TD n°9 : Structure des groupes finis

1 et 5/12/2023

Nous traiterons dans l'ordre les deux premières questions de l'exercice 1, puis les exercices 4, 5, les deux dernières de l'exercice 6 et le 8. Vous pouvez naviguer librement parmi les exercices restants ou parmi ceux de votre polycopié. Les exercices les plus délicats de la feuille sont marqués d'un ●.

Je reste disponible pour toute question concernant le TD, des maths, ou toute autre chose au bureau T13 (j'y suis à coups sûrs les mardis et vendredis juste avant le TD). Vous pouvez également m'envoyer un mail à nataniel.marquis@dma.ens.fr.

1. Get Sylow-we-oh, Low !

Exercice 1. Des exemples de Sylows

Pour chacun des groupes suivants et chaque premier p intervenant dans son cardinal, donner un p-Sylow, l'identifier à un p-groupe classique, puis donner le nombre de p-Sylow.

1. Le groupe $\mathbb{Z}/28\mathbb{Z}$.
2. Le groupe $\mathfrak{S}_5$.
3. Le groupe $\mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$.

● Exercice 2. Groupes d'ordre 40

Démontrer qu'il existe exactement 14 classes d'isomorphismes de groupes d'ordre 40 et en exhiber des représentants.

Exercice 3. Normalisons

Soit G un groupe fini, p un nombre premier et P un p-Sylow de G. Démontrer que

$$\mathrm{N}_G(\mathrm{N}_G(P)) = \mathrm{N}_G(P).$$

Exercice 4. Une condition arithmétique sur les groupes simples

Soit G un groupe simple fini.

1. Démontrer que pour tout sous-groupe H, nous avons $|G| \mid [G : H]!$.
2. Démontrer que pour tout premier p, le cardinal de G divise $\mathrm{n}_p(G)!$ où $\mathrm{n}_p(G)$ est le nombre de p-Sylow.

Exercice 5. Une réciproque à Lagrange

Démontrer que pour tout p-groupe G et tout diviseur p^i de son cardinal, il existe un sous-groupe distingué de G d'ordre p^i.

Exercice 6. Groupes d'ordre p^3

Soit p un nombre premier impair. Le but de cet exercice est de décrire à isomorphisme près les groupes finis de cardinal p^3. Nous donnerons trois méthodes selon l'ordre maximal d'un élément.

La première question traite du cas où il existe un élément d'ordre p^3 dans notre groupe G.

1. Démontrer que le groupe G est isomorphe à
$$\mathbb{Z}/p^3\mathbb{Z}.$$

Les questions suivantes traitent du cas où l'ordre maximal d'un élément de G est p^2.

2. Démontrer que si G est abélien, il est isomorphe à
$$\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$
3. Nous supposons désormais que G n'est pas abélien. Soit x un élément d'ordre p^2. Démontrer que $G/\mathrm{Z}(G)$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ puis que x n'est pas central.
4. Démontrer qu'il existe $y \notin \langle x \rangle$ tel que $x^p = y^p$ et $(\overline{x}, \overline{y})$ forment une base du quotient par le centre.
5. Démontrer que $[x^{-1} : y]$ est central, puis que
$$(yx^{-1})^p = [y : x^{-1}]^{\frac{p(p-1)}{2}}.$$
6. En utilisant que p est impair, démontrer qu'il existe un élément d'ordre p qui n'appartient pas à $\langle x \rangle$ et en déduire que G est isomorphe au groupe
$$\mathbb{Z}/p^2\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z},$$
où $\varphi(a) = [z \mapsto (1+p)^a z]$.

Les questions suivantes traitent du cas où l'ordre maximal d'un élément de G est p, autrement dit où G est p-élémentaire.

7. Démontrer qu'il existe un sous-groupe distingué de G isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$.
8. En considérant que les p-Sylow de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ sont conjugués, conclure que G est isomorphe à l'un des deux groupes
$$(\mathbb{Z}/p\mathbb{Z})^3 \text{ et } \mathrm{U}_3(\mathbb{Z}/p\mathbb{Z}).$$

Exercice 7. Groupes simples de cardinal inférieur à 60

Nous commençons l'exercice en prouvant en 3 questions qu'aucun groupe dont le cardinal ne possède que trois facteurs premiers (avec répétition) ne peut être simple. Dans la suite, les nombres $r > q > p$ seront des nombres premiers distincts.

1. Démontrer qu'un p-groupe possède un sous-groupe distingué.
2. Démontrer qu'un groupe de cardinal p^2q possède un sous-groupe de Sylow distingué. Démontrer qu'un groupe de cardinal q^2p possède un sous-groupe de Sylow distingué. On pourra compter les éléments qui appartiennent à un sous-groupe de Sylow.
3. Démontrer qu'un groupe de cardinal pqr possède un sous-groupe de Sylow distingué.

Nous finissons cet exercice en donnant une application des trois questions précédentes au classement des groupes simples. Soit G un sous-groupe simple de cardinal inférieur à 60.

1. Démontrer que G est de cardinal premier ou que $|G| \in \{24, 36, 40, 48, 54, 56, 60\}$.
2. En utilisant l'exercice 4, démontrer que $|G|$ est premier ou que $|G| \in \{56, 60\}$.
3. Conclure que le plus petit groupe simple non cyclique est $\mathfrak{A}_5$.

Exercice 8. Groupe simple d'ordre 168

Cet exercice vise à démontrer qu'une groupe simple d'ordre 168 est isomorphe à $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$. Nous fixons G un tel groupe.

1. Démontrer que les 7-Sylow de G sont au nombre de 8. Nous notons $\mathrm{Syl}(7)$ cet ensemble.
2. Soit $\iota : G \to \mathfrak{S}_{\mathrm{Syl}(7)}$ le morphisme induit par l'action par conjugaison. Démontrer que ι est injectif. Nous α un élément d'ordre 7 de G, démontrer que quitte à bien choisir la bijection de $\mathrm{Syl}(7)$ avec $\mathbb{P}^1(\mathbb{Z}/7\mathbb{Z})$, l'élément $\iota(\alpha)$ agit comme $x \mapsto x + 1$.

En particulier, le sous-groupe engendré par α est un 7-Sylow fixe par conjugaison de α : c'est le sous-groupe identifié à ∞ que nous fixerons pour la suite.

3. Démontrer qu'un élément de $\mathfrak{S}_{\mathbb{P}^1(\mathbb{Z}/7\mathbb{Z})}$ qui normalise $\langle x \mapsto x + 1\rangle$ s'écrit $x \mapsto ax + b$. Démontrer que quitte à conjuguer par une puissance de $[x \mapsto x + 1]$, un élément d'ordre 3 qui normalise $\langle x \mapsto x + 1\rangle$ s'écrit $x \mapsto 2^k x$ pour un certain k.
4. Donner le cardinal du normalisateur d'un 7-Sylow. Démontrer que, quitte à mieux choisir la bijection de $\mathrm{Syl}(7)$ avec $\mathbb{P}^1(\mathbb{Z}/7\mathbb{Z})$, il existe un élément β d'ordre 3 dans le normalisateur de ∞ tel que $\iota(\beta) = [x \mapsto 2x]$.
5. Démontrer que l'action de G sur $\mathrm{Syl}(7)$ est 2-transitive. En déduire que $\mathrm{n}_G(3) \geq 28$ puis que cette inégalité est une égalité.
6. Démontrer que $|\mathrm{N}_G(\langle\beta\rangle)| = 6$. En comptant de manière très fine les éléments d'ordre 1, 7, 3, 6 ou une puissance de 2, démontrer que ce normalisateur ne peut être cyclique.
7. Soit γ un élément d'ordre 2 dans $\mathrm{N}_G(\langle\beta\rangle)$. Démontrer que l'action de γ est sans point fixe puis qu'elle permute ∞ et 0.
8. Démontrer que $\gamma\beta\gamma^{-1} = \beta^{-1}$ puis que γ envoie le triplet $(1, 2, 4)$ sur $(3, 5, 6)$, $(5, 6, 3)$ ou $(6, 3, 5)$. Dans tous les cas, démontrer que l'action de γ est celle d'une homographie.

Nous avons trouvé trois éléments α, β et γ qui agissent par homographies.

9. En considérant son indice dans G, démontrer que le sous-groupe $\langle\alpha, \beta, \gamma\rangle$ est égal à G tout entier.
10. En vérifiant que les homographies introduites sont bien dans $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$, conclure.

2. Structure plus fine : Zassenhaus (Party) et (Todrick) Hall

Exercice 9. Théorème de Zassenhaus

Rappelons que le théorème de Schur-Zassenhaus affirme que toute suite exacte de groupes finis

$$1 \to N \to G \to K \to 1$$

où N et K sont d'ordres premiers entre eux est scindée. Autrement dit, tout sous-groupe distingué N d'ordre premier à son indice admet un complément. Nous nous proposons de démontrer que deux tels compléments sont conjugués par un élément de N. Commençons par démontrer le cas où N est abélien.

Dans le cas où N est abélien, considérons $\mathcal{R}(K)$ l'ensemble des sections ensemblistes de $G \to K$ que l'on voit comme des applications $\nabla : K \to G$ telles que la post-composition par la projection sur K est l'identité. Pour deux telles sections, on définit

$$(\nabla_1, \nabla_2) = \prod_{k \in K} \nabla_2(k)^{-1} \nabla_1(k)$$

qui est correctement défini par abélianité de N.

1. Démontrer que la relation $\nabla_1 \sim \nabla_2 \Leftrightarrow (\nabla_1, \nabla_2) = 1$ est d'équivalence. Montrer que l'action par multiplication à droite de G passe au quotient sur ${}^{\mathcal{R}(K)}/_{\sim}$.
2. Démontrer que pour tout $n \in N$, nous avons $(\nabla_1 n, \nabla_2) = (\nabla_1, \nabla_2) n^{|K|}$. En déduire que N agit transitivement et librement sur ${}^{\mathcal{R}(K)}/_{\sim}$.
3. Soit K' un complément de N. Démontrer que le stabilisateur de $[K']$ est égal à K'.
4. En déduire que deux compléments sont conjugués par N.

Il s'agit à présent d'attaquer le cas quelconque par récurrence sur $|N|$. Les cas de base sont les cas abéliens déjà traités.

1. Montrer que $\mathrm{D}(N)$ est un sous-groupe distingué de G, et un sous-groupe strict de N.
2. Soient K_1, K_2 deux compléments de N dans K. Conclure en utilisant les deux suites exactes :

$$1 \to {}^{N}/_{\mathrm{D}(N)} \to {}^{G}/_{\mathrm{D}(N)} \to K \to 1$$

$$1 \to \mathrm{D}(N) \to \mathrm{D}(N)K_1 \to K \to 1.$$

Exercice 10. Autour du théorème de Hall

Rappelons que le théorème de Hall affirme que pour tout groupe résoluble fini G et tout diviseur d de $|G|$ premier à ${}^{|G|}/_{d}$, il existe un sous-groupe de cardinal d dans G.

1. Avec l'exemple de $\mathfrak{A}_5$, démontrer que l'hypothèse de résolubilité n'est pas superflue.
2. Démontrer que tous les sous-groupes de Hall sont conjugués.

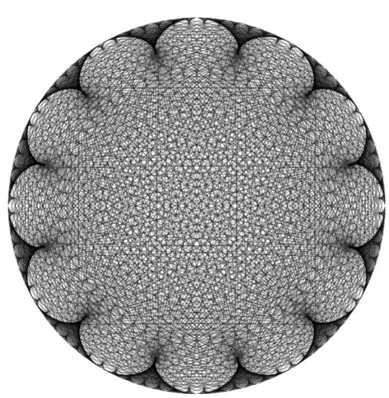

Figure 1 – Puissance 13^e appliquée aux racines 1000-ièmes de l'unité.