Université Nice Côte d'Azur
Année 2020-2021

Fiche thématique : Groupes

Table des matières

1. Rappels

1.1. Groupes opérant sur un ensemble.

- Généralités :
  - ◇ on dit qu'un groupe G opère sur un ensemble G s'il existe un morphisme de groupes $\mathrm{G} \to \mathcal{S}_E$;
  - ◇ l'orbite d'un élément $e \in E$ est par définition le sous-ensemble $\mathcal{O}_{\mathrm{G}}(e) = \{g \cdot e \,|\, g \in \mathrm{G}\}$; bien sûr si e' appartient à $\mathcal{O}_{\mathrm{G}}(e)$, alors $\mathcal{O}_{\mathrm{G}}(e) = \mathcal{O}_{\mathrm{G}}(e')$;
  - ◇ le stabilisateur de $e \in E$ est par définition le sous-groupe
  $$\mathrm{Stab}_{\mathrm{G}}(e) = \{g \in \mathrm{G} \,|\, g \cdot e = e\};$$
  si $e' = g \cdot e$, alors $\mathrm{Stab}_{\mathrm{G}}(e') = g\,\mathrm{Stab}_{\mathrm{G}}(e)\,g^{-1}$;
  - ◇ on a $|\mathcal{O}_{\mathrm{G}}(e)| = [\mathrm{G} : \mathrm{Stab}_{\mathrm{G}}(e)]$;
  - ◇ équation aux classes :
  $$|E| = |E^{\mathrm{G}}| + \sum_{\substack{\mathcal{O}_{\mathrm{G}}(e) \in \mathcal{O} \\ |\mathcal{O}_{\mathrm{G}}(e)| \neq 1}} |\mathcal{O}_{\mathrm{G}}(e)|$$
  où $\mathcal{O}$ est l'ensemble des orbites ;
  - ◇ formule de Burnside : $\displaystyle\sum_{g \in \mathrm{G}} |\mathrm{Fix}(g)| = |\mathcal{O}| \cdot |\mathrm{G}|$;
  - ◇ l'action est fidèle si $\mathrm{G} \to \mathcal{S}_E$ est injective ;
  - ◇ l'action est transitive s'il n'y a qu'une seule orbite ;
  - ◇ l'action est k-transitive si pour tout k-uplet $(x_1, \ldots, x_k)$ d'éléments de E tous distincts, et tout autre k-uplet $(y_1, \ldots, y_k)$ d'éléments de E tous distincts, il existe g dans G tel que $g \cdot x_i = y_i$ pour tout $1 \leq i \leq k$.

- Cas où E est un groupe :
  - $E = \mathrm{G}$: il y a trois actions classiques, translation à gauche, à droite par g^{-1} et par conjugaison ;
    - on s'intéresse en particulier aux classes de conjugaison (par exemple le groupe symétrique avec la décomposition en cycles à supports disjoints),
    - le centre d'un p-groupe n'est pas réduit à l'élément neutre,
    - tout corps fini est commutatif.
  - E est un sous-groupe de G :
    - s'il est distingué on peut faire opérer G par conjugaison (par exemple soit H un sous-groupe distingué de cardinal p dans un p-groupe, montrer que H est contenu dans le centre),
    - les classes de similitude, d'équivalence, de congruence avec les matrices.
  - E est un quotient de G :
    - soit H un sous-groupe de $\mathcal{S}_n$ d'indice $1 < k < n$ (resp. $k = n$), montrer que $k = 2$ et $\mathrm{H} = \mathcal{A}_n$ (resp. $\mathrm{H} \simeq \mathcal{S}_{n-1}$) ;
    - soit H un sous-groupe d'indice p de G où p est le plus petit premier divisant $|\mathrm{G}|$, en déduire que $\mathrm{H} \triangleleft \mathrm{G}$.
  - E est un ensemble de sous-groupes de G :
    - théorème de Sylow,
    - si G possède un 2-Sylow cyclique, alors G n'est pas simple.
  - E est un autre groupe : on demande que $\mathrm{G} \to \mathcal{S}_E$ s'envoie sur $\mathrm{Aut}(E)$ ce qui permet de définir la notion de produit semi-direct :
    - groupe diédral,
    - trouver tous les groupes d'ordre 30.
- De la géométrie :
  - opération transitive de $\mathrm{GL}(n, \Bbbk)$ sur les bases de $\Bbbk^n$ ce qui dans le cas réel nous amène à la notion d'orientation ;
  - les différentes géométries : affines (rapport de proportionnalité), projectives (birapport), semblables (angles), hyperboliques (angles hyperboliques)...
  - sous-groupes finis de $\mathrm{SO}(3, \mathbb{R})$ et polyèdres réguliers ;
  - lemme du ping-pong ;
  - classification des quadriques projectives ;
  - décomposition de Bruhat : $\mathrm{T}(n, \mathbb{C}) \backslash \mathrm{GL}(n, \mathbb{C}) / \mathrm{T}(n, \mathbb{C}) \simeq \mathcal{S}_n$ où $\mathrm{T}(n, \mathbb{C})$ désigne l'ensemble des matrices triangulaires supérieures. On interprète ce résultat en termes de drapeaux : l'ensemble des classes de paires de drapeaux complets sous l'action de $\mathrm{GL}(n, \mathbb{C})$ est en bijection avec $\mathcal{S}_n$;
  - groupe circulaire ;
  - un groupe libre de rang 2 dans $\mathrm{SO}(3, \mathbb{R})$ et paradoxe de Banach-Tarski ;
  - groupes de pavages (euclidiens, sphériques ou hyperboliques) ;
  - $\mathrm{PGL}(n, \Bbbk)$ agit sur $\mathbb{P}^{n-1}(\Bbbk)$: applications à $n = 2$, 3 et $\Bbbk = \mathbb{F}_2$, $\mathbb{F}_3$;

- ◇ action d'un groupe topologique : si G est un groupe topologique compact agissant sur un espace séparé X alors pour tout $x \in X$, ${}^{\mathrm{G}}\!/_{\mathrm{Stab}_{\mathrm{G}}(X)} \to \mathcal{O}_{\mathrm{G}}(x)$ est un homéomorphisme (par exemple ${}^{\mathrm{SO}(n)}\!/_{\mathrm{SO}(n-1)}$ et $\mathbb{S}^{n-1}$ sont homéomorphes de sorte qu'en particulier $\mathrm{SO}(n)$ est connexe) ;
- ◇ quaternions et groupe orthogonal.

• De la combinatoire :
- ◇ soit G un groupe d'ordre pq qui opère sur un ensemble E de cardinal $n = pq - p - q$; montrer qu'il existe au moins un point fixe et que n est le plus grand cardinal tel que cet énoncé soit vrai ;
- ◇ nombre de coloriages du cube avec c couleurs ;
- ◇ colliers de perles avec 4 bleues, 3 rouges et 2 vertes.

• Théorie des représentations des groupes finis : exemple du groupe symétrique.
• Polynômes symétriques et antisymétriques.

1.2. **Groupe des permutations.**

1.2.1. *Étude du groupe.* Ordre du groupe $\mathcal{S}_n$: $n!$

◇ Formule de conjugaison. On écrit les cycles sous la forme $(i_1 \ \dots \ i_k)$. Attention, il y a k écritures différentes pour le même cycle :

$$\sigma(i_1 \ \dots \ i_k)\sigma^{-1} = (\sigma(i_1) \ \dots \ \sigma(i_k)).$$

◇ Décomposition en cycles à supports disjoints. Exposant, Générateurs.

On a existence et unicité à permutation près de la décomposition en cycles. On en déduit que l'exposant du groupe est le ppcm de $\{1, 2, \dots, n\}$. Il en découle également que les cycles constituent un système de générateurs, puis, les transpositions, grâce à la formule $(i_1 \ i_2 \ \dots \ ik) = (i_1 \ i_2) \dots (i_{k-1} \ i_k)$. Les transpositions de type $(k \ k+1)$ forment un système de générateurs (avec relations de tresses). Pour finir, il faut noter le système de générateurs le plus petit possible (mais dont les relations sont compliquées) donné par $(1\ 2)$ et $(1\ 2 \ \dots \ n)$.

◇ Classes de conjugaison-paramétrisation, cardinal.

Grâce à la décomposition (unique) en cycles, on peut paramétrer les classes de conjugaison via les longueurs de cycles. On peut supposer les longueurs λ_i des cycles décroissantes, de sorte que $\lambda = (\lambda_1, \dots, \lambda_s)$ est la partition associée à la classe de conjugaison de σ. Le nombre de classes de conjugaison de $\mathcal{S}_n$ est donc égal au nombre $p(n)$ de partitions de n, donné par la série génératrice

$$\sum_{n \geq 0} p(n) z^n = \prod_{k \geq 1} \frac{1}{1 - z^k}.$$

Le cardinal d'une classe est donné par

***Proposition* 1.1.** — *Soit σ une permutation de $\mathcal{S}_n$ associée à une partition $\lambda = (\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_s)$ de n. Soit $a_j(\lambda)$ le nombre de fois où j apparaît dans la partition λ, c'est-à-dire, le nombre de supports de cycles C_i de cardinal j. Alors, le cardinal de la classe de conjugaison de σ est égal à*

$$|\mathcal{C}_\sigma| = \frac{n!}{\prod_j a_j(\lambda)! j^{a_j(\lambda)}}$$

◇ Caractères (morphismes) de $\mathcal{S}_n$ dans le groupe multiplicatif $\mathbb{C}^*$.

En utilisant le système de générateurs donné par les transpositions, on montre qu'il y a au plus deux tels morphismes (dont un trivial). On peut ensuite exhiber le morphisme [1]

$$\operatorname{sgn}(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i} = \prod_{(i,j)\in\mathcal{P}_{2,n}} \frac{\sigma(j)-\sigma(i)}{j-i}$$

où $\mathcal{P}_{2,n}$ désigne l'ensemble des parties de $\{1,\ldots,n\}$ à 2 éléments. Notons que $\frac{\sigma(j)-\sigma(i)}{j-i}$ est bien défini pour $\{i,j\}\in\mathcal{P}_{2,n}$, car il ne dépend pas de l'ordre dans lequel on a choisi i et j. Du coup, on introduit le groupe alterné $\mathcal{A}_n := \ker\operatorname{sgn}$.

◇ Automorphismes de $\mathcal{S}_n$.

En utilisant le cardinal des classes de conjugaison d'éléments d'ordre 2, on obtient que tout automorphisme est intérieur (en montrant que toute transposition s'envoie sur une transposition, voir [Per82]), sauf pour $n=6$ où l'on a une exception numérique entre transpositions et 3-transpositions :

$$\frac{6!}{4!2^1} = \frac{6!}{3!2^3}$$

Il n'est pas très difficile de prouver la présence d'un automorphisme extérieur de $\mathcal{S}_6$: on fait par exemple agir $\mathcal{S}_5$ sur ses six 5-Sylow. L'image de l'action est un sous-groupe transitif H de $\mathcal{S}_6$. On fait ensuite agir $\mathcal{S}_6$ sur $\mathcal{S}_6/\mathrm{H}$ qui possède 6 éléments (comme dans la démonstration de H d'indice n implique $\mathrm{H}\simeq\mathcal{S}_{n-1}$), et on obtient, par cette action, un morphisme de $\mathcal{S}_6$ dans lui-même qui en fait est un automorphisme de $\mathcal{S}_6$ et qui envoie H, qui est transitif, sur le stabilisateur de id, qui ne l'est pas.

1.2.2. *Sous-groupes de $\mathcal{S}_n$.*

◇ Le centre.

Le centre de $\mathcal{S}_n$ est trivial pour $n\neq 2$. C'est juste une application de la formule de conjugaison.

◇ Le groupe dérivé = le groupe alterné, qui est engendré par les 3-cycles : $D(\mathcal{S}_n)=\mathcal{A}_n$. L'inclusion directe est évidente. Pour l'inclusion inverse, on le fait en deux temps : d'une part les 3-cycles engendrent $\mathcal{A}_n$ et d'autre part on vérifie qu'ils sont bien dans $D(\mathcal{S}_n)$. C'est très utile : on obtient souvent des morphismes qui partent de $\mathcal{S}_n$ (par des actions de groupes), puis, que l'on dérive.

◇ Le seul sous-groupe d'indice 2 de $\mathcal{S}_n$ est $\mathcal{A}_n$.

---

1. La signature est bien un morphisme de $\mathcal{S}_n$ dans $\mathbb{C}^*$ puisque pour σ, τ dans $\mathcal{S}_n$ nous avons

$$\begin{aligned}
\operatorname{sgn}(\sigma\circ\tau) &= \prod_{\{i,\,j\}\in\mathcal{P}_{2,n}} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i} \\
&= \prod_{\{i,\,j\}\in\mathcal{P}_{2,n}} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \prod_{\{i,\,j\}\in\mathcal{P}_{2,n}} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \prod_{\{k,\,\ell\}\in\mathcal{P}_{2,n}} \frac{\sigma(k)-\sigma(\ell)}{k-\ell} \prod_{\{i,\,j\}\in\mathcal{P}_{2,n}} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).
\end{aligned}$$

◇ Simplicité du groupe alterné.

On montre qu'un sous-groupe distingué contient un 3-cycle, puis, il les contient tous. C'est historique dans la non résolution par radicaux d'une équation de degré 5.

◇ Tout sous-groupe d'indice n de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$ (mais pour $n = 6$ il peut ne pas être le stabilisateur d'un élément). Bien connaître la preuve qui passe par l'action d'un groupe G sur ses classes G/H.

◇ Groupe dérivé du groupe alterné. C'est toujours lui-même sauf pour $n = 3$ (groupe trivial) et $n = 4$ (le groupe de Klein).

1.2.3. *Applications.*

◇ Actions du groupe symétrique.

Il faut remarquer que $\mathcal{S}_n$, à l'instar de $\mathrm{GL}_n(\Bbbk)$, arrive avec une action naturelle. Elle est n-transitive, ce qui constitue un record absolu, quand on sait à quel point la triple-transitivité est rare dans la nature.

- Théorème de Cayley.
- Polynômes symétriques. On a une action par automorphismes de $\mathcal{S}_n$ sur l'algèbre des polynômes à n indéterminées. La sous-algèbre des invariants est l'algèbre des polynômes symétriques. Parmi eux, il y a les polynômes symétriques élémentaires et les polynômes de Newton. Les premiers sont importants car ils engendrent la sous-algèbre des invariants (en toute caractéristique, et même sur $\mathbb{Z}$!) De plus, les fonctions symétriques élémentaires en les racines d'un polynôme unitaire sont les coefficients du polynôme.
- Représentations du groupe symétrique : la triviale, la signature, la naturelle (matrices de permutation), la standard (liée à la double transitivité de l'action naturelle de $\mathcal{S}_n$, ce qui consitute un joli développement, voir. Il est bon de savoir calculer la table de caractères pour $n \leq 5$.
- La table des caractères de $\mathcal{S}_n$ est à coefficients dans $\mathbb{Z}$.

◇ Autres applications

- Le déterminant. Sans signature pas de déterminant. En fait, l'unicité d'une forme n-linéaire alternée à constante près sur un espace vectoriel de dimension n est assez claire, mais l'existence, pas du tout. Cela provient essentiellement de l'existence de la signature.
- Représentation du groupe du tétraèdre ou du groupe de l'icosaèdre.

◇ Exercices classiques :

- La formule de Wilson avec les p-Sylow de $\mathcal{S}_p$, p premier.
- Peut-on voir $\mathcal{S}_n$ comme produit semi-direct de $\mathcal{A}_n$?

2. Exercices

2.1. **Groupes finis, exemple et applications.**

Exercice 1 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 $n\geq 5$).

Solution 1

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 $(v,e_1,e_2,\dots,e_{n-1})$ 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

$$|\mathrm{GL}(n,\Bbbk)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1}).$$

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

$$|\mathrm{SL}(n,\Bbbk)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1}.$$

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 $Z(\mathrm{SL}(n,\Bbbk)) = \{\lambda\mathrm{Id}\,|\,\lambda^n=1\}$. Or il y a $\mathrm{pgcd}(n,q-1)$ racines $n$ièmes de l'unité dans un corps $\Bbbk$ de cardinal q [2] donc

$$|\mathrm{PSL}(n,\Bbbk)| = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{n-2})q^{n-1}}{\mathrm{pgcd}(n,q-1)}.$$

2. 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.

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 $\mathcal{A}_4$ [3] 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 $\mathcal{A}_5$ [4].

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 2 Trouver un groupe fini G non réduit au neutre tel que : le centre de G est {id}, le sous-groupe dérivé de G est G, mais G n'est pas simple.

Solution 2 Il suffit de prendre $\mathrm{G} = \mathrm{G}_1 \times \mathrm{G}_2$, où G_1 et G_2 sont deux groupes simples non abéliens (par exemple $\mathrm{G}_1 = \mathrm{G}_2 = \mathcal{A}_5$). Alors G n'est pas simple car il contient les sous-groupes distingués non triviaux $\mathrm{G}_1 \times \{\mathrm{id}\}$ et $\{\mathrm{id}\} \times \mathrm{G}_2$. On voit tout de suite que le centre de G est le produit direct des centres de G_1 et G_2, et son sous-groupe dérivé est le produit des sous-groupes dérivés de G_1 et G_2, ce qui donne le résultat vu que pour un groupe simple non abélien H, le centre de H est trivial et son sous-groupe dérivé est H.

Exercice 3 Soit D le groupe diédral de cardinal 8 (groupe des isométries du carré). Calculer le centre, le sous-groupe dérivé, et l'abélianisé de D. Mêmes questions pour le groupe des quaternions $\mathbb{H}_8$ d'ordre 8.

---

3. 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.

4. 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.

Solution 3 On voit très facilement que le centre $Z(\mathrm{D})$ de D consiste en $\{\pm\mathrm{id}\}$. Comme ${}^{\mathrm{D}}\!/_{Z(\mathrm{D})}$ est abélien (il est de cardinal 4), son sous-groupe dérivé est inclus dans $Z(\mathrm{D})$, c'est donc $Z(\mathrm{D})$ car ce ne peut pas être le groupe trivial vu que D n'est pas abélien. Comme tout élément g de D vérifie $g^2 \in Z(\mathrm{D})$ (vérification immédiate), tous les éléments non triviaux de ${}^{\mathrm{D}}\!/_{Z(\mathrm{D})}$ sont d'ordre 2, ce qui fait que ce groupe d'ordre 4 n'est pas cyclique, il est 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 $ij = -ji = k$, $ki = -ik = j$, $jk = -kj = i$, ainsi que $i^2 = j^2 = k^2 = -1$. On voit alors que le centre de $\mathbb{H}_8$ est $Z(\mathbb{H}_8) = \{\pm\mathrm{id}\}$. Comme pour D, on en déduit que le sous-groupe dérivé est $Z(\mathbb{H}_8)$ et que l'abélianisé ${}^{\mathbb{H}_8}\!/_{Z(\mathbb{H}_8)}$ est isomorphe à $\left({}^{\mathbb{Z}}\!/_{2\mathbb{Z}}\right)^2$.

Noter que D et $\mathbb{H}_8$ ne sont pas pour autant isomorphes, car D possède cinq éléments d'ordre 2 alors que $\mathbb{H}_8$ n'en a qu'un.

Exercice 4 Soit G un groupe fini tel que le quotient de G par son centre soit abélien. Le groupe G est-il toujours abélien ?

Solution 4 Non : il suffit de prendre 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), donc le quotient ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est de cardinal au plus 4, ce qui implique ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ abélien. C'est l'hypothèse ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ cyclique qui implique G abélien (et donc $\mathrm{G} = Z(\mathrm{G})$).

Exercice 5 Quels sont les groupes finis G tels que tout élément x de G vérifie $x^2 = 1$?

Solution 5 Un tel groupe G est abélien car si x, y sont dans G, alors $x = x^{-1}$ et $y = y^{-1}$, mais aussi $(xy) = (xy)^{-1} = y^{-1}x^{-1}$, ce qui donne $xy = yx$. Notant alors G additivement, on a $2x = 0$ pour tout $x \in \mathrm{G}$, et alors, G est isomorphe au groupe additif $({}^{\mathbb{Z}}\!/_{2\mathbb{Z}})^r$ avec $r \in \mathbb{N}$. Réciproquement, un tel groupe convient bien.

2.2. **Groupes abéliens et non abéliens finis.**

Exercice 6 Le groupe $\mathcal{A}_4$ est-il simple ? le groupe $\mathcal{S}_4$ est-il simple ?

Solution 6 Le groupe $\mathcal{A}_4$ n'est pas simple : le groupe

$$V_4 \simeq \big\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\big\}$$

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 7 Donner un p-Sylow de $\mathrm{GL}(n, \mathbb{F}_p)$.

Solution 7 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 8 Soit G un groupe. Soient a, b deux éléments de G d'ordre fini. Le groupe engendré par a et b est-il fini ?

Solution 8 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 9 Soit G un groupe. Montrer que G est abélien si et seulement si ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est cyclique (rappel : $Z(\mathrm{G})$ désigne le centre du groupe G).

Solution 9 Si G est abélien, alors $Z(\mathrm{G}) = \mathrm{G}$ et ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est cyclique.

Réciproquement supposons que G soit cyclique. Soit γ un élément de G dont l'image $\overline{\gamma}$ dans ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$ est un générateur de ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$.

Montrons que pour tout g dans G il existe z dans $Z(\mathrm{G})$ et n dans $\mathbb{Z}$ tels que $g = z\gamma^n$: notons $\overline{g}$ l'image de $n \in G$ dans ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$. Puisque ${}^{\mathrm{G}}\!/_{Z(\mathrm{G})} = \langle\overline{\gamma}\rangle$, il existe un entier $n \in \mathbb{Z}$ tel que $\overline{g} = \overline{\gamma}^n$. Par suite $z = g\gamma^{-n}$ appartient au noyau du morphisme $\mathrm{G} \to {}^{\mathrm{G}}\!/_{Z(\mathrm{G})}$, *i.e.* $z = g\gamma^{-n}$ appartient à $Z(\mathrm{G})$. D'où $g = z\gamma^n$.

Soient g et g' deux éléments quelconques de G. Ils s'écrivent respectivement $g = z\gamma^n$ et $g' = z'\gamma^{n'}$ avec z, z' dans $Z(\mathrm{G})$ et n, n' dans $\mathbb{Z}$. Alors

$$gg' = z\gamma^n z'\gamma^{n'} = zz'\gamma^n\gamma^{n'} = zz'\gamma^{n'}\gamma^n = z'\gamma^{n'}z\gamma^n = g'g$$

autrement dit le groupe G est abélien.

Exercice 10 Dans le lemme chinois expliciter rapidement comment on construit l'isomorphisme.

Solution 10 **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 11 Donner un exemple de groupe fini simple.

Solution 11 Le groupe des permutations $\mathcal{A}_n$ dès que $n \geq 5$.

Exercice 12 Montrer qu'il n'existe pas de groupe simple d'ordre 30.

Solution 12 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 13 Soit p un nombre premier, soit G un groupe d'ordre p^2. Montrer que G est abélien.

Solution 13 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.

Exercice 14 Décomposer la permutation (1 2 3 4 5)(1 3 5)(3 2) en produit de cycles à support disjoint.

Solution 14 On a (1 2 3 4 5)(1 3 5)(3 2) = (2 1 4 5).

Exercice 15 Donner des applications de l'équation aux classes.

Solution 15 Applications de l'équation aux classes : le centre d'un p-groupe n'est pas trivial, théorème de Wedderburn.

Exercice 16 Donner des applications de la formule de Burnside.

Solution 16 Applications de la formule de Burnside : petit théorème de Fermat, les colliers de Polya.

Exercice 17 Soit G un groupe fini tel que le quotient de G par son centre soit abélien. Le groupe G est-il toujours abélien ?

Solution 17 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 18 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.

Solution 18 Nous utilisons le théorème de structure des groupes abéliens finis. Si $|\mathrm{G}| > 1$, alors il existe une suite d'entiers $1 < a_1 \,|\, a_2 \,|\, \ldots \,|\, a_r$ tels que

$$\mathrm{G} \simeq {}^{\mathbb{Z}}\!/_{a_1\mathbb{Z}} \times {}^{\mathbb{Z}}\!/_{a_2\mathbb{Z}} \times \ldots \times {}^{\mathbb{Z}}\!/_{a_r\mathbb{Z}}$$

Montrons que $r = 1$. Puisque $a_r\mathrm{G} = \{0\}$ nous avons

$$\#\{z \in \Bbbk \,|\, z^{a_r} = 1\} \geq |\mathrm{G}| = a_1 a_2 \ldots a_r.$$

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 $a_1 a_2 \ldots a_r \leq a_r$ qui conduit à $r = 1$.

2.3. **Groupes opérant sur un ensemble.**

Exercice 19 Soit G un groupe fini. Soit p le plus petit nombre premier divisant l'ordre de 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 ${}^{\mathrm{G}}\!/_{\mathrm{H}}$ par $h \cdot (a\mathrm{H}) := (ha)\mathrm{H}$ pour tout $h \in \mathrm{H}$ et 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 l'une des orbites aurait un cardinal $\geq p$.

c) Conclure.

Solution 19

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 H 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 20 Soit E un espace vectoriel de dimension finie n sur un corps $\Bbbk$.

a) On fait 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 ?

Solution 20

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 21

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 donnée une opération $(g, x) \mapsto g \cdot x$ de G sur X telle que pour tout $g \in \mathrm{G}$, 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 ? Même question pour l'opération par conjugaison.

c) On prend $G = (\mathbb{Z}/3\mathbb{Z}, +)$ et $X = (\mathbb{Z}/13\mathbb{Z}, +)$. Combien y a-t-il d'actions de G sur X par automorphismes ? Même question en remplaçant $\mathbb{Z}/13\mathbb{Z}$ par le groupe symétrique $\mathcal{S}_3$.

Solution 21

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 22 Soit E un espace euclidien. On fait opérer son groupe orthogonal $\mathrm{O}(E)$ 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 ?

Solution 22

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 23 Soit G un groupe. Soit $x_0 \in \mathrm{G}$. On appelle centralisateur de x_0 l'ensemble G_{x_0} des éléments x de G vérifiant $xx_0 = x_0x$.

a) Montrer que G_{x_0} est un sous-groupe de G. Est-il toujours distingué ?

b) Supposons G fini. Soit C la classe de conjugaison de x_0 . Trouver une relation entre $|\mathrm{G}|$, $|C|$, et $|\mathrm{G}_{x_0}|$.

Solution 23

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

$$|\mathrm{G}| = |C| \cdot |\mathrm{G}_g|.$$

2.4. **Groupes des permutations d'un ensemble fini.**

Exercice 24 On considère le groupe $\mathrm{G} = \mathcal{A}_4$. Soit $D(\mathrm{G})$ son sous-groupe dérivé. Soit V_4 le sous-groupe de G constitué de l'identité et des doubles transpositions.

a) Montrer que $V_4 \lhd \mathrm{G}$, puis que $D(\mathrm{G}) \subset V_4$ (on observera que G/V_4 est de cardinal 3).

b) Montrer que $D(\mathrm{G}) \neq \{\mathrm{id}\}$ et que G ne possède pas de sous-groupe distingué de cardinal 2.

c) En déduire que $D(\mathrm{G}) = V_4$.

d) Montrer que si H est un sous-groupe d'indice 2 d'un groupe fini A, alors $\mathrm{H} \lhd A$ (regarder les classes à gauche et à droite suivant G).

e) Soit H un sous-groupe de $\mathrm{G} = \mathcal{A}_4$. Montrer que si H est d'indice 2, alors $D(\mathrm{G}) \subset \mathrm{H}$ (on considèrera G/H) et aboutir à une contradiction en utilisant c). Ainsi G (qui est de cardinal 12) n'a pas de sous-groupe de cardinal 6.

f) Montrer au contraire que pour tout $d \in \mathbb{N}^*$ tel que d divise 24, le groupe $\mathcal{S}_4$ possède un sous-groupe de cardinal d.

Solution 24

a) Si on conjugue la double transposition $(a\ b)(c\ d)$ par une permutation σ, on obtient $(\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$, ce qui montre que V_4 est distingué dans $\mathcal{S}_4$, et donc a fortiori dans $\mathcal{A}_4$. Ensuite, comme G/V_4 est d'ordre $\frac{12}{4} = 3$, il est cyclique d'ordre 3 (car 3 est premier) et en particulier abélien, ce qui montre que $D(\mathrm{G}) \subset V_4$.

b) On voit facilement que G n'est pas abélien, donc $D(\mathrm{G}) \neq \{\mathrm{id}\}$. D'autre part un sous-groupe H de G d'ordre 2 est composé de l'identité et d'une double transposition $\tau = (a\ b)(c\ d)$. Si on conjugue τ par $\sigma \in \mathrm{G}$ nous obtenons $(\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$, qui ne reste pas dans H si on choisit par exemple $\sigma \in \mathrm{G}$ telle que $\sigma(a) = a$ et $\sigma(b) = c$, ce qui est toujours possible.

c) On a vu que $D(\mathrm{G}) \subset V_4$, donc l'ordre de $D(\mathrm{G})$ divise 4, mais on a aussi vu que ce ne peut être ni 1 ni 2, donc c'est 4 et $D(\mathrm{G}) = V_4$.

d) Soit $a \notin \mathrm{H}$. Comme le cardinal de l'ensemble G/H des classes à gauche est 2, cet ensemble est composé de H et de la classe $a\mathrm{H}$, qui est le complémentaire de H dans A. De même l'ensemble $\mathrm{H}\backslash\mathrm{G}$ des classes à droite est composé de H et de Ha, qui est aussi le complémentaire de H dans A. Ainsi $a\mathrm{H} = \mathrm{H}a$, et ceci reste vrai quand $a \in \mathrm{H}$. Finalement $a\mathrm{H}a^{-1} = \mathrm{H}$ pour tout $a \in A$, autrement dit $\mathrm{H} \triangleleft A$.

e) D'après d), on a $\mathrm{H} \triangleleft \mathrm{G}$. Alors, le groupe G/H est abélien puisque d'ordre 2, ce qui montre que $\mathrm{H} \supset D(\mathrm{G})$. Mais d'après c), le groupe $D(\mathrm{G})$ est d'ordre 4 alors que H est d'ordre 6, ce qui contredit le théorème de Lagrange.

f) C'est clair pour $d = 1$ et $d = 24$. Pour d = 2, on prend le groupe engendré par une transposition, pour d = 3 celui engendré par un 3-cycle et pour $d =$ 4 celui engendré par un 4-cycle. Pour $d = 6$, le sous-groupe des permutations laissant fixe 1 est isomorphe à $\mathcal{S}_3$, il est donc de cardinal 6. Pour $d = 12$, on prend le sous-groupe $\mathcal{A}_4$. Reste le cas $d = 8$, auquel cas on a un sous-groupe isomorphe au groupe diédral D_4 (cf. exercice 2.4), par exemple celui engendré par un 4-cycle et une transposition.

Exercice 25 Soit $n \geq 2$ un entier. On se propose de montrer que le sous-groupe dérivé de $\mathcal{S}_n$ est $\mathcal{A}_n$, sans utiliser la simplicité de $\mathcal{A}_n$ pour $n \geq 5$. On rappelle que pour $n \geq 3$, le groupe $\mathcal{A}_n$ est engendré par les 3-cycles.

a) Vérifier directement le résultat pour $n = 2$ et $n = 3$.

b) On suppose $n \geq 4$. Soit c un 3-cycle de $\mathcal{S}_n$. Montrer qu'il existe une transposition τ telle que τc soit conjugué de τ dans $\mathcal{S}_n$.

c) En déduire que c est un commutateur et conclure.

Solution 25 On note déjà que comme la signature d'un commutateur est 1, on a toujours $D(\mathcal{S}_n) \subset \mathcal{A}_n$.

a) Pour $n = 2$, on a $\mathcal{S}_2$ abélien et $\mathcal{A}_2$ trivial, donc $\mathcal{A}_2$ est bien le sous-groupe dérivé de $\mathcal{A}_2$.

   Pour $n = 3$, le sous-groupe dérivé de $\mathcal{S}_3$ est non trivial car $\mathcal{S}_3$ est non abélien, et inclus dans $\mathcal{A}_3$ qui est de cardinal premier, donc c'est forcément $\mathcal{A}_3$.

b) Soit $\upsilon = (\alpha\ \beta\ \gamma)$. Si τ est la transposition $(\beta\ \gamma)$, alors $\tau\upsilon = (\alpha\ \gamma)$, qui s'écrit $\sigma\tau\sigma^{-1}$ où σ est une permutation envoyant β sur α et fixant γ.

c) D'après b), le 3-cycle $\upsilon = \tau^{-1}\sigma\tau\sigma^{-1}$ est bien un commutateur. Ainsi $D(\mathcal{S}_n)$ contient n'importe quel 3-cycle, donc contient $\mathcal{A}_n$ (qui est engendré par les 3-cycles). Finalement $D(\mathcal{S}_n) = \mathcal{A}_n$.

Exercice 26 Soit $n \geq 5$. Trouver tous les morphismes de groupes de $\mathcal{S}_n$ dans $(\mathbb{Z}/12\mathbb{Z}, +)$. Que se passe-t-il si on remplace $\mathbb{Z}/12\mathbb{Z}$ par un groupe abélien quelconque ? Et si on prend $n = 4$?

Solution 26 Puisque $\mathbb{Z}/12\mathbb{Z}$ est abélien, le noyau d'un tel morphisme contient le sous-groupe dérivé de $\mathcal{S}_n$ (en effet l'image de tout commutateur est triviale). Comme ce sous-groupe est $\mathcal{A}_n$ (cf. exercice 2.4), un tel morphisme est trivial, ou bien se factorise en un morphisme injectif $Sn/An \simeq \{\pm \mathrm{id}\} \to \mathbb{Z}/12\mathbb{Z}$, l'isomorphisme étant induit par la signature. Ainsi, le seul morphisme non trivial est celui obtenu en composant la signature avec le morphisme envoyant 1 sur $\overline{0}$ et -1 sur $\overline{6}$. Ceci s'applique encore à $n = 4$. Si on remplace $\mathbb{Z}/12\mathbb{Z}$ par un groupe abélien A, les morphismes non triviaux sont obtenus en composant la signature avec le morphisme envoyant 1 sur le neutre de A et -1 sur un élément arbitraire d'ordre 2 de A.

Exercice 27 Soit D_4 le groupe des isométries d'un carré. Montrer qu'on peut le voir comme un sous-groupe de $\mathcal{S}_4$ et donner son cardinal. Est-ce que D_4 est isomorphe à un sous-groupe distingué de $\mathcal{S}_4$ (on pourra utiliser l'Exercice 2.4) ?

Solution 27 Soient a_1, a_2, a_3, a_4 les quatre sommets du carré et O son centre. Toute isométrie du plan qui laisse stable l'ensemble $\{a_1, a_2, a_3, a_4\}$ permute les sommets, d'où un morphisme $\phi\colon \mathrm{D}_4 \to \mathcal{S}_4$ qui est clairement injectif car une applicaiton affine induisant l'identité sur un ensemble de trois points non alignés est l'identité. Notons que D_4 contient déjà au moins 8 éléments : l'identité, les rotations de centre O et d'angles $\frac{\pi}{2}$, $-\frac{\pi}{2}$, π et les quatre symétries orthogonales d'axes respectifs les deux diagonales et les deux médiatrices des cotés. Ainsi le cardinal de D_4 est au moins 8 et divise 24, mais ce n'est pas 24 car ϕ n'est pas surjectif (par exemple, il ne contient pas la permutation envoyant a_1 sur lui-même et a_2 sur a_3 si a_1a_2 est un côté et a_1a_3 une diagonale). Finalement le cardinal de D_4 est exactement 8. Or $\mathcal{S}_4$ n'a pas de sous groupe distingué d'ordre 8, car un tel sous-groupe H vérifierait $\mathcal{S}_4/\mathrm{H}$ abélien (puisque de cardinal 3), et H devrait contenir le sous-groupe dérivé de $\mathcal{S}_4$, lequel est de cardinal 12 via l'exercice 2.4.

Exercice 28 Soit p un nombre premier. Quels sont les p-Sylow de $\mathcal{S}_p$?

Solution 28 Puisque l'ordre de $\mathcal{S}_p$ est $p!$, un tel p-Sylow est d'ordre p, donc est cyclique. Ainsi les p-Sylow sont tout simplement les p-cycles.

Exercice 29 Soit $\Bbbk$ un corps. Soit $A = \Bbbk[X_1, \ldots, X_n]$ la $\Bbbk$-algèbre des polynômes en n indéterminées. On note B la sous-algèbre de A constituée des polynômes symétriques.

a) Les $\Bbbk$-algèbres A et B sont-elles isomorphes ?

b) Soit $P \in A$; pour toute permutation $\sigma \in \mathcal{S}_n$, on note P^σ le polynôme $P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. Montrer que le polynôme

$$S := \prod_{\sigma \in \mathcal{S}_n} P^\sigma$$

est symétrique.

c) Soit $L = \mathrm{Frac}A = \Bbbk(X_1, \ldots, X_n)$ le corps des fractions rationnelles en n indéterminées. On note M le sous-corps de L constitué des fractions rationnelles F symétriques, c'est-à-dire telles que $F^\sigma = F$ pour toute permutation σ de $\mathcal{S}_n$, où $F_\sigma := F(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. Montrer que M est l'ensemble des fractions rationnelles qui peuvent s'écrire $F = \frac{P}{Q}$, avec P et Q dans B.

d) En déduire que $M = \mathrm{Frac}B$. Les corps L et M sont-ils isomorphes ?

Solution 29

a) Soient σ_1, …, σ_n les polynômes symétriques élémentaires. Le théorème de structure des polynômes symétriques dit exactement que le morphisme de $\Bbbk$-algèbres de A dans B qui envoie tout polynôme P sur $P(\sigma_1, \ldots, \sigma_n)$ est un isomorphisme !

b) On a clairement $P^{\sigma\tau} = (P^\sigma)^\tau$ (autrement dit l'application de $\mathcal{S}_n \times A$ dans A qui envoie (σ, P) sur P^σ est une opération à droite) ; de plus $P \mapsto P^\sigma$ est un automorphisme de $\Bbbk$-algèbres pour toute permutation σ. On en déduit immédiatement que S vérifie $S^\tau = \tau$ pour toute permutation τ, autrement dit S est symétrique.

c) Soit $F = \frac{G}{H}$ une fraction rationnelle symétrique, avec G et H dans A. On a aussi

$$F = \frac{\displaystyle\prod_{\sigma \in \mathcal{S}_n} G^\sigma}{H \cdot \displaystyle\prod_{\sigma \neq \mathrm{id}} G^\sigma}$$

D'après b), le numérateur est dans B. C'est aussi le cas du dénominateur D, car pour toute permutation τ nous avons

$$D^\tau = H^\tau \cdot \prod_{\sigma \neq \tau} G^\sigma = H \cdot \prod_{\sigma \neq \mathrm{id}} G^\sigma$$

vu que $H^\tau \cdot G = H \cdot G^\tau$ via l'hypothèse que F est symétrique.

d) Le quotient de deux polynômes symétriques est clairement dans M, et le c) nous dit que la réciproque est vraie. Ainsi on a bien $M = \mathrm{Frac}B$. Le a) implique alors que L et M sont des corps isomorphes (et même qu'il y a un isomorphisme de corps de L sur M qui est aussi un isomorphisme de $\Bbbk$-algèbres, autrement dit qui induit l'identité sur $\Bbbk$).

Références

[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.