

Fiche thématique : Groupes

TABLE DES MATIÈRES

1. Rappels	1
1.1. Groupes opérant sur un ensemble	1
1.2. Groupe des permutations	3
2. Exercices	5
2.1. Groupes finis, exemple et applications	5
2.2. Groupes abéliens et non abéliens finis	6
2.3. Groupes opérant sur un ensemble	7
2.4. Groupes des permutations d'un ensemble fini	8
Références	9

1. RAPPELS

1.1. Groupes opérant sur un ensemble.

- Généralités :
 - ◊ on dit qu'un groupe G opère sur un ensemble E s'il existe un morphisme de groupes $G \rightarrow \mathcal{S}_E$;
 - ◊ l'orbite d'un élément $e \in E$ est par définition le sous-ensemble $\mathcal{O}_G(e) = \{g \cdot e \mid g \in G\}$; bien sûr si e' appartient à $\mathcal{O}_G(e)$, alors $\mathcal{O}_G(e) = \mathcal{O}_G(e')$;
 - ◊ le stabilisateur de $e \in E$ est par définition le sous-groupe

$$\text{Stab}_G(e) = \{g \in G \mid g \cdot e = e\};$$

- ◊ si $e' = g \cdot e$, alors $\text{Stab}_G(e') = g \text{Stab}_G(e) g^{-1}$;
- ◊ on a $|\mathcal{O}_G(e)| = [G : \text{Stab}_G(e)]$;
- ◊ équation aux classes :

$$|E| = |E^G| + \sum_{\substack{\mathcal{O}_G(e) \in \mathcal{O} \\ |\mathcal{O}_G(e)| \neq 1}} |\mathcal{O}_G(e)|$$

où $\mathcal{O}$ est l'ensemble des orbites ;

- ◊ formule de Burnside : $\sum_{g \in G} |\text{Fix}(g)| = |\mathcal{O}| \cdot |G|$;
- ◊ l'action est fidèle si $G \rightarrow \mathcal{S}_E$ 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 $(x_1, \dots, x_k)$ d'éléments de E tous distincts, et tout autre k -uplet $(y_1, \dots, y_k)$ 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 :
 - ◊ $E = G$: 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 dis-joints),
 - * 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 $H = \mathcal{A}_n$ (resp. $H \simeq \mathcal{S}_{n-1}$) ;
 - * soit H un sous-groupe d'indice p de G où p est le plus petit premier divisant $|G|$, en déduire que $H \triangleleft G$.
 - ◊ 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 $G \rightarrow \mathcal{S}_E$ s'envoie sur $\text{Aut}(E)$ 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 $\text{GL}(n, \mathbb{K})$ sur les bases de $\mathbb{K}^n$ 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 $\text{SO}(3, \mathbb{R})$ et polyèdres réguliers ;
 - ◊ lemme du ping-pong ;
 - ◊ classification des quadriques projectives ;
 - ◊ décomposition de Bruhat : $\text{T}(n, \mathbb{C}) \backslash \text{GL}(n, \mathbb{C}) / \text{T}(n, \mathbb{C}) \simeq \mathcal{S}_n$ où $\text{T}(n, \mathbb{C})$ 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 $\text{GL}(n, \mathbb{C})$ est en bijection avec $\mathcal{S}_n$;
 - ◊ groupe circulaire ;
 - ◊ un groupe libre de rang 2 dans $\text{SO}(3, \mathbb{R})$ et paradoxe de Banach-Tarski ;
 - ◊ groupes de pavages (euclidiens, sphériques ou hyperboliques) ;
 - ◊ $\text{PGL}(n, \mathbb{K})$ agit sur $\mathbb{P}^{n-1}(\mathbb{K})$: applications à $n = 2, 3$ et $\mathbb{K} = \mathbb{F}_2, \mathbb{F}_3$;

- ◊ action d'un groupe topologique : si G est un groupe topologique compact agissant sur un espace séparé X alors pour tout $x \in X$, $G/\text{Stab}_G(x) \rightarrow \mathcal{O}_G(x)$ est un homéomorphisme (par exemple $\text{SO}(n)/\text{SO}(n-1)$ et $\mathbb{S}^{n-1}$ sont homéomorphes de sorte qu'en particulier $\text{SO}(n)$ 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 $(i_1 i_2 \dots i_k) = (i_1 i_2) \dots (i_{k-1} i_k)$. 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 morphisme¹

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

où $\mathcal{P}_{2,n}$ désigne l'ensemble des parties de $\{1, \dots, n\}$ 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 $\mathcal{A}_n := \ker \text{sgn}$.

- ◇ 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 $\mathcal{S}_6/H$ qui possède 6 éléments (comme dans la démonstration de H d'indice n implique $H \simeq \mathcal{S}_{n-1}$), 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

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

- ◇ 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 $GL_n(\mathbb{k})$, 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 constitue 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 $\mathbb{k} = \mathbb{F}_q$ un corps fini de cardinal q . Considérons le groupe linéaire $GL(n, \mathbb{k})$ et son sous-groupe $SL(n, \mathbb{k})$.

- Montrer que le centre de $GL(n, \mathbb{k})$ (resp. de $SL(n, \mathbb{k})$) est constitué des matrices scalaires de ce groupe.
- Notons $PGL(n, \mathbb{k})$ (resp. $PSL(n, \mathbb{k})$) le quotient de $GL(n, \mathbb{k})$ (resp. $SL(n, \mathbb{k})$) par son centre. Calculer les ordres de $SL(n, \mathbb{k})$, $PGL(n, \mathbb{k})$ et $PSL(n, \mathbb{k})$.

Soit n un entier. Soit E le $\mathbb{k}$ -espace vectoriel $\mathbb{k}^n$. Désignons par $\mathbb{P}(E)$ l'ensemble des droites vectorielles de $\mathbb{k}^n$ (espace projectif de dimension $n-1$).

- c) Montrer qu'il existe un morphisme injectif Φ de $\mathrm{PGL}(n, \mathbb{k})$ 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 $\mathrm{PGL}(2, \mathbb{k})$ 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 triviale de la simplicité des groupes alternés : tout sous-groupe d'indice n de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$ pour $n \geq 5$).

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

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.

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?

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

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?

Exercice 7 Donner 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?

Exercice 9 Soit G un groupe. Montrer que G est abélien si et seulement si $G/Z(G)$ est cyclique (rappel : $Z(G)$ désigne le centre du groupe G).

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

Exercice 11 Donner un exemple de groupe fini simple.

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

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

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

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

Exercice 16 Donner des applications de la formule de Burnside.

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 ?

Exercice 18 Soit $\mathbb{k}$ un corps commutatif. Soit G un sous-groupe fini du groupe multiplicatif $\mathbb{k}^\times = \mathbb{k} \setminus \{0\}$ de $\mathbb{k}$. Montrer que G est cyclique.

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 .

- Montrer que H opère sur l'ensemble des classes à gauche G/H par $h \cdot (aH) := (ha)H$ pour tout $h \in H$ et tout $a \in G$. Quel est le stabilisateur de aH ? Quelle est l'orbite de la classe H ?
- Montrer que si H n'était pas distingué dans G , alors au moins l'une des orbites aurait un cardinal $\geq p$.
- Conclure.

Exercice 20 Soit E un espace vectoriel de dimension finie n sur un corps $\mathbb{k}$.

- On fait opérer le groupe linéaire $G := \text{GL}(E)$ sur l'ensemble des sous-espaces vectoriels de E par : $g \cdot F := g(F)$ pour tout $g \in G$ et tout sous-espace F de E . Quelles sont les orbites pour cette action ?
- On prend $\mathbb{k} = \mathbb{Z}/7\mathbb{Z}$ et $n = 5$. Combien E possède-t-il de sous-espaces vectoriels de dimension 3 ?

Exercice 21

- Combien y a-t-il d'opérations du groupe $\mathbb{Z}/4\mathbb{Z}$ sur l'ensemble $\{1, 2, 3, 4, 5\}$?
- 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 $g \in G$, 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.
- 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 $\mathcal{S}_3$.

Exercice 22 Soit E un espace euclidien. On fait opérer son groupe orthogonal $O(E)$ sur l'ensemble des sous-espaces vectoriels de E .

- Quelles sont les orbites pour cette action ?
- Donner un énoncé analogue pour les espaces hermitiens.

- c) Y a-t-il un énoncé analogue pour le groupe orthogonal $O(q)$ d'un espace vectoriel de dimension finie muni d'une forme quadratique non dégénérée q ?

Exercice 23 Soit G un groupe. Soit $x_0 \in G$. 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 $|G|$, $|C|$, et $|G_{x_0}|$.

2.4. Groupes des permutations d'un ensemble fini.

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

- a) Montrer que $V_4 \triangleleft G$, puis que $D(G) \subset V_4$ (on observera que G/V_4 est de cardinal 3).
 b) Montrer que $D(G) \neq \{\text{id}\}$ et que G ne possède pas de sous-groupe distingué de cardinal 2.
 c) En déduire que $D(G) = V_4$.
 d) Montrer que si H est un sous-groupe d'indice 2 d'un groupe fini A , alors $H \triangleleft A$ (regarder les classes à gauche et à droite suivant G).
 e) Soit H un sous-groupe de $G = \mathcal{A}_4$. Montrer que si H est d'indice 2, alors $D(G) \subset H$ (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 .

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.

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 $n = 4$?

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) ?

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

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

- a) Les $\mathbb{k}$ -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 $P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$. Montrer que le polynôme

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

est symétrique.

- c) Soit $L = \text{Frac}A = \mathbb{k}(X_1, \dots, X_n)$ 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 $F_\sigma := F(X_{\sigma(1)}, \dots, X_{\sigma(n)})$. 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 $M = \text{Frac}B$. Les corps L et M sont-ils isomorphes ?

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.