de formes modulaires pour les sous-groupes de congruence de $\mathrm{SL}(2,\mathbb{Z})$.

Théorème 8.4.6

Le groupe dérivé de $\mathrm{SL}(2,\mathbb{Z})$ est un sous-groupe de congruence d'indice 12 de $\mathrm{SL}(2,\mathbb{Z})$.

Démonstration. — Comme $\mathrm{SL}(2,\mathbb{Z})$ est engendré par S et T et comme

- ◇ S est d'ordre 4,
- ◇ ST est d'ordre 6,
- ◇ $S^2 = (ST)^3 = -\mathrm{id}$

l'abélianisé $\mathrm{SL}(2,\mathbb{Z})/D(\mathrm{SL}(2,\mathbb{Z}))$ de $\mathrm{SL}(2,\mathbb{Z})$ est engendré par $g = \overline{S}$ et $h = \overline{ST}$ avec

$$g^4 = \mathrm{id}, \qquad h^6 = \mathrm{id}, \qquad g^2 = h^3.$$

Puisque $\mathrm{SL}(2,\mathbb{Z})/D(\mathrm{SL}(2,\mathbb{Z}))$ est abélien chacun de ses éléments est de la forme $g^i h^j$ avec $0 \leq i \leq 3$ et $0 \leq j \leq 5$. Mais $g^2 = h^3$ donc tout élément de l'abélianisé de $\mathrm{SL}(2,\mathbb{Z})$ s'écrit $g^i h^j$ avec $0 \leq i \leq 1$ et $0 \leq j \leq 5$. Le nombre de tels éléments (distincts) étant majoré par 12 nous obtenons l'inégalité

$$[\mathrm{SL}(2,\mathbb{Z}) : D(\mathrm{SL}(2,\mathbb{Z}))] \leq 12.$$

Montrons désormais que $[\mathrm{SL}(2,\mathbb{Z}) : D(\mathrm{SL}(2,\mathbb{Z}))]$ a un quotient abélien d'ordre 12 ce qui entraîne que $[\mathrm{SL}(2,\mathbb{Z}) : D(\mathrm{SL}(2,\mathbb{Z}))] \geq 12$ et donc que $[\mathrm{SL}(2,\mathbb{Z}) : D(\mathrm{SL}(2,\mathbb{Z}))] = 12$.

- ◇ Considérons la composée du morphisme de réduction avec le morphisme de signature

$$\mathrm{SL}(2,\mathbb{Z}) \longrightarrow \mathrm{SL}\Big(2, \mathbb{Z}/2\mathbb{Z}\Big) = \mathrm{GL}\Big(2, \mathbb{Z}/2\mathbb{Z}\Big) \simeq \mathfrak{S}_3 \longrightarrow \{\pm 1\};$$

elle est surjective. Ainsi $\mathrm{SL}(2,\mathbb{Z})$ a un groupe quotient d'ordre 2 qui est abélien.

Par suite $[\mathrm{SL}(2,\mathbb{Z}) : D(\mathrm{SL}(2,\mathbb{Z}))]$ est divisible par 2.

◇ Le groupe $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ est d'ordre 24 et possède un 2-Sylow distingué [4]

$$\begin{aligned}
\mathrm{G} &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \right\} \\
&= \langle \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \rangle
\end{aligned}$$

(isomorphe à $\mathbb{H}_8$). Par suite la composée

$$\mathrm{SL}(2, \mathbb{Z}) \longrightarrow \mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right) \longrightarrow \mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)/\mathrm{G}$$

est un morphisme de $\mathrm{SL}(2, \mathbb{Z})$ dans un groupe d'ordre $\frac{24}{2^3} = 3$ qui est abélien.

Il en résulte que $[\mathrm{SL}(2, \mathbb{Z}) : D(\mathrm{SL}(2, \mathbb{Z}))]$ est divisible par 3.

◇ Le groupe $\mathrm{SL}\left(2, \mathbb{Z}/4\mathbb{Z}\right)$ qui est d'ordre 48 possède un sous-groupe distingué d'indice 4 (à vérifier) ; le groupe quotient correspondant est d'ordre 4 donc abélien et $[\mathrm{SL}(2, \mathbb{Z}) : D(\mathrm{SL}(2, \mathbb{Z}))]$ est divisible par 4.

Finalement $[\mathrm{SL}(2, \mathbb{Z}) : D(\mathrm{SL}(2, \mathbb{Z}))]$ est divisible par 2, 3, 4 mais aussi $2 \times 3 = 6$ et $3 \times 4 = 12$.

Reste à montrer que $D(\mathrm{SL}(2, \mathbb{Z}))$ est un sous-groupe de congruence de $\mathrm{SL}(2, \mathbb{Z})$. Puisque $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right) \times \mathrm{SL}\left(2, \mathbb{Z}/4\mathbb{Z}\right)$ a un quotient abélien H d'ordre $3 \times 4 = 12$ la composée φ définie par

$$\mathrm{SL}(2, \mathbb{Z}) \xrightarrow{\varphi_1} \mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right) \times \mathrm{SL}\left(2, \mathbb{Z}/4\mathbb{Z}\right) \xrightarrow{\varphi_2} \mathrm{H}$$

a pour noyau $D(\mathrm{SL}(2, \mathbb{Z}))$. Mais $\Gamma(12)$ est contenu dans $\ker \varphi_1$ donc dans $\ker \varphi = D(\mathrm{SL}(2, \mathbb{Z}))$. □

Remarque 8.4.7. — Le groupe dérivé de $\mathrm{SL}(2, \mathbb{Z})$ est engendré par

$$[S, T] = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} \qquad \text{et} \qquad [S, T^{-1}] = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

4. D'après le troisième théorème de Sylow le groupe $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ possède un ou trois 2-Sylow ; notons qu'un tel 2-Sylow est d'ordre 8. Soit K un sous-groupe d'ordre 8 dans $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$. Les matrices de K sont annulées par le polynôme $X^8 - 1$ qui est à racines simples en caractéristique 3 (ses racines sont les éléments non nuls du corps $\mathbb{F}_9$). Une matrice M de K est donc diagonalisable, et de polynôme caractéristique $X^2 - (\operatorname{tr} M)X + 1$. Si $\operatorname{tr} M = \pm 1$, nous avons une racine double, car sur $\mathbb{Z}/3\mathbb{Z}$ nous avons $X^2 - X + 1 = (X+1)^2$ et $X^2 + X + 1 = (X-1)^2$. Dans ce cas $M = \pm \mathrm{id}$. Sinon $\operatorname{tr} M = 0$ et il y a exactement 6 matrices de trace nulle dans $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$. Ainsi $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ admet un seul sous-groupe d'ordre 8, c'est un 2-Sylow qui est distingué. On peut vérifier qu'il est non abélien et contient un élément d'ordre 2 central, il est donc isomorphe à $\mathbb{H}_8$.

Définition 8.4.2

Soit $k \geq 2$. Un sous-groupe de $\mathrm{SL}(k, \mathbb{Z})$ est un sous-groupe de congruence s'il contient le noyau du morphisme de réduction

$$\mathrm{SL}(k, \mathbb{Z}) \to \mathrm{SL}\left(k, \mathbb{Z}/n\mathbb{Z}\right)$$

(qui est surjectif) pour un certain $n \in \mathbb{Z}^+$.

Comme dans le cas $k = 2$ tout sous-groupe de congruence de $\mathrm{SL}(k, \mathbb{Z})$ est d'indice fini. Le groupe $\mathrm{SL}(2, \mathbb{Z})$ contient des sous-groupes d'indice fini qui ne sont pas des groupes de congruence. En fait la plupart des sous-groupes d'indice fini de $\mathrm{SL}(2, \mathbb{Z})$ ne sont pas des groupes de congruence : parmi les sous-groupes d'indice n de $\mathrm{SL}(2, \mathbb{Z})$ la proportion des groupes de congruence tend vers 0 lorsque n tend vers $+\infty$. Par contre dès que $n \geq 3$ les sous-groupes d'indice fini de $\mathrm{SL}(n, \mathbb{Z})$ sont des sous-groupes de congruence (c'est un théorème dû à Bass, Lazard, Serre et Mennicke).

8.4.6. Sous-groupes d'indice fini de $\mathrm{SL}(2, \mathbb{Z})$ qui ne sont pas des sous-groupes de congruence. — L'existence de sous-groupes d'indice fini de $\mathrm{SL}(2, \mathbb{Z})$ qui ne sont pas des sous-groupes de congruence a été annoncée par Klein dès 1879. Les premiers exemples apparaissent en 1887 dans des articles (indépendants) de Fricke et Pick. Nous n'allons pas présenter leur construction ici. La construction que nous allons présenter est une application du Théorème de Jordan-Hölder. Elle nécessite de faire quelques rappels.

Soit G un groupe ; notons e son élément neutre. Nous appelons *suite de composition* de G toute suite finie $(\mathrm{G}_0, \mathrm{G}_1, \ldots, \mathrm{G}_r)$ de sous-groupes de G telle que

- $\mathrm{G} = \mathrm{G}_0 \supseteq \mathrm{G}_1 \supseteq \ldots \supseteq \mathrm{G}_r = \{e\}$,
- G_{i+1} soit un sous-groupe normal de G_i pour tout $0 \leq i \leq r-1$.

Les quotients $\mathrm{G}_i/\mathrm{G}_{i+1}$ sont appelés les *quotients de la suite*.

Soient $\Sigma_1 = (\mathrm{G}_0, \mathrm{G}_1, \ldots, \mathrm{G}_r)$ et $\Sigma_2 = (\mathrm{H}_0, \mathrm{H}_1, \ldots, \mathrm{H}_s)$ deux suites de composition de G. On dit que Σ_2 est un *raffinement* de Σ_1, ou encore que Σ_2 est plus *fine* que Σ_1, si Σ_1 est extraite de Σ_2, *i.e.* s'il existe des indices $0 = j(0) < j(1) < \ldots < j(r) = s$ tels que $\mathrm{G}_i = \mathrm{H}_{j(i)}$ pour tout $1 \leq i \leq r-1$. Les suites Σ_1 et Σ_2 sont *équivalentes* si $r = s$ et s'il existe une permutation σ de l'ensemble $\{0, 1, \ldots, r-1\}$ telle que pour tout $0 \leq i \leq r-1$, le quotient $\mathrm{G}_i/\mathrm{G}_{i+1}$ soit isomorphe au quotient $\mathrm{H}_{\sigma(i)}/\mathrm{H}_{\sigma(i)+1}$. Soit $\Sigma = (\mathrm{G}_0, \mathrm{G}_1, \ldots, \mathrm{G}_r)$ une suite de composition de G. Les trois conditions suivantes sont équivalentes :

a) Σ est strictement décroissante et n'admet pas d'autre raffinement strictement décroissant qu'elle-même ;

b) les quotients de Σ sont tous des groupes simples ;

c) pour tout $0 \leq i \leq r-1$, le groupe G_{i+1} est un sous-groupe distingué maximal de G_i (c'est-à-dire un élément maximal, relativement à l'inclusion, de l'ensemble des sous-groupes propres distingués de G_i).

Nous appelons *suite de Jordan-Hölder* une suite de composition possédant les propriétés équivalentes a) à c).

Énonçons sans démonstration les quelques faits suivants :

- ◇ Pour tout groupe G, la suite $(\mathrm{G}, \{e\})$ est une suite de composition. C'est une suite de Jordan-Hölder si et seulement si G est simple.
- ◇ $\mathfrak{S}_3 \supset \mathcal{A}_3 \supset \{e\}$ est une suite de Jordan-Hölder.
- ◇ Théorème de raffinement de Schreier : pour deux suites de composition d'un même groupe, il existe toujours un raffinement de la première et un raffinement de la seconde qui sont équivalents. Ainsi si un groupe admet une suite de Jordan-Hölder, toute suite de composition strictement décroissante de ce groupe admet un raffinement qui est une suite de Jordan-Hölder.
- ◇ Si un groupe résoluble G admet une suite de Jordan-Hölder, chaque groupe quotient de cette suite est à la fois simple et résoluble, donc est cyclique d'ordre premier, et G est donc fini. En particulier, un groupe abélien infini n'admet pas de suite de Jordan-Hölder.
- ◇ Tout groupe fini admet une suite de Jordan-Hölder.
- ◇ Théorème de Jordan-Hölder : deux suites de Jordan-Hölder d'un même groupe sont toujours équivalentes.

Lemme 8.4.6: [Con]

Soit H un groupe fini simple. Soient G_1, G_2, …, G_k des groupes finis non triviaux. Si pour tout $1 \leq i \leq k$ le groupe H n'est le quotient d'aucune suite de Jordan-Hölder de G_i, alors H n'est le quotient d'aucune suite de Jordan-Hölder de $\mathrm{G}_1 \times \mathrm{G}_2 \times \ldots \mathrm{G}_k$.

Théorème 8.4.7

Soit $k \geq 6$. Pour tout $n \geq 2$ le groupe alterné $\mathcal{A}_k$ n'est pas un quotient de $\mathrm{SL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$.

Remarque 8.4.8. — La borne $n \geq 6$ est optimale ; en effet

- ◇ $\mathcal{A}_3$ est isomorphe au quotient de $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ par son 2-Sylow distingué ;
- ◇ $\mathcal{A}_4$ et $\mathrm{PSL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ sont isomorphes (Théorème 7.7.4) ;
- ◇ $\mathcal{A}_5$ et $\mathrm{PSL}\left(2, \mathbb{Z}/5\mathbb{Z}\right)$ sont isomorphes (Théorème 7.7.4).

Démonstration. — Écrivons n sous la forme $n = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$, les p_i désignant des nombres premiers. Le théorème des restes chinois assure que

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{m} \mathbb{Z}/p_i^{r_i}\mathbb{Z}.$$

Alors

$$\mathrm{SL}\Big(2, \mathbb{Z}/n\mathbb{Z}\Big) \simeq \prod_{i=1}^{m} \mathrm{SL}\Big(2, \mathbb{Z}/p_i^{r_i}\mathbb{Z}\Big).$$

Le Lemme 8.4.6 assure qu'il suffit de montrer que $\mathcal{A}_k$, $k \geq 6$,n'est pas un facteur de composition de $\mathrm{SL}\Big(2, \mathbb{Z}/p^r\mathbb{Z}\Big)$ pour tout p premier.

Considérons le morphisme de réduction

$$\mathrm{SL}\Big(2, \mathbb{Z}/p^r\mathbb{Z}\Big) \to \mathrm{SL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$$

qui est surjectif. Désignons par K son noyau. Nous avons la suite de composition suivante

$$\{\mathrm{id} \bmod p^r\} \lhd \mathrm{K} \lhd \mathrm{SL}\Big(2, \mathbb{Z}/p^r\mathbb{Z}\Big)$$

dont les facteurs sont modulo isomorphisme K et $\mathrm{SL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$. Il en résulte que les facteurs de composition de $\mathrm{SL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$ s'obtiennent à partir des facteurs de composition de K et de $\mathrm{SL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$.

Déterminons les facteurs de composition de K. Le groupe

$$\mathrm{K} = \Big\{M \in \mathrm{SL}\Big(2, \mathbb{Z}/p^r\mathbb{Z}\Big) \mid M \equiv \mathrm{id} \bmod p\Big\}$$

est un p-groupe ; en effet si $M \equiv \mathrm{id} \bmod p$ alors par récurrence $M^{p^k} \equiv \mathrm{id} \bmod p^{k+1}$ pour tout $k \geq 0$ d'où $M^{p^{r-1}} \equiv \mathrm{id} \bmod p^r$. Ainsi tous les éléments de K sont d'ordre une puissance de p. Or un groupe fini dont tous les éléments sont d'ordre une puissance de p est un p-groupe d'après Cauchy dont K est un p-groupe [5]. Les facteurs de composition d'un p-groupe fini, donc de K, sont tous cycliques d'ordre p.

Déterminons désormais les facteurs de composition de $\mathrm{SL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$.

— Supposons $p \geq 5$; le groupe $\mathrm{PSL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big) = \mathrm{SL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)/\{\pm \mathrm{id}\}$ est simple pour $p \geq 5$ donc

$$\{\mathrm{id}\} \lhd \{\pm \mathrm{id}\} \lhd \mathrm{SL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$$

est une suite de composition de $\mathrm{SL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$ et les facteurs de composition de $\mathrm{SL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$ sont $\mathbb{Z}/2\mathbb{Z}$ et $\mathrm{PSL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$.

5. Notons que l'ordre de K peut être calculé mais que nous n'en avons pas besoin.

— Supposons maintenant $p < 5$. Comme

$$\mathrm{SL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big) = \mathrm{GL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big) \simeq \mathfrak{S}_3 \qquad \text{et} \qquad \mathrm{SL}\Big(2, \mathbb{Z}/3\mathbb{Z}\Big)\Big/\{\pm \mathrm{id}\} \simeq \mathcal{A}_4$$

les facteurs de composition de $\mathrm{SL}\Big(2, \mathbb{Z}/2\mathbb{Z}\Big)$ et $\mathrm{SL}\Big(2, \mathbb{Z}/3\mathbb{Z}\Big)$ sont cycliques d'ordre 2 ou 3.

Finalement si $p \leq 3$, tout facteur de composition de $\mathrm{SL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$ est cyclique et pour tout premier $p \geq 5$ le groupe $\mathrm{SL}\Big(2, \mathbb{Z}/p^r\mathbb{Z}\Big)$ a un unique facteur de composition non abélien : $\mathrm{PSL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$. Ainsi si $\mathcal{A}_k$, $k \geq 6$, était un facteur de composition de $\mathrm{SL}\Big(2, \mathbb{Z}/p^r\mathbb{Z}\Big)$, alors $\mathcal{A}_k$ serait isomorphe à un $\mathrm{PSL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)$ pour un certain $p \geq 5$. Or $\Big|\mathrm{PSL}\Big(2, \mathbb{Z}/p\mathbb{Z}\Big)\Big| = \frac{(p^2-1)p}{2}$ et $|\mathcal{A}_k| = \frac{k!}{2}$ donc on se ramène à la question suivante : quand a-t-on

$$k! = (p-1)p(p+1) \tag{8.4.8}$$

Si $k < p$, alors $k!$ n'est pas divisble par p donc (8.4.8) n'a pas de solution si $k < p$.

Si $k = p$, alors (8.4.8) se réécrit $p! = (p-1)!p(p+1)$ soit $(p-2)! = p+1$ qui a une unique solution $p = 5 (= k)$.

Si $k = p+1$, alors (8.4.8) se réécrit $(p+1)! = (p-1)p(p+1)$ soit $(p-2)! = 1$ d'où $p = 3$: contradiction avec le fait que $p \geq 5$.

Si $k \geq p+2$, alors (8.4.8) n'a pas de solution.

Finalement (8.4.8) a une seule solution : $p = k = 5$ (en effet $\mathrm{PSL}(2, \mathbb{F}_5) \simeq \mathcal{A}_5$, Théorème 7.7.4) et dès que $k \geq 6$ le groupe alterné $\mathcal{A}_k$ n'est pas un quotient de $\mathrm{SL}\Big(2, \mathbb{Z}/n\mathbb{Z}\Big)$ et ce pour tout $n \geq 2$. □

Alors que le Théorème 8.4.7 assure que la plupart des $\mathcal{A}_n$ ne sont pas des quotients de $\mathrm{SL}\Big(2, \mathbb{Z}/n\mathbb{Z}\Big)$ l'énoncé suivant assure que la plupart des $\mathcal{A}_n$ sont des quotients de $\mathrm{SL}(2, \mathbb{Z})$:

Théorème 8.4.8

Dès que $n \geq 9$ le groupe alterné $\mathcal{A}_n$ est un quotient de $\mathrm{SL}(2, \mathbb{Z})$.

Exemple 8.4.5. — Le groupe alterné $\mathcal{A}_9$ est engendré par

$$(1\ 4)(2\ 9)(3\ 7)(5\ 6) \qquad \text{et} \qquad (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)$$

qui sont d'ordre 2 et 3 respectivement. Un morphisme surjectif de $\mathrm{SL}(2, \mathbb{Z})$ dans $\mathcal{A}_9$ est la composée de la projection canonique $\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{PSL}(2, \mathbb{Z})$ et de

$$\mathrm{PSL}(2, \mathbb{Z}) \to \mathcal{A}_9 \qquad \begin{cases} \overline{S} \to (1\ 4)(2\ 9)(3\ 7)(5\ 6) \\ \overline{ST} \to (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9) \end{cases}$$

Proposition 8.4.2

Dès que $n \geq 9$ il existe un morphisme surjectif de $\mathrm{PSL}(2, \mathbb{Z})$ dans le groupe alterné $\mathcal{A}_n$.

Lemme 8.4.7

[[**DW71**]] Dès que $n \geq 9$ le groupe alterné $\mathcal{A}_n$ est engendré par un élément d'ordre 2 et un élément d'ordre 3.

Démonstration de la Proposition 8.4.2. — Elle découle du Lemme 8.4.7 et du Théorème 8.4.2. □

Démonstration du Théorème 8.4.8. — On compose la projection canonique

$$\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{PSL}(2, \mathbb{Z})$$

avec le morphisme de la Proposition 8.4.2. □

8.4.7. Classe de conjugaison dans $\mathrm{SL}(2, \mathbb{Z})$. —

8.4.8. Les groupes $\mathrm{SL}(n, \mathbb{Z})$. —

CHAPITRE 9

ACTIONS DE GROUPES ET ALGÈBRE LINÉAIRE

Les actions de groupes sur des espaces de matrices illustrent une méthode uniforme pour les problèmes de classification rencontrés en mathématiques. En effet, un groupe, en agissant, partitionne en orbites l'ensemble sur lequel il agit. La nature de la classification dépend du choix du groupe agissant :

- ⋄ groupe linéaire pour des classifications linéaires ;
- ⋄ groupe affine pour des classifications affines ;
- ⋄ groupe $\mathrm{O}(n, \mathbb{R})$ pour des classifications euclidiennes ;
- ⋄ groupe projectif pour les classifications projectives, avec le groupe projectif.

Chaque orbite se voit munie d'un classifiant (invariant total) et souvent d'une matrice de forme normale. Dans les espaces de matrices, le problème de classification provient principalement du problème de changement de base. En effet, les matrices sont utilisées pour coder des objets (applications linéaires, endomorphismes, formes quadratiques, représentations), mais ce codage dépend de façon drastique d'une base ; il faut alors gérer le problème de changement de base.

Dans un premier temps, nous cherchons à décrire les actions, décrire les classifiants, trouver des algorithmes pour calculer les classifiants et déterminer les formes normales. Dans un second temps, nous allons pouvoir, si le corps est $\mathbb{R}$ ou $\mathbb{C}$, mettre une topologie sur l'espace de matrices, puis, chercher à décrire les adhérences d'orbites. Si le corps est fini, on peut chercher les cardinaux de chaque orbite. Enfin, dans un troisième temps, nous pouvons nous intéresser à des problèmes de descente, c'est-à-dire comment passer de la classification sur un corps $\mathbb{L}$ à un sous-corps $\Bbbk$.

Le premier exemple édifiant que tout le monde peut comprendre est l'action de Steinitz. Une même application linéaire va être codée dans deux paires de bases différentes, $(\mathcal{B}, \mathcal{C})$ et $(\mathcal{B}', \mathcal{C}')$, et les matrices respectives vont vérifier $A' = P^{-1}AQ$ où P, resp. Q, désigne la matrice de passage de $\mathcal{C}$ à $\mathcal{C}'$, resp. de $\mathcal{B}$ à $\mathcal{B}'$. Le classifiant est le rang, qui se calcule grâce au pivot de Gauss sur les lignes (à gauche) et sur les colonnes (à droite). La matrice de forme normale de rang r est la matrice avec r "1" sur sa diagonale, et des zéros ailleurs. Il n'y a ici pas d'obstruction de descente, puisque le rang est indépendant du corps de base (le rang est égal

à la taille du plus grand mineur non nul), et donc deux matrices sur $\Bbbk$ sont équivalentes sur $\mathbb{L}$ si et seulement si elles le sont sur $\Bbbk$. De plus, si $\mathcal{O}_r$ est l'orbite des matrices de rang r sur $\mathbb{R}$ ou $\mathbb{C}$, alors son adhérence est donnée par la réunion des $\mathcal{O}_{r'}$, où $0 \leq r' \leq r$. Le cardinal d'une orbite sur un corps fini est un exercice qui utilise l'ordre du groupe linéaire et l'ordre d'un stabilisateur. Nous pouvons traiter le cas de l'action par conjugaison de $\mathrm{GL}(n, \mathbb{C})$ sur les matrices diagonalisables sur $\mathbb{C}$, et même sur les matrices nilpotentes. Dans le second cas, nous tombons, pour les formes normales, sur les réduites de Jordan. Le premier cas a sa petite spécificité : les orbites sont toutes fermées et cela constitue même une caractérisation des matrices diagonalisables. Dans tous les cas, nous n'avons pas d'obstruction de descente : deux matrices carrées sur $\Bbbk$ sont $\mathbb{L}$-semblables si et seulement si elles sont $\Bbbk$-semblables. Nous pouvons ensuite traiter le cas de l'action de $\mathrm{GL}(n, \Bbbk)$ par congruence sur l'espace $\mathrm{S}(n, \Bbbk)$ des matrices symétriques. Les choses dépendent de façon drastique du corps de base. En général sont traités les cas où le corps de base est $\mathbb{C}$ (dans ce contexte l'invariant est le rang), $\mathbb{R}$ (dans ce contexte l'invariant est la signature par le théorème de Sylvester), et $\mathbb{F}_q$ (dans ce contexte l'invariant est le discriminant). L'algorithme dominant est la fameuse méthode de Gauss. Il y a aussi l'action à gauche de $\mathrm{GL}(n, \Bbbk)$ sur l'espace $\mathrm{M}((n, m), \Bbbk)$. En effet quand on veut résoudre le système linéaire $AX = Y$, on intervient par combinaisons linéaires sur les lignes et donc, uniquement à gauche sur $A \in \mathrm{M}((n, m), \Bbbk)$. On effectue un algorithme de pivot, mais uniquement à gauche (le pivot à droite correspondrait à des changements de variables). L'action $P \cdot A = PA$ doit être comprise. Les formes normales sont alors les matrices échelonnées réduites : pour tout A, il existe une unique matrice échelonnée réduite E telle que $PA = E$ pour un P dans $\mathrm{GL}(n, \Bbbk)$.

Se donner une représentation complexe d'un groupe fini G d'ordre n revient à se donner n matrices $A_g \in \mathrm{M}(m, \mathbb{C})$, $g \in \mathrm{G}$, qui vérifient les mêmes relations que dans le groupe : $gh = k$ implique $A_g A_h = A_k$. On peut se demander s'il existe une matrice de passage P , si les PA_gP^{-1} sont réelles pour tout g. Un superbe résultat dans le cas d'une représentation irréductible est donné par l'indicatrice de Frobenius-Schur.

9.1. Action par translation du groupe linéaire : pivot de Gauss

9.2. Action par translation des groupes orthogonal et unitaire

9.3. Actions de Steinitz : matrices équivalentes

9.3.1. Théorème du rang. — Le théorème du rang, corollaire de la base incomplète (§9.3.3, assure que deux matrices sont équivalentes si et seulement si elles ont même rang. Nous revisitons cet énoncé en terme d'invariant d'action de groupe.

Soit $\Bbbk$ un corps. Considérons une application linéaire $\varphi \colon \Bbbk^n \to \Bbbk^m$. Soient $\mathcal{B}$ et $\mathcal{C}$ des bases de $\Bbbk^n$ et $\Bbbk^m$ respectivement. Notons $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ la matrice de φ dans les bases $\mathcal{B}$ et $\mathcal{C}$ (a_{ij} est la $i$ème coordonnée de $\varphi(e_j)$ dans la base $\mathcal{C}$). C'est un élément du $\Bbbk$-espace vectoriel $\mathrm{M}((m, n), \Bbbk)$ des matrices de taille $m \times n$ à coefficients dans $\Bbbk$.

Il est tentant d'associer un outil pratique (la matrice) à un objet théorique (l'application linéaire) mais cette association pose un problème : le choix des bases $\mathcal{B}$ et $\mathcal{C}$. Ceci nous amène à introduire une relation :

Définition 9.3.1

Deux matrices A et B sont *équivalentes* si et seulement si il existe P et Q matrices inversibles telles que $B = PAQ^{-1}$.

Rappelons que si $\varphi\colon \Bbbk^n \to \Bbbk^m$ est une application linéaire et si A est la matrice de φ dans les bases $\mathcal{B}$ et $\mathcal{C}$ de $\Bbbk^n$ et $\Bbbk^m$ respectivement, alors le *rang* de A, noté $\operatorname{rg} A$, est défini par :

$$\operatorname{rg} A = \operatorname{rg} \varphi = \dim \operatorname{im} \varphi = \dim E$$

où E est l'espace vectoriel engendré par les colonnes (ou les lignes) de A.

Théorème 9.3.1: (Théorème du rang)

Les matrices A et B deux élements de $\mathrm{M}((m,n),\Bbbk)$ sont équivalentes si et seulement si $\operatorname{rg} A = \operatorname{rg} B$.

Corollaire 9.3.1

Tout hyperplan de $\mathrm{M}(n,\Bbbk)$ contient au moins une matrice inversible.

Lemme 9.3.1

Soit A un élément de $\mathrm{M}(n,\Bbbk)$. On note f_A la forme linéaire définie pour tout $M \in \mathrm{M}(n,\Bbbk)$ par $f_A(M) = \operatorname{tr}(AM)$. L'application

$$f\colon \mathrm{M}(n,\Bbbk) \to \mathrm{M}(n,\Bbbk)^*, \qquad A \mapsto f_A$$

est un isomorphisme.

Démonstration. — Désignons par $(E_{ij})_{1\le i,\, j\le n}$ la base canonique de $\mathrm{M}(n,\Bbbk)$. Rappelons que

$$\forall\, 1 \le i,\, j,\, k,\, \ell \le n \quad E_{ij}E_{k\ell} = \delta_{jk}E_{i\ell}.$$

L'application f est linéaire. Pour des raisons de dimension il suffit de montrer qu'elle est injective. Soit $A = (a_{ij})_{1\le i,\, j\le n}$ telle que $f_A = 0$. Alors pour tout $1 \le i,\, j \le n$ nous avons

$$0 = \operatorname{tr}\Big(AE_{i_0j_0}\Big) = \operatorname{tr}\Big(\sum_{1\le i,\, j\le n} a_{ij}E_{ij}E_{i_0j_0}\Big) = \operatorname{tr}\Big(\sum_{i=1}^{n} a_{ii_0}E_{ii_0}E_{i_0j_0}\Big) = \sum_{i=1}^{n} a_{ii_0}\operatorname{tr}\Big(E_{ij_0}\Big) = a_{j_0i_0}$$

Il en résulte que $A = 0$. □

Démonstration. — Soit H un hyperplan de $\mathrm{M}(n,\Bbbk)$; c'est le noyau d'une forme linéaire non nulle φ. Il existe $A \in \mathrm{M}(n,\Bbbk)$ non nulle telle que pour toute matrice $M \in \mathrm{M}(n,\Bbbk)$ nous ayons

$\varphi(M) = \mathrm{tr}(AM)$ (Lemme 9.3.1). Nous sommes donc ramenés à montrer qu'il existe M inversible telle que AM soit de trace nulle. Notons $r \geq 1$ le rang de A. Il existe P et Q dans $\mathrm{GL}(n, \Bbbk)$ tels que $PAQ^{-1} = \mathrm{id}_{r,0} = \left(\begin{array}{c|c} \mathrm{id}_r & 0 \\ \hline 0 & 0 \end{array}\right)$. Ainsi pour tout $M \in \mathrm{M}(n, \Bbbk)$

$$\mathrm{tr}(AM) = \mathrm{tr}(P^{-1}\mathrm{id}_{r,0}QM) = \mathrm{tr}(\mathrm{id}_{r,0}QMP^{-1});$$

il suffit donc de trouver une matrice inversible Y telle que $\mathrm{tr}(\mathrm{id}_{r,0}Y) = 0$, on pose alors $M = Q^{-1}YP$. La matrice $Y = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & \ddots & \ddots & \vdots & 0 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$ convient car la diagonale de $\mathrm{id}_{r,0}Y$ est nulle. $\square$

Rappelons que le groupe $\mathrm{GL}(n, \Bbbk) \times \mathrm{GL}(p, \Bbbk)$ agit sur $\mathrm{M}((n,p), \Bbbk)$

$$\mathrm{GL}(n, \Bbbk) \times \mathrm{GL}(p, \Bbbk) \times \mathrm{M}((n,p), \Bbbk) \to \mathrm{M}(n, \Bbbk), \qquad ((P,Q), M) \mapsto PMQ^{-1}$$

et que deux matrices conjuguées sous cette action sont dites r-équivalentes. Deux matrices sont r-équivalentes si et seulement si elles représentent la même application linéaire dans deux paires de bases différentes.

Théorème 9.3.2

Considérons l'action de Steinitz :

$$\mathrm{GL}(n, \Bbbk) \times \mathrm{GL}(p, \Bbbk) \times \mathrm{M}((n,p), \Bbbk) \to \mathrm{M}(n, \Bbbk), \qquad ((P,Q), M) \mapsto PMQ^{-1}$$

Soit $1 \leq r \leq \min(n,p)$ un entier. L'orbite de $\mathrm{id}_{r,0} = \left(\begin{array}{c|c} \mathrm{id}_r & 0 \\ \hline 0 & 0 \end{array}\right)$ est l'ensemble des matrices de rang r.

Démonstration. — Soit $r \in [\![1, \min(n,p)]\!]$. Notons $\mathrm{id}_r \in \mathrm{M}(r, \Bbbk)$ la matrice identité, $\mathrm{id}_{r,0} \in \mathrm{M}((n,p), \Bbbk)$ la matrice décrite par blocs de la manière suivante $\mathrm{id}_{r,0} = \left(\begin{array}{c|c} \mathrm{id}_r & 0 \\ \hline 0 & 0 \end{array}\right)$ et $\mathcal{O}_r$ l'orbite de $\mathrm{id}_{r,0}$ sous l'action de Steinitz. Désignons par $\varphi_r \colon \Bbbk^p \to \Bbbk^n$ l'application linéaire dont la matrice dans les bases canoniques est id_r. On vérifie que $\mathrm{rg}(\varphi_r) = \dim \varphi_r(\Bbbk^p) = r$.

Si $A \in \mathrm{M}((n,p), \Bbbk)$ est un élément de $\mathcal{O}_r$, alors il existe $P \in \mathrm{M}(n, \Bbbk)$ et $Q \in \mathrm{M}(p, \Bbbk)$ telles que $A = P\mathrm{id}_{r,0}Q^{-1}$. La matrice A représente donc φ_r dans deux autres bases. En particulier A et $\mathrm{id}_{r,0}$ ont même rang.

Soit $A \in \mathrm{M}((n,p),\Bbbk)$ et $f\colon \Bbbk^p \to \Bbbk^n$ l'application linéaire qu'elle représente dans les bases canoniques. Soit $s \in \mathbb{N}$ tel que $\dim \ker f = p - s$. On note $\{e_{s+1}, \cdots, e_p\}$ une base de $\ker f$ que l'on complète pour obtenir une base $\mathcal{E} = \{e_1, \cdots, e_s, e_{s+1}, \cdots e_p\}$ de $\Bbbk^p$. Pour tout $i \in [\![1,s]\!]$, on pose $f_i = f(e_i)$. La famille $\{f_1, \cdots f_s\}$ est une famille libre. En effet, si $(\alpha_1, \cdots, \alpha_s) \in \Bbbk^s$ est tel que $\sum_{i=1}^{s} \alpha_i f_i = 0$. Alors $\sum_{i=1}^{s} \alpha_i f(e_i) = 0$. Soit encore $f\left(\sum_{i=1}^{s} \alpha_i e_i\right) = 0$. C'est-à-dire que $\sum_{i=1}^{s} \alpha_i e_i \in \ker f$ ce qui n'est possible, par construction de la base $\mathcal{E}$, que si on a $\sum_{i=1}^{s} \alpha_i e_i = 0$ ce qui implique que pour tout $i \in [\![1,s]\!]$ on a $\alpha_i = 0$. La famille $\{f_1, \cdots, f_s\}$ est donc libre et elle se complète en une base $\mathcal{F} = \{f_1, \cdots, f_s, f_{s+1}, \cdots, f_n\}$ de $\Bbbk^n$. Pour tout $i \in [\![1,s]\!]$, $f(e_i) = f_i$ et pour tout $i \in [\![s+1,p]\!]$, $f(e_i) = 0$, ainsi la matrice de f dans les bases $\mathcal{E}$ et $\mathcal{F}$ est C_s. On en déduit qu'il existe $P \in \mathrm{M}(n,\Bbbk)$ et $Q \in \mathrm{M}(p,\Bbbk)$ telles que $A = PC_sQ^{-1}$. La matrice A est de rang s et elle appartient à $\mathcal{O}_s$.

En conclusion, l'orbite de C_s est l'ensemble des matrices de rang s. □

Par suite le théorème du rang peut se reformuler comme suit :

Corollaire 9.3.2

Considérons l'action de Steinitz :

$$\mathrm{GL}(n,\Bbbk) \times \mathrm{GL}(p,\Bbbk) \times \mathrm{M}((n,p),\Bbbk) \to \mathrm{M}(n,\Bbbk), \qquad ((P,Q),M) \mapsto PMQ^{-1}$$

Soient A et B dans $\mathrm{M}_{m,n}(\Bbbk)$. Alors $\mathcal{O}_A = \mathcal{O}_B$ si et seulement si A et B sont r-équivalentes.

Une autre conséquence est la suivante :

Corollaire 9.3.3

Considérons l'action de Steinitz :

$$\mathrm{GL}(n,\Bbbk) \times \mathrm{GL}(p,\Bbbk) \times \mathrm{M}((n,p),\Bbbk) \to \mathrm{M}(n,\Bbbk), \qquad ((P,Q),M) \mapsto PMQ^{-1}$$

Le nombre d'orbites pour cette action est $\min(n+1, p+1)$.

Considérons l'application

$$\phi_A\colon \mathrm{G} \to \mathcal{O}_A, \qquad g \mapsto g \cdot A.$$

Elle est par définition surjective. Nous pouvons nous demander si elle est injective. Soient g et g' dans G nous avons

$$\begin{aligned} \phi_A(g') = \phi_A(g) \quad &\Leftrightarrow \quad g' \cdot A = g \cdot A \Leftrightarrow g^{-1}(g' \cdot A) = g^{-1}(g \cdot A) \\ &\Leftrightarrow \quad (g^{-1}g') \cdot A = (g^{-1}g) \cdot A \Leftrightarrow (g^{-1}g') \cdot A = A \end{aligned}$$

Nous sommes donc amenés à nous intéresser au stabilisateur de A sous l'action de G :

$$\begin{aligned}\mathrm{St}(A) &= \{h \in \mathrm{G} \,|\, h \cdot A = A\} \\ &= \{(P,Q) \in \mathrm{GL}(m,\Bbbk) \times \mathrm{GL}(n,\Bbbk) \,|\, PAQ^{-1} = A\}\end{aligned}$$

C'est un sous-groupe de G en général non distingué. Ainsi

$$\begin{aligned}\phi_A(g') = \phi_A(g) &\iff g^{-1}g' \in \mathrm{St}(A) \\ &\iff g' \in g\mathrm{St}(A) \\ &\iff g \text{ et } g' \text{ appartiennent à la même classe } \overline{g} \in {}^{\mathrm{G}}\!/_{\mathrm{St}(A)}.\end{aligned}$$

Ainsi $\phi_A(g') = \phi_A(g)$ si et seulement si $\overline{g} = \overline{g'}$ et nous ne pouvons donc pas affirmer que ϕ_A est injective.

Théorème 9.3.3

Posons $\mathrm{G} = \mathrm{GL}(m,\Bbbk) \times \mathrm{GL}(n,\Bbbk)$. Considérons

$$\mathrm{G} \times \mathrm{M}((m,n),\Bbbk) \to \mathrm{M}((m,n),\Bbbk), \qquad (P,Q,A) \mapsto (P,Q) \cdot A = PAQ^{-1}.$$

Soit ϕ_A l'application définie par

$$\phi_A \colon \mathrm{G} \to \mathcal{O}_A, \qquad g \mapsto g \cdot A.$$

Il existe une unique application $\overline{\phi_A} \colon {}^{\mathrm{G}}\!/_{\mathrm{St}(A)} \to \mathcal{O}_A$ telle que le diagramme

$$\begin{tikzcd} \mathrm{G} \arrow[r, "\phi_A"] \arrow[d, "\pi"'] & \mathcal{O}_A \\ {}^{\mathrm{G}}\!/_{\mathrm{St}(A)} \arrow[ur, "\overline{\phi_A}"'] & \end{tikzcd}$$

commute.
De plus $\overline{\phi_A}$ est bijective.

Remarque 9.3.1. — L'application $\overline{\phi_A}$ est une bijection mais pas un isomorphisme de groupes ; en effet, d'une part $\mathcal{O}_A$ n'est pas nécessairement un groupe, d'autre part $\mathrm{St}(A)$ n'est pas nécessairement un sous-groupe distingué de G.

Démonstration. — Supposons que g' appartienne à $\overline{g} = g\mathrm{St}(A)$. Il existe donc $h \in \mathrm{St}(A)$ tel que $g' = gh$. Ainsi

$$\phi_A(g') = g' \cdot A = (gh) \cdot A = g(h \cdot A) = g \cdot A = \phi_A(g)$$

i.e. $\phi_A(g')$ ne dépend pas de l'élément $g \in \overline{g}$. Nous pouvons donc bien définir $\overline{\phi_A}(\overline{g}) = \phi_A(g)$ et $\overline{\phi_A} \circ \pi = \phi_A$: le diagramme commute.

De plus

◇ $\overline{\phi_A}\left({}^{\mathrm{G}}\!/_{\mathrm{St}(A)}\right) = \phi_A(\mathrm{G})$ donc $\overline{\phi_A}$ est surjective ;

◇ et

$$\overline{\phi_A}(\overline{g}) = \overline{\phi_A}(\overline{g'}) \Rightarrow \phi_A(g) = \phi_A(g') \Rightarrow g = g'\mathrm{St}(A) \Rightarrow \overline{g} = \overline{g'}$$

donc $\overline{\phi_A}$ est injective.

Enfin $\overline{\phi_A}$ est clairement unique. □

Corollaire 9.3.4

Posons $\mathrm{G} = \mathrm{GL}(m, \Bbbk) \times \mathrm{GL}(n, \Bbbk)$. Considérons

$$\mathrm{G} \times \mathrm{M}((m,n), \Bbbk) \to \mathrm{M}((m,n), \Bbbk), \qquad (P, Q, A) \mapsto (P, Q) \cdot A = PAQ^{-1}.$$

Si $\Bbbk$ est un corps fini, alors

$$|\mathcal{O}_A| = \left|{}^{\mathrm{GL}(m,\Bbbk) \times \mathrm{GL}(n,\Bbbk)}\!/_{\mathrm{St}(A)}\right|.$$

Les éléments d'une même orbite ayant des propriétés similaires nous nous ramènerons souvent à une « forme normale pratique » de $\mathcal{O}_A$ comme par exemple $\mathrm{id}_{r,0} = \begin{pmatrix} \mathrm{id}_r & 0 \\ 0 & 0 \end{pmatrix}$ si $r = \mathrm{rg}A$.

Proposition 9.3.1

Soit $A \in \mathrm{M}((m,n), \Bbbk)$ de rang r. Alors

$$\mathrm{St}(A) = g\mathrm{St}(\mathrm{id}_{r,0})g^{-1} \simeq \mathrm{St}(\mathrm{id}_{r,0}).$$

Démonstration. — Puisque A est de rang r, il existe $g \in \mathrm{GL}(n, \Bbbk)$ telle que $A = g\mathrm{id}_{r,0}$. Par suite $\mathrm{St}(A) = \mathrm{St}(g\mathrm{id}_{r,0})$. Ainsi si h appartient à G_A, alors

$$h \cdot (g\mathrm{id}_{r,0}) = g\mathrm{id}_{r,0} \Leftrightarrow hg \cdot \mathrm{id}_{r,0} = g\mathrm{id}_{r,0} \Leftrightarrow g^{-1}hg \cdot \mathrm{id}_{r,0} = \mathrm{id}_{r,0} \Leftrightarrow h \in g\mathrm{St}(\mathrm{id}_{r,0})g^{-1}.$$

Il en résulte que $\mathrm{St}(A) = g\mathrm{St}(\mathrm{id}_{r,0})g^{-1}$.

Par ailleurs $g\mathrm{St}(\mathrm{id}_{r,0})g^{-1} \simeq \mathrm{St}(\mathrm{id}_{r,0})$ d'où l'énoncé. □

Autrement dit l'étude de $\mathrm{St}(A)$ se ramène à l'étude de $\mathrm{St}(\mathrm{id}_{r,0})$. Étudions donc $\mathrm{St}(\mathrm{id}_{r,0})$. Soit $(P,Q) = \left(\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}, \begin{pmatrix} \alpha' & \gamma' \\ \beta' & \delta' \end{pmatrix}\right)$ dans $\mathrm{St}(\mathrm{id}_{r,0})$; alors

$$\begin{aligned}
P\mathrm{id}_{r,0}Q^{-1} = \mathrm{id}_{r,0} &\iff \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\begin{pmatrix} \mathrm{id}_r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \alpha' & \gamma' \\ \beta' & \delta' \end{pmatrix}^{-1} = \begin{pmatrix} \mathrm{id}_r & 0 \\ 0 & 0 \end{pmatrix} \\
&\iff \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\begin{pmatrix} \mathrm{id}_r & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \mathrm{id}_r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \alpha' & \gamma' \\ \beta' & \delta' \end{pmatrix} \\
&\iff \begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix} = \begin{pmatrix} \alpha' & \gamma' \\ 0 & 0 \end{pmatrix} \\
&\iff \alpha = \alpha',\ \beta = 0,\ \gamma' = 0 \\
&\iff P = \begin{pmatrix} \alpha & \gamma \\ 0 & \delta \end{pmatrix},\ Q = \begin{pmatrix} \alpha & 0 \\ \beta' & \delta' \end{pmatrix}.
\end{aligned}$$

Notons que P appartient à $\mathrm{GL}(m,\Bbbk)$ et que $\det P = \det\alpha\det\delta$ donc α appartient à $\mathrm{GL}(r,\Bbbk)$ et δ appartient à $\mathrm{GL}(n-r,\Bbbk)$. La matrice γ appartient elle à $\mathrm{M}((r,n-r),\Bbbk)$. De même β' appartient à $\mathrm{M}((n-r,r),\Bbbk)$ et δ' à $\mathrm{GL}(n-r,\Bbbk)$. Le groupe $\mathrm{St}(\mathrm{id}_{r,0})$ s'écrit donc sous forme de produits directs et semi-directs de groupes classiques :

$$\begin{aligned}
\mathrm{St}(\mathrm{id}_{r,0}) &= \begin{pmatrix} \mathrm{GL}(r,\Bbbk) & \mathrm{M}((r,n-r),\Bbbk) \\ 0 & \mathrm{GL}(m-r,\Bbbk) \end{pmatrix}\begin{pmatrix} \mathrm{GL}(r,\Bbbk) & 0 \\ \mathrm{M}((n-r,r),\Bbbk) & \mathrm{GL}(n-r,\Bbbk) \end{pmatrix} \\
&= \mathrm{GL}(r,\Bbbk)\times\mathrm{GL}(m-r,\Bbbk)\times\mathrm{GL}(n-r,\Bbbk)\ltimes\Big(\mathrm{M}((r,m-r),\Bbbk)\oplus\mathrm{M}((n-r,r),\Bbbk)\Big)
\end{aligned}$$

9.3.2. Propriétés topologiques. — Soit $\Bbbk \in \{\mathbb{R}, \mathbb{C}\}$. Les espaces de matrices sur $\Bbbk$ sont munis de la topologie de $\mathbb{R}$-espace vectoriel normé. Les opérations $+$ et $\times$ (produit matriciel) font intervenir uniquement des polynômes en les variables et sont donc continues pour cette topologie.

Il est naturel d'étudier la topologie des orbites $\mathcal{O}_r$ des matrices de rang r. Elles ne sont en général ni ouvertes, ni fermées mais leur adhérence est donnée par :

Proposition 9.3.2

Soient m et n deux entiers. Pour $0 \leq r \leq \min(m,n)$ nous notons $\mathcal{O}_r$ l'orbite des matrices $m \times n$ de rang r à coefficients dans $\Bbbk$. Alors l'adhérence de l'ensemble des matrices de rang r de $\mathrm{M}((n,m),\Bbbk)$ est l'ensemble des matrices de rang $\leq r$:

$$\overline{\mathcal{O}_r} = \bigcup_{0 \leq k \leq r} \mathcal{O}_k \quad \text{(réunion disjointe)}$$

Démonstration. — Avant de démontrer cette égalité introduisons quelques notations. Étant données deux parties $I \subset \{1, 2, \ldots, m\}$ et $J \subset \{1, 2, \ldots, n\}$ de même cardinal, le mineur d'indice (I,J) est l'application

$$\Delta_{I,J} \colon \mathrm{M}((m,n),\Bbbk) \to \Bbbk, \qquad (a_{i,j})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \mapsto \det(a_{i,j})_{\substack{i \in I \\ j \in J}}$$

Un théorème important d'algèbre linéaire caractérise le rang d'une matrice A comme l'ordre du plus grand mineur non nul

$$\operatorname{rg} A = \max\big\{r \in \mathbb{N},\ \exists\, I,\ \exists\, J,\ |I| = |J| = r \text{ et } \Delta_{I,J}(A) \neq 0\big\}.$$

Montrons d'abord que la réunion $\bigcup_{0 \leq k \leq r} \mathcal{O}_k$ des $\mathcal{O}_k$ $(0 \leq k \leq r)$ est un fermé de $\mathrm{M}((m,n),\Bbbk)$. Le rang d'une matrice A est au plus r si et seulement si tous ses mineurs d'ordre supérieur ou égaux à $r+1$ sont nuls (en fait, en utilisant le développement du déterminant par rapport à une colonne, on voit que les mineurs d'ordre $r+1$ suffisent). En d'autres termes

$$\bigcup_{0 \leq k \leq r} \mathcal{O}_k = \bigcap_{|I|=|J| \geq r+1} \Delta_{I,J}^{-1}(\{0\}).$$

Par continuité des fonctions $\Delta_{I,J}$ la partie $\bigcup_{0 \leq k \leq r} \mathcal{O}_k$ est fermée en tant qu'intersection de fermés.

Par construction $\mathcal{O}_r$ est inclus dans $\bigcup_{0 \leq k \leq r} \mathcal{O}_k$, qui est fermé, donc $\overline{\mathcal{O}_r}$ est inclus dans $\bigcup_{0 \leq k \leq r} \mathcal{O}_k$.

Réciproquement soit A une matrice de rang $k \leq r$. D'après le théorème du rang il existe P et Q inversibles telles que $A = P\mathrm{id}_k Q^{-1}$. Pour $\varepsilon \in \Bbbk$ on définit une matrice par blocs

$$A(\varepsilon) = P \begin{pmatrix} \mathrm{id}_k & 0 & 0 \\ 0 & \varepsilon \mathrm{id}_{r-k} 0 & \\ 0 & 0 & 0 \end{pmatrix} Q^{-1}.$$

La matrice $A(\varepsilon)$ dépend continûment de ε ; lorsque $\varepsilon \neq 0$, la matrice $A(\varepsilon)$ appartient à $\mathcal{O}_r$; pour $\varepsilon = 0$ on a : $A(0) = A$. Ainsi A appartient à l'adhérence de $\mathcal{O}_r$. Il vient : $\bigcup_{0 \leq k \leq r} \mathcal{O}_k \subset \overline{\mathcal{O}_r}$. $\square$

Corollaire 9.3.5

L'unique orbite fermée est l'orbite de la matrice nulle, dite « minimale » : $\mathcal{O}_0 = \{0\}$. L'unique orbite ouverte est dite l'orbite « maximale » : $\mathcal{O}_{\min(m,n)} = \mathrm{GL}(\min(m,n), \Bbbk)$. En particulier si $m = n$, le groupe des matrices inversibles $\mathrm{GL}(n, \Bbbk)$ est ouvert dans $\mathrm{M}(n, \Bbbk)$.

Corollaire 9.3.6

L'ensemble des matrices de rang r qui apparaît comme une orbite sous l'action de Steinitz est localement fermé.

Démonstration. — Notons $\mathcal{O}_r$ l'ensemble des matrices de rang r. Les matrices de rang inférieur ou égal à r sont obtenues comme les matrices dont les mineurs d'ordre $r+1$ sont tous nuls. Notons $\overline{\mathcal{O}_r}$ leur ensemble qui est donc fermé. L'orbite $\mathcal{O}$ est alors l'intersection de $\overline{\mathcal{O}_r}$ et du complémentaire de $\overline{\mathcal{O}_{r-1}}$. □

Corollaire 9.3.7

La fonction $\mathrm{rg}\colon \mathrm{M}(n, \Bbbk) \to \mathbb{N}$ n'est pas continue (on munit $\mathbb{N}$ de la topologie discrète).

En effet la fibre d'un fermé n'est pas fermée : $\mathrm{rg}^{-1}(\{r\}) = \mathcal{O}_r$.

Par contre la fonction $\mathrm{rg}\colon \mathrm{M}(n, \Bbbk) \to \mathbb{N}$ est semi-continue inférieurement : la fibre $\mathrm{rg}^{-1}(\{0, 1, \ldots, r\}) = \bigcup_{0 \leq k \leq r} \mathcal{O}_k$ est fermée. On l'illustre à travers l'énoncé suivant :

Corollaire 9.3.8

Soit $(A_k)_{k \in \mathbb{N}}$ une suite de matrices de même rang r qui converge vers B. Alors $\mathrm{rg}\, B \leq r$.

Proposition 9.3.3

- ◇ L'ensemble $\mathcal{O}_p$ des matrices de rang p est connexe.
- ◇ L'ensemble $\mathcal{P}_p$ des projecteurs de rang p est connexe.
- ◇ Les composantes connexes de l'ensemble des projecteurs $\mathcal{P}$ sont les $\mathcal{P}_p$.

Démonstration. — ◇ Considérons l'application

$$\phi\colon \mathrm{GL}(n, \mathbb{C}) \times \mathrm{GL}(n, \mathbb{C}) \to \mathrm{M}(n, \mathbb{C}), \qquad (P, Q) \mapsto P \mathrm{id}_{p,0} Q^{-1}$$

où $\mathrm{id}_{p,0} = \begin{pmatrix} \mathrm{id}_p & 0 \\ 0 & 0 \end{pmatrix}$. Cette application est continue et $\mathcal{O}_p = \phi(\mathrm{GL}(n, \mathbb{C}) \times \mathrm{GL}(n, \mathbb{C}))$ d'où le résultat.

◇ Considérons l'application continue

$$\psi\colon \mathrm{GL}(n,\mathbb{C}) \to \mathrm{M}(n,\mathbb{C}), \qquad P \mapsto P\mathrm{id}_p P^{-1}.$$

Un projecteur est solution de $X^2 = X$. Comme

$$(P\mathrm{id}_{p,0}P^{-1})^2 = P\mathrm{id}_{p,0}P^{-1}$$

nous avons $\psi(\mathrm{GL}(n,\mathbb{C})) \subset \mathcal{P}_p$. De même tout projecteur de rang p s'écrit $\mathrm{id}_{p,0}P^{-1}$ donc $\mathcal{P}_p \subset \psi(\mathrm{GL}(n,\mathbb{C}))$. Finalement $\mathcal{P}_p = \psi(\mathrm{GL}(n,\mathbb{C}))$ et $\mathcal{P}_p$ est connexe.

◇ Soient p et q deux entiers distincts. Montrons que $A \in \mathcal{P}_p$ et $B \in \mathcal{P}_q$ ne sont pas dans la même composante connexe. L'application trace restreinte aux projecteurs $\mathrm{tr}_{|\mathcal{P}}$ est continue à valeurs dans $\{0, 1, 2, \ldots, n\}$ donc $\mathrm{tr}\, A \neq \mathrm{tr}\, B$. Or si P est un projecteur, nous avons $\mathrm{tr}\, P = \mathrm{rg}\, P$ (attention la réciproque est fausse) d'où $\mathrm{rg}\, A \neq \mathrm{rg}\, B$.

□

Les normes de l'espace vectoriel $\Bbbk^n$, $\Bbbk = \mathbb{R}$ ou $\mathbb{C}$, induisent des normes, dites subordonnées, sur $\mathbb{M}(n,\Bbbk)$:

◇ $||M|| = \sup\limits_{||x||=1} ||Mx||$;

◇ $||M||_1 = \sup\limits_{1\leq j\leq n} \sum\limits_{i=1}^{n} |m_{ij}|$ induite par la norme vectorielle $||x||_1 = \sum\limits_{i=1}^{n} |x_i|$;

◇ $||M||_2 = \sqrt{\rho(M^*M)}$ induite par la norme vectorielle $||x||_2 = \sqrt{\sum\limits_{i=1}^{n} |x_i|^2}$ où $M^* = {}^{\mathrm{t}}\overline{M}$ et $\rho(M)$ est le rayon spectral de M :

$$\rho(M) = \max\{|\lambda| \mid \lambda \text{ valeur propre de } M\};$$

◇ $||M||_\infty = \sup\limits_{1\leq i\leq n} \sum\limits_{j=1}^{n} |a_{i,j}|$ induite par la norme vectorielle $||x||_\infty = \max\limits_{1\leq i\leq n} |x_i|$.

Toutes les normes sur l'espace vectoriel de dimension finie $\mathrm{M}(n,\Bbbk)$ sont équivalentes mais les normes subordonnées ont l'avantage d'être multiplicatives, *i.e*

$$||AB|| \leq ||A|| \cdot ||B||.$$

Toute partie de $\mathrm{M}((n,m),\Bbbk)$ est désormais munie de la topologie induite par celle de l'espace vectoriel normé $\mathrm{M}((n,m),\Bbbk)$.

Définition 9.3.2

Un *groupe topologique* G est un groupe muni d'une topologie pour laquelle

$$\mu\colon \mathrm{G}\times\mathrm{G}\to\mathrm{G} \qquad (g,h)\mapsto gh$$

et

$$\iota\colon \mathrm{G}\to\mathrm{G} \qquad g\mapsto g^{-1}$$

sont continues.

Remarque 9.3.2. — Notons que ι est une involution, *i.e.* $\iota^2=\mathrm{id}$; en particulier ι est un homéomorphisme.

Remarque 9.3.3. — Signalons l'outil simple et fondamental suivant pour l'étude des groupes topologiques : la multiplication à gauche (resp. à droite) par $g\in\mathrm{G}$ est un homéomorphisme de G dans G qui envoie l'élément neutre e sur g. Une propriété vraie dans un voisinage de e a donc des chances de le rester dans un voisinage de g pour tout g.

Proposition 9.3.4

Soit $n\geq 1$ un entier.
Le groupe $\mathrm{GL}(n,\Bbbk)$ est un groupe topologique, ouvert et dense dans $\mathrm{M}(n,\Bbbk)$.
Le groupe $\mathrm{GL}(n,\mathbb{C})$ est connexe par arcs mais le groupe $\mathrm{GL}(n,\mathbb{R})$ n'est pas connexe.

Démonstration. — La fonction μ est continue comme composée de fonctions polynomiales.

La fonction ι est continue comme composée de fractions rationnelles sur leur domaine de définition [1] $\left(M^{-1}=\frac{{}^{\mathrm{t}}\mathrm{com}(M)}{\det M}\right)$.

Puisque l'application $\det\colon \mathrm{M}(n,\Bbbk)\to\mathbb{R}$ est continue

$$\mathrm{GL}(n,\Bbbk)=\left\{M\in\mathrm{M}(n,\Bbbk)\mid \det M\neq 0\right\}=\det{}^{-1}(\Bbbk^*)$$

est un ouvert.

1. Soit M une matrice carrée. Le cofacteur d'indice (i,j) de M est : $\left(\mathrm{com}M\right)_{i,j} := \det\left(M'_{i,j}\right) = (-1)^{i+j}\det\left(M_{i,j}\right)$ où

- $M'_{i,j}$ est la matrice carrée de taille n déduite de M en remplaçant la j-ème colonne par une colonne constituée uniquement de zéros, sauf un 1 sur la $i$ème ligne ;
- $M_{i,j}$ est la sous-matrice carrée de taille $n-1$ déduite de M en supprimant la $i$ème ligne et la $j$ème colonne (son déterminant fait donc partie des mineurs de M).

La *comatrice* de M est la matrice de ses cofacteurs.

D'une part

$$\overline{\mathrm{GL}(n,\Bbbk)} = \overline{\mathcal{O}_n} \qquad\qquad \bigcup_{0\leq k\leq n} \mathcal{O}_k = \mathrm{M}(n,\Bbbk)$$

et d'autre part la Proposition 9.3.2 assure que $\overline{\mathcal{O}_n} = \bigcup_{0\leq k\leq n} \mathcal{O}_k$ d'où

$$\overline{\mathrm{GL}(n,\Bbbk)} = \mathrm{M}(n,\Bbbk).$$

Comme $\operatorname{im}\det = \mathbb{R}^*$ est non connexe, le groupe $\mathrm{GL}(n,\mathbb{R})$ n'est pas connexe.

Montrons que $\mathrm{GL}(n,\mathbb{C})$ est connexe par arcs. Soient A et B dans $\mathrm{GL}(n,\mathbb{C})$; montrons qu'il existe un arc de $\mathrm{GL}(n,\mathbb{C})$ qui les relie. Considérons l'application

$$P\colon \mathbb{C} \to \mathbb{R}, \qquad\qquad z \mapsto \det(zA + (1-z)B).$$

Notons que P est un polynôme non nul : $P(1) = \det A \neq 0$. Par suite P possède un nombre fini de racines donc $\mathcal{C} = \{z \in \mathbb{C} \mid P(z) \neq 0\}$ est connexe par arcs (en effet c'est le plan complexe privé d'un nombre fini de points). Soit

$$\varphi\colon \mathcal{C} \to \mathrm{GL}(n,\mathbb{C}), \qquad\qquad z \mapsto zA + (1-z)B.$$

Puisque φ est continue et $\mathcal{C}$ connexe par arcs, $\varphi(\mathcal{C})$ est connexe par arcs. Nous concluons en remarquant que A et B appartiennent à $\varphi(\mathcal{C})$. □

Proposition 9.3.5

Soit n un entier. Soit $0 \leq r \leq n$ un entier. L'orbite $\mathcal{O}_r$ des matrices de $\mathrm{M}(n,\Bbbk)$, $\Bbbk = \mathbb{R}$ ou $\mathbb{C}$, de rang r est d'intérieur vide.

Démonstration. — Désignons par Λ_r l'ensemble des matrices de rang r.

L'ensemble Λ_0 est le singleton $\{0\}$ qui est un fermé d'intérieur vide.

L'ensemble Λ_n est le groupe linéaire $\mathrm{GL}(n,\mathbb{R})$. La Proposition 9.3.4 assure que Λ_n est un ouvert dense de $\mathrm{M}(n,\Bbbk)$. Nous en déduisons que les ensembles Λ_r pour $r < n$ sont d'intérieur vide puisqu'ils sont inclus dans le fermé $\mathrm{M}(n,\Bbbk) \smallsetminus \Lambda_n$ qui est d'intérieur vide. □

9.3.3. Le théorème de la base incomplète. —

Théorème 9.3.4

Toute famille libre d'un $\Bbbk$-espace vectoriel peut être complétée en une base.

Une formulation équivalente de cet énoncé en dimension finie est :

Proposition 9.3.6

Le groupe $\mathrm{GL}(n, \Bbbk)$ agit simplement et transitivement sur l'ensemble des bases vectorielles.

Démonstration. — Soient $p < n$ et $(a_i)_{1 \leq i \leq p}$ une famille de vecteurs d'un $\Bbbk$-espace vectoriel de dimension n.

La famille $(a_i)_{1 \leq i \leq p}$ est libre si et seulement si la matrice A formée par les vecteurs (en colonnes) de cette famille est de déterminant non nul, *i.e.* A appartient à $\mathrm{GL}(p, \Bbbk)$.

Puisque toute matrice inversible de taille p peut être complétée en une matrice inversible de taille n (en ajoutant des 1 sur la diagonale par exemple), nous obtenons une base si et seulement si nous avons une correspondance biunivoque entre les matrices inversibles et les bases vectorielles si et seulement si $\mathrm{GL}(n, \Bbbk)$ agit simplement et transitivement sur l'ensemble des bases vectorielles. □

Cet énoncé dont un corollaire assure qu'il existe une base dans tout espace vectoriel peut se décliner en de nombreuses variantes dont voici une liste (non exhaustive) ainsi que leur formulation en termes d'action de groupe :

Théorème 9.3.5

- Toute famille libre d'un espace vectoriel euclidien peut être complétée en une base orthonormale euclidienne (pour le produit scalaire euclidien).

  Le groupe $\mathrm{O}(n, \Bbbk)$ agit simplement et transitivement sur l'ensemble des bases orthonormales euclidiennes.
- Toute famille libre d'un espace vectoriel euclidien peut être complétée en une base orthonormale directe euclidienne.

  Le groupe $\mathrm{SO}(n, \Bbbk)$ agit simplement et transitivement sur l'ensemble des bases orthonormales directes euclidiennes.
- Toute famille libre d'un espace hermitien peut être complétée en une base orthonormale hermitienne (pour le produit scalaire hermitien).

  Le groupe $\mathrm{U}(n, \mathbb{C})$ agit simplement et transitivement sur l'ensemble des bases orthonormales hermitiennes.
- Toute famille libre d'un espace vectoriel hermitien peut être complétée en une base orthonormale directe hermitienne (pour le produit scalaire hermitien).

  Le groupe $\mathrm{SU}(n, \mathbb{C})$ agit simplement et transitivement sur l'ensemble des bases orthonormales directes hermitiennes.

9.4. Action de $\mathrm{GL}(n,\mathbb{C})$ par conjugaison

Comme dans §9.3 nous allons définir une action continue de groupe topologique sur un espace topologique, puis trouver des invariants totaux pour cette action et enfin regarder les adhérences d'orbites ou comment ces invariants totaux évoluent après passage à la limite. L'action étudiée dans ce paragraphe est l'action de $\mathrm{GL}(n,\Bbbk)$ sur $\mathrm{M}(n,\Bbbk)$ par conjugaison. Ce problème, qui se ramène à l'étude des matrices semblables (et donc aux fameux invariants de similitude), est beaucoup plus difficile, que celui des matrices équivalentes :

- ◇ il dépend du corps choisi et nous allons nous limiter au cas $\Bbbk = \mathbb{C}$,
- ◇ la classification est radicalement différente si on s'intéresse aux matrices diagonalisables, ou si elles sont nilpotentes. Nous étudierons les deux, et le cas général s'en déduit à l'aide de la décomposition de Dunford.

L'invariant total des matrices diagonalisables est le spectre avec multiplicité, et celui des matrices nilpotentes est la suite des dimensions des noyaux emboités. Pour l'étude topologique, il sera pratique de stocker l'information des noyaux emboités sous forme de tableaux de Young.

Le groupe $\mathrm{GL}(n,\mathbb{C})$ agit sur $\mathrm{M}(n,\mathbb{C})$ par conjugaison (ou par similitude) via

$$\mathrm{GL}(n,\mathbb{C}) \times \mathrm{M}(n,\mathbb{C}) \to \mathrm{M}(n,\mathbb{C}), \qquad (P,M) \mapsto P^{-1}MP.$$

Cette action correspond au changement de base pour les applications linéaires.

Définition 9.4.1

Deux matrices dans la même orbite pour cette action sont dites *semblables*.

Définition 9.4.2

Une matrice de $\mathrm{M}(n,\Bbbk)$ est *diagonalisable* dans $\Bbbk$ si elle est semblable à une matrice diagonale.
Une matrice de $\mathrm{M}(n,\Bbbk)$ est *trigonalisable* dans $\Bbbk$ si elle est semblable à une matrice triangulaire supérieure.

9.4.1. Action de $\mathrm{GL}(n,\mathbb{C})$ sur $\mathcal{D}(n,\mathbb{C})$ par conjugaison. — Notons $\mathcal{D}(n,\mathbb{C})$ les matrices diagonalisables sur $\mathbb{C}$. Rappelons que

$$\mathcal{O}_A = \{PAP^{-1} \mid P \in \mathrm{GL}(n,\mathbb{C})\}$$

est l'orbite de A sous l'action de $\mathrm{GL}(n,\mathbb{C})$ par conjugaison (matrices semblables à A). On considère le spectre d'une matrice comme la donnée de n complexes (non nécessairement distincts) à permutation près ; un spectre est donc un élément de $\mathbb{C}^n/\mathfrak{S}_n$.

Théorème 9.4.1

L'application

$$\varphi\colon \mathcal{D}(n,\mathbb{C})/\mathrm{GL}(n,\mathbb{C}) \to \mathbb{C}^n/\mathfrak{S}_n, \qquad \mathcal{O}_A \mapsto \mathrm{Spec}(A)$$

est bijective.

Démonstration. — L'application φ est bien définie car deux matrices diagonalisables semblables ont même spectre. Par conséquent le spectre ne dépend pas du choix de l'élément A de l'orbite $\mathcal{O}_A$.

L'application φ est surjective puisque pour tout spectre (à permutation près) il existe une matrice diagonale dont les éléments diagonaux sont les éléments du spectre (valeurs propres).

Supposons que $\mathrm{Spec}(A) = \mathrm{Spec}(B)$. Comme A et B sont diagonalisables, elles sont semblables à la matrice diagonale des valeurs propres donc appartiennent à la même orbite, $\mathcal{O}_A = \mathcal{O}_B$ et ainsi φ est injective. □

Corollaire 9.4.1

Le polynôme caractéristique est un invariant total de similitude pour les matrices diagonalisables.
Le spectre, c'est-à-dire les valeurs propres avec multiplicité, est un invariant total de similitude pour les matrices diagonalisables.

Remarque 9.4.1. — Par contre le polynôme minimal est un invariant mais pas un invariant total. Il est facile d'en trouver un exemple : les matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

ont même polynôme minimal mais ne sont pas semblables.

Passons maintenant à l'étude topologique ; nous allons montrer que les orbites sont fermées. En fait nous obtenons plus, nous obtenons une caractérisation topologique de la diagonalisation :

Proposition 9.4.1

Une matrice complexe A est diagonalisable si et seulement si son orbite $\mathcal{O}_A$ sous l'action de $\mathrm{GL}(n,\mathbb{C})$ est fermée dans $\mathrm{M}(n,\mathbb{C})$.

Démonstration. — Supposons que $A \in \mathrm{M}(n,\mathbb{C})$ soit diagonalisable. Soit $(B_k)_{k\in\mathbb{N}} \subset \mathcal{O}_A$ telles que $\lim\limits_{k\to+\infty} B_k = B$. Montrons que B appartient à $\mathcal{O}_A$. Notons λ_1, λ_2, ..., λ_n les valeurs propres de A (remarquons qu'elles sont de multiplicité 1 car A est diagonalisable). Puisque B_k appartient à $\mathcal{O}_A$ nous avons $\prod\limits_{i=1}^{n}(B_k - \lambda_i \mathrm{id}) = 0$. En passant à la limite ($k \to +\infty$) nous obtenons $\prod\limits_{i=1}^{n}(B - \lambda_i \mathrm{id}) = 0$; ainsi B est annulé par un polynôme scindé à racines simples ; B est donc diagonalisable.

Posons $r_{i,k} := \dim\ker(B_k - \lambda_i \mathrm{id})$ et $r_i = \dim\ker(B - \lambda_i \mathrm{id})$ les multiplicités géométriques. Nous avons

- $\sum\limits_{i=1}^{n} r_{i,k} = n$ car comme B_n est diagonalisable le lemme des noyaux assure que $E = \oplus_i \ker(B_k - \lambda_i \mathrm{id})$,
- $\sum\limits_{i=1}^{n} r_i = n$ car comme B est diagonalisable le lemme des noyaux assure que $E = \oplus_i \ker(B - \lambda_i \mathrm{id})$,
- $r_i \geq r_{i,k}$ par semi-continuité du rang.

Ainsi $r_i = r_{i,k}$ pour tout $k \in \mathbb{N}$. Finalement $\mathrm{Spec}(B_k) = \mathrm{Spec}(B)$ et B appartient à $\mathcal{O}_A$.

Réciproquement montrons que l'orbite d'une matrice non diagonalisable n'est pas fermée.

Lemme 9.4.1

Dans $\mathrm{M}(n,\mathbb{C})$ toute adhérence d'orbite contient une matrice diagonalisable.

Démonstration. — Soit A un élément de $\mathrm{M}(n,\mathbb{C})$. La matrice A est semblable à une matrice triangulaire inférieure $T = (t_{ij})$. Posons

$$P_\varepsilon = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \varepsilon & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \varepsilon^{n-1} \end{pmatrix}$$

où ε désigne un nombre complexe non nul. Un calcul montre que $P_\varepsilon T P_\varepsilon^{-1} = (\varepsilon^{i-j} t_{i,j})_{i,j}$. Par hypothèse $t_{i,j} = 0$ dès que $i - j < 0$; par suite $\lim\limits_{\varepsilon\to 0} P_\varepsilon T P_\varepsilon^{-1}$ est diagonale. □

Soit A une matrice non diagonalisable. Supposons par l'absurde que $\mathcal{O}_A$ est fermée. Le Lemme 9.4.1 assure que $\mathcal{O}_A = \overline{\mathcal{O}_A}$ contient une matrice diagonale D. Ainsi A est semblable à une matrice diagonale : absurde. □

Remarque 9.4.2. — On peut montrer que $\mathcal{D}(n,\mathbb{C})$ est dense dans $\mathrm{M}(n,\mathbb{C})$ et son intérieur est constitué des matrices dont toutes les valeurs propres sont différentes.

Remarque 9.4.3. — Une classe de conjugaison peut être fermée. En revanche elle n'est jamais ouverte. En effet deux matrices semblables ont même trace ce qui entraîne que toute classe de conjugaison est incluse dans un hyperplan affine défini par $\operatorname{tr} M = k$ où k est une constante ; la classe ne peut donc pas contenir une boule ouverte.

9.4.2. Action de $\mathrm{GL}(n,\mathbb{C})$ sur $\mathcal{N}(n,\mathbb{C})$ par conjugaison. — Après avoir étudié les orbites « diagonalisables » l'étape naturelle suivante est l'étude de l'action du groupe $\mathrm{GL}(n,\mathbb{C})$ sur l'ensemble des matrices nilpotentes de taille n.

Matrices nilpotentes

Soit n un entier ≥ 1. Une matrice $M \in \mathrm{M}(n,\mathbb{C})$ est dite *nilpotente* s'il existe un entier naturel non nul n tel que $M^n = 0$. On appelle *ordre de nilpotence* le plus petit entier m tel que $M^m = 0$.

Désignons par $\mathcal{N}(n,\mathbb{C})$ l'ensemble des matrices nilpotentes de taille n.

L'action par conjugaison de $\mathrm{GL}(n,\mathbb{C})$ sur $\mathrm{M}(n,\mathbb{C})$ stabilise $\mathcal{N}(n,\mathbb{C})$. Nous appelons *orbite nilpotente* une orbite de l'action restreinte à $\mathcal{N}(n,\mathbb{C})$, plus classiquement c'est une classe de similitude de matrices nilpotentes.

Remarque 9.4.4. — L'ordre de nilpotence dans la définition vérifie toujours $m \leq n$. Effectivement les valeurs propres de la matrice nilpotente M sont toutes nulles ; le théorème de Cayley-Hamilton assure que $M^n = 0$.

Noyaux itérés et injections de Frobenius

Soit $A \in \mathcal{N}(n,\mathbb{C})$ une matrice nilpotente. Désignons par $K_i = \ker A^i$ ses noyaux emboîtés et par k_i la dimension de K_i. Nous avons les inclusions suivantes

$$\{0\} = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \ldots \subsetneq K_n = \mathbb{C}^n.$$

Nous allons voir que la suite $(k_i)_i$ s'essouffle au sens suivant : les sauts de dimension vont en diminuant.

Lemme 9.4.2

Pour tout $1 \leq i \leq n-1$ nous avons

$$0 \leq \dim K_{i+1} - \dim K_i \leq \dim K_i - \dim K_{i-1}.$$

Démonstration. — Soit $1 \leq i \leq n-1$. La première inégalité découle de l'inclusion $K_i \subset K_{i+1}$.

Notons que $AK_{i+1} \subset K_i$. Considérons la composition

$$\begin{array}{ccccc} K_{i+1} & \xrightarrow{\nu} & K_i & \xrightarrow{\pi_i} & K_i/K_{i-1} \\ X & \mapsto & AX & \mapsto & \overline{AX} \end{array}$$

Nous avons

$$\ker(\pi_i \circ \nu) = (\pi_i \circ \nu)^{-1}(\{\overline{0}\}) = \nu^{-1}\Big(\pi_i^{-1}(\{\overline{0}\})\Big) = \nu^{-1}(K_{i-1}) = K_i.$$

Par passage au quotient nous obtenons donc une injection $K_{i+1}/K_i \hookrightarrow K_i/K_{i-1}$, celle-ci entraîne l'inégalité $\dim\left(K_{i+1}/K_i\right) \leq \dim\left(K_i/K_{i-1}\right)$. □

En particulier la suite $(k_i)_i$ est strictement croissante avant de devenir stationnaire (au pire à partir du rang n puisque A est nilpotente). Ainsi pour un certain rang m (qui est par définition l'indice de nilpotence)

$$\{0\} = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \ldots \subsetneq K_m = \mathbb{C}^n.$$

Le noyau K_i de A^i dépend bien évidemment de A mais sa dimension ne dépend que de l'orbite de A pour la conjugaison. Posons pour tout entier i

$$\lambda_i = \lambda_i(A) = k_i - k_{i-1}.$$

Partitions et diagrammes de Young

Rappelons qu'une partition d'un entier naturel n est une suite d'entiers naturels $(\lambda_j)_{j\geq 1}$ qui est décroissante au sens large, nulle à partir d'un certain rang $m+1$ et dont la somme des termes vaut n : $\sum_{j=1}^{m} \lambda_j = n$. Nous appelons *part* de λ les termes λ_j non nuls. Quitte à oublier ou ajouter une infinité de zéros nous pouvons identifier une partition à une suite finie décroissante d'entiers naturels non nuls.

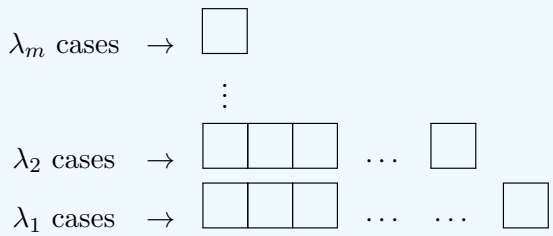
À une partition λ nous associons une suite d'entiers $(k_i)_i$ (croissante et qui s'essouffle) de la façon : pour tout j dans $\mathbb{N}^*$

$$k_j = \sum_{i=1}^{j} \lambda_i.$$

Le diagramme de Young est une visualisation d'une partition.

Définition 9.4.3: (Définition informelle)

Nous appelons *diagramme de Young* de taille n associé à une partition λ par n cases juxtaposées de la façon suivante :



Il y a une bijection entre partitions et diagrammes de Young. Si Y est un diagramme de Young nous notons $\lambda(Y)$ la partition associée et nous posons pour tout i

$$k_i(Y) = \sum_{j=1}^{i} \lambda_j(Y).$$

Définition 9.4.4: (Définition formelle)

Nous appelons *diagramme de Young « formel »* toute partie Y de $\mathbb{N}^* \times \mathbb{N}^*$ telle que pour tout $(i,j) \in Y$ on ait : $(k,\ell) \in Y$ pour tout $1 \leq k \leq i$ et tout $1 \leq \ell \leq j$. La *taille* d'un diagramme de Young est son cardinal.

Explicitons le lien entre définitions formelle et informelle : nous dessinons un petit carré dont le coin inférieur gauche est un point de Y vu comme partie de $\mathbb{R}^2$.

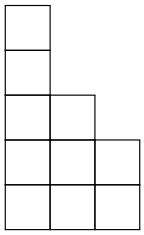
Lemme 9.4.3

Soit n un entier naturel. Les applications suivantes sont des bijections réciproques entre partitions de n et diagrammes de Young de taille n :

- ◇ à une partition λ nous associons
$$Y_\lambda = \{(i,j) \in \mathbb{N}^* \times \mathbb{N}^* \,|\, i \leq \lambda_j\};$$
- ◇ à un diagramme de Young Y nous associons $\lambda = \lambda_Y$ où pour tout j
$$\lambda_j = \max\{i \,|\, (i,j) \in Y\}.$$

On comprend λ_j comme le nombre de cases de la $j$ième ligne du diagramme.

Exemple 9.4.1. — La partition associée au diagramme



est $\lambda = (3,3,2,1,1)$ et réciproquement.

Démonstration. — Notons que les applications sont bien définies. En effet

- ◇ soit λ une partition. Soient $(i,j) \in Y_\lambda$ et $(k,\ell) \in \mathbb{N}^2$ avec $k \leq i$ et $\ell \leq j$. La suite λ étant décroissante nous avons $k \leq i \leq \lambda_j \leq \lambda_\ell$ donc $(k,\ell) \in Y$.
- ◇ soient Y un diagramme de Young et λ la suite d'entiers qui lui est associée. Soient j et ℓ deux entiers avec $\ell \leq j$. Nous devons montrer que $\lambda_j \leq \lambda_\ell$. Soit $i = \lambda_j$. Le point (i,j) appartient à Y donc (i,ℓ) aussi. Par définition de λ_ℓ nous avons $i \leq \lambda_\ell$.

Soit λ une partition. Nous avons : (i, j) appartient à Y_λ si et seulement si $i \leq \lambda_j$. Pour j fixé nous pouvons donc écrire $\lambda_j = \max\{m \mid (i, j) \in Y_\lambda\}$. Cela signifie que la partition associée à Y_λ est bien λ.

Le calcul de la composée dans l'autre sens est analogue. □

Diagramme de Young associé à une orbite nilpotente

Nous avons défini, pour chaque orbite nilpotente, deux suites d'entiers positifs ou nuls à partir d'un élément quelconque A de l'orbite :

- $k_i = \dim K_i$,
- $\lambda_i = k_i - k_{i-1}$.

Le Lemme 9.4.2 assure que $0 \leq \lambda_i \leq k_i$ pour tout i. De plus pour tout $i \in \mathbb{N}$

$$\lambda_{i+1} \leq \lambda_i \qquad \text{et} \qquad \sum_{j=1}^{n} \lambda_j = n.$$

Définition 9.4.5

Soit n un entier non nul. Soit $\mathcal{O}$ une orbite nilpotente de $\mathcal{N}(n, \mathbb{C})$. Nous appelons *partition associée à $\mathcal{O}$ (par les noyaux itérés)* et nous notons $\lambda_{\mathcal{O}} = (\lambda_i)_i$ la partition dont les parts sont

$$\lambda_i = k_i - k_{i-1}$$

où A est un élément quelconque de $\mathcal{O}$.

Définition 9.4.6

Nous apppelons *diagramme de Young* associé à une orbite nilpotente et nous notons $Y := Y(\mathcal{O})$, ou $Y(A)$ pour un élément quelconque A de $\mathcal{O}$, le diagramme de Young associé à la partition λ associée à $\mathcal{O}$ par les noyaux itérés :

$$\lambda_i = k_i - k_{i-1}.$$

Diagramme dual, partition duale

Informellement le diagramme dual Y^* d'un diagramme de Young Y est son symétrique par rapport à la diagonale principale. La partition duale d'une partition λ s'obtient en écrivant la liste des hauteurs des colonnes du diagramme de Young de λ.

Soit $\tau \colon \mathbb{N}^2 \to \mathbb{N}^2$, $(i, j) \mapsto (j, i)$ la symétrie. L'image $Y^* = \tau(Y)$ d'un diagramme de Young est encore un diagramme de Young car τ ne fait qu'échanger les conditions $k \leq i$ et $\ell \leq j$ de la définition. Autrement dit nous avons la propriété suivante :

Lemme 9.4.4

L'ensemble des diagrammes de Young est stable par la symétrie par rapport à la diagonale principale.

Lemme-Définition 9.4.1

Soit $\lambda = (\lambda_j)_j$ une partition. Pour $i \in \mathbb{N}$ posons

$$\mu_i = \#\{j \in \mathbb{N} \,|\, 1 \leq i \leq \lambda_j\}.$$

Alors $\mu = (\mu_i)_i$ est une partition et le diagramme de Young de μ est l'image de celui de λ par la symétrie par rapport à la diagonale principale.
La partition μ ainsi définie est la *partition duale* de μ ; elle est notée λ^*.

Exemple 9.4.2. — La partition duale de $\lambda = (3, 3, 2, 1, 1)$ est $\lambda^* = (5, 3, 2)$.

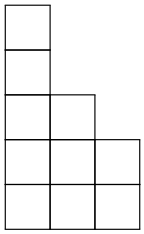
Démonstration. — Il suffit de montrer que pour tous i, j dans $\mathbb{N}^*$ $j \leq \mu_i$ si et seulement si $i \leq \lambda_j$.

Fixons i. Par définition de μ_i il y a exactement μ_i parts λ_j de λ qui sont supérieures ou égales à i. La suite λ étant décroissante ces parts sont donc λ_1, λ_2, ..., λ_{μ_i}. Autrement dit $1 \leq j \leq \mu_i$ si et seulement si $i \leq \lambda_j$. □

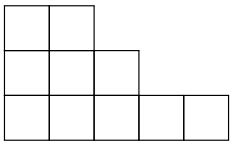
Définition 9.4.7

Soit Y un diagramme de Young. Le *diagramme de Young dual* de Y, noté Y^*, est le symétrique de Y par rapport à la diagonale principale c'est-à-dire son image par τ.

Exemple 9.4.3. — Le dual du diagramme de Young



est



Scindage des noyaux itérés

Nous allons montrer le théorème de Jordan de façon constructive. Nous disposons à partir d'une matrice nilpotente A la suite de ses noyaux itérés. Chaque noyau de la suite est un sous-espace stable par A néanmoins nous nous heurtons au problème suivant : un sous-espace stable n'a en général pas de supplémentaire stable. Pour palier ce problème nous allons partir d'éléments d'indice maximum, *i.e.* des vecteurs x de l'espace tels que $x \notin K_\ell$ avec ℓ maximal. Le levier de la démonstration est le fait que le sous-espace stable engendré par un tel vecteur possède un sous-espace supplémentaire stable.

Soit $A \in \mathcal{N}(n, \mathbb{C})$ une matrice nilpotente d'ordre m. Soit $K_i = \ker A^i$ pour tout i. Ces noyaux sont emboîtés

$$\{0\} \subsetneq K_1 \subsetneq K_2 \subsetneq \ldots \subsetneq K_\ell = \mathbb{C}^n.$$

Partons d'un sous-espace G_m supplémentaire de K_{m-1} dans $K_m = \mathbb{C}^n$ de sorte $K_{m-1} \oplus G_m = K_m$. Posons

$$\lambda_m = \dim G_m = \dim K_m - \dim K_{m-1}.$$

Si v appartient à G_m et $A^{m-1}v = 0$, alors $v = 0$ puisque par construction la restriction de A^{m-1} à G_m est injective. Par conséquent la restriction de A à G_m est également injective (puisque la composée d'injectifs reste injectif).

Soit $(v_m^1, v_m^2, \ldots, v_m^{\lambda_m})$ une base de G_m. Nous constructions un supplémentaire G_{m-1} de K_{m-2} dans K_{m-1} de la façon suivante : en utilisant la remarque précédente nous obtenons que $(Av_m^1, Av_m^2, \ldots, Av_m^{\lambda_m})$ est une famille libre qui engendre un sous-espace intersectant K_{m-2} trivialement. Cela revient à dire que cette famille reste libre quotientée dans K_{m-1}/K_{m-2}. Ainsi nous pouvons la compléter en une base de K_{m-1}/K_{m-2}. En relevant cette base dans K_{m-1} nous obtenons une base

$$(Av_m^1, Av_m^2, \ldots, Av_m^{\lambda_m}, v_{m-1}^{\lambda_m+1}, \ldots, v_{m-1}^{\lambda_{m-1}})$$

d'un supplémentaire G_{m-1} de K_{m-2} dans K_{m-1}. Renotons cette base

$$(v_{m-1}^1, Av_{m-1}^2, \ldots, Av_{m-1}^{\lambda_m}, v_{m-1}^{\lambda_m+1}, \ldots, v_{m-1}^{\lambda_{m-1}}).$$

Par récurrence descendante sur r nous construisons ainsi un supplémentaire G_r de K_{r-1} dans K_r de dimension $\lambda_r = k_r - k_{r-1}$. Par itération nous pouvons remplir le diagramme de Young de A ligne par ligne, successivement en multipliant par A puis en complétant :

v_m^1	v_m^2	$\cdots$	$v_m^{\lambda_m}$							
Av_m^1	Av_m^2	$\cdots$	$Av_m^{\lambda_m}$	$v_{m-1}^{\lambda_m+1}$	$\cdots$	$v_{m-1}^{\lambda_{m-1}}$				
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$			
$A^{n-r}v_m^1$	$A^{n-r}v_m^2$	$\cdots$	$A^{n-r}v_m^{\lambda_m}$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$v_r^{\lambda_r}$		
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$A^{m-1}v_m^1$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$v_1^{\lambda_1}$

L'image par A d'un vecteur est

- ◇ le vecteur situé dans la case en-dessous de lui s'il n'est pas dans la ligne du bas ;
- ◇ le vecteur nul s'il est dans la ligne du bas.

Nous obtenons alors en lisant le tableau colonne après colonne et de haut en bas une nouvelle base de $\mathbb{C}^n$:

$$(v_m^1, Av_m^1, \dots, A^{m-1}v_m^1, v_m^2, \dots, A^{m-1}v_m^2, \dots, v_1^{\lambda_1})$$

dans laquelle l'endomorphisme de $\mathbb{R}^n$ canoniquement associé à A s'écrit

$$A' = \begin{pmatrix} J_{\lambda_1^*} & & 0 \\ & \ddots & \\ 0 & & J_{\lambda_k^*} \end{pmatrix}$$

où

$$J_p = \begin{pmatrix} 0 & 0 & \dots & \dots & 0 \\ 1 & 0 & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

et $\lambda^* = (\lambda_j^*)_{1 \leq j \leq k}$ est la partition duale de λ. La matrice A' est appelée *réduite de Jordan* semblable à A au sens suivant :

Définition 9.4.8

Soit p un entier naturel non nul. La matrice

$$J_p = \begin{pmatrix} 0 & 0 & \dots & \dots & 0 \\ 1 & 0 & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

est appelé *bloc de Jordan nilpotent* de taille p, ou *bloc de Jordan associé à la valeur propre* 0.

On appelle *réduite de Jordan* (*nilpotente*) ou *forme normale de Jordan* toute matrice diagonale par blocs dont les blocs diagonaux sont des blocs de Jordan de taille décroissante.

Si $\nu = (\nu_i)_{i \geq 1}$ est une partition de n, alors J_ν désigne la matrice diagonale dont les blocs diagonaux sont les blocs de Jordan J_{nu_i} de tailles respectives ν_1, ν_2, ...

Nous pouvons donc énoncer la :

Proposition 9.4.2

Soient n un entier naturel et A une matrice nilpotente de taille n. Il existe une réduite de Jordan semblable à A.
Plus précisément soit λ la partition associée à A par les noyaux itérés dont les parts sont

$$\lambda_i = \dim \ker A^i - \dim \ker A^{i-1}$$

La matrice A est semblable à J_{λ^*}.

Classification des orbites nilpotentes

Théorème 9.4.2

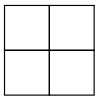
La classe de similitude d'une orbite nilpotente est caractérisée par son diagramme de Young : si A et B sont deux matrices nilpotentes de même taille, alors

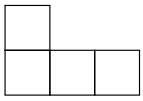
$$\mathcal{O}_A = \mathcal{O}_B \Longleftrightarrow Y(A) = Y(B).$$

Exemple 9.4.4. — Les matrices

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

sont nilpotentes, ont même polynôme caractéristique (X^4), même polynôme minimal (X^2) mais ne sont pas semblables car leurs diagrammes de Young sont respectivement





Une reformulation du Théorème 9.4.2 est :

Théorème 9.4.3

Soit n un entier naturel non nul. Pour une partition $\nu = (\nu_1, \nu_2, \ldots, \nu_m)$ de n (*i.e.* $n = \nu_1 + \nu_2 + \ldots + \nu_m$), notons J_ν la matrice diagonale par blocs dont les blocs diagonaux sont les blocs de Jordan de taille $\nu_1, \nu_2, \ldots, \nu_m$.
L'application qui à une partition ν de n associe la classe de similitude de J_ν, est une bijection de l'ensemble des partitions de n sur l'ensemble des classes de similitude de matrices nilpotentes de taille n.

Une seconde reformulation du Théorème 9.4.2 est :

Théorème 9.4.4

Soit n un entier naturel non nul. Soit A une matrice nilpotente de taille $n \times n$. Il existe une unique suite $(\nu_1, \nu_2, \ldots, \nu_m)$ décroissante d'entiers naturels non nuls telle que A soit semblable à la matrice J_ν.

Démonstration du Théorème 9.4.2. — Supposons que $\mathcal{O}_A = \mathcal{O}_B$ c'est-à-dire que les matrices A et B soient semblables. Il existe alors $P \in \mathrm{GL}(n, \mathbb{C})$ telle que $B = PAP^{-1}$ d'où

$$\dim \ker B^i = \dim \ker(PA^iP^{-1}) = \dim \ker A^i$$

pour tout i si bien que $Y(A) = Y(B)$.

Réciproquement supposons que $Y(A) = Y(B)$. Les matrices A et B ont alors la même partition $\lambda_A = \lambda_B$ et donc la même partition duale $\lambda_A^* = \lambda_B^*$; elles sont ainsi semblables à la même réduite de Jordan. Par suite A et B sont semblables, *i.e.* $\mathcal{O}_A = \mathcal{O}_B$. □

Ordre de dominance

Il est possible de définir de façon purement combinatoire un ordre sur les diagrammes de Young ou de manière équivalente sur les partitions. Via la bijection entre partitions et orbites nilpotentes cet ordre devient l'ordre de dégénérescence, ou ordre de Chevalley, sur les orbites.

Définition 9.4.9

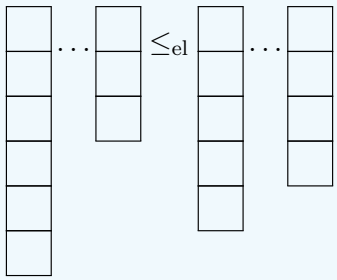
Soit n un entier naturel ≥ 1. Soient Y et Y' deux diagrammes de Young de taille n associés aux partitions $\lambda = \lambda(Y)$ et $\lambda' = \lambda(Y')$. Le diagramme Y *est inférieur ou égal à* Y' et nous notons $Y \leq Y'$ si pour tout i nous avons $k_i(Y) \leq k_i(Y')$ c'est-à-dire

$$\lambda_1 \leq \lambda'_1 \quad \lambda_1 + \lambda_2 \leq \lambda'_1 + \lambda'_2 \quad \ldots \quad \lambda_1 + \lambda_2 + \ldots + \lambda_i \leq \lambda'_1 + \lambda'_2 + \ldots + \lambda'_i, \quad \ldots$$

Il est immédiat de vérifier que $\leq$ est un ordre. On l'appelle *ordre de dominance*.

Définition 9.4.10

Soit n un entier naturel ≥ 1. Soient Y et Y' deux diagrammes de Young de taille n. On définit la relation élémentaire $Y \leq_{\mathrm{el}} Y'$ si $Y = Y'$ ou si Y' est identique à Y après qu'un bloc soit « tombé » du sommet d'une colonne sur une colonne plus à sa droite :



Le lien entre $\leq$ et $\leq_{\text{el}}$ est donné par la :

Proposition 9.4.3

L'ordre $\leq$ sur les diagrammes de Young est l'ordre engendré par les relations élémentaires $\leq_{\text{el}}$: $Y \leq Y'$ si et seulement s'il existe $k \in \mathbb{N}^*$ et Y_1, Y_2, ..., Y_k tels que

$$Y = Y_1 \leq_{\text{el}} Y_2 \leq_{\text{el}} \ldots \leq_{\text{el}} Y_k = Y'.$$

Pour une démonstration on renvoit à [**CG17**].

Adhérence des orbites nilpotentes

Déterminons l'adhérence de l'orbite $\mathcal{O}_A$ d'une matrice nilpontente complexe A. Le résultat utilise fortement le concept de diagramme de Young intorduit précédemment

Théorème 9.4.5

Soit A matrice nilpotente de taille n. L'adhérence de la classe de similitude de A est

$$\overline{\mathcal{O}_A} = \bigsqcup_{Y(B) \geq Y(A)} \mathcal{O}_B$$

Remarque 9.4.5. — Ainsi l'adhérence des orbites est caractérisée par un ordre partiel : la relation suivante, définie sur les orbites nilpotentes, est un ordre

$$\mathcal{O} \leq \mathcal{O}' \text{ si } \mathcal{O} \subset \overline{\mathcal{O}'}$$

appelée *ordre de Chevalley* ou *ordre de dégénérescence*.

Démonstration. — Nous allons montrer la double inclusion :

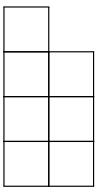
- Soit B un élément de $\overline{\mathcal{O}_A}$. Soit $(A_m)_m$ une suite d'éléments de $\mathcal{O}_A$ qui converge vers B. La semi-continuité inférieure du rang assure que pour tout i nous avons

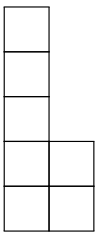
  $$k_i(Y(B)) = \dim \ker B^i \geq \dim \ker A_m^i = k_i(Y(A_m)) = k_i(Y(A)).$$

  Cela traduit l'inégalité de diagrammes : $Y(B) \geq Y(A)$.

- Nous allons montrer que toute orbite de la forme $\mathcal{O}_B$ avec $Y(A) \leq Y(B)$ est incluse dans l'adhérence. Commençons par montrer que si $Y(A) \leq_{\text{el}} Y(B)$ alors $\mathcal{O}_B \subset \overline{\mathcal{O}_A}$. Supposons que $Y(A)$ et $Y(B)$ ont seulement deux colonnes. Plus précisément supposons que B (resp. A) soit une matrice dont le diagramme de Young a deux colonnes de hauteur p et q (resp.

$p+1$ et $q-1$) :

B : 

A : 

Pour $m \in \mathbb{N}^*$ posons

$$A_m = \begin{pmatrix} J_p & 0 \\ 0 & J_q \end{pmatrix} + \frac{1}{m} E_{n,p}$$

où $E_{n,p}$ désigne la matrice élémentaire dont le seul coefficient non nul a pour indice (n,p). Nous pouvons vérifier que [2]

a) $\operatorname{rg} A_m = n-1$,

b) $A_m^{p+1} = 0$,

c) $A_m^p \neq 0$.

Alors $Y(A_m) = Y(A)$. En effet le diagramme $Y(A_m)$ possède deux colonnes, celle de gauche de hauteur $p+1$, la seconde s'en déduisant. Le Théorème 9.4.2 assure que A_m est semblable à A pour tout m et donc $\mathcal{O}_A = \mathcal{O}_{A_m}$. Puisque

$$\lim_{m \to +\infty} A_m = \begin{pmatrix} J_p & 0 \\ 0 & J_q \end{pmatrix} = B' \sim B$$

nous avons $B' \in \overline{\mathcal{O}_{A'}} = \overline{\mathcal{O}_A}$. Or $\overline{\mathcal{O}_A}$ est stable par l'action de $\mathrm{GL}(n,\mathbb{C})$ par continuité de l'action d'où $\mathcal{O}_B \subset \overline{\mathcal{O}_A}$.

Considérons maintenant le cas où $Y(A)$ et $Y(B)$ ont plus de deux colonnes. Puisque $Y(A) \leq_{\mathrm{el}} Y(B)$ toutes les colonnes sauf deux restent inchangées ; il suffit donc de construire la même suite $(A_m)_m$ en ajoutant éventuellement des blocs de Jordan constants par rapport à m lorsque la colonne correspondante est inchangée. Par conséquent si $Y(A) \leq_{\mathrm{el}} Y(B)$, alors $\mathcal{O}_B \subset \overline{\mathcal{O}_A}$.

Supposons que $Y(A) \leq Y(B)$. Nous pouvons trouver des diagrammes de Young Y_0, Y_1, …, Y_r et des matrices B_0, B_1, …, B_r telles que

$$Y(A) = Y_r = Y(B_r) \leq_{\mathrm{el}} Y_{r-1} = Y(B_{r-1}) \leq_{\mathrm{el}} \ldots \leq_{\mathrm{el}} Y_0 = Y(B_0) = Y(B)$$

Alors

$$\mathcal{O}_B = \mathcal{O}_{B_0} \subset \overline{O_{B_1}} \subset \overline{\overline{O_{B_2}}} \subset \ldots \subset \overline{\overline{\overset{\vdots}{\overline{O_{B_r}}}}} = \overline{\mathcal{O}_A}.$$

d'où l'énoncé.

2. L'assertion a) s'obtient en calculant le noyau de A_m, l'assertion b) en montrant que pour i nous avons $A^{p+1} e_i = 0$ et enfin pour l'assertion c) il suffit de voir que $A^p e_1 = \frac{1}{m} e_n \neq 0$.

□

Corollaire 9.4.2

L'orbite nulle est la seule orbite fermée.
L'orbite du bloc de Jordan de taille maximale est la seule orbite ouverte.
Elles sont caractérisées par les diagrammes

$$0_n : \underbrace{\square\square\cdots\square\square}_{n}$$

et

$$J_n : \left.\begin{array}{c}\square\\ \square\\ \vdots\\ \square\end{array}\right\} n$$

Quelles sont les propriétés topologiques des autres orbites ?

Corollaire 9.4.3

Toute classe $\mathcal{O}$ de similitude nilpotente est localement fermée, *i.e.* $\mathcal{O}$ est ouverte dans $\overline{\mathcal{O}}$.

Démonstration. — Soit Y le diagramme de Young associé à l'orbite nilpotente $\mathcal{O} = \mathcal{O}_Y$ (Théorème 9.4.2). Montrer que $\mathcal{O}$ est ouverte dans $\overline{\mathcal{O}}$ équivaut à montrer que $\overline{\mathcal{O}} \smallsetminus \mathcal{O}$ est fermé dans $\overline{\mathcal{O}}$. Or le Théorème 9.4.5 assure que

$$\overline{\mathcal{O}} \smallsetminus \mathcal{O} = \bigsqcup_{Y' > Y} \mathcal{O}_{Y'}$$

qui est fermé dans $\mathcal{M}(n,\mathbb{C})$ et donc dans $\overline{\mathcal{O}}$ par transitivité de l'ordre sur les diagrammes. □

9.4.3. Action de $\mathrm{GL}(n,\mathbb{C})$ sur $\mathrm{M}(n,\mathbb{C})$ par conjugaison. — Nous sommes tentés par l'idée de nous servir des classifications du cas diagonalisable (par le polynôme caractéristique) et du cas nilpotent (diagrammes de Young) et de conclure par la décomposition de Dunford. Nous verrons qu'il y a un piège (Remarque 9.4.6) mais avant ça rappelons quelques résultats obtenus précédemment.

◇ Cas diagonalisable.

- L'action par conjugaison de $\mathrm{GL}(n,\mathbb{C})$ stabilise l'ensemble $\mathcal{D}(n,\mathbb{C})$ des matrices diagonalisables de $\mathrm{M}(n,\mathbb{C})$.
- Deux matrices de $\mathcal{D}(n,\mathbb{C})$ sont conjuguées (*i.e.* semblables) si et seulement si elles ont même polynôme caractéristique, ou si elles ont mêmes valeurs propres avec multiplicités, modulo permutation. Autrement dit ${\mathrm{D}(n,\mathbb{C})}/{\mathrm{GL}(n,\mathbb{C})}$ et ${\mathbb{C}^n}/{\mathfrak{S}_n}$ sont en bijection. De plus lorsque les espaces sont munis de la topologie quotient, cette bijection établit un homéomorphisme entre l'espace quotient ${\mathrm{D}(n,\mathbb{C})}/{\mathrm{GL}(n,\mathbb{C})}$ et l'espace topologique connexe ${\mathbb{C}^n}/{\mathfrak{S}_n}$.
- Dans chaque orbite de $\mathrm{D}(n,\mathbb{C})$ il y a un élément de forme normale : la matrice diagonale $\mathrm{diag}(d_1,\, d_2,\, \ldots,\, d_n)$ où les d_i peuvent être choisis à permutation près.
- La « diagonalisabilité » possède une caractérisation topologique : une $\mathrm{GL}(n,\mathbb{C})$-orbite de $\mathrm{M}(n,\mathbb{C})$ appartient à $\mathrm{D}(n,\mathbb{C})$ si et seulement si elle est fermée. Néanmoins la réunion de toutes ces orbites fermées n'est plus un fermé (pour $n \geq 2$) puisqu'il s'agit de l'ensemble des matrices diagonalisables qui est dense dans $\mathrm{M}(n,\mathbb{C})$.

◇ Cas nilpotent.

- L'action par conjugaison de $\mathrm{GL}(n,\mathbb{C})$ stabilise l'ensemble $\mathcal{N}(n,\mathbb{C})$ des matrices nilpotentes de $\mathrm{M}(n,\mathbb{C})$.
- Concernant les invariants de similitude il y a deux aspects :
  - géométrique : deux matrices de $\mathcal{N}(n,\mathbb{C})$ sont conjuguées si et seulement si la suite (k_i) des dimensions des noyaux emboîtés est la même pour les deux matrices ;
  - algébrique, ou disons matriciel : deux matrices A et B de $\mathcal{N}(n,\mathbb{C})$ sont conjuguées si et seulement s'il existe une partition $(\nu_1 \geq \nu_2 \geq \ldots \geq \nu_s)$ telle que A et B sont conjuguées à la matrice diagonale par blocs $\mathrm{diag}(J_{\nu_1},\, J_{\nu_2},\, \ldots,\, J_{\nu_s})$. Le tableau de Young, qui est un objet combinatoire, fait le lien de part sa lecture à la fois horizontale et verticale entre les deux aspects. L'ensemble ${\mathcal{N}(n,\mathbb{C})}/{\mathrm{GL}(n,\mathbb{C})}$ et l'ensemble $\mathcal{P}_n$ des partitions de n sont en bijection. Par conséquent le cardinal de ${\mathcal{N}(n,\mathbb{C})}/{\mathrm{GL}(n,\mathbb{C})}$ est égal au nombre de partitions de n.
- Dans chaque orbite de $\mathrm{N}(n,\mathbb{C})$ il y a un élément de forme normale : la matrice diagonale par blocs $\mathrm{diag}(J_{\nu_1},\, J_{\nu_2},\, \ldots,\, J_{\nu_s})$.
- Il y a dans $\mathcal{N}(n,\mathbb{C})$ une unique orbite ouverte. Il s'agit de l'orbite de la matrice de Jordan indécomposable J_n. Nous pouvons également caractériser cette orbite
  - algébriquement : c'est l'ensemble des matrices N telles que $N^n = 0$ et $N^{n-1} \neq 0$;

— géométriquement : c'est l'ensemble des matrices N telles que $\dim \ker N^i = i$ pour tout $1 \leq i \leq n$;

— combinatoirement : c'est l'orbite associée au tableau de Young constitué d'une seule colonne.

Remarque 9.4.6. — Lorsque nous écrivons les décompositions de Dunford de deux matrices $A = D + N$ et $A' = D' + N'$, alors A est semblable à A' implique que D est semblable à D' et N est semblable à N'.

Mais la réciproque est fausse comme le montre le contre-exemple suivant. Les matrices

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

ne sont pas semblables car elles n'ont pas le même polynôme minimal ($X(X-1)^2$ pour la première et $X^2(X-1)$ pour la seconde).

Il faut donc avoir des hypothèses plus fines, non pas sur la décomposition de Dunford dans sa globalité, mais localement, *i.e.* pour chaque sous-espace caractéristique.

Dans l'énoncé qui suit notons n_w l'endomorphisme induit par la composante nilpotente n de l'endomorphisme u au sous-espace caractéristique associé à la valeur propre w.

Théorème 9.4.6

Soit $u = d + n$ et $u' = d' + n'$ les décompositions de Dunford de deux endomorphismes complexes de même polynôme caractéristique χ.
Si u est semblable à u', alors pour toute valeur propre w de u (donc de u'), le tableau de Young $Y(n_w)$ est égal au tableau de Young $Y(n'_w)$. En particulier d est semblable à d' et n est semblable à n'.
Réciproquement si pour toute racine w de χ, $Y(n_w) = Y(n'_w)$, alors u est semblable à u'.

Démonstration. — Écrivons χ sous la forme $\chi = \prod_w (X - w)^{k_w}$.

Supposons que les endomorphismes u et u' soient semblables. Soit g inversible tel que $u' = gug^{-1}$. Alors $d' + n' = gdg^{-1} + gng^{-1}$. Le membre de droite est également une décomposition de Dunford ; l'unicité de la décomposition de Dunford implique que d et d' sont semblables ainsi que n et n'.

Soit w, avec la multiplicité k_w dans le spectre de u (et donc dans celui de u'). L'automorphisme g envoie le sous-espace caractéristique $\ker(u - w\mathrm{id})^{k_w}$ de u sur le sous-espace caractéristique $\ker(u' - w\mathrm{id})^{k_w}$ de u'. Soit u_w (resp. u'_w) l'endomorphisme induit par u sur $\ker(u - w\mathrm{id})^{k_w}$

(resp. $\ker(u' - w\mathrm{id})^{k_w}$). Nous avons $u'_w = g u_w g^{-1}$ et comme, par construction de la décomposition de Dunford, $u_w = w\mathrm{id} + n_w$ et $u'_w = w\mathrm{id} + n'_w$ sont les décompositions de Dunford respectives de u_w et u'_w il vient donc $n'_w = g n_w g^{-1}$. Ainsi n'_w et n_w ont même dimensions de noyaux emboîtés.

Réciproquement désignons par $\nu_1 \geq \nu_2 \geq \ldots \geq \nu_s$ le nombre de cases des colonnes du tableau de Young $Y(n_w)$. Il existe une base de $\ker(u - w\mathrm{id})^{n_w}$ dans laquelle n_w s'écrit matriciellement $\mathrm{diag}(J_{\nu_1}, J_{\nu_2}, \ldots, J_{\nu_s})$; par suite u_w s'écrit matriciellement $w\mathrm{id}_{k_w} + \mathrm{diag}(J_{\nu_1}, J_{\nu_2}, \ldots, J_{\nu_s})$. Il en est de même pour u'_w puisque u_w et u'_w ont même tableau de Young associé. Ceci étant vrai pour toute valeur propre w, nous obtenons que u et u' ont des matrices communes dans des bases différentes, *i.e* que u et u' sont semblables.

□

Exemple 9.4.5. — Reprenons les matrices de la Remarque 9.4.6 ; elles ne sont pas semblables car pour la première nous avons

$T(Y_0) =$ $T(Y_1) =$

et pour la seconde

$T(Y_0) =$ $T(Y_1) =$

Invariants de similitude sur $\mathbb{C}$, cas général

- L'action par conjugaison de $\mathrm{GL}(n, \mathbb{C})$ stabilise l'espace $\mathrm{M}(n, \mathbb{C})$ des matrices de taille n à coefficients dans $\mathbb{C}$.

  Concernant les invariants de similitude il y a deux aspects :

- un aspect géométrique : deux matrices de $\mathrm{M}(n, \mathbb{C})$ sont conjuguées si et seulement si elles ont même spectre et si, pour tout élément w du spectre, la suite (k_i^w) des dimensions des noyaux emboîtés associés à la valeur propre w, à savoir les $\dim \ker(u - w\mathrm{id})^i$, est la même pour les deux matrices.
- un aspect matriciel : dans chaque orbite de $\mathrm{M}(n, \mathbb{C})$ il y a un élément de forme normale : la matrice diagonale par blocs

$$\mathrm{diag}\Big(\mathrm{diag}(J_{v_1^w} + w\mathrm{id}_{v_1^w}, J_{v_2^w} + w\mathrm{id}_{v_2^w}, \ldots, J_{v_{t^w}^w} + w\mathrm{id}_{v_{t^w}^w})\Big)$$

  unique modulo permutation des w dans le spectre pour une partition ν fixée pour chaque w dans le spectre.

Topologie des orbites

Fixons un polynôme $\chi = \prod (X - w_i)^{n_i}$ de degré n. Nous nous restreignons à l'action de $\mathrm{GL}(n, \mathbb{C})$ sur l'ensemble

$$\mathrm{M}(n, \chi) = \{M \in \mathrm{M}(n, \mathbb{C}) \,|\, \chi_M = \chi\}$$

des matrices qui ont pour polynôme caractéristique χ. Notons que $\mathrm{M}(n,\chi)$ est un fermé de l'espace des matrices puisque l'application $A \mapsto \chi_A$ est continue. L'énoncé suivant en résulte :

Théorème 9.4.7

La matrice M appartient à l'adhérence de l'orbite de M' si et seulement si $\chi_M = \chi_{M'}$ et, pour tout élément du spectre, nous avons $Y(N_w) \geq Y(N'_w)$.

9.4.4. Et sur $\mathbb{R}$? — Nous pouvons nous demander comment résoudre le problème analogue sur $\mathbb{R}$. Un résultat classique est le suivant :

Proposition 9.4.4

Deux matrices réelles sont $\mathrm{GL}(n,\mathbb{C})$-semblables si et seulement si elles sont $\mathrm{GL}(n,\mathbb{R})$-semblables.

Démonstration. — Soient A et B deux matrices réelles.

Si elles sont semblables sur $\mathbb{R}$, elles le sont sur $\mathbb{C}$.

Réciproquement supposons que A et B soient semblables sur $\mathbb{C}$, *i.e.* il existe $P \in \mathrm{GL}(n,\mathbb{C})$ telle que $A = P^{-1}BP$. Par conséquent $PA = BP$. On écrit alors $P = Q + \mathbf{i}R$ avec Q, R dans $\mathrm{M}(n,\mathbb{R})$. On a donc $QA + \mathbf{i}RA = BQ + \mathbf{i}BR$. En travaillant coefficients par coefficients et en identifiant partie réelle et partie imaginaire nous obtenons $QA = BQ$ et $RA = BR$. Par suite pour tout $t \in \mathbb{R}$ nous avons $(Q + tR)A = B(Q + tR)$. Puisque $Q + tR$ appartient à $\mathrm{M}(n,\mathbb{R})$ il s'agit de montrer qu'il existe au moins un réel t pour lequel $Q + tR$ appartient à $\mathrm{GL}(n,\mathbb{R})$. Considérons l'application

$$\varphi\colon \mathbb{C} \to \mathbb{C}, \qquad t \mapsto \det(Q + tR)$$

L'application φ est une application polynomiale puisque le déterminant en est une. Comme P appartient à $\mathrm{GL}(n,\mathbb{C})$ on en déduit que $\varphi(\mathbf{i}) \neq 0$ et en particulier l'application φ est non nulle. L'application polynomiale φ admet donc un nombre fini de racines et il s'en suit qu'il existe $t \in \mathbb{R}$ tel que $\varphi(t) \neq 0$ soit $\det(Q + tR) \neq 0$ ou encore $Q + tR$ appartient à $\mathrm{GL}(n,\mathbb{R})$. □

Corollaire 9.4.4

L'orbite d'une matrice réelle A sous l'action de $\mathrm{GL}(n,\mathbb{R})$ est donc exactement l'intersection de l'orbite de A sous l'action de $\mathrm{GL}(n,\mathbb{C})$ avec $\mathrm{M}(n,\mathbb{R})$:

$$\mathrm{GL}(n,\mathbb{R}) \cdot A = \mathrm{GL}(n,\mathbb{C}) \cdot A \cap \mathrm{M}(n,\mathbb{R}).$$

9.5. Exemples d'actions classiques de groupes classiques

groupe	ensemble	action	espace quotient	invariant
$\Bbbk^*$	vecteurs non nuls : $\Bbbk^{n+1} \smallsetminus \{0\}$	$\lambda \cdot v = \lambda v$	$\mathbb{P}^n_{\Bbbk}$	droites de $\Bbbk^{n+1}$
$\mathrm{SO}(2)$	couples de droites du plan	action diagonale	$\mathbb{R}/\pi\mathbb{R}$	angles de droites
$\mathrm{SO}(2)$	couples de vecteurs de norme 1	$g \cdot (v, v') = (gv, gv')$	$\mathbb{R}/2\pi\mathbb{R}$	angles orientés de vecteurs
$\mathrm{GL}(n, \Bbbk)$	sous-espaces vectoriels de $\Bbbk^n$	$g \cdot F = g(F)$	$\{0, 1, \ldots, n\}$	dimension

groupe	ensemble	action	espace quotient	invariant
$\mathrm{GL}(m,\Bbbk)$ $\times\mathrm{GL}(n,\Bbbk)$	$M_{m,n}(\Bbbk)$	$(P,Q)\cdot A = PAQ^{-1}$	$\{0,\,1,\,\ldots,\min(m,n)\}$	rang
$\mathrm{GL}(n,\Bbbk)$	matrices diagonalisables	$P\cdot A = PAP^{-1}$	$\Bbbk^n/\mathfrak{S}_n$	valeurs propres
$\mathrm{GL}(n,\Bbbk)$	matrices nilpotentes	$P\cdot A = PAP^{-1}$	partitions de n	tableaux de Young

groupe	ensemble	action	espace quotient	invariant
$\mathrm{GL}(n,\mathbb{R})$	matrices symétriques	$P \cdot A = PA^{\mathrm{t}}P$	$\{(p,q,r) \in \mathbb{N}^3 \mid p+q+r=n\}$	signature et rang
$\mathrm{GL}(n,\mathbb{R})$	matrices symétriques inversibles	$P \cdot A = PA^{\mathrm{t}}P$	$\{(p,q) \in \mathbb{N}^2 \mid p+q=n\}$	signature
$\mathrm{PGL}(2,\mathbb{C})$	quadruplets de points de $\mathbb{C} \cup \{\infty\}$ dont les 3 premiers sont distincts	$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$	$\mathbb{P}^1_{\mathbb{C}}$	birapport

$\mathrm{GL}(n,\mathbb{Z})$	sous-réseaux de $\mathbb{Z}$	$g \cdot \mathcal{R} = g(\mathcal{R})$	$d_1 \mid d_2 \mid \ldots \mid d_r \in \mathbb{N}$, $0 \leq r \leq n$	rang et invariants de la base adaptée
$\mathrm{GL}(n,\mathbb{C})$	$\mathrm{M}(n,\mathbb{C})$	$P \cdot A = PAP^{-1}$	$P_1 \mid P_2 \mid \ldots \mid P_n$ polynômes unitaires	invariants de similitude
$\mathrm{GA}(n,\mathbb{R})$	coniques du plan	$g \cdot \mathcal{C} = g(\mathcal{C})$	ellipses, hyperboles, paraboles...	classification des coniques

9.5.1. Exemples d'actions transitives liées au théorème de la base incomplète. —

groupe	ensemble	stabilisateur
$\mathfrak{S}_n$	$\{1, 2, \ldots, n\}$	de $1 \leq k \leq n$: $\mathfrak{S}_{\{1,2,\ldots,n\} \smallsetminus \{k\}}$
$\mathrm{GL}(n, \Bbbk)$	$\Bbbk^n \smallsetminus \{0\}$	de e_1 : $\mathrm{GL}(n-1, \Bbbk) \ltimes \Bbbk^{n-1}$
$\mathrm{O}(q)$	$\Bbbk^n \smallsetminus \{0\}$	
$\mathrm{SO}(n)$	$\mathbb{S}^{n-1}$	de e_1 : $\mathrm{SO}(n-1)$
$\mathrm{SU}(n)$	$\mathbb{S}^{2n-2}$	de e_1 : $\mathrm{SU}(n-1)$

9.5.2. Exemples d'actions simplement transitives liées au théorème de la base incomplète. —

groupe	ensemble
$\mathrm{GL}(n, \Bbbk)$	{ bases vectorielles de $\Bbbk^n$ }
$\mathrm{O}(n)$	{ bases orthonormales euclidiennes }
$\mathrm{SO}(n)$	{ bases orthonormales directes euclidiennes }
$\mathrm{SU}(n)$	{ bases orthonormales directes hermitiennes }
$\mathrm{Sp}(n, \Bbbk)$	{ bases orthonormées symplectiques }
$\mathrm{GA}(n, \Bbbk)$	{ repères affines (bases de $\mathbb{A}^n$) }

CHAPITRE 10

THÉORÈMES DE SYLOW

D'après le théorème de Lagrange si G est un groupe fini et H un sous-groupe de G, alors |H| divise |G|. Réciproquement, on peut se demander si dans un groupe d'ordre n il existe pour tout diviseur d de n un (ou plusieurs) sous-groupe d'ordre d. La réponse est non en général ; par exemple $\mathcal{A}_4$ est un groupe d'ordre 12 qui ne contient pas de sous-groupe d'ordre 6 (Exemple 1.6.13). Néanmoins il y a toute une classe de groupes où cette propriété est vraie, ce sont les sous-groupes de Sylow.

Dans ce paragraphe p désigne un nombre premier.

Rappelons qu'un groupe G est un p-groupe si tout élément de G a pour ordre une puissance de p.

Exemples 10.0.1. — Un groupe d'ordre p^α, $\alpha \geq 1$, est un p-groupe.

Un sous-groupe d'ordre p^α d'un groupe G est un p-sous-groupe de G.

Définition 10.0.1

Soit G un groupe d'ordre $p^\alpha m$ avec m et p premiers entre eux. Un sous-groupe de G d'ordre p^α est un *p-sous-groupe de Sylow* de G ou un *p-Sylow* de G.

Remarque 10.0.1. — Un p-Sylow est un p-groupe mais la réciproque est fausse. Dans le groupe $\mathbb{Z}/12\mathbb{Z}$ d'ordre $12 = 2^2 \times 3$ le sous-groupe $\langle 6 \rangle = \{0, 6\}$ est un 2-groupe mais pas un 2-Sylow.

Dans un groupe d'ordre $100 = 2^2 \times 5^2$, un 2-Sylow est d'ordre 4, un 5-Sylow est d'ordre 25 et un p-Sylow est trivial si $p \notin \{2, 5\}$. Dans un groupe d'ordre $12 = 2^2 \times 3$, un 2-Sylow est d'ordre 4, un 3-Sylow est d'ordre 3, et p-Sylow est trivial si $p > 3$. Donnons quelques exemples de Sylow dans les groupes d'ordre 12.

Exemple 10.0.2. — Dans $\mathbb{Z}/12\mathbb{Z}$ l'unique 2-Sylow est $\langle 3\rangle = \{0, 3, 6, 9\}$ et l'unique 3-Sylow est $\langle 4\rangle = \{0, 4, 8\}$

Exemple 10.0.3. — Dans $\mathcal{A}_4$ il y a un sous-groupe d'ordre 4, donc l'unique 2-Sylow est

$$\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = \langle (1\ 2)(3\ 4), (1\ 4)(2\ 3)\rangle$$

Il y a quatre 3-Sylow

$$\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} = \langle (1\ 2\ 3)\rangle, \qquad \{\mathrm{id}, (1\ 2\ 4), (1\ 4\ 2)\} = \langle (1\ 2\ 4)\rangle,$$
$$\{\mathrm{id}, (1\ 3\ 4), (1\ 4\ 3)\} = \langle (1\ 3\ 4)\rangle, \qquad \{\mathrm{id}, (2\ 3\ 4), (2\ 4\ 3)\} = \langle (2\ 3\ 4)\rangle.$$

Exemple 10.0.4. — Le groupe D_{12} contient trois 2-Sylow d'ordre 4 :

$$\{\mathrm{id}, r^3, s, r^3s\} = \langle r^3, s\rangle, \quad \{\mathrm{id}, r^3, rs, r^4s\} = \langle r^3, rs\rangle, \quad \{\mathrm{id}, r^3, r^2s, r^5s\} = \langle r^3, r^2s\rangle.$$

Le groupe D_{12} contient un unique 3-Sylow : $\{\mathrm{id}, r^2, r^4\} = \langle r^2\rangle$.

Exemple 10.0.5. — Le groupe $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ est d'ordre $24 = 2^3 \times 3$. Il n'est pas isomorphe à $\mathfrak{S}_4$; en effet $Z\left(\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)\right) = \{\mathrm{id}, -\mathrm{id}\}$ alors que $Z(\mathfrak{S}_4) = \mathrm{id}$. Un calcul explicite assure que $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ compte huit éléments d'ordre une puissance de 2 :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix},$$
$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}.$$

Ils forment l'unique 2-Sylow de $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ qui est isomorphe au groupe des quaternions $\mathbb{H}_8$.

Le groupe $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ compte quatre 3-Sylow :

$$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\rangle, \quad \langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\rangle, \quad \langle \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}\rangle, \quad \langle \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}\rangle.$$

Exemple 10.0.6. — Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments (p premier). Soit $\mathrm{G} = \mathrm{GL}(n, \mathbb{F}_p)$, $n \in \mathbb{N}^*$. Le groupe G est un groupe fini d'ordre

$$|\mathrm{G}| = (p^n - 1)(p^n - p)\dots(p^n - p^{n-1});$$

en effet se donner une matrice de G revient à choisir une première colonne non nulle (il y a $p^n - 1$ choix), puis une seconde colonne qui n'est pas multiple de la première (ce qui fait $p^n - p$ choix) puis une troisième colonne qui n'est pas combinaison des deux premières ce qui fait $p^n - p^2$ choix etc. En particulier

$$|\mathrm{G}| = p^{n(n-1)/2}\underbrace{(p^n - 1)(p^{n-1} - 1)(p^{n-2} - 1)\dots(p - 1)}_{m}$$

et m est premier à p.

L'ensemble des matrices triangulaires supérieures strictes

$$\mathrm{P} = \{A = (a_{ij}) \,|\, a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1\}$$

est un p-sous-groupe de Sylow de G. En effet comme les a_{ij}, pour $i < j$, sont quelconques on a

$$|\mathrm{P}| = p \times p^2 \times \ldots \times p^{n-1} = p^{n(n-1)/2}.$$

10.1. Les Théorèmes de Sylow et leurs premières conséquences

L'énoncé suivant atteste l'existence des sous-groupes de Sylow :

Théorème 10.1.1: (Premier théorème de Sylow)

Un groupe fini G contient un p-Sylow pour tout premier p et tout p-sous-groupe de G est contenu dans un p-Sylow de G.

Remarque 10.1.1. — Si p ne divise pas $|\mathrm{G}|$, le groupe G admet un unique p-Sylow, à savoir $\{e\}$.

La partie existence du Théorème 10.1.1 est illustrée dans les Exemples 10.0.2, 10.0.3, 10.0.4, 10.0.5.

Première démonstration de la première assertion du Théorème 10.1.1

Lemme 10.1.1

Soit G un groupe fini. Soit p un nombre premier tel que p divise $|\mathrm{G}|$. Écrivons $|\mathrm{G}|$ sous la forme $p^\alpha m$ où $\alpha \geq 1$ et $\mathrm{pgcd}(m, p) = 1$.
Soit H un sous-groupe de G et soit S un p-Sylow de G. Il existe $a \in \mathrm{G}$ tel que $a\mathrm{S}a^{-1} \cap \mathrm{H}$ soit un p-Sylow de H.

Démonstration. — Notons ${}^{\mathrm{G}}\!/_{\mathrm{S}}$ l'ensemble des classes à gauche modulo S. Le groupe G agit sur ${}^{\mathrm{G}}\!/_{\mathrm{S}}$ par translation à gauche :

$$\mathrm{G} \times {}^{\mathrm{G}}\!/_{\mathrm{S}} \to {}^{\mathrm{G}}\!/_{\mathrm{S}}, \qquad (g, a\mathrm{S}) \mapsto g \cdot a\mathrm{S} = ga\mathrm{S}.$$

Le stabilisateur

$$\mathrm{St}(a\mathrm{S}) = \{g \in \mathrm{G} \,|\, g \cdot a\mathrm{S} = a\mathrm{S}\}$$

de $a\mathrm{S}$ est $a\mathrm{S}a^{-1}$. Mais H opère lui aussi sur ${}^{\mathrm{G}}\!/_{\mathrm{S}}$ par restriction avec $a\mathrm{S}a^{-1} \cap \mathrm{H}$ comme stabilisateur de $a\mathrm{S}$.

Montrons qu'un de ces groupes est un Sylow de H. Ce sont déjà des p-groupes. Il suffit donc que pour un $a \in \mathrm{G}$, $\#{}^{\mathrm{H}}\!/_{(a\mathrm{S}a^{-1} \cap \mathrm{H})}$ soit premier à p.

Rappelons que l'application

$$\mathrm{G}/\mathrm{St}(x) \to \mathcal{O}_x \qquad\qquad \overline{g} \mapsto g \cdot x$$

de l'ensemble des classes à gauche dans l'orbite de x est bien définie et est une bijection.

Ainsi $\#\mathrm{H}/(a\mathrm{S}a^{-1} \cap \mathrm{H}) = \#\mathcal{O}_{a\mathrm{S}}$ où $\#\mathcal{O}_{a\mathrm{S}}$ désigne le cardinal de l'orbite de $a\mathrm{S}$ dans G/S sous l'action de H. Si tous ces nombres étaient divisibles par p, il en serait de même de $\left|\mathrm{G}/\mathrm{S}\right|$ car G/S est réunion des orbites $\mathcal{O}_{a\mathrm{S}}$: contradiction avec le fait que S est un p-Sylow de G. □

Soit G un groupe d'ordre fini n. Soit p un diviseur de n. On plonge G dans $\mathfrak{S}_n$ (Théorème 6.1.1). Puis on plonge $\mathfrak{S}_n$ dans $\mathrm{GL}(n, \mathbb{F}_p)$: l'élément σ de $\mathfrak{S}_n$ s'envoie sur l'endomorphisme u_σ défini dans la base canonique par : $u_\sigma(e_i) = e_{\sigma(i)}$.

On a donc réalisé G comme un sous-groupe de $\mathrm{GL}(n, \mathbb{F}_p)$ qui possède un p-Sylow (Exemple 10.0.6), donc G aussi par le Lemme 10.1.1. □

Démonstration du Théorème 10.1.1. — Soit p^k la plus grande puissance de p dans $|\mathrm{G}|$. Le résultat est évident si $k = 0$, puisque le sous-groupe trivial est un p-Sylow ; on peut donc supposer que $k \geq 1$ donc p divise $|\mathrm{G}|$. Nous allons démontrer un résultat plus fort qui s'énonce comme suit : G possède un sous-groupe d'ordre p^i pour $0 \leq i \leq k$. Plus précisément, si $|\mathrm{H}| = p^i$ avec $i < k$, nous allons montrer l'existence d'un p-sous-groupe $\mathrm{H}' \supset \mathrm{H}$ tel que $[\mathrm{H}' : \mathrm{H}] = p$, d'où $|\mathrm{H}'| = p^{i+1}$.

Considérons l'action par translation à gauche de H sur l'ensemble quotient G/H :

$$\mathrm{H} \times \mathrm{G}/\mathrm{H} \to \mathrm{G}/\mathrm{H}, \qquad\qquad (h, g\mathrm{H}) \mapsto h \cdot g\mathrm{H} = hg\mathrm{H}$$

Puisque H est un p-groupe, la Proposition 6.3.1 assure que

$$\#\mathrm{G}/\mathrm{H} \equiv_p \#\mathrm{G}/\mathrm{H}^{\mathrm{H}}$$

Un élément $g\mathrm{H}$ de G/H est fixé par l'action par translation à gauche de H si et seulement si

$$\begin{aligned} hg\mathrm{H} = g\mathrm{H} \quad \forall\, h \in \mathrm{H} \quad &\iff \quad hg \in g\mathrm{H} \quad \forall\, h \in \mathrm{H} \\ &\iff \quad g^{-1}hg \in \mathrm{H} \quad \forall\, h \in \mathrm{H} \\ &\iff \quad g^{-1}\mathrm{H}g \subset \mathrm{H} \\ &\iff \quad g^{-1}\mathrm{H}g \subset \mathrm{H} \text{ car } |g^{-1}\mathrm{H}g| = |\mathrm{H}| \\ &\iff \quad g \in \mathrm{N}_{\mathrm{G}}(\mathrm{H}). \end{aligned}$$

Autrement dit $\mathrm{G}/\mathrm{H}^{\mathrm{H}} = \{g\mathrm{H} \,|\, g \in \mathrm{N}_{\mathrm{G}}(\mathrm{H})\} = \mathrm{N}_{\mathrm{G}}(\mathrm{H})/\mathrm{H}$. Par conséquent $\#\mathrm{G}/\mathrm{H} \equiv_p \#\mathrm{G}/\mathrm{H}^{\mathrm{H}}$ se réécrit

$$[\mathrm{G} : \mathrm{H}] \equiv_p [\mathrm{N}_{\mathrm{G}}(\mathrm{H}) : \mathrm{H}].$$

Puisque H est un sous-groupe distingué de $\mathrm{N}_{\mathrm{G}}(\mathrm{H})$, le quotient $\mathrm{N}_{\mathrm{G}}(\mathrm{H})/\mathrm{H}$ est un groupe.

Lorsque $|\mathrm{H}| = p^i$ avec $i < k$, l'indice $[\mathrm{G} : \mathrm{H}]$ est divisible par p, donc $[\mathrm{G} : \mathrm{H}] \equiv_p [\mathrm{N}_{\mathrm{G}}(\mathrm{H}) : \mathrm{H}]$ implique que $[N_{\mathrm{G}}(\mathrm{H}) : \mathrm{H}]$ est divisible par p ; par conséquent $\mathrm{N}_{\mathrm{G}}(\mathrm{H})/\mathrm{H}$ est un groupe d'ordre

divisible par p. Ainsi ${}^{\mathrm{N_G(H)}}\!/_{\mathrm{H}}$ a un sous-groupe d'ordre p d'après le Théorème de Cauchy (Théorème 3.7.1). Tous les sous-groupes du groupe quotient ${}^{\mathrm{N_G(H)}}\!/_{\mathrm{H}}$ sont de la forme ${}^{\mathrm{H}'}\!/_{\mathrm{H}}$, où H' est un sous-groupe tel que $\mathrm{H} \subset \mathrm{H}' \subset \mathrm{N_G(H)}$. Donc un sous-groupe d'ordre p dans ${}^{\mathrm{N_G(H)}}\!/_{\mathrm{H}}$ est ${}^{\mathrm{H}'}\!/_{\mathrm{H}}$ tel que $[\mathrm{H}' : \mathrm{H}] = p$, donc $|\mathrm{H}'| = p|\mathrm{H}| = p^{i+1}$. On peut répéter cet argument jusqu'à obtenir un sous-groupe d'ordre p^k. □

Nous avons donc démontré la

Proposition 10.1.1

Un groupe fini d'ordre $p^k m$ avec p premier et $\mathrm{pgcd}(p, m) = 1$ possède un sous-groupe d'ordre p^i pour $0 \leq i \leq k$.

Exemple 10.1.1. — Le groupe D_8 d'ordre $8 = 2^3$ admet

- ◇ un sous-groupe d'ordre 1 ($\{e\}$) ;
- ◇ des sous-groupes d'ordre 2 : $\langle s\rangle$, $\langle rs\rangle$, $\langle r^2 s\rangle$, $\langle r^3 s\rangle$, $\langle r^2\rangle$;
- ◇ des sous-groupes d'ordre 4 qui sont distingués dans D_8 : $\langle r\rangle$, $\langle r^2,\, s\rangle$;
- ◇ un sous-groupe d'ordre 8 (D_8).

Le deuxième théorème de Sylow étudie la conjugaison des p-sous-groupes de Sylow :

Théorème 10.1.2: Second théorème de Sylow

Soit G un groupe fini. Pour tout nombre premier p les p-Sylow de G sont conjugués deux à deux.

Remarque 10.1.2. — Soit G un groupe fini. Soit φ un automorphisme de G.

Si P est un p-Sylow de G, alors $|\varphi(\mathrm{P})| = |\mathrm{P}| = p^\alpha$; ainsi $\varphi(\mathrm{P})$ est un p-Sylow de G.

Si de plus P est l'unique p-Sylow de G, alors $\varphi(\mathrm{P}) = \mathrm{P}$, *i.e.* P est un sous-groupe caractéristique de G.

Remarque 10.1.3. — Le Théorème 10.1.2 assure que si H et K sont deux p-Sylow de G, il existe $g \in \mathrm{G}$ tel que $g\mathrm{H}g^{-1} = \mathrm{K}$. Ceci est illustré dans le tableau ci-dessous :

groupe	ordre	p	H	K	g
$\mathcal{A}_4$	12	3	$\langle(1\ 2\ 3)\rangle$	$\langle(1\ 2\ 4)\rangle$	$(2\ 4\ 3)$
D_{12}	12	2	$\langle r^3,\, s\rangle$	$\langle r^3,\, rs\rangle$	r^2
$\mathrm{SL}\left(2, {}^{\mathbb{Z}}\!/_{3\mathbb{Z}}\right)$	24	3	$\langle\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\rangle$	$\langle\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\rangle$	$\begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}$

Lorsqu'on essaie de conjuguer un sous-groupe cyclique à un autre sous-groupe cyclique, il faut être prudent : les générateurs des deux groupes ne doivent pas nécessairement être conjugués. Par exemple, dans $\mathcal{A}_4$ les sous-groupes $\langle(1\ 2\ 3)\rangle = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$ et $\langle(1\ 2\ 4)\rangle = \{\mathrm{id}, (1\ 2\ 4), (1\ 4\ 2)\}$ sont conjugués, mais la classe de conjugaison de $(1\ 2\ 3)$ dans $\mathcal{A}_4$ est $(1\ 2\ 3), (1\ 4\ 2), (1\ 3\ 4), (2\ 4\ 3)$; il n'y a donc aucun moyen de conjuguer $(1\ 2\ 3)$ à $(1\ 2\ 4)$ par un élément de $\mathcal{A}_4$; il faut conjuguer $(1\ 2\ 3)$ à $(1\ 4\ 2)$. Les matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ sont conjuguées dans $\mathrm{GL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ mais pas dans $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$. Les sous-groupes $\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$ et $\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \rangle$ sont conjugués dans $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ et une matrice de conjugaison doit envoyer $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ sur $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.

Donnons comme application des Théorèmes 10.1.2 et 6.4.5, l'argument de Frattini énoncé et démontré par Frattini en 1885 :

Lemme 10.1.2: (Frattini)

Soient G un groupe fini et $\mathrm{H} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. Pour tout $\mathrm{S} \in \mathrm{Syl}_p(\mathrm{H})$ nous avons $\mathrm{G} = \mathrm{H}N_{\mathrm{G}}(\mathrm{S})$.

Démonstration. — Puisque G agit par conjugaison sur H, il agit sur $\mathrm{Syl}_p(\mathrm{H})$ pour tout p premier. Le deuxième théorème de Sylow (Théorème 10.1.2) assure que l'action par conjugaison de H sur $\mathrm{Syl}_p(\mathrm{H})$ est transtive. Il résulte que pour tout $\mathrm{S} \in \mathrm{Syl}_p(\mathrm{H})$ nous avons $\mathrm{G} = \mathrm{H}\mathrm{St}_{\mathrm{G}}(\mathrm{S}) = \mathrm{H}N_{\mathrm{G}}(\mathrm{S})$. □

Corollaire 10.1.1

Soient G un groupe fini et S un p-Sylow de G. Si H est un sous-groupe de G tel que $N_{\mathrm{G}}(\mathrm{S}) \subset \mathrm{H}$, alors $N_{\mathrm{G}}(\mathrm{H}) = \mathrm{H}$.

Démonstration. — Les inclusions $N_{\mathrm{G}}(\mathrm{S}) \subset \mathrm{H} \subset \mathrm{G}$ entraînent les inclusions $\mathrm{S} \subset \mathrm{H} \subset \mathrm{G}$.

Étant donné que S est un p-Sylow de G, S est aussi un p-Sylow de H. D'autre part H est un sous-groupe distingué de $N_{\mathrm{G}}(\mathrm{H})$. En appliquant le Lemme 10.1.2 au groupe H considéré comme sous-groupe de $N_{\mathrm{G}}(\mathrm{H})$, nous obtenons que $N_{\mathrm{G}}(\mathrm{H}) = \mathrm{H}N_{\mathrm{G}}(\mathrm{S})$. Finalement l'inclusion $N_{\mathrm{G}}(\mathrm{S}) \subset \mathrm{H}$ implique l'égalité $N_{\mathrm{G}}(\mathrm{H}) = \mathrm{H}$. □

Démonstration du Théorème 10.1.2. — Soient P et Q deux p-Sylow de G. Considérons l'action de Q sur ${}^{\mathrm{G}}\!/_{\mathrm{P}}$ par translation à gauche :

$$\mathrm{Q} \times {}^{\mathrm{G}}\!/_{\mathrm{P}} \to {}^{\mathrm{G}}\!/_{\mathrm{P}}, \qquad (q, g\mathrm{P}) \mapsto q \cdot g\mathrm{P} = qg\mathrm{P}$$

Comme Q est un p-groupe, la Proposition 7.3.1 assure que $\#{}^{\mathrm{G}}\!/_{\mathrm{P}} \equiv_p \#{}^{\mathrm{G}}\!/_{\mathrm{P}}{}^{\mathrm{Q}}$ c'est-à-dire $[\mathrm{G} : \mathrm{P}] \equiv_p \#{}^{\mathrm{G}}\!/_{\mathrm{P}}{}^{\mathrm{Q}}$. Notons que P étant un p-Sylow de G, nous avons $[\mathrm{G} : \mathrm{P}] \not\equiv_p 0$. Par suite $\#{}^{\mathrm{G}}\!/_{\mathrm{P}}{}^{\mathrm{Q}} \not\equiv_p 0$: il y a (au moins) un point fixe dans ${}^{\mathrm{G}}\!/_{\mathrm{P}}$. Soit $g\mathrm{P}$ un point fixe de ${}^{\mathrm{G}}\!/_{\mathrm{P}}$; nous avons $qg\mathrm{P} = g\mathrm{P}$ pour tout $q \in \mathrm{Q}$ ou encore qg appartient à $g\mathrm{P}$ pour tout $q \in \mathrm{Q}$ d'où $\mathrm{Q} \subset g\mathrm{P}g^{-1}$. Finalement d'une part $\mathrm{Q} \subset g\mathrm{P}g^{-1}$ et d'autre part $|\mathrm{Q}| = |g\mathrm{P}g^{-1}|$ d'où l'égalité $\mathrm{Q} = g\mathrm{P}g^{-1}$. □

Théorème 10.1.3: Troisième théorème de Sylow

Soit G un groupe fini. Écrivons $|\mathrm{G}|$ sous la forme $p^\alpha m$ où p désigne un nombre premier, $\alpha \geq 1$ et $\mathrm{pgcd}(m, p) = 1$.
Soit n_p le nombre de p-Sylow de G. Alors $n_p \equiv_p 1$ et n_p divise m.

Remarque 10.1.4. — Que dit le Théorème 10.1.2 sur le nombre de 2-Sylow et 3-Sylow d'un groupe d'ordre $12 = 2^2 \times 3$? Pour $p = 2$ et $p = 3$ les conditions de divisibilité du Théorème 10.1.2 sont $n_2 \mid 3$ et $n_3 \mid 4$ et les conditions de congruence sont $n_2 \equiv_2 1$ et $n_3 \equiv_3 1$. Les conditions de divisibilité impliquent que n_2 appartient à $\{1, 3\}$ et n_3 appartient à $\{1, 2, 4\}$. La congruence $n_2 \equiv_2 1$ ne nous dit rien de nouveau (1 et 3 sont tous deux impairs), mais la congruence $n_3 \equiv_3 1$ exclut la possibilité $n_3 = 2$. Ainsi lorsque $|\mathrm{G}| = 12$, l'entier n_2 vaut 1 ou 3 et n_3 vaut 1 ou 4.

Remarque 10.1.5. — Que dit le Théorème 10.1.2 sur le nombre de 2-Sylow et 3-Sylow d'un groupe d'ordre 24 ? Nous constatons de nouveau que n_2 vaut 1 ou 3 tandis que n_3 vaut 1 ou 4. (Par exemple à partir de $n_3|8$ et $n_3 \equiv_3 1$ les seuls choix sont $n_3 = 1$ et $n_3 = 4$).

Le tableau ci-dessous donne les valeurs de n_2 et n_3 dans certains des exemples évoqués précédemment.

groupe	ordre	n_2	n_3
${}^{\mathbb{Z}}\!/_{12\mathbb{Z}}$	12	1	1
$\mathcal{A}_4$	12	1	4
D_{12}	12	3	1
$\mathrm{SL}\left(2, {}^{\mathbb{Z}}\!/_{3\mathbb{Z}}\right)$	24	1	4

Démonstration du Théorème 10.1.3. — ⋄ Montrons tout d'abord que $n_p \equiv_p 1$. Considérons l'action de P sur $\mathrm{Syl}_p(\mathrm{G})$ par conjugaison :

$$\mathrm{P} \times \mathrm{Syl}_p(\mathrm{G}) \to \mathrm{Syl}_p(\mathrm{G}), \qquad (g, \mathrm{H}) \mapsto g \cdot \mathrm{H} = g\mathrm{H}g^{-1}$$

Le cardinal de $\mathrm{Syl}_p(\mathrm{G})$ est n_p. Comme P est un p-groupe, la Proposition 7.3.1 assure que $\#\mathrm{Syl}_p(\mathrm{G}) \equiv_p \#\mathrm{Syl}_p(\mathrm{G})^{\mathrm{P}}$, soit $n_p \equiv_p \#\mathrm{Syl}_p(\mathrm{G})^{\mathrm{P}}$. Un élément de $\mathrm{Syl}_p(\mathrm{G})^{\mathrm{P}}$ est un élément Q de $\mathrm{Syl}_p(\mathrm{G})$ tel que $g\mathrm{Q}g^{-1} = \mathrm{Q}$ pour tout $g \in \mathrm{P}$. Notons que P appartient à $\mathrm{Syl}_p(\mathrm{G})^{\mathrm{P}}$. Soit Q un autre élément de $\mathrm{Syl}_p(\mathrm{G})^{\mathrm{P}}$. Remarquons que $\mathrm{Q}, \mathrm{P} \subset \mathrm{N}_{\mathrm{G}}(\mathrm{Q})$ et donc que Q et P sont des p-Sylow de $\mathrm{N}_{\mathrm{G}}(\mathrm{Q})$. Le Théorème 10.1.2 appliqué au groupe $\mathrm{N}_{\mathrm{G}}(\mathrm{Q})$ assure que P et Q sont conjugués dans $\mathrm{N}_{\mathrm{G}}(\mathrm{Q})$. Comme Q est un sous-groupe distingué de $N_{\mathrm{G}}(\mathrm{Q})$ l'unique sous-groupe de $N_{\mathrm{G}}(\mathrm{Q})$ conjugué à Q est Q. Il en résulte que $\mathrm{P} = \mathrm{Q}$. Par suite P est l'unique point fixe de l'action de P sur $\mathrm{Syl}_p(\mathrm{G})$; on en déduit que $n_p \equiv_p 1$.

◇ Montrons désormais que n_p divise m. Considérons l'action de G par conjugaison sur $\mathrm{Syl}_p(\mathrm{G})$:

$$\mathrm{G} \times \mathrm{Syl}_p(\mathrm{G}) \to \mathrm{Syl}_p(\mathrm{G}), \qquad (g, \mathrm{H}) \mapsto g \cdot \mathrm{H} = g\mathrm{H}g^{-1}$$

Puisque les p-Sylow sont deux à deux conjugués (Théorème 10.1.2), l'action est transitive (*i.e.* il y a une orbite). Le cardinal d'un ensemble sur lequel un groupe agit avec une unique orbite divise l'ordre du groupe (cela découle d'une part du fait que le cardinal de l'ensemble est égal à celui de l'orbite et d'autre part de la bijection entre l'orbite d'un élément et le quotient du groupe par le stabilisateur de cet élément), donc n_p divise $|\mathrm{G}|$. L'égalité $n_p \equiv_p 1$ assure que n_p est relativement premier à p, donc n_p divise $|\mathrm{G}| = p^\alpha m$ implique n_p divise m.

□

Théorème 10.1.4

Soit G un groupe fini. Pour tout premier p, on désigne par n_p le nombre de p-Sylow de G. Soit P un p-Sylow de G. Alors $n_p = [\mathrm{G} : N_{\mathrm{G}}(\mathrm{P})]$.

Démonstration. — Soit P un p-Sylow de G. Considérons l'action de G sur $\mathrm{Syl}_p(\mathrm{G})$ par conjugaison

$$\mathrm{G} \times \mathrm{Syl}_p(\mathrm{G}) \to \mathrm{Syl}_p(\mathrm{G}), \qquad (g, \mathrm{H}) \mapsto g \cdot \mathrm{H} = g\mathrm{H}g^{-1}$$

La Proposition 6.3.1 assure que

$$n_p = \#\mathrm{Syl}_p(\mathrm{G}) = [\mathrm{G} : \mathrm{St}_{\mathrm{G}}(\mathrm{P})].$$

Mais

$$\mathrm{St}_{\mathrm{G}}(\mathrm{P}) = \{g \in \mathrm{G} \,|\, g\mathrm{P}g^{-1} = \mathrm{P}\} = N_{\mathrm{G}}(\mathrm{P})$$

d'où $n_p = [\mathrm{G} : N_{\mathrm{G}}(\mathrm{P})]$. □

Dans certaines démonstrations du Théorème 10.1.1, on montre que si H est un p-sous-groupe de G qui n'est pas un p-sous-groupe de Sylow alors $\mathrm{H} \subsetneq N_{\mathrm{G}}(\mathrm{H})$. Que peut-on dire de $N_{\mathrm{G}}(\mathrm{P})$ lorsque P est un p-Sylow ? Il peut ou non être plus grand (au sens de l'inclusion) que P, mais nous montrerons que prendre le normalisateur une seconde fois ne donnera rien de nouveau.

Théorème 10.1.5

Soit G un groupe fini. Soit P un p-Sylow de G. Alors $N_{\mathrm{G}}(N_{\mathrm{G}}(\mathrm{P})) = N_{\mathrm{G}}(\mathrm{P})$.
Plus généralement, si H est un sous-groupe de G qui contient $N_{\mathrm{G}}(\mathrm{P})$, alors $N_{\mathrm{G}}(\mathrm{H}) = \mathrm{H}$.

Démonstration. — L'inclusion $\mathrm{H} \subset N_{\mathrm{G}}(\mathrm{H})$ est immédiate. Montrons que réciproquement $N_{\mathrm{G}}(\mathrm{H}) \subset \mathrm{H}$. Soit x un élément de $N_{\mathrm{G}}(\mathrm{H})$; alors $x\mathrm{H}x^{-1} = \mathrm{H}$. Comme $\mathrm{P} \subset N_{\mathrm{G}}(\mathrm{P}) \subset \mathrm{H}$ nous obtenons que $x\mathrm{P}x^{-1} \subset x\mathrm{H}x^{-1} = \mathrm{H}$. Ainsi P et $x\mathrm{P}x^{-1}$ sont tous deux des p-Sylow de H. Le Théorème 10.1.2 assure l'existence de $y \in \mathrm{H}$ tel que $x\mathrm{P}x^{-1} = y\mathrm{P}y^{-1}$. Par suite $(y^{-1}x)\mathrm{P}(y^{-1}x)^{-1} = \mathrm{P}$ d'où $y^{-1}x \in N_{\mathrm{G}}(\mathrm{P}) \subset \mathrm{H}$; finalement x appartient à $y\mathrm{H} = \mathrm{H}$. □

Pour chaque théorème de Sylow, le tableau qui suit répertorie un groupe, un ensemble sur lequel le groupe agit et l'action. Soit $\mathrm{Syl}_p(\mathrm{G})$ l'ensemble des p-Sylow de G, $n_p = \#\mathrm{Syl}_p(\mathrm{G})$:

Énoncé	groupe	ensemble	action
Théorème 10.1.1	p-sous-groupe H	G/H	multiplication à gauche
Théorème 10.1.2	p-Sylow Q	G/P	multiplication à gauche
Théorème 10.1.3, $n_p \mid m$	G	$\mathrm{Syl}_p(\mathrm{G})$	conjugaison
Théorème 10.1.3, $n_p \equiv_p 1$	$\mathrm{P} \in \mathrm{Syl}_p(\mathrm{G})$	$\mathrm{Syl}_p(\mathrm{G})$	conjugaison
Théorème 10.1.4	G	$\mathrm{Syl}_p(\mathrm{G})$	conjugaison

Nous proposons une seconde démonstration du Théorème de Cauchy (*voir* le Théorème 3.7.1 pour une première version) :

Corollaire 10.1.2: (Théorème de Cauchy)

Soit G un groupe fini. Si p est un nombre premier qui divise $|\mathrm{G}|$, alors G contient un élément d'ordre p.

Démonstration. — Écrivons $|\mathrm{G}|$ sous la forme $p^\alpha m$ où $\alpha \geq 1$ et m est premier avec p.

Raisonnons par l'absurde, *i.e.* supposons qu'aucun élément de G soit d'ordre p. Alors l'ordre de tout élément de G n'est pas divisible par p ; en effet si $|\langle g \rangle| = ap$, alors g^a est d'ordre p. En particulier, tout élément du p-Sylow de G (l'existence de ce p-Sylow est assurée par le Théorème 10.1.1) est d'ordre non divisible par p et par ailleurs d'ordre divisant p^a : contradiction. □

Donnons une application du Théorème 6.4.2 pour compter les groupes de Sylow d'un groupe G. Désignons par $n_p(\mathrm{G})$ le cardinal de $\mathrm{Syl}_p(\mathrm{G})$. Si $\mathrm{H} \subset \mathrm{G}$ et $\mathrm{N} \triangleleft \mathrm{G}$, alors $n_p(\mathrm{H}) \leq n_p(\mathrm{G})$ et $n_p\left(\mathrm{G}/\mathrm{N}\right) \leq n_p(\mathrm{G})$. Ces inégalités pourraient-elles vraiment être des « divisibilités » ? Pas toujours. Il y a plusieurs copies de $\mathcal{A}_4$ dans $\mathcal{A}_5$, et $n_3(\mathcal{A}_4) = 4$ tandis que $n_3(\mathcal{A}_5) = 10$.

Cependant, si nous nous en tenons uniquement aux sous-groupes distingués, nous obtenons une relation de divisibilité :

Corollaire 10.1.3

Soit G un groupe fini. Soit $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué de G. Alors $n_p(\mathrm{N})$ divise $n_p(\mathrm{G})$ et $n_p\left({}^{\mathrm{G}}\!/_{\mathrm{N}}\right)$ divise $n_p(\mathrm{G})$.

Pour démontrer ce résultat nous aurons besoin de l'énoncé suivant :

Lemme 10.1.3

Soit G un groupe fini. Soit N un sous-groupe distingué de G.

1. Si P est un p-Sylow de G, alors $\mathrm{P} \cap \mathrm{N}$ est un p-Sylow de N ;
2. ${}^{\mathrm{PN}}\!/_{\mathrm{N}}$ est un p-Sylow de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$.

Démonstration. —

1. D'après les Théorèmes de Sylow, $\mathrm{P} \cap \mathrm{N}$ est contenu dans un p-Sylow K de N. Puisque K est un p-sous-groupe de G, il est contenu dans un conjugué de P, *i.e.* $\mathrm{K} \subset g\mathrm{P}g^{-1}$ d'où $g^{-1}\mathrm{K}g \subset \mathrm{P}$. Ainsi $g^{-1}\mathrm{K}g \subset g^{-1}\mathrm{N}g = \mathrm{N}$ donc $g^{-1}\mathrm{K}g \subset \mathrm{P} \cap \mathrm{N} \subset \mathrm{K}$. Comme $|\mathrm{K}| = |g^{-1}\mathrm{K}g|$, nous obtenons $|\mathrm{P} \cap \mathrm{N}| = |\mathrm{K}|$; par suite $\mathrm{P} \cap \mathrm{N} = \mathrm{K}$ est un p-Sylow de N.
2. Remarquons d'abord que ${}^{\mathrm{PN}}\!/_{\mathrm{N}}$ est un p-groupe (chaque élément est d'ordre une puissance de p). D'une part les inclusions $\mathrm{N} \subset \mathrm{PN} \subset \mathrm{G}$ assurent que $\left[{}^{\mathrm{G}}\!/_{\mathrm{N}} : {}^{\mathrm{PN}}\!/_{\mathrm{N}}\right] = [\mathrm{G} : \mathrm{PN}]$, d'autre part les inclusions $\mathrm{P} \subset \mathrm{PN} \subset \mathrm{G}$ assurent que $[\mathrm{G} : \mathrm{PN}] \not\equiv_p 0$. Par conséquent ${}^{\mathrm{PN}}\!/_{\mathrm{N}}$ est un p-sous-groupe de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$ dont l'indice n'est pas divisible par p, donc ${}^{\mathrm{PN}}\!/_{\mathrm{N}}$ est un sous-groupe p-Sylow de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$.

□

Démonstration. — Posons $X = \mathrm{Syl}_p(\mathrm{G})$ et $Y = \mathrm{Syl}_p(\mathrm{N})$. Le groupe G agit sur X et Y par conjugaison. Le second théorème de Sylow (Théorème 10.1.2) assure que l'action de N sur Y est transitive ainsi l'action de G sur Y est transitive. Le Lemme 10.1.3 assure que pour tout p-Sylow P de G l'intersection $\mathrm{P} \cap \mathrm{N}$ est un p-Sylow de Y ; nous pouvons donc considérer l'application

$$f : X \to Y, \qquad \mathrm{P} \mapsto \mathrm{P} \cap \mathrm{N}.$$

Puisque $g(\mathrm{P} \cap \mathrm{N})g^{-1} = g\mathrm{P}g^{-1} \cap g\mathrm{N}g^{-1} = g\mathrm{P}g^{-1} \cap \mathrm{N}$, f respecte l'action par conjugaison de G sur X et Y. Le Théorème 6.4.2 assure que $|Y|$ divise $|X|$, *i.e.* que $n_p(\mathrm{N})$ divise $n_p(\mathrm{G})$.

Posons $X = \mathrm{Syl}_p(\mathrm{G})$ et $Y = \mathrm{Syl}_p\left({}^{\mathrm{G}}\!/_{\mathrm{N}}\right)$. Le groupe G agit sur X et Y par conjugaison. L'action de G sur Y est transitive. Le Lemme 10.1.3 assure que pour tout p-Sylow P de G le

quotient PN/N est un p-Sylow de Y ; nous pouvons donc considérer l'application

$$f\colon X \to Y, \qquad \mathrm{PN}/\mathrm{N}.$$

Puisque f respecte l'action par conjugaison de G sur X et Y le Théorème 6.4.2 assure que $\#Y$ divise $\#X$, *i.e.* que $n_p\left(\mathrm{G}/\mathrm{N}\right)$ divise $n_p(\mathrm{G})$. □

10.2. Théorèmes de Sylow et sous-groupes distingués

Corollaire 10.2.1

Soit G un groupe fini. Si S est un p-Sylow de G, alors

$$\mathrm{S} \triangleleft \mathrm{G} \iff \mathrm{S} \text{ est l'unique } p\text{-Sylow de G} \iff n_p = 1.$$

Remarque 10.2.1. — En particulier, les théorèmes de Sylow sont un outil pour démontrer qu'un groupe a un sous-groupe distingué distinct de $\{e\}$ et du groupe tout entier : on peut essayer de montrer $n_p = 1$ pour certains p. Attention néanmoins il existe des groupes, $\mathfrak{S}_4$ par exemple, qui possèdent des sous-groupes distingués non triviaux mais pas de sous-groupes Sylow normaux non triviaux.

Démonstration du Corollaire 10.2.1. — Tous les p-Sylow sont conjugués (Théorème 10.1.2), donc $n_p = 1$ précisément lorsqu'un p-Sylow de G est conjugué à lui-même, c'est-à-dire qu'il est un sous-groupe distingué de G. □

Théorème 10.2.1

Soit G un groupe fini. Si p et q sont des facteurs premiers différents de $|\mathrm{G}|$, si $n_p = 1$ et $n_q = 1$; alors les éléments du p-Sylow commutent avec les éléments du q-Sylow.

Remarque 10.2.2. — Attention le Théorème 10.2.1 ne dit pas que le p-Sylow (resp. le q-Sylow) de G est abélien.

Démonstration. — Soient P le p-Sylow et Q le q-Sylow. Puisque $|\mathrm{P}|$ et $|\mathrm{Q}|$ sont premiers entre eux, $\mathrm{P} \cap \mathrm{Q} = \{e\}$ par Lagrange. Les sous-groupes P et Q de G sont distingués dans G d'après le Corollaire 10.2.1. Si x appartient à P et y à Q, alors

- ◇ $xyx^{-1}y^{-1}$ s'écrit aussi $\underbrace{(xyx^{-1})}_{\in \mathrm{Q}}\underbrace{y^{-1}}_{\in \mathrm{Q}} \in \mathrm{Q}$, en particulier $xyx^{-1}y^{-1}$ appartient à Q,
- ◇ $xyx^{-1}y^{-1}$ s'écrit aussi $\underbrace{x}_{\in \mathrm{P}}\underbrace{(yx^{-1}y^{-1})}_{\in \mathrm{P}} \in \mathrm{P}$, en particulier $xyx^{-1}y^{-1}$ appartient à P.

Comme $\mathrm{P} \cap \mathrm{Q} = \{e\}$ nous obtenons $xyx^{-1}y^{-1} = e$, à savoir $xy = yx$. □

Théorème 10.2.2

Les sous-groupes d'un groupe fini G sont distingués si et seulement si G est isomorphe au produit direct de ses sous-groupes de Sylow.

Démonstration. — Si un groupe est isomorphe au produit direct de ses Sylow alors ses Sylow sont distingués puisqu'un facteur d'un produit direct est un sous-groupe distingué du produit direct.

Réciproquement, supposons que G soit fini et que ses Sylow soient tous distingués. Écrivez les Sylow non triviaux sous la forme $\mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_m$. Le Théorème 10.2.1 assure que les éléments de P_i et P_j commutent lorsque $i \neq j$. Par suite

$$\varphi\colon \mathrm{P}_1 \times \mathrm{P}_2 \times \ldots \times \mathrm{P}_m \to \mathrm{G}, \qquad (x_1, x_2, \ldots, x_m) \mapsto x_1 x_2 \ldots x_m$$

est un morphisme de groupes. D'une part, ce morphisme est injectif : l'ordre d'un produit $g_1 g_2 \ldots g_m$ d'éléments qui commutent et sont d'ordre premiers entre eux deux à deux est égal au produit des ordres des g_i. D'autre part $|\mathrm{P}_1 \times \mathrm{P}_2 \times \ldots \times \mathrm{P}_m| = |\mathrm{G}|$. Nous en déduisons que φ est un isomorphisme de groupes. □

Les conséquences des théorèmes de Sylow dans la suite de ce paragraphe sont des cas où l'ordre de G force G à avoir un sous-groupe distingué non trivial (généralement, mais pas toujours, un Sylow distingué). Ce sujet est une source populaire d'applications, en partie parce qu'il peut être utilisé pour déterminer, à isomorphisme près, tous les groupes d'un ordre donné.

Proposition 10.2.1

Un groupe d'ordre 63 n'est pas simple.

Démonstration. — Soit G un groupe d'ordre 63. Notons que $63 = 3^2 \times 7$. On s'intéresse donc aux sous-groupes de Sylow d'ordre 7. D'une part n_7 est congru à 1 modulo 7, d'autre part n_7 divise 9 (Théorème 10.1.3). Il en résulte que $n_7 = 1$. Par conséquent G n'est pas simple (Corollaire 10.2.1). □

Théorème 10.2.3

Soit G un groupe fini d'ordre 20 ou 100. Alors G possède un 5-Sylow distingué.

Démonstration. — Soit n_5 le nombre de 5-Sylow de G. Le troisième Théorème de Sylow 10.1.3 assure que n_5 divise 4 et $n_5 \equiv_5 1$; par suite $n_5 = 1$. □

Lemme 10.2.1

Soit G un groupe fini. Si G contient k sous-groupes d'ordre p (premier), alors G possède $k(p-1)$ éléments d'ordre p.

Démonstration. — Tous les éléments non triviaux d'un groupe d'ordre p premier sont d'ordre p. Réciproquement un élément d'ordre p engendre un sous-groupe d'ordre p. Le Théorème de Lagrange (Théorème 1.6.4) assure que des sous-groupes distincts d'ordre p s'intersectent trivialement. Ainsi chaque sous-groupe d'ordre p compte $p-1$ éléments d'ordre p et aucun d'entre eux n'appartient à un autre groupe d'ordre p. Le nombre d'éléments d'ordre p est donc $k(p-1)$. □

Théorème 10.2.4

Soit G un groupe d'ordre 12. Alors ou bien G contient un 2-Sylow distingué, ou bien G contient un 3-Sylow distingué.

Exemple 10.2.1. — Par exemple,

- ◇ $\mathcal{A}_4$ compte un 2-Sylow et quatre 3-Sylow.
- ◇ alors que D_{12} compte trois 2-Sylow et un 3-Sylow.

Démonstration. — Le troisième Théorème de Sylow (Théorème 10.1.3) assure que

- ◇ n_2 divise 3, donc $n_2 = 1$ ou 3.
- ◇ n_3 divise 4 et $n_3 \equiv_3 1$, donc $n_3 = 1$ ou 4.

Supposons que $n_3 \neq 1$. Par suite $n_3 = 4$. Puisque les 3-Sylows sont d'ordre 3, le groupe G possède $n_3 \times 2 = 8$ éléments d'ordre 3 (Lemme 10.2.1). Le nombre d'éléments restants est de $12 - 8 = 4$. Un 2-Sylow est d'ordre 4 ; il en résulte que $n_2 = 1$. □

Théorème 10.2.5

Soit G un groupe d'ordre 24. Alors G contient un sous-groupe distingué d'ordre 4 ou 8.

Démonstration. — Soit P un 2-Sylow de G ; en particulier P est d'ordre 8. Considérons l'action par translation à gauche

$$\mathrm{G} \times {}^{\mathrm{G}}\!/_{\mathrm{P}}, \qquad (g, h\mathrm{P}) \mapsto g \cdot h\mathrm{P} = (gh)\mathrm{P}.$$

Elle induit un morphisme $\varphi\colon \mathrm{G} \to \mathfrak{S}_{\mathrm{G}/\mathrm{P}} \simeq \mathfrak{S}_3$. Désignons par K le noyau de φ. Nous avons :

- ◇ K est un sous-groupe de P donc $|\mathrm{K}|$ divise 8,
- ◇ ${}^{\mathrm{G}}\!/_{\mathrm{K}}$ se plonge dans $\mathfrak{S}_3$ donc $\left|{}^{\mathrm{G}}\!/_{\mathrm{K}}\right|$ divise $|\mathfrak{S}_3|$; autrement dit $\frac{|\mathrm{G}|}{|\mathrm{K}|}$ divise 6 et 4 divise $|\mathrm{K}|$.

Il en résulte que $|\mathrm{K}|$ vaut 4 ou 8. Puisque K est le noyau de φ, K est un sous-groupe distingué de G. $\square$

Exemple 10.2.2. — Considérons le groupe $\mathfrak{S}_4$. Il compte trois 2-Sylow ; en particulier $\mathfrak{S}_4$ ne possède pas de sous-groupe distingué d'ordre 8 (Corollaire 10.2.1). Ainsi le Théorème 10.2.5 assure que $\mathfrak{S}_4$ possède un sous-groupe distingué d'ordre 4. En effet,

$$\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\} \lhd \mathfrak{S}_4.$$

Le sous-groupe $\langle (1\ 2\ 3\ 4)\rangle$ de $\mathfrak{S}_4$ est d'ordre 4 mais pas distingué dans $\mathfrak{S}_4$.

Exemple 10.2.3. — Le groupe $\mathrm{SL}\left(2, \mathbb{Z}/3\mathbb{Z}\right)$ est d'ordre 24 et possède un 2-Sylow distingué.

10.2.1. Classification des groupes d'ordre 15. — Soit G un groupe d'ordre 15. Nous avons $15 = 3 \times 5$. Le nombre de 5-Sylow de G divise 3 et est congru à 1 modulo 5, le groupe G contient donc exactement un 5-Sylow que l'on note H. Puisque H est d'ordre 5 il est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Soit K un 3-Sylow de G ; il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

Le groupe H est distingué dans G, $|\mathrm{H}|$ et $|\mathrm{K}|$ sont premiers entre eux et $|\mathrm{H}| \cdot |\mathrm{K}| = |\mathrm{G}|$. Par conséquent G s'identifie à $\mathrm{H} \rtimes_\psi \mathrm{K}$ pour un certain morphisme $\phi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$. Il existe donc un morphisme $\varphi\colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/5\mathbb{Z}\right)$ tel que $\mathrm{G} \simeq \mathbb{Z}/5\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$. Comme 3 est premier à $\left|\left(\mathbb{Z}/5\mathbb{Z}\right)^\times\right| = 4$ le morphisme φ est trivial [1] et G est isomorphe au produit direct $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ c'est-à-dire à $\mathbb{Z}/15\mathbb{Z}$.

10.2.2. Classification des groupes d'ordre 21. — Soit G un sous-groupe d'ordre $21 = 3 \times 7$. Soit n_7 le nombre de 7-Sylow de G. Alors $n_7 \equiv_7 1$ et n_7 divise 3, *i.e.* $n_7 = 1$. Le groupe G contient donc un unique 7-Sylow H qui est donc distingué dans G. Puisque $|\mathrm{H}| = 7$, nous avons l'isomorphisme $\mathrm{H} \simeq \mathbb{Z}/7\mathbb{Z}$. Soit K un 3-Sylow de G ; il est isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Comme

- $\mathrm{H} \lhd \mathrm{G}$,
- $|\mathrm{H}|$ et $|\mathrm{K}|$ sont premiers entre eux,
- $|\mathrm{H}| \cdot |\mathrm{K}| = |\mathrm{G}|$

le groupe G s'identifie à $\mathrm{H} \rtimes_\psi \mathrm{K}$ pour un certain morphisme $\psi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$. Il existe donc un morphisme

$$\varphi\colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/7\mathbb{Z}\right)$$

tel que $\mathrm{G} \simeq \mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$. Nous sommes dans l'un des deux cas suivants, exclusifs l'un de l'autre :

- G est isomorphe à $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/21\mathbb{Z}$;

1. Supposons que m est premier au cardinal de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$. Dans ce cas tout élément de m-torsion de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ est trivial ; le seul produit semi-direct de la forme $\mathbb{Z}/5\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ est donc le produit direct $\mathbb{Z}/n\mathbb{Z} \times_\varphi \mathbb{Z}/m\mathbb{Z}$.

◇ G est isomorphe à $\mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ où $\varphi(\underbrace{\overline{r}}_{\text{mod } 3})(x) = \underbrace{\overline{2}^r}_{\text{mod } 7} x$.

En effet nous allons décrire tous les produits semi-directs de la forme $\mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$. Rappelons que $\mathrm{Aut}\big(\mathbb{Z}/7\mathbb{Z}\big) \simeq \big(\mathbb{Z}/7\mathbb{Z}\big)^\times$ (Proposition 7.6.2). Le groupe $\big(\mathbb{Z}/7\mathbb{Z}\big)^\times$ est égal à $\{-\overline{3}, -\overline{2}, -\overline{1}, \overline{1}, \overline{2}, \overline{3}\}$; il est cyclique (en effet si $\Bbbk$ est un corps commutatif et si G est un sous-groupe fini de $\Bbbk^\times$, alors G est cyclique). Nous avons $\overline{2} \neq \overline{1}$ et $\overline{2}^3 = \overline{8} = \overline{1}$. Par suite $\overline{2}$ est d'ordre 3 et $\langle\overline{2}\rangle = \{\overline{1}, \overline{2}, \overline{4}\}$ est donc l'unique sous-groupe d'ordre 3 de $\big(\mathbb{Z}/7\mathbb{Z}\big)^\times$ qui est aussi le groupe des éléments de 3-torsion de $\big(\mathbb{Z}/7\mathbb{Z}\big)^\times$. Les produits semi-directs cherchés sont donc les suivants :

◇ le produit $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{1}}} \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/21\mathbb{Z}$;

◇ le produit $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{2}}} \mathbb{Z}/3\mathbb{Z}$ dont la loi interne est donnée par

$$(\overline{u}, \overline{r}) \cdot (\overline{v}, \overline{s}) = (\overline{u} + \overline{2}^r \overline{v}, \overline{r} + \overline{s});$$

◇ le produit $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{4}}} \mathbb{Z}/3\mathbb{Z}$ dont la loi interne est donnée par

$$(\overline{u}, \overline{r}) \cdot (\overline{v}, \overline{s}) = (\overline{u} + \overline{4}^r \overline{v}, \overline{r} + \overline{s}).$$

Les groupes $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{2}}} \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{4}}} \mathbb{Z}/3\mathbb{Z}$ sont non abéliens. En effet dans $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{2}}} \mathbb{Z}/3\mathbb{Z}$ nous avons

$$(\overline{1}, \overline{0}) \cdot (\overline{0}, \overline{1}) = (\overline{1}, \overline{1}) \neq (\overline{2}, \overline{1}) = (\overline{0}, \overline{1}) \cdot (\overline{1}, \overline{0})$$

et dans $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{4}}} \mathbb{Z}/3\mathbb{Z}$ nous avons

$$(\overline{1}, \overline{0}) \cdot (\overline{0}, \overline{1}) = (\overline{1}, \overline{1}) \neq (\overline{4}, \overline{1}) = (\overline{0}, \overline{1}) \cdot (\overline{1}, \overline{0})$$

En particulier, ils sont tous deux non isomorphes au produit direct $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Par contre $(\overline{u}, \overline{r}) \mapsto (\overline{u}, 2\overline{r})$ définit un isomorphisme de groupes de $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{2}}} \mathbb{Z}/3\mathbb{Z}$ sur $\mathbb{Z}/7\mathbb{Z} \rtimes_{\varphi_{\overline{4}}} \mathbb{Z}/3\mathbb{Z}$ de réciproque donnée par la même formule.

10.3. Description des Sylow de certains groupes « classiques »

10.3.1. Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$**.** — Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments (p premier). Soit $\mathrm{G} = \mathrm{GL}(n, \mathbb{F}_p)$, $n \in \mathbb{N}^*$. Nous avons vu dans l'Exemple 10.0.6 que l'ensemble des matrices triangulaires supérieures strictes

$$\mathrm{P} = \big\{A = (a_{ij}) \,|\, a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1\big\}$$

est un p-sous-groupe de Sylow de G. Le Théorème 10.1.2 assure que les p-Sylow de G sont les sous-groupes de la forme $M\mathrm{P}M^{-1}$ où M appartient à $\mathrm{GL}(n, \mathbb{F}_p)$.

10.3.2. Sylow de $\mathfrak{S}_4$ et $\mathcal{A}_4$. — Soient ν_p le nombre de p-Sylow de $\mathfrak{S}_4$ et n_p le nombre de p-Sylow de $\mathcal{A}_4$.

Le groupe $\mathfrak{S}_4$ est d'ordre $24 = 2^3 \times 3$ et le groupe $\mathcal{A}_4$ d'ordre $12 = 2^2 \times 3$.

Le troisième théorème de Sylow (Théorème 10.1.3) assurent que

- ◇ ν_3 divise $2^3 = 8$ et $\nu_3 \equiv_3 1$, c'est-à-dire ν_3 appartient à $\{1, 4\}$;
- ◇ n_3 divise $2^2 = 4$ et $n_3 \equiv_3 1$, c'est-à-dire n_3 appartient à $\{1, 4\}$;
- ◇ ν_2 divise 3 et $\nu_2 \equiv_2 1$, c'est-à-dire ν_2 appartient à $\{1, 3\}$;
- ◇ n_2 divise 3 et $n_2 \equiv_2 1$, c'est-à-dire n_2 appartient à $\{1, 3\}$.

Un 3-Sylow de $\mathfrak{S}_4$ est un sous-groupe de $\mathfrak{S}_4$ d'ordre 3, *i.e.* isomorphe à $\mathbb{Z}/3\mathbb{Z}$ ou encore un sous-groupe engendré par un élément d'ordre 3. Comme les seuls éléments d'ordre 3 de $\mathfrak{S}_4$ sont les 3-cycles, les 3-Sylow de $\mathfrak{S}_4$ sont

$$\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}, \quad \{\mathrm{id}, (1\ 2\ 4), (1\ 4\ 2)\}, \quad \{\mathrm{id}, (1\ 3\ 4), (1\ 4\ 3)\}, \quad \{\mathrm{id}, (2\ 3\ 4), (2\ 4\ 3)\}.$$

Par suite $\nu_3 = 4$. Notons que tous ces groupes sont contenus dans $\mathcal{A}_4$, ce sont donc également les 3-Sylow de $\mathcal{A}_4$ si bien que $n_3 = 4$.

Construisons désormais les 2-Sylow de $\mathfrak{S}_4$. Introduisons l'ensemble X des partitions de $\{1, 2, 3, 4\}$ en deux sous-ensembles à deux éléments ; autrement dit X est constitué des trois éléments suivants

$$P_1 = \{1, 2\} \bigsqcup \{3, 4\}, \qquad P_2 = \{1, 3\} \bigsqcup \{2, 4\}, \qquad P_3 = \{1, 4\} \bigsqcup \{2, 3\}.$$

Faisons agir $\mathfrak{S}_4$ sur X ; la transposition $(2\ 3)$ envoie P_1 sur P_2, la transposition $(2\ 4)$ envoie P_1 sur P_3 donc l'action est transitive. Par suite $|\mathrm{St}_{\mathfrak{S}_4}(P_1)| = \frac{24}{3} = 8$. C'est donc un 2-Sylow de $\mathfrak{S}_4$. L'ensemble des 2-Sylow de $\mathfrak{S}_4$ est l'ensemble des conjugués de $\mathrm{St}_{\mathfrak{S}_4}(P_1)$, *i.e.*

$$\{\mathrm{St}_{\mathfrak{S}_4}(P_1), \mathrm{St}_{\mathfrak{S}_4}(P_2), \mathrm{St}_{\mathfrak{S}_4}(P_3)\}$$

(rappelons que si G est un groupe agissant sur un ensemble X, si x appartient à X et y appartient à $\mathrm{St}_{\mathrm{G}}(x)$, alors $\mathrm{St}_{\mathrm{G}}(y)$ est égal au conjugué de $\mathrm{St}_{\mathrm{G}}(x)$ par n'importe quel élément de G qui envoie x sur y). Or

$$\begin{aligned}
\mathrm{St}_{\mathfrak{S}_4}(P_1) &= \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3), (1\ 2), (3\ 4)\} \\
\mathrm{St}_{\mathfrak{S}_4}(P_2) &= \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2), (1\ 3), (2\ 4)\} \\
\mathrm{St}_{\mathfrak{S}_4}(P_3) &= \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2), (1\ 4), (2\ 3)\}
\end{aligned}$$

Ces groupes sont donc les 2-Sylow de $\mathfrak{S}_4$. Ils sont deux à deux distincts donc $\nu_2 = 3$. De plus

$$\mathrm{St}_{\mathfrak{S}_4}(P_1) \cap \mathrm{St}_{\mathfrak{S}_4}(P_2) \cap \mathrm{St}_{\mathfrak{S}_4}(P_3) = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Cette intersection coïncide avec le noyau du morphisme $\mathfrak{S}_4 \to \mathfrak{S}_X \simeq \mathfrak{S}_3$ induit par l'action de $\mathfrak{S}_4$ sur X ; c'est en particulier un sous-groupe distingué de $\mathfrak{S}_4$ qui est contenu dans $\mathcal{A}_4$. Il est a fortiori distingué dans $\mathcal{A}_4$. Il est d'ordre 4, c'est donc un 2-Sylow de $\mathcal{A}_4$; puisqu'il est distingué dans $\mathcal{A}_4$ c'est le seul 2-Sylow de $\mathcal{A}_4$ (Corollaire 10.2.1).

10.3.3. Sylow $\mathcal{A}_5$ et $\mathfrak{S}_5$. —

Théorème 10.3.1

Les groupes $\mathcal{A}_5$ et $\mathfrak{S}_5$ ont chacun dix sous-groupes d'ordre 3 et six sous-groupes d'ordre 5.

Démonstration. — Un élément d'ordre impair dans un groupe symétrique est une permutation paire, donc les 3-Sylow et les 5-Sylow de $\mathfrak{S}_5$ sont contenus dans $\mathcal{A}_5$. Il suffit donc de se concentrer sur $\mathcal{A}_5$.

Comme $|\mathcal{A}_5| = \frac{|\mathfrak{S}_5|}{2} = \frac{5!}{2} = 60 = 2^2 \times 3 \times 5$, les 3-Sylow sont d'ordre 3 et les 5-Sylows sont d'ordre 5. Désignons par n_3 (resp. n_5) le nombre de 3-Sylow (resp. 5-Sylow).

Le troisième Théorème de Sylow (Théorème 10.1.3) assure que $n_3 \,|\, 20$ et $n_3 \equiv_3 1$; ainsi n_3 appartient à $\{1, 4, 10\}$. Le nombre de 3-cycles $(a\ b\ c)$ dans $\mathcal{A}_5$ est 20, et ceux-ci viennent par paires inverses, ce qui donne 10 sous-groupes d'ordre 3. Par suite $n_3 = 10$.

En ce qui concerne les 5-Sylows, d'après le troisième Théorème de Sylow (Théorème 10.1.3) nous avons : $n_5 \,|\, 12$ et $n_5 \equiv_5 1$; il en résulte que n_5 vaut 1 ou 6. Les sous-groupes de $\mathcal{A}_5$ engendrés par $(1\ 2\ 3\ 4\ 5)$ et par $(2\ 1\ 3\ 4\ 5)$ sont différents, par conséquent $\mathcal{A}_5$ possède au moins deux sous-groupes distincts d'ordre 5 et $n_5 > 1$. Il s'en suit que $n_5 = 6$. □

10.3.4. Sylow de D_{2n}. —

Écrivons n sous la forme $p^\alpha q$ avec p premier, $\alpha \in \mathbb{N} \smallsetminus \{0\}$ et q entier non multiple de p.

- ◇ Supposons dans un premier temps que p est impair. Le sous-groupe $\langle r \rangle$ amdet un p-Sylow S. Ce dernier est aussi un p-Sylow de G car p est distinct de 2. Le Théorème 5.2.14 assure que $\mathrm{S} = \langle r^q \rangle$ et $\mathrm{S} \triangleleft \mathrm{D}_{2n}$ et que S est l'unique p-Sylow de D_{2n}.
- ◇ Supposons désormais que p soit pair.
  - Si n est impair, alors les 2-Sylow de G sont des sous-groupes d'ordre 2 et il s'agit des sous-groupes $\langle r^k s \rangle$, $0 \leq k \leq n-1$. Ils sont au nombre de n et conjugués ce qui est conforme au second Théorème de Sylow.
  - Si n est pair, alors tout 2-Sylow de S de D_{2n} est d'ordre $2^{\ell+1}$ et par le Théorème de Lagrange on ne peut avoir $\mathrm{S} \subseteq \langle r \rangle$. Il en résulte que S contient au moins une réflexion. Il est donc de la forme $\langle r^d, r^k s \rangle$ où d divise n et $0 \leq k \leq d-1$. Comme $|\langle r^d, r^k s \rangle| = 2\frac{n}{d} = 2^{\ell+1}\frac{q}{d}$ nous avons $d = q$ et les 2-Sylow de D_{2n} sont les q sous-groupes $\langle r^q, s \rangle$, $\langle r^q, rs \rangle$, …, $\langle r^q, r^{q-1}s \rangle$.

10.3.5. Sylow de groupes de certains groupes de matrices. —

Théorème 10.3.2

Le groupe $\mathrm{Aff}\left(\mathbb{Z}/5\mathbb{Z}\right)$ contient cinq 2-Sylow et un 5-Sylow.

Démonstration. — Le groupe $\mathrm{Aff}\left(\mathbb{Z}/5\mathbb{Z}\right)$ est isomorphe au groupe

$$\left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \left(\mathbb{Z}/5\mathbb{Z}\right)^{\times},\, b \in \mathbb{Z}/5\mathbb{Z}\right\}.$$

Il est d'ordre $4 \times 5 = 2^2 \times 5$. Ainsi les 2-Sylow sont d'ordre 4 et les 5-Sylow d'ordre 5.

Soit n_2 (resp. n_5) le nombre de 2-Sylow (resp. 5-Sylow).

Le troisième Théorème de Sylow (Théorème 10.1.3) assure que n_2 divise 5 et $n_2 \equiv_2 1$ d'où $n_2 \in \{1, 5\}$. Les matrices $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ engendrent deux 2-Sylow distincts ; par suite $n_2 = 5$.

D'après le troisième Théorème de Sylow (Théorème 10.1.3) nous avons : n_5 divise 4 et $n_5 \equiv_5 1$; alors $n_5 = 1$. □

Puisque nous connaissons le nombre de 2-Sylow et le nombre de 5-Sylow, nous pouvons rechercher tous les p-Sylow de $\mathrm{Aff}\left(\mathbb{Z}/5\mathbb{Z}\right)$. Les cinq matrices $\begin{pmatrix} 2 & j \\ 0 & 1 \end{pmatrix}$, où $j \in \mathbb{Z}/5\mathbb{Z}$, engendrent différents sous-groupes d'ordre 4, ce sont donc tous les 2-Sylow (et ils sont cycliques). La matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre 5 et engendre donc l'unique sous-groupe 5-Sylow. Pour illustrer le Théorème 10.1.2 dans $\mathrm{Aff}\left(\mathbb{Z}/5\mathbb{Z}\right)$, chaque élément d'ordre une puissance de 2 est conjugué à un élément du sous-groupe $\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \rangle$. Par exemple, $\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre 4 et un calcul explicite révèle

$$\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 0 & 1 \end{pmatrix}^{-1}.$$

La matrice $\begin{pmatrix} 4 & 4 \\ 0 & 1 \end{pmatrix}$ est d'ordre 2 et

$$\begin{pmatrix} 4 & 4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{2} \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix}^{-1}.$$

Remarque 10.3.1. — Il faut faire attention lorsqu'on applique les Théorèmes de Sylow. Soit G un groupe d'ordre $|\mathrm{G}| = 42 = 2 \times 3 \times 7$. Le troisième Théorème de Sylow assure que n_2 appartient à $\{1, 3, 7, 21\}$, $n_3 \in \{1, 7\}$ et $n_7 = 1$. Si p désigne un nombre premier, alors les différents sous-groupes d'ordre p s'intersectent trivialement, les $p-1$ éléments non triviaux d'un groupe d'ordre p sont d'ordre p ; il y a donc $n_p(p-1)$ éléments d'ordre p. En particulier G

compte six éléments d'ordre 7. Supposons que $n_2 = 21$ et $n_3 = 7$. Il y a au au plus vingt et un éléments d'ordre 2 et au plus quatorze éléments d'ordre 3. En ajoutant à ce décompte l'unique élément d'ordre 1, nous avons compté au plus $6 + 21 + 14 + 1 = 42$ éléments, qui est l'ordre de G. Puisque nous avons utilisé les possibilités maximales pour n_2 et n_3, et avons obtenu 42 éléments, n_2 et n_3 ne peuvent pas être plus petits que les choix maximaux, donc $n_2 = 21$ et $n_3 = 7$. Ce raisonnement est faux ; en effet, par exemple

- ◇ pour le groupe abélien $\mathbb{Z}/42\mathbb{Z}$ nous avons $n_2 = n_3 = 1$,
- ◇ pour le groupe $\mathrm{Aff}\left(\mathbb{Z}/7\mathbb{Z}\right)$ nous avons $n_2 = n_3 = 7$.

L'erreur quand on écrit « Puisque nous avons utilisé les possibilités maximales pour n_2 et n_3, et avons obtenu 42 éléments, n_2 et n_3 ne peuvent pas être plus petits que les choix maximaux, donc $n_2 = 21$ et $n_3 = 7$. » est que certains éléments peuvent avoir un ordre autre que 1, 2, 3 ou 7.

Théorème 10.3.3

Soit p un nombre premier. Chaque élément de $\mathrm{GL}\left(2, \mathbb{Z}/p\mathbb{Z}\right)$ d'ordre p est conjugué à une matrice triangulaire supérieure $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Le nombre de p-Sylow de $\mathrm{GL}\left(2, \mathbb{Z}/p\mathbb{Z}\right)$ est $p + 1$.

Démonstration. — Posons $\mathrm{G} = \mathrm{GL}\left(2, \mathbb{Z}/p\mathbb{Z}\right)$. Le groupe G est d'ordre $(p^2 - 1)(p^2 - p) = p(p-1)(p^2-1)$. En effet se donner un élément de G c'est se donner une première colonne non nulle (il y a $p^2 - 1$ colonne non nulle) et une seconde colonne non colinéaire à la première (il y a $p^2 - p$ telles colonnes). Un p-Sylow est donc d'ordre p. La matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre p donc engendre un p-Sylow qui est $\mathrm{P} = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{Z}/p\mathbb{Z} \right\}$. Puisque les p-Sylow sont conjugués, une matrice d'ordre p est conjuguée à une puissance de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. D'après le Théorème 10.1.4 le nombre de p-Sylow est $[\mathrm{G} : \mathrm{N_G(P)}]$. Déterminons $\mathrm{N_G(P)}$. Notons que $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartient à $\mathrm{N_G(P)}$ si et seulement si $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ conjugue $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ à une

puissance $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Puisque

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 - \frac{ac}{\Delta} & \frac{a^2}{\Delta} \\ -\frac{c^2}{\Delta} & 1 + \frac{ac}{\Delta} \end{pmatrix}$$

avec $\Delta = ad - bc \neq 0$, nous constatons que $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartient à $\mathrm{N_G(P)}$ si et seulement si $c = 0$. Autrement $\mathrm{N_G(P)} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{G} \right\}$. L'ordre de $\mathrm{N_G(P)}$ est $(p-1)^2 p$. Il en résulte que

$$n_p = [\mathrm{G} : \mathrm{N_G(P)}] = \frac{p(p-1)(p^2-1)}{(p-1)^2 p} = p + 1.$$

□

Corollaire 10.3.1

Le groupe $\mathrm{GL}\left(2, \mathbb{Z}/p\mathbb{Z}\right)$ compte $p^2 - 1$ éléments d'ordre p.

Démonstration. — Chaque p-Sylow compte $p - 1$ éléments d'ordre p. Deux p-Sylow distincts s'intersectent trivialement ; par suite le nombre d'éléments d'ordre p est

$$(p-1)n_p = (p-1)(p+1) = p^2 - 1.$$

□

Théorème 10.3.4

Le groupe $\mathrm{Aff}\left(\mathbb{Z}/p^2\mathbb{Z}\right)$ contient un unique p-Sylow.

Démonstration. — *Première démonstration possible* :

Le groupe $\mathrm{Aff}\left(\mathbb{Z}/p^2\mathbb{Z}\right)$ est d'ordre $p^2\phi(p^2) = p^3(p-1)$. Ainsi un p-Sylow est d'ordre p^3.

Le troisième théorème de Sylow (Théorème 10.1.3) assure que le nombre n_p de p-Sylow vérifie les propriétés suivantes : n_p divise $p - 1$ et $n_p \equiv_p 1$. Il en résulte que $n_p = 1$.

Seconde démonstration possible :

Le groupe $\mathrm{Aff}\left(\mathbb{Z}/p^2\mathbb{Z}\right)$ est d'ordre $p^2\phi(p^2) = p^3(p-1)$. Ainsi un p-Sylow est d'ordre p^3.

Le sous-groupe

$$\mathrm{P} = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \, a \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times, \, b \in \mathbb{Z}/p^2\mathbb{Z}, \, a^p = 1 \right\}$$

de $\mathrm{Aff}\left(\mathbb{Z}/p^2\mathbb{Z}\right)$ est un groupe d'ordre p^3 (il y a p choix pour le coefficient a et p^2 choix pour le coefficient b), *i.e.* P est un p-Sylow de $\mathrm{Aff}\left(\mathbb{Z}/p^2\mathbb{Z}\right)$. Par ailleurs P est le noyau du morphisme de groupes

$$\mathrm{Aff}\left(\mathbb{Z}/p^2\mathbb{Z}\right) \to \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times, \qquad \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto a^p;$$

en particulier, P est distingué dans $\mathrm{Aff}\left(\mathbb{Z}/p^2\mathbb{Z}\right)$. Le Corollaire 10.2.1 permet de conclure. □

L'unique p-Sylow de $\mathrm{Aff}\left(\mathbb{Z}/p^2\mathbb{Z}\right)$ est un groupe non-abélien d'ordre p^3. Il possède un élément d'ordre p^2, l'élément $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, et n'est donc pas isomorphe à

$$\mathrm{Heis}\left(\mathbb{Z}/p\mathbb{Z}\right) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, a,\, b,\, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

lorsque $p \neq 1$ car chaque élément de $\mathrm{Heis}\left(\mathbb{Z}/p\mathbb{Z}\right) \smallsetminus \{e\}$ est d'ordre p. En fait on peut montrer qu'un groupe non abélien d'ordre p^3, où p désigne un nombre premier impair, est isomorphe à $\mathrm{Heis}\left(\mathbb{Z}/p\mathbb{Z}\right)$ ou à l'unique p-Sylow de $\mathrm{Aff}\left(\mathbb{Z}/p^2\mathbb{Z}\right)$.

Peut-on caractériser $\mathrm{Heis}\left(\mathbb{Z}/p\mathbb{Z}\right)$ comme étant l'unique p-Sylow d'un groupe plus grand ? La réponse est donnée par l'énoncé suivant :

Théorème 10.3.5

Pour p premier $\mathrm{Heis}\left(\mathbb{Z}/p\mathbb{Z}\right)$ est l'unique p-Sylow du groupe des matrices triangulaires

$$\left\{ \begin{pmatrix} d_1 & a & b \\ 0 & d_2 & c \\ 0 & 0 & d_3 \end{pmatrix} \mid d_i \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times,\, a,\, b,\, c \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

Démonstration. — Posons

$$\mathrm{U} = \left\{ \begin{pmatrix} d_1 & a & b \\ 0 & d_2 & c \\ 0 & 0 & d_3 \end{pmatrix} \mid d_i \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times,\, a,\, b,\, c \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

Le groupe U est d'ordre $(p-1)^3p^3$. Il en résulte que $\mathrm{Heis}\left(\mathbb{Z}/p\mathbb{Z}\right)$ est un p-Sylow de U.

Considérons l'application

$$\mathrm{U} \to \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/p\mathbb{Z}\right)^\times ;$$

on peut vérifier que c'est un morphsime de groupes dont le noyau est $\mathrm{Heis}\left(\mathbb{Z}/p\mathbb{Z}\right)$. En particulier, $\mathrm{Heis}\left(\mathbb{Z}/p\mathbb{Z}\right)$ est un sous-groupe distingué de U ; c'est donc l'unique p-Sylow de U (Corollaire 10.2.1). □

Théorème 10.3.6

Soit $\Bbbk$ un corps fini à q éléments. Si p est un nombre premier divisant $q-1$, alors le nombre de p-Sylow de $\mathrm{Aff}(\Bbbk)$ est q.

Démonstration. — Le groupe $\mathrm{Aff}(\Bbbk)$ est d'ordre $q(q-1)$ et contient $\mathrm{H} = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \middle| a \in \Bbbk^\times \right\}$ qui est d'ordre $q-1$. Soit p^r la puissance la plus élevée de p divisant $q-1$. Soit P le sous-groupe p-Sylow de H (il est unique puisque H est abélien). Alors P est également un p-Sylow de $\mathrm{Aff}(\Bbbk)$ et le nombre de p-Sylow de $\mathrm{Aff}(\Bbbk)$ est $[\mathrm{Aff}(\Bbbk) : N(\mathrm{P})]$ d'après le Théorème 10.1.4, où $N(\mathrm{P})$ désigne le normalisateur de P dans $\mathrm{Aff}(\Bbbk)$.

Comme H est abélien, $\mathrm{P} \subset \mathrm{H}$, donc $\mathrm{H} \subset N(\mathrm{P})$. Soit $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ un élément de $N(\mathrm{P})$. Choisissons un élément de $\mathrm{P} \smallsetminus \{\mathrm{id}\}$, par exemple $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$. Alors

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & y(1-a) \\ 0 & 1 \end{pmatrix}$$

Pour qu'il appartienne à P, il faut au moins que $y(1-a) = 0$, soit $y = 0$ puisque $a \neq 1$. Ainsi $N(\mathrm{P}) \subset \mathrm{H}$. Le nombre de sous-groupes p-Sylow de $\mathrm{Aff}(\Bbbk)$ est $[\mathrm{Aff}(\Bbbk) : \mathrm{H}] = \frac{q(q-1)}{q-1} = q$. □

Soit n un entier tel que $n \equiv_p 1$; existe-t-il un groupe fini dans lequel le nombre de p-Sylow est n ? La réponse est oui lorsque $n = 1$ (il suffit de considérer $\mathbb{Z}/p\mathbb{Z}$). Supposons désormais que $n > 1$. Lorsque p vaut 2 la réponse est positive en utilisant les groupes diédraux : lorsque $n > 1$ est impair un 2-Sylow de D_{2n} est d'ordre 2 et les éléments d'ordre 2 sont précisément les n réflexions ; ainsi D_{2n} compte n 2-Sylow. Si $p \neq 2$, la réponse n'est pas oui : il n'existe pas de groupe fini G dans lequel $n_3 = 22$ ou $n_5 = 21$ ou $n_p = 1 + 3p$ pour $p \geq 7$ premier ([**Hal67**]).

10.4. Propriétés de commutativité

Tous les groupes d'ordre p^2 sont abéliens. Le théorème de Cauchy (Théorème 3.7.1) peut être utilisé pour montrer que tous les groupes d'ordre pq avec les nombres premiers $p < q$ et $q \not\equiv_p 1$ (par exemple, $pq = 15$) sont abéliens (et en fait cycliques). Les théorèmes de Sylow fournissent des outils supplémentaires pour montrer que tous les groupes d'un ordre donné sont abéliens.

Théorème 10.4.1

Tout groupe d'ordre 45 est abélien.

Lemme 10.4.1

Soit G un groupe. Soit H un sous-groupe de G et soit N un sous-groupe distingué de G. Les trois propriétés suivantes sont satisfaites :

1. l'ensemble NH est un sous-groupe de G ;
2. $\mathrm{NH} = \mathrm{HN} = \{hn \mid h \in \mathrm{H},\ n \in \mathrm{N}\}$;
3. si $|\mathrm{H}|$ et $|\mathrm{N}|$ sont premiers entre eux, alors $|\mathrm{NH}| = |\mathrm{N}|\,|\mathrm{H}|$.

Démonstration. — 1. L'ensemble NH contient $e = e \times e$.

Soient n_1, n_2 dans N et h_1, h_2 dans H ; notons que $(n_1h_1)(n_2h_2)$ s'écrit aussi $n_1(h_1n_2h_1^{-1})h_1h_2$. Puisque $\mathrm{N} \triangleleft \mathrm{G}$, nous avons : $h_1n_2h_1^{-1}$ appartient à N et comme N est un groupe $n_1(h_1n_2h_1^{-1})$ appartient à N. Par ailleurs H étant un groupe h_1h_2 est un élément de H. Il en résulte que $(n_1h_1)(n_2h_2)$ appartient à NH.

Soit n dans N et soit h dans H ; alors $(nh)^{-1}$ s'écrit aussi

$$h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1}.$$

Étant donné que $\mathrm{N} \triangleleft \mathrm{G}$ $h^{-1}n^{-1}h \in \mathrm{N}$ et $(h^{-1}n^{-1}h)h^{-1} \in \mathrm{NH}$, soit $(nh)^{-1} \in \mathrm{NH}$.

2. Soient $n \in \mathrm{N}$ et $h \in \mathrm{H}$, alors d'une part $nh = h(h^{-1}nh)$, d'autre part $h^{-1}nh$ appartient à N (en effet $\mathrm{N} \triangleleft \mathrm{G}$) d'où nh appartient à HN et $\mathrm{NH} \subset \mathrm{HN}$.

   Soient $n \in \mathrm{N}$ et $h \in \mathrm{H}$, alors d'une part $hn = (hnh^{-1})h$, d'autre part hnh^{-1} appartient à N (en effet $\mathrm{N} \triangleleft \mathrm{G}$) d'où hn appartient à NH et $\mathrm{HN} \subset \mathrm{NH}$.

   Finalement les inclusions $\mathrm{NH} \subset \mathrm{HN}$ et $\mathrm{HN} \subset \mathrm{NH}$ entraînent $\mathrm{HN} = \mathrm{NH}$.

3. Chaque élément de NH est de la forme nh pour un certain $n \in \mathrm{N}$ et un certain $h \in \mathrm{H}$. Cette écriture pour un élément est unique ; en effet si $nh = n'h'$; alors $(n')^{-1}n = h'h^{-1}$ appartient à $\mathrm{N} \cap \mathrm{H}$. Puisque $\mathrm{pgcd}(\mathrm{N}, \mathrm{H}) = 1$, $\mathrm{N} \cap \mathrm{H}$ est un sous-groupe d'ordre divisant $|\mathrm{N}$ et $|\mathrm{H}$; il en résulte que $|\mathrm{H} \cap \mathrm{N}| = 1$. Ainsi $\mathrm{H} \cap \mathrm{N} = \{e\}$ et $(n')^{-1}n = h'h^{-1} = e$. D'où $n = n'$ et $h = h'$. Compter les différents produits nh avec n dans N et $h \in \mathrm{H}$ équivaut à compter les paires ordonnées (n, h) avec n dans N et $h \in \mathrm{H}$. Le nombre de ces paires est $|\mathrm{NH}|$.

□

Démonstration du Théorème 10.4.1. — Soit G un groupe d'ordre 45. Puisque $45 = 3^2 \times 5$, un 3-Sylow de G est d'ordre 9 et un 5-Sylow de G est d'ordre 5. Le Troisième Théorème de Sylow (Théorème 10.1.3) assure que

- ◇ d'une part n_3 divise 5 et $n_3 \equiv_3 1$;
- ◇ d'autre part n_5 divise 9 et $n_5 \equiv_5 1$.

Il en résulte que $n_3 = n_5 = 1$. Par conséquent, G possède un unique 3-Sylow P qui est distingué et un unique 5-Sylow Q qui est distingué. De plus $|\mathrm{P}| = 9$ et $|\mathrm{Q}| = 5$. Alors P est abélien et Q est cyclique donc abélien. D'après le Lemme 10.4.1 l'ensemble $\mathrm{PQ} = \{ab \mid a \in \mathrm{P},\, b \in \mathrm{Q}\}$ est un sous-groupe de G. Par ailleurs comme P et Q sont des sous-groupes de PQ, le Théorème de Lagrange (Théorème 1.6.4) assure que $|\mathrm{PQ}|$ est divisible par 9 et par 5 donc par 45. Ainsi $\mathrm{PQ} = \mathrm{G}$. Les groupes P et Q étant tous deux abéliens, le groupe G est abélien si les éléments de P commutent avec les éléments de Q ce qui est assuré par le Théorème 10.2.1. □

Soient p et q des nombres premiers tels que $p < q$. Nous allons utiliser les théorèmes de Sylow et une propriété du produit semi-direct pour déterminer les groupes d'ordre pq à isomorphisme près ; notons que nous avions déjà donner la classification des groupes d'ordre pq (*voir* §3.7.4, Théorème 3.7.6) en utilisant le théorème de Cauchy (Théorème 3.7.1). L'intérêt de cette application est de voir comment différents produits semi-directs peuvent être isomorphes. Nous allons distinguer les cas $q \equiv_p 1$ et $q \not\equiv_p 1$. Commençons par l'éventualité $q \not\equiv_p 1$.

Théorème 10.4.2

Soient p et q deux nombres premiers tels que $p < q$ et $q \not\equiv_p 1$. Tout groupe d'ordre pq est cyclique.

Démonstration. — Soit G un groupe d'ordre pq, où $p < q$ et $q \not\equiv_p 1$. D'après le théorème de Cauchy, G possède un élément a d'ordre p et un élément b d'ordre q. Soient $\mathrm{P} = \langle a \rangle$ et $\mathrm{Q} = \langle b \rangle$. Les sous-groupes P et Q sont respectivement d'ordre p et q et sont respectivement des p-Sylow et q-Sylow de G. Le troisième Théorème de Sylow (Théorème 10.1.3) assure que

- ◇ n_p divise q et $n_p \equiv_p 1$;
- ◇ n_q divise p et $n_q \equiv_q 1$.

Alors n_p vaut 1 ou q, mais puisque $q \not\equiv_p 1$ nous avons $n_p \neq q$; ainsi $n_p = 1$. Comme $1 < p < q$ nous ne pouvons pas avoir $p \equiv_q 1$, donc n_q vaut 1. Par conséquent les groupes P et Q sont tous deux des sous-groupes distingués de G. Le Théorème 10.2.1 assure que les éléments de P commutent avec les éléments de Q. Il en résulte que a et b commutent ; étant donné qu'ils sont d'ordres premiers p et q, leur produit ab est d'ordre pq. Comme $|\mathrm{G}| = pq$, le groupe G est cyclique. □

Corollaire 10.4.1

Soit G un groupe d'ordre pq où $p < q$ désignent des nombres premiers distincts tels que $q \not\equiv_p 1$. Alors G possède un q-Sylow distingué.

Démonstration. — D'après la démonstration du Théorème 10.4.2 nous avons l'égalité $n_q = 1$. □

Pour finir intéressons-nous au cas p, q premiers distincts tels que $p < q$ et $q \equiv_p 1$.

Lemme 10.4.2

Considérons un produit semi-direct $\mathrm{H} \rtimes_\varphi \mathrm{K}$. Si $f\colon \mathrm{K} \to \mathrm{K}$ est un automorphisme, alors $\mathrm{H} \rtimes_\varphi \mathrm{K}$ et $\mathrm{H} \rtimes_{\varphi\circ f} \mathrm{K}$ sont isomorphes.

La démonstration est laissée en exercice.

Théorème 10.4.3

Soient p et q deux nombres premiers tels que $p < q$ et $q \equiv_p 1$. Il existe deux groupes d'ordre pq à isomorphisme près : l'un est cyclique et l'autre n'est pas abélien.

Démonstration. — Soit G un groupe d'ordre pq. Le Théorème de Cauchy assure l'existence d'un sous-groupe P d'ordre p et d'un sous-groupe Q d'ordre q. Soit n_p (resp. n_q) le nombre de p-Sylow (resp. q-Sylow) de G. D'après le troisième théorème de Sylow d'une part $n_p \equiv_p 1$ et $n_p \mid q$; d'autre part $n_q \equiv_q 1$ et $n_q \mid p$. Puisque p est premier $n_q \mid p$ implique $n_q = 1$ ou $n_q = p$. Mais comme $p < q$, $p \not\equiv_q 1$, il en résulte que $n_q \neq p$, c'est-à-dire $n_q = 1$ et $\mathrm{Q} \triangleleft \mathrm{G}$.

Nous nous intéressons maintenant aux p-Sylow. Les égalités $n_p \equiv_p 1$ et $n_p \mid q$ conduisent à l'alternative : $n_p = 1$ ou $n_p = q$.

- Cas 1 : $n_p = 1$. En particulier le troisième Théorème de Sylow assure que $\mathrm{P} \triangleleft \mathrm{G}$. Soient x un élément de P et y un élément de Q. Alors $xyx^{-1}y^{-1}$ appartient à l'intersection $\mathrm{P} \cap \mathrm{Q}$ qui est triviale ; il en résulte que pour tout $x \in \mathrm{P}$ et pour tout $y \in \mathrm{Q}$ nous avons $xy = yx$. Ainsi pour tout $x \in \mathrm{P} \smallsetminus \{e\}$ et pour tout $y \in \mathrm{Q} \smallsetminus \{e\}$ d'une part x est d'ordre p, y est d'ordre q et d'autre part $xy = yx$; par conséquent xy est d'ordre pq. En particulier $\mathrm{G} = \langle xy \rangle$ et G est cyclique.
- Cas 2 : $n_p = q$. En particulier G ne peut pas être cyclique (dans les groupes cycliques tous les Sylow sont distingués). Puisque $\mathrm{Q} \triangleleft \mathrm{G}$ et $\mathrm{Q} \cap \mathrm{P} = \{e\}$, QP est un sous-groupe de G d'ordre $qp = |\mathrm{G}|$, donc $\mathrm{G} = \mathrm{QP} = \mathrm{PQ}$. Le Théorème 3.6.5 assure que $\mathrm{G} \simeq \mathrm{Q} \rtimes_\varphi \mathrm{P}$ où $\varphi\colon \mathrm{P} \to \mathrm{Aut}(\mathrm{Q})$ est l'action par conjugaison de P sur Q.

Les constructions de produits semi-directs sont inchangées, à isomorphisme près, si nous remplaçons les groupes impliqués par des groupes isomorphes. Nous pouvons donc supposer

que $\mathrm{P} = \mathbb{Z}/p\mathbb{Z}$ et $\mathrm{Q} = \mathbb{Z}/q\mathbb{Z}$. Alors tout groupe non cyclique d'ordre pq est de la forme $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ pour un morphisme non trivial

$$\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \left(\mathbb{Z}/q\mathbb{Z}\right)^\times.$$

Nous allons montrer qu'il y a $p-1$ tels morphismes et que tous ces morphismes définissent des produits semi-directs isomorphes. Les différents morphismes $\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ sont déterminés par l'image de 1 qui est nécessairement envoyé sur une solution de $z^p \equiv_q 1$ dans $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$. Le cas $z = 1$ est le cas du morphisme trivial, cas qui ne nous intéresse pas. Puisque $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ est d'ordre $q-1$ et $p \mid (q-1)$ (qui est équivalent à $q \equiv_p 1$), le groupe $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ contient des éléments d'ordre p d'après le théorème de Cauchy. Chaque solution de $z^p \equiv_q 1$, avec $z \not\equiv_p 1$, induit un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ muni de la loi

$$(a,b)(c,d) = (a + \varphi_b(c), b+d) = (a + z^b c, b+d). \tag{10.4.1}$$

(Noter que si $z = 1$, il s'agit du produit direct).

L'ensemble $\mathrm{K} = \{z \in \left(\mathbb{Z}/q\mathbb{Z}\right)^\times \mid z^p \equiv_q 1\}$ est un sous-groupe non trivial de $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$. Chaque élément z de $\mathrm{K} \smallsetminus \{1\}$ engendre un sous-groupe $\langle z \rangle$ d'ordre p. Pour tout q premier, le groupe $(\mathbb{Z}/q\mathbb{Z})^\times$ est cyclique, il contient donc un unique sous-groupe d'ordre p. Ainsi $\left\{z \in \left(\mathbb{Z}/q\mathbb{Z}\right)^\times \mid z^p \equiv_p 1\right\}$ est d'ordre p. Il s'en suit que le nombre de φ est p et le nombre de φ non triviaux est $p-1$.

Deux φ non triviaux sont associés (par (10.4.1)) à deux éléments z d'ordre p dans $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$, appelés eux z_1 et z_2. Ils engendrent le même sous-groupe, donc $z_2 = z_1^r$ pour certains $r \in \mathbb{Z}$ (nécessairement $(r,p) = 1$). Nous montrerons à partir de la relation $z_2 = z_1^r$ que les produits semi-directs associés à z_1 et z_2 sont des groupes isomorphes. Soient $\varphi_1, \varphi_2\colon \mathbb{Z}/p\mathbb{Z} \to \left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ les morphismes associés à z_1 et z_2 :

$$\varphi_1(b) = z_1^b, \qquad\qquad \varphi_2(b) = z_2^b = z_1^{br};$$

les lois de groupe sont

$$(a,b)(c,d) = (a + z_1^b c, b+d) \qquad \text{et} \qquad (a,b)(c,d) = (a + z_2^b c, b+d) = (a + z_1^{rb} c, b+d).$$

Remarqupns que $\varphi_2 = \varphi_1 \circ f$ où $f\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $x \mapsto rx$. Ce f est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$ donc $\mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_2} \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi_1} \mathbb{Z}/p\mathbb{Z}$ (Lemme 10.4.2). Ainsi, lorsque $p < q$ et $q \equiv_p 1$, il existe (à isomorphisme près) deux groupes d'ordre pq. $\square$

Si $q \equiv_p 1$, un groupe matriciel non abélien d'ordre pq est

$$\left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \mid x \in \left(\mathbb{Z}/q\mathbb{Z}\right)^\times,\ y \in \mathbb{Z}/q\mathbb{Z}, x^p \equiv_q 1 \right\} \subset \mathrm{Aff}\left(\mathbb{Z}/q\mathbb{Z}\right).$$

10.5. Le groupe $\mathcal{A}_n$ est simple dès que $n \geq 5$, version ? ? ?

Théorème 10.5.1

Le groupe $\mathcal{A}_5$ est simple.

Lemme 10.5.1

Tout p-Sylow distingué d'un groupe d'ordre fini est caractéristique.

Démonstration. — Soit G un groupe d'ordre fini. Soit H un p-Sylow de G qui est distingué. Soit φ un automorphisme de G. L'image de H par φ est un sous-groupe de même ordre que H, *i.e.* $\varphi(\mathrm{H})$ est un p-Sylow de G. Mais H est l'unique p-Sylow de G car H est distingué. Par conséquent $\varphi(\mathrm{H}) = \mathrm{H}$. □

Lemme 10.5.2

Tout groupe d'ordre 15 est cyclique.

Démonstration. — Soit H un groupe d'ordre 15. Il a exactement un sous-groupe d'ordre 5 et un sous-groupe d'ordre 3. Ces deux sous-groupes sont distingués dans H. Par suite $\mathrm{H} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$ et est donc cyclique. □

Lemme 10.5.3

Tout groupe d'ordre 30 contient un sous-groupe distingué d'ordre 15.

Démonstration. — Soit G un groupe d'ordre 30. Remarquons tout d'abord que tout sous-groupe d'ordre 15 de G est distingué dans G car il est d'indice 2 dans G.

Il suffit donc de démontrer l'existence d'un sous-groupe d'ordre 15 dans le groupe G.

- ◇ Supposons que G contienne plus d'un seul 5-Sylow, *i.e.* $n_5 > 1$. Puisque

$$n_5 \equiv_5 1 \qquad\qquad n_5 \mid 6$$

  on a $n_5 = 6$. Ainsi on a 6×4 éléments d'ordre 5, ce qui en ajoutant e fait 25 éléments de G. Il y a donc exactement un seul 3-Sylow que nous noterons K (sinon il y en aurait 10 donc 20 éléments d'ordre 3 soit 45 éléments au moins dans G). En particulier K est distingué dans G. Si H est l'un des sous-groupes d'ordre 5, $\mathrm{K} \cap \mathrm{H} = \{e\}$ et KH est un sous-groupe d'ordre 15 de G.
- ◇ Supposons que G contienne un seul 5-Sylow H ; il est alors distingué dans G. Si K est l'un des sous-groupes d'ordre 3 de G (il y en a au moins un) $\mathrm{K} \cap \mathrm{H} = \{e\}$ et KH est un sous-groupe d'ordre 15 dans le groupe G.

□

Lemme 10.5.4

Tout groupe d'ordre 30 ne contient qu'un seul 5-Sylow (d'ordre 5).

Démonstration. — Dans la démonstration du Lemme 10.5.3 nous avons vu d'une part que tout groupe G d'ordre 30 contient un sous-groupe K d'ordre 3 et un sous-groupe H d'ordre 5 et d'autre part que K ou H est distingué dans G.

Les groupes K et H sont distingués dans KH et sont donc caract éristiques dans le groupe cyclique KH (Lemme 10.5.1) qui est distingué dans G. Donc en fait K et H sont distingués dans G et G a un unique 5-Sylow. □

Lemme 10.5.5

Tout groupe d'ordre 20 contient un seul sous-groupe d'ordre 5.

Démonstration. — Soit G un groupe d'ordre $20 = 4 \times 5$. Le groupe G contient un sous-groupe distingué d'ordre 5 : d'après les théorèmes de Sylow

$$n_5 \equiv_5 1 \qquad\qquad n_5 \mid 4$$

d'où $n_5 = 1$. □

Lemme 10.5.6

Tout groupe d'ordre 12 contient un sous-groupe caractéristique.

Démonstration. — Soit G un groupe d'ordre 12. Intéressons-nous aux 3-Sylow de G. Les théorèmes de Sylow assurent que

$$n_3 \equiv_3 1 \qquad\qquad n_3 \mid 4$$

Il en résulte que $n_3 = 1$ ou $n_3 = 4$.

- Si $n_3 = 1$, alors ce sous-groupe est un sous-groupe caractéristique d'ordre 3 (Lemme 10.5.1).
- Si $n_3 = 4$, on dénombre $4 \times 2 = 8$ éléments d'ordre 3 ; en ajoutant le neutre on compte donc 9 éléments. Considérons maintenant les 2-Sylow de G. D'après les théorèmes de Sylow on a

  $$n_2 \equiv_2 1 \qquad\qquad n_2 \mid 3$$

  Ainsi n_2 appartient à $\{1, 3\}$. Si $n_2 = 3$, on a trois sous-groupes d'ordre 4, soit trop d'éléments. Ainsi $n_2 = 1$, l'unique 2-Sylow est distingué et donc caractéristique (Lemme 10.5.2).

□

Lemme 10.5.7

Tout groupe d'ordre 6 contient un sous-groupe caractéristique.

Démonstration. — Soit G un groupe d'ordre $6 = 2 \times 3$. Considérons ces 3-Sylow. Les théorèmes de Sylow assurent que

$$n_3 \equiv_3 1 \qquad\qquad n_3 \mid 2$$

autrement dit que $n_3 = 1$. Ainsi G compte un unique 3-Sylow qui est donc distingué dans G et le Lemme 10.5.2 permet de conclure. □

Lemme 10.5.8

Tout groupe d'ordre 60 qui contient plus qu'un seul 5-Sylow est simple.

Démonstration. — Soit G un groupe d'ordre 60. Supposons que $n_5 > 1$. D'après les théorèmes de Sylow

$$n_5 \equiv_5 1 \qquad\qquad n_5 \mid 12$$

d'où $n_5 = 6$.

Raisonnons par l'absurde : supposons que G ne soit pas simple. Soit H un sous-groupe distingué propre de G.

Si $|\mathrm{H}|$ est divisible par 5 alors H contient au moins un 5-Sylow de G. Mais H est distingué et les 5-Sylow se déduisent les uns des autres par conjugaison ; ainsi H contient tous les 5-Sylow de G. On en d'éduit que H contient déjà 6×4 éléments d'ordre 5. Par ailleurs $|\mathrm{H}|$ divise 60 donc $|\mathrm{H}| = 30$ (rappelons que comme H est un sous-groupe propre de G, on a $|\mathrm{H}| < 60$. Mais dans ce cas H ne contient qu'un seul sous-groupe d'ordre 5 : contradiction avec le fait qu'il en contient 6. Par suite $|\mathrm{H}|$ n'est pas divisible par 5.

Si $|\mathrm{H}|$ appartient à $\{6, 12\}$, alors il existe un sous-groupe caractéristique de H d'ordre 2, 3 ou 4. Ce sous-groupe caractéristique de H, qui est lui-même distingué dans G, est distingué dans G. Nous pouvons donc maintenant supposer que H est d'ordre 2, 3 ou 4.

Dans ce cas G/H est d'ordre 30, 20 ou 15. Dans ces trois cas G/H contient un sous-groupe distingué d'ordre 5. Considérons la surjection canonique $\pi \colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$. Le sous-groupe $\pi^{-1}(\mathrm{K})$ contient H et est distingué dans G. Or $\pi^{-1}(\mathrm{K})/\mathrm{H}$ est isomorphe à $\mathrm{K} = \pi(\pi^{-1}(\mathrm{K}))$ donc $|\pi^{-1}(\mathrm{K})|$ est divisible par 5 : contradiction. □

Démonstration du Théorème 10.5.1. — Le groupe $\mathcal{A}_5$ est d'ordre 60 et contient au moins deux 5-Sylow distincts engendrés par les 5-cycles (1 2 3 4 5) et (1 3 2 4 5). Le Lemme 10.5.8 assure donc que $\mathcal{A}_5$ est simple. □

Lemme 10.5.9

Soit $n \geq 6$. Supposons que $\mathcal{A}_{n-1}$ soit simple. Soit H un sous-groupe distingué propre de $\mathcal{A}_n$. Il existe $\tau \in \mathrm{H}$ distincte de l'identité qui a au moins un point fixe.

Démonstration. — Supposons que $\mathrm{H} \neq \{\mathrm{id}\}$.

Remarque 10.5.1. — Supposons que pour tout $\tau \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$. Alors si τ_1 et τ_2 sont deux éléments de H qui coïncident en un point i, ils sont égaux. En effet si $\tau_1(i) = \tau_2(i)$ alors $\tau_2^{-1}\tau_1(i) = i$. De plus $\tau_2^{-1}\tau_1$ appartient à H donc par hypothèse $\tau_2^{-1}\tau_1 = \mathrm{id}$, *i.e.* $\tau_1 = \tau_2$.

Supposons que pour tout $\tau \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$. Considérons un élément τ de H. Si la décomposition ed τ en produit de cycles disjoints contient un cycle d'ordre ≥ 3 alors on peut écrire

$$\tau = (a_1\ a_2\ a_3\ \ldots)(b_1\ b_2\ \ldots)\ldots$$

Puisque $n \geq 6$ il existe σ dans $\mathcal{A}_n$ tel que $\sigma(a_1) = a_1$, $\sigma(a_2) = a_2$ et $\sigma(a_3) \neq a_3$. Alors

$$\sigma\tau\sigma^{-1} = (a_1\ a_2\ \sigma(a_3)\ \ldots)(\sigma(b_1)\ \sigma(b_2)\ \ldots)\ldots$$

Ainsi $\sigma\tau\sigma^{-1}(a_1) = \tau(a_1) = a_2$. À noter que $\sigma\tau\sigma^{-1}$ appartient à H car H est distingué. La Remarque 10.5.1 assure donc que $\sigma\tau\sigma^{-1} = \tau$. Mais $\sigma\tau\sigma^{-1}(a_2) = \sigma(a_3) \neq a_3$ et $a_3 = \tau(a_2)$ donc $\sigma\tau\sigma^{-1}(a_2) \neq \tau(a_2)$: contradiction. Ainsi aucun élément de H ne contient dans sa décomposition en cycles disjoints des cycles d'ordre ≥ 3. Les éléments de H sont donc des produits de transpositions disjointes.

Considérons un élément τ de H. D'après ce qui précède τ est un produit de transpositions disjointes. À noter que si τ contient une double transposition alors elle laisse fixe un élément ce qui est contraire à l'hypothèse. Ainsi τ s'écrit

$$\tau = (a_1\ a_2)(a_3\ a_4)(a_5\ a_6)\ldots$$

Soit $\sigma = (a_1\ a_2)(a_3\ a_5)$. Alors on a

$$\sigma\tau\sigma^{-1} = (a_1\ a_2)(a_5\ a_4)(a_3\ a_6)\ldots$$

D'une part $\sigma\tau\sigma^{-1}(a_2) = \tau(a_2)$ donc $\sigma\tau\sigma^{-1} = \tau$ (Remarque 10.5.1). D'autre part $\sigma\tau\sigma^{-1}(a_3) = \tau(a_3)$: contradiction. Il existe donc un élément τ dans $\mathrm{H} \smallsetminus \{\mathrm{id}\}$ pour lequel $\tau(i) = i$ pour un certain $1 \leq i \leq n$. □

Lemme 10.5.10

Soit $n \geq 6$. Supposons que $\mathcal{A}_{n-1}$ soit simple. Soit H un sous-groupe distingué propre de $\mathcal{A}_n$. Pour tout $1 \leq j \leq n$ le sous-groupe $\mathrm{G}_j = \mathrm{St}_{\mathcal{A}_n}(\{j\})$ est inclus dans H.

Démonstration. — Soit τ un élément de $\mathrm{H} \smallsetminus \{\mathrm{id}\}$ pour lequel il existe $A \leq i \leq n$ tel que $\tau(i) \neq i$ (l'existence d'un tel τ est assurée par le Lemme 10.5.9). Ainsi τ appartient à $\mathrm{G}_i \cap \mathrm{H}$ qui est un sous-groupe distingué de G_i. Or G_i est isomorphe à $\mathcal{A}_{n-1}$ donc l'hypothèse de récurrence implique que G_i est simple. Or τ est non trivial donc $\mathrm{G}_i \cap \mathrm{H} = \mathrm{G}_i$, c'est-à-dire G_i est inclus dans H.

Par ailleurs pour tout σ dans $\mathfrak{S}_n$ on a $\sigma \mathrm{G}_i \sigma^{-1} = G_{\sigma(i)}$. De plus $\mathrm{G}_i \subset \mathrm{H}$ donc $\sigma \mathrm{G}_i \sigma^{-1} \subset \sigma \mathrm{H} \sigma^{-1} = \mathrm{H}$. Il en résulte que pour tout $1 \leq j \leq n$ on a l'inclustion $\mathrm{G}_j \subset \mathrm{H}$. □

Lemme 10.5.11

Soit $n \geq 6$. Supposons que $\mathcal{A}_{n-1}$ soit simple. Soit H un sous-groupe distingué propre de $\mathcal{A}_n$ non trivial. Alors $\mathcal{A}_n = \mathrm{H}$.

Démonstration. — Considérons un élément g de $\mathcal{A}_n$. C'est un produit d'un nombre pair de transpositions, il s'écrit donc

$$g = t_1 t_2 \dots t_k$$

où chaque t_j est un produit de deux transpositions. Le support de chaque t_j contient au plus quatre éléments donc t_j appartient à G_i pour un i extérieur à ce support. Par suite $\mathcal{A}_n \subset \mathrm{G}_1 \mathrm{G}_2 \dots \mathrm{G}_n$. Mais $\mathrm{G}_1 \mathrm{G}_2 \dots \mathrm{G}_n \subset \mathrm{H}$ (Lemme 10.5.10). Il en résulte que $\mathcal{A}_n \subset \mathrm{H}$. Or $\mathrm{H} \subset \mathcal{A}_n$ donc $\mathcal{A}_n = \mathrm{H}$. □

Démonstration du Théorème 5.1.12. — Le groupe $\mathcal{A}_5$ est simple (Théorème 10.5.1). Pour $n \geq 6$ tout sous-groupe distingué de $\mathcal{A}_n$ différent de $\{\mathrm{id}\}$ est égal à $\mathcal{A}_n$ (Lemme 10.5.11). □

10.6. Automorphismes extérieurs de $\mathfrak{S}_6$, version 2

Étudions désormais les automorphismes extérieurs de $\mathfrak{S}_6$.

Rappelons l'énoncé suivant :

Théorème 10.6.1

Soit $n \geq 5$. Les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathfrak{S}_n$.

Lemme 10.6.1

L'ensemble $\mathrm{Syl}_5(\mathfrak{S}_5)$ des 5-sous-groupes de Sylow de $\mathfrak{S}_5$ est de cardinal 6.

Démonstration. — On a $|\mathfrak{S}_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$. L'ordre d'un élément de $\mathrm{Syl}_5(\mathfrak{S}_5)$ est donc 5. Or 5 est premier donc tout élément de $\mathrm{Syl}_5(\mathfrak{S}_5)$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Posons $n_5 = \#\mathrm{Syl}_5(\mathfrak{S}_5)$.

Les théorèmes de Sylow assurent que

$$\begin{cases} n_5 \equiv_5 1 \\ n_5 \text{ divise } 2^3 \cdot 3 = 24 \end{cases}$$

Par conséquent n_5 appartient à $\{1, 6\}$.

Supposons que $n_5 = 1$. Alors $\mathfrak{S}_5$ a un unique 5-Sylow qui est distingué : contradiction avec le fait que les sous-groupes distingués de $\mathfrak{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathfrak{S}_5$. Par suite $n_5 = 6$. □

Lemme 10.6.2

Numérotons arbitrairement de 1 à 6 les éléments de $\mathrm{Syl}_5(\mathfrak{S}_5)$. Faisons opérer $\mathfrak{S}_5$ sur $\mathrm{Syl}_5(\mathfrak{S}_5) \simeq \{1, 2, 3, 4, 5, 6\}$ par conjugaison. La morphisme $\mathfrak{S}_5 \to \mathfrak{S}_6$ associé est injectif. Notons G son image.

Démonstration. — Soit K le noyau du morphisme de $\mathfrak{S}_5$ vers $\mathfrak{S}_{\mathrm{G}}$. Il est contenu dans le stabilisateur de chacun des éléments de $\mathrm{Syl}_5(\mathfrak{S}_5)$. L'action de G sur $\mathrm{Syl}_5(\mathfrak{S}_5)$ est transitive (théorème de Sylow). Il en résulte que le stabilisateur de chaque élément de $\mathrm{Syl}_5(\mathfrak{S}_5)$ a pour cardinal $\frac{120}{6} = 20$. Donc $|\mathrm{K}|$ divise 20. Puisque K est distingué dans $\mathfrak{S}_5$, que $|\mathrm{K}|$ divise 20 et que les sous-groupes distingués de $\mathfrak{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathfrak{S}_5$, on obtient que $\mathrm{K} = \{\mathrm{id}\}$. □

Lemme 10.6.3

Numérotons arbitrairement de 1 à 6 les éléments de $\mathfrak{S}_6/\mathrm{G}$. Faisons opérer $\mathfrak{S}_6$ sur $\mathfrak{S}_6/\mathrm{G} \simeq \{1, 2, 3, 4, 5, 6\}$ par translations.
Le morphisme $\varphi\colon \mathfrak{S}_6 \to \mathfrak{S}_6$ associé est un automorphisme.

Démonstration. — Soit K' le noyau du morphisme naturel de $\mathfrak{S}_6$ dans $\mathfrak{S}_{\mathfrak{S}_6/\mathrm{G}}$. Il est contenu dans le stabilisateur des éléments de $\mathfrak{S}_6/\mathrm{G}$ et en particulier dans celui de la classe triviale G qui n'est autre que G. Ainsi $|\mathrm{K}'|$ divise $|\mathrm{G}| = 120$. On a donc

$$\begin{cases} \mathrm{K}' \lhd \mathfrak{S}_6 \\ |\mathrm{K}'| \text{ divise } 120 \\ \text{les sous-groupes distingués de } \mathfrak{S}_6 \text{ sont } \{\mathrm{id}, \mathcal{A}_6, \mathfrak{S}_6\} \end{cases}$$

d'où $\mathrm{K}' = \{\mathrm{id}\}$. Autrement dit le morphisme φ est injectif. Pour des raisons de cardinalité φ est bijectif. □

Lemme 10.6.4

Le groupe G n'a pas de points fixes sur $\{1, 2, 3, 4, 5, 6\}$.
Le groupe $\varphi(\mathrm{G})$ admet un point fixe.
L'automorphisme φ n'est pas intérieur.

Démonstration. — Si G avait un point fixe sur $\{1, 2, 3, 4, 5, 6\} \simeq \mathfrak{S}$ cela signifierait qu'il existe un 5-sous-groupe de Sylow invariant par conjugaison, *i.e.* distingué, ce qui est absurde. Par contre $\varphi(\mathrm{G})$ a un point fixe, celui qui correspond à la classe triviale G, invariante sous l'action de G par translation.

Supposons que φ soit intérieur donc de la forme

$$\sigma \mapsto \sigma_0 \circ \sigma \circ \sigma_0^{-1}$$

pour un certain σ_0. Soit p un point fixe de $\varphi(\mathrm{G})$. On aurait alors pour tout $g \in \mathrm{G}$

$$\begin{aligned} g(\sigma_0^{-1}p) &= \sigma_0^{-1}(\sigma_0(g(\sigma_0^{-1}(p)))) \\ &= \sigma_0^{-1}((\sigma_0 \circ g \circ \sigma_0^{-1})(p)) \\ &= \sigma_0^{-1}(\varphi(g)(p)) \\ &= \sigma_0^{-1}(p) \end{aligned}$$

car p est fixe sous $\varphi(\mathrm{G})$. On aboutit alors à une contradiction. □

10.7. Classification des groupes d'ordre 12

Les groupes d'ordre 12 ont été classifiés, à isomorphisme près, pour la première fois dans les années 1880. Kempe a donné une liste de cinq groupes que Cayley a corrigée quelques années plus tard. Nous allons décrire ces cinq groupes à l'aide de produits semi-directs ; deux sont abéliens, les autres sont $\mathcal{A}_4$, D_{12} et un groupe « moins connu ».

Théorème 10.7.1

Un groupe d'ordre 12 est un produit semi-direct d'un groupe d'ordre 3 et d'un groupe d'ordre 4.

Démonstration. — Soit G un groupe d'ordre 12. Puisque $12 = 2^2 \times 3$, un 2-Sylow de G est d'ordre 4 alors qu'un 3-Sylow de G est d'ordre 3.

Désignons par n_2 (resp. n_3) le nombre de 2- Sylow (resp. 3-Sylow) de G. D'après le Théorème 10.2.4 nous avons l'alternative suivante : $n_2 = 1$ ou $n_3 = 1$.

Soit S_2 un 2-Sylow de G et soit S_3 un 3-Sylow de G.

Puisque S_2 et S_3 sont d'ordre premier, nous avons : $\mathrm{S}_2 \cap \mathrm{S}_3 = \{e\}$. De plus le cardinal de l'ensemble $\mathrm{S}_2\mathrm{S}_3 = \{xy \,|x \in \mathrm{S}_2,\, y \in \mathrm{S}_3\}$ est $\frac{|\mathrm{S}_2|\,|\mathrm{S}_3|}{|\mathrm{S}_2 \cap \mathrm{S}_3|} = 12 = |\mathrm{G}|$. Ainsi $\mathrm{G} = \mathrm{S}_2\mathrm{S}_3$. Comme l'un des S_i est distingué dans G, le groupe G est un produit semi-direct de S_2 et S_3 :

- ◇ $\mathrm{G} \simeq \mathrm{S}_2 \rtimes \mathrm{S}_3$ si $\mathrm{S}_2 \lhd \mathrm{G}$,
- ◇ $\mathrm{G} \simeq \mathrm{S}_3 \rtimes \mathrm{S}_2$ si $\mathrm{S}_3 \lhd \mathrm{G}$.

□

Remarque 10.7.1. — Dans l'énoncé précédent la notation $\mathrm{S}_2 \rtimes \mathrm{S}_3$ peut faire référence à plus d'un groupe puisqu'il pourrait y avoir différentes actions $\mathrm{S}_3 \to \mathrm{Aut}(\mathrm{S}_2)$ induisant des produits semi-directs non isomorphes.

D'une part un groupe d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$, d'autre part un groupe d'ordre 3 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, donc tout groupe d'ordre 12 est un produit semi-direct de la forme

$$\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}, \qquad \left(\mathbb{Z}/2\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/3\mathbb{Z}, \qquad \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}, \qquad \mathbb{Z}/3\mathbb{Z} \rtimes \left(\mathbb{Z}/2\mathbb{Z}\right)^2.$$

Pour les déterminer à isomorphisme près, nous cherchons comment $\mathbb{Z}/4\mathbb{Z}$ et $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$ agissent par automorphismes sur $\mathbb{Z}/3\mathbb{Z}$ et comment $\mathbb{Z}/3\mathbb{Z}$ agit par automorphismes sur $\mathbb{Z}/4\mathbb{Z}$ et $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$.

Théorème 10.7.2

Les groupes d'ordre 12 sont à isomorphisme près : $\mathbb{Z}/12\mathbb{Z}$, $\left(\mathbb{Z}/2\mathbb{Z}\right)^2 \times \times \mathbb{Z}/3\mathbb{Z}$, $\mathcal{A}_4$, D_{12} et le produit semi-direct non trivial $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.

On dit *le* produit semi-direct non trivial $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ car il n'y a qu'un seul morphisme non trivial de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathrm{Aut}\left(\mathbb{Z}/3\mathbb{Z}\right) = \left(\mathbb{Z}/3\mathbb{Z}\right)^\times$:

$$\mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/3\mathbb{Z}\right) = \left(\mathbb{Z}/3\mathbb{Z}\right)^\times, \qquad k \bmod 4 \mapsto (-1)^k \bmod 3.$$

La loi du groupe correspondant $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ est

$$(a,b)(c,d) = (a + (-1)^b c, b + d). \tag{10.7.1}$$

Ce groupe est engendré par $x = (1,0)$ et $y = (0,1)$ avec $x^3 = e$, $y^4 = e$ et $yxy^{-1} = x^{-1}$. Un modèle dans $\mathrm{SL}(2,\mathbb{C})$ pour ce groupe est : $x = \begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}$ avec $\omega = \exp\left(\frac{2\mathbf{i}\pi}{3}\right)$ et $y = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$.

Dans la démonstration du Théorème 10.7.2, nous ferons appel à la propriété suivante : pour tout produit semi-direct $\mathrm{H} \rtimes_\varphi \mathrm{K}$ et pour tout automorphisme $f\colon \mathrm{K} \to \mathrm{K}$, nous avons l'isomorphisme $\mathrm{H} \rtimes_\varphi \mathrm{K} \simeq \mathrm{H} \rtimes_{\varphi \circ f} \mathrm{K}$.

Le tableau suivant répertorie des propriétés permettant de distinguer les différents groupes d'ordre 12 à isomorphisme près (si $n_3 = 4$ alors $\mathrm{G} \simeq \mathcal{A}_4$ car G agit par conjugaison sur ses quatre sous-groupes de 3-Sylow donc induit un isomorphisme entre G avec $\mathcal{A}_4$.)

groupe	abélien	n_2	n_3	2-Sylow
$\mathbb{Z}/12\mathbb{Z}$	oui	1	1	cyclique
$\left(\mathbb{Z}/2\mathbb{Z}\right)^2 \times \mathbb{Z}/3\mathbb{Z}$	oui	1	1	non cyclique
$\mathcal{A}_4$	non	1	4	non cyclique
D_{12}	non	3	1	non cyclique
$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$	non	3	1	cycliques

Par exemple, voici cinq groupes d'ordre 12 :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3, \qquad \mathrm{PSL}(2, \mathbb{F}_3), \qquad \mathrm{Aff}\left(\mathbb{Z}/6\mathbb{Z}\right), \qquad \mathrm{Aff}(\mathbb{F}_4).$$

Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ est abélien et possède un 2-Sylow non cyclique, il est donc isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^2 \times \mathbb{Z}/3\mathbb{Z}$ (nous pouvons aussi utiliser le théorème des restes chinois). Les groupes restants ne sont pas abéliens. Puisque $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3$ possède un unique 3-Sylow et un 2-Sylow non cyclique, $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3$ est isomorphe à D_{12}. Le groupe $\mathrm{PSL}(2, \mathbb{F}_3)$ possède strictement plus de un 3-Sylow ; ainsi $\mathrm{PSL}(2, \mathbb{F}_3)$ est isomorphe à $\mathcal{A}_4$. Le groupe $\mathrm{Aff}\left(\mathbb{Z}/6\mathbb{Z}\right)$ possède strictement plus d'un 2-Sylow non cyclique, donc $\mathrm{Aff}\left(\mathbb{Z}/6\mathbb{Z}\right)$ et D_{12} sont isomorphes. Enfin, $\mathrm{Aff}(\mathbb{F}_4)$ possède strictement plus d'un 3-Sylow ; par conséquent $\mathrm{Aff}(\mathbb{F}_4)$ est isomorphe à $\mathcal{A}_4$.

Le tableau suivant répertorie le nombre d'éléments d'ordre d, d étant un diviseur de 12, des différents groupes d'ordre 12 (nous désignons par ν_i le nombre d'éléments d'ordre i) :

groupe	ν_1	ν_2	ν_3	ν_4	ν_6	ν_{12}
$\mathbb{Z}/12\mathbb{Z}$	1	1	2	2	2	4
$\left(\mathbb{Z}/2\mathbb{Z}\right)^2 \times \mathbb{Z}/3\mathbb{Z}$	1	3	2	0	6	0
$\mathcal{A}_4$	1	3	8	0	0	0
D_{12}	1	7	2	0	2	0
$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$	1	1	2	6	2	0

Une autre façon de distinguer les groupes d'ordre 12 consiste à compter les éléments d'ordre 2 et considérer la propriété d'abélianité :

groupe	abélien	#{ éléments d'ordre 2}
$\mathbb{Z}/12\mathbb{Z}$	oui	1
$\left(\mathbb{Z}/2\mathbb{Z}\right)^2 \times \mathbb{Z}/3\mathbb{Z}$	oui	3
$\mathcal{A}_4$	non	3
D_{12}	non	7
$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$	non	1

Le groupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ est abélien et possède trois éléments d'ordre 2, il est donc isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^2\times\mathbb{Z}/3\mathbb{Z}$ (nous pouvons aussi utiliser le théorème des restes chinois). Les groupes restants ne sont pas abéliens. Puisque $\mathbb{Z}/2\mathbb{Z}\times\mathfrak{S}_3$ possède sept éléments d'ordre 2, le groupe $\mathbb{Z}/2\mathbb{Z}\times\mathfrak{S}_3$ est isomorphe à D_{12}. Le groupe $\mathrm{PSL}(2,\mathbb{F}_3)$ possède trois éléments d'ordre 2 ; ainsi $\mathrm{PSL}(2,\mathbb{F}_3)$ est isomorphe à $\mathcal{A}_4$. Le groupe $\mathrm{Aff}\left(\mathbb{Z}/6\mathbb{Z}\right)$ possède sept éléments d'ordre 2, donc $\mathrm{Aff}\left(\mathbb{Z}/6\mathbb{Z}\right)$ et D_{12} sont isomorphes. Enfin, $\mathrm{Aff}(\mathbb{F}_4)$ possède trois éléments d'ordre 2 ; par conséquent $\mathrm{Aff}(\mathbb{F}_4)$ est isomorphe à $\mathcal{A}_4$.

Démonstration du Théorème 10.7.2. — Les groupes d'automorphismes des Sylow possibles sont :

$$\mathrm{Aut}\left(\mathbb{Z}/4\mathbb{Z}\right) \simeq \left(\mathbb{Z}/4\mathbb{Z}\right)^\times = \{\pm 1 \bmod 4\}, \qquad \mathrm{Aut}\left(\left(\mathbb{Z}/2\mathbb{Z}\right)^2\right) \simeq \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right),$$
$$\mathrm{Aut}\left(\mathbb{Z}/3\mathbb{Z}\right) \simeq \left(\mathbb{Z}/3\mathbb{Z}\right)^\times = \{\pm 1 \bmod 3\} \qquad .$$

- ◇ Premier cas : $n_2 = 1$, $\mathrm{S}_2 \simeq \mathbb{Z}/4\mathbb{Z}$. Puisque le 2-Sylow est distingué, le 3-Sylow agit sur lui. Notre groupe est un produit semi-direct $\mathbb{Z}/4\mathbb{Z}\rtimes\mathbb{Z}/3\mathbb{Z}$ et l'action du deuxième groupe sur le premier est donnée par un morphisme $\phi\colon \mathbb{Z}/3\mathbb{Z} \to \left(\mathbb{Z}/4\mathbb{Z}\right)^\times$. Puisque $\left|\mathbb{Z}/3\mathbb{Z}\right| = 3$ et $\left|\left(\mathbb{Z}/4\mathbb{Z}\right)^\times\right| = 2$, le morphisme ϕ est trivial. Par suite le produit semi-direct est trivial : c'est le produit direct $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ qui est cyclique d'ordre 12 (un générateur est $(1,1)$).
- ◇ Deuxième cas : $n_2 = 1$, $\mathrm{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Il faut comprendre tous les morphismes $\phi\colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{GL}\left(2,\mathbb{Z}/2\mathbb{Z}\right)$. Le morphisme trivial conduit au produit direct $\left(\mathbb{Z}/2\mathbb{Z}\right)^2\times\mathbb{Z}/3\mathbb{Z}$. Qu'en est-il des morphismes non triviaux $\phi\colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{GL}\left(2,\mathbb{Z}/2\mathbb{Z}\right)$? Le groupe $\mathrm{GL}\left(2,\mathbb{Z}/2\mathbb{Z}\right)$ est d'ordre 6 (il est isomorphe à $\mathfrak{S}_3$) ; il possède un sous-groupe d'ordre 3 : $\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}\right\}$. Un morphisme non trivial $\phi\colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{GL}\left(2,\mathbb{Z}/2\mathbb{Z}\right)$ est déterminé par l'image A de 1 mod 3, qui vérifie $A^3 = \mathrm{Id}$. Pour que ϕ soit non trivial, A doit être d'ordre 3 ; il y a deux choix pour A. En effet, les deux matrices d'ordre 3

dans $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ et elles sont inverses l'une de l'autre. Appelons l'une A, l'autre A^{-1}. Les morphismes associés à A et A^{-1} sont respectivement définis par $\phi(k \bmod 3) = A^k$ et $\psi(k \bmod 3) = A^{-k}$. On peut vérifier que $\psi = \phi \circ f$ où f est l'automorphisme de $\mathbb{Z}/3\mathbb{Z}$ défini par $f(x) = -x$. En particulier ϕ et ψ définissent à isomorphisme près le même produit semi-direct. Ainsi à isomorphisme près il existe un seul produit semi-direct non trivial $\left(\mathbb{Z}/2\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/3\mathbb{Z}$. Étant donné que $\mathcal{A}_4$ est un sous-groupe d'ordre 12 possédant un unique 2-Sylow non cyclique, ce produit semi-direct est isomorphe à $\mathcal{A}_4$.

Supposons désormais que $n_2 \neq 1$, donc $n_2 = 3$ et $n_3 = 1$. Puisque $n_2 > 1$, le groupe n'est pas abélien ; c'est donc un produit semi-direct non trivial (un produit direct de groupes abéliens est abélien).

◇ Troisième cas : $n_2 = 3$, $n_3 = 1$ et $\mathrm{S}_2 \simeq \mathbb{Z}/4\mathbb{Z}$. Notre groupe est $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, construit à partir d'un morphisme non trivial $\phi\colon \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/3\mathbb{Z}\right) = \left(\mathbb{Z}/3\mathbb{Z}\right)^\times$. Or il y a un seul choix pour ϕ car ϕ doit envoyer 1 mod 4 sur -1 mod 3, ce qui entraîne : $\phi(c \bmod 4) = (-1)^c \bmod 3$. Par conséquent il y a un seul produit semi-direct non trivial $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ et son opération de groupe est donnée par (10.7.1).

◇ Quatrième cas : $n_2 = 3$, $n_3 = 1$ et $\mathrm{S}_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Le groupe est $\mathbb{Z}/3\mathbb{Z} \rtimes \left(\mathbb{Z}/2\mathbb{Z}\right)^2$ construit à partir d'un morphisme non trivial $\phi\colon \left(\mathbb{Z}/2\mathbb{Z}\right)^2 \to \left(\mathbb{Z}/3\mathbb{Z}\right)^\times$. Le groupe $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$ a pour générateurs $(1,0)$ et $(0,1)$ et $\phi(a,b) = \phi(1,0)^a\phi(0,1)^b$ avec $\phi(1,0) = \pm 1$ et $\phi(0,1) = \pm 1$. Réciproquement cette formule pour ϕ définit un morphisme puisque a et b appartiennent à $\mathbb{Z}/2\mathbb{Z}$ et que les exposants sur ± 1 n'ont d'importance que mod 2. Le morphisme ϕ n'étant pas trivial, $\phi(1,0)$ et $\phi(0,1)$ ne valent pas tous les deux 1, il y a donc pour $\phi\colon \left(\mathbb{Z}/2\mathbb{Z}\right)^2 \to (\mathbb{Z}/3\mathbb{Z})^\times$ les trois possibilités suivantes :

$$\phi(a,b) = (-1)^a, \qquad \phi(a,b) = (-1)^b, \qquad \phi(a,b) = (-1)^a(-1)^b = (-1)^{a+b}.$$

Ces trois ϕ conduisent à des produits semi-directs isomorphes :

- si on précompose le premier ϕ avec la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ on obtient le second ϕ,
- si on précompose le premier ϕ avec la matrice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ on obtient le troisième ϕ.

Autrement dit, il y a, à isomorphisme près, un unique groupe non-abélien d'ordre 12 possédant un unique 3-Sylow et trois 2-Sylow isomorphes à $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$; il s'agit de D_{12} dont le 3-Sylow distingué est $\{1, r^2, r^4\}$.

□

10.8. Extension des théorèmes de Sylow

10.8.1. Extension des premier et second théorèmes de Sylow au cas des p-groupes. — Il est naturel de se demander si/comment les théorèmes de Sylow peuvent être étendus aux p-sous-groupes qui sont pas les sous-groupes p-Sylow. Le premier théorème de Sylow (Théorème 10.1.1) se généralise comme suit.

Théorème 10.8.1

Soit G un groupe fini. Si p^d divise $|\mathrm{G}|$, alors G contient un sous-groupe d'ordre p^d.

Une partie du second théorème de Sylow (Théorème 10.1.2) s'étend aux p-sous-groupes qui ne sont pas des Sylow.

Théorème 10.8.2

Soit G un groupe fini. Si p^d divise $|\mathrm{G}|$ et si $d > 0$, alors tout sous-groupe de G d'ordre p^{d-1} est d'indice p dans un sous-groupe de G.

Soit p^k la plus grande puissance de p divisant $|\mathrm{G}|$. Puisque le sous-groupe trivial est un p-groupe, le Théorème 10.8.2 assure l'existence d'une chaîne de p-sous-groupes de G

$$\{e\} = \mathrm{G}_0 \subset \mathrm{G}_1 \subset \mathrm{G}_2 \subset \ldots \subset \mathrm{G}_k \subset \mathrm{G}, \tag{10.8.1}$$

telle que $[\mathrm{G}_i : \mathrm{G}_{i-1}] = p$, *i.e.* $|\mathrm{G}_i| = p^i$. Notons que le Théorème 10.8.1 est un cas particulier du Théorème 10.8.2. Nous le présentons et nous le démontrons néanmoins pour illustrer certaines techniques. Sachant que pour chaque groupe fini G (et premier p) nous avons une chaîne de la forme (10.8.1), nous pouvons en construire une qui passe par un p-sous-groupe H de G :

- ◇ on commence par H et on utilise le Théorème 10.8.2 pour construire des sous-groupes successivement p fois plus grands jusqu'à à arriver à un p-Sylow de G ;
- ◇ on applique ensuite le Théorème 10.8.2 à H et on construit à partir de l'identité une chaîne de p-sous-groupes comme dans (10.8.1) jusqu'à à arriver à H.

La propriété de conjugaison des p-Sylow du Théorème 10.1.2 ne se prolonge pas aux p-sous-groupes propres : le nombre de classes de conjugaison de p-sous-groupes d'ordre fixé non maximal peut être supérieur à 1. Par exemple,

- ◇ dans $\mathfrak{S}_{p^2}$, il y a p classes de conjugaison de sous-groupes d'ordre p ;
- ◇ si G est un p-groupe non abélien contenant un élément h qui d'une part est d'ordre p et d'autre part n'appartient pas à $Z(\mathrm{G})$, alors $\langle h \rangle$ et un sous-groupe d'ordre p dans $Z(\mathrm{G})$ sont des sous-groupes non conjugués d'ordre p.

Démonstration du Théorème 10.8.1. — Nous raisonnons par récurrence sur l'ordre de G. Les cas où G est trivial ou d'ordre premier sont triviaux.

Supposons maintenant que $|\mathrm{G}| > 1$ et que tout groupe G' tel que $|\mathrm{G}'| < |\mathrm{G}|$ possède un sous-groupe d'ordre une puissance d'un nombre premier divisant $|\mathrm{G}'|$. Soit p^d tel que p est

premier, $p^d > 1$ et $p^d \mid |\mathrm{G}|$; nous cherchons un sous-groupe de G d'ordre p^d. Si G possède un sous-groupe propre H tel que p^d divise $|\mathrm{H}|$, alors, par récurrence, H possède un sous-groupe d'ordre p^d et ce sous-groupe est également contenu dans G.

Supposons désormais qu'aucun sous-groupe propre H de G soit d'ordre divisible par p^d. Comme $|\mathrm{G}| = |\mathrm{H}|[\mathrm{G} : \mathrm{H}]$ est divisible par p^d, l'indice de tout sous-groupe propre de G est divisible par p. L'équation aux classes (§3.1.1) s'écrit

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{r} [\mathrm{G} : Z_{g_i}],$$

où g_1, g_2, …, g_r représentent les classes de conjugaison de cardinal supérieur à 1. L'entier p divise $|\mathrm{G}|$ et p divise $[\mathrm{G} : Z_{g_i}]$ pour chaque i puisque chaque sous-groupe Z_{g_i} de G est propre (si $Z_{g_i} = \mathrm{G}$ alors le cardinal de la classe de conjugaison de g_i vaut 1). Il en résulte que p divise $|Z(\mathrm{G})|$. Le Théorème de Cauchy assure que $Z(\mathrm{G})$ possède un élément h d'ordre p. Comme h appartient à $Z(\mathrm{G})$, $\langle h \rangle$ est un sous-groupe distingué de G.

Nous considérons maintenant le groupe quotient ${}^{\mathrm{G}}\!/_{\langle h \rangle}$, qui est un groupe d'ordre strictement plus petit que $|\mathrm{G}|$. Étant donné que p^{d-1} divise $\left|{}^{\mathrm{G}}\!/_{\langle h \rangle}\right|$, nous obtenons par hypothèse de récurrence : ${}^{\mathrm{G}}\!/_{\langle h \rangle}$ possède un sous-groupe d'ordre p^{d-1}. Son image réciproque par $\mathrm{G} \to {}^{\mathrm{G}}\!/_{\langle h \rangle}$ est un sous-groupe de G d'ordre $pp^{d-1} = p^d$. □

Démonstration du Théorème 10.8.2. — Le Théorème de Cauchy assure que G contient un sous-groupe d'ordre p dans G, c'est le cas $d = 1$.

Supposons désormais que $d > 1$. Soit H un sous-groupe de G d'ordre p^{d-1}. Nous cherchons un sous-groupe K de G tel que $[\mathrm{K} : \mathrm{H}] = p$. Considérons l'action par multiplication à gauche de H sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$. Puisque H est un p-groupe non trivial, nous avons

$$\left|{}^{\mathrm{G}}\!/_{\mathrm{H}}\right| \equiv_p \#\{\text{ points fixes }\}. \tag{10.8.2}$$

Le membre de gauche de la congruence est $[\mathrm{G} : \mathrm{H}]$ qui est divisible par p. Déterminons les points fixes de l'action de H sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$; nous avons

$$\begin{aligned}
& \{g\mathrm{H} \mid hg\mathrm{H} = g\mathrm{H} \text{ pour tout } h \in \mathrm{H}\} \\
= \; & \{g\mathrm{H} \mid g^{-1}hg \in \mathrm{H} \text{ pour tout } h \in \mathrm{H}\} \\
= \; & \{g\mathrm{H} \mid g^{-1}\mathrm{H}g = \mathrm{H}\} \\
= \; & \{g\mathrm{H} \mid g \in N(\mathrm{H})\} \\
= \; & {}^{N(\mathrm{H})}\!/_{\mathrm{H}}.
\end{aligned}$$

Par suite l'ensemble des points fixes de l'action de H sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ est ${}^{N(\mathrm{H})}\!/_{\mathrm{H}}$ (qui a une structure de groupe puisque $\mathrm{H} \triangleleft N(\mathrm{H})$). D'après (10.8.2) l'entier p divise $\left|{}^{N(\mathrm{H})}\!/_{\mathrm{H}}\right|$. Le Théorème de Cauchy assure que ${}^{N(\mathrm{H})}\!/_{\mathrm{H}}$ contient un sous-groupe H' d'ordre p. L'image réciproque de H'

par $\pi\colon N(\mathrm{H}) \to {}^{N(\mathrm{H})}\!/_{\mathrm{H}}$ est un sous-groupe $\pi^{-1}(\mathrm{H}')$ de $N(\mathrm{H})$ d'ordre $pp^{d-1} = p^d$ qui contient H et $[\pi^{-1}(\mathrm{H}') : \mathrm{H}] = p$. □

Corollaire 10.8.1

Soit G un groupe fini. Soit H un p-sous-groupe de G.
Alors
$$[\mathrm{G} : \mathrm{H}] \equiv_p [N(\mathrm{H}) : \mathrm{H}];$$
en particulier si p divise $[\mathrm{G} : \mathrm{H}]$, alors $[N_{\mathrm{G}}(\mathrm{H}) : \mathrm{H}]$ donc $\mathrm{H} \neq N_{\mathrm{G}}(\mathrm{H})$.

Démonstration. — Considérons l'action par translation à gauche de H sur l'ensemble quotient ${}^{\mathrm{G}}\!/_{\mathrm{H}}$:
$$\mathrm{H} \times {}^{\mathrm{G}}\!/_{\mathrm{H}} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}, \qquad (h, g\mathrm{H}) \mapsto h \cdot g\mathrm{H} = hg\mathrm{H}$$
Puisque H est un p-groupe, la Proposition 6.3.1 assure que
$$\#{}^{\mathrm{G}}\!/_{\mathrm{H}} \equiv_p \#{}^{\mathrm{G}}\!/_{\mathrm{H}}{}^{\mathrm{H}}$$
Un élément $g\mathrm{H}$ de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ est fixé par l'action par translation à gauche de H si et seulement si
$$\begin{aligned} hg\mathrm{H} = g\mathrm{H} \quad \forall\, h \in \mathrm{H} &\iff hg \in g\mathrm{H} \quad \forall\, h \in \mathrm{H} \\ &\iff g^{-1}hg \in \mathrm{H} \quad \forall\, h \in \mathrm{H} \\ &\iff g^{-1}\mathrm{H}g \subset \mathrm{H} \\ &\iff g^{-1}\mathrm{H}g \subset \mathrm{H} \text{ car } |g^{-1}\mathrm{H}g| = |\mathrm{H}| \\ &\iff g \in \mathrm{N}_{\mathrm{G}}(\mathrm{H}). \end{aligned}$$
Autrement dit ${}^{\mathrm{G}}\!/_{\mathrm{H}}{}^{\mathrm{H}} = \{g\mathrm{H} \,|\, g \in \mathrm{N}_{\mathrm{G}}(\mathrm{H})\} = {}^{\mathrm{N}_{\mathrm{G}}(\mathrm{H})}\!/_{\mathrm{H}}$. Par conséquent $\#{}^{\mathrm{G}}\!/_{\mathrm{H}} \equiv_p \#{}^{\mathrm{G}}\!/_{\mathrm{H}}{}^{\mathrm{H}}$ se réécrit
$$[\mathrm{G} : \mathrm{H}] \equiv_p [\mathrm{N}_{\mathrm{G}}(\mathrm{H}) : \mathrm{H}].$$
Lorsque p divise $[\mathrm{G} : \mathrm{H}]$, $[N_{\mathrm{G}}(\mathrm{H}) : \mathrm{H}] \neq 1$ d'où $\mathrm{H} \neq N_{\mathrm{G}}(\mathrm{H})$. □

10.8.2. Extension du troisième théorème de Sylow. — Nous démontrons une extension d'une partie du troisième théorème de Sylow à l'aide des relations de G-équivalence (§**??**).

Théorème 10.8.3

Soit G un groupe fini. Soit p un diviseur premier de $|\mathrm{G}|$. Pour chaque p-sous-groupe H de G, le nombre de p-sous-groupes intermédiaires $\mathrm{H} \subset \mathrm{K} \subset \mathrm{G}$ d'ordre fixé est congru à 1 modulo p.

Le cas du Théorème 10.8.3 où H est trivial et les sous-groupes sont d'ordre une puissance de p maximale est contenu dans le troisième Théorème de Sylow. Le cas où H est trivial et l'ordre fixé est une puissance arbitraire de p divisant $|\mathrm{G}|$ est dû à Frobenius (1895).

Théorème 10.8.4

Soit G un groupe fini agissant transitivement sur un ensemble X. Supposons que le stabilisateur d'un point de X est un p-sous-groupe de G, où p désigne un nombre premier. Si p^m divise $\#X$, alors le nombre de relations de G-équivalence sur X dont les classes d'équivalence sont chacune de cardinal p^m est congru à 1 modulo p.

Notons qu'on peut déduire le Théorème 10.8.3 du Théorème 10.8.4. Le Théorème **??** appliqué à l'action usuelle de G sur G/H assure que les relations de G-équivalence sur G/H sont en bijection avec les sous-groupes contenus entre H et G ; de plus, le cardinal d'une classe d'équivalence dans une relation d'équivalence est égal à l'indice de H dans le sous-groupe correspondant à cette relation d'équivalence. Comme H est un p-sous-groupe de G, un sous-groupe intermédiaire $\mathrm{H} \subset \mathrm{K} \subset \mathrm{G}$ est un p-sous-groupe si et seulement si $[\mathrm{K} : \mathrm{H}]$ est une puissance de p. Les Théorèmes 10.8.3 et 10.8.4 sont donc équivalents.

Démonstration du Théorème 10.8.4. — Écrivons $\#X$ sous la forme rp^m. Soit $x \in X$. Posons $T = \{Y \subset X \,|\, \#Y = p^m\}$. Notons que le groupe G agit sur T par translation à gauche. Remarquons que $\#T = \binom{rp^m}{p^m}$.

Soit $Y \in T$. Lorsque g parcourt G les ensembles gY recouvrent X (le groupe G agit transitivement sur X) ; de plus, chacun est de cardinal p^m. Il en résulte que

$$\#X \leq \#\{gY \,|\, g \in \mathrm{G}\} \cdot \#Y.$$

avec égalité précisément lorsque $\{gY \,|\, g \in \mathrm{G}\}$ est une partition de X. En écrivant explicitement le cardinal de X et celui de Y, cette inégalité devient

$$r \leq \#\{gY \,|\, g \in \mathrm{G}\} \tag{10.8.3}$$

avec égalité si et seulement si $\{gY \,|\, g \in \mathrm{G}\}$ est une partition de X.

Posons $\mathrm{K}_Y = \{g \in \mathrm{G} \,|\, gY = Y\}$; c'est le stabilisateur de Y pour l'action de G sur T. Soient $y \in Y$ et $H_y = \mathrm{St}(y) = \{g \in \mathrm{G} \,|\, gy = y\}$. Par hypothèse il s'agit d'un p-sous-groupe de G. Considérons

$$\widetilde{Y} = \{g \in \mathrm{G} \,|\, gy \in Y\}.$$

C'est un sous-ensemble de G (il n'y a aucune raison pour qu'il soit stable par inversion, *i.e.* il n'y a aucune raison pour que ce soit un sous-groupe de G). Nous avons les inclusions $\mathrm{H}_y \subset \widetilde{Y}$ et $\mathrm{K}_Y \subset \widetilde{Y}$. Notons que si g et g' désignent deux éléments de $\widetilde{Y}$, alors $gy = g'y$ si et seulement si $g\mathrm{H}_y = g'\mathrm{H}_y$. Puisque $\mathrm{H}_y \subset \widetilde{Y}$, $\widetilde{Y}$ est l'union de $\#Y$ classes à gauche modulo H_y ; par suite

$$|\widetilde{Y}| = |Y|\,|\mathrm{H}_y|, \tag{10.8.4}$$

est une puissance de p. Si k appartient à K_Y et g appartient à $\widetilde{Y}$, alors kgy appartient à $kY = Y$, donc kg appartient à $\widetilde{Y}$. Ainsi K_Y agit par multiplication à gauche sur $\widetilde{Y}$. Puisque $\widetilde{Y}$ est un sous-ensemble de G, ses K_Y-orbites sont des classes à droite modulo K_Y et $|\mathrm{K}_Y|$ divise

$|\widetilde{Y}|$. Ainsi, d'après 10.8.4, K_Y est un p-sous-groupe de G. Puisque $\{gY \mid g \in \mathrm{G}\}$ est une G-orbite dans T et puisque le stabilisateur de Y est K_Y, nous avons

$$|\{gY \mid g \in \mathrm{G}\}| = [\mathrm{G} : \mathrm{K}_Y] = \frac{|\mathrm{G}|}{|\mathrm{K}_Y|} = \frac{[\mathrm{G} : \mathrm{H}_y]|\mathrm{H}_y|}{|\mathrm{K}_Y|} = \frac{rp^m|\mathrm{H}_y|}{|\mathrm{K}_Y|} = rp^{i(Y)}$$

pour un certain entier $i(Y)$. D'après (10.8.3) nous avons l'inégalité $p^{i(Y)} \geq 1$ d'où $i(Y) \geq 0$.

Nous appliquons maintenant la Proposition 6.3.1 à l'action de G sur T. Soit $y \in X$. Chaque G-orbite dans T est une collection d'ensembles $\{gY \mid g \in \mathrm{G}\}$; elle recouvre X, nous pouvons donc choisir Y de sorte que Y contient y (l'action de G sur X étant transitive au moins un des ensembles gY contient y et nous pouvons le renommer Y). Soient $Y_1, Y_2, \ldots, Y_d$ les représentants des différentes G-orbites dans T. Alors

$$|T| = \sum_{j=1}^{d} |\{gY_j \mid g \in \mathrm{G}\}|,$$

donc

$$\binom{rp^m}{p^m} = \sum_{j=1}^{d} rp^{i(Y_j)}$$

Comme $\binom{rp^m}{p^m} = r\binom{rp^m-1}{p^m-1}$ nous avons

$$\binom{rp^m-1}{p^m-1} = \sum_{j=1}^{d} p^{i(Y_j)} \equiv_p |\{j \mid i(Y_j) = 0\}|. \tag{10.8.5}$$

Pour quel $Y \in T$ a-t-on $i(Y) = 0$? D'après la définition de $i(Y)$, le fait que $i(Y) = 0$ équivaut à $|\{gY \mid g \in \mathrm{G}\}| = r$ ce qui équivaut au fait que les ensembles $\{gY \mid g \in \mathrm{G}\}$ forment une partition de X (*voir* (10.8.3)) Cette partition contient des classes d'équivalence pour une relation de G-équivalence sur X où les classes sont de cardinal p^m. Donc

$$|\{j \mid i(Y_j) = 0\}| = |\{\text{relations de G-équivalence avec des classes de cardinal } p^m\}|. \tag{10.8.6}$$

Le membre gauche de (10.8.5) peut être calculé directement modulo p en utilisant un résultat de Lucas : si $a = a_0 + a_1p + \ldots + a_np^n$ et $b = b_0 + b_1p + \ldots + b_np^n$ où $0 \leq a_i$, $b_i \leq p-1$ pour $j < n$ et a_n, $b_n \geq 0$, alors

$$\binom{a}{b} \equiv_p \binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_n}{b_n}.$$

En particulier, puisque

$$\begin{aligned} rp^m - 1 &= (p-1) + (p-1)p + \ldots + (p-1)p^{m-1} + (r-1)p^m, \\ p^m - 1 &= (p-1) + (p-1)p + \ldots + (p-1)p^{m-1}, \end{aligned}$$

la congruence de Lucas montre que $\binom{rp^m-1}{pm-1} \equiv_p \prod_{i=0}^{m-1}\binom{p-1}{p-1} \cdot \binom{r-1}{0} \equiv_p 1.$ □

CHAPITRE 11

REPRÉSENTATIONS DES GROUPES

Aux confins de la théorie des groupes et de la géométrie (linéaire) trône la théorie des représentations. Une représentation est une action linéaire d'un groupe sur un espace. Il s'agit donc de plonger un groupe (ou un quotient du groupe) dans un groupe de matrices. Autrement dit la théorie des représentations des groupes permet l'étude des groupes abstraits en représentant leurs éléments par des matrices inversibles. Nous disposons alors des méthodes de l'algèbre linéaire qui rendent souvent l'étude de ces groupes plus facile et permettent d'en obtenir de nouvelles propriétés.

11.1. Représentations

Soit G un groupe. Soit V un $\Bbbk$-espace vectoriel. Une *représentation linéaire* de G dans V est un morphisme de groupes

$$\rho\colon \mathrm{G} \to \mathrm{GL}(V).$$

Autrement dit les éléments de G sont représentés comme des automorphismes de V ou plus simplement si V est de dimension finie et que nous en choisissons une base comme des matrices inversibles. La représentation (V, ρ) est *fidèle* si ρ est injectif, auquel cas ρ permet de représenter le groupe abstrait G de manière concrète comme un sous-groupe de $\mathrm{GL}(V)$. Si V est de dimension finie, le choix d'une base fournit une représentation encore plus concrète comme groupe de matrices.

Une telle représentation sera notée (V, ρ) ou plus simplement en l'absence d'ambiguïté, ρ ou V. L'action d'un élément $g \in \mathrm{G}$ sur V est souvent notée $g \cdot v = \rho(g)(v)$. C'est une action du groupe G sur V.

Exemple 11.1.1. — Une représentation de G dans un espace vectoriel de dimension 1 est un morphisme $\rho\colon \mathrm{G} \to \Bbbk^\times$. Si G est fini, l'image est un sous-groupe cyclique.

Exemple 11.1.2. — Pour tout $\Bbbk$-espace vectoriel V la *représentation triviale* ρ_{triv} sur V est définie par $\rho_{\mathrm{triv}}(g) = \mathrm{id}_V$ pour tout $g \in \mathrm{G}$.

Exemple 11.1.3. — Si G est défini comme un sous-groupe de $\mathrm{GL}(V)$ (ce qui est le cas des groupes classiques, le groupe diédral, les sous-groupes $\mathcal{A}_4$, $\mathcal{A}_5$ et $\mathfrak{S}_4$ de $\mathrm{SO}(3,\mathbb{R})$ mais aussi les sous-groupes $\mathrm{O}(n,\mathbb{R})$, $\mathrm{SO}(n,\mathbb{R})$, $\mathrm{GL}(n,\mathbb{R})$ de $\mathrm{GL}(n,\mathbb{C})$), l'inclusion $\mathrm{G} \hookrightarrow \mathrm{GL}(V)$ est appelée la *représentation standard*.

Exemple 11.1.4. — Si E est un ensemble fini muni d'une action (à gauche) de G donnée par $(g,x) \mapsto g \cdot x$, nous définissons la *représentation de permutation* (V_E, ρ), associée à E, comme l'espace vectoriel V_E de dimension $|E|$, de base $(e_x)_{x\in E}$, muni de l'action linéaire de G donnée, sur les vecteurs de la base, par $g \cdot e_x = e_{g\cdot x}$. Si g_1, g_2 appartiennent à G, si x appartient à E, nous avons

$$g_1 \cdot (g_2 \cdot e_x) = g_1 \cdot (e_{g_2\cdot x}) = e_{g_1 g_2 \cdot x} = g_1 g_2 \cdot e_x$$

ce qui montre que la formule précédente définit bien une action de G sur V_E. Dans la base $(e_x)_{x\in E}$ la matrice de g est une *matrice de permutation*, *i.e.*

- ◇ a exactement un 1 par ligne et par colonne et tous les autres coefficients sont nuls
- ◇ et le terme diagonal est égal à 1 si et seulement si $g \cdot x = x$ (*i.e.* si x est un point fixe de g), sinon il vaut 0.

Un cas particulier intéressant est celui où G est fini, $E = \mathrm{G}$, et l'action de G est donnée par la multiplication à gauche (*i.e.* $g \cdot h = gh$). La représentation (V_{G}, ρ) ainsi obtenue est la *représentation régulière* de G, nous la noterons ρ_R.

La représentation régulière est fidèle (en effet $\rho_R(g)(h) = g \cdot h = gh$ donc $\rho_R(g)(h) = h$ si et seulement si $gh = h$ si et seulement si $g = e$).

Exemple 11.1.5. — Le groupe des quaternions a pour présentation

$$\mathbb{H}_8 = \langle i,\, j \,|\, i^4 = j^4 = 1,\, i^2 = j^2,\, i^{-1}ji = j^{-1}\rangle.$$

On peut vérifier que

$$\rho\colon \mathbb{H}_8 \to \mathrm{GL}(2,\mathbb{C}) \qquad i \mapsto \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix} \qquad j \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

définit une représentation de $\mathbb{H}_8$.

***Exemple 11.1.6* (Représentations de $\mathbb{Z}$).** —

- ◇ Si λ appartient à $\mathbb{C}^*$, alors $n \mapsto \lambda^n$ est un morphisme de groupes de $\mathbb{Z}$ dans $\mathbb{C}^*$, ce qui induit une représentation de $\mathbb{Z}$ notée $C(\lambda)$, l'action de $n \in \mathbb{Z}$ sur $z \in \mathbb{C}$ étant donnée par $C(\lambda)(z) = \lambda^n z$ (ce que nous pouvons aussi écrire $n \cdot z = \lambda^n z$).
- ◇ Si V est un $\mathbb{C}$-espace vectoriel et si $u\colon V \to V$ est un isomorphisme linéaire, l'application $n \mapsto u^n$ est un morphisme de groupes de $\mathbb{Z}$ dans $\mathrm{GL}(V)$ ce qui fait de V une représentation du groupe additif $\mathbb{Z}$, l'action de $n \in \mathbb{Z}$ sur $v \in V$ étant donnée par $n \cdot v = u^n(v)$. Réciproquement si V est une représentation de $\mathbb{Z}$, alors $u = \rho_V(1)$ appartient à $\mathrm{GL}(V)$ et nous avons $\rho_V(n) = u^n$ pour tout $n \in \mathbb{Z}$ et donc $n \cdot v = u^n(v)$ si n appartient à $\mathbb{Z}$ et v à

V. Autrement dit une représentation de $\mathbb{Z}$ n'est rien d'autre que la donnée d'un $\mathbb{C}$-espace vectoriel V et d'un élément u de $\mathrm{GL}(V)$.

***Exemple 11.1.7* (Représentations de $\mathbb{Z}/n\mathbb{Z}$).** — Si V est un $\mathbb{C}$-espace vectoriel muni d'un isomorphisme linéaire u tel que $u^n = 1$, alors l'application $n \mapsto u^n$ est un morphisme de groupes de $\mathbb{Z}$ dans $\mathrm{GL}(V)$ dont le noyau contient $n\mathbb{Z}$. Il induit donc un morphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathrm{GL}(V)$ ce qui fait de V une représentation de $\mathbb{Z}/n\mathbb{Z}$, l'action de $\overline{n} \in \mathbb{Z}/n\mathbb{Z}$ sur $v \in V$ étant donnée par $n \cdot v = u^n(v)$.

Réciproquement si V est une représentation de $\mathbb{Z}/n\mathbb{Z}$ et si $u = \rho(1) \in \mathrm{GL}(V)$, alors $u^n = \rho(n) = \rho(0) = 1$ car $n = 0$ dans $\mathbb{Z}/n\mathbb{Z}$. Autrement dit une représentation de $\mathbb{Z}/n\mathbb{Z}$ n'est rien d'autre que la donnée d'un $\mathbb{C}$-espace vectoriel V et d'un élément u de $\mathrm{GL}(V)$ vérifiant $u^n = 1$.

Remarque 11.1.1. — Dans les Exemples 11.1.6 et 11.1.7 nous disposons d'une présentation du groupe à partir de générateurs (dans les deux cas G est engendré par 1) et de relations entre les générateurs (pas de relation dans le cas de $\mathbb{Z}$, une relation $n = 0$ dans le cas de $\mathbb{Z}/n\mathbb{Z}$). Ceci permet de décrire une représentation de G en disant ce que fait chaque générateur, les relations entre les générateurs imposant des relations entre leurs actions. Ce type de description est très efficace quand on dispose d'une présentation simple du groupe G.

Par exemple le groupe $\mathbb{Z}^2$ est engendré par $e_1 = (1,0)$ et $e_2 = (0,1)$ et est décrit par la relation de commutation $e_1 + e_2 = e_2 + e_1$. Une représentation de $\mathbb{Z}^2$ est donc la donnée d'un $\mathbb{C}$-espace vectoriel V et de deux éléments de $\mathrm{GL}(V)$ commutant entre eux.

Le groupe $\mathrm{SL}(2,\mathbb{Z})$ est engendré par les matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et toute relation entre S et T est conséquence des relations

$$S^4 = \mathrm{id}, \qquad S^2T = TS^2, \qquad (ST)^3 = S^2;$$

une représentation de $\mathrm{SL}(2,\mathbb{Z})$ est donc la donnée d'un $\mathbb{C}$-espace vectoriel V et de deux éléments u et v de $\mathrm{GL}(V)$ vérifiant $u^4 = \mathrm{id}$, $u^2v = vu^2$ et $(uv)^3 = u^2$.

***Exemple 11.1.8* (Somme directe de représentations).** — Considérons (V_1, ρ_1) et (V_2, ρ_2) deux représentations du même groupe G sur un corps $\Bbbk$. On dispose du $\Bbbk$-espace vectoriel $V_1 \oplus V_2$ « somme directe abstraite » (si on souhaite c'est simplement $V_1 \times V_2$) qu'on promeut en représentation de G en définissant $\rho(g) = (\rho_1(g), \rho_2(g))$ (matriciellement la représentation somme directe $V_1 \oplus V_2$ est donnée par des matrices diagonales par blocs).

***Exemple 11.1.9* (Représentation $\mathrm{Hom}(V_1, V_2)$).** — Considérons (V_1, ρ_1) et (V_2, ρ_2) deux représentations du groupe G sur un même corps $\Bbbk$. On définit une représentation $\mathrm{Hom}(V_1, V_2)$ par (en appliquant le principe de conjugaison) :

$$\forall\, g \in \mathrm{G} \quad \forall\, f \in \mathcal{L}(V_1, V_2) \qquad \rho(g)(f) = \rho_2(g) \circ f \circ \rho_1(g)^{-1} = \rho_2(g) \circ f \circ \rho_1(g^{-1})$$

(*i.e.* $g \cdot f = gfg^{-1}$).

On définit bien ainsi une représentation. Tout d'abord constatons que $\rho(g)$ est bien une application linéaire. Ensuite pour tout $f \in \mathcal{L}_{\Bbbk}(V_1, V_2)$ et pour tous g, h dans G nous avons

$$\begin{aligned}\rho(gh)(f) &= \rho_2(gh) \circ f \circ \rho_1((gh)^{-1}) \\ &= \rho_2(g) \circ \Big(\rho_2(h) \circ f \circ \rho_1(h^{-1})\Big) \circ \rho_1(g^{-1}) \\ &= \rho(g)(\rho(h)(f))\end{aligned}$$

Il est intéressant de voir $\rho(g)(f)$ comme l'unique application linéaire $V_1 \to V_2$ faisant commuter le diagramme

$$\begin{tikzcd} V_1 \arrow[r, "f"] \arrow[d, "g"', "\simeq"] & V_2 \arrow[d, "g"', "\simeq"] \\ V_1 \arrow[r, "g\cdot f"'] & V_2 \end{tikzcd}$$

Cette opération munit $\mathcal{L}_k(V_1, V_2)$ d'une structure de G-espace vectoriel.

***Exemple 11.1.10* (Contragrédiente).** — C'est la représentation duale d'une représentation (V, ρ) au sens de l'exemple précédent :

$$\forall\, g \in \mathrm{G} \quad \forall\, \ell \in V^* \qquad \rho^*(g)(\ell) = \rho_{\mathrm{triv}}(g) \circ \ell \circ \rho(g)^{-1} = \ell \circ \rho(g)^{-1}$$

c'est-à-dire

$$\rho^*(g) = {}^{\mathrm{t}}\rho(g)^{-1} \in \mathrm{GL}(V^*).$$

11.1.1. — Soit (V, ρ) une représentation de G. La *dimension* ou le *degré* de la représentation est $\dim V$.

Une *sous-représentation* de (V, ρ) est un sous-espace vectoriel $W \subset V$ stable sous l'action de G. On parle de *sous-espace* G-*invariant*. Dans ce cas nous avons des représentations induites sur W et sur le quotient V/W.

Exemple 11.1.11. — En reprenant les notations de l'Exemple 11.1.6 nous avons $\dim C(\lambda) = 1$ pour tout $\lambda \in \mathbb{C}^*$.

Exemple 11.1.12. — Si n est impair, alors le groupe diédral

$$\mathrm{D}_{2n} = \langle r,\, s \mid s^2 = r^n = srs^{-1}r = \mathrm{id}\rangle$$

admet deux représentations complexes de degré 1 : celle donnée par

$$s \mapsto 1, \qquad\qquad r \mapsto 1$$

et celle donnée par

$$s \mapsto -1, \qquad\qquad r \mapsto 1.$$

Si n est pair, alors le groupe diédral D_{2n} admet quatre représentations complexes de degré 1 données par

$$s \mapsto (-1)^k, \qquad\qquad r \mapsto (-1)^\ell$$

avec $0 \leq k,\ \ell \leq 1$.

Les autres représentations sont toutes de degré 2 ; elles sont en nombre $\frac{n-1}{2}$ si n est impair et $\frac{n}{2} - 1$ si n est pair [1]. Nous pouvons les définir comme suit

$$\rho_\ell \colon r \mapsto \begin{pmatrix} \zeta^\ell & 0 \\ 0 & \zeta^{-\ell} \end{pmatrix} \qquad\qquad \rho_\ell \colon s \mapsto \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

où ζ désigne une racine primitive $n$ième de l'unité et $1 \leq \ell \leq n-1$. Deux telles représentations ρ_{ℓ_1} et ρ_{ℓ_2} sont isomorphes si et seulement si $\ell_1 + \ell_2 = n$:

$$\rho_{\ell_1}(s)\rho_{\ell_1}(r)\rho_{\ell_1}(s^{-1}) = \rho_{\ell_1}(r)^{-1} = \rho_{n-\ell_1}(r).$$

Exemple 11.1.13. — Le sous-espace vectoriel

$$V^{\mathrm{G}} = \{v \in V \mid \forall\, g \in \mathrm{G} \quad g \cdot v = v\}$$

des vecteurs fixes sous G est un sous-espace G-invariant : si h appartient à G et v appartient à V^{G}, on a pour tout $g \in \mathrm{G}$

$$g \cdot (h \cdot v) = g \cdot v = v = h \cdot v$$

donc $h \cdot v$ appartient à V^{G}.

Exemple 11.1.14. — Si $V = \Bbbk^n$ est la représentation du groupe symétrique $\mathfrak{S}_n$, alors l'hyperplan

$$V_0 = \Big\{(x_1, \ldots, x_n) \in V \mid \sum_{i=1}^n x_i = 0\Big\}$$

est une sous-représentation de V, ainsi que la droite

$$V_1 = \Bbbk(1, \ldots, 1)$$

qui en est un supplémentaire si et seulement si la caractéristique de $\Bbbk$ ne divise pas n.

***Exemple 11.1.15* (Construction d'une représentation de dimension 2 de $\mathfrak{S}_3$)**

Soient $A = (1, 0)$, $B = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ et $C = \left(-\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$. Les points A, B et C sont les sommets d'un triangle équilatéral de centre de gravité $O = (0, 0)$. Les isométries du plan laissant stable ce triangle fixent O et donc sont linéaires. Elles forment donc un sous-groupe de $\mathrm{O}(2, \mathbb{R}) \subset \mathrm{GL}(2, \mathbb{C})$ qui n'est autre que D_6. L'injection de D_6 dans $\mathrm{GL}(2, \mathbb{C})$ fait de $\mathbb{C}^2$ une représentation du groupe D_6 et nous allons montrer que ce groupe est isomorphe à $\mathfrak{S}_3$ pour construire notre représentation de $\mathfrak{S}_3$. Un élément de D_6 laisse fixe l'ensemble $\{A,\ B,\ C\}$

1. Nous utilisons ici d'une part que le nombre de représentations irréductibles d'un groupe G est égal au nombre de classes de conjugaison de G (Corollaire 11.2.1) et d'autre part la description des classes de conjugaison de D_{2n} (Proposition **??**)

et fournit un morphisme de groupes φ de D_6 dans le groupe des permutations $\mathfrak{S}_{\{A,B,C\}}$ de $\{A, B, C\}$. Puisque A, B et C ne sont pas alignés, un élément de D_6 est uniquement déterminé par les images de A, B et C ce qui signifie que φ est injectif. Par ailleurs φ est surjectif car D_6 contient

- ◇ les symétries par rapport aux droites (OA), (OB) et (OC) qui s'envoient respectivement sur les transpositions $(B\ C)$, $(A\ C)$ et $(A\ B)$;
- ◇ les rotations d'angle 0, $\frac{2\pi}{3}$ et $-\frac{2\pi}{3}$ dont les images respectives sont l'identité et les 3-cycles $(A\ B\ C)$ et $(A\ C\ B)$.

Ainsi $\varphi\colon \mathrm{D}_6 \to \mathfrak{S}_{\{A,B,C\}}$ est un isomorphisme de groupes. La bijection

$$1 \mapsto A \qquad\qquad 2 \mapsto B \qquad\qquad 3 \mapsto C$$

de $\{1, 2, 3\}$ sur $\{A, B, C\}$ fournit un isomorphisme $\psi\colon \mathfrak{S}_3 \xrightarrow{\simeq} \mathfrak{S}_{\{A,B,C\}}$. Nous obtenons un morphisme de groupes de $\mathfrak{S}_3$ dans $\mathrm{GL}(2,\mathbb{C})$ en composant $\varphi^{-1} \circ \psi\colon \mathfrak{S}_3 \to \mathrm{D}_6$ avec l'injection de D_6 dans $\mathrm{GL}(2,\mathbb{C})$. Ce morphisme fait de $\mathbb{C}^2$ une représentation de $\mathfrak{S}_3$.

Remarque 11.1.2. — Soit G un groupe fini. Tout élément de G est alors d'ordre fini. Soit (V,ρ) une représentation de G. Si $g \in \mathrm{G}$ est d'ordre n, alors $\rho(g)^n = \rho(g^n) = \mathrm{id}$. Puisque le polynôme $X^n - 1$ n'a que des racines simples, $\rho(g)$ est diagonalisable et comme les valeurs propres de $\rho(g)$ sont des racines de $X^n - 1$ ce sont des racines de l'unité.

Un *morphisme* entre des représentations (V,ρ_V) et (W,ρ_W) d'un groupe G est une application linéaire $u\colon V \to W$ telle que

$$\forall\, g \in \mathrm{G} \qquad u \circ \rho_V(g) = \rho_W(g) \circ u.$$

Dans ce cas $\ker u$ et $\operatorname{im} u$ sont des sous-représentations de V et W et u induit un isomorphisme de représentations

$$V/_{\ker u} \xrightarrow{\sim} \operatorname{im} u.$$

L'espace vectoriel des morphismes entre les représentations V et W est noté $\mathrm{Hom}_{\mathrm{G}}(V,W)$ ou $\mathrm{Hom}(\rho_V,\rho_W)$. Des représentations ρ_V et ρ_W de dimension finie d'un groupe G sont *isomorphes* si et seulement s'il existe une base de V et une base de W dans lesquelles pour tout $g \in \mathrm{G}$ les matrices de $\rho_V(g)$ et $\rho_W(g)$ sont les mêmes.

Exemple 11.1.16. — En posant

$$\rho(\overline{1}) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad \rho'(\overline{1}) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

nous définissons deux représentations fidèles de $\mathbb{Z}/_{2\mathbb{Z}}$ dans $\mathrm{GL}(2,\mathbb{C})$ qui sont non isomorphes (comparer les ensembles de points fixes).

11.1.2. Représentations irréductibles. —

Définition 11.1.1

Une représentation V est *irréductible* si elle est non nulle et si ses seules sous-représentations sont 0 et V.

Toute représentation de dimension 1 est bien sûr irréductible.

Exemple 11.1.17. — Si G est abélien et si $\Bbbk$ est algébriquement clos, les seules représentations irréductibles V de dimension finie de G sont de dimension 1. Soit g dans G et soit $W \subseteq V$ un sous-espace propre (non nul) de $\rho(g)$, pour une valeur propre $\lambda \in \Bbbk$. Puisque G est abélien, nous avons

$$\forall\, h \in \mathrm{G}, \forall\, x \in W \qquad \rho(g)\big(\rho(h)(x)\big) = \rho(h)\big(\rho(g)(x)\big) = \rho(h)(\lambda x) = \lambda\rho(h)(x);$$

ainsi $\rho(h)(x)$ appartient à W. Le sous-espace vectoriel W de V est donc stable par tous les $\rho(h)$: c'est une sous-représentation non nulle de V. Puisque V est irréductible elle est égale à V. Par conséquent tous les $\rho(g)$ sont des homothéties. Toute droite $D \subset V$ est alors une sous-représentation. Par suite $D = V$.

Exemple 11.1.18. — Les représentations de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}$ sont données par l'image d'un générateur qui doit être une racine n-ième de l'unité dans $\mathbb{C}$ (Exemple 11.1.7). Nous obtenons ainsi les n représentations irréductibles ρ_0, ρ_1, …, ρ_{n-1} de $\mathbb{Z}/n\mathbb{Z}$ données par

$$\rho_j(k) = \exp\left(\frac{2kj\pi\mathbf{i}}{n}\right) \qquad \forall\, k \in \mathbb{Z}/n\mathbb{Z}.$$

Remarquons que ceci n'est plus vrai lorsque $\Bbbk = \mathbb{R}$: la représentation de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{R}^2$ qui à $k \in \mathbb{Z}/n\mathbb{Z}$ associe la rotation d'angle $\frac{2k\pi}{n}$ est irréductible lorsque $n \geq 3$; en effet aucune droite n'est laissée stable par une telle rotation.

Exemple 11.1.19. — Les représentations du groupe diédral (Exemple 11.1.12) sont irréductibles. En effet, les seules droites stables par $\rho_j(r)$ sont les axes $\mathbb{C}(e_1)$ et $\mathbb{C}(e_2)$. Mais $\mathbb{C}(e_1)$ et $\mathbb{C}(e_2)$ ne sont pas stables par $\rho_j(s)$. Ainsi

- ◇ si n est pair, les représentations ρ_j, $1 \leq j \leq \frac{n}{2} - 1$, sont irréductibles.
- ◇ si n est impair, les représentations ρ_j, $1 \leq j \leq \frac{n-1}{2}$, sont irréductibles.

Exemple 11.1.20. — Si $\dim V \geq 2$, les représentations standards de $\mathrm{SL}(V)$ et $\mathrm{GL}(V)$ sont irréductibles puisque ces groupes opèrent transitivement sur $V \smallsetminus \{0\}$. C'est aussi le cas pour $\mathrm{O}(n, \mathbb{R})$, qui opère transitivement sur la sphère unité $\mathbb{S}^{n-1}$, qui engendre l'espace vectoriel $\mathbb{R}^n$.

Exemple 11.1.21. — Soient $\rho_V \colon \mathrm{G} \to \mathrm{GL}(V)$ et $\rho_W \colon \mathrm{G} \to \mathrm{GL}(W)$ deux représentations de G. Si W est de dimension 1, alors le groupe $\mathrm{GL}(W)$ s'identifie canoniquement à $\Bbbk^\times$ et la

représentation $\rho_{V\otimes W}\colon \mathrm{G} \to \mathrm{GL}(V\otimes W)$ est isomorphe à la représentation

$$\mathrm{G} \to \mathrm{GL}(V) \qquad\qquad g \mapsto \rho_W(g)\rho_V(g)$$

dont les sous-espaces G-invariants sont les mêmes que ceux de ρ_V. Ce n'est plus vrai en général si $\dim W > 1$ même si ρ_W est irréductible !

Exemple 11.1.22. — La représentation de $\mathfrak{S}_3$ sur $\mathbb{C}^2$ de l'Exemple 11.1.15 est irréductible. Raisonnons par l'absurde : supposons qu'elle ne soit pas irréductible. Puisqu'elle est de dimension 2 une sous-représentation distincte de 0 ou $\mathbb{C}^2$ est une droite de $\mathbb{C}^2$. Une telle droite est en particulier stable par les symétries orthogonales s_{OA} et s_{OB} par rapport aux droites (OA) et (OB) ce qui est impossible ; en effet les droites stables par s_{OA} sont les axes de coordonnées qui ne sont pas stables par s_{OB}.

Exemple 11.1.23. — Soit (V,ρ) une représentation de $\mathbb{Z}$. Soit $u = \rho(1)$. Comme $\mathbb{C}$ est algébriquement clos u admet une valeur propre λ non nulle car u est inversible. Soit $e_\lambda \in V$ un vecteur propre pour la valeur propre λ. Nous avons $n\cdot e_\lambda = u^n(e_\lambda) = \lambda^n e_\lambda$ pour tout $n\in\mathbb{Z}$; la droite $\mathbb{C}e_\lambda$ est donc stable sous l'action de $\mathbb{Z}$ et est une sous-représentation de $\mathbb{Z}$ isomorphe à la représentation $C(\lambda)$ de l'Exemple 11.1.6. En particulier si $\dim V \geq 2$ alors V n'est pas irréductible et toute représentation irréductible de $\mathbb{Z}$ est de dimension 1, isomorphe à $C(\lambda)$ pour un $\lambda\in\mathbb{C}^*$ uniquement déterminé.

Supposons désormais que u soit diagonalisable. Soit $(e_1,\ldots,e_d)$ une base de V constituée de vecteurs propres de u. Soit λ_i la valeur propre associée à e_i. Alors V est la somme directe $\bigoplus_{i=1}^{d}\mathbb{C}e_i$ des droites $\mathbb{C}e_i$ qui sont des sous-représentations de V, chaque $\mathbb{C}e_i$ étant isomorphe à $C(\lambda_i)$ en tant que représentation de $\mathbb{Z}$. Nous en déduisons que V est, en tant que représentation de $\mathbb{Z}$, isomorphe à $\bigoplus_{i=1}^{d} C(\lambda_i)$.

Remarques 11.1.3. —

(i) Dire que V est isomorphe à $\bigoplus_{i=1}^{d} C(\lambda_i)$ signifie juste que $u=\rho(1)$ est diagonalisable et que son polynôme caractéristique est $\prod_{i=1}^{d}(X-\lambda_i)$ ce qui est nettement moins précis que d'exhiber une base de vecteurs propres et donc un isomorphisme de $\bigoplus_{i=1}^{d} C(\lambda_i)$ sur V entre représentations de $\mathbb{Z}$.

(ii) Si u est diagonalisable, si les valeurs propres de u sont $\lambda_1,\lambda_2,\ldots,\lambda_r$ avec $\lambda_i\neq\lambda_j$ si $i\neq j$ et si la multiplicité de λ_i est m_i, alors $V\simeq\bigoplus_{i=1}^{r} m_i C(\lambda_i)$.

(iii) Si u n'est pas diagonalisable, la représentation V ne se décompose pas comme une somme directe de représentations irréductibles.

Exemple 11.1.24. — La représentation de permutation de $\mathfrak{S}_n$ sur $\Bbbk^n$ n'est pas irréductible puisque la droite engendrée par $(1, 1, \ldots, 1)$ est stable sous $\mathfrak{S}_n$ (*voir* Exemple 11.1.14).

Plus généralement une représentation de permutation de dimension finie $\neq 1$ n'est jamais irréductible.

Exemple 11.1.25. — Si G est un p-groupe fini et si $\Bbbk$ est de caractéristique p, alors toute représentation admet des vecteurs fixes non nuls. En effet soit $v \in V$ non nul, considérons le $\mathbb{F}_p$-espace vectoriel W engendré par les vecteurs $g \cdot v$, $g \in \mathrm{G}$. C'est une $\mathbb{F}_p$-représentation de G de dimension finie. Son nombre d'éléments est p^n pour un certain n. Il y a au moins un vecteur fixe, le vecteur nul, et la formule des classes pour l'action de G sur W assure que le nombre de vecteurs fixes est divisible par p.

Puisque toute représentation de G admet des vecteurs fixes non nuls, la seule représentation irréductible est, à isomorphisme près, la représentation triviale.

Exemple 11.1.26. — Combinons les Exemples 11.1.17 et 11.1.25. Considérons le groupe $\mathrm{G} = \mathbb{Z}/p\mathbb{Z}$. Suppsons que $\Bbbk$ soit algébriquement clos. Alors les représentations irréductibles de G sont toutes de dimension 1 et de la forme

$$\rho_\zeta \colon \mathrm{G} \to \mathrm{GL}(1, \Bbbk) = \Bbbk^\times \qquad\qquad n \mapsto \zeta^n$$

pour ζ une racine p-ième de l'unité.

Si la caractéristique de $\Bbbk$ est différente de p, alors il y a p représentations irréductibles non-isomorphes deux à deux (p racines p-ième de l'unité).

Si la caractéristique de $\Bbbk$ vaut p, alors il y a une seule représentation irréductible, la représentation triviale ; en effet la seule racine p-ième de l'unité est 1.

Remarque 11.1.4. — Si la restriction d'une représentation ρ de G à un sous-groupe de G est irréductible, il est immédiat que ρ elle-même est irréductible.

11.1.3. Supplémentaire G-invariant. — Si W est une sous-représentation de V, il n'existe pas en général de supplémentaire G-invariant de W dans V.

Exemple 11.1.27. — Soit $\mathrm{G} \subset \mathrm{GL}(2, \Bbbk)$ le groupe des matrices triangulaires supérieures. Il se représente dans $V = \Bbbk^2$ par la représentation standard. La droite $W = \Bbbk e_1$ est une sous-représentation dépourvue de supplémentaire G-invariant.

Si $\Bbbk$ est le corps $\mathbb{F}_p$, nous obtenons donc un exemple avec un groupe G fini de cardinal $p(p-1)^2$.

Il y a néanmoins un résultat général d'existence de supplémentaire G-invariant pour certains groupes finis :

Théorème 11.1.1

Soit G un groupe fini tel que la caractéristique de $\Bbbk$ ne divise pas $|\mathrm{G}|$. Soit V une représentation de G.
Tout sous-espace G-invariant de V admet un supplémentaire G-invariant.

Corollaire 11.1.1

Soit G un groupe fini tel que la caractéristique de $\Bbbk$ ne divise pas $|\mathrm{G}|$. Toute représentation de G de dimension finie est somme directe de représentations irréductibles.

Démonstration du Théorème 11.1.1 dans le cas $\Bbbk = \mathbb{R}$ ou $\mathbb{C}$. — Supposons que $\Bbbk = \mathbb{R}$ ou que $\Bbbk = \mathbb{C}$ et que V soit de dimension finie. Considérons un produit scalaire ou un produit hermitien sur V ; notons-le $\langle\, ,\, \rangle_0$. Définissons le produit scalaire suivant

$$\langle v, w\rangle = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\langle g\cdot v, g\cdot w\rangle_0.$$

Ce nouvau produit scalaire est G-invariant, *i.e.* pour tout $g \in \mathrm{G}$ nous avons

$$\langle g\cdot v, g\cdot w\rangle = \langle v, w\rangle$$

si bien que ρ est à valeurs dans $\mathrm{O}(V)$ ou $\mathrm{U}(V)$. En particulier si W est un sous-espace G-invariant, $W^\perp$ est aussi G-invariant et fournit le supplémentaire recherché. □

Remarque 11.1.5. — L'ingrédient essentiel de la démonstration consiste à fabriquer un produit scalaire G-invariant par moyennisation d'un produit scalaire donné quelconque. Si G est un groupe topologique compact, il est muni d'une mesure de probabilité G-invariante, la mesure de Haar ; en remplaçant

$$\langle v,\, w\rangle = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\langle g\cdot v,\, g\cdot w\rangle_0$$

par l'intégration sur le groupe la démonstration s'étend à ce cas.

Démonstration du Théorème 11.1.1. — Nous appliquons encore un procédé de moyennisation. Considérons un projecteur quelconque $p_0\colon V \to V$ d'image un sous-espace G-invariant W. Posons

$$p := \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\rho(g)\circ p_0\circ\rho(g)^{-1} \in \mathrm{End}(V).$$

Étant donné que $\rho(g)$ préserve W l'image de cet endomorphisme est contenue dans W. Si v appartient à W, alors $\rho(g)^{-1}(v)$ appartient à W donc $p_0\circ\rho(g)^{-1}(v) = \rho(g)^{-1}(v)$ et $p(v) = v$. Ainsi p est un projecteur d'image W.

Montrons que son noyau est invariant par G : pour tout $h \in \mathrm{G}$ nous avons

$$\rho(h)\circ p\circ\rho(h)^{-1} = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\rho(h)\circ\rho(g)\circ p_0\circ\rho(g)^{-1}\circ\rho(h)^{-1} = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\rho(hg)\circ p_0\circ\rho(hg)^{-1} = p$$

i.e. $\rho(h) \circ p = p \circ \rho(h)$. Autrement dit p est un endomorphisme de la représentation ρ. Par conséquent son noyau (supplémentaire de W) est bien invariant par G. □

Lemme 11.1.1: (Lemme de Schur)

Soit G un groupe. Soient (V, ρ_V) et (W, ρ_W) des représentations irréductibles de G. Soit $u\colon V \to W$ un morphisme de représentations.

1. Ou bien u est nul, ou bien u est un isomorphisme.
2. Si $V = W$ est de dimension finie et si $\Bbbk$ est algébriquement clos, alors l'application u est une homothétie.

Démonstration. — 1. Les sous-espaces $\ker u$ et $\operatorname{im} u$ sont G-invariants donc triviaux.

2. Si λ est une valeur propre de u, alors $\ker(u - \lambda \mathrm{id})$ est G-invariant et non nul donc égal à V. Autrement dit u est une homothétie.

□

Supposons que G soit un groupe fini tel que la caractéristique de $\Bbbk$ ne divise pas $|\mathrm{G}|$. Rappelons que si G est un groupe fini nous pouvons composer le morphisme de groupes de Cayley

$$\mathrm{G} \hookrightarrow \mathrm{Bij}(\mathrm{G}), \qquad g \mapsto (x \mapsto gx)$$

avec la représentation de permutation pour obtenir la représentation régulière (Exemple 11.1.4)

$$\rho_R\colon \mathrm{G} \to \mathrm{Bij}(\mathrm{G}) \to \mathrm{GL}(\Bbbk^{\mathrm{G}})$$

où $\Bbbk^{\mathrm{G}}$ désigne l'espace vectoriel des fonctions de G dans $\Bbbk$. Si $\delta_h\colon \mathrm{G} \to \Bbbk$ est la fonction caractéristique d'un élément h de G la famille $(\delta_h)_{h\in\mathrm{G}}$ forme une base de $\Bbbk^{\mathrm{G}}$. Nous avons

$$\rho_R(g)(\delta_h) = \delta_{gh}$$

et pour tout $f \in \Bbbk^{\mathrm{G}}$

$$\rho_R(g)(f)\colon g' \mapsto f(g^{-1}g') \qquad \forall\, g' \in \mathrm{G}.$$

Le Corollaire 11.1.1 assure que la représentation régulière $\Bbbk^{\mathrm{G}}$ se décompose en somme

$$\Bbbk^{\mathrm{G}} = \bigoplus R_i$$

de représentations irréductibles. Soit (V, ρ) une représentation de G et soit $v_0 \in V$. L'application linéaire

$$u\colon \Bbbk^{\mathrm{G}} \to V \qquad \Big(f\colon \mathrm{G} \to \Bbbk\Big) \mapsto \sum_{g\in\mathrm{G}} f(g)\rho(g)(v_0)$$

est un morphisme de représentations. En effet d'une part pour tout $g \in \mathrm{G}$ nous avons

$$u(\delta_g) = \rho(g)(v_0)$$

d'autre part pour tous h et g dans G nous avons

$$u \circ \rho_R(h)(\delta_g) = u(\delta_{hg}) = \rho(hg)(v_0) = \rho(h) \circ \rho(g)(v_0) = \rho(h) \circ u(\delta_g)$$

et donc

$$u \circ \rho_R(h) = \rho(h) \circ u.$$

Si v_0 est non nul, l'application u n'est pas nulle ($u(\delta_e) = v_0$). Si de plus V est irréductible alors u est surjective et la restriction $u_{|R_i}$ n'est pas nulle pour un certain i. Le Lemme de Schur assure que $u_{|R_i}$ est un isomorphisme et donc que V est isomorphe à la représentation R_i.

Nous pouvons donc énoncer le résultat suivant :

Proposition 11.1.1

Soit G un groupe fini tel que la caractéristique de $\Bbbk$ ne divise pas $|\mathrm{G}|$. Il n'y a à isomorphisme près qu'un nombre fini de représentations irréductibles de G et chacune est de dimension $\leq |\mathrm{G}|$.

Remarque 11.1.6. — Il y a des énoncés plus précis lorsque $\Bbbk$ est algébriquement clos.

Proposition 11.1.2

Soit G un groupe fini tel que la caractéristique de $\Bbbk$ ne divise pas $|\mathrm{G}|$. Soient ρ_1, ρ_2, ..., ρ_ℓ les représentations irréductibles de G.
Toute représentation de G de dimension finie se décompose en $\oplus \rho_i^{n_i}$ où les entiers naturels n_i sont uniquement déterminés par la représentation.

Démonstration. — L'existence d'une telle décomposition est assurée par le Corollaire 11.1.1.

Montrons l'unicité des n_i. La démonstration se fait par récurrence sur la dimension de la représentation. Supposons que $V = \oplus V_i$ soit isomorphe à $W = \oplus W_j$ où les V_i et les W_j sont des représentations irréductibles (éventuellement répétées). Montrons qu'à permutation près (V_i) et (W_i) sont la même collection de représentations. Considérons l'isomorphisme de représentations

$$u\colon \bigoplus_i V_i \xrightarrow{\sim} \bigoplus_j W_j$$

dont nous noterons l'inverse u'. Soient $p_i\colon V \to V_i$ et $q_j\colon W \to W_j$ les projections. Considérons les morphismes de représentations

$$u_j\colon V_1 \xrightarrow{u_{|V_1}} W \xrightarrow{q_j} W_j \xrightarrow{u'_{|W_j}} V \xrightarrow{p_1} V_1.$$

Nous avons

$$\sum_j u_j = \sum_j p_1 \circ u'_{|W_j} \circ q_j \circ u_{|V_1} = p_1 \circ \Big(\sum_j u'_{|W_j} \circ q_j\Big) \circ u_{|V_1} = p_1 \circ u' \circ u_{|V_1} = \mathrm{id}_{V_1}.$$

Un des u_j au moins est non nul. Quitte à renuméroter les W_j nous pouvons supposer qu'il s'agit de u_1. Les morphismes de représentations $q_1 \circ u_{|V_1}\colon V_1 \to W_1$ et $p_1 \circ u'_{|W_1}\colon W_1 \to V_1$ sont alors non nuls. Le Lemme de Schur assure que ce sont des isomorphismes.

Pour appliquer l'hypothèse de récurrence il suffit de montrer que le morphisme de représentations

$$(\mathrm{id}_W - q_1)u_{|\bigoplus_{i\geq 2} V_i} : \bigoplus_{i\geq 2} V_i \to \bigoplus_{j\geq 2} W_j$$

entre représentations de même dimension est encore un isomorphisme. C'est le cas : si $x \in \bigoplus_{i\geq 2} V_i$ est dans le noyau, alors $u(x)$ appartient à W_1 et $p_1(u'(u(x))) = p_1(x) = 0$; puisque $p_1 \circ u'_{|W_1}$ est un isomorphisme nous avons $u(x) = 0$ et $x = 0$. Ce morphisme est donc injectif. Étant donné que $\dim \bigoplus_{i\geq 2} V_i = \dim \bigoplus_{j\geq 2} W_j$ c'est un isomorphisme. □

Remarque 11.1.7. — Sous les hypothèses de la Proposition 11.1.2 nous pouvons donc décomposer une représentation (V, ρ) de dimension finie du groupe G en somme directe $V = \bigoplus_i V_i$ de représentations irréductibles. Cette décomposition n'est en général pas unique ! Par exemple si tous les $\rho(g)$ sont l'identité, la seule représentation irréductible qui intervient est la représentation triviale, de dimension 1, il s'agit simplement de décomposer V en somme directe de droites ce qui peut être fait de bien des façons.

11.2. Caractères

Dans ce paragraphe nous supposons que G est fini, que $\Bbbk$ est algébriquement clos et que la caractéristique de $\Bbbk$ ne divise pas $|\mathrm{G}|$.

Si (V, ρ) est une représentation de dimension finie de G, on appelle *caractère* de ρ la fonction

$$\chi_\rho \colon \mathrm{G} \to \Bbbk, \qquad g \mapsto \mathrm{tr}(\rho(g)).$$

Lorsque (V, ρ) est irréductible nous parlons de *caractère irréductible*. Remarquons que $\chi_\rho(e) = \mathrm{tr}(\rho(e)) = \mathrm{tr}(\mathrm{id}_{\mathrm{GL}(V)}) = \dim V$; le caractère détermine donc la dimension de la représentation. En particulier la valeur de χ_ρ en l'élément neutre est donc un entier ; cet entier est aussi appelé le *degré* du caractère χ_ρ.

Pour tous g, h dans G nous avons

$$\chi_\rho(hgh^{-1}) = \mathrm{tr}(\rho(h)\rho(g)\rho(h)^{-1}) = \mathrm{tr}(\rho(g)) = \chi_\rho(g).$$

On dit que χ_ρ est une *fonction centrale*, ou encore *invariante par conjugaison*.

Plus généralement une fonction $f \colon \mathrm{G} \to \Bbbk$ est centrale si et seulement si elle est constante sur chaque classe de conjugaison C de G. Nous notons alors $f(C)$ sa valeur sur la classe C. Le $\Bbbk$-espace vectoriel de toutes les fonctions centrales sur le groupe G est noté $\mathscr{C}(\mathrm{G})$. La dimension de $\mathscr{C}(\mathrm{G})$ est égale au nombre de classes de conjugaison de G.

Exemple 11.2.1. — Considérons la représentation de permutation. Reprenons les notations de l'Exemple 11.1.4. Dans la base $(e_x)_{x\in E}$ la matrice de g est une matrice de permutation et

l'élément diagonal est égal à 1 si et seulement si $g \cdot x = x$, sinon il vaut 0. Nous en déduisons que la trace de la matrice de g est le nombre de points fixes de g agissant sur E ; autrement dit

$$\chi_\rho(g) = \big|\{x \in E \,|\, g \cdot x = x\}\big|.$$

Exemple 11.2.2. — Considérons la représentation régulière. Reprenons les notations de l'Exemple 11.1.4. Puisque $gh = h$ implique $g = e$ nous obtenons que le caractère de la représentation régulière est donné par

$$\chi_R(g) = \begin{cases} |\mathrm{G}| \text{ si } g = e \\ 0 \text{ si } g \neq e \end{cases}$$

Le caractère de la représentation régulière est donc $|\mathrm{G}|$ fois la fonction caractéristique δ_{C_e} de la classe de conjugaison $C_e = \{e\}$.

Exemple 11.2.3. — La représentation standard de D_{2n} dans $\mathbb{C}^2$ est donnée par

$$\rho\colon \mathrm{D}_{2n} \to \mathrm{GL}(2, \mathbb{C}) \qquad r \mapsto \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \qquad s \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Le caractère de la représentation standard de D_{2n} dans $\mathbb{C}^2$ est donné par

$$\chi(r^k) = 2\cos\left(\frac{2k\pi}{n}\right), \qquad \chi(r^k s) = 0.$$

Il vaut donc 0 sur $\{s, rs, \ldots, r^{n-1}s\}$ (qui est la réunion de une ou deux classes de conjugaison selon que n est impair ou non) et $2\cos\left(\frac{2k\pi}{n}\right)$ sur chaque classe de conjugaison $\{r^k, r^{-k}\}$.

Exemple 11.2.4. — Le groupe $\mathfrak{S}_3$ possède trois classes de conjugaison, celle de l'élément neutre, celle à trois éléments d'une transposition τ et celle à deux éléments d'un 3-cycle σ. Le caractère de la représentation standard (représentation de permutation) de $\mathfrak{S}_3$ dans $\mathbb{C}^3$ vaut

$$\begin{cases} 3 \text{ sur } e \\ 1 \text{ sur les transpositions} \\ 0 \text{ sur les 3-cycles} \end{cases}$$

Plus généralement les classes de conjugaison de $\mathfrak{S}_n$ sont en bijection avec les partitions de n (Proposition **??**)

$$n = k_1 + k_2 + \ldots + k_r, \quad r \in \mathbb{N}, \quad 1 \leq k_1 \leq k_2 \leq \ldots \leq k_r$$

une telle partition correspondant aux produits de cycles à supports disjoints d'ordre $k_1, k_2, \ldots, k_r$. Sur la classe de conjugaison correspondante le caractère de la représentation standard de $\mathfrak{S}_n$ dans $\mathbb{C}^n$ vaut $\max\{i \,|\, k_i = 1\}$ (c'est le nombre de points fixes de la permutation).

***Exemple 11.2.5* (Caractère d'une représentation de dimension 1)**

Se donner une classe d'isomorphie de représentation $\Bbbk$-linéaire de dimension 1 de G revient à se donner un morphisme de G vers $\Bbbk$ [2]. Si ρ est un tel morphisme, la classe d'isomorphisme correspondante est celle de $(\Bbbk,\, g \mapsto \rho(g)\mathrm{id}_{\Bbbk})$; le caractère associé est $g \mapsto \mathrm{tr}(\rho(g)\mathrm{id}_{\Bbbk}) = \rho(g)$: en dimension 1 le caractère d'une représentation coïncide avec le morphisme $\mathrm{G} \to \Bbbk^{\times}$ qui la définit à isomorphisme près.

***Exemple 11.2.6* (Caractères d'un groupe abélien).** — Soit G un groupe abélien fini. Supposons que $\Bbbk = \mathbb{C}$. Les représentations irréductibles de G sont exactement les représentations de G de dimension 1 (Exemple 11.1.17). Se donner une classe d'isomorphie d'une telle représentation revient à se donner un morphisme de G vers $\mathbb{C}^{\times}$, qui coïncide alors avec le caractère irréductible correspondant (Exemple 11.2.5). L'ensemble des caractères irréductibles de G est donc égal à $\mathrm{Hom}(\mathrm{G}, \mathbb{C}^{\times})$.

Puisque G est abélien les classes de conjugaison de G sont les singletons $\{g\}$ avec $g \in \mathrm{G}$. Par suite l'ensemble des caractères irréductibles de G a pour cardinal $|\mathrm{G}|$. Il en résulte que $|\mathrm{Hom}(\mathrm{G}, \mathbb{C}^{\times})| = |\mathrm{G}|$.

Notons qu'on peut démontrer cette égalité sans faire appel à la théorie des représentations tout en étant beaucoup plus précis :

Lemme 11.2.1

Le groupe $\mathrm{Hom}(\mathrm{G}, \mathbb{C}^{\times})$ est isomorphe à G.
En particulier son ordre est égal à $|\mathrm{G}|$.

Démonstration. — Notons G additivement. Le Théorème **??** assure l'existence d'une famille finie $(d_1, d_2, \ldots, d_n)$ d'entiers > 1 telle que $d_1 | d_2 | \ldots | d_r$ et d'un isomorphisme

$$\mathrm{G} \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}.$$

2. Soit G un groupe. Soit V un $\Bbbk$-espace vectoriel de dimension 1. Se donner une représentation de G d'espace sous-jacent V revient à se donner un morphisme $\rho\colon \mathrm{G} \to \mathrm{GL}(V) \simeq \Bbbk^{\times}$. Soient ρ et ρ' deux morphismes de G dans $\Bbbk^{\times}$. Soient V et V' deux $\Bbbk$-espaces vectoriels de dimension 1. On voit V (respectivement V') comme une représentation de G via ρ (respectivement ρ'). Soit u un isomorphisme $\Bbbk$-linéaire entre V et V'. L'application u est équivariante si et seulement si $u \circ \rho(g)\mathrm{id}_V \circ u^{-1} = \rho'(g)\mathrm{id}_{V'}$ pour tout $g \in \mathrm{G}$ soit encore si et seulement si $\rho(g)\mathrm{id}_{V'} = \rho'(g)\mathrm{id}_{V'}$ pour tout $g \in \mathrm{G}$, c'est-à-dire enfin si et seulement si $\rho = \rho'$. Notons que cette dernière condition ne fait plus intervenir u : si elle est satisfaite tout isomorphisme $\Bbbk$-linéaire entre V et V' est donc un isomorphisme de représentations.

L'ensemble des classes d'isomorphie de représentations $\Bbbk$-linéaires de dimension 1 de G est donc en bijection naturelle avec l'ensemble des morphismes $\rho\colon \mathrm{G} \to \Bbbk^{\times}$. La classe associée à un tel morphisme est celle de la représentation $(D, g \mapsto \rho(g)\mathrm{id}_{\Bbbk})$ pour n'importe quelle $\Bbbk$-droite vectorielle D.

Pour toute famille de morphismes $\left(h_i\colon \mathbb{Z}/d_i\mathbb{Z} \to \mathbb{C}^\times\right)_{1\leq i\leq r}$ il existe un et un seul morphisme $h\colon \mathrm{G} \to \mathbb{C}^\times$ tel que $h_{\big|\mathbb{Z}/d_i\mathbb{Z}} = h_i$ pour tout i, à savoir

$$h\colon (x_1, x_2, \ldots, x_r) \mapsto \prod_i h_i(x_i).$$

On peut vérifier que $(h_1, h_2, \ldots, h_r) \mapsto h$ établit un isomorphisme entre

$$\mathrm{Hom}\left(\mathbb{Z}/d_1\mathbb{Z}, \mathbb{C}\right) \times \mathrm{Hom}\left(\mathbb{Z}/d_2\mathbb{Z}, \mathbb{C}\right) \times \ldots \times \mathrm{Hom}\left(\mathbb{Z}/d_r\mathbb{Z}, \mathbb{C}\right)$$

et $\mathrm{Hom}(\mathrm{G}, \mathbb{C}^\times)$.

Il suffit donc pour conclure de montrer que $\mathrm{Hom}\left(\mathbb{Z}/d\mathbb{Z}, \mathbb{C}^\times\right)$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$ pour tout $d \geq 1$. Soit $d \geq 1$. Le groupe $\mathrm{Hom}\left(\mathbb{Z}/d\mathbb{Z}, \mathbb{C}^\times\right)$ s'identifie au groupe des éléments de d-torsion de $\mathbb{C}^\times$, *i.e.* au groupe des racines d-ièmes de l'unité de $\mathbb{C}^\times$. Or le groupe des racines d-ièmes de l'unité est cyclique et de cardinal d (il est engendré par $\exp\left(\frac{2\mathbf{i}\pi}{d}\right)$) d'où le résultat. □

Proposition 11.2.1

1. Des représentations de dimension finie isomorphes ont même caractère.
2. Nous avons $\chi_{V\oplus W} = \chi_V + \chi_W$.
3. Si $W \subset V$ est une sous-représentation de V, alors $\chi_V = \chi_W + \chi_{V/W}$.
4. Reprenons les notations de l'Exemple 11.1.9. Si G est fini et g appartient à G, alors
$$\chi_{\mathrm{Hom}(V_1,V_2)}(g) = \overline{\chi_{V_1}(g)}\chi_{V_2}(g).$$
5. Reprenons les notations de l'Exemple 11.1.10, alors $\chi_{V^*} = \overline{\chi_V}$.

Démonstration. — Démontrons 4. Si g est fixé nous pouvons choisir une base $(e_i)_{i\in I}$ de V_1 et une base $(f_j)_{j\in J}$ de V_2 dans lesquelles les actions de g sont diagonales. Il existe donc des racines de l'unité α_i pour $i \in I$ et β_j pour $j \in J$ tels que $g \cdot e_i = \alpha_i e_i$ si $i \in I$ et $g \cdot f_j = \beta_j f_j$ si $j \in J$. Nous avons alors

$$\chi_{V_1}(g) = \sum_{i\in I} \alpha_i \qquad\qquad \chi_{V_2}(g) = \sum_{j\in J} \beta_j$$

Si $(i,j) \in I \times J$, soit $u_{i,j}\colon V_1 \to V_2$ l'application linéaire définie par $u_{i,j}(e_i) = f_j$ et $u_{i,j}(e_{i'}) = 0$ si $i \neq i'$. Les $u_{i,j}$, pour $(i,j) \in I \times J$ forment une base de $\mathrm{Hom}(V_1, V_2)$ et nous avons

$$g \cdot u_{i,j} = \alpha_i^{-1}\beta_j u_{i,j} = \overline{\alpha_i}\beta_j u_{i,j}$$

Par conséquent

$$\chi_{\mathrm{Hom}(V_1,V_2)}(g) = \sum_{(i,j)\in I\times J} \overline{\alpha_i}\beta_j = \Big(\sum_{i\in I}\overline{\alpha_i}\Big)\Big(\sum_{j\in J}\beta_j\Big) = \overline{\chi_{V_1}(g)}\chi_{V_2}(g).$$

Nous en déduisons 5. En effet si $V_1 = V$ et V_2 est la représentation triviale, la représentation $\mathrm{Hom}(V_1, V_2) = \mathrm{Hom}(V, \mathbb{C})$ est la représentation duale V^* de V. Nous avons d'après ce qui précède $\chi_{V^*} = \overline{\chi_V}$. □

Introduisons sur le $\Bbbk$-espace vectoriel $\Bbbk^{\mathrm{G}} = \{f \colon \mathrm{G} \to \Bbbk\}$ la forme bilinéaire symétrique

$$\langle f,\, f' \rangle = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g^{-1}) f'(g).$$

Notons que $\langle f,\, \delta_g \rangle = \frac{1}{|\mathrm{G}|} f(g^{-1})$ donc cette forme est non dégénérée.

Théorème 11.2.1

Soit G un groupe fini. Les caractères des représentations irréductibles de dimension finie forment une base orthonormale du $\Bbbk$-espace vectoriel $\mathscr{C}(\mathrm{G})$ des fonctions centrales sur G.

Démonstration. — La démonstration du théorème va utiliser les deux Lemmes suivants. Soient (V, ρ_V) et (W, ρ_W) des représentations de G. Soit u dans $\mathrm{Hom}(V, W)$. Posons

$$\pi(u) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \rho_W(g) \circ u \circ \rho_V(g^{-1}) \in \mathrm{Hom}(V, W).$$

Lemme 11.2.2

L'endomorphisme π de $\mathrm{Hom}(V, W)$ ainsi défini est un projecteur d'image $\mathrm{Hom}_{\mathrm{G}}(V, W)$ et

$$\mathrm{tr}(\pi) = \langle \chi_V, \chi_W \rangle.$$

Démonstration. — Rappelons que

$$\mathrm{Hom}_{\mathrm{G}}(V, W) = \{u \in \mathrm{Hom}(V, W) \,|\, \forall\, h \in \mathrm{G} \quad u \circ \rho_V(h) = \rho_W(h) \circ u\}.$$

Si u appartient à $\mathrm{Hom}_{\mathrm{G}}(V, W)$, nous avons

$$\begin{aligned}
\rho_W(h) \circ \pi(u) \circ \rho_V(h)^{-1} &= \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \rho_W(h) \circ \rho_W(g) \circ u \circ \rho_V(g)^{-1} \circ \rho_V(h)^{-1} \\
&= \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \rho_W(hg) \circ u \circ \rho_V(g^{-1} h^{-1}) \\
&= \frac{1}{|\mathrm{G}|} \sum_{g' \in \mathrm{G}} \rho_W(g') \circ u \circ \rho_V(g'^{-1}) \\
&= \pi(u)
\end{aligned}$$

De plus si u appartient à $\mathrm{Hom}_{\mathrm{G}}(V, W)$ nous avons $\pi(u) = u$ de sorte que π est bien un projecteur d'image $\mathrm{Hom}_{\mathrm{G}}(V, W)$.

Calculons $\mathrm{tr}(\pi)$ dans une base de $\mathrm{Hom}(V,W)$. Choisissons des bases de V et W et notons e_{ij} l'élément de $\mathrm{Hom}(V,W)$ dont la matrice dans ces bases a tous ses coefficients nuls sauf celui situé à la $i$ème ligne et la $j$ème colonne qui vaut 1. Les e_{ij} forment une base de $\mathrm{Hom}(V,W)$ et

$$\Big(\rho_W(g)\circ e_{ij}\circ\rho_V(g)^{-1}\Big)_{k\ell}=\rho_W(g)_{ki}\rho_V(g^{-1})_{j\ell}$$

En appliquant ceci au cas particulier $i=k$ et $j=\ell$ nous obtenons

$$\begin{aligned}\mathrm{tr}(\pi) &= \sum_{i,j}\pi(e_{ij})_{ij}\\ &= \sum_{i,j}\frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\rho_W(g)_{ii}\rho_V(g^{-1})_{jj}\\ &= \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\Big(\sum_i\rho_W(g)_{ii}\Big)\Big(\sum_j\rho_V(g^{-1})_{jj}\Big)\\ &= \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}\chi_W(g)\chi_V(g^{-1}).\end{aligned}$$

□

Soient (V,ρ_V) et (W,ρ_W) des représentations irréductibles de G, le lemme de Schur assure que

$$\mathrm{Hom}_{\mathrm{G}}(V,W)=\begin{cases}0 \text{ si } V \text{ et } W \text{ ne sont pas isomorphes}\\ \Bbbk \text{ si } V \text{ et } W \text{ sont isomorphes}\end{cases}$$

Puisque le rang d'un projecteur est sa trace le Lemme 11.2.2 assure que

$$\langle\chi_V,\chi_W\rangle=\mathrm{tr}(\pi)=\begin{cases}0 \text{ si } V \text{ et } W \text{ ne sont pas isomorphes}\\ 1 \text{ si } V \text{ et } W \text{ sont isomorphes}\end{cases}$$

Ainsi la famille (χ_V) pour V irréductible (ou plus exactement pour V décrivant l'ensemble des classes d'isomorphisme de représentations irréductibles de G) est orthonormale. Il reste à voir que la famille (χ_V) engendre $\mathscr{C}(\mathrm{G})$.

Lemme 11.2.3

Soit (V,ρ) une représentation de G. Si $f\colon \mathrm{G}\to\Bbbk$ est une fonction centrale, nous posons

$$f_\rho=\frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}}f(g)\rho(g^{-1})\in\mathrm{End}(V).$$

Alors

1. f_ρ appartient à $\mathrm{End}_{\mathrm{G}}(V)$ et $\mathrm{tr}(f_\rho)=\langle f,\,\chi_\rho\rangle$;
2. si (V,ρ) est irréductible, alors $\dim V$ est inversible dans $\Bbbk$ et f_ρ est l'homothétie de V de rapport $\frac{\langle f,\chi_\rho\rangle}{\dim V}$.

Démonstration. — 1. Puisque f est centrale nous avons pour tout $h \in \mathrm{G}$

$$\begin{aligned}
\rho(h) \circ f_\rho \circ \rho(h)^{-1} &= \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\rho(hg^{-1}h^{-1}) \\
&= \frac{1}{|\mathrm{G}|} \sum_{g' \in \mathrm{G}} f(h^{-1}g'h)\rho(g'^{-1}) \\
&= \frac{1}{|\mathrm{G}|} \sum_{g' \in \mathrm{G}} f(g')\rho(g'^{-1}) \\
&= f_\rho.
\end{aligned}$$

Ainsi f_ρ appartient à $\mathrm{End}_{\mathrm{G}}(V)$ et sa trace est

$$\mathrm{tr}(f_\rho) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\chi_\rho(g^{-1}) = \langle f,\, \chi_\rho \rangle.$$

2. Supposons que ρ soit irréductible. Le Lemme de Schur (Lemme 11.1.1) et la première assertion appliqués à la fonction centrale $f = \chi_\rho$ assure que χ_ρ est une homothétie. Si λ est son rapport, nous avons

$$\mathrm{tr}(\chi_\rho) = \dim V \cdot \lambda = \langle \chi_\rho,\, \chi_\rho \rangle = 1.$$

En particulier $\dim V$ est inversible dans $\Bbbk$.

Soit f une fonction centrale quelconque. Le Lemme de Schur (Lemme 11.1.1) assure que f_ρ est une homothétie. Sa trace étant $\langle f,\, \chi_\rho \rangle$ son rapport est $\frac{\langle f,\, \chi_\rho \rangle}{\dim V}$.

□

Si une fonction centrale $f \in \mathscr{C}(\mathrm{G})$ est orthogonale à tous les caractères χ_ρ le Lemme précédent assure que $f_\rho = 0$ pour toute représentation ρ irréductible et donc pour toute représentation puisque $f_{\rho \oplus \rho'} = f_\rho \oplus f_{\rho'}$. Appliquons cela à la représentation régulière ; nous obtenons $f_{\rho_R} = 0$ d'où

$$0 = f_{\rho_R}(\varepsilon_e) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\rho_R(g^{-1})(\varepsilon_e) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\varepsilon_{g^{-1}}$$

dans $\Bbbk^{\mathrm{G}}$ ce qui implique $f = 0$ puisque les $\varepsilon_{g^{-1}}$ forment une base de $\Bbbk^{\mathrm{G}}$. Tout élément f de $\mathscr{C}(\mathrm{G})$ s'écrit $\sum_{\rho \text{ irr}} \langle f,\, \chi_\rho \rangle \chi_\rho$. □

Corollaire 11.2.1

1. Le nombre de représentations irréductibles de G est égal au nombre de classes de conjugaison de G.
2. Soient $\chi_1, \chi_2, \ldots, \chi_\ell$ les caractères des représentations irréductibles de G. Soient C et C' des classes de conjugaison dans G. Nous avons
$$\sum_{i=1}^{\ell} \chi_i(C^{-1})\chi_i(C') = \begin{cases} \frac{|\mathrm{G}|}{|C|} \text{ si } C = C' \\ 0 \text{ sinon} \end{cases}$$
L'entier $|C|$ divise l'ordre de G puisque c'est le cardinal d'une orbite pour l'action de G sur lui-même par conjugaison.

Démonstration. — La dimension de $\mathscr{C}(\mathrm{G})$ est égale au nombre de classes de conjugaison dans G d'où la première assertion.

Soit δ_C la fonction caractéristique de C. Alors $f = \delta_C$ est une fonction centrale qui se décompose sur la base orthonormale des caractères χ_i des représentations irréductibles :
$$\delta_C = \sum_{i=1}^{\ell} \langle \delta_C, \chi_i \rangle \chi_i$$
avec
$$\langle \delta_C, \chi_i \rangle = \frac{1}{|\mathrm{G}|} |C| \chi_i(C^{-1}).$$
Il en résulte que
$$\delta_C = \frac{|C|}{|\mathrm{G}|} \sum_{i=1}^{\ell} \chi_i(C^{-1})\chi_i.$$
□

La décomposition $V = \bigoplus_i V_i$ d'une représentation en somme directe de représentations irréductibles n'est pas unique. Par contre si nous regroupons tous les V_i isomorphes à la même représentation irréductible nous obtenons une décomposition $V = \bigoplus_j W_j$ en *composantes isotypiques* indépendante des choix.

Exemple 11.2.7. — Considérons la représentation régulière d'un groupe fini G. Chaque représentation irréductible de G est « contenue » dans la représentation régulière un nombre de fois égal à son degré : G a un nombre fini de représentations irréductibles (V_i, ρ_i) et les composantes isotypiques de la représentation régulière sont équivalentes à :
$$\underbrace{(V_i, \rho_i) \oplus (V_i, \rho_i) \oplus \ldots \oplus (V_i, \rho_i)}_{\dim(V_i) \text{ termes}}.$$

Théorème 11.2.2

Soit (V, ρ) une représentation de dimension finie du groupe fini G. La projection de V sur la composante isotypique correspondant à une représentation irréductible (U, ψ) est donnée par

$$p_U = \frac{\dim U}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \chi_\psi(g)\rho(g^{-1})$$

En particulier la décomposition en composantes isotypiques ne dépend que de la représentation (V, ρ).

Démonstration. — Soit f une fonction centrale sur G. Par définition l'endomorphisme f_ρ de V laisse stable toute sous-représentation (V_i, ρ_i) de (V, ρ) et se restreint à V_i en f_{ρ_i}. Si de plus V_i est irréductible f_{ρ_i} est l'homothétie de V_i de rapport $\frac{\langle f, \chi_i \rangle}{\dim V_i}$ (Lemme 11.2.3).

Le Théorème 11.2.1 assure que si f est le caractère χ_ψ d'une représentation irréductible (U, ψ) alors

$$(\chi_\psi)_{\rho_{|V_i}} = \begin{cases} \frac{1}{\dim V_i}\mathrm{id}_{V_i} \text{ si } V_i \text{ est isomorphe à } U \\ 0 \text{ sinon} \end{cases}$$

Comme $p_U = (\dim U)(\chi_\psi)_\rho$ sa restriction à V_i est donc l'identité de V_i si V_i est isomorphe à U et 0 sinon. □

Montrons maintenant qu'en caractéristique 0 une représentation est déterminée par son caractère. Nous pouvons aussi identifier les représentations irréductibles comme celles dont le caractère est de norme 1.

Proposition 11.2.2

Notons ρ_1, ρ_2, …, ρ_ℓ les représentations irréductibles du groupe fini G. Soit ρ une représentation de G. Décomposons ρ sous la forme $\rho = \bigoplus_{i=1}^{\ell} \rho_i^{n_i}$. Alors

$$\langle \chi_\rho, \chi_{\rho_i} \rangle = n_i \qquad\qquad \langle \chi_\rho, \chi_\rho \rangle = \Big(\sum_{i=1}^{\ell} n_i^2 \Big).$$

Si de plus $\Bbbk$ est de caractéristique nulle, alors

- ◇ des représentations ρ' et ρ'' de G sont isomorphes si et seulement si $\chi_\rho = \chi_{\rho'}$;
- ◇ ρ est irréductible si et seulement si $\langle \chi_\rho, \chi_\rho \rangle = 1$;
- ◇ la représentation régulière se décompose en $\Bbbk^{\mathrm{G}} = \bigoplus_{i=1}^{\ell} \rho_i^{\deg \rho_i}$, en particulier

$$\sum_{i=1}^{\ell} \deg(\rho_i)^2 = |\mathrm{G}|.$$

Remarque 11.2.1. — Si la caractéristique de $\Bbbk$ est p il est faux que le caractère détermine la représentation ; en effet pour toute représentation V le caractère de V^p est nul.

Remarque 11.2.2. — Nous verrons ultérieurement une autre contrainte importante sur les dimensions des représentations irréductibles : elles divisent l'ordre du groupe.

Démonstration. — À partir de $\chi_\rho = \sum_{i=1}^{\ell} n_i \chi_{\rho_i}$ nous obtenons

$$\langle \chi_\rho, \chi_{\rho_i} \rangle = n_i \qquad\qquad \langle \chi_\rho, \chi_\rho \rangle = \Big(\sum_{i=1}^{\ell} n_i^2 \Big).$$

Ainsi en caractéristique nulle χ_ρ détermine les entiers n_i et donc toute la représentation ρ ; de plus ρ est irréductible si et seulement si $\langle \chi_\rho, \chi_\rho \rangle = 1$.

Considérons la représentation régulière ρ_R ; comme $\chi_{\rho_R} = |\mathrm{G}| \delta_{\{e\}}$ nous obtenons

$$\langle \chi_{\rho_R}, \chi_{\rho_i} \rangle = \chi_{\rho_i}(e) = \deg \rho_i.$$

Par conséquent la représentation régulière est isomorphe à $\bigoplus_{i=1}^{\ell} \rho_i^{\deg \rho_i}$. □

Nous avons vu dans l'Exemple 11.1.17 que si G est un groupe abélien et si $\Bbbk$ est algébriquement clos les seules représentations irréductibles de dimension finie de G sont de dimension 1. Plus précisément nous avons la :

Proposition 11.2.3

Supposons que $\Bbbk$ soit de caractéristique nulle. Le groupe G est abélien si et seulement si toutes ses représentations irréductibles sont de dimension 1.

Remarque 11.2.3. — Cet énoncé n'est plus vrai en général (il existe des p-groupes non abéliens [3]).

Démonstration. — Un groupe G est abélien si et seulement s'il a exactement $|\mathrm{G}|$ classes de conjugaison donc $|\mathrm{G}|$ représentations irréductibles. Or $|\mathrm{G}| = \sum_{i=1}^{\ell} \deg(\rho_i)^2$ donc $\ell \leq |\mathrm{G}|$ avec égalité si et seulement si toutes les représentations irréductibles sont de dimension 1. □

11.3. Table des caractères

Dans ce qui suit $\Bbbk = \mathbb{C}$. Pour toute représentation (V, ρ) d'un groupe fini G nous avons $\rho(g)^{|\mathrm{G}|} = \mathrm{id}_V$; ainsi les valeurs propres de $\rho(g)$ sont des racines de l'unité et celles de $\rho(g^{-1})$ sont leurs conjugués. Il s'ensuit que

$$\chi_\rho(g^{-1}) = \mathrm{tr}(\rho(g^{-1})) = \overline{\mathrm{tr}(\rho(g))} = \overline{\chi_\rho(g)}.$$

Par conséquent

$$\langle \chi_\rho, \chi_{\rho'} \rangle = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \overline{\chi_\rho(g)} \chi_{\rho'}(g). \tag{11.3.1}$$

De plus si $\chi_1, \chi_2, \ldots, \chi_\ell$ sont les caractères des représentations irréductibles de G, le Corollaire 11.2.1 assure que

$$\sum_{i=1}^{\ell} \overline{\chi_i(C)} \chi_i(C') = \begin{cases} \frac{|\mathrm{G}|}{|C|} \text{ si } C = C' \\ 0 \text{ sinon} \end{cases} \tag{11.3.2}$$

Comme $\chi_\rho(g)$ est la somme des valeurs propres de $\rho(g)$ nous avons aussi

$$\forall\, g \in \mathrm{G} \quad |\chi_\rho(g)| \leq \chi_\rho(e) = \dim(V).$$

De plus $\chi_\rho(g) = \chi_\rho(e)$ si et seulement si $\rho(g) = \mathrm{id}_V$. Par suite on définit

$$\ker \chi_\rho = \{g \in \mathrm{G} \,|\, \chi_\rho(g) = \chi_\rho(e)\} \lhd \mathrm{G}.$$

De même $|\chi_\rho(g)| = \chi_\rho(e)$ si et seulement si $\rho(g)$ est une homothétie.

La *table des caractères* de G donne la valeur de chaque caractère sur chaque classe de conjugaison. Les lignes correspondent aux caractères et les colonnes aux classes de conjugaison. C'est en quelque sorte la carte du groupe G. D'après le Corollaire 11.2.1 c'est une table carrée. Les différentes relations obtenues précédemment se traduisent comme suit :

3. par exemple $\mathbb{H}_8$, D_8

- ◇ les colonnes sont orthogonales pour le produit scalaire hermitien standard ;
- ◇ la colonne correspondant à la classe de conjugaison C est de norme hermitienne au carré $\frac{|\mathrm{G}|}{|C|}$ (*voir* (11.3.2)) ;
- ◇ les lignes sont orthogonales et de norme au carré $|\mathrm{G}|$ pour le produit scalaire hermitien pondéré par le cardinal des classes de conjugaison (11.3.1) ;
- ◇ la somme des lignes pondérées par les dimensions $\chi(e)$ est la ligne $|\mathrm{G}|\ 0\ 0 \ldots 0$.

Remarque 11.3.1. — Ces propriétés permettent de remplir la table des caractères en n'en connaissant qu'une partie.

Exemple 11.3.1. — Le groupe $\{\pm\mathrm{id}\}$ a deux classes de conjugaison id et $-\mathrm{id}$ et deux caractères irréductibles $\chi_{\rho_{\mathrm{triv}}}$ et χ (de dimension 1 puisque $\{\pm\mathrm{id}\}$ est abélien). Sa table de caractères est très facile a établir :

classes de conjugaison / caractères	id	$-\mathrm{id}$
$\chi_{\rho_{\mathrm{triv}}}$	1	1
χ	1	-1

Nous verrons plus loin des exemples pour lesquels la table est un peu plus difficile à établir.

***Remarque 11.3.2* (Sous-groupes distingués).** — Un sous-groupe distingué de G est réunion de classes de conjugaison (c'est essentiellement la définition de sous-groupe distingué). Pour chaque caractère χ_ρ, la réunion des classes de conjugaison sur lesquelles χ_ρ prend la valeur $\chi_\rho(e)$ est un sous-groupe distingué $\mathrm{G}_\chi \triangleleft \mathrm{G}$: c'est le noyau de la représentation correspondante d'après ce qu'on a vu précédemment.

> *Tout sous-groupe distingué* $\mathrm{K} \triangleleft \mathrm{G}$ *est intersection de noyaux de représentations irréductibles.*

En effet considérons $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{K}}$ la projection canonique et $\rho_R^{\mathrm{G}/\mathrm{K}}$ la représentation régulière du quotient. Cette dernière, comme toute représentation régulière, est fidèle donc $\mathrm{K} = \ker\left(\rho_R^{\mathrm{G}/\mathrm{K}} \circ \pi\right)$. On obtient ce noyau comme intersections de noyaux $\ker \chi_\rho$ en décomposant la représentation $\rho_R^{\mathrm{G}/\mathrm{K}} \circ \pi$ de G en somme de représentations irréductibles.

***Remarque 11.3.3* (Simplicité).** — En particulier le groupe G est simple si et seulement si tous les G_χ à part $\mathrm{G}_{\chi_{\mathrm{triv}}} = \mathrm{G}$ sont triviaux. Autrement dit le groupe G est simple si et seulement si dans chaque ligne exceptée celle correspondant à la représentation triviale (qui est la seule composée uniquement de 1) la valeur $\chi(e)$ n'apparaît qu'une seule fois (dans la colonne correspondant à la classe $\{e\}$).

***Remarque 11.3.4* (Représentations de dimension 1).** — Soit G un groupe fini. Le *groupe dual* $\widehat{\mathrm{G}}$ de G est le groupe des morphismes de G dans $\mathbb{C}^*$. Les éléments de $\widehat{\mathrm{G}}$ sont appelés *caractères linéaires* de G. Les caractères linéaires s'identifient aux représentations de degré 1 puisque $\mathrm{GL}(1,\mathbb{C}) \simeq \mathbb{C}^*$. Ainsi, en vertu de la Proposition 11.2.1, il y a autant de caractères linéaires que de classes d'isomorphie de représentations de degré 1 de G.

***Remarque 11.3.5* (Abélianisé, sous-groupes dérivés).** — Soit $\pi\colon \mathrm{G} \to \mathrm{G}^{\mathrm{ab}} = {}^{\mathrm{G}}\!/_{D(\mathrm{G})}$ la surjection canonique de G sur son abélianisé. L'application

$$\widehat{\mathrm{G}^{\mathrm{ab}}} \to \widehat{\mathrm{G}}, \qquad \chi \mapsto \chi \circ \pi$$

est un isomorphisme de groupes. Par conséquent le nombre de représentations de degré 1 de G est égal $|\mathrm{G}^{\mathrm{ab}}|$.

Les représentations de dimension 1 sont des morphismes

$$\mathrm{G} \to \mathrm{GL}(1,\mathbb{C}) = \mathbb{C}^*;$$

elles se factorisent donc par le quotient $\mathrm{G} \to {}^{\mathrm{G}}\!/_{D(\mathrm{G})} = \mathrm{G}^{\mathrm{ab}}$ puisque $\mathbb{C}^*$ est abélien (c'est la propriété universelle du quotient).

Ainsi en pratique si nous connaissons $D(\mathrm{G})$, nous obtenons toutes les représentations de degré 1. Sinon une fois que nous aurons établi la table des caractères de G, nous pourrons déterminer $D(\mathrm{G})$ en vertu de l'énoncé suivant

> *Le sous-groupe dérivé $D(\mathrm{G})$ est l'intersection des noyaux des représentations de dimension 1 :*
>
> $$D(\mathrm{G}) = \bigcap_{\chi \in \widehat{\mathrm{G}}} \ker \chi$$

En effet le sous-groupe dérivé est le noyau de la représentation $\pi \circ \rho_R^{\mathrm{ab}}$ de G où ρ_R^{ab} désigne la représentation régulière de l'abélianisé de G. On conclut en utilisant d'une part qu'on obtient le noyau de la représentation $\pi \circ \rho_R^{\mathrm{ab}}$ comme intersection de noyau $\ker \chi$ en décomposant la représentation $\pi \circ \rho_R^{\mathrm{ab}}$ de G en somme de représentations irréductibles et d'autre part que toute sous-représentation irréductible de $\pi \circ \rho_R^{\mathrm{ab}}$ est de dimension 1 puisque G^{ab} est abélien.

Remarque 11.3.6. — Si $\varepsilon\colon \mathrm{G} \to \mathbb{C}^*$ est un caractère de degré 1 de G, et χ est le caractère d'une représentation irréductible ρ, alors $\varepsilon\chi$ est encore le caractère d'une représentation irréductible, à savoir la représentation $s \mapsto \varepsilon(s)\rho(s)$ (vérification immédiate). Cette remarque est souvent utile pour les groupes symétriques (en prenant pour ε la signature).

***Remarque 11.3.7* (Centre de G).** — Si g appartient au centre $Z(\mathrm{G})$ de G, alors $\rho_i(g)$ commute avec tous les $\rho_i(h)$. Le Lemme de Schur (Lemme 11.1.1) assure alors que $\rho_i(g)$ est une homothétie de rapport une racine de l'unité et $|\chi_i(g)| = \chi_i(e)$ pour tout i. Réciproquement si $|\chi_i(g)| = \chi_i(e)$, nous avons vu que $\rho_i(g)$ est une homothétie donc commute avec tous les $\rho_i(h)$. Si c'est vrai pour tout i, alors $\rho(g)$ commute avec tous les $\rho(h)$ et ceci pour toute représentation ρ. Si on applique cela à une représentation fidèle (*i.e.* une représentation pour laquelle ρ est

injective) comme la représentation régulière nous obtenons que g appartient au centre $Z(\mathrm{G})$ de G.

Le centre $Z(\mathrm{G})$ de G est donc la réunion des classes de conjugaison C pour lesquelles $|\chi_i(C)| = \chi_i(e)$ pour tout i.

11.3.1. Les groupes cycliques. — Un groupe cyclique étant abélien il n'a que des représentations de dimension 1 (Exemple 11.1.17 et Proposition 11.2.3) c'est-à-dire des caractères au sens premier du terme (des morphismes de G dans le groupe multiplicatif $\mathbb{C}^*$). Soit $\mathrm{G} = \{e, g, g^2, \ldots, g^{n-1}\}$ un groupe cyclique d'ordre n et de générateur g. Posons $\omega_n = \exp\left(\frac{2\pi\mathbf{i}}{n}\right)$. Les caractères de G sont de la forme

$$\chi_j \colon \mathrm{G} \to \mathbb{C}^* \qquad\qquad h = g^k \mapsto (\omega_n^j)^k = \exp\left(\frac{2\mathbf{i}k\pi j}{n}\right)$$

où $0 \leq j \leq n-1$.

Le groupe G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. La table de $\mathbb{Z}/n\mathbb{Z}$ est la matrice de Vandermonde

	$\overline{0}$	$\overline{1}$	$\ldots$	$\overline{n-1}$
χ_0	1	1	$\ldots$	1
χ_1	1	ω_n	$\ldots$	ω_n^{n-1}
χ_2	1	ω_n^2	$\ldots$	$\omega_n^{2(n-1)}$
$\vdots$	$\vdots$			$\vdots$
χ_{n-1}	1	ω_n^{n-1}	$\ldots$	$\omega_n^{(n-1)(n-1)}$

11.3.2. Le groupe dicyclique d'ordre 12 ([Rau00]). — , *i.e.* la troisième classe d'isomorphie de groupes d'ordre 12 non abéliens autre que celles de D_{12} et $\mathcal{A}_4$

Il s'agit du produit semi-direct $\mathrm{G} = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, le groupe $\mathbb{Z}/4\mathbb{Z}$ agit en envoyant la classe de 1 sur l'automorphisme $x \mapsto -x$ [4].

Une présentation de G est donnée par

$$\langle a, b \,|\, a^6 = 1,\, b^2 = a^3,\, b^{-1}ab = a^{-1}\rangle$$

4. Plus généralement le groupe dicyclique Dic_n est défini pour tout entier $n \geq 2$ par la présentation

$$\mathrm{Dic}_n = \langle a, b \,|\, a^{2n} = 1,\, b^2 = a^n,\, b^{-1}ab = a^{-1}\rangle$$

Les groupes Dic_{2^m} sont les groupes quaternioniques. En particulier, $\mathbb{H}_8 = \mathrm{Dic}_2$ est le groupe des quaternions.

Le groupe Dic_n est un groupe non abélien d'ordre $4n$, extension par le sous-groupe cyclique engendré par a (normal et d'ordre $2n$) d'un groupe d'ordre 2. Pour n impair le groupe Dic_n est isomorphe à un produit semi-direct : c'est le produit semi-direct de $\mathbb{Z}/n\mathbb{Z}$ par $\mathbb{Z}/4\mathbb{Z}$ où ce dernier agit en envoyant la classe de 1 sur l'automorphisme $x \mapsto -x$.

Le groupe Dic_n est aussi une extension par son centre (le sous-groupe d'ordre 2 engendré par $a^n = b^2$) du groupe diédral D_{4n}. Cette extension est, elle aussi, non scindée.

dont nous déduisons

$$\mathrm{G} = \{a^k b^\ell \,|\, 0 \leq k \leq 2,\, 0 \leq \ell \leq 3\}.$$

De plus (on pourra s'aider du fait que $ba^p b^{-1} = a^{2p}$ pour tout p mais aussi $b^\ell a b^{-\ell} = a^{2^\ell}$ pour tout ℓ et encore $b^\ell a^k b^{-\ell} = a^{k\times 2^\ell}$ pour tous k, ℓ)

$$Z(\mathrm{G}) = \langle b^2 \rangle, \qquad D(\mathrm{G}) = \langle a \rangle, \qquad \mathrm{G}^{\mathrm{ab}} = \langle b \rangle \simeq \mathbb{Z}/4\mathbb{Z}$$

En particulier le groupe G admet $|\mathrm{G}^{\mathrm{ab}}| = \left|\mathbb{Z}/4\mathbb{Z}\right| = 4$ représentations irréductibles de degré 1 déterminées par l'image de b qui doit être une racine 4-ième de l'unité.

Le groupe G a six classes de conjugaison

$$C_1 = \{e\}, \qquad C_2 = \{b^2\}, \qquad C_3 = \{a,\, a^2\},$$
$$C_4 = \{ab^2,\, a^2b^2\}, \qquad C_5 = \{b,\, ab,\, a^2b\}, \qquad C_6 = \{b^3,\, ab^3,\, a^2b^3\}.$$

Il s'ensuit que G possède six représentations irréductibles. Nous en avons déjà déterminé quatre. À partir de $|\mathrm{G}| = \sum_i (\deg \rho_i)^2$ nous obtenons que les deux autres représentations irréductibles de G sont de degré 2.

Le groupe G a trois 2-Sylow :

$$\mathrm{S}_1 = \langle b \rangle, \qquad \mathrm{S}_2 = \{e,\, b^2,\, ab,\, ab^3\}, \qquad \mathrm{S}_3 = \{e,\, b^2,\, a^2b,\, a^2b^3\}.$$

L'action de G par conjugaison sur ses 2-Sylow définit une représentation ρ de G qui conduit au caractère

	C_1	C_2	C_3	C_4	C_5	C_6
χ_3	3	3	0	0	1	1

Puisque $\langle \chi_3, \chi_3 \rangle = 2 = 1 + 1$ nous en déduisons que $\chi_3 = \chi_2 + \chi_{\rho_{\mathrm{triv}}}$ où χ_2 est irréductible de degré 2. En effet

	C_1	C_2	C_3	C_4	C_5	C_6
χ_2	2	2	-1	-1	0	0

et

$$\begin{aligned}
\langle \chi_2, \chi_2 \rangle &= \frac{1}{12}\Big(1 \times 2 \times \overline{2} + 1 \times 2 \times \overline{2} + 2 \times (-1) \times \overline{-1} + 2 \times (-1) \times \overline{-1} + 3 \times 0 \times \overline{0} + 3 \times 0 \times \overline{0}\Big) \\
&= \frac{1}{12}(4 + 4 + 2 + 2) \\
&= 1.
\end{aligned}$$

La seconde représentation irréductible de degré 2, de caractère χ_2', est donnée par la représentation matricielle suivante

$$a \mapsto \begin{pmatrix} -\frac{1}{2} & \frac{\mathbf{i}\sqrt{3}}{2} \\ \frac{\mathbf{i}\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \qquad b \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Il s'ensuit que la table de caractère de $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ est

	C_1	C_2	C_3	C_4	C_5	C_6
ψ_0	1	1	1	1	1	1
ψ_1	1	-1	1	-1	$\mathbf{i}$	$-\mathbf{i}$
ψ_2	1	1	1	1	-1	-1
ψ_3	1	-1	1	-1	$-\mathbf{i}$	$\mathbf{i}$
χ_2	2	2	-1	-1	0	0
χ_2'	2	-2	-1	1	0	0

11.3.3. Le groupe $\mathfrak{S}_3 = \mathrm{D}_6$. — Les classes de conjugaison de $\mathfrak{S}_3$ sont (Théorème 5.1.5)

$$C_1 = \{\mathrm{id}\}, \qquad C_2 = \{(1\ 2),\ (1\ 3),\ (2\ 3)\}, \qquad C_3 = \{(1\ 2\ 3),\ (1\ 3\ 2)\}.$$

Ainsi $\mathfrak{S}_3$ a trois représentations irréductibles à équivalence près. Il y a la représentation triviale ρ_{triv} qui est irréductible. On a aussi la représentation signature

$$\mathrm{sgn}\colon \mathfrak{S}_3 \to \mathrm{GL}(1, \mathbb{C}) \simeq \mathbb{C}^*, \qquad \sigma \mapsto \mathrm{sgn}(\sigma)$$

qui est de degré 1 ; elle est irréductible car

$$\langle \chi_{\mathrm{sgn}}, \chi_{\mathrm{sgn}} \rangle = \frac{1}{6}\Big(\underbrace{1}_{\#C_1} \times \underbrace{1}_{\chi_{\mathrm{sgn}}((\mathrm{id}))} \times \overline{1} + \underbrace{3}_{\#C_2} \times \underbrace{(-1)}_{\chi_{\mathrm{sgn}}((1\ 2))} \times \overline{(-1)} + \underbrace{2}_{\#C_3} \times \underbrace{1}_{\chi_{\mathrm{sgn}}((1\ 2\ 3))} \times \overline{1} \Big) = 1$$

Enfin on a la représentation décrite dans l'Exemple 11.1.15 dite représentation standard et notée ρ_S. Notons que

$$(\deg \rho_{\mathrm{triv}})^2 + (\deg \mathrm{sgn})^2 + (\deg \rho_S)^2 = 1^2 + 1^2 + 2^2 = 6$$

autrement dit $(\deg \rho_{\mathrm{triv}})^2 + (\deg \mathrm{sgn})^2 + (\deg \rho_S)^2 = |\mathfrak{S}_3|$.

Ainsi la table de caractères de $\mathfrak{S}_3$ est

	C_1	C_2	C_3
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1
sgn	1	-1	1
χ_{ρ_S}	2	0	-1

A noter que les colonnes sont bien orthogonales.

11.3.4. Les groupes diédraux D_{2n}. —

11.3.4.1. *Le cas général.* — Rappelons quelques propriétés des groupes diédraux. Le groupe D_{2n} a pour présentation

$$\mathrm{D}_{2n} = \langle r,\, s \mid s^2 = r^n = rsrs = \mathrm{id}\rangle.$$

Le centre de D_{2n} est (Théorème 5.2.6)

$$Z(\mathrm{D}_{2n}) = \begin{cases} \mathrm{id} \text{ si } n \text{ est impair} \\ \{\mathrm{id},\, r^{n/2}\} \text{ si } n \text{ est pair} \end{cases}$$

et le groupe dérivé de D_{2n} (Théorème 5.2.7) est

$$D(\mathrm{D}_{2n}) = \begin{cases} \langle r\rangle \text{ si } n \text{ est impair} \\ \langle r^2\rangle \text{ si } n \text{ est pair} \end{cases}$$

Les éléments sont

- ⋄ ou bien de la forme r^k, $0 \leq k \leq n-1$ et on parle de rotations,
- ⋄ ou bien de la forme $r^k s$, $0 \leq k \leq n-1$ et on parle de symétries.

En particulier D_{2n} contient un sous-groupe abélien d'indice 2 de sorte que toutes les représentations irréductibles de D_{2n} sont de degré 1 ou 2. En effet

Lemme 11.3.1

Soit G un groupe fini. Soit H un sous-groupe abélien de G d'indice n.
Toutes les représentations irréductibles de G sont de degré $\leq n$.

Démonstration. — Soit $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$ une représentation irréductible de G. Soit $\rho_{|\mathrm{H}}\colon \mathrm{H} \to \mathrm{GL}(V)$ sa restriction. Elle s'écrit comme une somme directe de représentations de degré 1 (le groupe H étant abélien, ses représentations irréductibles sont de degré 1). En particulier il existe un sous-espace vectoriel W de V tel que

$$\dim W = 1 \qquad\qquad \rho(H)(W) \subset W.$$

Considérons un système de représentants $g_1 = \mathrm{id}$, g_2, g_3, …, g_n de G/H. Alors le sous-espace

$$W' = \rho(g_1)(W) + \rho(g_2)(W) + \ldots + \rho(g_n)(W)$$

est stable par ρ de sorte que $V = W'$ (car ρ est irréductible). Il en résulte que $\dim W' = \dim V \leq n$. □

Nous allons distinguer le cas n pair du cas n impair.

- ⋄ Supposons pour commencer que n est pair (Proposition 5.2.1).

  Les symétries forment deux classes de conjugaison

$$\{s,\, r^2 s,\, r^4 s,\, \ldots, r^{n-2} s\} \qquad\qquad \{rs,\, r^3 s,\, \ldots, r^{n-1} s\}$$

et les rotations forment $\frac{n}{2}+1$ classes de conjugaison

$$\{\mathrm{id}\}, \qquad \{r,\, r^{n-1}\}, \qquad \dots \qquad \{r^k,\, r^{n-k}\}, \qquad \dots, \qquad \{r^{\frac{n}{2}-1},\, r^{\frac{n}{2}+1}\}, \qquad \{r^{\frac{n}{2}}\}.$$

Ainsi D_{2n} possède $3+\frac{n}{2}$ classes de conjugaison donc $3+\frac{n}{2}$ représentations irréductibles à équivalence près. Étant donné que $D(\mathrm{D}_{2n}) = \langle r^2\rangle$ l'abélianisé $\mathrm{D}_{2n}^{\mathrm{ab}}$ de D_{2n} est isomorphe au groupe de Klein qui est d'ordre 4. Il en résulte que D_{2n} possède 4 caractères de degré 1. Les caractères de degré 1 sont les morphismes de groupes

$$\mathrm{D}_{2n}^{\mathrm{ab}} = \langle \overline{r},\, \overline{s}\rangle \to \mathbb{C}^*.$$

Ils sont caractérisés par les valeurs

	r	s
χ_1	1	1
χ_2	1	-1
χ_3	-1	1
χ_4	-1	-1

Ainsi le groupe D_{2n} possède à équivalence près $3+\frac{n}{2}-4=\frac{n}{2}-1$ représentations irréductibles de degré 2.

Posons $\zeta = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$. Pour $0 \le j \le n-1$ considérons la représentation ρ_j définie par

$$\rho_j \colon \mathrm{D}_{2n} \to \mathrm{GL}(2,\mathbb{C}), \qquad r \mapsto \begin{pmatrix} \zeta^j & 0 \\ 0 & \zeta^{-j} \end{pmatrix}, \qquad s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Remarquons que

$$\rho_j(s)\rho_j(r)\rho_j(s^{-1}) = \rho_j(r)^{-1} = \rho_{n-j}(r);$$

en particulier les représentations ρ_j et ρ_{n-j} sont équivalentes. Nous sommes donc amenés à considérer les ρ_j pour $0 \le j \le \frac{n}{2}$. De plus

$$\chi_{\rho_0} = \chi_1 + \chi_2, \qquad \chi_{\rho_{\frac{n}{2}}} = \chi_3 + \chi_4;$$

en particulier les représentations ρ_0 et $\rho_{\frac{n}{2}}$ ne sont pas irréductibles. Finalement nous ne gardons que les ρ_j pour $1 \le j \le \frac{n}{2}-1$. Pour ces représentations les seules droites stables par $\rho_j(r)$ sont les axes $\mathbb{C}(e_1)$ et $\mathbb{C}(e_2)$. Mais $\mathbb{C}(e_1)$ et $\mathbb{C}(e_2)$ ne sont pas stables par $\rho_j(s)$. Les représentations ρ_j, $1 \le j \le \frac{n}{2}-1$, sont donc irréductibles. De plus pour tout $0 \le k \le n-1$ nous avons

$$\chi_{\rho_j}(r^k) = 2\cos\left(k\frac{2\pi}{n}\right) \qquad \chi_{\rho_j}(r^k s) = 0$$

◇ Supposons désormais que n est impair (Proposition 5.2.1).

Les symétries forment une seule classe de conjugaison :

$$\{s,\, rs,\, \dots,\, r^{n-1}s\}$$

tandis que les rotations forment $\frac{n+1}{2}$ classes de conjugaison :

$$\{\mathrm{id}\}, \qquad \{r,\, r^{n-1}\}, \qquad \dots \qquad \{r^k,\, r^{n-k}\}, \qquad \dots, \qquad \{r^{\frac{n-1}{2}},\, r^{\frac{n+1}{2}}\}.$$

Ainsi D_{2n} possède $\frac{n+1}{2}+1$ classes de conjugaison et donc $\frac{n+1}{2}+1$ représentations irréductibles à équivalence près.

Comme $D(\mathrm{D}_{2n}) = \langle r\rangle$ nous avons $\mathrm{D}_{2n}^{\mathrm{ab}} = {}^{\mathrm{D}_{2n}}\!/_{D(\mathrm{D}_{2n})} = {}^{\mathrm{D}_{2n}}\!/_{\langle r\rangle} \simeq \langle s\rangle$. Par conséquent D_{2n} possède deux caractères de degré 1. Les caractères de degré 1 sont les morphismes de groupes

$$\mathrm{D}_{2n}^{\mathrm{ab}} = \langle \overline{s}\rangle \to \mathbb{C}^*$$

ils sont caractérisés par les valeurs

	r	s
χ_1	1	1
χ_2	1	-1

Le groupe D_{2n} possède donc à équivalence près $\frac{n-1}{2}$ représentations irréductibles de degré 2.

Posons $\zeta = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$. Pour $0 \le j \le n-1$ considérons la représentation

$$\rho_j \colon \mathrm{D}_{2n} \to \mathrm{GL}(2,\mathbb{C}), \qquad r \mapsto \begin{pmatrix} \zeta^j & 0 \\ 0 & \zeta^{-j} \end{pmatrix}, \qquad s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Notons que

$$\rho_j(s)\rho_j(r)\rho_j(s^{-1}) = \rho_j(r)^{-1} = \rho_{n-j}(r);$$

en particulier les représentations ρ_j et ρ_{n-j} sont équivalentes. Nous sommes donc amenés à considérer les ρ_j pour $1 \le j \le \frac{n-1}{2}$. Les seules droites stables par $\rho_j(r)$ sont les axes $\mathbb{C}(e_1)$ et $\mathbb{C}(e_2)$. Mais $\mathbb{C}(e_1)$ et $\mathbb{C}(e_2)$ ne sont pas stables par $\rho_j(s)$. Les représentations ρ_j, $1 \le j \le \frac{n-1}{2}$, sont donc irréductibles. De plus pour tout $0 \le k \le n-1$ nous avons

$$\chi_{\rho_j}(r^k) = 2\cos\left(k\frac{2\pi}{n}\right) \qquad\qquad \chi_{\rho_j}(r^k s) = 0.$$

11.3.4.2. *Le groupe* D_8. — Le groupe de symétries du carré est engendré par une rotation r d'angle $\frac{\pi}{2}$ et une symétrie s. Le groupe D_8 a 5 classes de conjugaison (Proposition 5.2.1) : $\{\mathrm{id}\}$, $\{r^2\}$, $\{r,\, r^3\}$, $\{s,\, r^2 s\}$ et $\{rs,\, r^3 s\}$. Le sous-groupe $D(\mathrm{D}_8) = {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} = \{\mathrm{id},\, -\mathrm{id} = r^2\}$ est distingué dans D_8 et dans le quotient les trois éléments distincts r, s et rs sont d'ordre 2 donc

$$\mathrm{D}_8^{\mathrm{ab}} = {}^{\mathrm{D}_8}\!/_{D(\mathrm{D}_8)} = {}^{\mathrm{D}_8}\!/_{{}^{\mathbb{Z}}\!/_{2\mathbb{Z}}} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}.$$

Nous avons donc quatre représentations de dimension 1 correspondant aux quatre morphismes

$${}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \to \mathbb{C}^\times;$$

la cinquième doit donc être de dimension 2 (en effet $|\mathrm{D}_8| = 8$ donc $|\mathrm{D}_8| - (1^2 + 1^2 + 1^2 + 1^2) = 4 = 2^2$). C'est la représentation standard dans $\mathbb{C}^2$ (Exemple 11.2.3) d'où la dernière ligne de la table (que l'on peut aussi obtenir en utilisant que les colonnes sont orthogonales).

Ainsi

	$\{\mathrm{id}\}$	$\{r^2\}$	$\{r,\, r^3\}$	$\{s,\, r^2s\}$	$\{rs,\, r^3s\}$
χ_{triv}	1	1	1	1	1
χ_1	1	1	-1	1	-1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	-1	1
χ_4	2	-2	0	0	0

Les sous-groupes distingués de D_8 sont D_8, $\ker\chi_1 = \{\mathrm{id},\, r^2,\, s,\, r^2s\}$, $\ker\chi_2 = \{\mathrm{id},\, r,\, r^2,\, r^3\}$, $\ker\chi_3 = \{\mathrm{id},\, r^2,\, rs,\, r^3s\}$, $\{\mathrm{id}\}$ et leurs intersections ; autrement dit les sous-groupes distingués de D_8 sont

$$\mathrm{D}_8, \qquad \{\mathrm{id}\}, \qquad \langle r\rangle = \ker\chi_2 \simeq \mathbb{Z}/4\mathbb{Z}, \qquad \langle r^2\rangle = \{\mathrm{id},\, r^2\} \simeq \mathbb{Z}/2\mathbb{Z},$$

$$\ker\chi_1 = \langle s,\, r^2\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad \ker\chi_3 = \langle rs,\, r^2\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Le groupe dérivé de D_8 est $\ker\chi_1 \cap \ker\chi_2 \cap \ker\chi_3 = \{\mathrm{id},\, r^2\}$ et le centre de D_8 est $\{g \in \mathrm{D}_8 \,|\, \forall\, i\, |\chi_i(g)| = \chi_i(\mathrm{id})\} = \{\mathrm{id},\, r^2\}$.

11.3.5. Le groupe des quaternions. — Rappelons que le groupe des quaternions est

$$\mathbb{H}_8 = \{1,\, -1,\, i,\, -i,\, j,\, -j,\, k,\, -k\}$$

avec

$$i^2 = j^2 = k^2 = -1 \qquad ij = -ji = k \qquad jk = -kj = i \qquad ki = -ik = j$$

C'est l'un des deux groupes non abéliens ($ij = -ji$) d'ordre 8.

Le groupe $\mathbb{H}_8$ possède cinq classes de conjugaison

$$\{1\}, \qquad \{-1\}, \qquad \{i,\, -i\}, \qquad \{j,\, -j\}, \qquad \{k,\, -k\}.$$

Puisque $D(\mathbb{H}_8) = \{1,\, -1\}$, l'abélianisé $\mathbb{H}_8/D(\mathbb{H}_8)$ de $\mathbb{H}_8$ est isomorphe au groupe de Klein, *i.e.* est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il en résulte que $\mathbb{H}_8$ possède quatre caractères de degré 1. Ainsi si ρ_i est une représentation irréductible de $\mathbb{H}_8$ de degré d_i nous avons

- ⋄ d'une part $d_1 = d_2 = d_3 = d_4 = 1$,
- ⋄ d'autre part $\displaystyle\sum_{i=1}^{5} d_i^2 = 8$.

Par conséquent $d_1 = d_2 = d_3 = d_4 = 1$ et $d_5 = 2$.

La table des caractères de $\mathbb{H}_8$ est donc

	$\{1\}$	$\{-1\}$	$\{i, -i\}$	$\{j, -j\}$	$\{k, -k\}$
χ_{triv}	1	1	1	1	1
χ_1	1	1	-1	1	-1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	-1	1
χ_4	2				

On peut obtenir la dernière ligne en utilisant que les colonnes sont orthogonales :

	$\{1\}$	$\{-1\}$	$\{i, -i\}$	$\{j, -j\}$	$\{k, -k\}$
χ_{triv}	1	1	1	1	1
χ_1	1	1	-1	1	-1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	-1	1
χ_4	2	-2	0	0	0

On peut aussi voir que $\rho_4 \colon \mathbb{H}_8 \to \mathrm{GL}(2, \mathbb{C})$ définie par

$$\rho_4(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \rho_4(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \rho_4(k) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \rho_4(-1) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

est une représentation dont le caractère est donné par

$$\chi_4(1) = 2, \qquad \chi_4(-1) = -2, \qquad \chi_4(i) = 0, \qquad \chi_4(j) = 0, \qquad \chi_4(k) = 0.$$

Cette représentation est irréductible car

$$\langle \chi_4, \chi_4 \rangle = \frac{1}{8}\Big(1 \times 2^2 + (-1) \times (-2)^2 + 2 \times 0 + 2 \times 0 + 2 \times 0\Big) = 1.$$

Remarque 11.3.8. — Les deux exemples précédents (D_8 et $\mathbb{H}_8$) montrent que deux groupes non isomorphes G et H peuvent avoir des tables de caractères « isomorphes » au sens où il existe une bijection des classes de conjugaison de G sur celles de H, respectivement des classes de représentations irréductibles de G sur celles de H telles que les tables obtenues soient les mêmes. Il existe néanmoins deux façons de distinguer deux groupes ayant la même table à partir de la table.

L'application $g \mapsto g^2$ est compatible à la conjugaison donc induit une application $c \mapsto c^2$ de l'ensemble des classes de conjugaison de G dans lui-même. Pour D_8 nous avons

$$\{s, r^2 s\}^2 = \{e\}$$

tandis que pour $\mathbb{H}_8$ nous avons

$$\{\pm j\}^2 = \{-1\}.$$

Autrement dit la bijection entre les classes de conjugaison qui rend les tables de caractères identiques n'est pas compatible à l'opération « carré des classes de conjugaison » ce qui permet de distinguer les deux groupes.

Si on le souhaite, on peut au lieu de considérer une opération sur les classes de conjugaison considérer une opération sur les représentations. Si (V, ρ) est une représentation de G, alors

$$\mathrm{Sym}^2 V := {}^{V \otimes V}\!\big/_{\mathrm{Vect}\big((v_1 \otimes v_2 - v_2 \otimes v_1) \,|\, v_1,\, v_2 \in V\big)}$$

est une représentation quotient de $\rho \otimes \rho$ notée $\mathrm{Sym}^2(\rho)$ dont le caractère est donné par

$$\chi_{\mathrm{Sym}^2(\rho)}(g) = \frac{1}{2}\big(\chi_\rho(g)^2 + \chi_\rho(g^2)\big).$$

Ainsi $\mathrm{Sym}^2(\chi_4(\mathrm{D}_8)) = \chi_{\mathrm{triv}}(\mathrm{D}_8) + \chi_1(\mathrm{D}_8) + \chi_3(\mathrm{D}_8)$ tandis que $\mathrm{Sym}^2(\chi_4(\mathbb{H}_8)) = \chi_1(\mathbb{H}_8) + \chi_2(\mathbb{H}_8) + \chi_3(\mathbb{H}_8)$. Ainsi la bijection entre les caractères de $\mathbb{D}_8$ et ceux de $\mathbb{H}_8$ n'est pas compatible à l'opération « carré symétrique » ce qui permet de distinguer les deux groupes.

11.3.6. Le groupe $\mathfrak{S}_4$. — Le groupe symétrique $\mathfrak{S}_4$ possède cinq classes de conjugaison (Théorème 5.1.5) :

$$\begin{aligned}
C_1 &= \{\mathrm{id}\},\\
C_2 &= \{(1\ 2),\ (1\ 3),\ (1\ 4),\ (2\ 3),\ (2\ 4),\ (3\ 4)\},\\
C_3 &= \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\},\\
C_4 &= \{(1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3)\},\\
C_5 &= \{(1\ 2\ 3\ 4),\ (1\ 2\ 4\ 3),\ (1\ 3\ 2\ 4),\ (1\ 3\ 4\ 2),\ (1\ 4\ 2\ 3),\ (1\ 4\ 3\ 2)\}.
\end{aligned}$$

Il y a donc cinq représetntations irréductibles à équivalence près. On peut déjà donner deux représentations de degré 1

- ⋄ la représentation triviale ρ_{triv} ;
- ⋄ la représentation signature sgn.

Intéressons-nous à la représentation par permutations. Notons $\mathcal{B} = (e_1, e_2, e_3, e_4)$ la base canonique de $\mathbb{C}^4$. On définit la représentation par permutations par

$$\rho_P \colon \mathfrak{S}_4 \to \mathrm{GL}(\mathbb{C}^4) \qquad\qquad \sigma \mapsto (e_i \mapsto e_{\sigma(i)}).$$

Cette représentation laisse stable $\mathrm{Vect}(1,1,1,1)$ dont

$$H = \{x = (x_1, x_2, x_3, x_4) \in \mathbb{C}^4 \,|\, x_1 + x_2 + x_3 + x_4 = 0\}$$

est un supplémentaitre stable. Elle induit une représentation ρ_S sur H. Comme ρ_P induit la représentation triviale sur $\mathrm{Vect}(1,1,1,1)$ nous avons la relation $\chi_{\rho_P} = \chi_{\rho_{\mathrm{triv}}} + \chi_{\rho_S}$. Reste à savoir si χ_{ρ_S} est irréductible, *i.e.* si $\langle \chi_{\rho_S}, \chi_{\rho_S} \rangle = 1$. Mais $\chi_{\rho_P}(\sigma)$ est le nombre de 1 sur la

diagonale de la matrice de permutations σ, c'est-à-dire le nombre de points fixes de σ (Exemple 11.1.4). Ainsi

$$\chi_{\rho_P}(\mathrm{id}) = 4, \quad \chi_{\rho_P}((1\ 2)) = 2, \quad \chi_{\rho_P}((1\ 2)(3\ 4)) = 0, \quad \chi_{\rho_P}((1\ 2\ 3)) = 1, \quad \chi_{\rho_P}((1\ 2\ 3\ 4)) = 0$$

(en effet $\mathrm{Fix}(\mathrm{id}) = \{1, 2, 3, 4\}$, $\mathrm{Fix}((1\ 2)) = \{3, 4\}$, $\mathrm{Fix}((1\ 2)(3\ 4)) = \emptyset$, $\mathrm{Fix}((1\ 2\ 3)) = \{4\}$ et $\mathrm{Fix}((1\ 2\ 3\ 4)) = \emptyset$) d'où (puisque $\chi_{\rho_S}(g) = \chi_{\rho_P}(g) - \chi_{\rho_{\mathrm{triv}}}(g) = \chi_{\rho_P}(g) - 1$)

$$\chi_{\rho_S}(\mathrm{id}) = 3, \quad \chi_{\rho_S}((1\ 2)) = 1, \quad \chi_{\rho_S}((1\ 2)(3\ 4)) = -1, \quad \chi_{\rho_S}((1\ 2\ 3)) = 0, \quad \chi_{\rho_S}((1\ 2\ 3\ 4)) = -1.$$

Il en résulte que

$$\begin{aligned}\langle \chi_{\rho_S}, \chi_{\rho_S}\rangle &= \frac{1}{|\mathfrak{S}_4|}\Big(1 \times 3 \times \overline{3} + 6 \times 1 \times \overline{1} + 3 \times (-1) \times \overline{(-1)} + 8 \times 0 \times \overline{0} + 6 \times (-1) \times \overline{(-1)}\Big) \\ &= \frac{1}{24}(9 + 6 + 3 + 6)\end{aligned}$$

Nous en déduisons que ρ_S est une représentation irréductible de degré 3. Nous la notons ρ_4.

Déterminons les deux autres représentations irréductibles de $\mathfrak{S}_4$ notées ρ_3 et ρ_5. Commençons par déterminer leurs degrés : l'identité

$$(\deg \rho_{\mathrm{triv}})^2 + (\deg \mathrm{sgn})^2 + (\deg \rho_3)^2 + (\deg \rho_4)^2 + (\deg \rho_5)^2 = |\mathfrak{S}_4|$$

conduit à

$$24 - (\deg \rho_{\mathrm{triv}})^2 - (\deg \mathrm{sgn})^2 - (\deg \rho_4)^2 = (\deg \rho_3)^2 + (\deg \rho_5)^2$$

soit $13 = (\deg \rho_3)^2 + (\deg \rho_5)^2$. Nous en déduisons que $\{\deg \rho_3, \deg \rho_5\} = \{2, 3\}$.

Considérons la représentation

$$\rho_5 \colon \mathfrak{S}_4 \to \mathrm{GL}(H), \qquad \sigma \mapsto \mathrm{sgn}(\sigma)\rho_4(\sigma).$$

Alors $\chi_{\rho_5} = \mathrm{sgn}\chi_{\rho_4}$ d'où

$$\begin{aligned}&\chi_{\rho_5}(\mathrm{id}) = 1 \times 3 = 3, && \chi_{\rho_5}((1\ 2)) = (-1) \times 1 = -1, \\ &\chi_{\rho_5}((1\ 2\ 3)) = 1 \times 0 = 0, && \chi_{\rho_5}((1\ 2\ 3\ 4)) = (-1) \times (-1) = 1, \\ &\chi_{\rho_5}((1\ 2)(3\ 4)) = 1 \times (-1) = -1.\end{aligned}$$

En particulier

$$\begin{aligned}\langle \chi_{\rho_5}, \chi_{\rho_5}\rangle &= \frac{1}{24}\Big(1 \times 3 \times 3 + 6 \times (-1) \times (-1) + 3 \times (-1) \times (-1) + 8 \times 0 \times 0 + 6 \times 1 \times 1\Big) \\ &= \frac{1}{24}\Big(9 + 6 + 3 + 6\Big) \\ &= 1.\end{aligned}$$

Il s'ensuit que ρ_5 est irréductible. De plus $\deg \rho_5 = \dim H = 3$.

Remarque 11.3.9. — On peut donner une interprétation géométrique de ρ_5 : c'est la représentation de $\mathfrak{S}_4$ comme $\mathrm{Isom}^+(C_6)$ (Proposition 12.3.4).

Commençons à écrire la table de caractères de $\mathfrak{S}_4$:

	$C(\mathrm{id})$	$C((1\ 2))$	$C((1\ 2)(3\ 4))$	$C((1\ 2\ 3))$	$C((1\ 2\ 3\ 4))$
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1
χ_{ρ_3}	2	?	?	?	?
χ_{ρ_4}	3	1	-1	0	-1
χ_{ρ_5}	3	-1	-1	0	1

où $C(g)$ désigne la classe de conjugaison de $g \in \mathfrak{S}_4$.

En utilisant que les colonnes de la table de $\mathfrak{S}_4$ sont orthogonales nous obtenons

	$C(\mathrm{id})$	$C((1\ 2))$	$C((1\ 2)(3\ 4))$	$C((1\ 2\ 3))$	$C((1\ 2\ 3\ 4))$
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1
χ_{ρ_3}	2	0	2	-1	0
χ_{ρ_4}	3	1	-1	0	-1
χ_{ρ_5}	3	-1	-1	0	1

Rappelons que les sous-groupes distingués de $\mathfrak{S}_4$ sont les intersections $\bigcap_{i\in I} \ker \chi_{\rho_i}$ où $I \subset$ [triv, sgn, 3, 4, 5]. La table des caractères de $\mathfrak{S}_4$ assure que

$$\begin{aligned}
&\ker \chi_{\rho_{\mathrm{triv}}} = \mathfrak{S}_4\\
&\ker \chi_{\rho_{\mathrm{sgn}}} = \{\mathrm{id},\, C((1\ 2)(3\ 4)),\, C(1\ 2\ 3)\} = \mathcal{A}_4\\
&\ker \chi_{\rho_3} = \{\mathrm{id},\, C((1\ 2)(3\ 4))\} \simeq \mathcal{K}\\
&\ker \chi_{\rho_4} = \{\mathrm{id}\}\\
&\ker \chi_{\rho_5} = \{\mathrm{id}\}
\end{aligned}$$

Par suite les sous-groupes distingués de $\mathfrak{S}_4$ sont

$$\mathfrak{S}_4, \qquad \{\mathrm{id}\}, \qquad \mathcal{A}_4, \qquad \{\mathrm{id},\, (1\ 2)(3\ 4),\, (1\ 3)(2\ 4),\, (1\ 4)(2\ 3)\} \simeq \mathcal{K}$$

(on rappelle que $\mathcal{K}$ désigne le groupe de Klein).

Explicitons ρ_3. Nous avons la décomposition en produit semi-direct

$$\mathfrak{S}_4 \simeq \mathcal{K} \rtimes \mathfrak{S}_3.$$

À cette décomposition correspond un morphisme surjectif de groupes

$$\pi\colon \mathfrak{S}_4 \to {}^{\mathfrak{S}_4}\!/_{\mathcal{K}} \simeq \mathfrak{S}_3$$

d'où par composition avec la représentation standard $\widetilde{\rho_S}$ de $\mathfrak{S}_3$ une représentation de degré 2

$$\rho_3 \colon \mathfrak{S}_4 \xrightarrow{\pi} \mathfrak{S}_3 \xrightarrow{\widetilde{\rho_S}} \mathrm{GL}(\widetilde{H})$$

où $\widetilde{H}$ désigne l'hyperplan de $\mathbb{C}^3$ d'équation $x_1 + x_2 + x_3 = 0$, $\mathcal{B} = (e_1, e_2, e_3)$ la base canonique de $\mathbb{C}^3$ et $\widetilde{\rho_S} \colon \mathfrak{S}_3 \to \mathrm{GL}(\widetilde{H})$ la représentation standard de $\mathfrak{S}_3$ induite par la représentation par permutation

$$\widetilde{\rho_P} \colon \mathfrak{S}_3 \to \mathrm{GL}(\mathbb{C}^3), \qquad \sigma \mapsto (e_i \mapsto e_{\sigma(i)}).$$

Pour tout σ dans $\mathfrak{S}_4$ nous avons

$$\chi_{\rho_3}(\sigma) = \chi_{\widetilde{\rho_S}}(\pi(\sigma))$$

soit

$$\begin{aligned}
&\chi_{\rho_3}(\mathrm{id}) = 2\\
&\chi_{\rho_3}((1\ 2)) = 0\\
&\chi_{\rho_3}((1\ 2)(3\ 4)) = 2\\
&\chi_{\rho_3}((1\ 2\ 3)) = -1\\
&\chi_{\rho_3}((1\ 2\ 3\ 4)) = \chi_{\rho_3}((1\ 4)(1\ 2\ 3)) = 0
\end{aligned}$$

De plus

$$\langle \chi_{\rho_3}, \chi_{\rho_3} \rangle = \frac{1}{24}\Big(1\times2\times2+6\times0\times0+3\times2\times2+8\times(-1)\times(-1)+6\times0\times0\Big) = \frac{1}{24}\Big(4+12+8\Big) = 1$$

autrement dit χ_{ρ_3} est irréductible.

11.3.7. Le groupe $\mathcal{A}_4$. — Rappelons que le groupe $\mathcal{A}_4$ est le sous-groupe des permutations de $\mathfrak{S}_4$ de signature 1. Comme $\mathfrak{S}_4$ a $4! = 24$ éléments, le groupe $\mathcal{A}_4$ est d'ordre 12 ; les éléments de $\mathcal{A}_4$ sont

- ◇ id,
- ◇ les trois produits de deux transpositions

  $$s_2 = (1\ 2)(3\ 4) \qquad s_3 = (1\ 3)(2\ 4) \qquad s_4 = (1\ 4)(2\ 3)$$

  qui sont d'ordre 2,
- ◇ les huit 3-cycles

  $$(1\ 2\ 3) \quad (2\ 3\ 4) \quad (3\ 4\ 1) \quad (4\ 1\ 2) \quad (1\ 3\ 2) \quad (2\ 4\ 3) \quad (3\ 1\ 4) \quad (4\ 2\ 1)$$

  qui sont d'ordre 3.

Nous allons établir la table des caractères de $\mathcal{A}_4$. Il y a plusieurs façons d'arriver au résultat. La manière la plus systématique consiste à déterminer les classes de conjugaison de $\mathcal{A}_4$, construire toutes les représentations irréductibles de $\mathcal{A}_4$ et calculer la valeur de leurs caractères sur les classes de conjugaison. C'est ce que nous allons faire avant de montrer que certains des résultats démontrés précédemment permettent quelques raccourcis.

a) Désignons par t le 3-cycle $(1\ 2\ 3)$. Notons que $t^2 = (1\ 3\ 2)$ et que comme t est d'ordre 3, le sous-groupe $\mathrm{T} = \langle t \rangle = \{\mathrm{id},\, t,\, t^2\}$ de $\mathcal{A}_4$ engendré par t est d'ordre 3.

b) Le sous-groupe $\mathrm{H} = \{\mathrm{id},\, s_2,\, s_3,\, s_4\}$ de $\mathcal{A}_4$ est abélien et distingué dans $\mathcal{A}_4$. En effet un 2-Sylow de $\mathcal{A}_4$ est d'ordre 4 et comme H est d'ordre 4 et contient tous les éléments de $\mathcal{A}_4$ d'ordre divisant 4 cela montre qu'il n'y a qu'un seul 2-Sylow qui est par conséquent distingué dans $\mathcal{A}_4$ et que ce 2-Sylow est H.

De plus tous les éléments de H sont d'ordre divisant 2 donc H est abélien [5].

c) Tout élément de $\mathcal{A}_4$ peut s'écrire de manière unique sous la forme $t^\ell h$ avec $\ell \in \{0,\, 1,\, 2\}$ et $h \in \mathrm{H}$.

Considérons

$$\varphi\colon \mathrm{T} \times \mathrm{H} \to \mathcal{A}_4, \qquad (c, h) \mapsto ch.$$

C'est une injection de $\mathrm{T} \times \mathrm{H}$ dans $\mathcal{A}_4$. En effet soient (c_1, h_1) et (c_2, h_2) dans $\mathrm{T} \times \mathrm{H}$ tels que $c_1 h_1 = c_2 h_2$. Alors $c_2^{-1} c_1 = h_2 h_1^{-1}$; en particulier puisque $c_2^{-1} c_1$ appartient à T et $h_2 h_1^{-1}$ appartient à H, les éléments $c_2 c_1^{-1}$ et $h_2 h_1^{-1}$ appartiennent à $\mathrm{T} \cap \mathrm{H}$. Or $\mathrm{T} \cap \mathrm{H} = \{\mathrm{id}\}$ donc $(c_1, h_1) = (c_2, h_2)$. Remarquons que $|\mathrm{T} \times \mathrm{H}| = |\mathcal{A}_4|$; il en résulte que φ est une bijection ce qui permet de conclure.

d) On peut vérifier que les 3-cycles t et t^2 ne commutent à aucun élément de $\mathrm{H} \smallsetminus \{\mathrm{id}\}$ par un calcul direct.

e) Montrons que les classes de conjugaison de $\mathcal{A}_4$ sont

$$C_1 = \{\mathrm{id}\}, \qquad C_2 = \mathrm{H} \smallsetminus \{\mathrm{id}\}, \qquad C_3 = t\mathrm{H}, \qquad C_4 = t^2\mathrm{H}.$$

Comme dans tout groupe la classe de conjugaison de l'élément neutre a un seul élément C_1 appartient à l'ensemble $\mathrm{conj}(\mathcal{A}_4)$ des classes de conjugaison de $\mathcal{A}_4$.

Soit s un élement de C_2. Soit g un élément de $\mathcal{A}_4$ qui commute à s ; d'après c) nous pouvons écrire g sous la forme $t^a h$, avec $a \in \{0,\, 1,\, 2\}$ et $h \in \mathrm{H}$. Nous avons $t^a h s = s t^a h$ donc $t^a h s h = s t^a h^2$. Comme H est abélien et $h^2 = \mathrm{id}$ nous obtenons $t^a s = s t^a$ ce qui entraîne $a = 0$ (en effet les 3-cycles t et t^2 ne commutent à aucun élément de $\mathrm{H} \smallsetminus \{\mathrm{id}\}$). Le centralisateur de s est donc H et le cardinal de la classe de conjugaison de s est égal à $\frac{|\mathcal{A}_4|}{|\mathrm{H}|} = 3$. Puisqu'un conjugué de s est d'ordre 2, cette classe de conjugaison est incluse dans C_2 et lui est égale pour des raisons de cardinal.

Enfin le centralisateur de t et t^2 est T ; en effet si $t^a h t = t t^a h$ alors $ht = th$ et donc $h = \mathrm{id}$. Il s'ensuit que la classe de conjugaison de t est de cardinal $\frac{|\mathcal{A}_4|}{|\mathrm{T}|} = 4$. Or

$$(t^a h) t (t^a h)^{-1} = t^a h t h^{-1} t^{-a} = t(t^{a-1} h t^{1-a})(t^a h^{-1} t^{-a}) \in t\mathrm{H}$$

5. En effet soit G un groupe dont tous les éléments sont d'ordre divisant 2 ; si g et h sont deux éléments de G, alors d'une part $(gh)^2 = e$ et d'autre part $g^2 h^2 = e$ d'où $(gh)^2 = g^2 h^2$ soit $ghgh = gghh$ et $gh = gh$.

car H est distingué dans $\mathcal{A}_4$. Donc $t^{a-1}ht^{1-a}$ et $t^a h^{-1} t^{-a}$ appartiennent à H. La classe de conjugaison de t est donc contenue dans C_3 et lui est égale pour des raisons de cardinalité. On obtient de la même façon que la classe de conjugaison de t^2 est C_4.

f) Soit $\zeta = \mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}$ une racine primitive 3ième de l'unité. Rappelons que μ_n désigne l'ensemble des racines $n$ième de l'unité. Pour $0 \leq j \leq 2$ on définit $\eta^j \colon \mathcal{A}_4 \to \mu_3$ par $\eta^j(t^a h) = \zeta^{ja}$ si $0 \leq a \leq 2$ et $h \in \mathrm{H}$. Alors $\eta^0 = \mathrm{id}$, η et η^2 sont des caractères linéaires distincts de $\mathcal{A}_4$.

En effet si $0 \leq a,\, b \leq 2$ et si $h,\, g$ appartiennent à H, alors $t^a h t^b g = t^{a+b}(t^{-b} h t^b) g$. Puisque H est distingué dans $\mathcal{A}_4$, on a $t^{-b} h t^b$ appartient à H et donc $(t^{-b} h t^b) g$ appartient à H. De plus $\eta^j(t^a h t^b g) = \zeta^{j(a+b)} = \zeta^{ja}\zeta^{jb} = \eta^j(t^a h)\eta^j(t^b g)$.

g) Soit V la représentation de permutation associée à l'action naturelle de $\mathcal{A}_4$ sur $\{1,\, 2,\, 3,\, 4\}$. Rappelons que cette représentation est $\mathbb{C}^4$ muni de l'action de $\mathcal{A}_4$ définie dans la base canonique $(e_1,\, e_2,\, e_3,\, e_4)$ par $g(e_i) = e_{g(i)}$. L'hyperplan W d'équation $x_1+x_2+x_3+x_4 = 0$ est stable par $\mathcal{A}_4$ et la représentation obtenue est irréductible de caractère :

$$\chi_W(\mathrm{id}) = 3, \qquad \chi_W(g) = -1 \text{ si } g \in \mathrm{H} \smallsetminus \{\mathrm{id}\}, \qquad \chi_W(g) = 0 \text{ si } g \notin \mathrm{H}.$$

En effet la représentation V se décompose sous la forme $V' \oplus W$ où V' est la droite engendrée par $e_1 + e_2 + e_3 + e_4$. Puisque V est une repésentation de permutation $\chi_V(g)$ est le nombre de points fixes de g agissant sur $\{1,\, 2,\, 3,\, 4\}$. Nous avons donc

$$\chi_V(\mathrm{id}) = 4, \qquad \chi_V(g) = 0 \text{ si } g \in \mathrm{H} \smallsetminus \{\mathrm{id}\}, \qquad \chi_V(g) = 1 \text{ si } g \notin \mathrm{H}.$$

Nous en déduisons le caractère de W car $\chi_V = \chi_{V'} + \chi_W$ et $\chi_{V'}(g) = 1$ pour tout $g \in \mathcal{A}_4$ (en effet $e_1 + e_2 + e_3 + e_4$ est fixe par $\mathcal{A}_4$ donc $\chi_{V'} \simeq \chi_{\rho_{\mathrm{triv}}}$). Par suite

$$\chi_W(\mathrm{id}) = 3, \qquad \chi_W(g) = -1 \text{ si } g \in \mathrm{H} \smallsetminus \{\mathrm{id}\}, \qquad \chi_W(g) = 0 \text{ si } g \notin \mathrm{H}.$$

Montrons que W est irréductible. Commençons par constater que si g appartient à $\mathcal{A}_4$ et si $v = (x_1, x_2, x_3, x_4)$ appartient à $\mathbb{C}^4$, alors

$$g \cdot v = x_1 e_{g(1)} + x_2 e_{g(2)} + x_3 e_{g(3)} + x_4 e_{g(4)} = (x_{g^{-1}(1)}, x_{g^{-1}(2)}, x_{g^{-1}(3)}, x_{g^{-1}(4)}).$$

Supposons que v appartienne à $W \smallsetminus \{0\}$; soit W' le sous-espace de W engendré par les $g \cdot v$ pour $g \in \mathcal{A}_4$. Montrons que $W = W'$ quel que soit v. Il existe donc $i \neq j$ tel que $x_i \neq x_j$; sans perdre de généralité on peut supposer que $x_1 \neq x_2$. L'image de v par le 3-cycle t est alors (x_3, x_1, x_2, x_4) ; il s'ensuit que W' qui contient $t \cdot v$ et v contient $w = t \cdot v - v = (x_3 - x_1, x_1 - x_2, x_2 - x_3, 0)$. Le sous-espace W' contient aussi $w + g \cdot w$ si $g = (1\ 3)(2\ 4)$, et comme

$$w + g \cdot w = (x_1 - x_2)(e_2 + e_4 - e_1 - e_3)$$

et $x_1 - x_2 \neq 0$ il contient le vecteur $f_1 = e_1 - e_2 + e_3 - e_4$. Il contient donc aussi les images $f_2 = e_1 + e_2 - e_3 - e_4$ et $f_3 = e_1 - e_2 - e_3 + e_4$ de f_1 par les 3-cycles $(2\ 4\ 3)$ et $(2\ 3\ 4)$. Puisque f_1, f_2 et f_3 forment une base de W nous avons l'égalité recherchée $W = W'$.

h) Le groupe $\mathcal{A}_4$ compte quatre classes de conjugaison, il a donc quatre représentations irréductibles à isomorphismes près qui sont les trois caractères linéaires ρ_{triv}, η et η^2 et la représentation W de dimension 3. Les valeurs des caractères de ces représentations ont été calculées ci-dessus d'où la table des caractères de $\mathcal{A}_4$:

	C_1	C_2	C_3	C_4
$\chi_{\rho_{\text{triv}}}$	1	1	1	1
χ_η	1	1	ζ	ζ^2
χ_{η^2}	1	1	ζ^2	ζ
χ_W	3	-1	0	0

Remarque 11.3.10. — Le groupe dérivé $D(\mathcal{A}_4)$ de $\mathcal{A}_4$ est isomorphe au groupe de Klein $\mathcal{K}$. Par suite l'abélianisé de $\mathcal{A}_4$ qui est le quotient $\mathcal{A}_4/\mathcal{K}$ est d'ordre $\frac{12}{4} = 3$. Il en résulte que $\mathcal{A}_4$ possède $\frac{12}{4} = 3$ caractères de degré 1. Notons $\mathrm{Irr}(\mathcal{A}_4)$ l'ensemble des représentations irréductibles de $\mathcal{A}_4$. La formule de la Proposition 11.2.2 assure que

$$12 = |\mathcal{A}_4| = 1 + 1 + 1 + \sum_{\substack{\rho \in \mathrm{Irr}(\mathcal{A}_4) \\ \deg \rho > 1}} (\deg \rho)^2;$$

soit

$$9 = \sum_{\substack{\rho \in \mathrm{Irr}(\mathcal{A}_4) \\ \deg \rho > 1}} (\deg \rho)^2.$$

Nous en déduisons que $\{\rho \in \mathrm{Irr}(\mathcal{A}_4) \mid \deg \rho > 1\}$ est constitué d'une unique représentation de degré 3.

Remarque 11.3.11. — On peut utiliser la Proposition 11.2.2 pour démontrer l'irréductibilité de W :

$$\langle \chi_W, \chi_W \rangle = \frac{1}{12}(3^2 + 3 \times (-1)^2 + 8 \times 0) = 1$$

donc W est irréductible.

Remarque 11.3.12. — Supposons que nous ayons construit des représentations ρ_{triv}, η, η^2 et W dont les caractères prennent les valeurs de la table sur C_1, C_2, C_3 et C_4 mais qu'on ne sache pas quelles sont les classes de conjugaison de $\mathcal{A}_4$. On peut en déduire que ces classes sont exactement C_1, C_2, C_3 et C_4 ce qui permet de se passer des points d) et e) ci-dessus. En effet comme $1^2 + 1^2 + 1^2 + 3^2 = 12$ la formule de la Proposition 11.2.2 assure que les représentations irréductibles de G sont ρ_{triv}, η, η^2 et W et donc que $\mathcal{A}_4$ a quatre classes de conjugaison (Corollaire 11.2.1). Or si $i \neq j$, il existe une représentation irréductible de $\mathcal{A}_4$ prenant des valeurs distinctes sur C_i et C_j. Comme une représentation irréductible de $\mathcal{A}_4$ est constante sur une classe de conjugaison, nous en déduisons que si C est une classe de conjugaison dans $\mathcal{A}_4$ il existe $1 \leq i(C) \leq 4$ tel que $C \subset C_{i(C)}$. Les éléments de C formant une partition de $\mathcal{A}_4$

l'application $C \mapsto i(C)$ est surjective ; les deux ensembles ayant le même nombre d'éléments elle est bijective. De plus $C_{i(C)} = C$ sinon un élément de $C_{i(C)} \smallsetminus C$ ne serait pas dans la réunion des classes de conjugaison. Ainsi les classes de conjugaison de $\mathcal{A}_4$ sont les C_i.

Remarque 11.3.13. — Notons $\mathrm{Irr}(\mathcal{A}_4)$ l'ensemble des représentations irréductibles de $\mathcal{A}_4$. Supposons W construite. La formule de la Proposition 11.2.2 assure que

$$12 = |\mathcal{A}_4| = 9 + \sum_{\rho \in \mathrm{Irr}(\mathcal{A}_4) \smallsetminus \{W\}} (\deg \rho)^2;$$

de plus il y a une unique manière décrire 3 comme une somme de carrés. Par conséquent le groupe $\mathcal{A}_4$ a trois caractères linéaires distincts. Autrement dit le groupe $\widehat{\mathcal{A}_4}$ des caractères linéaires de $\mathcal{A}_4$ est d'ordre 3 donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$; en particulier il est cyclique et si on note η un générateur les éléments de $\widehat{\mathcal{A}_4}$ sont η, η^2 et le caractère trivial. Puisque η est d'ordre 3 il est à valeurs dans le groupe μ_3 des racines 3-ièmes de l'unité et son image étant un sous-groupe de μ_3 non réduit à l'identité c'est μ_3 tout entier. En particulier l'image de η est d'ordre 3 et son noyau d'ordre $\frac{12}{3} = 4$. Par ailleurs $\mathrm{H} \subset \ker \chi$ car l'unique élément de μ_3 d'ordre divisant 2 est 1. Il s'ensuit que $\ker \chi = \mathrm{H}$ ce qui permet de donner une autre démonstration de b). Enfin comme t n'appartient pas à H nous avons $\eta(t) \neq 1$ et donc $\eta(t) = \rho$ ou $\eta(t) = \rho^2$. Quitte à remplacer η par η^2 nous pouvons supposer que $\eta(t) = \rho$. Alors

$$\eta(g) = \begin{cases} 1 \text{ si } g \in \mathrm{H} = C_1 \cup C_2 \\ \rho \text{ si } g \in C_3 = t\mathrm{H} \\ \rho^2 \text{ si } g \in C_4 = t^2\mathrm{H} \end{cases}$$

Ceci permet en utilisant la Remarque 11.3.12 de compléter la table des caractères de $\mathcal{A}_4$ sans avoir utilisé un seul des points a)-e) au sujet de la structure de $\mathcal{A}_4$, ni le point f).

11.3.8. Le groupe $\mathcal{A}_5$. — Nous allons établir la table des caractères du groupe $\mathcal{A}_5$ d'ordre 60.

11.3.8.1. *Classes de conjugaison de $\mathcal{A}_5$.* — Le groupe $\mathcal{A}_5$ a cinq classes de conjugaison (Exemple **??**) :

- ◇ la classe C_1 de l'élément neutre, de cardinal 1 ;
- ◇ la classe C_3 des 3-cycles (d'ordre 3), de cardinal 20 ;
- ◇ la classe $C_{2,2}$ des produits de deux transpositions de supports disjoints (d'ordre 2), de cardinal 15 ;
- ◇ deux classes C_5 et C_5' de cardinal 12 dont la réunion est l'ensemble des 5-cycles (d'ordre 5). De plus si t est un 5-cycle, alors t et t^2 ne sont pas dans la même classe. Désignons par exemple par C_5 la classe de $t_0 = (1\ 2\ 3\ 4\ 5)$ et par C_5' la classe de $t_0' = (1\ 3\ 5\ 2\ 4)$.

11.3.8.2. *Table de caractères.* — Le nombre de représentations irréductibles de $\mathcal{A}_5$ est égal au nombre de ses classes de conjugaison, c'est-à-dire 5. Par ailleurs tout groupe admet la représentation triviale de dimension 1 comme représentation irréductible, donc $\mathcal{A}_5$ aussi.

Désignons par d_2, d_3, d_4 et d_5 les degrés des représentations irréductibles de $\mathcal{A}_5$ distinctes de la représentation triviale. Nous avons

$$1 + d_2^2 + d_3^2 + d_4^2 + d_5^2 = |\mathcal{A}_5|$$

soit

$$d_2^2 + d_3^2 + d_4^2 + d_5^2 = 59.$$

Or 59 s'écrit d'une seule manière comme somme de 4 carrés : $3^2 + 3^2 + 4^2 + 5^2 = 59$ donc $\{d_2, d_3, d_4, d_5\} = \{3, 3, 4, 5\}$.

Notons U la représentation de dimension 4, V celle de dimension 5 et W, W' celles de dimension 3. Nous avons alors le début de la table de caractères :

	C_1	C_3	$C_{2,2}$	C_5	C'_5
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1	1	1
χ_U	4				
χ_V	5				
χ_W	3				
$\chi_{W'}$	3				

Soit T la matrice 5×5 définie par la table des caractères de $\mathcal{A}_5$. Désignons par T^* l'adjointe de T. D'après (11.3.2) la matrice TT^* est la matrice diagonale dont le coefficient sur la colonne correspondant à la classe C est $\frac{|\mathrm{G}|}{|C|}$. C'est donc la matrice diagonale de coefficients $\frac{60}{1} = 60$, $\frac{60}{20} = 3$, $\frac{60}{15} = 4$, $\frac{60}{12} = 5$ et $\frac{60}{12} = 5$.

Le coefficient diagonal de TT^* sur la ligne correspondant à la classe C est aussi égal à $\sum_{\chi \in \mathrm{Irr}(\mathcal{A}_5)} |\chi(C)|^2$ où $\mathrm{Irr}(\mathcal{A}_5)$ désigne l'ensemble des représentations irréductibles de $\mathcal{A}_5$. D'après ce qui précède ce coefficient est majoré par 5 si $C \neq C_1$. Par conséquent $|\chi(C)| < 3$ pour tout $\chi \in \mathrm{Irr}(\mathcal{A}_5)$ si $C \neq C_1$. Par ailleurs $|\chi(e)| \geq 3$ si χ appartient à $\mathrm{Irr}(\mathcal{A}_5) \smallsetminus \{\rho_{\mathrm{triv}}\}$. Par suite $|\chi(g)| \neq |\chi(e)|$ pour tout $\chi \in \mathrm{Irr}(\mathcal{A}_5) \smallsetminus \{\rho_{\mathrm{triv}}\}$ et $g \neq e$.

Montrons que $\mathcal{A}_5$ est simple. Raisonnons par l'absurde, *i.e.* supposons que $\mathcal{A}_5$ ne soit pas simple. Alors il existe un morphisme de groupes surjectif $f\colon \mathcal{A}_5 \to \mathrm{H}$ tel que $\mathrm{H} \neq \{e\}$ et $\ker f \neq \{e\}$. Comme $H \neq \{e\}$ il existe une représentation irréductible V de H distincte de la représentation triviale (dernière égalité de la Proposition 11.2.2). Mais alors $\rho_V \circ f$ est un morphisme de groupes de $\mathcal{A}_5$ dans $\mathrm{GL}(V)$ ce qui permet de considérer V comme une représentation de $\mathcal{A}_5$. Puisque les images de $v \in V$ sous l'action de $\mathcal{A}_5$ sont les mêmes que celles sous l'action de H la représentation V de $\mathcal{A}_5$ est irréductible. De plus pour tout $g \in \ker f$ nous avons $\chi_V(g) = \chi_V(e)$: contradiction avec ce qui précède.

Soit U' la représentation de permutation de $\mathcal{A}_5$ associée à l'action naturelle de $\{1, 2, \ldots, 5\}$ (*i.e.* $g(e_i) = e_{g(i)}$ si g appartient à $\mathcal{A}_5$ et si $1 \leq i \leq 5$). Soit U l'hyperplan de U' d'équation $x_1 + x_2 + \ldots + x_5 = 0$.

Nous avons

$$g \cdot (x_1 e_1 + x_2 e_2 + \ldots + x_5 e_5) = x_1 e_{g(1)} + x_2 e_{g(2)} + \ldots + x_5 e_{g(5)}$$

et donc $g \cdot (x_1, x_2, \ldots, x_5) = (x_{g^{-1}(1)}, x_{g^{-1}(2)}, \ldots, x_{g^{-1}(5)})$. Nous en déduisons le fait que les coordonnées de $g \cdot x$ sont les mêmes que celles de x à permutation près, et donc que les sommes des coordonnées de x et de $g \cdot x$ sont les mêmes. Il s'ensuit la stabilité de U sous l'action de $\mathcal{A}_5$.

Pour $x \in U$ nous désignons par U_x le sous-espace de U engendré par les $g \cdot x$ pour $g \in \mathcal{A}_5$. La stabilité de U_x par $\mathcal{A}_5$ résulte de ce que $h \cdot (g \cdot x) = hg \cdot x$ et donc que le translaté d'une combinaison linéaire de translatés de x est encore une combinaison linéaire de translatés de x. Soit $x = (x_1, x_2, \ldots, x_5)$. Comme x appartient à U il existe $i \neq j$ tels que $x_i \neq x_j$. Quitte à remplacer x par $h \cdot x$ avec $h \in \mathrm{A}_5$ vérifiant $h(1) = i$ et $h(2) = j$ nous pouvons supposer que $i = 1$ et $j = 2$. Soit $g = (1\ 3\ 2)$; alors $g \cdot x = (x_2, x_3, x_1, x_4, x_5)$ et $y = g \cdot x - x = (y_1, y_2, y_3, 0, 0)$ avec $y_1 = x_2 - x_1 \neq 0$. Puisque y appartient à U_x il existe un élément non nul y de U_x ayant deux coordonnées nulles.

Puisque y appartient à U_x, les trois coordonnées non nulles de y ne sont pas toutes égales et il existe $i \neq j$ tels que $y_i \neq y_j$. Comme ci-dessus nous pouvons supposer que $i = 1$, $j = 2$ et $y_4 = y_5 = 0$. Soit $g' = (1\ 2)(4\ 5)$. Soit $w = g' \cdot y - y$. Alors w appartient à U_x et $w = (y_2 - y_1, y_1 - y_2, 0, 0, 0)$ est non nul et a trois coordonnées nulles.

Montrons désormais que U est irréductible. Il s'agit de montrer que si $x \in U$ non nul, alors le sous-espace U_x de U engendré par les $g \cdot x$ est égal à U. Or U_x contient un vecteur de la forme $e_i - e_j$, avec $i \neq j$. Comme

$$g \cdot (e_i - e_j) = e_{g(i)} - e_{g(j)}$$

et comme pour tout couple $i' \neq j'$ il existe $g \in \mathcal{A}_5$ tel que $g(i) = i'$ et $g(j) = j'$ on obtient que U_x contient $e_i - e_j$ pour tout couple $i \neq j$. Il contient donc en particulier la base $e_i - e_1$, pour $2 \leq i \leq 5$, de U ce qui permet de conclure.

Déterminons les caractères de U et U'. Puisque U' est une représentation de permutation $\chi_{U'}(g)$ est le nombre de points fixes de $g \in \mathcal{A}_5$ agissant sur $\{1, 2, \ldots, 5\}$. Par suite

$$\chi_{U'}(C_1) = 5, \qquad \chi_{U'}(C_3) = 2, \chi_{U'}(C_{2,2}) = 1, \chi_{U'}(C_5) = 0, \chi_{U'}(C_5') = 0.$$

La représentation U' est la somme directe de U et de la droite engendrée par $e_1 + e_2 + \ldots + e_5$ sur laquelle $\mathcal{A}_5$ agit trivialement. Nous avons donc $\chi_{U'}(g) = \chi_U(g) + \chi_{\rho_{\mathrm{triv}}}(g)$ d'où $\chi_U(g) = \chi_{U'}(g) - 1$ pour tout $g \in \mathcal{A}_5$, *i.e.*

$$\chi_U(C_1) = 4, \qquad \chi_U(C_3) = 1, \qquad \chi_U(C_{2,2}) = 0, \qquad \chi_U(C_5) = -1, \qquad \chi_U(C_5') = -1.$$

Notons au passage qu'on retrouve que U est irréductible :

$$\langle \chi_U, \chi_U \rangle = \frac{1}{60}\Big(4^2 + 20 \times 1^2 + 15 \times 0^2 + 12 \times (-1)^2 + 12 \times (-1)^2\Big) = 1.$$

11.3.9. Le groupe $\mathfrak{S}_5$. —

11.4. Groupes abéliens finis et représentations linéaires des groupes finis

, [**Col11**, p. 132-134]

On propose une preuve de la partie « existence » du théorème de structure des groupes abéliens finis reposant sur les notions d'exposant d'un groupe et de dual d'un groupe.

Soit G un groupe fini. Notons $\widehat{\mathrm{G}}$ l'ensemble des caractères linéaires de G. Notons que $\widehat{\mathrm{G}}$ est un groupe abélien pour la multiplication des caractères linéaires : si χ_1, χ_2 appartiennent à $\widehat{\mathrm{G}}$, alors

$$\chi_1(g)\chi_2(g) = \chi_1\chi_2(g) \qquad \forall\, g \in \mathrm{G};$$

on peut donc considérer le groupe $\widehat{\widehat{\mathrm{G}}}$ de ses caractères linéaires. La formule de multiplication ci-dessus montre que si $g \in \mathrm{G}$, alors $\chi \mapsto \chi(g)$ est un caractère linéaire de $\widehat{\mathrm{G}}$, d'où une application naturelle

$$\iota\colon \mathrm{G} \to \widehat{\widehat{\mathrm{G}}}$$

définie par

$$\iota(g)(\chi) = \chi(g).$$

Cette application est un morphisme de groupes puisque si g, h appartiennent à G alors

$$\iota(gh)(\chi) = \chi(gh) = \chi(g)\chi(h) = (\iota(g))(\chi)(\iota(h))(\chi) \qquad \forall\, \chi \in \widehat{\mathrm{G}}$$

et donc $\iota(gh) = \iota(g)\iota(h)$.

Proposition 11.4.1

Si G est un groupe fini, alors $\iota\colon \mathrm{G} \to \widehat{\widehat{\mathrm{G}}}$ est un isomorphisme de groupes.

Définition 11.4.1

Soit G un groupe abélien fini. L'exposant $\exp(\mathrm{G})$ de G est le maximum des ordres des éléments de G.

Lemme 11.4.1

Si G est un groupe abélien fini, alors G et $\widehat{\mathrm{G}}$ ont même exposant.

Démonstration. — Si H est un groupe abélien fini, on note $N(\mathrm{H})$ son exposant.

Si χ est un élément de $\widehat{\mathrm{H}}$, alors pour tout $g \in \mathrm{G}$

$$\chi^{N(\mathrm{H})}(g) = \chi(g)^{N(\mathrm{H})} = \chi(g^{N(\mathrm{H})}) = \chi(e_{\mathrm{G}}) = e_{\mathrm{G}}$$

et donc $\chi^{N(\mathrm{H})} = \mathrm{id}$. Il en résulte que l'exposant de $\widehat{\mathrm{H}}$ divise celui de H.

En particulier l'exposant de $\widehat{\mathrm{G}}$ divise celui de G et $N(\widehat{\mathrm{G}}) \subseteq N(\mathrm{G})$. De même l'exposant de $\widehat{\widehat{\mathrm{G}}}$ divise celui de $\widehat{\mathrm{G}}$ et $N(\widehat{\widehat{\mathrm{G}}}) \subseteq N(\widehat{\mathrm{G}})$. D'où

$$N(\widehat{\widehat{\mathrm{G}}}) \subseteq N(\widehat{\mathrm{G}}) \subseteq N(\mathrm{G}) \tag{11.4.1}$$

Mais G et $\widehat{\widehat{\mathrm{G}}}$ sont isomorphes donc $N(\widehat{\widehat{\mathrm{G}}}) = N(\mathrm{G})$ et (11.4.1) implique $N(\widehat{\widehat{\mathrm{G}}}) = N(\widehat{\mathrm{G}}) = N(\mathrm{G})$. □

Théorème 11.4.1

Soit G un groupe abélien fini. Il existe $r \in \mathbb{N}$ et des entiers $N_1, N_2, \ldots, N_r$ où N_r est l'exposant de G et N_{i+1} divise N_i si $i \leq r-1$ tels que

$$\mathrm{G} \simeq \oplus_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}.$$

Démonstration (*par récurrence sur* $|\mathrm{G}|$). — Si $|\mathrm{G}| = 1$, alors $r = 0$.

Supposons donc que $|\mathrm{G}| > 1$. Posons $N = N_1 = \exp(\mathrm{G})$. Alors $\chi(g)$ est une racine N-ième de l'unité pour tous $\chi \in \widehat{\mathrm{G}}$ et $g \in \mathrm{G}$. Notons que $N = \exp(\widehat{\mathrm{G}})$ (Lemme 11.4.1). Il existe donc χ_1 d'ordre N et comme $\chi_1(\mathrm{G})$ est un sous-groupe du groupe cyclique $\mu_N = \{z \in \mathbb{C} \mid z^N = 1\}$, c'est μ_N tout entier. Il existe donc $g_1 \in \mathrm{G}$ tel que $\chi_1(g_1) = \exp\left(\frac{2\mathrm{i}\pi}{N}\right)$. L'ordre de g_1 divise N (définition de $\exp(\mathrm{G})$) ; ainsi g_1 est d'ordre N et le sous-groupe $\mathrm{H}_1 = \langle g_1 \rangle$ de G est isomorphe à $\mathbb{Z}/N\mathbb{Z}$.

Montrons que $\mathrm{G} = \mathrm{H}_1 \oplus \ker \chi_1$: χ_1 induit un isomorphisme de H_1 sur μ_N car χ_1 est surjectif et $|\mathrm{H}_1| = |\mu_N| = N$. Notons $\alpha \colon \mu_N \to \mathrm{H}_1$ son inverse. Soit $g \in \mathrm{G}$; alors $a = \alpha(\chi_1(g)) \in \mathrm{H}_1$ et $b = a^{-1}g$ vérifie

$$\chi_1(b) = \chi_1(a^{-1}g) = \chi_1(a^{-1})\chi_1(g) = \chi_1(a)^{-1}\chi_1(g) = 1.$$

Ainsi b appartient à $\ker \chi_1$. On peut donc écrire tout élément g de G sous la forme ab avec $a \in \mathrm{H}_1$ et $b \in \ker \chi_1$.

Puisque χ_1 est injectif sur H_1 nous avons $\mathrm{H}_1 \cap \ker \chi_1 = \{1\}$. Il en résulte que $\mathrm{G} = \mathrm{H}_1 \oplus \ker \chi_1$.

Comme l'exposant de $\ker \chi_1 \subset \mathrm{G}$ divise l'exposant de G, l'hypothèse de récurrence assure que

$$\ker \chi_1 \simeq \bigoplus_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$$

et donc que

$$\mathrm{G} = \mathrm{H}_1 \oplus \ker \chi_1 = \mathbb{Z}/N\mathbb{Z} \oplus \ker \chi_1 \simeq \mathbb{Z}/N\mathbb{Z} \oplus \bigoplus_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$$

□

11.5. Applications

11.5.1. Caractères et sous-groupes normaux de $\mathfrak{S}_4$, [CG13, p. 364]**, [Szp09**, p. 422]**, [Ale99]**, **[CG15**, F. 18 p. 490, p. 523]**, [RW10**, p. 55, Exercice I.1.51 p. 70, p. 534]**, [Pey04**, p. 229-232]**.** —

Il y a plusieurs manières d'aborder ce développement donc bien expliciter lors de son plan ce que l'on va faire. Par exemple « Je vais montrer que le groupe des rotations préservant un cube est isomorphe à $\mathfrak{S}_4$; puis à l'aide de la formule de Burnside je vais dénombrer les coloriages d'un cube avec c couleurs ». Ou encore « Je vais dresser la liste des classes de conjugaison de $\mathfrak{S}_4$ en donnant leur interprétation comme isométries du cube, dresser la table des caractères de $\mathfrak{S}_4$ en utilisant des résultats mentionnés dans le plan et illustrer le fait que la table des caractères permet de retrouver tous les sous-groupes distingués propres (ici $\mathcal{K} \triangleleft \mathfrak{S}_4$ et $\mathcal{A}_4 \triangleleft \mathfrak{S}_4$) ».

11.5.1.1. *Isomorphisme.* —

Théorème 11.5.1

Le groupe $\mathrm{Isom}^+(\text{cube})$ des rotations de $\mathbb{R}^3$ préservant un cube est isomorphe au groupe symétrique $\mathfrak{S}_4$.

Remarque 11.5.1. — Si g est une isométrie qui fixe trois sommets du cube qui sont deux à deux non opposés, alors $g = \mathrm{id}$ (car ces sommets forment une base de l'espace vectoriel d'origine le centre du cube).

Démonstration. — Les quatre diagonales du cube sont caractérisées comme les couples de sommets réalisant la distance maximale entre deux sommets. Il en résulte que le groupe $\mathrm{Isom}^+(\text{cube})$ agit sur l'ensemble $\{D_1, D_2, D_3, D_4\}$ des grandes diagonales ; le morphisme associé est

$$\phi\colon \mathrm{Isom}^+(\text{cube}) \to \mathfrak{S}_4, \qquad f \mapsto \sigma$$

tel que $f(D_i) = D_{\sigma(i)}$ pour tout $1 \leq i \leq 4$.

Montrons que ϕ est injectif. Supposons que f appartient à $\ker \phi$, *i.e.* que f préserve chaque diagonale D_i. Notons que f ne peut pas échanger les deux sommets de chaque diagonale car sinon $f = -\mathrm{id}$ par la Remarque 11.5.1 appliquée à $-\mathrm{id} \circ f$. Il existe donc deux sommets d'une grande diagonale, disons A_1 et A_1' dans D_1 quitte à renuméroter, qui sont fixés par f. Mais pour chaque autre diagonale D_i les sommets A_i et A_i' ne sont pas équidistants de A_1, donc fixés également ; finalement f fixe tous les sommets et $f = \mathrm{id}$ (Remarque 11.5.1).

Finalement montrons que ϕ est surjectif. Les transpositions engendrent $\mathfrak{S}_4$, il suffit donc de montrer que les six transpositions de $\mathfrak{S}_4$ sont dans l'image. Or les transpositions correspondent aux images des rotations d'angle π et d'axe passant par les milieux des arêtes opposées. □

Remarque 11.5.2. — Nous pourrions aussi montrer d'abord que $\mathrm{Isom}^+(\text{cube})$ et $\mathfrak{S}_4$ ont même ordre (24). Le dénombrement se fait en termes de « drapeaux » du cube ([**Szp09**, p. 414]).

Nous pouvons alors nous contenter de montrer l'injectivité ou la surjectivité du morphisme ϕ introduit dans la démonstration du Théorème 11.5.1.

11.5.1.2. *Table de caractères,* [**CG15**, F. 18 p. 490, p. 523]. — Il y a 5 classes de conjugaison dans le groupe $\mathfrak{S}_4$, voici leur interprétation en termes d'isométries directes préservant un cube (l'action sur les 4 grandes diagonales permet l'identification avec $\mathfrak{S}_4$) ainsi que leur cardinal :

- ◇ classe du neutre de cardinal 1 ;
- ◇ classe des transpositions, rotations d'angle π d'axe passant par les milieux de deux arêtes opposées, de cardinal 6 ;
- ◇ classe des 3-cycles, rotations d'angle $\pm\frac{2\pi}{3}$ d'axe passant par les deux sommets opposés, de cardinal 8 ;
- ◇ classe des 4-cycles, rotations d'angle $\pm\frac{\pi}{2}$ d'axe passant par les milieux de faces opposées, de cardinal 6 ;
- ◇ classe des double transpositions, carrés des précédentes (rotations d'angle π d'axe passant par les milieux des faces opposées).

La théorie générale assure donc qu'il y a 5 représentations irréductibles de $\mathfrak{S}_4$, les voici ainsi que leurs caractères :

- ◇ la représentation triviale ;
- ◇ la représentation signature χ_{sgn} ;
- ◇ la représentation ρ_3 de degré 3 provenant de la représentation par permutation de $\mathfrak{S}_4$ sur $\mathbb{C}^4$ modulo la droite invariante ;
- ◇ la même tordue par la signature (on pourra justifier l'irréductibilité) ;
- ◇ la représentation ρ_2 de degré 2 provenant de la représentation par permutation de $\mathfrak{S}_3$, via le morphisme $\mathfrak{S}_4 \to \mathfrak{S}_3$ ($\mathfrak{S}_4$ agit sur les paires de faces opposées du cube).

	$C(\mathrm{id})$	$C((1\ 2))$	$C((1\ 2)(3\ 4))$	$C((1\ 2\ 3))$	$C((1\ 2\ 3\ 4))$
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1
χ_{ρ_3}	3	1	-1	0	-1
$\chi_{\mathrm{sgn}} \otimes \chi_{\rho_3}$	3	-1	-1	0	1
χ_{ρ_2}	2	0	2	-1	0

Les deuxième et cinquième lignes donnent des sous-groupes distingués non triviaux, respectivement $\mathcal{A}_4$ et $\mathcal{K}$.

11.5.2. Le cube et les représentations de $\mathfrak{S}_4$, [CG15, p. 490, p. 493], [Pey04, p. 230-232]. —

Illustrer sur le cas des rotations préservant un cube comme retrouver les sous-groupes distingués à partir d'une table de caractères.

11.5.2.1. *Représentation par permutation.* — Pour construire une table de caractères nous avons besoin d'un procédé de construction de représentations irréductibles. Les représentations par permutations « font souvent l'affaire ».

***Exemple 11.5.1* (Représentation par permutations).** — Soit G un groupe fini agissant sur un ensemble fini X. Notons $\mathbb{C}X$ l'espace vectoriel muni de la base canonique e_x indexée par X. Faisons agir G sur $\mathbb{C}X$ en posant

$$\rho(g)(e_x) = e_{g\cdot x}.$$

On appelle ρ la représentation par permutations (associée à l'action de G sur X). Remarquons que la somme $s = \sum_{x\in X} e_x$ est invariante. Désignons par V_X le quotient $\mathbb{C}X/\mathbb{C}s$ qui s'identifie à un sous-espace supplémentaire stable de $\mathbb{C}s$.

—

Proposition 11.5.1

Soit G un groupe agissant sur un ensemble fini X. Soit V_X le quotient de la représentation par permutation associée (notations de l'Exemple 11.5.1).

1. Le caractère χ de la représentation est donné par
$$\chi(g) = |\mathrm{Fix}(g)| - 1.$$
2. Si G agit deux fois transitivement sur X, alors V_X est irréductible.

Démonstration. —

1. Le caractère de la représentation par permutation avant quotient est $g \mapsto |\mathrm{Fix}(g)|$: un 1 sur la diagonale d'une matrice de permutations correspoond à un point fixe. Par ailleurs la représentation triviale sur $\mathbb{C}s$ est de caratère identiquement 1. On conclut par additivité du caractère en écrivant $\mathbb{C}X = V_X \oplus \mathbb{C}s$ (matriciellement on calcule la trace d'une matrice diagonale par blocs de taille $n-1$ et 1).
2. D'après ce qui précède nous avons
$$\langle \chi, \chi\rangle = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} \left(|\mathrm{Fix}(g)| - 1\right)^2 = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} |\mathrm{Fix}(g)|^2 - 2\frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} |\mathrm{Fix}(g)| + 1$$
L'action étant transitive la formule de Burnside assure que
$$1 = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} |\mathrm{Fix}(g)|.$$

L'action étant doublement transitive l'action diagonale de G sur $X \times X$ admet deux orbites : la diagonale et son complément. Par suite la formule de Burnside appliquée à cette action entraîne

$$2 = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |(X \times X)^g| = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|^2.$$

Par conséquent $\langle \chi, \chi \rangle = 2 - 2 + 1 = 1$ ce qui donne l'irréductibilité attendue.

□

11.5.2.2. *La table des caractères de* $\mathfrak{S}_4$. — Le groupe des isométries directes (*i.e.* les rotations) de $\mathbb{R}^3$ préservant un cube est isomorphe à $\mathfrak{S}_4$ via l'action sur les grandes diagonales (Proposition 12.3.4).

La table de caractères de $\mathfrak{S}_4$ est

	$C(\mathrm{id})$	$C((1\ 2))$	$C((1\ 2)(3\ 4))$	$C((1\ 2\ 3))$	$C((1\ 2\ 3\ 4))$
$\chi_{\rho_{\mathrm{triv}}}$	1	1	1	1	1
$\chi_{\mathrm{perm_tetr}}$	1	-1	1	1	-1
$\chi_{\mathrm{perm_diag}}$	3	1	-1	0	-1
$\chi_{\mathrm{perm_tetr}} \otimes \chi_{\mathrm{perm_diag}}$	3	-1	-1	0	1
via $\mathfrak{S}_3$	2	0	2	-1	0

où

- ◇ $\chi_{\mathrm{perm_tetr}}$ est la représentation irréductible de degré 1 obtenue par permutation des deux tétraèdres inscrits dans le cube, c'est aussi la signature,
- ◇ $\chi_{\mathrm{perm_diag}}$ est la représentation irréductible de degré 3 obtenue par permutation des quatre diagonales,
- ◇ la représentation $\chi_{\mathrm{perm_tetr}} \otimes \chi_{\mathrm{perm_diag}}$ correspond à la représentation $\mathfrak{S}_4 \simeq \mathrm{Isom}^+(\mathrm{cube}) \subset \mathrm{SO}(3, \mathbb{R})$ dont on est parti,
- ◇ via $\mathfrak{S}_3$ est la représentation irréductible de degré 2 obtenue par permutation des trois paires de faces opposées.

Proposition 11.5.2: Résumé des propriétés d'une table de caractères

1. Chaque ligne distincte de la représentation triviale a « somme nulle » :
$$\sum_{g\in \mathrm{G}} \chi(g) = 0.$$
2. Deux lignes distinctes sont orthogonales :
$$\sum_{g\in \mathrm{G}} \overline{\chi(g)}\chi'(g) = 0.$$
3. La « norme » d'une ligne correspond à l'ordre du groupe (caractérise l'irréductibilité) :
$$\sum_{g\in \mathrm{G}} \overline{\chi(g)}\chi(g) = |\mathrm{G}|.$$
4. La somme des carrés des degrés coïncide avec l'ordre du groupe :
$$\sum_i (\deg \rho_i)^2 = |\mathrm{G}|.$$
5. La somme de chaque colonne distincte de la classe du neutre est nulle :
$$\sum_i (\deg \rho_i)\chi_i(g) = 0.$$
6. Deux colonnes distinctes sont orthogonales :
$$\sum_i \overline{\chi_i(C)}\chi_i(C') = 0$$

Démonstration. — 1. Relation d'orthogonalité entre χ et $\chi_{\rho_{\mathrm{triv}}}$.

2. Relation d'orthogonalité à nouveau.
3. C'est la formule $\frac{1}{|\mathrm{G}|}\sum_{g\in \mathrm{G}} \overline{\chi(g)}\chi(g) = \sum m_i^2$.
4. Chaque représentation V_i apparaît avec multiplicité $\dim V_i$ dans la représentation régulière qui est de dimension $|\mathrm{G}|$.
5. La représentation régulière est de caractère nul contre tout $g \neq e$.
6. Notons U la matrice de la tables de caractères (les lignes sont indicées par les caractères irréductibles, les colonnes par les classes de conjugaison) et D la matrice diagonale de même dimension où les termes diagonaux sont les $\dim S_i$. À partir de $UDU^* = |\mathrm{G}|\,\mathrm{id}$ nous obtenons $\frac{1}{|\mathrm{G}|}D = U^{-1}U^{*-1}$ puis $|\mathrm{G}|D^{-1} = U^*U$.

□

11.5.2.3. *Sous-groupes distingués.* —

Proposition 11.5.3

Soit G un groupe fini. Soit $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$ une représentation de caractère χ sur un $\mathbb{C}$-espace vectoriel V de dimension d. Alors

$$\ker \rho = \{g \in \mathrm{G} \mid \chi(g) = d\}.$$

Démonstration. — L'endomorphisme $\rho(g)$ est diagonalisable, car d'ordre fini, et ses valeurs propres sont d racines de l'unités. La condition $\chi(g) = d$ implique que ces racines de l'unité sont toutes égales à 1 et donc que $\rho(g)$ est l'identité. □

Proposition 11.5.4

Soit $\mathrm{H} \triangleleft \mathrm{G}$ un sous-groupe distingué d'un groupe fini. Alors H est l'intersection de noyaux de représentations irréductibles de G.

Démonstration. — Soit $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ le morphisme quotient. Soit ρ_{H} la représentation régulière de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$. Alors comme la représentation ρ_{H} est fidèle, H est le noyau de la représentation $\rho_{\mathrm{H}} \circ \pi$. En écrivant $\rho_{\mathrm{H}} \circ \pi$ comme une somme directe de représentations irréductibles nous obtenons le résultat. □

Exemple 11.5.2. — En observant la table de caractères nous retrouvons les sous-groupes distingués propres de $\mathfrak{S}_4$: $\mathcal{K}$ et $\mathcal{A}_4$.

11.5.3. Théorème de Molien. — , [**CG15**, p. 497], [**Pey04**, p. 219 et 288], [**RW10**, p. 320], [**CLO97**, Chapter 7, §2] à faire

Une motivation historique pour le développement de la théorie des représentations est l'étude des sous-groupes finis de $\mathrm{GL}(V)$*, où* V *est l'espace vectoriel des polynômes en* n *variables. Comprendre les polynômes laissés fixes par un tel groupe est une question basique. Le théorème de Molien permet de calculer les dimensions de tels polynômes invariants, homogènes et d'un degré donné.*

11.5.4. Représentations réelles et groupes d'ordre 8**, [CG15**, p. 477-482]**.** —

On illustre sur le cas de D_8 *et* $\mathbb{H}_8$ *la notion d'indicatrice de Frobenius-Schur qui permet de repérer qu'une représentation définie a priori sur les complexes est isomorphe à une représentation définie sur les réels.*

11.5.4.1. *Table de caractères.* —

- ◇ Table de caractères du groupe quaternionique $\mathbb{H}_8$.

Il y a cinq classes de conjugaison qui sont $\pm\mathrm{id}$, $\pm I$, $\pm J$ et $\pm K$ où

$$I = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix} \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad K = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$$

Puisque $D(\mathbb{H}_8) = \{1, -1\}$, l'abélianisé $\mathbb{H}_8/D(\mathbb{H}_8)$ de $\mathbb{H}_8$ est isomorphe au groupe de Klein, *i.e.* est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il en résulte que $\mathbb{H}_8$ possède quatre caractères de degré 1. Ainsi si ρ_i est une représentation irréductible de $\mathbb{H}_8$ de degré d_i nous avons

- ◇ d'une part $d_1 = d_2 = d_3 = d_4 = 1$,
- ◇ d'autre part $\displaystyle\sum_{i=1}^{5} d_i^2 = 8$.

Par conséquent $d_1 = d_2 = d_3 = d_4 = 1$ et $d_5 = 2$.

On obtient la dernière ligne en utilisant que les colonnes sont orthogonales ; la quantité $\frac{1}{|\mathrm{G}|}\sum_g \chi(g^2)$ s'appelle *l'indicatrice de Frobenius-Schur*.

	$\{\mathrm{id}\}$	$\{-\mathrm{id}\}$	$\{\pm I\}$	$\{\pm J\}$	$\{\pm K\}$	$\frac{1}{\lvert\mathrm{G}\rvert}\sum_g \chi(g^2)$
χ_{triv}	1	1	1	1	1	1
χ_1	1	1	-1	1	-1	1
χ_2	1	1	1	-1	-1	1
χ_3	1	1	-1	-1	1	1
χ_4	2	-2	0	0	0	-1

◇ Table de caractères du groupe D_8.

Le groupe de symétries du carré est engendré par une rotation r d'angle $\frac{\pi}{2}$ et une symétrie s. D'après ce qui précède D_8 a 5 classes de conjugaison : $\{\mathrm{id}\}$, $\{r^2\}$, $\{r, r^3\}$, $\{s, r^2 s\}$ et $\{rs, r^3 s\}$. Le sous-groupe $D(\mathrm{D}_8) = \mathbb{Z}/2\mathbb{Z} = \{\mathrm{id}, -\mathrm{id} = r^2\}$ est distingué dans D_8 et dans le quotient les trois éléments distincts r, s et rs sont d'ordre 2 donc

$$\mathrm{D}_8^{\mathrm{ab}} = \mathrm{D}_8/D(\mathrm{D}_8) = \mathrm{D}_8/\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Nous avons donc quatre représentations de dimension 1 correspondant aux quatre morphismes

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{C}^\times;$$

la cinquième doit donc être de dimension 2 (en effet $|\mathrm{D}_8| = 8$ donc $|\mathrm{D}_8| - (1^2+1^2+1^2+1^2) = 4 = 2^2$). C'est la représentation standard dans $\mathbb{C}^2$ (Exemple 11.2.3) d'où la dernière ligne de la table (que l'on peut aussi obtenir en utilisant que les colonnes sont orthogonales).

Ainsi

	$\{\mathrm{id}\}$	$\{r^2\}$	$\{r,\, r^3\}$	$\{s,\, r^2 s\}$	$\{rs,\, r^3 s\}$	$\frac{1}{\lvert G\rvert}\sum_g \chi(g^2)$
χ_{triv}	1	1	1	1	1	1
χ_1	1	1	-1	1	-1	1
χ_2	1	1	1	-1	-1	1
χ_3	1	1	-1	-1	1	1
χ_4	2	-2	0	0	0	1

11.5.4.2. *Représentation induite sur les matrices symétriques.* — Si $\rho\colon \mathrm{G} \to \mathrm{GL}(n,\mathbb{C})$ est une représentation de caractère χ, nous obtenons une représentation ρ_{sym} dans l'espace des formes bilinéaires symétriques, que nous identifions à l'espace Sym_n des matrices symétriques, en composant par

$$\mathrm{GL}(n,\mathbb{C}) \to \mathrm{GL}(\mathrm{Sym}_n), \qquad P \mapsto (M \mapsto {}^{\mathrm{t}}P^{-1}MP^{-1})$$

Lemme 11.5.1: [CG15]

Le caractère de la représentation ρ_{sym} est

$$\Psi\colon g \mapsto \frac{\chi(g^{-1})^2 + \chi(g^{-2})}{2}$$

Si de plus ρ est irréductible et χ est à valeurs réelles nous avons

$$2\langle \chi_{\mathrm{triv}}, \Psi\rangle - 1 = \frac{1}{\lvert \mathrm{G}\rvert}\sum_{g\in \mathrm{G}} \chi(g^2)$$

où $\langle \chi_{\mathrm{triv}}, \Psi\rangle$ s'interprète comme la dimension de l'espace des formes bilinéaires symétriques G-invariantes.

Démonstration. — Soit $g \in \mathrm{G}$ fixé. On choisit sur $\mathbb{C}^n$ une base qui diagonalise $\rho(g)$ et on note λ_i les valeurs propres de $\rho(g^{-1})$. Sur Sym_n on choisit comme base les matrices $S_{i,j} = E_{i,j} + E_{j,i}$ somme de deux matrices élémentaires, avec $1 \leq i \leq j \leq n$. Alors $S_{i,j}$ est un vecteur propre de ρ_{sym} de valeur propre $\lambda_i\lambda_j$. La trace de $\rho_{\mathrm{sym}}(g)$ est donc

$$\begin{aligned}
\sum_{1\leq i\leq j\leq n} \lambda_i\lambda_j &= \sum_{1\leq i\leq n} \lambda_i^2 + \sum_{1\leq i<j\leq n} \lambda_i\lambda_j \\
&= \frac{1}{2}\Big(\sum_{1\leq i\leq n} \lambda_i\Big)^2 + \frac{1}{2}\sum_{1\leq i\leq n} \lambda_i^2 \\
&= \frac{\chi(g^{-1})^2 + \chi(g^{-2})}{2}
\end{aligned}$$

Passons à la seconde assertion. D'une part

$$\begin{aligned} 2\langle \chi_{\text{triv}}, \Psi\rangle &= \frac{2}{|\mathrm{G}|}\sum_{g\in \mathrm{G}} \Psi(g) \\ &= \frac{1}{|\mathrm{G}|}\sum_{g\in \mathrm{G}} \chi(g)^2 + \frac{1}{|\mathrm{G}|}\sum_{g\in \mathrm{G}} \chi(g)^2 \\ &= \langle \overline{\chi}, \chi\rangle + \frac{1}{|\mathrm{G}|}\sum_{g\in \mathrm{G}} \chi(g^2) \end{aligned}$$

et d'autre part puisque ρ est irréductible réel $1 = \langle \chi, \chi\rangle = \langle \overline{\chi}, \chi\rangle$. □

11.5.4.3. *Représentations réalisables sur* $\mathbb{R}$. — Soit $\rho\colon \mathrm{G} \to \mathrm{GL}(n, \mathbb{C})$ une représentation de caractère χ. On dit que ρ *se réalise sur* $\mathbb{R}$ si ρ est isomorphe à une représentation ρ' qui provient d'une représentation $\mathrm{G} \to \mathrm{GL}(n, \mathbb{R})$ via l'injection naturelle $\mathrm{GL}(n, \mathbb{R}) \hookrightarrow \mathrm{GL}(n, \mathbb{C})$. Si ρ se réalise sur $\mathbb{R}$, alors χ est à valeurs réelles. Par contre la réciproque est fausse ; en effet considérons la représentation de $\mathbb{H}_8$ dans $\mathrm{GL}(2, \mathbb{C})$ via les matrices I, J, K, les traces sont réelles et pourtant $\mathbb{H}_8$ n'est pas isomorphe à un sous-groupe de $\mathrm{O}(2, \mathbb{R})$ (les sous-groupes finis de $\mathrm{O}(2, \mathbb{R})$ sont cycliques ou diédraux.

Proposition 11.5.5: [CG15]

Une représentation irréductible $\rho\colon \mathrm{G} \to \mathrm{GL}(n, \mathbb{C})$ est réalisable sur $\mathbb{R}$ si et seulement si $\frac{1}{|\mathrm{G}|}\sum_{g\in \mathrm{G}} \chi(g^2) = 1$.

Démonstration. — Nous allons montrer que les trois assertions suivantes sont équivalentes :

1. ρ est réalisable sur $\mathbb{R}$;
2. il existe une forme bilinéaire symétrique non nulle sur $\mathbb{C}^n$ invariante par G ;
3. $\frac{1}{|\mathrm{G}|}\sum_{g\in \mathrm{G}} \chi(g^2) = 1$.

Commençons par montrer que (1) $\Rightarrow$ (2) : un produit scalaire réel invariant (moyennisation) s'étend sur $\mathbb{C}$ en la forme bilinéaire invariante attendue.

Continuons avec (2) $\Rightarrow$ (1) : notons β la forme bilinéaire symétrique non nulle G-invariante. β est non dégénérée car sinon son noyau correspondrait à une sous-représentation propre ce qui est exclu par hypothèse : ρ est supposée irréductible. Par ailleurs par moyennisation du produit standard on sait qu'il existe $\langle \cdot, \cdot\rangle$ un produit hermitien G-invariant (disons antilinéaire par rapport à la première variable). Il existe alors $\varphi\colon \mathbb{C}^n \to \mathbb{C}^n$ semi-linéaire tel que $\beta(u, v) = \langle \varphi(u), v\rangle$:

$$\langle \varphi(\lambda u), v\rangle = \beta(\lambda u, v) = \lambda\beta(u, v) = \lambda\langle \varphi(u), v\rangle = \langle \overline{\lambda}\varphi(u), v\rangle.$$

L'itéré second φ^2 est linéaire. Vérifions maintenant que sa matrice est hermitienne définie positive :

$$\begin{aligned}\langle\varphi^2(u),v\rangle &= \beta(\varphi(u),v)\\ &= \beta(v,\varphi(u))\\ &= \lambda\langle\varphi(u),v\rangle\\ &= \langle\overline{\lambda}\varphi(u),v\rangle\end{aligned}$$

et donc également

$$\langle\varphi^2(u),u\rangle = \langle\varphi(u),\varphi(u)\rangle.$$

Montrons que φ est G-invariante :

$$\langle\rho(g)\varphi(u),v\rangle = \langle\varphi(u),\rho(g)^{-1}v\rangle = \beta(u,\rho(g)^{-1}v) = \beta(\rho(g)u,v) = \langle\varphi(\rho(g)u),v\rangle.$$

Ainsi φ^2 est un G-endomorphisme d'une représentation irréductible, par le Lemme de Schur nous en déduisons que φ^2 est une homothétie de rapport un réel $\lambda > 0$. Alors φ (vu comme $\mathbb{R}$-endomorphisme de $\mathbb{R}^{2n}$) est annulé par $X^2-\lambda$ et admet pour valeurs propres $\pm\sqrt{\lambda}$, d'espaces propres associés $V_\pm$. De plus la relation de semi-linéarité $\varphi(\mathbf{i}v) = -\mathbf{i}\varphi(v)$ implique que $\mathbf{i}V_+ = V_-$. En particulier $\dim_{\mathbb{R}} V_+ = \dim_{\mathbb{C}} V$ et le complexifié de V_+ est V : autrement dit V_+ est une réalisation réelle de ρ.

Poursuivons avec (3) $\Rightarrow$ (2) : le Lemme 11.5.1 assure que $\langle\chi_{\text{triv}},\Psi\rangle = 1$. Il en résulte que la multiplicité de la représentation triviale dans la représentation induite par ρ sur les matrices symétriques est 1. Autrement dit il existe une forme bilinéaire invariante par ρ (unique à un facteur multiplicatif près).

Finissons avec (2) $\Rightarrow$ (3) : une forme bilinéaire (symétrique ou non) invariante s'identifie à un morphisme de représentation de V vers V^* (Remarque 11.5.3). D'après le Lemme de Schur l'espace de tels morphismes est de dimension 1. Ainsi l'espace des formes bilinéaires symétriques invariantes par ρ est ou bien trivial, ou bien de dimension 1. Nous sommes ici dans le second cas et le Lemme 11.5.1 assure que ceci équivaut à $\frac{1}{|\mathrm{G}|}\sum\chi(g^2) = 1$. □

Remarque 11.5.3. — Revenons sur l'assertion « une forme bilinéaire (symétrique ou non) invariante s'identifie à un morphisme de représentation de V vers V^* ».

Notons $\mathrm{Bil}(V)$ les formes bilinéaires sur V et $\mathrm{Hom}(V,V^*)$ les morphismes de représentations de V vers V^*.

Commençons par les identifications sans action en termes matriciels : on choisit une base de $V \simeq \mathbb{C}^n$ et donc également une base duale pour V^* :

- ◇ V s'identifie à l'espace des vecteurs colonne ;
- ◇ le dual $V^* = \mathrm{Hom}(V,\mathbb{C})$ s'identifie à l'espace des vecteurs lignes ;
- ◇ les morphismes dans $\mathrm{Hom}(V,V^*)$ sont codés par des matrices carrées M via

$$x \in V \mapsto {}^{\mathrm{t}}xM \in V^*;$$

- ⋄ les formes bilinéaires dans $\mathrm{Bil}(V)$ sont aussi codées par des matrices M via
$$(x, y) \in V \times V \mapsto {}^{\mathrm{t}}xMy \in \mathbb{C}.$$

Maintenant étudions la compatibilité avec l'action de G. Nous avons quatre représentations à disposition :

- ⋄ la représentation initiale $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$;
- ⋄ la représentation ρ^* induite sur V^* par précomposition par $\rho(g)^{-1}$:
$$\rho^*(g)\colon V^* \to V^*, \qquad {}^{\mathrm{t}}y \mapsto {}^{\mathrm{t}}y\rho(g)^{-1}$$
- ⋄ la représentation ρ_{Hom} induite sur $\mathrm{Hom}(V, V^*)$ par précomposition par $\rho(g)^{-1}$ et post-composition par $\rho^*(g)$
$$\rho_{\mathrm{Hom}}(g)\colon \mathrm{Hom}(V, V^*) \to \mathrm{Hom}(V, V^*), \qquad (x \mapsto {}^{\mathrm{t}}xM) \mapsto \big(x \mapsto {}^{\mathrm{t}}x{}^{\mathrm{t}}\rho(g)^{-1}M\rho(g)^{-1}\big)$$
(en effet on connaît les trois étapes pour construire le terme de droite :
$$x \in V \mapsto \rho(g)^{-1}x \in V \mapsto {}^{\mathrm{t}}x{}^{\mathrm{t}}\rho(g)^{-1}M \in V^* \mapsto \rho^*(g)\big({}^{\mathrm{t}}x{}^{\mathrm{t}}\rho(g)^{-1}M\big) \in V^*)$$
- ⋄ la représentation ρ_{Bil} que nous avons défini sur les formes bilinéaires :
$$\rho_{\mathrm{Bil}}(g)\colon \mathrm{Bil}(V) \to \mathrm{Bil}(V), \qquad M \mapsto {}^{\mathrm{t}}\rho(g)M\rho(g)^{-1}$$

CHAPITRE 12

GÉOMÉTRIE

La notion de point est introduite tôt, puis vient celle de vecteur joignant deux points donnés. Lorsqu'on établit proprement les fondements de la géométrie, il s'avère plus simple d'inverser le processus : on introduit tout d'abord les vecteurs, ou plus exactement les espaces vectoriels dont les éléments sont appelés vecteurs ; on ne définit qu'ensuite les espaces affines, dont les éléments sont appelés points, et dans lesquels deux points définissent un vecteur au sens des espaces vectoriels.

Les espaces affines. — C'est à ces espaces affines, qui sont donc plus proches de l'intuition première que les espaces vectoriels, que nous nous intéresserons pour commencer. Leur définition consiste essentiellement à prendre comme axiomes les propriétés usuelles des vecteurs définis par deux points, comme par exemple la relation de Chasles.

Nous verrons aussi qu'ils ne sont pas si éloignés que ça des espaces vectoriels. Plus précisément, une fois donné un espace affine E, on peut, en choisissant un point O de E, voir de façon naturelle E comme un espace vectoriel dont l'origine est O. Le point crucial est que O peut être choisi arbitrairement : contrairement à un espace vectoriel dans lequel l'origine jouit de propriétés spécifiques (c'est l'élément neutre de l'addition), un espace affine ne possède a priori aucun point privilégié. Tous jouent le même rôle et ce n'est qu'occasionnellement, pour des besoins précis (calculatoires ou géométriques) que l'on choisit d'en distinguer un, adapté à la situation considérée, en lui conférant le statut d'origine. Notons que cela est tout à fait cohérent avec l'intuition que nous pouvons avoir de notre espace ambiant : s'il peut être commode, dans certains cas, d'en fixer une origine, il n'y a aucun point qui semble prédestiné à ce rôle.

L'exemple typique d'espace affine est le suivant : on se donne un espace vectoriel E, un sous-espace vectoriel F de E, un vecteur v de E. Soit $\mathcal{F}$ le translaté $F + v$ de F par v, c'est-à-dire l'ensemble $\{f + v \mid f \in F\} \subset E$; il admet une structure naturelle d'espace affine (notons que si v n'appartient pas à $\mathcal{F}$, c'est-à-dire si $\mathcal{F} \neq F$, alors $\mathcal{F}$ n'est pas un sous-espace vectoriel de E, car il ne contient pas l'origine). L'application $f \mapsto f - v$ permet d'identifier $\mathcal{F}$ à l'espace vectoriel F (avec v qui correspond à l'origine). Mais ce n'est pas la seule : si w est un vecteur de la forme $v + f$ avec $f \in F$ alors $\mathcal{F}$ est aussi égal à $F + w$, et l'on peut donc également

identifier $\mathcal{F}$ à F par l'application $f \mapsto f - w$; c'est cette fois-ci w qui correspond à l'origine. Si v n'appartient pas à F il n'y a pas de vecteur privilégié parmi ceux qui sont de la forme $v + f$ avec $f \in F$, et il n'y a donc pas, parmi les différentes façons d'identifier $\mathcal{F}$ à F que nous avons décrites (qui sont associées à différents choix d'origine), une qui soit meilleure, ou plus naturelle, que les autres ; on retrouve bien le phénomène évoqué ci-dessus.

Les formules de la géométrie affine. — Venons-en à l'aspect calculatoire de la théorie. En algèbre linéaire, les formules (équations des sous-espaces vectoriels, description des applications linéaires...) sont pour l'essentiel des formules linéaires en les coordonnées, c'est-à-dire de la forme $\sum a_i x_i$, sans terme constant : c'est encore une manifestation du rôle particulier de l'origine, qui appartient à tous les sous-espaces vectoriels, est envoyée sur l'origine par toute application linéaire, etc. Puisqu'en géométrie affine ce privilège est abrogé, nous devrons travailler avec des formules affines en les coordonnées, c'est-à-dire de la forme $\sum a_i x_i + b$. La présence de ce terme constant complique parfois les choses – et c'est, en un sens, la raison technique pour laquelle nous étudions les espaces vectoriels avant les espaces affines.

Sous-espaces affines, applications affines. — Les sous-espaces vectoriels et les applications linéaires ont leurs pendants en géométrie affine - ce sont les sous-espaces affines et les applications affines, que nous étudierons. De nouveaux phénomènes apparaissent, toujours et encore liés à l'absence de point privilégié :

- ◇ l'intersection de deux sous-espaces affines peut très bien être vide (par exemple l'intersection de deux droites parallèles dans le plan est vide, ou encore l'intersection d'un plan et une droite parallèles dans l'espace), alors que l'intersection de deux sous-espaces vectoriels contient toujours l'origine ;
- ◇ une application affine peut très bien ne pas avoir de point fixe (par exemple une translation n'a pas de point fixe, ou encore la composée d'une rotation autour d'un axe et d'une translation parallèle à l'axe en question n'a pas de point fixe), alors qu'une application linéaire fixe toujours l'origine.

Les barycentres et les coordonnées barycentriques. — Nous aborderons ensuite la notion de barycentre et à laquelle on peut plus ou moins penser comme à un analogue affine de la notion de combinaison linéaire. Elle débouchera sur le calcul en coordonnées barycentriques. Celui-ci présente à première vue un avantage par rapport au calcul en coordonnées cartésiennes (on y manipule pour l'essentiel des formules sans terme constant) et un inconvénient (il y a une variable de plus : par exemple, on doit manipuler trois coordonnées barycentriques lorsqu'on travaille dans le plan). On se rend compte à la pratique qu'il possède également deux atouts spécifiques, qui justifient son introduction :

- ◇ il permet d'exploiter la symétrie de certaines situations ; ainsi, si on travaille avec un triangle (ABC), les trois points A, B et C jouent le même rôle ; si on décide (par exemple) de travailler dans le repère cartésien $(A, \overrightarrow{AB}, \overrightarrow{AC})$, cette symétrie est rompue puisque A

est privilégié, alors qu'elle est préservée si on travaille en coordonnées barycentriques dans le repère (A, B, C) ; aussi ce dernier point de vue conduira-t-il souvent à des calculs plus simples et des formules plus élégantes ;

- ◇ il permet de mettre en évidence l'analogie entre certains phénomènes, et de les aborder de manière unifiée : il traite par exemple exactement de la même manière les triplets de droites parallèles et les triplets de droites concourantes dans le plan (ce qui traduit le fait, auquel on pourrait donner un sens mathématique rigoureux, que trois droites parallèles sont concourantes à l'infini).

Les espaces affines euclidiens. — Les notions évoquées jusqu'à maintenant (espaces affines, sous-espaces affines, applications affines, barycentres), ne font finalement appel qu'aux quatre opérations, ce qui permet de leur donner un sens sur un corps quelconque.

Nous pouvons aussi aborder des concepts qui requièrent quant à eux de travailler sur le corps des nombres réels. Plus précisément, nous nous intéressons aux espaces affines sur $\mathbb{R}$ dont l'espace vectoriel sous-jacent est euclidien, c'est-à-dire de dimension finie et muni d'un produit scalaire ; c'est ce qu'on appelle les espaces affines euclidiens.

Dans un espace affine euclidien, on sait définir la distance entre deux points, puis les applications affines qui conservent les distances ; ce sont les isométries affines. On sait aussi dire ce que sont l'angle entre deux vecteurs (ou deux droites) et sa mesure (ces notions n'ont rien de spécifiquement affine, existent déjà dans les espaces vectoriels euclidiens et c'est à leur propos que nous y reviendrons), mais on se heurte à leur sujet à deux difficultés :

- ◇ la première, c'est que les définir rigoureusement est délicat ;
- ◇ la seconde est liée aux problèmes d'orientation, qui correspondent à des subtilités de la « vraie vie ». Par exemple, on peut essayer de répondre aux questions suivantes :
  - i) Si deux roues tournent dans un même plan, cela a-t-il un sens de demander si elles tournent toutes deux dans le même sens ?
  - ii) Si deux roues tournent dans l'espace (en position arbitraire l'une par rapport à l'autre), cela a-t-il un sens de demander si elles tournent toutes deux dans le même sens ?

12.1. Géométrie euclidienne

à faire

12.1.2. Isométrie euclidienne. — Considérons l'espace euclidien $\mathbb{R}^n$ muni du produit scalaire $\langle\,,\,\rangle$ qui donne la norme euclidienne $||v|| = \sqrt{\langle v,\, v\rangle}$. La distance associée est donnée par $d(x, y) = ||x - y||$.

Définition 12.1.1

Une *isométrie euclidienne* φ est une application bijective de $\mathbb{R}^n$ qui préserve la norme euclidienne, *i.e.* qui vérifie

$$\forall\, x,\, y \in \mathbb{R}^n \qquad d(\varphi(x), \varphi(y)) = d(x, y).$$

Le *groupe des isométries euclidiennes* est $\mathrm{Isom}(\mathbb{R}^n, d)$.

Les translations et les éléments du groupe orthogonal $\mathrm{O}(n, \mathbb{R})$ sont des isométries euclidiennes. L'énoncé suivant donne toutes ces isométries :

Théorème 12.1.1

Toute isométrie de $(\mathbb{R}^n, d)$ est une application affine.
Toute isométrie de $(\mathbb{R}^n, d)$ qui fixe l'origine est donnée par un élément de $\mathrm{O}(n, \mathbb{R})$.
Le groupe $\mathrm{Isom}(\mathbb{R}^n)$ se décompose en un produit semi-direct de la façon suivante :

$$\mathrm{Isom}(\mathbb{R}^n) = \mathrm{O}(n, \mathbb{R}) \ltimes (\mathbb{R}^n, +)$$

où $(\mathbb{R}^n, +)$ est identifié au groupe des translations de $\mathbb{R}^n$.

Rappelons qu'une application $f\colon \mathbb{R}^n \to \mathbb{R}^n$ est *affine* s'il existe une application linéaire $A\colon \mathbb{R}^n \to \mathbb{R}^n$ et un élément b de $\mathbb{R}^n$ tels que pour tout $x \in \mathbb{R}^n$ on ait $f(x) = Ax + b$. Remarquons que le couple (A, b) est unique. En effet $b = f(0)$ et A est l'application linéaire $x \mapsto f(x) - f(0)$.

Pour $x \in \mathbb{R}^n$ nous notons τ_x la translation de vecteur x ; autrement dit $\tau_x(y) = y + x$ pour tout $y \in \mathbb{R}^n$.

Démonstration. — Soit f un élément de $\mathrm{Isom}(\mathbb{R}^n)$. Notons $\tau_{-f(0)}$ la translation de vecteur $-f(0)$. Si $g = \tau_{-f(0)} \circ f$ est linéaire, alors $f = \tau_{f(0)} \circ g$ est affine. Il suffit donc de traiter le cas $f(0) = 0$.

Soit donc f un élément de $\mathrm{Isom}(\mathbb{R}^n)$ tel que $f(0) = 0$. Montrons que f préserve la norme et le produit scalaire. Soit x dans $\mathbb{R}^n$, alors

$$||f(x)|| = ||f(x) - f(0)|| = d(f(x), f(0)) = d(x, 0) = ||x - 0|| = ||x||$$

autrement dit f préserve la norme. Puisque f préserve la norme, nous avons pour tous x, y dans $\mathbb{R}^n$

$$||f(x) - f(y)||^2 = ||x - y||^2$$

soit

$$||f(x)||^2 + ||f(y)||^2 - 2\langle f(x),\, f(y)\rangle = ||x||^2 + ||y||^2 - 2\langle x,\, y\rangle$$

ou encore

$$||x||^2 + ||y||^2 - 2\langle f(x),\, f(y)\rangle = ||x||^2 + ||y||^2 - 2\langle x,\, y\rangle$$

et

$$\langle f(x),\, f(y)\rangle = \langle x,\, y\rangle.$$

L'application f préserve donc le produit scalaire.

Soient x, y dans $\mathbb{R}^n$ et λ dans $\mathbb{R}$; nous avons

$$\begin{aligned}
||f(\lambda x + y) - \lambda f(x) - f(y)||^2 &= ||f(\lambda x + y)||^2 + \lambda^2 ||f(x)||^2 + ||f(y)||^2 \\
&\quad -2\lambda\langle f(x),\, f(\lambda x + y)\rangle - 2\langle f(y),\, f(\lambda x + y)\rangle \\
&\quad +2\lambda\langle f(x),\, f(y)\rangle \\
&= ||\lambda x + y||^2 + \lambda^2 ||x||^2 + ||y||^2 \\
&\quad -2\lambda\langle x,\, \lambda x + y\rangle - 2\langle y,\, \lambda x + y\rangle + 2\lambda\langle x,\, y\rangle \\
&= ||(\lambda x + y) - \lambda x - y||^2 \\
&= 0.
\end{aligned}$$

Autrement dit pour tous x et y dans $\mathbb{R}^n$ nous avons $||f(\lambda x + y) - \lambda f(x) - f(y)||^2 = 0$ soit $f(\lambda x + y) = \lambda f(x) + f(y)$: f est donc linéaire.

Soient f et g deux isométries de $\mathbb{R}^n$. D'après ce qui précède ce sont des applications affines. Il existe donc A, A' dans $\mathrm{O}(n, \mathbb{R})$ et b, b' dans $\mathbb{R}^n$ tels que

$$f(x) = Ax + b \qquad\qquad g(x) = A'x + b'.$$

La composée $f \circ g$ s'écrit $f(g(x)) = AA'x + (Ab' + b)$. L'application

$$\varphi\colon \mathrm{Isom}(\mathbb{R}^n) \to \mathrm{O}(n, \mathbb{R}) \qquad\qquad f \mapsto A$$

qui à f associe sa partie linéaire est donc un morphisme de groupes. Son noyau $\ker\varphi$ est l'ensemble des isométries f telles que $A = \mathrm{id}$, c'est-à-dire telles que $f(x) = x + b$ ou encore telles que f est une translation. Le noyau de φ s'identifie donc à $(\mathbb{R}^n, +)$ via l'isomorphisme $b \mapsto \tau_b$. L'ensemble des translations est un sous-groupe distingué de $\mathrm{Isom}(\mathbb{R}^n)$. Son intersection avec $\mathrm{O}(n, \mathbb{R})$ est réduite à $\{\mathrm{id}\}$. De plus si $f(x) = Ax + b$, alors $f = \tau_b \circ A$. Nous avons donc bien la décomposition en produit semi-direct. □

Une notion importante en géométrie euclidienne est la notion d'angle. Soient A, B, C trois points de $\mathbb{R}^n$ tels que $A \neq B$, $C \neq B$; la *mesure de l'angle* $\widehat{ABC}$ est le nombre $\alpha \in [0, \pi]$ tel que

$$\cos\alpha = \frac{|\langle \overrightarrow{BA},\, \overrightarrow{BC}\rangle|}{||\overrightarrow{BA}|| \cdot ||\overrightarrow{BC}||}. \tag{12.1.1}$$

Remarquons que nous parlons ici d'*angle géométrique* aussi appelé *angle non orienté*. Ce nombre est bien défini car $\frac{|\langle \overrightarrow{BA}, \overrightarrow{BC} \rangle|}{||\overrightarrow{BA}|| \cdot ||\overrightarrow{BC}||} \in [0,1]$ par l'inégalité de Cauchy-Schwarz.

Proposition 12.1.1

Les isométries de $\mathbb{R}^n$ préservent les angles. Autrement dit pour tout $g \in \mathrm{Isom}(\mathbb{R}^n)$, pour tous A, B, $C \in \mathbb{R}^n$ avec $A \neq B$ et $C \neq B$ nous avons

$$g(A)\widehat{g(B)}g(C) = \widehat{ABC}$$

Démonstration. — La partie linéaire d'une isométrie est un élément de $\mathrm{O}(n, \mathbb{R})$ qui préserve le produit scalaire et la norme et (12.1.1) ne fait intervenir que des normes et un produit scalaire. □

Toute rotation plane est la composée de deux symétries ; ce résultat se généralise en dimension supérieure :

Théorème 12.1.2

Le groupe $\mathrm{Isom}(\mathbb{R}^n)$ est engendré par les symétries orthogonales par rapport à des hyperplans affines.
Plus précisément, toute isométrie de $\mathbb{R}^n$ est la composée d'au plus $n+1$ telles symétries.

Lemme 12.1.1

Soient $f \in \mathrm{Isom}(\mathbb{R}^n)$ et $F \subset \mathbb{R}^n$ une partie finie. Si f préserve F (*i.e.* $f(F) = F$), alors f fixe l'isobarycentre de F.
En particulier, $\mathrm{Stab}_{\mathrm{Isom}(\mathbb{R}^n)}(F)$ est conjugué à un sous-groupe de $\mathrm{O}(n, \mathbb{R})$.

Démonstration. — Les isométries étant affines l'isobarycentre des points x_1, x_2, …, x_n est l'isobarycentre des $f(x_1)$, $f(x_2)$, …, $f(x_n)$ c'est-à-dire le même point. □

Lemme 12.1.2

Soit f une isométrie donnée par $f(x) = Ax + b$ avec $A \in \mathrm{O}(n, \mathbb{R})$ et $b \in \mathbb{R}^n$.
Alors f possède un point fixe si et seulement si b appartient à $\mathrm{Im}(A - \mathrm{id})$.

Démonstration. — Soit x un point fixe de f, alors $Ax + b = x$, *i.e.* $b = (\mathrm{id} - A)x \in \mathrm{Im}(A - \mathrm{id})$.

Réciproquement, si $b \in \mathrm{Im}(A - \mathrm{id})$, alors il existe x tel que $b = (A - \mathrm{id})x$ et donc x est un point fixe de f. □

12.1.3. Dimension 2. — Avant d'énoncer la classification des isométries en dimension deux rappelons la notion suivante.

Soient D une droite du plan et $\overrightarrow{v}$ un vecteur directeur de D. Une *symétrie glissée* d'axe D et de direction $\overrightarrow{v}$ est la composée de la réflexion d'axe D et de la translation de vecteur $\overrightarrow{v}$. L'image d'un point M est donc obtenue en effectuant d'abord la symétrie orthogonale d'axe D, puis la translation de vecteur $\overrightarrow{v}$ (ou vice-versa).

Proposition 12.1.2

Les éléments de $\mathrm{Isom}(\mathbb{R}^2)$ sont :

- ◇ les translations,
- ◇ les rotations,
- ◇ les symétries axiales ou réflexions,
- ◇ les symétries glissées.

L'idée de la démonstration est d'étudier les éventuels points fixes avec le Lemme 12.1.2 ; pour plus de détails on renvoie à [**Aud06**].

Définitions 12.1.1

Soient $n \geq 2$ et A_1, A_2, …, A_n des points du plan tels que $A_i \neq A_{i+1}$ pour $i \in \mathbb{Z}/n\mathbb{Z}$.
La *ligne polygonale* $\mathcal{L}$ associée à ces points est la suite $([A_1, A_2], [A_2, A_3], , \ldots, [A_n, A_1])$.
Les segments $[A_i, A_{i+1}]$ sont les *côtés* de $\mathcal{L}$, les points A_i ses *sommets*.
La ligne polygonale $\mathcal{L}$ est *simple* si lorsque deux côtés s'intersectent alors ce sont deux côtés consécutifs (*i.e.* de la forme $[A_{i-1}, A_i]$ et $[A_i, A_{i+1}]$) et leur intersection est réduite à un point (nécessairement A_i).

Théorème 12.1.3: Théorème de Jordan pour les polygones

Soit $\mathcal{L}$ une ligne polygonale simple. Le complémentaire de la réunion des côtés de $\mathcal{L}$ a deux composantes connexes, l'une bornée appelée *intérieur* et une non-bornée appelée *extérieur*.

Définition 12.1.2

On appelle *polygone* la réunion des côtés d'une ligne polygonale simple et de son intérieur.
Un polygone est *convexe* si son intérieur l'est.

Définition 12.1.3

Un polygone convexe est *régulier* si tous ses côtés sont égaux et tous ses angles sont égaux.

Soit A une partie de E. L'*enveloppe convexe* de A est l'intersection de toutes les parties convexes de E qui contiennent A. Une caractérisation de A est la suivante : l'enveloppe convexe de A est la plus petite partie convexe de E qui contient A.

Théorème-Définition 12.1.1

Soit $P = A_1A_2 \dots A_n$ un polygone convexe à n côtés. Les conditions sont équivalentes :

1. P est régulier ;
2. tous les côtés de P sont égaux et les points A_i sont cocycliques (*i.e.* sur un même cercle) ;
3. les sommets de P sont sur un cercle de centre O et tous les angles au centre $\widehat{A_iOA_{i+1}}$ sont égaux ;
4. le polygone est semblable à l'enveloppe convexe de $\left\{e^{2\mathrm{i}\pi k/n} \mid k \in \mathbb{Z}/n\mathbb{Z}\right\}$.

Le point O est alors le *centre circonscrit* au polygone P.

Démonstration. — Montrons que $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$.

Commençons par montrer que $1 \Rightarrow 2$. Supposons que P soit régulier. Trois points non alignés déterminent toujours un unique cercle (le centre de ce cercle est le centre circonscrit, intersection des médiatrices). Montrons que quatre points consécutifs sont cocycliques ; cela montrera que ce cercle ne dépend pas des quatre points choisis et que les A_i sont donc tous cocycliques. Soit $i \in \mathbb{Z}/n\mathbb{Z}$; considérons les points A_{i-1}, A_i, A_{i+1} et A_{i+2}. Les bissectrices des angles en A_i et A_{i+1} se coupent en un point O. Le polygone P étant régulier nous avons $\widehat{OA_{i+1}A_i} = \widehat{OA_iA_{i+1}}$; le triangle OA_iA_{i+1} est donc isocèle en O, *i.e.* $||OA_i|| = ||OA_{i+1}||$. De plus puisque les angles $\widehat{OA_{i+1}A_i}$ et $\widehat{OA_{i+1}A_{i+2}}$ sont égaux et puisque $||A_iA_{i+1}|| = ||A_{i+1}A_{i+2}||$ la symétrie d'axe (OA_{i+1}) envoie A_i sur A_{i+2} et fixe O. Il s'en suit que $||A_iO|| = ||A_{i+2}O||$. De même nous montrons que $||A_{i+1}O|| = ||A_{i-1}O||$ et les quatre points sont sur un cercle de centre O.

Montrons que $2 \Rightarrow 3$. Si les côtés de P sont tous égaux et les A_i sur un cercle, alors l'angle $\widehat{A_iOA_{i+1}}$ est donné par la formule d'Al-Kashi [1] qui ne fait intervenir que les longueurs $||OA_i|| = ||OA_{i+1}||$ et $||A_iA_{i+1}||$ qui ne dépendent pas de i. Par suite les angles au centre $\widehat{A_iOA_{i+1}}$ sont tous égaux.

1. On appelle formule d'Al-Kashi, ou loi des cosinus, ou encore théorème de Pythagore généralisé l'égalité suivante, valable dans tout triangle ABC, qui relie la longueur des côtés en utilisant le cosinus d'un des angles du triangle : $||BC||^2 = ||AC||^2 + ||AB||^2 - 2||AC|| \cdot ||AB|| \cos(\widehat{BAC})$.

Finalement montrons que $3 \Rightarrow 1$. Supposons que tous les A_i soient sur un cercle de centre O et que tous les angles au centre $\widehat{A_iOA_{i+1}}$ sont tous égaux à un certain α. Les triangles OA_iA_{i+1} sont donc isocèles en O. Par conséquent les angles $\widehat{OA_iA_{i+1}}$ et $\widehat{OA_{i+1}A_i}$ sont égaux à un certain α_i qui vérifie $\alpha + 2\alpha_i = \pi$. Il en résulte que tous les α_i sont égaux à $\frac{\pi-\alpha}{2}$ et que tous les $\widehat{A_{i-1}A_iA_{i+1}} = \widehat{A_{i+1}A_iO} + \widehat{OA_iA_{i+1}}$ sont égaux à $\pi - \alpha$. Les longueurs $||A_iA_{i+1}||$ sont données par $2r\tan\left(\frac{\alpha}{2}\right)$ où r désigne le rayon du cercle. Elles sont donc toutes égales et le polygone est régulier. □

Si $E \subset \mathbb{R}^n$, nous notons $\mathrm{Isom}(E)$ le sous-groupe de $\mathrm{Isom}(\mathbb{R}^n)$ qui préserve E. Nous notons aussi $\mathrm{Isom}^+(E)$ le sous-groupe de $\mathrm{Isom}(E)$ des isométries qui préservent l'orientation.

Théorème 12.1.4

Si $P_n = A_0A_1 \dots A_{n-1}$ est un polygone régulier à n côtés, alors $\mathrm{Isom}(P_n) \simeq \mathrm{D}_{2n}$.

Démonstration. — Le groupe diédral D_{2n} est un sous-groupe du groupe $\mathrm{Isom}(P_n)$.

Reste à montrer que $\mathrm{Isom}(P_n) \subset \mathrm{D}_{2n}$. Soit f dans $\mathrm{Isom}(P_n)$. Désignons par O le centre du cercle circonscrit à P_n. Il existe i tel que $A_i = f(A_0)$. Notons ρ la rotation de centre O telle que $\rho(A_0) = A_i$. Ainsi $g = \rho^{-1}f$ fixe A_0. Les deux seuls sommets les plus proches de A_0 sont A_1 et A_{-1}. Puisque g préserve les distances et fixe A_0 nous avons $g(A_1) = A_{\pm 1}$. Si $g(A_1) = A_1$, nous posons $h = g$; sinon nous posons $h = \sigma g$ où σ désigne la symétrie par rapport à la droite (OA_0). Par suite $h(A_0) = A_0$ et $h(A_1) = A_1$. Un raisonnement analogue conduit à $h(A_2) \in \{A_2, A_0\}$; comme h est une bijection, l'égalité $h(A_0) = A_0$ implique $h(A_2) = A_2$. Par récurrence nous obtenons que $h(A_i) = A_i$ pour tout $i \in \mathbb{Z}/n\mathbb{Z}$. Puisque h est affine et fixe trois points non alignés, h coïncide avec id. Finalement ou bien $f = \rho\sigma$ ou bien $f = \rho$. Dans les deux cas f appartient à D_{2n}. □

12.1.4. Dimension 3. — Avant d'énoncer la classification des isométries en dimension trois rappelons qu'un *vissage* (ou *rotation glissée*) est un déplacement dans un espace affine euclidien qui est la composée commutative d'une rotation et d'une translation selon un vecteur dirigeant l'axe de rotation (si la rotation n'est pas l'identité). Une *anti-rotation* est un type particulier d'antidéplacement (*i.e.* d'isométrie qui renverse l'orientation) de l'espace euclidien de dimension 3 (espace affine euclidien ou espace vectoriel euclidien, suivant le contexte) : c'est la composée commutative d'une rotation d'angle ϑ autour d'un axe Δ et d'une réflexion par rapport à un plan perpendiculaire à Δ.

Théorème 12.1.5

Les éléments de $\mathrm{Isom}(\mathbb{R}^3)$ sont :

— les translations,

— les rotations,

— les rotations glissées,

— les symétries orthogonales par rapport à un plan,

— les symétries glissées,

— les anti-rotations.

Pour une preuve on renvoie à [**Aud06**].

12.2. Simplicité du groupe des rotations de $\mathbb{R}^3$

Rappelons que $\mathrm{SO}(3,\mathbb{R})$ est le groupe des rotations de l'espace euclidien canonique $\mathbb{R}^3$. Le théorème suivant montre que le groupe $\mathrm{SO}(3,\mathbb{R})$ est simple :

Théorème 12.2.1

Le groupe $\mathrm{SO}(3,\mathbb{R})$ est simple.

Soit G un sous-groupe de $\mathrm{SO}(3,\mathbb{R})$. Nous désignons par G_0 la composante connexe par arcs de id dans G.

Le groupe $\mathrm{SO}(3,\mathbb{R})$ est une partie de l'espace vectoriel $\mathcal{L}(\mathbb{R}^3)$ muni de sa topologie d'espace normé. Un chemin de G est une application $\gamma\colon [0,1] \to \mathrm{G}$ continue, $\gamma(0)$ est l'origine du chemin et $\gamma(1)$ son extrémité.

Lemme 12.2.1

On considère sur G la relation $\mathcal{R}$ définie par $g\mathcal{R}h$ s'il existe un chemin de G d'origine g et d'extrémité h. Cette relation est une relation d'équivalence.

Démonstration. — Si $g \in \mathrm{G}$, alors $g\mathcal{R}g$ comme on le voit en considérant $\gamma\colon t \mapsto g$.

Si γ est un chemin d'origine g et d'extrémité h, l'application $t \mapsto \gamma(1-t)$ est un chemin d'origine h et d'extrémité g.

Si $g\mathcal{R}h$ et $h\mathcal{R}k$ et si γ_1 (resp. γ_2) est un chemin de G d'orgine g (resp. h) et d'extrémité h (resp. k) l'application $\gamma_3\colon [0,1] \to \mathrm{G}$ définie par

$$\gamma_3(t) = \begin{cases} \gamma_1(2t) \text{ si } 0 \leq t \leq 1/2 \\ \gamma_2(2t-1) \text{ si } 1/2 \leq t \leq 1 \end{cases}$$

est un chemin d'origine g et d'extrémité k.

Les classes d'équivalence pour cette relation sont les composantes connexes par arcs de G. □

Lemme 12.2.2

La composante connexe par arcs G_0 de id dans G est un sous-groupe de G.

Démonstration. — Par définition G_0 contient id. Soient g et h deux éléments de G_0. Soit γ_1 (resp. γ_2) un chemin de G_0 reliant id à g (resp. h). Considérons l'application

$$\gamma_3 \colon t \mapsto \gamma_1(t)\big(\gamma_2(t)\big)^{-1}.$$

Pour tout $t \in [0,1]$ $\gamma_1(t)$ et $\gamma_2(t)$ appartiennent à G donc $\gamma_1(t)\gamma_2(t)$ appartient à G (en effet G est un sous-groupe de $\mathrm{SO}(3,\mathbb{R})$). Enfin l'application $g \mapsto g^{-1}$ est continue sur $\mathrm{SO}(3,\mathbb{R})$: si on identifie un élément de $\mathrm{SO}(3,\mathbb{R})$ à sa matrice dans la base canonique les coefficients de g^{-1} dépendent polynomialement des coefficients de g. De plus $\gamma_3(0) = \mathrm{id}\mathrm{id} = \mathrm{id}$ et $\gamma_3(1) = gh^{-1}$. Ainsi γ_3 est un chemin de id à gh^{-1} et gh^{-1} appartient à G_0. Il en résulte que G_0 est un sous-groupe de G. □

Lemme 12.2.3

Si G est distingué dans $\mathrm{SO}(3,\mathbb{R})$, alors G_0 est distingué dans $\mathrm{SO}(3,\mathbb{R})$.

Démonstration. — Soient g un élément de G_0, γ_1 un chemin de G de id à g et h un élément de $\mathrm{SO}(3,\mathbb{R})$. Considérons l'application

$$\gamma_2 \colon [0,1] \to \mathrm{SO}(3,\mathbb{R}) \qquad\qquad t \mapsto h\gamma_1(t)h^{-1}.$$

Pour tout $t \in [0,1]$ $\gamma_1(t)$ appartient à G et G étant distingué $h\gamma_1(t)h^{-1}$ appartient à G. L'application γ_1 est continue de même que la multiplication à gauche ou à droite par un élément de $\mathrm{SO}(3,\mathbb{R})$; par conséquent γ_2 est continue. De plus

$$\gamma_2(0) = h\mathrm{id}h^{-1} = \mathrm{id} \qquad\qquad \gamma_2(1) = hgh^{-1}.$$

L'application γ_2 est donc un chemin de id à hgh^{-1} et hgh^{-1} appartient à G_0. Autrement dit G_0 est distingué dans $\mathrm{SO}(3,\mathbb{R})$.

□

Lemme 12.2.4

Supposons que G soit un sous-groupe de $\mathrm{SO}(3,\mathbb{R})$ connexe par arcs, distingué et non réduit à $\{\mathrm{id}\}$. Alors G contient une rotation d'angle π.

Démonstration. — Si ϑ est l'angle d'une rotation g de $\mathbb{R}^3$ (si on change l'orientation de l'axe de la rotation l'angle est changé en son opposé donc ϑ est défini au signe près), alors il existe une base orthonormale dans laquelle sa matrice est

$$\begin{pmatrix} \cos\vartheta & -\sin\vartheta & 0 \\ \sin\vartheta & \cos\vartheta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

si bien que $\operatorname{Tr} g = 2\cos\vartheta + 1$ et donc l'application

$$\mathrm{SO}(3,\mathbb{R}) \to [-1,1] \qquad\qquad g \mapsto \cos\vartheta = \frac{\operatorname{Tr} g - 1}{2}$$

est une application continue.

Montrons que G contient une rotation r d'angle $\pm\frac{\pi}{2}$, alors r^2 sera une rotation de G d'angle π. Par hypothèse G contient un élément g distinct de id. Quitte à considérer g^{-1} on peut supposer qu'une mesure ϑ de son angle appartient à $]0,\pi]$. Si $\cos\vartheta \leq 0$ on pose $s = g$. Si $\cos\vartheta > 0$, alors $\vartheta \in \left]0, \frac{\pi}{2}\right]$. Notons N la partie entière de $\frac{\pi}{2\vartheta}$, *i.e.* $N = E\left(\frac{\pi}{2\vartheta}\right)$. Alors

$$N\vartheta \leq \frac{\pi}{2} < (N+1)\vartheta < 2 \times \frac{\pi}{2} = \pi.$$

En particulier g^{N+1} est une rotation d'angle $(N+1)\vartheta \in \left[\frac{\pi}{2}, \pi\right[$. On pose alors $s = g^{N+1}$. Ainsi G contient une rotation s d'angle ϑ avec $\cos\vartheta \leq 0$.

Le groupe G étant connexe par arcs il existe un chemin γ de id à s. L'application

$$\varphi\colon [0,1] \to [-1,1] \qquad\qquad t \mapsto \frac{\operatorname{Tr}(\gamma(t)) - 1}{2}$$

est continue car Tr et γ le sont. Par ailleurs $\varphi(0) = \cos 0 = 1$ et $\varphi(1) = \frac{\operatorname{Tr}(s)-1}{2} \leq 0$. Le théorème des valeurs intermédiaires assure donc l'existence de $t_0 \in [0,1]$ tel que $\varphi(t_0) = 0$. La rotation $r = \gamma(t_0)$ a un angle de $\pm\frac{\pi}{2}$. Par conséquent $R = r^2$ est une rotation d'angle π, *i.e.* un retournement. □

Lemme 12.2.5

Les retournements, c'est-à-dire les rotations d'angle π, engendrent le groupe $\mathrm{SO}(3,\mathbb{R})$.

Démonstration. — Tout élément de $\mathrm{SO}(3,\mathbb{R})$ est la composition d'un nombre pair de réflexions [2]. Il suffit donc de montrer que la composée de deux réflexions est une composée de deux retournements.

2. Soit $\Bbbk$ un corps commutatif. Soit E un $\Bbbk$-espace vectoriel de dimension n. Soit q une forme sesquilinéaire sur E, non dégénérée et symétrique. Rappelons qu'on appelle isométries de E relativement à q les automorphismes $u \in \mathrm{GL}(E)$ qui vérifient : $\forall\, x, y \in E$, $q(u(x), u(y)) = q(x,y)$. On appelle groupe orthogonal l'ensemble des isométries de E relativement à q et on note $O(q)$ ce groupe.

Soient x et y deux points de $\mathbb{R}^3 \smallsetminus \{0\}$. On désigne par τ_x et τ_y les réflexions respectives par rapport à $x^\perp$ et $y^\perp$. On a

$$\tau_x \circ \tau_y = (-\tau_x) \circ (-\tau_y)$$

et $-\tau_x$ et $-\tau_y$ sont des retournements. □

Lemme 12.2.6

Supposons que G soit un sous-groupe de $\mathrm{SO}(3,\mathbb{R})$ connexe par arcs, distingué et non réduit à $\{\mathrm{id}\}$. Alors $\mathrm{G} = \mathrm{SO}(3,\mathbb{R})$.

Démonstration. — D'après le Lemme 12.2.4 le groupe G contient un retournement R. Puisque G est distingué pour tout g dans $\mathrm{SO}(3,\mathbb{R})$ l'élément gRg^{-1} appartient à G. Par ailleurs $\mathrm{Tr}(gRg^{-1}) = \mathrm{Tr}(R)$ donc gRg^{-1} est aussi un retournement. Si le vecteur u appartient à l'axe Δ de R on a $(gRg^{-1})(g(u)) = g(u)$, c'est-à-dire gRg^{-1} est un retournement d'axe $g(\Delta)$. Étant donnée une droite D de $\mathbb{R}^3$ on peut trouver une rotation g de $\mathbb{R}^3$ telle que $D = g(\Delta)$ en prenant un axe orthogonal à D et Δ et un angle ad hoc (*i.e.* $\mathrm{SO}(3,\mathbb{R})$ agit transitivement sur les droites de $\mathbb{R}^3$). Le groupe G contient donc tous les retournements. On conclut en invoquant le Lemme 12.2.5 qui assure que les retournements engendrent $\mathrm{SO}(3,\mathbb{R})$. □

Démonstration du Théorème 12.2.1. — Soit G un sous-groupe distingué de $\mathrm{SO}(3,\mathbb{R})$. Montrons que $\mathrm{G} = \{\mathrm{id}\}$ ou $\mathrm{G} = \mathrm{SO}(3,\mathbb{R})$. Désignons par G_0 la composante connexe par arcs de id.

Théorème 12.2.2: [Per82]

Le groupe $O(q)$ est engendré par les réflexions.

Démontrons ce résultat par récurrence sur n.
La propriété est claire pour $n = 1$.
Soit $n > 1$ et supposons le résultat établi jusqu'à $n-1$. Soit $u \in O(q)$.

1. Supposons qu'il existe $x \in E$, $x \neq 0$, non isotrope tel que $u(x) = x$. Soit $H = \langle x \rangle^\perp$ l'hyperplan orthogonal, non isotrope lui aussi. Nous avons $u(H) = H$; nous pouvons appliquer l'hypothèse de récurrence à $u_{|H}$:
$$u_{|H} = \tau_1\tau_2 \dots \tau_r$$
où τ_i est une réflexion de H. Posons $\sigma_i = \tau_i \perp \mathrm{id}_{H^\perp}$; alors σ_i est une réflexion de E et comme $u(x) = x$ on a $u = \sigma_1\sigma_2 \dots \sigma_r$.
2. Soit $x \in E$, $x \neq 0$, non isotrope et soit $y = u(x)$. Supposons $x - y$ non isotrope. Soit $H = (x-y)^\perp$. Comme $x + y$ appartient à H, nous avons si τ_H désigne la réflexion par rapport à H $\tau_H(y) = x$ donc $\tau_H \circ u(x) = x$. Nous sommes ramené au cas 1. : $\tau_H \circ u = \tau_1\tau_2 \dots \tau_r$ et $u = \tau_H \circ \tau_1\tau_2 \dots \tau_r$.
3. Avec les notations de 2., si le vecteur $x - y$ est isotrope, alors $x + y$ est non isotrope (en effet si $q(x) = q(y) \neq 0$, alors l'un des vecteurs $x + y$ ou $x - y$ est non isotrope ; sinon $q(x+y) = 0 = 2q(x) + 2f(x,y)$, $q(x-y) = 0 = 2q(x) - 2f(x,y)$ d'où en ajoutant $4q(x) = 0$: contradiction). Alors, si $H = \langle x+y \rangle^\perp$, nous avons $\tau_H(y) = -x$. Soit alors $L = \langle x \rangle^\perp$, nous avons $\tau_L(x) = -x$, d'où $\tau_L\tau_H u(x) = x$ et nous sommes ramenés au cas 1.

Les Lemmes 12.2.2 et 12.2.3 assurent que G_0 est un sous-groupe distingué de $\mathrm{SO}(3,\mathbb{R})$; par définition G_0 est connexe par arcs. Si $\mathrm{G}_0 \neq \{\mathrm{id}\}$, alors $\mathrm{G}_0 = \mathrm{SO}(3,\mathbb{R})$ (Lemme 12.2.6) et donc $\mathrm{G} = \mathrm{SO}(3,\mathbb{R})$.

Supposons que $\mathrm{G}_0 = \{\mathrm{id}\}$ et montrons que $\mathrm{G} = \{\mathrm{id}\}$. Remarquons que toutes les composantes connexes par arcs de G sont des singletons ; en effet si g' est dans la composante de g, relié par le chemin γ, alors $t \mapsto g^{-1}\gamma(t)$ est un chemin de G reliant id à $g^{-1}g'$. Par suite $g^{-1}g'$ appartient à $\mathrm{G}_0 = \{\mathrm{id}\}$ et $g' = g$.

Raisonnons par l'absurde : supposons que G contienne un élément g distinct de id. Soit h une rotation quelconque non triviale. Soit ϑ une mesure de l'angle de h. Pour tout $t \in [0,1]$ on désigne par h_t la rotation de même axe et d'angle $t\vartheta$. L'application $t \mapsto h_t$ est continue car elle se traduit matriciellement dans une certaine base orthonormale par

$$t \mapsto \begin{pmatrix} \cos(t\vartheta) & -\sin(t\vartheta) & 0 \\ \sin(t\vartheta) & \cos(t\vartheta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

L'application

$$[0,1] \to \mathrm{G} \qquad\qquad t \mapsto h_t g h_t^{-1}$$

est un chemin de G (car G est distingué) d'origine g et d'extrémité hgh^{-1}. Il s'en suit que hgh^{-1} appartient à la composante connexe par arcs de g. Cette dernière étant réduite à un singleton on obtient $hgh^{-1} = g$. Or si g est une rotation d'axe Δ, alors hgh^{-1} est une rotation d'axe $h(\Delta)$. Par conséquent $h(\Delta) = \Delta$ ce qui est impossible (une droite ne peut pas être invariante par toutes les rotations de l'espace). □

12.3. Solides platoniciens

, [**CG13**, Chapitre 12]

Ce paragraphe illustre l'importance des groupes et des actions de groupes sur des objets concrets de l'espace.

Définitions 12.3.1

Un *polyèdre convexe* P est un compact d'intérieur non vide tel que P est l'intersection d'un nombre fini de demi-espaces délimités par des plans affines H_1, H_2, …, H_n.
Les *faces* de P sont les intersections de P avec les H_i. Ce sont des polygones convexes.
Leurs arêtes sont appelées *arêtes* de P et leurs sommets sont appelés *sommets*.

Proposition 12.3.1

Soit P un polyèdre convexe. Alors :

- ◇ Le nombre de côtés d'une face est au moins 3.
- ◇ Le nombre d'arêtes issues d'un sommet est égal au nombre de faces qui contiennent ce sommet et ce nombre est au moins 3.
- ◇ Une arête appartient à exactement deux faces.
- ◇ La somme des angles en un sommet est strictement inférieure à 2π.

Pour une démonstration de cet énoncé voir par exemple [**Ber77**].

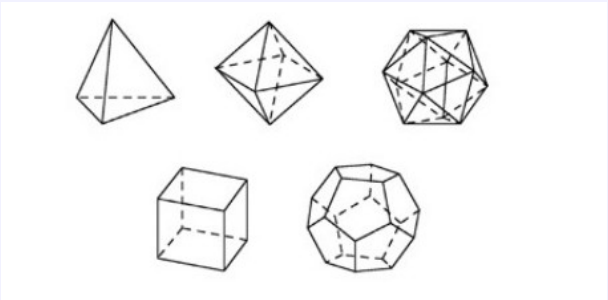
Définitions 12.3.2

Un polyèdre convexe est *régulier* si toutes ces faces sont des polygones réguliers à p côtés et tous ses sommets appartiennent à exactement q faces.
Dans $\mathbb{R}^3$, un *solide Platonicien* est un polyèdre de dimension 3 régulier (faces identiques et régulières) convexe.
Le couple (p, q) est appelé *symbole de Schläfli* du polyèdre régulier.

Théorème 12.3.1

Il existe exactement cinq types de polyèdres convexes réguliers correspondant aux symboles de Schläfli suivants :

polyèdre	symbole de Schläfli
tétraèdre régulier	$(3, 3)$
cube	$(4, 3)$
octaèdre régulier	$(3, 4)$
icosaèdre régulier	$(3, 5)$
dodécaèdre régulier	$(5, 3)$



Démonstration. — Soit (p, q) le symbole de Schläfli d'un polyèdre régulier. Étant donné que chaque face a au moins trois côtés et que chaque sommet est entouré par au moins trois faces, nous avons p, $q \geq 3$.

La somme des angles dans un polygone convexe à p côtés vaut $(p-2)\pi$ (cela se voit en découpant le polygone en $p-2$ triangles à partir d'un sommet choisi). Les angles d'un polygone régulier à p côtés sont donc égaux à $\frac{p-2}{p}\pi$. Puisque $p \geq 3$, nous avons $\frac{p-2}{p}\pi \geq \frac{\pi}{3}$. La somme des angles autour d'un sommet est strictement inférieure à 2π donc $q\frac{\pi}{3} < 2\pi$ et donc $q < 6$. Comme $q \geq 3$, nous avons l'inégalité $3\,\frac{p-2}{p}\pi < 2\pi$ et donc $p < 6$. Il en résulte que $3 \leq p$, $q \leq 5$.

Les couples $(4, 4)$, $(4, 5)$, $(5, 4)$ et $(5, 5)$ ne satisfont pas la condition $q\frac{p-2}{q}\pi < 2\pi$ et donc les seuls couples possibles sont ceux annoncés. □

La liste des polyèdres réguliers étant établie, nous nous intéressons à leurs groupes d'isométries. Le *dual* d'un polyèdre est l'enveloppe convexe des milieux de ses faces. Par exemple le dual du cube est un octaèdre. Plus généralement le dual du polyèdre régulier de symbole (p, q) est le polyèdre régulier de symbole (q, p). Le passage au polyèdre dual échange les faces et les sommets. On peut vérifier qu'un polyèdre et son dual ont le même groupe d'isométries.

Proposition 12.3.2

Soit $X \subset \mathbb{R}^3$. Désignons par $\mathrm{Isom}(X)$ le groupe des isométries de $\mathbb{R}^3$ qui préservent X.
Si O est le centre de symétrie de X et si g est une isométrie de X, alors $g(O) = O$.
De plus $\mathrm{Isom}(X) \simeq \mathrm{Isom}^+(X) \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. — Tout élément du groupe affine $\mathrm{GA}(3, \mathbb{R})$ conserve le barycentre donc g conserve le centre de symétrie de X, *i.e.* $g(O) = O$.

Notons $s_O \in \mathrm{Isom}^-(X)$ la symétrie centrale en O.

Le morphisme

$$\mathrm{Isom}(X) \to \mathrm{Isom}^+(X) \times \mathbb{Z}/2\mathbb{Z} \qquad g \mapsto \begin{cases} (g, 0) \text{ si } g \in \mathrm{Isom}^+(X) \\ (gs_O, 1) \text{ sinon} \end{cases}$$

est un isomorphisme. De plus s_O commute avec tout élément de $\mathrm{Isom}^+(X)$; en effet vectoriellement il s'agit de l'homothétie de rapport -1. Par conséquent le produit est direct. □

Proposition 12.3.3

Le groupe d'isométries du tétraèdre régulier Δ_4 est isomorphe à $\mathfrak{S}_4$.
Le groupe d'isométries directes du tétraèdre régulier Δ_4 est isomorphe à $\mathcal{A}_4$.

Démonstration. — Notons Δ_4 le tétraèdre régulier. Désignons par $\mathrm{Isom}(\Delta_4)$ les isométries du tétraèdre régulier et par $\mathrm{Isom}^+(\Delta_4)$ les isométries directes du tétraèdre régulier. Soit $\mathfrak{S} = \{A, B, C, D\}$ l'ensemble des sommets du tétraèdre.

Considérons l'action de $\mathrm{Isom}(\Delta_4)$ sur $\mathfrak{S}$. Ainsi

$$\varphi\colon \mathrm{Isom}(\Delta_4) \to \mathfrak{S}_4 \qquad\qquad g \mapsto g_{|\mathfrak{S}}$$

est un morphisme de groupes.

Si $\varphi(g) = \mathrm{id}_{\mathfrak{S}}$, alors g stabilise $\mathfrak{S}$ qui est un repère de l'espace affine ; il en résulte que $g = \mathrm{id}_{\mathbb{R}^3}$. Par suite φ est injectif, *i.e.* $\mathrm{Isom}(\Delta_4)$ s'injecte dans $\mathfrak{S}_4$.

Soit M le milieu du segment $[AB]$. La réflexion r_{AB} par rapport au plan MCD réalise la transposition $(A\ B)$, *i.e.* $\varphi(r_{AB}) = (A\ B)$. Ainsi toutes les transpositions appartiennent à $\mathrm{Isom}(\Delta_4)$ d'où l'inclusion $\mathfrak{S}_4 \subset \mathrm{Isom}(\Delta_4)$ (rappelons que les transpositions engendrent le groupe symétrique).

Finalement φ est un isomorphisme et $\mathrm{Isom}(\Delta_4) \simeq \mathfrak{S}_4$.

Le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$ est le groupe alterné $\mathcal{A}_n$. Le groupe $\mathrm{Isom}^+(\Delta_4)$ étant d'indice 2 dans $\mathrm{Isom}(\Delta_4)$ nous avons $\mathrm{Isom}^+(\Delta_4) \simeq \mathcal{A}_4$. □

Proposition 12.3.4

Le groupe d'isométries directes du cube est isomorphe à $\mathfrak{S}_4$.
Le groupe d'isométries du cube est isomorphe à $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.
Par dualité le groupe d'isométries directes de l'octaèdre régulier est isomorphe à $\mathfrak{S}_4$ et le groupe d'isométries de l'octaèdre régulier est isomorphe à $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Une partie de cet énoncé a déja été démontré (Théorème 11.5.1), par soucis de clarté nous démontrons ci-dessous la Proposition 12.3.4 dans son intégralité.

Démonstration. — Notons C_6 le cube. Désignons par $\mathrm{Isom}(C_6)$ les isométries du cube et par $\mathrm{Isom}^+(C_6)$ les isométries directes du cube. Soit $\mathcal{D} = \{D_1, D_2, D_3, D_4\}$ l'ensemble des grandes diagonales du cube (elles sont préservées par les isométries de C_6 car ce sont les plus grandes longueurs que l'on peut trouver dans le cube).

Ainsi

$$\varphi\colon \mathrm{Isom}^+(C_6) \to \mathfrak{S}_4 \qquad\qquad g \mapsto g_{|\mathcal{D}}$$

Notons $D_i = A_iG_i$ les diagonales de C_6. Désignons par s_0 la symétrie centrale en 0. Si $\varphi(g) = \mathrm{id}_{\mathcal{D}}$, alors

- ◇ ou bien $\begin{cases} g(A_1) = A_1 \\ g(G_1) = G_1 \end{cases}$ et dans ce cas en utilisant le fait que g fixe toutes les diagonales et les deux points opposés A_1 et G_1 nous obtenons que g fixe tous les sommets. Il en résulte que $g = \mathrm{id}_{\mathbb{R}^3}$.
- ◇ ou bien $\begin{cases} g(A_1) = G_1 \\ g(G_1) = A_1 \end{cases}$ et $s_0g = \mathrm{id}$ d'après ce qui précède. Il s'en suit que g est la symétrie centrale s_0 en 0 : contradiction avec $g \in \mathrm{Isom}^+(C_6)$.

Ainsi $\ker \varphi = \{\mathrm{id}_{\mathbb{R}^3}\}$ et nous avons l'inclusion $\mathrm{Isom}^+(C_6) \subset \mathfrak{S}_4$.

Les transpositions sont toutes réalisées grâce à des retournements d'axes reliant les milieux des arêtes joignant les diagonales).

Par suite $\mathrm{Isom}^+(C_6) \simeq \mathfrak{S}_4$.

La seconde assertion découle du fait que le cube admet un centre de symétrie et de la Proposition 12.3.2. □

Proposition 12.3.5

Le groupe d'isométries du dodécaèdre est isomorphe à $\mathcal{A}_5 \times \mathbb{Z}/2\mathbb{Z}$.
Le groupe d'isométries directes du dodécaèdre est isomorphe à $\mathcal{A}_5$.
Par dualité le groupe d'isométries de l'icosaèdre est isomorphe à $\mathcal{A}_5 \times \mathbb{Z}/2\mathbb{Z}$ et son groupe d'isométries directes est isomorphe à $\mathcal{A}_5$.

Idée de la démonstration. — Notons P_{12} le dodécaèdre. Désignons par $\mathrm{Isom}(P_{12})$ les isométries du dodécaèdre et par $\mathrm{Isom}^+(P_{12})$ les isométries du dodécaèdre.

On admet qu'exactement 5 cubes distincts $C_1, C_2, \ldots, C_5$ sont inscrits dans le dodécaèdre.

Le groupe $\mathrm{Isom}^+(P_{12})$ agit sur l'ensemble $\mathcal{C} = \{C_1, C_2, C_3, C_4, C_5\}$ des cubes inscrits d'où le morphisme

$$\varphi\colon \mathrm{Isom}^+(P_{12}) \to \mathfrak{S}_5 \qquad\qquad g \mapsto g_{|\mathcal{C}}$$

Soit g dans $\ker \varphi$, *i.e.* soit g dans $\mathrm{Isom}^+(P_{12})$ tel que $g_{|\mathcal{C}} = \mathrm{id}_{\mathcal{C}}$. Alors $g(C_i) = C_i$ pour $1 \leq i \leq 5$. Alors g fixe les grandes diagonales du dodécaèdre et n'est pas une symétrie centrale ; il s'en suit que $g = \mathrm{id}_{\mathbb{R}^3}$. L'action est donc fidèle et $\mathrm{Isom}^+(P_{12}) \subset \mathfrak{S}_5$.

Déterminons le nombre d'éléments de $\mathrm{Isom}^+(P_{12})$. Comme les éléments de $\mathrm{Isom}^+(P_{12})$ sont des rotations cela revient à compter les axes possibles puis les angles possibles :

- l'identité ;
- axe de sommet à sommet opposé, $\frac{20}{2} = 10$ axes possibles, les angles (non nuls) $\frac{2\pi}{3}$, $\frac{4\pi}{3}$;
- axe de milieu d'arête à milieu d'arête opposée, $\frac{30}{2} = 15$ axes possibles, les angles (non nuls) π ;
- axe passant par le centre de P_{12} et le centre d'une des faces de P_{12}, $\frac{12}{2} = 6$ axes possibles, les angles (non nuls) $\frac{2\pi}{5}$, $\frac{4\pi}{5}$, $\frac{6\pi}{5}$, $\frac{8\pi}{5}$.

En tout cela fait $10 \times 2 + 15 \times 1 + 6 \times 4 + 1 = 60$ éléments.

Le dodécaèdre ayant un centre de symétrie la Proposition 12.3.2 assure que $\mathrm{Isom}(P_{12}) \simeq \mathcal{A}_5 \times \mathbb{Z}/2\mathbb{Z}$. □

Sous-groupes de Sylow d'un groupe d'isométries. — Les groupes d'isométries des solides platoniciens ont l'avantage d'avoir des p-Sylow « visibles à l'oeil nu ». Voici quelques exemples témoins de l'interaction omniprésente entre groupes et géométrie :

- ◇ On peut se demander combien $\mathcal{A}_4$ possède de 3-Sylow. Bien sûr, nous avons la méthode arithmétique qui consiste à regarder les valeurs possibles (ici 1 et 4) et à éliminer selon certaines considérations. Mais nous pouvons aussi utiliser une méthode algébrique puisque $\mathcal{A}_4$ se réalise comme groupe d'isométries directes du tétraèdre. Comme ses 3-Sylow ont pour ordre 3, ce sont des rotations d'ordre 3 et la seule possibilité est la rotation autour d'un axe passant par le milieu des faces. Il y a donc quatre 3-Sylow correspondant aux quatre faces d'un tétraèdre.
- ◇ On peut se demander combien $\mathfrak{S}_4$ possède de 3-Sylow. Même méthode, mais cette fois-ci le groupe $\mathfrak{S}_4$ se réalise comme groupe d'isométrie directe de deux manières : celui du cube et celui de l'octaèdre. Visuellement, c'est en tant que groupe de l'octaèdre qu'on voit le mieux les 3-Sylow car ils sont en bijection avec ses paires de faces opposées (triangulaires). Le groupe $\mathfrak{S}_4$ contient donc quatre 3-Sylow.
- ◇ On peut se demander combien $\mathcal{A}_5$ possède de 3-Sylow. Réponse : 10 correspondant aux paires de faces opposées de l'icosaèdre.
- ◇ On peut se demander combien $\mathcal{A}_5$ possède de 5-Sylow. Réponse : 6 correspondant aux paires de faces opposées du dodécaèdre.
- ◇ On peut se demander combien $\mathfrak{S}_4$ possède de 2-Sylow. Réponse : 3... justification géométrique bien sûr !

12.4. Les sous-groupes finis de $\mathrm{SO}(3,\mathbb{R})$

, [**CG17**, chap. 12], [**CG15**, chap. 9], [**Szp09**, p. 434-437]

Théorème 12.4.1

Tout sous-groupe fini de $\mathrm{SO}(3,\mathbb{R})$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, D_{2n}, $\mathcal{A}_4$, $\mathfrak{S}_4$ ou $\mathcal{A}_5$.
Plus précisément si G est un sous-groupe fini de $\mathrm{SO}(3,\mathbb{R})$, alors G est conjugué au groupe des rotations préservant l'un des polyèdres suivants (les cas $n = 1$, 2 mis à part)

- ◇ $\mathrm{Isom}^+($ pyramide de base un polygone régulier à n côtés $) \simeq \mathbb{Z}/n\mathbb{Z}$;
- ◇ $\mathrm{Isom}^+($ double pyramide de base un polygone régulier à n côtés $) \simeq \mathrm{D}_{2n}$;
- ◇ $\mathrm{Isom}^+($ tétraèdre régulier $) \simeq \mathcal{A}_4$;
- ◇ $\mathrm{Isom}^+($ cube $) \simeq \mathfrak{S}_4$;
- ◇ $\mathrm{Isom}^+($ icosaèdre régulier $) \simeq \mathcal{A}_5$.

Lemme 12.4.1: (Formule de Burnside)

Soit G un groupe fini agissant sur un ensemble fini E. Désignons par $\mathrm{G}\backslash E$ l'ensemble des orbites et par $\mathrm{Fix}(g) = \{x \in E \,|\, g \cdot x = x\}$ l'ensemble des points fixes de g dans E. Alors

$$|\mathrm{G}\backslash E| = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|$$

Démonstration. — Soit $S = \{(x, g) \in E \times \mathrm{G} \,|\, g \cdot x = x\}$. On calcule le cardinal de S de deux façons différentes. D'une part

$$|S| = \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|$$

et d'autre part

$$\begin{aligned} |S| &= \sum_{x \in E} |\mathrm{Stab}_{\mathrm{G}}(x)| = \sum_{\mathcal{O} \in \mathrm{G}\backslash E} \sum_{x \in \mathcal{O}} |\mathrm{Stab}_{\mathrm{G}}(x)| \\ &= \sum_{\mathcal{O} \in \mathrm{G}\backslash E} \sum_{x \in \mathcal{O}} \frac{|\mathrm{G}|}{|\mathcal{O}|} = |\mathrm{G}| \sum_{\mathcal{O} \in \mathrm{G}\backslash E} \sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}|} \\ &= |\mathrm{G}| \sum_{\mathcal{O} \in \mathrm{G}\backslash E} |\mathcal{O}| \cdot \frac{1}{|\mathcal{O}|} = |\mathrm{G}| \sum_{\mathcal{O} \in \mathrm{G}\backslash E} 1 \\ &= |\mathrm{G}| \cdot |\mathrm{G}\backslash E|. \end{aligned}$$

□

Lemme 12.4.2

Tout sous-groupe fini G de $\mathrm{SO}(2, \mathbb{R})$ est monogène, engendré par la rotation d'angle $\frac{2\pi}{n}$ où $n = |\mathrm{G}|$.

Démonstration. — Si n est un entier, nous notons H_n le sous-groupe de $\mathrm{SO}(2, \mathbb{R})$ formé des rotations d'angle multiple de $\frac{2\pi}{n}$. C'est un sous-groupe d'ordre n engendré par la rotation d'angle $\frac{2\pi}{n}$.

Soit G un sous-groupe de $\mathrm{SO}(2, \mathbb{R})$ d'ordre n. Pour tout g dans G nous avons $g^n = \mathrm{id}$; en particulier tout élément g de G est une rotation d'angle multiple de $\frac{2\pi}{n}$. Autrement dit $\mathrm{G} \subset \mathrm{H}_n$. Par ailleurs $|\mathrm{H}_n| = n$ donc $\mathrm{G} = \mathrm{H}_n$.

□

Esquisse de démonstration du Théorème 12.4.1. — Soit G un sous-groupe fini d'ordre n de $\mathrm{SO}(3, \mathbb{R})$. À tout élément de $\mathrm{G} \smallsetminus \{\mathrm{id}\}$ on associe deux pôles qui sont l'intersection de l'axe de la

rotation avec la sphère unité de $\mathbb{R}^3$. Le groupe G agit sur l'ensemble E des pôles des éléments de G qui est fini et par définition on a l'inégalité suivante

$$|E| \leq 2(n-1).$$

Toute rotation non triviale de G fixe exactement deux pôles et l'identité fixe tous les éléments de G. Par conséquent la formule de Burnside (Lemme 12.4.1) assure que le nombre k d'orbites de cette action est

$$k = \frac{2(n-1)+|E|}{n} = 2 + \frac{|E|-2}{n}$$

À partir de $|E| \leq 2(n-1)$ et $k = 2 + \frac{|E|-2}{n}$ on obtient

$$k \leq 2 + \frac{2(n-1)-2}{n} = \frac{4(n-1)}{n} < 4.$$

Ainsi k appartient à $\{2, 3\}$.

a. Si $k = 2$, alors G est cyclique. En effet puisque

$$k = 2 + \frac{|E|-2}{n}$$

on a $k = 2$ si et seulement si $|E| = 2$. Dans ce cas toutes les rotations de G ont le même axe et G peut être vu comme un sous-groupe fini de rotations du plan orthogonal à cet unique axe. Le Lemme 12.4.2 implique que G est cyclique.

b. Supposons que $k = 3$. Notons ω_1, ω_2 et ω_3 les orbites ; désignons par n_1, n_2 et n_3 les cardinaux des stabilisateurs correspondants. Quitte à réindicer les n_i on peut supposer que $n_1 \leq n_2 \leq n_3$.

Alors

b.1. si $n_1 = n_2 = 2$, alors $|\mathrm{G}| = |\mathrm{D}_{2n_3}| = 2n_3$;

b.2. sinon on est dans l'une des situations suivantes :

- ◇ $(n_1, n_2, n_3) = (2, 3, 3)$ et $|\mathrm{G}| = |\mathcal{A}_4| = 12$;
- ◇ $(n_1, n_2, n_3) = (2, 3, 4)$ et $|\mathrm{G}| = |\mathfrak{S}_4| = 24$;
- ◇ $(n_1, n_2, n_3) = (2, 3, 5)$ et $|\mathrm{G}| = |\mathcal{A}_5| = 60$.

Commençons par déterminer les triplets possibles. La formule de Burnside assure que $3 = 2 + \frac{|E|-2}{n}$. Par ailleurs $|\omega_i| = \frac{n}{n_i}$ donc

$$\frac{|E|}{n} = \frac{|\omega_1| + |\omega_2| + |\omega_3|}{n} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3}.$$

Finalement on obtient la condition

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1 + \frac{2}{n} \tag{12.4.1}$$

Par définition un pôle est fixé par au moins l'identité et une autre rotation donc $n_1 \geq 2$. La condition (12.4.1) assure que $n_1 = 2$. Un argument analogue assure que $2 \leq n_2 \leq n_3$.

Si $n_2 = 2$ alors n_3 est arbitraire et $n = 2n_3$. Si $n_2 = 3$, alors $3 \leq n_3 \leq 5$ ce qui d'où les trois cas ci-dessus. De plus $n = \frac{12n_3}{6-n_3}$, soit $n = 12$ (resp. $n = 24$, resp. $n = 60$) si $n_3 = 3$ (resp. $n_3 = 4$, resp. $n_3 = 5$).

Traitons par exemple le cas $|\mathrm{G}| = 12$, *i.e.* $(n_1, n_2, n_3) = (2, 3, 3)$. L'orbite ω_3 est de cardinal $\frac{12}{3} = 4$; désignons par x_1, x_2, x_3 et x_4 ses éléments. On peut supposer que x_1 et x_2 ne sont pas symétriques par rapport à l'origine. Puisque $|\mathrm{Stab}(x_1)|\,|\mathrm{Orb}(x_1)| = 12$ il existe une rotation $r \in \mathrm{Stab}(x_1)$ d'ordre 3 ; quitte à réindicer les x_i on a $x_3 = r(x_2)$, $x_4 = r^{-1}(x_2)$. En particulier les points x_2, x_3 et x_4 sont équidistants de x_1. On peut bien entendu faire le même raisonnement pour tout x_i ; on obtient donc que x_1, x_2, x_3 et x_4 sont les sommets d'un tétraèdre régulier préservé par G. Or le groupe des rotations qui préservent un tétraèdre est d'ordre 12 et G est d'ordre 12. Le groupe G coïncide donc avec le groupe des rotations préservant un tétraèdre (isomorphe à $\mathcal{A}_4$ qui est l'unique sous-groupe d'indice 2 dans $\mathfrak{S}_4$).

□

Remarque 12.4.1. — Le groupe $\mathfrak{S}_4$ intervient à la fois comme $\mathrm{Isom}^+(\text{cube})$ et comme $\mathrm{Isom}(\text{tétraèdre})$. On peut transposer dans chacun de ces trois points de vue tout ce que l'on sait sur ce groupe (classe de conjugaison, sous-groupes d'ordre donné, etc)

12.5. Géométrie affine

12.5.1. Espaces affines. — Rappelons qu'une action d'un groupe G sur un ensemble E est simplement transitive si elle est transitive et libre, *i.e.* si pour tous x, y dans E il existe un unique $g \in \mathrm{G}$ tel que $gx = y$.

Définition 12.5.1

Soit E un espace vectoriel. Un *espace affine* $\mathcal{A}$ est un ensemble muni d'une action simplement transitive de $(E, +)$.
L'espace vectoriel E est appelé *la direction de* $\mathcal{A}$.
La *dimension* de $\mathcal{A}$ est la dimension de E.

Soit $\alpha\colon E \times \mathcal{A} \to \mathcal{A}$ l'action ci-dessus. Notons $\tau_v(A) = \alpha(v, A)$. L'application $A \mapsto \tau_v(A)$ est appelée *translation de vecteur* v. On note aussi $\tau_v(A) = A + v$. Étant donnée que α est une action, nous avons

$$\tau_v \circ \tau_u = \tau_{u+v}$$

ce qui correspond à $(A + u) + v = A + (u + v)$.

Soit $\mathcal{A}$ un espace affine de direction E. Soient A, B deux éléments de $\mathcal{A}$. Il existe un unique $v \in E$ tel que $B = A + v$. Nous désignons v par $\overrightarrow{AB} \in E$.

Lemme 12.5.1: [Relation de Chasles]

Soient A, B et C trois points d'un espace affine. Alors
$$\overrightarrow{AC} = \overrightarrow{AB} + \overrightarrow{BC}.$$

Démonstration. — Posons $u = \overrightarrow{AB}$ et $v = \overrightarrow{BC}$. Nous avons $B = A + u$ et $C = B + v$. Alors $A + u + v = C$ et $\overrightarrow{AC} = u + v$ ou encore $\overrightarrow{AC} = \overrightarrow{AB} + \overrightarrow{BC}$. □

Définitions 12.5.1

Soit $\mathcal{A}$ un espace affine de direction E. Soit F un sous-espace vectoriel de E.
Un *sous-espace affine* $\mathcal{F}$ de direction F est un ensemble tel qu'il existe $A \in \mathcal{F}$ avec $\mathcal{F} = \{A + v \mid v \in F\}$.
En particulier nous appelons *droite affine* un sous-espace affine de dimension 1 et *plan affine* un sous-espace affine de dimension 2.

Lemme 12.5.2

Soit $(\mathcal{F}_i)_{i\in I}$ une collection de sous-espaces affines de direction $(F_i)_{i\in I}$.
L'intersection $\bigcap_{i\in I} \mathcal{F}_i$ est vide ou un sous-espace affine de direction $\bigcap_{i\in I} F_i$.

Démonstration. — Supposons que l'intersection $\bigcap_{i\in I} \mathcal{F}_i$ soit non vide. Soit $A \in \bigcap_{i\in I} \mathcal{F}_i$. On écrit $\mathcal{F}_i = \{A + v \mid v \in F_i\}$ pour tout $i \in I$. Un point $B = A + v$ appartient à $\bigcap_{i\in I} \mathcal{F}_i$ si et seulement si v appartient à $\bigcap_{i\in I} F_i$. □

Définition 12.5.2

Soient $\mathcal{A}$ un espace affine et $P \subset \mathcal{A}$ un sous-espace non vide.
Le *sous-espace engendré par* P est l'intersection de tous les sous-espaces affines qui contiennent P. C'est le plus petit sous-espace affine (au sens de l'inclusion) qui contient P.

Exemple 12.5.1. — Soient E un $\Bbbk$-espace vectoriel et $\mathcal{A}$ un espace affine de direction E. Soient A et B deux points distincts de $\mathcal{A}$. Le sous-espace affine engendré par A et B est la droite $(AB) = \{A + \lambda\overrightarrow{AB} \mid \lambda \in \Bbbk\}$.

Définition 12.5.3

Deux sous-espaces affines sont *parallèles* s'ils ont même direction.

Définition 12.5.4

Soient $\mathcal{A}$ un espace affine et O un point de $\mathcal{A}$. L'application

$$E \to \mathcal{A}, \qquad v \mapsto O + v$$

est une bijection permettant de transporter la structure d'espace vectoriel de E à $\mathcal{A}$. L'espace vectoriel obtenu est appelé le *vectorialisé* de $\mathcal{A}$ en O.

Exemple 12.5.2. — Un espace vectoriel E possède une structure canonique d'espace affine obtenue en faisant agir $(E, +)$ sur lui-même par translations.

Remarque 12.5.1. — Attention la structure d'espace vectoriel ainsi construite dépend du point O choisi.

Ainsi un espace vectoriel est la donnée d'un espace affine et d'une origine. En oubliant l'origine d'un espace vectoriel nous obtenons un espace affine et en rajoutant une origine à un espace affine nous obtenons un espace vectoriel.

Définition 12.5.5

Soient $\mathcal{A}$ et $\mathcal{A}'$ deux espaces affines de directions E et E', espaces vectoriels sur un même corps.
Une application $\varphi\colon \mathcal{A} \to \mathcal{A}'$ est *affine* s'il existe une application linéaire $L\colon E \to E'$ telle que

$$\overrightarrow{\varphi(A)\varphi(B)} = L(\overrightarrow{AB}) \quad \forall\, A,\, B \in \mathcal{A}.$$

Proposition 12.5.1

L'image directe d'un sous-espace affine par une application affine est un sous-espace affine.
L'image réciproque d'un sous-espace affine par une application affine est un sous-espace affine.

Démonstration. — Soit φ une application affine de partie linéaire L. Soit $\mathcal{F}$ un sous-espace affine de direction F contenant un point A. Alors

$$\begin{aligned}\varphi(\mathcal{F}) &= \{\varphi(B) \,|\, B \in \mathcal{F}\}\\ &= \{\varphi(A) + L(\overrightarrow{AB}) \,|\, B \in \mathcal{F}\}\\ &= \{\varphi(A) + L(u) \,|\, u \in F\}\\ &= \{\varphi(A) + v \,|\, v \in L(F)\}\end{aligned}$$

Par suite $\varphi(\mathcal{F})$ est le sous-espace affine contenant $\varphi(A)$ et de direction $L(F)$.

La seconde assertion se démontre de la même façon et repose sur le fait que l'image réciproque d'un sous-espace vectoriel par une application linéaire est un sous-espace vectoriel. □

Rappelons que trois points sont *alignés* s'il existe une droite affine les contenant tous les trois.

Corollaire 12.5.1

Les applications affines préservent l'alignement.

Démonstration. — L'image d'une droite affine est un sous-espace affine de dimension au plus 1, *i.e.* une droite ou un point. Par conséquent les images de trois points alignés sont encore alignées. □

12.5.2. Groupe affine. —

Lemme 12.5.3

Soit $\mathcal{A}$ un espace affine de direction E.
Soient φ et φ' deux applications affines de parties linéaires L et L'.
La composée $\varphi' \circ \varphi$ est affine de partie linéaire $L' \circ L$.
Si φ est affine inversible de partie linéaire L, alors φ^{-1} est affine de partie linéaire L^{-1}.

Démonstration. — Soient φ, φ' deux applications affines de parties linéaires L, L'.

Si A et B sont deux points de $\mathcal{A}$, alors

$$\overrightarrow{\varphi'(\varphi(A))\varphi'(\varphi(B))} = L'\Big(\overrightarrow{\varphi(A)\varphi(B)}\Big) = L'(L(\overrightarrow{AB})).$$

Autrement dit $\varphi' \circ \varphi$ est affine de partie linéaire $L' \circ L$.

Soit φ une application affine inversible de partie linéaire L. Puisque φ est bijective, pour tout $v \in E$ il existe un unique $u \in E$ tel que $\varphi(A + u) = \varphi(A) + v$, soit

$$\overrightarrow{\varphi(A)\varphi(A + u)} = L(u) = v$$

ainsi L est linéaire inversible.

Pour montrer que φ^{-1} est affine il suffit de montrer que

$$\varphi^{-1}(\varphi(A)+v) = A + L^{-1}(v) \quad \forall\, A \in \mathcal{A}, \forall\, v \in E.$$

Soient $A \in \mathcal{A}$ et $v \in E$; posons $u = L^{-1}(v)$; alors

$$\varphi^{-1}(\varphi(A)+v) = \varphi^{-1}(\varphi(A)+L(u)) = \varphi^{-1}(\varphi(A+u)) = A+u = A+L^{-1}(v).$$

□

Théorème 12.5.1

Soit $\mathcal{A}$ un espace affine de direction E.
Les transformations affines inversibles forment un groupe appelé *groupe affine* $\mathrm{GA}(\mathcal{A})$.
De plus

$$\mathrm{GA}(\mathcal{A}) \simeq \mathrm{GL}(E) \ltimes E.$$

Démonstration. — L'identité est une application affine de partie linéaire l'identité de E.

Le Lemme 12.5.3 assure que l'ensemble des transformations affines inversibles est stable par composition et passage à l'inverse. C'est donc un sous-groupe du groupe des bijections de $\mathcal{A}$.

L'application

$$\Psi\colon \mathrm{GA}(\mathcal{A}) \to \mathrm{GL}(E), \qquad \varphi \mapsto L$$

qui associe à une application affine inversible sa partie linéaire est un morphisme de groupes (Lemme 12.5.3). Son noyau est donc l'ensemble des applications affines de partie linéaire l'identité, c'est-à-dire pour tous A, B dans $\mathcal{A}$

$$\overrightarrow{\varphi(A)\varphi(B)} = \overrightarrow{AB}.$$

Fixons A ; posons $u = \overrightarrow{A\varphi(A)}$. Alors

$$\overrightarrow{B\varphi(B)} = \overrightarrow{BA} + \overrightarrow{A\varphi(A)} + \overrightarrow{\varphi(A)\varphi(B)} = \overrightarrow{BA} + \overrightarrow{A\varphi(A)} + \overrightarrow{AB} = \overrightarrow{A\varphi(A)} = u \quad \forall\, B \in \mathcal{A}.$$

Par conséquent $\varphi(B) = B + u$ et φ est la translation de vecteur u.

Soit $O \in \mathcal{A}$ une origine. Vectorialisons $\mathcal{A}$ en O. Nous pouvons alors identifier $\mathrm{GL}(E)$ avec le sous-groupe de $\mathrm{GA}(\mathcal{A})$ qui fixe O. Plus précisément pour $A \in \mathcal{A}$ et $L \in \mathrm{GL}(E)$

$$L(A) = O + L(\overrightarrow{OA}).$$

De même nous identifions $(E, +)$ avec le groupe des translations.

Un élément appartenant à la fois au groupe des translations et à $\mathrm{GL}(E)$ est donc un élément qui fixe O et dont la partie linéaire est l'identité, c'est donc l'identité de $\mathcal{A}$. Le groupe des translations coïncide avec $\ker \Psi$, c'est donc un sous-groupe distingué de $\mathrm{GA}(\mathcal{A})$. Remarquons de plus que tout élément de $\mathrm{GA}(\mathcal{A})$ est la composée d'une translation et d'une application linéaire. En effet soit φ une application affine de partie linéaire L. Posons $u = \overrightarrow{O\varphi(O)}$. Pour

tout $A \in \mathcal{A}$ nous avons $\overrightarrow{\varphi(O)\varphi(A)} = L(\overrightarrow{OA})$ et donc $\overrightarrow{O\varphi(A)} = L(\overrightarrow{OA}) + \overrightarrow{O\varphi(O)}$. En utilisant l'identification entre A et $\overrightarrow{OA}$ cela s'écrit

$$\varphi(A) = L(A) + u;$$

autrement dit φ est la composée de l'application linéaire L et de la translation de vecteur u. □

Remarque 12.5.2. — Dans l'identification $\mathrm{GA}(\mathcal{A}) \simeq \mathrm{GL}(E) \ltimes E$ nous utilisons une origine. L'identification n'est pas canonique puisqu'elle dépend de ce choix.

12.5.3. Théorème fondamental de la géométrie affine. — Une bijection φ d'un espace affine $\mathcal{A}$ *préserve l'alignement* si pour tout triplet de points A, B, C ces points sont alignés si et seulement si les points $\varphi(A)$, $\varphi(B)$ et $\varphi(C)$ sont alignés.

Théorème 12.5.2

[Théorème fondamental de la géométrie affine] Soit $\mathcal{A}$ un espace affine réel de dimension finie ≥ 2.
Toute bijection de $\mathcal{A}$ qui préserve l'alignement est une transformation affine.

Remarque 12.5.3. — Cet énoncé est propre au cas réel.

Proposition 12.5.2

Le seul automorphisme du corps $(\mathbb{R}, +, \times)$ est l'identité.

Démonstration. — Soit σ un automorphisme de $(\mathbb{R}, +, \times)$. Puisque 0 (resp. 1) est l'élément neutre de la loi $+$ (resp. $\times$) nous avons $\sigma(0) = 0$ et $\sigma(1) = 1$. Pour tout $n \in \mathbb{N}$ nous avons

$$\sigma(n) = \sigma(\underbrace{1 + 1 + \ldots + 1}_{n \text{ fois}}) = \underbrace{\sigma(1) + \sigma(1) + \ldots + \sigma(1)}_{n \text{ fois}} = \underbrace{1 + 1 + \ldots + 1}_{n \text{ fois}} = n.$$

Étant donné que

$$0 = \sigma(n + (-n)) = \sigma(n) + \sigma(-n) = n + \sigma(-n)$$

nous obtenons que $\sigma(-n) = -n$. Ainsi pour tout $n \in \mathbb{Z}$ nous avons $\sigma(n) = n$.

Pour tout $p \in \mathbb{N}^*$ nous avons

$$1 = \sigma\left(p \times \frac{1}{p}\right) = \sigma(p) \times \sigma\left(\frac{1}{p}\right) = p \times \sigma\left(\frac{1}{p}\right)$$

et donc $\sigma\left(\frac{1}{p}\right) = \frac{1}{p}$. Pour tous $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ nous avons

$$\sigma\left(\frac{p}{q}\right) = \frac{\sigma(p)}{\sigma(q)} = \frac{p}{q}$$

et donc pour tout $r \in \mathbb{Q}$ nous avons $\sigma(r) = r$.

Soit x dans $\mathbb{R}^+$ alors $x = \sqrt{x}^2$ et

$$\sigma(x) = \sigma(\sqrt{x}^2) = \left(\sigma(\sqrt{x})\right)^2 \geq 0.$$

Soient x et y tels que $x \geq y$ alors $x - y \geq 0$ et $\sigma(x - y) \geq 0$ ou encore $\sigma(x) - \sigma(y) \geq 0$, *i.e.* $\sigma(x) \geq \sigma(y)$. Soient x un réel et $(x_n^+)_{n\in\mathbb{N}}$, $(x_n^-)_{n\in\mathbb{N}}$ deux suites de nombres rationnels tels que

- $x_n^- \leq x \leq x_n^+$ pour tout $n \in \mathbb{N}$;
- $\lim\limits_{n\to+\infty} x_n^+ = x$;
- $\lim\limits_{n\to+\infty} x_n^- = x$.

Alors

$$x_n^- = \sigma(x_n^-) \leq \sigma(x) \leq \sigma(x_n^+) = x_n^+.$$

En passant à la limite nous obtenons donc $\sigma(x) = x$. □

Lemme 12.5.4

Soient A, B, C trois points non alignés dans un espace affine $\mathcal{A}$. Le plan engendré par ces trois points est la réunion des droites (DE) avec $D \in (AB)$ et $E \in (AC)$.

Démonstration. — Soit F un point du plan engendré par A, B et C. Si F appartient à $(AB) \cup (AC)$ l'énoncé est démontré.

Supposons désormais que F est ni sur (AB), ni sur (AC). Soit $\mathcal{D}$ la parallèle à (BC) passant par F. Cette droite n'est parallèle ni à (AB), ni à (AC) (sinon $(AC) = (AB)$) et elle rencontre ces deux droites en un point D et E comme annoncé. □

Démonstration du Théorème 12.5.2. — Soit φ une application bijective de $\mathcal{A}$ dans $\mathcal{A}$ qui préserve l'alignement. Cela signifie que l'image d'une droite est une droite. En effet soient A et B deux points distincts de $\mathcal{A}$. La droite (AB) est exactement l'ensemble des points C tels que A, B et C sont alignés et donc son image est l'ensemble des points $\varphi(C)$ alignés avec $\varphi(A)$ et $\varphi(B)$, *i.e.* la droite $(\varphi(A)\varphi(B))$.

Le Lemme 12.5.4 assure que l'image du plan engendré par A, B et C est le plan engendré par $\varphi(A)$, $\varphi(B)$ et $\varphi(C)$.

Soient $\mathcal{D}_1$ et $\mathcal{D}_2$ deux droites parallèles disjointes ; elles sont incluses dans un plan et ne se rencontrent pas. Leurs images vérifient les mêmes conditions et sont donc parallèles.

Soient O une origine et A, B, C trois points non alignés tels que $\overrightarrow{OC} = \overrightarrow{OA} + \overrightarrow{OB}$, *i.e.* $(OA) \mathbin{/\!/} (BC)$ et $(OB) \mathbin{/\!/} (AC)$. Les images vérifient les mêmes conditions de parallélisme ainsi $\overrightarrow{\varphi(O)\varphi(C)} = \overrightarrow{\varphi(O)\varphi(A)} + \overrightarrow{\varphi(O)\varphi(B)}$.

Fixons une droite (OA). Si λ désigne un réel nous notons $\sigma(\lambda)$ l'unique réel tel que

$$\varphi(O + \lambda\overrightarrow{OA}) = \varphi(O) + \sigma(\lambda)\overrightarrow{\varphi(O)\varphi(A)}$$

ou encore tel que

$$\overrightarrow{\varphi(O)\varphi(O+\lambda\overrightarrow{OA})} = \sigma(\lambda)\overrightarrow{\varphi(O)\varphi(A)}$$

L'application $\sigma\colon \lambda \mapsto \lambda(\sigma)$ est une bijection de $\mathbb{R}$ puisque φ est une bijection de (OA) sur $(\varphi(O)\varphi(A))$.

Montrons que c'est un morphisme de corps. Soient λ_1, λ_2 dans $\mathbb{R}$. Posons $A_1 = O + \lambda_1\overrightarrow{OA}$ et $A_2 = O + \lambda_2\overrightarrow{OA}$. Nous allons géométriquement construire le point $O + (\lambda_1 + \lambda_2)\overrightarrow{OA}$. Puisque $\mathcal{A}$ est de dimension au moins 2 nous pouvons choisir $B \in \mathcal{A} \smallsetminus (OA)$. Soit D l'intersection de la parallèle à (OA) passant par B et de la parallèle à (BA_1) passant par O. Il en résulte que le quadrilatère DBA_1O est un parallélogramme et donc $\overrightarrow{DB} = \overrightarrow{OA_1}$. Soit A_3 l'intersection de la parallèle à (DA_2) passant par B et de la droite (OA). Nous avons $\overrightarrow{A_2A_3} = \overrightarrow{DB} = \overrightarrow{OA_1}$. Il s'en suit que

$$\overrightarrow{OA_3} = \overrightarrow{OA_2} + \overrightarrow{A_2A_3} = \overrightarrow{OA_1} + \overrightarrow{OA_2}.$$

Étant donné que φ envoie droite sur droite et préserve le parallélisme, les points $\varphi(O)$, $\varphi(A)$, $\varphi(A_1)$, $\varphi(A_2)$, $\varphi(A_3)$, $\varphi(D)$ et $\varphi(B)$ satisfont les mêmes relations de parallélogrammes. Par suite

$$\overrightarrow{\varphi(O)\varphi(A_3)} = \overrightarrow{\varphi(O)\varphi(A_2)} + \overrightarrow{\varphi(A_2)\varphi(A_3)} = \overrightarrow{\varphi(O)\varphi(A_1)} + \overrightarrow{\varphi(O)\varphi(A_2)}.$$

d'où

$$\sigma(\lambda_1 + \lambda_2)\overrightarrow{OA} = \sigma(\lambda_1)\overrightarrow{OA} + \sigma(\lambda_2)\overrightarrow{OA}$$

et $\sigma(\lambda_1 + \lambda_2) = \sigma(\lambda_1) + \sigma(\lambda_2)$.

Reprenons les mêmes notations pour λ_1, λ_2, O, A, B, A_1 et A_2. Désignons par A_3 le point $O + \lambda_1\lambda_2\overrightarrow{OA}$. Notons C l'intersection de (OB) et de la parallèle à (BA) passant par A_2. Le théorème de Thalès assure que $\overrightarrow{OC} = \lambda_2\overrightarrow{OB}$. Soit D l'intersection de (OB) et de la parallèle à (CA) passant par A_1. D'après le théorème de Thalès $\overrightarrow{OD} = \lambda_1\overrightarrow{OC} = \lambda_1\lambda_2\overrightarrow{OB}$. Finalement le point d'intersection A' de la parallèle à (AB) passant par D satisfait $\overrightarrow{OA'} = \lambda_1\lambda_2\overrightarrow{OA}$, *i.e.* $A' = A_3$.

L'image par φ de cette construction vérifie les mêmes propriétés de parallélisme. Ainsi $\sigma(\lambda_1\lambda_2) = \sigma(\lambda_1)\sigma(\lambda_2)$.

Il en résulte que σ est un morphisme du corps $\mathbb{R}$ donc l'identité d'après la Proposition 12.5.2. $\square$

INDEX

2-transitive (action), 293
ℓ-cycle, 182
$\mathbb{Z}$-base (groupe libre de type fini), 167
$\mathbb{Z}$-base canonique, 166
$\mathbb{Z}$-libre (système), 166
n-torsion, 149
n-transitive (action), 312
p-Sylow, 409
p-groupe, 91, 284
p-sous-groupe de Sylow, 409
r-équivalentes (matrices), 247
élément neutre, 12
élément neutre à droite, 12
élément neutre à gauche, 12
équivalence à droite, 38
équivalence à gauche, 38
équivalentes (actions), 274
équivalentes (matrices), 373
équivalentes (suites), 366
abélien (groupe), 14
action (groupe sur un ensemble), 244
action de Steinitz, 247
alignés (points), 531
alignement préservé, 533
angle géométrique, 512
angle non orienté, 512
anneau principal, 145
anti-rotation, 515
application affine, 510, 530
application induite, 9
arêtes (polyèdre), 520
bloc de Jordan associé à la valeur propre 0, 394
côtés (ligne polygonale), 513
caractère (d'une représentation), 463
caractère linéaire, 475
centralisateur, 24
centre circonscrit (polygone), 514
centre d'un groupe, 24
classe (d'équivalence), 3
classe (partition), 1
classe à droite, 39
classe à gauche, 39
classe de conjugaison, 86
comatrice, 382
commutateurs, 51
commutatif (groupe), 14
complémentaires (sous-groupes), 127
composantes isotypiques, 470
congruence (sous-groupe de), 363
conjugaison, 59
conjugué, 85
conjugué (quaternionique), 306
conjugués (éléments), 202
conjugué (sous-groupe), 259
contragrédiente, 89
convexe (polygone), 513
cycle de longueur ℓ, 182

cyclique (groupe), 26
de type fini, 50
degré (d'un caractère), 463
degré (représentation), 454
diagonalisable (matrice), 385
diagramme de Young, 389, 391
diagramme de Young dual, 392
dimension, 528
dimension (représentation), 454
direction (espace affine), 528
distingué, 40, 97
diviseurs élémentaires, 158
droite affine, 529
droite projective, 310
droite projective associée à E, 310
droite projective standard sur $\mathbb{k}$, 310
dual (groupe), 475
dual (polyèdre régulier), 522
ensemble des classes à droite, 39
ensemble des classes à gauche, 39
ensemble quotient, 8
enveloppe convexe, 514
espace affine, 528
exposant, 155
faces (polyèdre), 520
facteurs invariants, 158, 168
facteurs invariants (matrice), 173
fidèle (représentation), 451
fidèlement, 250
fine (suite), 366
finiment engendré, 50
fixateur, 254
fixe (point), 180, 254
fonction centrale, 463
forme normale de Jordan, 394
formule des classes, 263
générateur (groupe), 26
générateurs (groupe), 50
graphe (relation), 2
groupe, 14
groupe (racines de l'unité), 16
groupe affine, 532
groupe affine de $\mathbb{R}$, 16
groupe affine sur $\mathbb{Z}$, 237
groupe dérivé, 51
groupe de Klein, 18
groupe des automorphismes intérieurs, 99
groupe des isométries euclidiennes, 510
groupe des tresses, 353
groupe diédral, 19
groupe diédral infini, 121
groupe modulaire, 341
groupe orthogonal, 23
groupe symétrique, 21
groupe topologique, 382
groupe unitaire, 23
groupe, $\mathbb{S}^1$, 16
homographie, 310
homomorphisme de groupes, 55
imaginaires quaternioniques, 306
impaire (permutation), 188, 199
indicateur d'Euler, 154
indicatrice d'Euler, 18
indice, 44
intérieur (automorphisme), 89
invariante par conjugaison, 463
inversion, 187
irréductible (caractère), 463
irréductible (représentation), 457
isométrie de $\mathbb{R}^2$, 92
isométrie euclidienne, 510
isomorphes (groupes), 66
isomorphes (représentations), 456
isomorphisme de groupes, 57
Jordan-Hölder (suite), 367
libre (action), 276
libre de type fini (groupe), 165
ligne polygonale, 513
loi de composition interne, 12
loi unitaire, 12
longueur, 336
mesure de l'angle, 511
monoïde, 335
monoïde libre, 336
monogène (groupe), 26
morphisme (groupes), 55

morphisme (monoïdes), 335
morphisme (représentations), 456
morphisme d'évaluation, 340
morphisme trivial, 59
mot, 336
mot vide, 336
nilpotente (matrice), 388
nombre premier, 147
normalisateur (sous-groupe), 259, 260
noyau d'un morphisme de groupes, 64
orbite (d'un point), 252
ordre (d'un élément), 26
ordre d'un groupe, 26
ordre de Chevalley, 397
ordre de dégénérescence, 397
ordre de nilpotence (matrice), 388
paire (permutation), 188, 199
parallèles (sous-espaces affines), 530
part (d'une partition), 389
partition (ensemble), 1
partition (entier), 162
partition associée à $\mathcal{O}$, 391
partition duale, 392
passe au quotient modulo n, 9
permutation, 21
plan affine, 529
plus grand diviseur commun, 146
plus petit multiple commun, 146
polyèdre convexe (dimension 3), 520
polygone, 513
présentation (groupe), 343
premiers entre eux, 146
produit libre, 353
projection canonique, 8
présentation, 19
quaternions (corps des), 306
quotient (d'une suite de composition), 366
réduction, 103
réduit (mot), 338
réduite de Jordan, 394
réduite de Jordan (nilpotente), 394
réflexive (relation), 3
régulière (action de groupe), 295
régulier (polyèdre convexe dimension 3), 521
régulier (polygone convexe), 514
régulier à droite, 13
régulier à gauche, 13
résoluble (groupe), 322
racines n ième de l'unité, 16
raffinement (suite), 366
rang (groupe libre de type fini), 167
rang d'une matrice, 253
relation, 2
relation d'équivalence, 3
représentant, 88
représentant (classe d'équivalence), 8
représentation de permutation, 452
représentation linéaire, 451
représentation régulière, 452
représentation standard, 452
représentation triviale, 451
rotation glissée, 515
section, 129
semblables (matrices), 385
signature (permutation), 188, 197
simple (ligne polygonale), 513
simplement transitive (action), 250, 312
solide Platonicien, 521
somme (groupes), 144
somme directe (groupes), 144
somme directe externe, 144
sommets (ligne polygonale), 513
sommets (polyèdre), 520
sous-espace G-invariant, 454
sous-espace affine, 529
sous-espace affine engendré, 529
sous-groupe, 22
sous-groupe distingué, 40
sous-groupe engendré, 26
sous-groupe propre, 23
sous-représentation, 454
stabilisateur, 254
stabilisateur (élément), 254
stabilisateur (ensemble), 254
suite de composition, 366

support (permutation), 180
symétrie glissée, 513
symétrique, 13
symétrique (relation), 3
symétrique à droite, 13
symétrique à gauche, 13
symbole de Schläfli, 521
système de générateurs, 50
table de Cayley, 14
table des caractères, 473
théorème (petit) de Fermat, 30
théorème d'Euler, 30
torsion (élément), 26, 171
torsion (groupe), 171
transformations homographiques, 314
transitive (relation), 3
transitivement, 250
translation, 528
transposition, 182
trigonalisable (matrice), 385
trivial (groupe), 14
vectorialisé (espace affine), 530
vissage, 515

BIBLIOGRAPHIE

[Ale99] M. Alessandri. *Thème de géométrie*. Dunod, 1999.

[Alp93] R. C. Alperin. Notes : $PSL_2(Z) = Z_2 * Z_3$. *Amer. Math. Monthly*, 100(4) :385–386, 1993.

[Aud06] M. Audin. *Géométrie*. EDP Sciences. 2006.

[Ber77] M. Berger. *Géométrie. Vol. 2*. CEDIC, Paris ; Nathan Information, Paris, 1977. Espaces euclidiens, triangles, cercles et sphères.

[Bur11] W. Burnside. Theory of groups of finite order. 2nd edition. Cambridge : University Press. xxiv, 512 S. (1911)., 1911.

[CG13] P. Caldero and J. Germoni. *Histoires Hédonistes de Groupes et de Géométries. Tome premier*. Calvage et Mounet, 2013.

[CG15] P. Caldero and J. Germoni. *Histoires Hédonistes de Groupes et de Géométries-Tome 2*. Calvage et Mounet, 2015.

[CG17] P. Caldero and J. Germoni. *Nouvelles Histoires Hédonistes de Groupes et de Géométries*. Calvage et Mounet, 2017.

[CLO97] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

[Col11] P. Colmez. *Éléments d'analyse et d'algèbre (et de théorie des nombres)*. École Polytechnique, 2011.

[Con] K. Conrad. $\mathrm{SL}(2, \mathbb{Z})$. *https ://kconrad.math.uconn.edu/blurbs/grouptheory/SL(2,Z).pdf*.

[DW71] I. M. S. Dey and J. Wiegold. Generators for alternating and symmetric groups. *J. Austral. Math. Soc.*, 12 :63–68, 1971.

[Gas66] W. Gaschütz. Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen. *J. Algebra*, 4 :1–2, 1966.

[Hal67] M. Hall, Jr. On the number of Sylow subgroups in a finite group. *J. Algebra*, 7 :363–371, 1967.

[KT08] C. Kassel and V. Turaev. *Braid groups*, volume 247 of *Graduate Texts in Mathematics*. Springer, New York, 2008. With the graphical assistance of Olivier Dodane.

[Lan03] E. Landau. Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante. *Math. Ann.*, 56(4) :671–676, 1903.

[LS01] R. C. Lyndon and P. E. Schupp. *Combinatorial group theory*. Classics in Mathematics. Springer-Verlag, Berlin, 2001. Reprint of the 1977 edition.

[Mil10] G. A. Miller. Groups involving only a small number of sets of conjugate operators. *Arch. der Math. u. Phys. (3)*, 17 :199–204, 1910.

[Per82] D. Perrin. *Cours d'algèbre*, volume 18 of *Collection de l'École Normale Supérieure de Jeunes Filles*. École Normale Supérieure de Jeunes Filles, Paris, 1982. Edited with the collaboration of Marc Cabanes and Martine Duchene.

[Pey04] G. Peyré. *L'algèbre discrète de la transformée de Fourier*. Ellipses, 2004.

[Pol68] J. Poland. Finite groups with a given number of conjugate classes. *Canadian J. Math.*, 20 :456–464, 1968.

[Rau00] G. Rauch. *Les groupes finis et leurs représentations*. Ellipses, 2000.

[Rob96] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

[RW10] J.-P. Ramis and A. Warusfel. *Cours de mathématique vol.1 algèbre et géométrie*. De Boeck, 2010.

[Ser77] J.-P. Serre. *Arbres, amalgames,* SL_2. Société Mathématique de France, Paris, 1977. Avec un sommaire anglais, Rédigé avec la collaboration de Hyman Bass, Astérisque, No. 46.

[Szp09] A. Szpirglas. *Mathématiques L3 : Algèbre*. Pearson, 2009.

[VLS07] A. Vera-López and Josu Sangroniz. The finite groups with thirteen and fourteen conjugacy classes. *Math. Nachr.*, 280(5-6) :676–694, 2007.