GROUPES ET GÉOMÉTRIE

GROUPES ET GÉOMÉTRIE

Université Nice Sophia Antipolis – Groupes et géométrie
Année 2019-2020

TABLE DES MATIÈRES

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.

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 ;
- ◇ le groupe $\mathrm{O}(n, \mathbb{R})$ 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 suivants : décrire les actions, décrire les classificants, trouver des algorithmes pour calculer les classifiants, 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 $\underline{e}'$. Le classificant 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 [1] ; par suite 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 $\mathcal{O}_{r'}$, $0 \leq r' \leq r$. 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 $\mathbb{L}$-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

GROUPES

1.1. Lois, groupes : généralités et exemples

Définition 1.1.1. — 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*.
- ◇ 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
$$x * a = y * a \quad \Longleftrightarrow x = y.$$

Le couple $(\mathrm{G}, *)$ est un *groupe* si la loi interne $*$ est associative, possède un élément neutre e et si tout élément de G a 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*.

Remarque 1.1.1. — 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.

1.1.1. Premiers exemples. —

Exemple 1.1.1 (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 1.1.2 (Les groupes $\mathbb{R}$ et $\mathbb{C}$)**.** — L'ensemble $\mathbb{R}$ (resp. $\mathbb{C}$) muni de l'addition est un groupe dont l'élément neutre est 0 et l'inverse de x est $-x$.

Exemple 1.1.3. — 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 1.1.4 (Les groupes $\mathbb{R}^\times$ et $\mathbb{C}^\times$)**.** — L'ensemble $\mathbb{R}^\times$ (resp. $\mathbb{C}^\times$) des nombres réels (resp. 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 $\mathbb{R}^\times$ (resp. $\mathbb{C}^\times$), il sera désormais toujours sous-entendu que sa loi de composition interne est la multiplication.

Exemple 1.1.5 (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.

Exemple 1.1.6 (Le groupe $\mathbb{Z}/n\mathbb{Z}$)**.** — On fixe un entier $n \geq 1$.

Soit a un entier. La *classe* de a modulo n est l'ensemble des entiers b tels que $b - a$ soit multiple de n. En d'autres termes, cette classe est l'ensemble des entiers de la forme $a + kn$ avec $k \in \mathbb{Z}$; elle contient a (prendre $k = 0$). Soit b un élément de la classe de a modulo n et soit c un entier quelconque. On a $c - a = c - b + (b - a)$. Comme $b - a$ est multiple de n, on voit que si $c - b$ est multiple de n alors $c - a$ est multiple de n ; en écrivant $c - b = c - a - (b - a)$ on voit de même que si $c - a$ est multiple de n alors $c - b$ est multiple de n. Par conséquent,

$c-a$ est multiple de n si et seulement si $c-b$ est multiple de n ; autrement dit, la classe de a modulo n est égale à la classe de b modulo n. La classe de a modulo n sera notée $\overline{a}$.

Soient a et b deux entiers. On a $\overline{a}=\overline{b}$ si et seulement si b appartient à $\overline{a}$, c'est-à-dire si et seulement si $b-a$ est multiple de n (on dit alors que a et b sont égaux modulo n).

En effet, si $\overline{a}=\overline{b}$ alors comme b appartient à $\overline{b}$, il appartient à $\overline{a}$. Et si b appartient à $\overline{a}$, on a $b=a$ d'après ce qui précède.

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes modulo n ; on dit parfois que $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ modulo n. Les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont donc les $\overline{a}$ pour a parcourant $\mathbb{Z}$; on dispose ainsi D'une surjection $a\mapsto\overline{a}$ de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ qui est appelée la réduction modulo n. D'après ce qui précède on a $\overline{a}=\overline{b}$ si et seulement si $b-a$ est multiple de n.

Nous avons une surjection

$$\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z} \qquad\qquad a\mapsto\overline{a}$$

et $\overline{a}=\overline{b}$ si et seulement si $b-a$ est multiple de n. Nous pouvons donc voir $\mathbb{Z}/n\mathbb{Z}$ comme un ensemble de nombres fabriqué en partant des entiers relatifs usuels et en mettant la règle suivante : deux nombres coïncident dès que leur différence est un multiple de n.

Soit a un élément de $\mathbb{Z}$. La théorie de la division euclidienne assure qu'il existe un unique couple (q,r) d'éléments de $\mathbb{Z}$ tels que $r\in\{0,\,1,\,\ldots,\,n-1\}$ et $a=nq+r$. On a donc $\overline{a}=\overline{r}$. Soit s un entier appartenant à $\{0,\,1,\,\ldots,\,n-1\}$. On a $\overline{s}=\overline{r}$ si et seulement si $s-r$ est multiple de n. Mais comme s et r sont tous deux compris entre 0 et $n-1$, la différence $r-s$ est multiple de n si et seulement $r-s=0$ c'est-à-dire si et seulement si $s=r$. Autrement dit, r est l'unique entier compris entre 0 et $n-1$ dont la classe modulo n est égale à $\overline{r}$.

Ainsi tout élément de $\mathbb{Z}/n\mathbb{Z}$ est égal à $\overline{r}$ pour un unique élément r de $\{0,\,1,\,\ldots,\,n-1\}$. Par conséquent, les éléments $\overline{0}$, $\overline{1}$, …, $\overline{n-1}$ de $\mathbb{Z}/n\mathbb{Z}$ sont deux à deux distincts et $\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\,\overline{1},\,\ldots,\,\overline{n-1}\}$. Le cardinal de $\mathbb{Z}/n\mathbb{Z}$ est donc égal à n.

Considérons par exemple le cas où $n=3$. L'ensemble $\mathbb{Z}/3\mathbb{Z}$ compte 3 éléments, à savoir $\overline{0}$, $\overline{1}$ et $\overline{2}$. Si a est un entier quelconque, pour savoir auquel de ces 3 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 $\overline{(-47)}=\overline{1}$.

Soit $n>0$ un entier quelconque. Soit E un ensemble. Soit f une application de $\mathbb{Z}$ vers 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 : il pourrait exister deux éléments distincts a et b de $\mathbb{Z}$ tels que $\overline{a}=\overline{b}$ et $f(a)\neq f(b)$. On dit que f *passe au quotient modulo* n si $f(a)=f(b)$ dès que $\overline{a}=\overline{b}$. 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.

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 $(-1)^1 = -1$.

Ces considérations se généralisent au cas d'applications de $\mathbb{Z}^r$ dans E (r désignant un entier positif) : si une telle application f passe au quotient modulo n, *i.e.* est telle que $f(a_1, a_2, \ldots, a_r) = f(b_1, b_2, \ldots, b_r)$ dès que $\overline{a_i} = \overline{b_i}$ pour tout i, alors f induit une application de $\left(\mathbb{Z}/n\mathbb{Z}\right)^r$ vers E donnée par la formule $(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_r}) \mapsto f(a_1, a_2, \ldots, a_r)$.

Application. Considérons l'application

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \qquad\qquad (a,b) \mapsto \overline{a+b}$$

Elle passe au quotient modulo n. En effet, soient a, α, b et β quatre éléments de $\mathbb{Z}$ tels que $\overline{a} = \overline{\alpha}$ et $\overline{b} = \overline{\beta}$. Montrons que $\overline{a+b} = \overline{\alpha+\beta}$. Nous avons

$$(\alpha+\beta) - (a+b) = \alpha + \beta - a - b = (\alpha - a) + (\beta - b).$$

Par hypothèse il existe un entier ℓ tel que $\alpha - a = n\ell$ et un entier j tel que $\beta - b = nj$. Par suite

$$(\alpha+\beta) - (a+b) = n\ell - nj = n(\ell - j)$$

autrement dit $(\alpha+\beta)-(a+b)$ est un multiple de n, *i.e.* $\overline{a+b} = \overline{\alpha+\beta}$. Cette application induit donc une application de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ donnée par la formule

$$(\overline{a}, \overline{b}) \mapsto \overline{a+b}.$$

Notons la encore $+$. En d'autres termes nous avons ainsi défini une loi de composition interne $+$ sur $\mathbb{Z}/n\mathbb{Z}$ donnée par la formule

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

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

$$\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b+c} \tag{1.1.1}$$

$$= \overline{a + (b+c)} \tag{1.1.2}$$

$$= \overline{(a+b)+c} \tag{1.1.3}$$

$$= \overline{a+b} + \overline{c} \tag{1.1.4}$$

$$= (\overline{a} + \overline{b}) + \overline{c} \tag{1.1.5}$$

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

$$\overline{a}+\overline{b} = \overline{a+b} \tag{1.1.6}$$

$$= \overline{b+a} \tag{1.1.7}$$

$$= \overline{b}+\overline{a} \tag{1.1.8}$$

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 1.1.7 (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. On le note $\mathcal{K}$.

Il a quatre éléments ; tous, sauf l'élément neutre, ont un ordre égal à 2, et le produit de deux éléments distincts d'ordre 2 est égal au troisième.

Exemple 1.1.8 (Le groupe diédral)**.** — Le *groupe diédral* est le groupe des isométries du plan euclidien préservant un polygone régulier à n côtés. Il contient

- les n rotations $\rho\left(O, \frac{2k\pi}{n}\right)$ pour $k=0,\,1,\,\ldots,\,n-1$ (O désigne le centre du polygone),
- les n réflexions (*i.e.* symétries) par rapport aux droites passant par O et les sommets ou milieux des côtés du polygone.

Nous verrons qu'il est isomorphe à $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ et qu'il a pour présentation

$$\mathrm{D}_{2n} = \langle r,\, s \,|\, r^n = e,\, s^2 = e,\, rsrs = e\rangle.$$

Exemple 1.1.9 (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 formulles

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

Le groupe ainsi obtenu est non abélien : $ij=-ji$. Plus précisément le groupe des quaternions est l'un des deux groupes non abéliens d'ordre 8.

Le groupe des automorphismes intérieurs de $\mathbb{H}_8$ est isomorphe à $\mathbb{H}_8$ modulo son centre, et est par conséquent aussi isomorphe au groupe de Klein V. Le groupe des automorphismes de $\mathbb{H}_8$ est isomorphe au groupe symétrique $\mathcal{S}_4$. Le groupe des automorphismes extérieurs de $\mathbb{H}_8$ est alors $\mathcal{S}_4/V$ qui est isomorphe à $\mathcal{S}_3$.

1.1.2. Le groupe des permutations. — Soit E un ensemble et soit $\mathcal{S}_E$ 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 $\mathcal{S}_E$. Cette loi est associative et id_E en est un élément neutre. Si $\sigma \in \mathcal{S}_E$, la bijection réciproque σ^{-1} est un symétrique de σ pour la loi $\circ$. L'ensemble $\mathcal{S}_E$ muni de la composition des permutations est donc un groupe.

Lorsque nous parlerons du groupe $\mathcal{S}_E$, 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 $\mathcal{S}_\emptyset$ 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 néecessairement g sur g). Le groupe $\mathcal{S}_{\{g\}}$ 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 $\mathcal{S}_E$ compte alors deux éléments : l'identité et la permutation τ qui échange a et b. Le groupe $\mathcal{S}_E$ 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 $\mathcal{S}_E$ 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 $\mathcal{S}_E$ n'est pas abélien.

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

Pour décrire un élément de $\mathcal{S}_n$, 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 :

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

Par exemple

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

désigne l'élément de $\mathcal{S}_3$ 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 $\mathcal{S}_3$.

Lemme 1.1.1. — *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 $\mathcal{S}_X$ a pour cardinal $n!$.

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 en rang $< n$. 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 $\mathcal{S}_n$ pour les petites valeurs de n :

- ◇ $\mathcal{S}_0 = \{\mathrm{id}\}$;
- ◇ $\mathcal{S}_1 = \{\mathrm{id}\}$;
- ◇ $\mathcal{S}_2$ compte $2 = 2!$ (Lemme 1.1.1) éléments qui sont

$$\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

- ◇ $\mathcal{S}_3$ compte $6 = 3!$ (Lemme 1.1.1) éléments qui sont

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

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

◇ $\mathcal{S}_4$ compte $24 = 4!$ (Lemme 1.1.1) éléments qui sont

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

1.1.2.1. *Support d'une permutation.* — Soit E un ensemble. Soit σ un élément de $\mathcal{S}_E$. 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 1.1.2. — 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 1.1.3. — 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 1.1.10. — 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 1.1.11. — 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 1.1.4. — 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 $\mathrm{Supp}(\sigma\sigma^{-1}) \subsetneq \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\sigma^{-1})$.

1.1.2.2. *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 X 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 $\sigma_1\sigma_2\dots\sigma_n = \mathrm{id}$ si et seulement si son support est vide ; ainsi $\sigma_1\sigma_2\dots\sigma_n = \mathrm{id}$ si et seulement si $\mathrm{Suppp}(\sigma_i)$ est vide pour tout i soit si et seulement si $\sigma_i = \mathrm{id}$ pour tout i.

1.1.2.3. *Cycles.* — Soit E un ensemble.

Soient a_1, a_2, …, a_ℓ des éléments deux à deux distinct de E avec ℓ entier au moins égal à 2. Désignons par $(a_1\ a_2\ \dots\ a_\ell)$ la permutation de E définie par

- ◇ si $x \notin \{a_1, a_2, \dots, a_\ell\}$ 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 1.1.12. — 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, …, a_ℓ des éléments de E deux à deux distincts. Soit σ le ℓ-cycle $(a_1\ a_2\ \dots\ a_\ell)$. Par définition $\mathrm{Supp}(\sigma) = \{a_1, a_2, \dots, a_\ell\}$. L'écriture de σ sous la forme $(a_1\ a_2\ \dots\ a_\ell)$ n'est pas unique. En effet $\sigma = (a_2\ a_3\ \dots a_\ell\ a_1)$ et plus généralement $\sigma = (a_i\ a_{i+1}\ \dots\ a_\ell\ a_1\ a_2\ \dots\ a_{i-1})$ pour tout $1 \leq i \leq \ell$.

Exemple 1.1.13. — 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 $\sigma = (a_1\ a_2\ \dots\ a_\ell)$ envoie a_ℓ sur $a_{\ell-1}$, $a_{\ell-1}$ sur $a_{\ell-2}$, …, a_3 sur a_2, a_2 sur a_1, a_1 sur a_ℓ. Autrement dit σ^{-1} est le ℓ-cycle $(a_\ell\ a_{\ell-1}\ \dots\ a_3\ a_2\ a_1)$. En d'autres termes l'inverse d'un cycle est un cycle obtenu par renversement de l'ordre des termes.

Exemple 1.1.14. — Si $E = \{1, 2, 3, 4, 5\}$ et $\sigma = (1\ 5\ 4\ 2)$ alors $\sigma^{-1} = (2\ 4\ 5\ 1)$.

Considérons un élément c de $\mathbb{Z}/\ell\mathbb{Z}$. Il existe un unique entier $n \in \{1, 2, \dots, \ell\}$ 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 $\{a_1, a_2, \dots, a_\ell\}$. 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 1.1.15. — 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 1.1.2. — *Soit E un ensemble fini. Soit σ une permutation de E.*

Il existe une famille finie C_1, C_2, …, C_r de cycles sur E à supports deux à deux disjoints tels que $\sigma = C_1C_2 \dots C_r$.

De plus cette écriture est « unique à permutation près des C_i ». En d'autres termes si $D_1D_2 \dots D_s$ 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 $\{1, 2, \dots, r\}$ telle que $D_i = C_{\tau(i)}$ pour tout i.*

Exemple 1.1.16. — 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 1.1.17. — 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 1.1.18. — 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

$$\sigma = (1\ \ 3\ \ 2\ \ 10)(4)(5\ \ 7\ \ 8)(6\ \ 9)$$

Démonstration du Théorème 1.1.2. — ◇ 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, …, 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 $\{D_1, D_2, \dots, D_s\} = \{C_1, C_2, \dots, C_r\}$.

□

Cette démonstration permet de décrire 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, …, 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 $C_{y_1}, C_{y_2}, \ldots, C_{y_i}$ est égale au support de σ on arrête, sinon on prend pour y_{i+1} n'importe quel élément de $\mathrm{Supp}(\sigma) \setminus \Big(\mathrm{Supp}(C_{y_1}) \bigsqcup \mathrm{Supp}(C_{y_2}) \bigsqcup \ldots \bigsqcup \mathrm{Supp}(C_{y_i})\Big)$

L'écriture cherchée est alors $\sigma = C_{y_1} C_{y_2} \ldots C_{y_s}$ (les cycles C_{y_i} sont eux-mêmes construits par le procédé décrit précédemment).

Voyons ce que cela donne sur un exemple concret :

Exemple 1.1.19. — 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 1.1.5. — Nous avons précédemment donné la liste des éléments de $\mathcal{S}_4$. Le « type »d'une décomposition est le nombre de cycles de chaque longueur qu'elle met en jeu. La liste des éléments de $\mathcal{S}_4$ 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 1.1.3. — *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

$$(a_1\ a_2\ \ldots\ a_\ell) = (a_1\ a_2)(a_2\ a_3)\ldots(a_{\ell-1}\ a_\ell). \tag{1.1.9}$$

Si E est fini, toute permutation de E peut s'écrire comme un produit de cycles à supports deux à deux disjoints (Théorème 1.1.2). Puisque tout cycle sur E est produit de transpositions (1.1.2) *toute permutation de E est produit de transpositions.*

Soit $n \geq 0$ un entier et soit σ un élément de $\mathcal{S}_n$. 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 1.1.2. — Soit $n \geq 0$ un entier et soit σ un élément de $\mathcal{S}_n$. 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 1.1.20. — Soit σ la permutation de $\mathcal{S}_4$ 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 1.1.4. — *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 1.1.3. — Soit n un entier. Soit $\sigma \in \mathcal{S}_n$. 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 1.1.21. — La permutation identité est paire.

Exemple 1.1.22. — Soit σ la permutation de $\mathcal{S}_4$ 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 $\mathcal{S}_n$. Par définition $\mathrm{sgn}(\sigma\tau) = (-1)^{\mathrm{I}(\sigma\tau)}$. Le théorème 1.1.4 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 $\mathcal{S}_n$ 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 1.1.23. — Soit n un entier. Soit $\tau = (a\ b)$ une transposition de $\mathcal{S}_n$. 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 :

- $\diamond$ $i = a$ et $a < j \leq b$;
- $\diamond$ $a \leq i < b$ 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 1.1.24. — Soit n un entier. Soit $2 \leq \ell \leq n$ et soit c un ℓ-cycle de $\mathcal{S}_n$. 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 1.1.25. — 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 1.1.24.

Exemple 1.1.26. — Soit n un entier. Soit σ un élément de $\mathcal{S}_n$. 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.

1.1.3. —

Définition 1.1.4. — 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 1.1.27. — Si G est un groupe, alors G et $\{e\}$ sont des sous-groupes de G.

Exemple 1.1.28. — Pour tout $k \in \mathbb{N}$, l'ensemble $k\mathbb{Z} := \{kn \,|\, n \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.

Exemple 1.1.29. — Le sous-ensemble $\mathbb{R}^\times$ de $\mathbb{C}^\times$ en est un sous-groupe (et sa structure de groupe héritée de celle de $\mathbb{C}^\times$ est sa structure de groupe usuelle).

Exemple 1.1.30. — Le sous-ensemble $\{-1, 1\}$ de $\mathbb{R}^\times$ en est un sous-groupe.

Exemple 1.1.31. — 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 1.1.32. — Soit K le sous-ensemble $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ de $\mathcal{S}_4$. 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 $\mathcal{S}_4$. Il est isomorphe à $\mathcal{K}$.

Exemple 1.1.33. — 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 1.1.34. — 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 1.1.5. — Un sous-groupe *propre* de G est un sous-groupe de G distinct de $\{e\}$ et de G.

Définition 1.1.6. — Le *sous-groupe engendré par une partie* P de G est le plus petit sous-groupe de G, noté $\langle P\rangle$, contenant P. C'est aussi l'intersection de tous les sous-groupes de G qui contiennent P.

Définition 1.1.7. — Un groupe est *monogène* s'il est engendré par une partie contenant un seul élément g ; on le note alors $\langle g\rangle$. Dans ce cas

$$\langle g\rangle = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots, g^n, \dots\}.$$

Si $P = \{g_1, g_2, \dots, g_n\}$ est une partie finie de G, alors $\langle P\rangle$ est l'ensemble des produits finis (« mots ») d'éléments de P et de leurs inverses.

Exemple 1.1.35. — Le groupe $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est monogène, en effet $\mathbb{Z}/n\mathbb{Z} = \langle 1\rangle$.

Exemple 1.1.36. — Supposons que $\mathrm{G} = \mathcal{S}_4$ 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 1.1.37. — Supposons que $\mathrm{G} = \mathcal{S}_4$ 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 1.1.38. — Supposons que $\mathrm{G} = \mathbb{Z}$. Le sous-groupe $\langle g \rangle$ de $\mathbb{Z}$ est l'ensemble des entiers de la forme $ng = gn$ avec $n \in \mathbb{Z}$; c'est donc tout simplement l'ensemble des multiples de g, que l'on note 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 1.1.5. — *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 $\delta = bd = d$.

□

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 $n \in \mathbb{Z} \setminus \mathbb{N}$ 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 $n \in \mathbb{Z} \setminus \mathbb{N}$ on a $g^n = (g^{-1})^{-n}$.

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 1.1.8. — 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.

L'*ordre d'un élément* $g \in \mathrm{G}$ est l'ordre de $\langle g \rangle$.

Remarque 1.1.6. — Lorsque l'ordre de g est fini, c'est aussi le plus petit entier positif non nul k tel que $g^k = e$. Soit k l'ordre de g ; si ℓ est un entier positif non nul tel que $g^\ell = e$ alors k divise ℓ.

Exemple 1.1.39. — Le groupe symétrique $\mathcal{S}_n$ est un groupe fini d'ordre $n!$.

Exemple 1.1.40. — Soit $n \geq 2$ un entier. Le groupe $\mathbb{Z}/n\mathbb{Z}$ est un groupe fini.

Exemple 1.1.41. — Les trois éléments i, j et k du groupe des quaternions $\mathbb{H}_8$ sont tous d'ordre 4 dans $\mathbb{H}_8$ et deux quelconques d'entre eux engendrent le groupe entier.

Définition 1.1.9. — Un groupe monogène G d'ordre fini n est dit *cyclique*. Dans ce cas

$$\mathrm{G} = \langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$$

et $g^n = e$.

Exemple 1.1.42. — Le groupe $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ est cyclique.

Exemple 1.1.43. — Tous les sous-groupes propres du groupe des quaternions $\mathbb{H}_8$ sont cycliques.

Définition 1.1.10. — Le *centre* d'un groupe 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 centre $Z(\mathrm{G})$ est un sous-groupe abélien de G.

Exemple 1.1.44. — Si G est abélien, alors $Z(\mathrm{G})$ et G coïncident.

Exemple 1.1.45. — Le centre du groupe des quaternions $\mathbb{H}_8$ est non trivial : $Z(\mathbb{H}_8) = \{1, -1\}$.

Exemple 1.1.46. — Notons que $\mathcal{S}_1 = \{\mathrm{id}\}$ donc $Z(\mathcal{S}_1) = \{\mathrm{id}\}$.

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

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

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

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b)) \tag{1.1.10}$$

Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ \ 2) = (1\ \ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ \ 2) \circ \sigma^{-1} = (1\ \ 2)$. Par suite (1.1.10) 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.

Définition 1.1.11. — Soient G et H deux groupes ; on note e_{G} l'élément neutre de G et e_{H} l'élément neutre de G′. 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

$$\forall\, g, h \in \mathrm{G} \qquad \varphi(gh) = \varphi(g)\varphi(h) \qquad\qquad \varphi(e_{\mathrm{G}}) = e_{\mathrm{H}}$$

Exemple 1.1.47. — Soit G un groupe. L'identité $\mathrm{id}\colon \mathrm{G} \to \mathrm{G}$, $g \mapsto g$ est un morphisme.

Exemple 1.1.48. — Soit G un groupe. Pour tout sous-groupe H de G l'inclustion $\mathrm{H} \hookrightarrow \mathrm{G}$ est un morphisme.

Exemple 1.1.49. — Rappelons que $\{-1, 1\}$ est un sous-groupe de $\mathbb{R}^\times$. Pour tout entier n, la signature est un morphisme de $\mathcal{S}_n$ dans $\{-1, 1\}$.

Exemple 1.1.50. — Soient G et H deux groupes. Notons e_{H} l'élément neutre de H. L'application constante

$$\mathrm{G} \to \mathrm{H} \qquad\qquad g \mapsto e_{\mathrm{H}}$$

est un morphisme.

Exemple 1.1.51. — Soient $\varphi\colon \mathrm{G} \to \mathrm{G}'$ et $\varphi'\colon \mathrm{G}' \to \mathrm{G}''$ deux morphismes de groupes. La composée $\varphi' \circ \varphi\colon \mathrm{G} \to \mathrm{G}''$ est un morphisme de groupes. En effet pour tous g et h dans G nous avons

$$\begin{aligned}(\varphi' \circ \varphi)(gh) &= \varphi'(\varphi(gh)) \\ &= \varphi'(\varphi(g)\varphi(h)) \\ &= \varphi'(\varphi(g))\varphi'(\varphi(h)) \\ &= (\varphi' \circ \varphi)(g)(\varphi' \circ \varphi)(h)\end{aligned}$$

(la seconde égalité vient du fait que φ est un morphisme et la troisième du fait que φ' est un morphisme).

Exemple 1.1.52. — Soit $n \geq 1$ un entier. L'application

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \qquad\qquad g \mapsto \overline{g}$$

est un morphisme de groupes. Cela résulte du fait que $\overline{g+h} = \overline{g} + \overline{h}$ pour tout $(g, h) \in \mathbb{Z}^2$.

Définition 1.1.12. — Soit $\varphi\colon \mathrm{G} \to \mathrm{H}$ un morphisme de groupes. Le *noyau* de φ est défini par

$$\ker \varphi = \{g \in \mathrm{G} \,|\, \varphi(g) = e\}.$$

C'est un sous-groupe de G. En effet $\ker \varphi = \varphi^{-1}(\{e_{\mathrm{G}}\})$ et

Lemme 1.1.6. — *Soit $\varphi\colon \mathrm{G} \to \mathrm{H}$ un morphisme de groupes.*
Soit H' un sous-groupe de H. *L'image réciproque $\varphi^{-1}(\mathrm{H}')$ est un sous-groupe de* G.

Démonstration. — Comme $e_{\mathrm{H}} \in \mathrm{H}'$ (car H' est un sous-groupe de H) et comme $\varphi(e_{\mathrm{G}}) = e_{\mathrm{H}}$ on a $e_{\mathrm{G}} \in \varphi^{-1}(\mathrm{H}')$.

Soient g et g' deux éléments de $\varphi^{-1}(\mathrm{H}')$. Par définition, $\varphi(g) \in \mathrm{H}'$ et $\varphi(g') \in \mathrm{H}'$. Alors $\varphi(gg') = \varphi(g)\varphi(g') \in \mathrm{H}'$ (car H' est un sous-groupe de H). Ainsi $gg' \in \varphi^{-1}(\mathrm{H}')$.

Soit g un élément de $\varphi^{-1}(\mathrm{H}')$. Par définition, $\varphi(g) \in \mathrm{H}'$. Alors $\varphi(g^{-1}) = \varphi(g)^{-1} \in \mathrm{H}'$ (car H' est un sous-groupe de H) et g^{-1} appartient à $\varphi^{-1}(\mathrm{H}')$.

Il s'ensuit que $\varphi^{-1}(\mathrm{H}')$ est un sous-groupe de G. □

Exemple 1.1.53. — Soit n un entier. Soit $\varepsilon\colon \mathcal{S}_n \to \{-1, 1\}$ la signature. Son noyau, appelé *groupe alterné*, est d'après ce qui précède un sous-groupe de $\mathcal{S}_n$ noté $\mathcal{A}_n$; par définition $\mathcal{A}_n$ est constitué des permutations paires.

1. Supposons que $n = 0$ ou $n = 1$. Alors $\mathcal{S}_n = \{\mathrm{id}\}$ et $\varepsilon(\mathrm{id}) = 1$. Il en résulte que $\mathcal{A}_n = \mathcal{S}_n = \{\mathrm{id}\}$ et que l'image de ε est égale à $\{1\}$.
2. Supposons que $n \geq 2$. Le groupe $\mathcal{S}_n$ contient alors la transposition $(1\ \ 2)$. Sa signature est -1 ; par conséquent l'image de ε est $\{-1, 1\}$ tout entier : la signature est surjective.

Le groupe $\mathcal{A}_n$, qui ne contient pas $(1\ 2)$, est un sous-groupe strict de $\mathcal{S}_n$. Lorsque $n = 2$ le groupe $\mathcal{S}_n$ coïncide avec $\{\mathrm{id}, (1\ 2)\}$ et le groupe $\mathcal{A}_n$ avec $\{\mathrm{id}\}$. Par contre lorsque $n \geq 3$ le groupe $\mathcal{A}_n$ est non trivial : il contient $(1\ 2\ 3)$.

Détaillons les cas $n = 3$ et $n = 4$:

- ◇ Le cas $n = 3$. Une permutation de $\{1, 2, 3\}$ est ou bien l'identité, ou bien une transposition, ou bien un 3-cycle (aucun autre type de décomposition en produit de cycles à supports deux à deux disjoints n'est possible). L'identité et les 3-cycles sont paires, les transpositions quant à elles sont impaires.
  Puisqu'un 3-cycle de $\{1, 2, 3\}$ a pour support $\{1, 2, 3\}$ tout entier, il y a exactement deux tels 3-cycles : $(1\ 2\ 3)$ et $(1\ 3\ 2)$. Par conséquent $\mathcal{A}_3 = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$.
- ◇ Le cas $n = 4$. Nous avons précédemment donné la liste des éléments de $\mathcal{S}_4$, classés en fonction de leur écriture comme produit de cycles à supports deux à deux disjoints. L'identité et les 3-cyles sont paires, les produits de deux transpositions aussi. Par contre les transpositions et les 4-cycles sont impaires. Le groupe $\mathcal{A}_4$ est donc égal à

$$\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3),$$
$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

Lemme 1.1.7. — *Le morphisme de groupes $\varphi\colon \mathrm{G} \to \mathrm{H}$ est injectif si et seulement si son noyau est trivial, i.e.* $\ker\varphi = \{e_\mathrm{G}\}$.

Démonstration. — Supposons φ injectif. Soit g un élément de $\ker\varphi$. Alors $\varphi(g) = e_\mathrm{H} = \varphi(e_\mathrm{G})$ donc $g = e_\mathrm{G}$ par injectivité de φ et $\ker\varphi$ est trivial.

Réciproquement supposons que $\ker\varphi$ est trivial et soient g et g' deux éléments de G tels que $\varphi(g) = \varphi(g')$. Nous avons $\varphi(g'g^{-1}) = \varphi(g')\varphi(g)^{-1} = e_\mathrm{H}$; autrement dit $g^{-1}g'$ appartient à $\ker\varphi$ et comme celui-ci est trivial, $g^{-1}g' = e_\mathrm{G}$ soit $g = g'$. Ainsi φ est injectif. □

Définition 1.1.13. — Soit $\varphi\colon \mathrm{G} \to \mathrm{H}$ un morphisme de groupes. L'*image* de φ est définie par

$$\mathrm{Im}\,\varphi = \{h \in \mathrm{H} \mid \exists\, g \in \mathrm{G},\ \varphi(g) = h\}$$

ou encore

$$\mathrm{Im}\,\varphi = \{\varphi(g) \mid g \in \mathrm{G}\}.$$

C'est un sous-groupe de H. En effet plus généralement on a

Lemme 1.1.8. — *Soit $\varphi\colon \mathrm{G} \to \mathrm{H}$ un morphisme de groupes.*
Soit G' un sous-groupe de G. *L'image $\varphi(\mathrm{G}')$ est un sous-groupe de* H.

Démonstration. — Comme $e_\mathrm{G} \in \mathrm{G}'$ (car G' est un sous-groupe de G) et $\varphi(e_\mathrm{G}) = e_\mathrm{H}$ nous avons $e_\mathrm{H} \in \varphi(\mathrm{G}')$.

Soient h et h' deux éléments de $\varphi(\mathrm{G}')$. Par définition, il existe deux éléments g et g' de G' tels que $\varphi(g) = h$ et $\varphi(g') = h'$. Alors $hh' = \varphi(g)\varphi(g') = \varphi(gg')$; puisque $gg' \in \mathrm{G}'$ (car G' est un sous-groupe de G) nous avons $hh' \in \varphi(\mathrm{G}')$.

Soit h un élément de $\varphi(\mathrm{G}')$. Par définition, il existe $g \in \mathrm{G}'$ tel que $\varphi(g) = h$. Alors $h^{-1} = \varphi(g)^{-1} = \varphi(g^{-1})$; puisque $g^{-1} \in \mathrm{G}'$ (car G' est un sous-groupe de G), nous avons $h^{-1} \in \varphi(\mathrm{G}')$. Ainsi $\varphi(\mathrm{G}')$ est bien un sous-groupe de H. En particulier $\varphi(\mathrm{G})$ est un sous-groupe de H. □

Définition 1.1.14. — Un morphisme de groupes dont l'image est le sous-groupe trivial est dit *trivial*.

Définition 1.1.15. — 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.

Tout groupe cyclique d'ordre n est isomorphe au groupe additif $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$.

Proposition 1.1.9. — *Un groupe monogène est isomorphe à* $\mathbb{Z}$ *ou* $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. — Soit G un groupe monogène. Il est engendré par un élément g. Il suffit alors de considérer l'homomorphisme surjectif

$$\mathbb{Z} \to \mathrm{G} \qquad\qquad n \mapsto g^n.$$

□

Relations à droite et à gauche. Soit G un groupe dont la loi sera noté 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 G/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

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

Toutes les classes à gauche et à droite ont même cardinal, celui de H. Il y a une bijection naturelle entre G/H et $\mathrm{H}\backslash\mathrm{G}$ donnée par $g\mathrm{H} \mapsto \mathrm{H}g^{-1}$.

Le cardinal de G/H est appelé l'*indice* de H dans G et est noté $[\mathrm{G} : \mathrm{H}]$. Lorsque $[\mathrm{G} : \mathrm{H}]$ est fini, cet indice est le nombre de classes à gauche, ou le nombre de classes à droite. On a alors

$$|\mathrm{G}| = [\mathrm{G} : \mathrm{H}] \times |\mathrm{H}|.$$

En particulier

Théorème 1.1.10 (Théorème de LAGRANGE)**.** — *Soit* G *un groupe fini. L'ordre de tout sous-groupe de* G *divise* |G|.

Corollaire 1.1.11. — *Soit* G *un groupe fini. L'ordre de tout élément de* G *divise* |G|.

Démonstration. — Soit $g \in \mathrm{G}$. L'ordre de g est par définition l'ordre de $\langle g \rangle$. Mais $\langle g \rangle$ est un sous-groupe de G, le Théorème 1.1.10 permet de conclure. □

1.2. Actions de groupes, sous-groupes distingués, produits semi-directs

Soit G un groupe, soit E un ensemble.

1.2.1. Actions de groupes. — Le groupe G *agit à gauche* sur E s'il existe une application $\varphi\colon \mathrm{G} \times E \to E$ vérifiant

- ◇ pour tout $x \in E$, $\varphi(e, x) = x$;
- ◇ pour tous g, g' dans G, pour tout x dans E

$$\varphi(gg', x) = \varphi(g, \varphi(g', x)).$$

On note $\varphi(g, x) = g \cdot x$; ceci permet de réécrire les propriétés ci-dessus comme suit :

$$e \cdot x = x \qquad\qquad (gg') \cdot x = g \cdot (g' \cdot x).$$

Le groupe G *agit à droite* sur E s'il existe une application $\varphi\colon \mathrm{G} \times E \to E$ vérifiant

- — pour tout $x \in E$, $\varphi(e, x) = x$;
- — pour tous g, g' dans G, pour tout x dans E

$$\varphi(gg', x) = \varphi(g', \varphi(g, x)).$$

On note $\varphi(g, x) = x \cdot g$; ceci permet de réécrire les propriétés ci-dessus comme suit :

$$x \cdot e = x \qquad\qquad x \cdot (gg') = (x \cdot g) \cdot g'.$$

Dans la suite nous ne parlerons que d'actions à gauche que nous appelons simplement actions. On dit aussi que G *opère* sur E.

Se donner une action de G sur E revient à se donner un morphisme de groupes Φ de G dans le groupe $\mathcal{S}_E$ des bijections de E dans lui-même. Pour tout $g \in \mathrm{G}$ on définit $\Phi(g)\colon E \to E$ par

$$\Phi(g)(x) = g \cdot x.$$

Tout morphisme de G dans $\mathcal{S}_E$ définit une action à gauche de G sur E.

Définition 1.2.1. — Soit E un ensemble. Soit G un groupe.

Le groupe G *opère transitivement* sur E si

$$\forall\, x \in E, \forall\, y \in E \qquad \exists\, g \in \mathrm{G} \quad g \cdot x = y.$$

Le groupe G *opère fidèlement* si $\Phi\colon \mathrm{G} \to \mathcal{S}_E$ est injectif, *i.e.* si $g \cdot x = x$ pour tout $x \in E$ implique $g = e$.

Notons que $\mathrm{G}/\ker \Phi$ opère fidèlement sur E.

Si G n'opère pas transitivement on introduit la relation d'équivalence suivante :

$$x \mathcal{R} y \quad \Longleftrightarrow \quad \exists\, g \in \mathrm{G} \quad g \cdot x = y$$

qui mesure le défaut de transitivité. Les classes d'équivalence sont appelées les *orbites* de E sous l'action de G. Les orbites forment donc une partition de E. L'orbite de $x \in E$ est notée $\mathcal{O}_x$. Notons que G opère transitivement sur $\mathcal{O}_x$.

Exemple 1.2.1. — Les orbites du groupe orthogonal $\mathrm{O}(n, \mathbb{R})$ dans son opération naturelle sur $\mathbb{R}^n$ sont les sphères centrées en l'origine.

Exemple 1.2.2 (Décomposition d'une permutation en produit de cycles disjoints)**.** —

Le groupe $\mathcal{S}_n$ opère sur $E = \{1, 2, \ldots, n\}$. Soit $\sigma \in \mathcal{S}_n$ une permutation. Le groupe cyclique $\langle \sigma \rangle$ engendré par σ opère aussi sur E. Soient $\mathcal{O}_1$, $\mathcal{O}_2$, …, $\mathcal{O}_k$ les orbites de E sous l'action de $\langle \sigma \rangle$. Alors les permutations σ_i définies par

$$\sigma_i(x) = \begin{cases} x & \text{si } x \notin \mathcal{O}_i \\ \sigma(x) & \text{si } x \in \mathcal{O}_i \end{cases}$$

sont des cycles, d'ordre $|\mathcal{O}_i|$, deux à deux permutables. De plus $\sigma = \sigma_1 \sigma_2 \ldots \sigma_k$.

Par exemple si $E = \{1, 2, \ldots, 8\}$ et

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix}$$

nous avons $\sigma = (1\ 3\ 4\ 5)(2\ 6\ 8)(7) = (1\ 3\ 4\ 5)(2\ 6\ 8)$; en général les cycles d'ordre 1 sont omis dans l'écriture de σ.

Un élément x de E est *fixe* sous l'action de G si pour tout g dans G on a $g \cdot x = x$.

Soit $A \subset E$. Le *fixateur* de A sous l'action de G est

$$\mathrm{Fix}_{\mathrm{G}}(A) = \{g \in \mathrm{G} \,|\, \forall\, a \in A \quad g \cdot a = a\}.$$

Le *stabilisateur* de A sous l'action de G est

$$\mathrm{Stab}_{\mathrm{G}}(A) = \{g \in \mathrm{G} \,|\, \forall\, a \in A \quad g \cdot a \in A\}.$$

Ces ensembles sont des sous-groupes de G.

Notons que lorsque $A = \{x\}$, on a $\mathrm{Fix}_{\mathrm{G}}(\{x\}) = \mathrm{Stab}_{\mathrm{G}}(\{x\})$ que l'on note souvent G_x.

Exemple 1.2.3. —

Considérons l'action du groupe $\mathcal{S}_n$ sur $E = \{1, 2, \ldots, n\}$. Le stabilisateur d'un point est isomorphe à $\mathcal{S}_{n-1}$.

Orbites et stabilisateurs sont liés par la remarque suivante :

Proposition 1.2.1. —

Soit G *un groupe opérant sur un ensemble* E.

L'application

$$\mathrm{G}/\mathrm{Stab}_{\mathrm{G}}(\{x\}) \to \mathcal{O}_x \qquad\qquad \overline{g} \mapsto g \cdot x$$

est bien définie et est une bijection.

On en déduit l'énoncé suivant.

Corollaire 1.2.2. —

Soit G *un groupe opérant sur un ensemble* E. *Pour tout* $x \in E$ *nous avons*

$$|\mathcal{O}_x| = \frac{|\mathrm{G}|}{|\mathrm{Stab}_{\mathrm{G}}(\{x\})|};$$

en particulier $|\mathcal{O}_x|$ *divise* $|\mathrm{G}|$.

Premier exemple d'action de groupe : action par translation Le groupe G agit sur lui-même par translation à gauche : $g \cdot x = gx$. Cette action définit un morphisme injectif de G dans $\mathcal{S}_{\mathrm{G}}$. Si G est d'ordre fini n, alors $\mathcal{S}_{\mathrm{G}}$ est isomorphe au groupe $\mathcal{S}_n$ des permutations des n éléments de $\{1, 2, \ldots, n\}$ (ou groupe symétrique) ce qui démontre le *théorème de* Cayley :

Théorème 1.2.3 (Théorème de Cayley)***.*** — *Tout groupe fini est isomorphe à un sous-groupe d'un groupe symétrique.*

Tout sous-groupe H d'un groupe G agit par translation à gauche sur les ensembles quotients G/K où K est un sous-groupe de G. Le stabilisateur de la classe à gauche gK est $\mathrm{H} \cap g\mathrm{K}g^{-1}$. Un point fixe gK est tel que $\mathrm{H} \subset g\mathrm{K}g^{-1}$.

Deuxième exemple d'action de groupe : action par conjugaison. — Le groupe G agit sur lui-même par *conjugaison* ou encore par *automorphismes intérieurs* : $\mathrm{G} \times \mathrm{G} \to \mathrm{G}$, $(g, x) \mapsto g \cdot x = gxg^{-1}$. Les orbites pour cette action sont appelées *classes de conjugaison*.

En particulier, si G est le groupe linéaire $\mathrm{GL}(n, \Bbbk)$ les classes de conjugaison regroupent les matrices semblables.

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.

Le groupe G opère sur l'ensemble de ses sous-groupes par automorphisme intérieur : $g \cdot \mathrm{H} = g\mathrm{H}g^{-1}$. Le stabilisateur d'un sous-groupe H sous cette action s'appelle le *normalisateur* de H et est noté $\mathrm{N}_{\mathrm{G}}(\mathrm{H})$. Le sous-groupe H est distingué dans son normalisateur. Deux sous-groupes H et K qui sont dans la même orbite pour cette action, c'est-à-dire tels que $\mathrm{K} = g\mathrm{H}g^{-1}$ pour un élément g de G, sont *conjugués*. Par exemple dans $\mathcal{S}_3$ les trois sous-groupes à deux éléments sont conjugués et sont leurs propres normalisateurs.

Explicitons cette action dans le cas du groupe symétrique.

Proposition 1.2.4. — *Si $\sigma = (a_1\ a_2\ \dots\ a_k) \in \mathcal{S}_n$ est un k-cycle et τ un élément de $\mathcal{S}_n$, nous avons*

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(a_1)\ \tau(a_2)\ \dots\ \tau(a_k)). \tag{1.2.1}$$

Tous les k-cycles sont conjugués dans $\mathcal{S}_n$.

Les classes de conjugaison de $\mathcal{S}_n$ 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 » 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 :

$$\frac{n!}{1^{k_1}k_1!\,2^{k_2}k_2!\,\dots\,m^{k_m}k_m!}.$$

Démonstration. — Si $x \notin \{\tau(a_1), \tau(a_2), \dots, \tau(a_k)\}$, alors $\tau^{-1}(x) \notin \{a_1, a_2, \dots, a_k\}$ donc $\tau \circ \sigma \circ \tau^{-1}(x) = x$. Si en revanche $x = \tau(a_i)$, alors $\tau \circ \sigma\tau^{-1}(x) = \tau \circ \sigma(a_i) = \tau(a_{i+1})$. D'où l'égalité (1.2.1).

Écrivons $\sigma = \sigma_1\sigma_2 \dots \sigma_r$ comme produit de cycles à supports disjoints de longueurs k_1, k_2, …, k_r que nous pouvons ordonner de sorte que $1 \leq k_1 \leq k_2 \leq \ldots \leq k_r$. Alors

$$\tau \circ \sigma \circ \tau^{-1} = (\tau \circ \sigma_1 \circ \tau^{-1}) \circ (\tau \circ \sigma_2 \circ \tau^{-1}) \circ \ldots \circ (\tau \circ \sigma_r \circ \tau^{-1}) \tag{1.2.2}$$

est encore un produit de cycles disjoints de mêmes longueurs k_1, k_2, …, k_r que ceux de σ. Une classe de conjugaison détermine donc bien une partition de $n = k_1+k_2+\ldots+k_r$. Réciproquement compte tenu de (1.2.1) et (1.2.2) nous voyons que des permutations correspondant à la même partition sont conjuguées. □

Exemple 1.2.4. —

1. Les deux partitions de 2 sont 1+1 et 0+2. Les classes de conjugaison correspondantes dans $\mathcal{S}_2$ 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 $\mathcal{S}_3$ 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 $\mathcal{S}_4$ sont $\{\mathrm{id}\}$, les six transpositions, les trois doubles transpositions, les huit 3-cycles et les six 4-cycles.

Exemple 1.2.5 (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 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 $t_0' = (1\ 3\ 5\ 2\ 4)$.

En effet les classes de conjugaison de $\mathcal{A}_5$ peuvent se déduire de celles de $\mathcal{S}_5$. 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 $\mathcal{S}_5$ dans $\mathcal{A}_5$ revient à comprendre le lien du centralisateur Z_g de g dans $\mathcal{S}_5$ avec son centralisateur $Z_g \cap \mathcal{A}_5$ dans $\mathcal{A}_5$.

Rappelons $\mathcal{A}_5$ est le noyau du morphisme

$$\mathrm{sgn}\colon \mathcal{S}_5 \to \{1, -1\}.$$

Par suite si H est un sous-groupe de $\mathcal{S}_5$, 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 $\mathcal{S}_5$. Si $C \cap \mathcal{A}_5 \neq \emptyset$, alors le caractère χ_{sgn} de $\mathcal{S}_5$ 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 $\mathcal{S}_5$, alors nous avons l'alternative suivante

◇ ou bien $Z_g \subset \mathcal{A}_5$ et alors

$$|C_g| = \frac{|\mathcal{A}_5|}{|Z_g|} = \frac{1}{2}\frac{|\mathcal{S}_5|}{|Z_g|} = \frac{1}{2}|C|$$

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

$$|C_g| = \frac{|\mathcal{A}_5|}{|Z_g \cap \mathcal{A}_5|} = \frac{\frac{|\mathcal{S}_5|}{2}}{\frac{|Z_g|}{2}} = \frac{|\mathcal{S}_5|}{|Z_g|} = |C|$$

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 $\sigma = (2\ 3\ 5\ 4) \in \mathcal{S}_5 \smallsetminus \mathcal{A}_5$. À partir de

$$(1\ 3\ 5\ 2\ 4) = \sigma(1\ 2\ 3\ 4\ 5)\sigma^{-1}$$

nous obtenons que t_0 et t_0^2 ne sont pas dans la même classe de conjugaison de $\mathcal{A}_5$. Puisque les 5-cycles sont toujours conjugués dans $\mathcal{S}_5$ pour tout 5-cycle t, les 5-cycles t et t^2 ne sont pas dans la même classe.

De manière générale la conjugaison préserve les propriétés d'une transformation. Par exemple si $\sigma \in \mathrm{O}(3,\mathbb{R})$ est une rotation autour d'une droite D et τ appartient à $\mathrm{O}(3,\mathbb{R})$, alors $\tau\circ\sigma\circ\tau^{-1}$ est une rotation de même angle autour de la droite $\tau(D)$.

On dit que E est un *ensemble transitif* sous l'action de G si E ne contient qu'une seule orbite.

Dans ce cas si H est le fixateur (ou le stabilisateur) d'un élément quelconque x de E il existe une bijection $\varphi\colon E \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ telle que $\varphi(g\cdot x) = g\cdot\varphi(x)$ (on fait agir G sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ comme ci-dessus, *i.e.* par $g\cdot(x\mathrm{H}) = (gx)\mathrm{H}$). Lorsque E et G sont finis, on a

$$\mathrm{Card}(E) = \frac{|\mathrm{G}|}{|\mathrm{H}|} = \frac{|\mathrm{G}|}{|\mathrm{Fix}_{\mathrm{G}}(x)|}$$

Les fixateurs de deux éléments de E ont même ordre et de plus sont deux groupes conjugués.

Si E n'est pas transitif les résultats ci-dessus s'appliquent à toute orbite de E, car toute orbite est transitive sous l'action de G.

Application. On a l'égalité

$${}^{\mathrm{G}}\!/_{\mathrm{N_G(H)}} = \{g\mathrm{H}g^{-1} \,|\, g \in \mathrm{G}\}.$$

Par conséquent le nombre de sous-groupes conjugués à un sous-groupe H donné est égal à l'indice du normalisé de H dans G.

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 |G|.

Proposition 1.2.5 (Formule des classes)***.*** — *Soit E un ensemble fini. Soit* G *un groupe fini. Soient $\mathcal{O}_{s_1}$, $\mathcal{O}_{s_2}$, …, $\mathcal{O}_{s_n}$ les orbites de E sous l'action de* G*. On a l'égalité*

$$card(E) = \sum_{i=1}^{n} card(\mathcal{O}_{s_i}) = \sum_{i=1}^{n} \frac{|\mathrm{G}|}{|\mathrm{Fix}_{\mathrm{G}}(s_i)|} = [\mathrm{G} : \mathrm{Stab}_{\mathrm{G}}(\{x\})].$$

Considérons l'action de G sur lui-même par conjugaison. L'orbite d'un élément h du centre $Z(\mathrm{G})$ de G est égale à $\{h\}$. Le fixateur d'un élément quelconque g de G pour l'action considérée est le centralisateur $\mathrm{C_G}(g)$ de cet élément. On a

$$\mathrm{C_G}(g) = \{h \in \mathrm{G} \,|\, gh = hg\}.$$

Par conséquent si G est un groupe fini, le nombre d'éléments conjugués à $g \in \mathrm{G}$ est égal à l'indice du centralisateur de g dans G. Enfin 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

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{q} \mathrm{card}(\mathcal{O}_{g_i}) = |Z(\mathrm{G})| + \sum_{i=1}^{q} \frac{|\mathrm{G}|}{|\mathrm{C_G}(g_i)|}.$$

Définition 1.2.2. — 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 $D(\mathrm{G})$.

Exemple 1.2.6. — Si G est abélien, alors $D(\mathrm{G}) = \{e_{\mathrm{G}}\}$.

Exemple 1.2.7. — Si $\sigma = (1\ 2\ 3)$, alors $D(\mathcal{S}_3) = \{\mathrm{id}, \sigma, \sigma^2\}$.

Exemple 1.2.8. — Nous avons $D(\mathcal{A}_5) = \mathcal{A}_5$.

Exemple 1.2.9. — Le groupe dérivé du groupe des quaternions $\mathbb{H}_8$ est $\{1, -1\}$.

1.2.2. Sous-groupes distingués, groupes quotients. — Lorsqu'un sous-groupe H de G est distingué, on peut munir G/H $\left(\text{et } \mathrm{H}\backslash\mathrm{G}\right)$ d'une structure de groupe induite par celle de G.

Définition 1.2.3. — Un sous-groupe H d'un groupe G est *distingué* si pour tout $g \in \mathrm{G}$ on a $g\mathrm{H} = \mathrm{H}g$.

Autrement dit dire que H est distingué dans G revient à dire que pour tout $g \in \mathrm{G}$ on a $g\mathrm{H}g^{-1} = \mathrm{H}$, ou encore que H est stable par conjugaison.

Lorsqu'un sous-groupe H d'un groupe G est distingué, on note $\mathrm{H} \triangleleft \mathrm{G}$.

Lorsqu'un sous-groupe H est distingué dans G, les relations à droite et à gauche modulo H coïncident et $\mathrm{G}/\mathrm{H} = \mathrm{H}\backslash\mathrm{G}$.

Exemple 1.2.10. — Soient G et H deux groupes. Le noyau d'un morphisme de groupes de G dans H est un sous-groupe distingué de G.

Exemple 1.2.11. — Soit G un groupe. Le sous-groupe des automorphismes intérieurs de G est distingué dans le groupe des automorphismes de G.

Exemple 1.2.12. — Soit G un groupe. Le groupe dérivé $D(\mathrm{G})$ de G est un sous-groupe distingué de G.

Soit G un groupe. Soit H un sous-groupe distingué de G. On définit une loi interne sur G/H :

$$(g\mathrm{H}) \cdot (g'\mathrm{H}) = gg'\mathrm{H}.$$

Muni de cette loi G/H est un groupe, appelé *groupe quotient* de G par H et l'application surjective canonique $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$ est un morphisme de groupes. L'élément neutre pour cette loi de groupe est H.

Remarque 1.2.1. — Lorsque G est un groupe et H un sous-groupe distingué de G, les éléments de G/H sont notés $g\mathrm{H}$ ou encore $[g]$. Par exemple $[e] = \mathrm{H}$.

Exemple 1.2.13. — Le groupe quotient $\mathbb{H}_8/Z(\mathbb{H}_8) = \mathbb{H}_8/\{\pm 1\}$ est isomorphe au groupe de Klein $\mathcal{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il y a cinq classes de conjugaison : $\{1\}$, $\{-1\}$, $\{i, -i\}$, $\{j, -j\}$, $\{k, -k\}$.

Soient G et G′ deux groupes. Soit $\varphi\colon \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes.

1. Le morphisme φ *passe au quotient* par $\ker\varphi$ en définissant un morphisme
$$\overline{\varphi}\colon \mathrm{G}/\ker\varphi \to \mathrm{G}'.$$
Ceci signifie que $\varphi(g)$ ne dépend que de la classe $[g]$ de g modulo $\ker\varphi$ (rappel : $\ker\varphi$ est un sous-groupe distingué de G) ou encore que si $g = h$ modulo $\ker\varphi$, alors $\varphi(g) = \varphi(h)$. On peut donc poser pour $[g] \in \mathrm{G}/\ker\varphi$
$$\overline{\varphi}([g]) = \varphi(g).$$
Si on restreint l'ensemble d'arrivée de $\overline{\varphi}$ à $\mathrm{Im}\varphi = \mathrm{Im}\overline{\varphi}$ on obtient l'isomorphisme suivant
$$\widetilde{\varphi}\colon \mathrm{G}/\ker\varphi \to \mathrm{Im}\,\varphi.$$
2. Plus généralement si H est un sous-groupe distingué de G tel que $\mathrm{H} \subset \ker\varphi$, alors le morphisme φ passe au quotient par H en définissant un morphisme $\overline{\varphi}\colon \mathrm{G}/\mathrm{H} \to \mathrm{G}'$.

   Une autre façon de dire que φ passe au quotient est de dire qu'il existe un morphisme $\overline{\varphi}$ tel que $\varphi = \overline{\varphi} \circ \pi$
$$\begin{array}{ccc} \mathrm{G} & \xrightarrow{\varphi} & \mathrm{G}' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\varphi}} & \\ \mathrm{G}/\mathrm{H} & & \end{array}$$
où $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$ est la surjection canonique. On dit que φ *se factorise par* π.
3. Revenons au cas $\mathrm{H} = \ker\varphi$. Notons i l'inclusion de $\mathrm{Im}\,\varphi$ dans G′. La décomposition canonique du morphisme φ est : $\varphi = i \circ \widetilde{\varphi} \circ \pi$
$$\mathrm{G} \xrightarrow[\text{surjectif}]{\pi} \mathrm{G}/\ker\varphi \xrightarrow[\text{isomorphisme}]{\widetilde{\varphi}} \mathrm{Im}\,\varphi \xrightarrow[\text{injectif}]{i} \mathrm{G}'$$

Soit G un groupe. Soient H et K deux sous-groupes distingués de G tels que
- $\mathrm{K} \subset \mathrm{H}$;
- $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{K}$ est la surjection canonique.

Alors
- H/K est isomorphe au sous-groupe distingué $\pi(\mathrm{H})$ de G/K. En général on identifie $\pi(\mathrm{H})$ et H/K.
- G/H est isomorphe à $\mathrm{G}/\mathrm{K}/\mathrm{H}/\mathrm{K}$.

Soit G un groupe. Soient H un sous-groupe distingué de G et K un sous-groupe de G. Alors
- ◇ HK = KH et HK est un sous-groupe de G ;
- ◇ H est un sous-groupe distingué de HK ;
- ◇ $^{\mathrm{HK}}\!/_{\mathrm{H}}$ et $^{\mathrm{K}}\!/_{\mathrm{K}\cap\mathrm{H}}$ sont isomorphes.

Application. Soit $\varphi\colon \mathrm{G}\to\mathrm{G}'$ un morphisme de groupes. Soit K' un sous-groupe de G'. L'image réciproque $\mathrm{K}=\varphi^{-1}(\mathrm{K}')$ de K' par φ est un sous-groupe distingué de G et $^{\mathrm{G}}\!/_{\mathrm{K}}$ est isomorphe à $^{\mathrm{G}'}\!/_{\mathrm{K}'}$.

Définition 1.2.4. — Soit G un groupe. Un sous-groupe de G qui est stable par tout automorphisme de G est dit *caractéristique*.

Exemple 1.2.14. — Soit G un groupe. Le groupe $D(\mathrm{G})$ engendré par les commutateurs de G est caractéristique. En effet si φ est un automorphisme de G, si g et h sont des éléments de G, alors $\varphi(ghg^{-1}h^{-1})=\varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1}$ autrement dit les commutateurs sont conservés.

Tout sous-groupe caractéristique de G est distingué dans G.

Tout sous-groupe caractéristique d'un sous-groupe distingué de G est un sous-groupe distingué de G.

Définition 1.2.5. — Un groupe *simple* est un groupe qui ne contient aucun sous-groupe distingué propre.

Les groupes abéliens simples sont isomorphes à $\left(^{\mathbb{Z}}\!/_{p\mathbb{Z}},+\right)$ où p est premier.

1.3. Applications

1.3.1. Les groupes $^{\mathrm{SU}(2,\mathbb{C})}\!/_{\{\pm\mathrm{id}\}}$ et $\mathrm{SO}(3,\mathbb{R})$ sont isomorphes. —

Référence : [**CG17**, p. 232-234]

Leçons possibles :

182 : *Applications des nombres complexes à la géométrie.*

108 : *Exemples de parties génératrices D'un groupe. Applications.*

191 : *Exemples d'utilisation des techniques d'algèbre en géométrie.*

103 : *Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.*

Soit $E=\mathbb{R}^n$ et soit q la forme quadratique canonique $q(x_1,x_2,\dots,x_n)=\sum_{k=1}^{n}x_k^2$. 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 $n\times n$

$$\mathrm{O}(n,\mathbb{R})=\left\{A\in\mathrm{GL}(n,\mathbb{R})\,|\,{}^{\mathrm{t}}AA=A{}^{\mathrm{t}}A=\mathrm{Id}\right\}$$

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

$$\mathrm{SU}(2,\mathbb{C}) = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in M(2,\mathbb{C}) \mid |a|^2 + |b|^2 = 1 \right\}.$$

Rappelons que le groupe $\mathrm{SU}(2,\mathbb{C})$ est difféomorphe à la sphère $\mathbb{S}^3 \subset \mathbb{R}^4$ via

$$\varphi\colon \mathbb{S}^3 \subset \mathbb{R}^4 \to \mathrm{SU}(2,\mathbb{C}), \qquad (\alpha,\beta,\gamma,\delta) \mapsto \begin{pmatrix} \alpha + \mathbf{i}\beta & -\gamma + \mathbf{i}\delta \\ \gamma + \mathbf{i}\delta & \alpha - \mathbf{i}\beta \end{pmatrix}.$$

Théorème 1.3.1. — *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 1.3.2. — *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 1.3.1. — Rappelons que

$$\mathbb{H} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \in M(2,\mathbb{C}) \mid a,\, b \in \mathbb{C} \right\}.$$

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

$$\begin{aligned} \varphi\colon \mathrm{SU}(2,\mathbb{C}) &\to \mathrm{Aut}(\mathbb{H}) \\ h &\mapsto \varphi_h\colon \mathbb{H} \to \mathbb{H} \\ & \qquad u \mapsto huh^{-1} \end{aligned}$$

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

$$\begin{aligned} \varphi\colon \mathrm{SU}(2,\mathbb{C}) &\to \mathrm{O}(\mathbb{I}) \\ h &\mapsto \varphi_h\colon \mathbb{I} \to \mathbb{I} \\ & \qquad u \mapsto huh^{-1} \end{aligned}$$

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

$$\ker\varphi = \{M \in \mathrm{SU}(2,\mathbb{C}) \,|\, \text{ } M \text{ commute avec } I,\, J \text{ et } K\}.$$

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 1.3.2 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 $\varphi_h(u) = -u$.

□

1.3.2. Théorème de Wedderburn. — *Référence :* [**Per82**, p. 82]

Leçons possibles :

101 : *Groupe opérant sur un ensemble. Exemples et applications.*

123 : *Corps finis. Applications.*

Théorème 1.3.3. — *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 $\mu_n(\Bbbk)$

$$\mu_n(\Bbbk) = \{\zeta \in \Bbbk \,|\, \zeta^n = 1\}.$$

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 (voir [Perrin, Cours d'algèbre, page 24]). 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 1.3.1. —
- ◇ Si ζ est une racine n-ième primitive de l'unité, les autres sont les ζ^m avec $\operatorname{pgcd}(n, m) = 1$.
- ◇ Le polynôme $\phi_{n,\Bbbk}$ est unitaire, de degré $\varphi(n)$.

Proposition 1.3.4. — *On a la formule*

$$X^n - 1 = \prod_{d|n} \phi_{d,\Bbbk}(X).$$

Démonstration. — Cela résulte de l'égalité

$$X^n - 1 = \prod_{d|n} \phi_d(X)$$

(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 1.3.2. — En comparant les degrés des polynômes on retrouve la formule

$$n = \sum_{d|n} \varphi(d).$$

Démonstration du Théorème 1.3.3. — 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 $|\Bbbk| = q^n$.

Si $\Bbbk$ est commutatif la démonstration est terminée. Supposons donc $\Bbbk$ non commutatif. En particulier $n > 1$. Alors $\Bbbk^*$ opère sur lui-même par automorphismes intérieurs

$$\iota_g \colon \Bbbk^* \to \Bbbk^*, \qquad\qquad x \mapsto gxg^{-1}.$$

Considérons cette action. Pour $g \in \Bbbk^*$ on note $\mathcal{O}_g$ l'orbite de g. Posons

$$\Bbbk_g = \{x \in \Bbbk \,|\, gx = xg\}.$$

Notons que $\Bbbk_g$ est un sous-corps de $\Bbbk$ (pas nécessairement commutatif). Le stabilisateur de g est $\Bbbk_g^*$.

On a $|\Bbbk_g| = q^d$; de plus d divise n (en effet l'inclusion $\Bbbk_g^* \subset \Bbbk^*$ entraîne que $q^d - 1$ divise $q^n - 1$ et pour $q \in \mathbb{N}$, $q \geq 2$, ceci implique que d divise n). Le cardinal de $\mathcal{O}_g$ est

$$|\mathcal{O}_g| = \frac{|\Bbbk^*|}{|\Bbbk_g^*|} = \frac{q^n - 1}{q^d - 1}.$$

Par définition des polynômes cyclotomiques on a dans $\mathbb{Z}$

$$q^n - 1 = \prod_{m|n} \phi_m(q)$$

et

$$q^d - 1 = \prod_{m|d} \phi_m(q).$$

Il en résulte que

$$\frac{q^n - 1}{q^d - 1} = \prod_{m|n,\, m\not|d} \phi_m(q).$$

En particulier $\phi_n(q)$ divise $\frac{q^n-1}{q^d-1}$.

D'après l'équation aux classes

$$|\Bbbk^*| = |Z(\Bbbk)^*| + \sum_{g \notin Z(\Bbbk)} |\mathcal{O}_g|.$$

Or $g \notin Z(\Bbbk)$ si et seulement si $d \neq n$ de sorte que

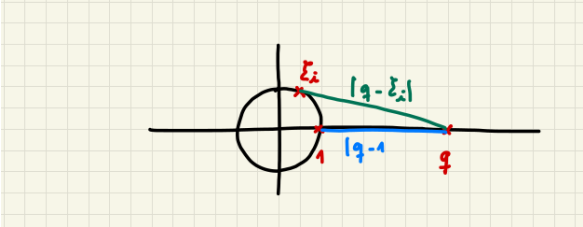
$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}$$

la somme portant sur un certain nombre de diviseurs stricts de n. 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

$$\begin{cases} |\xi_i| = 1 \\ \xi_i \neq 1 \text{ (car } n \neq 1) \end{cases}$$

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. □

1.3.3. Automorphismes de $\mathbb{Z}/n\mathbb{Z}$. — *Références :* [**Per82**, p. 24-26], [**Ser77**, p. 12-13]

Leçons possibles :

120 : *Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.*

104 : *Groupes abéliens et non abéliens finis. Exemples et applications.*

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 1.3.5. — *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 1.3.1. — 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 1.3.5 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 1.3.6. — *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 1.3.5). Considérons

$$\varphi \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) \mapsto \varphi(\overline{1}) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$$

Montrons que φ est l'homothétie de rapport $\overline{a} = \varphi(\overline{1})$. Nous pouvons supposer que $a \geq 1$. Pour tout $0 \leq x \leq n-1$ on écrit

$$\varphi(\overline{x}) = \varphi(\underbrace{\overline{1}+\overline{1}+\ldots+\overline{1}}_{x \text{ fois}}) = \underbrace{\varphi(\overline{1})+\varphi(\overline{1})+\ldots+\varphi(\overline{1})}_{x \text{ fois}} = \underbrace{\overline{a}+\overline{a}+\ldots+\overline{a}}_{x \text{ fois}} = \overline{ax}.$$

Ceci implique que la bijection

$$\varphi \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) \mapsto \varphi(\overline{1}) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$$

est un morphisme de groupes donc un isomorphisme.

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 :

Proposition 1.3.7 (Lemme chinois)**.** — *Si p et q sont premiers entre eux, alors*

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Démonstration. — Soit $\overline{n}$, resp. $\widehat{n}$, resp. $\dot{n}$ la classe de n modulo pq, resp. p, resp. q. Considérons l'homomorphisme

$$\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \qquad \overline{n} \mapsto (\widehat{n}, \dot{n})$$

Il est injectif car $\operatorname{pgcd}(p,q) = 1$. On conclut grâce à l'égalité $\left|\mathbb{Z}/pq\mathbb{Z}\right| = \left|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}\right|$. □

Proposition 1.3.8. — *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 1.3.9. — *Si p est un nombre premier, alors*

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

Remarque 1.3.3. — 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

$$n = \#(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} \#\Phi_d = \sum_{d|n} \varphi(d).$$

Lemme 1.3.10. — *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 1.3.9. — On applique le Lemme 1.3.10 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 1.3.11. — *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 1.3.12. — *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 $i \geq 2$ p^{k+3} est en facteur donc

$$(1+p)^{p^{k+1}} = 1 + p^{k+2}(\lambda + up).$$

□

Démonstration de la Proposition 1.3.11. — D'après le Lemme 1.3.12 $1 + p$ est un élément d'ordre $p^{\alpha-1}$ de $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$. En effet

$$(1+p)^{p^{\alpha-1}} = 1 + \lambda p^\alpha \equiv 1 \bmod p^\alpha$$

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 1.3.9). 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 1.3.12 et le groupe est cyclique. □

Il reste à traiter le cas $p = 2$:

Proposition 1.3.13. — *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 1.3.4. — Le groupe $\left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times$ n'est donc pas cyclique dès que $\alpha \geq 3$.

Lemme 1.3.14. — *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 1.3.13. — 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 1.3.14). 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 :

$$\left(\mathbb{Z}/2^{\alpha}\mathbb{Z}\right)^{\times} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$

□

1.3.4. Isomorphismes exceptionnels. — *Référence :* [**Per82**, p. 106]

Leçons possibles :

101 : *Groupe opérant sur un ensemble. Exemples et applications.*

103 : *Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.*

104 : *Groupes abéliens et non abéliens finis. Exemples et applications.*

105 : *Groupe des permutations d'un ensemble fini. Applications.*

106 : *Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.*

Quelques rappels

Définitions 1.3.2. — Soit E un plan vectoriel (*i.e.* un espace vectoriel de dimension 2) sur $\mathbb{k}$.

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 $\mathbb{k}^2$ est notée $\mathbb{P}^1(\mathbb{k})$; elle est appelée *droite projective standard sur* $\mathbb{k}$.

Soit E un plan vectoriel. A tout vecteur $x \in E \setminus \{0\}$ associons la droite vectorielle $\mathbb{k}x$. On définit ainsi une application canonique

$$p\colon E \setminus \{0\} \to \mathbb{P}(E) \qquad\qquad x \mapsto [x].$$

Elle est surjective : si D est une droite vectorielle de E et x un vecteur non nul de D, nous avons $D = \mathbb{k}x = [x]$. La relation d'équivalence $\mathcal{R}$ sur $E \setminus \{0\}$ associée à p est la *relation de colinéarité* : si x et y appartiennent à $E \setminus \{0\}$, alors $x\mathcal{R}y$ équivaut à $\mathbb{k}x = \mathbb{k}y$. Les classes modulo $\mathcal{R}$ sont donc les $D \setminus \{0\}$ où D appartient à $\mathbb{P}(E)$. Nous identifions donc, via p, l'ensemble $\mathbb{P}(E)$ à l'ensemble quotient $E \setminus \{0\}/\mathcal{R}$.

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 1.3.3. — 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 1.3.15. — *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 1.3.16. — *Soient Δ et Δ' deux droites projectives et t_1, t_2, t_3 (resp. t'_1, t'_2, t'_3) trois points de Δ (resp. 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 (resp. 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 1.3.5. — 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 $\mathcal{S}_{\mathbb{P}(E)}$ des permutations de $\mathbb{P}(E)$.

Proposition 1.3.17. — *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 $\mathcal{S}_{\mathbb{P}(E)}$, 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 1.3.5.

Concernant la seconde assertion : la surjectivité résulte de la définition d'une homographie et la description du noyau du Lemme 1.3.15 □

L'énoncé suivant est une simple traduction du Théorème 1.3.16 lorsque $E = E'$:

Théorème 1.3.18. — *Soit E un plan vectoriel. L'opération naturelle de $\mathrm{PGL}(E)$, qui est un sous-groupe de $\mathcal{S}_{\mathbb{P}(E)}$, sur $\mathbb{P}(E)$ est simplement 3 fois transitif*[1]*. Autrement dit étant donnés trois points distincts t_1, t_2, t_3 (resp. 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 1.3.19. — *Considérons l'application*

$$\varphi \colon \Bbbk^2 \smallsetminus \{0\} \to \widehat{\Bbbk} \qquad\qquad (x, y) \mapsto \begin{cases} \frac{x}{y} \text{ si } y \neq 0 \\ \infty \text{ si } y = 0 \end{cases}$$

Alors φ induit une bijection Φ de $\mathbb{P}^1(\Bbbk) = {}^{(\Bbbk^2 \smallsetminus \{0\})}\!/_{\mathcal{R}}$ sur $\widehat{\Bbbk}$.

---

1. 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, …, x_n et n points distincts y_1, y_2, …, y_n quelconques dans E, il existe toujours au moins un élément g de G tel que $g \cdot x_1 = y_1$, $g \cdot x_2 = y_2$, …, $g \cdot x_n = y_n$

Démonstration. — Tout d'abord φ est surjective. En effet $\infty = \varphi((1,0))$ et $t = \varphi((t,1))$ pour tout $k \in \Bbbk$.

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 ou bien $y = y' = 0$ ou bien $y \neq 0$, $y' \neq 0$ 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 1.3.20. — *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 $z = \varphi((x,y))$ 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 $\widetilde{h}(z) = \varphi((x',y'))$ c'est-à-dire

$$\widetilde{h}(z) = \varphi((ax+by, cx+dy)).$$

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
$$\widetilde{h}(z) = \varphi(y(az+b, cx+d)) = \varphi((az+b, cz+d)).$$
   - ◇ 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 $\widetilde{h}(z) = \varphi((az+b, 0)) = \infty$.
2. Supposons que $z = \infty$, *i.e.* que $y = 0$. Alors $x \neq 0$ et
$$\widetilde{h}(\infty) = \varphi(x(a,c)) = \varphi((a,c)).$$
   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 1.3.19 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 $\mathcal{S}_{\widehat{\Bbbk}}$. 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 1.3.20. Rappelons que

$$\mathrm{GL}(2,\Bbbk) \to \mathrm{PGL}(2,\Bbbk) \qquad\qquad M \mapsto [M]$$

est un morphisme surjectif dont le noyau est $\{\lambda \mathrm{id} \mid \lambda \in \Bbbk^*\}$. Par ailleurs l'opération naturelle de $\mathrm{PGL}(2,\Bbbk)$ sur $\widehat{\Bbbk}$ est simplement 3 fois transitive comme dans le Théorème 1.3.18. L'énoncé suivant donne la description du stabilisateur de ∞ :

Lemme 1.3.21. — *Le stabilisateur de ∞ dans l'opération 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 1.3.20 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 1.3.6 (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 1.3.18 assure que $\mathrm{PGL}(E)$ opère simplement 3 fois transitivement sur $\mathbb{P}(E)$, *i.e.* il opère 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'opération naturelle et fidèle de $\mathrm{PGL}(E)$ sur $\mathbb{P}(E)$ est associé un morphisme injectif de $\mathrm{PGL}(E)$ dans $\mathcal{S}_{\mathbb{P}(E)}$. En numérotant les points de $\mathbb{P}(E)$ on obtient donc un morphisme injectif de $\mathrm{PGL}(E)$ dans $\mathcal{S}_{q+1}$, *i.e.* $\mathrm{PGL}(E)$ est isomorphe à un sous-groupe de $\mathcal{S}_{q+1}$.

Théorème 1.3.22. — *On a les isomorphismes suivants*

1. $\mathrm{GL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2) = \mathrm{PSL}(2,\mathbb{F}_2) \simeq \mathcal{S}_3$;
2. $\mathrm{PGL}(2,\mathbb{F}_3) \simeq \mathcal{S}_4$ *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. $\mathrm{PGL}(2,\mathbb{F}_5) \simeq \mathcal{S}_5$ *et* $\mathrm{PSL}(2,\mathbb{F}_5) \simeq \mathcal{A}_5$.

Lemme 1.3.23. — *Tout sous-groupe d'indice n dans $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$.*

Démonstration. — Soit H un sous-groupe d'indice n dans $\mathcal{S}_n$.

Si $n \leq 3$, on vérifie l'énoncé directement.

Si $n = 4$, alors : si $\mathrm{H} \not\simeq \mathcal{S}_3$, 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 $\mathcal{S}_4$ ne contient pas d'élément d'ordre 6.

Supposons $n \geq 5$. Le groupe $\mathcal{S}_n$, et donc aussi H, opère par translation à gauche sur $E = {}^{\mathcal{S}_n}\!/_{\mathrm{H}}$ d'où un homomorphisme

$$\varphi\colon \mathcal{S}_n \to \mathcal{S}_E \simeq \mathcal{S}_n.$$

Puisque $\ker\varphi = \bigcap_{a\in\mathcal{S}_n} a\mathrm{H}a^{-1}$, $\ker\varphi$ est distingué dans $\mathcal{S}_n$ et $\ker\varphi \subset \mathrm{H}$ on a $\ker\varphi = \{\mathrm{id}\}$ (rappel : pour $n \geq 5$ les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$). Pour des raisons de cardinalité ($|\mathcal{S}_n| = |\mathcal{S}_E \simeq \mathcal{S}_n|$), φ est un isomorphisme.

Comme H est le stabilisateur de la classe de idH on a : $\varphi(\mathrm{H}) \subset \mathcal{S}_n$ est le stabilisateur d'un point et c'est donc un sous-groupe isomorphe à $\mathcal{S}_{n-1}$. □

Démonstration du Théorème 1.3.22. — 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 $\mathrm{GL}(E)$ opère sur $\mathbb{P}(E)$ et les homothéties opérant trivialement $\mathrm{PGL}(E)$ opère aussi sur $\mathbb{P}(E)$. De plus $\mathrm{PGL}(E)$ opère fidèlement sur $\mathbb{P}(E)$ ([**Per82**, p. 98]).

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

$$\varphi\colon \mathrm{PGL}(2,\mathbb{F}_q) \hookrightarrow \mathcal{S}_{q+1}.$$

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 $\mathrm{PGL}(2,\mathbb{F}_3) \simeq \mathcal{S}_4$. Puisque $\mathcal{A}_4$ est le seul sous-groupe d'indice 2 dans $\mathcal{S}_4$ 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 $\mathcal{S}_5$ 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 $\mathcal{S}_6$. Ainsi, d'après le Lemme 1.3.23, le groupe $\mathrm{PGL}(2,\mathbb{F}_5)$ est isomorphe à $\mathcal{S}_5$. Il en résulte que
$$\mathrm{PSL}(2,\mathbb{F}_5) \simeq \mathcal{A}_5.$$

□

1.3.5. Sous-groupes additifs de $\mathbb{R}$. —

Proposition 1.3.24. — *Soit* G *un sous-groupe de* $(\mathbb{R},+)$ *non réduit à* $\{0\}$. *Alors* G *est ou bien dense dans* $\mathbb{R}$, *ou bien monogène, i.e. de la forme* $a\mathbb{Z}$ *avec* $a>0$ *(donc discret).*

Démonstration. — Si G est monogène, *i.e.* si $\mathrm{G} = a\mathbb{Z}$, avec $a>0$, alors a est le plus petit élément strictement positif de G. Si G est dense dans $\mathbb{R}$, alors $\mathrm{G}\cap\mathbb{R}_+^*$ n'a pas de plus petit élément mais une borne inférieure non nulle. On introduit donc
$$\mathrm{G}_+ = \mathrm{G}\cap\mathbb{R}_+^* \qquad\qquad a = \inf \mathrm{G}_+$$
Le réel $a \geq 0$ est bien défini car G_+ est non vide et minorée. En effet il existe un élément g dans G non nul donc x ou $-x$ est dans G_+ qui est minoré par 0.

On va distinguer le cas $a>0$ du cas $a=0$.

- ◇ Supposons $a>0$. Montrons que a appartient à G puis que $\mathrm{G} = a\mathbb{Z}$.

  Raisonnons par l'absurde : supposons que a n'appartienne pas à G. Puisque $a>0$, on a $2a>a$. Il existe g dans G_+ tel que $g<2a$. Comme a n'appartient pas à G, on a les inégalités $a<g<2a$. Il existe alors h dans G_+ tel que $h<g$. On a $a<h<g<2a$ car a n'appartient pas à G. De plus comme g et h appatiennent à G, la différence $g-h$ appartient à G et on a même $g-h$ appartient à G_+. D'une part $a<h$ donc $a-h<0$ et $2a-h<a$, d'autre part $g<2a$ donc $g-h<2a-h$. Par conséquent $g-h<a$: contradiction avec la définition de a. Par suite a appartient à G. Ainsi le groupe $a\mathbb{Z}$ engendré par a est inclus dans G.

  Réciproquement soit g un élément de G. Posons $k = E\left(\frac{g}{a}\right) \in \mathbb{Z}$. Puisque G est un groupe le réel $g-ak$ appartient à G. Comme $k \leq \frac{g}{a} < k+1$ on a $0 \leq g-ak < a = \min \mathrm{G}_+$. Nécessairement $g-ak=0$ et $g = ak \in a\mathbb{Z}$. Il en résulte que $\mathrm{G} = a\mathbb{Z}$.
- ◇ Supposons que $a=0$. Montrons qu'alors G est dense dans $\mathbb{R}$, autrement dit que G rencontre tout intervalle ouvert de $\mathbb{R}$. Soit $I =]\alpha,\beta[$ un intervalle ouvert de $\mathbb{R}$. Comme $a=0$ il existe $g \in \mathrm{G}$ tel que $0<g<\beta-\alpha$. Le sous-groupe $g\mathbb{Z}$ engendré par g est inclus dans G et intersecte I (sinon il existerait $k\in\mathbb{Z}$ tel que $I \subset]kg,(k+1)g[$ ce qui contredirait l'inégalité $g<\beta-\alpha$). Il s'en suit que G est dense dans $\mathbb{R}$.

□

1.3.6. Étude du groupe $\mathrm{O}(p,q)$. — *Références :* [**CG17**]

Leçons possibles :

171 *: formes quadratiques réelles. Coniques. Exemples et applications*

106 *: groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de* $\mathrm{GL}(E)$. *Applications.*

156 : *exponentielle de matrices. Applications.*

150 : *exemples d'actions de groupes sur les espaces de matrices.*

Soit n un entier naturel. L'ensemble des matrices symétriques définies positives de taille $n \times n$ est

$$\begin{aligned} \mathrm{S}^{++}(n,\mathbb{R}) &= \left\{ S \in \mathrm{GL}(n,\mathbb{R}) \mid \left\{ \begin{array}{ll} {}^{\mathrm{t}}S = S & \\ \forall\, x \in \mathbb{R}^n \smallsetminus \{0\} & {}^{\mathrm{t}}xSx > 0 \end{array} \right. \right\} \\ &= \left\{ P\,{}^{\mathrm{t}}P \in \mathrm{M}(n,\mathbb{R}) \mid P \in \mathrm{GL}(n,\mathbb{R}) \right\} \end{aligned}$$

Remarque 1.3.7. — L'ensemble des matrices symétriques définies positives forme un système homogène (*i.e.* un espace sur lequel un groupe agit de façon transitive).

Théorème 1.3.25 (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

$$I_{p,q} = \left(\begin{array}{cccc|cccc} 1 & 0 & \ldots & 0 & & & & \\ 0 & \ddots & \ddots & \vdots & & & & \\ \vdots & \ddots & \ddots & 0 & & 0 & & \\ 0 & \ldots & 0 & 1 & & & & \\ \hline & & & & -1 & 0 & \ldots & 0 \\ & & & & 0 & \ddots & \ddots & \vdots \\ & 0 & & & \vdots & \ddots & \ddots & 0 \\ & & & & 0 & \ldots & 0 & -1 \end{array} \right)$$

Proposition 1.3.26. — *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 $T = {}^tMM$. On peut vérifier que $S^2 = T$. Montrons que $\mathrm{O}(p,q)$ est stable par transposition :

$$\begin{aligned} M \in \mathrm{O}(p,q) &\Rightarrow MI_{p,q}{}^tM = I_{p,q} \\ &\Rightarrow {}^tM^{-1}I_{p,q}M^{-1} = I_{p,q} \\ &\Rightarrow {}^tM^{-1} \in \mathrm{O}(p,q) \\ &\Rightarrow {}^tM \in \mathrm{O}(p,q) \end{aligned}$$

On en déduit que $T = {}^tMM \in \mathrm{O}(p,q)$ 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

$$\begin{aligned} T \in \mathrm{O}(p,q) &\Leftrightarrow TI_{p,q}{}^tT = I_{p,q} \\ &\Leftrightarrow {}^tT = I_{p,q}T^{-1}I_{p,q}^{-1} \\ &\Leftrightarrow {}^t\exp(U) = I_{p,q}(\exp U)^{-1}I_{p,q}^{-1} \\ &\Leftrightarrow \exp({}^tU) = I_{p,q}\exp(-U)I_{p,q}^{-1} \\ &\Leftrightarrow \exp({}^tU) = \exp(-I_{p,q}UI_{p,q}^{-1}) \\ &\Leftrightarrow {}^tU = U = -I_{p,q}UI_{p,q}^{-1} \quad (\exp\colon \mathrm{S}(n,\mathbb{R}) \to \mathrm{S}^{++}(n,\mathbb{R}) \text{ est bijective}) \\ &\Leftrightarrow UI_{p,q} + I_{p,q}U = 0 \\ &\Leftrightarrow \frac{U}{2}I_{p,q} + I_{p,q}\frac{U}{2} = 0 \\ &\Leftrightarrow \frac{{}^tU}{2} = -I_{p,q}\frac{U}{2}I_{p,q}^{-1} \end{aligned}$$

$$\begin{aligned} T \in \mathrm{O}(p,q) &\Leftrightarrow \exp\left(\frac{{}^tU}{2}\right) = \exp\left(-I_{p,q}\frac{U}{2}I_{p,q}^{-1}\right) \\ &\Leftrightarrow {}^t\exp\left(\frac{{}^tU}{2}\right) = I_{p,q}\exp\left(\frac{U}{2}\right)^{-1}I_{p,q}^{-1} \end{aligned}$$

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 $SI_{p,q}{}^tS = I_{p,q}$, *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

$$\mathrm{O}(p,q) \simeq (\mathrm{O}(p,q) \cap \mathrm{O}(n)) \times (\mathrm{O}(p,q) \cap \mathrm{S}^{++}(n,\mathbb{R})).$$

« 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

$$0 = \left(\begin{array}{c|c} A & C \\ \hline B & D \end{array}\right) \in \mathrm{O}(p,q) \Leftrightarrow \begin{cases} {}^tAA - {}^tBB = I_p \\ {}^tAC - {}^tBD = 0 \\ {}^tCA - {}^tDB = 0 \\ {}^tCC - {}^tDD = -I_q \end{cases}$$

En effet

$$\begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix} = \begin{pmatrix} {}^tA & {}^tB \\ {}^tC & {}^tD \end{pmatrix} \begin{pmatrix} I_p & 0 \\ 0 & I_q \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$
$$= \begin{pmatrix} {}^tA & {}^tB \\ {}^tC & {}^tD \end{pmatrix} \begin{pmatrix} A & C \\ -B & -D \end{pmatrix}$$
$$= \begin{pmatrix} {}^tAA - {}^tBB & {}^tAC - {}^tBD \\ {}^tCA - {}^tDB & {}^tCC - {}^tDD \end{pmatrix}$$

D'autre part nous avons

$$O \in \mathrm{O}(n) \iff \begin{cases} {}^tAA + {}^tBB = I_p \\ {}^tAC + {}^tBD = 0 \\ {}^tCA + {}^tDB = 0 \\ {}^tCC + {}^tDD = I_q \end{cases}$$

car

$$\begin{pmatrix} I_p & 0 \\ 0 & I_q \end{pmatrix} = \begin{pmatrix} {}^tA & {}^tB \\ {}^tC & {}^tD \end{pmatrix} \begin{pmatrix} A & C \\ B & D \end{pmatrix}$$
$$= \begin{pmatrix} {}^tAA + {}^tBB & {}^tAC + {}^tBD \\ {}^tCA + {}^tDB & {}^tCC + {}^tDD \end{pmatrix}$$

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

$$\mathrm{O}(p,q) \simeq \mathrm{O}(p) \times \mathrm{O}(q) \times \mathbb{R}^{pq}.$$

□

1.3.7. Un théorème de Burnside. — *Référence :* [**FGN09**, p. 185-186]

Leçons possibles :

104 : *Groupes abéliens et non abéliens finis. Exemples et applications.*

191 : *Exemples d'utilisation des techniques d'algèbre en géométrie.*

Lemme 1.3.27. — *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 1.3.28. — *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 1.3.27 la matrice $D - I_n$ est nilpotente. □

Lemme 1.3.29. — *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 1.3.28). 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 1.3.30. — *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 1.3.29 assure que l'application

$$f \colon \mathrm{G} \to \mathbb{C}^m \qquad A \mapsto (\mathrm{Tr}(AM_i))_{1 \leq i \leq m},$$

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

$$X = \{\mathrm{Tr}(A) \,|\, A \in \mathrm{G}\}$$

Pour conclure il suffit donc de montrer que X est fini. D'après ce qui précède

$$\{\text{valeurs propres de } A \,|\, A \in \mathrm{G}\} \subset \mu_N = \{\text{racines } N\text{ièmes de } 1\}.$$

Il en résulte que X est fini. □

1.3.8. Théorème de Lie-Kolchin. — *Référence :* [**CG17**, Exercice IV-B6]

Leçons possibles :

106 : *Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de* $\mathrm{GL}(E)$. *Applications.*

150 : *Exemples d'actions de groupes sur les espaces de matrices.*

154 : *Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes D'un espace vectoriel de dimension finie. Applications..*

157 : *Endomorphismes trigonalisables. Endomorphismes nilpotents.*

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 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

$$\{\mathrm{id}\}=\mathrm{G}_0\triangleleft\mathrm{G}_1\triangleleft\ldots\triangleleft\mathrm{G}_{n-1}\triangleleft\mathrm{G}_n=\mathrm{G}$$

où pour tout $0\leq i\leq n-1$ le groupe G_i est un sous-groupe normal de G_{i+1} et le groupe quotient ${}^{\mathrm{G}_{i+1}}\!/_{\mathrm{G}_i}$ est abélien.

Théorème 1.3.31 (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 1.3.8. — 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, $0\leq\leq\ell$, 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

  $$X=\{[g,h]\,|\,g,\,h\in\mathrm{G}\}$$

  de $D(\mathrm{G})$ qui est l'image de $\mathrm{G}\times\mathrm{G}$ par le commutateur est également connexe. D'après [**CG17**, II-F5] 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

  $$V=\{v\in\mathbb{C}^n\,|\,\mathrm{A}v\in\mathbb{C}v\}$$

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 $a \in \mathrm{A}$ 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 $g(v)$, $g \in \mathrm{G}$. 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 $D^{\ell-2}(\mathrm{G})$. 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 GL(W) (resp. 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.

1.4. Groupes libres ; groupes définis par générateurs et relations

1.4.1. 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 1.4.1. — Un *monoïde* est un ensemble M
- ◇ qui est muni d'une loi de composition interne associative
- ◇ qui possède un élément neutre (nécessairement unique).

Définition 1.4.2. — Soit M, resp. N, un monoïde de neutre e_M, resp. 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 1.4.1. — L'ensemble $\mathbb{N}$ muni de l'addition est un monoïde. Ce n'est pas un groupe : 1 n'a pas d'inverse.

Exemple 1.4.2. — Un groupe est un monoïde.

Plus précisément un groupe est un monoïde dans lequel tout élément a un inverse.

Exemple 1.4.3. — 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 1.4.1. — 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 1.4.3. — 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 1.4.1. — *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

$$x_1 x_2 \dots x_n \mapsto f(x_1) f(x_2) \dots f(x_n).$$

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 [2]

$$E \to E^{-1} \qquad\qquad x \mapsto x^{-1}.$$

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 $\Lambda(E \sqcup E^{-1})/\mathcal{R}$.

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 1.4.2. — *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 $f(x x^{-1}) = f(x^{-1} x) = e = f(\emptyset)$. Donc $\overline{x x^{-1}} = \overline{x^{-1} x} = \overline{\emptyset}$ et $\overline{x}$ est inversible d'inverse $\overline{x^{-1}}$. □

Lemme 1.4.3 (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*

$$\varphi\colon F(E) \to \mathrm{G}$$

2. Attention E^{-1} et x^{-1} sont de simples notations.

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 1.4.1 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 1.4.4. — 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 1.4.4. — *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 1.4.2. — 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 1.4.4. — 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 1.4.4. — 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

- $\diamond$ xm si m n'est pas de la forme $x^{-1}m'$,
- $\diamond$ 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

- $\diamond$ $x^{-1}m$ si m n'est pas de la forme xm',
- $\diamond$ m' si m est de la forme xm'.

Cette application ensembliste de E dans $\mathcal{S}_X$ induit en vertu de la propriété universelle de $F(E)$ un morphisme de groupes de $F(E)$ vers $\mathcal{S}_X$, 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 1.4.3. — 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 1.4.4. — 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 1.4.5. — L'unique mot sur un alphabet vide est le mot vide, par suite le groupe $F(\emptyset)$ est trivial.

Exemple 1.4.6. — 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 $\mathbb{Z}$.

1.4.2. 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 1.4.5. — 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 $\langle E \,|\, R\rangle$. Si $E = \{x_1, x_2, \dots, x_n\}$, nous écrirons souvent $\langle x_1, x_2, \dots, x_n \,|\, R\rangle$ au lieu de $\langle \{x_1, x_2, \dots, x_n\} \,|\, R\rangle$.

Proposition 1.4.5 (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 1.4.7. —

Tout groupe fini est de présentation finie.

Exemple 1.4.8. —

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 1.4.9. —

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 1.4.10 (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 1.4.11 (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

$$\{a,\, b\} \to \mathbb{Z}^2 \qquad\qquad \begin{cases} a \mapsto (1,0) \\ b \mapsto (0,1) \end{cases}$$

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

$$\mathbb{Z}^2 \to \langle a, b \,|\, aba^{-1}b^{-1}\rangle \qquad\qquad (n,m) \mapsto \overline{a}^n\overline{b}^m$$

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 1.4.5. —

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

$$\{a, b\} \to \mathbb{Z}^2 \qquad\qquad \begin{cases} a \mapsto (1,0) \\ b \mapsto (0,1) \end{cases}$$

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 1.4.6 (Le problème du mot)***.*** —

Soit E un ensemble. Soit R un ensemble de mots sur l'alphabet $E \sqcup E^{-1}$. Le morphisme quotient

$$F(E) \to \langle E \,|\, R\rangle \qquad\qquad m \mapsto m(\overline{x})_x$$

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 1.4.12. — 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 1.4.13. — 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 1.4.14. — 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 1.4.15. — 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 1.4.16. — 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

$$\begin{aligned} \langle A,\, B \,|\, A^2 = B^2 = (AB)^2 \rangle &= \langle A,\, B,\, R,\, S \,|\, R = A,\, S = B,\, A^2 = B^2 = (AB)^2 \rangle \\ &= \langle R,\, S \,|\, R^2 = S^2 = (RS)^2 \rangle \\ &= \langle R,\, S,\, T \,|\, T = RS,\, R^2 = S^2 = T^2 \rangle \\ &= \langle R,\, S,\, T \,|\, R^2 = S^2 = T^2 = RST \rangle. \end{aligned}$$

1.5. Le groupe $\mathrm{SL}(2, \mathbb{Z})$

1.5.1. Générateurs de $\mathrm{SL}(2, \mathbb{Z})$. —

Lemme 1.5.1. — *Les matrices*

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

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 $\beta(M)$ (resp. $\delta(M)$) au lieu de β (resp. 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

$$\beta(AM) = \beta(M) + \delta(M) \qquad \text{et} \qquad \delta(AM) = \delta(M) \tag{1.5.1}$$

et

$$\beta(TM) = \delta(M) \qquad \text{et} \qquad \delta(TM) = -\beta(M). \tag{1.5.2}$$

Les égalités (1.5.1) 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 (1.5.2) 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 1.5.2. — *Les matrices*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \textit{et} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

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

$$S \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \qquad T^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + nc & b + nd \\ c & d \end{pmatrix} \tag{1.5.3}$$

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 (1.5.3) 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.* (1.5.3)). 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 1.5.1. — 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 1.5.1. — 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

$$T^3ST^2ST^4S = \begin{pmatrix} 17 & -5 \\ 7 & -2 \end{pmatrix}.$$

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

$$\begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix} = T^3ST^2ST^4ST^2.$$

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 1.5.3. — *Le groupe* $\mathrm{SL}(2,\mathbb{Z})$ *est engendré par*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \textit{et} \qquad U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

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 1.5.4. — *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 1.5.2). 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 1.5.5. — *L'image de tout morphisme de* $\mathrm{SL}(2,\mathbb{Z})$ *dans* $\mathbb{C}^*$ *est contenue dans le groupe des racines* 12*ième de l'unité.*

Démonstration. — Le Corollaire 1.5.4 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 1.5.2. — 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.

1.5.2. Générateurs de $\mathrm{PSL}(2,\mathbb{Z})$. — 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

$$\left\{\mathbb{C}\to\mathbb{C},\ z\mapsto \frac{az+b}{cz+d}\,\middle|\, a,\ b,\ c,\ d\in\mathbb{Z},\ ad-bc=1\right\}.$$

Lemme 1.5.6. — *Le groupe* $\mathrm{PSL}(2,\mathbb{Z})$ *est engendré par* $\overline{S}$ *et* $\overline{ST}$ *où*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \textit{et} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

sont les matrices introduites au Théorème 1.5.2.

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

$$y^{i_0}xy^{i_1}x\dots y^{i_{n-1}}xy^{i_n} \tag{1.5.4}$$

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 1.5.2. — Nous verrons que l'écriture (1.5.4) est unique au §1.5.3, autrement dit x et y engendrent librement [3] $\mathrm{PSL}(2,\mathbb{Z})$:

$$\mathrm{PSL}(2,\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z}$$

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 $y^3 = 1$.

1.5.3. 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

$$\begin{cases} \sigma_i\sigma_j = \sigma_j\sigma_i \text{ pour tout } 1 \leq i,\, j \leq n-1 \text{ et } |i-j| \geq 2 \\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ pour tout } 1 \leq i \leq n-2 \end{cases}$$

Par définition $B_1 = \{\mathrm{id}\}$ et B_2 est le groupe cyclique infini $\langle\sigma_1\rangle$.

Considérons les trois groupes de présentation

$$\langle a,\, b \,|\, aba = bab,\, (aba)^4 = 1\rangle \tag{1.5.5}$$

$$\langle s,\, t \,|\, s^3 = t^2,\, t^4 = 1\rangle \tag{1.5.6}$$

$$\langle s,\, t \,|\, s^3 = t^2 = 1\rangle \tag{1.5.7}$$

Lemme 1.5.7. — *Les présentations* (1.5.5) *et* (1.5.6) *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 $(\sigma_1\sigma_2\sigma_1)^4$.*

Démonstration. — Montrons comment passer de (1.5.5) à (1.5.6). 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 (1.5.5) et (1.5.6) définissent des groupes isomorphes.

---

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 $f \circ j = h$.

En remplaçant a par σ_1 et b par σ_2 dans (1.5.5) 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 1.5.3. — $(\sigma_1\sigma_2\sigma_1)^4 = \big((\sigma_1\sigma_2\sigma_1)^2\big)^2$ et $(\sigma_1\sigma_2\sigma_1)^2$ engendre le centre de B_3 (*voir* [**KT08**, Theorem 1.24]).

Remarque 1.5.4. — On déduit de (1.5.6) une troisième présentation de G :

$$\mathrm{G} = \langle u,\, v \,|\, u^2 = (uv)^3,\, u^4 = 1\rangle.$$

Lemme 1.5.8. — *Le groupe* H *défini par* (1.5.7) *est isomorphe au quotient de* B_3 *par son centre.*

Démonstration. — À partir des présentations (1.5.6) et (1.5.7) 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 1.5.1) 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 1.5.9. — *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 1.5.10. — *Le morphisme $f\colon \mathrm{G} \to \mathrm{SL}(2,\mathbb{Z})$ est injectif (resp. surjectif) si et seulement si $\overline{f}$ est injectif (resp. 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 1.5.9. — D'après le Lemme 1.5.10 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 1.5.1 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

$$\langle s,\, t \,|\, s^3 = t^2 = 1\rangle$$

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 $\overline{A}$ (resp. $\overline{B}$) désigne l'image de A (resp. 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 $\mathrm{PSL}(2,\mathbb{Z})$:

Théorème 1.5.11 ([**Alp93**])**.** — *Nous avons*

$$\mathrm{PSL}(2,\mathbb{Z}) = \mathbb{Z}\!\diagup_{2\mathbb{Z}} * \mathbb{Z}\!\diagup_{3\mathbb{Z}}$$

Donnons une caractérisation des produits libres, nous renvoyons à [**LS01**] pour une démonstration :

Proposition 1.5.12 ([**LS01**])**.** — *Soit* G *un groupe. Soient* H *et* K *deux sous-groupes de* G*. Le groupe* G *est le produit libre* $\mathrm{H} * \mathrm{K}$ *de* H *et* K *si et seulement si*

- ◇ H *et* K *engendrent* G *;*
- ◇ *si* w *s'écrit*

$$h_1k_1h_2k_2\dots h_nk_n$$

avec $h_1 \in \mathrm{H}$*,* $h_i \in \mathrm{H} \smallsetminus \{e\}$ *pour tout* $2 \leq i \leq n$*,* $k_j \in \mathrm{K} \smallsetminus \{e\}$ *pour tout* $1 \leq j \leq n-1$ *et* $k_n \in \mathrm{K}$*, alors* w *n'est pas trivial.*

Démonstration du Théorème 1.5.11. — Le groupe $\mathrm{SL}(2,\mathbb{Z})$ est engendré par (Théorème 1.5.2)

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

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 $w = (\overline{TS})\dots\overline{S}$, alors $w(\mathcal{P}) \subset \overline{TS}(\mathcal{N})$ est un ensemble d'irrationnels positifs minorés par 1.

— Si $w = (\overline{TS})^{-1}\dots\overline{S}$, 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 $w \neq \mathrm{id}$.

Le Lemme 1.5.12 permet de conclure. □

1.5.4. Sous-groupes libres de $\mathrm{SL}(2,\mathbb{Z})$**.** — Rappelons l'énoncé suivant appelé Lemme du Ping Pong :

Lemme 1.5.13. — *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*

$$\begin{cases} X_2 \not\subset X_1 & \\ \gamma(X_2) \subset X_1 & \forall\, \gamma \in \Gamma_1 \smallsetminus \{e\} \\ \gamma(X_1) \subset X_2 & \forall\, \gamma \in \Gamma_2 \smallsetminus \{e\} \end{cases}$$

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.

◇ 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.

□

Proposition 1.5.14. — *Les deux matrices*

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad \textit{et} \qquad \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

engendrent un sous-groupe de $\mathrm{SL}(2,\mathbb{Z})$ *qui est libre de rang* 2.

Remarque 1.5.5. — 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

$$\Gamma_1 = \left\{ \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \,|\, n \in \mathbb{Z} \right\}$$

et

$$\Gamma_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \,|\, n \in \mathbb{Z} \right\}.$$

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

$$X_1 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \,|\, |x| > |y| \right\}$$

et

$$X_2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \,|\, |x| < |y| \right\}$$

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 permet de conclure. □

1.5.5. 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 1.5.15. — *Le groupe*

$$\Gamma(2) = \left\{ M \in \mathrm{SL}(2, \mathbb{Z}) \,|\, M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ mod\ 2 \right\}$$

est engendré par les matrices

$$-\mathrm{id} \qquad T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad \textit{et} \qquad U^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

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 1.5.2. 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 1.5.16. — *Le morphisme de réduction*

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}\Big(2, \mathbb{Z}\big/_{n\mathbb{Z}}\Big)$$

est surjectif.

Démonstration. — Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de $\mathrm{SL}\Big(2, \mathbb{Z}\big/_{n\mathbb{Z}}\Big)$. Le théorème des restes chinois assure l'existence de b' tel que

- $\diamond$ $b \equiv b' \bmod n$,
- $\diamond$ 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 1.5.3. — 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

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}\Big(2, \mathbb{Z}\big/_{21\mathbb{Z}}\Big).$$

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 1.5.17. — *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 1.5.18. — *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 1.5.3 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 1.5.19. — *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 1.5.15 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

$$\mathrm{SL}(2,\mathbb{Z})/\Gamma(2) \simeq \mathrm{SL}\Big(2, \mathbb{Z}/2\mathbb{Z}\Big).$$

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 $\mathrm{SL}\Big(2, \mathbb{Z}/2\mathbb{Z}\Big)$ est $\frac{6}{3} = 2$. □

Remarque 1.5.6. — 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 1.5.1. — 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 1.5.4. — La démonstration du Corollaire 1.5.19 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

$$\mathrm{SL}(2,\mathbb{Z})/\Gamma(2) \simeq \mathrm{SL}\Big(2, \mathbb{Z}/2\mathbb{Z}\Big)$$

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 1.5.20. — *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

$$\mathrm{SL}(2,\mathbb{Z}) \longrightarrow \mathrm{SL}\Big(2, \mathbb{Z}/2\mathbb{Z}\Big) = \mathrm{GL}\Big(2, \mathbb{Z}/2\mathbb{Z}\Big) \simeq \mathcal{S}_3 \longrightarrow \{\pm 1\};$$

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 1.5.7. — 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 1.5.2. — 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

$$\mathrm{SL}(k,\mathbb{Z}) \to \mathrm{SL}\Big(k, {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\Big)$$

(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).

1.5.6. 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.
- ◇ $\mathcal{S}_3 \supset \mathcal{A}_3 \supset \{e\}$ 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 1.5.21 ([**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 1.5.22. — *Soit* $k \geq 6$*. Pour tout* $n \geq 2$ *le groupe alterné* $\mathcal{A}_k$ *n'est pas un quotient de* $\mathrm{SL}\Big(2, \mathbb{Z}\big/_{n\mathbb{Z}}\Big)$.

Remarque 1.5.8. — La borne $n \geq 6$ est optimale ; en effet

- ◇ $\mathcal{A}_3$ est isomorphe au quotient de $\mathrm{SL}\Big(2, \mathbb{Z}\big/_{3\mathbb{Z}}\Big)$ par son 2-Sylow distingué ;
- ◇ $\mathcal{A}_4$ et $\mathrm{PSL}\Big(2, \mathbb{Z}\big/_{3\mathbb{Z}}\Big)$ sont isomorphes (Théorème 1.3.22) ;
- ◇ $\mathcal{A}_5$ et $\mathrm{PSL}\Big(2, \mathbb{Z}\big/_{5\mathbb{Z}}\Big)$ sont isomorphes (Théorème 1.3.22).

Démonstration. — Écrivons n sous la forme $n = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$, les p_i désignant des nombres premiers. Le théorème des restes chinois assure que

$$\mathbb{Z}\big/_{n\mathbb{Z}} \simeq \prod_{i=1}^{m} \mathbb{Z}\big/_{p_i^{r_i}\mathbb{Z}}.$$

Alors

$$\mathrm{SL}\Big(2, \mathbb{Z}\big/_{n\mathbb{Z}}\Big) \simeq \prod_{i=1}^{m} \mathrm{SL}\Big(2, \mathbb{Z}\big/_{p_i^{r_i}\mathbb{Z}}\Big).$$

Le Lemme 1.5.21 assure qu'il suffit de montrer que $\mathcal{A}_k$, $k \geq 6$,n'est pas un facteur de composition de $\mathrm{SL}\Big(2, \mathbb{Z}\big/_{p^r\mathbb{Z}}\Big)$ pour tout p premier.

Considérons le morphisme de réduction

$$\mathrm{SL}\Big(2, \mathbb{Z}\big/p^r\mathbb{Z}\Big) \to \mathrm{SL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)$$

qui est surjectif. Désignons par K son noyau. Nous avons la suite de composition suivante

$$\{\mathrm{id} \bmod p^r\} \lhd \mathrm{K} \lhd \mathrm{SL}\Big(2, \mathbb{Z}\big/p^r\mathbb{Z}\Big)$$

dont les facteurs sont modulo isomorphisme K et $\mathrm{SL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)$. Il en résulte que les facteurs de composition de $\mathrm{SL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)$ s'obtiennent à partir des facteurs de composition de K et de $\mathrm{SL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)$.

Déterminons les facteurs de composition de K. Le groupe

$$\mathrm{K} = \Big\{M \in \mathrm{SL}\Big(2, \mathbb{Z}\big/p^r\mathbb{Z}\Big) \mid M \equiv \mathrm{id} \bmod p\Big\}$$

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 $\mathrm{SL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)$.

— Supposons $p \geq 5$; le groupe $\mathrm{PSL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big) = \mathrm{SL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)\Big/\{\pm \mathrm{id}\}$ est simple pour $p \geq 5$ donc

$$\{\mathrm{id}\} \lhd \{\pm \mathrm{id}\} \lhd \mathrm{SL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)$$

est une suite de composition de $\mathrm{SL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)$ et les facteurs de composition de $\mathrm{SL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)$ sont $\mathbb{Z}\big/2\mathbb{Z}$ et $\mathrm{PSL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)$.

— Supposons maintenant $p < 5$. Comme

$$\mathrm{SL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big) = \mathrm{GL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big) \simeq \mathcal{S}_3 \qquad \text{et} \qquad \mathrm{SL}\Big(2, \mathbb{Z}\big/3\mathbb{Z}\Big)\Big/\{\pm \mathrm{id}\} \simeq \mathcal{A}_4$$

les facteurs de composition de $\mathrm{SL}\Big(2, \mathbb{Z}\big/2\mathbb{Z}\Big)$ et $\mathrm{SL}\Big(2, \mathbb{Z}\big/3\mathbb{Z}\Big)$ sont cycliques d'ordre 2 ou 3.

Finalement si $p \leq 3$, tout facteur de composition de $\mathrm{SL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)$ est cyclique et pour tout premier $p \geq 5$ le groupe $\mathrm{SL}\Big(2, \mathbb{Z}\big/p^r\mathbb{Z}\Big)$ a un unique facteur de composition non abélien : $\mathrm{PSL}\Big(2, \mathbb{Z}\big/p\mathbb{Z}\Big)$. Ainsi si $\mathcal{A}_k$, $k \geq 6$, était un facteur de composition de $\mathrm{SL}\Big(2, \mathbb{Z}\big/p^r\mathbb{Z}\Big)$, alors $\mathcal{A}_k$

5. Notons que l'ordre de K peut être calculé mais que nous n'en avons pas besoin.

serait isomorphe à un $\mathrm{PSL}\left(2, \mathbb{Z}/p\mathbb{Z}\right)$ pour un certain $p \geq 5$. Or $|\mathrm{PSL}\left(2, \mathbb{Z}/p\mathbb{Z}\right)| = \frac{(p^2-1)p}{2}$ et $|\mathcal{A}_k| = \frac{k!}{2}$ donc on se ramène à la question suivante : quand a-t-on

$$k! = (p-1)p(p+1) \tag{1.5.8}$$

Si $k < p$, alors $k!$ n'est pas divisble par p donc (1.5.8) n'a pas de solution si $k < p$.

Si $k = p$, alors (1.5.8) 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 (1.5.8) 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 (1.5.8) n'a pas de solution.

Finalement (1.5.8) a une seule solution : $p = k = 5$ (en effet $\mathrm{PSL}(2, \mathbb{F}_5) \simeq \mathcal{A}_5$, Théorème 1.3.22) et dès que $k \geq 6$ le groupe alterné $\mathcal{A}_k$ n'est pas un quotient de $\mathrm{SL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$ et ce pour tout $n \geq 2$. □

Alors que le Théorème 1.5.22 assure que la plupart des $\mathcal{A}_n$ ne sont pas des quotients de $\mathrm{SL}\left(2, \mathbb{Z}/n\mathbb{Z}\right)$ l'énoncé suivant assure que la plupart des $\mathcal{A}_n$ sont des quotients de $\mathrm{SL}(2, \mathbb{Z})$:

Théorème 1.5.23. — *Dès que $n \geq 9$ le groupe alterné $\mathcal{A}_n$ est un quotient de* $\mathrm{SL}(2, \mathbb{Z})$.

Exemple 1.5.5. — 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 1.5.24. — *Dès que $n \geq 9$ il existe un morphisme surjectif de* $\mathrm{PSL}(2, \mathbb{Z})$ *dans le groupe alterné $\mathcal{A}_n$.*

Lemme 1.5.25 ([**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 1.5.24. — Elle découle du Lemme 1.5.25 et du Théorème 1.5.9. □

Démonstration du Théorème 1.5.23. — On compose la projection canonique

$$\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{PSL}(2, \mathbb{Z})$$

avec le morphisme de la Proposition 1.5.24. □

1.6. Produits directs et semi-directs

Soient G, H et N trois groupes. Soient $i\colon \mathrm{N} \to \mathrm{G}$ et $p\colon \mathrm{G} \to \mathrm{H}$ deux morphismes de groupes. Si

- $\diamond$ i est injectif,
- $\diamond$ p est surjectif,
- $\diamond$ $\operatorname{im} i = \ker p$,

on parle de *suite exacte* et on note

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1.$$

Exemple 1.6.1. — Le groupe symétrique $\mathcal{S}_3$ compte six éléments

$$\mathrm{id}, \qquad (1\ 2), \qquad (1\ 3), \qquad (2\ 3), \qquad \sigma = (1\ 2\ 3), \qquad \sigma^2 = \sigma^{-1} = (1\ 3\ 2).$$

Il contient un sous-groupe distingué d'ordre 3

$$\langle \sigma \rangle = \{1, \sigma, \sigma^2\} = \mathcal{A}_3$$

isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et on a la suite exacte suivante

$$1 \longrightarrow \mathcal{A}_3 \simeq \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathcal{S}_3 \xrightarrow{\mathrm{sgn}} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1.$$

Soient G un groupe, $\mathrm{N} \triangleleft \mathrm{G}$ un sous-groupe distingué et G/N le groupe quotient. Connaissant N et G/N nous cherchons à reconstituer G. Plus généralement étant donnés deux groupes N et H nous cherchons tous les groupes G tels qu'on ait une suite exacte

$$1 \longrightarrow \mathrm{N} \longrightarrow \mathrm{G} \longrightarrow \mathrm{H} \longrightarrow 1.$$

Un tel groupe G est une *extension* de N par H. Le problème général est délicat et nous en étudions deux cas particuliers : les produits directs et les produits semi-directs.

1.6.1. Produits directs. — 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 :

$$(n, h)(n', h') = (nn', hh').$$

On a alors une projection $p\colon \mathrm{G} \to \mathrm{H}$ définie par $p(n, h) = h$. C'est un morphisme de groupes surjectif de noyau le sous-groupe distingué

$$\overline{\mathrm{N}} = \{(n, 1) \mid n \in \mathrm{N}\}.$$

Considérons $i\colon \mathrm{N} \to \mathrm{N} \times \mathrm{H}$, $n \mapsto (n, 1)$. On a la suite exacte

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{N} \times \mathrm{H} \xrightarrow{p} \mathrm{H} \longrightarrow 1.$$

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

- $\diamond$ 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 $\mathrm{N} \times \mathrm{H}$.

Un exemple classique de produit direct est donné par le lemme chinois :

Lemme 1.6.1 (Lemme chinois)**.** — *Si p et q sont premiers entre eux, alors*

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Démonstration. — Soit $[n]_{pq}$, resp. $[n]_p$, resp. $[n]_q$ la classe de n modulo pq, resp. p, resp. q. Considérons le morphisme

$$\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \qquad [n]_{pq} \mapsto ([n]_p, [n]_q)$$

Il est injectif car $\mathrm{pgcd}(p, q) = 1$.

L'égalité $\left|\mathbb{Z}/pq\mathbb{Z}\right| = \left|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}\right|$ permet de conclure. □

1.6.2. Produits semi-directs. — Le produit semi-direct est une variante affaiblie du produit direct.

Soient G un groupe et N un sous-groupe distingué de G. Si i est l'inclusion on a une suite exacte

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{G}/\mathrm{N} \longrightarrow 1.$$

Supposons que comme dans le cas du produit direct, il existe un sous-groupe H de G tel que $p_{|\mathrm{H}}$ induise un isomorphisme de H sur G/N. Contrairement au cas du produit direct H n'est pas distingué a priori. Par conséquent

◇ $\mathrm{N} \cap \mathrm{H} = \{e\}$;

◇ $\mathrm{G} = \mathrm{NH} = \{nh \,|\, n \in \mathrm{N},\, h \in \mathrm{H}\}$.

Nous avons les deux propriétés suivantes :

◇ comme dans le cas du produit direct G est en bijection avec le produit ensembliste $\mathrm{N} \times \mathrm{H}$;

◇ la multiplication n'est pas celle du produit direct, elle est "tordue" au moyen de l'opération de H sur N par conjugaison $h \cdot n = hnh^{-1}$; on a

$$(n, h)(n', h') = (n(h \cdot n'), hh').$$

Cette opération de H sur N n'est pas seulement ensembliste, le groupe H opère sur N par automorphismes de groupes.

En effet

◇ si $g \in \mathrm{G}$ et si $\overline{g} = p(g)$, il existe $h \in \mathrm{H}$ tel que $p(h) = \overline{g}$ donc gh^{-1} appartient à N. L'écriture de g sous la forme nh est unique (en effet supposons que $nh = n'h'$, soit que $n'^{-1}n = h'h^{-1}$; puisque $\mathrm{N} \cap \mathrm{H} = \{e\}$ on a $n'^{-1}n = h'h^{-1} = e$, *i.e.* $(n, h) = (n', h')$) de sorte que G est en bijection avec NH.

◇ Si on calcule le produit de deux éléments de G, alors

$$(nh)(n'h') = nhn'h' = n\underbrace{hn'h^{-1}}_{h\cdot n'}hh'$$

avec $hn'h^{-1}$ appartient à N car N est distingué dans G.

On définit donc le produit semi-direct comme suit.

Proposition-Définition 1.6.2. — ◇ *Soient* N *et* H *deux groupes. Soit* $\mathrm{Aut}(\mathrm{N})$ *le groupe des automorphismes de groupe de* N. *Soit* $\varphi\colon \mathrm{H} \to \mathrm{Aut}(\mathrm{N})$ *un morphisme qui définit une opération de* H *sur* N *par la formule* $h \cdot n = \varphi(h)(n)$.

On définit sur l'ensemble produit $\mathrm{N} \times \mathrm{H}$ *une loi par*

$$(n,h)(n',h') = \big(n(h \cdot n'), hh'\big).$$

Alors $\mathrm{N} \times \mathrm{H}$, *muni de cette loi, est un groupe appelé produit semi-direct de* N *par* H *relativement à* φ *et noté* $\mathrm{N} \rtimes_\varphi \mathrm{H}$ *ou plus simplement* $\mathrm{N} \rtimes \mathrm{H}$.

◇ *On a la suite exacte*

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{N} \rtimes \mathrm{H} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

où $i\colon n \mapsto (n,1)$ *et* $p\colon (n,h) \mapsto h$, *de sorte que* $\mathrm{N} \rtimes \mathrm{H}$ *est une extension de* N *par* H.

Remarques 1.6.1. — ◇ Le groupe $\mathrm{N} \rtimes \mathrm{H}$ contient deux sous-groupes isomorphes respectivement à N et H

$$\overline{\mathrm{N}} = \big\{(n,1) \,|\, n \in \mathrm{N}\big\}, \qquad \overline{\mathrm{H}} = \big\{(1,h) \,|\, h \in \mathrm{H}\big\}.$$

◇ Nous avons $\overline{\mathrm{N}} \cap \overline{\mathrm{H}} = \{e\}$ et $\mathrm{N} \rtimes \mathrm{H} = \overline{\mathrm{N}}\,\overline{\mathrm{H}}$ car $(n,1)(1,h) = (n,h)$.

◇ Si φ n'est pas trivial, alors le groupe obtenu n'est pas abélien ($(1,h)(n,1) = (h \cdot n, h)$ est en général distinct de (n,h)).

◇ Si nous identifions N et H à $\overline{\mathrm{N}}$ et $\overline{\mathrm{H}}$, alors $\varphi\colon h \mapsto h \cdot n = \varphi(h)(n)\colon n \mapsto hnh^{-1}$.

Donnons des conditions permettant d'assurer que G est un produit.

Proposition 1.6.3. — a) *Si on a une suite exacte*

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

et s'il existe un relèvement $\overline{\mathrm{H}}$ *de* H, *c'est-à-dire un sous-groupe* $\overline{\mathrm{H}}$ *de* G *tel que la restriction de la projection* p *à* $\overline{\mathrm{H}}$ *soit un isomorphisme de* $\overline{\mathrm{H}}$ *sur* H, *le groupe* G *est isomorphe à un produit semi-direct* $\mathrm{N} \rtimes \mathrm{H}$. *Cela revient à dire que* p *possède une section, i.e. qu'il existe un morphisme* $s\colon \mathrm{H} \to \mathrm{G}$ *tel que* $p \circ s = \mathrm{id}_\mathrm{H}$. *L'extension est alors dite scindée.*

b) *Soit* G *un groupe. Soient* N *et* H *deux sous-groupes de* G *tels que*

◇ $\mathrm{N} \lhd \mathrm{G}$,

◇ $\mathrm{N} \cap \mathrm{H} = \{e\}$,

◇ $\mathrm{G} = \mathrm{NH}$.

Alors $\mathrm{G} \simeq \mathrm{N} \rtimes \mathrm{H}$.

On peut caractériser les produits directs parmi les produits semi-directs :

Proposition 1.6.4. — *Soient* N *et* H *deux groupes. Soit* $\mathrm{Aut}(\mathrm{N})$ *le groupe des automorphismes de groupe de* N. *Soit* $\varphi\colon \mathrm{H} \to \mathrm{Aut}(\mathrm{N})$ *un morphisme qui définit une opération de* H *sur* N *par la formule* $h \cdot n = \varphi(h)(n)$.

Soit $\mathrm{G} = \mathrm{N} \rtimes_\varphi \mathrm{H}$. *Soit* $\overline{\mathrm{H}}$ *le sous-groupe des éléments* $(1,h)$.

Les propriétés suivantes sont équivalentes :
— *φ est trivial (i.e. nous avons $\varphi(h) = \mathrm{id}_N$ pour tout $h \in H$) ;*
— *le sous-groupe $\overline{H}$ est distingué dans G ;*
— *la loi de groupe sur G est celle du produit direct.*
(C'est le cas en particulier si l'extension est centrale, i.e. si $N \subset Z(G)$).

Remarques 1.6.2. —
◇ Soient N et H deux groupes. Soient $\varphi\colon H \to \mathrm{Aut}(N)$ et $\psi\colon H \to \mathrm{Aut}(N)$ deux morphismes. S'il existe $u \in \mathrm{Aut}(N)$ tel que $\psi(h) = u \circ \varphi(h) \circ u^{-1}$ ("actions conjuguées") alors $N \rtimes_\varphi H \simeq N \rtimes_\psi H$.
◇ Soient N et H deux groupes. Soient $\varphi\colon H \to \mathrm{Aut}(N)$ et $\psi\colon H \to \mathrm{Aut}(N)$ deux morphismes. S'il existe $\alpha \in \mathrm{Aut}(H)$ tel que $\varphi = \psi \circ \alpha$, alors $N \rtimes_\varphi H \simeq N \rtimes_\psi H$ (envoyer $nh \in N \rtimes_\varphi H$ sur $n\alpha(h) \in N \rtimes_\psi H$).

Exemple 1.6.2 (Le groupe linéaire)***.*** — Soit $\Bbbk$ un corps. Soit $n \in \mathbb{N}^*$. La suite exacte

$$1 \longrightarrow \mathrm{SL}(n,\Bbbk) \longrightarrow \mathrm{GL}(n,\Bbbk) \xrightarrow{\det} \Bbbk^* \longrightarrow 1$$

est scindée (envoyer $\lambda \in \Bbbk^*$ sur la matrice $\mathrm{diag}(\lambda, 1, 1, \ldots, 1)$). Par conséquent $\mathrm{GL}(n,\Bbbk) \simeq \mathrm{SL}(n,\Bbbk) \rtimes \Bbbk^*$.

Exemple 1.6.3 (Le groupe affine)***.*** — Soit L le groupe affine de $\mathbb{R}$ constitué des applications de la forme $x \mapsto ax + b$ avec $a \neq 0$. Soit H le groupe des translations $x \mapsto x + b$, isomorphe à $\mathbb{R}$, et soit K le sous-groupe des homothéties de centre 0

$$K = \{x \mapsto ax \,|\, a \in \mathbb{R}^*\}$$

isomorphe à $\mathbb{R}^*$. Le groupe affine est donc isomorphe au produit semi-direct $\mathbb{R} \rtimes \mathbb{R}^*$ dans lequel le produit s'écrit

$$(b, a)(b', a') = (b + ab', aa').$$

En effet tout élément $f\colon x \mapsto ax + b$ de L s'écrit $g \circ h$ où g désigne l'élément de H donné par $x \mapsto x+b$ et h désigne l'élément de K donné par $x \mapsto ax$. Considérons maintenant $f\colon x \mapsto ax+b$ et $g\colon x \mapsto a'x + b'$ dans L, alors

$$f \circ g(x) = f(g(x)) = f(a'x + b') = a(a'x + b') + b = aa'x + (ab' + b).$$

Exemple 1.6.4 (Le groupe symétrique)***.*** — Nous avons la suite exacte suivante définie par la signature

$$1 \longrightarrow \mathcal{A}_n \longrightarrow \mathcal{S}_n \xrightarrow{\mathrm{sgn}} \{-1, 1\} \to 1.$$

Si τ est une transposition, nous avons une section s de sgn en posant $s(1) = \mathrm{id}$ et $s(-1) = \tau$. La Proposition 1.6.3 assure que

$$\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \{-1, 1\} \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z}$$

et le produit n'est pas direct.

Exemple 1.6.5 (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 $(\mathbb{Z}/2\mathbb{Z})^3$ qui sont les seuls possibles.

Exemple 1.6.6 (Le groupe diédral, v1)**.** — 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 ρ d'angle $\frac{2\pi}{n}$ et la symétrie σ autour de l'axe des abscisses dans $\mathbb{R}^2$. Autrement dit il s'agit du groupe engendré par les matrices

$$\rho = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix} \qquad \sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Puisque ρ et σ laissent invariant l'ensemble des sommets du polyèdre régulier à n côtés, noté P_n, le groupe D_{2n} laisse invariant ce polyèdre régulier.

La rotation ρ engendre le groupe des rotations d'angle $\frac{2k\pi}{n}$ avec $0 \leq k \leq n-1$ et donc $\langle\rho\rangle \simeq \mathbb{Z}/n\mathbb{Z}$. De plus $\sigma^2 = \mathrm{id}$ ainsi $\langle\sigma\rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

Un calcul montre que

$$\sigma\rho\sigma^{-1} = \sigma\rho\sigma = \rho^{-1}$$

et par récurrence nous obtenons

$$\sigma\rho^k\sigma^{-1} = \rho^{-k}.$$

Par suite tous les éléments de $\langle\rho,\, \sigma\rangle$ sont de la forme ρ^k ou $\rho^k\sigma$. Par conséquent

$$\mathrm{D}_{2n} = \{\rho^k,\, \rho^k\sigma \,|\, 0 \leq k \leq n-1\}.$$

ce groupe se décompose en produit semi-direct

$$\mathrm{D}_{2n} \simeq \langle\rho\rangle \rtimes \langle\sigma\rangle.$$

En effet

— $\langle\rho\rangle \cap \langle\sigma\rangle = \{\mathrm{id}\}$,

— tout élément de D_{2n} est le produit d'un élément de $\langle\rho\rangle$ par un élément de $\langle\sigma\rangle$

— comme $\sigma\rho^k\sigma^{-1} = \rho^{-k}$ le sous-groupe $\langle\rho\rangle$ 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

$$\varphi(0) = \mathrm{id} \qquad \varphi(1)(m) = -m$$

est un morphisme de groupes et la description précédente montre que

$$\mathrm{D}_{2n} \simeq \mathbb{Z}/2\mathbb{Z} \ltimes_\varphi \mathbb{Z}/n\mathbb{Z}.$$

Exemple 1.6.7 (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 $\tau = \tau_1$ et notons σ la symétrie en 0, c'est-à-dire $\sigma(m) = -m$. Le *groupe diédral infini* D_∞ est le sous-groupe $\langle \tau, \sigma \rangle$ des bijections de $\mathbb{Z}$ dans lui-même.

Remarquons que $\sigma^2 = \mathrm{id}$ et $\sigma\tau_m\sigma = \tau_{-m}$. Comme pour le groupe diédral nous pouvons montrer que

$$\mathrm{D}_\infty \simeq \langle \tau \rangle \rtimes \langle \sigma \rangle.$$

En identifiant $\langle \tau \rangle$ à $(\mathbb{Z}, +)$ via l'isomorphisme $n \mapsto \tau_n = \tau^n$ et $\langle \sigma \rangle$ à $\mathbb{Z}/2\mathbb{Z}$ via $i \mapsto \sigma^i$ nous obtenons la décomposition en produit semi-direct

$$\mathrm{D}_\infty \simeq \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

Exemple 1.6.8. — 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 $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.

1.7. Théorèmes de Sylow

Référence : [**Per82**, p. 18-20]

Leçons possibles :

101 *: Groupe opérant sur un ensemble. Exemples et applications.*

104 *: Groupes abéliens et non abéliens finis. Exemples et applications.*

103 *: Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.*

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 de cardinal 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 sous-groupe de cardinal 12 qui ne contient pas de sous-groupe d'ordre 6. 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.

Définition 1.7.1. — Un groupe G est un *p-groupe* si tout élément de G a pour ordre une puissance de p.

Exemples 1.7.1. — 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 1.7.2. — 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.

Exemple 1.7.2. — 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 fini de cardinal

$$|\mathrm{G}| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1});$$

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

$$|\mathrm{P}| = p \times p^2 \times \ldots \times p^{n-1} = p^{n(n-1)/2}.$$

L'énoncé suivant atteste l'existence des sous-groupes de Sylow :

Théorème 1.7.1 (Premier théorème de Sylow)***.*** — *Soit* G *un groupe fini. Soit p un nombre premier tel que p divise $|\mathrm{G}|$. Écrivons $|\mathrm{G}| = p^\alpha m$ où $\alpha \geq 1$ et m est premier avec p.*

Il existe au moins un p-Sylow dans G*, c'est-à-dire un sous-groupe d'ordre p^α.*

Remarque 1.7.1. — Notons que nous n'avons pas supposé $\alpha \geq 1$; si $\alpha = 0$, c'est-à-dire si p ne divise pas $|\mathrm{G}|$, le groupe G admet un unique p-Sylow, à savoir $\{e\}$.

Avant de démontrer ce résultat donnons un lemme qui permet, connaissant un Sylow d'un groupe G d'en trouver un pour un sous-groupe H :

Lemme 1.7.2. — *Soit* G *un groupe fini. Soit p un nombre premier tel que p divise $|\mathrm{G}|$. Écrivons $|\mathrm{G}| = p^\alpha m$ où $\alpha \geq 1$ et m est premier avec p.*

Soient H *un sous-groupe de* G *et soit* S *un p-Sylow de* G*. Alors il existe $a \in \mathrm{G}$ tel que $a\mathrm{S}a^{-1} \cap \mathrm{H}$ soit un p-Sylow de* H*.*

Démonstration. — Notons G/S l'ensemble des classes à gauche modulo S (*i.e.* l'ensemble des parties $a\mathrm{S}$ pour $a \in \mathrm{G}$). Le groupe G opère sur G/S par translation à gauche (en posant $g \cdot (a\mathrm{S}) = (ga)\mathrm{S}$). Le stabilisateur

$$\mathrm{Stab}(a\mathrm{S}) = \{g \in \mathrm{G} \,|\, g \cdot a\mathrm{S} = a\mathrm{S}\}$$

de aS 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 aS.

Montrons qu'un de ces groupes est un Sylow de H. Ce sont déjà des p-groupes. Il suffit donc que pour un $a \in \mathrm{G}$, $\left|{}^{\mathrm{H}}\!/_{(a\mathrm{S}a^{-1} \cap \mathrm{H})}\right|$ soit premier à p.

Rappelons que l'application

$$ {}^{\mathrm{G}}\!/_{\mathrm{Stab}(x)} \to \mathcal{O}(x) \qquad\qquad \overline{g} \mapsto g \cdot x $$

de l'ensemble des classes à gauche dans l'orbite de x est bien définie et est une bijection.

Ainsi $\left|{}^{\mathrm{H}}\!/_{(a\mathrm{S}a^{-1} \cap \mathrm{H})}\right| = |\mathcal{O}(a\mathrm{S})|$ où $|\mathcal{O}(a\mathrm{S})|$ désigne le cardinal de l'orbite de aS dans ${}^{\mathrm{G}}\!/_{\mathrm{S}}$ 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 ${}^{\mathrm{G}}\!/_{\mathrm{S}}$ est réunion des orbites $\mathcal{O}(a\mathrm{S})$: contradiction avec le fait que S est un p-Sylow de G. □

Démonstration du Théorème 1.7.1. — Soit G un groupe d'ordre fini n. Soit p un diviseur de n. On plonge G dans $\mathcal{S}_n$ (théorème de Cayley). Puis on plonge $\mathcal{S}_n$ dans $\mathrm{GL}(n, \mathbb{F}_p)$: l'élément σ de $\mathcal{S}_n$ 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 1.7.2), donc G aussi par le Lemme 1.7.2. □

Le deuxième théorème de Sylow étudie la conjugaison des p-sous-groupes de Sylow.

Théorème 1.7.3 (Second et troisième théorèmes de Sylow)**.** — *Soit* G *un groupe fini. Soit p un nombre premier tel que p divise $|\mathrm{G}|$. Écrivons $|\mathrm{G}| = p^\alpha m$ où $\alpha \geq 1$ et m est premier avec p.*

Soit n_p le nombre de p-Sylow de G*.*

- ◇ *Si* H *est un p-Sylow de* G *et* K *est un p-sous-groupe de* G*, alors* K *est contenu dans un conjugué de* H *: il existe $g \in \mathrm{G}$ tel que* K *est un sous-groupe de $g\mathrm{H}g^{-1}$, ou encore $g^{-1}\mathrm{K}g \subset \mathrm{H}$.*
- ◇ *Les p-Sylow de* G *sont conjugués deux à deux.*
- ◇ *$n_p \equiv 1 \ (mod\ p)$ et n_p divise m.*

Remarque 1.7.2. — Soit G un groupe fini. Soit φ un automorphisme de G.

Si S est un p-Sylow de G, alors $|\varphi(\mathrm{S})| = |\mathrm{S}| = p^\alpha$; ainsi $\varphi(\mathrm{S})$ est un p-Sylow de G.

Si de plus S est l'unique p-Sylow de G, alors $\varphi(\mathrm{S}) = \mathrm{S}$, *i.e.* S est un sous-groupe caractéristique de G.

Corollaire 1.7.4. — *Si* S *est un p-Sylow de* G*, alors*

$$ \mathrm{S} \triangleleft \mathrm{G} \Leftrightarrow \mathrm{S} \text{ est l'unique } p\text{-Sylow de } \mathrm{G} \Leftrightarrow n_p = 1. $$

Lemme 1.7.5. — *Soit* G *un p-groupe opérant sur un ensemble X. Soit*

$$ X^{\mathrm{G}} = \{x \in X \,|\, \forall\, g \in \mathrm{G} \quad g \cdot x = x\} $$

l'ensemble des points fixes sous G*, alors $|X| \equiv |X^{\mathrm{G}}|$ mod p.*

Démonstration. — Écrivons X comme réunion disjointe de ses orbites sous G en remarquant que $x \in X^{\mathrm{G}}$ si et seulement si $\mathcal{O}(x) = \{x\}$. Si x n'appartient pas à X^{G}, alors $|\mathcal{O}(x)| > 1$ et comme $|\mathcal{O}(x)|$ divise $|\mathrm{G}| = p^n$, p divise $|\mathcal{O}(x)|$. Le résultat provient alors de l'égalité

$$|X| = |X^{\mathrm{G}}| + \sum_{x \notin X^{\mathrm{G}}} |\mathcal{O}(x)|.$$

□

Démonstration du Théorème 1.7.3. — Si H est un p-sous-groupe de G et si S est un p-Sylow de G, alors d'après le Lemme 1.7.2 il existe $a \in \mathrm{G}$ tel que $a\mathrm{S}a^{-1} \cap \mathrm{H}$ soit un p-Sylow de H. Mais comme H est un p-groupe, $a\mathrm{S}a^{-1} \cap \mathrm{H} = \mathrm{H}$. Par suite H est inclus dans $a\mathrm{S}a^{-1}$ qui est un Sylow. Si de plus H est un Sylow on a $\mathrm{H} = a\mathrm{S}a^{-1}$. On a donc montré les deux premières assertions.

Montrons maintenant la troisième assertion.

Faisons opérer G par conjugaison sur l'ensemble X de ses p-Sylow [6] Soit S un p-Sylow, S opère lui aussi sur X et on a (Lemme 1.7.5)

$$|X| \equiv |X^{\mathrm{S}}| \bmod p$$

Montrons que $|X^{\mathrm{S}}| = 1$. Bien sûr si $s \in \mathrm{S}$, on a $s\mathrm{S}s^{-1} = \mathrm{S}$, autrement dit $\mathrm{S} \in X^{\mathrm{S}}$. Montrer que $|X^{\mathrm{S}}| = 1$ revient donc à montrer que S est l'unique élément de X^{S}. Soit T un élément de X^{S}, *i.e* T est un p-Sylow tel que :

$$\forall\, s \in \mathrm{S} \quad s\mathrm{T}s^{-1} = \mathrm{T}$$

Considérons le sous-groupe N de G engendré par S et T. On a $\mathrm{S} \subset \mathrm{N}$, $\mathrm{T} \subset \mathrm{N}$ et ce sont a fortiori des p-Sylow de N. Mais comme S normalise T on a $\mathrm{T} \lhd \mathrm{N}$. Le Corollaire 1.7.4 assure que T est l'unique Sylow de N. Ainsi $\mathrm{S} = \mathrm{T}$.

Les p-Sylow forment une orbite sous G donc n_p divise m (en effet les p-Sylow forment une orbite sous G donc n_p divise $|\mathrm{G}| = p^\alpha m$ d'après le Corollaire 1.2.2 et $n_p \equiv 1 \bmod p$). □

Corollaire 1.7.6 (Théorème de Cauchy)**.** — *Soit* G *un groupe.*

Si p est un nombre premier qui divise l'ordre de 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 Premier Théorème de Sylow) est d'ordre non divisible par p et par ailleurs cet ordre divise p^a : contradiction. □

Corollaire 1.7.7. — *Si* G *est un groupe tel que $|\mathrm{G}| = p^\alpha m$ avec $p \not| m$, alors* G *contient des sous-groupes d'ordre p^i pour tout $i \leq \alpha$.*

6. Si G est un groupe et X l'ensemble de ses sous-groupes, alors G opère sur X par automorphisme intérieur : $g \cdot \mathrm{H} = g\mathrm{H}g^{-1}$.

Démonstration. — Soit S un p-SYLOW de G ; alors $|\mathrm{S}| = p^\alpha$. Puisque S est un p-groupe, $Z(\mathrm{S}) \neq \{e\}$. Le théorème de CAUCHY (Corollaire 1.7.6) assure l'existence d'un élément g d'ordre p dans $Z(\mathrm{S})$.

Le groupe $\langle g\rangle$ est un sous-groupe de $\mathrm{S} \subset \mathrm{G}$ d'ordre p, nous avons donc montré l'énoncé pour $i = 1$.

Supposons que tout sous-groupe de S d'ordre p^i, $i < \alpha$, contient un sous-groupe d'ordre p^j pour tout entier $j \leq i$. L'hypothèse de récurrence assure l'existence d'un sous-groupe H_{i-1} d'ordre p^{i-1} dans $\mathrm{S}/\langle g\rangle$. Désignons par $\pi\colon \mathrm{S} \to \mathrm{S}/\langle g\rangle$. Le groupe $\pi^{-1}(\mathrm{H}_{i-1})$ est un sous-groupe de S et donc de G d'ordre p^i. □

Terminons ce paragraphe par quelques exemples.

1.7.1. Le cas 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 1.7.2 que 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. Le Théorème 1.7.3 assure que les p-SYLOW de G sont les sous-groupes de la forme $M\mathrm{P}M^{-1}$ où M appartient à $\mathrm{GL}(n, \mathbb{F}_p)$.

1.7.2. Application du Corollaire 1.7.4 : —

Proposition 1.7.8. — *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. Il en résulte que $n_7 = 1$. Par conséquent G n'est pas simple (Corollaire 1.7.4). □

1.7.3. Les groupes $\mathcal{S}_4$ et $\mathcal{A}_4$. — Soient ν_p le nombre de p-SYLOW de $\mathcal{S}_4$ et n_p le nombre de p-SYLOW de $\mathcal{A}_4$.

Le groupe $\mathcal{S}_4$ est d'ordre $24 = 2^3 \times 3$ et le groupe $\mathcal{A}_4$ d'ordre $12 = 2^2 \times 3$.

Les théorèmes de SYLOW assurent que

- ◇ ν_3 divise $2^3 = 8$ et est congru à 1 modulo 3, c'est-à-dire ν_3 appartient à $\{1, 4\}$;
- ◇ n_3 divise $2^2 = 4$ et est congru à 1 modulo 3, c'est-à-dire n_3 appartient à $\{1, 4\}$;
- ◇ ν_2 divise 3 et est congru à 1 modulo 2, c'est-à-dire ν_2 appartient à $\{1, 3\}$;
- ◇ n_2 divise 3 et est congru à 1 modulo 2, c'est-à-dire n_2 appartient à $\{1, 3\}$.

Un 3-SYLOW de $\mathcal{S}_4$ est un sous-groupe de $\mathcal{S}_4$ 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 $\mathcal{S}_4$ sont les 3-cycles, les 3-SYLOW de $\mathcal{S}_4$ sont

- ◇ $\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$,
- ◇ $\{\mathrm{id}, (1\ 2\ 4), (1\ 4\ 2)\}$,
- ◇ $\{\mathrm{id}, (1\ 3\ 4), (1\ 4\ 3)\}$,

$\diamond$ $\{\mathrm{id},\ (2\ 3\ 4),\ (2\ 4\ 3)\}$.

Par suite $n_3 = 4$. 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 $\nu_3 = 4$.

Construisons désormais les 2-Sylow de $\mathcal{S}_4$. Introduisons l'ensemble E des partitions de $\{1,\ 2,\ 3,\ 4\}$ en deux sous-ensembles à deux éléments ; autrement dit E 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 $\mathcal{S}_4$ sur E ; 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 $|\mathrm{Stab}_{\mathcal{S}_4}(P_1)| = \frac{24}{3} = 8$. C'est donc un 2-Sylow de $\mathcal{S}_4$. L'ensemble des 2-Sylow de $\mathcal{S}_4$ est l'ensemble des conjugués de $\mathrm{Stab}_{\mathcal{S}_4}(P_1)$, *i.e.*

$$\{\mathrm{Stab}_{\mathcal{S}_4}(P_1),\ \mathrm{Stab}_{\mathcal{S}_4}(P_2),\ \mathrm{Stab}_{\mathcal{S}_4}(P_3)\}$$

(rappelons que si G est un groupe opérant sur un ensemble E, si x appartient à E et y appartient à $\mathrm{G}x$, alors $\mathrm{Stab}_{\mathrm{G}}(y)$ est égal au conjugué de $\mathrm{Stab}_{\mathrm{G}}(x)$ par n'importe quel élément de G qui envoie x sur y). Or

$$\begin{aligned}
\mathrm{Stab}_{\mathcal{S}_4}(P_1) &= \{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\ (1\ 3\ 2\ 4),\ (1\ 4\ 2\ 3),\ (1\ 2),\ (3\ 4)\} \\
\mathrm{Stab}_{\mathcal{S}_4}(P_2) &= \{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\ (1\ 2\ 3\ 4),\ (1\ 4\ 3\ 2),\ (1\ 3),\ (2\ 4)\} \\
\mathrm{Stab}_{\mathcal{S}_4}(P_3) &= \{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\ (1\ 2\ 4\ 3),\ (1\ 3\ 4\ 2),\ (1\ 4),\ (2\ 3)\}
\end{aligned}$$

Ces groupes sont donc les 2-Sylow de $\mathcal{S}_4$. Ils sont deux à deux distincts donc $\nu_2 = 3$. De plus

$$\mathrm{Stab}_{\mathcal{S}_4}(P_1) \cap \mathrm{Stab}_{\mathcal{S}_4}(P_2) \cap \mathrm{Stab}_{\mathcal{S}_4}(P_3) = \{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

Cette intersection coïncide avec le noyau du morphisme $\mathcal{S}_4 \to \mathcal{S}_E \simeq \mathcal{S}_3$ induit par l'action de $\mathcal{S}_4$ sur E ; c'est en particulier un sous-groupe distingué de $\mathcal{S}_4$ 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 1.7.4).

1.7.4. Classification des groupes d'ordre 15**.** — Soit G un groupe de cardinal 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 $\phi\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{N})$. 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 $\left(\mathbb{Z}/5\mathbb{Z}\right)^\times = 4$ le morphisme φ est trivial [7] et G est isomorphe au produit direct $\mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/m\mathbb{Z}$ c'est-à-dire à $\mathbb{Z}/15\mathbb{Z}$

7. 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 $\mathbb{Z}/n\mathbb{Z} \times_\varphi \mathbb{Z}/m\mathbb{Z}$.

1.7.5. 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 $n_7 \equiv 1 \bmod 7$ et $n_7|3$, *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

- $\mathrm{G} \triangleleft \mathrm{G}$,
- $|\mathrm{H}|$ 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

$$\varphi\colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}\big(\mathbb{Z}/7\mathbb{Z}\big)$$

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 $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/21\mathbb{Z}$;
- G est isomorphe à $\mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/3\mathbb{Z}$ où $\varphi(\underbrace{\overline{r}}_{\bmod 3})(x) = \underbrace{\overline{2}^r}_{\bmod 7}\, x$.

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 1.3.6). 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 en conséquence 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.

1.7.6. Groupes d'ordre pq. — *Référence :* [**Per82**, p. 27-28]

Leçons possibles :

103 : *Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.*

104 : *Groupes abéliens et non abéliens finis. Exemples et applications.*

Théorème 1.7.9. — *Soient p et q des nombres premiers avec $p < q$.*

- ◇ *Si p ne divise pas $q-1$, alors tout groupe d'ordre pq est cyclique.*
- ◇ *Si p divise $q-1$, il y a deux groupes d'ordre pq non isomorphes : le groupe cyclique et un produit semi-direct non abélien.*

Énonçons le résultat suivant dont nous aurons besoin :

Lemme 1.7.10. — *Soient* H *et* N *deux groupes. Soient φ et ψ deux opérations de* H *sur* N *et α un automorphisme de* H *tels que le diagramme suivant commute*

$$\begin{array}{ccc} & H & \\ {\scriptstyle\alpha}\swarrow & & \searrow{\scriptstyle\varphi} \\ H & \xrightarrow[\psi]{} & \mathrm{Aut}(N) \end{array}$$

i.e. $\varphi = \psi \circ \alpha$.

L'application $(n,h) \mapsto (n, \alpha(h))$ est un isomorphisme de $\mathrm{N} \rtimes_\psi \mathrm{H}$ *sur* $\mathrm{N} \rtimes_\varphi \mathrm{H}$.

Démonstration du Théorème 1.7.9. — Soit G un groupe d'ordre pq où p et q désignent des nombres premiers tels que $p < q$. Soit Q un q-Sylow de G.

D'après les théorèmes de Sylow

$$\begin{cases} n_q \text{ divise } p \\ n_q \equiv 1 \bmod q \end{cases}$$

où n_q est le nombre de q-Sylow de G. Par suite $n_q = 1$ et Q est distingué dans G.

Puique p est premier, $\mathbb{Q} \simeq \mathbb{Z}/q\mathbb{Z}$. De même $\mathrm{G}/\mathrm{Q} \simeq \mathbb{Z}/p\mathbb{Z}$. Si P est un p-Sylow quelconque il fournit un relèvement de G/Q et donc

$$\mathrm{G} \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Calculons ces produits. Nous avons $\mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ (Proposition 1.3.6 Lemme 1.3.9). L'opération de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$ correspond donc à un morphisme

$$\varphi \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}.$$

Nous avons l'alternative suivante :

- ◇ p ne divise pas $q-1$, alors φ est trivial, le produit est direct et $\mathrm{G} \simeq \mathbb{Z}/pq\mathbb{Z}$ est cyclique.

◇ p divise $q-1$, $\mathbb{Z}/(q-1)\mathbb{Z}$ possède un unique sous-groupe d'ordre p, il y a donc une opération non triviale. De plus deux telles opérations diffèrent d'un automorphisme de $\mathbb{Z}/p\mathbb{Z}$. Le lemme 1.7.10 assure que les produits correspondants sont isomorphes.

□

1.8. Les groupes symétriques et alternés

1.8.1. Une autre définition de la signature. — Donnons une seconde définition de la *signature*.

Soit n un entier. Pour tout $\sigma \in \mathcal{S}_n$ 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 $\mathcal{S}_n$ 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 $\sigma \in \mathcal{S}_n$.

Si σ un élément de $\mathcal{S}_n$, 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 $\mathcal{S}_n$; 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 $\mathcal{S}_n$ dans $\{-1, 1\}$, appelé *signature*.

Proposition-Définition 1.8.1. — *Soit E un ensemble fini de cardinal n. Soit Φ une bijection de E sur $\{1, 2, \ldots, n\}$. Le morphisme de groupes*

$$\mathcal{S}_E \to \{-1, 1\} \qquad\qquad \sigma \mapsto \mathrm{sgn}(\Phi \circ \sigma \circ \Phi^{-1})$$

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 $\mathcal{S}_E$. 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 $\mathcal{S}_n$. Par suite leurs images par le morphisme sgn sont conjuguées dans $\{-1, 1\}$ et sont finalement égales puisque $\{-1, 1\}$ est abélien [8]. □

Exemple 1.8.1 (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 1.8.1 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* (resp. impaire) si sa signature est 1 (resp. -1). D'après ce qui précède σ est paire (resp. impaire) si et seulement si elle s'écrit comme le produit d'un nombre pair (resp. impair) de transpositions.

Calculons la signature dans le cas général. Soit E un ensemble fini. Soit C un ℓ-cycle de $\mathcal{S}_E$. Puisque C s'écrit comme un produit de $\ell - 1$ transpositions (Lemme 1.1.3) nous avons $\mathrm{sgn}(C) = (-1)^{\ell-1}$. Considérons maintenant une permutation quelconque de $\mathcal{S}_E$. 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

$$\mathrm{sgn}(\sigma) = \prod_i (-1)^{\ell_i - 1} = (-1)^{\sum_i \ell_i - r}.$$

8. Soient h et h' deux éléments conjugués de G ; soit $g \in \mathrm{G}$ 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 $\varphi(h') = \varphi(h)$.

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.

1.8.2. Décomposition d'une permutation en transpositions. —

Référence : [**Com98**, p. 79-81]

Leçons possibles :

101 : *Groupe opérant sur un ensemble. Exemples et applications.*

104 : *Groupes abéliens et non abéliens finis. Exemples et applications.*

105 : *Groupe des permutations d'un ensemble fini. Applications.*

108 : *Exemples de parties génératrices D'un groupe. Applications.*

Théorème 1.8.2. — *Toute permutation $s \in \mathcal{S}_n$ est un produit de transpositions.*

Proposition 1.8.3. — *Toute permutation $s \in \mathcal{S}_n$ s'écrit de manière unique (modulo l'ordre des termes) comme un produit de cycles disjoints*

$$s = c_1 c_2 \dots c_p.$$

L'ordre de s est le ppcm des ordres de c_1, c_2, …, c_p.

Proposition 1.8.4. — *Soient* G *un groupe et $g \in$ G. L'application $f\colon k \mapsto a^k$ est un morphisme de $\mathbb{Z}$ sur le sous-groupe $\langle a \rangle$ engendré par a.*

Si f est injectif, alors $\langle a \rangle$ est isomorphe à $\mathbb{Z}$.

Si f n'est pas injectif, alors $\langle a \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}^*$ est le plus petit entier non nul tel que $a^n = e$. Dans ce cas, les entiers k tels que $a^k = e$ sont les multiples de n et $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$.

Proposition 1.8.5. — *Les sous-groupes de $(\mathbb{Z}, +)$ sont les sous-ensembles $n\mathbb{Z}$ où $n \in \mathbb{N}$.*

Démonstration. — Notons que $0 \in n\mathbb{Z}$. Soient g, g' dans $n\mathbb{Z}$, *i.e.* $g = nk$ et $g' = nk'$ avec k et k dans $\mathbb{Z}$. Ainsi $g - g' = n(k - k')$ appartient à $n\mathbb{Z}$. Il en résulte que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Réciproquement soit G un sous-groupe de $\mathbb{Z}$. Si G est réduit à $\{0\}$, alors G $= 0\mathbb{Z}$. Supposons désormais que G $\neq \{0\}$; alors il existe $g \neq 0$ dans G. Remarquons que $-g \in$ G donc G$\cap\mathbb{N}^* \neq \emptyset$. Soit n le plus petit élément de G $\cap\, \mathbb{N}^*$. Pour tout $k \in \mathbb{N}$ on a

$$nk = \underbrace{n + n + \ldots + n}_{k \text{ fois}} \in G$$

et $n(-k) = -(nk) \in$ G. Ainsi $n\mathbb{Z} \subset$ G. Soit $g \in$ G positif. La division de g par n conduit à $g = nq + r$ avec $0 \leq r < n$ et $q \in \mathbb{N}$. Il en résulte que

$$r = g - \underbrace{n + n + \ldots + n}_{q \text{ fois}}$$

appartient à G. Supposons r non nul : alors n n'est pas le plus petit élément de $\mathrm{G} \cap \mathbb{N}$: contradiction. Par suite $r = 0$ et $g = nq \in n\mathbb{Z}$. Si $g \in \mathrm{G}$ est négatif, alors $-g \in \mathrm{G}$ est positif et appartient donc à $n\mathbb{Z}$. Il s'en suit que $\mathrm{G} \subset n\mathbb{Z}$ et donc $\mathrm{G} = n\mathbb{Z}$. □

Démonstration de la Proposition 1.8.4. — L'application $f_0 \colon \mathbb{N} \to \langle a \rangle$, $k \mapsto a^k$ vérifie

$$\forall\, k \in \mathbb{N} \qquad \forall\, k' \in \mathbb{N} \qquad f_0(k+k') = a^{k+k'} = a^k a^{k'} = f_0(k) f_0(k').$$

La propriété universelle du symétrisé $\mathbb{Z}$ de $\mathbb{N}$ permet de prolonger f_0 en un morphisme f de $\mathbb{Z}$ dans $\langle a \rangle$. Pour $k = -|k| < 0$, on a $f(-|k|) = f(|k|)^{-1} = (a^{|k|})^{-1} = a^k$. Par suite $\mathrm{im} f = \{a^k \,|\, k \in \mathbb{Z}\} = \langle a \rangle$.

D'après la Proposition 1.8.5 il existe $n \in \mathbb{N}$ tel que $\ker f = n\mathbb{Z}$. Si $n = 0$, alors f est injective ; c'est un isomorphisme f de $\mathbb{Z}$ dans $\langle a \rangle$. Si n est non nul, le théorème d'isomorphisme assure l'existence d'un isomorphisme $\overline{f}$ entre $\mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z}$ et $\langle a \rangle$. Par définition le noyau de f est l'ensemble des $k \in \mathbb{Z}$ tels que $a^k = e$, c'est-à-dire l'ensemble $n\mathbb{Z}$ des multiples de n. Puisque $0, 1, \ldots, n-1$ sont des représentants des n classes modulo $n\mathbb{Z}$ leurs images $e = a^0$, a, a^2, …, a^{n-1} par $\overline{f}$ sont les éléments de $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f) = \langle a \rangle$. □

Proposition 1.8.6. — *Soit E un ensemble. Soit* G *un groupe. Considérons une action à gauche de* G *sur E.*

(i) La relation

$$x \mathcal{R} y \iff (\exists\, g \in \mathrm{G} \quad g \cdot x = y)$$

est une relation d'équivalence sur E.

(ii) Soit $x \in E$; alors

$$\mathrm{G}_x = \{g \in \mathrm{G} \,|\, g \cdot x = x\}$$

est un sous-groupe de G.

(iii) Soit $x \in E$, soit $g_0 \in \mathrm{G}$ et soit $y = g_0 \cdot x$. Alors

$$\mathrm{G}_y = g_0 \mathrm{G}_x g_0^{-1} \qquad\qquad \{g \in \mathrm{G} \,|\, g \cdot x = y\} = g_0 \mathrm{G}_x$$

Démonstration. — (i) Pour tout $x \in E$ on a $x \mathcal{R} x$ car $e \cdot x = x$; la relation $\mathcal{R}$ est donc réflexive. Si $x \mathcal{R} y$ alors il existe $g \in \mathrm{G}$ tel que $g \cdot x = y$ d'où $x = g^{-1} \cdot y$, *i.e.* $y \mathcal{R} x$. Ainsi $\mathcal{R}$ est symétrique. Enfin elle est transitive car

$$(g \cdot x = y \text{ et } g' \cdot y = z) \Rightarrow g'g \cdot x = z$$

(ii) Direct.

(iii) Pour tout g dans G on a d'une part

$$\begin{aligned} g \in \mathrm{G}_y &\iff g \cdot (g_0 \cdot x) = g_0 \cdot x \\ &\iff (g_0^{-1} g g_0) \cdot x = x \\ &\iff g_0^{-1} g g_0 \in \mathrm{G}_x \\ &\iff g \in g_0 \mathrm{G}_x g_0^{-1} \end{aligned}$$

d'autre part

$$\begin{aligned} g \in \{g \in \mathrm{G} \,|\, g \cdot x = y\} &\iff g \cdot x = y \\ &\iff g \cdot x = g_0 \cdot x \\ &\iff g_0^{-1} g \cdot x = x \\ &\iff g_0^{-1} g \in \mathrm{G}_x \\ &\iff g \in g_0 \mathrm{G}_x \end{aligned}$$

□

Démonstration de la Proposition 1.8.3. — La Proposition 1.8.5 assure que $k \mapsto s^k$ est un morphisme du groupe additif $\mathbb{Z}$ dans $\mathcal{S}_n$. C'est une action de $\mathbb{Z}$ sur l'ensemble $E = \{1, 2, \ldots, n\}$. Soient $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_p$ les orbites qui ne sont pas réduites à un point, *i.e.* les orbites des éléments du support de s. Soit i_1 dans $\mathcal{O}_1$. Son stabilisateur est un sous-groupe de $\mathbb{Z}$ donc de la forme $k\mathbb{Z}$ (Proposition 1.8.5). Les éléments de $\mathcal{O}_1$ sont

$$i_1,\ i_2 = s(i_1),\ i_3 = s(i_2) = s^2(i_1),\ \ldots,\ i_k = s(i_{k-1}) = s^{k-1}(i_1).$$

D'après la Proposition 1.8.6 (iii) ces éléments sont bijectivement associés aux classes de $\mathbb{Z}$ modulo le stabilisateur $k\mathbb{Z}$ et sont donc distincts. On a $s^k(i_1) = i_1$. L'action de s sur l'orbite $\mathcal{O}_1$ est la même que celle du cycle $c_1 = (i_1\ i_2\ \ldots\ i_k)$. De même il existe des cycles c_2, c_3, …, c_p ayant pour supports les orbites $\mathcal{O}_2$, $\mathcal{O}_3$, …, $\mathcal{O}_p$ ayant la même action que s sur ces orbites. Les cycles c_1, c_2, …, c_p commutent car ils sont disjoints et $(c_1 c_2 \ldots c_p)(i) = s(i)$ pour tout point i du support $\bigcup_{m=1}^{p} \mathcal{O}_m$ de s. Les autres éléments de E sont fixes par s et $c_1 c_2 \ldots c_p$ donc $s = c_1 c_2 \ldots c_p$.

Montrons l'unicité (modulo l'ordre des cycles) de l'expression $s = c_1 c_2 \ldots c_p$ par récurrence sur p. Si $p = 0$, *i.e.* si $s = \mathrm{id}$, l'unicité est évidente. Soit $p \geq 1$. Supposons que les permutations pouvant s'exprimer comme produit de moins de p cycles disjoints ont une écriture unique (modulo l'ordre des cycles). Considérons une permutation s qui est le produit de p cycles disjoints :

$$s = c_1 c_2 \ldots c_p$$

Soit $s = c'_1 c'_2 \ldots c'_q$ une autre décomposition de s en cycles disjoints. Soit i un élément du support $\mathcal{O}_1$ de c_1. Il appartient au support d'un des cycles c'_j et à un seul. Quitte à réindicer les c'_j on peut supposer que i appartient au support de c'_1. Pour tout r dans $\mathbb{Z}$ on a

$$s^{r(i)} = c_1^{r(i)} = (c'_1)^{r(i)}.$$

Ainsi $c_1 = c'_1$. Par conséquent $c_1 c_2 \ldots c_p = c'_1 c'_2 \ldots c'_q$ entraîne $c_2 c_3 \ldots c_p = c'_2 c'_3 \ldots c'_q$. D'après l'hypothèse de récurrence on obtient $p = q$ et $\{c_2, c_3, \ldots, c_p\} = \{c'_2, c'_3, \ldots, c'_p\}$.

Comme les cycles commutent on a pour tout entier n

$$s^n = c_1^n c_2^n \ldots c_p^n$$

Les supports des c_i étant disjoints, $s^n = \mathrm{id}$ si et seulement si $(c_1^n, c_2^n, \ldots, c_p^n) = (\mathrm{id}, \mathrm{id}, \ldots, \mathrm{id})$, *i.e.* si et seulement si n est multiple commun des ordres $k_1, k_2, \ldots, k_p$ de $c_1, c_2, \ldots, c_p$. Le plus petit entier strictement positif n tel que $s^n = \mathrm{id}$ est donc $\mathrm{ppcm}(k_1, k_2, \ldots, k_p)$. □

Démonstration du Théorème 1.8.2. — D'après la Proposition 1.8.3 il suffit de montrer que tout cycle $(i_1\ i_2\ \ldots\ i_p)$ est un produit de transpositions. Montrons par récurrence sur la longueur p du cycle que

$$(i_1\ i_2\ \ldots\ i_p) = (i_1\ i_2)(i_2\ i_3)\ldots(i_{p-1}\ i_p).$$

La formule est vraie pour $p = 2$.

Supposons que $p > 2$ et que la formule soit vraie pour $p-1$, *i.e.*

$$(i_1\ i_2\ \ldots\ i_{p-1}) = (i_1\ i_2)(i_2\ i_3)\ldots(i_{p-1}\ i_{p-1});$$

alors

$$(i_1\ i_2)(i_2\ i_3)\ldots(i_{p-1}\ i_p) = (i_1\ i_2\ \ldots\ i_{p-1})(i_{p-1}\ i_p) = (i_1\ i_2\ \ldots\ i_p).$$

□

1.8.3. Simplicité du groupe alterné. —

Théorème 1.8.7. — *Le groupe $\mathcal{A}_n$ est simple dès que $n \geq 5$.*

Nous allons donner deux démonstrations de ce résultat.

1.8.3.1. *Le groupe $\mathcal{A}_n$ est simple dès que $n \geq 5$, version* 1. —

Référence : [**Per82**, p. 28-30]

Leçons possibles :

103 : *Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.*

105 : *Groupe des permutations d'un ensemble fini. Applications.*

104 : *Groupes abéliens et non abéliens finis. Exemples et applications.*

108 : *Exemples de parties génératrices d'un groupe. Applications.*

Corollaire 1.8.8. — *Dès que $n \geq 5$, on a $D(\mathcal{A}_n) = \mathcal{A}_n$.*
Dès que $n \geq 2$, on a $D(\mathcal{S}_n) = \mathcal{A}_n$.

Remarque 1.8.1. — Le Corollaire est une conséquence évidente du Théorème 1.8.7 mais il peut se montrer directement. Donnons quelques détails. On a les inclusions suivantes :

$$D(\mathcal{A}_n) \subset D(\mathcal{S}_n) \subset \mathcal{A}_n$$

Lemme 1.8.9. — *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 $\rho \in \mathcal{S}_n$ 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 $\mathcal{S}_n$. 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 1.8.10. — *Dès que $n \geq 3$ les 3-cycles engendrent $\mathcal{A}_n$.*

Démonstration. — Puisque le groupe $\mathcal{S}_n$ 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 1.8.9) : 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 $D(\mathcal{S}_n) = \mathcal{A}_n$ dès que $n \geq 2$.

Remarques 1.8.2. — 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 1.8.7 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 1.8.9). 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 (resp. 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 1.8.3. — 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 $\mathcal{S}_5$.

Démonstration du théorème 1.8.7 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 1.8.9) ils appartiennent tous à H et puisqu'ils engendrent $\mathcal{A}_n$ (Lemme 1.8.10) on a $\mathrm{H} = \mathcal{A}_n$. □

Remarque 1.8.4. — 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 1.8.11. — *Dès que $n \geq 5$ les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.*

Avant de démontrer ce résultat donnons quelques résultats intermédiaires.

Lemme 1.8.12. — *Soit $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathcal{S}_n$. Alors*

$$\sigma(a\ b)\sigma^{-1} = (\sigma(a)\ \sigma(b)).$$

Lemme 1.8.13. — *Soit $n \geq 3$. Le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$.*

Démonstration. — Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma(1\ 2) = (1\ 2)\sigma$, *i.e.* $\sigma(1\ 2)\sigma^{-1} = (1\ 2)$. Par suite (Lemme 1.8.12)

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

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 1.8.11. — Soit $\mathrm{H} \triangleleft \mathcal{S}_n$. 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 $\mathrm{H} = \mathcal{S}_n$.

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 $\tau \in \mathcal{S}_n$ 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 $\mathcal{S}_n$ d'où $\sigma = \mathrm{id}$ (Lemme 1.8.13) : contradiction. Il en résulte que $\mathrm{H} = \{\mathrm{id}\}$. □

1.8.3.2. *Le groupe $\mathcal{A}_n$ est simple dès que $n \geq 5$, version 2.* —

Référence : [**Szp08**, p. 99, 110-112, 126-127, 141-142].

Leçons possibles :

103 : *Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.*

105 : *Groupe des permutations d'un ensemble fini. Applications.*

104 : *Groupes abéliens et non abéliens finis. Exemples et applications.*

108 : *Exemples de parties génératrices d'un groupe. Applications.*

Théorème 1.8.14. — *Le groupe $\mathcal{A}_5$ est simple.*

Lemme 1.8.15. — *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 1.8.16. — *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 1.8.17. — *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

$$n_5 \equiv 1 \pmod 5 \qquad\qquad n_5 \mid 6$$

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) $K \cap \mathrm{H} = \{e\}$ et KH est un sous-groupe d'ordre 15 dans le groupe G.

□

Lemme 1.8.18. — *Tout groupe d'ordre* 30 *ne contient qu'un seul* 5-*Sylow* (*d'ordre* 5).

Démonstration. — Dans la démonstration du Lemme 1.8.17 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 1.8.15) qui est distingué dans G. Donc en fait K et H sont distingués dans G et G a un unique 5-Sylow. □

Lemme 1.8.19. — *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

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \mid 4$$

d'où $n_5 = 1$. □

Lemme 1.8.20. — *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

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \,|\, 4$$

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 1.8.15).
- 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

  $$n_2 \equiv 1 \bmod 2 \qquad\qquad n_2 \,|\, 3$$

  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 1.8.16).

□

Lemme 1.8.21. — *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

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \,|\, 2$$

autrement dit que $n_3 = 1$. Ainsi G compte un unique 3-Sylow qui est donc distingué dans G et le Lemme 1.8.16 permet de conclure. □

Lemme 1.8.22. — *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

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \,|\, 12$$

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 |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 |H| divise 60 donc $|H| = 30$ (rappelons que comme H est un sous-groupe propre de G, on a $|H| < 60$. 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 |H| n'est pas divisible par 5.

Si |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 $^{\mathrm{G}}\!/_{\mathrm{H}}$ est d'ordre 30, 20 ou 15. Dans ces trois cas $^{\mathrm{G}}\!/_{\mathrm{H}}$ 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 $K = \pi(\pi^{-1}(\mathrm{K}))$ donc $|\pi^{-1}(\mathrm{K})|$ est divisible par 5 : contradiction. □

Démonstration du Théorème 1.8.14. — 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 1.8.22 assure donc que $\mathcal{A}_5$ est simple. □

Lemme 1.8.23. — *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 1.8.5. — 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 1.8.5 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 1.8.5). 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 1.8.24. — *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 $\mathrm{G}_j = \mathrm{Stab}_{\mathcal{A}_n}(\{j\})$ 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 1.8.23). 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 $\mathcal{S}_n$ 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 1.8.25. — *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 1.8.24). Il en résulte que $\mathcal{A}_n \subset \mathrm{H}$. Or $H \subset \mathcal{A}_n$ donc $\mathcal{A}_n = \mathrm{H}$. □

Démonstration du Théorème 1.8.7. — Le groupe $\mathcal{A}_5$ est simple (Théorème 1.8.14). Pour $n \geq 6$ tout sous-groupe distingué de $\mathcal{A}_n$ différent de $\{\mathrm{id}\}$ est égal à $\mathcal{A}_n$ (Lemme 1.8.25). □

1.8.4. Les automorphismes de $\mathcal{S}_n$. —

Référence : [**Per82**, p. 30]

Leçons possibles :

101 *: Groupe opérant sur un ensemble. Exemples et applications.*

104 *: Groupes abéliens et non abéliens finis. Exemples et applications.*

105 *: Groupe des permutations d'un ensemble fini. Applications.*

108 *: Exemples de parties génératrices D'un groupe. Applications.*

Puisque $n \geq 3$ le centre $Z(\mathcal{S}_n)$ de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$ (Lemme 1.8.27). Par suite $\mathcal{S}_n$ agit fidèlement sur lui-même par conjugaison. Autrement dit le groupe $\mathrm{Int}(\mathcal{S}_n)$ des automorphismes intérieurs de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_n$.

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 $\mathcal{S}_6$.

1.8.4.1. *Automorphismes de $\mathcal{S}_n$, $n \neq 6$.* —

Lemme 1.8.26. — *Soit $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathcal{S}_n$. Alors*

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

Lemme 1.8.27. — *Soit $n \geq 3$. Le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$.*

Démonstration. — Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite (Lemme 1.8.26)

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

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 1.8.28. — *Soit $n \geq 3$. Supposons que $n \neq 6$; alors*

$$\mathrm{Aut}(\mathcal{S}_n) = \mathrm{Int}(\mathcal{S}_n) \simeq \mathcal{S}_n.$$

Lemme 1.8.29. — *Soit φ un automorphisme de $\mathcal{S}_n$ qui envoie transpositions sur transpositions. Alors φ appartient à $\mathrm{Int}(\mathcal{S}_n)$.*

Démonstration. — Les transpositions de la forme $(1\ \ i)$ où $2 \leq i \leq n$ engendrent $\mathcal{S}_n$. 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

$$\tau_2 = (\alpha_1\ \ \alpha_2) \qquad\qquad \tau_3 = (\alpha_1\ \ \alpha_3)$$

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

$$\tau_2 \circ \tau_k = (\alpha_1\ \ \alpha_2\ \ \alpha_3) \qquad\qquad \tau_3 \circ \tau_k = (\alpha_1\ \ \alpha_3\ \ \alpha_2)$$

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 $\mathcal{S}_n$.

L'automorphisme φ et la conjugaison par α coïncident sur les générateurs $(1\ \ j)$ de $\mathcal{S}_n$; ils coïncident donc sur $\mathcal{S}_n$ tout entier. □

Démonstration du Théorème 1.8.28. — Soit φ un automorphisme non intérieur de $\mathcal{S}_n$. Montrons que $n = 6$.

D'après le Lemme 1.8.29 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

$$\mathrm{C}(\tau) = \{f \in \mathcal{S}_n \mid f \circ \tau = \tau \circ f\}.$$

On a

$$\mathrm{C}(\tau) = \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{engendré par } \tau} \times \underbrace{\mathcal{S}_{n-2}}_{\text{permutations de support disjoint de celui de } \tau}$$

En particulier on a un morphisme surjectif

$$\psi \colon \mathrm{C}(\tau) \to \mathcal{S}_{n-2}$$

de noyau $\mathbb{Z}/2\mathbb{Z}$.

Posons $\mathrm{H} = \mathrm{C}(\varphi(\tau)) = \{f \in \mathcal{S}_n \mid f \circ \varphi(\tau) = \varphi(\tau) \circ f\}$. 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 $(\mathbb{Z}/2\mathbb{Z})^k$. De plus N est le noyau du morphisme

$$\begin{array}{rcl} \mathrm{H} & \to & \mathcal{S}_k \\ h & \mapsto & \text{permutation induite sur les } k \text{ transpositions de la décomposition de } \varphi(\tau) \end{array}$$

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 :

$$\begin{cases} \mathrm{N}' \lhd \mathrm{C}(\tau) \\ \mathrm{N}' \simeq (\mathbb{Z}/2\mathbb{Z})^k \end{cases}$$

Via ψ on obtient que $\mathcal{S}_{n-2}$ contient un sous-groupe distingué isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$ ou $(\mathbb{Z}/2\mathbb{Z})^{k-1}$ suivant que $\tau \in \mathrm{N}'$ ou $\tau \notin \mathrm{N}'$.

Or les sous-groupes distingués de $\mathcal{S}_n$ sont

- $\diamond$ $\{\mathrm{id}\}$, $\mathcal{A}_n$, $\mathcal{S}_n$ si $n \neq 4$;
- $\diamond$ $\{\mathrm{id}\}$, $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathcal{A}_4$, $\mathcal{S}_4$.

On en déduit les deux possibilités suivantes

- $\diamond$ $n = 4$ car $\mathcal{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ peut alors correspondre à $(\mathbb{Z}/2\mathbb{Z})^{k-1}$ avec $k = 2$;
- $\diamond$ $n = 6$ car $\mathcal{S}_4$ contient $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Supposons que $n = 4$. Le centralisateur d'une transposition dans $\mathcal{S}_4$ est de cardinal 4 (c'est le groupe V_4) 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 V_4 mais aussi au moins un 4-cycle) : contradiction.

Ainsi $n = 6$. □

1.8.4.2. *Automorphismes extérieurs de $\mathcal{S}_6$, version* 1. — Étudions désormais les automorphismes extérieurs de $\mathcal{S}_6$.

Rappelons l'énoncé suivant :

Théorème 1.8.30. — *Soit $n \geq 5$. Les sous-groupes distingués de $\mathcal{S}_n$ sont* $\{\mathrm{id}\}$, $\mathcal{A}_n$ *et* $\mathcal{S}_n$.

Lemme 1.8.31. — *L'ensemble* $\mathrm{Syl}_5(\mathcal{S}_5)$ *des* 5*-sous-groupes de* Sylow *de* $\mathcal{S}_5$ *est de cardinal* 6.

Lemme 1.8.32. — *Numérotons arbitrairement de* 1 *à* 6 *les éléments de* $\mathrm{Syl}_5(\mathcal{S}_5)$. *Faisons opérer* $\mathcal{S}_5$ *sur* $\mathrm{Syl}_5(\mathcal{S}_5) \simeq \{1, 2, 3, 4, 5, 6\}$ *par conjugaison. La morphisme* $\mathcal{S}_5 \to \mathcal{S}_6$ *associé est injectif. Notons* G *son image.*

Lemme 1.8.33. — *Numérotons arbitrairement de* 1 *à* 6 *les éléments de* $\mathcal{S}_6/\mathrm{G}$. *Faisons opérer* $\mathcal{S}_6$ *sur* $\mathcal{S}_6/\mathrm{G} \simeq \{1, 2, 3, 4, 5, 6\}$ *par translations.*

Le morphisme $\varphi\colon \mathcal{S}_6 \to \mathcal{S}_6$ *associé est un automorphisme.*

Lemme 1.8.34. — *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 du Lemme 1.8.31. — On a $|\mathcal{S}_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$. L'ordre d'un élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ est donc 5. Or 5 est premier donc tout élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Posons $n_5 = \#\mathrm{Syl}_5(\mathcal{S}_5)$. Les théorèmes de Sylow assurent que

$$\begin{cases} n_5 \equiv 1 \bmod 5 \\ n_5 \text{ divise } 2^3 \cdot 3 = 24 \end{cases}$$

Par conséquent n_5 appartient à $\{1, 6\}$.

Supposons que $n_5 = 1$. Alors $\mathcal{S}_5$ a un unique 5-Sylow qui est distingué : contradiction avec le fait que les sous-groupes distingués de $\mathcal{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$. Par suite $n_5 = 6$. □

Démonstration du Lemme 1.8.32. — Soit K le noyau du morphisme de $\mathcal{S}_5$ vers $\mathcal{S}_\mathrm{G}$. Il est contenu dans le stabilisateur de chacun des éléments de $\mathrm{Syl}_5(\mathcal{S}_5)$. L'action de G sur $\mathrm{Syl}_5(\mathcal{S}_5)$ est transitive (théorème de Sylow). Il en résulte que le stabilisateur de chaque élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ a pour cardinal $\frac{120}{6} = 20$. Donc $|\mathrm{K}|$ divise 20. Puisque K est distingué dans $\mathcal{S}_5$, que $|\mathrm{K}|$ divise 20 et que les sous-groupes distingués de $\mathcal{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$, on obtient que $\mathrm{K} = \{\mathrm{id}\}$. □

Démonstration du Lemme 1.8.33. — Soit K' le noyau du morphisme naturel de $\mathcal{S}_6$ dans $\mathcal{S}_{\mathcal{S}_6/\mathrm{G}}$. Il est contenu dans le stabilisateur des éléments de $\mathcal{S}_6/\mathrm{G}$ 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

$$\begin{cases} \mathrm{K}' \lhd \mathcal{S}_6 \\ |\mathrm{K}'| \text{ divise } 120 \\ \text{les sous-groupes distingués de } \mathcal{S}_6 \text{ sont } \{\mathrm{id}, \mathcal{A}_6, \mathcal{S}_6\} \end{cases}$$

d'où $\mathrm{K}' = \{\mathrm{id}\}$. Autrement dit le morphisme φ est injectif. Pour des raisons de cardinalité φ est bijectif. □

Démonstration du Lemme 1.8.34. — Si G avait un point fixe sur $\{1, 2, 3, 4, 5, 6\} \simeq \mathcal{S}$ 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. □

1.8.4.3. *Automorphismes extérieurs de $\mathcal{S}_6$, version* 2. — Rappel : soit G un groupe. Si H est un sous-groupe de G d'incide r, nous obtenons un morphisme de G dans $\mathcal{S}_r$ en faisant agir G sur les classes à gauche modulo H. Plus précisément si $g_1\mathrm{H}$, …, $g_r\mathrm{H}$ désignent les r classes à gauche, nous associons une permutation $\sigma \in \mathcal{S}_r$ à un élément $g \in \mathrm{G}$ en posant

$$(gg_i)\mathrm{H} = g_{\sigma(i)}\mathrm{H}$$

Notons que $i \mapsto \sigma(i)$ est une bijection : l'inverse est donné par l'action de g^{-1}.

Lemme 1.8.35. — *Soit $n \geq 5$. Si* H *est un sous-groupe de $\mathcal{S}_n$ d'indice n qui agit transitivement sur $\{1, 2, \ldots, n\}$, alors le morphisme $\psi\colon \mathcal{S}_n \to \mathcal{S}_n$ associé à l'action de $\mathcal{S}_n$ sur les classes de $\mathcal{S}_n$ modulo* H *est un automorphisme non intérieur.*

Démonstration. — Considérons l'action

$$\mathcal{S}_n \times \mathcal{S}_n/\mathrm{H} \to \mathcal{S}_n/\mathrm{H} \qquad\qquad (g, g_i\mathrm{H}) \mapsto g_{\sigma(i)}\mathrm{H} := (gg_i)\mathrm{H}$$

Par définition un élément g appartient à $\ker\psi$ si et seulement si

$$g \in \bigcap_{i=1}^{n} \mathrm{Stab}(g_i\mathrm{H}).$$

En particulier $\ker\psi$ est contenu dans H. Comme H est d'indice $n \geq 3$ et comme les seuls sous-groupes distingués de $\mathcal{S}_n$ sont d'indice 1 ou 2 ou n on a $\ker\psi = \{\mathrm{id}\}$. Par suite ψ est un automorphisme.

Raisonnons par l'absurde : supposons que ψ soit un automorphisme intérieur. Alors il existe $a \in \mathcal{S}_n$ tel que $\psi(\mathrm{H}) = a\mathrm{H}a^{-1}$. Ainsi $\psi(\mathrm{H})$ agit transitivement sur $\{1, 2, \ldots, n\}$. En effet soient

i, j dans $\{1, 2, \ldots, n\}$; il existe par hypothèse un élément h de H tel que $h(a^{-1}(i)) = a^{-1}(j)$, donc aha^{-1} est un élément de $a\mathrm{H}a^{-1}$ qui envoie i sur j. Remarquons que si $g_i\mathrm{H} = \mathrm{H}$ est la classe de l'élément neutre modulo H, alors $\psi(\mathrm{H})$ fixe i ; en effet si $h \in \mathrm{H}$, alors

$$hg_i\mathrm{H} = h\mathrm{H} = \mathrm{H} = g_i\mathrm{H}$$

et donc n'agit pas transitivement. □

Proposition 1.8.36. — *Il existe un sous-groupe* H *de* $\mathcal{S}_6$ *d'indice* 6 *qui agit transitivement sur*

$$\{1, 2, 3, 4, 5, 6\}.$$

Démonstration. — Considérons l'action de $\mathrm{GL}(2, \mathbb{F}_5)$ sur les six droites du plan $(\mathbb{F}_5)^2$. Cette action est transitive. Elle devient fidèle après avoir quotienté par le sous-groupe des homothéties qui est d'ordre 4. Autrement dit cette action induit un morphisme injectif de $\mathrm{PGL}(2, \mathbb{F}_5)$ dans $\mathcal{S}_6$; l'image H de ce morphisme agit transitivement sur $\{1, 2, 3, 4, 5, 6\}$. L'ordre de $\mathrm{GL}(2, \mathbb{F}_5)$ est $24 \cdot 20 = 5! \cdot 4$. Par conséquent

$$|\mathrm{H}| = |\mathrm{PGL}(2, \mathbb{F}_5)| = 5!$$

Ainsi H est un sous-groupe d'indice 6 dans $\mathcal{S}_6$. □

CHAPITRE 2

GÉOMÉTRIE

2.1. Géométrie euclidienne

2.1.1. 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 2.1.1. — 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 élements du groupe orthogonal $\mathrm{O}(n, \mathbb{R})$ sont des isométries euclidiennes. L'énoncé suivant donne toutes ces isométries :

Théorème 2.1.1. — *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. 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

$$\cos\alpha = \frac{|\langle \overrightarrow{BA}, \overrightarrow{BC} \rangle|}{||\overrightarrow{BA}|| \cdot ||\overrightarrow{BC}||}. \tag{2.1.1}$$

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 2.1.2. — *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*

$$\widehat{g(A)g(B)g(C)} = \widehat{ABC}$$

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 (2.1.1) 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 2.1.3. — *Le groupe $\mathrm{Isom}(\mathbb{R}^n)$ est engendré par les symétries orthogonales par rapport à des hyperplans affines.*

Plus exactement toute isométrie de $\mathbb{R}^n$ est la composée d'au plus $n+1$ telles symétries.

Lemme 2.1.4. — *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 2.1.5. — *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. □

2.1.2. 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 2.1.6. — *Les éléments de* $\mathrm{Isom}(\mathbb{R}^2)$ *sont :*
- *les translations,*
- *les rotations,*
- *les symétries axiales ou réflexions,*
- *les symétries glissées.*

Pour une preuve on renvoie à [**Aud06**] (l'idée est d'étudier les éventuels points fixes avec le Lemme 2.1.5).

Définitions 2.1.2. — 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 2.1.7 (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 2.1.3. — 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 2.1.4. — Un polygone convexe est *régulier* si tous ses côtés sont égaux et tous ses angles sont égaux.

Théorème 2.1.8. — *Soit* $P = A_1A_2 \ldots A_n$ *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*[1] *de* $\left\{e^{2\mathbf{i}\pi k/n} \mid k \in \mathbb{Z}/n\mathbb{Z}\right\}$.

Le point O du théorème est alors le *centre circonscrit* au polygone P.

Démonstration. — Montrons que $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$.

1. 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.

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.

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 [2] 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.

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 $\widehat{A_{i-1}A_iA_{i+1}} = \widehat{A_{i+1}A_i}O + \widehat{OA_iA_{i+1}}$ 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 2.1.9. — *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}. □

2. 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 : $||BC||^2 = ||AC||^2 + ||AB||^2 - 2||AC|| \cdot ||AB|| \cos(\widehat{BAC})$.

2.1.3. 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 2.1.10. — *Les éléments de* $\mathrm{Isom}(\mathbb{R}^3)$ *sont :*
- *les translations,*
- *les rotations,*
- *les rotations glissées* (*appelées aussi vissages*),
- *les symétries orthogonales par rapport à un plan,*
- *les symétries glissées,*
- *les anti-rotations.*

Pour une preuve on renvoie à [**Aud06**].

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 2.1.11. — *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 2.1.12. — *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 2.1.13. — *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 $\gamma_3(0) = \mathrm{idid} = \mathrm{id}$ 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 2.1.14. — *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 2.1.15. — *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. Il suffit de montrer que cette application prend la valeur -1 pour avoir une rotation $g \in \mathrm{G}$ d'angle π.

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

$$\varphi\colon [0,1] \to [-1,1] \qquad\qquad t \mapsto \frac{\mathrm{Tr}(\gamma(t)) - 1}{2}$$

est continue car Tr et γ le sont. Par ailleurs $\varphi(0) = \cos 0 = 1$ et $\varphi(1) = \frac{\mathrm{Tr}(s)-1}{2} \leq 0$. 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 2.1.16. — *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. 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. □

Lemme 2.1.17. — *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 2.1.15 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 2.1.16 qui assure que les retournements engendrent $\mathrm{SO}(3,\mathbb{R})$. □

Démonstration du Théorème 2.1.11. — 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. Les Lemmes 2.1.13 et 2.1.14 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 2.1.17) 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). □

Définitions 2.1.5. — 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 2.1.18. — *Soit P un polyèdre convexe.*

1. *Le nombre de côtés d'une face est au moins* 3.
2. *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.
3. *Une arête appartient à exactement deux faces.*
4. *La somme des angles en un sommet est strictement inférieure à 2π.*

Pour une démonstration de cet énoncé voir par exemple [**Ber77**].

Définitions 2.1.6. — 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.

Le couple (p,q) est appelé *symbole de Schläfli* du polyèdre régulier.

Théorème 2.1.19. — *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	$(3,4)$
isocaèdre 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 2.1.20. — *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

$$\mathrm{Isom}(X) \to \mathrm{Isom}^+(X) \times \mathbb{Z}/2\mathbb{Z} \qquad\qquad g \mapsto \begin{cases} (g,0) \text{ si } g \in \mathrm{Isom}^+(X) \\ (gs_O,1) \text{ sinon} \end{cases}$$

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 2.1.21. — *Le groupe d'isométries du tétraèdre régulier Δ_4 est isomorphe à $\mathcal{S}_4$.*

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 $\mathcal{S} = \{A, B, C, D\}$ l'ensemble des sommets du tétraèdre.

Considérons l'action de $\mathrm{Isom}(\Delta_4)$ sur $\mathcal{S}$. Ainsi

$$\varphi\colon \mathrm{Isom}(\Delta_4) \to \mathcal{S}_4 \qquad\qquad g \mapsto g_{|\mathcal{S}}$$

est un morphisme de groupes.

Si $\varphi(g) = \mathrm{id}_{\mathcal{S}}$, alors g stabilise $\mathcal{S}$ 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 $\mathcal{S}_4$.

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 $\mathcal{S}_4 \subset \mathrm{Isom}(\Delta_4)$ (rappelons que les transpositions engendrent le groupe symétrique).

Finalement φ est un isomorphisme et $\mathrm{Isom}(\Delta_4) \simeq \mathcal{S}_4$.

Le seul sous-groupe d'indice 2 de $\mathcal{S}_n$ 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 2.1.22. — *Le groupe d'isométries directes du cube est isomorphe à $\mathcal{S}_4$.*

Le groupe d'isométries du cube est isomorphe à $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Par dualité le groupe d'isométries directes de l'octaèdre régulier est isomorphe à $\mathcal{S}_4$ et le groupe d'isométries de l'octaèdre régulier est isomorphe à $\mathcal{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

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

$$\varphi\colon \mathrm{Isom}^+(C_6) \to \mathcal{S}_4 \qquad\qquad g \mapsto g_{|\mathcal{D}}$$

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 $s_0 g = \mathrm{id}$ 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 $\ker\varphi = \{\mathrm{id}_{\mathbb{R}^3}\}$ et nous avons l'inclusion $\mathrm{Isom}^+(C_6) \subset \mathcal{S}_4$.

Les transpositions sont toutes réalisées grâce à des retournements d'axes reliant les milieux des arêtes joignant les diagonales).

Par suite $\mathrm{Isom}^+(C_6) \simeq \mathcal{S}_4$.

La seconde assertion découle du fait que le cube admet un centre de symétrie et de la Proposition 2.1.20. □

Proposition 2.1.23. — *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, …, 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

$$\varphi\colon \mathrm{Isom}^+(P_{12}) \to \mathcal{S}_5 \qquad\qquad g \mapsto g_{|\mathcal{C}}$$

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 $\mathrm{Isom}^+(P_{12}) \subset \mathcal{S}_5$.

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 2.1.20 assure que $\mathrm{Isom}(P_{12}) \simeq \mathcal{A}_5 \times \mathbb{Z}/2\mathbb{Z}$. □

2.2. Les sous-groupes finis de $\mathrm{SO}(3,\mathbb{R})$

Références : [**CG17**, chap. 12], [**CG15**, chap. 9], [**Szp09**, p. 434-437]

Leçons possibles :

101 : *Groupe opérant sur un ensemble. Exemples et applications.*

104 : *Groupes abéliens et non abéliens finis. Exemples et applications.*

191 : *Exemples d'utilisation des techniques d'algèbre en géométrie.*

Théorème 2.2.1. — *Tout sous-groupe fini de* $\mathrm{SO}(3,\mathbb{R})$ *est isomorphe à* $\mathbb{Z}/n\mathbb{Z}$, D_{2n}, $\mathcal{A}_4$, $\mathcal{S}_4$ *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*)

— Isom^+(*pyramide de base un polygone régulier à* n *côtés*) $\simeq \mathbb{Z}/n\mathbb{Z}$;
— Isom^+(*double pyramide de base un polygone régulier à* n *côtés*) $\simeq \mathrm{D}_{2n}$;
— Isom^+(*tétraèdre régulier*) $\simeq \mathcal{A}_4$;
— Isom^+(*cube*) $\simeq \mathcal{S}_4$;
— Isom^+(*icosaèdre régulier*) $\simeq \mathcal{A}_5$.

Lemme 2.2.2 (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* $\mathrm{Fix}(g) = \{x \in E \mid g \cdot x = x\}$ *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. — On calcule le cardinal de E de deux façons différentes. D'une part

$$|E| = \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|$$

et d'autre part

$$\begin{aligned} |E| &= \sum_{x \in E} |\mathrm{Stab}_{\mathrm{G}}(x)| = \sum_{\mathcal{O} \in \mathrm{G}\backslash E} \sum_{x \in \mathcal{O}} |\mathrm{Stab}_{\mathrm{G}}(x)| \\ &= \sum_{\mathcal{O} \in \mathrm{G}\backslash E} \sum_{x \in \mathcal{O}} \frac{|\mathrm{G}|}{|\mathcal{O}|} = |\mathrm{G}| \sum_{\mathcal{O} \in \mathrm{G}\backslash E} \sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}|} \\ &= |\mathrm{G}| \sum_{\mathcal{O} \in \mathrm{G}\backslash E} |\mathcal{O}| \cdot \frac{1}{|\mathcal{O}|} = |\mathrm{G}| \sum_{\mathcal{O} \in \mathrm{G}\backslash E} 1 \\ &= |\mathrm{G}| \cdot |\mathrm{G}\backslash E|. \end{aligned}$$

□

Lemme 2.2.3. — *Tout sous-groupe fini de* $\mathrm{SO}(2,\mathbb{R})$ *est cyclique.*

Plus particulièrement tout sous-groupe fini de $\mathrm{SO}(2,\mathbb{R})$ *est monogène, engendré par la rotation d'angle* $\frac{2\pi}{n}$ *où* n *est le cardinal du groupe.*

Démonstration. — Commençons par rappeler que $\mathbb{R}/2\pi\mathbb{Z}$ et $\mathrm{SO}(2,\mathbb{R})$ sont isomorphes :

$$\mathbb{R}/2\pi\mathbb{Z} \xrightarrow{\sim} \mathrm{SO}(2,\mathbb{R}) \qquad\qquad \vartheta \mapsto \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}$$

Nous sommes donc ramenés à étudier les sous-groupes finis de $\mathbb{R}/2\pi\mathbb{Z}$.

Soient H un sous-groupe fini de $\mathbb{R}/2\pi\mathbb{Z}$, $p\colon \mathbb{R} \to \mathbb{R}/2\pi\mathbb{Z}$ la projection canonique et $\mathrm{G} = p^{-1}(\mathrm{H})$. On peut vérifier que G est un sous-groupe discret de $\mathbb{R}$. En effet supposons G dense ;

la restriction de p à $[0,1]$ étant injective l'image de $\mathrm{G} \cap [0,1]$ est une partie infinie de H : contradiction. La Proposition 1.3.24 assure donc que G est monogène.

Soit α un générateur de G. Le théorème de LAGRANGE assure que $n\alpha \equiv 0 \pmod{2\pi}$ où n est le cardinal de H. Il existe donc un entier k tel que $\alpha = \frac{2k\pi}{n}$. D'après l'identité de Bezout le groupe engendré par α est aussi le groupe d'ordre $\frac{n}{d}$ engendré par $\frac{2\pi d}{n}$ où d est le pgcd de k et n. Il en résulte que $d = \pm 1$, *i.e.* que tout sous-groupe fini d'ordre n de $\mathbb{R}/2\pi\mathbb{Z}$ est monogène, engendré apr la classe modulo 2π de $\frac{2\pi}{n}$. □

Esquisse de démonstration du Théorème 2.2.1. — 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 2.2.2) 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 2.2.3 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 $|\mathrm{G}| = |\mathcal{S}_4| = 24$;
- ◇ $(n_1, n_2, n_3) = (2,3,5)$ 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

$$\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} = 1 + \frac{2}{n} \tag{2.2.1}$$

Par définition un pôle est fixé par au moins l'identité et une autre rotation donc $n_1 \geq 2$. La condition (2.2.1) 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 $\mathcal{S}_4$).

□

Remarque 2.2.1. — Le groupe $\mathcal{S}_4$ intervient à la fois comme Isom^+(cube) et comme Isom(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)

2.3. Géométrie affine

2.3.1. 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 2.3.1. — 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 2.3.1 (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 2.3.2. — 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 $\mathcal{F}=\{A+v\,|\,v\in F\}$.

En particulier nous appelons *droite affine* un sous-espace affine de dimension 1 et *plan affine* un sous-espace affine de dimension 2.

Lemme 2.3.2. — *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 $\mathcal{F}_i=\{A+v\,|\,v\in F_i\}$ 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 2.3.3. — 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 2.3.1. — 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 $(AB)=\{A+\lambda\overrightarrow{AB}\,|\,\lambda\in\Bbbk\}$.

Définition 2.3.4. — Deux sous-espaces affines sont *parallèles* s'ils ont même direction.

Définition 2.3.5. — Soient $\mathcal{A}$ un espace affine et O un point de $\mathcal{A}$. L'application

$$E\to\mathcal{A},\qquad\qquad v\mapsto O+v$$

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 2.3.2. — Un espace vectoriel E possède une structure canonique d'espace affine obtenue en faisant agir $(E, +)$ sur lui-même par translations.

Remarque 2.3.1. — 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 2.3.6. — 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 2.3.3. — *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 2.3.4. — *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. □

2.3.2. Groupe affine. —

Lemme 2.3.5. — *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 2.3.6. — *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 2.3.5 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 2.3.5). 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 2.3.2. — 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.

2.3.3. 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 2.3.7 (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 2.3.3. —

Cet énoncé est propre au cas réel.

Proposition 2.3.8. —

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

- $\diamond$ $x_n^- \leq x \leq x_n^+$ pour tout $n \in \mathbb{N}$;
- $\diamond$ $\lim\limits_{n\to+\infty} x_n^+ = x$;
- $\diamond$ $\lim\limits_{n\to+\infty} x_n^- = x$.

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 2.3.9. — *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 2.3.7. — 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 2.3.9 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.* $(OA) /\!\!/ (BC)$ et $(OB) /\!\!/ (AC)$. 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 $B \in \mathcal{A} \setminus (OA)$. 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 2.3.8. □

CHAPITRE 3

GROUPES ABÉLIENS DE TYPE FINI

Le théorème chinois fournit des exemples de groupes abéliens finis qui se décomposent en produit de groupes cycliques plus simples. Par exemple le groupe $\mathbb{Z}/6\mathbb{Z}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. D'autre part $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$ est un groupe abélien d'ordre 4 qui n'est pas cyclique puisque ses éléments sont d'ordre au plus 2 ; en particulier il n'est pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Dans ce chapitre nous nous intéressons à l'existence et l'unicité de la décomposition, à isomorphisme près, d'un groupe abélien fini en un produit de groupes cycliques. Nous donnons aussi un théorème de structure pour les groupes abéliens de type fini.

3.1. Définitions et notations

Rappelons que la loi d'un groupe abélien G sera toujours notée additivement et l'élément neutre sera désigné par 0. L'opposé d'un élément g de G est noté $-g$ et si n est un entier naturel, ng se définit par récurrence

$$0g := 0 \qquad\qquad ng := g + (n-1)g.$$

Posons alors $(-n)g := -(ng)$. Autrement dit nous venons de définir une action de l'anneau $\mathbb{Z}$ sur le groupe abélien G.

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 3.1.1. — Un groupe engendré par un élément est
- ◇ soit réduit à l'élément neutre,
- ◇ soit égal à $\mathbb{Z}$,
- ◇ soit cyclique et fini.

Convention : le système vide engendre le groupe réduit à l'élément neutre.

Exemple 3.1.2. — L'ensemble

$$\mathrm{G} = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}\}$$

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.

3.2. Groupes abéliens libres de type fini

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 3.2.1 (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 3.2.2. — Le sous-ensemble de $\mathbb{R}$ défini par

$$A = \{a + b\sqrt{2} + c\sqrt{3} \,|\, a, b, c \in \mathbb{Z}\}$$

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 3.2.3. — Le sous-ensemble de $\mathbb{C}$ appelé aussi entiers de Gauss

$$\mathbb{Z}[\mathbf{i}] = \{a + \mathbf{i}b \,|\, a,\, b \in \mathbb{Z}\}$$

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 3.2.1. — *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 $\widetilde{\varphi}(e_1)$, $\widetilde{\varphi}(e_2)$, …, $\widetilde{\varphi}(e_r)$ 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, $\sum_{j=1}^{r} \lambda_j e_j$ 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 3.2.2. — *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 3.2.3. — *Un sous-groupe d'un groupe libre de rang r est libre. Son rang s est au plus égal à r.*

Exemple 3.2.4. — 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 3.2.4).

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

$$\mathrm{M} \to \mathbb{Z}, \qquad\qquad x \mapsto x_r.$$

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

  $$\mathrm{M}_{r-1} \times \mathbb{Z} \to \mathrm{M}, \qquad\qquad (x, n) \mapsto x + nz$$

  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. En effet pour toute relation

$$\sum_{i=1}^{r} \lambda_i a_i = 0$$

dans 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 3.2.5. — 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 3.2.3 :

Théorème 3.2.4. — *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, …, e_s *de* $\mathcal{B}$ *et des entiers* a_1, a_2, …, a_s *non nuls tels que*

1. *les éléments* a_1e_1, a_2e_2, …, 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, …, 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*

$$\mathbb{Z}^{r-s} \times \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_s\mathbb{Z}$$

Démonstration. — 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 $x_1 = a_1e_1$ et $f(e_1) = 1$. Montrons que $\mathrm{L} \simeq \mathbb{Z} \times \ker f$. Considérons le morphisme

$$\phi\colon \mathbb{Z} \times \ker f \to \mathrm{L} \qquad (a, x) \mapsto ae_1 + x.$$

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

$$\varphi\colon \mathbb{Z} \times (\mathrm{M} \cap \ker f) \to \mathrm{M} \qquad (a, x) \mapsto ax_1 + x$$

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, …, a_s tels que $(a_2e_2, a_3e_3, \ldots, a_se_s)$ 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 $(a_1e_1, a_2e_2, \ldots, a_se_s)$ 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 $(a_1e_1, a_2e_2, \ldots, a_se_s)$)

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 gcd 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 $n \times n$ 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 $B_{IJ} = A_IQ_J$ 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. □

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 3.2.4

assure que le groupe G est isomorphe à

$$\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_s\mathbb{Z} \times \mathbb{Z}^{r-s}.$$

3.3. 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.

Définition 3.3.1. — Soit G un groupe abélien fini (noté additivement). Soit I l'ensemble des entiers d tels que $dg = 0$ pour tout $g \in \mathrm{G}$. On vérifie immédiatement que I est un idéal de $\mathbb{Z}$. Soit e l'entier ≥ 0 tel que $I = e\mathbb{Z}$. On dit que e est l'*exposant* de G.

Remarque 3.3.1 (Exposant et ordre)**.** — Soit G un groupe fini d'ordre n. Le théorème de Lagrange assure que $ng = 0$ pour tout g dans G (en effet si g un élément de G, alors $|\langle g\rangle|$ divise $|\mathrm{G}|$ autrement dit l'ordre de g divise n). Par suite l'exposant e de G divise l'ordre n de G.

Notons que cette relation de divisibilité peut être stricte : le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ a pour exposant 2 et pour ordre 4.

Remarque 3.3.2 (Autre expression de l'exposant)**.** — Pour tout $g \in \mathrm{G}$ on désigne par 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 [1] Puisque l'ensemble I des entiers d tels que $dg = 0$ pour tout $g \in \mathrm{G}$ est l'intersection des I_g pour g parcourant G, l'exposant de G est le ppcm des ordres des éléments de G.

Proposition 3.3.1. — *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 et sans torsion. Puisque G est abélien de type fini le Théorème 3.2.4

$$\mathrm{G} \simeq \mathbb{Z}^r \times \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_s\mathbb{Z}$$

1. Soit G un groupe et soit g un élément de G. Soit φ l'unique morphisme de $\mathbb{Z}$ dans G qui envoie 1 sur g. Nous avons $\varphi(n) = g^n$ pour tout $n \in \mathbb{Z}$ si bien que $\operatorname{im}\varphi = \langle g\rangle$. Le noyau de φ est un sous-groupe de $\mathbb{Z}$; il s'écrit donc $d\mathbb{Z}$ pour un unique $d \in \mathbb{N}$ (Proposition 1.1.5). Il s'en suit que φ induit un isomorphisme entre $\mathbb{Z}/d\mathbb{Z}$ et $\langle g\rangle$. L'ordre de g est infini si $d = 0$ et égal à d sinon.

où $r \geq 0$, $a_j \geq 0$ pour tout $1 \leq j \leq s$ et n_{i+1} divise n_i 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 $|G| = a_1 a_2 \ldots a_s < \infty$. □

Théorème 3.3.2. — *Soit* G *un groupe abélien. Soit* d *un entier non nul tel que* $d\mathrm{G} = \{0\}$ (*autrement dit tous les éléments de* G *ont un ordre qui divise* d).

Supposons de plus que $d = d_1 d_2$ *avec* d_1, d_2 *premiers entre eux. Notons* G_{d_1} (*resp.* G_{d_2}) *le sous-groupe des éléments de* G *annulés par* d_1 (*resp.* d_2).

Alors G *est isomorphe au produit des deux sous-groupes* G_{d_1} *et* G_{d_2} *:*

$$\mathrm{G} \simeq \mathrm{G}_{d_1} \times \mathrm{G}_{d_2}.$$

Lemme 3.3.3. — *Soit* G *un groupe abélien fini. Soit* p *un nombre premier qui divise l'ordre* $|\mathrm{G}|$ *de* G.

Alors G *contient un élément d'ordre* p.

Démonstration. — Soit e l'exposant de G.

L'ordre $|\mathrm{G}|$ de G divise e (Remarque 3.3.1). Par suite p divise e et G contient un élément g dont l'ordre est divisible par p. On conclut en remarquant que si l'ordre de g est pq, alors qg est d'ordre p. □

Corollaire-Définition 3.3.4. — *Soit* G *un groupe abélien fini d'ordre* d *dont la décomposition en facteurs premiers est* $d = \prod_{i=1}^{\ell} p_i^{n_i}$.

Alors

$$\mathrm{G} \simeq \mathrm{G}_1 \times \mathrm{G}_2 \times \ldots \times \mathrm{G}_\ell$$

où G_i *est le sous-groupe des éléments annulés par* $p_i^{n_i}$, $i = 1, \ldots, \ell$.

On dit que c'est la décomposition primaire de G.

La décomposition primaire de G permet de voir G comme le produit de ses sous-groupes de Sylow (qui sont tous distingués puisque G est abélien).

Exemple 3.3.1. — 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

$$\square\ \square\ \ldots\ \square\ \square$$

   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 3.3.5. — *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 3.3.2. — 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 3.3.5 nous aurons besoin de l'énoncé suivant :

Lemme 3.3.6. — *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 G est y. Puisque $p^m y$ est nul dans G/H, $p^m z$ appartient à H. Par conséquent 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 3.3.5. — 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 $\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^{N_2}\mathbb{Z} \times \mathbb{Z}/p^{N_3}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{N_s}\mathbb{Z}$. Comme p^r est l'ordre maximal d'un élément de G, nous avons l'inégalité $r \geq N_2$.

Pour tout $2 \leq j \leq s$, le Lemme 3.3.6 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

$$\sigma \colon \mathbb{Z}/p^{N_2}\mathbb{Z} \times \mathbb{Z}/p^{N_3}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{N_s}\mathbb{Z} \to \mathrm{G} \quad (a_2, a_3, \ldots, a_s) \mapsto a_2y_2 + a_3y_3 + \ldots + a_sy_s$$

est injectif ; sa composée avec le morphisme quotient $\mathrm{G} \to \mathrm{G}/\mathrm{H}$ est un isomorphisme.

L'isomorphisme recherché ϕ entre $\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^{N_2}\mathbb{Z} \times \mathbb{Z}/p^{N_3}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{N_s}\mathbb{Z}$ 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 surfjectif en utilisant que sa composée avec la surjection canonique $\mathrm{G} \to \mathrm{G}/\mathrm{H}$ est surjective ;
- ◇ ϕ est injective 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).

Posons $N_1 = r$ et $y_1 = x$. Reste à montrer l'unicité de la partition $n = N_1 + N_2 + \ldots + N_s$, $N_1 \geq N_2 \geq \ldots \geq N_s$. Sa donnée est équivalente à celle du tableau suivant

□ □ … □ □ □
□ □ … □ □
⋮
□ … □
□

dont la j-ème ligne à N_j cases. La j-ème ligne représente l'action de la multiplication par p sur le sous-groupe engendré par y_j d'ordre p^{N_j}. La première colonne à gauche représente donc le

noyau de la multiplication par p sur G. Nous en déduisons que le nombre de lignes, *i.e.* s, est déterminé par ce noyau. On peut vérifier que

$$ps = |p^{n-1}\mathrm{G}|.$$

De manière analogue le noyau de la multiplication par p^k sur G est représenté par les k premières colonnes. Si s_k est le nombre de lignes de longueur au moins k, on peut vérifier que $s_1 = s$ et

$$(p^k - p^{k-1})s_k = |p^{n-k}\mathrm{G}| - |p^{n-k+1}\mathrm{G}|$$

□

Ainsi soit G un groupe abélien fini d'ordre d. Considérons la décomposition de d en facteurs premiers

$$d = \prod_{i=1}^{\ell} p_i^{n_i}.$$

Le Théorème 3.3.2 assure que G admet une décomposition de la forme

$$\mathrm{G}_1 \times \mathrm{G}_2 \times \ldots \times \mathrm{G}_\ell$$

où chaque G_i a, d'après le Théorème 3.3.5, une décomposition associée à une unique partition $N_i = N_{i,1} + N_{i,2} + \ldots + N_{i,s_i}$, $N_{i,1} \geq N_{i,2} \geq \ldots \geq N_{i,s_i}$.

En écrivant les entiers sous forme d'un tableau

$$\begin{array}{r} p_1^{N_{1,s_1}}|\ldots|\ldots|\ldots|\ldots|p_1^{N_{1,2}}|p_1^{N_{1,1}} \\ p_2^{N_{2,s_2}}|\ldots|\ldots|p_2^{N_{2,2}}|p_2^{N_{2,1}} \\ \vdots \\ p_\ell^{N_{\ell,s_\ell}}|\ldots|p_\ell^{N_{\ell,2}}|p_\ell^{N_{\ell,1}} \end{array}$$

et en recombinant suivant les colonnes de ce tableau, nous obtenons en appliquant le théorème chinois une décomposition de G en un produit

$$\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_s\mathbb{Z}$$

où a_j est le produit des entiers non nuls situés sur la j-ème colonne du tableau ; en particulier $a_1|a_2|\ldots|a_s$. Le tableau ne dépendant que de G la suite $a_1, a_2, \ldots, a_s$ est entièrement déterminée par G. Les *facteurs invariants* du groupe G sont les éléments de cette suite.

En écrivant $a_i = p_1^{\alpha_{i,1}} p_2^{\alpha_{i,2}} \ldots p_r^{\alpha_{i,r}}$ avec p_i premiers, $\alpha_{1,j} \geq \alpha_{2,j} \geq \ldots \geq \alpha_{\ell,j}$, les $p_i^{\alpha_{i,j}}$ sont appelés les *diviseurs élémentaires* de G.

Exemple 3.3.3. — Soit G le groupe de type fini dont les facteurs invariants sont $d_1 = 30$, $d_2 = 15$, $d_3 = 3$ et $d_4 = 3$.

Notons que $d_1 = 5 \times 3 \times 2$ et $d_2 = 5 \times 3$.

Par suite les diviseurs élémentaires sont 5, 5, 3, 3, 3, 3 et 2.

Exemple 3.3.4. — 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.

Ordonnons les diviseurs élémentaires comme suit

$$\begin{array}{r} 2 \mid 2 \mid 2^3 \mid 2^5 \\ 3 \mid 3^3 \\ 5 \end{array}$$

Les facteurs invariants de G sont donc

$$d_1 = 2^5 \times 3^3 \times 5 = 4320, \qquad d_2 = 2^3 \times 3 = 24, \qquad d_3 = 2 \qquad d_4 = 2.$$

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 3.3.5. — 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

$$\mathbb{Z}/162\mathbb{Z} \simeq \mathbb{Z}/3^4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad\qquad \mathbb{Z}/21\mathbb{Z} \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

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. Ordonnons-les comme suit

$$\begin{array}{r} 3 \mid 3^4 \\ 7 \\ 2 \end{array}$$

et les facteurs invariants sont $d_1 = 3^4 \times 7 \times 2 = 1134$ et $d_2 = 3$. Il s'en suit que

$$\mathrm{G} \simeq \mathbb{Z}^2 \times \mathbb{Z}/1134\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

Exemple 3.3.6. — 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. Ordonnons-les comme suit

$$\begin{array}{r} 2 \mid 2 \mid 2^2 \mid 2^3 \\ 3 \mid 3 \mid 3 \\ 5 \mid 5^2 \end{array}$$

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 3.3.7. — ◇ 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. Ordonnons-les comme suit

$$\begin{array}{c} 2 \mid 2^3 \\ 3^2 \mid 3^3 \\ 5 \end{array}$$

Les facteurs invariants de G sont donc $2 \times 3^2 = 18$ et $2^3 \times 3^3 \times 5 = 1080$.

◇ 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 :

$${}^{\mathbb{Z}}\!/_{8\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{9\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$$
$${}^{\mathbb{Z}}\!/_{8\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$$
$${}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{4\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{9\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$$
$${}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{4\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$$
$${}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{9\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$$
$${}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{3\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$$

Théorème 3.3.7. — *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

$$\mathrm{G} \to \mathrm{L} \qquad\qquad x \mapsto ax$$

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 $\mathrm{L} \cap \mathrm{T} = \{0\}$ donc ax est nul. L'application

$$\mathrm{G}/\mathrm{T} \to \mathrm{L} \qquad\qquad \overline{x} \mapsto ax$$

est bien définie et injective. Le groupe G/T s'identifie à un sous-groupe de L qui est libre (Théorème 3.2.3). Or nous avons aussi un morphisme injectif de L dans G/T induit par l'application quotient. D'après la Proposition 3.2.1 les groupes L et G/T sont libres et de même rang. Soient x_1, x_2, …, x_s des éléments de G dont les classes $\overline{x_1}$, $\overline{x_2}$, …, $\overline{x}_s$ forment une $\mathbb{Z}$-base de G/T. Considérons le morphisme

$$\phi\colon \mathrm{T} \times \mathbb{Z}^s \to \mathrm{G} \qquad\qquad (x, n_1, n_2, \ldots, n_s) \mapsto x + \sum_{i=1}^{s} n_i x_i.$$

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. □

CHAPITRE 4

REPRÉSENTATIONS DES GROUPES

4.1. 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 fidèle, 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 4.1.1. — 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 4.1.2. — 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 4.1.3. — 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 $\mathcal{S}_4$ 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 4.1.4. — 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 4.1.5. — Le groupe des quaternions a pour présentation

$$\mathbb{H}_8 = \langle i,\, j \mid i^4 = j^4 = 1,\, i^2 = j^2,\, i^{-1} j i = j^{-1} \rangle.$$

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 4.1.6 (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 $u = \rho(1)$ 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 4.1.7 (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 $n \in \mathbb{Z}$ sur $v \in V$ étant donnée par $n \cdot v = u^n(v)$.

Réciproquement si V est une représentation de $\mathbb{Z}/n\mathbb{Z}$ 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 4.1.1. — Dans les Exemples 4.1.6 et 4.1.7 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 4.1.8 (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 4.1.9 (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 $\mathrm{Hom}(V_1, V_2)$ *i.e.* $(\mathcal{L}(V_1, V_2), \rho)$ sur le $\Bbbk$-espace vectoriel $\mathcal{L}_\Bbbk(V_1, V_2)$ 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

$$\begin{aligned} \rho(gh)(f) &= \rho_2(gh) \circ f \circ \rho_1((gh)^{-1}) \\ &= \rho_2(g) \circ \Big(\rho_2(h) \circ f \circ \rho_1(h^{-1})\Big) \circ \rho_1(g^{-1}) \\ &= \rho(g)\big(\rho(h)(f)\big) \end{aligned}$$

Il est intéressant de voir $\rho(g)(f)$ comme l'unique application linéaire $V_1 \to V_2$ faisant commuter le diagramme

$$\begin{array}{ccc} V_1 & \xrightarrow{f} & V_2 \\ {\scriptstyle g}\big\downarrow{\scriptstyle \simeq} & & {\scriptstyle g}\big\downarrow{\scriptstyle \simeq} \\ V_1 & \xrightarrow[g\cdot f]{} & V_2 \end{array}$$

Cette opération munit $\mathcal{L}_k(V_1, V_2)$ d'une structure de G-espace vectoriel.

Exemple 4.1.10 (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

$$\rho^*(g) = {}^{\mathrm{t}}\rho(g)^{-1} \in \mathrm{GL}(V^*).$$

4.1.1. — 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 4.1.11. — En reprenant les notations de l'Exemple 4.1.6 nous avons $\dim C(\lambda) = 1$ pour tout $\lambda \in \mathbb{C}^*$.

Exemple 4.1.12. — Si n est impair, alors le groupe diédral

$$\mathrm{D}_{2n} = \langle r,\, s \,|\, s^2 = r^n = srs^{-1}r = \mathrm{id} \rangle$$

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. Nous pouvons les définir comme suit

$$r \mapsto \begin{pmatrix} \zeta^\ell & 0 \\ 0 & \zeta^{-\ell} \end{pmatrix} \qquad\qquad s \mapsto \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

où ζ désigne une racine primitive $n$ième de l'unité et $1 \leq \ell \leq n-1$. Deux telles représentations sont isomorphes seulement pour ℓ_1 et ℓ_2 telles que $\ell_1 + \ell_2 = n$.

Exemple 4.1.13. — Le sous-espace vectoriel

$$V^{\mathrm{G}} = \{v \in V \,|\, \forall\, g \in \mathrm{G} \quad g \cdot v = v\}$$

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 4.1.14. — Si $V = \Bbbk^n$ est la représentation du groupe symétrique $\mathcal{S}_n$, alors l'hyperplan

$$V_0 = \Big\{(x_1, \ldots, x_n) \in V \,|\, \sum_{i=1}^{n} x_i = 0\Big\}$$

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 4.1.15 (Construction d'une représentation de dimension 2 de $\mathcal{S}_3$)***.*** —

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 $\mathcal{S}_3$ pour construire notre représentation de $\mathcal{S}_3$. Un élément de D_6 laisse fixe l'ensemble $\{A, B, C\}$ et fournit un morphisme de groupes φ de D_6 dans le groupe des permutations $\mathcal{S}_{\{A,B,C\}}$ 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 $\varphi\colon \mathrm{D}_6 \to \mathcal{S}_{\{A,B,C\}}$ 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 $\psi\colon \mathcal{S}_3 \xrightarrow{\simeq} \mathcal{S}_{\{A,B,C\}}$. Nous obtenons un morphisme de groupes de $\mathcal{S}_3$ dans $\mathrm{GL}(2, \mathbb{C})$ en composant $\varphi^{-1} \circ \psi\colon \mathcal{S}_3 \to \mathrm{D}_6$ avec l'injection de D_6 dans $\mathrm{GL}(2, \mathbb{C})$. Ce morphisme fait de $\mathbb{C}^2$ une représentation de $\mathcal{S}_3$.

Remarque 4.1.2. —

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 4.1.16. —

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).

Si V et W sont des représentations de G, nous pouvons former les représentations suivantes :

- $V \oplus W$ pour $\rho(g) = (\rho_V(g), \rho_W(g))$;
- $V \otimes W$ pour $\rho(g) = \rho_V(g) \otimes \rho_W(g)$;
- V^* pour $\rho^*(g) = {}^{\mathrm{t}}\rho(g^{-1})$;
- $\mathrm{Hom}_{\Bbbk}(V, W) = V^* \otimes W$ pour $\rho(g)(u) = \rho_W(g) \circ u \circ \rho_V(g^{-1})$;
- T^dV, Λ^dV et S^dV sont aussi des représentations de G (on associe à $g \in \mathrm{G}$ les endomorphismes $(\rho_V(g))^{\otimes d}$, $\Lambda^d(\rho_V(g))$ et $S^d(\rho_V(g))$). Si $\Bbbk$ est de caractéristique distincte de 2, nous avons

$$V \otimes V \simeq \Lambda^2 V \oplus S^2 V.$$

4.1.2. Représentations irréductibles

Définition 4.1.1. — 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 4.1.17. — 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 4.1.18. — 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 4.1.7). 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 4.1.19. — Les représentations du groupe diédral (Exemple 4.1.12) sont irréductibles.

Exemple 4.1.20. — 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 4.1.21. — 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 4.1.22. — La représentation de $\mathcal{S}_3$ sur $\mathbb{C}^2$ de l'Exemple 4.1.15 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 4.1.23. — 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 $\mathbb{C}(\lambda)$ de l'Exemple 4.1.6. 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 $\mathbb{C}(\lambda)$ 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 $\mathbb{C}(\lambda_i)$ en tant que représentation de $\mathbb{Z}$. Nous en déduisons que V est, en tant que représentation de $\mathbb{Z}$, isomorphe à $\bigoplus_{i=1}^{d} \mathbb{C}(\lambda_i)$.

Remarques 4.1.3. —

(i) Dire que V est isomorphe à $\bigoplus_{i=1}^{d} \mathbb{C}(\lambda_i)$ 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 $\bigoplus_{i=1}^{d} \mathbb{C}(\lambda_i)$ 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 $V \simeq \bigoplus_{i=1}^{r} m_i \mathbb{C}(\lambda_i)$.

(iii) Si u n'est pas diagonalisable, la représentation V ne se décompose pas comme une somme directe de représentations irréductibles.

Exemple 4.1.24. — La représentation de permutation de $\mathcal{S}_n$ sur $\Bbbk^n$ n'est pas irréductible puisque la droite engendrée par $(1, 1, \ldots, 1)$ est stable sous $\mathcal{S}_n$ (*voir* Exemple 4.1.14).

Plus généralement une représentation de permutation de dimension finie $\neq 1$ n'est jamais irréductible.

Exemple 4.1.25. — 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 4.1.26. — Combinons les Exemples 4.1.17 et 4.1.25. 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 4.1.4. — 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.

4.1.3. 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 4.1.27. — 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 4.1.1. — *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 4.1.2. — *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 4.1.1 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 4.1.5. — 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 4.1.1. — 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 4.1.3 (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* $\rho_V=\rho_W$*, si* V *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

$$G\hookrightarrow\mathrm{Bij}(\mathrm{G}),\qquad\qquad g\mapsto(x\mapsto gx)$$

avec la représentation de permutation pour obtenir la représentation régulière (Exemple 4.1.4)

$$\rho_R \colon \mathrm{G} \to \mathrm{Bij}(\mathrm{G}) \to \mathrm{GL}(\Bbbk^{\mathrm{G}})$$

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 4.1.2 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

$$u \colon \Bbbk^{\mathrm{G}} \to V \qquad\qquad \Big(f \colon \mathrm{G} \to \Bbbk\Big) \mapsto \sum_{g\in\mathrm{G}} f(g)\rho(g)(v_0)$$

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 4.1.4. — *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 4.1.6. — Il y a des énoncés plus précis lorsque $\Bbbk$ est algébriquement clos.

Proposition 4.1.5. — *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 4.1.2.

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

$$\sum_j u_j = \sum_j p_1 \circ u'_{|W_j} \circ q_j \circ u_{|V_1} = p_1 \circ \Big(\sum_j p_1 \circ u'_{|W_j} \circ q_j\Big) \circ u_{|V_1} = p_1 \circ u' \circ u_{|V_1} = \mathrm{id}_{V_1}.$$

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 $q_1 \circ u_{|V_1} : V_1 \to W_1$ et $p_1 \circ u'_{|W_1} : W_1 \to V_1$ 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

$$(\mathrm{id}_W - q_1)u_{|\bigoplus_{i\geq 2} V_i}\colon \bigoplus_{i\geq 2} V_i \to \bigoplus_{j\geq 2} W_j$$

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 4.1.7. — Sous les hypothèses de la Proposition 4.1.5 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.

4.2. 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

$$\chi_\rho \colon \mathrm{G} \to \Bbbk, \qquad\qquad g \mapsto \mathrm{tr}(\rho(g)).$$

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 4.2.1. — Considérons la représentation de permutation. Reprenons les notations de l'Exemple 4.1.4. 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 4.2.2. — Considérons la représentation régulière. Reprenons les notations de l'Exemple 4.1.4. 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 4.2.3. — 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

$$\chi(r^k) = 2\cos\left(\frac{2k\pi}{n}\right), \qquad\qquad \chi(r^k s) = 0.$$

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 4.2.4. — Le groupe $\mathcal{S}_3$ 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 $\mathcal{S}_3$ 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 $\mathcal{S}_n$ sont en bijection avec les partitions de n (Proposition 1.2.4)

$$n = k_1 + k_2 + \ldots + k_r, \quad r \in \mathbb{N}, \quad 1 \leq k_1 \leq k_2 \leq \ldots \leq k_r$$

une telle partition correspondant aux produits de cycles à supports disjoints d'ordre k_1, k_2, …, k_r. Sur la classe de conjugaison correspondante le caractère de la représentation standard de $\mathcal{S}_n$ dans $\mathbb{C}^n$ vaut $\max\{i \,|\, k_i = 1\}$ (c'est le nombre de points fixes de la permutation).

Exemple 4.2.5 (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 $\Bbbk^{\times}$[1]. 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 4.2.6 (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 4.1.17). 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 4.2.5). 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 $|\mathrm{Hom}(\mathrm{G}, \mathbb{C}^{\times})| = |\mathrm{G}|$.

---

1. 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 (resp. V') comme une représentation de G via ρ (resp. 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.

Notons qu'on peut démontrer cette égalité sans faire appel à la théorie des représentations tout en étant beaucoup plus précis :

Lemme 4.2.1. —
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 3.2.4 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

$$\mathrm{G} \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}.$$

Pour tout 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 $h_{\left|\mathbb{Z}/d_i\mathbb{Z}\right.} = h_i$ pour tout i, à savoir

$$(x_1, x_2, \ldots, x_r) \mapsto \prod_i h_i(x_i);$$

on peut vérifier que $(h_1, h_2, \ldots, h_r) \mapsto h$ établit un isomorphisme entre

$$\mathrm{Hom}\left(\mathbb{Z}/d_1\mathbb{Z}, \mathbb{C}\right) \times \mathrm{Hom}\left(\mathbb{Z}/d_2\mathbb{Z}, \mathbb{C}\right) \times \ldots \mathrm{Hom}\left(\mathbb{Z}/d_r\mathbb{Z}, \mathbb{C}\right)$$

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 4.2.2. — *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 4.1.9. 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 4.1.10, 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 $\langle f,\, \varepsilon_g\rangle = \frac{1}{|\mathrm{G}|}f(g^{-1})$ donc cette forme est non dégénérée.

Théorème 4.2.3. — *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 4.2.4. — *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

$$\mathrm{Hom}_{\mathrm{G}}(V, W) = \{u \in \mathrm{Hom}(V, W) \,|\, \forall\, h \in \mathrm{G} \quad u \circ \rho_V(h) = \rho_W(h) \circ u\}.$$

Pour tout élément u de $\mathrm{Hom}(V, W)$ et pour tout $h \in \mathrm{G}$ nous avons

De plus 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 4.2.4 assure que

$$\langle\chi_V,\chi_W\rangle=\mathrm{tr}(\pi)=\begin{cases}0 \text{ si } V \text{ et } W \text{ ne sont pas isomorphes}\\ \Bbbk \text{ si } V \text{ et } W \text{ sont isomorphes}\end{cases}$$

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 4.2.5. — *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 4.1.3) 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 4.1.3) 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 4.2.6. — *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.

Théorème 4.2.7. — *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 4.2.5).

Le Théorème 4.2.3 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 4.2.8. — *Notons $\rho_1, \rho_2, \ldots, \rho_\ell$ 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 4.2.1. — 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 4.2.2. — 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 4.1.17 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 4.2.9. — *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 4.2.3. — Cet énoncé n'est plus vrai en général (il existe des p-groupes non abéliens).

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. □

4.3. 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

$$\langle \chi_\rho, \chi_{\rho'} \rangle = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \overline{\chi_\rho(g)} \chi_{\rho'}(g). \tag{4.3.1}$$

De plus si $\chi_1, \chi_2, \ldots, \chi_\ell$ sont les caractères des représentations irréductibles de G, le Corollaire 4.2.6 assure que

$$\sum_{i=1}^{\ell} \overline{\chi_i(C)} \chi_i(C') = \begin{cases} \frac{|\mathrm{G}|}{|C|} \text{ si } C = C' \\ 0 \text{ sinon} \end{cases} \tag{4.3.2}$$

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

$$\{g \in \mathrm{G} \,|\, \chi_\rho(g) = \chi_\rho(e)\} = \ker \rho \lhd \mathrm{G}.$$

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 4.2.6 c'est une table carrée. Les différentes relations obtenues précédemment se traduisent comme suit :

- ◇ 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* (4.3.2)) ;
- ◇ les lignes sont orthogonales et de norme au carré $|\mathrm{G}|$ pour le produit scalaire hermitien pondéré par le cardinal des classes de conjugaison (4.3.1) ;
- ◇ la somme des lignes pondérées par les dimensions $\chi(e)$ est la ligne $|\mathrm{G}|\ 0\ 0\ \ldots\ 0$.

Remarque 4.3.1. — Ces propriétés permettent de remplir la table des caractères en n'en connaissant qu'une partie.

Exemple 4.3.1. — 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 :

caractères \ classes de conjugaison	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 4.3.2 (Sous-groupes distingués)***.*** — Cette table peut être utilisée pour étudier les sous-groupes distingués de G. Un tel sous-groupe est réunion de classes de conjugaison. Pour chaque caractère χ, la réunion des classes sur lesquelles χ prend la valeur $\chi(e)$ est un sous-groupe $\mathrm{G}_\chi \triangleleft \mathrm{G}$ et tout sous-groupe distingué de G est obtenu comme intersection de G_χ.

Remarque 4.3.3 (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 4.3.4 (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 4.2.2, il y a autant de caractères linéaires que de classes d'isomorphie de représentations de degré 1 de G.

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 $|G^{ab}|$.

Remarque 4.3.5. — Si $\varepsilon\colon G \to \mathbb{C}^*$ 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 4.3.6 (Centre de G)***.*** — Si g appartient au centre $Z(G)$ de G, alors $\rho_i(g)$ commute avec tous les $\rho_i(h)$. Le Lemme de Schur (Lemme 4.1.3) 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 $Z(G)$ de G.

Le centre $Z(G)$ de G est donc la réunion des classes de conjugaison C pour lesquelles $|\chi_i(C)| = \chi_i(e)$ pour tout i.

4.3.1. Les groupes cycliques. — Un groupe cyclique étant abélien il n'a que des représentations de dimension 1 (Exemple 4.1.17 et Proposition 4.2.9) c'est-à-dire des caractères au sens premier du terme (des morphismes de G dans le groupe multiplicatif $\mathbb{C}^*$). Soit $G = \{e, g, g^2, \ldots, g^{n-1}\}$ un groupe cyclique d'ordre n et de générateur g. Posons $\omega_n = \exp\left(\frac{2\mathbf{i}\pi}{n}\right)$. Les caractères de G sont de la forme

$$\chi_i\colon G \to \mathbb{C}^* \qquad\qquad h = g^k \mapsto (\omega_n^j)^k = \exp\left(\frac{2\mathbf{i}\pi j}{n}\right)$$

où $0 \leq j \leq n-1$.

La groupe G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. La table de $\mathbb{Z}/n\mathbb{Z}$ est la matrice de Vandermonde

	$\overline{0}$	$\overline{1}$	...	$\overline{n-1}$
χ_0	1	1	...	1
χ_1	1	ω_n	...	ω_n^{n-1}
χ_2	1	ω_n^2	...	$\omega_n^{2(n-1)}$
$\vdots$	$\vdots$			$\vdots$
χ_{n-1}	1	ω_n^{n-1}	...	$\omega_n^{(n-1)(n-1)}$

4.3.2. Le groupe dicyclique d'ordre 12. — Il s'agit du produit semi-direct $G = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ (*i.e.* la troisième classe d'isomorphie de groupes d'ordre 12 non abéliens autre que celles de D_{12} et $\mathcal{A}_4$).

Une présentation de G est donnée par

$$\langle a,\, b \,|\, a^3,\, b^4,\, bab^{-1}a^{-2}\rangle$$

dont nous déduisons

$$\mathrm{G} = \{a^k b^\ell \,|\, 0 \leq k \leq 2,\, 0 \leq \ell \leq 3\}.$$

De plus $Z(\mathrm{G}) = \langle b^2\rangle$, $D(\mathrm{G}) = \langle a\rangle$ et $\mathrm{G}^{\mathrm{ab}} = \langle b\rangle \simeq \mathbb{Z}/4\mathbb{Z}$ [2]. 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

$$\langle \chi_2, \chi_2\rangle = \frac{1}{12}\Big(1\times 2\times \overline{2} + 1\times 2\times \overline{2} + 2\times(-1)\times\overline{-1} + 2\times(-1)\times\overline{-1} + 3\times 0\times\overline{0} + 3\times 0\times\overline{0}\Big) = \frac{1}{12}(4+4+2+2) = 1.$$

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

2. On pourra s'aider du fait que $ba^pb^{-1} = a^{2p}$ 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.

	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

4.3.3. Le groupe $\mathcal{S}_3 = \mathrm{D}_6$. — Les classes de conjugaison de $\mathcal{S}_3$ sont (Proposition 1.2.4)

$$C_1 = \{\mathrm{id}\}, \qquad C_2 = \{(1\ 2),\ (1\ 3),\ (2\ 3)\}, \qquad C_3 = \{(1\ 2\ 3),\ (1\ 3\ 2)\}.$$

Ainsi $\mathcal{S}_3$ a trois représentations irréductibles à équivalence près. Il y a la représentation triviale ρ_{triv} qui est irréductible. On a aussi la représentation signature

$$\mathrm{sgn}\colon \mathcal{S}_3 \to \mathrm{GL}(1,\mathbb{C}) \simeq \mathbb{C}^*, \qquad \sigma \mapsto \mathrm{sgn}(\sigma)$$

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 4.1.15 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 $(\deg \rho_{\mathrm{triv}})^2 + (\deg \mathrm{sgn})^2 + (\deg \rho_S)^2 = |\mathcal{S}_3|$.

Ainsi la table de caractères de $\mathcal{S}_3$ 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.

4.3.4. Les groupes diédraux D_{2n}. —

4.3.4.1. *Le cas général.* — Rappelons quelques propriétés des groupes diédraux. Le groupe D_{2n} a pour présentation

$$\mathrm{D}_{2n} = \langle r,\, s \,|\, s^2 = r^n = rsrs = \mathrm{id} \rangle.$$

Le centre de D_{2n} est

$$Z(\mathrm{D}_{2n}) = \begin{cases} \mathrm{id} \text{ si } n \text{ est impair} \\ \{\mathrm{id},\, r^{n/2}\} \text{ si } n \text{ est pair} \end{cases}$$

et le groupe dérivé de D_{2n} 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 4.3.1. — *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. 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.

  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

  $$\{\mathrm{id}\}, \qquad \{r, r^{n-1}\}, \qquad \ldots \qquad \{r^k, r^{n-k}\}, \qquad \ldots, \qquad \{r^{\frac{n}{2}-1}, r^{\frac{n}{2}+1}\}, \qquad \{r^{\frac{n}{2}}\}.$$

  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 $\zeta = \mathrm{e}^{\frac{2\mathbf{i}\pi}{n}}$. Pour $0 \leq j \leq n-1$ 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 $0 \leq j \leq \frac{n}{2}$. 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 $1 \leq j \leq \frac{n}{2} - 1$. 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, $1 \leq j \leq \frac{n}{2} - 1$, sont donc irréductibles. De plus pour tout $0 \leq k \leq n-1$ 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.

Les symétries forment une seule classe de conjugaison :

$$\{s,\, rs,\, \ldots,\, r^{n-1}s\}$$

tandis que les rotations forment $\frac{n+1}{2}$ classes de conjugaison :

$$\{\mathrm{id}\}, \qquad \{r,\, r^{n-1}\}, \qquad \ldots \qquad \{r^k,\, r^{n-k}\}, \qquad \ldots, \qquad \{r^{\frac{n-1}{2}},\, r^{\frac{n+1}{2}}\}.$$

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 $\zeta = \mathrm{e}^{\frac{2\mathbf{i}\pi}{n}}$. Pour $0 \leq j \leq n-1$ 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 $1 \leq j \leq \frac{n-1}{2}$. 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, $1 \leq j \leq \frac{n-1}{2}$, sont donc irréductibles. De plus pour tout $0 \leq k \leq n-1$ nous avons

$$\chi_{\rho_j}(r^k) = 2\cos\left(k\frac{2\pi}{n}\right) \qquad \chi_{\rho_j}(r^k s) = 0.$$

4.3.4.2. *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. 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 4.2.3) d'où la dernière ligne de la table (que l'on peut aussi obtenir en utilisant que les colonnes sont orthogonales).

Ainsi

	$\{\mathrm{id}\}$	$\{r, r^2\}$	$\{r, r^3\}$	$\{s, r^2 s\}$	$\{rs, r^3 s\}$
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, $\ker\chi_1 = \{\mathrm{id}, r^2, s, r^2 s\}$, $\ker\chi_2 = \{\mathrm{id}, r, r^2, r^3\}$, $\ker\chi_3 = \{\mathrm{id}, r^2, rs, r^3 s\}$, $\{\mathrm{id}\}$ 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 $\ker\chi_1 \cap \ker\chi_2 = \{\mathrm{id}, r^2\}$ et le centre de D_8 est $\{g \in \mathrm{D}_8 \,|\, \forall\, i\, |\chi_i(g)| = \chi_i(\mathrm{id})\} = \{\mathrm{id}, r^2\}$.

4.3.5. 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 $\sum_{i=1}^{5} d_i^2 = 8$.

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

	$\{\mathrm{id}\}$	$\{r, r^2\}$	$\{r, r^3\}$	$\{s, r^2s\}$	$\{rs, r^3s\}$
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				

On peut obtenir la dernière ligne en utilisant que les colonnes sont orthogonales :

	$\{\mathrm{id}\}$	$\{r, r^2\}$	$\{r, r^3\}$	$\{s, r^2s\}$	$\{rs, r^3s\}$
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

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 4.3.7. — 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

$$\mathrm{Sym}^2 V := {}^{V \otimes V}\!\diagup_{\mathrm{Vect}\left((v_1 \otimes v_2 - v_2 \otimes v_1) \,|\, v_1,\, v_2 \in V\right)}$$

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.

4.3.6. Le groupe $\mathcal{S}_4$. — Le groupe symétrique $\mathcal{S}_4$ possède cinq classes de conjugaison (Proposition 1.2.4) :

$$\begin{aligned}
C_1 &= \{\mathrm{id}\},\\
C_2 &= \{(1\ 2),\ (1\ 3),\ (1\ 4),\ (2\ 3),\ (2\ 4),\ (3\ 4)\},\\
C_3 &= \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\},\\
C_4 &= \{(1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3)\},\\
C_5 &= \{(1\ 2\ 3\ 4),\ (1\ 2\ 4\ 3),\ (1\ 3\ 2\ 4),\ (1\ 3\ 4\ 2),\ (1\ 4\ 2\ 3),\ (1\ 4\ 3\ 2)\}.
\end{aligned}$$

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

$$\rho_P \colon \mathcal{S}_4 \to \mathrm{GL}(\mathbb{C}^4) \qquad\qquad \sigma \mapsto (e_i \mapsto e_{\sigma(i)}).$$

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 appelée représentation standard 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 4.1.4). 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

$$\begin{aligned}
\langle \chi_{\rho_S}, \chi_{\rho_S}\rangle &= \frac{1}{|\mathcal{S}_4|}\Big(1 \times 3 \times \overline{3} + 6 \times 1 \times \overline{1} + 3 \times (-1) \times \overline{(-1)} + 8 \times 0 \times \overline{0} + 6 \times (-1) \times \overline{(-1)}\Big)\\
&= \frac{1}{24}(9 + 6 + 3 + 6)
\end{aligned}$$

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 $\mathcal{A}_4$ notées ρ_3 et ρ_5. Commençons par déterminer leurs degrés : l'identité

$$(\deg \rho_{\mathrm{triv}})^2 + (\deg \mathrm{sgn})^2 + (\deg \rho_3^2)^2 + (\deg \rho_4^2)^2 + (\deg \rho_5^2)^2 = |\mathcal{S}_4|$$

conduit à

$$24 - (\deg \rho_{\text{triv}})^2 - (\deg \text{sgn})^2 - (\deg \rho_4)^2 = (\deg \rho_3)^2 + (\deg \rho_5)^2$$

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

$$\rho_5 \colon \mathcal{S}_4 \to \mathrm{GL}(H), \qquad \sigma \mapsto \mathrm{sgn}(\sigma)\rho_4(\sigma).$$

Alors $\chi_{\rho_5} = \mathrm{sgn}\chi_{\rho_4}$ d'où

$\chi_{\rho_S}(\mathrm{id}) = 1 \times 3 = 3$, $\chi_{\rho_S}((1\ 2)) = (-1) \times 1 = -1$, $\chi_{\rho_S}((1\ 2)(3\ 4)) = 1 \times (-1) = -1$,
$\chi_{\rho_S}((1\ 2\ 3)) = 1 \times 0 = 0$, $\chi_{\rho_S}((1\ 2\ 3\ 4)) = (-1) \times (-1) = 1$.

En particulier

$$\langle \chi_{\rho_5}, \chi_{\rho_5} \rangle = \frac{1}{24}\Big(1{\times}3{\times}3{+}6{\times}(-1){\times}(-1){+}3{\times}(-1){\times}(-1){+}8{\times}0{\times}0{+}6{\times}1{\times}1\Big) = \frac{1}{24}\Big(9{+}6{+}3{+}6\Big) = 1.$$

Il s'ensuit que ρ_5 est irréductible. De plus $\deg \rho_5 = \dim H = 3$.

Remarque 4.3.8. — On peut donner une interprétation géométrique de ρ_5 : c'est la représentation de $\mathcal{S}_4$ comme $\mathrm{Isom}^+(C_6)$ (Proposition 2.1.22).

Commençons à écrire la table de caractères de $\mathcal{S}_4$:

	$C(\mathrm{id})$	$C((1\ 2))$	$C((1\ 2)(3\ 4))$	$C((1\ 2\ 3))$	$C((1\ 2\ 3\ 4))$
$\chi_{\rho_{\text{triv}}}$	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 $g \in \mathcal{S}_4$.

En utilisant que les colonnes de la table de $\mathcal{S}_4$ sont orthogonales nous obtenons

	$C(\mathrm{id})$	$C((1\ 2))$	$C((1\ 2)(3\ 4))$	$C((1\ 2\ 3))$	$C((1\ 2\ 3\ 4))$
$\chi_{\rho_{\text{triv}}}$	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 $\mathcal{S}_4$ sont les intersections $\bigcap_{i\in I}\ker\chi_{\rho_i}$ où $I\subset$ [triv, sgn, 3, 4, 5]. La table des caractères de $\mathcal{S}_4$ assure que

$$\begin{aligned}
&\ker\chi_{\rho_{\text{triv}}}=\mathcal{S}_4\\
&\ker\chi_{\rho_{\text{sgn}}}=\{\text{id},\,C((1\ 2)(3\ 4)),\,C(1\ 2\ 3)\}\\
&\ker\chi_{\rho_3}=\{\text{id}\}\\
&\ker\chi_{\rho_4}=\{\text{id},\,C(1\ 2)\}\\
&\ker\chi_{\rho_5}=\{\text{id},\,C(1\ 2\ 3\ 4)\}
\end{aligned}$$

Par suite les sous-groupes distingués de $\mathcal{S}_4$ sont

$$\mathcal{S}_4,\qquad \{\text{id}\},\qquad \mathcal{A}_4,\qquad \{\text{id},\,(1\ 2)(3\ 4),\,(1\ 3)(2\ 4),\,(1\ 4)(2\ 3)\}\simeq\mathcal{K}$$

(on rappelle que $\mathcal{K}$ désigne le groupe de Klein).

Explicitons ρ_3. Nous avons la décomposition en produit semi-direct

$$\mathcal{S}_4\simeq\mathcal{K}\rtimes\mathcal{S}_3.$$

À cette décomposition correspond un morphisme surjectif de groupes

$$\pi\colon\mathcal{S}_4\to{}^{\mathcal{S}_4}\!/_{\mathcal{K}}\simeq\mathcal{S}_3$$

d'où par composition avec la représentation standard $\widetilde{\rho_S}$ de $\mathcal{S}_3$ une représentation de degré 2

$$\rho_3\colon\mathcal{S}_4\xrightarrow{\pi}\mathcal{S}_3\xrightarrow{\widetilde{\rho_S}}\mathrm{GL}(\widetilde{H})$$

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 $\widetilde{\rho_S}\colon\mathcal{S}_3\to\mathrm{GL}(\widetilde{H})$ la représentation standard de $\mathcal{S}_3$ induite par la représentation par permutation

$$\widetilde{\rho_P}\colon\mathcal{S}_3\to\mathrm{GL}(\mathbb{C}^3),\qquad\qquad \sigma\mapsto(e_i\mapsto e_{\sigma(i)}).$$

Pour tout σ dans $\mathcal{S}_4$ nous avons

$$\chi_{\rho_3}(\sigma)=\chi_{\widetilde{\rho_S}}(\pi(\sigma))$$

soit

$$\begin{aligned}
&\chi_{\rho_3}(\text{id})=2\\
&\chi_{\rho_3}((1\ 2))=0\\
&\chi_{\rho_3}((1\ 2)(3\ 4))=2\\
&\chi_{\rho_3}((1\ 2\ 3))=-1\\
&\chi_{\rho_3}((1\ 2\ 3\ 4))=\chi_{\rho_3}((1\ 4)(1\ 2\ 3))=0
\end{aligned}$$

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.

4.3.7. Le groupe $\mathcal{A}_4$. — Rappelons que le groupe $\mathcal{A}_4$ est le sous-groupe des permutations de $\mathcal{S}_4$ de signature 1. Comme $\mathcal{S}_4$ 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

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

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 [3].

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.

3. 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 $gh = gh$.

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 $\mathcal{A}_4$.

Si s appartient à C_2 et si $t^a h$, avec $a \in \{0,\, 1,\, 2\}$ et $h \in \mathrm{H}$, commute à s, alors $t^a hs = st^a h$ donc $t^a hsh = st^a h^2$. Comme H est abélien et $h^2 = \mathrm{id}$ nous obtenons $t^a s = st^a$ ce qui entraîne $a = 0$. Le centralisateur de s est donc G 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 $t^a ht = tt^a h$ 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

$$(t^a h)t(t^a h)^{-1} = t^a hth^{-1}t^{-a} = t(t^{a-1}ht^{1-a})(t^a h^{-1}t^{-a}) \in t\mathrm{H}$$

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 $t^a ht^b g = t^{a+b}(t^{-b}ht^b)g$. Puisque H est distingué dans $\mathcal{A}_4$, on a $t^{-b}ht^b$ appartient à H et donc $(t^{-b}ht^b)g$ appartient à H. De plus $\eta^j(t^a ht^b g) = \zeta^{j(a+b)} = \zeta^{ja}\zeta^{jb} = \eta^j(t^a h)\eta^j(t^b g)$.

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 4.3.9. — 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 4.2.8 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 4.3.10. — On peut utiliser la Proposition 4.2.8 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 4.3.11. — Supposons que nous ayons construit des reprśentations 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 4.2.8 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 4.2.6). 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 4.3.12. — Notons $\text{Irr}(\mathcal{A}_4)$ l'ensemble des représentations irréductibles de $\mathcal{A}_4$. Supposons W construite. La formule de la Proposition 4.2.8 assure que

$$12 = |\mathcal{A}_4| = 9 + \sum_{\rho \in \text{Irr}(\mathcal{A}_4) \smallsetminus \{W\}} (\deg \rho)^2;$$

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 $\text{H} \subset \ker \chi$ car l'unique élément de μ_3 d'ordre divisant 2 est 1. Il s'ensuit que $\ker \chi = \text{H}$ 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

$$\eta(g) = \begin{cases} 1 \text{ si } g \in \text{H} = C_1 \cup C_2 \\ \rho \text{ si } g \in C_3 = t\text{H} \\ \rho^2 \text{ si } g \in C_4 = t^2\text{H} \end{cases}$$

Ceci permet en utilisant la Remarque 4.3.11 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).

4.3.8. Le groupe $\mathcal{S}_5$. —

4.4. Propriété d'intégralité

4.5. Groupes abéliens finis et représentations linéaires des groupes finis

Référence : [**Col11**, p. 132-134]

Leçons possibles :

104 : *Groupes abéliens et non abéliens finis. Exemples et applications.*

110 : *Structure et dualité des groupes abéliens finis. Applications.*

102 : *Groupe des nombres complexes de module* 1. *Sous-groupes des racines de l'unité. Applications.*

107 : *Représentations et caractères d'un groupe fini sur un* $\mathbb{C}$*-espace vectoriel. Exemples.*

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 4.5.1. — *Si* G *est un groupe fini, alors* $\iota \colon \mathrm{G} \to \widehat{\widehat{\mathrm{G}}}$ *est un isomorphisme de groupes.*

Définition 4.5.1. — Soit G un groupe abélien fini. L'exposant $\exp(\mathrm{G})$ de G est le maximum des ordres des éléments de G.

Lemme 4.5.2. — *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

$$N(\widehat{\widehat{\mathrm{G}}}) \subseteq N(\widehat{\mathrm{G}}) \subseteq N(\mathrm{G}) \tag{4.5.1}$$

Mais G et $\widehat{\widehat{\mathrm{G}}}$ sont isomorphes donc $N(\widehat{\widehat{\mathrm{G}}}) = N(\mathrm{G})$ et (5.8.1) implique $N(\widehat{\widehat{\mathrm{G}}}) = N(\widehat{\mathrm{G}}) = N(\mathrm{G})$. □

Théorème 4.5.3. — *Soit* G *un groupe abélien fini. Il existe* $r \in \mathbb{N}$ *et des entiers* N_1, N_2, …, 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* |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 4.5.2). Il existe donc χ_1 d'ordre N et comme $\chi_1(\mathrm{G})$ est un sous-groupe du groupe cyclique $\mu_N = \{z \in \mathbb{C} \,|\, z^N = 1\}$, c'est μ_N tout entier. Il existe donc $g_1 \in \mathrm{G}$ tel que $\chi_1(g_1) = \exp\left(\frac{2\mathbf{i}\pi}{N}\right)$. 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

$$\mathrm{G} = \mathrm{H}_1 \oplus \ker \chi_1 = \mathbb{Z}/N\mathbb{Z} \oplus \ker \chi_1 \simeq \mathbb{Z}/N\mathbb{Z} \oplus \bigoplus_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$$

□

CHAPITRE 5

EXERCICES

5.1. Premiers pas

Exercice 1 Parmi les ensembles suivants lesquels sont des groupes pour l'opération donnée ?

1. $\mathbb{Q}^*$, $+$;
2. $\mathbb{Q}^*$, $\cdot$;
3. $\mathbb{Z}/n\mathbb{Z}$, $\cdot$;
4. $\mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$, $\cdot$;
5. $\{M \in \mathrm{M}_{n,n}(\mathbb{R}) \mid \det M = 1\}$, $\cdot$;
6. $\{M \in \mathrm{M}_{n,n}(\mathbb{R}) \mid \det M = 0\}$, $+$.

Éléments de réponse 1

2. $\mathbb{Q}^*$, $\cdot$;
5. $\{M \in \mathrm{M}_{n,n}(\mathbb{R}) \mid \det M = 1\}$, $\cdot$

sont des groupes.

Remarque sur le 4. : $\mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$, $\cdot$ n'est pas un groupe en général. Si n est premier, alors $\mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\} = \left(\mathbb{Z}/n\mathbb{Z}\right)^*$ est un groupe.

Remarque sur le 6. : l'opération $+$ n'est pas interne. Soient

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix};$$

nous avons

$$\det A = 0 \qquad \det B = 0 \qquad \det A + B = 1 \neq 0.$$

Exercice 2 Parmi les groupes suivants lesquels sont abéliens ?

1. $\mathbb{R}[x]_{\leq 8}$, $+$ (les polynômes de degré $d \leq 8$ dans une variable x à coefficients réels) ;
2. $\mathrm{GL}(n, \mathbb{R})$, $\cdot$ (les matrices inversibles de taille $n \times n$ à coefficients réels) ;
3. $\mathcal{S}_4$, $\circ$.

Éléments de réponse 2 $\mathbb{R}[x]_{\leq 8}$, $+$ (les polynômes de degré $d \leq 8$ dans une variable x à coefficients réels) est un groupe abélien.

Exercice 3 Lesquels des ensembles A sont des sous-groupes du groupe G donné ?

1. $A = \mathbb{R}[x]_8$, $+$ (les polynômes de degré 8) et $\mathrm{G} = \mathbb{R}[x]_{\leq 8}$, $+$;
2. $A = 100\mathbb{Z}$ et $\mathrm{G} = 10\mathbb{Z}$;
3. $A = \mathbb{Z}/10\mathbb{Z}$ et $\mathrm{G} = \mathbb{Z}/100\mathbb{Z}$;
4. $A = \mathbb{Z}/10\mathbb{Z}$ et $\mathrm{G} = \mathbb{Z}$.

Éléments de réponse 3 $A = 100\mathbb{Z}$ est un sous-groupe de $\mathrm{G} = 10\mathbb{Z}$.

Remarque sur le 3. : $\mathbb{Z}/10\mathbb{Z} \not\subseteq \mathbb{Z}/100\mathbb{Z}$.

Remarque sur le 4. : $\mathbb{Z}/10\mathbb{Z} \not\subseteq \mathbb{Z}$.

Exercice 4 Quels sont les éléments de $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$?

1. $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$;
2. $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{7}$;
3. $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$;
4. $\overline{3}$, $\overline{5}$, $\overline{7}$, $\overline{9}$.

Éléments de réponse 4

1. $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$;
2. $\overline{3}$, $\overline{5}$, $\overline{7}$, $\overline{9}$

sont les éléments de $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$.

Exercice 5 Pour quelles opérations parmi l'addition $+$ et la multiplication $\cdot$ l'ensemble suivant est-il un groupe ?

1. $\mathbb{Z}$;
2. $\mathbb{C}$;
3. $\mathbb{C}^*$;
4. $\mathbb{Z}/8\mathbb{Z}$;
5. $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$;

6. $\mathbb{Z}/7\mathbb{Z}$;
7. $\left(\mathbb{Z}/7\mathbb{Z}\right)^*$;
8. $\{1, -1\}$.

Éléments de réponse 5

1. $\mathbb{Z}$, $+$;
2. $\mathbb{C}$, $+$;
3. $\mathbb{C}^*$, $\cdot$;
4. $\mathbb{Z}/8\mathbb{Z}$, $+$;
5. $\left(\mathbb{Z}/8\mathbb{Z}\right)^*$, $\cdot$;
6. $\mathbb{Z}/7\mathbb{Z}$, $+$, $\cdot$;
7. $\left(\mathbb{Z}/7\mathbb{Z}\right)^*$, $\cdot$;
8. $\{1, -1\}$, $\cdot$

sont des groupes.

Exercice 6

1. Quel est l'ordre de 0 dans $\mathbb{Z}$?
2. Quel est l'ordre de 1 dans $\mathbb{Z}$?
3. Quel est l'ordre de 2 dans $\mathbb{Z}$?
4. Quel est l'ordre de B dans $\mathcal{P}(A), \Delta$, avec A, $B \neq \emptyset$?
5. Quel est l'ordre de 1 dans $\mathbb{Z}/9\mathbb{Z}$?
6. Quel est l'ordre de 1 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$?
7. Quel est l'ordre de 4 dans $\mathbb{Z}/9\mathbb{Z}$?
8. Quel est l'ordre de 4 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$?

Éléments de réponse 6

1. L'ordre de 0 dans $\mathbb{Z}$ est : 1.
2. L'ordre de 1 dans $\mathbb{Z}$ est : ∞.
3. L'ordre de 2 dans $\mathbb{Z}$ est : ∞.
4. L'ordre de B dans $\mathcal{P}(A), \Delta$, avec A, $B \neq \emptyset$ est : 2.
5. L'ordre de 1 dans $\mathbb{Z}/9\mathbb{Z}$ est : 9.

6. L'ordre de 1 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$ est : 1.
7. L'ordre de 4 dans $\mathbb{Z}/9\mathbb{Z}$ est : 9.
8. L'ordre de 4 dans $\left(\mathbb{Z}/9\mathbb{Z}\right)^*$ est : 3.

Exercice 7 Compléter pour obtenir un énoncé correct : Soit x un élément d'un groupe fini G. Si $x^k = e_{\mathrm{G}}$ pour un certain $k \in \mathbb{N}^*$, alors

1. k divise l'ordre de G ;
2. l'ordre de x divise k ;
3. k divise l'ordre de x.

Éléments de réponse 7 Soit x un élément d'un groupe fini G. Si $x^k = e_{\mathrm{G}}$ pour un certain $k \in \mathbb{N}^*$, alors

2. l'ordre de x divise k.

Remarque sur l'assertion 1. : rappelons que $g^k = e$, $k \in \mathbb{N}^*$, si et seulement si l'ordre $o(g)$ de g divise k. Le théorème de Lagrange assure que $o(g) = |\langle g \rangle|$ divise $|\mathrm{G}|$. Si $k = o(g) + |\mathrm{G}|$, alors

$$g^k = g^{o(g)+|\mathrm{G}|} = g^{o(g)} g^{|\mathrm{G}|} = ee = e$$

mais $k = o(g) + |\mathrm{G}|$ ne divise pas $|\mathrm{G}|$.

Exercice 8 Compléter pour obtenir un énoncé correct : Soit G le groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Soit $g = ([1]_4, [4]_6)$.

1. $\langle g \rangle = \{([1]_4, [4]_6), ([2]_4, [2]_6), ([3]_4, [0]_6), ([0]_4, [4]_6)\}$;
2. $\langle g \rangle = \{([1]_4, [4]_6), ([2]_4, [2]_6), ([3]_4, [0]_6), ([0]_4, [4]_6), ([1]_4, [2]_6), ([2]_4, [0]_6), ([3]_4, [4]_6), ([0]_4, [2]_6), ([1]_4, [0]_6), ([2]_4, [4]_6), ([3]_4, [2]_6), ([0]_4, [0]_6)\}$;
3. $\langle g \rangle = \mathrm{G}$.

Éléments de réponse 8 Soit G le groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Soit $g = ([1]_4, [4]_6)$.

2. $\langle g \rangle = \{([1]_4, [4]_6), ([2]_4, [2]_6), ([3]_4, [0]_6), ([0]_4, [4]_6), ([1]_4, [2]_6), ([2]_4, [0]_6), ([3]_4, [4]_6), ([0]_4, [2]_6), ([1]_4,$

Exercice 9 Quelles sont les implications correctes ?

1. Si G est un groupe abélien, alors G est cyclique ;
2. Si G est un groupe cyclique, alors G est abélien ;
3. Si G est d'ordre p, avec p un nombre premier, alors G est cyclique ;
4. Si G est d'ordre fini et cyclique, alors G est d'ordre premier.

Éléments de réponse 9 Les assertions correctes sont :

2. Si G est un groupe cyclique, alors G est abélien ; en effet si G est cyclique, il existe $g \in \mathrm{G}$ tel que $\mathrm{G} = \langle g \rangle$. Soient a et b dans G, ils s'écrivent aussi g^ℓ et g^k, ℓ, $k \in \mathbb{Z}$ et
$$ab = g^\ell g^k = g^{\ell+k} = g^{k+\ell} = g^k g^\ell = ba.$$
3. Si G est d'ordre p, avec p un nombre premier, alors G est cyclique. En effet soit $g \in \mathrm{G} \setminus \{e\}$. Le théorème de LAGRANGE assure que l'ordre de g divise p. Puisque p est premier, l'ordre de g est p et g est un générateur de G.

Remarque sur le 1. : l'assertion est fausse, considérons par exemple $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, c'est un groupe abélien, non cyclique.

Remarque sur le 4. : l'assertion est fausse, considérons par exemple $\mathrm{G} = \mathbb{Z}/4\mathbb{Z}$, c'est un groupe d'ordre fini et cyclique mais 4 n'est pas premier.

Exercice 10 La décomposition de la permutation (1 2 3 4)(2 3)(1 4 3) de $\mathcal{S}_4$ en cycles disjoints est :

1. (3 2 4) ;
2. id ;
3. (2 4 3)(1) ;
4. (1)(2)(3)(4).

Éléments de réponse 10 La décomposition de la permutation (1 2 3 4)(2 3)(1 4 3) de $\mathcal{S}_4$ en cycles disjoints est :

1. (3 2 4) ;
3. (2 4 3)(1).

Exercice 11 L'ordre de l'élément (1 3)(2 4 5)(6 9 8 7) dans $\mathcal{S}_{11}$ est

1. 9 ;
2. 11 ;
3. 12 ;
4. 24.

Éléments de réponse 11 L'ordre de l'élément (1 3)(2 4 5)(6 9 8 7) dans $\mathcal{S}_{11}$ est 12. En effet l'élément (1 3)(2 4 5)(6 9 8 7) a pour décomposition en cycles à supports disjoints (1 3)(2 4 5)(6 9 8 7). De plus
$$o\big((1\ 3)\big) = 2 \qquad o\big((2\ 4\ 5)\big) = 3 \qquad o\big((6\ 9\ 8\ 7)\big) = 4$$
L'ordre de (1 3)(2 4 5)(6 9 8 7) est $\mathrm{ppcm}(2, 3, 4) = 12$.

Exercice 12 Soit $\mathrm{D}_8 = \{\mathrm{id}, r, r^2, r^3, s, sr, sr^2, sr^3\}$ le groupe diédral d'ordre 8. Pour rappel, dans ce groupe on a $r^4 = \mathrm{id}$, $s^2 = \mathrm{id}$ et $r^k s = sr^{-k}$, pour $k \in \mathbb{Z}$. Parmi les énoncés suivants lesquels sont vrais ?

1. Dans D_8 il y a 4 réflexions et 4 rotations ;
2. Dans D_8 il y a exactement 4 éléments d'ordre 2 ;
3. Dans D_8 il y a exactement 4 éléments d'ordre 4.

Éléments de réponse 12 Soit $\mathrm{D}_8 = \{\mathrm{id}, r, r^2, r^3, s, sr, sr^2, sr^3\}$ le groupe diédral d'ordre 8. Pour rappel, dans ce groupe on a $r^4 = \mathrm{id}$, $s^2 = \mathrm{id}$ et $r^k s = sr^{-k}$, pour $k \in \mathbb{Z}$. L'énoncé suivant est vrai :

1. Dans D_8 il y a 4 réflexions et 4 rotations.

Les autres assertions sont fausses. En effet id, r, r^2 et r^3 sont des rotations alors que s, sr, sr^2 et sr^3 sont des réflexions. Les éléments d'ordre 2 sont les réflexions et r^2. Les éléments d'ordre 4 sont r et r^3.

Exercice 13 Soit G le groupe des isométries qui préservent un polygône régulier $\mathcal{P}$ à 5 côtés. Parmi les énoncés suivants lesquels sont corrects ?

1. $\mathrm{G} = \mathrm{D}_{10}$;
2. $\mathrm{G} = \mathrm{D}_5$;
3. Si $x \in \mathrm{G}$ est d'ordre 2, alors x préserve exactement un sommet de $\mathcal{P}$;
4. Si $x \in \mathrm{G}$ est d'ordre 2, alors x préserve exactement deux sommets de $\mathcal{P}$;
5. Dans G, il y a des éléments d'ordre 1, 2 et 5 ;
6. Dans G, il y a des éléments d'ordre 1, 2, 5 et 10.

Éléments de réponse 13 Soit G le groupe des isométries qui préservent un polygône régulier $\mathcal{P}$ à 5 côtés. Les énoncés suivants sont corrects :

1. $\mathrm{G} = \mathrm{D}_{10}$;
3. Si $x \in \mathrm{G}$ est d'ordre 2, alors x préserve exactement un sommet de $\mathcal{P}$;
5. Dans G, il y a des éléments d'ordre 1, 2 et 5.

Exercice 14 Soit $(\mathrm{G}, *) = (\mathbb{Z}, +)$, $\mathrm{H} = 4\mathbb{Z}$ et $g = 3$. Alors $g * \mathrm{H}$ est égal à :

1. $3 + 4\mathbb{Z}$;
2. $12\mathbb{Z}$;
3. $\{\ldots, -1, 3, 7, 11, \ldots\}$;
4. $-5 * \mathrm{H}$.

Éléments de réponse 14 Soit $(\mathrm{G}, *) = (\mathbb{Z}, +)$, $\mathrm{H} = 4\mathbb{Z}$ et $g = 3$. Alors $g * \mathrm{H}$ est égal à :

1. $3 + 4\mathbb{Z}$;
3. $\{\ldots, -1, 3, 7, 11, \ldots\}$;
4. $-5 * \mathrm{H}$.

Exercice 15 Soient G un groupe et H un sous-groupe distingué de G. Parmi les énoncés suivants lesquels sont corrects ?

1. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $ghg^{-1} \in \mathrm{H}$;
2. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $g^{-1}hg \in \mathrm{H}$;
3. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $hgh^{-1} \in \mathrm{H}$;
4. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $h^{-1}gh \in \mathrm{H}$.

Éléments de réponse 15 Soient G un groupe et H un sous-groupe distingué de G. Les énoncés suivants sont corrects :

1. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $ghg^{-1} \in \mathrm{H}$;
2. $\forall\, g \in \mathrm{G}$, $\forall\, h \in \mathrm{H}$, on a $g^{-1}hg \in \mathrm{H}$.

Exercice 16 Soient G un groupe et H un sous-groupe propre de G. Parmi les énoncés suivants lesquels sont corrects ?

1. En général, il y a exactement une classe à gauche suivant H qui est un sous-groupe de G.
2. Si H est distingué dans G, alors les classes à gauche dans G suivant H sont des sous-groupes de G ;
3. En général, il y a autant de classes à gauche que de classes à droite ;
4. Si H est distingué dans G, alors il y a autant de classes à gauche que de classes à droite ;
5. Soit $g \in \mathrm{G}$. Si H est distingué dans G, alors $g\mathrm{H} = \mathrm{H}g$.

Éléments de réponse 16 Soient G un groupe et H un sous-groupe propre de G. Les énoncés suivants sont corrects :

1. En général, il y a exactement une classe à gauche suivant H qui est un sous-groupe de G.
3. En général, il y a autant de classes à gauche que de classes à droite ;
4. Si H est distingué dans G, alors il y a autant de classes à gauche que de classes à droite ;
5. Soit $g \in \mathrm{G}$. Si H est distingué dans G, alors $g\mathrm{H} = \mathrm{H}g$.

Exercice 17 Soit G un groupe. Parmi les énoncés suivants lesquels sont corrects ?

1. Si G n'est pas abélien, alors G a au moins un sous-groupe propre (*i.e.* distinct de $\{e_\mathrm{G}\}$ et de G) qui n'est pas distingué dans G ;

2. Si G est abélien, alors tous les sous-groupes de G sont distingués dans G ;
3. Si G est abélien et H est un sous-groupe propre de G, alors $^{G}/_{H}$ est abélien ;
4. Si G n'est pas abélien et H est un sous-groupe distingué propre de G, alors $^{G}/_{H}$ n'est pas abélien ;
5. Si G est cyclique et H est un sous-groupe de G, alors $^{G}/_{H}$ est cyclique ;
6. Si G n'est pas cyclique et H est un sous-groupe de G, alors $^{G}/_{H}$ n'est pas cyclique.

Éléments de réponse 17 Soit G un groupe. Les énoncés suivants sont corrects :

2. Si G est abélien, alors tous les sous-groupes de G sont distingués dans G ; cela découle de la définition de sous-groupe distingué.
3. Si G est abélien et H est un sous-groupe propre de G, alors $^{G}/_{H}$ est abélien ; En effet soient $g_1\mathrm{H}$ et $g_2\mathrm{H}$ deux éléments de $^{G}/_{H}$, alors
$$\begin{aligned} g_1\mathrm{H}\cdot g_2\mathrm{H} &= g_1g_2\mathrm{H} \text{ (définition de cette opération)} \\ &= g_2g_1\mathrm{H} \text{ (car G est abélien)} \\ &= g_2\mathrm{H}\cdot g_1\mathrm{H} \text{ (définition de cette opération)} \end{aligned}$$
5. Si G est cyclique et H est un sous-groupe de G, alors $^{G}/_{H}$ est cyclique. En effet soit x un générateur de G. Soit $g\mathrm{H}$ un élément de $^{G}/_{H}$. Il existe $k \in \mathbb{Z}$ tel que $g = x^k$ donc $g\mathrm{H} = x^k\mathrm{H} = (x\mathrm{H})^k$. Ainsi $x\mathrm{H}$ est un générateur de $^{G}/_{H}$.

L'assertion 1. est fausse. Le groupe des quaternions $\mathbb{H}_8$ n'est pas abélien et n'a pas de sous-groupe propre qui n'est pas distingué.

L'assertion 4. est fausse. Considérons par exemple les groupes $\mathrm{G} = \mathrm{D}_8$ et $\mathrm{H} = \langle r\rangle$, alors $^{G}/_{H} \simeq {}^{\mathbb{Z}}/_{2\mathbb{Z}}$ et donc $^{G}/_{H}$ est abélien.

L'assertion 6. est fausse. Considérons par exemple les groupes $\mathrm{G} = {}^{\mathbb{Z}}/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}/_{2\mathbb{Z}}$ et $\mathrm{H} = \langle(\overline{1}, \overline{0})\rangle$. Le groupe G n'est pas cyclique mais $^{G}/_{H} \simeq {}^{\mathbb{Z}}/_{2\mathbb{Z}}$ est cyclique.

Exercice 18 Soient G un groupe et H un sous-groupe de G. Parmi les énoncés suivants lesquels sont corrects ?

1. Si l'ordre de G est infini, alors le nombre de classes à gauche dans G suivant H est infini ;
2. Si l'ordre de G est infini et l'ordre de H est infini, alors le nombre de classes à gauche dans G suivant H est infini ;
3. Si l'ordre de G est infini et l'ordre de H est fini, alors le nombre de classes à gauche dans G suivant H est infini ;
4. Si l'ordre de G est fini, alors le nombre de classes à gauche dans G suivant H divise l'ordre de H ;

5. Si l'ordre de G est fini, alors le nombre de classes à gauche dans G suivant H divise l'ordre de G.

Éléments de réponse 18 Soient G un groupe et H un sous-groupe de G. Les énoncés suivants sont corrects :

3. Si l'ordre de G est infini et l'ordre de H est fini, alors le nombre de classes à gauche dans G suivant H est infini. En effet les classes à gauche forment une partition de G. Toute classe à gauche suivant H est en bijection avec H. S'il n'y avait qu'un nombre fini de classes à gauche suivant H, alors G serait fini.
5. Si l'ordre de G est fini, alors le nombre de classes à gauche dans G suivant H divise l'ordre de G. Cela découle du théorème de Lagrange.

L'assertion 1. est fausse. Considérons par exemple $\mathrm{G} = \mathbb{Z}$ et $\mathrm{H} = 2\mathbb{Z}$. Il y a deux classes à gauche.

L'assertion 2. est fausse. Considérons par exemple $\mathrm{G} = \mathbb{Z}$ et $\mathrm{H} = 2\mathbb{Z}$. Il y a deux classes à gauche.

Exercice 19 Pour l'action $\cdot$ donnée du groupe G sur l'ensemble A, déterminer :

1. l'élément $\overline{1} \cdot \overline{3}$ si $\cdot$ est l'action de $\mathrm{G} = \mathbb{Z}/6\mathbb{Z}$ sur lui-même ($A = \mathrm{G}$) par translation ;
2. l'élément $\overline{5} \cdot \overline{1}$ si $\cdot$ est l'action de $\mathrm{G} = \left(\mathbb{Z}/6\mathbb{Z}\right)^*$ sur lui-même ($A = \mathrm{G}$) par translation ;
3. l'élément $(1\ 2) \cdot 2$ si $\cdot$ est l'action triviale de $\mathrm{G} = \mathcal{S}_3$ sur $A = \{1, 2, 3, 4\}$;
4. l'élément $(1\ 2) \cdot (3\ 4)$ si $\cdot$ est l'action par conjugaison de $\mathrm{G} = \mathcal{S}_4$ sur lui-même ($A = \mathrm{G}$).

Éléments de réponse 19

1. Si $\cdot$ est l'action de $\mathrm{G} = \mathbb{Z}/6\mathbb{Z}$ sur lui-même ($A = \mathrm{G}$) par translation, alors l'élément $\overline{1} \cdot \overline{3}$ est $\overline{1} + \overline{3} = \overline{4}$;
2. si $\cdot$ est l'action de $\mathrm{G} = \left(\mathbb{Z}/6\mathbb{Z}\right)^*$ sur lui-même ($A = \mathrm{G}$) par translation, alors l'élément $\overline{5} \cdot \overline{1}$ est $\overline{5}$;
3. si $\cdot$ est l'action triviale de $\mathrm{G} = \mathcal{S}_3$ sur $A = \{1, 2, 3, 4\}$, alors l'élément $(1\ 2) \cdot 2$ est 2 ;
4. si $\cdot$ est l'action par conjugaison de $\mathrm{G} = \mathcal{S}_4$ sur lui-même ($A = \mathrm{G}$) l'élément $(1\ 2) \cdot (3\ 4)$ est
$$(1\ 2) \circ (3\ 4) \circ (1\ 2)^{-1} = (3\ 4).$$

Exercice 20 Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$.

1. L'élément $g \cdot a$ à quel ensemble appartient-il ?
2. Si $g = e_{\mathrm{G}}$, alors que vaut $g \cdot a$?
3. Est-ce que l'orbite de a est un sous-ensemble de A ou de G ?

4. Est-ce que le stabilisateur de a est un sous-ensemble de A ou de G ?
5. De quel ensemble est-ce que le noyau de l'action est un sous-groupe ?

Éléments de réponse 20 Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$.

1. L'élément $g \cdot a$ appartient à A.
2. Si $g = e_{\mathrm{G}}$, alors $g \cdot a = a$.
3. L'orbite de a est un sous-ensemble de A.
4. Le stabilisateur de a est un sous-ensemble de G ?
5. Le noyau de l'action est un sous-groupe de G.

Exercice 21 Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$. Vrai ou faux ?

1. Si $g \cdot a = b$, alors $g = b \cdot a^{-1}$;
2. Si $g \cdot a = b$, alors $a = g^{-1} \cdot b$;
3. L'orbite de a est un groupe ;
4. Le stabilisateur de g est un groupe ;
5. Si le noyau de l'action est $\{e_{\mathrm{G}}\}$, alors l'action est fidèle ;
6. L'action est transitive si et seulement s'il n'y a qu'une seule orbite ;
7. Le stabilisateur de g est un sous-groupe distingué de G.

Éléments de réponse 21 Soit $\cdot$ une action du groupe G sur l'ensemble A. Soient $g \in \mathrm{G}$ et $a \in A$.

1. Si $g \cdot a = b$, alors $g = b \cdot a^{-1}$; faux : écrire a^{-1} n'a pas de sens.
2. Si $g \cdot a = b$, alors $a = g^{-1} \cdot b$; vrai : si $g \cdot a = b$, alors $g^{-1} \cdot (g \cdot a) = g^{-1} \cdot b$ soit $(g^{-1} g) \cdot a = g^{-1} \cdot b$ ou encore $a = g^{-1} b$.
3. L'orbite de a est un groupe ; faux : les orbites forment une partition de A, ce sont des ensembles sans structure.
4. Le stabilisateur de g est un groupe ; vrai.
5. Si le noyau de l'action est $\{e_{\mathrm{G}}\}$, alors l'action est fidèle ; vrai.
6. L'action est transitive si et seulement s'il n'y a qu'une seule orbite ; vrai.
7. Le stabilisateur de g est un sous-groupe distingué de G ; faux.

Exercice 22 Soit G un groupe. Soient a, b deux éléments de G d'ordre fini. Le groupe engendré par a et b est-il fini ?

Éléments de réponse 22 Non (considérer par exemple le groupe G des permutations de $\mathbb{Z}$ engendré par $f(x) = -x$ et $g(x) = 1 - x$. Alors $f \circ f = \mathrm{id}$, $g \circ g = \mathrm{id}$ mais $f \circ g \colon x \mapsto x - 1$ donc $(f \circ g)^n \colon x \mapsto x - n$. Le groupe G contient donc tous les éléments de la forme $x \mapsto x - n$ avec n dans $\mathbb{Z}$. En particulier il est infini.

Exercice 23 Dans le lemme chinois expliciter rapidement comment on construit l'isomorphisme.

Éléments de réponse 23 **Lemme chinois.** *Si p et q sont premiers entre eux, alors*

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Soit $\overline{n}$, resp. $\widehat{n}$, resp. $\dot{n}$ la classe de n modulo pq, resp. p, resp. q. Considérons le morphisme

$$\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \qquad \overline{n} \mapsto (\widehat{n}, \dot{n})$$

Il est injectif car $\mathrm{pgcd}(p, q) = 1$. On conclut grâce à l'égalité $\left|\mathbb{Z}/pq\mathbb{Z}\right| = \left|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}\right|$.

Exercice 24 Donner un exemple de groupe fini simple.

Éléments de réponse 24 Le groupe des permutations $\mathcal{A}_n$ dès que $n \geq 5$.

5.2. Seconds pas

Exercice 25 Soit $\mathrm{G} = \{a + b\sqrt{2} \,|\, a \in \mathbb{Q},\, b \in \mathbb{Q}\} \subset \mathbb{R}$.

1. Montrer que G est un groupe pour l'addition.
2. Montrer que l'ensemble des éléments non nuls de G est un groupe pour la multiplication.

Éléments de réponse 25 Soit $\mathrm{G} = \{a + b\sqrt{2} \,|\, a \in \mathbb{Q},\, b \in \mathbb{Q}\} \subset \mathbb{R}$.

1. Montrons que G est un groupe pour l'addition. Il suffit de montrer que G est un sous-groupe du groupe additif $\mathbb{R}$. Or on a
$$(a + b\sqrt{2}) - (a' + b'\sqrt{2}) = (a - a') + (b - b')\sqrt{2}.$$
2. Montrons que l'ensemble des éléments non nuls de G est un groupe pour la multiplication. Il suffit de montrer que $\mathrm{G} \smallsetminus \{0\}$ est un sous-groupe du groupe multiplicatif $\mathbb{R}^*$. Introduisons la quantité conjuguée $a' - b'\sqrt{2}$ de $a' + b'\sqrt{2}$. En multipliant numérateur et dénominateur par la quantité conjuguée nous obtenons
$$\frac{a + b\sqrt{2}}{a' + b'\sqrt{2}} = \frac{(a + b\sqrt{2})(a' + b'\sqrt{2})}{a'^2 - 2b'^2} = \frac{aa' - 2bb' + (ab' + a'b)\sqrt{2}}{a'^2 - 2b'^2}$$

Ainsi $G \setminus \{0\}$ est bien un sous-groupe du groupe multiplicatif $\mathbb{R}^*$.

Exercice 26 Soit G un groupe. Soient H et K deux sous-groupes de G.
Montrer que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.
En déduire qu'un groupe n'est jamais la réunion de deux de ses sous-groupes propres.

Éléments de réponse 26 Soit G un groupe. Soient H et K deux sous-groupes de G.
Montrons que $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$.
Si $K \subset H$ alors $H \cup K = H$ et $H \cup K$ est donc un sous-groupe de G.
Réciproquement si $H \cup K$ est un sous-groupe de G et si H n'est pas inclus dans K il existe $h \in H$ tel que $h \notin K$, en particulier h n'est pas l'élément neutre. Alors pour tout $k \in K$ nous avons $hk \in H \cup K$ (car $H \cup K$ est un sous-groupe de G) ; ainsi pour tout $k \in K$ nous avons l'alternative : hk appartient à H ou hk appartient à K. Si hk appartient à K, alors puisque K est un sous-groupe de G nous avons $h = (hk)k^{-1}$ appartient à K : contradiction avec l'hypothèse. Par conséquent hk appartient à H ; comme H est un sous-groupe de G nous avons : $k = h^{-1}(hk)$ appartient à H. Il en résulte que $K \subset H$.

Montrons qu'un groupe n'est jamais la réunion de deux de ses sous-groupes propres.
Raisonnons par l'absurde : supposons que G soit la réunion de deux de ses sous-groupes propres ; alors l'un est inclus dans l'autre d'après ce qui précède et dans ce cas le plus gros est G : contradiction avec le fait que les sous-groupes soient propres.

Exercice 27 On dit qu'un élément g d'un groupe G est indéfiniment divisible si pour tout $n \in \mathbb{N}^*$ il existe un élément h de G tel que $h^n = g$.

1. Quels sont les éléments indéfiniment divisibles de $(\mathbb{Q}, +)$? Quels sont les éléments indéfiniment divisibles de $(\mathbb{Q}_+^*, \times)$?
2. Soit $\varphi\colon (\mathbb{Q}, +) \to (\mathbb{Q}_+^*, \times)$ un homomorphisme de groupes.
   Pour tout entier $n > 0$ calculer $\varphi(n)$, puis $\varphi(1/n)$ en fonction de $\varphi(1)$.
3. Montrer que φ est constant.
4. En déduire que $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$ ne sont pas isomorphes.

Remarque : par contre $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes ; la fonction $x \mapsto \exp x$ réalise un isomorphisme entre ces deux groupes.

Éléments de réponse 27

1. Déterminons les éléments indéfiniment divisibles de $(\mathbb{Q}, +)$.

   Soit $x \in \mathbb{Q}$. Cet élément est indéfiniment divisible pour la loi d'addition car pour tout entier naturel n non nul nous avons $n \times \frac{x}{n} = x$. Autrement dit tous les éléments de $\mathbb{Q}$ sont indéfiniment divisibles pour l'addition.

   Déterminons les éléments indéfiniment divisibles de $(\mathbb{Q}_+^*, \times)$.

Soit $x \in \mathbb{Q}^*$ indéfiniment divisible. Alors pour tout $n \in \mathbb{N}^*$ $x^{1/n}$ existe et appartient à $\mathbb{Q}_+^*$. Il en résulte que $x = 1$.

2. Soit $\varphi\colon (\mathbb{Q}, +) \to (\mathbb{Q}_+^*, \times)$ un homomorphisme de groupes.

   Pour tout entier $n > 0$ calculons $\varphi(n)$, puis $\varphi(1/n)$ en fonction de $\varphi(1)$. Pour tout entier $n > 0$ nous avons

   $$\varphi(n) = \varphi(1 + 1 + \ldots + 1) = \varphi(1)^n.$$

   Pour tout entier $n > 0$ nous avons

   $$\varphi(1) = \varphi\left(n \times \frac{1}{n}\right) = \varphi\left(\frac{1}{n} + \frac{1}{n} + \ldots + \frac{1}{n}\right) = \varphi\left(\frac{1}{n}\right)^n$$

   d'où $\varphi\left(\frac{1}{n}\right) = \varphi(1)^{1/n}$.

3. Montrons que φ est constant.

   Pour tout $n > 0$ il existe $h = \varphi\left(\frac{1}{n}\right)$ tel que $h^n = \varphi(1)$. Ainsi $\varphi(1)$ est indéfiniment divisible pour la multiplication. D'après ce qui précède nous avons donc $\varphi(1) = 1$.

   Ainsi pour tout n, nous avons $\varphi(n) = 1$ et $\varphi\left(\frac{1}{n}\right) = 1$. De plus pour tout rationnel $\frac{p}{q}$ nous avons $\varphi\left(\frac{p}{q}\right) = \left(\varphi\left(\frac{1}{q}\right)\right)^p = 1$. Le morphisme φ est donc constant.

4. Montrons $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$ ne sont pas isomorphes.

   Raisonnons par l'absurde : supposons qu'il existe un isomorphisme ψ entre $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$. En particulier ψ est un homomorphisme entre ces deux groupes. D'après ce qui précède ψ est donc constant ce qui n'est pas possible pour un isomorphisme.

Exercice 28 Soit G un groupe fini. Montrer que, pour tout g et tout h dans G

1. g et g^{-1} ont même ordre ;
2. g et hgh^{-1} ont même ordre ;
3. gh et hg ont même ordre.

Éléments de réponse 28 Soit G un groupe fini.

1. Soit g dans G. Montrons que g et g^{-1} ont même ordre.

   Soit $g \in$ G. Notons k l'ordre de g et ℓ l'ordre de g^{-1}. D'une part $(g^{-1})^k = e$ donc ℓ divise k. D'autre part $g^\ell = e$ donc k divise ℓ. Finalement $k = \ell$.

2. Montrons que, pour tout g et tout h du groupe G les éléments g et hgh^{-1} ont même ordre.

   Notons k l'ordre de g et ℓ l'ordre de hgh^{-1}.

   On vérifie que $(hgh^{-1})^k = e$ donc ℓ divise k.

   Par ailleurs $h^{-1}(hgh^{-1})h$ a pour ordre k et $\left(h^{-1}(hgh^{-1})h\right)^\ell = e$ donc k divise ℓ.

   Il s'en suit que $k = \ell$.

3. Montrons que, pour tout g et tout h du groupe G, les éléments gh et hg ont même ordre.

   Désignons par k l'ordre de gh et par ℓ l'ordre de hg. Remarquons que $hg = h(gh)h^{-1}$. D'après 2. $h(gh)h^{-1}$ et gh ont même ordre donc hg et gh ont même ordre.

Exercice 29 Soit G un groupe abélien.

Montrer que les éléments d'ordre fini de G forment un sous-groupe de G.

Éléments de réponse 29 Soit G un groupe abélien. Soit H l'ensemble des éléments d'ordre fini. Puisque G est abélien, si $g \in \mathrm{H}$ et $h \in \mathrm{H}$, alors gh appartient à H ; en effet $(gh)^k = g^k h^k$ et donc l'ordre de gh divise le produit des ordres de g et h.

Soit $g \in \mathrm{H}$. Notons k l'ordre de g et ℓ l'ordre de g^{-1}. D'une part $(g^{-1})^k = e$ donc ℓ divise k. D'autre part $g^\ell = e$ donc k divise ℓ. Finalement $k = \ell$.

L'élément e est d'ordre fini donc dans H.

Ainsi H est un sous-groupe de G.

Exercice 30 Soit G un groupe possédant un seul élément d'ordre 2. Notons le g.

Montrer que g est dans le centre de G.

Éléments de réponse 30 Soit h un élément quelconque de G. Nous avons

$$(h^{-1}gh)(h^{-1}gh) = h^{-1}g(hh^{-1})gh = h^{-1}g^2h = h^{-1}h = e.$$

Or g est l'unique élément d'ordre 2 de G donc :

- ou bien $h^{-1}gh = e$ soit $g = e$: contradiction ;
- ou bien $h^{-1}gh = g$ soit $gh = hg$.

Il en résulte que g commute avec tous les éléments de G ; c'est-à-dire $g \in Z(\mathrm{G})$.

Exercice 31 Soit G un groupe abélien fini d'ordre k. Soit n un entier premier avec k. Montrer que pour tout élément g de G il existe un élément h de G tel que $g = h^n$.

(Indication : considérer l'application $\varphi\colon \mathrm{G} \to \mathrm{G}$ définie par $\varphi(h) = h^n$ et montrer que φ est un isomorphisme de G.)

Éléments de réponse 31 Soit G un groupe abélien fini d'ordre k. Soit n un entier premier avec k. Considérons l'application $\varphi\colon \mathrm{G} \to \mathrm{G}$ définie par $\varphi(g) = g^n$.

Montrons que φ est un isomorphisme.

Tout d'abord c'est un homomorphisme ; en effet G est abélien donc $(gh)^n = g^n h^n$, *i.e.* $\varphi(gh) = \varphi(g)\varphi(h)$.

Le noyau $\ker\varphi$ de φ est constitué des éléments g de G tels que $g^n = e$. Donc non seulement n est premier avec k mais n est divisible par l'ordre de g qui divise k. Par suite $n = 1$ ou $g = e$. Pour $n > 1$ nécessairement $\ker\varphi = \{e\}$. Il en résulte que φ est une injection d'un ensemble fini dans lui-même, c'est donc un homomorphisme bijectif de groupes et donc un isomorphisme.

Il s'en suit que φ est surjective, *i.e.* pour tout élément g de G il existe $h \in \mathrm{G}$ tel que $\varphi(h) = g$ soit tel que $h^n = g$.

Exercice 32 Montrer qu'un groupe d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Éléments de réponse 32 Dans un groupe d'ordre 4 tous les éléments exceptés le neutre sont d'ordre 2 ou 4.

Si G contient un élément d'ordre 4, alors G est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Sinon il n'y a que des éléments d'ordre 2 et G est isomorphe à $\left(\mathbb{Z}/4\mathbb{Z}\right)^2$. (1)

Exercice 33

1. Montrer qu'une matrice carrée d'ordre 2 à coefficients dans $\mathbb{Z}$ est dans $\mathrm{GL}(2,\mathbb{Z})$ si et seulement si elle a pour déterminant 1 ou -1.
2. Posons $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Déterminer l'ordre de A, l'ordre de B, l'ordre de AB.

Éléments de réponse 33

1. Montrons qu'une matrice carrée d'ordre 2 à coefficients dans $\mathbb{Z}$ est dans $\mathrm{GL}(2,\mathbb{Z})$ si et seulement si elle a pour déterminant 1 ou -1.

   Le déterminant d'une matrice à coefficients entiers est entier. Soit A une telle matrice qu'on suppose inversible et telle que son inverse soit aussi à coefficients entiers.

   Nous avons $\det(AA^{-1}) = \det A(\det A)^{-1} = 1$. Par suite $\det A$ est inversible dans $\mathbb{Z}$ et est égal à ± 1.

   Réciproquement soit A une matrice carrée de taille $n \times n$ à coefficients dans $\mathbb{Z}$ de déterminant égal à ± 1. En tant que matrice à coefficients réels A est inversible et son inverse a pour coefficients les quotients des mineurs de taille $(n-1) \times (n-1)$ et de $\det A = \pm 1$. Ces mineurs sont des entiers, donc ces quotients sont des entiers et l'inverse de A est à coefficients dans $\mathbb{Z}$.

---

1. Montrons qu'un groupe G où chaque élément est son propre inverse est abélien. Si tout élément de G est son propre inverse, alors pour tout couple (a,b) d'éléments de G nous avons $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. Par conséquent G est abélien.

   Montrons qu'on peut munir G d'une structure d'espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$. Pour définir une structure d'espace vectoriel sur G (qui est déjà muni d'une structure de groupe abélien) il faut définir la loi externe et la seule définition possible est

   $$[0]_a = [0], \qquad [1]_a = a.$$

   Les quatre conditions pour que cette loi externe soit celle d'un espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$ sont vérifiées.

   En déduire que, si G est d'ordre fini, l'ordre de G est une puissance de 2. Puisque G est d'ordre fini, c'est un espace vectoriel de dimension finie sur $\mathbb{Z}/2\mathbb{Z}$, soit n. Il en résulte que G est isomorphe en tant qu'espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$ à $\left(\mathbb{Z}/2\mathbb{Z}\right)^n$ et l'ordre de G est 2^n.

2. Posons $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. L'ordre de A est 4, l'ordre de B est 3, l'ordre de $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est infini car $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

Exercice 34 Montrer que $C_n = \left\{ \exp\left(\frac{2\mathbf{i}\pi k}{n}\right), \mid k \in \mathbb{Z} \right\}$ est un groupe cyclique d'ordre n pour la multiplication des nombres complexes.

Éléments de réponse 34 Montrons que $C_n = \left\{ \exp\left(\frac{2\mathbf{i}\pi k}{n}\right), \mid k \in \mathbb{Z} \right\}$ est un groupe cyclique d'ordre n pour la multiplication des nombres complexes.

Si $k = \ell \pmod n$, alors $\exp\left(\frac{2\mathbf{i}\pi k}{n}\right) = \exp\left(\frac{2\mathbf{i}\pi \ell}{n}\right)$. On peut donc définir l'application φ de $\mathbb{Z}/n\mathbb{Z}$ dans C_n par $\varphi([k]) = \exp\left(\frac{2\mathbf{i}\pi k}{n}\right)$. C'est un morphisme de groupes. De plus $\ker\varphi = \{[0]\}$ et $\mathbb{Z}/n\mathbb{Z}$ et C_n ont même ordre. Il en résulte que φ est un isomorphisme de groupes.

Le groupe $\mathbb{Z}/n\mathbb{Z}$ étant cyclique C_n est aussi un groupe cyclique.

Exercice 35 Soit p un nombre premier. Montrer qu'à isomorphisme près il y a un seul groupe d'ordre p.

Éléments de réponse 35 Soit p un nombre premier. Soit G un groupe d'ordre p. Remarquons que G n'est pas réduit à $\{e\}$ puisque $p \geq 2$. Soit g un élément de $\mathrm{G} \setminus \{e\}$; il est nécessairement d'ordre p. Le groupe G est donc cyclique. Comme il est d'ordre p, il est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Exercice 36 Soit G un groupe d'ordre $n > 2$. Montrer qu'il n'existe aucun sous-groupe de G d'ordre $n - 1$.

Éléments de réponse 36 Soit G un groupe d'ordre $n > 2$. Montrons qu'il n'existe aucun sous-groupe de G d'ordre $n - 1$.

Si $n > 2$, alors $\mathrm{pgcd}(n, n-1) = 1$ donc aucun sous-groupe ne peut avoir pour ordre $n - 1$ qui sinon diviserait n.

Exercice 37

1. Déterminer l'ensemble des éléments d'ordre fini de $\mathrm{G} = \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (pour $n \in \mathbb{N}^*$).
2. Soit H' l'ensemble des éléments d'ordre infini de G. Considérons $\mathrm{H} = \mathrm{H}' \cup \{e\}$ où e est l'élément neutre de G.

   Montrer que, même si H n'est pas vide, H n'est pas un sous-groupe de G.

Éléments de réponse 37

1. Les éléments d'ordre fini de $\mathrm{G} = \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (pour $n \in \mathbb{N}^*$) sont les couples $(0, x)$.

2. Soit H′ l'ensemble des éléments d'ordre infini de G. Considérons H = H′ ∪ {(0, [0])}, l'élément neutre de G est (0, [0]).

   Montrons que, même si H n'est pas vide, H n'est pas un sous-groupe de G. Soient (1, [0]) et (−1, [1]). Ce sont des éléments de H. Leur somme (0, [1]) n'appartient pas à H. Il s'en suit que H n'est pas un sous-groupe de G.

Exercice 38 Montrer que $\mathbb{Z} \times \mathbb{Z}$ n'est pas monogène.

Éléments de réponse 38 Montrons que $\mathbb{Z} \times \mathbb{Z}$ n'est pas monogène.

Raisonnons par l'absurde. Supposons que $\mathbb{Z}\times\mathbb{Z} = \langle (x, y)\rangle$. Notons que nécessairement $xy \neq 0$. Remarquons que $\langle (x, y)\rangle = \{(kx, ky) \mid k \in \mathbb{Z}\}$, en particulier $(x, 2y)$ n'appartient pas à $\langle (x, y)\rangle$ mais $(x, 2y)$ appartient à $\mathbb{Z} \times \mathbb{Z}$: contradiction.

Exercice 39 Montrer que $\mathbb{Z}$ et $\mathbb{Z} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ ne sont pas isomorphes.

Éléments de réponse 39 Montrer que $\mathbb{Z}$ et $\mathbb{Z} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ ne sont pas isomorphes. Le groupe $\mathbb{Z}$ ne contient aucun élément d'ordre fini alors que $(0, 1)$ est un élément d'ordre 2 de $\mathbb{Z} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. Par conséquent ces deux groupes ne sont pas isomorphes.

Exercice 40

1. Montrer que pour tout $n \in \mathbb{N}^*$ le groupe ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$ contient exactement un sous-groupe cyclique d'ordre n.
2. Montrer que tout groupe est la réunion de ses sous-groupes monogènes.
3. Comparer les ordres de deux sous-groupes cycliques G et H de ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$ qui vérifient G ⊂ H.
4. Soit α un élément de ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$; déterminer tous les sous-groupes cycliques qui le contiennent.
5. Déterminer les homomorphismes de ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ dans ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$.
6. Déterminer les homomorphismes de ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$ dans $\mathbb{Z}$.

Éléments de réponse 40

1. Montrons que pour tout $n \in \mathbb{N}^*$ le groupe ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$ contient exactement un sous-groupe cyclique d'ordre n.

   Tout élément $\overline{r} \in {}^{\mathbb{Q}}\!/_{\mathbb{Z}}$ admet un représentant r dans l'intervalle $[0, 1[$. Écrivons r sous la forme $\frac{p}{q}$ avec p et q premiers entre eux et $p < q$ ou $p = 0$.

   Soit H un sous-groupe cyclique d'ordre n, engendré par $\overline{r}$ avec $r = \frac{p}{q}$, $(p, q) = 1$ et $p < q$. Nous avons $n\overline{r} = \overline{r0}$, *i.e.* $\frac{np}{q} \in \mathbb{Z}$. Puisque p et q sont premiers entre eux q divise n ; autrement dit $n = qq'$ avec q' dans $\mathbb{Z}$ et $r = \frac{pq'}{n} = \frac{a}{n}$.

   Par conséquent le sous-groupe cyclique H est dans $\langle [1/n]\rangle$. Or $[1/n]$ est d'ordre n donc $\mathrm{H} = \langle [1/n]\rangle$ est le seul sous-groupe d'ordre n cyclique de ${}^{\mathbb{Q}}\!/_{\mathbb{Z}}$.

2. Montrons que tout groupe est la réunion de ses sous-groupes monogènes.

   Tout élément d'un groupe engendre un sous-groupe monogène donc tout groupe est réunion de ses sous-groupes monogènes.

3. Comparons les ordres de deux sous-groupes cycliques G et H de $\mathbb{Q}/\mathbb{Z}$ qui vérifient $G \subset H$.

   Soit G un sous-groupe cyclique d'ordre p contenu dans le sous-groupe cyclique H d'ordre n. Nous avons $G = \langle [1/p] \rangle$, $H = \langle [1/n] \rangle$ et p divise n.

4. Soit α un élément de $\mathbb{Q}/\mathbb{Z}$; déterminons tous les sous-groupes cycliques qui le contiennent.

   Tout élément non nul α de $\mathbb{Q}/\mathbb{Z}$ est de la forme $\alpha = \overline{p/q}$ avec $(p,q) = 1$ et $p < q$. Cet élément est donc élément du sous-groupe cyclique d'ordre q de $\mathbb{Q}/\mathbb{Z}$ soit $\langle \overline{1}q \rangle$. Ainsi l'élément α est dans tous les sous-groupes cycliques $\langle \overline{1/n} \rangle$ où q divise n. De plus tous les sous-groupes monogènes de $\mathbb{Q}/\mathbb{Z}$ sont cyclique.

5. Déterminons les homomorphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Q}/\mathbb{Z}$.

   Soit φ un homomorphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Q}/\mathbb{Z}$. L'image de φ est un sous-groupe cyclique de $\mathbb{Q}/\mathbb{Z}$ contenu dans le sous-groupe cyclique $\langle [1/n] \rangle$. Pour déterminer φ il suffit donc de se donner l'image de $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ dans $\langle \frac{\overline{1}}{n} \rangle$. Il y a donc n homomorphismes possibles.

6. Déterminons les homomorphismes de $\mathbb{Q}/\mathbb{Z}$ dans $\mathbb{Z}$.

   L'image d'un élément d'ordre fini par un homomorphisme est un élément d'ordre fini. Le groupe $\mathbb{Z}$ possède un unique élément d'ordre fini : 0. Il s'en suit que tous les éléments d'ordre fini de $\mathbb{Q}/\mathbb{Z}$ ont pour image 0. La question 2. assure que tout élément de $\mathbb{Q}/\mathbb{Z}$ est d'ordre fini. Par suite le seul homomorphisme de $\mathbb{Q}/\mathbb{Z}$ dans $\mathbb{Z}$ est l'homomorphisme nul.

Exercice 41 Montrer qu'un groupe est fini si et seulement si il n'a qu'un nombre fini de sous-groupes.

Éléments de réponse 41 Soit G un groupe fini. L'ensemble des sous-groupes de G est un sous-ensemble de l'ensemble des parties de G qui est de cardinal fini. Ainsi G ne contient qu'un nombre fini de sous-groupes.

Réciproquement soit G un groupe ne possédant qu'un nombre fini de sous-groupes. Nous avons

$$G = \bigcup_{g \in G} \langle g \rangle.$$

Les sous-groupes de la forme $\langle g \rangle$, qui sont les sous-groupes monogènes, sont en nombre fini. En fixant dans chacun d'eux un générateur nous les écrivons $\langle g_1 \rangle$, $\langle g_2 \rangle$, …, $\langle g_k \rangle$ de sorte que

$$G = \bigcup_{i=1}^{k} \langle g_i \rangle.$$

Si l'un des $\langle g_i \rangle$ est infini, il est isomorphe à $\mathbb{Z}$ et contient de ce fait une infinité de sous-groupes : contradiction avec l'hypothèse « G contient un nombre fini de sous-groupes ». Ainsi tous les

sous-groupes $\langle g_i \rangle$, $i = 1, 2, \ldots, k$, sont d'ordre fini. Leur réunion est donc de cardinal fini mais cette réunion est G. Par conséquent G est un groupe fini.

Exercice 42 Quels sont les éléments d'ordre 3 du groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$?

Éléments de réponse 42 On cherche $(\overline{x}, \overline{y}) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ tel que $3 = o(\overline{x}, \overline{y}) = \text{ppcm}(o(\overline{x}), o(\overline{y}))$, *i.e.* tel que

- $o(\overline{x}) = 1$ et $o(\overline{y}) = 3$;
- $o(\overline{x}) = 3$ et $o(\overline{y}) = 1$;
- $o(\overline{x}) = 3$ et $o(\overline{y}) = 3$.

Par ailleurs

- $o(\overline{x}) = 3$ si et seulement si $\overline{x} \in \{\overline{1}, \overline{2}\}$,
- $o(\overline{x}) = 1$ si et seulement si $\overline{x} = \overline{0}$,
- $o(\overline{y}) = 3$ si et seulement si $\overline{y} \in \{\overline{2}, \overline{4}\}$,
- $o(\overline{y}) = 1$ si et seulement si $\overline{y} = \overline{0}$.

Il en résulte que les éléments d'ordre 3 de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ sont

$$(\overline{0}, \overline{2}), \quad (\overline{0}, \overline{4}), \quad (\overline{1}, \overline{0}), \quad (\overline{2}, \overline{0}), \quad (\overline{1}, \overline{2}), \quad (\overline{1}, \overline{4}), \quad (\overline{2}, \overline{2}), \quad (\overline{2}, \overline{4}).$$

Exercice 43 Étudier le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Éléments de réponse 43 La table de multiplication de $\mathrm{G} = \mathrm{Aut}\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) = \{e, a_1, a_2, a_3\}$ est :

- $\forall i \; ea_i = a_i$;
- $\forall\, i \; a_i^2 = e$;
- $\forall\, i \; \forall\, j \neq i \; a_i a_j = a_k$ où $k \neq i$, $k \neq j$, où $i, j, k \in \{1, 2, 3\}$.

Tout automorphisme φ de G laisse fixe e. Il permute donc les autres éléments a_1, a_2 et a_3.

Réciproquement pour toute permutation φ de ces trois éléments, en posant $\varphi(e) = e$, on obtient une bijection de G sur G qui respecte la table de multiplication ci-dessus. C'est donc un automorphisme.

Ainsi Aut(G) est d'ordre $3! = 6$ et isomorphe au groupe $\mathcal{S}_3$ des permutations de $\{1, 2, 3\}$.

Exercice 44 Donner un exemple de groupe et de sous-groupes dont la réunion n'est pas un sous-groupe.

Éléments de réponse 44 Dans $\mathbb{Z}$ la réunion des sous-groupes $2\mathbb{Z}$ et $3\mathbb{Z}$ n'est pas un groupe. En effet la somme $2 + 3 = 5$ d'un élément de $2\mathbb{Z}$ et d'un élément de $3\mathbb{Z}$ n'est ni multiple de 2, ni multiple de 3.

Exercice 45 Dans les groupes suivants, donner un exemple d'élément d'ordre 4 s'il en existe, sinon donner un argument pour justifier qu'il n'y en a pas :

(a) le groupe linéaire $\mathrm{GL}(2,\mathbb{R})$;
(b) le groupe alterné $\mathcal{A}_8$;
(c) le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}(3,\mathbb{R})$ des rotations de $\mathbb{R}^3$ préservant un tétraèdre régulier T ;
(d) un groupe d'ordre 16 quelconque (attention il s'agit de déterminer si *tout* sous-groupe d'ordre 16 admet un élément d'ordre 4).

Éléments de réponse 45
(a) La rotation d'angle $\pi/2$ est un exemple d'élément d'ordre 4 dans $\mathrm{GL}(2,\mathbb{R})$, sa matrice est $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
(b) $(1\,2\,3\,4)(5\,6)$ est un exemple d'élément d'ordre 4 dans $\mathcal{A}_8$.
(c) Le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}(3,\mathbb{R})$ ne contient pas d'élément d'ordre 4. Il contient douze éléments dont huit d'ordre 3, trois d'ordre 2 et l'identité.
Autre justification possible : $\mathrm{Isom}^+(T) \subset \mathrm{SO}(3,\mathbb{R})$ est isomorphe à $\mathcal{A}_4$ et $\mathcal{A}_4$ ne contient pas d'élément d'ordre 4 (les 4-cycles ne sont pas de signature 1).
(d) Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe d'ordre 16 qui contient le neutre d'ordre 1 et des éléments d'ordre 2.

Exercice 46 Soit G un groupe abélien infini. Montrer que l'ensemble T des éléments d'ordre fini de G est un sous-groupe de G.
Si $\mathrm{T} = \{e\}$, on dit que G est sans torsion.
Montrer que G/T est sans torsion.

Éléments de réponse 46 Puisque $o(e) = 1$, on a $e \in \mathrm{T}$. Soient x, $y \in \mathrm{T}$ d'ordres k, $m \in \mathbb{N}^*$. On a $(xy)^{km} = (x^k)^m (y^m)^k = e$ donc $xy \in \mathrm{T}$. Comme $o(x) = o(x^{-1})$, on a $x^{-1} \in \mathrm{T}$. Ainsi T est un sous-groupe de G.

Considérons l'application canonique $\varphi\colon \mathrm{G} \to \mathrm{G}/\mathrm{T}$. Soit $a \in \mathrm{G}/\mathrm{T}$ d'ordre fini $s \in \mathbb{N}^*$. Il existe $x \in \mathrm{G}$ tel que $a = \varphi(x)$. On a

$$\varphi(x^s) = a^s = e$$

donc $x^s \in \mathrm{T} = \ker\varphi$. Il existe donc $r \in \mathbb{N}^*$ tel que $x^{sr} = (x^s)^r = e$ ce qui prouve que $x \in \mathrm{T}$ et donc que $a = \varphi(x) = e$. Par suite G/T est sans torsion.

Exercice 47 Soit G un groupe tel que $g^2 = e$ pour tout g dans G.
Montrer que G est abélien.

Éléments de réponse 47 Pour tous g, h dans G on a $(gh)^2 = e$, soit $ghgh = e$, d'où $(ghgh)(hg) = hg$. Mais $(ghgh)(hg) = ghgh^2g$. Or h appartient à G donc $h^2 = e$ et $ghgh^2g = ghg^2$. Puisque g est dans G on a $g^2 = e$ et $ghg^2 = gh$. Ainsi $(ghgh)(hg) = hg$ se réécrit $gh = hg$.

Exercice 48 Soit G un groupe fini.
a) Montrer que des éléments conjugués dans G sont de même ordre.

b) Deux éléments de même ordre dans G sont-ils toujours conjugués ?

c) Trouver tous les groupes abéliens finis G pour lesquels la question précédente a une réponse positive. Un exemple non abélien ?

Éléments de réponse 48

a) Soient g, h dans G et n dans $\mathbb{N}$. On a $(hgh^{-1})^n = hg^nh^{-1}$. Ainsi $(hgh^{-1})^n = e$ si et seulement si $hg^nh^{-1} = e$ si et seulement si $g^n = h^{-1}eh$ autrement dit si et seulement si $g^n = e$.

b) Deux éléments de même ordre dans un groupe fini ne sont pas toujours conjugués. Considérons par exemple le groupe $\mathbb{Z}/3\mathbb{Z}$; il contient deux éléments d'ordre 3 qui ne sont pas conjugués.

c) Soit G un groupe abélien fini. Les classes de conjugaison de G sont réduites à un élément. La question précédente a une réponse positive si et seulement si tous les éléments de G ont des ordres distincts. Or si un groupe contient un élément g d'ordre $n \geq 3$, alors il admet d'autres éléments d'ordre n, par exemple g^{-1}. Ainsi les seuls groupes abéliens qui conviennent sont le groupe trivial et le groupe $\mathbb{Z}/2\mathbb{Z}$.

Si G est le groupe des permutations $\mathcal{S}_3$, alors les éléments d'ordre 2 sont les transpositions (1 2), (1 3) et (2 3) qui sont conjuguées et les éléments d'ordre 3 sont les 3-cyles (1 2 3) et (1 3 2) qui sont également conjugués. Le groupe $G = \mathcal{S}_3$ est donc un groupe fini non abélien tel que deux éléments de même ordre dans G sont toujours conjugués.

Exercice 49 Soit $\varphi\colon \mathrm{G}_1 \to \mathrm{G}_2$ un morphisme de groupes. Soit g un élément de G_1 d'ordre fini.

Montrer que l'ordre de $\varphi(g)$ divise l'ordre de g.

Éléments de réponse 49 Soit n l'ordre de g. On a $g^n = e$ donc $\varphi(g)^n = \varphi(g^n) = \varphi(e) = e$, autrement dit l'ordre de $\varphi(g)$ divise n.

Exercice 50

a) Soit G un sous-groupe de $(\mathbb{R}, +)$ non réduit à $\{0\}$. Montrer que G est ou bien dense dans $\mathbb{R}$, ou bien monogène, *i.e.* de la forme $a\mathbb{Z}$ avec $a > 0$ (donc discret).

b) Soient α et β deux réels non nuls. Discuter de la nature du sous-groupe additif qu'ils engendrent.

c) Soit $\beta \notin \mathbb{Q}$. Montrer que $\mathbb{N}\beta + \mathbb{Z}$ est dense dans $\mathbb{R}$.

d) Soit $\vartheta \notin 2\pi\mathbb{Q}$. Montrer que $\{\exp(\mathbf{i}n\vartheta) \,|\, n \in \mathbb{N}\}$ est dense dans le cercle unité $\mathbb{S}^2$ de $\mathbb{C}$.

En déduire

i) qu'un sous-groupe G de $\mathbb{S}^1$ est soit fini (auquel cas égal au groupe des racines $n$ièmes de l'unité où $n = |\mathrm{G}|$), soit dense dans $\mathbb{S}^1$;

ii) les valeurs d'adhérence de la suite $(\sin(n))_{n\geq 0}$.

Éléments de réponse 50

a) Soit G un sous-groupe de $(\mathbb{R},+)$ non réduit à $\{0\}$. Montrons que G est ou bien dense dans $\mathbb{R}$, ou bien monogène, *i.e.* de la forme $a\mathbb{Z}$ avec $a>0$ (donc discret).

Si G est monogène, *i.e.* si $\mathrm{G}=a\mathbb{Z}$, avec $a>0$, alors a est le plus petit élément strictement positif de G. Si G est dense dans $\mathbb{R}$, alors $\mathrm{G}\cap\mathbb{R}_+^*$ n'a pas de plus petit élément mais une borne inférieure non nulle. On introduit donc

$$\mathrm{G}_+=\mathrm{G}\cap\mathbb{R}_+^* \qquad\qquad a=\inf \mathrm{G}_+$$

Le réel $a\geq 0$ est bien défini car G_+ est non vide et minorée. En effet il existe un élément g dans G non nul donc x ou $-x$ est dans G_+ qui est minoré par 0.

On va distinguer le cas $a>0$ du cas $a=0$.

◇ Supposons $a>0$. Montrons que a appartient à G puis que $\mathrm{G}=a\mathbb{Z}$.
Raisonnons par l'absurde : supposons que a n'appartienne pas à G. Puisque $a>0$, on a $2a>a$. Il existe g dans G_+ tel que $g<2a$. Comme a n'appartient pas à G, on a les inégalités $a<g<2a$. Il existe alors h dans G_+ tel que $h<g$. On a $a<h<g<2a$ car a n'appartient pas à G. De plus comme g et h appatiennent à G, la différence $g-h$ appartient à G et on a même $g-h$ appartient à G_+. D'une part $a<h$ donc $a-h<0$ et $2a-h<a$, d'autre part $g<2a$ donc $g-h<2a-h$. Par conséquent $g-h<a$: contradiction avec la définition de a. Par suite a appartient à G. Ainsi le groupe $a\mathbb{Z}$ engendré par a est inclus dans G.
Réciproquement soit g un élément de G. Posons $k=E\left(\frac{g}{a}\right)\in\mathbb{Z}$. Puisque G est un groupe le réel $g-ak$ appartient à G. Comme $k\leq\frac{g}{a}<k+1$ on a $0\leq g-ak<a=\min \mathrm{G}_+$. Nécessairement $g-ak=0$ et $g=ak\in a\mathbb{Z}$. Il en résulte que $\mathrm{G}=a\mathbb{Z}$.

◇ Supposons que $a=0$. Montrons qu'alors G est dense dans $\mathbb{R}$, autrement dit que G rencontre tout intervalle ouvert de $\mathbb{R}$. Soit $I=]\alpha,\beta[$ un intervalle ouvert de $\mathbb{R}$. Comme $a=0$ il existe $g\in\mathrm{G}$ tel que $0<g<\beta-\alpha$. Le sous-groupe $g\mathbb{Z}$ engendré par g est inclus dans G et intersecte I (sinon il existerait $k\in\mathbb{Z}$ tel que $I\subset]kg,(k+1)g[$ ce qui contredirait l'inégalité $g<\beta-\alpha$). Il s'en suit que G est dense dans $\mathbb{R}$.

b) Il s'agit d'étudier le groupe $\mathrm{G}=\alpha\mathbb{Z}+\beta\mathbb{Z}\neq\{0\}$.

Supposons qu'il existe $a>0$ tel que $\mathrm{G}=a\mathbb{Z}$. Puisque α et β appartiennent à G, il existe k et ℓ dans $\mathbb{Z}$ tels que $\alpha=ka$ et $\beta=\ell a$. Le rapport $\frac{\alpha}{\beta}$ s'écrit aussi $\frac{k}{\ell}$ et appartient à $\mathbb{Q}$.

Réciproquement supposons que $\frac{\alpha}{\beta}$ soit rationnel. Écrivons $\frac{\alpha}{\beta}$ sous la forme $\frac{k}{\ell}$ avec k et ℓ premiers entre eux. Alors

$$\alpha\mathbb{Z}+\beta\mathbb{Z}=\beta\left(\frac{k}{\ell}\mathbb{Z}+\mathbb{Z}\right)=\frac{\beta}{\ell}(k\mathbb{Z}+\ell\mathbb{Z})=\frac{\beta}{\ell}\mathbb{Z}$$

car k et ℓ sont premiers entre eux.

Ainsi si $\frac{\alpha}{\beta}$ appartient à $\mathbb{Q}$, alors G est monogène et sinon G est dense dans $\mathbb{R}$.

c) Soit $\beta \notin \mathbb{Q}$. Montrons que $\mathbb{N}\beta + \mathbb{Z}$ est dense dans $\mathbb{R}$.

Le sous-groupe additif $\mathrm{G} = \mathbb{Z} + \beta\mathbb{Z}$ de $\mathbb{R}$ est dense d'après b). Montrons que l'ensemble $\mathbb{N}\beta + \mathbb{Z}$ reste encore dense. Soient $a < b$ deux réels. Nous pouvons trouver un élément $x = v\beta + u \in \mathrm{G}$ tel que $0 < x < b - a$.

- ◇ Supposons que v soit un entier naturel, *i.e.* que x appartienne à $\mathbb{N}\beta + \mathbb{Z}$. Choisissons un entier $n_0 < a$. Les éléments de la suite $(kx + n_0)_{k\geq 0}$ appartiennent à $\mathbb{N}\beta + \mathbb{Z}$ et un argument analogue à celui de a) assure que l'un d'eux au moins appartient à $]a, b[$.
- ◇ Supposons que $v < 0$. Alors $-x$ appartient à $\mathbb{N}\beta + \mathbb{Z}$ et $-(b-a) < -x < 0$. Choisissons $n_0 \in \mathbb{Z}$ avec $n_0 > b$. Alors au moins un élément de la suite $(n_0 - kx)_{k\geq 0}$ appartient à $]a, b[$.

d) Soit $\vartheta \notin 2\pi\mathbb{Q}$. Montrons que $\{\exp(\mathbf{i}n\vartheta) \,|\, n \in \mathbb{N}\}$ est dense dans le cercle unité $\mathbb{S}^1$ de $\mathbb{C}$.

Posons $\Omega = \{\exp(\mathbf{i}n\vartheta) \,|\, n \in \mathbb{N}\}$. Il s'agit de l'image par l'application $f\colon x \mapsto \exp(2\mathbf{i}\pi x)$ de l'ensemble $\mathbb{Z} + \frac{\vartheta}{2\pi}\mathbb{N}$. Puisque f est continue et que Ω est dense dans $\mathbb{R}$ d'après c) l'image $f(\Omega)$ de Ω par f est dense dans $f(\mathbb{R}) = \mathbb{S}^1$.

i) D'après a) un sous-groupe G de $\mathbb{S}^1$ est soit fini (auquel cas égal au groupe des racines $n$ièmes de l'unité où $n = |\mathrm{G}|$), soit dense dans $\mathbb{S}^1$.

ii) Si $\vartheta = 1$, alors $\frac{1}{\pi}$ n'est pas rationnel et l'ensemble $\{\exp(\mathbf{i}n) \,|\, n \in \mathbb{N}\}$ est dense dans $\mathbb{S}^1$. Puisque l'application qui à un nombre complexe associe sa partie imaginaire est continue, l'ensemble $\{\sin(n) \,|\, n \in \mathbb{N}\}$ est dense dans $[-1, 1]$. Pour tout $-1 \leq a \leq 1$, pour tout $\varepsilon > 0$ et pour tout $N \in \mathbb{N}$ nous sommes alors assurés de trouver un entier $n \geq N$ tel que $|\sin(n) - a| \leq \varepsilon$. Autrement dit tout réel de $[-1, 1]$ est une valeur d'adhérence de la suite $(\sin(n))_{n\geq 0}$. L'autre inclusion est directe. Finalement l'ensemble des valeurs d'adhérences de la suite $(\sin(n))_{n\geq 0}$ est le segment $[-1, 1]$.

Exercice 51 Montrer que le morphisme $\xi\colon \mathbb{R} \to \mathbb{U}$, $x \mapsto \exp(\mathbf{i}x)$ est un morphisme surjectif du groupe additif $\mathbb{R}$ dans le groupe multiplicatif $\mathbb{U}$.

Éléments de réponse 51

Exercice 52 Montrer que si $n \geq 2$, le seul sous-groupe fini de $(\mathbb{C}^*, \cdot)$ de cardinal n est μ_n [2].

Éléments de réponse 52 Soit G un sous-groupe fini de $(\mathbb{C}^*, \cdot)$ de cardinal n. Soit g un élément de G. L'ordre de g divise n ; en particulier $g^n = \mathrm{id}$. Il en résulte que $\mathrm{G} \subset \mu_n$.

De plus $|\mathrm{G}| = |\mu_n|$.

Il en résulte que $\mathrm{G} = \mu_n$.

2. μ_n désigne le groupe des racines $n$ième de l'unité.

5.3. Actions de groupes, sous-groupes distingués

Exercice 53 Soit $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ le groupe des matrices inversibles 2×2 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.

1. Quel est l'ordre de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$?
2. Soit E un espace vectoriel de dimension 2 sur le corps $\mathbb{Z}/2\mathbb{Z}$. Définir une action non triviale de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sur E.
3. En déduire que $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est isomorphe au groupe $\mathcal{S}_3$ des permutations de l'ensemble $\{1, 2, 3\}$.

Éléments de réponse 53

1. Les éléments de $\mathrm{G} = \mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sont les matrices inversibles dans $\mathbb{Z}/2\mathbb{Z}$. En voici la liste
$$\begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{0} & \overline{1} \end{pmatrix} \quad \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix}$$
Il en résulte que G est un groupe d'ordre 6.
2. Soit E un espace vectoriel de dimension 2 sur le corps $\mathbb{Z}/2\mathbb{Z}$. Définissons une action non triviale de $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ sur E.

   À chaque base (v, w) de l'espace vectoriel E correspond une action de G sur E : pour $g \in \mathrm{G}$ et $u \in E$ on définit $g * u \in E$ comme l'image du vecteur u par l'application linéaire de matrice g dans la base (v, w).
3. Montrons que $\mathrm{GL}\left(2, \mathbb{Z}/2\mathbb{Z}\right)$ est isomorphe au groupe $\mathcal{S}_3$ des permutations de l'ensemble $\{1, 2, 3\}$.

   Fixons une base de E et considérons l'action correspondante de G sur E. Pour tout $g \in \mathrm{G}$ l'application $\varphi_g \colon u \mapsto g * u$ est définie par les images des vecteurs non nuls de E ; en effet le vecteur nul a toujours pour image lui-même.

   Ainsi à tout élément de G est associée une permutation de $E \smallsetminus \{0\}$. Or E compte $2^2 = 4$ éléments. Soient v_1, v_2 et v_3 les trois vecteurs non nuls de E. Alors
$$g \mapsto \left((v_1, v_2, v_3) \mapsto (g * v_1, g * v_2, g * v_3)\right)$$
   définit un homomorphisme de groupes de G dans $\mathcal{S}_3$. Cet homomorphisme est injectif. Par suite G est isomorphe à un sous-groupe de $\mathcal{S}_3$. Puisque G et $\mathcal{S}_3$ ont même ordre, G est isomorphe à $\mathcal{S}_3$.

Exercice 54 Soit p un nombre premier. Soit $n \geq 1$ un entier. Soient G un groupe d'ordre p^n et $Z(\mathrm{G})$ son centre. Considérons un sous-groupe distingué H de G non trivial.

1. Montrer que $\mathrm{H} \cap Z(\mathrm{G}) \neq \{e\}$.
2. Montrer que l'ordre de $Z(\mathrm{G})$ est > 1.

Indication : faire agir G par conjugaison sur H.

Éléments de réponse 54 Soit p un nombre premier. Soit $n \geq 1$ un entier. Soient G un groupe d'ordre p^n et $Z(\mathrm{G})$ son centre. Considérons un sous-groupe distingué H de G non trivial.

1. Montrons que $\mathrm{H} \cap Z(\mathrm{G}) \neq \{e\}$. Faisons agir G par conjugaison sur H ; notons que c'est possible car H étant distingué dans G nous avons $\forall\, g \in \mathrm{G}$, $g\mathrm{H}g^{-1} \subset \mathrm{H}$.

   L'ordre de H est une puissance de p soit p^β car $|\mathrm{H}|$ divise $|\mathrm{G}|$ qui est une puissance de p. L'ordre de H est aussi somme des cardinaux des orbites pour cette action ; chacune de ces orbites a pour cardinal un diviseur de $|\mathrm{G}|$, c'est-à-dire de p^n donc une puissance de p.

   Raisonnons par l'absurde : supposons que $Z(\mathrm{G}) \cap \mathrm{H} = \{e\}$; alors une seule des orbites est réduite à un seul élément : l'orbite de e. Nous avons alors

   $$|\mathrm{H}| = p^\beta = 1 + \text{ somme de puissances de } p$$

   contradiction. Par suite $Z(\mathrm{G}) \cap \mathrm{H} \neq \{e\}$.
2. Montrons que l'ordre de $Z(\mathrm{G})$ est > 1. Nous allons encore appliquer la formule des classes. Remarquons que les orbites de G pour l'action de G par conjugaison sur lui-même ont pour cardinal des puissances de p ; en effet ces cardinaux sont des diviseurs de $|\mathrm{G}| = p^n$.

   Raisonnons par l'absurde : supposons que $|Z(\mathrm{G})| = 1$, alors

   $$p^n = |\mathrm{G}| = 1 + \text{ somme de puissances de } p$$

   contradiction. Il en résulte que $|Z(\mathrm{G})| > 1$.

Exercice 55 Soient G un groupe fini et $Z(\mathrm{G})$ son centre. Considérons l'action de G sur lui-même par conjugaison.

1. Supposons G non abélien. Soit g un élément de $\mathrm{G} \setminus Z(\mathrm{G})$; notons $\mathrm{Stab}(g)$ le stabilisateur de g.

   Montrer que $Z(\mathrm{G}) \subset \mathrm{Stab}(g) \subset \mathrm{G}$ (les inclusions sont strictes).
2. En déduire que si G n'est pas abélien, alors $Z(\mathrm{G})$ est un sous-groupe de G dont l'indice est strictement supérieur au plus petit nombre premier divisant l'ordre $|\mathrm{G}|$ de G.
3. Soit p un nombre premier. Soit n un entier.

   Quelles sont les valeurs possibles pour l'ordre du centre d'un groupe d'ordre p^n ?

   Quel est le centre d'un groupe d'ordre p^2 ?

   Quel est le centre d'un groupe non abélien d'ordre p^3 ?
4. Donner un exemple de groupe d'ordre p^3 non abélien.
5. Montrer que si G est d'ordre p^2, alors $\mathrm{G} \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Éléments de réponse 55 Soient G un groupe fini et $Z(\mathrm{G})$ son centre. Considérons l'action de G sur lui-même par conjugaison.

1. Supposons G non abélien. Soit g un élément de $\mathrm{G} \setminus Z(\mathrm{G})$; notons $\mathrm{Stab}(g)$ le stabilisateur de g.

   Montrons que $Z(\mathrm{G}) \subset \mathrm{Stab}(g) \subset \mathrm{G}$ (les inclusions sont strictes).

   L'inclusion $Z(\mathrm{G}) \subseteq \mathrm{Stab}(g)$ est claire.

   Soit $g \in \mathrm{G} \setminus Z(\mathrm{G})$ (un tel élément existe car G n'est pas abélien). Remarquons que g appartient à $\mathrm{Stab}(g)$; en effet $ggg^{-1} = g$. Par suite $Z(\mathrm{G})$ est strictement inclus dans $\mathrm{Stab}(g)$.

   Soit $g \in \mathrm{G} \setminus Z(\mathrm{G})$ (un tel élément existe car G n'est pas abélien). Puisque $g \notin Z(\mathrm{G})$ il existe un élément $h \in \mathrm{G}$ qui ne commute pas avec g donc qui n'appartient pas à $\mathrm{Stab}(g)$. Il en résulte que $\mathrm{Stab}(g)$ est un sous-groupe propre de G.

2. Supposons que G ne soit pas abélien, montrons qu'alors $Z(\mathrm{G})$ est un sous-groupe de G dont l'indice est strictement supérieur au plus petit nombre premier p divisant l'ordre $|\mathrm{G}|$ de G.

   D'après 1. si G n'est pas abélien et si g appartient à $\mathrm{G} \setminus Z(\mathrm{G})$, alors l'indice de $|\mathrm{G} : Z(\mathrm{G})| > |\mathrm{G} : \mathrm{Stab}(g)|$. Mais $|\mathrm{G} : \mathrm{Stab}(g)| \geq p$ car $|\mathrm{G} : \mathrm{Stab}(g)|$ divise $|\mathrm{G}|$. Par suite $|\mathrm{G} : Z(\mathrm{G})| > p$.

3. Soit p un nombre premier. Soit n un entier.

   Donnons les valeurs possibles pour l'ordre du centre d'un groupe d'ordre p^n.

   Si G est abélien, alors $|Z(\mathrm{G})| = p^n$.

   Si G n'est pas abélien, alors $|\mathrm{G} : Z(\mathrm{G})| > p$ donc $|Z(\mathrm{G})| < p^{n-1}$. L'exercice précédent assure que $Z(\mathrm{G})$ n'est pas réduit à l'élément neutre donc $|Z(\mathrm{G})| \geq p$. Finalement lorsque G n'est pas abélien, nous avons

   $$|Z(\mathrm{G})| \in \{p, p^2, \ldots, p^{n-2}\}$$

   Si $n = 2$, le groupe G est nécessairement abélien.

   Déterminons le centre d'un groupe d'ordre p^2. Le centre d'un groupe G d'ordre p^2 est donc G tout entier.

   Déterminons le centre d'un groupe non abélien d'ordre p^3. Le centre d'un groupe non abélien d'ordre p^3 est d'ordre p.

4. Donnons un exemple de groupe d'ordre p^3 non abélien.

   Le groupe des quaternions est un groupe d'ordre 2^3 (ici $p = 2$) et n'est pas abélien.

5. Montrons que si G est d'ordre p^2, alors $\mathrm{G} \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

   Soit G un groupe d'ordre p^2. Il est abélien. Nous avons l'alternative suivante :
   — ou bien G contient un élément d'ordre p^2 auquel cas G est cyclique et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$;

— ou bien tous les éléments de $\mathrm{G} \smallsetminus \{e\}$ sont d'ordre p. Soient x et y deux éléments de $\mathrm{G} \smallsetminus \{e\}$ tels que $y \notin \langle x \rangle$. Alors $\langle x \rangle \cap \langle y \rangle = \{e\}$. En effet le sous-groupe $\langle x \rangle \cap \langle y \rangle$ est d'ordre strictement inférieur à p et d'ordre divisant p donc d'ordre 1. Puisque tout sous-groupe du groupe abélien G est distingué G est isomorphe à $\langle x \rangle \times \langle y \rangle$ (Exercice 10). Or $\langle x \rangle \simeq \langle y \rangle \simeq \mathbb{Z}/p\mathbb{Z}$. Ainsi $\mathrm{G} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 56 Soient E un ensemble et G un groupe opérant sur E. Soient g et h des éléments de E appartenant à la même orbite.

Montrer que les stabilisateurs Stab_g et Stab_h sont des sous-groupes conjugués de G.

En déduire que Stab_g et Stab_h ont même ordre.

Éléments de réponse 56 Soient E un ensemble et G un groupe opérant sur E. Soient g et h des éléments de E appartenant à la même orbite. Alors il existe x dans G tel que $h = x \cdot g$.

Soit $y \in \mathrm{Stab}_g$. Alors $y \cdot g = g$. De plus d'une part $y \cdot g = y \cdot (x^{-1}h)$ et d'autre part $g = x^{-1}h$. Par conséquent $y \cdot (x^{-1}h) = x^{-1}h$, soit $xyx^{-1} \cdot h = h$ c'est-à-dire xyx^{-1} appartient à Stab_h. Autrement dit $x\mathrm{Stab}_g x^{-1} \subset \mathrm{Stab}_h$.

Un raisonnement similaire conduit à $\mathrm{Stab}_h \subset x\mathrm{Stab}_g x^{-1}$.

Il s'en suit que $\mathrm{Stab}_h = x\mathrm{Stab}_g x^{-1}$.

L'application $y \mapsto xyx^{-1}$ est un automorphisme de G. C'est donc une bijection et l'image de Stab_g par cet automorphisme est Stab_h. Ces deux ensembles ont donc même cardinal.

Exercice 57 Soit E un ensemble fini. Soit G un groupe fini qui opère sur E. Pour tout g dans G on définit

$$E^g = \{s \in E \,|\, gs = s\}.$$

Autrement dit E^g est l'ensemble des points fixes de E sous l'action de g. Pour $s \in E$, on note G_s le fixateur de s pour l'action de G sur E.

1. Construire la table de l'opération

$$\varphi\colon \mathrm{G} \times E \to \{ \text{ vrai=V, faux=F } \}$$

définie par

$$\begin{cases} \varphi(g,s) = V \text{ si } gs = s \\ \varphi(g,s) = F \text{ sinon} \end{cases}$$

dans le cas où $\mathrm{G} = \mathrm{D}_6$ et $E = \{A, B, C\}$ où ABC est un triangle équilatéral.

2. Démontrer que $\displaystyle\sum_{s \in E} |\mathrm{G}_s| = \sum_{g \in \mathrm{G}} \mathrm{card}(E^g)$.

3. En déduire la formule de Burnside

$$|\mathrm{G}| \times \text{ le nombre d'orbites } = \sum_{g \in \mathrm{G}} \mathrm{card}(E^g).$$

Éléments de réponse 57

1. Construisons la table de l'opération

$$\varphi\colon \mathrm{G} \times E \to \{ \text{ vrai=V, faux=F } \}$$

définie par

$$\begin{cases} \varphi(g,s) = V \text{ si } gs = s \\ \varphi(g,s) = F \text{ sinon} \end{cases}$$

dans le cas où $\mathrm{G} = \mathrm{D}_6$ et $E = \{A, B, C\}$ où ABC est un triangle équilatéral.

Désignons par O le centre de gravité du triangle équilatéral ABC et par ρ la rotation de centre O et d'angle $\frac{2\pi}{3}$. Soient s_A, s_B et s_C les symétries d'axes respectifs AO, BO et CO.

Nous obtenons la table suivante

	A	B	C
id	V	V	V
ρ	F	F	F
ρ^2	F	F	F
s_A	V	F	F
s_B	F	V	F
s_C	F	F	V

En effet

(a) $\mathrm{id}(A) = A$, $\mathrm{id}(B) = B$ et $\mathrm{id}(C) = C$;

(b) $\rho(A) \in \{B, C\}$, $\rho(B) \in \{A, C\}$ et $\rho(C) \in \{A, B\}$;

(c) $\rho^2(A) \in \{B, C\}$, $\rho^2(B) \in \{A, C\}$ et $\rho^2(C) \in \{A, B\}$;

(d) $s_A(A) = A$, $s_A(B) = C$ et $s_A(C) = B$;

(e) $s_B(B) = B$, $s_B(A) = C$ et $s_B(C) = A$;

(f) $s_C(C) = C$, $s_C(A) = B$ et $s_C(B) = A$.

2. Montrons que $\displaystyle\sum_{s\in E} |\mathrm{G}_s| = \sum_{g\in \mathrm{G}} \mathrm{card}(E^g)$.

Posons $p = |\mathrm{G}|$. Notons g_1, g_2, …, g_p les éléments de G. Posons $q = \mathrm{card}(E)$. Notons s_1, s_2, …, s_q les éléments de E.

D'une part

$$\begin{aligned} \varphi^{-1}(V) &= \{(g,s) \in \mathrm{G} \times E \,|\, gs = s\} \\ &= \{(g,s) \in \mathrm{G} \times E \,|\, s \in E^g\} \\ &= \{g_1\} \times E^{g_1} \cup \{g_2\} \times E^{g_2} \cup \ldots \cup \{g_p\} \times E^{g_p} \end{aligned}$$

ce qui conduit à

$$\mathrm{card}(\varphi^{-1}(V)) = \sum_{g\in \mathrm{G}} \mathrm{card}(E^g)$$

D'autre part

$$\begin{aligned}\varphi^{-1}(V) &= \{(g,s)\in \mathrm{G}\times E \,|\, gs=s\}\\ &= \{(g,s)\in \mathrm{G}\times E \,|\, g\in \mathrm{G}_s\}\\ &= \mathrm{G}_{s_1}\times\{s_1\}\cup \mathrm{G}_{s_2}\times\{s_2\}\cup\ldots\cup \mathrm{G}_{s_q}\times\{s_q\}\end{aligned}$$

ce qui entraîne

$$\mathrm{card}(\varphi^{-1}(V)) = \sum_{s\in E} |\mathrm{G}_s|.$$

Il en résulte que

$$\sum_{g\in \mathrm{G}} \mathrm{card}(E^g) = \sum_{s\in E} |\mathrm{G}_s|.$$

3. Si s est un élément de E, on désigne par $\mathcal{O}_s$ l'orbite de s sous l'action de G. On sait que $|\mathrm{G}_s| = \frac{|\mathrm{G}|}{\mathrm{card}(\mathcal{O}_s)}$. Par suite

$$\sum_{g\in \mathrm{G}} \mathrm{card}(E^g) = |\mathrm{G}|\left(\frac{1}{\mathrm{card}(\mathcal{O}_{s_1})}+\frac{1}{\mathrm{card}(\mathcal{O}_{s_2})}+\ldots+\frac{1}{\mathrm{card}(\mathcal{O}_{s_q})}\right)$$

Soient σ_1, σ_2, …, σ_r des éléments de E tels que E est la réunion disjointe des $\mathcal{O}_{\sigma_i}$ pour $1\leq i\leq r$. Nous avons

$$\sum_{s\in\mathcal{O}_{\sigma_i}} \frac{1}{\mathrm{card}(\mathcal{O}_s)} = \sum_{s\in\mathcal{O}_{\sigma_i}} \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})} = \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})}\sum_{s\in\mathcal{O}_{\sigma_i}} 1 = \frac{1}{\mathrm{card}(\mathcal{O}_{\sigma_i})}\times \mathrm{card}(\mathcal{O}_{\sigma_i}) = 1$$

d'où la formule de Burnside.

Exercice 58 Combien $(\mathbb{F}_2)^n$ admet-il de sous-espaces vectoriels de dimension k ?

Éléments de réponse 58 Soit $0\leq k\leq n$. Le groupe $\mathrm{GL}(n,\mathbb{F}_2)$ agit transitivement sur l'ensemble Λ_k des sous-espaces vectoriels de dimension k de $(\mathbb{F}_2)^n$. L'ordre du groupe $\mathrm{GL}(n,\mathbb{F}_2)$ est

$$\begin{aligned}&(2^n-1)\times(2^n-2)\times\ldots\times(2^n-2^{n-1})\\ &\quad=(2^n-1)\times 2\times(2^{n-1}-1)\times\ldots\times 2^{n-1}\times(2-1)\\ &\quad=2\times 2^2\times\ldots\times 2^{n-1}\times(2^n-1)\times(2^{n-1}-1)\times\ldots\times(2-1)\\ &\quad=2^{1+2+\ldots+(n-1)}\times(2^n-1)\times(2^{n-1}-1)\times\ldots\times(2-1)\\ &\quad=2^{\frac{n(n-1)}{2}}\times(2^n-1)\times(2^{n-1}-1)\times\ldots\times(2-1)\end{aligned}$$

Le stabilisateur de $(\mathbb{F}_2)^k\times\{0_{n-k}\}$ sous l'action de $\mathrm{GL}(n,\mathbb{F}_2)$ sur Λ_k est d'ordre [3]

$$\underbrace{(2^k-1)(2^k-2)\ldots(2^k-2^{k-1})}_{|\mathrm{GL}(k,\mathbb{F}_2)|}\times(2^n-2^k)(2^n-2^{k+1})\ldots(2^n-2^{n-1}).$$

3. cela revient à choisir une matrice de $\mathrm{GL}(k,\mathbb{F}_2)$ puis à choisir un vecteur non nul linéairement indépendant avec les k premiers puis un vecteur non nul linéairement indépendant avec les $k+1$ premiers...

Simplifions cette expression :

$$\begin{aligned}
&(2^k-1)(2^k-2)\dots(2^k-2^{k-1})(2^n-2^k)(2^n-2^{k+1})\dots(2^n-2^{n-1})\\
&\quad=\Big((2^k-1)(2^k-2)\dots(2^k-2^{k-1})\Big)\Big((2^n-2^k)(2^n-2^{k+1})\dots(2^n-2^{n-1})\Big)\\
&\quad=\Big((2^k-1)\times 2\times(2^{k-1}-1)\times\dots\times 2^{k-1}\times(2-1)\Big)\\
&\qquad\Big(2^k\times(2^{n-k}-1)\times 2^{k+1}\times(2^{n-k-1}-1)\times\dots\times 2^{n-1}\times(2-1)\Big)\\
&\quad=2\times 2^2\times\dots 2^k\times 2^{k+1}\times\dots\times 2^{n-1}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1)\\
&\qquad\times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times(2-1)\\
&\quad=2^{1+2+\dots+(n-1)}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1)\\
&\qquad\times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times\times(2-1)\\
&\quad=2^{\frac{n(n-1)}{2}}\times(2^k-1)\times(2^{k-1}-1)\times\dots\times(2-1)\\
&\qquad\times(2^{n-k}-1)\times(2^{n-k-1}-1)\times\dots\times\times(2-1)
\end{aligned}$$

Le ratio de ces deux quantités donne le cardinal recherché soit

$$\frac{(2^n-1)(2^{n-1}-1)\dots(2^{n-k+1}-1)}{(2^k-1)(2^{k-1}-1)\dots(2-1)}.$$

Exercice 59 Soit G un groupe. Soient H et K deux sous-groupes distingués de G.

Montrer que le sous-groupe de G engendré par $\mathrm{H}\cup\mathrm{K}$ est aussi distingué dans G.

Éléments de réponse 59 Soient $g\in\mathrm{G}$ et $x\in\langle\mathrm{H}\cup\mathrm{K}\rangle$. Il existe donc y_1, y_2, …, y_m dans $\mathrm{H}\cup\mathrm{K}$ tels que $x=y_1y_2\dots y_m$ et

$$gxg^{-1}=gy_1y_2\dots y_mg^{-1}.$$

Si y_1 appartient à H alors puisque H est distingué dans G il existe $y_1'\in\mathrm{H}$ tel que $gy_1=y_1'g$. Si y_1 appartient à K alors puisque K est distingué dans G il existe $y_1''\in\mathrm{K}$ tel que $gy_1=y_1''g$. Ainsi il existe $z_1\in\mathrm{H}\cup\mathrm{K}$ tel que $gy_1=z_1g$.

En fait pour tout $1\leq i\leq m$ il existe $z_i\in\mathrm{H}\cup\mathrm{K}$ tel que $gy_i=z_ig$.

Nous obtenons donc

$$\begin{aligned}
gxg^{-1} &= gy_1y_2\dots y_mg^{-1}\\
&= z_1gy_2\dots y_mg^{-1}\\
&= z_1z_2g\dots y_mg^{-1}\\
&= \dots\\
&= z_1z_2\dots z_mgg^{-1}\\
&= z_1z_2\dots z_m
\end{aligned}$$

Or $z_1 z_2 \dots z_m$ appartient à $\mathrm{H} \cup \mathrm{K}$ donc gxg^{-1} appartient à $\mathrm{H} \cup \mathrm{K}$. Ainsi $\langle \mathrm{H} \cup \mathrm{K} \rangle$ est distingué dans G.

Exercice 60 Soit G un groupe. Rappelons que le centralisateur d'un élément de G est l'ensemble des éléments de G qui commutent avec lui.

1. Montrer que le centralisateur d'un élément de G est un sous-groupe de G.
2. Dans $\mathcal{S}_4$ quel est le centralisateur de $(1\ 2)$? Est-ce un sous-groupe distingué de $\mathcal{S}_4$?

Éléments de réponse 60

1. Soit G un groupe. Montrons que le centralisateur C_g d'un élément g de G est un sous-groupe de G.

   Notons que e appartient à C_g.

   Soit x dans C_g. Alors $gx = xg$ d'où $x^{-1}gxx^{-1} = x^{-1}xgx^{-1}$ c'est-à-dire $x^{-1}g = gx^{-1}$, autrement dit x^{-1} appartient à C_g.

   Soient x et y dans C_g. Alors

   $$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$$

   i.e. xy appartient à C_g.

   Il en résulte que C_g est un sous-groupe de G.

2. Déterminons le centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$.

   Soit σ un élément de $\mathcal{S}_n$. Si $(i\ j)$ est une transposition quelconque alors $\sigma(i\ j)\sigma^{-1} = (\sigma(i)\ \sigma(j))$. En effet soit $y \in \{1, 2, \dots, n\}$;
   - si $y = \sigma(i)$, alors $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = \sigma(j)$;
   - si $y = \sigma(j)$, alors $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = \sigma(i)$;
   - si $y \notin \{\sigma(i), \sigma(j)\}$, alors $\big((i\ j)\sigma^{-1}\big)(y) = \sigma^{-1}(y)$ et $\big(\sigma(i\ j)\sigma^{-1}\big)(y) = y$.

   Ainsi le centralisateur de $(i\ j)$ est constitué des permutations $\sigma \in \mathcal{S}_n$ qui laisse l'ensemble $\{i, j\}$ invariant, *i.e.* des permutations $\sigma \in \mathcal{S}_n$ telles que $\sigma(i) = i$ ou j et $\sigma(j) = j$ ou i. En particulier le centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$ est $\{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$.

   Considérons la permutation $(3\ 4)$ qui appartient au centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$. Conjuguons là par la transposition $(2\ 3)$. Nous obtenons $(2\ 4)$, *i.e.* $(2\ 3)(1\ 2)(2\ 3) = (2\ 4)$. En particulier $(2\ 3)(1\ 2)(2\ 3)$ n'appartient pas au centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$. Le centralisateur de $(1\ 2)$ dans $\mathcal{S}_4$ n'est donc pas un sous-groupe distingué de $\mathcal{S}_4$.

Exercice 61 Soit G un groupe. Soient H et K deux groupes de G. Considérons un sous-groupe L de $\mathrm{H} \cap \mathrm{K}$ qui est distingué dans H et dans K.

Montrer que L est distingué dans le sous-groupe de G engendré par $\mathrm{H} \cup \mathrm{K}$.

Éléments de réponse 61 Le sous-groupe L est un sous-groupe de $\langle \mathrm{H} \cup \mathrm{K} \rangle$. Soit z un élément de $\langle \mathrm{H} \cup \mathrm{K} \rangle$. Nous pouvons écrire z sous la forme $z_1 z_2 \dots z_m$ les z_i, $1 \leq i \leq m$, appartenant à $\mathrm{H} \cup \mathrm{K}$.

Soit $\ell \in \mathrm{L}$; alors

$$z\ell z^{-1} = z_1 z_2 \dots (z_m \ell z_m^{-1}) \dots z_2^{-1} z_1^{-1}.$$

L'élément $z_m \ell z_m^{-1}$ appartient à L ; en effet si z_m appartient à H (resp. K), nous utilisons le fait que L est distingué dans H (resp. K).

Nous en déduisons de la même façon que $z_{m-1} z_m \ell z_m^{-1} z_{m-1}^{-1}$ appartient à L. Par récurrence $z\ell z^{-1}$ appartient à L ce qui prouve que L est distingué dans $\langle \mathrm{H} \cup \mathrm{K} \rangle$.

Exercice 62 Montrer que dans un groupe tout sous-groupe d'indice 2 est distingué.

Éléments de réponse 62 Soit G un groupe. Soit H un sous-groupe d'indice 2 de G. Nous avons donc ${}^{\mathrm{G}}\!/_{\mathrm{H}} = \{\mathrm{H},\, x\mathrm{H}\}$ où $x \neq \mathrm{H}$ et $\mathrm{G} = \mathrm{H} \cup x\mathrm{H}$ avec $\mathrm{H} \cap x\mathrm{H} = \emptyset$.

Soit $g \in \mathrm{G}$. Ou bien $g \in \mathrm{H}$ et $g\mathrm{H}g^{-1} = \mathrm{H}$. Ou bien $g \notin \mathrm{H}$ et $g \in x\mathrm{H}$; il existe donc $h_0 \in \mathrm{H}$ tel que $g = xh_0$. Soit alors $h \in \mathrm{H}$; nous avons

$$ghg^{-1} = xh_0 h h_0^{-1} x^{-1} = xh'x^{-1}$$

où $h' = h_0 h h_0^{-1} \in \mathrm{H}$. Si $xh'x^{-1}$ n'appartient pas à H, alors $xh'x^{-1}$ appartient à xH, *i.e.* $xh'x^{-1}$ s'écrit xh_1 avec h_1 dans H. Ceci implique que x appartient à H : contradiction. Par conséquent $xh'x^{-1}$ appartient à H, *i.e.* ghg^{-1} appartient à H. Autrement dit H est un sous-groupe distingué de G.

Exercice 63 Soit G un groupe. Soient H et K des sous-groupes de G. Supposons que

- H et K sont des sous-groupes distingués de G ;
- $\mathrm{H} \cap \mathrm{K} = \{e\}$;
- $\mathrm{HK} = \mathrm{G}$.

Considérons l'application

$$\varphi \colon \mathrm{H} \times \mathrm{K} \to \mathrm{G} \qquad\qquad \varphi(h,k) = hk.$$

1. Montrer que φ est une application injective.
2. Montrer que φ est un isomorphisme de groupes.

Éléments de réponse 63

1. Montrons que φ est une application injective.

   Soient h et h' dans H, soient k et k' dans K. Supposons que $\varphi(h,k) = \varphi(h',k')$, *i.e.* $hk = h'k'$ ce que nous pouvons réécrire $h'^{-1}h = k'k^{-1}$. D'une part $h'^{-1}h$ appartient à H, d'autre part $k'^{-1}k$ appartient à K. Il en résulte que $h'^{-1}h = k'k^{-1}$ appartient à $\mathrm{H} \cap \mathrm{K} = \{e\}$. Ainsi $h = h'$, $k = k'$ et φ est injective.

2. Montrons que φ est un isomorphisme de groupes.

   Par hypothèse $\mathrm{HK} = \mathrm{G}$ donc φ est surjective.

   Soient h, h' dans H et k, k' dans K. Le groupe K étant distingué dans G nous avons $hk = k_1 h$ pour un certain k_1 dans K. Comme H est distingué nous avons $k_1 h = h_1 k_1$ pour

un certain h_1 dans H. Or φ est injective donc $h = h_1$, $k = k_1$ et h et k commutent. Par conséquent $hkh'k')hh'kk'$ d'où

- HK est un sous-groupe de G : la loi est stable dans HK, e appartient à HK et g^{-1} appartient à HK si g appartient à HK ;
- φ est un morphisme de groupes.

Par suite φ est un isomorphisme de groupes.

Exercice 64 Soit G un groupe. Soient H et K deux sous-groupes propres de G. Supposons que

- H et K sont des sous-groupes d'indice 2 dans G ;
- $\mathrm{H} \cap \mathrm{K} = \{e\}$.

Montrer que G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Éléments de réponse 64 Les groupes H et K sont d'indice 2 dans G ils sont donc distingués dans G (Exercice 9).

De plus $\mathrm{H} \cap \mathrm{K} = \{e\}$ donc HK est un sous-groupe distingué de G. En effet

- Soient h, h' dans H et k, k' dans K. Le groupe K étant distingué dans G nous avons $hk = k_1 h$ pour un certain k_1 dans K. Comme H est distingué nous avons $k_1 h = h_1 k_1$ pour un certain h_1 dans H. Or φ est injective donc $h = h_1$, $k = k_1$ et h et k commutent. Par conséquent $hkh'k')hh'kk'$. Ainsi HK est un sous-groupe de G : la loi est stable dans HK, e appartient à HK et g^{-1} appartient à HK si g appartient à HK.
- Le groupe HK est distingué dans G ; en effet soient $g \in \mathrm{G}$, $h \in \mathrm{H}$ et $k \in \mathrm{K}$. Comme H est distingué dans G l'élémeent $ghkg^{-1}$ s'écrit aussi $h_1 gkg^{-1}$ avec h_1 dans H. Par ailleurs $h_1 gkg^{-1} = h_1 k_1 gg^{-1} = h_1 k_1$ avec k_1 dans K car K est distingué dans G. Il s'en suit que $ghkg^{-1}$ appartient à HK.
- Montrons que H et K sont d'ordre 2. Nous avons $\mathrm{G} = \mathrm{H} \cup x\mathrm{H}$ avec $x \notin \mathrm{H}$. Comme K est d'indice 2 il est d'ordre au moins 2 et contient donc au moins un élément k qui n'est pas dans H (en particulier $k \neq e$). Nous pouvons donc prendre pour x cet élément k. Ainsi $\mathrm{G} = \mathrm{H} \cup k\mathrm{H}$ avec $\mathrm{H} \cap k\mathrm{H} = \emptyset$. Soit $k' \in \mathrm{K} \setminus \{e\}$. Ainsi k' n'appartient pas à H et $k' \in k\mathrm{H}$. Il existe donc $h \in \mathrm{H}$ tel que $k' = kh$. Par suite $h = k^{-1}k'$ est aussi dans K donc $h = e$ et $k = k'$. Le groupe K contient donc seulement deux éléments : e et k.

  De même nous obtenons que H est d'ordre 2.

  Ainsi H et K sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$.
- Montrons que $\mathrm{G} = \mathrm{KH}$. Soit $g \in \mathrm{G}$. Alors ou bien g appartient à H et donc g appartient à HK, ou bien g appartient à kH, *i.e.* $g = kh$ avec $h \in \mathrm{H}$. Or $\mathrm{HK} = \mathrm{KH}$ donc g appartient à HK.

Finalement G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 65 Pour a et b réels on définit l'application

$$\tau_{a,b} \colon \mathbb{R} \to \mathbb{R} \qquad\qquad x \mapsto ax + b.$$

1. Soit $\mathrm{G} = \{\tau_{a,b} \,|\, a \neq 0\}$.

   Montrer que G est un groupe pour la composition des applications.

2. Soit $\mathrm{H} = \{\tau_{a,b} \,|\, a \neq 0,\, a \in \mathbb{Q}\}$.

   Montrer que H est un sous-groupe de G.

3. Décrire les classes à droite de H dans G.

   Montrer que toute classe à gauche (modulo H) est classe à droite (modulo H). (Indication : considérer l'application qui à l'élément $\tau_{a,b}$ de G associe la classe de a dans $\mathbb{R}^*/\mathbb{Q}^*$)

4. Donner un exemple d'un sous-groupe K de G tel qu'une classe à gauche ne soit pas classe à droite.

5. Soit $\mathrm{N} = \{\tau_{a,b} \,|\, a = 1\}$.

   Montrer que N est un sous-groupe distingué de G.

Éléments de réponse 65

1. Soit $\mathrm{G} = \{\tau_{a,b} \,|\, a \neq 0\}$.

   Montrons que G est un groupe pour la composition des applications.

   Soient $\tau_{a,b}$ et $\tau_{a',b'}$ deux éléments de G. Alors $\tau_{a,b}^{-1} = \tau_{1/a,-b/a}$ (notons que $a \neq 0$). De plus $\tau_{a',b'} \circ \tau_{a,b}^{-1} = \tau_{a'/a,-a'b/a+b'}$. Par suite G est un sous-groupe du groupe des bijections de $\mathbb{R}$ dans $\mathbb{R}$.

2. Soit $\mathrm{H} = \{\tau_{a,b} \,|\, a \neq 0,\, a \in \mathbb{Q}\}$.

   Montrons que H est un sous-groupe de G.

   Soient $\tau_{a,b}$ et $\tau_{a',b'}$ deux éléments de H. Alors $\tau_{a,b}^{-1} = \tau_{1/a,-b/a}$ (notons que $a \neq 0$). De plus $\tau_{a',b'} \circ \tau_{a,b}^{-1} = \tau_{a'/a,-a'b/a+b'}$. Par suite H est un sous-groupe de G.

3. Décrivons les classes à droite de H dans G et montrons que toute classe à gauche (mod H) est classe à droite (modulo H).

   La classe à droite de l'élément $\tau_{\alpha,\beta}$ de G est l'ensemble des $\tau_{\alpha a,\alpha b+\beta}$ où $a \in \mathbb{Q}$.

   Pour montrer que toute classe à gauche est une classe à droite il suffit de montrer que H est distingué dans G. Considérons le morphisme de groupes

   $$\varphi\colon \mathrm{G} \to \mathbb{R}^*/\mathbb{Q}^* \qquad\qquad \tau_{a,b} \mapsto \text{ la classe de } a \text{ dans } \mathbb{R}^*/\mathbb{Q}^*$$

   Son noyau est H qui est donc distingué dans G.

4. Donnons un exemple d'un sous-groupe K de G tel qu'une classe à gauche ne soit pas classe à droite.

   Soit K le sous-groupe de G des éléments $\tau_{a,b}$ où a et b sont rationnels. Les classes à gauche et à droite de K dans G ne coïncident pas.

5. Soit $\mathrm{N} = \{\tau_{a,b} \,|\, a = 1\}$.

   Montrons que N est un sous-groupe distingué de G.

   L'identité appartient à N. Soient $\tau_{1,b}$ et $\tau_{1,b'}$ deux éléments de N. Nous avons $\tau_{1,b} \circ \tau_{1,b'}^{-1} = \tau_{1,b-b'}$; en particulier $\tau_{1,b} \circ \tau_{1,b'}^{-1}$ appartient à N. Ainsi N est un sous-groupe de G.

   Soit $\tau_{\alpha,\beta}$ un élément quelconque de G et soit $\tau_{1,b}$ un élément quelconque de N. Alors

$$\tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{\alpha,\beta}^{-1} = \tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{1/\alpha,-\beta/\alpha} = \tau_{1,\alpha b};$$

   ainsi $\tau_{\alpha,\beta} \circ \tau_{1,b} \circ \tau_{\alpha,\beta}^{-1}$ appartient à N ce qui prouve que N est un sous-groupe distingué de G.

Exercice 66 Soit H un sous-groupe d'un groupe G tel que toute classe à gauche modulo H soit classe à droite modulo H. Le sous-groupe H est-il distingué ?

Éléments de réponse 66 Supposons que H ne soit pas distingué dans G. Cela signifie qu'il existe $g \in \mathrm{G} \setminus \{e\}$ tel que $g\mathrm{H} \neq \mathrm{H}g$ ou encore qu'il existe $h \in \mathrm{H}$ tel que gh n'appartient pas à $\mathrm{H}g$.

Ainsi gh appartient à une autre classe à droite que nous noterons $\mathrm{H}g'$ ($\mathrm{H}g' \neq \mathrm{H}g$). Puisque toute classe à gauche est une classe à droite et que les classes à droite forment une partition de G la classe à droite qui est égale à gH est nécessairement $\mathrm{H}g'$.

Donc g appartient à gH et Hg. Comme $g\mathrm{H} = \mathrm{H}g'$ l'élément g appartient aussi à $\mathrm{H}g'$. Autrement dit g appartient à $\mathrm{H}g \cap \mathrm{H}g'$. Ceci n'est possible que si $g = e$ ou $\mathrm{H}g = \mathrm{H}g'$. Mais par hypothèse $g \neq e$ et $\mathrm{H}g \neq \mathrm{H}g'$.

Il en résulte que H est distingué dans G.

Exercice 67 Soit G un groupe fini. Soit H un sous-groupe de G. Soit N un sous-groupe distingué de G.

Montrer que si |H| et [G : N] sont premiers entre eux, alors H est un sous-groupe de N.

Éléments de réponse 67 Raisonnons par l'absurde : supposons que H ne soit pas un sous-groupe de N. Alors il existe $h \in \mathrm{H}$ qui n'est pas un élément de N. Il s'en suit que hN est un élément différent de l'élément neutre N de G/N.

Soit q l'ordre de hN dans G/N. On sait que $q \neq 1$ et que q divise $|\mathrm{G}/\mathrm{N}| = [\mathrm{G} : \mathrm{N}]$. Par ailleurs $h^{|\mathrm{H}|} = e$ donc $(h\mathrm{K})^{|\mathrm{H}|} = \mathrm{H}$. Par suite q divise |H|. Ainsi $q \neq 1$ est un diviseur commun à [G : N] et |H| qui sont premiers entre eux : contradiction. Il en résulte que H est un sous-groupe de N.

Exercice 68 Soit G un groupe qui ne contient qu'un seul sous-groupe H d'ordre n.

Montrer que H est distingué dans G.

Éléments de réponse 68 Nous allons montrer que H est un sous-groupe caractérisque de G. Soit φ un automorphisme de G et $\varphi_{|\mathrm{H}} : \mathrm{H} \to \varphi(\mathrm{H})$ la restriction de φ à H et à son image. Comme φ est un automorphisme de G, $\varphi_{|\mathrm{H}}$ est bijective. C'est donc un isomorphisme de groupes. Étant

donné que H est fini d'ordre n, $\varphi(\mathrm{H})$ est fini d'ordre n. Or H est l'unique sous-groupe de G d'ordre n donc $\varphi(\mathrm{H}) = \mathrm{H}$.

Puisque H est un sous-groupe caractéristique de G c'est un sous-groupe distingué de G.

Exercice 69 Soit H un sous-groupe de G tel que le produit de deux classes à gauche modulo H soit une classe à gauche modulo H.

Le sous-groupe H est-il distingué dans G ?

Éléments de réponse 69 Comme le produit de deux classes à gauche est une classe à gauche pour tout couple (g, g') d'éléments de G il existe $g'' \in \mathrm{G}$ tel que $g\mathrm{H}g'\mathrm{H} = g''\mathrm{H}$. En particulier il existe g'' tel que $g\mathrm{H}g^{-1}\mathrm{H} = g''\mathrm{H}$. Et pour tout élément h de H il existe h' et h'' dans H tels que $ghg^{-1}h' = g''h''$. En particulier puisque e appartient à H il existe h'' dans H tel que $geg^{-1}e = g''h''$ ce qui se réécrit $e = g''h''$. Ainsi $g'' = h''^{-1} \in \mathrm{H}$ et $g\mathrm{H}g^{-1}\mathrm{H} = \mathrm{H}$, c'est-à-dire $g\mathrm{H}g^{-1} = \mathrm{H}$. Le sous-groupe H est donc distingué dans G.

Exercice 70 Soit G un groupe. Soit H un sous-groupe distingué de G.

Montrer que si H est cyclique tout sous-groupe de H est distingué dans G.

Éléments de réponse 70 Soit h un générateur de H. Soit K un sous-groupe du groupe cyclique distingué H. Alors tous les éléments de K sont égaux à une puissance de h et K est lui-même cyclique engendré par une puissance de h.

Posons $p_0 = \inf\{p \in \mathbb{N}^* \,|\, h^p \in \mathrm{K}\}$. Soit h^p un élément de K. Nous avons $p = qp_0 + r$ avec $0 \leq r < p_0$. Par suite $h^p = (h^{p_0})^q h^r$ et $h^r = h^p(h^{-p_0})^q$ appartient à K. Puisque $p_0 = \inf\{p \in \mathbb{N}^* \,|\, h^p \in \mathrm{K}\}$ nous avons nécessairement $r = 0$ et $\mathrm{K} = \langle h^{p_0} \rangle$.

Puisque H est distingué dans G pour tout $g \in \mathrm{G}$ il existe q tel que $ghg^{-1} = h^q$. Par conséquent $gh^{p_0}g^{-1} = h^{qp_0}$ et K est distingué dans G.

Exercice 71 Soient A un groupe et C un sous-groupe distingué de A. Soient B un groupe et D un sous-groupe distingué de B.

Montrer que $^{\mathrm{A}\times\mathrm{B}}\!/_{\mathrm{C}\times\mathrm{D}} \simeq {}^{\mathrm{A}}\!/_{\mathrm{C}} \times {}^{\mathrm{B}}\!/_{\mathrm{D}}$.

Éléments de réponse 71 Considérons l'homomorphisme de groupes entre $\mathrm{A}\times\mathrm{B}$ et ${}^{\mathrm{A}}\!/_{\mathrm{C}}\times{}^{\mathrm{B}}\!/_{\mathrm{D}}$ donné par

$$\varphi((a,b)) = (a\mathrm{C}, b\mathrm{D}).$$

Le noyau de φ est égal à

$$\begin{aligned} \ker\varphi &= \{(a,b) \in \mathrm{A}\times\mathrm{B} \,|\, a\mathrm{C} = \mathrm{C} \text{ et } b\mathrm{D} = \mathrm{D}\} \\ &= \{(a,b) \in \mathrm{A}\times\mathrm{B} \,|\, a \in \mathrm{C} \text{ et } b \in \mathrm{D}\} \\ &= \mathrm{C}\times\mathrm{D}. \end{aligned}$$

Par ailleurs $(a\mathrm{C}, b\mathrm{D})$ est l'image de (a,b) par φ donc φ est surjectif. Il en résulte que φ induit un isomorphisme entre $^{\mathrm{A}\times\mathrm{B}}\!/_{\mathrm{C}\times\mathrm{D}}$ et ${}^{\mathrm{A}}\!/_{\mathrm{C}} \times {}^{\mathrm{B}}\!/_{\mathrm{D}}$.

Exercice 72 Soient G_1 et G_2 deux groupes non isomorphes.

1. Montrer que $Z(G_1) \times Z(G_2)$ est isomorphe à $Z(G_1 \times G_2)$.
2. Supposons que G_1 et G_2 sont des groupes simples.
   (a) Montrer que $G_1 \times G_2$ contient un sous-groupe distingué H_1 isomorphe à G_1 et un sous-groupe distingué H_2 isomorphe à G_2.
   (b) Montrer que si H est un sous-groupe distingué de $G_1 \times G_2$, alors $H \cap H_1$ est distingué dans H_1 et $H \cap H_2$ est distingué dans H_2.
   (c) En déduire que H_1 et H_2 sont les seuls sous-groupes distingués de $G_1 \times G_2$.

Éléments de réponse 72

1. Montrons que $Z(G_1) \times Z(G_2)$ est isomorphe à $Z(G_1 \times G_2)$.
   Soit $(x_1, x_2) \in G_1 \times G_2$; alors (x_1, x_2) appartient à $Z(G_1 \times G_2)$ si et seulement si
   $$\forall\, (y_1, y_2) \in G_1 \times G_2 \qquad (x_1, x_2)(y_1, y_2) = (y_1, y_2)(x_1, x_2)$$
   si et seulement si
   $$\forall\, (y_1, y_2) \in G_1 \times G_2 \qquad (x_1 y_1, x_2 y_2) = (y_1 x_1, y_2 x_2)$$
   si et seulement si
   $$\forall\, (y_1, y_2) \in G_1 \times G_2 \qquad x_1 y_1 = y_1 x_1 \text{ et } x_2 y_2 = y_2 x_2.$$
   Par conséquent (x_1, x_2) appartient à $Z(G_1 \times G_2)$ si et seulement si x_1 appartient à $Z(G_1)$ et x_2 appartient à $Z(G_2)$. Ainsi
   $$Z(G_1 \times G_2) \simeq Z(G_1) \times Z(G_2).$$
2. Supposons que G_1 et G_2 sont des groupes simples.
   (a) Montrons que $G_1 \times G_2$ contient un sous-groupe distingué H_1 isomorphe à G_1 et un sous-groupe distingué H_2 isomorphe à G_2.
   Soit $H_1 = G_1 \times \{e_2\}$ où e_2 est l'élément neutre de G_2. Le groupe H_1 est un sous-groupe de $G_1 \times G_2$ isomorphe à G_1. De plus H_1 est distingué dans $G_1 \times G_2$ car pour tout $(x_1, x_2) \in G_1 \times G_2$, pour tout $(x, e_2) \in H_1$ nous avons
   $$(x_1, x_2)(x, e_2)(x_1, x_2)^{-1} = (x_1, x_2)(x, e_2)(x_1^{-1}, x_2^{-1}) = (x_1 x x_1^{-1}, x_2 x_2^{-1}) = (x_1 x x_1^{-1}, e_2)$$
   et $(x_1, x_2)(x, e_2)(x_1, x_2)^{-1}$ appartient à H_1.
   De même $H_2 = \{e_1\} \times G_2$ est un sous-groupe distingué de $G_1 \times G_2$.
   (b) Montrons que si H est un sous-groupe distingué de $G_1 \times G_2$, alors $H \cap H_1$ est distingué dans H_1 et $H \cap H_2$ est distingué dans H_2.
   Soit $(x_1, e_2) \in H_1$ et soit $(x, e_2) \in H \cap H_1$; nous avons
   $$(x_1, e_2)(x, e_2)(x_1, e_2)^{-1} = (x_1, e_2)(x, e_2)(x_1^{-1}, e_2) = (x_1 x x_1^{-1}, e_2)$$
   donc $(x_1, e_2)(x, e_2)(x_1, e_2)^{-1}$ appartient à H_1. Par ailleurs H est un sous-groupe distingué de $G_1 \times G_2$ donc $(x_1, e_2)(x, e_2)(x_1, e_2)^{-1}$ appartient à H. Finalement

$(x_1, e_2)(x, e_2)(x_1, e_2)^{-1}$ appartient à $\mathrm{H} \cap \mathrm{H}_1$ et $\mathrm{H} \cap \mathrm{H}_1$ est un sous-groupe distingué de H_1.

De même $\mathrm{H} \cap \mathrm{H}_2$ est un sous-groupe distingué de H_2.

(c) Les sous-groupes H_1 et H_2 sont isomorphes à G_1 et G_2 respectivement. Les groupes G_1 et G_2 étant simples les groupes H_1 et H_2 sont aussi simples. Il y a donc quatre cas possibles qui sont les suivants :

i) $\mathrm{H} \cap \mathrm{H}_1 = \mathrm{H}_1$ et $\mathrm{H} \cap \mathrm{H}_2 = \mathrm{H}_2$ auquel cas $\mathrm{H} = \mathrm{G}_1 \times \mathrm{G}_2$.

ii) $\mathrm{H} \cap \mathrm{H}_1 = \mathrm{H}_1$ et $\mathrm{H} \cap \mathrm{H}_2 = \{(e_1, e_2)\}$ auquel cas $\mathrm{H} = \mathrm{H}_1$.

iii) $\mathrm{H} \cap \mathrm{H}_1 = \{(e_1, e_2)\}$ et $\mathrm{H} \cap \mathrm{H}_2 = \mathrm{H}_2$ auquel cas $\mathrm{H} = \mathrm{H}_2$.

iv) $\mathrm{H} \cap \mathrm{H}_1 = \{(e_1, e_2)\}$ et $\mathrm{H} \cap \mathrm{H}_2 = \{(e_1, e_2)\}$ auquel cas $\mathrm{H} = \{(e_1, e_2)\}$. En effet $\mathrm{HH}_1/\mathrm{H}_1$ (qui est isomorphe à H) est distingué dans G/H_1, groupe qui est lui-même isomorphe à G_2.

De la même façon nous obtenons que si H n'est pas trivial il est isomorphe à G_1.

Ainsi si H n'est pas trivial, il est isomorphe à G_1 et à G_2 et G_1 et G_2 sont isomorphes : contradiction. Par conséquent $\mathrm{H} = \{(e_1, e_2)\}$.

Ainsi les seuls sous-groupes distingués propres de $\mathrm{G}_1 \times \mathrm{G}_2$ sont H_1 et H_2.

Exercice 73 Soient G un groupe et H un sous-groupe de G.

(a) Montrer qu'en posant $g \cdot a\mathrm{H} = (ga)\mathrm{H}$, où a, $g \in \mathrm{G}$, on définit une action de G sur l'ensemble G/H des classes à gauche modulo H.

(b) Montrer que cette action est transitive.

Déterminer le stabilisateur de aH.

(c) On suppose G fini. Calculer le cardinal d'une orbite et retrouver un théorème classique.

Éléments de réponse 73

(a) Posons $X = \mathrm{G}/\mathrm{H}$. Soient g dans G et x dans X. Désignons par a, a' deux représentants de la classe à gauche x. On a $a\mathrm{H} = a'\mathrm{H} = x$ ou encore $a^{-1}a' \in \mathrm{H}$. Or

$$(ga)^{-1}ga' = a^{-1}g^{-1}ga' = a^{-1}a' \in \mathrm{H}$$

donc $ga\mathrm{H} = ga'\mathrm{H}$.

Si on remplace a par un autre représentant a' de la classe $x = a\mathrm{H}$, alors $ga'\mathrm{H} = ga\mathrm{H}$. La formule a donc bien un sens et définit une application de $\mathrm{G} \times X \to X$.

C'est bien une action de G sur X puisque

- $\forall\, x = a\mathrm{H} \in X$ nous avons $e \cdot x = ea\mathrm{H} = a\mathrm{H} = x$,
- $\forall\, x = a\mathrm{H} \in X$, $\forall\, g \in \mathrm{G}$, $\forall\, g' \in \mathrm{G}$ nous avons

$$g \cdot (g' \cdot x) = g \cdot (g'a\mathrm{H}) = g(g'a)\mathrm{H} = (gg')a\mathrm{H} = gg' \cdot x$$

(b) Pour tous $x = a\mathrm{H} \in X$ et $y = b\mathrm{H} \in X$ il existe $g \in \mathrm{G}$ tel que $g \cdot x = y$ (prendre $g = ba^{-1}$). Il existe donc une seule orbite, égale à X.

Le stabilisateur de $x = a\mathrm{H}$ est $a\mathrm{H}a^{-1}$ car :

$$g \in \mathrm{G}_x \iff ga\mathrm{H} = a\mathrm{H} \iff a^{-1}ga\mathrm{H} = \mathrm{H} \iff a^{-1}ga \in \mathrm{H} \iff g \in a\mathrm{H}a^{-1}.$$

(c) Comme $\mathrm{G}_x = a\mathrm{H}a^{-1} = \mathrm{Ad}_a(\mathrm{H}) \simeq \mathrm{H}$, on retrouve le théorème de Lagrange

$$[\mathrm{G} : \mathrm{H}] = \mathrm{card}\left(\mathrm{G}/\mathrm{H}\right) = \mathrm{card}(\mathrm{orb}(x)) = \frac{[\mathrm{G} : 1]}{[\mathrm{G}_x : 1]} = \frac{[\mathrm{G} : 1]}{[\mathrm{H} : 1]}.$$

Exercice 74 Soient p un nombre premier et $a > 1$. En utilisant une action de groupe que l'on précisera montrer que tout groupe G d'ordre p^a admet un élément central (*i.e.* qui commute avec tout élément de G) d'ordre p.

Éléments de réponse 74 Faisons agir G sur lui-même par conjugaison. Les orbites sont ou bien de cardinal 1 (pour chaque élément du centre), ou bien de cardinal une puissance de p non égale à 1. En écrivant G comme une union d'orbites on a donc $|Z(\mathrm{G})| \equiv 0 \bmod p$, ce qui interdit à $Z(\mathrm{G})$ d'être trivial. Soit $g \in Z(\mathrm{G}) \smallsetminus \{1\}$, alors g est d'ordre p^b pour un certain $1 \leq b \leq a$. Alors $g^{p^{b-1}}$ appartient à $Z(\mathrm{G})$ et est d'ordre p.

Exercice 75 Soit G un groupe. Soient H et K deux sous-groupes de G tels que $\mathrm{K} \subset \mathrm{H} \subset \mathrm{G}$.

a) Supposons que G soit fini. Montrer que

$$|\mathrm{G} : \mathrm{K}| = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}|.$$

b) On ne suppose plus que G est fini. On suppose par contre que H et K sont distingués dans G. Montrer que

$$|\mathrm{G} : \mathrm{K}| = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}|.$$

Éléments de réponse 75

a) Comme G est fini, on a

$$|\mathrm{G}| = |\mathrm{G} : \mathrm{H}|\,|\mathrm{H}| \qquad |\mathrm{H}| = |\mathrm{H} : \mathrm{K}|\,|\mathrm{K}| \qquad |\mathrm{G}| = |\mathrm{G} : \mathrm{K}|\,|\mathrm{K}|$$

L'ordre d'un groupe n'est jamais nul donc $|\mathrm{K}| \neq 0$ et

$$|\mathrm{G} : \mathrm{K}| = \frac{|\mathrm{G}|}{|\mathrm{K}|} = \frac{|\mathrm{G} : \mathrm{H}|\,|\mathrm{H}|}{|\mathrm{K}|} = |\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}|.$$

b) Les groupes G/H et $\mathrm{G}/\mathrm{K}\big/\mathrm{H}/\mathrm{K}$ sont isomorphes donc $\left|\mathrm{G}/\mathrm{H}\right| = \left|\mathrm{G}/\mathrm{K}\big/\mathrm{H}/\mathrm{K}\right|$ soit $|\mathrm{G} : \mathrm{H}| = \left|\mathrm{G}/\mathrm{K} : \mathrm{H}/\mathrm{K}\right|$ d'où $|\mathrm{G} : \mathrm{H}|\left|\mathrm{H}/\mathrm{K}\right| = \left|\mathrm{G}/\mathrm{K}\right|$, *i.e.*

$$|\mathrm{G} : \mathrm{H}| \cdot |\mathrm{H} : \mathrm{K}| = |\mathrm{G} : \mathrm{K}|.$$

Exercice 76 Soit G un groupe. Les assertions suivantes sont-elles vraies ou fausses ? Justifier.

a) Si tout sous-groupe H de G est distingué dans G, alors G est abélien.

b) Si $\mathrm{H} \lhd \mathrm{G}$ et $\mathrm{K} \lhd \mathrm{H}$, alors $\mathrm{K} \lhd \mathrm{G}$.

c) Soient g et h dans G d'ordre fini. Alors gh est d'ordre fini.

d) Si G a un nombre fini de sous-groupes, alors G est fini.

e) Si H et K sont des sous-groupes de G, alors $\langle \mathrm{H} \cup \mathrm{K} \rangle = \mathrm{HK}$.

Éléments de réponse 76

a) Faux. Considérons le groupe H des quaternions. Rappelons qu'il est défini de la façon suivante : H est l'ensemble

$$\mathrm{H} = \{ \pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k} \}$$

et la loi de groupe est définie par

$$(-1)^2 = 1,\ \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$
$$(-1)\cdot\mathbf{i} = \mathbf{i}\cdot(-1) = -\mathbf{i},\ (-1)\cdot\mathbf{j} = \mathbf{j}\cdot(-1) = -\mathbf{j},\ (-1)\cdot\mathbf{k} = \mathbf{k}\cdot(-1) = -\mathbf{k}$$
$$\mathbf{i}\cdot\mathbf{j} = -\mathbf{j}\cdot\mathbf{i} = \mathbf{k}.$$

Les sous-groupes de H sont
— le sous-groupe trivial {id} qui est distingué,
— le sous-groupe de cardinal 2 engendré par -1 qui est distingué car contenu dans le centre de H,
— les sous-groupes de cardinal 4 sont d'indice 2 dans H donc distingués,
— le sous-groupe H entier qui est distingué.
Les sous-groupes de H sont donc tous distingués mais H n'est pas abélien.

b) Faux. Considérons par exemple $\mathrm{G} = \mathcal{S}_4$, $\mathrm{H} = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{K} = \{\mathrm{id}, (1\ 2)(3\ 4)\} \simeq \mathbb{Z}/2\mathbb{Z}$.

c) Faux. Pour avoir un contre-exemple il faut que le groupe G soit infini et non abélien. Prenons par exemple $\mathrm{G} = \mathrm{GL}(2, \mathbb{Q})$, $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. L'élément g est d'ordre 2, l'élément h est d'ordre 3 mais $gh = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini.

d) Vrai. Tout élément de G est d'ordre fini : si g est d'ordre infini, alors le sous-groupe engendré par g est isomorphe à $\mathbb{Z}$ et contient donc une infinité de sous-groupes distincts. Or G a un nombre fini de sous-groupes cycliques notés $\langle g_1 \rangle, \ldots, \langle g_n \rangle$. Donc pour tout g dans G il existe i tel que $\langle g \rangle = \langle g_i \rangle$, autrement dit g est une puissance de g_i. Ceci assure que le cardinal de G est borné par la somme des ordres des g_i. Il s'en suit que G est fini.

e) Faux. L'inclusion $\mathrm{HK} \subset \langle \mathrm{H} \cup \mathrm{K} \rangle$ est toujours vérifiée. En revanche le sous-ensemble HK n'est en général pas un sous-groupe de G contrairement à $\langle \mathrm{H} \cup \mathrm{K} \rangle$. En effet prenons par exemple $\mathrm{G} = \mathcal{S}_3$, $\mathrm{H} = \{\mathrm{id}, (1\ 2)\}$ et $\mathrm{K} = \{\mathrm{id}, (1\ 3)\}$. Alors $\langle \mathrm{H} \cup \mathrm{K} \rangle$ coïncide avec G et $\mathrm{HK} = \{\mathrm{id}, (1\ 2), (1\ 3), (1\ 3\ 2)\}$ n'est pas un sous-groupe de G.

La réponse est vraie si l'on suppose que H ou K est distingué dans G (exercice).

Exercice 77 Soit S un sous-ensemble non vide d'un groupe fini G. Soit $N(S) = \{g \in \mathrm{G} \,|\, gSg^{-1} = S\}$ le normalisateur de S dans G. Soit $C(S) = \{g \in \mathrm{G} \,|\, \forall\, s \in S,\, gsg^{-1} = s\}$ le centralisateur de S dans G.

Montrer que

a) $N(S) \subset \mathrm{G}$ et $C(S) \lhd N(S)$.

b) $N(S) = \mathrm{G}$ si et seulement si $S = \bigcup_{g \in \mathrm{G}} gSg^{-1}$.

c) Si $\mathrm{H} \lhd \mathrm{G}$, alors $C(\mathrm{H}) \lhd \mathrm{G}$.

d) Si $\mathrm{H} \subset \mathrm{G}$, alors $N(\mathrm{H})$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

Éléments de réponse 77

a) Montrons que $N(S) \subset \mathrm{G}$ et $C(S) \lhd N(S)$. Bien sûr e appartient à $N(S)$. Soient g et h dans $N(S)$. Alors

$$(gh)S(gh)^{-1} = g(hSh^{-1})g^{-1} = gSg^{-1} = S$$

donc gh appartient à $N(S)$. Si g appartient à $N(S)$ on a $gSg^{-1} = S$ donc en multipliant à gauche et à droite par g^{-1} et g respectivement on a $S = g^{-1}Sg$, autrement dit g^{-1} appartient à $N(S)$. Ainsi $N(S)$ est un sous-groupe de G.

De même $C(S)$ est un sous-groupe de G contenu dans $N(S)$. Montrons que $C(S)$ est distingué dans $N(S)$. Soient $g \in C(S)$ et $h \in N(S)$. Soit $s \in S$. Alors

$$(hgh^{-1})s(hgh^{-1})^{-1} = hg(h^{-1}sh)g^{-1}h^{-1}$$

et comme h appartient à $N(S)$, on a $h^{-1}sh$ appartient à S. Donc puisque g appartient à $C(S)$

$$g(h^{-1}sh)g^{-1} = h^{-1}sh$$

et finalement

$$(hgh^{-1})s(hgh^{-1})^{-1} = h(h^{-1}sh)h^{-1} = s.$$

Ainsi hgh^{-1} appartient à $C(S)$ et $C(S) \lhd N(S)$.

b) Montrons que $N(S) = \mathrm{G}$ si et seulement si $S = \bigcup_{g \in \mathrm{G}} gSg^{-1}$.

Supposons que $N(S) = \mathrm{G}$. Alors pour tout $g \in \mathrm{G}$, on a $gSg^{-1} = S$ donc $S = \bigcup_{g \in \mathrm{G}} gSg^{-1}$.

Réciproquement supposons que $S = \bigcup_{g \in \mathrm{G}} gSg^{-1}$. Pour tout $g \in \mathrm{G}$ nous avons $g^{-1}Sg \subset S$ donc en multipliant par g et g^{-1} à gauche et à droite respectivement nous avons $S \subset gSg^{-1} \subset S$ d'où $S = gSg^{-1}$. Ainsi g appartient à $N(S)$ et $\mathrm{G} = N(S)$.

c) Montrons que si $\mathrm{H} \triangleleft \mathrm{G}$, alors $C(\mathrm{H}) \triangleleft \mathrm{G}$. Supposons que H soit distingué dans G. Soient g dans G, c dans $C(\mathrm{H})$ et h dans H. Nous avons

$$(gcg^{-1})h(gcg^{-1})^{-1} = gc(g^{-1}hg)c^{-1}g^{-1}$$

puisque H est distingué dans G nous savons que $g^{-1}hg$ appartient à H. Or c appartient à $C(\mathrm{H})$ donc $c(g^{-1}hg)c^{-1} = g^{-1}hg$ et finalement

$$(gcg^{-1})h(gcg^{-1})^{-1}$$

ce qui assure que gcg^{-1} appartient à $C(\mathrm{H})$. Le groupe $C(\mathrm{H})$ est donc distingué dans G.

d) Montrons que si $\mathrm{H} \subset \mathrm{G}$, alors $N(\mathrm{H})$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

Par définition et a) $N(\mathrm{H})$ est un sous-groupe de G contenant H et H est distingué dans $N(\mathrm{H})$. Considérons un sous-groupe K de G contenant H tel que $\mathrm{H} \triangleleft \mathrm{K}$. Par définition nous avons $k\mathrm{H}k^{-1} = \mathrm{H}$ pour tout $k \in \mathrm{K}$. Par conséquent k appartient à $N(\mathrm{H})$ donc $\mathrm{K} \subset N(\mathrm{H})$ ce qui assure la maximalité de $N(\mathrm{H})$ parmi les sous-groupes de G concernés.

Exercice 78 Soit G un groupe. Désignons par Aut(G) le groupe des automorphismes de G. Si a appartient à G, notons $\varphi(a)$ l'application

$$\varphi(a)\colon \mathrm{G} \to \mathrm{G} \qquad\qquad g \mapsto aga^{-1}.$$

a) Montrer que pour tout a dans G l'application $\varphi(a)$ est un automorphisme de G (appelé automorphisme intérieur de G).

b) Montrer que $\varphi\colon \mathrm{G} \to \mathrm{Aut}(G)$, $g \mapsto \varphi(g)$ est un homomorphisme de groupes de G dans Aut(G).

c) Notons Int(G) l'ensemble des automorphismes intérieurs de G. Montrer que Int(G) est un sous-groupe distingué de Aut(G).

d) Notons $Z(\mathrm{G})$ le centre de G. Montrer que $\mathrm{Int}(\mathrm{G}) \simeq {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

Éléments de réponse 78

a) Il faut montrer que $\varphi(a)$ est un homomorphisme de G dans G ; bien sûr $\varphi(a)(e) = e$. Il reste donc à montrer que $\varphi(a)(gg') = \varphi(a)(g)\varphi(a)(g')$. Or

$$\varphi(a)(gg') = agg'a^{-1} = (aga^{-1})(ag'a^{-1}) = \varphi(a)(g)\varphi(a')(g).$$

Montrons que $\ker \varphi(a) = \{e\}$. Soit $g \in \ker \varphi(a)$, autrement dit $aga^{-1} = e$ d'où $g = a^{-1}a = e$. Ainsi $\varphi(a)$ est un homomorphisme injectif.

Soit g dans G. On a $g = a(a^{-1}ga)a^{-1} = \varphi(a)(a^{-1}ga)$. Autrement dit $\varphi(a)$ est surjectif.

Il en résulte que $\varphi(a)$ est un automorphisme de G et $(\varphi(a))^{-1} = \varphi(a^{-1})$.

b) D'une part $\varphi(e)(g) = ege^{-1} = g$, *i.e.* $\varphi(e) = \mathrm{id}$. D'autre part
$$\varphi(a) \circ \varphi(a')(g) = a(a'ga'^{-1})a^{-1} = (aa')g(aa')^{-1} = \varphi(aa')(g)$$
c'est-à-dire $\varphi(a) \circ \varphi(a') = \varphi(aa')$. Par suite φ est un homomorphisme de groupes de G dans Aut(G).

c) Int(G) est l'image de G par l'homomorphisme de groupes φ ; c'est donc un sous-groupe de Aut(G).

Soit τ un automorphisme de G ; alors
$$\tau \circ \varphi(a) \circ \tau^{-1}(g) = \tau(a\tau^{-1}(g)a^{-1}) = \tau(a)\tau(\tau^{-1}(g))\tau(a^{-1}) = \tau(a)g\tau(a^{-1})$$
Ainsi $\tau \circ \varphi(a) \circ \tau^{-1} = \varphi(\tau(a))$ appartient à $\operatorname{Im}\varphi$. Le groupe Int(G) est distingué dans Aut(G).

d) D'une part $\ker\varphi$ est le centre $Z(\mathrm{G})$ de G, d'autre part $\operatorname{Im}\varphi = \mathrm{Int}(\mathrm{G})$. Le théorème d'isomorphisme assure que $\mathrm{Int}(\mathrm{G}) \simeq {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

Exercice 79 Soit G un groupe et soit $\mathrm{H} \triangleleft \mathrm{G}$ un sous-groupe distingué.

a) Décrire les sous-groupes distingués de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ en fonction de ceux de G.

b) Soit K un sous-groupe de G.

i) Si K est distingué dans G et contient H, montrer que
$${}^{\mathrm{G}}\!/_{\mathrm{H}}{}^{\mathrm{K}}\!/_{\mathrm{H}} \simeq {}^{\mathrm{G}}\!/_{\mathrm{K}}$$

ii) Montrer que HK est un sous-groupe de G égal à KH.

iii) Montrer que H est distingué dans HK.

iv) Montrer que
$${}^{\mathrm{K}}\!/_{(\mathrm{K} \cap \mathrm{H})} \simeq {}^{\mathrm{HK}}\!/_{\mathrm{H}}.$$

Éléments de réponse 79 Soit G un groupe et soit $H \triangleleft \mathrm{G}$ un sous-groupe distingué.

a) Décrivons les sous-groupes distingués de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ en fonction de ceux de G. On note $\pi : \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ la projection canonique. La correspondance $K \mapsto \pi(K)$ établit une bijection entre l'ensemble des sous-groupes de G contenant H et l'ensemble des sous-groupes de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ donc la réciproque est donnée par $\overline{K} \mapsto \pi^{-1}(\overline{K})$. Cette bijection induit une bijection entre les sous-groupes distingués de G contenant H et les sous-groupes distingués de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

b) Soit K un sous-groupe de G.

i) Supposons que K soit distingué dans G et que K contienne H. Montrons que
$${}^{\mathrm{G}}\!/_{\mathrm{H}}{}^{\mathrm{K}}\!/_{\mathrm{H}} \simeq {}^{\mathrm{G}}\!/_{\mathrm{K}}$$
Le morphisme $\pi : \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ composé avec la projection $\pi' : {}^{\mathrm{G}}\!/_{\mathrm{H}} \to ({}^{\mathrm{G}}\!/_{\mathrm{H}})/({}^{\mathrm{K}}\!/_{\mathrm{H}})$ induit un morphisme surjectif $q : \mathrm{G} \to ({}^{\mathrm{G}}\!/_{\mathrm{H}})/({}^{\mathrm{K}}\!/_{\mathrm{H}})$. Par construction un élément

g de G appartient à $\ker q$ si et seulement si $\pi(g)$ appartient à $\ker \pi' = {}^{\mathrm{K}}\!/_{\mathrm{H}}$ si et seulement si g appartient à K. Ainsi $\ker q = \mathrm{K}$. Le théorème de factorisation assure alors que q induit un isomorphisme entre $\mathrm{G}/\ker q = {}^{\mathrm{G}}\!/_{\mathrm{K}}$ et $({}^{\mathrm{G}}\!/_{\mathrm{H}})/({}^{\mathrm{K}}\!/_{\mathrm{H}})$.

ii) Montrons que HK est un sous-groupe de G égal à KH.

Soient h, h' dans H et k, k' dans K. Le groupe H étant distingué dans G il existe h'' dans H tel que $k \cdot h' = h'' \cdot k$. Par suite

$$(h \cdot k) \cdot (h' \cdot k') = (h \cdot h'') \cdot (k \cdot k')$$

appartient à HK et HK est un sous-groupe de G.

iv) Montrons que $\mathrm{K}/(\mathrm{K} \cap \mathrm{H})$ et $(\mathrm{HK})/\mathrm{H}$ sont isomorphes. L'inclusion $\mathrm{K} \to \mathrm{HK}$ induit un morphisme $p\colon \mathrm{K} \to (\mathrm{HK})/\mathrm{H}$. Montrons que p est surjectif : si h est dans H et k dans K, alors la classe $(h \cdot k)\mathrm{H} = k\mathrm{H}$ est l'image de k par p, donc p est surjectif. De plus un élément $k \in \mathrm{K}$ appartient à $\ker p$ si et seulement si il est dans H. Autrement dit $\ker p = \mathrm{K} \cap \mathrm{H}$. On conclut à l'aide du théorème de factorisation.

Exercice 80 Soit G un groupe fini. Soient H et K des sous-groupes de G. Supposons que
— H et K sont des sous-groupes distingués de G ;
— $\mathrm{H} \cap \mathrm{K} = \{e\}$.
Montrer que HK est un sous-groupe distingué de G d'ordre $|\mathrm{H}||\mathrm{K}|$.

Éléments de réponse 80 Montrons tout d'abord que HK est un sous-groupe de G. On définit l'application φ par

$$\varphi\colon \mathrm{H} \times \mathrm{K} \to \mathrm{HK} \qquad\qquad (h,k) \mapsto hk.$$

Cette application est injective. En effet soient h, h' dans H et k, k' dans K tels que $f(h,k) = f(h',k')$, *i.e.* $hk = h'k'$. On en déduit que $hh'^{-1} = k'k^{-1}$; de plus $hh'^{-1} = k'k^{-1}$ appartient à $\mathrm{H} \cap K = \{e\}$. Donc $hh'^{-1} = e$ et $kk'^{-1} = e$ c'est-à-dire $(h,k) = (h',k')$. Cette application est par définition surjective. Soient h, h' dans H et soient k, k' dans K. Puisque K est distingué il existe k_1 dans K tel que $hk = k_1 h$. Comme H est distingué il existe h_1 dans H tel que $k_1 h = h_1 k_1$. Ainsi $hk = h_1 k_1$. Mais φ est injective d'où $h = h_1$, $k = k_1$ et h et k commutent $(hk = kh)$. Donc $hkh'k' = hh'kk'$. On en déduit que
— HK est un sous-groupe de G : la loi est stable dans HK, e appartient à HK et si $g \in \mathrm{HK}$, alors $g^{-1} \in \mathrm{H}K$;
— φ est un homomorphisme.
En particulier φ est un isomorphisme de groupes.

Montrons que HK est distingué dans G. Soient $g \in \mathrm{G}$, $h \in \mathrm{H}$ et $k \in \mathrm{K}$. Alors

$$ghkg^{-1} = (ghg^{-1})(gkg^{-1}) = h_1(gkg^{-1})$$

avec h_1 dans H car H est distingué dans G. Par ailleurs $h_1 gkg^{-1} = h_1 k_1$ avec k_1 dans K car K est distingué dans G. Donc $ghkg^{-1}$ appartient à HK et HK est distingué dans G.

Montrons que HK est d'ordre |H||K|. Comme φ est un isomorphisme de groupes l'ordre de HK est celui de $\mathrm{H} \times \mathrm{K}$, *i.e.* |H||K|.

Exercice 81 Soit G un groupe de centre $Z(\mathrm{G})$.

a) Montrer que $Z(\mathrm{G})$ est un sous-groupe distingué de G.

b) Montrer que si ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est monogène (*i.e.* ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est engendré par un seul élément), alors G est abélien.

Éléments de réponse 81

a) Le centre de G est un sous-groupe de G. En effet si $x \in Z(\mathrm{G})$ et $y \in Z(\mathrm{G})$, alors $y^{-1} \in Z(\mathrm{G})$ et pour tout élément g de G on a $xy^{-1}g = xgy^{-1} = gxy^{-1}$ ce qui implique que xy^{-1} appartient à $Z(\mathrm{G})$.

Par ailleurs soit $g \in \mathrm{G}$ et soit $c \in Z(\mathrm{G})$. Comme c commute avec tous les éléments de G nous avons

$$gcg^{-1} = cgg^{-1} = c.$$

Donc $gZ(\mathrm{G})g^{-1} = Z(\mathrm{G})$ et $Z(\mathrm{G})$ est un sous-groupe distingué dans G.

b) Si $\mathrm{G} = Z(\mathrm{G})$, alors G est abélien. Si $\mathrm{G} \neq Z(\mathrm{G})$ et si ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est monogène non trivial, alors il existe un élément x de G tel que $x \notin Z(\mathrm{G})$ et ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})} = \langle xZ(\mathrm{G})\rangle$. Soit y dans G. Ou bien $y \in Z(\mathrm{G})$ et $xy = yx$. Ou bien $y \notin Z(\mathrm{G})$ et il existe $n \in \mathbb{N}$ tel que $y \in (xZ(\mathrm{G}))^n = x^nZ(\mathrm{G})$, autrement dit $y = x^nc$ avec $c \in Z(\mathrm{G})$. Dans ce cas $xy = xx^nc = x^ncx = yx$. Ainsi x commute avec tous les éléments de G, *i.e.* $x \in Z(\mathrm{G})$: contradiction. Ainsi $\mathrm{G} = Z(\mathrm{G})$ et G est abélien.

Exercice 82 On note $\mathbb{H}_8$ le sous-groupe de $\mathrm{GL}(2,\mathbb{C})$, appelé *groupe des quaternions* engendré par les trois matrices

$$I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad J = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix} \qquad K = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}$$

1. Calculer l'ordre de $\mathbb{H}_8$.
2. Exhiber les sous-groupes de $\mathbb{H}_8$.
3. Exhiber les sous-groupes distingués de $\mathbb{H}_8$.
4. Est-il isomorphe au groupe diédral D_8 ?

Éléments de réponse 82

1. On vérifie que

$$I^2 = J^2 = K^2 = -\mathrm{id} \qquad IJ = K.$$

Par conséquent le groupe des quaternions est

$$\mathbb{H}_8 = \{\mathrm{id},\ -\mathrm{id},\ I,\ -I,\ J,\ -J,\ K,\ -K\}.$$

En particulier il est d'ordre 8.

2. D'après le théorème de LAGRANGE les sous-groupes propres de $\mathbb{H}_8$ sont d'ordre 2 ou 4. Il y a un seul sous-groupe d'ordre 2 : $\langle -\mathrm{id}\rangle$ et trois sous-groupes d'ordre 4 : $\langle I\rangle$, $\langle J\rangle$, $\langle K\rangle$.
3. Tous les sous-groupes de $\mathbb{H}_8$ sont distingués.
4. Le groupe diédral D_8 compte 5 éléments d'ordre 2 donc n'est pas isomorphe à $\mathbb{H}_8$ qui n'en compte qu'un.

Exercice 83 Soit Q_8 le groupe des matrices 2×2 inversibles engendré par $\begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$ et $\begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}$. Ce groupe est appelé le groupe des quaternions.

a) Quel est l'ordre de Q_8 ?
b) Montrer que Q_8 n'a qu'un élément d'ordre 2.
c) Quel est le centre de Q_8 ?
d) Montrer que tous les sous-groupes de Q_8 sont distingués.
e) Peut-on trouver un isomorphisme entre Q_8 et un produit semi-direct de $\mathbb{Z}/4\mathbb{Z}$ avec $\mathbb{Z}/2\mathbb{Z}$?

Éléments de réponse 83 Posons $\mathcal{I} = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$, $\mathcal{J} = \begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}$, $\mathcal{K} = \mathcal{I}\mathcal{J} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

a) On vérifie que Id est l'élément neutre,

$$-\mathrm{Id}M = -M \quad \forall\, M \in \{\mathcal{I},\ \mathcal{J},\ \mathcal{K}\} \qquad \mathcal{I}^2 = \mathcal{J}^2 = \mathcal{K}^2 = -\mathrm{Id}$$
$$\mathcal{I}\mathcal{J} = \mathcal{K},\ \mathcal{J}\mathcal{K} = \mathcal{I},\ \mathcal{K}\mathcal{I} = \mathcal{J} \qquad \mathcal{J}\mathcal{I} = -\mathcal{K},\ \mathcal{K}\mathcal{J} = -\mathcal{I},\ \mathcal{I}\mathcal{K} = -\mathcal{J}$$

Il en résulte que Q_8 contient 8 élements.

b) D'après ce qui précède l'unique élément d'ordre 2 est $-\mathrm{Id}$.
c) D'après ce qui précède le centre de Q_8 est $\{\mathrm{Id},\ -\mathrm{Id}\}$.
d) Les sous-groupes de Q_8 sont le groupe trivial, le centre de Q_8 et

$$\langle\mathcal{I}\rangle = \{\mathrm{Id},\ -\mathrm{Id},\ \mathcal{I},\ -\mathcal{I}\} \qquad \langle\mathcal{J}\rangle = \{\mathrm{Id},\ -\mathrm{Id},\ \mathcal{J},\ -\mathcal{J}\} \qquad \langle\mathcal{K}\rangle = \{\mathrm{Id},\ -\mathrm{Id},\ \mathcal{K},\ -\mathcal{K}\}$$

e) Les groupes $\langle\mathcal{I}\rangle$, $\langle\mathcal{J}\rangle$ et $\langle\mathcal{K}\rangle$ sont tous trois cycliques d'ordre 4 donc isomorphes à $\mathbb{Z}/4\mathbb{Z}$ mais aucun d'entre eux ne peut être un facteur semi-direct de Q_8 car l'autre facteur serait d'ordre 2 et d'intersection réduite à $\{\mathrm{Id}\}$ avec le facteur d'ordre 4. Or tous ces sous-groupes d'ordre 4 contiennent le sous-groupe d'ordre 2. Par conséquent Q_8 ne peut s'obtenir comme produit semi-direct de deux de ses sous-groupes propres.

Exercice 84 Soit G un groupe d'ordre 55 possédant deux sous-groupes distingués d'ordre 5 et 11 respectivement. Montrer que G est isomorphe à $\mathbb{Z}/55\mathbb{Z}$.

Éléments de réponse 84 Si H et K sont d'ordre respectif 5 et 11, alors $\mathrm{H} \cap \mathrm{K} = \{e\}$ (en effet tous les éléments de $\mathrm{H} \setminus \{e\}$ sont d'ordre 5 et tous les éléments de $\mathrm{K} \setminus \{e\}$ sont d'ordre 11.

L'exercice 5.3 assure que HK est un sous-groupe de G d'ordre $5 \times 11 = 55$ qui est l'ordre de G. Il en résulte que $\mathrm{G} = \mathrm{HK}$. Alors HK est isomorphe à $\mathrm{H} \times \mathrm{K}$. Par suite G est isomorphe à $\mathrm{H} \times \mathrm{K}$. Or H est isomorphe à $\mathbb{Z}/5\mathbb{Z}$ et K est isomorphe à $\mathbb{Z}/11\mathbb{Z}$ donc G est isomorphe à $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} = \mathbb{Z}/55\mathbb{Z}$ (théorème chinois).

Exercice 85 [Formule de Burnside et coloriage de polyèdres]

1. Soit G un groupe fini agissant sur un ensemble fini X. Pour tout $x \in X$ on désigne par $\mathcal{O}_x$ l'orbite de x par l'action de G et par G_x son stabilisateur.
   a) Soient $x \in X$ et $y \in \mathcal{O}_x$. Trouvez $z \in \mathrm{G}$ tel que
   $$\mathrm{G}_y = z^{-1}\mathrm{G}_x z.$$
   b) Montrer que pour tout $x \in X$
   $$|\mathrm{G} = | = \sum_{y \in \mathcal{O}_x} |\mathrm{G}_y|.$$
   c) En déduire que
   $$|\Omega| = \frac{1}{|\mathrm{G}|} \sum_{x \in X} |\mathrm{G}_x|$$
   où $\Omega = \{\mathcal{O}_x \,|\, x \in X\}$ est l'ensemble des orbites dans X par l'action de G.
   d) En décomposant de deux façons différentes l'ensemble $F = \{(g, x) \in \mathrm{G} \times X \,|\, g \cdot x = x\}$ déduire de la question précédente la formule de Burnside
   $$|\Omega| = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|$$
   où $\mathrm{Fix}(g)$ est l'ensemble des points $x \in X$ tels que $g \cdot x = x$.
2. On cherche maintenant à déterminer le nombre de façons de colorier les faces et les arêtes d'un tétraèdre régulier, où K couleurs sont disponibles, à chaque face et à chaque arête étant attribuée une couleur et une seule. Le tétraèdre T est vu comme un sous-ensemble de l'espace vectoriel $\mathbb{R}^3$ et on le suppose centré en 0.

   Nous identifions deux coloriages du tétraèdre s'il existe une rotation R de l'espace euclidien $\mathbb{R}^3$ qui préserve le tétraèdre, *i.e.* $R(T) = T$, et qui envoie le premier coloriage sur le second.
   a) Soit X l'ensemble des coloriages où on interdit cette identification. Quel est le cardinal de X ?

b) Montrer que l'ensemble des rotations préservant T, muni de la loi de composition, est un groupe.
Notons G ce groupe. On admet qu'il est fini et plus précisément que $|\mathrm{G}| = 12$:
- l'identité $\mathrm{id}_{\mathbb{R}^3}$;
- 3 rotations d'axe passant par le milieu d'une arête et le milieu de l'arête opposée, et d'angle π ;
- 8 rotations d'axe passant par un sommet et le centre de la face opposée, et d'angle $\pm 2\pi/3$.

c) Le groupe G agit naturellement sur X, et chaque coloriage du tétraèdre correspond à une orbite $\mathcal{O}_x$ dans X par l'action de G. Exprimer le nombre de coloriages du tétraèdre en fonction de K.

Éléments de réponse 85

1. Voir cours

2. On cherche maintenant à déterminer le nombre de façons de colorier les faces et les arêtes d'un tétraèdre régulier, où K couleurs sont disponibles, à chaque face et à chaque arête étant attribuée une couleur et une seule. Le tétraèdre T est vu comme un sous-ensemble de l'espace vectoriel $\mathbb{R}^3$ et on le suppose centré en 0.

   Nous identifions deux coloriages du tétraèdre s'il existe une rotation R de l'espace euclidien $\mathbb{R}^3$ qui préserve le tétraèdre, *i.e.* $R(T) = T$, et qui envoie le premier coloriage sur le second.

   a) Soit X l'ensemble des coloriages où on interdit cette identification. Quel est le cardinal de X ?
   Un tétraèdre régulier a quatre faces S_1, S_2, S_3, S_4 et six arêtes A_1, A_2, …, A_6. En particulier il y a dix objets à colorier. On a donc $|X| = k^{10}$.

   b) Montrons que l'ensemble des rotations préservant T, muni de la loi de composition, est un groupe.
   Voir cours.
   Notons G ce groupe. On admet qu'il est fini et plus précisément que $|\mathrm{G}| = 12$:
   - l'identité $\mathrm{id}_{\mathbb{R}^3}$;
   - 3 rotations d'axe passant par le milieu d'une arête et le milieu de l'arête opposée, et d'angle π ;
   - 8 rotations d'axe passant par un sommet et le centre de la face opposée, et d'angle $\pm 2\pi/3$.

   c) Le groupe G agit naturellement sur X, et chaque coloriage du tétraèdre correspond à une orbite $\mathcal{O}_x$ dans X par l'action de G. Exprimons le nombre de coloriages du tétraèdre en fonction de K.

Appliquons la formule de Burnside : soit n le nombre de coloriages, ou de manière équivalente le nombre d'orbites de G sur X. Alors

$$n = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|$$

Trois cas sont à distinguer :

- Si $g = \mathrm{id}$, alors $\mathrm{Fix}(g) = X$; par suite $|\mathrm{Fix}(g)| = |X| = k^{10}$.
- Si G est l'une des trois rotations d'axe passant par le milieu d'une arête et le milieu de l'arête opposée, et d'angle π. Alors $|\mathrm{Fix}(g)| = k^6$.
- Si G est l'une des huit rotations d'axe passant par un sommet et le centre de la face opposée, et d'angle $\pm\frac{2\pi}{3}$. Par conséquent $|\mathrm{Fix}(g)| = k^4$.

Finalement

$$n = \frac{1}{12}\left(k^{10} + 3 \cdot k^6 + 8 \cdot k^4\right)$$

Exercice 86

1. Soit G un groupe fini de cardinal p^m avec p premier et $m \in \mathbb{N}^*$ qui opère sur un ensemble fini non vide E. Posons

   $$E^{\mathrm{G}} = \{x \in E \,|\, \forall\, g \in \mathrm{G},\, g \cdot x = x\}.$$

   Montrer que $|E^{\mathrm{G}}| = |E| \bmod p$.
2. Soit H un groupe fini d'ordre n. Soit p un diviseur premier de n. Montrer que H contient un élément d'ordre p (lemme de Cauchy). Indication : faire agir $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble E des $(x_1, x_2, \ldots, x_p)$ de H^p tels que $x_1 x_2 \ldots x_p = e$.
3. Soit H un groupe fini d'ordre n. Soit $m \in \mathbb{N}^*$ tel que pour tout $x \in \mathrm{H}$ on ait $x^m = e$. Montrer que n divise une puissance de m.

Éléments de réponse 86

1. Si x appartient à E, nous notons $\mathcal{O}(x)$ l'orbite de x sous l'action de G. Les éléments de E^{G} sont exactement les éléments x de E tels que $\mathcal{O}(x) = \{x\}$. Notons ω_1, ω_2, …, ω_r les orbites de E de cardinal strictement supérieur à 1. Si x_i est un élément de ω_i, alors $|\omega_i| = [\mathrm{G} : \mathrm{Stab}_{\mathrm{G}}(x_i)]$, c'est donc une puissance de p. Il résulte de l'équation aux classes que

   $$|E| = |E^{\mathrm{G}}| + \sum_{i=1}^{r} |\omega_i| \equiv |E^{\mathrm{G}}| \mod p$$

2. Soit $(x_1, x_2, \ldots, x_p)$ un élément de E. Nous avons $x_1 x_2 \ldots x_p = e$. En multipliant à gauche par x_1^{-1} et à droite par x_1 nous obtenons $x_2 x_3 \ldots x_p x_1 = e$, *i.e.* $(x_2, x_3, \ldots, x_p, x_1)$ appartient à E. Notons c le cycle $(1\ 2\ \ldots\ p)$ de $\mathcal{S}_p$. Il s'agit d'un élément d'ordre p qui

engendre un sous-groupe cyclique K isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Nous définissons une opération de K sur l'ensemble H^p par

$$c \cdot (x_1, x_2, \ldots, x_p) = (x_{c(1)}, x_{c(2)}, \ldots, x_{c(p)}) = (x_2, x_3, \ldots, x_p, x_1).$$

La remarque ci-dessus montre que E est stable par cette opération. Appliquons alors le résultat de la question précédente à l'opération induite sur E. Nous avons $|E| \equiv |E^{\mathrm{K}}| \mod p$. Le cardinal de E est n^{p-1} (en effet on peut choisir x_1, x_2, …, x_{p-1} quelconques, x_p est alors déterminé de manière unique). Comme p divise n, $|E^{\mathrm{K}}|$ est nul modulo p. Or les éléments de E^{K} sont justement les p-uplets $(x, x, \ldots, x)$ avec $x^p = e$. Notons que E^{K} contient le p-uplet $(e, e, \ldots, e)$; en particulier E^{K} est non vide et par suite E^{K} a un cardinal supérieur à p. Il y a donc au moins $(p-1)$ éléments d'ordre p dans H.

3. Il suffit de montrer que tous les facteurs premiers de n sont des facteurs premiers de m. Soit p un premier divisant n. Le lemme de Cauchy garantit l'existence d'un élément $x \in \mathrm{H}$ d'ordre p. Or par hypothèse $x^m = e$ donc p divise m.

Exercice 87 Soit G un groupe fini. Soit p le plus petit nombre premier divisant $|\mathrm{G}|$. Soit H un sous-groupe de G d'indice p. On se propose de montrer que H est distingué dans G.

a) Montrer que H opère sur l'ensemble des classes à gauche G/H par $h \cdot (a\mathrm{H}) = (ha)\mathrm{H}$ pour tout $h \in \mathrm{H}$ et pour tout $a \in \mathrm{G}$.

Quel est le stabilisateur de $a\mathrm{H}$?

Quelle est l'orbite de la classe H ?

b) Montrer que si H n'était pas distingué dans G, alors au moins une des orbites aurait un cardinal $\geq p$.

c) Conclure.

Éléments de réponse 87

a) On peut vérifier que $h \cdot (a\mathrm{H}) = (ha)\mathrm{H}$ est bien définie : si $a\mathrm{H} = b\mathrm{H}$, alors $(ha)\mathrm{H} = (hb)\mathrm{H}$ donc $h \cdot (a\mathrm{H})$ ne dépend pas du représentant a choisi dans une même classe à gauche), et que ceci définit une opération de groupe.

Le stabilisateur de $a\mathrm{H}$ est $\mathrm{H} \cap a\mathrm{H}a^{-1}$ car dire que $h \in \mathrm{H}$ vérifie $h \cdot (a\mathrm{H}) = a\mathrm{H}$ signifie que $a^{-1}(ha)$ appartient à H ou encore que h appartient à $a\mathrm{H}a^{-1}$.

L'orbite de H est réduite à H.

b) Si H n'est pas distingué dans G, alors il y a au moins une orbite dont le cardinal n'est pas 1 puisque cela signifie qu'il existe $a \in \mathrm{G}$ et $h \in \mathrm{H}$ tel que $a^{-1}(ha)$ n'appartient pas à H. Puisque le cardinal de cette orbite divise celui de H (donc aussi celui de G par le théorème de Lagrange) ce cardinal est au moins p étant donné que p est le plus petit diviseur ≥ 2 de $|\mathrm{G}|$.

c) Si G n'est pas distingué dans G, alors il y a au moins une orbite de cardinal au moins p mais il y a aussi une orbite de cardinal 1 (celle de H). L'équation aux classes assure alors que $\left|{}^{\mathrm{G}}\!/_{\mathrm{H}}\right| \geq p+1$: contradiction avec le fait que $[\mathrm{G} : \mathrm{H}] = p$.

Exercice 88 Soit E un espace vectoriel de dimension finie n sur un corps $\Bbbk$.

a) Faisons opérer le groupe linéaire $\mathrm{G} = \mathrm{GL}(E)$ sur l'ensemble des sous-espaces vectoriels de E par $g \cdot F := g(F)$ pour tout $g \in \mathrm{G}$ et tout sous-espace F de E. Quelles sont les orbites pour cette action ?

b) On prend $\Bbbk = {}^{\mathbb{Z}}\!/_{7\mathbb{Z}}$ et $n = 5$. Combien E possède-t-il de sous-espaces vectoriels de dimension 3 ?

Éléments de réponse 88

a) L'orbite d'un sous-espace de dimension d ne contient que des sous-espaces de dimension d.

Réciproquement si F et G sont des sous-espaces de dimension d, on choisit une base $(f_1, f_2, \ldots, f_d)$ de F que l'on complète en une base $(f_1, f_2, \ldots, f_d, f_{d+1}, \ldots, f_n)$ de E. De même on peut prendre une base $(g_1, g_2, \ldots, g_d)$ de F que l'on complète en une base $(g_1, g_2, \ldots, g_d, g_{d+1}, \ldots, g_n)$ de E. L'endomorphisme qui envoie f_i sur g_i est bijectif et vérifie $u(F) = G$. Finalement les orbites sont les sous-espaces de dimension d pour $d = 0, 1, \ldots, n$.

b) Fixons un sous-espace F de dimension 3 (on sait qu'il y en a au moins 1). D'après a) le nombre cherché est le cardinal de l'orbite de F sous l'action de $\mathrm{GL}(E)$ ou encore l'ordre de $\mathrm{GL}(E)$ divisé par celui du stabilisateur S de F. Le cardinal de $\mathrm{GL}(E)$ est obtenu en comptant le nombre de bases de E, il vaut

$$(7^5-1)(7^5-7)(7^5-7^2)(7^5-7^3)(7^5-7^4).$$

En prenant une base de F que l'on complète en une base de E on voit que S est isomorphe au groupe des matrices-bloc de la forme

$$\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$$

où $A \in \mathrm{GL}(3, \mathbb{F}_7)$, $B \in \mathrm{M}_{3,2}(\mathbb{F}_7)$ et $C \in \mathrm{GL}(2, \mathbb{F}_7)$. Ainsi

$$|S| = (7^3-1)(7^3-7)(7^3-7^2)(7^2-1)(7^2-7)7^6.$$

Par suite le cardinal cherché est

$$\begin{aligned}
&\frac{(7^5-1)(7^5-7)(7^5-7^2)(7^5-7^3)(7^5-7^4)}{(7^3-1)(7^3-7)(7^3-7^2)(7^2-1)(7^2-7)7^6}\\
&\qquad=\frac{7\times 7^2\times 7^3\times 7^4\times(7^5-1)(7^4-1)(7^3-1)(7^2-1)(7-1)}{7\times 7^2\times 7\times 7^6\times(7^3-1)(7^2-1)(7-1)(7^2-1)(7-1)}\\
&\qquad=\frac{(7^5-1)(7^4-1)}{(7^2-1)(7-1)}\\
&\qquad=140050
\end{aligned}$$

Exercice 89

a) Combien y a-t-il d'opérations du groupe $\mathbb{Z}/4\mathbb{Z}$ sur l'ensemble $\{1, 2, 3, 4, 5\}$?

b) Soient G et X deux groupes. On dit que G *opère par automorphismes sur* X si on s'est donné une opération $(g, x) \mapsto g \cdot x$ de G sur X telle que pour tout $g \in$ G l'application $x \mapsto g \cdot x$ soit un automorphisme de X.

L'opération de G sur lui-même par translation est-elle une opération par automorphismes ?

L'opération de G sur lui-même par conjugaison est-elle une opération par automorphismes ?

c) Si G $= \left(\mathbb{Z}/3\mathbb{Z}, +\right)$ et $X = \left(\mathbb{Z}/13\mathbb{Z}, +\right)$ combien y a-t-il d'actions de G sur X par automorphismes ?

d) Si G $= \left(\mathbb{Z}/3\mathbb{Z}, +\right)$ et $X = \left(\mathcal{S}_3, \circ\right)$ combien y a-t-il d'actions de G sur X par automorphismes ?

Éléments de réponse 89

a) On cherche le nombre de morphismes de $\mathbb{Z}/4\mathbb{Z}$ dans le groupe des permutations $\mathcal{S}_5$. Se donner un tel morphisme f revient à se donner un élément d'ordre divisant 4 (à savoir $f(\overline{1})$) dans $\mathcal{S}_5$. Or $\mathcal{S}_5$ contient
— un élément d'ordre 1 (l'identité),
— $\binom{5}{2} = 10$ transpositions,
— $5 \cdot 3 = 15$ doubles transpositions (cinq façons de choisir le point fixe puis trois double transpositions avec les quatre éléments restants),
— $5 \cdot 6 = 30$ 4-cycles (cinq façons de choisir le point fixe et six 4-cycles dans le groupe des permutations des quatre éléments restants).
Il y a donc au total $1 + 10 + 15 + 30 = 56$ possibilités.

b) L'opération de G sur lui-même par translation n'est pas une opération par automorphismes.

L'opération de G sur lui-même par conjugaison est une opération par automorphismes.

c) Le groupe des automorphismes de X est isomorphe au groupe multiplicatif de l'anneau $\mathbb{Z}/13\mathbb{Z}$ (en effet si on pose $\varphi_a(x) = ax$ on peut vérifier que $a \mapsto \varphi_a$ est un isomorphisme de $\left(\mathbb{Z}/13\mathbb{Z}\right)^\times$ sur $\mathrm{Aut}(X)$) lequel est isomorphe au groupe additif $\mathbb{Z}/12\mathbb{Z}$ car 13 est premier. On cherche donc le nombre de morphismes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/12\mathbb{Z}$ ou encore le nombre d'éléments de $\mathbb{Z}/12\mathbb{Z}$ d'ordre divisant 3. Il y a ainsi 3 possibilités.

d) Les seuls automorphismes de $\mathcal{S}_3$ sont intérieurs. Le groupe des automorphismes de $\mathcal{S}_3$ est donc isomorphe à $\mathcal{S}_3$ quotienté par son centre, c'est-à-dire à $\mathcal{S}_3$. On est donc ramené à chercher le nombre d'éléments d'ordre 1 ou 3 dans $\mathcal{S}_3$ et il y a 3 possibilités.

Exercice 90 Soit E un espace euclidien. On fait opérer le groupe orthogonal $\mathrm{O}(E)$ de E sur l'ensemble des sous-espaces vectoriels de E.

a) Quelles sont les orbites pour cette action ?

b) Donner un énoncé analogue pour les espaces hermitiens.

c) Y a-t-il un énoncé analogue pour le groupe orthogonal $\mathrm{O}(q)$ d'un espace vectoriel de dimension finie muni d'une forme quadratique non dégénérée q ?

Éléments de réponse 90

a) L'orbite d'un sous-espace de dimension d ne contient que des sous-espaces de dimension d.

Réciproquement si F et G sont des sous-espaces de dimension d, on choisit une base orthonormée $(f_1, f_2, \ldots, f_d)$ de F que l'on complète en une base orthonormée $(f_1, f_2, \ldots, f_d, f_{d+1}, \ldots, f_n)$ de E. De même on peut prendre une base orthonormée $(g_1, g_2, \ldots, g_d)$ de F que l'on complète en une base orthonormée $(g_1, g_2, \ldots, g_d, g_{d+1}, \ldots, g_n)$ de E. L'endomorphisme qui envoie f_i sur g_i est bijectif et vérifie $u(F) = G$. Finalement les orbites sont les sous-espaces de dimension d pour $d = 0, 1, \ldots, n$.

b) Idem en remplaçant le groupe orthogonal de E par le groupe unitaire de E.

c) Il est clair que si F est un sous-espace une condition nécessaire pour qu'un autre sous-espace G soit dans l'orbite de F est que les restrictions de q à F et G soient des formes quadratiques isomorphes (ce qui entraîne en particulier $\dim F = \dim G$ mais n'est pas équivalent à cette condition. Cette condition est en fait suffisante mais c'est un énoncé difficile, le théorème de Witt ([**Per82**]).

Exercice 91 Soit G un groupe. Soit g un élément de G. On appelle *centralisateur* de g l'ensemble G_g des éléments h de G tels que $hg = gh$.

a) Montrer que G_g est un sous-groupe de G. Est-il toujours distingué ?

b) Supposons que G soit fini. Soit C la classe de conjugaison de g. Trouver une relation entre $|\mathrm{G}|$, $|C|$ et $|\mathrm{G}_g|$.

Éléments de réponse 91

a) Il est immédiat que G_g est un sous-groupe de G mais il n'est pas toujours distingué : par exemple dans $\mathcal{S}_3$ le centralisateur d'une transposition τ n'est pas distingué dans $\mathcal{S}_3$.

b) La groupe G opère par conjugaison sur lui-même. Par définition C est l'orbite de g et G_{g_0} son stabilisateur d'où

$$|\mathrm{G}| = |C| \cdot |\mathrm{G}_g|.$$

Exercice 92 Soit G un groupe opérant sur un ensemble X. Si (g, x) appartient à $\mathrm{G} \times X$ quelle relation peut-on écrire entre $\mathrm{Stab}(x)$ et $\mathrm{Stab}(g \cdot x)$?

Éléments de réponse 92 Nous avons $\mathrm{Stab}(g \cdot x) = g \cdot \mathrm{Stab}(x) \cdot g^{-1}$.

Exercice 93 Soit G un groupe d'ordre 33 agissant sur un ensemble X de cardinal 19. Montrer qu'il existe une orbite de cardinal 1.

Éléments de réponse 93 Utiliser la formule des classes.

Exercice 94 Pour chaque polyèdre régulier et convexe $\mathcal{P}$ d'un espace euclidien $\mathcal{E}$ de dimension 3 déterminer le nombre d'isométries de $\mathcal{E}$ préservant $\mathcal{P}$.

Éléments de réponse 94 Le groupe $\mathrm{Isom}(\mathcal{P})$ agit transitivement sur $\mathcal{P}$; il suffit donc de déterminer l'ordre du stabilisateur d'un sommet de $\mathcal{P}$.

Exercice 95 Combien de colliers de 9 perles différents peut-on faire avec 4 perles bleues, 3 perles blanches et 2 perles oranges ?

Éléments de réponse 95 Il faut compter le nombre d'orbites en considérant l'action du groupe diédral D_9 sur un polygone régulier à 9 côtés dont on a coloré les sommets en suivant l'énoncé. En utilisant la formule de Burnside on trouve que l'on peut réaliser 76 colliers distincts.

Exercice 96 Montrer que nous avons les isomorphismes suivants

$$\mathrm{PGL}(2, \mathbb{F}_2) \simeq \mathcal{S}_3, \qquad \mathrm{PGL}(2, \mathbb{F}_3) \simeq \mathcal{S}_4, \qquad \mathrm{PSL}(2, \mathbb{F}_3) \simeq \mathcal{A}_4, \qquad \mathrm{PGL}(2, \mathbb{F}_4) \simeq \mathcal{A}_5.$$

Éléments de réponse 96 Le groupe $\mathrm{PGL}(n, \mathbb{F}_q)$ agit fidèlement sur les droites de $\mathbb{F}_q^n$.

Exercice 97 Soit $\Bbbk$ un corps commutatif. Considérons l'action du groupe $\mathrm{GL}(m, \Bbbk) \times \mathrm{GL}(n, \Bbbk)$ sur $\mathrm{M}_{m,n}(\Bbbk)$ définie par $\big((P, Q), M\big) \mapsto PMQ^{-1}$.

Déterminer le nombre d'orbites de cette action.

Éléments de réponse 97 Il s'agit de classer les matrices à équivalence près. On en déduit qu'il y a $\min(m,n)+1$ orbites.

Exercice 98 Soit $\Bbbk$ un corps commutatif. Considérons l'action de $\mathrm{GL}(n,\Bbbk)$ sur $\mathrm{Sym}(n,\Bbbk)$ définie par

$$(P,S)\mapsto PS{}^{\mathrm{t}}P$$

a) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk=\mathbb{C}$.
b) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk=\mathbb{R}$.
c) Déterminer le nombre d'orbites de cette action lorsque $\Bbbk=\mathbb{F}_p$ lorsque p désigne un nombre premier impair.

Éléments de réponse 98 Il s'agit de classer les formes bilinéaires sur $\Bbbk^n$.
— Si $\Bbbk=\mathbb{C}$, alors il y a $n+1$ orbites.
— Si $\Bbbk=\mathbb{R}$, alors il y a $\frac{(n+2)(n+1)}{2}$ orbites.
— Si $\Bbbk=\mathbb{F}_p$, alors il y a $2n+1$ orbites.

Exercice 99 Soit G un groupe d'ordre $n\in\mathbb{N}^*$ et soit $\Bbbk$ un corps commutatif. Montrer qu'il existe un morphisme de groupes injectif de G dans $\mathrm{GL}(n,\Bbbk)$. **Éléments de réponse 99** Utiliser le théorème de Cayley.

Exercice 100 Soit G un groupe d'ordre $2m$ avec $m\in\mathbb{N}^*$ impair. Montrer que G admet un sous-groupe d'indice 2.

Éléments de réponse 100 Utiliser le théorème de Cayley.

Exercice 101 Déterminer les groupes finis admettant exactement deux classes de conjugaison.

Éléments de réponse 101 Avec la formule des classes on trouve $\mathrm{G}\simeq{}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.

Exercice 102 Déterminer les groupes finis admettant exactement trois classes de conjugaison.

Éléments de réponse 102 La formule des classes assure qu'il existe un couple (a,b) dans $\mathbb{N}^2$ tel que $1\leq b\leq a\leq|\mathrm{G}|$ et

$$1=\frac{1}{|\mathrm{G}|}+\frac{1}{a}+\frac{1}{b}.$$

Nous en déduisons que $1\leq b\leq 3$ puis en étudiant les différents cas nous obtenons que $\mathrm{Card}(\mathrm{G})\leq 6$. Finalement nous obtenons que $\mathrm{G}\simeq{}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$ ou $\mathrm{G}\simeq\mathcal{S}_3$.

Exercice 103 Soit G un groupe d'ordre p^n où n appartient à $\mathbb{N}^*$ et p est un nombre premier. Montrer que le centre de G n'est pas trivial.

Éléments de réponse 103 Faire agir G sur lui-même et utiliser la formule des classes.

Exercice 104 Soit G un groupe d'ordre infini. Supposons que G admette un sous-groupe propre H d'indice fini. Montrer que G n'est pas simple.

Éléments de réponse 104 Faire agir G sur G/H par translation des classes.

Exercice 105 Soit G un groupe fini d'ordre $n \geq 2$. Soit p le plus petit facteur premier de n. Montrer que si H est un sous-groupe de G d'ordre p alors H est central.

Éléments de réponse 105 Faire agir G sur H par conjugaison. Étudier le cardinal de chaque orbite pour obtenir qu'elles sont des singletons.

Exercice 106 Soit G un groupe opérant sur un ensemble E. On note pour $g \in \mathrm{G}$ et $x \in E$ l'action de g sur x par : $g \cdot x$.

1. Montrer que pour tout x dans le E le stabilisateur
$$\mathrm{Stab}_{\mathrm{G}}(x) = \mathrm{G}_x = \{g \in \mathrm{G} \,|\, g \cdot x = x\}$$
de x est un sous-groupe de G.

   Soit maintenant $n \in \mathbb{N}$, $n \geq 2$. Notons G le groupe orthogonal $(\mathrm{O}(n, \mathbb{R}), \circ)$. Posons
$$\forall\, f \in \mathrm{G},\ \forall\, v \in \mathbb{R}^n \qquad f \cdot v = f(v).$$
   Désignons par $\mathcal{C} = (e_1, e_2, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$.

2. Montrer que
$$\mathrm{G} \times \mathbb{R}^n \to \mathbb{R}^n \qquad\qquad (f, v) \mapsto f \cdot v$$
définit une action du groupe G sur l'ensemble $\mathbb{R}^n$.

3. Déterminer l'orbite
$$\mathcal{O}_v^{\mathrm{G}} = \{f \cdot v \,|\, f \in \mathrm{G}\}$$
d'un élément v de $\mathbb{R}^n$ sous l'action de G.

4. Montrer que f appartient à G_{e_1} si et seulement si la matrice représentative de f dans $\mathcal{C}$ est du type
$$\begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$$
où P désigne un élément de $\mathrm{O}(n-1, \mathbb{R})$.

5. En déduire que $\mathrm{G}_{e_1} \simeq \mathrm{O}(n-1, \mathbb{R})$ en explicitant un isomorphisme entre $\mathrm{O}(n-1, \mathbb{R})$ et G_{e_1}.

6. Soit $x \in \mathbb{R}^n \setminus \{0\}$. Donner un isomorphisme de groupes $\phi_x \colon \mathrm{G}_x \xrightarrow{\sim} \mathrm{G}_{e_1}$.

7. Pour quels $x \in \mathbb{R}^n$ a-t-on $\mathrm{G}_x \lhd \mathrm{O}(n, \mathbb{R})$?

8. Soit $x \in \mathbb{R}^n \setminus \{0\}$. Nous restreignons l'action de G sur $\mathbb{R}^n$ à celle de G_x. Donner l'orbite
$$\mathcal{O}_v^{\mathrm{G}_x} = \{f \cdot v \,|\, f \in \mathrm{G}_x\}$$
d'un élément v de $\mathbb{R}^n$ sous cette action (peut-être s'aider d'un dessin).

Éléments de réponse 106

1. Montrons que pour tout x dans le E le stabilisateur
$$\mathrm{Stab}_{\mathrm{G}}(x) = \mathrm{G}_x = \{g \in \mathrm{G} \,|\, g \cdot x = x\}$$
de x est un sous-groupe de G.

Soit x dans E. Par définition d'une action $e \cdot x = x$ ce qui conduit à $e \in \mathrm{G}_x$.

Si g et g' appartiennent à G_x nous avons
$$(gg') \cdot x = g \cdot (g' \cdot x) = g \cdot x = x$$
donc gg' appartient à G_x.

Enfin si g appartient à G_x, alors $x = g \cdot x$ et en faisant agir g^{-1} de part et d'autre de l'égalité nous obtenons
$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$
ce qui montre que g^{-1} appartient à G_x.

En conclusion G_x est un sous-groupe de G.

Soit maintenant $n \in \mathbb{N}$, $n \geq 2$. Notons G le groupe orthogonal $(\mathrm{O}(n, \mathbb{R}), \circ)$. Posons
$$\forall\, f \in \mathrm{G},\ \forall\, v \in \mathbb{R}^n \qquad f \cdot v = f(v).$$
Désignons par $\mathcal{C}_n = (e_1, e_2, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$.

2. Montrons que
$$\mathrm{G} \times \mathbb{R}^n \to \mathbb{R}^n \qquad\qquad (f, v) \mapsto f \cdot v$$
définit une action du groupe G sur l'ensemble $\mathbb{R}^n$.

Soit v dans $\mathbb{R}^n$. Nous avons
$$\mathrm{id}_{\mathbb{R}^n} \cdot v = \mathrm{id}_{\mathbb{R}^n}(v) = v$$
et si f, g appartiennent à $\mathrm{O}(n, \mathbb{R})$
$$(f \circ g) \cdot v = (f \circ g)(v) = f(g(v)) = f \cdot g(v) = f \cdot (g \cdot v).$$

3. Déterminons l'orbite
$$\mathcal{O}_v^{\mathrm{G}} = \{f \cdot v \,|\, f \in \mathrm{G}\}$$
d'un élément v de $\mathbb{R}^n$ sous l'action de G.

Soit v dans $\mathbb{R}^n$.

Si $v = 0$, quel que soit $f \in \mathrm{O}(n, \mathbb{R})$ $f(v) = 0$ et

$$\mathcal{O}_0^{\mathrm{G}} = \{f \cdot 0 \,|\, f \in \mathrm{G}\} = \{0\}.$$

Si $v \neq 0$, alors du fait que les éléments $f \in \mathrm{O}(n, \mathbb{R})$ conservent la norme pour le produit scalaire standard de $\mathbb{R}^n$ nous avons $||f(v)|| = ||v||$ et donc $\mathcal{O}_v^{\mathrm{G}}$ est contenue dans la sphère $S(0, ||v||)$ de centre 0 et de rayon $||v||$. Réciproquement soit u dans $\mathbb{R}^n$ tel que $||v|| = ||u||$, soient $\mathcal{B}_u = \left(\frac{u}{||u||}, u_2, u_2, \ldots u_n\right)$ et $\mathcal{B}_v = \left(\frac{v}{||v||}, v_2, v_2, \ldots v_n\right)$ deux bases orthonormées de $\mathbb{R}^n$ (on peut compléter par le procédé de Gram-Schmidt un vecteur de norme 1 en une base orthonormée en dimension finie) et soit f l'application linéaire qui transforme $\mathcal{B}_v$ en $\mathcal{B}_u$. Puisque $\mathcal{B}_v$ et $\mathcal{B}_u$ sont deux bases orthonormées, f appartient à $\mathrm{O}(n, \mathbb{R})$. De plus $f\left(\frac{v}{||v||}\right) = \frac{u}{||u||}$ et $||u|| = ||v||$ entraînent $f(v) = u$. Finalement u appartient à $\mathcal{O}_v^{\mathrm{G}}$ et $\mathcal{O}_v^{\mathrm{G}} = S(0, ||v||)$ si $v \neq 0$.

4. Montrons que f appartient à G_{e_1} si et seulement si la matrice représentative de f dans $\mathcal{C}_n$ est du type

$$\begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$$

où P désigne un élément de $\mathrm{O}(n-1, \mathbb{R})$.

Si f appartient à G_{e_1}, alors $f(e_1) = e_1$ et donc la première colonne de la matrice M représentant f dans la base canonique est : $\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. D'autre part $f(e_1) = e_1$ étant orthogonal à $f(e_2), f(e_3), \ldots, f(e_n)$ puisque f préserve le produit scalaire la première ligne de M est $(1\ 0\ 0\ \ldots\ 0)$. Par suite $M = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$. Puisque ${}^{\mathrm{t}}MM = \mathrm{id}_n$ nécessairement ${}^{\mathrm{t}}PP = \mathrm{id}_{n-1}$; anisi P appartient à $\mathrm{O}(n-1, \mathbb{R})$.

Réciproquement si

$$M = mat(f, \mathcal{C}_n) = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$$

avec P dans $\mathrm{O}(n-1, \mathbb{R})$ nous avons bien : f appartient à $\mathrm{O}(n-1, \mathbb{R})$ (car ${}^{\mathrm{t}}MM = \begin{pmatrix} 1 & 0 \\ 0 & {}^{\mathrm{t}}PP \end{pmatrix} = \mathrm{id}_n$) et $f(e_1) = e_1$.

5. Montrons que $\mathrm{G}_{e_1} \simeq \mathrm{O}(n-1, \mathbb{R})$ en explicitant un isomorphisme entre $\mathrm{O}(n-1, \mathbb{R})$ et G_{e_1}.

D'après 4. l'application $\Psi \colon \mathrm{O}(n-1, \mathbb{R}) \to \mathrm{G}_{e_1}$ définie par $\Psi(g) = f$ où $mat(f, \mathcal{C}_n) = \begin{pmatrix} 1 & 0 \\ 0 & P \end{pmatrix}$ et $mat(g, \mathcal{C}_{n-1}) = P$ est bien à valeurs dans G_{e_1}. L'application Ψ est bien

un morphisme de groupes : à la composition des applications correspond le produit des matrices. De plus g appartient à $\ker\Psi$ si et seulement si $mat(g,\mathcal{C}_{n-1}) = \mathrm{id}_{n-1}$ si et seulement si $g = \mathrm{id}_{\mathbb{R}^{n-1}}$ ce qui prouve que Ψ est injective. La surjectivité de Ψ résulte directement de 4.

6. Soit $x \in \mathbb{R}^n \setminus \{0\}$. Donnons un isomorphisme de groupes $\phi_x \colon \mathrm{G}_x \xrightarrow{\sim} \mathrm{G}_{e_1}$.

   Soit x dans $\mathbb{R}^n \setminus \{0\}$. Soit h dans $\mathrm{O}(n-1,\mathbb{R})$ tel que $h(e_1) = \frac{x}{||x||}$ (une telle application existe d'après 3.*) Considérons*

   $$\phi_x \colon \mathrm{G}_x \to \mathrm{G}_{e_1} \qquad\qquad f \mapsto h \circ f \circ h^{-1}.$$

   Notons que $\phi_x(f)$ appartient à $\mathrm{O}(n-1,\mathbb{R})$ puisque f et h appartiennent à $\mathrm{O}(n-1,\mathbb{R})$. D'autre part

   $$\phi_x(f)(e_1) = h(f(h^{-1}(e_1))) = h\left(f\left(\frac{x}{||x||}\right)\right) = h\left(\frac{x}{||x||}\right) = e_1$$

   ainsi ϕ_x est bien à valeurs dans G_{e_1}. Le fait que ϕ_x est un isomorphisme de groupes se vérifie directement.

7. Déterminons les $x \in \mathbb{R}^n$ pour lesquels on a $\mathrm{G}_x \lhd \mathrm{O}(n,\mathbb{R})$.

   Soit x dans $\mathbb{R}^n$.

   Si $x = 0$, alors $\mathrm{G}_0 = \mathrm{O}(n,\mathbb{R})$ et $\mathrm{G}_0 \lhd \mathrm{O}(n,\mathbb{R})$.

   Supposons $x \neq 0$. Soit f dans $\mathrm{G}_x \setminus \{\mathrm{id}_{\mathbb{R}^n}\}$ (rappelons que d'après 3. *G_x n'est pas réduit à $\mathrm{id}_{\mathbb{R}^n}$). Il existe y dans $\mathbb{R}^n$ tel que $||y|| = ||x||$ et $f(y) \neq y$. D'après* 3. *on peut alors construire h dans $\mathrm{O}(n,\mathbb{R})$ tel que $h(y) = x$. Alors $h(f(h^{-1}(x))) \neq x$ (en effet $h^{-1}(x) = y$ donc $f(h^{-1}(x)) = f(y) \neq y$). Ainsi G_x n'est pas distingué dans $\mathrm{O}(n,\mathbb{R})$.*

   Finalement $\mathrm{G}_x \lhd \mathrm{O}(n,\mathbb{R})$ si et seulement si $x = 0$.

8. Soit $x \in \mathbb{R}^n \setminus \{0\}$. Nous restreignons l'action de G sur $\mathbb{R}^n$ à celle de G_x. Donnons l'orbite

   $$\mathcal{O}_v^{\mathrm{G}_x} = \{f \cdot v \mid f \in \mathrm{G}_x\}$$

   d'un élément v de $\mathbb{R}^n$ sous cette action.

   D'après 4. *un élément f de G_x s'identifie à une application orthogonale de $\mathrm{O}(n-1,\mathbb{R})$ qui agit sur $x^\perp$ (en identifiant $\mathbb{R}^{n-1}$ et $x^\perp$) en laissant fixe la direction x. Écrivons v dans une base orthonormée commençant par $\frac{x}{||x||}$; on voit que l'image par f de v appartient à $S(0,||v||)$ (car f conserve la norme) et aussi à l'hyperplan affine $\mathcal{H}$ de $\mathbb{R}^n$ orthogonal à x et passant par la projection orthogonale π de v sur la droite x (car f préserve la coordonnée suivant $\frac{x}{||x||}$). L'intersection de $S(0,||v||)$ et de $\mathcal{H}$ est la sphère $S_{\mathcal{H}}$ de $\mathcal{H}$ centrée en $\pi(v)$ et de rayon $dist(v,\mathrm{vect}(x))$. Réciproquement si u appartient à $S_{\mathcal{H}}$ la projection orthogonale $p(u)$ de u sur $x^\perp$ est de même norme que la projection orthogonale $p(v)$ de v sur $x^\perp$. Il existe donc une application orthogonale f de $\mathrm{O}(n-1,\mathbb{R})$ qui envoie $p(u)$ sur $p(v)$ (nous avons identifié $\mathbb{R}^{n-1}$ et $x^\perp$). Nous étendons alors f à $\widetilde{f}$ sur $\mathbb{R}^n$ tout entier en imposant que $\widetilde{f}$ laisse fixe la direction x. L'application $\widetilde{f}$ appartient à G_x et envoie u sur v. Il s'en suit que $\mathcal{O}_v^{\mathrm{G}_x} = S_{\mathcal{H}}$.*

Exercice 107 Soient G un p-groupe et H un sous-groupe non trivial distingué de G.
Montrer que $\mathrm{H} \cap Z(\mathrm{G})$ n'est pas réduit à l'élément neutre.

Éléments de réponse 107 Le sous-groupe H de G étant distingué G agit par conjugaison sur H. Puisque G est un p-groupe H l'est aussi et les orbites non triviales de cette action sont de cardinal divisible par p. On en déduit que la réunion des orbites triviales, c'est-à-dire l'ensemble $\mathrm{H} \cap Z(\mathrm{G})$ des points fixes, est aussi de cardinal divisible par p. Comme il contient l'élément neutre il contient au moins p éléments et n'est donc pas réduit à l'élément neutre.

Exercice 108

1. Soit G un groupe fini. Soit H un sous-groupe strict de G. Montrer qu'il existe $x \in \mathrm{G}$ tel que la classe de conjugaison de x ne rencontre pas H.
2. Donner un contre-exemple si G n'est pas fini.

Éléments de réponse 108

1. Soient x et g dans G. Nous avons $gxg^{-1} \in \mathrm{H} \iff x \in g^{-1}\mathrm{H}g$. On est donc ramené à montrer que la réunion $\bigcup_{g\in\mathrm{G}} g\mathrm{H}g^{-1}$ des conjugués de H n'est pas égale à G. Pour cela on va majorer le cardinal de $\bigcup_{g\in\mathrm{G}} g\mathrm{H}g^{-1}$ et montrer que cette réunion contient strictement moins d'éléments que G. Notons que si g_1 et g_2 sont dans la même classe à gauche modulo H, *i.e.* s'il existe $h \in \mathrm{H}$ tel que $g_2 = g_1 h$, alors
$$g_2\mathrm{H}g_2^{-1} = g_1(h\mathrm{H}h^{-1})g_1^{-1} = g_1\mathrm{H}g_1^{-1}.$$
Dans la réunion ci-dessus on peut donc prendre un système de représentants des classes à gauche modulo H. Soit g_1, g_2, …, g_k un tel système de représentants, $k = \frac{|\mathrm{G}|}{|\mathrm{H}|}$ étant l'indice de H dans G. Les conjugués de H ayant au moins l'élément neutre en commun il vient
$$\left|\bigcup_{g\in\mathrm{G}} g\mathrm{H}g^{-1}\right| = \left|\bigcup_{i=1}^{k} g_i\mathrm{H}g_i^{-1}\right| \leq 1 + (|\mathrm{H}|-1)k = |\mathrm{G}| + 1 - \frac{|\mathrm{G}|}{|\mathrm{H}|} < |\mathrm{G}|$$
car par hypothèse $|\mathrm{H}| < |\mathrm{G}|$ donc $1 < \frac{|\mathrm{G}|}{|\mathrm{H}|}$ et $1 - \frac{|\mathrm{G}|}{|\mathrm{H}|} < 0$.
2. Le résultat précédent ne s'étend pas à un groupe infini. Prenons par exemple $\mathrm{G} = \mathrm{GL}(n, \mathbb{C})$ et H le sous-groupe de G formé des matrices triangulaires supérieures inversibles. Toute matrice de G étant trigonalisable la classe de conjugaison de toute matrice de G rencontre H.

Exercice 109 Soit $\Bbbk = \mathbb{F}_q$ un corps fini de cardinal q. Considérons le groupe linéaire $\mathrm{GL}(n, \Bbbk)$ et son sous-groupe $\mathrm{SL}(n, \Bbbk)$.

a) Montrer que le centre de $\mathrm{GL}(n,\Bbbk)$ (resp. de $\mathrm{SL}(n,\Bbbk)$) est constitué des matrices scalaires de ce groupe.

b) Notons $\mathrm{PGL}(n,\Bbbk)$ (resp. $\mathrm{PSL}(n,\Bbbk)$) le quotient de $\mathrm{GL}(n,\Bbbk)$ (resp. $\mathrm{SL}(n,\Bbbk)$) par son centre. Calculer les ordres de $\mathrm{SL}(n,\Bbbk)$, $\mathrm{PGL}(n,\Bbbk)$ et $\mathrm{PSL}(n,\Bbbk)$.

Soit n un entier. Soit E le $\Bbbk$-espace vectoriel $\Bbbk^n$. Désignons par $\mathbb{P}(E)$ l'ensemble des droites vectorielles de $\Bbbk^n$ (espace projectif de dimension $n-1$).

c) Montrer qu'il existe un morphisme injectif Φ de $\mathrm{PGL}(n,\Bbbk)$ dans le groupe symétrique $\mathcal{S}_{\mathbb{P}(E)}$.

Dans la suite on suppose que $n=2$.

d) Montrer que $\mathbb{P}(E)$ est de cardinal $q+1$; on identifie Φ à un morphisme de $\mathrm{PGL}(2,\Bbbk)$ dans $\mathcal{S}_{q+1}$.

e) Supposons que $q=2$. Montrer que Φ induit des isomorphismes de $\mathrm{PGL}(2,\mathbb{F}_2)$ et $\mathrm{PSL}(2,\mathbb{F}_2)$ sur $\mathcal{S}_3$.

f) Supposons que $q=3$. Montrer que Φ induit un isomorphisme de $\mathrm{PGL}(2,\mathbb{F}_3)$ sur $\mathcal{S}_4$ et de $\mathrm{PSL}(2,\mathbb{F}_3)$ sur $\mathcal{A}_4$. Les groupes $\mathrm{PGL}(2,\mathbb{F}_3)$ et $\mathrm{SL}(2,\mathbb{F}_3)$ sont-ils isomorphes ?

g) Supposons que $q=4$. Montrer que Φ induit des isomorphismes de $\mathrm{PGL}(2,\mathbb{F}_4)$ et $\mathrm{PSL}(2,\mathbb{F}_4)$ sur $\mathcal{A}_5$.

h) Supposons que $q=5$. Montrer que Φ induit un isomorphisme de $\mathrm{PGL}(2,\mathbb{F}_5)$ sur $\mathcal{S}_5$ et de $\mathrm{PSL}(2,\mathbb{F}_5)$ sur $\mathcal{A}_5$ (rappelons une conséquence non trviale de la simplicité des groupes alternés : tout sous-groupe d'indice n de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$ pour $n\geq 5$).

Éléments de réponse 109

a) Montrons plus généralement (sur un corps $\Bbbk$ quelconque) que si un endomorphisme f de $\Bbbk^n$ commute avec tous les endomorphismes de déterminant 1, alors f est une homothétie. Pour cela montrons que tout vecteur $v\neq 0$ de $\Bbbk^n$ est vecteur propre pour f. Complétons v en une base $(v,e_1,e_2,\ldots,e_{n-1})$ de $\Bbbk^n$. Soit M la matrice de f dans cette base. Alors M commute avec la matrice de Jordan J_n donc laisse stable le noyau de J_n qui est $\Bbbk\cdot v$. Ainsi v est bien vecteur propre pour f.

b) Nous avons

$$|\mathrm{GL}(n,\Bbbk)| = (q^n-1)(q^n-q)\ldots(q^n-q^{n-1}).$$

Par définition $\mathrm{SL}(n,\Bbbk)$ est le noyau du morphisme de groupes surjectif

$$\det\colon \mathrm{GL}(n,\Bbbk)\to\Bbbk^*;$$

son cardinal est celui de $\mathrm{GL}(n,\Bbbk)$ divisé par $q-1$, soit

$$|\mathrm{SL}(n,\Bbbk)| = (q^n-1)(q^n-q)\ldots(q^n-q^{n-2})q^{n-1}.$$

De plus $\mathrm{PGL}(n,\Bbbk)$ est le quotient de $\mathrm{GL}(n,\Bbbk)$ par un groupe isomorphe à $\Bbbk^*$ (les matrices scalaires non nulles) donc $|\mathrm{PGL}(n,\Bbbk)| = |\mathrm{SL}(n,\Bbbk)|$.

Pour finir $|\mathrm{PSL}(n,\Bbbk)| = \frac{|\mathrm{SL}(n,\Bbbk)|}{|Z(\mathrm{SL}(n,\Bbbk))|}$ et $Z(\mathrm{SL}(n,\Bbbk)) = \{\lambda \mathrm{Id} \mid \lambda^n = 1\}$. Or il y a $\mathrm{pgcd}(n, q-1)$ racines $n$ièmes de l'unité dans un corps $\Bbbk$ de cardinal q [4] donc

$$|\mathrm{PSL}(n,\Bbbk)| = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1}}{\mathrm{pgcd}(n,q-1)}.$$

c) Faisons opérer $\mathrm{PGL}(n,\Bbbk)$ sur l'ensemble $\mathbb{P}(E)$ des droites vectorielles de E par $\overline{g}\cdot D = g(D)$ où g appartient à $\mathrm{GL}(n,\Bbbk)$ et $\overline{g}$ est son image dans $\mathrm{PGL}(n,\Bbbk)$. Ceci est bien défini car si $\overline{g_1} = \overline{g_2}$, alors g_1 et g_2 sont proportionnels et $g_1(D) = g_2(D)$. L'opération est fidèle car les seuls éléments g de $\mathrm{GL}(n,\Bbbk)$ qui stabilisent toutes les droites sont les homothéties. Nous obtenons donc un morphisme injectif Φ de $\mathrm{PGL}(n,\Bbbk)$ dans $\mathcal{S}_{\mathbb{P}(E)}$.

d) Les droites vectorielles de E sont données par une équation $y = ax$ dans le plan, avec $a \neq 0$, ou par l'équation $x = 0$. Il y a donc $q+1$ droites, *i.e.* $|\mathbb{P}(E)| = q+1$.

e) D'après c) les groupes $\mathrm{PGL}(2,\mathbb{F}_2)$ et $\mathrm{PSL}(2,\mathbb{F}_2)$ coïncident et sont d'ordre 6. De plus $\mathcal{S}_3$ est d'ordre 6. Ainsi le morphisme injectif Φ est aussi surjectif d'où le résultat.

f) D'une part $|\mathrm{PGL}(2,\mathbb{F}_3)| = (3^2-1)\times 3 = 24$ d'autre part $|\mathcal{S}_4| = 24$. Ainsi Φ réalise un isomorphisme entre entre $\mathrm{PGL}(2,\mathbb{F}_3)$ et $\mathcal{S}_4$. Comme $\mathrm{pgcd}(2,3-1) = 2$ le groupe $\mathrm{PSL}(2,\mathbb{F}_3)$ est, d'après c), un sous-groupe d'indice 2 de $\mathrm{PGL}(2,\mathbb{F}_3)$. Puisque le seul sous-groupe d'indice 2 de $\mathcal{S}_4$ est $\mathcal{A}_4$ [5] nous obtenons que Φ induit un isomorphisme entre $\mathrm{PSL}(2,\mathbb{F}_3)$ et $\mathcal{A}_4$.

Les groupes $\mathrm{PGL}(2,\mathbb{F}_3)$ et $\mathrm{SL}(2,\mathbb{F}_3)$ ne sont pas isomorphes. En effet $Z(\mathrm{SL}(2,\mathbb{F}_3))$ est d'ordre 2 alors que le centre de $\mathrm{PGL}(2,\mathbb{F}_3) \simeq \mathcal{S}_4$ est trivial.

g) D'une part $|\mathrm{PGL}(2,\mathbb{F}_4)| = (4^2-1)\times 4 = 60$, d'autre part comme $\mathrm{pgcd}(2,4-1) = 1$ nous avons $\mathrm{PGL}(2,\mathbb{F}_4) = \mathrm{PSL}(2,\mathbb{F}_4)$. Par suite Φ induit un des isomorphismes de $\mathrm{PGL}(2,\mathbb{F}_4)$ et $\mathrm{PSL}(2,\mathbb{F}_4)$ sur un sous-groupe d'indice 2 de $\mathcal{S}_5$ qui ne peut être que $\mathcal{A}_5$ [6].

h) L'ordre de $\mathrm{PGL}(2,\mathbb{F}_5)$ est $(5^2-1)\times 5 = 120$ donc Φ induit un isomorphisme de $\mathrm{PGL}(2,\mathbb{F}_5)$ sur un sous-groupe d'indice 6 de $\mathcal{S}_6$ lequel est isomorphe à $\mathcal{S}_5$ d'après le résultat rappelé. Étant donné que $\mathrm{pgcd}(2,5-1) = 2$, le groupe $\mathrm{PSL}(2,\mathbb{F}_5)$ est un sous-groupe d'indice 2 de $\mathrm{PGL}(2,\mathbb{F}_5) \simeq \mathcal{S}_5$ et est donc isomorphe, via Φ, à $\mathcal{A}_5$.

Exercice 110 Donner des applications de l'équation aux classes.

Éléments de réponse 110 Applications de l'équation aux classes : le centre d'un p-groupe n'est pas trivial, théorème de Wedderburn.

Exercice 111 Donner des applications de la formule de Burnside.

---

4. En effet $\Bbbk^*$ est un groupe cyclique d'ordre $q-1$. Nous sommes donc ramenés à compter le nombre de solutions x de $nx = 0$ dans $\mathbb{Z}/(q-1)\mathbb{Z}$ ce qui donne le résultat.

5. En effet, dès que $m \geq 2$ le seul morphisme non trivial de $\mathcal{S}_m$ dans le groupe multiplicatif $\{\pm 1\}$ est la signature.

6. En effet, dès que $m \geq 2$ le seul morphisme non trivial de $\mathcal{S}_m$ dans le groupe multiplicatif $\{\pm 1\}$ est la signature.

Éléments de réponse 111 Applications de la formule de Burnside : petit théorème de Fermat, les colliers de Polya.

Exercice 112 Trouver un groupe fini $\mathrm{G} \neq \{e\}$ tel que le centre de G est $\{e\}$, le sous-groupe dérivé de G est G mais G n'est pas simple.

Éléments de réponse 112 Considérons $\mathrm{G} = \mathrm{G}_1 \times \mathrm{G}_2$ où G_1 et G_2 sont deux groupes simples non abéliens, par exemple $\mathrm{G}_1 = \mathrm{G}_2 = \mathcal{A}_5$. Le groupe G n'est pas simple : il contient par exemple le sous-groupe distingué non trivial $\mathrm{G}_1 \times \{e\}$. De plus d'une part $Z(\mathrm{G}) = Z(\mathrm{G}_1) \times Z(\mathrm{G}_2)$, d'autre part $Z(\mathrm{G}_1) = Z(\mathrm{G}_2) = \{e\}$. Et enfin d'une part $[\mathrm{G}, \mathrm{G}] = [\mathrm{G}_1, \mathrm{G}_1] \times [\mathrm{G}_2, \mathrm{G}_2]$ et d'autre part $[\mathrm{G}_i, \mathrm{G}_i] = \mathrm{G}_i$ pour $i = 1, 2$.

Exercice 113 Soit D le groupe diédral d'ordre 8 (groupe des isométries du carré). Calculer le centre, le sous-groupe dérivé et l'abélianisé de D.

Soit $\mathbb{H}_8$ le groupe des quaternions d'ordre 8. Calculer le centre, le sous-groupe dérivé et l'abélianisé de $\mathbb{H}_8$.

Éléments de réponse 113 Le centre $Z(\mathrm{D})$ de D est $\{\pm \mathrm{id}\}$. Puisque le quotient $\mathrm{D}/Z(\mathrm{D})$ est abélien (il est d'ordre 4) son sous-groupe dérivé est inclus dans $Z(\mathrm{D})$. Étant donné que D n'est pas abélien, le groupe dérivé de $\mathrm{D}/Z(\mathrm{D})$ ne peut pas être trivial et coïncide donc avec $Z(\mathrm{D})$. On peut vérifier que tout élément g de D satisfait $g^2 \in Z(\mathrm{D})$. Ainsi tous les éléments non triviaux de $\mathrm{D}/Z(\mathrm{D})$ sont d'ordre 2. Par suite ce groupe d'ordre 4 n'est pas cyclique ; il est donc isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$.

Les règles de calcul dans $\mathbb{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ sont

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

Le centre $Z(\mathbb{H}_8)$ est donc réduit à $\{\pm 1\}$. Comme pour D nous en déduisons que le groupe dérivé de $\mathbb{H}_8$ est $Z(\mathbb{H}_8)$ et que l'abélianisé $\mathbb{H}_8/Z(\mathbb{H}_8)$ de $\mathbb{H}_8$ est isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$.

Notons que D et $\mathbb{H}_8$ ne sont pas isomorphes pour autant : D possède 5 éléments d'ordre 2 alors que $\mathbb{H}_8$ n'en possède qu'un.

Exercice 114 Soit G un groupe fini tel que le quotient de G par son centre soit abélien. Le groupe G est-il toujours abélien ?

Éléments de réponse 114 Non. Considérons par exemple un groupe non abélien G d'ordre 8 comme le groupe diédral. Son centre $Z(\mathrm{G})$ est non trivial car G est un 2-groupe. Par conséquent le quotient $\mathrm{G}/Z(\mathrm{G})$ est d'ordre au plus 4 et $\mathrm{G}/Z(\mathrm{G})$ est abélien.

Exercice 115 Quels sont les groupes finis G tels que tout élément g de G vérifie $g^2 = e$?

Éléments de réponse 115 Un tel groupe G est abélien ; en effet si g et h sont deux éléments de G alors $g = g^{-1}$ et $h = h^{-1}$ mais aussi $(gh) = (gh)^{-1}$ soit $gh = h^{-1}g^{-1}$ ou encore $gh = hg$. Notons alors G additivement. Nous avons alors $2g = 0$ pour tout $g \in \mathrm{G}$. Le groupe G est alors isomorphe au groupe additif $\left(\mathbb{Z}/2\mathbb{Z}\right)^r$ pour un certain $r \in \mathbb{N}$. Réciproquement un tel groupe convient.

Exercice 116 Soit p un nombre premier, soit G un groupe d'ordre p^2. Montrer que G est abélien.

Éléments de réponse 116 L'équation aux classes pour l'action de G sur lui-même par conjugaison assure que le centre $Z(\mathrm{G})$ de G n'est pas réduit à l'élément neutre. En faisons agir G sur lui-même par conjugaison

$$\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \qquad (g,h) \mapsto hgh^{-1}.$$

Notons que g appartient à $Z(\mathrm{G})$ si et seulement si l'orbite $\mathcal{O}_g$ de g sous cette action est réduite à $\{g\}$. L'équation aux classes assure que

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{r} |\mathcal{O}_{g_i}|.$$

D'après le théorème de Lagrange $|\mathcal{O}_{g_i}|$ divise p donc

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_{i=1}^{r} |\mathcal{O}_{g_i}|$$

conduit à

$$|\mathrm{G}| \equiv |Z(\mathrm{G})| \bmod p$$

soit

$$0 \equiv |Z(\mathrm{G})| \bmod p.$$

Mais e_G appartient à $Z(\mathrm{G})$ donc $|Z(\mathrm{G})| \geq p$. Par suite $Z(\mathrm{G})$ est de cardinal p ou p^2.

Si $|Z(\mathrm{G})| = p^2$, alors $\mathrm{G} = Z(\mathrm{G})$ est abélien.

Si $|Z(\mathrm{G})| = p$, alors $\mathrm{G}/Z(\mathrm{G})$ est de cardinal p premier, $\mathrm{G}/Z(\mathrm{G})$ est cyclique et G est, d'après a), abélien.

5.4. Groupe des permutations

Exercice 117 Le groupe $\mathcal{A}_4$ est-il simple ? le groupe $\mathcal{S}_4$ est-il simple ?

Éléments de réponse 117 Le groupe $\mathcal{A}_4$ n'est pas simple : le groupe

$$V_4 \simeq \{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

est un sous-groupe distingué non trivial et strict de $\mathcal{A}_4$.

Le groupe $\mathcal{S}_4$ n'est pas simple : le groupe $\mathcal{A}_4$ est un sous-groupe distingué non trivial et strict de $\mathcal{S}_4$.

Exercice 118 Décomposer la permutation $(1\ 2\ 3\ 4\ 5)(1\ 3\ 5)(3\ 2)$ en produit de cycles à support disjoint.

Éléments de réponse 118 On a $(1\ 2\ 3\ 4\ 5)(1\ 3\ 5)(3\ 2) = (2\ 1\ 4\ 5)$.

Exercice 119 Exprimer comme produit de cycles disjoints :

1. $(1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$;
2. $(1\ 2)(1\ 2\ 3)(1\ 2)$.

Quelle est la signature de ces permutations ?

Éléments de réponse 119

1. Posons $\sigma_1 = (1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$. Explicitons σ_1 :

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 5\ 2\ 3\ 4\ 1\ 6\ 7\ 8\ 9 \\ 5\ 2\ 3\ 4\ 6\ 7\ 8\ 9\ 1 \\ 4\ 2\ 3\ 5\ 6\ 7\ 8\ 9\ 1 \\ 4\ 3\ 1\ 5\ 6\ 7\ 8\ 9\ 2 \end{array}$$

   Donc $\sigma_1 = (4\ 3\ 1\ 5\ 6\ 7\ 8\ 9\ 2)$.

   C'est une permutation paire, de signature 1 ; en effet la signature d'un cycle d'ordre p est $(-1)^{p-1}$.

2. Posons $\sigma_2 = (1\ 2)(1\ 2\ 3)(1\ 2)$. Explicitons σ_2 :

$$\begin{array}{c} 1\ 2\ 3 \\ 2\ 1\ 3 \\ 3\ 2\ 1 \\ 3\ 1\ 2 \end{array}$$

   Ainsi $\sigma_2 = (3\ 1\ 2)$.

   C'est une permutation paire, de signature 1 ; en effet la signature d'un cycle d'ordre p est $(-1)^{p-1}$.

Exercice 120 Calculer aba^{-1} pour

1. $a = (1\ 3\ 5)(1\ 2)$, $b = (1\ 5\ 7\ 9)$;
2. $a = (5\ 7\ 9)$, $b = (1\ 2\ 3)$.

Éléments de réponse 120

1. Calcul de aba^{-1} pour $a = (1\ 3\ 5)(1\ 2)$, $b = (1\ 5\ 7\ 9)$.

   Explicitons a :

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 2\ 1\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 2\ 3\ 5\ 4\ 1\ 6\ 7\ 8\ 9 \end{array}$$

autrement dit $a = (1\ 2\ 3\ 5)$. Il s'en suit que

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 2 & 4 & 3 & 6 & 7 & 8 & 9 \end{matrix}$$

Finalement nous obtenons

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 2 & 4 & 3 & 6 & 7 & 8 & 9 \\ 7 & 5 & 2 & 4 & 3 & 6 & 9 & 8 & 1 \\ 7 & 1 & 3 & 4 & 5 & 6 & 9 & 8 & 2 \end{matrix}$$

2. Calcul de aba^{-1} pour $a = (5\ 7\ 9)$, $b = (1\ 2\ 3)$. Les cycles a et b sont à supports disjoints donc commutent. Ainsi $aba^{-1} = aa^{-1}b = b$, autrement dit $aba^{-1} = b$.

Exercice 121 Déterminer la parité des permutations suivantes et les écrire comme produits de transpositions :

$$\sigma_1 = (1\ 3\ 5)(5\ 4\ 3\ 2)(5\ 6\ 7\ 8), \qquad \sigma_2 = (1\ 2)(2\ 4)(1\ 7)(7\ 6\ 8).$$

Éléments de réponse 121 L'application signature est un morphisme de $\mathcal{S}_8$ dans le groupe multiplicatif $\{-1, 1\}$.

La permutation σ_1 est le produit d'un cycle pair avec deux cycles impairs, elle est donc paire.

La permutation σ_2 est le produit de 3 cycles impairs et d'un cycle pair, elle est donc impaire.

Autre méthode :

$$\sigma_1 = (3\ \ 5)(5\ \ 1)(2\ \ 3)(4\ \ 2)(2\ \ 5)(7\ \ 8)(6\ \ 8)(5\ \ 8)$$

donc $\operatorname{sgn}(\sigma_1) = (-1)^8 = 1$ et

$$\sigma_2 = (1\ \ 2)(2\ \ 4)(1\ \ 7)(6\ \ 8)(7\ \ 8)$$

donc $\operatorname{sgn}(\sigma_1) = (-1)^5 = -1$.

Exercice 122 Soit σ la permutation de $\{1, 2, \ldots, 12\}$ définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{pmatrix}$$

Calculer σ^{2000}.

Éléments de réponse 122 Posons $\sigma_1 = (1\ 10\ 5\ 7\ 2\ 9\ 12)$, $\sigma_2 = (3\ 8\ 6)$ et $\sigma_3 = (4\ 11)$.

Ces trois permutations sont à supports disjoints deux à deux donc commutent. Il en résulte que $\sigma^{2000} = \sigma_1^{2000}\sigma_2^{2000}\sigma_3^{2000}$.

Par ailleurs σ_1 est d'ordre 7 et $2000 = 285 \times 7 + 5$ d'où $\sigma_1^{2000} = \sigma_1^5$.
De plus σ_2 est d'ordre 3 et $2000 = 666 \times 3 + 2$ d'où $\sigma_2^{2000} = \sigma_2^2$.
Enfin σ_3 est d'ordre 2 et $2000 = 1000 \times 2$ d'où $\sigma_3^{2000} = \mathrm{id}$.
Par suite

$$\sigma^{2000} = \sigma_1^5\sigma_2^2 = (1\ \ 9\ \ 7\ \ 10\ \ 12\ \ 2\ \ 5)(3\ \ 8\ \ 6)$$

Exercice 123 Soit n un entier, soit σ une permutation de $\{1, 2, \ldots, n\}$ et soit $(x_1\ \ x_2\ \ \ldots\ \ x_k)$ un cycle de $\mathcal{S}_n$.
Calculer $\sigma(x_1\ \ x_2\ \ \ldots\ \ x_k)\sigma^{-1}$.

Éléments de réponse 123 Pour $1 \leq i \leq j$ posons $\sigma(x_i) = y_i$. Alors $\sigma^{-1}(y_i) = x_i$ et $\big((x_1\ \ x_2\ \ \ldots\ \ x_k)\sigma^{-1}\big)(y_i) = \big((x_1\ \ x_2\ \ \ldots\ \ x_k)\big)(x_i) = x_{i+1}$ donc $\sigma(x_1\ \ x_2\ \ \ldots\ \ x_k)\sigma^{-1}(y_i) = \sigma(x_{i+1}) = y_{i+1}$.
Par ailleurs si $y \notin \{y_1, y_2, \ldots, y_k\}$, alors $\big(\sigma(x_1\ \ x_2\ \ \ldots\ \ x_k)\sigma^{-1}\big)(y) = y$.
Il en résulte que

$$\sigma(x_1\ \ x_2\ \ \ldots\ \ x_k)\sigma^{-1} = (\sigma(x_1)\ \ \sigma(x_2)\ \ \ldots\ \ \sigma(x_k))$$

Exercice 124 Dans le groupe $\mathcal{S}_7$ calculer le produit

$$(4\ 5\ 6)(5\ 6\ 7)(6\ 7\ 1)(1\ 2\ 3)(2\ 3\ 4)(3\ 4\ 5).$$

Éléments de réponse 124 Nous avons

$$\begin{array}{c} 1\ 2\ 3\ 4\ 5\ 6\ 7 \\ 1\ 2\ 4\ 5\ 3\ 6\ 7 \\ 1\ 3\ 2\ 5\ 4\ 6\ 7 \\ 2\ 1\ 3\ 5\ 4\ 6\ 7 \\ 2\ 6\ 3\ 5\ 4\ 7\ 1 \\ 2\ 7\ 3\ 6\ 4\ 5\ 1 \\ 2\ 7\ 3\ 4\ 5\ 6\ 1 \end{array}$$

Exercice 125 Soit n un entier. Construire des homomorphismes injectifs de $\mathcal{S}_n$ dans $\mathcal{S}_{n+1}$.

Éléments de réponse 125 Soit x un élément de $\{1, 2, \ldots, n+1\}$. Posons $E_x = \{1, 2, \ldots, n+1\} \setminus \{x\}$. Il existe un isomorphisme φ entre $\mathcal{S}_n$ et $\mathcal{S}_{E_x}$. Le morphisme $f_x \colon \mathcal{S}_n \to \mathcal{S}_{n+1}$ défini par

$$\begin{cases} f_x(\sigma)(i) = \varphi(\sigma)(i) \text{ pour } i \in E_x \\ f_x(\sigma)(x) = x \end{cases}$$

est injectif.

Exercice 126 Montrer que si c et γ sont des n-cycles de $\mathcal{S}_n$ qui commutent entre eux, il existe un entier r tel que $\gamma = c^r$.

Éléments de réponse 126 Soient $c = (1 \ \ c(1) \ \ c^2(1) \ \ \ldots \ \ c^{n-1}(1))$ et $\gamma = (1 \ \ \gamma(1) \ \ \gamma^2(1) \ \ \ldots \ \ \gamma^{n-1}(1))$ deux n-cycles de $\mathcal{S}_n$ qui commutent entre eux, *i.e.* $c\gamma = \gamma c$.

L'ensemble $\{1, 2, \ldots, n\}$ coïncide avec $\{1, c(1), c^2(1), \ldots, c^{n-1}(1)\}$. Par conséquent il existe $0 \leq r \leq n-1$ tel que $\gamma(1) = c^r(1)$. De plus si $i \in \{1, \ldots, n\}$, alors il existe $0 \leq s \leq n-1$ tel que $i = c^s(1)$. Il en résulte que

$$\gamma(i) = \gamma(c^s(1)) = c^s(\gamma(1)) = c^s(c^r(1)) = c^r(c^s(1)) = c^s(i).$$

Par suite $\gamma = c^s$.

Autre méthode : faisons agir $\mathcal{S}_n$ sur l'ensemble des n-cycles par conjugaison (c'est possible car les n-cycles sont dans la même orbite pour cette action). Cet ensemble est de cardinal $(n-1)!$ En effet un n-cycle σ s'écrit $(1 \ \ \sigma(1) \ \ \sigma(2) \ \ \ldots \ \ \sigma(n-1))$ et nous avons $(n-1)$ choix pour $\sigma(1)$ puis $(n-2)$ choix pour $\sigma(2)$ etc. Le groupe $\mathcal{S}_n$ agit transitivement sur cet ensemble. L'indice du stabilisateur de c pour cette action est $(n-1)!$ et son cardinal est n. Ce stabilisateur est le centralisateur de c qui contient au moins les n puissances de c et tout n-cycle qui commute avec c est donc égal à une puissance de c.

Exercice 127 Soit $n \geq 3$ un entier. Sachant que le groupe $\mathcal{S}_n$ est engendré par l'ensemble des transpositions de $\{1, 2, \ldots, n\}$ montrer que $\mathcal{S}_n$ est engendré par les ensembles suivants de permutations :

1. $(1\ 2), \ldots, (1\ n)$;
2. $(1\ 2), (2\ 3), \ldots, (n-1\ n)$;
3. $(1\ 2), (2\ 3\ \ldots\ n)$.

Éléments de réponse 127

1. Notons que $(i\ j) = (i\ 1)(j\ 1)(i\ 1)$ lorsque $i \neq j$;
2. Soit $i < j$.

   Si $j > i+1$, alors

$$(i\ j) = (j-1\ j)(i\ j-1)(j-1\ j) \tag{5.4.1}$$

   Si $j - 1 = i + 1$, alors $(i\ j) \in \langle (1\ 2), (2\ 3), \ldots, (n-1\ n) \rangle$.

Sinon nous appliquons (5.8.1) en remplaçant $(i\ j)$ par $(i\ j-1)$ et nous arrivons de proche en proche au résultat.

3. Nous avons
$$(2\ 3\ \ldots\ n)(1\ 2)(2\ 3\ \ldots\ n)^{-1} = (1\ 3).$$
Par suite par récurrence pour $i > 2$ nous avons
$$(1\ i) = (2\ 3\ \ldots\ n)^{i-2}(1\ 2)(2\ 3\ \ldots\ n)^{-i+2}$$
d'où le résultat (en utilisant la première question).

Exercice 128 Soit G un sous-groupe de $\mathcal{S}_4$ opérant sur $\{1, 2, 3, 4\}$ par l'action induite par l'action naturelle de $\mathcal{S}_4$.

Pour $i = 1, 2, 3, 4$ on note $\mathcal{O}_i$ l'orbite de i et S_i le stabilisateur de i.

Déterminer $\mathcal{O}_i$ et S_i pour $i = 1, 2, 3, 4$ dans chacun des cas suivants :

1. $\mathrm{G} = \langle (1\ 2\ 3) \rangle$;
2. $\mathrm{G} = \langle (1\ 2\ 3\ 4) \rangle$;
3. $\mathrm{G} = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$;
4. $\mathrm{G} = \{e, (1\ 2), (1\ 2)(3\ 4), (3\ 4)\}$;
5. $\mathrm{G} = \mathcal{A}_4$.

Éléments de réponse 128

1. Supposons que $\mathrm{G} = \langle (1\ 2\ 3) \rangle$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3\}$ et $S_i = \mathrm{id}$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3\}$ et $S_i = \mathrm{id}$.
   Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3\}$ et $S_i = \mathrm{id}$.
   Si $i = 4$, alors $\mathcal{O}_i = \{4\}$ et $S_i = \mathrm{G}$.
2. Supposons que $\mathrm{G} = \langle (1\ 2\ 3\ 4) \rangle$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 4$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
3. Supposons que $\mathrm{G} = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.
   Si $i = 4$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \mathrm{id}$.

4. Supposons que $G = \{\mathrm{id}, (1\ 2), (1\ 2)(3\ 4), (3\ 4)\}$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2\}$ et $S_i = \{\mathrm{id}, (3\ 4)\}$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2\}$ et $S_i = \{\mathrm{id}, (3\ 4)\}$.
   Si $i = 3$, alors $\mathcal{O}_i = \{3, 4\}$ et $S_i = \{\mathrm{id}, (1\ 2)\}$.
   Si $i = 4$, alors $\mathcal{O}_i = \{3, 4\}$ et $S_i = \{\mathrm{id}, (1\ 2)\}$.
5. Supposons que $G = \mathcal{A}_4$.
   Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle(2\ 3\ 4)\rangle$.
   Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle(1\ 3\ 4)\rangle$.
   Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle(1\ 2\ 4)\rangle$.
   Si $i = 4$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle(1\ 2\ 3)\rangle$.

Exercice 129 Établir la table de $\mathcal{S}_3$ et de $\mathbb{Z}/6\mathbb{Z}$.
Quels sont les sous-groupes de $\mathcal{S}_3$?
Quels sont les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$?

Éléments de réponse 129 La table de $\mathcal{S}_3$ est

	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	id	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	id	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	id	(1 2 3)

La table de $\mathbb{Z}/6\mathbb{Z}$ est

	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[4]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Les sous-groupes de $\mathcal{S}_3$ sont :
- un sous-groupe d'ordre 1 ;
- trois sous-groupes d'ordre 2 : $\langle(1\ 2)\rangle$, $\langle(1\ 3)\rangle$, $\langle(2\ 3)\rangle$;
- un sous-groupe d'ordre 3 : $\langle(1\ 2\ 3)\rangle$.

Les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ sont :
- un sous-groupe d'ordre 1 ;

- un sous-groupes d'ordre 2 : $\langle [3] \rangle$;
- un sous-groupes d'ordre 3 : $\langle [2] \rangle$.

Exercice 130

a) Déterminer les classes de conjugaison dans $\mathcal{S}_n$.

b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Éléments de réponse 130

a) Soit $c = (a_1 \ \dots \ a_k)$ un k-cycle de $\mathcal{S}_n$. Pour tout $\sigma \in \mathcal{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1) \ \dots \ \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathcal{S}_n$ sont paramétrées par les partitions de l'entier n. Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que

$$m_1 \leq \ldots \leq m_r \qquad\qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.

b) Puisque $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ la classe de conjugaison dans $\mathcal{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathcal{S}_n$, la classe de conjugaison de σ dans $\mathcal{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathcal{S}_n$ on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$; les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1 \ \dots \ a_{2k+1}) \qquad\qquad c' = (a'_1 \ \dots \ a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1 \ a'_1) \ldots (a_{2k+1} \ a'_{2k+1})$$

nous avons pour tout $\tau \in \mathcal{S}_n$

$$\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$$

et les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ. On voit que $(i \ j)\sigma(i \ j)$ n'est pas conjuguée à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathcal{S}_n$.

Exercice 131 Considérons les deux éléments suivants du groupe symétrique $\mathcal{S}_9$

$$\sigma_1 = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9) \qquad \sigma_2 = (1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)$$

Justifier pourquoi σ_1 et σ_2 sont conjugués, puis exhiber une permutation $\omega \in \mathcal{S}_9$ telle que $\sigma_2 = \omega\sigma_1\omega^{-1}$.

Quel est le cardinal (une expression sous forme de produit d'entiers suffit) de la classe de conjugaison de σ_1 dans $\mathcal{S}_9$?

Éléments de réponse 131 Les décompositions canoniques des permutations σ_1 et σ_2 font intervenir des cycles de même longueur (2, 3 et 4), ces deux permutations sont donc conjuguées. En écrivant

$$\sigma_1 = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9) \qquad \sigma_2 = (8\ 9)(5\ 6\ 7)(1\ 2\ 3\ 4)$$

nous trouvons parmi de nombreux choix possibles $\omega = (1\ 8\ 3\ 5\ 7\ 2\ 9\ 4\ 6)$

Le cardinal de la classe de conjugaison s'obtient en calculant le nombre de permutations de $\mathcal{S}_9$ de type 2, 3, 4 :

- $(9 \cdot 8)/2 = 9 \cdot 4$ choix possibles pour la transposition ;
- $2 \cdot (7 \cdot 6 \cdot 5)/6 = 7 \cdot 5 \cdot 2$ choix possibles pour le 3-cycle ;
- 6 choix possibles pour le 4-cycle.

soit finalement $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$ choix possibles.

Exercice 132 Montrer que le groupe symétrique $\mathcal{S}_3$ est isomorphe à son groupe d'automorphisme $\mathrm{Aut}(\mathcal{S}_3)$.

Éléments de réponse 132 L'application qui à σ fait correspondre l'automorphisme intérieur $\sigma' \mapsto \sigma\sigma'\sigma^{-1}$ est un morphisme injectif de $\mathcal{S}_3$ dans $\mathrm{Aut}(\mathcal{S}_3)$, car le centre de $\mathcal{S}_3$ est trivial.

De plus un élément de $\mathrm{Aut}(\mathcal{S}_3)$ est déterminé par l'image des générateurs $(1\,2)$ et $(1\,3)$. Il y a donc au plus 6 choix possibles (choisir deux parmi les trois éléments d'ordre 2 de $\mathcal{S}_3$), donc en comparant les ordres nous obtenons que le morphisme ci-dessus est en fait un isomorphisme.

Exercice 133 Montrer que tout sous-groupe d'indice n dans $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$.

Éléments de réponse 133 Soit H un sous-groupe d'indice n dans $\mathcal{S}_n$.

Si $n \geq 3$, on vérifie l'énoncé directement.

Si $n = 4$, alors si $\mathrm{H} \not\simeq \mathcal{S}_3$, 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 $\mathcal{S}_4$ ne contient pas d'élément d'ordre 6.

Supposons $n \geq 5$. Le groupe $\mathcal{S}_n$, et donc aussi H, opère par translation à gauche sur $E = {}^{\mathcal{S}_n}\!/_{\mathrm{H}}$ d'où un homomorphisme

$$\varphi \colon \mathcal{S}_n \to \mathcal{S}_E \simeq \mathcal{S}_n.$$

Puisque $\ker\varphi = \bigcap_{a\in\mathcal{S}_n} a\mathrm{H}a^{-1}$, $\ker\varphi$ est distingué dans $\mathcal{S}_n$ et $\ker\varphi \subset \mathrm{H}$ on a $\ker\varphi = \{\mathrm{id}\}$ (rappel : pour $n \geq 5$ les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$). Pour des raisons de cardinalité ($|\mathcal{S}_n| = |\mathcal{S}_E \simeq \mathcal{S}_n|$), φ est un isomorphisme.

Comme H est le stabilisateur de la classe de idH on a : $\varphi(\mathrm{H}) \subset \mathcal{S}_n$ est le stabilisateur d'un point et c'est donc un sous-groupe isomorphe à $\mathcal{S}_{n-1}$.

Exercice 134

a) Déterminer les classes de conjugaison dans $\mathcal{S}_n$.

b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Éléments de réponse 134

a) Soit $c = (a_1\ \ldots\ a_k)$ un k-cycle de $\mathcal{S}_n$. Pour tout $\sigma \in \mathcal{S}_n$ on a

$$\sigma c\sigma^{-1} = (\sigma(a_1)\ \ldots\ \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathcal{S}_n$ sont paramétrées par les partitions de l'entier n. Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que

$$m_1 \leq \ldots \leq m_r \qquad\qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.

b) Puisque $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ la classe de conjugaison dans $\mathcal{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathcal{S}_n$, la classe de conjugaison de σ dans $\mathcal{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathcal{S}_n$ on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$; les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1\ \ldots\ a_{2k+1}) \qquad\qquad c' = (a'_1\ \ldots\ a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1\ a'_1)\ldots(a_{2k+1}\ a'_{2k+1})$$

nous avons pour tout $\tau \in \mathcal{S}_n$

$$\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$$

et les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ. On voit que $(i\ j)\sigma(i\ j)$ n'est pas conjuguée à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathcal{S}_n$.

Exercice 135 Soit n un entier. Rappelons que $\mathcal{A}_n$ est le sous-groupe de $\mathcal{S}_n$ formé par les permutations paires.

a) Montrer que le produit de deux transpositions distinctes de $\mathcal{S}_n$ est un 3-cycle ou un produit de deux 3-cycles. En déduire que $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles de $\mathcal{S}_n$.

b) i) Montrer que pour $n \geq 3$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles $(1\ 2\ 3)$, …, $(1\ 2\ n)$. En déduire que $\mathcal{A}_n$ est pour $n \geq 3$ stable par tout automorphisme ϕ de $\mathcal{S}_n$ (autrement dit $\mathcal{A}_n$ est un sous-groupe caractéristique de $\mathcal{S}_n$).

ii) Montrer que $\mathcal{A}_n$ est engendré
— si n est impair ≥ 5 par $(1\ 2\ 3)$ et $(3\ 4\ \ldots\ n)$;
— si n est pair ≥ 4 par $(1\ 2\ 3)$ et $(1\ 2)(3\ 4\ \ldots\ n)$.

c) Montrer que pour $n \geq 5$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des permutations de $\mathcal{S}_n$ de la forme $(a\ b)(c\ d)$ avec a, b, c, d deux à deux distincts.

Éléments de réponse 135

a) Soient $i < j < k < l$. Nous avons

$$(i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l)$$

Or $(i\ j)(j\ k) = (i\ j\ k)$ donc

$$(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l).$$

Tout élément σ de $\mathcal{A}_n$ est le produit d'un nombre pair de transpositions donc un produit de 3-cycles. Le sous-groupe de $\mathcal{A}_n$ engendré par les 3-cycles contient donc $\mathcal{A}_n$, c'est donc $\mathcal{A}_n$.

b) i) Soient i, j et k des éléments de $\{1, \ldots, n\}$ tels que $i < j < k$. Nous avons

$$(i\ j\ k) = (1\ 2\ i)(2\ j\ k)(1\ 2\ i)^{-1}$$

et

$$(2\ j\ k) = (1\ 2\ j)(1\ 2\ k)(1\ 2\ j)^{-1}$$

donc $\mathcal{A}_n \subset \langle (1\ 2\ 3), \ldots, (1\ 2\ n)\rangle$. Il en résulte que

$$\mathcal{A}_n = \langle (1\ 2\ 3), \ldots, (1\ 2\ n)\rangle.$$

Soient ϕ un automorphisme de $\mathcal{S}_n$ et σ un 3-cycle. L'ordre de $\phi(\sigma)$ est 3. Donc $\phi(\sigma)$ est un produit de 3-cycles car son ordre est le ppcm des longueurs des cycles qui interviennent dans sa décomposition en cycles. Le groupe $\mathcal{A}_n$ est donc caractéristique dans $\mathcal{S}_n$.

ii) Pour $i \geq 4$ et $n \geq 4$ nous avons

$$(1\ 2\ i) = (3\ 4\ \ldots\ n)^{i-3}(1\ 2\ 3)(3\ 4\ \ldots\ n)^{-3+i}.$$

Par ailleurs si $n \geq 5$ est impair, $(3\ 4\ \ldots\ n)$ est une permutation paire car c'est un cycle de longueur impaire $n-2$. Ainsi pour $n \geq 5$ impair on a

$$\mathcal{A}_n = \langle (1\ 2\ 3),\ (3\ 4\ \ldots\ n) \rangle$$

Nous avons

$$(1\ 2)^{\alpha}(1\ 2\ i)(1\ 2)^{\alpha} = \begin{cases} (1\ 2\ i) \text{ pour } \alpha \text{ pair} \\ (1\ 2\ i)^{-1} \text{ pour } \alpha \text{ impair} \end{cases}$$

Donc puisque pour $i \geq 4$ et $n \geq 4$

$$(1\ 2\ i) = (3\ 4\ \ldots\ n)^{i-3}(1\ 2\ 3)(3\ 4\ \ldots\ n)^{-3+i}.$$

alors pour $i \geq 4$ impair et $n \geq 4$

$$(1\ 2\ i) = [(1\ 2)(3\ 4\ \ldots\ n)]^{i-3}(1\ 2\ 3)[(1\ 2)(3\ 4\ \ldots\ n)]^{-3+i}.$$

Et pour $i \geq 4$ pair et $n \geq 4$

$$(1\ 2\ i) = \big[\big((1\ 2)(3\ 4\ \ldots\ n)\big)^{i-3}(1\ 2\ 3)\big((1\ 2)(3\ 4\ \ldots\ n)\big)^{-3+i}\big]^{-1}.$$

Or si $n \geq 4$ est pair $(1\ 2)(3\ 4\ \ldots\ n)$ est une pemutation paire. Par conséquent le groupe $\mathcal{A}_n$ est engendré par $(1\ 2\ 3)$ et $(1\ 2)(3\ 4\ \ldots\ n)$.

c) Il suffit de montrer que tout 3-cycle $(i\ j\ k)$ (avec $i < j < k$) est produit de permutations de la forme $(a\ b)(c\ d)$ où a, b, c et d sont deux à deux distincts. Puisque $n \geq 5$ il existe ℓ et m dans $\{1, 2, \ldots, n\}$ tels que i, j, k, ℓ et m soient 2 à 2 distincts. Or nous avons

$$(i\ j\ k) = (m\ \ell)(j\ k)(m\ \ell)(i\ k)$$

d'où le résultat.

Exercice 136 Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un morphisme injectif de $\mathcal{S}_n$ dans $\mathcal{A}_{n+2}$.

Éléments de réponse 136 Considérons l'application $\psi\colon \mathcal{S}_n \to \mathcal{A}_{n+2}$ définie par

$$\begin{cases} \psi(\sigma) = \sigma \text{ si } \sigma \text{ est une permutation paire} \\ \psi(\sigma) = \sigma \circ (n+1\ \ n+2) \text{ si } \sigma \text{ est une permutation impaire} \end{cases}$$

L'application ψ est injective par unicité de la décomposition en cycles à supports disjoints.

On peut vérifier que ψ est un morphisme de groupes.

Exercice 137 Construire un morphisme surjectif de $\mathcal{S}_4$ sur $\mathcal{S}_3$.

Éléments de réponse 137 Faire agir $\mathcal{S}_4$ par conjugaison sur les éléments d'ordre 2 de $\mathcal{S}_4$ qui ne sont pas des transpositions.

5.5. Autour des théorèmes de Sylow

Exercice 138 Donner un p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$.

Éléments de réponse 138 Le sous-groupe des matrices triangulaires supérieures strictes de $\mathrm{GL}(n, \mathbb{F}_p)$ est un p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$.

Exercice 139 Montrer qu'il n'existe pas de groupe simple d'ordre 30.

Éléments de réponse 139 Supposons qu'il existe un groupe simple d'ordre 30. Considérons les p-Sylow de G. Désignons par n_p le nombre de p-Sylow de G.

Rappelons que $30 = 2 \times 3 \times 5$.

Les théorèmes de Sylow assurent que

$$n_2 \in \{3, 5, 15\}, \qquad n_3 = 10, \qquad n_5 = 6.$$

On en déduit que le groupe G contient 24 éléments d'ordre 5 (les intersections des 5-Sylow sont restreintes à l'élément neutre) et au moins 20 éléments d'ordre 3. En particulier d'une part $|\mathrm{G}| = 30$, d'autre part $|\mathrm{G}| \geq 44$.

Exercice 140 Montrer qu'un groupe d'ordre 200 n'est pas simple.

Éléments de réponse 140 Soit G un groupe d'ordre 200. Notons que $200 = 2^3 \times 5^2$. D'après les Théorèmes de Sylow le nombre de 5-Sylow de G est congru à 1 modulo 5 et divise $2^3 = 8$ donc vaut 1. L'unique 5-Sylow de G est donc nécessairement distingué dans G ; en particulier G n'est pas simple.

Exercice 141 Soit G un groupe d'ordre 15.

1. Combien G possède-t-il d'éléments d'ordre 3 ?
2. Combien G possède-t-il d'éléments d'ordre 5 ?
3. Démontrer que G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Éléments de réponse 141

1. Soit n_3 le nombre de 3-Sylow de G. D'après les théorèmes de Sylow, $n_3 \equiv 1 \bmod 3$ et $n_3|5$, *i.e.* $n_3 = 1$. Soit H l'unique 3-Sylow de G. Tout élément d'ordre 3 engendre un sous-groupe d'ordre 3. Il y a donc exactement deux éléments d'ordre 3 : si $\mathrm{H} = \{\mathrm{id}, g, h\}$, alors ces éléments sont g et h.
2. De la même façon, on montre que G possède quatre éléments d'ordre 5. Soit n_5 le nombre de 3-Sylow de G. Les théorèmes de Sylow assurent que $n_5 \equiv 1 \bmod 5$ et $n_5|3$ soit que $n_5 = 1$. Mais tout élément d'ordre 5 engendre un sous-groupe d'ordre 5. Il y a donc exactement quatre éléments d'ordre 5.

3. L'ordre d'un élément de G est un diviseur de 15, donc est égal à 1, 3, 5 ou 15. Comme il y a un élément d'ordre 1, deux éléments d'ordre 3 et quatre éléments d'ordre 5, il y a huit éléments d'ordre 15. Ainsi G possède un élément d'ordre son cardinal ; G est donc le groupe cyclique engendré par cet élément, *i.e.* G est isomorphe à $\mathbb{Z}/15\mathbb{Z}$.

Exercice 142 Soient p un nombre premier et n un entier naturel avec $p > n$. Considérons un groupe G d'ordre pn et H un sous-groupe de G d'ordre p. Montrer que H est un sous-groupe distingué de G.

Indication : compter les p-SYLOW de G.

Éléments de réponse 142 D'après les hypothèses, $\text{pgcd}(p, n) = 1$, donc H est un p-SYLOW de G. Notons n_p le nombre de p-SYLOW de G. Alors par les théorèmes de SYLOW, $n_p \equiv 1 \bmod p$ et $n_p | n$. Si $n_p \neq 1$, alors $n_p \geq p + 1$, ce qui contredit que n_p divise n puisque $n < p$. Ainsi, $n_p = 1$ et H est l'unique p-SYLOW de G donc est distingué dans G.

Exercice 143 Déterminer à isomorphisme près tous les groupes d'ordre 33.

Éléments de réponse 143 Soit G un groupe d'ordre 33.

Les éléments de G sont d'ordre 1, 3, 11 ou 33. Une application directe des théorèmes de SYLOW montre que G contient un unique 3-SYLOW et un unique 11-SYLOW. En effet soit n_p le nombre de p-SYLOW de G ; d'une part $n_3 \equiv 1 \bmod 3$ et $n_3 | 11$, d'autre part $n_{11} \equiv 1 \bmod 11$ et $n_{11} | 3$, *i.e.* $n_{11} = 1$. Les éléments d'ordre 3 et 11 sont contenus dans ces deux groupes. On a au plus $1 + (3 - 1) + (11 - 1) = 1 + 2 + 10 = 13$ éléments d'ordre 1, 3 ou 11. Il existe donc un élément d'ordre 33 dans G qui est donc cyclique isomorphe à $\mathbb{Z}/33\mathbb{Z}$.

Exercice 144

1. Quels sont les sous-groupes de SYLOW de $\mathcal{A}_4$?
2. Déterminer l'ordre de tous les éléments de $\mathcal{A}_4$.

   Le groupe $\mathcal{A}_4$ possède-t-il un sous-groupe cyclique d'ordre 6 ?
3. Soit H un sous-groupe de $\mathcal{A}_4$ engendré par un élément d'ordre 2 et un élément d'ordre 3.

   Montrer que H contient au moins trois éléments d'ordre 3.

   Peut-il être isomorphe à $\mathcal{S}_3$?

   En déduire qu'il n'y a pas de sous-groupe d'ordre 6 dans $\mathcal{A}_4$.
4. Donner la liste des sous-groupes de $\mathcal{A}_4$.

Éléments de réponse 144

1. Déterminons les les sous-groupes de Sylow de $\mathcal{A}_4$.

   L'ordre de $\mathcal{A}_4$ est $12 = 2^2 \times 3$. Soient n_2 le nombre de sous-groupes de Sylow d'ordre $2^2 = 4$ et n_3 le nombre de sous-groupes de Sylow d'ordre 3. Les théorèmes de Sylow assurent que

   $$n_2 \equiv 1 \bmod 2 \qquad n_2 | 3$$

   $$n_3 \equiv 1 \bmod 3 \qquad n_3 | 2^2 = 4$$

   autrement dit que $n_2 \in \{1, 3\}$ et $n_3 \in \{1, 4\}$.

   Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois donc $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4 isomorphe au groupe de Klein, *i.e.* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (en effet d'après le théorème de Lagrange un sous-groupe K de $\mathcal{A}_4$ d'ordre 4 contient des éléments d'ordre 1, 2 ou 4 ; mais $\mathcal{A}_4$ ne contient pas d'élément d'ordre 2 donc K contient des éléments d'ordre 1 ou 4. Comme $\mathcal{A}_4$ contient un seul élément d'ordre 1 et trois éléments d'ordre 4 il contient un seul sous-groupe d'ordre 4).

   Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.

2. Déterminons l'ordre de tous les éléments de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ possède-t-il un sous-groupe cyclique d'ordre 6 ?

   Le groupe $\mathcal{A}_4$ contient trois éléments d'ordre 2, huit éléments d'ordre 3 et un élément d'ordre 1. Le groupe $\mathcal{A}_4$ ne contient donc aucun élément d'ordre 6 et ne contient donc pas de sous-groupe cyclique d'ordre 6.

3. Soit H un sous-groupe de $\mathcal{A}_4$ engendré par un élément d'ordre 2 et un élément d'ordre 3.

   Notons que

   $$(a\ b)(c\ d)(a\ b\ c) = (b\ d\ c)$$

   Le groupe H contient les 3-cycles : $(a\ b\ c)$, $(a\ c\ b)$ et $(b\ d\ c)$ donc les trois sous-groupes d'ordre 3

   $$\langle (a\ b\ c) \rangle, \qquad \langle (a\ c\ b) \rangle, \qquad \langle (b\ d\ c) \rangle.$$

   Un groupe d'ordre 6 ne contient qu'un sous-groupe d'ordre 3 (en effet soit K un sous-groupe d'ordre $6 = 2 \times 3$. Désignons par n_3' le nombre de 3-Sylow de K ; d'une part $n_3' \equiv 1 \bmod 3$ d'autre part $n_3' | 2$ donc $n_3' = 1$). Par conséquent le groupe H n'est pas d'ordre 6. En particulier H ne peut pas être isomorphe à $\mathcal{S}_3$ qui est d'ordre 6.

4. Le groupe $\mathcal{A}_4$ contient :
   — un sous-groupe d'ordre 1 : $\{\mathrm{id}\}$;
   — trois sous-groupes d'ordre 2 :

   $$\langle (1\ 2)(3\ 4) \rangle \qquad \langle (1\ 3)(2\ 4) \rangle \qquad \langle (1\ 4)(2\ 3) \rangle ;$$

— quatre sous-groupes d'ordre 3 :

$$\langle(1\ 2\ 3)\rangle \qquad \langle(1\ 2\ 4)\rangle \qquad \langle(1\ 3\ 4)\rangle \qquad \langle(2\ 3\ 4)\rangle;$$

— un sous-groupe d'ordre 4 :

$$\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

Exercice 145 [Simplicité de $\mathcal{A}_n$, $n \geq 5$]

I) Commençons par démontrer que le groupe $\mathcal{A}_5$ est simple.

Soit G un groupe. Un sous-groupe H de G est caractéristique si pour tout automorphisme φ de G on $\varphi(\mathrm{H}) \subset \mathrm{H}$.

I) a) Montrer que tout p-Sylow distingué d'un groupe d'ordre fini est caractéristique.

I) b) Montrer que tout groupe d'ordre 15 est cyclique.

I) c) Montrer que tout groupe d'ordre 30 contient un sous-groupe distingué d'ordre 15.

I) d) Montrer que tout groupe d'ordre 30 ne contient qu'un seul 5-Sylow (d'ordre 5).

I) e) Montrer que tout groupe d'ordre 20 contient un seul sous-groupe d'ordre 5.

I) f) Montrer que tout groupe d'ordre 12 contient un sous-groupe caractéristique.

I) g) Montrer que tout groupe d'ordre 6 contient un sous-groupe caractéristique.

I) h) Montrer que tout groupe d'ordre 60 qui contient strictement plus d'un 5-Sylow est simple.

I) i) Montrer que le groupe $\mathcal{A}_5$ est simple.

II) Soit $n \geq 6$. Supposons que $\mathcal{A}_{n-1}$ soit simple. Soit H un sous-groupe distingué de $\mathcal{A}_n$ non trivial.

II) a) Montrer qu'il existe $\tau \in \mathrm{H}$ distinct de l'identité qui a au moins un point fixe.

II) b) Montrer que pour tout $1 \leq j \leq n$ le sous-groupe $\mathrm{G}_j = \mathrm{Stab}_{\mathcal{A}_n}(\{j\})$ est inclus dans H.

II) c) Supposons que $\mathrm{H} \neq \{\mathrm{id}\}$. Montrer que $\mathcal{A}_n = \mathrm{H}$.

II) d) En déduire que $\mathcal{A}_n$ est simple pour $n \geq 5$.

Éléments de réponse 145

I) a) Soit G un groupe d'ordre fini. Soit H un p-Sylow de G qui est distingué dans G. 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 dans G. Par conséquent $\varphi(\mathrm{H}) = \mathrm{H}$.

I) b) 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 $H \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$ et est donc cyclique.

I) c) 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

$$n_5 \equiv 1 \pmod 5 \qquad\qquad n_5 \mid 6$$

on a $n_5 = 6$. Ainsi on a 6×4 éléments d'ordre 5, ce qui en ajoutant id 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, $K \cap H = \{id\}$ 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) $K \cap H = \{id\}$ et KH est un sous-groupe d'ordre 15 dans le groupe G.

I) d) Au I) c) on a 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 caractéristiques (voir I)a)) dans le groupe KH qui est cyclique et distingué dans G (car d'indice 2 dans G). Donc en fait K et H sont distingués dans G et G a un unique 5-Sylow.

I) e) Soit G un groupe d'ordre $20 = 2^2 \times 5$. Le groupe G contient un sous-groupe distingué d'ordre 5 : d'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \mid 4$$

d'où $n_5 = 1$.

I) f) Soit G un groupe d'ordre 12. Intéressons-nous aux 3-Sylow de G. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \mid 4$$

Il en résulte que $n_3 = 1$ ou $n_3 = 4$.

— Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est distingué dans G ; ce sous-groupe est un sous-groupe caractéristique d'ordre 3 (cf I) a)).

— 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

$$n_2 \equiv 1 \bmod 2 \qquad\qquad n_2 \mid 3$$

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 dans G et donc caractéristique dans G (cf I) a)).

I) g) Soit G un groupe d'ordre $6 = 2 \times 3$. Considérons ses 3-Sylow. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \,|\, 2$$

autrement dit que $n_3 = 1$. Ainsi G compte un unique 3-Sylow qui est donc distingué dans G et I) b) permet de conclure.

I) h) Soit G un groupe d'ordre 60 qui contient strictement plus d'un 5-Sylow. D'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \,|\, 12$$

d'où $n_5 \in \{1, 6\}$. Par hypothèse $n_5 \neq 1$ donc $n_5 = 6$.

Raisonnons par l'absurde : supposons que G ne soit pas simple. Soit H un sous-groupe distingué propre de G. Notons que

$$|\mathrm{H}| \in \{2, 3, 4, 5, 6, 10, 12, 15, 20, 30\}.$$

- ◇ 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 déduit 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 (voir I)d)) : 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 (d'après I)f) et I)g)). 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 (on renvoie à I)d) si G/H est d'ordre 30, à I)e) si G/H est d'ordre 20 ; enfin si G/H est d'ordre $15 = 3 \times 5$ et si n_5 est le nombre de 5-Sylow de G/H, les théorèmes de Sylow assurent que $n_5 \equiv 1 \bmod 5$ et n_5 divise 3 donc $n_5 = 1$). Donc G/H contient un sous-groupe K distingué d'ordre 5. Considérons la surjection canonique $\pi : \mathrm{G} \to \mathrm{G}/\mathrm{H}$. 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 (voir le premier ◇ du I)h)).

I) i) 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). D'après I) h) le groupe $\mathcal{A}_5$ est simple.

II) a) **Remarque**. 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.* $\tau_1 = \tau_2$.

Raisonnons par l'absurde : supposons qu'aucun élément non trivial de H n'a de point fixe, *i.e.* supposons que pour tout $\tau \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$.

◇ Montrons dans un premier temps qu'aucun élément de H ne contient dans sa décomposition en cycles disjoints des cycles d'ordre ≥ 3. Raisonnons par l'absurde : supposons qu'il existe τ dans H tel que la décomposition de 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 qui précède 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 est 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 $\sigma\tau\sigma^{-1} = \tau$ (cf Remarque). D'autre part $\sigma\tau\sigma^{-1}(a_3) = \tau(a_3)$: contradiction.

Le groupe H contient donc au moins un élément non trivial qui possède un point fixe.

II) b) Soit τ un élément de $\mathrm{H} \smallsetminus \{\mathrm{id}\}$ pour lequel il existe $1 \leq i \leq n$ tel que $\tau(i) = i$ (l'existence d'un tel τ est assurée par II) a)). 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 donc ou bien $\mathrm{G}_i \cap \mathrm{H} = \mathrm{G}_i$ ou bien $\mathrm{G}_i \cap \mathrm{H} = \{\mathrm{id}\}$. Or τ est un élément non trivial de $\mathrm{G}_i \cap \mathrm{H}$ 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 $\mathcal{S}_n$ on a $\sigma\mathrm{G}_i\sigma^{-1} = \mathrm{G}_{\sigma(i)}$ d'où $\mathrm{G}_i \subset \mathrm{H}$ donc $\mathrm{G}_{\sigma(i)} = \sigma\mathrm{G}_i\sigma^{-1} \subset \sigma\mathrm{H}\sigma^{-1} = \mathrm{H}$. Autrement dit pour tout $1 \leq j \leq n$ on a l'inclusion $\mathrm{G}_j \subset \mathrm{H}$.

II) c) Bien sûr $\mathrm{H} \subset \mathcal{A}_n$ donc pour montrer que $\mathcal{A}_n = \mathrm{H}$ il suffit de montrer que $\mathcal{A}_n \subset \mathrm{H}$. 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 $\mathrm{G}_1\mathrm{G}_2 \dots \mathrm{G}_n \subset \mathrm{H}$ (cf II) b)). Il en résulte que $\mathcal{A}_n \subset \mathrm{H}$.

II) d) Le groupe $\mathcal{A}_5$ est simple (I)i)). Pour $n \geq 6$ tout sous-groupe distingué de $\mathcal{A}_n$ différent de $\{\mathrm{id}\}$ est égal à $\mathcal{A}_n$ (cf II) c)).

Exercice 146 Soit $\mathrm{G} = \mathrm{SL}(2, \mathbb{F}_2)$ le groupe des matrices à coefficients dans le corps à deux éléments et de déterminant 1.

1. Quel est l'ordre de G ? Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?
2. Soit X l'ensemble des 2-Sylow de G. Donner la liste de ses éléments.

   On fait opérer G sur X par conjugaison : si $g \in \mathrm{G}$ et $S \in X$ on pose

   $$g \cdot S = gSg^{-1} = \{ghg^{-1} \mid h \in S\}$$

   Montrer par un calcul direct que cette action est transitive.

   Quel est le stabilisateur de

   $$S_0 = \left\{\mathrm{Id}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\} ?$$

3. On note $\mathcal{S}_X$ le groupe des bijections de X dans lui-même.

   Montrer que

   $$\phi \colon \mathrm{G} \to \mathcal{S}_X, \qquad g \mapsto (S \mapsto g \cdot S)$$

   est un isomorphisme de groupes.

Éléments de réponse 146

1. Déterminons l'ordre de G. Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de G. Nous avons $ad + bc = \overline{1}$ donc
   — ou bien $ad = \overline{1}$ et $bc = \overline{0}$;
   — ou bien $ad = \overline{0}$ et $bc = \overline{1}$.

   On a $ad = \overline{1}$ et $bc = \overline{0}$ si et seulement si $(a, b, c, d) = (1, 0, 1, 1)$ ou $(a, b, c, d) = (1, 1, 0, 1)$ ou $(a, b, c, d) = (1, 0, 0, 1)$ ce qui donne 3 possibilités.

   De même $ad = \overline{0}$ et $bc = \overline{1}$ donne 3 possibilités.

   Déterminer ses 2-Sylow et 3-Sylow. Que peut-on dire du 3-Sylow ?

Soient n_2 le nombre de 2-Sylow de G et n_3 le nombre de 3-Sylow de G. Les théorèmes de Sylow assurent que

$$n_2 \equiv 1 \bmod 2 \qquad\qquad n_2|3$$

et

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3|2$$

Par conséquent $n_3 = 1$, *i.e.* G contient un unique 3-Sylow qui est donc distingué dans G. Le seul sous-groupe d'ordre 3 est constitué de l'identité, de $D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ et $D^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

Les éléments d'ordre 2 sont

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

2. Soit X l'ensemble des 2-Sylow de G. La liste des éléments de X est : $\{\langle A\rangle, \langle B\rangle, \langle C\rangle\}$.

   On fait opérer G sur X par conjugaison : si $g \in \mathrm{G}$ et $S \in X$ on pose

   $$g \cdot S = gSg^{-1} = \{ghg^{-1} \,|\, h \in S\}$$

   Montrons par un calcul direct que cette action est transitive :

   $$B \cdot \langle A\rangle = \langle C\rangle \qquad A \cdot \langle C\rangle = \langle B\rangle \qquad C \cdot \langle B\rangle = \langle A\rangle$$

   Quel est le stabilisateur de

   $$S_0 = \left\{\mathrm{Id}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right\}?$$

   Déterminons le stabilisateur de $\langle A\rangle$. C'est un sous-groupe de G dont l'ordre divise $|\mathrm{G}|$. Il contient Id et A mais ni B, ni C. Par ailleurs $B \cdot \langle A\rangle = \langle C\rangle$. Ce stabilisateur est donc $\langle A\rangle$.

3. On note $\mathcal{S}_X$ le groupe des bijections de X dans lui-même.

   Montrer que

   $$\phi\colon \mathrm{G} \to \mathcal{S}_X, \qquad\qquad g \mapsto (S \mapsto g \cdot S)$$

   est un isomorphisme de groupes.

   Puisque G agit sur X le morphisme ϕ est un morphisme de groupes. Il est injectif car $\ker\phi = \{e_{\mathrm{G}}\}$. Comme $\mathcal{S}_X$ et G ont même ordre (6) nous obtenons que ϕ est un isomorphisme.

Exercice 147 Montrer que $\mathcal{S}_4$ possède trois 2-sous-groupes de SYLOW isomorphes à D_8.

Éléments de réponse 147 Le groupe $\mathcal{S}_4$ est d'ordre $24 = 2^3 \times 3$. Par ailleurs D_8 est le groupe des isométries du plan qui conservent un carré donc $D_8 \subset \mathcal{S}_4$.

Soit n_2 le nombre de 2-SYLOW de $\mathcal{S}_4$. Le groupe D_8 est l'un de ces 2-SYLOW. Les théorèmes de SYLOW assurent que n_2 divise 3 et $n_2 \equiv 1 \bmod 2$. Il s'en suit que $n_2 \in \{1, 3\}$. Si $n_2 = 1$, alors D_8 est distingué dans $\mathcal{S}_4$. Désignons les sommets du carré préservé par D_8 par 1, 2, 3 et 4 dans l'ordre où on les rencontre lorsqu'on se déplace dans le sens positif sur ce carré. Soit r la rotation d'angle $\frac{\pi}{2}$. C'est la permutation (1 2 3 4). Notons que $(2\ 3)r(2\ 3) = (1\ 3\ 2\ 4)$ n'appartient pas à D_8. Ainsi D_8 n'est pas distingué dans $\mathcal{S}_4$. Il y a donc 3 sous-groupes d'ordre 8 qui sont conjugués donc isomorphes. Ces trois sous-groupes sont les trois 2-SYLOW de $\mathcal{S}_4$.

Exercice 148 Soit G un groupe. Soit p un nombre premier divisant $|G|$.

Montrer que si H est un p-sous-groupe de G distingué dans G, alors H est contenu dans tout p-sous-groupe de SYLOW de G.

Éléments de réponse 148 Si H est un p-sous-groupe de G, il existe un p-SYLOW de G qui contient H. Puisque $H \triangleleft G$ et que les p-SYLOW sont conjugués entre eux, H se trouve dans tous les p-SYLOW de G.

Exercice 149 Montrer qu'un groupe d'ordre 56 n'est pas simple.

Éléments de réponse 149 Soit G un groupe d'ordre $56 = 2^3 \times 7$. Soit n_2 le nombre de 2-SYLOW et n_7 le nombre de 7-SYLOW.

D'après les théorèmes de SYLOW

$$n_2 \equiv 1 \pmod 2 \qquad n_2 | 7$$

$$n_7 \equiv 1 \pmod 7 \qquad n_7 | 8$$

Par conséquent $n_2 \in \{1, 7\}$ et $n_7 \in \{1, 8\}$.

Si $n_7 = 1$, alors d'après les théorèmes de SYLOW G possède un sous-groupe distingué propre donc G n'est pas simple.

Supposons que $n_7 \neq 1$, alors $n_7 = 8$ et G compte huit sous-groupes d'ordre 7, c'est-à-dire déjà $8(7-1) = 48$ éléments d'ordre 7 (remarque : $7 - 1 =$ nombre d'éléments non triviaux d'un sous-groupe d'ordre 7). En ajoutant l'élément neutre nous avons donc "listé" 49 éléments du groupe G. Nous allons les noter $g_1 = e$, g_2, …, g_{49}. Supposons que $n_2 = 7$. Soit S un 2-SYLOW de G ; il est d'ordre 8. Notons e, h_2, …, h_8 ses éléments. Pour des raisons d'ordre les h_i n'appartiennent pas $\{g_1, g_2, \ldots, g_{49}\}$. Donc G contient les éléments distincts g_1, g_2, …, g_{49}, h_2, h_3, …, h_8 ; en particulier $|G| \geq 49 + 7 = 56$. Par hypothèse $n_2 = 7$ donc G contient un 2-SYLOW T distinct de S. Soit k dans $T \setminus S$. Pour des raisons d'ordre k n'appartient pas $\{g_1, g_2, \ldots, g_{49}\}$. Par suite G contient les éléments distincts g_1, g_2, …, g_{49}, h_2, h_3, …, h_8, k.

En particulier $|\mathrm{G}| \geq 49 + 7 + 1 = 57$: contradiction. Par conséquent $n_2 \neq 7$ et $n_2 = 1$; d'après les théorèmes de Sylow G possède un sous-groupe distingué propre donc G n'est pas simple.

Exercice 150 Montrer qu'un groupe d'ordre pq, où p et q sont premiers et distincts, ne peut être simple.

Éléments de réponse 150 Soit G un groupe d'ordre pq. Quitte à renommer p et q nous pouvons supposer que $p > q$. Soit n_p le nombre de p-Sylow de G.

Les théorèmes de Sylow assurent que $n_p \equiv 1 \pmod{p}$ et n_p divise q, autrement dit que $n_p \equiv 1 \pmod{p}$ et $n_p \in \{1, q\}$. Mais comme $p > q$, $q \not\equiv 1 \pmod{p}$. Par suite $n_p = 1$, *i.e.* il y a un seul p-Sylow dans G qui est un sous-groupe d'ordre p distingué dans G et propre. Il s'en suit que G n'est pas simple.

Exercice 151 Soient p et q deux nombres premiers.

Montrer qu'il existe au plus deux structures de groupes d'ordre pq.

Éléments de réponse 151

Exercice 152 Soit $\mathrm{G} = \mathrm{SL}(2, \mathbb{F}_3)$ le groupe des matrices 2×2 de déterminant égal à 1 et à coefficients dans le corps $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

1. Montrer que G est d'ordre 24.
2. Quel est l'ordre des éléments $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ de G ?
3. Combien G a-t-il de 3-sous-groupes de Sylow ?
4. Montrer que le sous-groupe H engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est le seul sous-groupe de G d'ordre 8.
5. Montrer que G est produit semi-direct de H par un sous-groupe K d'ordre 3.
6. Montrer que le centre de $Z(\mathrm{G})$ de G est égal à $\{\mathrm{id}, -\mathrm{id}\}$.
7. Montrer que $\mathrm{G}/Z(\mathrm{G}) \simeq \mathcal{A}_4$ (rappelons que les éléments (1 2 3), (1 2)(3 4) et (1 3)(2 4) engendrent le groupe $\mathcal{A}_4$).

Éléments de réponse 152

1. Montrons que G est d'ordre 24.

   Une matrice de G s'écrit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $ad - bc = \overline{1}$ et a, b, c et d dans $\mathbb{Z}/3\mathbb{Z}$. Cela donne 24 cas possibles pour M.

2. Les ordres cherchés sont des diviseurs de 24 bien sûr. La matrice $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$ est d'ordre 6. Les matrices $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ sont d'ordre 3.

3. Soit n_3 le nombre de 3-SYLOW de G qui est d'ordre $24 = 2^3 \times 3$. Notons que les 3-SYLOW sont donc d'ordre 3. Les théorèmes de SYLOW assurent que $n_3 \equiv 1 \pmod 3$ et que n_3 divise $2^3 = 8$. Il s'en suit que $n_3 \in \{1, 4\}$. D'après 2. il y a au moins deux sous-groupes de G d'ordre 3. Par conséquent $n_3 = 4$.

4. Montrer que le sous-groupe H engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est le seul sous-groupe de G d'ordre 8.

   Vérifions dans un premier temps que H est d'ordre 8. En effet $A^2 = B^2 = -\mathrm{id}$ donc A et B sont d'ordre 4. Posons $C = AB = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$. On vérifie que

$$\mathrm{H} = \{\mathrm{id}, -\mathrm{id}, A, -A, B, -B, C, -C\}$$

   (le groupe H est le groupe des quaternions).

   Soit $N = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Alors $N^{-1} = \begin{pmatrix} d & b \\ -c & a \end{pmatrix}$.

   Posons $M = NAN^{-1}$ et $L = NBN^{-1}$. Remarquons que si x appartient à $\mathbb{Z}/3\mathbb{Z}$ et $x \neq \overline{O}$, alors $x^2 = \overline{1}$.

   Un calcul montre que

$$M = \begin{pmatrix} bd + ac & -(a^2 + b^2) \\ (c^2 + d^2) & -(bd + ac) \end{pmatrix}$$

   Comme N appartient à G, nous avons $ad - bc = \overline{1}$.

   Si $a = \overline{0}$, alors $-bc = \overline{1}$ et $b = -c$. Si $d = \overline{0}$, alors $M = A$ appartient à H. Si $d \neq \overline{0}$, alors $M = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} = -C$ ou $M = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} = -M$; dans les deux cas M appartient à H.

   Si maintenant $abcd \neq \overline{0}$, alors $a = -d$ et $b = c$ donc $M = -A$ appartient à H.

   On démontre de manière analogue que L appartient à H. Ainsi H est distingué dans G. Of H est un 2-SYLOW de G. Par suite il n'y a qu'un seul 2-SYLOW dans G puisque par conjugaison à partir d'un 2-SYLOW on obtient tous les 2-SYLOW. Or les 2-SYLOW sont les sous-groupes d'ordre 8 de G. Il y a donc un unique sous-groupe d'ordre 8 dans G qui est H.

5. Montrons que G est produit semi-direct de H par un sous-groupe K d'ordre 3.

Soit K l'un des sous-groupes d'ordre 3 de G. Nous avons les propriétés suivantes : $\mathrm{H} \cap \mathrm{K} = \{e\}$, H est distingué dans G et $3 \times 8 = 24$. Il s'en suit que G est un produit semi-direct de H par K.

Nous avons $\mathrm{G} = \mathrm{H} \rtimes_\rho \mathrm{K}$ où $\rho\colon \mathrm{K} \to \mathrm{Aut}(\mathrm{H})$ est tel que $\rho(k)$ est l'automorphisme intérieur associé à l'élément $k \in \mathrm{K}$.

6. Montrons que le centre de $Z(\mathrm{G})$ de G est égal à $\{\mathrm{id}, -\mathrm{id}\}$.

   Un élément M de G appartient à $Z(\mathrm{G})$ si en particulier $MA = AM$ et $MB = BM$.

   Or $AM = MA$ si et seulement si

$$\begin{pmatrix} -c & -d \\ a & b \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$$

   et $BM = MB$ si et seulement si

$$\begin{pmatrix} a+b & b+d \\ a+c & b-d \end{pmatrix} = \begin{pmatrix} a+b & a-b \\ c+d & c-d \end{pmatrix}.$$

   Ces deux égalités conduisent à $a = d$, $b = -c$, $b + d = a - b$, $a = d$ et $b = c$, soit à $a = d$ et $b = c = 0$, *i.e.* à $M = \pm\mathrm{id}$. Par suite $Z(\mathrm{G}) = \{\mathrm{id}, \mathrm{id}\}$.

7. Montrons que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})} \simeq \mathcal{A}_4$.

   Considérons ici G comme produit semi-direct de H par K. Définir un morphisme φ de G dans $\mathcal{A}_4$ c'est définir φ sur H et K en respectant l'action de K sur H. Définir φ sur H c'est le définir sur les générateurs A et B en s'assurant que leurs images vérifient les mêmes relations, c'est-à-dire $A^2 = B^2 = (AB)^2$. On vérifie que φ défini par

$$\varphi(A) = (1\ 2)(3\ 4) \qquad \varphi(B) = (1\ 3)(2\ 4) \qquad \varphi(C) = (1\ 2\ 3)$$

   convient et que $\ker\varphi = \{\mathrm{id}, -\mathrm{id}\}$. Par suite ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})} = {}^{\mathrm{G}}\!/_{\ker\varphi} \simeq \mathcal{A}_4$.

Exercice 153 Soit G′ un sous-groupe d'ordre $p(p-1)$ de $\mathcal{S}_p$.
Montrer que G′ est le normalisateur d'un p-Sylow de $\mathcal{S}_p$.
En déduire que K est conjugué de tous les sous-groupes d'ordre $p(p-1)$ de $\mathcal{S}_p$.

Éléments de réponse 153

Exercice 154 Si G est un groupe, on peut faire agir G par conjugaison sur lui-même.

(1) Montrer que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.

(2) (i) Si G est un p-groupe, p premier, montrer que le centre de G n'est pas réduit à $\{1\}$.
   (ii) Soit G un groupe tel que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ soit cyclique. Montrer qu'alors G est abélien.

(3) Montrer que le groupe des matrices triangulaires supérieures unipotentes

$$\mathrm{G} = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{F}_p) \right\}$$

est un groupe non-abélien d'ordre p^3.

Éléments de réponse 154

(1) Montrons que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.

C'est la définition du centre :

$$Z(\mathrm{G}) = \{x \in \mathrm{G} \,|\, gxg^{-1} = x \text{ pour tout } g \in \mathrm{G}\}.$$

(2) (i) Si G est un p-groupe, p premier, montrons que le centre de G n'est pas réduit à $\{1\}$. Notons Ω_i, $i \in I$, les orbites non réduites à un singleton. Puisque $|\Omega_i|$ divise $|\mathrm{G}|$ chaque $|\Omega_i|$ est une puissance de p distincte de 1. En écrivant G comme une union disjointe d'orbites on obtient

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_i |\Omega_i|$$

soit

$$0 \equiv |Z(\mathrm{G})| \bmod p.$$

Ceci montre que $|Z(\mathrm{G})| \neq 1$.

(ii) Soit G un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ soit cyclique. Montrons qu'alors G est abélien.

Par hypothèse il existe un élément a de G dont la classe $\overline{a} \in \mathrm{G}/Z(\mathrm{G})$ engendre $\mathrm{G}/Z(\mathrm{G})$. Tout élément de G peut alors s'écrire $a^k h$ avec $k \in \mathbb{Z}$ et $h \in Z(\mathrm{G})$. Puisque

$$a^k h \cdot a^{k'} h' = a^{k+k'} hh' = a^{k+k'} h'h = a^{k'} h' a^k h$$

le groupe G est aélien.

(3) Montrons que le groupe des matrices triangulaires supérieures unipotentes

$$\mathrm{G} = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{F}_p) \right\}$$

est un groupe non-abélien d'ordre p^3.

Chacun des coefficients $*$ est un élément arbitraire de $\mathbb{F}_p$ d'où p^3 choix possibles ; de plus

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

ne commutent pas d'où le résultat.

Exercice 155 Soit G un groupe fini d'ordre $|\mathrm{G}| = p^a m$ avec p premier et $\mathrm{pgcd}(p, m) = 1$. Soient $S \subset \mathrm{G}$ un p-Sylow et H un sous-groupe de G. Montrer qu'il existe $g \in \mathrm{G}$ tel que $gSg^{-1} \cap \mathrm{H}$ soit un p-Sylow de H.

Éléments de réponse 155 On a $|\mathrm{G}| = p^a m$ et $|\mathrm{H}| = p^b n$. On fait agir G (et donc également H) par translation sur l'ensemble X des classes à gauche de G modulo S. Notons que $g' \in \mathrm{Stab}(gS)$ équivaut à $g' \in gSg^{-1}$. Par ailleurs l'ensemble X est de cardinal m qui n'est pas un multiple de p. L'une des orbites Ω de X sous l'action de H est donc de cardinal p^c pour un certain $c \leq b$. Mais comme de plus $|\mathrm{Stab}(x)| \cdot |\Omega| = |\mathrm{H}| = p^b n$ et $\mathrm{pgcd}(|\Omega|, p) = 1$ on a finalement $|\Omega| = n$ et $|\mathrm{Stab}(x)| = p^b$ comme attendu.

Exercice 156

(1) Soient $\Bbbk$ un corps et G un groupe fini. Montrer qu'il existe un entier n tel que G soit isomorphe à un sous-groupe de $\mathrm{GL}(n, \Bbbk)$. [Indication : on pourra commencer par plonger G dans un groupe symétrique.]

(2) Soit $\mathbb{F}_p$ le corps à p éléments où p désigne un nombre premier. Montrer que le groupe des matrices triangulaires supérieures avec des 1 sur la diagonale est un p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$.

Éléments de réponse 156

(1) Tout groupe fini se plonge dans un groupe symétrique $\mathcal{S}_n$ en faisant agir G sur lui-même par translation ce qui montre que $n = |\mathrm{G}|$ convient. De plus le groupe symétrique $\mathcal{S}_n$ se plonge dans $\mathrm{GL}(n, \Bbbk)$ pour tout corps $\Bbbk$ en faisant agir $\mathcal{S}_n$ sur les vecteurs d'une base de $\Bbbk^n$.

(2) Le cardinal de $\mathrm{GL}(n, \mathbb{F}_p)$ est (compter les base de $(\mathbb{F}_p)^n$

$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}) = p^{1+2+\dots+(n-1)} m$$

avec $\mathrm{pgcd}(m, p) = 1$. Or $p^{1+2+\dots+(n-1)}$ est le cardinal du groupe des matrices triangulaires unipotentes.

Exercice 157 Supposons qu'il existe un groupe simple G d'ordre 180.

a) Montrer que G contient trente six 5-Sylow.

b) Montrer que G contient dix 3-Sylow. Montrer que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e_{\mathrm{G}}$ (Indication : considérer les ordres possibles pour le centralisateur de g, observer qu'un groupe d'ordre 18 admet un unique 3-Sylow).

c) Conclure.

Éléments de réponse 157

a) Montrons que G contient trente six 5-SYLOW. Pour tout premier p qui divise $|\mathrm{G}|$ notons n_p le nombre de p-SYLOW de G. Les théorèmes de SYLOW assurent que n_5 divise 36 et $n_5 \equiv 1 \pmod 5$. Ceci implique que n_5 appartient à $\{1, 6, 36\}$. Puisque par hypothèse G est simple on ne peut avoir $n_5 = 1$ (sinon l'unique 5-SYLOW serait distingué dans G). Il en résulte que n_5 appartient à $\{6, 36\}$. Supposons que $n_5 = 6$. Alors l'action transitive de G par conjugaison sur l'ensemble de ses 5-SYLOW induit un morphisme non trivial $\mathrm{G} \to \mathcal{S}_6$. Le groupe G étant par hypothèse simple, le noyau de ce morphisme est trivial, *i.e.* ce morphisme est injectif. Le morphisme $\mathrm{G} \to {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ donné par la signature a nécessairement un noyau trivial donc G est un sous-groupe de $\mathcal{A}_6$. D'une part $|\mathcal{A}_6| = \frac{|\mathcal{S}_6|}{2} = \frac{6!}{2} = 360$, d'autre part $|\mathrm{G}| = 180$, autrement dit G est d'indice 2 dans $\mathcal{A}_6$. Le groupe G est donc un sous-groupe distingué non trivial et propre de $\mathcal{A}_6$: contradiction avec le fait que $\mathcal{A}_6$ est simple. Par conséquent $n_5 = 36$.

b) Montrons que G contient dix 3-SYLOW. Pour tout premier p qui divise $|\mathrm{G}|$ notons n_p le nombre de p-SYLOW de G. Les théorèmes de SYLOW assurent que n_3 divise 20 et $n_3 \equiv 1 \pmod 3$. Ceci implique que n_3 appartient à $\{1, 4, 10\}$. Puisque par hypothèse G est simple on ne peut avoir $n_3 = 1$ (sinon l'unique 3-SYLOW serait distingué dans G). Si n_3 était égal à 4, on en déduirait comme au a) un morphisme injectif de G dans $\mathcal{S}_4$ ce qui est impossible car $180 = |\mathrm{G}| > |\mathcal{S}_4| = 4! = 24$. Ainsi $n_3 = 10$.

Montrons que deux 3-SYLOW distincts ne peuvent pas contenir un même élément $g \neq e_{\mathrm{G}}$.

Soient S et T deux 3-SYLOW de G distincts. Soit $g \in S \cap T$. Notons $Z = \{x \in \mathrm{G} \,|\, xg = gx\}$ le centralisateur de g dans G. Supposons que $g \neq e_{\mathrm{G}}$. Un groupe d'ordre 9 étant abélien, Z contient S et T. Par conséquent $|Z| \in \{18, 36, 45, 90\}$. L'action transitive de G sur ${}^{\mathrm{G}}\!/_{Z}$ induit un morphisme injectif de G vers $\mathcal{S}_{{}^{\mathrm{G}}/_{Z}}$. Or $|\mathrm{G}| = 180$ et $|\mathcal{S}_{{}^{\mathrm{G}}/_{Z}}| \in \{2, 4! = 24, 5! = 120, 10!\}$ donc $\left|\mathcal{S}_{{}^{\mathrm{G}}/_{Z}}\right| = 10!$ et $|Z| = 18$. Ainsi S et T sont des 3-SYLOW de Z et un groupe d'ordre 18 admet un unique 3-SYLOW d'où $S = T$: contradiction. Finalement $S \cap T = \{e_{\mathrm{G}}\}$.

c) D'après a) le groupe G contient exactement $36 \times 4 = 144$ éléments d'ordre 5.

D'après b) le groupe G contient dix 3-SYLOW dont les intersections deux à deux sont triviales. Par suite il y a dans G exactement $10 \times 8 = 80$ éléments distincts de e_{G} d'ordre divisant 9.

Ainsi G possède au moins $144 + 80 = 224 > 180$ éléments distincts : contradiction.

Il n'existe donc pas de groupe simple d'ordre 180.

Exercice 158 Expliciter les sous-groupes de SYLOW des groupes alternés $\mathcal{A}_4$ et $\mathcal{A}_5$.

Éléments de réponse 158 Déterminons les sous-groupes de SYLOW de $\mathcal{A}_4$. Le groupe $\mathcal{A}_4$ est d'ordre $12 = 2^2 \times 3$.

Les théorèmes de Sylow assurent que
— le nombre n_2 de sous-groupes d'ordre $2^2 = 4$ de $\mathcal{A}_4$ est 1 ou 3 ;
— le nombre n_3 de sous-groupes d'ordre 3 de $\mathcal{A}_4$ est 1 ou 4.

Le groupe $\mathcal{A}_4$ ne contient pas de cycle de longueur 4 donc les seuls éléments d'ordre pair sont les doubles transpositions. Il y en a trois ainsi $\mathcal{A}_4$ contient un seul sous-groupe d'ordre 4, isomorphe au groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe $\mathcal{A}_4$ contient les cycles de longueur 3. Il y en a plus de deux donc $n_3 = 4$.

Déterminons les sous-groupes de Sylow de $\mathcal{A}_5$. Le groupe $\mathcal{A}_5$ est d'ordre $60 = 2^2 \times 3 \times 5$.

Les 3-Sylow de $\mathcal{A}_5$ sont d'ordre 3, donc cycliques ; chacun est engendré par un 3-cycle et contient deux 3-cycles. Les 3-Sylow sont deux à deux d'intersection réduite à $\{e\}$. Comme il y a vingt 3-cycles dans $\mathcal{A}_5$, il y a dix 3-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 3-Sylow est $\equiv 1 \pmod 3$ et divise 20 ; c'est donc 1, 4 ou 10. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 5-Sylow. Si c'est 4 l'action par conjugaison de $\mathcal{A}_5$ sur l'ensemble de ses 3-Sylow induit un morphisme de $\mathcal{A}_5$ dans $\mathcal{S}_4$ qui est non trivial (car l'action par conjugaison est transitive) et donc injectif (car le noyau distingué est forcément trivial puisque $\mathcal{A}_5$ est simple) : contradiction avec le fait que l'ordre de $\mathcal{A}_5$ ne divise par celui de $\mathcal{S}_4$.

Les 5-Sylow de $\mathcal{A}_5$ sont d'ordre 5, donc cycliques ; chacun est engendré par un 5-cycle et contient quatre 5-cycles. Les 5-Sylow sont deux à deux d'intersection réduite à $\{1\}$. Comme il y a vingt-quatre 5-cycles dans $\mathcal{A}_5$, il y a six 5-Sylow.

On peut aussi utiliser les théorèmes de Sylow : le nombre de 5-Sylow est $\equiv 1 \pmod 5$ et divise 12 ; c'est donc 1 ou 6. Puisque $\mathcal{A}_5$ est simple il ne peut y avoir qu'un seul 3-Sylow. Par conséquent le nombre de 5-Sylow est 6.

On a donc déterminé $6 \times 4 = 24$ éléments d'ordre 5 et $2 \times 10 = 20$ éléments d'ordre 3 ce qui fait, en ajoutant l'identité, 45 éléments de $\mathcal{A}_5$.

Soit n_2 le nombre de 2-Sylow, *i.e.* le nombre de sous-groupes d'ordre 4 de $\mathcal{A}_5$. Rappelons qu'un groupe d'ordre 4 est soit cyclique, soit isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Le groupe $\mathcal{A}_5$ ne contient pas d'élément d'ordre 4. En effet les éléments d'ordre 4 du groupe symétrique $\mathcal{S}_5$ sont les 4-cycles qui sont des permutations impaires. Par suite chaque 2-Sylow est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; il est engendré par deux produits de deux transpositions qui commutent et contient trois éléments d'ordre 2. Les trois éléments d'ordre 2 sont les trois produits de deux transpositions qui commutent qu'on peut former avec quatre éléments de $\{1, 2, 3, 4, 5\}$. On en déduit que les 2-Sylow sont deux à deux d'intersection réduite à $\{e\}$. Il y a 15 éléments d'ordre 2 dans $\mathcal{A}_5$ et cinq 2-Sylow.

Exercice 159 Expliciter les sous-groupes de Sylow des groupes diédraux D_8 et D_{10}.

Éléments de réponse 159

i) Déterminons les sous-groupes de Sylow du groupe D_8. Le groupe D_8 est d'ordre $2^3 = 8$. Les 2-Sylow sont d'ordre 2^3, il n'y en a donc qu'un, c'est D_8.

ii) Déterminons les sous-groupes de Sylow du groupe D_{10}. Le groupe D_{10} est le groupe des isométries du plan qui conservent un pentagone régulier, il est d'ordre $2 \times 5 = 10$.

Soit n_2 le nombre de ses 2-Sylow, *i.e.* le nombre de ses sous-groupes d'ordre 2. D'après les théorèmes de Sylow $n_2 \equiv 1 \pmod 2$ et n_2 divise 5. Ainsi $n_2 \in \{1, 5\}$. Par ailleurs les sous-groupes de D_{10} engendrés par les cinq symétries par rapport aux médiatrices de chacun des côtés du pentagone sont cinq groupes d'ordre 2. Il s'en suit que $n_2 = 5$.

Soit n_5 le nombre de 5-Sylow de D_{10}, *i.e.* le nombre de sous-groupes d'ordre 5 de D_{10}. Les théorèmes de Sylow assurent que $n_5 \equiv 1 \pmod 2$ et n_5 divise 2. Il n'y a donc qu'un unique 5-Sylow, le sous-groupe engendré par la rotation d'angle $\frac{2\pi}{5}$ dont le centre est le centre du pentagone.

Exercice 160

a) Quel est l'ordre d'un p-Sylow de $\mathcal{S}_p$?

b) Combien y a-t-il de p-Sylow dans $\mathcal{S}_p$?

c) En déduire le théorème de Wilson, c'est à dire

$$(p-1)! \equiv -1 \bmod p.$$

Éléments de réponse 160

a) L'ordre de $\mathcal{S}_p$ est $p! = p(p-1)!$. De plus p et $(p-1)!$ sont premiers entre eux. Par suite un p-Sylow de $\mathcal{S}_p$ est d'ordre p.

b) Pour déterminer le nombre de p-Sylow de $\mathcal{S}_p$ on cherche combien il y a d'éléments d'ordre p de $\mathcal{S}_p$. Ce sont les p-cycles qui sont conjugués entre eux. Pour calculer leur nombre il suffit de calculer l'ordre du centralisateur C de l'un d'eux, par exemple du p-cycle $\sigma = (1\ 2\ \dots\ p)$. Si s est une permutation, alors

$$s\sigma s^{-1} = (s(1)\ s(2)\ \dots\ s(p))$$

Donc $s \in C$ si

$$(\sigma(1)\ \sigma(2)\ \dots\ \sigma(p)) = (s(1)\ s(2)\ \dots\ s(p))$$

c'est-à-dire si s est une puissance de la permutation circulaire d'ordre p. L'ordre de C est donc égal à p et il y a $\frac{p!}{p} = (p-1)!$ éléments d'ordre p dans $\mathcal{S}_p$ car $\mathcal{S}_p/C$ est en bijection avec les conjugués de σ.

Ces éléments d'ordre p se répartissent entre $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow de $\mathcal{S}_p$ qui contiennent chacun $(p-1)$ éléments d'ordre p.

Autre rédaction possible : un p-Sylow est d'ordre p, p étant premier, un p-Sylow est donc un sous-groupe cyclique d'ordre p. Il y a $(p-1)!$ p-cycles dans $\mathcal{S}_p$ donc $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow.

c) Notons n_p le nombre de p-SYLOW. D'après b) on a $n_p = (p-2)!$. D'après les théorèmes de SYLOW $n_p \equiv 1 \bmod p$. Donc $(p-2)! \equiv 1 \bmod p$ et $(p-1)! \equiv p-1 \bmod p$. Mais $p-1 \equiv -1 \bmod p$. Il en résulte que $(p-1)! \equiv -1 \bmod p$.

Exercice 161 On cherche à montrer que $\mathcal{A}_5$ est le seul groupe simple d'ordre 60.

a) Faire la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif. Décrire les classes de conjugaison dans $\mathcal{A}_5$.

b) Montrer que $\mathcal{A}_5$ est simple.

c) Soit G un groupe simple d'ordre $p^\alpha m$ avec $\alpha \geq 1$ et m non divisible par p. Notons n_p le nombre de p-SYLOW de G. Montrer que $|\mathrm{G}|$ divise $n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrer que le nombre de 2-SYLOW de G est égal à 5 ou à 15.

e) En déduire que G contient un sous-groupe d'ordre 12.

f) Conclure.

Éléments de réponse 161

a) Faisons la liste des éléments de $\mathcal{A}_5$ avec leur ordre respectif.

Les 60 éléments de $\mathcal{A}_5$ sont les suivants :

- l'identité d'ordre 1 qui forme une classe de conjugaison ;
- les double transpositions $(a\ b)(c\ d)$ où $\{a, b, c, d\}$ est de cardinal 4. Elles sont au nombre de 15, elles sont d'ordre 2 et elles forment une classe de conjugaison ;
- les 3-cycles $(a\ b\ c)$ où $\{a, b, c\}$ est de cardinal 3. Ils sont au nombre de 20, ils sont d'ordre 3 et forment une classe de conjugaison ;
- les 5-cycles $(a\ b\ c\ d\ e)$ où $\{a, b, c, d, e\}$ est de cardinal 5. Ils sont au nombre de 24, ils sont d'ordre 5 et forment deux classes de conjugaison : celle de (1 2 3 4 5) et (2 1 3 4 5).

Nous avons bien énuméré tous les éléments de $\mathcal{A}_5$: $1 + 15 + 20 + 24 = 60$.

b) Montrons que $\mathcal{A}_5$ est simple. Soit $\mathrm{H} \neq \{e\}$ un sous-groupe distingué de $\mathcal{A}_5$. Puisque H est distingué, H est réunion de classes de conjugaison dans $\mathcal{A}_5$. Comme aucun des entiers $1+15=16$, $1+12=13$, $1+24=25$, $1+15+12=28$, $1+15+24=40$, $1+20=21$, $1+20+15=36$, $1+20+12=33$, $1+20+24=45$ ne divise $60 = |\mathcal{A}_5|$, le théorème de LAGRANGE assure que H contient nécessairement toutes les classes de conjugaison de $\mathcal{A}_5$, donc $\mathrm{H} = \mathcal{A}_5$.

c) Regardons l'action transitive de G par conjugaison sur l'ensemble Syl_p de ses p-SYLOW. Comme G est simple $n_p > 1$. On obtient donc un morphisme non trivial $\mathrm{G} \to \mathcal{S}_{\mathrm{Syl}_p} \simeq \mathcal{S}_{n_p}$. Puisque G est simple ce morphisme est injectif. Il en résulte que $|\mathrm{G}|$ divise $|\mathcal{S}_{n_p}| = n_p!$.

d) Soit G un groupe simple d'ordre 60. Montrons que le nombre de 2-SYLOW de G est égal à 5 ou à 15.

Soit n_2 le nombre de 2-SYLOW. Les théorèmes de SYLOW assurent que n_2 est impair et divise 15 ; par suite n_2 appartient à $\{1, 3, 5, 15\}$. Le groupe G étant simple, $n_2 \neq 1$, *i.e.* n_2 appartient à $\{3, 5, 15\}$. Le groupe G est d'ordre $2^2 \cdot 15$; d'après le c) $|G|$ divise $n_2!$ donc $n_2 \neq 3$. Ainsi n_2 vaut 5 ou 15.

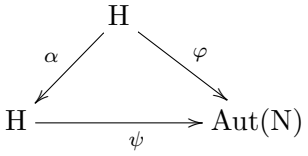
e) Montrons que G contient un sous-groupe d'ordre 12.

Supposons dans un premier temps que $n_2 = 5$; alors le normalisateur d'un 2-SYLOW de G est de cardinal $60/5 = 12$ d'où le résultat.

Supposons désormais que $n_2 = 15$. Montrons qu'il existe deux 2-SYLOW distincts S et T tels que $|S \cap T| = 2$. Sinon on aurait exactement $15 \cdot 3 + 1 = 46$ éléments d'ordre divisant 4. De plus les théorèmes de SYLOW assurent que $n_5 = 6$ donc que G contient $6 \cdot 4 = 24$ éléments d'ordre 5. Ainsi d'une part G contient au moins $46 + 24 = 70$ éléments et d'autre par $|G| = 60$: contradiction. On dispose donc de deux 2-SYLOW distincts S et T tels que $S \cap T = \{e, g\}$ avec g d'ordre 2. Désignons par H le centralisateur de g dans G. Alors H contient S et T donc son cardinal est multiple de 4 et > 6. Ainsi $|H|$ appartient à $\{12, 20, 60\}$. Si $|H| = 20$, alors l'action transitive de G sur G/H induit un morphisme injectif $G \to \mathcal{S}_{G/H} \simeq \mathcal{S}_3$: contradiction. Si $|H| = 60$, alors g est dans le centre de G ce qui assure que le centre $Z(G)$ de G est non trivial : contradiction avec le fait que G est simple. Il s'en suit que $|H| = 12$.

f) Soit H le sous-groupe de G d'ordre 12 construit au e). L'action transitive de G sur G/H induit un morphisme injectif $\varphi : G \to \mathcal{S}_{G/H} \simeq \mathcal{S}_5$. Ainsi G est isomorphe à un sous-groupe d'ordre 60 de $\mathcal{S}_5$ qui est nécessairement $\mathcal{A}_5$.

Exercice 162 Rappelons l'énoncé suivant dont nous aurons besoin : Soient H et N deux groupes. Soient φ et ψ deux opérations de H sur N et α un automorphisme de H tels que le diagramme suivant commute



i.e. $\varphi = \psi \circ \alpha$.

L'application $(n, h) \mapsto (n, \alpha(h))$ est un isomorphisme de $N \rtimes_\psi H$ sur $N \rtimes_\varphi H$.

Soient p et q des nombres premiers avec $p < q$. Montrer que

1. Si p ne divise pas $q - 1$, alors tout groupe d'ordre pq est cyclique.
2. Si p divise $q - 1$, alors il y a deux groupes d'ordre pq non isomorphes : le groupe cyclique et un produit semi-direct non abélien.

Indication : $\mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ ([Perrin, Cours d'algèbre, p. 24])

Éléments de réponse 162

Soit G un groupe d'ordre pq où p et q désignent des nombres premiers tels que $p < q$. Soit Q un q-Sylow de G.

D'après les théorèmes de Sylow

$$\begin{cases} n_q \text{ divise } p \\ n_q \equiv 1 \bmod q \end{cases}$$

où n_q est le nombre de q-Sylow de G. Par suite $n_q = 1$ et Q est distingué dans G.

Puique p est premier, $\mathbb{Q} \simeq \mathbb{Z}/q\mathbb{Z}$. De même $\mathrm{G}/\mathrm{Q} \simeq \mathbb{Z}/p\mathbb{Z}$. Si P est un p-Sylow quelconque il fournit un relèvement de G/Q et donc

$$\mathrm{G} \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Calculons ces produits. On a $\mathrm{Aut}\left(\mathbb{Z}/q\mathbb{Z}\right) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$. L'opération de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$ correspond donc à un morphisme

$$\varphi \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}.$$

On a l'alternative suivante :

- p ne divise pas $q-1$, alors φ est trivial, le produit est direct et $\mathrm{G} \simeq \mathbb{Z}/pq\mathbb{Z}$ est cyclique.
- p divise $q-1$, $\mathbb{Z}/(q-1)\mathbb{Z}$ possède un unique sous-groupe d'ordre p, il y a donc une opération non triviale. De plus deux telles opérations diffèrent d'un automorphisme de $\mathbb{Z}/p\mathbb{Z}$. L'énoncé rappelé assure que les produits correspondants sont isomorphes.

Exercice 163

Soit $n \geq 1$. On note $\mathrm{Int}(\mathcal{S}_n)$ le sous-groupe des automorphismes intérieurs de $\mathrm{Aut}(\mathcal{S}_n)$.

a) Soit $\phi \in \mathrm{Aut}(\mathcal{S}_n)$ tel que ϕ transforme toute transposition en une transposition.
Montrer que ϕ est intérieur.

b) Soit $\sigma \in \mathcal{S}_n$. Déterminer le cardinal du commutant

$$Z(\sigma) = \{\tau \in \mathcal{S}_n \mid \tau\sigma\tau^{-1} = \sigma\}$$

de σ.

c) En déduire que si $n \neq 6$, on a $\mathrm{Int}(\mathcal{S}_n) = \mathrm{Aut}(\mathcal{S}_n)$.

d) Soit $n \geq 5$ tel que $\mathrm{Int}(\mathcal{S}^n) = \mathrm{Aut}(\mathcal{S}_n)$. Montrer que tous les sous-groupes d'indice n de $\mathcal{S}_n$ sont conjugués.

e) En utilisant les 5-Sylow de $\mathcal{S}_5$ montrer qu'il existe un sous-groupe H d'indice 6 de $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

f) Soit q une puissance D'un nombre premier et $n \geq 2$. Construire un morphisme de groupes injectif canonique $\mathrm{PGL}_n(\mathbb{F}_q) \to \mathcal{S}_N$ avec $N = \frac{q^n-1}{q-1}$.

g) Construire géométriquement un sous-groupe H' d'indice 6 dans $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

h) En déduire que $\mathrm{Aut}(\mathcal{S}_6) \neq \mathrm{Int}(\mathcal{S}_6)$.

Éléments de réponse 163

a) Soit $\phi \in \mathrm{Aut}(\mathcal{S}_n)$ tel que ϕ transforme toute transposition en une transposition.

Montrons que ϕ est intérieur.

Puisque tout automorphisme de $\mathcal{S}_i$ est intérieur dès que $i \leq 3$ (à vérifier) on peut supposer que $n \geq 4$.

Le groupe symétrique est engendré par les transpositions $\tau_i = (1\ i)$ pour $i \geq 2$. Comme τ_i et τ_j ne commutent pas si $i \neq j$ les supports des transpositions $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ont exactement un point en commun noté α_1. Puisque $\varphi(\tau_i)$ a un point commun avec $\varphi(\tau_1)$, $\varphi(\tau_2)$ et $\varphi(\tau_3)$ ils ont nécessairement tous α_1 en commun. Écrivons $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$. L'application φ étant injective $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{1, 2 \ldots, n\}$. Définissons la permutation $\alpha \in \mathcal{S}_n$ par $\alpha(i) = \alpha_i$ pour tout $1 \leq i \leq n$. Ainsi φ est la conjugaison par α et φ appartient à $\mathrm{Int}(\mathcal{S}_n)$.

b) Soit $\sigma \in \mathcal{S}_n$. Déterminons le cardinal du commutant

$$Z(\sigma) = \left\{\tau \in \mathcal{S}_n \,|\, \tau\sigma\tau^{-1} = \sigma\right\}$$

de σ. Décomposons σ en produit de cycles à supports disjoints, k_1 cycles de longueur 1, …, k_n cycles de longueur n, avec $n = \sum_i ik_i$. Un élément qui commute à σ doit préserver la décomposition en cycles de σ et donc envoyer le support d'un k-cycle sur celui d'un autre k-cycle, en respectant l'ordre cyclique du support de ces cycles pour tout k. Ainsi le commutant d'un n-cycle de $\mathcal{S}_n$ est composé des puissances de ce dernier. Finalement on obtient

$$|Z(\sigma)| = \prod_i k_i! i^{k_i}.$$

c) Montrons que si $n \neq 6$, on a $\mathrm{Int}(\mathcal{S}_n) = \mathrm{Aut}(\mathcal{S}_n)$. Soit φ un automorphisme de $\mathcal{S}_n$. Si τ est une transposition de $\mathcal{S}_n$, alors $\varphi(\tau)$ est aussi d'ordre 2 et est donc un produit de k transpositions à supports disjoints. On a $|Z(\tau)| = |Z(\varphi(\tau))|$ ce qui se réécrit $2(n-2)! = 2^k k!(n-2k)!$. Puisque $n \neq 6$ on a $k = 1$. D'après a) φ est donc intérieur.

d) Soit $n \geq 5$ tel que $\mathrm{Int}(\mathcal{S}^n) = \mathrm{Aut}(\mathcal{S}_n)$. Montrons que tous les sous-groupes d'indice n de $\mathcal{S}_n$ sont conjugués. Soit H un sous-groupe d'indice n de $\mathcal{S}_n$. L'action transitive de $\mathcal{S}_n$ sur $\mathcal{S}_n/\mathrm{H}$ induit un morphisme de groupes

$$\phi\colon \mathcal{S}_n \to \mathcal{S}_{\mathcal{S}_n/\mathrm{H}} \simeq \mathcal{S}_n.$$

Puisque $\ker\phi$ est un sous-groupe distingué de $\mathcal{S}_n$, $\ker\phi \in \{\{\mathrm{id}\}, \mathcal{A}_n, \mathcal{S}_n\}$. Le groupe $\ker\phi$ agit trivialement sur la classe de H dans $\mathcal{S}_n/\mathrm{H}$, d'où $\ker\phi \subset \mathrm{H}$. Il en résulte que

$\ker\phi = \{\mathrm{id}\}$, *i.e.* que ϕ est injective. Ainsi φ appartient à $\mathrm{Aut}(\mathcal{S}_n)$. Par hypothèse il existe une permutation σ telle que ϕ soit la conjugaison par σ. Or par construction ϕ envoie H sur le stabilisateur d'un point (la classe de H) dans $\mathcal{S}_{\mathcal{S}_n/\mathrm{H}} \simeq \mathcal{S}_n$. Enfin dans $\mathcal{S}_n$ les stabilisateurs d'un point de $\{1, 2, \ldots, n\}$ sont tous conjugués.

e) En utilisant les 5-Sylow de $\mathcal{S}_5$ montrons qu'il existe un sous-groupe H d'indice 6 de $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$. Les théorèmes de Sylow assurent que $\mathcal{S}_5$ admet un ou six 5-Sylow. Comme $\mathcal{A}_5$ est simple $\mathcal{S}_5$ n'admet pas de sous-groupe distingué d'ordre 5 et $\mathcal{S}_5$ admet exactement six 5-Sylow. Notons X l'ensemble des 5-Sylow de $\mathcal{S}_5$. L'action de $\mathcal{S}_5$ sur X par conjugaison est transitive et induit un morphisme de groupes

$$\mu\colon \mathcal{S}_5 \to \mathcal{S}_X \simeq \mathcal{S}_6$$

dont le noyau est trivial (les sous-groupes distingués de $\mathcal{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$). Le groupe $\mathrm{H} = \mu(\mathcal{S}_5) \subset \mathcal{S}_6$ est un sous-groupe d'indice 6 de $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

f) Preuve géométrique, par récurrence sur n : l'espace projectif $\mathbb{P}^{n-1}(\Bbbk)$ est réunion disjointe d'un espace affine de dimension $n-1$ sur $\Bbbk$ (disons $\Bbbk^n$) et d'un hyperplan projectif de dimension $n-2$, *i.e.* isomorphe à un $\mathbb{P}^{n-2}(\Bbbk)$, appelé hyperplan à l'infini. On a donc $\mathbb{P}^{n-1}(\Bbbk) = \Bbbk^{-1} \sqcup \mathbb{P}^{n-2}(\Bbbk)$. On en déduit par récurrence la formule suivante

$$|\mathbb{P}^{n-1}(\mathbb{F}_q)| = q^{n-1} + q^{n-2} + \ldots + q + 1.$$

Autre preuve : le groupe $\mathrm{PGL}(\mathbb{F}_q^n)$ agit fidèlement sur $\mathbb{P}(\mathbb{F}_q^n)$ d'où le morphisme de groupes injectif

$$\varphi\colon \mathrm{PGL}(\mathbb{F}_q^n) \to \mathcal{S}_{\mathbb{P}^{n-1}(\mathbb{F}_q)}$$

Or par définition on a $\mathbb{P}^{n-1}(\mathbb{F}_q) = \mathbb{F}_q^n \smallsetminus \{0\}/\mathbb{F}_q^*$ donc $|\mathbb{P}^{n-1}(\mathbb{F}_q)| = \frac{|\mathbb{F}_q^n|}{|\mathbb{F}_q^*|} = \frac{q^n-1}{q-1}$. Par conséquent il existe un morphisme de groupes injectif

$$\varphi\colon \mathrm{PGL}(\mathbb{F}_q^n) \to \mathcal{S}_{\mathbb{P}^{n-1}(\mathbb{F}_q)}$$

g) Construisons géométriquement un sous-groupe H' d'indice 6 dans $\mathcal{S}_6$ opérant transitivement sur $\{1, 2, \ldots, 6\}$.

Le groupe $\mathrm{H}' = \mathrm{PGL}(2, \mathbb{F}_5)$ vu comme sous-groupe de $\mathcal{S}_6$ par action sur $\mathbb{P}^1(\mathbb{F}_5)$ n'est pas conjugué à $\mathcal{S}_5 = \mathrm{Stab}(6) \subset \mathcal{S}_6$ puisqu'il ne fixe aucun point.

h) Montrons que $\mathrm{Aut}(\mathcal{S}_6) \neq \mathrm{Int}(\mathcal{S}_6)$.

Les d), e) et g) assurent que le groupe $\mathcal{S}_6$ possède au moins un automorphisme extérieur.

Exercice 164 [Simplicité de $\mathcal{A}_n$, $g \geq 5$, version 2]

a) Montrer que le groupe $\mathcal{A}_5$ est simple.

b) Soit $n \geq 3$. Montrer que les 3-cycles engendrent $\mathcal{A}_n$.

c) Montrer que $\mathcal{A}_n$ est simple dès que $n \geq 5$.

d) Montrer que $\mathcal{A}_4$ n'est pas simple.

e) Soit $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathcal{S}_n$. Montrer que

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

f) Soit $n \geq 3$. Montrer que le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$.

g) Soit $n \geq 5$. Montrer que les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.

Éléments de réponse 164

a) 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 $\mathcal{A}_5$ [7]. 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 (resp. 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 $\mathrm{H} = \mathcal{A}_5$.

b) Puisque le groupe $\mathcal{S}_n$ est engendré par les produits de transpositions, le groupe $\mathcal{A}_n$ est engendré par les produits pairs de transpositions et on a

$$(a\ b)(b\ c) = (a\ b\ c)$$

$$(a\ b)(a\ c) = (a\ c\ b)$$

7. Le groupe $\mathcal{A}_5$ est 3 fois transitif sur $\{1, 2, \ldots, 5\}$, *i.e.* si a_1, a_2, a_3 sont distincts et b_1, b_2, b_3 sont distincts il existe $\sigma \in \mathcal{A}_5$ tel que $\sigma(a_i) = b_i$. En effet écrivons

$$\{1, 2, \ldots, 5\} = \{a_1, a_2, \ldots, a_5\} = \{b_1, b_2, \ldots, b_5\}$$

et considérons $\sigma \in \mathcal{S}_5$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1, 2, \ldots, 5$; si σ est paire c'est terminé, sinon nous composons σ avec la transposition $(a_4\ a_5)$.

Soient $\sigma = (a_1\ a_2\ a_3)$, $\tau = (b_1\ b_2\ b_3)$; d'après ce qui précède il existe φ dans $\mathcal{A}_5$ tel que $\varphi(a_i) = b_i$. Alors $\tau = \varphi\sigma\varphi^{-1}$

(notons au passage que tous les 3-cycles sont dans $\mathcal{A}_n$) et

$$(a\ b)(c\ d) = (a\ b)(a\ c)(a\ c)(c\ d) = (a\ c\ b)(a\ c\ d)$$

c) Posons $E = \{1, 2, \ldots, n\}$. Soit $\{\mathrm{id}\} \neq \mathrm{H} \triangleleft \mathcal{A}_n$. Soit $\sigma \in \mathrm{H} \setminus \{\mathrm{id}\}$. 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 $\rho(F) = F$, $\rho_{|E\setminus F} = \mathrm{id}_{|E\setminus F}$. 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

$$\begin{cases} \overline{u}_{|F} = u \\ \overline{u}_{|E\setminus F} = \mathrm{id}_{|E\setminus F} \end{cases}$$

Soit $\mathrm{H}_0 = \{u \in \mathcal{A}(F) \mid \overline{u} \in \mathrm{H}\} = \mathrm{H} \cap \mathcal{A}(F)$. 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 $\mathcal{A}_n$ [8] ils appartiennent tous à H et puisqu'ils engendrent $\mathcal{A}_n$ (cf b)) on a $\mathrm{H} = \mathcal{A}_n$.

d) 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.

---

8. Le groupe $\mathcal{A}_n$ est $(n-2)$ fois transitif sur $\{1, 2, \ldots, n\}$, *i.e.* si $a_1, a_2, \ldots, a_{n-2}$ sont distincts et b_1, b_2, b_{n-2} sont distincts il existe $\sigma \in \mathcal{A}_n$ tel que $\sigma(a_i) = b_i$. En effet 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 $\sigma \in \mathcal{S}_n$ telle que $\sigma(a_i) = b_i$ pour tout $i = 1, 2, \ldots, n$; si σ est paire c'est terminé, sinon nous composons σ avec la transposition $(a_{n-1}\ a_n)$.

Soient $\sigma = (a_1\ a_2\ a_3)$, $\tau = (b_1\ b_2\ \ldots\ b_3)$; d'après ce qui précède il existe φ dans $\mathcal{A}_n$ tel que $\varphi(a_i) = b_i$. Alors $\tau = \varphi\sigma\varphi^{-1}$

e) Calcul direct.

f) Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite d'après e)

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

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.

g) Soit $\mathrm{H} \triangleleft \mathcal{S}_n$. 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 $\mathrm{H} = \mathcal{S}_n$.

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 $\tau \in \mathcal{S}_n$ 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 $\mathcal{S}_n$ d'où $\sigma = \mathrm{id}$ (f)) : contradiction. Il en résulte que $\mathrm{H} = \{\mathrm{id}\}$.

Exercice 165 Soit G un groupe d'ordre 2009.

1. Montrer que $\mathrm{G} \simeq \mathrm{P} \times \mathrm{Q}$ où P est un groupe d'ordre 41 et Q est un groupe d'ordre 49. En déduire que chaque groupe d'ordre 2009 est abélien.
2. Classifier à isomorphisme près tous les groupes d'ordre 2009.
3. Soient P est un groupe d'ordre 41 et Q est un groupe d'ordre 49. Montrer que $\mathrm{Aut}(\mathrm{G}) \simeq \mathrm{Aut}(\mathrm{P}) \times \mathrm{Aut}(\mathrm{Q})$.
4. Montrer que
   a) si Q est cyclique, alors Aut(Q) est cyclique aussi. Quel est l'ordre de Aut(Q) quand Q est cyclique ?
   b) si Q n'est pas cyclique, alors Aut(Q) est isomorphe à $\mathrm{GL}(2, \mathbb{F}_7)$ où $\mathbb{F}_7$ est le corps à 7 éléments. Quel est l'ordre de $\mathrm{GL}(2, \mathbb{F}_7)$?

Éléments de réponse 165

1. Notons que $|\mathrm{G}| = 2009 = 7^2 \times 41$. D'après le premier théorème de Sylow le groupe G possède un 41-Sylow P d'ordre 41 et un 7-Sylow Q d'ordre 49. Notons n_p le nombre de p-Sylow de G. D'après le troisième théorème de Sylow
   - $\diamond$ n_{41} est congru à 1 modulo 41 et divise 49 donc est égal à 1 ;
   - $\diamond$ n_7 est congru à 1 modulo 7 et divise 41 donc est égal à 1.

Nous en déduisons que $\mathrm{P} \triangleleft \mathrm{G}$ et $\mathrm{Q} \triangleleft \mathrm{G}$.

Nous constatons aussi que $\mathrm{P} \cap \mathrm{Q} = \{e\}$, que $\mathrm{G} = \mathrm{PQ}$ et que les deux sous-groupes dans le produit sont distingués dans G. Tout ceci revient à dire $\mathrm{G} \simeq \mathrm{P} \times \mathrm{Q}$.

Reste à montrer que G est abélien. Notons que P et Q sont abéliens puisque P est d'ordre premier et que Q est d'ordre premier au carré. Par ailleurs les éléments de P commutent avec ceux de Q. Ainsi G est abélien.

2. D'après 1. tous les groupes d'ordre 2009 sont abéliens, il suffit donc pour répondre à cette question d'appliquer le théorème de structure pour les groupes abéliens de type fini. Ce théorème montre qu'il y a deux groupe non isomorphes d'ordre 2009

$$\mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z} \qquad \text{et} \qquad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/41\mathbb{Z}$$

soit encore

$$\mathbb{Z}/2009\mathbb{Z} \qquad \text{et} \qquad \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/287\mathbb{Z}$$

3. **Remarque**. Si φ est un automorphisme de G, alors $\varphi(\mathrm{P}) = \mathrm{P}$ et $\varphi(\mathrm{Q}) = \mathrm{Q}$. En effet comme dans tout groupe et pour tout p premier l'image par un morphisme d'un p-élément est un p-élément et que P et Q sont les seuls 41-Sylow et 7-Sylow de G respectivement, $\varphi(\mathrm{P}) \subset \mathrm{P}$ et $\varphi(\mathrm{Q}) \subset \mathrm{Q}$. Comme φ est une bijection ces deux inclusions sont en fait des égalités.

Il découle de la Remarque précédente que la restriction de tout automorphisme $\varphi \in \mathrm{Aut(G)}$ au sous-groupe P (resp. Q) est un automorphisme qu'on appellera φ_{P} (resp. φ_{Q}) de P (resp. Q). Les automorphismes de φ_{P} et φ_{Q} ainsi définis sont uniquement définis puisqu'ils sont les restrictions d'un même automorphisme aux sous-groupes P et Q respectivement.

Considérons l'application

$$\Phi \colon \mathrm{Aut(G)} \to \mathrm{Aut(P)} \times \mathrm{Aut(Q)}, \qquad \varphi \mapsto (\varphi_{\mathrm{P}}, \varphi_{\mathrm{Q}})$$

Remarquons que $\Phi(\mathrm{id}) = (\mathrm{id}, \mathrm{id})$. Soient φ et ϕ deux éléments de Aut(G). Alors d'une part

$$\begin{aligned}(\varphi \circ \phi)_{\mathrm{P}}(\mathrm{P}) &= (\varphi \circ \phi)(\mathrm{P}) \\ &= \varphi(\phi(\mathrm{P})) \\ &= \varphi_{\mathrm{P}}(\phi_{\mathrm{P}}(\mathrm{P})) \\ &= (\varphi_{\mathrm{P}} \circ \phi_{\mathrm{P}})(\mathrm{P})\end{aligned}$$

et d'autre part

$$\begin{aligned}(\varphi \circ \phi)_{\mathrm{Q}}(\mathrm{Q}) &= (\varphi \circ \phi)(\mathrm{Q}) \\ &= \varphi(\phi(\mathrm{Q})) \\ &= \varphi_{\mathrm{Q}}(\phi_{\mathrm{Q}}(\mathrm{Q})) \\ &= (\varphi_{\mathrm{Q}} \circ \phi_{\mathrm{Q}})(\mathrm{Q})\end{aligned}$$

Autrement dit Φ est un morphisme de groupes.

Montrons maintenant que Φ est un isomorphisme.

Commençons par montrer que Φ est injective. Un automorphisme φ de Aut(G) appartient à $\ker\Phi$ si et seulement si $\varphi_{\mathrm{P}} = \mathrm{id}_{\mathrm{P}}$ et $\varphi_{\mathrm{Q}} = \mathrm{id}_{\mathrm{Q}}$. Or tout élément de G s'écrit sous la forme xy avec $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. Ainsi

$$\varphi(xy) = \varphi(x)\varphi(y) = \varphi_{\mathrm{P}}(x)\varphi_{\mathrm{Q}}(y) = \mathrm{id}_{\mathrm{P}}(x)\mathrm{id}_{\mathrm{Q}}(y) = xy.$$

Montrons que Φ est surjective. Soient φ_1 dans Aut(P) et φ_2 dans Aut(Q). Considérons l'application

$$\varphi\colon \mathrm{G} \to \mathrm{G}, \qquad\qquad xy \mapsto \varphi_1(x)\varphi_2(y)$$

avec $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. L'application σ est définie sans ambiguïté puisque G étant la somme directe de P et de Q chacun de ses éléments s'écrit de manière unique comme produit d'un élément de P et d'un autre de Q Montrons que φ est un automorphisme de G dont l'image sous l'action de Φ est (φ_1, φ_2).

Le fait que φ_1 et φ_2 soient des morphismes de groupes entraîne que φ est un morphisme de groupes. Il en est de même pour la surjectivité de φ. Supposons que $\varphi(xy) = 1$ pour $x \in \mathrm{P}$ et $y \in \mathrm{Q}$. La définition de φ implique que $\varphi_1(x)\varphi_2(x) = 1$. Or $\varphi_1(x)$ appartient à P, $\varphi_2(y)$ appartient à Q et $\mathrm{P} \cap \mathrm{Q} = \{e\}$ donc $\varphi_1(x) = \varphi_2(y) = 1$. Puisque φ_1 est un automorphisme de P et φ_2 un automorphisme de Q nous obtenons $x = y = 1$. Comme $\mathrm{G} = \mathrm{PQ}$ tout élément de $\ker\varphi$ s'écrit comme produit d'un $x \in \mathrm{P}$ et d'un $y \in \mathrm{Q}$. Ainsi $\ker\varphi = \{e\}$.

Finalement φ est un automorphisme de G. Il s'ensuit de la définition de φ que $\varphi_{\mathrm{P}} = \varphi_1$ et $\varphi_{\mathrm{Q}} = \varphi_2$. Par conséquent $\Phi(\varphi) = (\varphi_1, \varphi_2)$. Ainsi Φ est surjective.

4. a) Si Q est cyclique, il est isomorphe à $\left(\mathbb{Z}/49\mathbb{Z}, +\right)$. Alors $|\mathrm{Aut(Q)}| = \varphi(49) = 7 \times 6 = 42$ où φ est la fonction indicatrice d'Euler. Comme $42 = 2 \times 3 \times 7$ le théorème chinois assure que Aut(Q) est cyclique d'ordre 42.

   b) Supposons maintenant que Q soit non cyclique. Alors $\mathrm{Q} \simeq \left(\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, +\right)$. Ce dernier groupe peut aussi être considéré comme l'espace vectoriel de dimension 2 sur le corps $\mathbb{F}_7$ avec la base canonique $e_1 = (1,0)$ et $e_2 = (0,1)$. La loi externe induite par $\mathbb{F}_7$ est décrite par les identités

$$\lambda e_1 = \underbrace{(1,0) + (1,0) + \ldots + (1,0)}_{\lambda \text{ fois}} \qquad \lambda e_2 = \underbrace{(0,1) + (0,1) + \ldots + (0,1)}_{\lambda \text{ fois}}$$

   avec $\lambda \in \mathbb{F}_7$, identités qui sont ensuite étendues au groupe tout entier par linéarité. Cette action est définie sans ambiguïté.

Soit $\varphi \in \mathrm{Aut}(\mathrm{Q})$, alors

$$\begin{aligned}\varphi(\lambda e_1) &= \varphi(\underbrace{(1,0)+(1,0)+\ldots+(1,0)}_{\lambda \text{ fois}}) \\ &= \underbrace{\varphi(1,0)+\varphi(1,0)+\ldots+\varphi(1,0)}_{\lambda \text{ fois}} \\ &= \lambda\varphi((1,0)) \\ &= \lambda\varphi(e_1)\end{aligned}$$

et

$$\begin{aligned}\varphi(\lambda e_2) &= \varphi(\underbrace{(0,1)+(0,1)+\ldots+(0,1)}_{\lambda \text{ fois}}) \\ &= \underbrace{\varphi(0,1)+\varphi(0,1)+\ldots+\varphi(0,1)}_{\lambda \text{ fois}} \\ &= \lambda\varphi((0,1)) \\ &= \lambda\varphi(e_2)\end{aligned}$$

Ainsi φ est une application linéaire. Étant bijectif $\varphi \in \mathrm{GL}(2,\mathbb{F}_7)$. Par suite $\mathrm{Aut}(\mathrm{Q}) \subset \mathrm{GL}(2,\mathbb{F}_7)$. L'autre inclusion est claire car chaque bijection linéaire de $\mathbb{F}_7 \times \mathbb{F}_7$ est aussi un automorphisme du groupe $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$. Finalement $|\mathrm{GL}(2,\mathbb{F}_7)| = (7^2-1)(7^2-7)$.

Exercice 166

1. Soit H un sous-groupe distingué de $\mathcal{S}_4$ qui contient un 4-cycle. Montrer que $\mathrm{H} = \mathcal{S}_4$.
2. Soient P_1 et P_2 deux sous-groupes d'ordre 8 de $\mathcal{S}_4$. Supposons que $\mathrm{P}_1 \cap \mathrm{P}_2$ contienne un 4-cycle. Montrer que $\mathrm{P}_1 = \mathrm{P}_2$ (indication : on montre que le normalisateur de $\mathrm{P}_1 \cap \mathrm{P}_2$ dans $\mathcal{S}_4$ contient $\mathrm{P}_1 \cup \mathrm{P}_2$, on considère le sous-groupe engendré par $\mathrm{P}_1 \cup \mathrm{P}_2$ et on utilise 1.)
3. D'après ce qui précède un 4-cycle est dans un unique sous-groupe d'ordre 8 de $\mathcal{S}_4$. En déduire le nombre de sous-groupes d'ordre 8 de $\mathcal{S}_4$ en comptant le nombre de 4-cycles.

Éléments de réponse 166

1. Les sous-groupes distingués de $\mathcal{S}_4$ sont id, $\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, $\mathcal{A}_4$ et $\mathcal{S}_4$. Le seul de ces sous-groupes qui contient un 4-cycle est $\mathcal{S}_4$.
2. Soient P_1 et P_2 deux sous-groupes d'ordre 8 de $\mathcal{S}_4$. Si $\mathrm{P}_1 \neq \mathrm{P}_2$, alors $\mathrm{P}_1 \cap \mathrm{P}_2$ contient un 4-cycle et est donc d'ordre 4. Par conséquent $\mathrm{P}_1 \cap \mathrm{P}_2$ est d'indice 2 dans P_1 donc distingué dans P_1. De même $\mathrm{P}_1 \cap \mathrm{P}_2$ est d'indice 2 dans P_2 donc distingué dans P_2. Par suite le normalisateur N de $\mathrm{P}_1 \cap \mathrm{P}_2$ dans $\mathcal{S}_4$ contient $\mathrm{P}_1 \cup \mathrm{P}_2$. Ainsi N est un sous-groupe de $\mathrm{P}_1 \cap \mathrm{P}_2$ d'ordre un diviseur de 24 qui est un multiple de 8 et > 8. Il en résulte que $|\mathrm{N}| = 24$ et donc que $\mathrm{N} = \mathcal{S}_4$. Ainsi $\mathrm{P}_1 \cap \mathrm{P}_2 \triangleleft \mathcal{S}_4$ et $\mathrm{P}_1 \cap \mathrm{P}_2 = \mathcal{S}_4$: absurde.

3. Déterminons le nombre de 4-cycles de $\mathcal{S}_4$. Un 4-cycle s'écrit de manière unique $(1\ i\ j\ k)$ où i, j et k sont trois entiers distincts parmi $\{2, 3, 4\}$. Il y a donc $3 \times 2 \times 1 =$ six 4-cycles dans $\mathcal{S}_4$. Soit n_2 le nombre de sous-groupes d'ordre 8. Ils sont tous isomorphes car ce sont les 2-Sylow qui sont tous conjugués. Soit k le nombre de 4-cycles dans un 2-Sylow. Nous avons donc $n_2 k = 6$ car un 4-cycle engendre un 2-groupe forcément contenu dans un 2-Sylow. De plus $k \geq 2$ car si c est un 4-cycle dans un sous-groupe P d'ordre 8, alors c^{-1} appartient à P. Si n_2 vaut 1 l'unique 2-Sylow contient un 4-cycle et est distingué dans $\mathcal{S}_4$ donc est $\mathcal{S}_4$: contradiction. Par suite $n_2 = 3$ et $k = 2$.

Exercice 167 Soit $n \geq 5$.

a) Montrer qu'un sous-groupe H d'indice n de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$.

b) En utilisant les théorèmes de Sylow sur les 5-Sylow de $\mathcal{S}_5$ construire un sous-groupe de $\mathcal{S}_6$ d'indice 6 qui n'est pas de la forme

$$\mathcal{S}_6(i) = \{\sigma \in \mathcal{S}_6 \,|\, \sigma(i) = i\}$$

avec $1 \leq i \leq 6$.

Éléments de réponse 167

a) Faire agir $\mathcal{S}_n$ sur $\mathcal{S}_n/\mathrm{H}$ par translation. Comme nous connaissons les sous-groupes distingués de $\mathcal{S}_n$ nous obtenons que le morphisme

$$\varphi\colon \mathrm{H} \to \mathrm{Bij}\left(\mathcal{S}_n/\mathrm{H}\right)$$

est injectif. De plus les éléments de $\varphi(\mathrm{H})$ fixent la classe H d'où le résultat.

b) Le troisième théorème de Sylow assure que $\mathcal{S}_5$ compte six 5-Sylow. Faisons agir $\mathcal{S}_5$ par conjugaison sur l'ensemble X des 5-Sylow. On obtient un morphisme de groupes

$$\varphi\colon \mathcal{S}_5 \to \mathrm{Bij}(X).$$

Le premier théorème de Sylow assure que cette action est transitive. Puisque nous connaissons les sous-groupes distingués de $\mathcal{S}_n$ nous obtenons que φ est injective. Finalement l'image de φ répond à la question.

Exercice 168

1. Soit G un groupe fini. Notons $\mathrm{Syl}_p(\mathrm{G})$ l'ensemble des p-sous-groupes de Sylow de G. Supposons que $|\mathrm{Syl}_p(\mathrm{G})| = m$. Montrons qu'il existe un morphisme non trivial $\rho\colon \mathrm{G} \to \mathcal{S}_m$.
2. Soit G un groupe de cardinal 36. Montrer qu'il n'est pas simple.

Éléments de réponse 168

1. D'après les théorèmes de Sylow l'action par conjugaison
$$\mathrm{G} \times \mathrm{Syl}_p(\mathrm{G}) \to \mathrm{Syl}_p(\mathrm{G}) \qquad\qquad (g, P) \mapsto gPg^{-1}$$
est transitive et détermine donc un morphisme non trivial $\rho\colon \mathrm{G} \to \mathrm{Bij}\big(\mathrm{Syl}_p(\mathrm{G})\big) \simeq \mathcal{S}_m$.

2. Remarquons que $|\mathrm{G}| = 2^2 \times 3^2$. Soit n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_3 divise $2^2 = 4$ et que $n_3 \equiv 1 \bmod 3$, autrement dit que n_3 appartient à $\{1, 4\}$.

   Si $n_3 = 1$, alors G contient un unique 3-Sylow qui est forcément distingué dans G ; en particulier G n'est pas simple.

   Si $n_3 = 4$, alors d'après 1. il existe un morphisme non trivial $\rho\colon \mathrm{G} \to \mathcal{S}_4$. Puisque $|\mathrm{G}| = 36$ ne divise pas $|\mathcal{S}_4| = 24$ ce morphisme n'est pas injectif et $\ker\rho$ est un sous-groupe distingué non trivial et propre de G.

Exercice 169 Soit G un groupe d'ordre 231.

1. Montrer que G admet un seul 7-Sylow et un seul 11-Sylow.
2. Montrer que si P est le 11-Sylow de G, alors P est contenu dans le centre de G (indication : on considère l'action d'un 3-Sylow et l'action d'un 7-Sylow de G sur P par conjugaison).
3. Montrer que G admet un unique sous-groupe d'ordre 77 et qu'il est distingué dans G. Est-ce que ce sous-groupe d'ordre 77 est cyclique ? Justifier.
4. Montrer que G admet un sous-groupe cyclique d'ordre 33.

Éléments de réponse 169

1. Montrons que G admet un seul 7-Sylow et un seul 11-Sylow.

   Soit n_p le nombre de p-Sylow de G.

   Le troisième théorème de Sylow assure que $n_7 \equiv 1 \bmod 7$ et que n_7 divise 33, soit que $n_7 = 1$.

   Le troisième théorème de Sylow assure que $n_{11} \equiv 1 \bmod 11$ et que n_{11} divise 21, soit que $n_{11} = 1$.

2. Montrons que si P est le 11-Sylow de G, alors P est contenu dans le centre de G.

   Comme $n_{11} = 1$ nous avons $\mathrm{P} \lhd \mathrm{G}$. Soit Q un 3-Sylow ; il agit sur P par conjugaison.

   L'équation aux classes s'écrit $|\mathrm{P}| = \sum_i \mathcal{O}_i$. Chaque orbite est de cardinal $\frac{|\mathrm{Q}|}{|\mathrm{Stab}\mathcal{O}_i|}$ et $\frac{|\mathrm{Q}|}{|\mathrm{Stab}\mathcal{O}_i|} \in \{1, 3\}$. C'est 1 si l'orbite est réduite à un point x_i tel que pour tout $g \in \mathrm{Q}$ $gx_ig^{-1} = x_i$. Par suite
$$|\mathrm{P}| = |\mathrm{P}^{\mathrm{Q}}| \bmod 3$$

où

$$\begin{aligned} \mathrm{P}^{\mathrm{Q}} &= \{p \in \mathrm{P} \,|\, \forall\, q \in \mathrm{Q},\, q \cdot p = p\} \\ &= \{p \in \mathrm{P} \,|\, \forall\, q \in \mathrm{Q},\, qpq^{-1} = p\} \\ &= \{p \in \mathrm{P} \,|\, \forall\, q \in \mathrm{Q},\, qp = pq\}. \end{aligned}$$

Comme $|\mathrm{P}^{\mathrm{Q}}|$ divise 11 et $11 \neq 1 \bmod 3$, $\mathrm{P}^{\mathrm{Q}} = \mathrm{P}$, *i.e.* le sous-groupe des éléments qui commutent à tous les éléments de P contient Q. De même les éléments qui commutent à tous les éléments de P contient un 7-Sylow et bien entendu P car P est cyclique. Le sous-groupe des éléments qui commutent à tous les éléments de P est d'ordre un multiple de 3, 7 et 11, c'est donc G.

3. Montrons que G admet un unique sous-groupe d'ordre 77 et qu'il est distingué dans G.

   Commençons par montrer l'existence d'un tel sous-groupe. Soit Q un 7-Sylow. Puisque $\mathrm{P} \triangleleft \mathrm{G}$ et $\mathrm{P} \cap \mathrm{Q} = \{\mathrm{id}\}$, PQ est un sous-groupe de G d'ordre 77. Comme $\mathrm{Q} \triangleleft \mathrm{G}$, $\mathrm{PQ} \triangleleft \mathrm{G}$.

   Montrons maintenant l'unicité. Soit H un sous-groupe de G d'ordre 77. Alors H contient un 11-Sylow et un 7-Sylow. Donc $\mathrm{H} = \mathrm{PQ}$. Soit p dans P d'ordre 11 et soit q dans Q d'ordre 7. Puisque $pq = qp$ (rappelons que p appartient à P et que $\mathrm{P} \subset Z(\mathrm{G})$) pq est d'ordre 77 donc PQ est cyclique.

4. Montrons que G admet un sous-groupe cyclique d'ordre 33.

   Soit R un 3-Sylow. Alors PR est un sous-groupe distingué de G d'ordre 33. En effet soient p d'ordre 11 dans P et r d'ordre 3 dans R. Puisque P est contenu dans le centre de G nous avons $pr = rp$ et pr est d'ordre 33.

Exercice 170 Rappelons que D_{2n} désigne le groupe à $2n$ éléments des isométries d'un polygone régulier à n côtés. On se propose de montrer que si G est un groupe de cardinal 70, alors G est isomorphe à l'un des groupes suivants

$$\mathbb{Z}/70\mathbb{Z} \qquad \mathrm{D}_{70} \qquad \mathrm{D}_{10} \times \mathbb{Z}/7\mathbb{Z} \qquad \mathrm{D}_{14} \times \mathbb{Z}/5\mathbb{Z}$$

Partie I

Soit G un groupe. Notons n_p le nombre de p-sous-groupes de Sylow de G et $o(n)$ le nombre d'éléments d'ordre n.

1. Soit p un premier impair. Montrer pourquoi un groupe de cardinal $2p$ est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou D_{2p}.
2. Que valent n_2 et n_p lorsque $\mathrm{G} = \mathrm{D}_{2p}$?

   Si S et T sont deux sous-groupes de G tels que $\mathrm{S} \cap \mathrm{T} = \{e\}$, alors on considère $\mathrm{ST} = \{st \,|\, s \in \mathrm{S},\, t \in \mathrm{T}\}$.
3. Montrer que si S est distingué dans G, alors $\mathrm{ST} = \mathrm{TS}$ est un sous-groupe de cardinal $|\mathrm{S}||\mathrm{T}|$.
4. Montrer que si S et T sont distingués dans G, alors ST est un sous-groupe isomorphe à $\mathrm{S} \times \mathrm{T}$. En déduire qu'un groupe de cardinal 35 est cyclique.

Partie II

Soit G un groupe de cardinal 70.

1. Exprimer $o(p)$ en terme de n_p et énumérer les valeurs possibles a priori pour n_2, n_5 et n_7.
2. Déduire de ce qui précède que G possède un sous-groupe K d'ordre 35. Montrer que K est distingué dans G.
3. En déduire que G contient un sous-groupe distingué $\mathrm{H} \simeq \mathbb{Z}/35\mathbb{Z}$.
4. Calculer n_2 dans le cas des quatre groupes

   $\mathbb{Z}/70\mathbb{Z}$ $\qquad$ D_{70} $\qquad$ $\mathrm{D}_{10} \times \mathbb{Z}/7\mathbb{Z}$ $\qquad$ $\mathrm{D}_{14} \times \mathbb{Z}/5\mathbb{Z}$

   En déduire qu'ils ne sont pas isomorphes.
5. Inversement montrer en considérant les valeurs possibles de n_2 que G est isomorphe à l'un des quatre groupes

   $\mathbb{Z}/70\mathbb{Z}$ $\qquad$ D_{70} $\qquad$ $\mathrm{D}_{10} \times \mathbb{Z}/7\mathbb{Z}$ $\qquad$ $\mathrm{D}_{14} \times \mathbb{Z}/5\mathbb{Z}$

Éléments de réponse 170

Partie I

1. Si $|\mathrm{G}| = 2p$, les théorèmes de Sylow assurent l'existence d'un sous-groupe distingué H de cardinal p donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et un sous-groupe d'ordre 2 disons $\mathrm{K} = \{e, s\}$. Soit r un générateur de H. Alors srs^{-1} appartient à H donc est égal à r^a pour un certain a. Alors d'une part $sr^as^{-1} = r^{a^2}$ et d'autre part $r = s^{-1}r^as$ qui se réécrit $r = sr^as^{-1}$ puisque $s^2 = e$. On en déduit que $r^{a^2} = r$ et donc $a^2 \equiv 1 \bmod p$ et donc $a \equiv \pm 1 \bmod p$. Si $a = 1$, l'élément s commute avec r donc rs est d'ordre $2p$ et $\mathrm{G} \simeq \mathbb{Z}/2p\mathbb{Z}$. Si $a = -1$, alors $srs^{-1} = r^{-1}$ ce qui caractérise le groupe diédral.
2. Nous avons $n_p = 1$ (il n'y a qu'un seul p Sylow qui est distingué dans G) et $n_2 = p$ (en effet il y a p éléments d'ordre 2, les symétries).
3. Si S est distingué dans G, alors pour tout $t \in \mathrm{G}$ nous avons $\mathrm{S}t = t\mathrm{S}$ d'où l'égalité $\mathrm{ST} = \mathrm{TS}$. Si $g = st$ et $g' = s't'$, alors $gg' = sts't' = s(ts't^{-1})tt'$ appartient à ST. Si $g = st$, alors $g^{-1} = t^{-1}s^{-1}$ appartient à $\mathrm{TS} = \mathrm{ST}$. Par suite ST est bien un sous-groupe de G.

   Montrons que l'application

   $$\phi\colon \mathrm{S} \times \mathrm{T} \to \mathrm{G} \qquad\qquad (s,t) \mapsto st$$

   est injective. Soient (s,t) et (s',t') dans $\mathrm{S} \times \mathrm{T}$ tels que $\phi(s,t) = \phi(s',t')$. L'égalité $\phi(s,t) = \phi(s',t')$ se réécrit $st = s't'$ dont on déduit $(s')^{-1}s = t't^{-1}$. En particulier $(s')^{-1}s = t't^{-1}$ est un élément de $\mathrm{S} \cap \mathrm{T}$; comme $\mathrm{S} \cap \mathrm{T} = \{e\}$, on obtient que $(s')^{-1}s = t't^{-1} = e$, soit que $s = s'$ et $t = t'$. Ainsi l'application ϕ est injective ; de plus son image est par définition ST. Par conséquent $|\mathrm{S} \times \mathrm{T}| = |\mathrm{ST}|$. Mais $|\mathrm{S} \times \mathrm{T}| = |\mathrm{S}| \cdot |\mathrm{T}|$ d'où $|\mathrm{S}| \cdot |\mathrm{T}| = |\mathrm{ST}|$.

4. D'une part $sts^{-1}t^{-1} = s(ts^{-1}t^{-1})$ donc $sts^{-1}t^{-1}$ appartient à S (par hypothèse $\mathrm{S} \lhd \mathrm{G}$), d'autre part $sts^{-1}t^{-1} = (sts^{-1})t^{-1}$ donc $sts^{-1}t^{-1}$ appartient à T (par hypothèse $\mathrm{T} \lhd \mathrm{G}$). Ainsi $sts^{-1}t^{-1}$ appartient à $\mathrm{S} \cap \mathrm{T} = \{e\}$, donc $sts^{-1}t^{-1} = e$ autrement dit s et t commutent. Ceci entraîne que ϕ est un morphisme ; en effet

$$\phi\big((s,t)\cdot(s',t')\big) = \phi(ss',tt') = ss'tt' = sts't' = \phi(s,t)\phi(s',t').$$

D'après ce qui précède $\phi\colon \mathrm{S}\times\mathrm{T} \to \mathrm{ST}$ est donc un isomorphisme.

Si $|\mathrm{G}| = 35$ le groupe contient un unique 5-Sylow $\mathrm{S} \simeq \mathbb{Z}/5\mathbb{Z}$ et un unique 7-Sylow $\mathrm{T} \simeq \mathbb{Z}/7\mathbb{Z}$. Comme ils sont tous les deux distingués dans G d'intersection triviale nous obtenons d'après les questions précédentes que

$$\mathrm{ST} = \mathrm{S}\times\mathrm{T} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

Enfin $|\mathrm{ST}| = 35 = |\mathrm{G}|$ conduit à $\mathrm{ST} = \mathrm{G}$.

Partie II

Soit G un groupe de cardinal 70.

1. Comme les p-Sylow sont de cardinal p (pour $p = 2$, 5 ou 7) ils sont deux à deux disjoints hormis l'élément e bien sûr qui est présent dans chacun d'entre eux. Ainsi si H_1, H_2, …, H_{n_p} désignent les p-Sylow de G nous avons

$$\Big|\bigcup_{i=1}^{n_p} \mathrm{H}_i \smallsetminus \{e\}\Big| = n_p(p-1)$$

Par ailleurs d'après les théorèmes de Sylow $\bigcup_{i=1}^{n_p} \mathrm{H}_i \smallsetminus \{e\}$ est l'ensemble des éléments d'ordre p. Ainsi $o(p) = n_p(p-1)$.

D'après les théorèmes de Sylow n_7 divise 10 et $n_7 \equiv 1 \bmod 7$ donc $n_7 = 1$.

D'après les théorèmes de Sylow n_5 divise 14 et $n_5 \equiv 1 \bmod 5$ donc $n_5 = 1$.

D'après les théorèmes de Sylow n_2 divise 35 et $n_2 \equiv 1 \bmod 2$ donc $n_2 \in \{1, 5, 7, 35\}$.

2. Soient S l'unique 5-Sylow de G et T l'unique 7-Sylow de G. Ils sont tous les deux distingués dans G donc $\mathrm{K} = \mathrm{ST}$ est un sous-groupe de cardinal 35 qui est automatiquement distingué dans G (on peut aussi remarquer que $[\mathrm{G} : \mathrm{K}] = 2$ donc K est distingué dans G).

3. D'après les questions qui précèdent nous avons

$$\mathrm{K} = \mathrm{ST} \simeq \mathrm{S}\times\mathrm{T} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/35\mathbb{Z}.$$

4. Désignons par $n_2(\mathrm{G})$ le nombre de 2-Sylow du groupe G.

Le groupe $\mathbb{Z}/70\mathbb{Z}$ étant abélien nous avons $n_2\big(\mathbb{Z}/70\mathbb{Z}\big) = 1$.

Le groupe D_{2n} contient n symétries d'ordre 2. Par conséquent $n_2(\mathrm{D}_{70}) = 35$. De plus si B est de cardinal impair, un 2-SYLOW de A×B est contenu dans A×$\{e\}$ donc $n_2(\mathrm{A}\times\{e\}) = n_2(\mathrm{A})$; par suite

$$n_2\Big(\mathrm{D}_{14} \times {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}\Big) = n_2(\mathrm{D}_{14}) = 7 \qquad\qquad n_2\Big(\mathrm{D}_{10} \times {}^{\mathbb{Z}}\!/_{7\mathbb{Z}}\Big) = n_2(\mathrm{D}_{10}) = 5.$$

5. Choisissons un générateur r de $\mathrm{ST} = \mathrm{K} \simeq {}^{\mathbb{Z}}\!/_{35\mathbb{Z}}$ et s un élément d'ordre 2. Posons $\mathrm{R} = \{e, s\}$. Observons que $srs^{-1} = r^a$ avec $a \in {}^{\mathbb{Z}}\!/_{35\mathbb{Z}}$ et $a^2 = 1$. Comme $a^2 \equiv 1 \bmod 35$ équivaut par le Lemme chinois à $a^2 \equiv 1 \bmod 5$ et $a^2 \equiv 1 \bmod 7$ on a quatre solutions :
   — $a \equiv 1 \bmod 35$,
   — $a \equiv -1 \bmod 35$,
   — $a \equiv 1 \bmod 5$ et $a \equiv -1 \bmod 7$,
   — $a \equiv -1 \bmod 5$ et $a \equiv 1 \bmod 7$.
   Intéressons-nous à chacune de ces éventualités :
   — si $a \equiv 1 \bmod 35$, alors R commute avec K et $\mathrm{G} \simeq \mathrm{K} \times \mathrm{R} \simeq {}^{\mathbb{Z}}\!/_{35\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \simeq {}^{\mathbb{Z}}\!/_{70\mathbb{Z}}$.
   — si $a \equiv -1 \bmod 35$, alors s commute avec S mais pas avec T ainsi S commute avec T et R donc avec le sous-groupe RT qui est d'ordre 14. Puisqu'il est non abélien RT doit être isomorphe à D_{14}. Par conséquent $\mathrm{G} \simeq \mathrm{S} \times \mathrm{RT} \simeq {}^{\mathbb{Z}}\!/_{5\mathbb{Z}} \times \mathrm{D}_{14}$.
   — le cas $a \equiv 1 \bmod 5$ et $a \equiv -1 \bmod 7$ se traite de la même façon que le cas précédent et on obtient $\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{7\mathbb{Z}} \times \mathrm{D}_{10}$.
   — si $a \equiv -1 \bmod 5$ et $a \equiv 1 \bmod 7$ alors $\mathrm{G} \simeq \mathrm{D}_{70}$.

5.6. Groupes et géométrie

Exercice 171 Montrer que le groupe affine $\mathrm{GA}(\mathcal{E})$ de l'espace affine dont l'espace vectoriel associé est E est isomorphe à un produit semi-direct de E et $\mathrm{GL}(E)$.

Éléments de réponse 171 Fixons un point O de $\mathcal{E}$. Soit $\mathrm{GA}_O(\mathcal{E})$ le sous-groupe de $\mathrm{GA}(\mathcal{E})$ formé des transformations affines qui laissent fixe le point O.

Soit $\mathrm{T}(\mathcal{E})$ le groupe des translations.

Le groupe $\mathrm{T}(\mathcal{E})$ est distingué dans $\mathrm{GA}(\mathcal{E})$. En effet soit $f \in \mathrm{GA}(\mathcal{E})$ une transformation affine ; notons $\overrightarrow{f}$ sa partie linéaire. Pour tout point M de $\mathcal{E}$ nous avons

$$f(M + \overrightarrow{u}) = f(M) + \overrightarrow{f}(\overrightarrow{u})$$

i.e.

$$(f \circ t_{\overrightarrow{u}})(M) = (t_{\overrightarrow{f}(\overrightarrow{u})} \circ f)(M)$$

ou encore

$$f \circ t_{\overrightarrow{u}} \circ f^{-1} = t_{\overrightarrow{f}(\overrightarrow{u})}.$$

Notons qu'une translation qui laisse fixe un point est égale à l'identité ; autrement dit $\mathrm{T}(\mathcal{E}) \cap \mathrm{GA}_O(\mathcal{E}) = \{\mathrm{id}\}$.

Enfin toute transformation affine est composée d'une transformation affine laissant fixe le point O et d'une translation, c'est-à-dire $\mathrm{T}(\mathcal{E})\mathrm{GA}_O(\mathcal{E}) = \mathrm{GA}(\mathcal{E})$. En effet une transformation affine $f \in \mathrm{GA}(\mathcal{E})$ s'écrit

$$f = t_{\overrightarrow{Of(O)}} \circ \left(t_{\overrightarrow{f(O)O}} \circ f \right)$$

et $t_{\overrightarrow{f(O)O}} \circ f$ laisse fixe le point O.

Le groupe $\mathrm{GA}(\mathcal{E})$ est donc le produit semi-direct du sous-groupe des translations par le sous-groupe laissant fixe O. [9]

Observons maintenant que l'action du sous-groupe $\mathrm{GA}_O(\mathcal{E})$ sur le sous-groupe distingué $\mathrm{T}(\mathcal{E})$ est donnée par la formule

$$f \circ t_{\overrightarrow{u}} \circ f^{-1} = t_{\overrightarrow{f}(\overrightarrow{u})}$$

Comme $\mathrm{T}(\mathcal{E})$ est isomorphe à E et comme $\mathrm{GA}_O(\mathcal{E})$ est isomorphe à $\mathrm{GL}(E)$ via l'application $f \mapsto \overrightarrow{f}$ nous avons

$$\mathrm{GA}(\mathcal{E}) \simeq E \rtimes_\rho \mathrm{GL}(E)$$

où $\rho(f) = \overrightarrow{f}$. Le produit de deux éléments de ce produit semi-direct

$$(\overrightarrow{u}, f)(\overrightarrow{v}, g) = (\overrightarrow{u} + f(\overrightarrow{v}), fg).$$

Exercice 172 Déterminer la composée de deux symétries vectorielles orthogonales planes.

Déterminer l'ordre de cette composée.

Éléments de réponse 172 Le déterminant d'une symétrie orthogonale est -1 ; la composée $r = s's$ de deux telles symétries s et s' est donc une isométrie directe, c'est-à-dire une rotation.

Déterminons l'angle θ de la rotation à partir des axes respectifs $\mathbb{R}\overrightarrow{u}$ et $\mathbb{R}\overrightarrow{u'}$ ($\overrightarrow{u}$ et $\overrightarrow{u'}$ unitaires) des symétries s et s'. Pour cela il suffit de déterminer l'image de $\overrightarrow{u}$ par r, ou plutôt l'angle $(\overrightarrow{u}, r(\overrightarrow{u}))$. Puisque $s(\overrightarrow{u}) = \overrightarrow{u}$ nous avons $r(\overrightarrow{u}) = s'(\overrightarrow{u})$ donc l'angle $(\overrightarrow{u}, r(\overrightarrow{u}))$ est aussi l'angle $(\overrightarrow{u}, s'(\overrightarrow{u}))$. Comme une symétrie renverse l'orientation nous avons

$$(\overrightarrow{u}, \overrightarrow{u'}) = -(s'(\overrightarrow{u}), s'(\overrightarrow{u'}))$$

d'où

$$(\overrightarrow{u}, \overrightarrow{u'}) = (s'(\overrightarrow{u'}), s'(\overrightarrow{u})).$$

Puisque $\overrightarrow{u'}$ appartient à l'axe de s' nous obtenons

$$(\overrightarrow{u}, \overrightarrow{u'}) = (\overrightarrow{u'}, s'(\overrightarrow{u})).$$

---

9. Soit G un groupe. Soient N et H deux sous-groupes de G tels que
   - $\mathrm{N} \lhd \mathrm{G}$,
   - $\mathrm{N} \cap \mathrm{H} = \{e\}$,
   - $\mathrm{G} = \mathrm{NH}$.

Alors $\mathrm{G} \simeq \mathrm{N} \rtimes \mathrm{H}$.

Il en résulte que

$$\theta = (\overrightarrow{u}, s'(\overrightarrow{u})) = (\overrightarrow{u}, \overrightarrow{u'}) + (\overrightarrow{u'}, s'(\overrightarrow{u})) = 2(\overrightarrow{u}, \overrightarrow{u'})$$

Notons que $\overrightarrow{u}$ peut être remplacé par $-\overrightarrow{u}$ ou $\overrightarrow{u'}$ par $-\overrightarrow{u'}$. L'angle $(\overrightarrow{u}, \overrightarrow{u'})$ n'est donc défini qu'à π près à partir de la donnée des deux symétries (ce n'est pas étonnant : la seule donnée intrinsèque est l'angle de droites $(\mathbb{R}\overrightarrow{u}, \mathbb{R}\overrightarrow{u'})$). Mais grâce à la multiplication par 2 l'angle θ se trouve être bien défini à 2π près.

Déterminons l'ordre de cette composée. L'ordre d'une rotation est infini si l'angle de la rotation n'est pas égal à $\frac{2k\pi}{n}$ pour n et k entiers. L'ordre de la rotation d'angle $\frac{2k\pi}{n}$ pour n et k premiers entre eux est n.

Exercice 173 Montrer que toute rotation plane se décompose en le produit de deux symétries.

Que pouvons-nous dire pour les rotations de l'espace ?

Éléments de réponse 173 Montrons que toute rotation plane se décompose en le produit de deux symétries.

D'après l'exercice précédent on peut décomposer toute rotation plane d'angle θ en le produit de deux symétries orthogonales : l'axe de la première est choisi au hasard, l'axe de la seconde fait un angle de $\frac{\theta}{2}$ avec la première.

Il y a un résultat analogue pour une rotation de l'espace d'axe $\mathbb{R}u$ et d'angle θ. Elle se décompose en le produit de deux symétries orthogonales par rapport à deux plans vectoriels contenant $\mathbb{R}u$ et qui font un angle égal à $\frac{\theta}{2}$ entre eux : la restriction de la rotation au plan vectoriel orthogonal à $\mathbb{R}u$ est une rotation plane.

Exercice 174 [Le groupe diédral]

Considérons un polygone régulier ayant un sommet P de coordonnées $(1, 0)$ et centré à l'origine du repère.

1. Déterminer le groupe D_6 des isométries du plan qui conservent un triangle équilatéral. Établir la table de D_6.
2. Déterminer le groupe D_8 des isométries du plan qui conservent carré. Déterminer les ordres des éléments de D_8. Établir la table de D_8.
3. Déterminer le groupe D_{2n} des isométries du plan qui conservent un polygone régulier à n côtés.
4. Soit $n \geq 2$ un entier. Considérons le groupe $\mathbb{Z}/n\mathbb{Z}$ et un générateur $[a]$ de ce groupe. Soit $\tau \in \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ défini par $\tau([c]) = -[c]$.

   Soit $\rho\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ défini par

   $$\rho([0]) = \mathrm{id} \qquad\qquad \rho([1]) = \tau.$$

   Montrer que D_{2n} est isomorphe au produit semi-direct de $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$ le long de ρ.

Éléments de réponse 174 Notons O l'origine de $\mathbb{R}^2$. Munissons $\mathbb{R}^2$ de l'orientation géométrique.

1. Commençons par déterminer les isométries (*i.e.* les symétries axiales et les rotations centrées en O) qui fixent un des sommets du triangle équilatéral. En dehors de l'identité il y a la symétrie d'axe la médiane issue du sommet considéré. Comme il y a trois sommets on obtient ainsi trois symétries dans D_6.

   Par ailleurs il y a les deux rotations centrées en O d'angle $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$.

   En ajoutant l'identité cela fait déjà 6 éléments dans D_6. Or une isométrie affine qui conserve le triangle équilatéral induit une permutation sur l'ensemble des sommets du triangle équilatéral qui sont au nombre de trois. Par suite D_6 est un sous-groupe de $\mathcal{S}_3$.

   Il y a $3! = 6$ permutations de ces trois sommets donc $\mathrm{D}_6 \simeq \mathcal{S}_3$ et nous avons listé tous les éléments de D_6.

   Désignons par A_1, A_2 et A_3 les sommets du triangle équilatéral. Pour $1 \leq i \leq 3$ notons s_i la symétrie qui laisse le point A_i fixe, r_1 la rotation d'angle $\frac{2\pi}{3}$ et $r_2^2 = r_1$ la rotation d'angle $\frac{4\pi}{3}$.

   La table de $\mathrm{D}_6 \simeq \mathcal{S}_3$ est la suivante

	id	s_1	s_2	s_3	r_1	r_2
id	id	s_1	s_2	s_3	r_1	r_2
s_1	s_1	id	r_1	r_2	s_2	s_3
s_2	s_2	r_2	id	r_1	s_3	s_1
s_3	s_3	r_1	r_2	id	s_1	s_2
r_1	r_1	s_3	s_1	s_2	r_2	id
r_2	r_2	s_2	s_3	s_1	id	r_1

2. Notons qu'une isométrie qui préserve un carré envoie chaque sommet sur un sommet, chaque côté sur un côté et chaque diagonale sur une diagonale.

   Déterminons les isométries du plan qui conservent le carré $[A_1, A_2, A_3, A_4]$ et qui laissent fixe le point A_1. De telles isométries laissent donc fixe la diagonale $[A_1, A_3]$ et donc le point A_3. Il n'y en a donc qu'une non triviale : la symétrie par rapport à cette diagonale.

   Cherchons les isométries du plan qui conservent le carré $[A_1, A_2, A_3, A_4]$ et qui envoient le point A_1 sur le point A_2. De telles isométries envoient donc la diagonale $[A_1, A_3]$ sur la diagonale $[A_2, A_4]$. Il en résulte que A_3 a pour image A_4. Il y a deux telles isométries
   - ◇ la symétrie par rapport à la médiatrice commune de $[A_1, A_2]$ et $[A_3, A_4]$ qui envoie A_4 sur A_3 et A_2 sur A_1 ;
   - ◇ la rotation d'angle $\frac{3\pi}{2}$ qui envoie A_4 sur A_1 et A_2 sur A_3.

   Cherchons les isométries du plan qui conservent le carré $[A_1, A_2, A_3, A_4]$ et qui envoient le point A_1 sur le point A_4. De telles isométries envoient donc la diagonale $[A_1, A_3]$ sur la diagonale $[A_2, A_4]$; le point A_3 a donc pour image le point A_2. Il y en a donc deux :

◇ la symétrie par rapport à la médiatrice commune de $[A_1, A_4]$ et $[A_2, A_3]$ qui envoie A_4 sur A_1 et A_2 sur A_3 ;
◇ la rotation d'angle $\frac{\pi}{2}$ qui envoie A_4 sur A_3 et A_2 sur A_1.

Restent les isométries qui envoient A_1 sur A_3 en conservant le carré. La diagonale $[A_2, A_4]$ est alors préservée. Il y en a deux :
◇ la symétrie par rapport à la diagonale $[A_2, A_4]$;
◇ la rotation d'angle π.

Notations :
◇ r_1 la rotation d'angle $\frac{\pi}{2}$;
◇ r_2 la rotation d'angle π ;
◇ r_3 la rotation d'angle $\frac{3\pi}{2}$;
◇ s_{12} la symétrie d'axe la médiatrice de $[A_1, A_2]$;
◇ s_{23} la symétrie d'axe la médiatrice de $[A_2, A_3]$;
◇ s_{13} la symétrie d'axe la médiatrice de $[A_1, A_3]$;
◇ s_{24} la symétrie d'axe la médiatrice de $[A_2, A_4]$.

Chacune des symétries est d'ordre 2 ; r_1 et r_3 sont d'ordre 4 et r_2 est d'ordre 2.

La table de D_8 est

	id	r_1	r_2	r_3	s_{12}	s_{23}	s_{13}	s_{24}
id	id	r_1	r_2	r_3	s_{12}	s_{23}	s_{13}	s_{24}
r_1	r_1	r_2	r_3	id	s_{13}	s_{24}	s_{23}	s_{12}
r_2	r_2	r_3	id	r_1	s_{23}	s_{12}	s_{24}	s_{13}
r_3	r_3	id	r_1	r_2	s_{24}	s_{13}	s_{12}	s_{23}
s_{12}	s_{12}	s_{24}	s_{23}	s_{13}	id	r_2	r_3	r_1
s_{23}	s_{23}	s_{13}	s_{12}	s_{24}	r_2	id	r_1	r_3
s_{13}	s_{13}	s_{12}	s_{24}	s_{23}	r_1	r_3	id	r_2
s_{24}	s_{24}	s_{23}	s_{13}	s_{12}	r_3	r_1	r_2	id

3. Soit P un polygone régulier à n côtés. Numérotons les sommets de P_n dans le sens trigonométrique, il s'écrit $[A_1, A_2, \ldots, A_n]$.

Pour une isométrie conservant le polygone chaque sommet va sur un sommet, chaque côté va sur un côté donc si A_1 a pour image A_k alors A_2 a pour image soit A_{k-1} soit A_{k+1}. Dans le premier cas l'isométrie est une symétrie (car ce n'est pas un élément de $\mathrm{SO}(2, \mathbb{R})$), dans le second cas l'isométrie est une rotation d'angle $\frac{2k\pi}{n}$. Les axes de symétrie possibles sont
◇ si n est pair les droites déterminées par un sommet quelconque et le centre (il y en a $\frac{n}{2}$) et les droites déterminées par les médiatrices des côté (il y en a $\frac{n}{2}$) ;
◇ si n est impair, les droites déterminées par un sommet quelconque et le centre qui sont les droites déterminées par les médiatrices des côtés (il y en a n).

Soit r la rotation d'angle $\frac{2\pi}{n}$ et soit s l'une des symétries de D_{2n}. Le groupe D_{2n} est engendré par s et r.

4. Le produit semi-direct $\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$ est d'ordre $2n$. Si $\beta = ([0],[1])$ et $\alpha = ([1],[0])$, alors
   - $\beta^2 = ([0],[0])$ où $([0],[0])$ est l'élément neutre du produit semi-direct, *i.e.* β est d'ordre 2 ;
   - $\alpha^n = ([0],[0])$, *i.e.* α est d'ordre n ;
   - et

$$\beta\alpha\beta^{-1} = ([0],[1])([1],[0])([0],[1]) = ([0],[1])([1],[1]) = ([n-1],[0]) = \alpha^{n-1}.$$

En effet, rappel : soient N et H deux groupes. Soit Aut(N) le groupe des automorphismes de groupe de N. Soit $\varphi\colon \mathrm{H} \to \mathrm{Aut(N)}$ un morphisme qui définit une opération de H sur N par la formule $h \cdot n = \varphi(h)(n)$.

On définit sur l'ensemble produit $\mathrm{N} \times \mathrm{H}$ une loi par

$$(n,h)(n',h') = \big(n(h \cdot n'), hh'\big).$$

Alors $\mathrm{N} \times \mathrm{H}$, muni de cette loi, est un groupe appelé *produit semi-direct* de N par H relativement à φ et noté $\mathrm{N} \rtimes_\varphi \mathrm{H}$ ou plus simplement $\mathrm{N} \rtimes \mathrm{H}$.

Ici $\mathrm{H} = \mathbb{Z}/2\mathbb{Z}$, $\mathrm{N} = \mathbb{Z}/n\mathbb{Z}$ et $\varphi = \rho$. Par suite

$$(n,h)(n',h') = \big(n + \rho(h)(n'), h + h'\big).$$

et

$$\begin{aligned}
([0],[1])([1],[0])([0],[1]) &= ([0],[1])([1] + \rho([0])([0]), [0]+[1]) \\
&= ([0],[1])([1],[1]) \\
&= ([0] + \rho([1])([1]), [1]+[1]) \\
&= (\rho([1])([1]), [2]) \\
&= ([0] + (-[1]), [0]) \\
&= ([n-1],[0])
\end{aligned}$$

Nous avons

$$\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z} = \{e,\, \alpha,\, \ldots,\, \alpha^{n-1},\, \beta,\, \beta\alpha,\, \beta\alpha^2,\, \ldots,\, \beta\alpha^{n-1}\}.$$

Rappelons que

$$\mathrm{D}_{2n} = \langle r,\, s \,|\, r^n = s^2 = rsrs = \mathrm{id}\rangle.$$

Soit φ l'homomorphisme défini par

$$\mathrm{D}_{2n} \to \mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z} \qquad \begin{cases} s \mapsto \beta \\ r \mapsto \alpha \end{cases}$$

Par construction c'est un isomorphisme.

Exercice 175 Soit $\tau \in \mathrm{Aut}\Big(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\Big)$ défini par $\tau([a],[b]) = ([b],[a])$.

Soit $\rho\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right)$ défini par

$$\rho([0]) = \mathrm{id} \qquad\qquad \rho([1]) = \tau.$$

Montrer que D_8 est isomorphe au produit semi-direct de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$ le long de ρ.

Éléments de réponse 175 Décrivons le produit semi-direct

$$\mathrm{G} = \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$$

Le groupe G est engendré par $\beta = ([0],[0],[1])$ qui est d'ordre 2, $\alpha_1 = ([1],[0],[0])$ et $\alpha_2 = ([0],[1],[0])$. Nous avons $\beta\alpha_1 = \alpha_2\beta$, $\beta\alpha_2 = \alpha_1\beta$. En effet vérifions la première relation : d'une part

$$\begin{aligned}
\beta\alpha_1 &= ([0],[0],[1])([1],[0],[0]) \\
&= (([0],[0]) + \tau([1])([1],[0]), [1]+[0]) \\
&= (([0],[0]) + ([0],[1]), [1]+[0]) \\
&= ([0],[1],[1])
\end{aligned}$$

et d'autre part

$$\begin{aligned}
\alpha_2\beta &= ([0],[1],[0])([0],[0],[1]) \\
&= (([0],[1]) + \tau([0])([0],[0]), [0]+[1]) \\
&= (([0],[1]) + ([0],[0]), [0]+[1]) \\
&= ([0],[1],[1])
\end{aligned}$$

Le groupe G est d'ordre 8 et

$$\mathrm{G} = \{e,\ \alpha_1,\ \alpha_2,\ \alpha_1\alpha_2,\ \beta,\ \beta\alpha_1,\ \beta\alpha_2,\ \beta\alpha_1\alpha_2\}.$$

Isomorphisme entre D_8 et G : l'image d'un élément d'ordre 2 est d'ordre 2, l'image d'un élément d'ordre 4 est d'ordre 4. Les éléments d'ordre 4 de G sont $\beta\alpha_1$ et $\beta\alpha_2$. Soit φ l'homomorphisme entre ces deux groupes qui envoie r sur $\beta\alpha_1$. Alors $\varphi(r^3) = \beta\alpha_2$ et $\varphi(r^2) = \alpha_1\alpha_2$. Prenons $\varphi(s) = \beta$. Nous pouvons vérifier qu'on a bien un isomorphisme.

Exercice 176 Déterminer le groupe des isométries du plan qui conservent un rectangle non carré.

Établir la table de ce groupe.

Éléments de réponse 176 Considérons un rectangle $ABCD$ tel que "A est le coin en haut à gauche, B le coin en haut à droite, C le coin en bas à droite, D le coin en bas à gauche, $[AB]$ et $[CD]$ sont les longueurs et $[BC]$ et $[AD]$ les largeurs." Prenons pour origine du repère le centre du rectangle.

Une isométrie qui conserve le rectangle laisse fixe le centre du rectangle donc le groupe recherché est isomorphe à un sous-groupe du groupe des isométries vectorielles. Par ailleurs une isométrie qui conserve le rectangle envoie chaque diagonale sur une diagonale.

Une isométrie qui conserve le rectangle et laisse fixe le sommet A laisse fixe la diagonale $[AC]$ et donc le sommet C et tous les autres sommets. Ainsi la seule isométrie qui conserve le rectangle et laisse fixe le sommet A est l'identité. Il en est de même lorsque l'on remplace A par B (resp. C, resp. D). Une isométrie qui conserve le rectangle et qui n'est pas l'identité ne fixe donc aucun sommet.

- ◇ ou bien A a pour image B alors C a pour image D et cette isométrie est la symétrie s_1 d'axe la médiatrice de $[AB]$;
- ◇ ou bien A a pour image D, alors B a pour image C et cette isométrie est la symétrie s_2 d'axe la médiatrice de $[AD]$;
- ◇ ou bien A et C sont échangés et cette isométrie est la rotation r d'angle π.

On a donc un groupe d'ordre 4, abélien, dont la table est :

	id	s_1	s_2	r
id	id	s_1	s_2	r
s_1	s_1	id	r	s_2
s_2	s_2	r	id	s_1
r	r	s_2	s_1	id

Exercice 177 Quel est le centre de $\mathcal{S}_3$? de D_8 ? de D_{12} ? de D_{4n} ?

Éléments de réponse 177 Rappelons que $\mathcal{S}_3 \simeq \mathrm{D}_6$. Le centre de $\mathcal{S}_3$ est trivial.

Considérons le groupe D_{4n}. Le centre de D_{4n} ne contient pas les rotations r_k d'angle $\frac{2k\pi}{2n} = \frac{k\pi}{n}$, pour $k \neq n$, car elles ne commutent pas avec les symétries.

Par contre le retournement r_0 donné par $k = n$ (*i.e.* la rotation d'angle π) commute avec tous les éléments de D_{4n} :

- avec les rotations de D_{4n} car l'ensemble des rotations est un sous-groupe cyclique de D_{4n} ;
- avec les symétries orthogonales car ce retournement est la composée de deux symétries orthogonales par rapport à des axes orthogonaux (r_0 s'écrit ss' avec s symétrie orthogonale de D_{4n} et s' la symétrie orthogonale d'axe orthogonal à celui de s ; d'une part $r_0 s = s'ss = s'$ et $sr_0 s = sss' = s'$).

Le centre de D_{4n} est donc $\{\mathrm{id}, r_0\}$.

Exercice 178 Soit $n \geq 3$; le sous-ensemble $\{g \in \mathrm{D}_{2n} \,|\, g^2 = \mathrm{id}\}$ de D_{2n} est-il un sous-groupe de D_{2n} ?

Éléments de réponse 178 La composée de deux symétries orthogonales éléments de D_{2n} est une rotation d'angle deux fois l'angle formé par les deux axes. Par suite dès que $n \geq 3$ l'un

de ces produits au moins est d'ordre différent de 2. Ainsi l'ensemble des éléments d'ordre 2 de D_{2n} n'est pas un sous-groupe de D_{2n}.

Exercice 179 Quelle est la matrice de la rotation de $\mathbb{R}^3$ d'angle θ autour de l'axe $\mathbb{R}e_2$?

Éléments de réponse 179 Le vecteur e_2 est vecteur propre pour la valeur propre 1 de la matrice, *i.e.* c'est un vecteur fixe pour la rotation considérée.

L'image de e_1 est dans le plan (e_1, e_3) et est égale à $\cos\theta e_1 - \sin\theta e_3$.

L'image de e_3 est dans le plan (e_1, e_3) et est égale à $\sin\theta e_1 + \cos\theta e_3$.

La matrice cherchée est donc

$$\begin{pmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{pmatrix}$$

Exercice 180 Soit $M \in \mathrm{O}(3,\mathbb{R})$ de déterminant -1.

Montrer que -1 est valeur propre de M.

Éléments de réponse 180 Puisque une isométrie vectorielle conserve les normes, ses valeurs propres sont de module 1. Ceci est donc vrai pour une matrice M de $\mathrm{O}(3,\mathbb{R})$ qui est la matrice d'une isométrie vectorielle. Si de plus $\det M = -1$, alors le produit des racines du polynôme caractéristique de M est -1. Par suite

- ou bien toutes les racines du polynôme caractéristique de M sont réelles et dans ce cas l'une ou trois d'entre elles sont égales à -1 ;
- ou bien deux d'entre elles sont complexes conjuguées, leur produit étant égal à 1 la dernière est -1.

Exercice 181 Soit M une matrice orthogonale 2×2 et de déterminant -1.

Montrer que M est la matrice d'une symétrie orthogonale.

Éléments de réponse 181 Les racines du polynôme caractéristique de M sont de module 1. Si elles sont complexes conjuguées mais dans ce cas le déterminant de M est 1 : contradiction. Elles sont donc toutes les deux réelles, l'une valant 1 et l'autre -1.

Il s'en suit que M est la matrice de la symétrie orthogonale d'axe la droite vectorielle propre associée à la valeur propre 1.

Exercice 182 Soit $M \in \mathrm{SO}(3,\mathbb{R})$ la rotation d'angle θ. Montrer que

$$\cos\theta = \frac{1}{2}\Big(\mathrm{Tr}\, M - 1\Big).$$

Éléments de réponse 182 Si M est la matrice d'une rotation d'angle θ, alors M est semblable à la matrice

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Par suite $\operatorname{Tr} M = 2\cos\theta - 1$ et $\cos\theta = \frac{1}{2}\Big(\operatorname{Tr} M - 1\Big)$.

Exercice 183 Soit s une symétrie plane d'axe $\mathcal{D}$.

1. Soit t une translation de vecteur $\overrightarrow{v}$. Montrer que la composée $t \circ s$ (resp. $s \circ t$) est une symétrie si et seulement si $\overrightarrow{v}$ est normal à $\mathcal{D}$.
2. Soit r une rotation de centre C. Montrer que la composée $r \circ s$ (resp. $s \circ r$) est une symétrie si et seulement si C appartient à $\mathcal{D}$.
3. Soient s' et s'' deux symétries axiales. Montrer que $s \circ s' \circ s''$ est une symétrie si et seulement si les axes de s' et s'' sont parallèles à $\mathcal{D}$ ou se rencontrent en un point de $\mathcal{D}$.

Éléments de réponse 183

1. Soit t une translation de vecteur $\overrightarrow{v}$. Montrons que la composée $t \circ s$ (resp. $s \circ t$) est une symétrie si et seulement si $\overrightarrow{v}$ est normal à $\mathcal{D}$.

   Supposons $\overrightarrow{v}$ normal à $\mathcal{D}$. Soit $t'(\mathcal{D}') = \mathcal{D}'$ où t' est la translation de vecteur $\overrightarrow{v}/2$. La droite $\mathcal{D}'$ est une droite de points fixes par ts qui est donc la symétrie orthogonale d'axe $\mathcal{D}'$.

   Soit t'' la translation de vecteur $-\overrightarrow{v}/2$. Posons $\mathcal{D}'' = t''(\mathcal{D})$. La droite $\mathcal{D}''$ est une droite de points fixes par st qui est donc la symétrie orthogonale d'axe $\mathcal{D}''$.

   Si ts est une symétrie orthogonale s' et si A est un point de l'axe de symétrie, nous avons $ts(A) = A$ donc $\overrightarrow{s(A)A} = \overrightarrow{v}$. Par suite $\overrightarrow{v}$ est normal à la droite $\mathcal{D}$ et d'après ce qui précède st est une symétrie orthogonale.

   Si st est une symétrie, nous arrivons à la même conclusion.

2. Soit r une rotation de centre C. Montrons que la composée $r \circ s$ (resp. $s \circ r$) est une symétrie si et seulement si C appartient à $\mathcal{D}$.

   Supposons que C appartienne à $\mathcal{D}$. Soit θ l'angle de la rotation r. Considérons la rotation r' de centre C et d'angle $-\frac{\theta}{2}$. Alors $\mathcal{D}' = r'(\mathcal{D})$ est une droite de points fixes de $s \circ r$ qui est une symétrie d'axe $\mathcal{D}'$.

   Soit r'' la rotation de centre C et d'angle $\frac{\theta}{2}$. Alors $\mathcal{D}'' = r''(\mathcal{D})$ est une droite de points fixes de $r \circ s$ qui est une symétrie d'axe $\mathcal{D}''$.

   Réciproquement supposons que $r \circ s$ soit une symétrie orthogonale d'axe $\mathcal{D}'$. Soit C' l'intersection de $\mathcal{D}$ et $\mathcal{D}'$. Nous avons $rs(C') = C'$ ainsi que $s(C') = C'$. Par conséquent $C' = r(C')$ et C' est le centre de la rotation r, c'est-à-dire C qui est donc sur $\mathcal{D}$. Dans ce cas $s \circ r$ est aussi une symétrie orthogonale.

La conclusion est identique en supposant a priori que $s \circ r$ est une symétrie.

3. Soient s' et s'' deux symétries axiales. Montrons que $s \circ s' \circ s''$ est une symétrie si et seulement si les axes de s' et s'' sont parallèles à $\mathcal{D}$ ou se rencontrent en un point de $\mathcal{D}$.

   Supposons que les axes de s' et s'' soient sécants en un point C. Alors $s' \circ s''$ est une rotation de centre C et d'après 2. $ss's''$ est une symétrie si et seulement si C appartient à $\mathcal{D}$.

   Supposons que les axes de s' et s'' soient parallèles alors $s' \circ s''$ est une translation de vecteur orthogonal à la direction commune et d'après 1. $ss's''$ est une symétrie si et seulement si cette direction commune est celle de $\mathcal{D}$.

Exercice 184 Montrer que pour une translation t de vecteur $\overrightarrow{u}$ et une symétrie s d'axe $\mathcal{D}$ nous avons $t \circ s = s \circ t$ si et seulement si $\overrightarrow{u}$ est dans la direction de $\mathcal{D}$.

Éléments de réponse 184 Si $st = ts$, alors pour tout point M de $\mathcal{D}$ nous avons $st(M) = ts(M) = t(M)$ donc $t(M)$ appartient à $\mathcal{D}$ et $\overrightarrow{u} = \overrightarrow{Mt(M)}$ est parallèle à $\mathcal{D}$.

Réciproquement supposons que $\overrightarrow{u}$ soit parallèle à $\mathcal{D}$. Posons $M' = ts(M)$ et $M'' = st(M)$. Nous avons $\overrightarrow{Ms(M)} = \overrightarrow{t(M)s(t(M))} = \overrightarrow{t(M)M''}$. Par conséquent $\overrightarrow{s(M)M''} = \overrightarrow{Mt(M)} = \overrightarrow{u}$ et donc $\overrightarrow{s(M)M''} = \overrightarrow{s(M)t(s(M))} = \overrightarrow{s(M)M'}$ $M'' = M'$. Il s'en suit que $st = ts$.

Exercice 185 Soit $\mathcal{R}$ le réseau plan des points à coordonnées entières dans un repère orthonormal $(O, \overrightarrow{i}, \overrightarrow{j})$.

Quelles sont les isométries affines qui conservent $\mathcal{R}$?

Quelles sont les centres des rotations affines qui conservent $\mathcal{R}$?

Éléments de réponse 185 Si une isométrie affine qui conserve le réseau $\mathcal{R}$ a exactement un point fixe, c'est une rotation autour de l'un des points du réseau d'angle $\frac{k\pi}{2}$, ou une rotation d'angle $\frac{k\pi}{2}$ autour de l'un des centres des carrés du type $[O, A, B, C]$ où O est le centre du repère, A a pour coordonnées $(1, 0)$, B a pour coordonnées $(1, 1)$, C a pour coordonnées $(0, 1)$. Enfin il y a aussi les symétries centrales autour des milieux des segments du type OA, AB, BC et CO.

Si une isométrie affine qui conserve le réseau $\mathcal{R}$ a une droite de points fixes, alors c'est une symétrie orthogonale par rapport aux droites du type OA, AB, BC et CO (côtés des carrés du type $[O, A, B, C]$) ainsi que AC et OC (diagonales des carrés du type $[O, A, B, C]$) et des médiatrices des segments OA et AB.

Si une isométrie affine qui conserve le réseau $\mathcal{R}$ n'a pas de point fixe, alors soit c'est une translation de vecteur $\in \mathbb{Z}e_1 + \mathbb{Z}e_2$ (où (e_1, e_2) est la base canonique de $\mathbb{R}^2$), soit c'est un produit d'une translation de ce type avec les autres isométries affines déjà trouvées.

Exercice 186 Soit $\mathfrak{S}$ la représentation graphique dans un repère orthonormal de la fonction sinus.

Quelles sont les isométries affines qui conservent la figure $\mathfrak{S}$?

Éléments de réponse 186 La figure $\mathfrak{S}$ est conservée par la rotation de centre l'origine du repère et d'angle π, par les translations de vecteurs $2k\pi e_1$ pour $k \in \mathbb{Z}$ et par les composées de telles applications.

Exercice 187 Déterminer les isométries affines qui conservent l'ensemble $\mathfrak{F}$ des points de coordonnées $(n, 0)$, $n \in \mathbb{Z}$, dans un repère orthonormal $(O, \overrightarrow{i}, \overrightarrow{j})$ du plan affine euclidien.

Éléments de réponse 187 La figure $\mathfrak{F}$ est l'ensemble des points à coordonnées entières de l'axe des abscisses. Elle est conservée par

- les rotations de centre les points de $\mathfrak{F}$ ou les milieux des segments joignant deux points de $\mathfrak{G}$ et d'angle π,
- la symétrie orthogonale par rapport à l'axe des x,
- la symétrie orthogonale par rapport à n'importe quelle droite verticale qui passe par des points de $\mathfrak{F}$ ou par le milieu du segment joignant deux points de $\mathfrak{F}$,
- toutes les translations de vecteur $\in \mathbb{Z}e_1$,
- les composées de telles applications.

Exercice 188 Notons $\mathrm{OA}(2, \mathbb{R})$ le groupe des déplacements de $\mathbb{R}^2$. Soit G un sous-groupe de $\mathrm{OA}(2, \mathbb{R})$ qui contient les rotations centrées en deux points distincts.

Montrer que G contient une translation.

Éléments de réponse 188 Toute rotation se décompose en une composée de deux symétries orthogonales. Soient A et B les deux points qui sont centres des rotations que G contient. Soit s la symétrie orthogonale d'axe (AB). Soit s_1 la symétrie orthogonale d'axe une droite quelconque $\mathcal{D}_1$ passant par A différente de (AB). Soit s_2 la symétrie orthogonale d'axe la droite $\mathcal{D}_2$ passant par B parallèle à $\mathcal{D}_1$.

Les rotations $s_1 s$ et $s s_2$ appartiennent à G ; par suite $(s_1 s)(s s_2)$ appartient à G, *i.e.* $s_1 s_2$ est dans G. Or la composée $s_1 s_2$ est une translation donc G contient une translation.

Exercice 189 Les actions considérées ci-après sont les actions naturelles.

1. Montrer que l'action de $\mathrm{GL}(n, \mathbb{R})$ sur $\mathbb{R}^n$ n'est pas transitive mais qu'elle définit sur l'ensemble des bases de $\mathbb{R}^n$ une action transitive.
2. Montrer que $\mathrm{SO}(2, \mathbb{R})$ agit transitivement sur le cercle unité de $\mathbb{R}^2$.
3. Montrer que $\mathrm{SO}(3, \mathbb{R})$ agit transitivement sur la sphère unitée de $\mathbb{R}^3$.

Éléments de réponse 189

1. Deux vecteurs quelconques de $\mathbb{R}^n$ sont dans la même orbite pour l'action de $\mathrm{GL}(n,\mathbb{R})$ sur $\mathbb{R}^n$ à condition qu'aucun des deux ne soit nul : l'orbite du vecteur nul est réduite à ce vecteur nul. L'action considérée n'est donc pas transitive.

   Par contre deux bases quelconques de $\mathbb{R}^n$ sont images l'une de l'autre par une unique application linéaire bijective. L'action de $\mathrm{GL}(n,\mathbb{R})$ sur l'ensemble des bases de $\mathbb{R}^n$ est donc transitive.
2. Deux vecteurs quelconques de $\mathbb{R}^2$ sont dans la même orbite pour l'action de $\mathrm{SO}(2,\mathbb{R})$ sur $\mathbb{R}^2$ à condition qu'ils aient même norme ; les éléments du cercle unité ont norme 1, par suite l'action de $\mathrm{SO}(2,\mathbb{R})$ est transitive sur le cercle unité.
3. Même chose qu'à la question précédente.

Exercice 190 Soit G un sous-groupe de $\mathrm{GL}(2,\mathbb{R})$. Déterminer l'orbite d'un point A de $\mathbb{R}^2 \setminus \{O\}$ quand G est le sous-groupe engendré par :

1. une symétrie par rapport à une droite ;
2. une rotation d'angle $\frac{\pi}{2}$;
3. une rotation d'angle $\frac{2\pi}{n}$ ($n > 0$ entier) ;
4. une rotation d'angle $\frac{2\pi}{n}$ ($n > 0$ entier) et une symétrie par rapport à une droite D (penser à distinguer deux cas).

Éléments de réponse 190 Notons que comme on considère l'action naturelle de $\mathrm{GL}(2,\mathbb{R})$ sur $\mathbb{R}^2$ les rotations dont on parle sont les rotations centrées en l'origine O du repère, les symétries dont on parle sont les symétries d'axes les droites qui passent par l'origine O du repère.

1. Si A est sur l'axe de la symétrie s considérée, alors son orbite est réduite à $\{A\}$; si A n'est pas sur cet axe, alors l'orbite de A est $\{A,\, s(A)\}$.
2. L'orbite de A est formée des quatre sommets du carré centré à l'origine (dont A).
3. L'orbite de A est formée des n sommets du polygone P régulier à n côtés centré à l'origine (dont A).
4. Soit P le polygone régulier à n côtés centré à l'origine. Si l'axe de la symétrie s est l'un des axes de symétrie de P l'orbite de A est l'ensemble des sommets de P ; sinon l'orbite de A est la réunion de l'ensemble des sommets de P et ceux de P' où P' est l'image de P par s.

Exercice 191 Rappelons que $\mathrm{SL}(2,\mathbb{R})$ désigne le groupe des applications linéaires de déterminant 1 de $\mathbb{R}^2$ dans lui-même.

Rappelons aussi que $\mathrm{SO}(2,\mathbb{R})$ désigne le groupe des applications linéaires orthogonales directes de $\mathbb{R}^2$ dans lui-même.

Notons $x \cdot y$ le produit scalaire usuel sur $\mathbb{R}^2$.

1. Soit G un sous-groupe fini de $\mathrm{SL}(2,\mathbb{R})$. Soit $g \in \mathrm{G}$. Soit $\varphi_g \colon \mathbb{R}^2 \to \mathbb{R}$ l'application définie par
$$\varphi_g(x,y) = g(x) \cdot g(y).$$
Montrer que $\psi = \sum_{g\in\mathrm{G}} \varphi_g$ est une forme bilinéaire symétrique définie positive sur $\mathbb{R}^2$.
2. Montrer que pour $g \in \mathrm{G}$ nous avons $\psi(g(x), g(y)) = \psi(x,y)$.
Montrer que la matrice d'un élément de G dans la base $\{e_1, e_2\}$ orthonormée pour ψ est de la forme
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$
En déduire que G est un sous-groupe fini de $\mathrm{SO}(2,\mathbb{R})$.
3. Quel est l'ordre d'un élément g de G ? En déduire que g est une rotation d'angle $\frac{2k\pi}{n}$ avec k et n convenables.
4. Montrer que G est cyclique.

Éléments de réponse 191

1. Remarquons que pour tout $g \in \mathrm{G}$ nous avons $\varphi_g(x,y) = \varphi_g(y,x)$. De plus
$$\begin{aligned} \varphi_g(x+x',y) &= g(x+x')g(y) \\ &= (g(x)+g(x'))g(y) \\ &= g(x)g(y) + g(x')g(y) \\ &= \varphi_g(x,y) + \varphi_g(x',y') \end{aligned}$$
et
$$\varphi_g(\lambda x, y) = g(\lambda x)g(y) = (\lambda g(x))g(y) = \lambda g(x)g(y) = \lambda\varphi_g(x,y).$$
Il en résulte que ψ est une forme bilinéaire symétrique.
Si $\psi(x,x) = 0$, alors
$$\sum_{g\in\mathrm{G}} \varphi_g(x,x) = \sum_{g\in\mathrm{G}} g(x)^2 = 0.$$
Or dans $\mathbb{R}^2$ une somme de carrés ne peut être nulle que si chacun des carrés est nul donc $g(x) = 0$ pour tout $g \in \mathrm{G}$. Toutes les applications linéaires $g \in \mathrm{G}$ sont de déterminant 1 donc inversibles ; il s'en suit que $x = 0$ et ψ est définie. C'est une forme définie positive puisque pour tout x, $\psi(x,x)$ est une somme de carrés.
2. Nous avons
$$\psi(g(x), g(y)) = \sum_{h\in\mathrm{G}} h(g(x))h(g(y)).$$
Puisque G est un groupe le morphisme $h \mapsto hg$ de G dans lui-même est injectif donc un isomorphisme car G est fini. Il s'en suit que
$$\sum_{h\in\mathrm{G}} h(g(x))h(g(y)) = \sum_{h\in\mathrm{G}} h'(x)h'(y)$$

autrement dit $\psi(g(x), g(y)) = \psi(x, y)$.

Les éléments de G préservent le produit scalaire associé à ψ donc G est un sous-groupe (fini) du groupe orthogonal associé à ce produit scalaire (qui est le groupe orthogonal classique) et la matrice d'un élément $g \in \mathrm{G}$ est donc de la forme

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

3. L'ordre d'un élément de G est fini et divise l'ordre de G. Le groupe G est fini d'ordre n donc si $g \in \mathrm{G}$ est d'ordre k_0, alors g est la rotation d'angle $\frac{2k\pi}{n}$ avec $kk_0 = n$.
4. Tout élément de $\langle g \rangle \subset \mathrm{G}$, où g est la rotation d'angle $\frac{2k\pi}{n}$ s'écrit g_0^k où g_0 est la rotation d'angle $\frac{2\pi}{n}$. Par suite $\mathrm{G} \subset \langle g_0 \rangle$; or $|\mathrm{G}| = |\langle g_0 \rangle|$ donc $\mathrm{G} = \langle g_0 \rangle$ et le groupe G est cyclique.

Exercice 192 [Quelques propriétés de $\mathrm{SL}(2, \mathbb{R})$]Désignons par $\mathrm{SL}(2, \mathbb{R})$ le groupe des matrices carrées de taille 2×2 à coefficients réels et de déterminant 1.

Pour $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{R})$ notons $t_u = a + d$.

1. Quel est le polynôme caractéristique P_u de u ? Quelles sont ses valeurs propres ?
2. Montrer que $P_u(u) = 0$.
3. Si P_u admet une racine double, montrer qu'alors
   — ou bien $u = \mathrm{Id}$, ou bien $u = -\mathrm{Id}$;
   — ou bien il existe $v \in \mathrm{SL}(2, \mathbb{R})$ tel que
   $$vuv^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{ou} \qquad vuv^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$
   — ou bien il existe $w \in \mathrm{SL}(2, \mathbb{R})$ tel que
   $$wuw^{-1} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \qquad \text{ou} \qquad wuw^{-1} = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$$
4. Si P_u admet deux racines distinctes réelles, montrer qu'il existe $v \in \mathrm{SL}(2, \mathbb{R})$ et $a \in \mathbb{R}^*$ tels que $vuv^{-1} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$. Y a-t-il une réciproque ?
5. Si P_u admet deux racines complexes non réelles distinctes montrer qu'il existe $v \in \mathrm{SL}(2, \mathbb{R})$ et a, $b \in \mathbb{R}$, $b \neq 0$, tels que $a^2 + b^2 = 1$ et $vuv^{-1} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.
6. En déduire pour tout $u \in \mathrm{SL}(2, \mathbb{R})$ l'équivalence, si $n \notin \{1, 2\}$, entre les deux assertions suivantes :
   — u est d'ordre n ;
   — il existe $k \in \mathbb{N}$ premier avec n tel que $t_u = 2\cos\left(\frac{2k\pi}{n}\right)$.

7. Soit $\mathrm{SL}(2,\mathbb{Z})$ le sous-groupe de $\mathrm{SL}(2,\mathbb{R})$ formé des matrices à coefficients dans $\mathbb{Z}$. Montrer que dans $\mathrm{SL}(2,\mathbb{Z})$ il y a :
   — un élément d'ordre 2 ;
   — une infinité d'éléments d'ordre 4, explicitez-les ;
   — une infinité d'éléments d'ordre 3, explicitez-les ;
   — une infinité d'éléments d'ordre 6, explicitez-les ;
   — aucun élément d'ordre n si $n \notin \{1, 2, 3, 4, 6\}$.

Éléments de réponse 192

1. Soit P_u le polynôme caractéristique de u. Le produit des racines de P_u est égal à $\det u$ qui vaut 1 (puisque $u \in \mathrm{SL}(2,\mathbb{R})$). La somme des racines de P_u est égale à $\mathrm{trace}(u) = t_u = a + d$. Par conséquent $P_u = X^2 - t_u X + 1$.

2. L'endomorphisme associé à u annule son polynôme caractéristique (théorème de Cayley-Hamilton) donc $P_u(u) = 0$.

3. Supposons que P_u admette une racine double. Alors $t_u^2 = 4$ et ou bien $P_u = (X-1)^2$, ou bien $P_u = (X+1)^2$. Nous avons l'alternative suivante :
   ◇ ou bien u est diagonalisable et u est semblable à id ou $-$id, *i.e.* u est égal à id ou $-$id ;
   ◇ ou bien u n'est pas diagonalisable et est semblable à sa forme de Jordan ; nous allons distinguer le cas $P_u = (X-1)^2$ du cas $P_u = (X+1)^2$.

   i) si $P_u = (X-1)^2$, alors u est semblable à $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Par suite il existe $v_0 \in \mathrm{GL}(2,\mathbb{R})$ tel que $u = v_0^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v_0$.

   Si $\det v_0 > 0$ et $\lambda^2 = \frac{1}{\det v_0}$, alors $v = \lambda v_0$ appartient à $\mathrm{SL}(2,\mathbb{R})$ et $u = v^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v$.

   Si $\det v_0 < 0$, $\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $v_0' = \sigma v_0$, alors $\det v_0' > 0$ et

$$u = v_0^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v_0 = v_0^{-1} \sigma \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \sigma v_0 = v_0'^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} v_0'$$

   Soit alors $v = \lambda v_0'$ avec $\lambda^2 = \frac{1}{\det v_0'}$. D'une part $v \in \mathrm{SL}(2,\mathbb{R})$ d'autre part

$$u = v^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} v$$

ii) Supposons que $P_u = (X+1)^2$ alors u est semblable à $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$. Il existe donc $v_0 \in \mathrm{GL}(2,\mathbb{R})$ tel que $u = v_0^{-1}\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v_0$. Soit $v = \lambda v_0$. Nous avons $\det v = \lambda^2 \det v_0$.

Si $\det v_0 > 0$ et $\lambda^2 = \frac{1}{\det v_0}$ alors v appartient à $\mathrm{SL}(2,\mathbb{R})$ et $u = v^{-1}\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v$.

Si $\det v_0 < 0$ et $v_0' = \sigma v_0$, alors $\det v_0' > 0$ et

$$u = v_0^{-1}\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v_0 = v_0^{-1}\sigma\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}\sigma v_0 = v_0'^{-1}\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} v_0'$$

Soit alors $v = \lambda v_0'$ avec $\lambda^2 = \frac{1}{\det v_0'}$. Ainsi v appartient à $\mathrm{SL}(2,\mathbb{R})$ et

$$u = v^{-1}\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} v.$$

4. Supposons que P_u admette deux racines réelles distinctes. Leur produit étant 1, elles sont inverses l'une de l'autre. La matrice u est donc semblable à une matrice de la forme $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$. Il existe donc $v_0 \in \mathrm{GL}(2,\mathbb{R})$ tel que $u = v_0^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} v_0$.

   Si $\det v_0 > 0$ et si $\lambda^2 = \frac{1}{\det v_0}$ alors $v = \lambda v_0$ appartient à $\mathrm{SL}(2,\mathbb{R})$ et

$$u = v^{-1}\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} v$$

   Si $\det v_0 < 0$ et si $\lambda^2 = -\frac{1}{\det v_0}$ alors $v = \lambda\sigma v_0$ appartient à $\mathrm{SL}(2,\mathbb{R})$ et

$$u = v^{-1}\begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{pmatrix} v.$$

   La réciproque est vraie pour $\alpha \neq \pm 1$.

5. Supposons que P_u admette deux racines complexes distinctes. Elles sont conjuguées et de module 1. Comme $u \in \mathrm{SL}(2,\mathbb{R})$ est de déterminant 1, c'est la matrice, dans la base canonique de $\mathbb{R}^2$, d'une application orthogonale directe g, donc ici (puisque g n'a pas de valeur propre réelle) la matrice d'une rotation d'angle ϑ. Par conséquent u est semblable à $\begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}$. Ainsi u est semblable à une matrice du type $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$ où $\alpha^2+\beta^2 =$

   1. Il existe donc $v_0 \in \mathrm{GL}(2,\mathbb{R})$ tel que $u = v_0^{-1}\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} v_0$.

      Si $\det v_0 > 0$ et si $\lambda^2 = \frac{1}{\det v_0}$, alors $v = \lambda v_0$ appartient à $\mathrm{SL}(2,\mathbb{R})$ et

$$u = v^{-1}\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} v.$$

Si $\det v_0 < 0$ et si λ est tel que $\lambda^2 = -\frac{1}{\det v_0}$ alors $v = \lambda \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} v_0$ et

$$u = v^{-1} \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} v.$$

6. Supposons que $n > 2$.
   - ◇ Si $u = \pm\mathrm{id}$, alors l'ordre de u est 1 ou 2.
   - ◇ Si $u = v^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v$, si $u = v^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} v$, si $u = v^{-1} \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} v$, si $u = v^{-1} \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} v$, si $u = v^{-1} \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} v$, alors l'ordre de u est infini.
   - ◇ Reste le cas où $u = v^{-1} \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} v$ avec $\alpha^2 + \beta^2 = 1$, alors u est la matrice d'une rotation d'angle φ.

   Ainsi $u \in \mathrm{SL}(2, \mathbb{R})$ est d'ordre n si et seulement si u est la matrice d'une rotation d'angle φ et d'ordre n. Une rotation r d'angle φ est d'ordre n si et seulement si $\varphi = \frac{2k\pi}{n}$ avec k et n premiers entre eux (sinon r serait d'ordre strictement inférieur à n). La trace de l'endomorphisme r est égale à $2\cos\left(\frac{2k\pi}{n}\right)$ et à t_u. Par suite $u \in \mathrm{SL}(2, \mathbb{R})$ est d'ordre n si et seulement si $t_u = 2\cos\left(\frac{2k\pi}{n}\right)$ avec k et n premiers entre eux.
7. Les éléments d'ordre n de $\mathrm{SL}(2, \mathbb{Z})$ sont des éléments d'ordre n de $\mathrm{SL}(2, \mathbb{R})$. D'après les questions qui précèdent
   - ◇ il y a un seul élément d'ordre 2 dans $\mathrm{SL}(2, \mathbb{Z})$, c'est $-\mathrm{id}$;
   - ◇ il y a une infinité d'éléments d'ordre 4 : ce sont les matrices u de $\mathrm{SL}(2, \mathbb{Z})$ telles que $t_u = 0$;
   - ◇ il y a une infinité d'éléments d'ordre 3 ; ce sont les matrices u de $\mathrm{SL}(2, \mathbb{Z})$ telles que $t_u = -1$;
   - ◇ il y a une infinité d'éléments d'ordre 6 ; ce sont les matrices u de $\mathrm{SL}(2, \mathbb{Z})$ telles que $t_u = 1$;
   - ◇ pour qu'un élément u de $\mathrm{SL}(2, \mathbb{Z})$ soit d'ordre $n > 2$ il faut et il suffit que $t_u = 2\cos\left(\frac{2k\pi}{n}\right)$ avec k et n premiers entre eux et que t_u appartienne à $\mathbb{Z}$. Or $2\cos\left(\frac{2k\pi}{n}\right)$ est entier seulement lorsque $n = 3$, 4 et 6. Il s'en suit qu'il n'y a pas d'éléments d'ordre $n \neq 1$, 2, 3, 4, 6 dans $\mathrm{SL}(2, \mathbb{Z})$.

Exercice 193 Soit D_{2n} le groupe diédral d'ordre $2n$ engendré par r d'ordre n et s d'ordre 2 tels que $rs = sr^{-1}$. Autrement dit

$$\mathrm{D}_{2n} = \langle r,\, s \,|\, r^n = s^2 = rsrs = \mathrm{id} \rangle.$$

Exprimer $r^2 s r^{-1} s^{-1} r^3 s^3$ sous la forme $r^i s$.

Éléments de réponse 193 Nous avons

$$r^2sr^{-1}s^{-1}r^3s^3 = r^2(sr^{-1})s^{-1}r^3(s^2s) = r^2(rs)s^{-1}r^3s = r^2r(ss^{-1})r^3s = r^6s.$$

Exercice 194 Faire la liste de tous les sous-groupes de D_8.

Éléments de réponse 194 Rappelons que

$$\mathrm{D}_8 = \langle r,\, s \,|\, r^4 = s^2 = \mathrm{id},\, rs = sr^{-1}\rangle = \{\mathrm{id},\, r,\, r^2,\, r^3,\, s,\, rs,\, r^2s,\, r^3s\}.$$

Bien entendu $\{\mathrm{id}\}$ et D_8 sont des sous-groupes de D_8.

Le groupe D_8 ne possède que deux éléments d'ordre 4, à savoir r et r^3 Chacun d'eux engendre le groupe $\langle r\rangle$ qui est cyclique d'ordre 4.

Le groupe D_8 possède cinq éléments d'ordre 2 qui sont r^2 et r^is avec $0 \leq i \leq 3$. Il y a donc cinq sous-groupes cycliques d'ordre 2 :

$$\langle r^2\rangle, \qquad \langle s\rangle \qquad \langle rs\rangle \qquad \langle r^2s\rangle \qquad \langle r^{-1}s\rangle.$$

Le groupe D_8 possède un sous-groupe d'ordre 4 non cyclique : $\langle r^2,\, s\rangle$ qui est abélien et isomorphe à $\mathbb{Z}\!/_{2\mathbb{Z}} \times \mathbb{Z}\!/_{2\mathbb{Z}}$ via

$$\mathbb{Z}\!/_{2\mathbb{Z}} \times \mathbb{Z}\!/_{2\mathbb{Z}} \to \langle r^2,\, s\rangle \qquad\qquad (i,j) \mapsto r^{2i}s^j.$$

En effet les groupes $\mathrm{G}_1 = \langle r^2\rangle$ et $\mathrm{G}_2 = \langle s\rangle$ satisfont les propriétés suivantes :

- $\mathrm{G}_1 \cap \mathrm{G}_2 = \{\mathrm{id}\}$;
- G_1 et G_2 commutent ;
- $\mathrm{G}_1\mathrm{G}_2 = \langle r^2,\, s\rangle$

donc $\langle r,\, s^2\rangle$ est isomorphe au produit direct de G_1 et G_2, et G_1 et G_2 sont cycliques d'ordre 2.

Le groupe D_8 ne contient pas d'autre sous-groupe ; en effet rappelons que si G est un sous-groupe de D_8, alors $|\mathrm{G}|$ divise $|\mathrm{D}_8| = 8$, *i.e.* $|\mathrm{G}| \in \{1,\, 2,\, 4,\, 8\}$. Nous pouvons récapituler ce qui précède comme suit

$\lvert\mathrm{G}\rvert = 1$	$\{\mathrm{id}\}$
$\lvert\mathrm{G}\rvert = 2$	$\langle r^2\rangle,\, \langle s\rangle,\, \langle r,\, s\rangle,\, \langle r^2,\, s\rangle,\, \langle r^{-1},\, s\rangle,$
$\lvert\mathrm{G}\rvert = 4$	$\langle r\rangle,\, \langle r^2,\, s\rangle,$
$\lvert\mathrm{G}\rvert = 8$	D_8

À isomorphisme près il y a cinq sous-groupes de D_8 : $\{\mathrm{id}\}$, $\mathbb{Z}\!/_{2\mathbb{Z}}$, $\mathbb{Z}\!/_{4\mathbb{Z}}$, $\mathbb{Z}\!/_{2\mathbb{Z}} \times \mathbb{Z}\!/_{2\mathbb{Z}}$ et D_8.

Exercice 195 Caractériser géométriquement l'endomorphisme f de $\mathbb{R}^3$ dont la matrice dans la base canonique est

$$A = \frac{1}{3}\begin{pmatrix} 2 & -1 & 2 \\ 2 & 2 & -1 \\ -1 & 2 & 2 \end{pmatrix}$$

Éléments de réponse 195 Les vecteurs colonnes de la matrice sont des vecteurs unitaires deux à deux orthogonaux. La matrice est donc orthogonale. De plus son déterminant est 1. Par suite A appartient à $\mathrm{SO}(3,\mathbb{R})$. La matrice A est donc une matrice de rotation. En réduisant nous obtenons que la trace de A vaut $1+2\cos\theta$ où θ est l'angle de la rotation (bien défini au signe près). Comme la trace de A vaut 2 nous avons $\cos\theta=\frac{1}{2}$ et $\theta=\frac{\pi}{3}$. L'axe correspond à la droite propre pour la valeur propre 1. Nous avons

$$3(A-\mathrm{Id})=\begin{pmatrix}-1&-1&2\\2&-1&-1\\-1&2&-1\end{pmatrix}$$

Cet axe est donc la droite engendrée par le vecteur $(1,1,1)$.

Exercice 196 Soient A et B deux éléments de $\mathrm{SO}(3,\mathbb{R})$. Donner une condition géométrique nécessaire et suffisante pour que A et B commutent (cette conditions fait intervenir des droites particulières de $\mathbb{R}^3$ associées à A et B).

Éléments de réponse 196 Si A ou B est l'identité, alors A et B commutent.

Supposons que ni A, ni B ne soit l'identité. Ce sont alors deux rotations d'angle non nul. Si A et B commutent, alors l'axe de B est laissé invariant par A et l'axe de A est laissé invariant par B. Notons $\mathcal{D}_A$ l'axe de A et $\mathcal{P}_A$ son orthogonal (qui est donc dans le plan de rotation de A). Soit $\mathcal{D}$ une droite invariante par A, il s'agit donc d'une droite propre pour A. Si A n'est pas un demi-tour, la seule droite invariante pour A est son axe (car A n'a que 1 comme valeur propre) ; si A est un demi-tour, il y a en plus le sous-espace propre associé à -1 qui est $\mathcal{P}_A$. Un raisonnement analogue s'applique à B. Il s'en suit que si A et B commutent, alors A et B ont même axe ou alors ce sont des demi-tours et leurs axes sont orthogonaux.

Réciproquement supposons que A et B aient même axe $\mathcal{D}$. Choisisons une base orthonormale telle que le premier vecteur soit un vecteur directeur de $\mathcal{D}$. Dans cette base A et B s'écrivent

$$A=\begin{pmatrix}1&0&0\\0&\cos(\alpha)&-\sin(\alpha)\\0&\sin(\alpha)&\cos(\alpha)\end{pmatrix}\qquad B=\begin{pmatrix}1&0&0\\0&\cos(\beta)&-\sin(\beta)\\0&\sin(\beta)&\cos(\beta)\end{pmatrix}$$

où α et β sont les angles respectifs de A et B. Un calcul matriciel montre alors que A et B commutent.

De même si A et B sont des demi-tour d'axes orthogonaux alors dans une base orthonormale où les deux premiers vecteurs sont des vecteurs directeurs des axes de A et B nous avons

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

et par conséquent A et B commutent.

Exercice 197 Soient E un espace vectoriel euclidien de dimension 3 et S sa sphère unité. Si D est une droite vectorielle de E, on note σ_D la rotation d'angle π autour de D (appelée aussi demi-tour). Par conséquent σ_D appartient au groupe spécial orthogonal $\mathrm{SO}(E)$ dont on rappelle qu'il est engendré par les demi-tours.

1. Soit D une droite vectoriel, soit g un élément de $\mathrm{SO}(E)$. Reconnaître l'endomorphisme $g \circ \sigma_D \circ g^{-1}$.
2. Soit $g \in \mathrm{SO}(E)$. Montrer que g est un demi-tour si et seulement s'il existe $x \in S$ tel que $g(x) = -x$.

   Dans les deux questions suivantes, nous nous donnons un sous-groupe G de $\mathrm{SO}(E)$ agissant transitivement sur S.
3. Montrer que G contient un demi-tour.
4. En déduire que $\mathrm{G} = \mathrm{SO}(E)$.

Éléments de réponse 197

1. Les deux endomorphismes g et $g \circ \sigma_D \circ g^{-1}$ sont des rotations et ont même trace. Ces deux rotations ont même angle, ce sont toutes les deux des demi-tours. D est la droite propre pour la valeur propre 1, par suite $g(D)$ est la droite propre de $g \circ \sigma_D \circ g^{-1}$ pour la valeur propre 1. Il s'en suit que $g \circ \sigma_D \circ g^{-1} = \sigma_{g(D)}$.
2. Soit g un élément de $\mathrm{SO}(E)$. Si g est un demi-tour σ_D, alors g a pour matrice dans une base orthonormale adaptée (e_1, e_2, e_3)

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

   Nous avons e_2 appartient à S et $g(e_2) = -e_2$.
3. Si G agit transitivement sur S, alors pour un $x \in S$ fixé il existe g tel que $g(x) = -x$ et donc par la question précédente g est un demi-tour dans G.
4. Comme G est un groupe et comme $\mathrm{SO}(E)$ est engendré par les demi-tours il suffit de montrer que G contient tous les demi-tours. D'après la question précédente il existe une droite D telle que σ_D appartient à G. Soit D' une autre droite. Soit $\overrightarrow{u}$ un vecteur directeur unitaire de D et $\overrightarrow{u'}$ un vecteur directeur unitaire de D'. Puisque G agit transitivement sur S il existe g dans G tel que $g(\overrightarrow{u}) = \overrightarrow{u'}$. Ainsi $g(D) = D'$. D'après 1. nous avons

$$g \circ \sigma_D \circ g^{-1} = \sigma_{g(D)} = \sigma_{D'} \in \mathrm{G}.$$

Exercice 198 Soit $n \in \mathbb{N}^*$. Soit G le sous-ensemble de $M(n+1, \mathbb{R})$ donné par les matrices de la forme

$$M = \left(\begin{array}{c|c} A & \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \\ \hline \begin{matrix} 0 \dots 0 \end{matrix} & 1 \end{array}\right)$$

où $A \in \mathrm{GL}(n, \mathbb{R})$ et $(x_1, x_2, \dots, x_n) \in \mathbb{R}^n$.

1. Montrer que G est un groupe.
2. Expliciter de quelle manière le groupe affine $\mathrm{GA}(\mathbb{R}^n)$ de R^n est isomorphe au groupe $\mathrm{GL}(n, \mathbb{R}) \ltimes \mathbb{R}^n$. En particulier explique comment effectuer la composée de φ, $\varphi' \in \mathrm{GA}(\mathbb{R}^n)$ où φ (resp. φ') pour partie linéaire $A \in \mathrm{GL}(n, \mathbb{R})$ (resp. $A' \in \mathrm{GL}(n, \mathbb{R})$) et vecteur de translation $v \in \mathbb{R}^n$ (resp. $v' \in \mathbb{R}^n$).
3. Montrer que G est isomorphe à $\mathrm{GA}(\mathbb{R}^n)$.

Éléments de réponse 198

1. Montrons qu'il s'agit d'un sous-groupe de $\mathrm{GL}(n+1, \mathbb{R})$.

   L'inverse de $\left(\begin{array}{c|c} A & \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \\ \hline \begin{matrix} 0 \dots 0 \end{matrix} & 1 \end{array}\right)$ est la matrice $\left(\begin{array}{c|c} A^{-1} & \begin{matrix} z_1 \\ \vdots \\ z_n \end{matrix} \\ \hline \begin{matrix} 0 \dots 0 \end{matrix} & 1 \end{array}\right)$ où $(z_1, z_2, \dots, z_n) = A^{-1}(-x_1, -x_2, \dots, -x_n)$.

   La composée de $\left(\begin{array}{c|c} A & \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \\ \hline \begin{matrix} 0 \dots 0 \end{matrix} & 1 \end{array}\right)$ avec $\left(\begin{array}{c|c} B & \begin{matrix} y_1 \\ \vdots \\ y_n \end{matrix} \\ \hline \begin{matrix} 0 \dots 0 \end{matrix} & 1 \end{array}\right)$ est $\left(\begin{array}{c|c} AB & \begin{matrix} x_1 + z_1 \\ \vdots \\ x_n + z_n \end{matrix} \\ \hline \begin{matrix} 0 \dots 0 \end{matrix} & 1 \end{array}\right)$ où $(z_1, z_2, \dots, z_n) = A(y_1, y_2, \dots, y_n)$. Il s'agit donc bien d'un sous-groupe.
2. Identifions les éléments de $\mathrm{GA}(\mathbb{R}^n)$ qui fixent 0 avec $\mathrm{GL}(\mathbb{R}^n)$. Les translations sont le morphisme du noyau $\mathrm{GA}(\mathbb{R}^n) \to \mathrm{GL}(\mathbb{R}^n)$. Les translations forment un sous-groupe isomorphe à $\mathbb{R}^n$ par l'application $v \in \mathbb{R}^n \mapsto \tau_v$ où τ_v est la translation de vecteur v.

   Si φ, φ' s'écrivent $\varphi = \tau_v \circ A$ et $\varphi' = \tau_{v'} \circ A'$, alors

   $$\varphi \circ \varphi'(x) = A(A'x + v') + v = AA'x + (Av' + v).$$

   La composée $\varphi \circ \varphi'$ a pour partie linéaire AA' et a pour partie translation, la translation de vecteur $Av' + v$.

3. Montrons que G est isomorphe à $\mathrm{GA}(\mathbb{R}^n)$. L'isomorphisme est donné par

$$\psi\colon \mathrm{GA}(\mathbb{R}^n) \to \mathrm{G} \qquad\qquad \varphi = \tau_v \circ A \mapsto \left(\begin{array}{c|c} A & \begin{matrix} v_1 \\ \vdots \\ v_n \end{matrix} \\ \hline 0\ldots0 & 1 \end{array}\right)$$

Il s'agit d'une bijection qui est, d'après 1. et 2., un morphisme de groupes :

$$\begin{aligned} \psi(\varphi\circ\varphi') &= \left(\begin{array}{c|c} AA' & \begin{matrix} v_1+w_1 \\ \vdots \\ v_n+w_n \end{matrix} \\ \hline 0\ldots0 & 1 \end{array}\right) = \left(\begin{array}{c|c} A & \begin{matrix} v_1 \\ \vdots \\ v_n \end{matrix} \\ \hline 0\ldots0 & 1 \end{array}\right)\left(\begin{array}{c|c} A' & \begin{matrix} v'_1 \\ \vdots \\ v'_n \end{matrix} \\ \hline 0\ldots0 & 1 \end{array}\right) \\ &= \psi(\varphi)+\psi(\varphi') \end{aligned}$$

où $w = Av'$.

Exercice 199 Soit E un espace affine euclidien de dimension n. On appelle similitude de E toute transformation affine bijective de E dans lui-même dont la partie linéaire est la composée d'une homothétie et d'une isométrie linéaire.

1. Montrer que les similitudes forment un groupe.
2. Soit φ une similitude. Démontrer que si L est la partie linéaire de φ, alors L s'écrit de matrice unique sous la forme $L = HR$ où H est une homothétie linéaire et R un élément de $\mathrm{SO}(n,\mathbb{R})$ et que de plus H et R commutent.

   Soit φ une bijection de E. On dit que φ préserve les angles (non-orientés) si pour tous points $A \neq B$, $C \in E$, $\varphi(A)\widehat{\varphi(B)}\varphi(C) = \widehat{ABC}$. Nous allons montrer que les similitudes sont extactement les transformations qui préservent les angles.
3. Montrer que les similitudes préservent les angles.

   Soit φ une bijection de E qui préservent les angles.
4. Montrer que φ préserve l'alignement.
5. Montrer que φ est affine.
6. Choisissons une origine O dans E. Trouver une translation τ tells que $(\tau^{-1}\circ\varphi)(O) = O$. Posons $\varphi' = \tau^{-1}\circ\varphi$.
7. Soit $A \neq O$. Posons $\lambda = \frac{||\overrightarrow{O\varphi'(A)}||}{||\overrightarrow{OA}||}$. Si h_λ est l'homothétie de rapport λ et de centre O, montrer que $\psi = h_\lambda^{-1}\circ\varphi'$ préserve le produit scalaire et la norme. On pourra utiliser des triangles isométriques.
8. En déduire que ψ est une isométrie et conclure.

Éléments de réponse 199 Désignons par h_λ l'homothétie de rapport λ.

1. Rappelons que les similitudes linéaires sont les composées d'homothéties linéaires de rapport positif et d'isométries linéaires.

   Les similitudes linéaires forment un sous-groupe de $\mathrm{GL}(E)$. En effet soient R, S dans $\mathrm{O}(E)$. Comme $(h_\lambda R)^{-1} = R^{-1}h_\lambda^{-1} = R^{-1}h_{\lambda^{-1}} = h_{\lambda^{-1}}R^{-1}$, $(h_\lambda R)^{-1}$ est une similitude linéaire. De même $(h_\lambda R)(h_\mu S) = h_{\lambda+\mu}T$ où T est l'isométrie linéaire RS donc $(h_\lambda R)(h_\mu S)$ est une similitude linéaire.

   Les similitudes affines sont l'image réciproque des similitudes linéaires par le morphisme $\mathrm{GA}(E) \to \mathrm{GL}(E)$; il s'agit donc d'un sous-groupe du groupe affine $\mathrm{GA}(E)$.

2. Dans l'écriture $L = HR$, HR commutent car H est une homothétie et donc commute avec tous les éléments de $\mathrm{GL}(E)$. Supposons qu'il existe deux écritures $L = h_\lambda R = h_\mu S$ avec R, S isométries linéaires et λ, $\mu > 0$ alors $|\det L| = \lambda = \mu$ et donc $h_\lambda = h_\mu$ et $R = h_{\lambda^{-1}}L = h_{\mu^{-1}}L = S$. Il y a donc bien unicité.

3. Rappelons que l'angle $\widehat{ABC}$ est l'unique réel $\alpha \in [0, \pi]$ tel que
$$\cos\alpha = \frac{\langle \overrightarrow{BA},\, \overrightarrow{BC}\rangle}{||\overrightarrow{BA}||\,||\overrightarrow{BC}||}.$$
   Soit φ une similitude dont la partie linéaire L s'écrit $h_\lambda R$ avec $R \in \mathrm{O}(E)$. Nous avons
$$\begin{aligned}
\cos(\varphi(A)\widehat{\varphi(B)}\varphi(C)) &= \frac{\langle \overrightarrow{\varphi(B)\varphi(A)},\, \overrightarrow{\varphi(B)\varphi(C)}\rangle}{||\overrightarrow{\varphi(B)\varphi(A)}||\,||\overrightarrow{\varphi(B)\varphi(C)}||} \\
&= \frac{\langle L(\overrightarrow{BA}),\, L(\overrightarrow{BC})\rangle}{||L(\overrightarrow{BA})||\,||L(\overrightarrow{BC})||} \\
&= \frac{\langle h_\lambda R(\overrightarrow{BA}),\, h_\lambda R(\overrightarrow{BC})\rangle}{||h_\lambda R(\overrightarrow{BA})||\,||h_\lambda R(\overrightarrow{BC})||} \\
&= \frac{\lambda^2\langle R(\overrightarrow{BA}), R(\overrightarrow{BC})\rangle}{\lambda^2||R(\overrightarrow{BA})||\,||R(\overrightarrow{BC})||} \\
&= \frac{\langle \overrightarrow{BA},\, \overrightarrow{BC}\rangle}{||\overrightarrow{BA}||\,||\overrightarrow{BC}||} \\
&= \cos(\widehat{ABC})
\end{aligned}$$
   Il en résulte que les similitudes préservent les angles.

4. Trois points A, B et C sont alignés si l'angle $\widehat{ABC}$ vaut 0 ou π. Si une transformation préserve les angles, elle préserve donc aussi l'alignement.

5. Puisque E est un espace vectoriel réel de dimension ≥ 2 une application bijective qui préserve l'alignement est affine. C'est le théorème fondamental de la géométrie affine.

6. La translation τ de vecteur $\overrightarrow{O\varphi(O)}$ convient et c'est la seule.

7. Soit $B \in E$. Les triangles OAB et $\psi(O)\psi(A)\psi(B)$ sont isométriques ; en effet ils ont trois angles égaux, $\psi(O) = O$ et $||\overrightarrow{O\psi(A)}|| = ||\overrightarrow{OA}||$. Par conséquent $||\overrightarrow{O\psi(B)}|| = ||\overrightarrow{OB}||$ et ψ est une application linéaire qui préserve la norme. Ensuite pour B, $C \neq O$ puisque ψ préserve les angles et $||\overrightarrow{OB}|| = ||\overrightarrow{OC}||$, on a $\langle\overrightarrow{OB}, \overrightarrow{OC}\rangle = \langle\overrightarrow{O\psi(B)}, \overrightarrow{O\psi(C)}\rangle$. Il s'en suit que ψ est une application linéaire orthogonale qui préserve aussi la norme.
8. Nous avons donc montré que $\varphi = \tau \circ h_\lambda \circ \psi$, *i.e.* la composée d'une translation et d'une similitude linéaire.

Exercice 200 Groupes et propriétés géométrique de l'orbite.

Soit E un espace affine euclidien. Soit f un élément du groupe $\mathrm{Isom}(E)$ des isométries de E. Soit G le sous-groupe de $\mathrm{Isom}(E)$ engendré par f. Soit p un point de E. Montrer que les assertions suivantes sont équivalentes :

(1) L'orbite de p sous G est bornée ;

(2) Toute orbite sous G d'un point de E est bornée ;

(3) f a un point fixe.

Éléments de réponse 200 Montrons que (3) implique (1).

Par hypothèse il existe $m \in E$ tel que $f(m) = m$. Pour tout $k \in \mathbb{N}$ nous avons

$$d(m, f^k(p)) = d(f^k(m), f^k(p)) = d(m, p)$$

ainsi l'orbite de p sous G est bornée.

Montrons que (1) implique (2).

Il existe $r > 0$ tel que $d(p, f^k(p)) \leq r$ pour tout $k \in \mathbb{N}$. Soit m un point de E alors $d(f^k(p), f^k(m)) = d(p, m)$. Par conséquent

$$d(p, f^k(m)) \leq d(p, f^k(p)) + d(f^k(p), f^k(m)) \leq r + d(p, m).$$

Montrons que (2) implique (3).

Le théorème de la forme réduite des isométries de E implique l'existence de $g \in \mathrm{Isom}(E)$ avec un point fixe p et $\overrightarrow{v} \in \ker(f - \mathrm{id}_E)$ tel que $f = t_{\overrightarrow{v}} \circ g = g \circ t_{\overrightarrow{v}}$. Ainsi $f^k(A) = A + k\overrightarrow{v}$ et donc $d(A, f^k(A)) = k||\overrightarrow{v}|| \to +\infty$ si $\overrightarrow{v} \neq \overrightarrow{0}$. Puisque la suite $(f^k(A))_k$ est bornée nous obtenons que $\overrightarrow{v} = \overrightarrow{0}$ ainsi $f = g$ a un point fixe.

5.7. Structure des groupes abéliens de type fini

Exercice 201 Soit G un groupe de type fini.

Un sous-groupe H de G est-il nécessairement de type fini ? Justifiez votre réponse.

Éléments de réponse 201 Soit G est un groupe de type fini ; G peut contenir un sous-groupe H qui n'est pas de type fini.

Considérons le sous-groupe G de $\mathrm{GL}(2,\mathbb{Q})$ engendré par les matrices

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Soit H le sous-groupe de G formé des matrices de G avec des 1 sur la diagonale. Raisonnons par l'absurde : supposons que H soit de type fini. Alors il existe un entier $N \geq 1$ tel que H soit contenu dans le sous-groupe de $\mathrm{GL}(2,\mathbb{Q})$ formé des matrices de la forme

$$\begin{pmatrix} 1 & \frac{a}{N} \\ 0 & 1 \end{pmatrix}$$

Or $A^{-N}BA^N = \begin{pmatrix} 1 & \frac{1}{2^N} \\ 0 & 1 \end{pmatrix}$: contradiction ($2^N > N$). Ainsi H n'est pas de type fini alors que G l'est.

Considérons par exemple le groupe libre G sur deux générateurs a et b. Soit H le sous-groupe engendré par tous les éléments de la forme ab^n avec $n \in \mathbb{N}$. Raisonnons par l'absurde : supposons que H soit de type fini. Alors il existe un entier N tel que dans tout mot de H le nombre de b consécutifs soit toujours strictement inférieur à N. Or ab^N appartient à H : contradiction. Le sous-groupe H de G n'est donc pas de type fini.

Exercice 202 Soit G un groupe abélien.

Montrer que $T(\mathrm{G}) = \{g \in \mathrm{G} \mid o(g) < \infty\}$ est un sous-groupe de G (appelé le sous-groupe de torsion de G).

Donner un exemple explicite pour lequel $T(\mathrm{G})$ n'est pas un sous-groupe de G si G n'est pas abélien.

Éléments de réponse 202 Soit G un groupe abélien.

Montrons que $T(\mathrm{G}) = \{g \in G \mid o(g) < \infty\}$ est un sous-groupe de G (appelé le sous-groupe de torsion de G).

Clairement $T(\mathrm{G})$ est contenu dans G. On a

- $o(e) = 1 < \infty$ donc $e \in T(\mathrm{G})$;
- soient g et h dans $T(\mathrm{G})$. Notons n (resp. m) l'ordre de g (resp. h). Par hypothèse $n < \infty$ et $m < \infty$. On a bien sûr $o(h^{-1}) = m$. Puisque G est abélien on a

  $$(gh^{-1})^{mn} = g^{mn}(h^{-1})^{mn}$$

  Par suite $(gh^{-1})^{mn} = (g^n)^m((h^{-1})^m)^n = e^m e^n = e$. Ainsi $o(gh^{-1}) \leq mn < \infty$ et gh^{-1} appartient à $T(\mathrm{G})$.

Ainsi $T(\mathrm{G})$ est un sous-groupe de G.

Montrons que si G n'est pas abélien, alors $T(\mathrm{G})$ n'est pas forcément un sous-groupe de G.

Considérons $\mathrm{G} = \mathrm{O}(2)$. Soit ρ la rotation d'angle θ où θ/π est irrationnel. Alors ρ n'appartient pas à $T(\mathrm{G})$. Mais $\rho = s_2 \circ s_1$ avec s_1, s_2 réflexions ; en particulier $o(s_1) = o(s_2) = 2$ et donc s_1, s_2 appartiennent à $T(\mathrm{G})$.

Exercice 203 Soit $n \in \mathbb{N}$, $n \geq 2$. Trouver le sous-groupe de torsion de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Montrer que l'ensemble des éléments d'ordre infini et l'élément neutre ne forment pas un sous-groupe de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Éléments de réponse 203 Soit $n \in \mathbb{N}$, $n \geq 2$. Déterminons le sous-groupe de torsion de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$:

$$\begin{aligned} T\left(\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\right) &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, o(a,b) < \infty\} \\ &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, \exists\, k \in \mathbb{N}^*,\, o(a,b) = k\} \\ &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, (ka, kb) = (0, \bar{0})\} \\ &= \{(a, \bar{b}) \in \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \,|\, a = 0 \text{ et } b \in \mathbb{Z}/n\mathbb{Z}\} \\ &= \{0\} \times \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

Montrons que l'ensemble des éléments d'ordre infini et l'élément neutre ne forment pas un sous-groupe de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Soient $(1,1)$ et $(-1,0)$ deux éléments de $\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Ils sont d'ordre infini mais $(1,1) + (-1,0) = (0,1)$ est d'ordre fini.

Exercice 204

a) Donner un exemple de groupe abélien qui n'est pas de type fini.

b) Si p est un nombre premier, quel est le groupe sous-jacent au corps $\mathbb{F}_{p^n}$?

c) Soient n, $m \geq 1$ deux entiers. Posons $\delta := \text{pgcd}(n,m)$ et $\mu := \text{ppcm}(n,m)$.
Montrer que les groupes $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z}$ sont isomorphes.

d) Montrer qu'un groupe abélien de type fini et de torsion est fini (ceci n'est plus vrai pour les groupes non-abéliens : voir par exemple [Calais, p. 294]).

e) Montrer qu'un groupe abélien fini est le produit de ses sous-groupes de Sylow.

Éléments de réponse 204

a) $(\mathbb{Q}, +)$ est un groupe abélien qui n'est pas de type fini (pour le vérifier raisonner par l'absurde).

b) Soit p un nombre premier.
Si $n = 1$, alors $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et le groupe sous-jacent est $\mathbb{Z}/p\mathbb{Z}$.
Si $n = 2$, alors le groupe sous-jacent à $\mathbb{F}_{p^2}$ est $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ car $\mathbb{Z}/p^2\mathbb{Z}$ possède un élément d'ordre p^2 alors que $\mathbb{F}_{p^2}$ est de caractéristique p donc sans élément d'ordre p^2.
De même pour n quelconque le groupe sous-jacent à $\mathbb{F}_{p^n}$ est $\left(\mathbb{Z}/p\mathbb{Z}\right)^n$.

c) Soient n, $m \geq 1$ deux entiers. Posons $\delta := \mathrm{pgcd}(n,m)$ et $\mu := \mathrm{ppcm}(n,m)$. Montrons que les groupes $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z}$ sont isomorphes.

Écrivons les décompositions de m et n en nombre premiers :

$$m = \prod_i p_i^{\alpha_i} \qquad\qquad n = \prod_i p_i^{\beta_i}$$

Alors

$$\delta = \prod_i p_i^{\min(\alpha_i,\beta_i)} \qquad\qquad \mu = \prod_i p_i^{\max(\alpha_i,\beta_i)}$$

D'une part

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \prod_i \mathbb{Z}/p_i^{\beta_i}\mathbb{Z} \simeq \prod_i \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \mathbb{Z}/p_i^{\beta_i}\mathbb{Z}\right)$$

d'autre part

$$\mathbb{Z}/\delta\mathbb{Z} \times \mathbb{Z}/\mu\mathbb{Z} \simeq \prod_i \left(\mathbb{Z}/p_i^{\min(\alpha_i,\beta_i)}\mathbb{Z} \times \mathbb{Z}/p_i^{\max(\alpha_i,\beta_i)}\mathbb{Z}\right)$$

Si $\min(\alpha_i,\beta_i) = \alpha_i$, alors $\max(\alpha_i,\beta_i) = \beta_i$; réciproquement si $\min(\alpha_i,\beta_i) = \beta_i$ alors $\max(\alpha_i,\beta_i) = \alpha_i$. Par conséquent tous les α_i et β_i apparaissent une fois et une seule dans le produit

$$\prod_i \left(\mathbb{Z}/p_i^{\min(\alpha_i,\beta_i)}\mathbb{Z} \times \mathbb{Z}/p_i^{\max(\alpha_i,\beta_i)}\mathbb{Z}\right)$$

qui est donc isomorphe à

$$\prod_i \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \times \mathbb{Z}/p_i^{\beta_i}\mathbb{Z}\right)$$

d) Montrons qu'un groupe abélien de type fini et de torsion est fini.

Soit G un groupe abélien de type fini et sans torsion. Puisque G est abélien de type fini on a

$$\mathrm{G} \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

où $r \geq 0$, $n_j \geq 0$ pour tout $1 \leq j \leq s$ et n_{i+1} divise n_i 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

$$\mathrm{G} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

En particulier $|G| = n_1 n_2 \ldots n_s < \infty$.

e) Montrer qu'un groupe abélien fini est le produit de ses sous-groupes de Sylow.

Soient G un groupe abélien et $(\mathrm{H}_i)_{1\leq i\leq r}$ une famille de sous-groupes d'ordre 2 à 2 premiers entre eux. Alors ces groupes sont en somme directe dans G. En effet soit d_i l'ordre de H_i. Rappelons que dans un groupe abélien si G est d'ordre m et h d'ordre n avec n, m premiers entre eux, alors gh est d'ordre mn. Ainsi pour tout i l'ordre de tout

élément de $\sum_{j\neq i} \mathrm{H}_j$ divise $\mathrm{ppcm}_{j\neq i}(d_j)$ donc est premier avec d_i. Il en résulte que nous avons pour tout i

$$\mathrm{H}_i \cap \Big(\sum_{j\neq i} \mathrm{H}_j\Big) = \{1\}$$

Par conséquent les H_i, $1 \leq i \leq r$, sont en somme directe.

D'après ce qui précède les différents p-Sylow d'un groupe abélien fini G sont en somme directe. L'égalité des cardinaux assure que G est la somme directe de ses sous-groupes de Sylow.

Exercice 205 Soit G un groupe abélien fini. Montrer qu'il existe dans G un élément dont l'ordre est égal à l'exposant de G.

Éléments de réponse 205 Soit G un groupe abélien fini. Montrons qu'il existe dans G un élément dont l'ordre est égal à l'exposant de G. Le théorème de structure assure que

$$\mathrm{G} \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$$

où d_i divise d_{i+1} pour tout $1 \leq i \leq r-1$.

L'exposant de G est d_r et $(0, 0, \ldots, 0, 1)$ est d'ordre d_r.

Exercice 206

a) Donner la décomposition primaire du groupe $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$. En déduire ses facteurs invariants.

b) Donner la décomposition primaire du groupe $\mathbb{Z}/54\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$. En déduire ses facteurs invariants.

Éléments de réponse 206

a) Donnons la décomposition primaire du groupe $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$.

Notons que $8 = 2^3$, $12 = 2^2 \times 3$ et $24 = 2^3 \times 3$. Ainsi

$$\mathrm{G} \simeq \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2^3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

et les diviseurs élémentaires de G sont 2^3, 2^2, 3, 2^3 et 3.

Déterminons les facteurs invariants de G. Réordonnons les diviseurs élémentaires comme suit

$$\begin{array}{c} 2^2 \mid 2^3 \mid 2^3 \\ 3 \mid 3 \end{array}$$

Les facteurs invariants de G sont donc $2^2 \times 1 = 4$, $2^3 \times 3 = 24$ et $2^3 \times 3 = 24$.

Par conséquent

$$\mathrm{G} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}.$$

b) Donnons la décomposition primaire du groupe $\mathbb{Z}/54\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$.
Notons que $54 = 2 \times 3^3$, $26 = 2 \times 13$ et $15 = 3 \times 5$. Ainsi

$$\mathrm{G} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

et les diviseurs élémentaires de G sont 2, 3^3, 2, 13, 3 et 5.
Donnons ses facteurs invariants. On ordonne les diviseurs élémentaires comme suit

$$\begin{array}{c} 2 \mid 2 \\ 3 \mid 3^3 \\ 5 \\ 13 \end{array}$$

Les facteurs invariants de G sont donc $2 \times 3 = 6$ et $2 \times 3^3 \times 5 \times 13 = 3510$.

Exercice 207

a) Le nombre de classes de conjugaison dans $\mathcal{S}_5$ est le même que le nombre de groupes abéliens de cardinal 32 à isomorphisme près. Pourquoi ?

b) Généraliser au nombre de classes de conjugaison dans $\mathcal{S}_n$.

Éléments de réponse 207

a) Le nombre de classes de conjugaison dans $\mathcal{S}_5$ est le même que le nombre de groupes abéliens de cardinal 32 à isomorphisme près. Expliquons pourquoi. Le nombre de classes de conjugaison dans $\mathcal{S}_5$ et le nombre de groupes abéliens de cardinal 32 à isomorphisme près sont chacun en bijection avec l'ensemble des partitions de 5 (rappelons qu'une partition d'un entier est une décomposition de cet entier en une somme d'entiers strictement positifs à l'ordre près des termes).

b) Généralisons au nombre de classes de conjugaison dans $\mathcal{S}_n$. Soit p un nombre premier. Notons G_n l'ensemble des classes d'isomorphismes de groupes abéliens de cardinal p^n, P_n l'ensemble des partitions de l'entier n et C_n l'ensemble des classes de conjugaison dans $\mathcal{S}_n$. Considérons

$$\varphi\colon P_n \to G_n \qquad (n_1, n_2, \ldots, n_r) \mapsto \text{ classe d'isomorphisme de } \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$$

et

$$\psi\colon P_n \to C_n \qquad (n_1, n_2, \ldots, n_r) \mapsto \text{ classe de conjugaison de la permutation } (1, 2, \ldots, n_1)(n_1+1, \ldots, n_1+n_2)\ldots(n_1+n_2+n_{r-1}+1, \ldots, n)$$

φ et ψ sont des bijections donc $|C_n| = |G_n|$: il y a autant de classes de conjugaison dans $\mathcal{S}_n$ que de classes d'isomorphisme de groupes abéliens d'ordre p^n.

Exercice 208 Déterminer la structure des groupes abéliens de type fini suivants :

$$\mathbb{Z}^2/\langle(1,3),(2,0)\rangle \qquad \mathbb{Z}^2/\langle(1,1),(1,-1)\rangle.$$

Éléments de réponse 208 Déterminons la structure du groupe abélien de type fini

$$\mathbb{Z}^2/\langle(1,3),(2,0)\rangle.$$

On a

$$\begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 3 & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix} \simeq \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

Par suite $\mathbb{Z}^2/\langle(1,3),(2,0)\rangle \simeq \mathbb{Z}/6\mathbb{Z}$.

On a

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 1 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

Par conséquent $\mathbb{Z}^2/\langle(1,1),(1,-1)\rangle \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercice 209 Soit H le sous-groupe de $\mathbb{Z}^2$ engendré par $(2,5)$, $(5,-1)$ et $(1,-2)$. Déterminer une base de H et décrire le quotient $\mathbb{Z}^2/\mathrm{H}$.

Éléments de réponse 209 On a

$$\begin{pmatrix} 2 & 5 & 1 \\ 5 & -1 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 \\ 9 & 9 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 1 \\ 0 & 9 & -2 \end{pmatrix}$$

donc $\mathrm{H} = \langle(0,9),(1,-2)\rangle$ est de rang 2.

De plus $\begin{pmatrix} 0 & 1 \\ 9 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 9 & 0 \end{pmatrix}$; par suite $\mathbb{Z}^2/\mathrm{H} \simeq \mathbb{Z}/9\mathbb{Z}$.

Exercice 210 Trouver une base du groupe suivant :

$$\mathrm{G} = \left\{(x,y,z) \in \mathbb{Z}^3 \;\middle|\; \begin{cases} 2x+3y+5z=0 \\ 3x-6y+2z=0 \end{cases}\right\}$$

Éléments de réponse 210 Soit G le groupe donné par :

$$\mathrm{G} = \left\{(x,y,z) \in \mathbb{Z}^3 \;\middle|\; \begin{cases} 2x+3y+5z=0 \\ 3x-6y+2z=0 \end{cases}\right\}$$

On a

$$\mathrm{G} = \left\{(x,y,z) \in \mathbb{Z}^3 \;\middle|\; \begin{cases} 2x+3y+5z=0 \\ 7x+12z=0 \end{cases}\right\}$$

Comme $7x + 12z = 0$ on écrit $x = 12k$ et $z = -7k$. Alors $2x + 3y + 5z = 0$ conduit à $3y = 11k$. On pose donc $k = 3l$ alors

$$x = 36\ell, \qquad y = 11\ell, \qquad z = -21\ell$$

Finalement

$$\mathrm{G} = \{\ell(36, 11, -21) \,|\, \ell \in \mathbb{Z}\} = \mathrm{Vect}(36, 11, -21)$$

et $\{(36, 11, -21)\}$ est une base de G.

Exercice 211 Soit G un groupe abélien fini.

Supposons que pour tout diviseur d de l'ordre n de G, il existe un et un seul sous-groupe d'ordre d dans G. Montrer que G est cyclique.

Éléments de réponse 211 Raisonnons par l'absurde. Supposons que G ne soit pas cyclique. Alors G est isomorphe à $\mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z} \times \ldots \times \mathbb{Z}/q_k\mathbb{Z}$ où $q_1|q_2|\ldots|q_k$ sont les invariants de G et $k \geq 2$. Il y a alors (au moins) deux sous-groupes distincts d'ordre q_1 : d'une part le facteur $\mathbb{Z}/q_1\mathbb{Z}$ et d'autre part l'unique sous-groupe d'ordre q_1 du facteur $\mathbb{Z}/q_2\mathbb{Z}$ associé au diviseur q_1 de q_2.

Exercice 212 Soit p un nombre premier. Soit G un groupe abélien fini d'ordre n tel que tous les éléments de G soient d'ordre une puissance de p.

1. Soit g un élément de $\mathrm{G} \setminus \{\mathrm{id}\}$. Soit $\mathrm{H} = \langle g \rangle$ le sous-groupe cyclique engendré par g.

   Montrer que tous les éléments de G/H sont d'ordre une puissance de p.

2. En déduire par récurrence sur n que G est d'ordre une puissance de p.

   (Indication : prendre comme hypothèse de récurrence que tous les groupes d'ordre $< n$ dont tous les éléments sont d'ordre une puissance de p sont d'ordre une puissance de p).

3. Soit G un groupe fini abélien d'ordre 12.

   Montrer que si G ne contient pas d'élément d'ordre 3, il ne contient que des éléments d'ordre 1, 2 ou 4.

   En déduire que G possède un élément d'ordre 3.

4. Supposons désormais que G est un groupe abélien d'ordre 12 non cyclique. Soit $\mathrm{g} \in \mathrm{G}$ un élement d'ordre 3. Soit $\mathrm{H} = \langle g \rangle$ le sous-groupe cyclique engendré par $\langle g \rangle$. Montrer que G/H ne peut être cyclique.

5. En déduire que $\mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

6. Montrer que $\mathrm{G} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Éléments de réponse 212

Exercice 213

1. Quels sont les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$?

   Montrer que si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ est la décomposition de n en produit de facteurs premiers, alors il y a exactement $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)$ sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.
2. Montrer que dans un groupe cyclique tous les sous-groupes sont caractéristiques [10].
3. Déduire de l'existence d'un p-Sylow dans un groupe G d'ordre $p^\alpha n$ (où p désigne un entier premier, n un entier premier avec p et $\alpha \geq 1$), le théorème de Cauchy, *i.e.* l'existence d'un élément d'ordre p.
4. Montrer qu'un groupe fini G a pour ordre une puissance d'un nombre premier p si et seulement si tout élément du groupe G a pour ordre une puissance de p.

Éléments de réponse 213

Exercice 214

1. Les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$ et $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$ sont-ils isomorphes ?
2. Les groupes $\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$ et $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}$ sont-ils isomorphes ?

Éléments de réponse 214

1. Les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z}$ et $\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$ ne sont pas isomorphes. En effet posons
   $$\mathrm{G}_1 = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/72\mathbb{Z} \qquad \mathrm{G}_2 = \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}.$$
   Nous avons $12 = 2^2 \times 3$, $72 = 2^3 \times 3^2$, $18 = 2 \times 3^2$ et $48 = 2^4 \times 3$. Les groupes G_1 et G_2 sont tous deux d'ordre $2^5 \times 3^3$. Les groupes G_i sont isomorphes à $\mathrm{A}_i \times \mathrm{B}_i$ pour $i = 1, 2$ où A_i est un groupe abélien d'ordre 2^5 et B_i un groupe abélien d'ordre 3^3. Le groupe A_1 est associé à la partition $(3, 2)$ de 5 et le groupe A_2 est associé à la partition $(4, 1)$ de 5 ; ils ne sont donc pas isomorphes. Par suite les groupes G_1 et G_2 ne sont pas isomorphes.
2. Les groupes $\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$ et $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}$ sont isomorphes. En effet posons
   $$\mathrm{G}_1 = \mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \qquad \mathrm{G}_2 = \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}.$$

Nous avons $72 = 2^3 \times 3^2$, $84 = 2^2 \times 3 \times 7$, $36 = 2^2 \times 3^2$ et $168 = 2^3 \times 3 \times 7$. Les groupes G_1 et G_2 sont donc de même ordre $2^5 \times 3^3 \times 7$. Les groupes G_i sont isomorphes à $\mathrm{A}_i \times \mathrm{B}_i \times \mathrm{C}_i$ où A_i est un groupe abélien d'ordre 2^5, B_i est un groupe abélien d'ordre 3^3 et C_i est un groupe abélien d'ordre 7. Les groupes A_1 et A_2 sont associés à la partition $(3, 2)$ de 5, ils sont isomorphes. Les groupes B_1 et B_2 sont associés à la partition $(2, 1)$ de 3 ; ils sont donc isomorphes. Les groupes C_1 et C_2 sont isomorphes. Il en résulte que G_1 et G_2 sont isomorphes.

Exercice 215 Trouver tous les couples d'entiers naturels (a, b) tels que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ soit isomorphe à $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

10. Soit G un groupe. Un sous-groupe de G qui est stable par tout automorphisme de G est dit caractéristique.

Éléments de réponse 215

Exercice 216 Soient a, b, c et d quatre entiers deux à deux premiers entre eux.
Montrer que $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ est isomorphe à $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$.

Éléments de réponse 216 Soient a, b, c et d quatre entiers deux à deux premiers entre eux.
Montrons que $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ est isomorphe à $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$.
Les nombres a, b, c et d étant premiers entre deux à deux nous avons

$$\begin{aligned}\mathbb{Z}/ab\mathbb{Z} &\simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}\\ \mathbb{Z}/cd\mathbb{Z} &\simeq \mathbb{Z}/c\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}\\ \mathbb{Z}/ac\mathbb{Z} &\simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}\\ \mathbb{Z}/bd\mathbb{Z} &\simeq \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}\end{aligned}$$

Par suite les deux groupes $\mathbb{Z}/ab\mathbb{Z} \times \mathbb{Z}/cd\mathbb{Z}$ et $\mathbb{Z}/ac\mathbb{Z} \times \mathbb{Z}/bd\mathbb{Z}$ sont isomorphes.

Exercice 217 Soit $\mathrm{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. Considérons les deux sous-groupes suivants de G :

$$\mathrm{H} = \mathbb{Z}/2\mathbb{Z} \times \{0\} \qquad\qquad \mathrm{K} = \{0\} \times \{0, 6\}.$$

Remarquons que $\mathrm{G} \simeq \mathrm{K} \simeq \mathbb{Z}/2\mathbb{Z}$ mais avons-nous $\mathrm{G}/\mathrm{H} \simeq \mathrm{G}/\mathrm{K}$?

Éléments de réponse 217 D'une part $\mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, d'autre part $\mathrm{G}/\mathrm{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) \times \mathbb{Z}/3\mathbb{Z}$.
Les deux premiers facteurs ne sont pas isomorphes donc les deux groupes ne sont pas isomorphes.

Exercice 218 Soient G, H et K des groupes abéliens finis.

1. Montrer que si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $\mathrm{G} \simeq \mathrm{H}$.
2. Montrer que si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $\mathrm{G} \simeq \mathrm{H}$.

Éléments de réponse 218 Soient G, H et K des groupes abéliens finis. Montrons que si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $\mathrm{G} \simeq$ Het que si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $\mathrm{G} \simeq \mathrm{H}$.
La décomposition primaire de G est $\prod_{i=1}^{s} \mathrm{A}_i$, celle de $\mathrm{G} \times \mathrm{G}$ est donc $\prod_{i=1}^{s} \mathrm{A}_i \times \mathrm{A}_i$.
La décomposition primaire de H est $\prod_{i=1}^{t} \mathrm{B}_i$, celle de $\mathrm{H} \times \mathrm{H}$ est donc $\prod_{i=1}^{t} \mathrm{B}_i \times \mathrm{B}_i$.
La décomposition primaire de K est $\prod_{i=1}^{u} \mathrm{C}_i$, celle de $\mathrm{G} \times \mathrm{K}$ est donc $\prod_{i=1}^{s} \mathrm{A}_i \times \prod_{i=1}^{u} \mathrm{C}_i$ et celle de $\mathrm{H} \times \mathrm{K}$ est donc $\prod_{i=1}^{s} \mathrm{B}_i \times \prod_{i=1}^{u} \mathrm{C}_i$.

Si $\mathrm{G} \times \mathrm{G} \simeq \mathrm{H} \times \mathrm{H}$, alors $s = t$ et $\mathrm{A}_i = \mathrm{B}_i$ pour tout i. Par suite $\mathrm{G} \simeq \mathrm{H}$.
Si $\mathrm{G} \times \mathrm{K} \simeq \mathrm{H} \times \mathrm{K}$, alors $s = t$ et $\mathrm{A}_i = \mathrm{B}_i$ pour tout i. Par conséquent $\mathrm{G} \simeq \mathrm{H}$.

Exercice 219

1. Exprimer tous les groupes abéliens d'ordre 99 comme sommes directes de sous-groupes cycliques.
2. Exprimer tous les groupes abéliens d'ordre 100 comme sommes directes de sous-groupes cycliques.

Éléments de réponse 219

1. Exprimons tous les groupes abéliens d'ordre 99 comme sommes directes de sous-groupes cycliques.

   Les groupes abéliens d'ordre $99 = 3^2 \times 11$ sont isomorphes
   - soit à $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$,
   - soit à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$.
2. Exprimons tous les groupes abéliens d'ordre 100 comme sommes directes de sous-groupes cycliques. Les groupes abéliens d'ordre $100 = 2^2 \times 5^2$ sont isomorphes
   - soit à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
   - soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$,
   - soit à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$,
   - soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Exercice 220 Combien existe-t-il, à isomorphisme près, de groupes abéliens d'ordre 10^6 ?

Éléments de réponse 220 Nous avons $10^6 = 2^6 \times 5^6$. Les partitions de 6 sont

$$
\begin{gathered}
(6) \\
(5,1) \\
(4,2) \\
(4,1,1) \\
(3,3) \\
(3,2,1) \\
(3,1,1,1) \\
(2,2,2) \\
(2,2,1,1) \\
(2,1,1,1,1) \\
(1,1,1,1,1,1)
\end{gathered}
$$

Elles sont donc au nombre de 11. Il y a donc à isomorphisme près $11^2 = 121$ groupes abéliens d'ordre 10^6.

Exercice 221

1. Soient G, H, G′ et H′ des groupes finis tels que $\mathrm{G} \simeq \mathrm{G}'$ et $\mathrm{G} \times \mathrm{H} \simeq \mathrm{G}' \times \mathrm{H}'$. Nous allons montrer qu'alors $\mathrm{H} \simeq \mathrm{H}'$.
   Étant donnés deux groupes finis G_1 et G_2, notons $m(\mathrm{G}_1, \mathrm{G}_2)$ le nombre de morphismes de groupes de G_1 vers G_2 et $i(\mathrm{G}_1, \mathrm{G}_2)$ le nombre de morphismes de groupes injectifs de G_1 vers G_2.
   a) Utiliser le premier théorème d'isomorphisme pour montrer que

$$m(\mathrm{G}_1, \mathrm{G}_2) = \sum_{\mathrm{N} \trianglelefteq \mathrm{G}_1} i\Big(\mathrm{G}_1 \big/ \mathrm{N}, \mathrm{G}_2\Big). \tag{5.7.1}$$

   b) Montrer pour tout groupe fini L que

$$m(\mathrm{L}, \mathrm{G}) \cdot m(\mathrm{L}, \mathrm{H}) = m(\mathrm{L}, \mathrm{G} \times \mathrm{H}).$$

   c) En déduire que pour tout groupe fini L on a l'égalité $m(\mathrm{L}, \mathrm{H}) = m(\mathrm{L}, \mathrm{H}')$.
   d) Par récurrence sur l'ordre de L, montrer en utilisant l'équation (5.7.3) que

$$i(\mathrm{L}, \mathrm{H}) = i(\mathrm{L}, \mathrm{H}'). \tag{5.7.2}$$

   e) Appliquer l'équation (5.7.4) à H pour en déduire que $\mathrm{H} \simeq \mathrm{H}'$.
   f) Donner un contre-exemple qui montre que si G, H, G′ et H′ sont des groupes quelconques tels que $\mathrm{G} \simeq \mathrm{G}'$ et $\mathrm{G} \times \mathrm{H} \simeq \mathrm{G}' \times \mathrm{H}'$, alors en général H et H′ ne sont pas isomorphes.

2. Nous allons appliquer le résultat obtenu dans la partie 1. pour montrer *l'unicité* du théorème de structure des groupes abéliens finis.
   Soit G un groupe abélien fini. Supposons que

$$\mathrm{G} \simeq \mathbb{Z} \big/ n_1\mathbb{Z} \times \mathbb{Z} \big/ n_2\mathbb{Z} \times \cdots \times \mathbb{Z} \big/ n_r\mathbb{Z}$$

   avec $n_r \mid n_{r_1} \mid \cdots n_2 \mid n_1$.
   a) Montrer que l'exposant de G est égal à n_1.
   b) Utiliser le résultat obtenu dans la partie 1. pour montrer que cette décomposition est unique.

Éléments de réponse 221

Exercice 222 Soit G un groupe abélien fini. Les assertions suivantes sont-elles vraies ou fausses ?

a) Pour tout d qui divise l'ordre de G, le groupe G admet un élément d'ordre d.
b) Pour tout d qui divise l'ordre de G, le groupe G admet un sous-groupe d'ordre d.

Éléments de réponse 222

Exercice 223

a) Déterminer à isomorphisme près tous les groupes abéliens d'ordre 12 et 72.

b) Déterminer à isomorphisme près tous les groupes abéliens d'ordre 10^6.

Éléments de réponse 223

a) Déterminons à isomorphisme près tous les groupes abéliens d'ordre 12.

Nous avons $12 = 2^2 \times 3$. De plus les partitions de 2 sont

$$2 \qquad\qquad 1, 1$$

Par conséquent il y a à isomorphisme près 2 groupes abéliens d'ordre 12 :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \qquad\qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

Déterminons à isomorphisme près tous les groupes abéliens d'ordre 72.

Nous avons $72 = 2^3 \times 3^2$. De plus les partitions de 2 sont

$$2 \qquad\qquad 1, 1$$

et celles de 3 sont

$$3 \qquad\qquad 2, 1 \qquad\qquad 1, 1, 1$$

Par conséquent il y a à isomorphisme près $2 \times 3 = 6$ groupes abéliens d'ordre 72 :

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/é\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \qquad \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/é\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

b) Déterminons à isomorphisme près tous les groupes abéliens d'ordre 10^6.

Nous avons $10^6 = 2^6 \times 5^6$. De plus les partitions de 6 sont

6

5, 1

4, 2

4, 1, 1

3, 3

3, 2, 1

3, 1, 1, 1

2, 2, 2

2, 2, 1, 1

2, 1, 1, 1, 1, 1

1, 1, 1, 1, 1, 1

Il y a donc à isomorphisme près $11^2 = 121$ groupes abéliens d'ordre 10^6.

Exercice 224

a) Soit G le groupe abélien de type fini

$$\langle g_1, g_2, g_3 \mid 5g_1 - 2g_2 + 12g_3 = 3g_1 + 4g_3 = 0\rangle.$$

Déterminer la structure de ce groupe.

b) Soit G le groupe abélien de type fini

$$\langle g_1, g_2, g_3, g_4 \mid 2g_1 + 4g_2 - 4g_4 = 6g_1 - 12g_3 + 3g_4 = 0\rangle.$$

Déterminer la structure de ce groupe.

Éléments de réponse 224

Exercice 225 Montrer que les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ et $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ sont isomorphes.

Éléments de réponse 225 Nous utilisons le lemme chinois pour voir que les deux groupes sont isomorphes au groupe

$$\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\right) \times \left(\mathbb{Z}/3\mathbb{Z} \times 9\mathbb{Z}/\mathbb{Z}\right) \times \left(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}\right)$$

Notons que cette écriture est la décomposition en composantes p-primaires.

Nous pouvons aussi écrire la décomposition en facteurs invariants de ces deux groupes, nous trouvons

$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/900\mathbb{Z}.$$

Exercice 226 Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Éléments de réponse 226 Montrons qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Soit G un groupe abélien fini non cyclique. Il est isomorphe à un produit

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \dots \mathbb{Z}/d_r\mathbb{Z}$$

avec $d_i \geq 2$ et $d_i \,|\, d_{i+1}$. Puisque G n'est pas cyclique, $r \geq 2$. Soit p un facteur premier de d_1 alors p disvise tous les d_i et $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à un sous-groupe de chacun des $\mathbb{Z}/d_i\mathbb{Z}$ (c'est le sous-groupe de p-torsion). Le sous-groupe de p torsion de G est isomorphe à $\left(\mathbb{Z}/p\mathbb{Z}\right)^r$ qui contient un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 227

a) Combien y a-t-il de groupes abéliens de cardinal 360 ? Faire la liste complète de ces groupes.

b) Plus généralement, pour tout entier n, combien y a-t-il de groupes abéliens de cardinal n ?

Éléments de réponse 227

a) La décomposition de 360 en facteurs premiers est $2^3 \times 3^2 \times 5$. Ainsi si G est un groupe de cardinal 360, alors le sous-groupe

$$T_2(\mathrm{G}) = \{g \in \mathrm{G} \,|\, \exists\, n \in \mathbb{N} \quad 2^n g = 0\}$$

de 2-torsion de G est un groupe abélien de cardinal 2^3, il y a donc trois classes d'isomorphisme de tels groupes : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$. De même il y a exactement deux classes d'isomorphisme possibles pour $T_3(\mathrm{G})$ à savoir $\mathbb{Z}/9\mathbb{Z}$ et $\left(\mathbb{Z}/3\mathbb{Z}\right)^2$. Par ailleurs $T_5(\mathrm{G})$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Il y a donc exactement six classes d'isomorphisme de groupes abéliens d'ordre 360 donc les décompositions p-primaires et les décompositions en facteurs invariants sont les suivantes :

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/360\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times 4\mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$
$$\left(\mathbb{Z}/2\mathbb{Z}\right)^3 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$$
$$\mathbb{Z}/8\mathbb{Z} \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$$

$$\left(\mathbb{Z}/2\mathbb{Z}\right)^3 \times \left(\mathbb{Z}/3\mathbb{Z}\right)^2 \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$$

b) Plus généralement, pour tout entier n, déterminons le nombre de groupes abéliens de cardinal n. Nous utilisons la classification des classes d'isomorphisme de groupes abéliens finis. Soit $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers. La classe d'isomorphisme d'un groupe abélien d'ordre n est caractérisée par ses facteurs invariants $(d_1, d_2, \dots, d_s)$ qui sont des entiers > 1 tels que $d_i \mid d_{i+1}$ et $d_1 d_2 \dots d_s = n$. Par suite chaque d_i se décompose comme suit : $d_i = p_1^{\alpha_{1,i}} p_2^{\alpha_{2,i}} \dots p_r^{\alpha_{r,i}}$ avec les contraintes suivantes : $\alpha_{i,j} \leq \alpha_{i+1,j}$ pour tout j, pour tout i et $\sum_{i=1}^{s} \alpha_{i,j} = \alpha_j$ et $\sum_{i=1}^{q} \alpha_{i,j} = \alpha_j$.

Il s'en suit que le nombre de choix possibles pour les a_i est exactement $\prod_{j=1}^{r} p(\alpha_j)$ où $p(\alpha)$ désigne le nombre de partitions de α, *i.e.* le nombre de façons d'écrire l'entier α comme une somme croissante d'entiers strictement positifs.

Exercice 228

a) On considère $\mathrm{H} = \{(a,b) \in \mathbb{Z}^2 \mid a - b \text{ est divisible par } 10\}$. Montrer que H est un sous-groupe de $\mathbb{Z}^2$. Calculer le rang de H. Donner une base de H. Décrire le quotient $\mathbb{Z}^2/\mathrm{H}$.

b) On note H le quotient de $\mathbb{Z}^3$ par le sous-groupe engendré par les vecteurs $(4,8,10)$ et $(6,2,0)$. Déterminer la structure du groupe H.

Éléments de réponse 228

a) Soit φ le morphisme de groupes donné par

$$\varphi\colon \mathbb{Z}^2 \to \mathbb{Z}/10\mathbb{Z}, \qquad (a,b) \mapsto a - b$$

Son noyau est H. En particulier H est un sous-groupe distinugé de $\mathbb{Z}^2$.

D'une part H contient $(1,1)$ et $(0,10)$ donc $\operatorname{rg} \mathrm{H} \geq 2$. D'autre part $\mathrm{H} \subset \mathbb{Z}^2$ donc $\operatorname{rg} \mathrm{H} \leq 2$. Finalement $\operatorname{rg} \mathrm{H} = 2$.

Soit (a,b) dans H. Il existe n dans $\mathbb{Z}$ tel que $a = b + 10n$ et

$$(a,b) = (a, a - 10n) = a(1,1) + (-n)(0,10).$$

Autrement dit $((1,1),(0,10))$ est une base de H.

Par ailleurs

$$\mathbb{Z}^2/\mathrm{H} = \langle (g_1,g_2) \mid g_1 + g_2 = 0,\ 10g_2 = 0 \rangle.$$

Puisque $\begin{pmatrix} 1 & 0 \\ 1 & 10 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix}$ les facteurs invariants de $\mathbb{Z}^2/\mathrm{H}$ sont 1 et 10 et $\mathbb{Z}^2/\mathrm{H} \simeq \mathbb{Z}/10\mathbb{Z}$.

b) Notons H le quotient de $\mathbb{Z}^3$ par le sous-groupe engendré par les vecteurs $(4, 8, 10)$ et $(6, 2, 0)$. Déterminons la structure du groupe H. Nous avons

$$\begin{pmatrix} 4 & 6 \\ 8 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} -20 & 0 \\ 8 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} -20 & 0 \\ 0 & 2 \\ 10 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 \\ 0 & 2 \\ 10 & 0 \end{pmatrix}$$

Ainsi les facteurs invariants de $\begin{pmatrix} 4 & 6 \\ 8 & 2 \\ 10 & 0 \end{pmatrix}$ sont 2 et 10 et $\mathrm{H} \simeq \mathbb{Z} \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{10\mathbb{Z}}$.

Exercice 229 Soit $n \geq 1$ un entier. Montrer que tout système libre maximal dans $\mathbb{Z}^n$ est de cardinal n.

Donner un exemple où un tel système n'est pas une base.

Éléments de réponse 229

Exercice 230 Soit $e_1 = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$ un vecteur tel que le pgcd de ses coordonnées vaut 1. Montrer que l'on peut compléter e_1 en une base $(e_1, e_2, \ldots, e_n)$ de $\mathbb{Z}^n$.

Éléments de réponse 230

Exercice 231 Déterminer les facteurs invariants des matrices suivantes à coefficients dans $\mathbb{Z}$:

a) $\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix}$;

b) $\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix}$;

c) $\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix}$.

Éléments de réponse 231 Nous pouvons procéder de deux manières différentes :

- soit en calculer le pgcd des coefficients de la matrice puis le pgcd des mineurs de taille 2, etc
- soit en appliquant l'algorithme de réduction des matrices à coefficients entiers via des opérations élémentaires sur les lignes et les colonnes.

Dans les deux cas nous obtenons ($\sim$ désigne l'équivalence des matrices à coefficients entiers) :

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix} \sim \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 16 \end{pmatrix}$$

Les facteurs invariants sont donc respectivement $(1, 6)$, $(3, 9)$ et $(1, 2, 16)$.

Détaillons la première équivalence :

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 \\ 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 \\ 0 & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

Détaillons la seconde équivalence

$$\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix} \sim \begin{pmatrix} 12 & -27 \\ 69 & -153 \end{pmatrix} \sim \begin{pmatrix} 12 & -27 \\ 9 & -18 \end{pmatrix} \sim \begin{pmatrix} 12 & -3 \\ 9 & 0 \end{pmatrix} \sim \begin{pmatrix} 12 & 3 \\ 9 & 0 \end{pmatrix} \sim \begin{pmatrix} 3 & 12 \\ 0 & 9 \end{pmatrix} \sim \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix}$$

Exercice 232

a) Soit G un groupe abélien de type fini. Soit $f\colon \mathrm{G} \to \mathrm{G}$ un morphisme surjectif. Montrer que f est un isomorphisme.

Ceci est-il nécessairement vrai si on remplace surjectif par injectif ?

b) Soit G un groupe abélien libre de type fini et soit $f\colon \mathrm{G} \to \mathrm{G}$ un morphisme. Définir le déterminant $\det(f) \in \mathbb{Z}$ de f. Montrer que f est injectif si et seulement si $\det(f) \neq 0$. Dans ce cas montrer que $|\det(f)| = |\mathrm{coker}(f)|$.

Éléments de réponse 232

Exercice 233 Le but de cet exercice est de redémontrer le théorème de structure des groupes abéliens finis.

On rappelle qu'un caractère d'un groupe abélien fini G est un morphisme $\mathrm{G} \to \mathbb{C}^*$.

a) Si H est un sous-groupe d'un groupe abélien fini G, montrer que tout caractère de H se prolonge en un caractère de G.

b) Soit G un groupe abélien fini. On désigne par H un sous-groupe de G engendré par un élément de G d'ordre maximal. Montrer qu'on a l'isomorphisme $\mathrm{G} \simeq \mathrm{H} \times {}^{\mathrm{G}}\!/_{\mathrm{H}}$.

c) Conclure.

Éléments de réponse 233

Exercice 234 [Propriété d'annulation de groupes dans un produit direct (démonstration de Vipul Naik)]

A. Soient G, H, G′ et H′ des groupes finis tels que $G \simeq G'$ et $G \times H \simeq G' \times H'$. Nous allons montrer qu'alors $H \simeq H'$.
Étant donnés deux groupes finis G_1 et G_2, notons $m(G_1, G_2)$ le nombre de morphismes de groupes de G_1 vers G_2 et $i(G_1, G_2)$ le nombre de morphismes de groupes injectifs de G_1 vers G_2.
a) Utiliser le premier théorème d'isomorphisme pour montrer que

$$m(G_1, G_2) = \sum_{N \trianglelefteq G_1} i\Big({}^{G_1}\!/_{N}, G_2\Big). \tag{5.7.3}$$

b) Montrer pour tout groupe fini L que

$$m(L, G) \cdot m(L, H) = m(L, G \times H).$$

c) En déduire que pour tout groupe fini L on a l'égalité $m(L, H) = m(L, H')$.
d) Par récurrence sur l'ordre de L, montrer en utilisant l'équation (5.7.3) que

$$i(L, H) = i(L, H'). \tag{5.7.4}$$

e) Appliquer l'équation (5.7.4) à H pour en déduire que $H \simeq H'$.
f) Donner un contre-exemple qui montre que si G, H, G′ et H′ sont des groupes quelconques tels que $G \simeq G'$ et $G \times H \simeq G' \times H'$, alors en général H et H′ ne sont pas isomorphes.

B. Nous allons appliquer le résultat obtenu dans la partie A. pour montrer *l'unicité* du théorème de structure des groupes abéliens finis.
Soit G un groupe abélien fini. Supposons que

$$G \simeq {}^{\mathbb{Z}}\!/_{n_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{n_2\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}\!/_{n_r\mathbb{Z}},$$

avec $n_r \mid n_{r_1} \mid \cdots n_2 \mid n_1$.
a) Montrer que l'exposant de G est égal à n_1.
b) Utiliser le résultat obtenu dans la partie A. pour montrer que cette décomposition est unique.

Éléments de réponse 234

Exercice 235 Soit $\Bbbk$ un corps commutatif. Soit G un sous-groupe fini du groupe multiplicatif $\Bbbk^\times = \Bbbk \smallsetminus \{0\}$ de $\Bbbk$. Montrer que G est cyclique.

Éléments de réponse 235 Nous utilisons le théorème de structure des groupes abéliens finis. Si $|G| > 1$, alors il existe une suite d'entiers $1 < a_1 \,|\, a_2 \,|\, \ldots \,|\, a_r$ tels que

$$G \simeq {}^{\mathbb{Z}}\!/_{a_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{a_2\mathbb{Z}} \times \ldots \times {}^{\mathbb{Z}}\!/_{a_r\mathbb{Z}}$$

Montrons que $r = 1$. Puisque $a_r G = \{0\}$ nous avons

$$\#\{z \in \Bbbk \,|\, z^{a_r} = 1\} \geq |G| = a_1 a_2 \ldots a_r.$$

Par ailleurs le nombre de racines dans $\Bbbk$ du polynôme $X^{a_r} - 1 \in \Bbbk[X]$ est inférieur ou égal à son degré parce que $\Bbbk$ est commutatif. Il en résulte l'inégalité $a_1 a_2 \dots a_r \leq a_r$ qui conduit à $r = 1$.

5.8. Produits semi-directs

Exercice 236 Soient N et H des groupes et soit $\phi\colon \mathrm{H} \to \mathrm{Aut(N)}$ un morphisme de groupes. Notons $\mathrm{N} \rtimes_\phi \mathrm{H}$ l'ensemble $\mathrm{N} \times \mathrm{H}$ muni de la loi de composition définie par

$$(n_1, h_1) \rtimes_\phi (n_2, h_2) = \big(n_1 \phi(h_1)(n_2), h_1 h_2\big).$$

1. Montrer que $\mathrm{N} \rtimes_\phi \mathrm{H}$ est un groupe appelé produit semi-direct de H par N relativement à ϕ.
2. Montrer que $\mathrm{N} \times \{e_\mathrm{H}\} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$ et $\{e_\mathrm{N}\} \times \mathrm{H} \subset \mathrm{N} \rtimes_\phi \mathrm{H}$.
3. Identifier le quotient de $\mathrm{N} \rtimes_\phi \mathrm{H}$ par $\mathrm{N} \times \{e_\mathrm{H}\}$.

Éléments de réponse 236

1. Montrons que $\mathrm{N} \rtimes_\phi \mathrm{H}$ est un groupe.
   - Commençons par montrer que la loi est associative.
     Soient n_1, n_2 et n_3 dans N. Soient h_1, h_2 et h_3 dans H. Par définition du produit nous avons

$$\big((n_1, h_1) \rtimes_\phi (n_2, h_2)\big) \rtimes_\phi (n_3, h_3) = \big(n_1 \phi(h_1)(n_2), h_1 h_2\big) \rtimes_\phi (n_3, h_3) = \big(n_1 \phi(h_1)(n_2) \phi(h_1 h_2)(n_3), h_1 h_2 h_3\big).$$

     De même nous avons

$$(n_1, h_1) \rtimes_\phi \big((n_2, h_2) \rtimes_\phi (n_3, h_3)\big) = (n_1, h_1) \rtimes_\phi \big(n_2 \phi(h_2)(n_3), h_2 h_3\big) = \big(n_1 \phi(h_1)\big(n_2 \phi(h_2)(n_3)\big)\big), h_1 h_2 h_3\big).$$

     Or $\phi(h_1)$ et ϕ sont des morphismes donc

     $$\phi(h_1)\big(n_2 \phi(h_2)(n_3)\big) = \phi(h_1)(n_2)\big(\phi(h_1) \circ \phi(h_2)\big)(n_3) = \phi(h_1)(n_2)\big(\phi(h_1 h_2)\big)(n_3)$$

     dont on déduit que

     $$\big((n_1, h_1) \rtimes_\phi (n_2, h_2)\big) \rtimes_\phi (n_3, h_3) = (n_1, h_1) \rtimes_\phi \big((n_2, h_2) \rtimes_\phi (n_3, h_3)\big).$$

     Par conséquent le produit $\rtimes_\phi$ est associatif.
   - On voit tout de suite que l'élément $(e_\mathrm{N}, e_\mathrm{H})$ est neutre pour la loi $\rtimes_\phi$.
   - Montrons que tout élément admet un inverse.
     Soient $n \in \mathrm{N}$ et $h \in \mathrm{H}$. Pour tous $n' \in \mathrm{N}$ et $h' \in \mathrm{H}$ nous avons

     $$(n, h) \rtimes_\phi (n', h') = (e_\mathrm{N}, e_\mathrm{H})$$

     si et seulement si

     $$(n \phi(n')(h'), h h') = (e_\mathrm{N}, e_\mathrm{H})$$

si et seulement si $h' = h^{-1}$ et $n' = \phi(h^{-1})(n^{-1})$. Le calcul de $(n', h') \rtimes_\phi (n, h)$ est similaire ce qui assure que (n, h) est inversible et que son inverse est $(n, h)^{-1} = (\phi(h^{-1})(n^{-1}), h^{-1})$.

Ainsi $\mathrm{N} \rtimes_\phi \mathrm{H}$ est bien un groupe.

2. Montrons que $\mathrm{N} \times \{e_\mathrm{H}\} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$ et $\{e_\mathrm{N}\} \times \mathrm{H} \subset \mathrm{N} \rtimes_\phi \mathrm{H}$.

Les formules définissant le produit assurent que $\mathrm{N} \times \{e_\mathrm{H}\}$ et $\{e_\mathrm{N}\} \times \mathrm{H}$ sont bien des sous-groupes de $\mathrm{N} \rtimes_\phi \mathrm{H}$ car $\phi(h)(e_\mathrm{N}) = e_\mathrm{N}$ pour tout $h \in \mathrm{H}$.

Montrons que $\mathrm{N} \times \{e_\mathrm{H}\}$ est distingué dans $\mathrm{N} \rtimes_\phi \mathrm{H}$. Soient n, n' dans N et h' dans H. Alors

$$\begin{aligned}(n, h) \rtimes_\phi (n', e_\mathrm{H}) \rtimes_\phi (n, h)^{-1} &= (n, h) \rtimes_\phi (n', e_\mathrm{H}) \rtimes_\phi (\phi(h^{-1})(n^{-1}), h^{-1}) \\ &= n\phi(h)(n'), h() \rtimes_\phi (\phi(h^{-1})(n^{-1}), h^{-1}) \\ &= (n\phi(h)(n')\phi(h)\big(\phi(h^{-1})(n^{-1})\big), e_\mathrm{H}) \\ &= (n\phi(h)(n')n^{-1}, e_\mathrm{H}) \in \mathrm{N} \times \{e_\mathrm{H}\}\end{aligned}$$

Ainsi $\mathrm{N} \times \{e_\mathrm{H}\}$ est distingué dans $\mathrm{N} \rtimes_\phi \mathrm{H}$.

Un calcul analogue montre que $\{e_\mathrm{N}\} \times \mathrm{H}$ n'est pas distingué en général.

3. Identifions le quotient de $\mathrm{N} \rtimes_\phi \mathrm{H}$ par $\mathrm{N} \times \{e_\mathrm{H}\}$.

Considérons l'application naturelle $\pi \colon \mathrm{N} \rtimes_\phi \mathrm{H} \to \mathrm{H}$ donnée par la seconde projection, *i.e.* $\pi(n, h) = h$.

Il est clair que π est surjective.

La définition de la loi de groupes assure que π est un morphisme de groupes.

Déterminons son noyau. Soient $n \in \mathrm{N}$ et $h \in \mathrm{H}$. Nous avons $\pi(n, h) = e_\mathrm{H}$ si et seulement si $h = e_\mathrm{H}$; ainsi $\ker \pi = \mathrm{N} \times \{e_\mathrm{H}\}$.

Finalement l'application π passe au quotient par son noyau et induit un isomorphisme de groupes :

$$\overline{\pi} \colon {}^{\mathrm{N} \rtimes_\phi \mathrm{H}}\!\diagup_{\mathrm{N} \times \{e_\mathrm{H}\}} \xrightarrow{\sim} \mathrm{H}$$

Exercice 237

Soit G un groupe. Soient N et H deux sous-groupes de G tels que $\mathrm{N} \cap \mathrm{H} = \{e\}$, $\mathrm{G} = \mathrm{NH}$ et $\mathrm{N} \lhd \mathrm{G}$.

1. Montrer que l'application

$$\begin{aligned} i \colon \mathrm{H} &\to \mathrm{Aut}(\mathrm{N}) \\ h &\mapsto i_h \colon \mathrm{N} \to \mathrm{N} \\ &\qquad n \mapsto hnh^{-1} \end{aligned}$$

est un morphisme de groupes.

2. Montrer que
$$f\colon \mathrm{N} \rtimes_i \mathrm{H} \to \mathrm{G} \qquad\qquad (n,h) \mapsto nh$$
est un isomorphisme de groupes.

On dit alors que G est le produit semi-direct de H par N.

Éléments de réponse 237

1. Montrons que l'application
$$\begin{array}{rcl} i\colon \mathrm{H} & \to & \mathrm{Aut(N)} \\ h & \mapsto & i_h\colon \mathrm{N} \to \mathrm{N} \\ & & \quad n \mapsto hnh^{-1} \end{array}$$
est un morphisme de groupes.

   L'application i est bien définie car $\mathrm{N} \lhd \mathrm{G}$. On vérifie directement que c'est un morphisme de groupes.

2. Montrons que
$$f\colon \mathrm{N} \rtimes_i \mathrm{H} \to \mathrm{G} \qquad\qquad (n,h) \mapsto nh$$
est un morphisme de groupes. Soient n, n' dans N et h, h' dans H. On a
$$f(n,h)f(n',h') = nhn'h'$$
et
$$f\big((n,h) \rtimes_i (n',h')\big) = f\big(ni(h)(n'),hh'\big) = f(nhn'h^{-1},hh') = nhn'h^{-1}hh' = nhn'h'$$
ce qui assure que $f\big((n,h) \rtimes_i (n',h')\big) = f(n,h)f(n',h')$. Ainsi f est bien un morphisme de groupes.

   Montrons maintenant que f est un isomorphisme de groupes. L'hypothèse $\mathrm{NH} = \mathrm{G}$ assure que f est surjectif et l'hypothèse $\mathrm{N} \cap \mathrm{H} = \{e\}$ assure que le noyau de f est trivial. Par suite f est un isomorphisme.

Exercice 238 Montrer que le produit semi-direct $\mathrm{N} \rtimes_\phi \mathrm{H}$ est direct si et seulement si ϕ est le morphisme trivial si et seulement si $\{e_\mathrm{N}\} \times \mathrm{H} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$.

Éléments de réponse 238 Le produit semi-direct $\mathrm{N} \rtimes_\phi \mathrm{H}$ est direct si et seulement si pour tous n, $n' \in \mathrm{N}$ et h, $h' \in \mathrm{H}$ on a
$$(n,h) \rtimes_\phi (n',h') = (n',hh')$$
si et seulement si pour tous n, $n' \in \mathrm{N}$ et $h \in \mathrm{H}$ $n\phi(h)(n') = nn'$ si et seulement si pour tous $n' \in \mathrm{N}$ et $h \in \mathrm{H}$ $\phi(h)(n') = nn'$ si et seulement si ϕ est le morphisme trivial.

Pour tous $n \in \mathrm{N}$ et h, $h' \in \mathrm{H}$ on a
$$(n,h) \rtimes_\phi (e_\mathrm{N},h') \rtimes_\phi (n,h)^{-1} = \big(n\phi(hh'h^{-1})(n^{-1}),hh'h^{-1}\big).$$

Ainsi le morphisme ϕ est trivial si et seulement si $\{e_{\mathrm{N}}\} \times \mathrm{H} \lhd \mathrm{N} \rtimes_\phi \mathrm{H}$.

Exercice 239 Soit

$$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

une suite exacte (courte).

1. Montrer que si G est le produit direct de H et N ou bien un produit semi-direct de H par N, alors on a une telle suite exacte.
2. Réciproquement soit une telle suite exacte. Si p possède une section, c'est-à-dire s'il existe un morphisme de groupes $s\colon \mathrm{H} \to \mathrm{G}$ tel que $p \circ s = \mathrm{id}_{\mathrm{H}}$, montrer que G est le produit semi-direct de H par N pour l'opération $h \cdot n = s(h)ns(h)^{-1}$.
3. Donner un exemple de suite exacte courte qui n'est pas un produit semi-direct.

Éléments de réponse 239

1. Supposons que $\mathrm{G} = \mathrm{N} \rtimes_\phi \mathrm{H}$. D'après l'Exercice 5.8 3. on dispose d'un morphisme surjectif $\pi\colon \mathrm{G} \to \mathrm{H}$ dont le noyau est le sous-groupe $\mathrm{N} \rtimes_\phi \{e_{\mathrm{H}}\}$ qui est isomorphe à N. Par suite on a bien une suite exacte

   $$1 \longrightarrow \mathrm{N} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{H} \longrightarrow 1$$

   où $i\colon \mathrm{N} \to \mathrm{G}$ est défini par $i(n) = (n, e_{\mathrm{H}})$. De plus on peut vérifier que l'application

   $$\mathrm{H} \to \mathrm{G} \qquad\qquad h \mapsto (e_{\mathrm{N}}, h)$$

   est une section de π.
2. C'est une conséquence de l'Exercice 5.8 appliqué aux sous-groupes $\mathrm{N}' = i(\mathrm{N})$ et $\mathrm{H}' = s(\mathrm{H})$ de G. Il suffit donc de vérifier que N′ et G′ satisfont les hypothèses de l'Exercice 5.8. Le groupe N′ est distingué dans G car $\mathrm{N}' = \ker p$. Soit $g \in \mathrm{G}$. Posons $h = s(\pi(g)) \in \mathrm{H}'$. Alors

   $$\pi(h) = \pi(s(\pi(g))) = \pi(g)$$

   donc $n = gh^{-1}$ appartient à $\ker \pi = \mathrm{N}'$. 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 $\pi(g) = e_{\mathrm{H}}$. Par suite $\pi(s(h)) = e_{\mathrm{H}}$, *i.e.* $h = e_{\mathrm{H}}$, donc $g = s(e_{\mathrm{H}}) = e_{\mathrm{G}}$. Il s'en suit que $\mathrm{N}' \cap \mathrm{H}' = \{e_{\mathrm{G}}\}$. Nous pouvons donc bien appliquer l'Exercice 5.8 pour conclure.
3. Considérons la suite exacte courte

   $$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

   où p est la réduction modulo 2. C'est bien une suite exacte courte, en revanche p n'admet pas de section puisque l'élément non trivial du quotient $\mathbb{Z}/2\mathbb{Z}$ est d'ordre 2 alors que tous ses antécédents par p sont d'ordre 4. Il s'en suit que $\mathbb{Z}/4\mathbb{Z}$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Un autre exemple est donné par le groupe des quaternions $\mathbb{H}_8$ dont le centre $Z(\mathbb{H}_8)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et le quotient correspondant est $\mathbb{H}_8/Z(\mathbb{H}_8) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ce qui fournit une suite exacte

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{H}_8 \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

telle que p n'admet pas de section (on peut par exemple le voir en listant les éléments d'ordre 2 dans $\mathbb{H}_8$). Il en résulte que $\mathbb{H}_8$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Exercice 240 Nous avons vu en cours que

$$\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{GL}(n,\Bbbk) \simeq \mathrm{SL}(n,\Bbbk) \rtimes \Bbbk^*.$$

Ces produits semi-directs sont-ils directs ?

Éléments de réponse 240 On peut vérifier que les produits

$$\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \mathbb{Z}/2\mathbb{Z} \qquad \mathrm{D}_{2n} \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

ne sont pas directs (sauf pour $n = 2$) quelle que soit la section choisie. On peut en fait vérifier qu'il n'existe pas d'isomorphisme (quelconque) entre ces groupes et les produits directs correspondants.

Le cas $\mathrm{GL}(n,\Bbbk) \simeq \mathrm{SL}(n,\Bbbk) \rtimes \Bbbk^*$ est moins évident pour $n \geq 2$. Si $x \mapsto x^n$ est un automorphisme de $\Bbbk^*$, on note $a\colon \Bbbk^\times \to \Bbbk^\times$ son inverse. L'application

$$\alpha\colon \mathrm{SL}(n,\Bbbk) \times \Bbbk^* \to \mathrm{GL}(n,\Bbbk) \qquad (A,t) \mapsto A\mathrm{diag}(a(t),a(t),\dots,a(t))$$

est un isomorphisme.

Réciproquement supposons qu'il existe un isomorphisme de groupes

$$\alpha\colon \mathrm{SL}(n,\Bbbk) \times \Bbbk^* \to \mathrm{GL}(n,\Bbbk) \qquad (A,t) \mapsto \phi(A)s(t).$$

Le sous-groupe dérivé de $\mathrm{SL}(n,\Bbbk) \times \Bbbk^*$ est $\mathrm{SL}(n,\Bbbk) \times \{1\}$ et celui de $\mathrm{GL}(n,\Bbbk)$ est $\mathrm{SL}(n,\Bbbk)$. Par conséquent ϕ est un automorphisme de $\mathrm{SL}(n,\Bbbk)$. De plus $\alpha(\Bbbk^*) = s(\Bbbk^*)$ commute avec tout élément de $\mathrm{GL}(n,\Bbbk)$ et est donc composé uniquement d'homothéties (le centre de $\mathrm{GL}(n,\Bbbk)$ est formé des homothéties). Ainsi l'application $t \mapsto s(t)$ est un morphisme injectif de $\Bbbk^*$ vers $\mathrm{GL}(n,\Bbbk)$ de la forme $t \mapsto \mathrm{diag}(a(t),a(t),\dots,a(t))$.

Le noyau de det étant $\mathrm{SL}(n,\Bbbk)$ on a $a(t)^n = 1$ si et seulement si $a(t) = 1$. Puisque $t \mapsto a(t)$ est injectif, $t \mapsto a(t)^n$ l'est aussi. Or det est surjectif sur $\Bbbk^*$ donc $t \mapsto a(t)^n = a(t^n)$ est bijectif. Il en résulte que $x \mapsto x^n$ est bijectif et donc un automorphisme de $\Bbbk^*$.

Ainsi $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$ si et seulement si le morphisme $(\cdot)^n\colon \Bbbk^* \to \Bbbk^*$ est un automorphisme. En particulier

- si $\Bbbk = \mathbb{R}$ et n est impair, alors $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$;

- si $\Bbbk$ est un corps fini de caractéristique p et si n est égal à une puissance de p, alors $\mathrm{GL}(n,\Bbbk)$ est isomorphe au produit direct de $\mathrm{SL}(n,\Bbbk)$ par $\Bbbk^*$.

Exercice 241 Soit $\mathrm{G} = \mathrm{N} \rtimes \mathrm{H}$. Soit K un sous-groupe de G contenant N. Montrer que $\mathrm{K} = \mathrm{N} \rtimes (\mathrm{K} \cap \mathrm{H})$.

Éléments de réponse 241 On va appliquer ce qu'on a vu dans l'Exercice 5.8 :
— $\mathrm{N} \lhd \mathrm{G}$ et $\mathrm{N} \subset \mathrm{K}$ donc $\mathrm{N} \lhd \mathrm{K}$;
— $\mathrm{H} \subset \mathrm{G}$ et $\mathrm{K} \subset \mathrm{G}$ donc $\mathrm{H} \cap \mathrm{K} \subset \mathrm{K}$;
— $\mathrm{N} \cap \mathrm{H} = \{e\}$ donc $\mathrm{N} \cap (\mathrm{K} \cap \mathrm{N}) = \{e\}$;
— $\mathrm{NH} = \mathrm{G}$ donc si $k \in \mathrm{K}$, alors $k = nh$ avec $n \in \mathrm{N}$ et $h \in \mathrm{H}$. Puisque $\mathrm{N} \subset \mathrm{K}$ nous en déduisons que $h \in \mathrm{H} \cap \mathrm{K}$. D'où $\mathrm{N}(\mathrm{H} \cap \mathrm{K}) = \mathrm{K}$.

Exercice 242 Soient H et N des groupes. Soient $\varphi, \psi \colon \mathrm{H} \to \mathrm{Aut}(\mathrm{N})$ des morphismes. On veut trouver des conditions nécessaires et suffisantes pour que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ soient isomorphes.

1. S'il existe un automorphisme α de H tel que $\psi = \varphi \circ \alpha$ montrer que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ sont isomorphes.
2. S'il existe un automorphisme u de N tel que
$$\forall\, h \in \mathrm{H} \qquad \phi(h) = u\psi(h)u^{-1}$$
montrer que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ sont isomorphes.
3. Si H est cyclique et si $\varphi(\mathrm{H}) = \psi(\mathrm{H})$ montrer que $\mathrm{N} \rtimes_\varphi \mathrm{H}$ et $\mathrm{N} \rtimes_\psi \mathrm{H}$ sont isomorphes.

Éléments de réponse 242

1. Le morphisme
$$\mathrm{N} \rtimes_\varphi \mathrm{H} \to \mathrm{N} \rtimes_\psi \mathrm{H} \qquad\qquad (n,h) \mapsto (n, \alpha(h))$$
est un isomorphisme.
2. Le morphisme
$$\mathrm{N} \rtimes_\varphi \mathrm{H} \to \mathrm{N} \rtimes_\psi \mathrm{H} \qquad\qquad (n,h) \mapsto (u(n), h)$$
est l'isomorphisme.
3. Le groupe H est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et $\mathrm{im}\,\varphi = \mathrm{im}\,\psi$ est isomorphe à $\mathbb{Z}/m\mathrm{Z}$ avec m diviseur de n. Il existe donc d premier à m tel que $\phi(1) = d\psi(1)$ dans $\mathbb{Z}/m\mathbb{Z}$. Puisque l'application
$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \to \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$$
est surjective, il existe $d' \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ qui s'envoie sur d.

   La multiplication par d' est un automorphisme α de $\mathbb{Z}/n\mathbb{Z}$ qui satisfait les conditions de 1. d'où le résultat.

Exercice 243 Montrer que tout groupe d'ordre 255 est cyclique.

Éléments de réponse 243 Soit G un groupe d'ordre $255 = 3 \times 5 \times 17$. Soit n_3 (resp. n_5, resp. n_{17}) le nombre de 3-Sylow (resp. 5-Sylow, resp. 17-Sylow) de G. Les théorèmes de Sylow assurent que

$$n_3 \in \{1, 85\}, \qquad n_5 \in \{1, 51\} \qquad n_{17} = 1.$$

On ne peut pas avoir $(n_3, n_5) = (85, 51)$ car on aurait trop d'éléments dans G. Donc $n_3 = 1$ ou $n_5 = 1$.

Supposons que $n_3 = 1$ (le cas $n_5 = 1$ se résoud de manière analogue). Notons S_3 le seul 3-Sylow de G, S_{17} le seul 17-Sylow de G et S_5 un 5-Sylow quelconque. Nous avons

— $S_3 S_{17} \simeq S_3 \times S_{17} \triangleleft \mathrm{G}$;
— $S_3 S_{17} \cap S_5 = \{e\}$;
— $S_3 S_{17} S_5 = \mathrm{G}$.

L'exercice 5.8 assure que $\mathrm{G} \simeq S_3 S_{17} \rtimes S_5$. Soit $\phi \colon S_5 \to \mathrm{Aut}(S_3 S_{17})$ le morphisme correspondant. On sait que $\mathrm{Aut}(S_3 S_{17}) \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{16\mathbb{Z}}$ donc ϕ est trivial et le produit semi-direct. On conclut par le lemme chinois.

Exercice 244 Soit p un nombre premier impair.

1. Déterminer les p-Sylow de $\mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$.
2. Soient ϕ et ψ des morphismes non triviaux de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ dans $\mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$. Pour tout entier k notons ϕ_k le morphisme ϕ_k défini par $\phi_k(x) = \phi(kx)$. Montrer qu'il existe un entier k et une matrice $P \in \mathrm{GL}\left(2, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)$ tels que $\psi = P \phi_k P^{-1}$.
3. Montrer qu'il existe un produit semi-direct non trivial $\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)^2 \rtimes {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$.
4. Montrer que le centre de ce dernier groupe est isomorphe à ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. (On rappelle que si G est un groupe tel que ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est monogène, alors G est abélien.)
5. Supposons que G est un groupe fini. Notons p le plus petit nombre premier divisant le cardinal de G.

   Montrer que tout sous-groupe de G d'indice p est distingué (indication : commencer par montrer que tout sous-groupe H de G d'indice p agit trivialement sur ${}^{\mathrm{G}}\!/_{\mathrm{H}}$, en déduire que H est distingué dans G).
6. Soit G un groupe d'ordre p^3 non cyclique contenant un élément g d'ordre p^2. Montrer que $\langle g \rangle$ est distingué dans G et que G est un produit semi-direct de ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ par $\langle g \rangle \simeq {}^{\mathbb{Z}}\!/_{p^2\mathbb{Z}}$.

Éléments de réponse 244

1. Les p-SYLOW de $\mathrm{GL}(2,\mathbb{F}_p)$ sont d'ordre p. Comme le sous-groupe
$$\mathrm{U} = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{F}_p \right\}$$
des matrices unipotentes supérieures est un p-SYLOW de $\mathrm{GL}(2,\mathbb{F}_p)$ et que tous sont conjugués, une matrice de $\mathrm{GL}(2,\mathbb{F}_p)$ est dans un p-SYLOW si et seulement si son polynôme caractéristique est $(X-1)^2$. On dénombre p^2 telles matrices (à la main...) et donc $(p+1)$ p-SYLOW distincts (car deux p-SYLOW distincts ne s'intersectent qu'en l'élément neutre). Remarquons que ce sont les conjugués de U par les $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, $a \in \mathbb{F}_p$, et par $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
2. Puisque les images de ψ et φ sont des p-SYLOW de $\mathrm{GL}(2,\mathbb{F}_p)$ elles sont conjuguées par une matrice $P \in \mathrm{GL}(2,\mathbb{F}_p)$. Notons
$$\varphi_{(P)} \colon \mathbb{Z}/p\mathbb{Z} \to \psi\left(\mathbb{Z}/p\mathbb{Z}\right) \qquad\qquad x \mapsto P\varphi(x)P^{-1}$$
c'est un isomorphisme. Dès lors $(\varphi_{(P)})^{-1} \circ \psi$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$, *i.e.* de la forme $x \mapsto kx$ pour un certain $k \in \mathbb{Z}$ premier avec p.
3. Puisque $\mathrm{Aut}\left(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\right) \simeq \mathrm{GL}(2,\mathbb{F}_p)$ le 1. assure l'existence d'un produit semi-direct non trivial $\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}$.
4. Comme le centre d'un p-groupe est non trivial, le centre de $\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ est d'ordre p, p^2 ou p^3. Si $Z\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}\right)$ était d'ordre p^2 ou p^3, alors $\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}$ serait abélien (en effet si G est un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ est monogène, alors G est abélien) : contradiction avec le fait que le produit semi-direct n'est pas trivial. Il s'en suit que $Z\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^2 \rtimes \mathbb{Z}/p\mathbb{Z}\right)$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
5. Notons p le plus petit nombre premier divisant le cardinal de G. Soit H un sous-groupe de G d'indice p. Posons $X = \mathrm{G}/\mathrm{H}$. C'est un ensemble de cardinal p, muni de l'action naturelle transitive de G. Cette action induit un morphisme de groupes finis $\varphi \colon \mathrm{G} \to \mathcal{S}_X$. Intéressons-nous à la restriction de cette action au sous-groupe H, autrement dit au morphisme $\varphi \colon \mathrm{H} \to \mathcal{S}_X$. Puisque H agit trivialement sur la classe x_0 de H dans $X = \mathrm{G}/\mathrm{H}$ l'action de H sur X induit une action de H sur $X' = X \smallsetminus \{x_0\}$ c'est-à-dire un morphisme de groupes $\psi \colon \mathrm{H} \to \mathcal{S}_{X'}$. Or $|X'| = p-1$ donc tous les facteurs premiers de $|\mathcal{S}_{X'}|$ sont strictement inférieurs à p. Or les facteurs premiers de $|\mathrm{H}|$ sont par hypothèse tous supérieurs ou égaux à p. Par suite $|\mathrm{H}|$ et $|\mathcal{S}_{X'}|$ sont premiers entre eux. Le morphisme ψ est donc trivial. Il en résulte que H agit trivialement sur X' et donc aussi sur X.

   Montrons que cela implique que G est distingué dans G. Soit $h \in \mathrm{H}$ et soit $g \in \mathrm{G}$. Puisque H agit trivialement sur X on a $h \cdot (g\mathrm{H}) = g\mathrm{H}$ donc $(g^{-1}hg)\mathrm{H} = \mathrm{H}$, par suite $g^{-1}hg$ appartient à H, *i.e.* H est distingué dans G.

6. Le sous-groupe $\langle g\rangle$ est d'indice p dans un groupe d'ordre p^3. D'après 5. le groupe $\langle g\rangle$ est donc distingué dans G.

   De plus le quotient $\mathrm{G}/\langle g\rangle$ est d'ordre p donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

   Soit $y \in \mathrm{G} \setminus \langle g\rangle$. Alors y^p appartient à $\langle g\rangle$ et $y^{p^2} = e$. Il existe donc $k \in \mathbb{Z}$ tel que $y^p = g^{pk}$. Comme $\langle g\rangle$ est distingué dans G il existe un entier $r \geq 0$ tel que $y^{-1}gy = g^r$. Alors pour tout $\ell \in \mathbb{N}$ nous avons $g^\ell y = yg^{\ell r}$. On cherche $z \in \mathrm{G} \setminus \langle g\rangle$ d'ordre p ; plus précisément on cherche $z \in \mathrm{G} \setminus \langle g\rangle$ d'ordre p sous la forme $z = yg^n$. Alors

$$z^p = (yg^n)^p = yg^nyg^n \dots yg^n;$$

   une simple récurrence assure que

$$z^p = y^p g^{n(r^{p-1}+r^{p-2}+\dots+r+1)} = g^{pk+n(r^{p-1}+r^{p-2}+\dots+r+1)}.$$

   Par suite z est d'ordre p si et seulement si

$$pk + n(r^{p-1} + r^{p-2} + \dots + r + 1) \equiv 0 \mod p^2. \tag{5.8.1}$$

   On cherche donc à résoudre (5.8.1) dont l'inconnue est $n \in \mathbb{Z}$. Posons $S := r^{p-1} + r^{p-2} + \dots + r + 1$. Alors $(r-1)S \equiv r - 1 \bmod p$ donc
   — soit $r \not\equiv 1 \bmod p$ et $S \equiv 1 \bmod p$;
   — soit $r \equiv 1 \bmod p$ et on vérifie que dans ce cas $S \equiv p \bmod p^2$ (utiliser que p est impair).
   Dans les deux cas l'équation (5.8.1) admet une solution $n_0 \in \mathbb{Z}$. Ainsi $z_0 = yg^{n_0} \in \mathrm{G} \setminus \langle g\rangle$ est d'ordre p. Les deux sous-groupes $\mathrm{N} = \langle g\rangle$ et $\mathrm{H} = \langle z\rangle$ satisfont les hypothèses de l'Exercice 5.8 ce qui assure que G est produit semi-direct de $\mathbb{Z}/p\mathbb{Z}$ par $\mathbb{Z}/p^2\mathbb{Z}$.

5.9. Groupes libres

Exercice 245 Soient r et s deux entiers > 1 premiers entre eux. Quel est l'ordre du groupe de présentation $\langle a \,|\, a^r,\, a^s\rangle$?

Éléments de réponse 245 L'ordre de a est un diviseur de r et s qui sont premiers entre eux donc a est d'ordre 1. Puisque G est engendré par a, le groupe G est d'ordre 1. Ainsi $\mathrm{G} = \{e_\mathrm{G}\}$.

Exercice 246 Soit G le groupe de présentation

$$\langle a,\, b,\, c \,|\, a^3 = b^3 = c^4 = e_\mathrm{G},\, ac = ca^{-1},\, aba^{-1} = bcb^{-1}\rangle.$$

Montrer que $ab^3a^{-1} = bc^3b^{-1}$ puis que $c = e_\mathrm{G}$; en déduire G.

Éléments de réponse 246 Nous avons

$$\begin{aligned} ab^3a^{-1} &= ab(a^{-1}a)b(a^{-1}a)ba^{-1} \\ &= (aba^{-1})(aba^{-1})(aba^{-1}) \\ &= (bcb^{-1})(bcb^{-1})(bcb^{-1}) \\ &= bc(b^{-1}b)c(b^{-1}b)cb^{-1} \\ &= bc^3b^{-1} \end{aligned}$$

Puisque $b^3 = e$, nous avons $ab^3a^{-1} = aa^{-1} = e_{\mathrm{G}}$. Comme $bc^3b^{-1} = ab^3a^{-1}$ nous obtenons que $bc^3b^{-1} = e_{\mathrm{G}}$ et que $c^3 = e_{\mathrm{G}}$. Par suite $c = c^4(c^3)^{-1} = e_{\mathrm{G}}(e_{\mathrm{G}})^{-1} = e_{\mathrm{G}}$.

Puisque $c = e$, la relation $ac = ca^{-1}$ devient $a = a^{-1}$ ou encore $a^2 = e$. Comme $a^3 = e$ nous obtenons $a = e$.

Enfin puisque $a = c = e_{\mathrm{G}}$ la relation $aba^{-1} = bcb^{-1}$ se réduit à $b = e_{\mathrm{G}}$. Comme a, b et c engendrent G nous obtenons $\mathrm{G} = \{e_{\mathrm{G}}\}$.

Exercice 247 Montrer que tout élément non trivial d'un groupe libre est d'ordre infini.

Éléments de réponse 247 Soit G un groupe libre. Soit g un élément non trivial de G. Raisonnons par l'absurde, *i.e.* supposons que g soit d'ordre fini n ; alors $g^n = e$. Or g^n est un mot formé avec les générateurs de G, la relation $g^n = e$ fournit donc une relation entre ces générateurs ce qui contredit le fait que G est un groupe libre.

Exercice 248 Quel est l'ordre du groupe G engendré par deux éléments x et y vérifiant les relations

$$x^3 = y^2 = (xy)^2 = 1\,?$$

Quels sont les sous-groupes de G ?

Éléments de réponse 248 Supposons que G ne soit pas trivial. Ceci implique que $x \neq y$ (en effet si $x = y$ alors $x^3 = 1$ se réécrirait $y^3 = 1$ et combiné à $y^2 = 1$ on obtiendrait $x = y = 1$.

L'ordre de x est 3 ; celui de y est 2. Il en résulte que $|\mathrm{G}|$ est un multiple de $2 \times 3 = 6$. Le groupe G contient e, x, x^2, y, xy et xy^2. Montrons qu'il n'y a pas d'autres éléments dans G. Commençons à écrire la table de G en utilisant ces six éléments

	e	x	x^2	y	xy	x^2y
e	e	x	x^2	y	xy	x^2y
x	x	x^2	e	xy	x^2y	y
x^2	x^2	e	x	x^2y	y	xy
y	y	x^2y	xy	e	x^2	x
xy	xy	y	x^2y	x	e	x^2
x^2y	x^2y	xy	y	x^2	x	e

Par suite cette table est complète et le groupe G compte 6 éléments.

Les sous-groupes de G sont

- ◇ le sous-groupe trivial,
- ◇ le groupe G lui-même,
- ◇ un unique (théorème de Sylow) sous-groupe d'ordre 3 : $\langle x\rangle$,
- ◇ trois sous-groupes d'ordre 2 exactement (théorème de SYLOW) : $\langle y\rangle$, $\langle xy\rangle$, $\langle x^2y\rangle$.

Exercice 249 Quel est l'ordre du groupe G engendré par deux éléments x et y vérifiant les relations

$$xy^2 = y^3x \qquad\qquad yx^3 = x^2y\,?$$

Éléments de réponse 249 À partir de $xy^2 = y^3x$ nous obtenons

$$y^2 = x^{-1}y^3x \qquad\qquad y^3 = xy^2x^{-1}$$

et

$$y^4 = x^{-1}y^6x \qquad\qquad y^6 = xy^4x^{-1}.$$

Par suite d'une part

$$y^9 = (y^3)^3 = (xy^2x^{-1})^3 = xy^6x^{-1}$$

et d'autre part

$$xy^6x^{-1} = x(y^6)x^{-1} = x(xy^4x^{-1})x^{-1} = x^2y^4x^{-2}.$$

On en déduit que $y^9 = x^2y^4x^{-2}$. De plus

$$y^9 = y^{-1}(y^9)y = y^{-1}(x^2y^4x^{-2})y = y^{-1}(x^2y)y^4(y^{-1}x^{-2})y = y^{-1}(x^2y)y^4(x^2y)^{-1}y$$

Mais $yx^3 = x^2y$ donc

$$y^9 = y^{-1}(x^2y)y^4(x^2y)^{-1}y = y^{-1}(yx^3)y^4(yx^3)^{-1}y = x^3y^4x^{-3}$$

Puisque $y^9 = x^2y^4x^{-2}$ nous obtenons

$$x^2y^4x^{-2} = x^3y^4x^{-3}$$

soit $y^4 = xy^4x^{-1}$. Mais on a vu précédemment que $y^6 = xy^4x^{-1}$ donc $y^4 = y^6$ soit $y^2 = e$. À partir de $xy^2 = y^3x$ on a $y^3 = e$ et finalement $y = e$. De plus $yx^3 = x^2y$ se réécrit $x^3 = x^2$ d'où $x = e$. Finalement G est le groupe trivial.

Exercice 250 Le groupe de FIBONNACCI [11] G est engendré par les éléments a, b, c et d vérifiant les relations

$$ab = c \qquad bc = d \qquad cd = a \qquad da = b.$$

Quel est l'ordre de G ?

11. Les groupes de FIBONNACCI ont été introduits par John CONWAY en 1965.

Éléments de réponse 250 À partir de $a = cd$ nous obtenons

$$a^2 = acd = cda = cb = ab^2$$

d'où $a = b^2$.

De même nous obtenons que $c^2 = b$, $d^2 = c$ et $a^2 = d$.

Par suite

$$d = a^2 = b^4 = c^8 = d^{16}$$

et $d^{15} = e$.

De la même façon nous obtenons que $a^{15} = b^{15} = c^{15} = e$.

A partir de $ab = c$ nous obtenons que $ab = a^4$ d'où $aa^8 = a^4$ et $a^5 = e$. De même $b^5 = c^5 = d^5 = e$. Par conséquent $d = a^2$, $b = a^3$, $c = a^4$ et $\mathrm{G} \simeq \mathbb{Z}/5\mathbb{Z}$.

Exercice 251 Exprimer comme produit direct de sous-groupes monogènes le sous-groupe multiplicatif de $\mathbb{Q}^*$ engendré par $\{-6, 6\}$.

Éléments de réponse 251 Le sous-groupe $\mathrm{H} = \langle 6\rangle$ de $\mathrm{G} = \langle 6, -6\rangle \subset \mathbb{Q}^*$ est monogène.

Le groupe G/H est monogène engendré par $(-6)\mathrm{H}$.

Le sous-groupe H est distingué dans G : il suffit de vérifier que $(-6) \times 6 \times (-6)^{-1}$ appartient à H ce qui est vrai puisque ce nombre vaut 6

Ainsi G est produit direct de deux groupes monogènes : $\mathrm{G} \simeq \mathrm{H} \times \mathrm{G}/\mathrm{H}$.

Exercice 252 Montrer que le groupe multiplicatif engendré par les matrices

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

est abélien.

Exprimer ce groupe, de deux façons différentes, comme produit direct de sous-groupes monogènes.

Éléments de réponse 252 Soit G le groupe multiplicatif engendré par les matrices

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

On peut vérifier que $AB = BA = -2\mathrm{id}$;

le groupe G est donc abélien. Le sous-groupe $\mathrm{H} = \langle A\rangle$ de G est monogène.

Le groupe G/H est monogène engendré par $B\mathrm{H}$.

Notons que $BAB^{-1} = A$; en particulier BAB^{-1} appartient à H et H est un sous-groupe distingué de G.

Il en résulte que G est isomorphe au produit direct des deux groupes monogènes H et G/H.

Exercice 253 [Présentation de $\mathcal{S}_n$] Montrer que

$$\mathcal{S}_n = \langle t_1, t_2, \ldots, t_{n-1} \,|\, t_i^2 = 1,\ (t_i t_{i+1})^3 = 1,\ [t_i, t_j] = 1 \text{ pour } 2 \leq |i-j|\rangle$$

(Indication : le groupe $\mathcal{S}_n$ est engendré par $(1\ 2)$, $(2\ 3)$, …, $(n-1\ n)$).

Éléments de réponse 253 Pour $1 \leq i \leq n-1$ posons $t_i = (i\ i+1)$. Le groupe $\mathcal{S}_n$ est engendré par ces transpositions. Cet ensemble de transpositions vérifie les relations données car une transposition est d'ordre 2, deux transpositions disjointes commutent (et pour les transpositions considérées t_i et t_j sont disjointes si et seulement si $|i-j|>1$), le produit $t_i t_{i+1}$ est égal au 3-cycles $(i\ i+1\ i+2)$ et est donc d'ordre 3. Par suite

$$\mathcal{S}_n = \langle t_1, t_2, \ldots, t_{n-1} \,|\, t_i^2 = \mathrm{id},\ (t_i t_{i+1})^3 = \mathrm{id},\ [t_i, t_j] = \mathrm{id} \text{ pour } |i-j|>1 \rangle$$

En effet soit H le sous-groupe de $\mathcal{S}_n$ engendré par les t_i. Le groupe H est distingué dans $\mathcal{S}_n$ car

$$\sigma t_i \sigma^{-1} = (\sigma(i)\ \sigma(i+1))$$

et toute transposition est dans H : si $|i-k|>1$,

$$(i\ k) = (k-1\ k)(i\ k)(k-1\ k).$$

Ainsi H contient $\mathcal{A}_n$ car tout sous-groupe distingué non trivial de $\mathcal{S}_n$ contient $\mathcal{A}_n$.

Mais H contient strictement $\mathcal{A}_n$ car les transpositions ne sont pas des permutations paires. L'indice de $\mathcal{A}_n$ dans $\mathcal{S}_n$ étant 2 nous obtenons que l'indice de H dans $\mathcal{S}_n$ est 1. Il s'ensuit que $\mathcal{S}_n = \mathrm{H}$.

Exercice 254 Rappelons que le groupe des quaternions $\mathbb{H}_8$ est le sous-groupe du groupe des matrices 2×2 inversibles à coefficients complexes engendré par

$$A = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix} \qquad \text{et} \qquad B = \begin{pmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{pmatrix}$$

Montrer que ce groupe admet les deux présentations suivantes

$$\langle A, B \,|\, A^2 = B^2 = (AB)^2 \rangle \qquad \langle R, S, T \,|\, R^2 = S^2 = T^2 = RST \rangle.$$

Éléments de réponse 254 On peut vérifier que $A^2 = B^2 = (AB)^2 = -\mathrm{id}$ d'où la première présentation pour $\mathbb{H}_8$ (en effet un groupe qui a cette présentation est d'ordre 8).

Posons $R = A$, $S = B$ et $T = AB$; alors $R^2 = S^2 = -\mathrm{id}$ d'après ce qu'on vient de voir. Par ailleurs $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ donc $T^2 = -\mathrm{id}$. Et $RST = ABAB = (AB)^2 = -\mathrm{id}$ d'où la deuxième présentation proposée.

Exercice 255 [Présentation de $\mathcal{A}_4$]

1. Soient $a = (2\ 3\ 4)$ et $b = (1\ 2)(3\ 4)$ deux éléments de $\mathcal{A}_4$. Montrer que
$$\langle a, b \,|\, a^3 = b^2 = (ab)^3 = e \rangle$$
est une présentation de $\mathcal{A}_4$.
2. Donner une seconde présentation de $\mathcal{A}_4$ en utilisant les deux 3-cycles $(2\ 3\ 4)$ et $(1\ 3\ 2)$.

Éléments de réponse 255

1. Rappelons que $\mathcal{A}_4$ est d'ordre 12. Le groupe G de présentation
$$\langle a,\, b \,|\, a^3 = b^2 = (ab)^3 = e\rangle$$
est d'ordre 12 ; en effet ses éléments sont
$$e,\ a,\ a^2,\ b,\ ab,\ a^2b,\ ba,\ ba^2,\ aba,\ a^2ba,\ aba^2,\ a^2ba^2.$$
Le morphisme φ de G dans $\mathcal{A}_4$ défini par
$$\varphi(a) = (1\ 2\ 3) \qquad\qquad \varphi(b) = (1\ 2)(3\ 4)$$
réalise un isomorphisme entre G et $\mathcal{A}_4$.
2. Posons $\alpha = (2\ 3\ 4)$ et $\beta = (1\ 3\ 2)$; alors $\alpha\beta = (1\ 4\ 2)$ et
$$\alpha^3 = \mathrm{id} \qquad\qquad \beta^3 = \mathrm{id} \qquad\qquad (\alpha\beta)^3 = \mathrm{id}$$
On peut vérifier que le groupe G de présentation
$$\langle \alpha,\, \beta,\, |\, \alpha^3 = \beta^3 = (\alpha\beta)^3 = e\rangle$$
est d'ordre 12. On en déduit que G et $\mathcal{A}_4$ sont isomorphes.

Exercice 256 [Présentation de $\mathcal{S}_4$] Nous allons montrer que le groupe $\mathcal{S}_4$ est isomorphe au groupe G de présentation
$$\langle a,\, b \,|\, a^3 = b^4 = (ab)^2 = e\rangle.$$
1. En utilisant les éléments $\alpha = (2\ 3\ 4)$ et $\beta = (1\ 3\ 2\ 4)$ de $\mathcal{S}_4$ montrer qu'il existe un morphisme de G sur $\mathcal{S}_4$. Désignons par H le sous-groupe de G engendré par a et b^2.
2. Montrer que bab^{-1} est un élément de H ; en déduire que H est un sous-groupe distingué de G.
3. Montrer que G/H a au plus deux éléments : les classes H et bH.
4. Montrer que $(ab^2)^3 = e$.
5. Conclure en utilisant la présentation de $\mathcal{A}_4$ obtenue précédemment.

Éléments de réponse 256

1. Remarquons que les permutations α et β considérées vérifient les relations
$$\alpha^3 = \mathrm{id}, \qquad\qquad \beta^4 = \mathrm{id}, \qquad\qquad (\alpha\beta)^2 = \mathrm{id}.$$
Il existe donc un morphisme φ de G sur $\mathcal{S}_4$ qui envoie a sur α et b sur β. C'est de plus un morphisme injectif.
2. Nous avons
$$bab^{-1} = bab^3 = (bab)b^2, \qquad\qquad bab = a^{-1} = a^2.$$
Donc $bab^{-1} = a^2b^2$ appartient à H. Puisque G est engendré par a et b, cette relation implique que H est distingué dans G.

3. Puisque G est engendré par a et b, ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ est engendré par $a\mathrm{H}$ et $b\mathrm{H}$, donc par $b\mathrm{H}$ car $a\mathrm{H} = \mathrm{H}$. Or $b^2\mathrm{H} = \mathrm{H}$ donc ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ contient au plus les deux éléments H et $b\mathrm{H}$.
4. Nous avons $abba = b^3a^2a^2b^3 = b^3ab^3$ car $ab = b^{-1}a^{-1} = b^3a^2$ et $ba = a^{-1}b^{-1} = a^2b^3$. Il en résulte que
$$(ab^2)^3 = abbabbabb = b^3ab^3b^2ab^2 = b^3abab^2 = b^3(abab)b = b^4 = e.$$
5. Le sous-groupe H de G a pour présentation
$$\langle a,\, c \,|\, a^3 = c^2 = (ac)^3\rangle$$
(poser $c = b^2$). Les groupes H et $\mathcal{A}_4$ ont même présentation et $\varphi(\mathrm{H}) \subset \mathcal{A}_4$ donc $\varphi(\mathrm{H}) = \mathcal{A}_4$; en particulier H et $\mathcal{A}_4$ sont isomorphes. Le sous-groupe H est d'indice 2 dans G et $\mathcal{A}_4$ est d'indice 2 dans $\mathcal{S}_4$. Ainsi $|\mathrm{G}| = |\mathcal{S}_4|$. Finalement φ est un morphisme injectif de G dans $\mathcal{S}_4$ et $|\mathrm{G}| = |\mathcal{S}_4|$ donc φ réalise un isomorphisme entre G et $\mathcal{S}_4$.

Exercice 257 [Présentation d'un produit semi-direct de groupes cycliques]

Notation : $[a]_m$ désigne un élément de ${}^{\mathbb{Z}}\!/_{m\mathbb{Z}}$ représenté par $a \in \mathbb{Z}$, avec $0 \leq a \leq m-1$. De même $[a]_n$ désigne un élément de ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ représenté par $a \in \mathbb{Z}$, avec $0 \leq a \leq n-1$.

Soient m, n des entiers ≥ 2 et
$$\tau\colon {}^{\mathbb{Z}}\!/_{m\mathbb{Z}} \to \mathrm{Aut}\left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\right)$$
un morphisme. Désignons par G le produit semi-direct ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \rtimes_\tau {}^{\mathbb{Z}}\!/_{m\mathbb{Z}}$ défini par τ.

Posons
$$[i]_n = \tau([1]_m)([1]_n) \qquad h = ([1]_n, [0]_m) \qquad k = ([0]_n, [1]_m).$$
Vérifions que
$$i^m \equiv 1 (\mathrm{mod\ n}) \qquad h^n = k^m = ([0]_n, [0]_m) \qquad khk^{-1} = h^i.$$
En déduire que G admet pour présentation
$$\langle a,\, b \,|\, a^n = b^m = e,\, ab = ba^i\rangle.$$

Éléments de réponse 257 Un morphisme $\tau\colon {}^{\mathbb{Z}}\!/_{m\mathbb{Z}} \to \mathrm{Aut}\left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\right)$ est entièrement déterminé par l'image $\tau([1]_m)$ de $[1]_m$ dans $\mathrm{Aut}\left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\right)$. Cette image est elle-même déterminée par l'image de $[1]_n$ par $\tau([1]_m)$. Par suite un morphisme $\tau\colon {}^{\mathbb{Z}}\!/_{m\mathbb{Z}} \to \mathrm{Aut}\left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}}\right)$ est entièrement déterminé par $[i]_n = \tau([1]_m)([1]_n)$. Comme $[1]_m$ est d'ordre m, on a $\tau([1]_m)^m = \mathrm{id}$. Ainsi $i^m \equiv 1 \pmod{n}$.

Clairement $h^n = k^m = ([0]_n, [0]_m)$. L'inverse de k dans G est $k^{-1} = ([0]_n, [m-1]_m)$. Il en résulte que

$$\begin{aligned} hk^{-1} &= ([1]_n, [0]_m)([0]_n, [m-1]_m) \\ &= ([1]_n + \tau([0]_m)([0]_n), [m-1]_m) \\ &= ([1]_n, [m-1]_m) \end{aligned}$$

et donc que

$$\begin{aligned} khk^{-1} &= ([0]_n, [1]_m)([1]_n, [m-1]_m) \\ &= ([0]_n + \tau([1]_m)([1]_n), [0]_m) \\ &= ([i]_n, [0]_m) \end{aligned}$$

En particulier $khk^{-1} = h^i$.

Le groupe G est engendré par $a = h$ et $b = k^{-1}$ qui vérifient $a^n = b^b a^i$. Une présentation de G est la suivante

$$\mathrm{G} = \langle a,\, b \,|\, a^n = b^m = e,\, ab = ba^i \rangle.$$

5.10. Représentations linéaires des groupes finis

Exercice 258 Montrer que tout groupe fini G admet une représentation fidèle sur tout corps $\Bbbk$.

Éléments de réponse 258 Première réponse possible : la représentation régulière de G sur $\Bbbk$ répond à la question.

Deuxième réponse possible : le théorème de Cauchy assure que G se plonge dans le groupe des permutations de G et ce dernier groupe se plonge dans un groupe linéaire via les matrices de permutations.

Exercice 259 Montrer que si G est un groupe d'ordre fini n, si ρ est une représentation de G, alors pour tout g dans G $\rho(g)$ est diagonalisable et son spectre est inclus dans μ_n.

Éléments de réponse 259 Soit G un groupe d'ordre fini n. Soit $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$, où V est un $\mathbb{C}$-espace vectoriel de dimension fini, une représentation de G.

Soit g un élément de G. L'ordre de g divise n ; en particulier g est d'ordre fini. L'automorphisme $\rho(g)$ est d'ordre fini puisque g l'est, *i.e.* il existe un entier k tel que $\rho(g)^k = \mathrm{Id}_V$. Alors :

$$X^k - 1 = \prod_{j=0}^{k-1} (X - \zeta^j) \in \mathbb{C}[X]$$

où ζ est une racine primitive $k$ième de l'unité, est un polynôme annulateur de $\rho(g)$ scindé à facteurs simples ; $\rho(g)$ est donc diagonalisable et ses valeurs propres sont les racines $k$ième de l'unité.

Exercice 260 Soit G un groupe fini. Soit H un sous-groupe distingué de G. Notons $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ la projection canonique. Soit ρ une représentation complexe de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

a) Montrer que $\rho \circ \pi$ est une représentation de G.

b) Montrer que ρ est irréductible si et seulement si $\rho \circ \pi$ est irréductible.

Éléments de réponse 260 Soit G un groupe fini. Soit H un sous-groupe distingué de G. Notons $\pi\colon \mathrm{G} \to {}^{\mathrm{G}}\!/_{\mathrm{H}}$ la projection canonique. Soit ρ une représentation complexe de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$.

a) Montrons que $\rho \circ \pi$ est une représentation de G.

La composée de deux morphismes de groupes étant un morphisme de groupes, $\rho \circ \pi$ est une représentation de G.

b) Montrons que ρ est irréductible si et seulement si $\rho \circ \pi$ est irréductible.

- Commençons par montrer que si $\rho \circ \pi$ est irréductible alors ρ l'est.
  Plus généralement si $f\colon \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes et si ρ est une représentation de G', on a l'implication suivante

  si $\rho \circ f$ est irréductible (comme représentation) de G, alors ρ est irréductible.

  En effet tout sous-espace stable par G' est stable par G puisque l'action de G se factorise par G'.
- Montrons que si ρ est irréductible, alors $\rho \circ \pi$ est irréductible.
  Soit W un sous-espace strict stable par G. Pour tout $\overline{x} \in {}^{\mathrm{G}}\!/_{\mathrm{H}}$ il existe $g \in \mathrm{G}$ tel que $\pi(g) = \overline{x}$ (ρ est surjective, si elle ne l'était pas l'implication serait fausse). Comme W est stable par g, il est stable par $\overline{x}$. Ainsi W est stable par tout élément de ${}^{\mathrm{G}}\!/_{\mathrm{H}}$. La représentation ρ étant irréductible $W = 0$ et $\rho \circ \pi$ est irréductible.

Exercice 261 Soient V un $\mathbb{C}$-espace vectoriel, G un groupe et (V, ρ) une représentation de G. On suppose qu'il existe $v \in V$ tel que $\{\rho(g)v \,|\, g \in \mathrm{G}\}$ forme une base de V.

Montrer que (V, ρ) est isomorphe à la représentation régulière de G.

Éléments de réponse 261

Soient V un $\mathbb{C}$-espace vectoriel, G un groupe et (V, ρ) une représentation de G. On suppose qu'il existe $v \in V$ tel que $\{\rho(g)v \,|\, g \in \mathrm{G}\}$ forme une base de V.

Montrons que (V, ρ) est isomorphe à la représentation régulière de G.

Soit W un espace vectoriel de base $\{e_j\}_{g\in \mathrm{G}}$; prendre par exemple $W = \mathbb{C}^G$ et $e_g =$ indicatrice de g. Rappelons que la représentation régulière ρ_R de G opère sur W par

$$\rho_R(h)(e_g) = e_{hg}$$

Considérons l'application linéaire ϕ définie sur la base (e_g) oar

$$\phi\colon W \to V, \qquad\qquad e_g \mapsto \rho(g)v$$

Puisque par hypothèse $(\rho(g)(v))_{g\in \mathrm{G}}$ est une base de V ϕ est un isomorphisme de $\mathbb{C}$-espaces vectoriels. Par définition ϕ est G-équivariante, *i.e.* $\phi \circ \rho_R(g) = \rho(g) \circ \phi$. En effet d'une part

$$(\phi \circ \rho_R(g))(e_h) = \phi(e_{gh}) = \rho(gh)(v)$$

et d'autre part

$$(\rho(g) \circ \phi)(e_h) = \rho(g)(\phi(e_h)) = \rho(g)(\rho(h)(v)) = \rho(gh)(v)$$

Ainsi ϕ est un isomorphisme entre ρ et ρ_R.

Exercice 262 Soit $\mathrm{G} = \mathcal{S}_3$ et soit V un $\mathbb{C}$-espace vectoriel possédant une base indexée par les éléments de G. Considérons l'application $T\colon \mathrm{G} \to \mathrm{GL}(V)$ définie par

$$T(g)(e_\tau) = e_{g\tau g^{-1}}.$$

a) Montrer que T est une représentation de G.

b) Soit j une racine cubique primitive de 1. Soit W le sous-espace de V dont une base est

$$\alpha = e_{(1\,2)} + je_{(1\,3)} + j^2 e_{(2\,3)} \qquad \beta = e_{(1\,2)} + j^2 e_{(1\,3)} + je_{(2\,3)}$$

Montrer que W est une sous-G-représentation de V. W est-il irréductible ?

c) Déterminer la décomposition de V en somme directe de sous-espaces irréductibles et expliciter l'action de G sur chacun de ses sous-espaces.

Éléments de réponse 262

Soit $\mathrm{G} = \mathcal{S}_3$ et soit V un $\mathbb{C}$-espace vectoriel possédant une base indexée par les éléments de G. Considérons l'application $T\colon \mathrm{G} \to \mathrm{GL}(V)$ définie par

$$T(g)(e_\tau) = e_{g\tau g^{-1}}.$$

a) Montrons que T est une représentation de G.

T est un morphisme de G dans $\mathrm{GL}(V)$: soient g et g' dans G on a d'une part

$$T(gg')(e_\tau) = e_{(gg')\tau(gg')^{-1}} = e_{gg'\tau g'^{-1}g^{-1}}$$

et d'autre part

$$T(g) \circ T(g')(e_\tau) = T(g)(e_{g'\tau g'^{-1}}) = e_{gg'\tau g'^{-1}g^{-1}}$$

d'où $T(gg') = T(g) \circ T(g')$.

b) Soit j une racine cubique primitive de 1. Soit W le sous-espace de V dont une base est

$$\alpha = e_{(1\,2)} + je_{(1\,3)} + j^2 e_{(2\,3)} \qquad \beta = e_{(1\,2)} + j^2 e_{(1\,3)} + je_{(2\,3)}$$

Montrons que W est une sous-G-représentation de V.

Le groupe $\mathcal{S}_3$ est engendré par (1 2) et (1 2 3). Il suffit donc de montrer que l'espace engendré par α et β est stable par $T((1\ 2))$ et $T((1\ 2\ 3))$. Un calcul montre que

$$T((1\ 2))(\alpha) = \beta, \qquad T((1\ 2\ 3))(\alpha) = j\alpha, \qquad T((1\ 2))(\beta) = \alpha, \qquad T((1\ 2\ 3))(\beta) = j^2\beta$$

W est-il irréductible ?

Un calcul montre qu'aucun sous-module de W de dimension 1 n'est stable par $\mathcal{S}_3$ donc W est irréductible.

c) Déterminons la décomposition de V en somme directe de sous-espaces irréductibles et expliciter l'action de G sur chacun de ses sous-espaces.

Remarquons que si C est une classe de conjugaison dans $\mathcal{S}_3$, alors $\sum_{g\in C} e_g$ est stable par T (c'est par définition même de T). On trouve ainsi trois sous-espaces stables sous $\mathcal{S}_3$ qui sont les droites

$$W_1 = \mathbb{C}\mathrm{id}, \qquad W_2 = \mathbb{C}(e_{(1\ 2)} + e_{(1\ 3)} + e_{(2\ 2)}), \qquad W_3 = \mathbb{C}(e_{(1\ 2\ 3)} + e_{(1\ 3\ 2)})$$

Enfin si on note sgn la signature on obtient

$$T(g)(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) = \mathrm{sgn}(g)(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)})$$

En effet d'une part

$$\begin{aligned} T((1\ 2))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) &= e_{(1\ 2)(1\ 2\ 3)(1\ 2)} - e_{(1\ 2)(1\ 3\ 2)(1\ 2)} \\ &= e_{(1\ 3\ 2)} - e_{(1\ 2\ 3)} \\ &= -(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \\ &= \mathrm{sgn}((1\ 2))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \end{aligned}$$

d'autre part

$$\begin{aligned} T((1\ 2\ 3))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) &= e_{(1\ 2\ 3)(1\ 2\ 3)(1\ 2\ 3)^{-1}} - e_{(1\ 2\ 3)(1\ 3\ 2)(1\ 2\ 3)} \\ &= e_{(1\ 2\ 3)(1\ 2\ 3)(1\ 3\ 2)} - e_{(1\ 2\ 3)(1\ 3\ 2)(1\ 3\ 2)} \\ &= (e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \\ &= \mathrm{sgn}((1\ 2\ 3))(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)}) \end{aligned}$$

L'espace $W_4 = \mathbb{C}(e_{(1\ 2\ 3)} - e_{(1\ 3\ 2)})$ est donc stable par $\mathcal{S}_3$.

On a finalement $V = W_1 \oplus W_2 \oplus W_3 \oplus W_4 \oplus W$ où W désigne l'unique représentation irréductible de dimension 2.

Exercice 263 Soit p un nombre premier. Soit $\Bbbk$ un corps algébriquement clos de caractéristique différente de p. Soit G un p-groupe.

Montrer que G possède une représentation non triviale de dimension 1 sur $\Bbbk$.

Éléments de réponse 263 Soit p un nombre premier. Soit $\Bbbk$ un corps algébriquement clos de caractéristique différente de p. Soit G un p-groupe.

Montrons que G possède une représentation non triviale de dimension 1 sur $\Bbbk$.

Le groupe G admet un sous-groupe distingué H d'indice p. Par conséquent $\mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/p\mathbb{Z}$. Le corps $\Bbbk$ est algébriquement clos de caractéristique $\neq p$. Par suite le polynôme $X^p - 1$ est scindé

à racines simples. Ainsi les racines p-ième de l'unité dans $\Bbbk^*$ forment un sous-groupe cyclique d'ordre p isomorphe à $\mathbb{Z}/p\mathbb{Z}$ d'où une injection de $\mathbb{Z}/p\mathbb{Z}$ dans $\Bbbk^*$. Le morphisme

$$\mathrm{G} \longrightarrow \mathrm{G}/\mathrm{H} \simeq \mathbb{Z}/p\mathbb{Z} \longrightarrow \Bbbk^*$$

est donc un caractère non trivial de G, *i.e.* une représentation non triviale de dimension 1 de G sur $\Bbbk$.

Exercice 264 Soit G un groupe fini et soit χ un caractère de G vérifiant

$$\forall\, g \in \mathrm{G} \qquad g \neq e \Rightarrow \chi(g) = 0.$$

Montrer que χ est un multiple entier du caractère de la représentation régulière de G.

Éléments de réponse 264 Soit G un groupe fini et soit χ un caractère de G vérifiant

$$\forall\, g \in \mathrm{G} \qquad g \neq e \Rightarrow \chi(g) = 0.$$

Montrons que χ est un multiple entier du caractère de la représentation régulière de G.

Rappel : le caractère de la représentation régulière est donné par

$$\chi_{\rho_R}(g) = \begin{cases} |\mathrm{G}| \text{ si } g = e \\ 0 \text{ sinon} \end{cases}$$

Il suffit de montrer que $|\mathrm{G}|$ divise $\chi(e)$. Notons χ_{triv} le caractère de la représentation triviale de G. On a

$$\langle \chi, \chi_{\mathrm{triv}} \rangle = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \chi(g)\overline{\chi_{\mathrm{triv}}(g)}$$

Comme $\chi(g) = 0$ pour tout $g \neq e$ on a $\displaystyle\sum_{g \in \mathrm{G}} \chi(g)\overline{\chi_{\mathrm{triv}}(g)} = \chi(e)\overline{\chi_{\mathrm{triv}}(e)} = \chi(e)$ autrement dit

$$\langle \chi, \chi_{\mathrm{triv}} \rangle = \frac{1}{|\mathrm{G}|}\chi(e)$$

donc $|\mathrm{G}|$ divise $\chi(e)$.

Exercice 265 Décrire les représentations irréductibles du groupe $\mathrm{GL}(3, \mathbb{F}_2)$ et écrire sa table de caractères.

Éléments de réponse 265

Exercice 266

a) Décrire les représentations irréductibles du groupe diédral D_{2n} et écrire sa table de caractères.

b) Déterminer les sous-groupes distingués de D_8 à l'aide de sa table de caractères.

Éléments de réponse 266

Exercice 267 Soit $\mathbb{H}_8 := \{\pm 1, \pm i, \pm j, \pm k\}$ le groupe des quaternions. Ecrire la table de caractères de $\mathbb{H}_8$ et décrire les représentations irréductibles.

Indication : On rappelle que $\mathbb{H}_8$ s'identifie à un sous-groupe de $\mathrm{SU}(2,\mathbb{C})$ en posant : $I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ et $K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$.

Éléments de réponse 267

On peut vérifier que $\mathbb{H}_8$ admet cinq classes de conjugaison qui sont

$$\{1\}, \quad \{-1\}, \quad \{\pm i\}, \quad \{\pm j\}, \quad \{\pm k\}$$

Le groupe dérivé $D(\mathrm{G})$ de G est donné par : $D(\mathrm{G}) = \{\pm 1\}$. Par conséquent

$$\mathrm{G}/D(\mathrm{G}) = \langle \bar{i}, \bar{j} \,|\, \bar{i}^2 = \bar{j}^2 = 1, \overline{ij} = \overline{ji} \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Ainsi G admet quatre représentations de dimension 1 correspondant aux quatre morphismes de groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{C}^*$. Il s'en suit que la cinquième représentation irréductible de $\mathbb{H}_8$ est de dimension 2. Son caractère se déduit des caractères précédents par orthogonalité.

La table des caractères de $\mathbb{H}_8$ est

$\mathbb{H}_8$	1	1	2	2	2
	$\{1\}$	$\{-1\}$	$\{\pm i\}$	$\{\pm j\}$	$\{\pm k\}$
χ_{triv}	1	1	1	1	1
χ_1	1	1	-1	1	-1
χ_2	1	1	1	-1	-1
$\chi_3 = \chi_1\chi_2$	1	1	-1	-1	1
χ_ρ	2	-2	0	0	0

Notons que les tables de $\mathbb{H}_8$ et D_8 sont les mêmes. La table de caractères ne détermine donc pas la classe d'isomorphisme d'un groupe fini.

Exercice 268 Décrire les représentations irréductibles du groupe symétrique $\mathcal{S}_3$ et écrire sa table de caractères.

Éléments de réponse 268

Exercice 269 [Table de caractères du groupe symétrique $\mathcal{S}_4$]

a) Décrire les représentations irréductibles de $\mathcal{S}_4$ et dresser sa table des caractères.

b) Déterminer les sous-groupes distingués de $\mathcal{S}_4$ à partir de sa table des caractères.

c) On rappelle que $\mathcal{S}_4$ s'identifie au groupe des isométries directes d'un cube (ou d'un octaèdre) et également au groupe des isométries (directes et indirectes) d'un tétraèdre. Que pensez-vous des représentations de dimension 3 associées ?

Éléments de réponse 269

Exercice 270

Déterminer, à isomorphisme près, le groupe dont la table des caractères est :

	e	C_2	C_3	C_4	C_5
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Éléments de réponse 270

Exercice 271

Décrire les représentations irréductibles du groupe $\mathcal{A}_4$ et écrire sa table de caractères.

Éléments de réponse 271

Exercice 272

a) Soit G un groupe fini abélien et soit χ un caractère de G sur $\mathbb{C}$.

Montrer que

$$\sum_{a\in \mathrm{G}} |\chi(a)|^2 \geq |\mathrm{G}| \cdot \chi(1).$$

b) Soit G un groupe fini et soit H un sous-groupe abélien de G d'indice $n \geq 1$.

Montrer que si χ est un caractère irréductible de G, on a $\chi(1) \leq n$. Que peut-on dire si $\chi(1) = n$?

Éléments de réponse 272

Exercice 273

Soit G un groupe fini. Soient ϕ et ψ des caractères de G dans $\mathbb{C}$.

a) Montrer que si ψ est de degré 1, alors $\phi\psi$ est irréductible si et seulement si ϕ est irréductible.

b) Montrer que si ψ est de degré strictement supérieur à 1, alors le caractère $\psi\overline{\psi}$ n'est pas irréductible.

c) Soit ϕ un caractère irréductible de G. On suppose que ϕ est le seul caractère irréductible de son degré. Montrer que s'il existe un caractère ψ de degré 1 et $g \in \mathrm{G}$ tel que $\psi(g) \neq 1$, alors $\phi(g) = 0$.

Éléments de réponse 273

Exercice 274

Soit p un nombre premier. Soit $n \geq 1$ un entier. On pose $q = p^n$. Soit G le groupe donné par

$$\mathrm{G} = \{x \mapsto ax + b \,|\, a \in \mathbb{F}_q^x,\, b \in \mathbb{F}_q\}.$$

a) Déterminer la table des caractères de G sur $\mathbb{C}$.

b) Déterminer les représentations irréductibles de G sur $\mathbb{C}$.

Éléments de réponse 274

Exercice 275

Soient p un nombre premier, G un p-groupe fini et $\Bbbk$ un corps de caractéristique p.

a) Montrer que toute représentation linéaire de G sur un $\Bbbk$-espace vectoriel non nul admet des vecteurs fixes non nuls.

b) Montrer que toute représentation irréductible de G à coefficients dans $\Bbbk$ est isomorphe à la représentation triviale.

Éléments de réponse 275

Exercice 276

a) Soient G un groupe abélien (éventuellement infini) et (V, ρ) une représentation complexe irréductible de G (de dimension éventuellement infinie). Sous quelles hypothèses cette représentation est-elle de dimension 1 ? Est-ce toujours le cas ?

b) Soient $\Bbbk$ un corps de caractéristique nulle, G un groupe (éventuellement infini) et (V, ρ) une représentation de G sur $\Bbbk$ (de dimension éventuellement infinie). Sous quelles hypothèses cette représentation est-elle somme directe de sous-représentations irréductibles ? Est-ce toujours le cas ?

Éléments de réponse 276

Exercice 277

Montrer que deux représentations de degré 1 d'un groupe G sont équivalentes si et seulement si elles coïncident.

Éléments de réponse 277

Exercice 278 Soit G un groupe.

a) Soient ρ_1 et ρ_n des représentations complexes de G de degré respectivement 1 et n. Montrer que

$$\rho_1 \cdot \rho_n \colon \mathrm{G} \longrightarrow \mathrm{GL}_n(\mathbb{C}), \qquad g \longmapsto \rho_1(g) \cdot \rho_n(g)$$

est une représentation de G.

b) Si ρ_n est irréductible, montrer que $\rho_1 \cdot \rho_n$ l'est aussi.

Éléments de réponse 278

Exercice 279 Soient G un groupe fini et H un sous-groupe distingué de G. Montrer que l'ensemble des représentations du groupe quotient G/H s'identifie naturellement aux représentations de G dont la restriction à H est triviale.
En déduire une injection de l'ensemble des représentations irréductibles de G/H dans l'ensemble des représentations irréductibles de G.

Éléments de réponse 279

Exercice 280

Soit $\rho \colon \mathrm{G} \longrightarrow \mathrm{GL}(V)$ une représentation irréductible d'un groupe abélien fini G dans un $\mathbb{C}$-espace vectoriel de dimension finie.

a) Utiliser le lemme de Schur pour montrer que $\rho(g)$ est une homothétie, pour tout $g \in \mathrm{G}$.

b) En déduire que chaque sous-espace vectoriel de V est ρ-invariant.

c) Conclure que le degré de ρ est égal à 1.

Éléments de réponse 280

Exercice 281

Soit ρ la représentation du groupe symétrique $\mathcal{S}_n$ dans $V = \mathbb{C}^n$ agissant par permutations des coordonnées (*i.e.* $\sigma \cdot (x_1, \ldots, x_n) := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$). Montrer que l'hyperplan H d'équation $\sum_{1 \leq i \leq n} x_i = 0$ est stable pour cette action et que la représentation associée est irréductible.

Éléments de réponse 281

Exercice 282

Montrer que tout groupe fini est isomorphe (par exemple via la représentation régulière) à un sous-groupe de $\mathrm{GL}(V)$ où V désigne un espace vectoriel approprié de dimension finie.

Éléments de réponse 282

Exercice 283

Soient G un groupe fini et $\rho\colon \mathrm{G} \to \mathrm{GL}_n(\mathbb{C})$ une représentation de G dans $\mathbb{C}^n$. Construire un produit scalaire hermitien $< \cdot, \cdot >_G$ sur $\mathbb{C}^n$ invariant par G, i.e.

$$\langle \rho(g)(x), \rho(g)(y) \rangle_{\mathrm{G}} = \langle x, y \rangle_{\mathrm{G}}, \qquad \forall\, x, y \in \mathbb{C}^n, \forall\, g \in \mathrm{G}.$$

Retrouver le lemme de MASCHKE : toute sous-représentation de ρ admet un supplémentaire stable par G.

Éléments de réponse 283

Exercice 284

Soient X un ensemble fini et G un groupe fini opérant sur X. Notons V la représentation de permutation de G sur $\mathbb{C}^X$ et χ_V son caractère.
Soit c le nombre d'orbites de l'action de G sur X. Montrer que c est égal au nombre de fois que V contient la représentation triviale 1. En déduire la formule de BURNSIDE :

$$c = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)|.$$

Éléments de réponse 284

Exercice 285

Soit G un groupe fini. Soit H un sous-groupe de G. Soit π une représentation de G de caractère χ.

a) Montrer que la restriction de π à H a pour caractère la restriction $\chi_{|\mathrm{H}}$.

b) Si π est irréductible, est-ce que $\chi_{|\mathrm{H}}$ est un caractère irréductible ?

Éléments de réponse 285

a) Montrons que la restriction de π à H a pour caractère la restriction $\chi_{|\mathrm{H}}$. Pour tout $h \in H$ on a

$$\chi_{\pi_{|\mathrm{H}}}(h) = \mathrm{tr}(\pi_{|\mathrm{H}}(h)) = \mathrm{tr}(\pi(h)) = \chi(h) = \chi_{|\mathrm{H}}(h).$$

b) Si π est irréductible, $\chi_{|\mathrm{H}}$ n'est pas nécessairement un caractère irréductible. En effet soit G un groupe fini non abélien. Soit $H = \{e_{\mathrm{G}}\}$ le sous-groupe trivial de G et soit π une représentation complexe irréductible de G de dimension ≥ 2 (une telle représentation existe). Alors toute droite de π est un sous-espace strict non nul de π stable par H donc $\chi_{|\mathrm{H}}$ n'est pas irréductible.

Exercice 286

Soit G un groupe fini. Soit H un sous-groupe de G. Soit (π, V) une représentation de H. On pose

$$W = \{f\colon \mathrm{G} \to V \,|\, \forall\, x \in \mathrm{G}\, \forall\, h \in H \quad f(hx) = \pi(h) f(x)\}$$

avec une action de G donnée par $g(f)\colon x \mapsto f(xg)$.

a) Montrer que W est une représentation de G. Quelle est sa dimension ?

b) Si π est irréductible, W est-elle une représentation irréductible de G ?

Éléments de réponse 286

a) Montrons que W est une représentation de G. On peut vérifier que
- W est un sous-espace vectoriel de V^{G} ;
- la formule $(g, f) \mapsto g(f)$ définit une action de groupes linéaire de G sur W ;
- pour tout $g \in \mathrm{G}$ et pour tout $f \in W$, on a $f(g)$ appartient à W. En effet, pour tout $h \in H$ et pour tout $x \in \mathrm{G}$ on a

$$f(g)(hx) = f(h(xg)) = \pi(h)f(xg) = \pi(h)f(g)(x).$$

Ces trois points assurent que W est naturellement une représentation de G.

Précisons la dimension de W.

Si $R \subset G$ désigne l'ensemble des représentants de G modulo H l'application

$$W \to V^R \qquad\qquad f \mapsto f_{|R}$$

est une application linéaire. C'est un isomorphisme par définition de W : un élément de W est entièrement déterminé par l'image des éléments de R. Par suite $\dim W = |R| \dim V$, *i.e.* $\dim X = [\mathrm{G} : \mathrm{H}] \dim V$.

b) Si π est irréductible, W n'est pas nécessairement une représentation irréductible de G. Considérons un groupe G non trivial et $H = \{e_{\mathrm{G}}\}$ le sous-groupe trivial. La représentation triviale de H, notée triv, est irréductible. On peut vérifier que $W(\mathrm{triv}) \simeq K[\mathrm{G}]$ où $K[\mathrm{G}]$ désigne la représentation régulière de G. Or cette dernière est irréductible si et seulement si $|\mathrm{G}| = 1$ ce que l'on a exclu.

Exercice 287 [Représentations et sous-groupes distingués, Peyre, l'algèbre discrète de la transformée de Fourier, pages 231-232]

Soit G un groupe fini dont e_{G} est l'élément neutre. Soient ρ_1, ρ_2, …, ρ_r un ensemble de représentants des classes d'isomorphies de représentations irréductibles. Soient χ_1, χ_2, …, χ_r les caractères irréductibles associés. Posons

$$K_{\chi_i} = \{g \in \mathrm{G} \,|\, \chi_i(g) = \chi_i(e_{\mathrm{G}})\}$$

a) Soit $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$ une représentation de caractère χ_V sur un espace V de dimension d. Soit g un élément d'ordre k de G. Alors
(i) $\rho(g)$ est diagonalisable ;
(ii) χ_V est somme de $\chi_V(1) = \dim V = d$ racines $k$ième de l'unité ;
(iii) $|\chi_V(g)| \leq \chi_V(e_{\mathrm{G}}) = d$;
(iv) $K_{\chi_V} = \{x \in \mathrm{G}, |\, \chi_V(x) = \chi_V(e_{\mathrm{G}})\}$ est un sous-groupe distingué de G. On l'appelle noyau de la représentation.

b) Soit $N \lhd \mathrm{G}$ un sous-groupe distingué de G. Soit ρ_U une représentation de G/N sur un espace vectoriel U.

Il existe une représentation canonique de G sur U telle que les sous-représentations de U sous l'action de G/N soient exactement celles de U sous l'action de G.

c) Soit V un espace vectoriel de dimension égale à l'ordre de G. Soit $(b_t)_{t\in\mathrm{G}}$ une base de V. La représentation régulière de G est la représentation

$$\begin{array}{rcl} \rho_{\mathrm{reg}}\colon \mathrm{G} & \to & \mathrm{GL}(V) \\ g & \mapsto & \rho_{\mathrm{reg}}(g)\colon V \to V \\ & & \qquad b_t \mapsto b_{gt} \end{array}$$

Soit $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$ une représentation de G. La représentation est fidèle si ρ est injectif.

Montrer que la représentation régulière est fidèle.

d) Montrer que les sous-groupes distingués de G sont les

$$\bigcap_{i\in I} K_{\chi_i}$$

où $I \subset \{1, 2, 3, \ldots, r\}$.

e) Montrer que G est simple si et seulement si

$$\forall\, i \neq 1,\ \forall\, g \in \mathrm{G} \qquad \chi_i(g) \neq \chi_i(e_{\mathrm{G}}).$$

Éléments de réponse 287

a) (i) Puisque $g^k = 1$, on a $\rho(g)^k = \mathrm{id}$. Le polynôme minimal de $\rho(g)$ divise donc $X^k - 1$ qui est scindé à racines simples.
(ii) Soient $\lambda_1, \lambda_2, \ldots, \lambda_d$ les valeurs propres de $\rho(g)$ qui sont des racines $k$ièmes de l'unité. On a $\chi_V(g) = \lambda_1 + \lambda_2 + \ldots + \lambda_d$.
(iii) On a $|\chi_V(g)| \leq |\lambda_1| + |\lambda_2| + \ldots + |\lambda_d| = d$.
(iv) Si $|\chi_V(g)| = d$, alors d'après (iii) les nombres complexes λ_i sont positivement liés sur $\mathbb{R}$; comme ils sont de module 1, ils sont tous égaux. Si $\chi_V(g) = d$, alors nécessairement $\omega_i = 1$ donc $\rho(g) = \mathrm{id}$. Ainsi $K_{\chi_V} = \ker\rho$ est bien un sous-groupe distingué.

b) Désignons par $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{N}$ la projection canonique. La représentation $\widetilde{\rho}_U$ définie par

$$\forall\, g \in \mathrm{G} \qquad \widetilde{\rho}_U(g) = \rho_U \circ \pi(g)$$

convient.

c) Direct.

d) Soit $\mathrm{N} \lhd G$ un sous-groupe distingué de G. Désignons par ρ_U la représentation régulière de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$. Autrement dit U est un espace vectoriel de dimension égale à $|{}^{\mathrm{G}}\!/_{\mathrm{N}}| = \frac{|\mathrm{G}|}{|\mathrm{N}|}$.

Soit $\mathrm{N} \lhd \mathrm{G}$ un sous-groupe distingué de G. Désignons par ρ_U la représentation régulière de ${}^{\mathrm{G}}\!/_{\mathrm{N}}$. Autrement dit U est un espace vectoriel de dimension égale à $|{}^{\mathrm{G}}\!/_{\mathrm{N}}| = \frac{|\mathrm{G}|}{|\mathrm{N}|}$ de base $(e_g)_{g \in {}^{\mathrm{G}}\!/_{\mathrm{N}}}$ et $\rho_U(h)(e_{\mathrm{G}}) = e_{hg}$. La représentation régulière est fidèle (c)) donc ρ_U est injective. Le b) permet d'étendre cette représentation en une représentation $\widetilde{\rho}_U \colon \mathrm{G} \to U$. Notons χ le caractère de la représentation $\widetilde{\rho}_U$. On a $\ker \widetilde{\rho}_U = \ker(\rho_U \circ \pi) = \mathrm{N}$ D'où $\mathrm{N} = K_\chi$. Ecrivons la décomposition de la représentation $\widetilde{\rho}_U$ en fonction des représentations irréductibles

$$\chi = a_1\chi_1 + a_2\chi_2 + \ldots + a_r\chi_r$$

D'après la troisième assertion de a) on a

$$\forall\, g \in \mathrm{G} \qquad |\chi(g)| \leq \sum_{i=1}^{r} a_i|\chi_i(g)| \leq \sum_{i=1}^{r} a_i|\chi_i(e_{\mathrm{G}})| = \chi(e_{\mathrm{G}}).$$

On a donc l'égalité $\chi(g) = \chi(e_{\mathrm{G}})$, *i.e.* $g \in K_\chi$, si et seulement si

$$\forall\, g \in \mathrm{G} \qquad |\chi(g)| = \sum_{i=1}^{r} a_i|\chi_i(g)| = \sum_{i=1}^{r} a_i|\chi_i(e_{\mathrm{G}})| = \chi(e_{\mathrm{G}})$$

autrement dit si et seulement si

$$\forall\, i \qquad a_i\chi_i(g) = a_i\chi_i(e_{\mathrm{G}}).$$

Ceci est finalement équivalent à

$$\forall\, i \qquad a_i > 0 \Rightarrow g \in K_{\chi_i}.$$

On obtient donc le résultat voulu avec $I = \{i \,|\, a_i > 0\}$.

Réciproquement comme les K_{χ_i} sont distingués tout sous-groupe du type $\bigcap_{i \in I} K_{\chi_i}$ l'est aussi.

e) Supposons qu'il existe un élément de $\mathrm{G} \smallsetminus \{e_{\mathrm{G}}\}$ tel que $\chi_i(g) = \chi_i(e_{\mathrm{G}})$; alors $K_{\chi_i} \subset \mathrm{G}$ est un sous-groupe distingué non trivial et G n'est pas simple.

Réciproquement si G n'est pas simple, il existe $g \neq e_{\mathrm{G}}$ dans un certain sous-groupe distingué $\mathrm{N} \lhd \mathrm{G}$ non trivial. Le d) assure que $\mathrm{N} = \bigcap_{i \in I} K_{\chi_i}$ donc g appartient à K_{χ_i} pour $i \in I \subset \{2, 3, \ldots, r\}$. Ceci signifie bien que $\chi_i(g) = \chi_i(e_{\mathrm{G}})$.

Exercice 288 Le but de cet exercice est de montrer que le centre du groupe $\mathrm{GL}_n(\mathbb{C})$ est le groupe des homothéties.

Une représentation ρ du groupe $\mathrm{GL}_n(\mathbb{C})$ est donnée par son action naturelle sur $\mathbb{C}^n$.

1. Montrer que la représentation ρ est irréductible.

2. Montrer que tout élément du centre de $\mathrm{GL}_n(\mathbb{C})$ est un morphisme de la représentation ρ, *i.e.* montrer que pour tout élément h du centre et pour tout élément M de $\mathrm{GL}_n(\mathbb{C})$ on a
$$\rho(M) \circ h = Mh = hM = h \circ \rho(M).$$
3. Conclure en utilisant le Lemme de Schur.

Éléments de réponse 288 Puisque ρ est l'action naturelle de $\mathrm{GL}_n(\mathbb{C})$ sur $\mathbb{C}^n$, ρ est l'identité de $\mathrm{GL}_n(\mathbb{C})$ dans $\mathrm{GL}_n(\mathbb{C})$.

1. Si un sous-espace vectoriel V de $\mathbb{C}^n$ est stable par tous les éléments de $\mathrm{GL}_n(\mathbb{C})$, alors $V = \{0\}$ ou $V = \mathbb{C}^n$, *i.e.* ρ est irréductible.
2. Soit h un élément du centre de $\mathrm{GL}_n(\mathbb{C})$. Pour tout M dans $\mathrm{GL}_n(\mathbb{C})$ on a
$$\rho(M) \circ h = Mh = hM = h \circ \rho(M)$$
ainsi h est bien un morphisme de la représentation ρ.
3. Comme ρ est irréductible, le Lemme de Schur assure que $h = \lambda \mathrm{id}$ avec $\lambda \in \mathbb{C}^*$, *i.e.* h est une homothétie.

Exercice 289 Soit G un groupe abélien.

1. Si $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$ est une représentation de G, montrer que tout élément G de G définit un G-morphisme $V \to V$.
2. En déduire que toute représentation irréductible de G est de dimension 1.
3. Donner toutes les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$.

Éléments de réponse 289

1. Pour tous G, h et x dans G on a
$$g \cdot (h \cdot x) = (gh) \cdot x = (hg) \cdot x = h \cdot (g \cdot x)$$
c'est-à-dire l'application $\rho(g)\colon x \mapsto g \cdot x$ est un G-morphisme pour tout $g \in \mathrm{G}$.
2. On suppose que V est une représentation irréductible de G. Si $g \in \mathrm{G}$, alors, d'après 1. et le Lemme de Schur, $\rho(g) = \lambda \mathrm{id}$. De plus comme $\rho(g) \in \mathrm{GL}(V)$, λ est non nul. Par conséquent tout sous-espace vectoriel de V est stable par G donc est une sous-représentation de G. Puisque V est irréductible, $\dim V = 1$.
3. D'après 1. une représentation irréductible de $\mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes
$$\rho\colon \mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}(1, \mathbb{C}) = \mathbb{C}^*$$
Tout élément k de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre divisant n ; par suite $\rho(k)$ est aussi d'ordre divisant n, *i.e.* $\rho(k)^n = 1$. Réciproquement pour tout racine $n$ième de l'unité ω l'application
$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*, \qquad k \mapsto \omega^k$$

est une représentation de $\mathbb{Z}/n\mathbb{Z}$. On les obtient donc toutes ainsi.

Notons aussi que l'espace des représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ peut être muni d'une structure de groupe qui le rend isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exercice 290 Soit G un groupe fini. Soit H un sous-groupe abélien de G.

Montrer que toute représentation irréductible de G est de dimension au plus [G : H].

Indication : si V est une représentation irréductible de G*, c'est aussi une représentation de* H*. On pourra considérer la représentation de* G *engendrée par une sous-représentation de* H*.*

Éléments de réponse 290

Soit V une représentation irréductible de G. C'est aussi par restriction une représentation irréductible de H. Puisque H est abélien, V vu comme représentation de H se décompose en somme directe de représentations de H de degré 1. Soit v un vecteur directeur d'une de ces représentations et soit V' le sous-espace vectoriel de V engendré par les vecteurs de la forme $g \cdot v$ où g parcourt G. Il est clair que $V' \neq \{0\}$ est une sous-représentation de V du groupe G ; ainsi $V' = V$. Or si $g' = gh$ avec h dans H, alors par définition de v, $g' \cdot v$ et $g \cdot v$ sont colinéaires. Par conséquent V' est engendré par [G : H] vecteurs, et est donc de dimension au plus [G : H].

Exercice 291 Montrer que tout groupe non abélien admet une représentation irréductible de dimension > 1.

Éléments de réponse 291

Soit G un groupe dont toutes les représentations irréductibles sont de degré 1. La somme des carrés des dimensions des représentations irréductibles de G est égale au cardinal de G ; par suite les classes de conjugaisons de G sont toutes réduites à un élément. Autrement dit G est abélien.

Exercice 292 Montrer que si V est une représentation d'un groupe fini vérifiant $\langle \chi_V, \chi_V \rangle = 2$, alors V est somme de deux représentations irréductibles.

Éléments de réponse 292

Si $V = \oplus V_i^{a_i}$, alors $\langle \chi_V, \chi_V \rangle = 2$ si et seulement si deux a_i distincts sont non nuls et égaux à 1.

Exercice 293 Soit $\mathcal{S}_3$ le groupe des permutations de $\{1, 2, 3\}$.

Notons e, s et t les trois classes de conjugaison de $\mathcal{S}_3$ où e est la classe de conjugaison de l'identité, s celle des transpositions et t celle des 3-cycles.

1. Montrer (sans les construire) que $\mathcal{S}_3$ a deux représentations irréductibles de dimension 1 et une de dimension 2.

2. Notons χ_1 le caractère de la représentation triviale, χ_2 celui de la signature sgn qui est l'autre représentation de dimension 1 et θ celui de la représentation W de dimension 2. De quelle représentation $\psi = \chi_1 + \chi_2 + 2\theta$ est-il le caractère ? Compléter la table

	e	s	t
χ_1			
χ_2			
$\chi_1 + \chi_2 + 2\theta$			
θ			

3. Faisons agir $\mathcal{S}_3$ sur lui-même par conjugaison intérieure ($g \cdot x = gxg^{-1}$). Notons V la représentation de permutation associée et χ son caractère. Calculer χ. En déduire les multiplicités de la représentation triviale, de la représentation sgn et de la représentation W dans la décomposition de V.

Éléments de réponse 293

Exercice 294 On se propose d'établir la table des caractères du groupe $\mathcal{S}_4$ des permutations de $\{1, 2, 3, 4\}$.

1. Soit V la représentation de permutation associée à l'action de $\mathcal{S}_4$ sur $\{1, 2, 3, 4\}$.
   a) Calculer χ_V et $\langle \chi_V, \chi_V \rangle$. En déduire que V est la somme directe $V_1 \oplus V_2$ de deux représentations irréductibles V_1, V_2 non isomorphes.
   b) Déterminer les sous-espaces V_1 et V_2 de V et montrer, en revenant à la définition, que ce sont des représentations irréductibles de $\mathcal{S}_4$.
   c) Calculer les caractères de V_1 et V_2. Quelles lignes de la table cela permet-il de remplir ?
2. Quelle est la seconde représentation de dimension 1 ? Comment peut-on obtenir la seconde de dimension 3 (pourquoi est-elle irréductible et différente de celle déjà construite ?) ?
3. Comment peut-on compléter la table des caractères de $\mathcal{S}_4$?

Éléments de réponse 294

Exercice 295 Soit $\Bbbk$ un corps. Soit $\mathrm{G} \subset \mathrm{GL}(2, \Bbbk)$ le sous-groupe des $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ avec $a \in \Bbbk^*$ et $b \in \Bbbk$. Faisons agir G sur $\Bbbk$ par

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

1. Calculer

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1}.$$

En déduire que les classes de conjugaison de G sont

$$C_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \qquad N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \Bbbk \smallsetminus \{0\} \right\}$$

et les

$$D_a = C_1 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid b \in \Bbbk \right\}$$

pour $a \in \Bbbk^* \smallsetminus \{1\}$.

2. Supposons désormais que $\Bbbk$ est fini, de cardinal q et donc que $|\mathrm{G}| = q(q-1)$ et G compte q classes de conjugaison. Désignons par V la représentation de permutation de G associée à l'action de G sur $\Bbbk$ et W l'hyperplan de V défini par

$$W = \Big\{ \sum_{x \in \Bbbk} \lambda_x e_x, \sum_{x \in \Bbbk} \lambda_x = 0 \Big\}$$

Montrer que W est une sous-représentation de V.

3. Calculer χ_W ; en déduire que W est irréductible.
4. Quelles sont les dimensions des autres représentations irréductibles de G ?
5. Comment peut-on construire un caractère linéaire de G à partir d'un caractère linéaire de $\Bbbk^*$?

   En déduire que si $\Bbbk = \mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, alors la table des caractères de G est la suivante

	C_1	N	D_2	D_4	D_3
χ_{triv}	1	1	1	1	1
η	1	1	-1	1	-1
η^2	1	1	1	-1	-1
η^3	1	1	-1	-1	1
χ_W	2	-2	0	0	0

6. Supposons que $q = 4$. Établir la table des caracères de G. Cette table vous rappelle-t-elle quelque chose ? Pouvez-vous expliquer cette coïncidence ?

Éléments de réponse 295

Exercice 296 Soit G un groupe non commutatif d'ordre 6.

1. Quels sont les ordres des éléments de G ?
2. Montrer que G a deux caractères irréductibles de degré 1 (notés $\mathbf{1}$ et η) et un de degré 2 (noté χ).
3. Montrer que G a trois classes de conjugaison. Quelles sont-elles ?
4. Montrer que $\eta(g) = 1$ si g est d'ordre 2 et que $\eta(g) = -1$ si g est d'ordre 2 (on s'intéressera à $\eta(g^2)$). En déduire le cardinal de chaque classe de conjugaison.

5. Dresser la table des caractères de G.

Éléments de réponse 296

Exercice 297 Faisons agir $\mathcal{S}_n$ sur $\mathbb{C}^n$ par permutation des éléments de la base canonique. Montrer que l'hyperplan $\sum_{i=1}^{n} x_i = 0$ est stable par $\mathcal{S}_n$ et que la représentation ainsi obtenue est irréductible (considérer $v - \sigma \cdot v$ où σ est une transposition).

En déduire une décomposition de $\mathbb{C}^n$ en somme de représentations irréductibles de $\mathcal{S}_n$.

Éléments de réponse 297

Exercice 298 Soit G un sous-groupe fini de $\mathrm{GL}(n, \mathbb{C})$. Montrer que $\sum_{M \in \mathrm{G}} \operatorname{tr} M$ est un entier. Comment cet entier s'interprète-t-il ?

Éléments de réponse 298

INDEX

Index

BIBLIOGRAPHIE

[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.

[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.

[Col11] P. Colmez. *Éléments d'analyse et d'algèbre (et de théorie des nombres)*. École Polytechnique, 2011.

[Com98] F. Combes. *Alèbre et Géométrie*. Bréal, 1998.

[Con]

[DW71] I. M. S. Dey and J. Wiegold. Generators for alternating and symmetric groups. *J. Austral. Math. Soc.*, 12 :63–68, 1971.

[FGN09] S. Francinou, H. Gianella, and S. Nicolas. *Exercices de mathématiques oraux x-ens, algèbre 2*. Cassini, 2009.

[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.

[LS01] R. C. Lyndon and P. E. Schupp. *Combinatorial group theory*. Classics in Mathematics. Springer-Verlag, Berlin, 2001. Reprint of the 1977 edition.

[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.

[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.

[Szp08] A. Szpirglas. *Exercices d'Alèbre*. Cassini, 2008.

[Szp09] A. Szpirglas. *Mathématiques L3 : Algèbre*. Pearson, 2009.