TD n°2 : Groupes et groupes cycliques

26 et 29/09/2023

Nous traiterons dans l'ordre les exercices 1 questions 2) et 3), 2, 5, 11, 17 et 12. 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 Échauffement sur les groupes

Exercice 1. Existence automatique d'inverses

1. Soit $(M, \star)$ un monoïde fini où tout élément est régulier. Démontrer que $(M, \star)$ est un groupe.
2. Soit $(G, \star)$ un groupe et H un sous-ensemble fini non vide de G stable par $\star$. Démontrer que H est un sous-groupe de G.
3. L'hypothèse de finitude est-elle nécessaire dans les deux questions précédentes ?
4. Soit $(M, \star)$ un monoïde tel que tout élément possède un inverse à gauche. Démontrer que $(M, \star)$ est un groupe.

Exercice 2. 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 3. 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 ?

2 Morphismes de groupes

Exercice 4. Propriété universelle des produits

Soit $(G_i)_{i \in I}$ une famille de groupes. Pour chaque élément j, nous définissons la projection

$$\pi_j : \prod_{i \in I} G_i \to G_j, \quad (g_i)_{i \in I} \mapsto g_j.$$

1. Vérifier que π_j est un morphisme de groupes.
2. Démontrer que, pour tout groupe H, l'application suivante est bien définie et bijective.

$$\mathrm{Hom}\left(H, \prod_{i\in I} G_i\right) \to \prod_{i\in I} \mathrm{Hom}\left(H, G_i\right), \quad f \mapsto (\pi_i \circ f)_{i\in I}.$$

Tout comme le cas du quotient (voir TD n°1, exercices 6 et 7), le produit de groupe muni des projections répond ainsi à un problème universel : capturer les familles de morphismes de groupes vers chaque G_i. Nous pourrions démontrer un analogue de la *naturalité* dont nous parlions pour le quotient.

Exercice 5. 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 6. 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 7. Il y a peu d'endomorphismes

Soit G un groupe fini d'ordre n.

1. Démontrer qu'il existe une famille de générateurs de G finie et minimale pour l'inclusion.
2. En bornant son cardinal, démontrer que G possède au plus $n^{\log_2(n)}$ endomorphismes.

Exercice 8. Il y a peu de groupes, et de nombreux automorphismes

Trouver les groupes finis dont le seul automorphisme est l'identité.

Remarque : on pourra sous peu généraliser le résultat sans hypothèse de finitude.

3 Autour de l'ordre d'un élément

Exercice 9. 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 10. 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 11. 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 12. Endomorphismes de certains produits

1. Soit G et G' deux groupes finis d'ordres premiers entre eux. Exhiber un isomorphisme de monoïdes

$$\mathrm{End}(G) \times \mathrm{End}(G') \cong \mathrm{End}(G \times G')$$

qui se restreint-corestreint en un isomorphisme si l'on remplace "endomorphisme" par "automorphisme".

Remarque : vous pouvez généraliser à une famille $(G_i)_{i \in I}$ de groupes d'exposants finis et deux à deux premiers entre eux et obtenir un isomorphisme

$$\prod_{i \in I} \mathrm{End}(G_i) \cong \mathrm{End}\left(\prod_{i \in I} G_i\right)$$

qui se restreint-corestreint pareillement.

2. Trouver un contre-exemple lorsque les ordres ne sont pas premiers entre eux.

Exercice 13. 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

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

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.

4 Groupes monogènes et cycliques

Exercice 14. 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 15. 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 16. Vrai/Faux, quatrième édition

Vrai ou Faux ? Un groupe dont tous les sous-groupes strictes sont cycliques est cyclique.

Exercice 17. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

Le but de cet exercice est de déterminer, pour tout entier n, la structure du groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^\times$. Nous commençons par essayer de dévisser le problème.

1. Soient A, B deux anneaux dont on notera $+$ et $\times$ les lois. On appelle morphisme d'anneaux une application de A dans B qui est un morphisme de groupes additifs et de monoïdes multiplicatifs. Ceci équivaut aux trois formules

$$\forall a, a' \in A, \quad f(a + a') = f(a) + f(a'), \quad f(aa') = f(a)f(a') \text{ et } f(1) = 1.$$

Démontrer l'égalité suivante entre les sous-ensembles de $A \times B$:

$$(A \times B)^\times = A^\times \times B^\times.$$

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

2. Remarquer que l'isomorphisme du théorème des restes choinois est un morphisme d'anneaux. En déduire que pour $\mathrm{pgcd}(n,m)=1$, le groupe $(\mathbb{Z}/nm\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$.
3. Retrouver ce résultat en utilisant l'exercice 12.

La question précédente permet de se ramener au cas $n=p^k$. Nous allons démontrer que pour tout nombre premier impair p, nous avons

$$\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times \cong \mathbb{Z}/p^{k-1}(p-1)\mathbb{Z}$$

puis que

$$\forall k \geq 2,\ \left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}.$$

4. Démontrer que $(\mathbb{Z}/p^k\mathbb{Z})^\times$ contient un élément d'ordre $p-1$.
5. Démontrer pour tout entier $r \geq 1$,

$$\forall (a,b) \in \mathbb{Z}^2,\ a \equiv b \mod p^r \implies a^p \equiv b^p \mod p^{r+1}.$$

En déduire pour tout premier p l'ordre de $\overline{1+p}$ dans $(\mathbb{Z}/p^k\mathbb{Z})^\times$.

6. Conclure si $p \neq 2$.
7. Traiter le cas $p=2$.
8. En guise d'application, déterminer les entiers naturels $n \geq 1$ tels que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

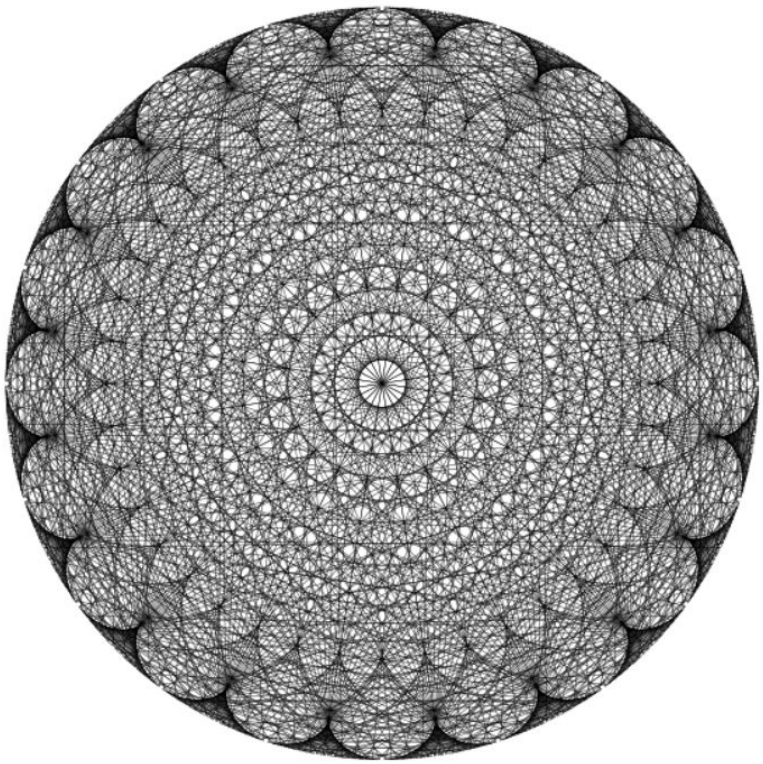

FIGURE 1 – Puissance $21^{\text{iéme}}$ appliquée aux racines 1000-ièmes.