Théorie des Groupes et Géométrie

TD n°1 : Les bases de la théorie des groupes

Action de groupes

Exercice 1 (Application des formules de comptage)

On fixe une action d'un groupe G sur un ensemble fini E.

1. On suppose que l'ordre de G est 15, que le cardinal de E est 17 et que E n'a pas de point fixé par tous les éléments du groupe G. Déterminer le nombre d'orbites et le cardinal de chacune d'elles.
2. Montrer que toute action d'un groupe d'ordre $143 = 11 \cdot 13$ sur un ensemble de cardinal 25 possède un point fixe.

Exercice 2 (Théorème de Cauchy)

Montrer le théorème de Cauchy : Tout groupe fini d'ordre divisible par un nombre premier p possède un élément d'ordre p. On pourra faire agir par permutation circulaire le groupe $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble des p-uplets $(x_1, \dots, x_p)$ de G tels que $x_1 \cdots x_p = 1$.

Exercice 3 (Sur la transitivité multiple)

Soit k un entier. On dit qu'une action est k-transitive lorsque pour tout $x_1, ..., x_k \in X$ distincts et tout $y_1, ..., y_k \in X$ distincts, il existe un $g \in G$ tel que $g \cdot x_i = y_i$ pour $i = 1, ..., k$. Soit $k \geqslant 2$.

- Montrer qu'une action est k-transitive si et seulement si elle est transitive et que l'action du stabilisateur <u>de tout point</u> $x \in X$ sur $X \setminus \{x\}$ est $(k-1)$-transitive.
- Montrer qu'une action est k-transitive si et seulement si elle est transitive et que l'action d'un stabilisateur <u>d'un point</u> $x \in X$ sur $X \setminus \{x\}$ est $(k-1)$-transitive.

Exercice 4 (Autour des p-groupes)

Soit p un nombre premier.

1. Montrer que le centre d'un p-groupe[1] G, n'est pas réduit à l'élément neutre.
2. Montrer que si le quotient d'un groupe par son centre est cyclique alors le groupe est abélien, donc égal à son centre.
3. Montrer qu'un groupe d'ordre p^2 est abélien. En déduire la liste des groupes d'ordre p^2.
4. Montrer que le centre Z d'un groupe non abélien G d'ordre p^3 est d'ordre p et $G/Z \simeq (\mathbb{Z}/p\mathbb{Z})^2$.
5. En déduire que $D(G) = Z$.

Exercice 5 (Lemme du Ping-Pong)

Soit G un groupe agissant sur un ensemble E. Soit E_1 et E_2 deux parties non vides et disjointes de E. Soit g_+ et g_- deux éléments de G tels que toute puissance (positive ou négative) de g_+ envoie tout élément de E_1 dans E_2 et toute puissance de g_- envoie tout élément de E_2 dans E_1.

1. Montrer que les mots de la forme $g_+^{k_1} g_-^{l_1} g_+^{k_2} g_-^{l_2} \cdots g_+^{k_d} g_-^{l_d} g_+^{k_{d+1}}$ ne sont pas égaux à l'élément neutre e_G.
2. En déduire en utilisant une conjugaison qu'aucun mot du groupe engendré par g_+ et g_- autre que le mot vide n'est égal à l'élément neutre. On dit alors que le groupe engendré par g_+ et g_- est un groupe libre.
3. Que dire si on suppose seulement que E_1 n'est pas inclus dans E_2 ?

1. i.e. un groupe fini d'ordre une puissance non nulle de p.

4. Montrer le sous groupe de $SL(2,\mathbb{Z})$ engendré par

$$A := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \text{ et } B := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

est libre, en considérant l'action naturelle sur $\mathbb{R}^2$ et les domaines $\{(x,y) \in \mathbb{R}^2, |x| < |y|\}$ et $\{(x,y) \in \mathbb{R}^2, |x| > |y|\}$ délimités par les diagonales.

Théorème de Sylow et produit semi-direct

Exercice 6

Soient $p < q$ deux nombres premiers. Soit G un groupe d'ordre pq.

1. Montrer que $s_q = 1$ où le nombre s_q est le nombre de q-Sylow de G.
2. En déduire que G est un produit semi-direct de $\mathbb{Z}/q\mathbb{Z}$ par $\mathbb{Z}/p\mathbb{Z}$.
3. Montrer que si $p \nmid q-1$ alors G est cyclique.
4. Montrer que si $p|q-1$ alors il existe à isomorphisme près deux groupes d'ordre pq : le groupe cyclique d'ordre pq et le groupe non-abélien d'ordre pq.

Rq le groupe diédral est l'exemple le plus simple du second cas.

Exercice 7

1. Montrer que tout groupe d'ordre 255 est résoluble.
2. Montrer que tout groupe d'ordre 35 est cyclique.
3. Montrer que tout groupe d'ordre 63 est résoluble.
4. Montrer que tout groupe d'ordre 325 est abélien.

Exercice 8 (Groupes d'ordre p^2q)

Soient $p < q$ deux nombres premiers distincts. Nous allons montrer que tout groupe G d'ordre p^2q n'est pas simple. On note s_q le nombre de q-Sylow de G.

1. Montrer que si $s_q \neq 1$ alors $p^2 \equiv 1[q]$.
2. En déduire qu'alors $p = 2$ et $q = 3$, faire ce cas à part.
3. Montrer que si $p \neq 2$ ou $q \neq 3$, alors G n'est pas simple et est le produit semi-direct d'un p-Sylow et d'un q-Sylow.

Petits groupes

Exercice 9 (Groupes d'ordre 12)

Soit G un groupe d'ordre 12. On note s_p le nombre de p-Sylow de G.

1. Faire la liste des groupes abéliens d'ordre 12.
2. Montrer que $s_2 = 1$ ou 3.
3. Montrer que $s_3 = 1$ ou 4.
4. Montrer que $s_2 = 3$ et $s_3 = 4$ est impossible.
5. On suppose à présent G non abélien et $s_2 = 1$, montrer que $s_3 = 4$ et que G est un produit semi-direct d'un groupe d'ordre 4 par un groupe d'ordre 3. Montrer que le 2-Sylow de G n'est pas cyclique.
6. On REsuppose G non abélien et $s_2 = 1$, mais on procède différemment. Trouver morphisme de G vers $\mathfrak{S}_4$ via une action transitive sur 4 objets. Montrer que cette action est fidèle. En déduire que G est isomorphe à $\mathfrak{A}_4$.
7. On suppose à présent G non abélien et $s_3 = 1$. En déduire que $s_2 = 3$ et que G est un produit semi-direct d'un sous-groupe N d'ordre 3 par un sous-groupe K d'ordre 4.
8. En déduire que G est isomorphe à $\mathbb{D}_6 = \mathbb{D}_3 \times \mathbb{Z}/_{2\mathbb{Z}}$ ou à l'unique produit semi-direct non-trivial $\mathbb{Z}/_{3\mathbb{Z}} \rtimes \mathbb{Z}/_{4\mathbb{Z}}$.
9. Conclusion : faire la liste des 5 groupes d'ordre 12.

Groupes symétriques et alternés

Exercice 10 ($\mathfrak{A}_4$ n'a pas de sous-groupe d'ordre 6)

Soit H un sous-groupe d'ordre 6 de $\mathfrak{A}_4$.

1. Montrer que pour tout $g \in \mathfrak{A}_4$, on a $g^2 \in H$.
2. En déduire que H contient tous les 3-cycles.
3. Conclure (éventuellement de deux manières...).
   La réciproque au Théorème de Lagrange est donc fausse. Il s'agit du plus petit contre-exemple.

Exercice 11 (Étude de $\mathfrak{S}_3$)

- Donner les structures de cycles possibles dans $\mathfrak{S}_3$, le nombre d'éléments de $\mathfrak{S}_3$ ayant cette structure, et leur signature.
- Décrire les sous-groupes de $\mathfrak{S}_3$, et ceux qui sont distingués dans $\mathfrak{S}_3$. Déterminer les sous-groupes de Sylow de $\mathfrak{S}_3$.
- Trouver une suite de compositions avec des facteurs abéliens de $\mathfrak{S}_3$.

Exercice 12 (Étude de $\mathfrak{S}_4$)

- Donner les structures de cycles possibles dans $\mathfrak{S}_4$, le nombre d'éléments de $\mathfrak{S}_4$ ayant cette structure, et leur signature.
- Déterminer les sous-groupes distingués de $\mathfrak{S}_4$.
- En déduire que $\mathfrak{A}_4$ n'est pas un groupe simple.
- Déterminer les sous-groupes de Sylow de $\mathfrak{S}_4$.
- Déterminer des suites de compositions avec des facteurs abéliens de $\mathfrak{S}_4$ et $\mathfrak{A}_4$.

Exercice 13

1. Soit $f : \mathfrak{S}_n \to A$ un homomorphisme de groupes de $\mathfrak{S}_n$ vers un groupe abélien. Démontrer que les transpositions ont toutes même image. Si $A = \mathbb{C}^\times$, en déduire que l'image d'une transposition est ± 1 et finalement que f est soit constante soit la signature.
2. Soit G d'indice 2 dans $\mathfrak{S}_n$. Démontrer que G est distingué puis que $G = \mathfrak{A}_n$.

Exercice 14 (Les sous-groupes distingués de $\mathfrak{S}_n$)

Le but de l'exercice est de déterminer les sous-groupes distingués de $\mathfrak{S}_n$ (pour $n \geq 5$).

1. Soit H un sous-groupe distingué de $\mathfrak{S}_n$. Montrer que $H \cap \mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{A}_n$. En déduire que H contient $\mathfrak{A}_n$ ou que $H \cap \mathfrak{A}_n = \{\mathrm{Id}\}$.
2. On suppose que $H \cap \mathfrak{A}_n = \{\mathrm{Id}\}$. Montrer que la restriction à H du morphisme signature est injective. Montrer que dans ce cas que tous les éléments de H sont dans le centre de $\mathfrak{S}_n$ et en déduire que $H = \{\mathrm{Id}\}$.
3. On suppose que H contient $\mathfrak{A}_n$. Montrer alors que $H = \mathfrak{S}_n$ ou $H = \mathfrak{A}_n$ suivant l'indice de H dans $\mathfrak{S}_n$.
4. Conclure : si $n \geqslant 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{\mathrm{Id}\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$..

Exercice 15

Le but de l'exercice est de déterminer les groupes dérivés successifs de $\mathfrak{S}_4$. On notera V_4 le sous-groupe des permutations de profil $(\cdot,\cdot)(\cdot,\cdot)$ (avec l'identité).

1. Montrer que $D(\mathfrak{S}_4) \subset \mathfrak{A}_4$.
2. Calculer les commutateurs $(1,2)(1,3)(1,2)^{-1}(1,3)^{-1}$ et $(1,2,3)(1,2,4)(1,2,3)^{-1}(1,2,4)^{-1}$.
3. Montrer que $D(\mathfrak{S}_4) = \mathfrak{A}_4$.
4. Montrer que $V_4 \subset D(\mathfrak{A}_4)$.
5. Vérifier que V_4 est distingué dans $\mathfrak{A}_4$ et que le quotient $\mathfrak{A}_4/V_4$ est un groupe abélien. En déduire que $D(\mathfrak{A}_4) \subset V_4$.
6. En déduire $D^2(\mathfrak{S}_4)$.
7. Calculer les autres groupes dérivés de $\mathfrak{S}_4$.

Exercice 16

1. Montrer que le sous-groupe de $\mathfrak{S}_n$ engendré par les carrés est égale au groupe $\mathfrak{A}_n$.
2. En déduire (une nouvelle fois, cf exo 11) que $\mathfrak{A}_n$ est l'unique sous-groupe d'indice 2 de $\mathfrak{S}_n$.

Exercice 17

1. Soit $n \geq 5$. Montrer que $\mathfrak{A}_n$ est le seul sous-groupe distingué strict non trivial de $\mathfrak{S}_n$.
2. Soit $n \in \mathbb{N}_{\geq 2}$. Montrer que tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

Résolubilité

Exercice 18 Groupe triangulaire supérieur

1. Montrer que le groupe de Heisenberg H des matrices $3 * 3$ triangulaires supérieures dont les coefficients diagonaux sont égaux à 1, est résoluble.
2. Montrer que le groupe B des matrices triangulaires supérieures $3 * 3$ inversibles est résoluble.

   Bien entendu, le résultat est aussi vrai pour les matrices triangulaires $n * n$.

Exercice 19

Soit G un groupe.

1. Montrer que R, S sont des sous-groupes résolubles G avec $R \triangleleft G$ alors RS est résoluble.
2. En déduire que tout groupe fini possède un unique sous-groupe $\mathcal{R}(G)$ normal résoluble et maximal pour ces propriétés.
3. Montrer que $G/\mathcal{R}(G)$ n'a pas de sous-groupe normal et résoluble.

Exercice 20

Soit G un groupe fini. Montrer l'alternative suivante : G contient un sous-groupe normal non-trivial abélien ou bien G contient un sous-groupe normal non-trivial parfait (i.e $H = D(H)$).

Exercice 21

Montrer que les assertions suivantes sont équivalentes :

- Tout groupe d'ordre impair est résoluble.
- Tout groupe fini simple non-abélien est d'ordre pair.

Le théorème de Feit-Thompson (1962) montrent qu'elles sont vraies.

À la maison - exo basique

Exercice 22 (Des petites questions)

On considère l'action d'un groupe G sur un ensemble X.

1. Montrer qu'un sous-ensemble de X est stable par G si et seulement s'il est réunion d'orbites.
2. Montrer que deux éléments dans la même orbite ont des stabilisateurs conjugués.
3. Montrer que deux éléments conjugués dans le groupe G fixent le même nombre d'éléments.
4. Soit E un ensemble et $Y = \{f : X \to E\}$ l'ensemble des applications de X vers E. Montrer que les formules suivantes $(g * f)(x) = f(g \cdot x)$ et $(g \odot f)(x) = f(g^{-1} \cdot x)$ définissent une action à droite et une action à gauche.

Exercice 23 (Coloriages du diamant)

Combien existe-il de coloriages différents, avec deux couleurs, de cette pyramide double à base carré, que nous appelerons "diamant" ? C'est le but de cet exercice.

Précisons que les faces sont isocèles mais pas équilatérales et qu'on identifiera deux façons de colorier si elles coïncident quitte à déplacer le diamant.

On considère le groupe D des isométries qui conservent globalement le diamant et son action naturelle sur le diamant.

1. Déterminer l'orbite et le stabilisateur d'un sommet A. En déduire le cardinal de D.
2. Déterminer la liste des éléments de D.
3. Calculer le nombre de façons de colorier le diamant.
4. On fait agir le groupe D de façon naturelle sur l'ensemble de ces façons de colorier. A quoi correspond en termes de cette action de groupe le nombre de coloriages différents ?
5. Calculer le nombre de façons de colorier fixées par chaque élément du groupe D.
6. Conclure.

Exercice 24

Déterminer les sous-groupes de Sylow de $\mathbb{Z}/24\mathbb{Z}$.

Exercice 25 (Groupes d'ordre $2p$)

Soient p un nombre premier impair et G un groupe à $2p$ éléments.

1. Montrer que G possède un élément r d'ordre p et un élément s d'ordre 2.
2. Montrer que $G = \langle r, s \rangle$ et que $\langle r \rangle$ est distingué dans G.
3. Montrer que le groupe $Aut(\langle r \rangle)$ des automorphismes de $\langle r \rangle$ est un groupe cyclique d'ordre $p-1$. En déduire que $Aut(\langle r \rangle)$ contient un unique élément d'ordre 2.
4. En déduire que $srs^{-1} = r$ ou $srs^{-1} = r^{-1}$ puis que G est isomorphe au groupe cyclique $\mathbb{Z}/2p\mathbb{Z}$ ou groupe diédral $\mathbb{D}_p$.
5. En déduire que $\mathfrak{S}_3$ est isomorphe à $\mathbb{D}_3$.
6. En déduire la classification des groupes d'ordre $6, 10, 14, 22, ...$.

Exercice 26 (Groupes d'ordre 8)

1. Lister les groupes abéliens d'ordre 8.
2. Soit G un groupe non abélien d'ordre 8. Montrer que G possède un élément a d'ordre 4 et aucun élément d'ordre 8.
3. Montrer que $\langle a \rangle$ est distingué dans G.
4. Soit $b \notin \langle a \rangle$, montrer que si l'ordre de b est 2 alors $bab^{-1} = a^{-1}$.
5. En déduire que ou bien G est isomorphe au groupe diédral $\mathbb{D}_4$ ou bien tous les éléments de $G \setminus \langle a \rangle$ sont d'ordre 4.
6. En supposant que G vérifie la seconde hypothèse, montrer que G possède 6 éléments d'ordre 4 et un élément d'ordre 2.
7. En déduire que G est isomorphe au groupe $\mathbb{H} = \{1, -1, i, -i, j, -j, k, -k\}$ où $i^2 = j^2 = k^2 = -1$ et $ij = k$.

Exercice 27 (Groupes d'ordre pq^β)

Soient $p < q$ deux nombres premiers distincts et $\beta \geqslant 1$ un entier. Soit G un groupe d'ordre pq^β.

1. Montrer que le q-Sylow S de G est unique.
2. Montrer que G est un produit semi-direct entre S et un autre groupe.

Exercice 28

1. Soit G un groupe, a et b deux éléments d'ordre fini qui commutent. On suppose que les sous-groupes engendrés $\langle a \rangle$ et $\langle b \rangle$ ont une intersection réduite au singleton élément neutre $\{e\}$.
   (a) Montrer qu'une égalité $(ab)^m = e$ implique $a^m = e$ et $b^m = e$.
   (b) Calculer l'ordre de ab.
2. Montrer que si deux éléments d'un groupe ont des ordres premiers entre eux, l'intersection des sous-groupes qu'ils engendrent est réduite au singleton élément neutre.
3. Retrouver que tout groupe abélien d'ordre 77 est cyclique.

Exercice 29

Soit p un nombre premier. On note φ la fonction indicatrice d'Euler.

1. Si $n \in \mathbb{N}^*$, montrer que $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ et en déduire que $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.
2. On suppose $p \geq 3$.
   (a) Soient a, b deux éléments d'un groupe G qui commutent et qui d'ordre m et n premiers entre eux. Montrer que ab est d'ordre mn. Le résultat reste-t-il vrai si m et n ne sont plus supposés premiers entre eux ?
   (b) Montrer que pour tout $k \in \mathbb{N}^*$ on a $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ avec $\lambda \in \mathbb{N}^*$ premier à p.
   (c) Si $\alpha \geq 2$, en déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z}) = \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$. On pourra considérer le morphisme naturel $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$.

À la maison - exo +

Exercice 30 (Action par translation sur G/H)

Soit G un groupe et H un sous-groupe. On considère l'action de G sur G/H par translation à gauche.

1. Montrer que cette action est transitive.
2. Identifier le stabilisateur de la classe xH.
3. En déduire le noyau de cette action.
4. *Application 1 :* Supposons G fini. Soit p le plus petit facteur premier de l'ordre de G. Soit H un sous-groupe de G d'indice p.
   - Montrer que les orbites de l'action de H sont réduites à des points.
   - En déduire que H est distingué.
5. *Application 2 :* Montrer qu'un groupe infini qui possède un sous-groupe d'indice fini n'est pas simple.

Exercice 31

Montrer que tout sous-groupe fini du groupe multiplicatif d'un corps (commutatif) est cyclique.