TD n°1 : Groupes et groupes cycliques
24 et 27/09/2024

Nous traiterons dans l'ordre les exercices 1, 5, 9 et 10. Vous pouvez naviguer librement parmi les exercices restants. 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.

Exercice 1. Vrai/Faux, première édition

Pour chaque affirmation qui suit, démontrer sa véracité ou trouver un contre-exemple :

1. Le groupe $\mathbb{Z}$ est isomorphe au produit de deux groupes non triviaux.
2. Soit G un groupe. Si G a un nombre fini de sous-groupes, alors G est fini.

● Exercice 2. Autour du type fini

1. Démontrer qu'un groupe fini est de type fini.
2. Démontrer que si H est un sous-groupe d'indice fini d'un groupe G de type fini, alors H est encore de type fini. Est-ce encore vrai sans l'hypothèse sur l'indice ?

Exercice 3. Autour de HK

Soient G un groupe, et H, K deux sous-groupes de G. Pour toute la suite, nous considérons l'application

$$f \,:\, H \times K \to G, \quad (h, k) \mapsto hk.$$

1. Démontrer que f est injective si, et seulement si, on a $H \cap K = \{e\}$.
2. Démontrer que $HK = \mathrm{Im}(f)$ est un sous-groupe de G si, et seulement si, on a $HK = KH$.
3. Démontrer que f est un morphisme de groupes si, et seulement si, on a

$$\forall (h, k) \in H \times K, \;\; hk = kh.$$

4. En déduire une condition nécessaire et suffisante portant sur H et K pour que f soit un isomorphisme de groupes.

Exercice 4. Vrai/Faux, deuxième édition

Pour chaque affirmation qui suit, démontrer sa véracité ou trouver un contre-exemple :

1. Il n'existe pas de morphisme surjectif de $(\mathbb{Q}, +)$ vers $(\mathbb{Q}_+^\times, \times)$.

Pour les trois questions suivantes, on se fixe G un groupe, H et K deux sous-groupes de G tels que $G = HK$.

2. On a $G = KH$.
3. Pour tout $(x, y) \in G^2$, on a $G = (xHx^{-1})(yKy^{-1})$.
4. Supposons $G = LH$ avec L un sous-groupe de G, ainsi que $K \cap H = L \cap H = \{e\}$, alors on a $K = L$.

Exercice 5. Groupes finis monogènes

On rappelle (ou alors reprouvez-le !) que les sous-groupes de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$ pour $n \in \mathbb{N}$. Rappelons également que pour un élément g d'un groupe G, l'application

$$\mathbb{Z} \to G, \;\; n \mapsto g^n$$

est un morphisme de groupes. S'il n'est pas injectif, on appelle ordre de g et on écrit $\omega(g)$ l'entier naturel tel que le noyau s'écrive $\omega(g)\mathbb{Z}$.

1. Vérifier que
$$\omega(g) = \min\{n \in \mathbb{N}_{\geq 1} \,|\, g^n = 1\} = \gcd\{n \in \mathbb{N}_{\geq 1} \,|\, g^n = 1\}.$$
2. Déduire que $g^n = 1 \Leftrightarrow \omega(g)|n$.

Soit $n \geq 2$ et $\zeta_n \in \mathbb{C}$ une racine primitive n-ième de l'unité (i.e. un élément de $(\mathbb{C}^\times, \times)$ d'ordre n). On appelle μ_n le sous-groupe des racines n-ièmes de l'unité.

3. Vérifier que
$$\mathbb{Z}/n\mathbb{Z} \to \mu_n, \;\; a + n\mathbb{Z} \mapsto \zeta_n^a$$
est un isomorphisme de groupes.

Par la suite, nous cherchons à retrouver les premiers résultats d'arithmétique en choisissant la meilleure vision entre $\mathbb{Z}/n\mathbb{Z}$ et μ_n. Il sera souvent pratique de se donner une intuition avec μ_n est parfois nécessaire de raisonner sur $\mathbb{Z}/n\mathbb{Z}$.

4. Soit $d|n$, combien y a-t-il d'éléments d'ordre d dans μ_n ?
5. Soit $k \in \mathbb{Z}$. Quel est l'ordre de $k + n\mathbb{Z}$ dans $n\mathbb{Z}$?
6. Prouver le théorème des restes chinois avec votre point de vue préféré, puis avec l'autre point de vue.
7. Démontrer que tout sous-groupe d'un groupe cyclique est cyclique.

Exercice 6. Vrai/Faux, troisième édition

Soit G un groupe. Pour chaque affirmation qui suit, démontrer sa véracité ou trouver un contre-exemple :

1. Soient $(x, y) \in G^2$ d'ordres finis. L'élément xy est d'ordre fini.
2. S'il existe un entier $n \geq 1$ tel que tout élément de G est d'ordre inférieur à n, alors G est fini.

Exercice 7. Produits de groupes monogènes

Soient G et G' deux groupes monogènes. Donner une condition nécessaire et suffisante pour que $G \times G'$ soit monogène.

Exercice 8. Ordre de l'image d'un élément

Soient $f : G_1 \to G_2$ un morphisme de groupes et $g \in G_1$ un élémnent d'ordre fini. Démontrer que l'ordre de $f(g)$ divise l'ordre de g.

Exercice 9. Ordre et conjugaison

Soit G un groupe fini. On rappelle que deux éléments g et g' sont dits conjugués dans G s'il existe $h \in G$ tels que $g = hg'h^{-1}$.

1. Démontrer que deux éléments conjugués dans G sont de même ordre.
2. Deux éléments de même ordre dans G sont-ils toujours conjugués ? Trouver tous les groupes abéliens finis pour lesquels la réponse est positive.

Exercice 10. Ordre de certaines puissances p-ièmes

Soient G un groupe, H l'un de ses sous-groupes et p un nombre premier. On pose $a \in G \backslash H$ tel que $a^p \in H$. Montrer que $\mathrm{ord}(a) = p\,\mathrm{ord}(a^p)$.

Exercice 11. Ordres et chaos

Le but de cet exercice est de montrer que l'ordre du produit de deux éléments d'ordre fini d'un groupe n'a aucune corrélation avec l'ordre desdits éléments.

1. Illustrer que dans $\mathrm{O}(2)$, le produit de deux éléments d'ordre 2 peut être d'un ordre arbitraire.

Nous commençons par regarder des groupes matriciels complexes pour davantage de simplicité. Soient a et b des entiers avec $a, b \geq 3$. On pose $\zeta_n = e^{2i\pi/n}$ pour $n > 1$ et l'on considère les éléments A, B et $U(t)$ (pour t complexe quelconque) de $\mathrm{SL}_2(\mathbb{C})$ définis par

$$A = \begin{pmatrix} \zeta_a & 0 \\ 0 & \zeta_a^{-1} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & \zeta_b + \zeta_b^{-1} \end{pmatrix} \text{ et } U(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

2. Démontrer[1] que A est d'ordre a, et que B est d'ordre b, dans le groupe $\mathrm{SL}_2(\mathbb{C})$.
3. On pose $B(t) = U(t)BU(t)^{-1}$. Calculer la trace de $AB(t)$.
4. On suppose $c \geq 3$ entier, ou $c = \infty$. Montrer que pour t bien choisi, le produit $AB(t)$ est d'ordre c.

Nous voudrions obtenir le même panel de contre-exemples pour des groupes finis, ce qui nous conduit à travailler sur le corps $\mathbb{F}_p$.

5. En choisissant correctement p, démontrer que pour tous entiers $a, b, c \geq 3$, il existe un groupe fini possédant un élément d'ordre a, un autre d'ordre b, de produit d'ordre c.

1. Avec un peu d'algèbre linéaire, vous pouvez éviter tout calcul.

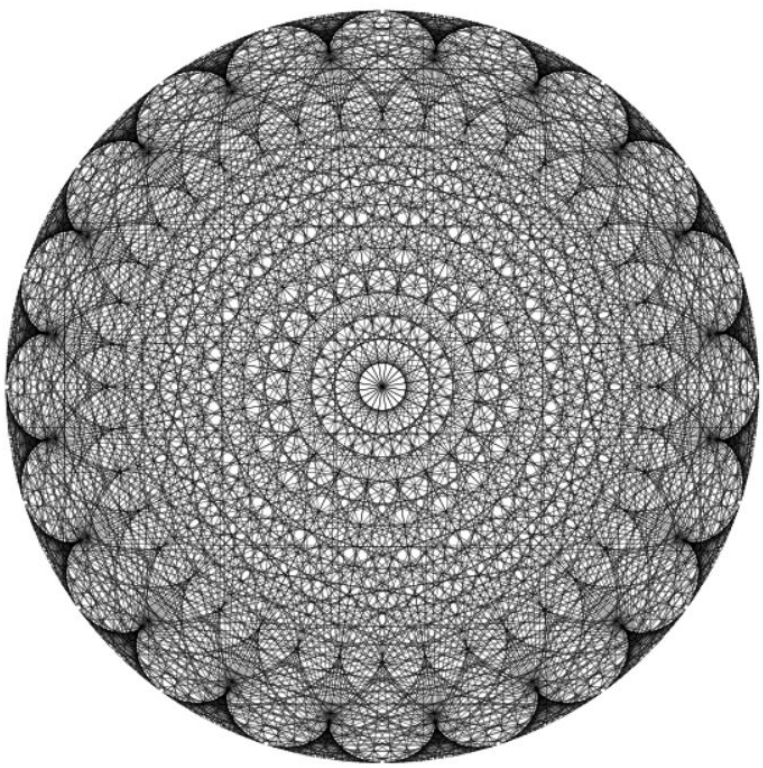

FIGURE 1 – Puissance $21^{\text{iéme}}$ appliquée aux racines 1000-ièmes.