TD n°4 : Groupes abéliens

13 et 17/10/2023

Nous traiterons dans l'ordre les exercices 1, 2, 5, 7 et 9. 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 Groupes abéliens

Exercice 1. Échauffement ?

Quelques questions avec des nombres précis pour pratiquer la structure des groupes abéliens de type fini.

1. Trouver tous les groupes abéliens d'ordre 8 à isomorphisme près, puis d'ordre 500.
2. Donner les facteurs invariants du groupe abélien $(\mathbb{Z}/392\mathbb{Z})^\times$.

Exercice 2. Sous-groupes des groupes abéliens finis

Soit G un groupe abélien fini.

1. Démontrer qu'il existe une unique famille $(n_{p,k})_{p\in\mathbb{P},\, k\geq 1}$ d'entiers presque tous nuls tels que
$$G \cong \prod_{p\in\mathbb{P}} \left[\prod_{k\geq 1} \left(\mathbb{Z}/p^k\mathbb{Z}\right)^{n_{p,k}} \right].$$
2. Soit d un entier divisant $|G|$. Démontrer qu'il existe un sous-groupe d'ordre d dans G.

Exercice 3. Il y a beaucoup d'automorphismes, version abélienne

Soit N un entier naturel.

1. Démontrer qu'il n'existe qu'un nombre fini de classes d'isomorphismes de groupes de cardinal inférieur à N.
2. Démontrer qu'il n'existe qu'un nombre fini de classes d'isomorphismes de groupes abéliens de type fini possédant moins de N automorphismes.

Exercice 4. Extension des scalaires

Dans cet exercice, nous fixons G un groupe abélien de loi notée additivement. Sur $G\times\mathbb{N}_{>0}$, nous définissons la relation $\sim$ comme

$$(g,n)\sim(g',n') \Leftrightarrow \exists m\in\mathbb{N}_{>0},\ \ m(n'g-ng')=0$$

et la loi

$$(g,n)+(g',n')=(n'g+ng',nn').$$

Pour se donner une intuition par la suite, vous pourrez penser au couple (g,n) comme au quotient g/n ce qui permet d'interpréter l'addition comme l'addition des fractions et la relation d'équivalence comme l'identification des différentes écritures d'une fraction.

1. Démontrer que $+$ munit $G\times\mathbb{N}_{>0}$ d'une structure de monoïde abélien de neutre $(0,1)$. Vérifier que $\sim$ est une relation d'équivalence compatible à l'addition [1].

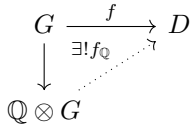
Le monoïde $\mathbb{Q}\otimes G$ est défini comme étant ensemblistement le quotient $(G\times\mathbb{N}_{>0})/\sim$ munit de la loi $+$ passée au quotient [2].

2. Démontrer que $\mathbb{Q}\otimes G$ est un groupe abélien, et vérifier que

$$G\to\mathbb{Q}\otimes G,\ \ g\mapsto[(g,1)]$$

est un morphisme de groupes.

3. Démontrer que $\mathbb{Q}\otimes G$ est uniquement divisible [3]. En déduire que pour groupe uniquement divisible D et tout morphisme de groupes $f:G\to D$, il existe un unique morphisme qui rend le diagramme suivant commutatif



4. Soient G,H deux groupes. Exhiber un isomorphisme entre $\mathbb{Q}\otimes(G\times H)$ et $(\mathbb{Q}\otimes G)\times(\mathbb{Q}\otimes H)$.
5. Soit à présent G un groupe abélien de type fini. Démontrer sans utiliser le théorème de struture que $\mathbb{Q}\otimes G$ est isomorphe à $\mathbb{Q}^r$ pour un entier r. Raffiner en démontrant que r est l'entier tel que $G\cong G_{\text{tors}}\times\mathbb{Z}^r$.
6. Démontrer que si $f:G\hookrightarrow G'$ est un morphisme injectif entre groupes abéliens de type fini, alors le morphisme déduit

$$\mathbb{Q}\otimes G\to\mathbb{Q}\otimes_{\mathbb{Z}}G',\ \ [(g,n)]\mapsto[(f(g),n)]$$

est injectif. En déduire que tout sous-groupe de type fini [4] de $\mathbb{Z}^n$ est isomorphe à un $\mathbb{Z}^m$ pour un certain $m\leq n$.

Exercice 5. Vrai/Faux

Soit G un groupe abélien de type fini. Les affirmations suivantes examinent ce que donnent les notions de famille libre et de famille génératrice. Pour chacune des affirmations suivantes, démontrer qu'elle est vraie ou trouver un contre-exemple. Attention, minimale ou maximale concernera toujours l'ordre de l'inclusion et non le cardinal.

1. Une famille génératrice minimale est libre.
2. Si G est sans torsion, une famille génératrice minimale est libre.

1. Ceci signifie que si $g\sim g'$ et $h\sim h'$ alors $g+g'\sim h+h'$.
2. Ce passage est possible précisément car nous avons démontrer que la loi étant invariante.
3. Un groupe H est uniquement divisible si $\forall h\in H,\ n\geq 1,\ \exists! h'\in H,\ \ h=nh'$.
4. Cette hypothèse de type fini n'est en réalité pas nécessaire.

3. Si G est sans torsion, il existe une famille génératrice et libre.
4. Une famille libre maximale est génératrice.
5. Le cardinal des familles génératrices minimales est borné par une constante indépendante de la famille.
6. Le cardinal des familles libres est borné par une constante indépendante de la famille.

Exercice 6. Sous-groupes de $\mathbb{R}^n$

Nous fixons dans cet exercice un entier naturel n. Nous cherchons à comprendre davantage les sous-groupes de $\mathbb{R}^n$. Nous commençons par traiter le cas où le sous-groupe G considéré est discret, i.e. pour tout $g \in G$, il existe un voisinage U de g tel que $U \cap G = \{g\}$. Nous chercherons à montrer qu'il existe un unique entier $m \geq n$ tel que $G \cong \mathbb{Z}^m$.

1. Démontrer que pour tout compact K de $\mathbb{R}^n$, l'intersection $K \cap G$ est finie.
2. Se ramener au cas où $\mathrm{Vect}(G) = \mathbb{R}^n$.

Nous posons alors $(e_i)_{1 \leq i \leq n}$ une base de $\mathbb{R}^n$ incluse dans G.

3. Soit $j \in [\![1, n]\!]$. Nous écrivons tout élément $g \in G$ comme

$$g = \sum_{i=1}^{n} x_{i,g} e_i.$$

Démontrer que $\{x_{1,g} \mid g \in G\}$ est un sous-groupe de $\mathbb{R}$ qui s'écrit $\alpha\mathbb{Z}$ pour un certain $\alpha \in]0, 1]$.

4. Conclure par récurrence que $G \cong \mathbb{Z}^n$.

Indication : on pourra considérer g_1 tel que $x_{1,g_1} = \alpha$.

Nous nous intéressons ensuite au cas d'un sous-groupe fermé, puis au cas général.

5. Soit G un sous-groupe fermé de $\mathbb{R}^n$. Démontrer qu'il existe un unique sous-$\mathbb{R}$-espace vectoriel V de $\mathbb{R}^n$, un supplémentaire W de V et un sous-groupe discret $\Gamma \subset W$ tel que

$$G = V \oplus \Gamma.$$

Indication : on pourra considérer le sous-$\mathbb{R}$-espace vectoriel maximal inclus dans G.

6. En déduire qu'il existe un unique couple $k, l \geq 0$ tel que $G \cong \mathbb{Z}^k \times \mathbb{R}^l$, et qu'il vérifie $k + l \leq n$.
7. Soit G un sous-groupe de $\mathbb{R}^n$. Démontrer qu'il existe (V, W), sous-espaces vectoriels supplémentaires de $\mathbb{R}^n$, un sous-groupe dense $\tilde{G} \subseteq V$ et un sous-groupe discret $\Gamma \subset W$ tel que

$$G = \tilde{G} \oplus \Gamma.$$

Qu'est-ce qui est unique dans cette écriture ?

2 Caractères

Exercice 7. Prolongement des caractères

Soit $H \leq G$ un sous-groupe d'un groupe abélien G noté additivement. Soit D un groupe abélien divisible[5] et $f : H \to D$ un morphisme de groupes.

5. Ceci signifique que tout élément possède une racine n-ième, pour tout $n \geq 1$.

1. Démontrer qu'il existe un morphisme de groupes $\widetilde{f} : G \to D$ tel que $\widetilde{f}_{|H} = f$.
2. Appliquer la question précédente pour retrouver que pour tout groupe abélien fini G, nous avons

$$\forall g \in G \backslash \{0\},\ \exists \chi \text{ caractère de } G,\ \chi(g) \neq 1.$$

Exercice 8. Coniques de $\mathbb{F}_p$

Le but de cet exercice est d'étudier le nombre de points sur les coniques de $\mathbb{F}_p$. Puisqu'ils s'agit d'équation polynomiales, nous préférerions la notation $\mathbb{F}_p$ pour désigner l'anneau $\mathbb{Z}/p\mathbb{Z}$, mais nous garderons cette notation plus proche de votre cours pour cet exercice. Soit p un nombre premier impair.

1. Soit $\chi \in \widehat{(\mathbb{Z}/p\mathbb{Z})^\times}$ non trivial. Démontrer que la somme de Jacobi $\mathrm{J}(\chi, \chi^{-1})$ vaut $-\chi(-1)$.
2. Soient $\alpha, \beta \in (\mathbb{Z}/p\mathbb{Z})^\times$. Nous considérons la conique

$$C = \left\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid \alpha x^2 + \beta y^2 = 1\right\}.$$

   Démontrer que

$$|C| = p - \left(\frac{-\alpha\beta}{p}\right)$$

   où $\left(\frac{\cdot}{p}\right)$ dénote le symbole de Legendre.
3. Démontrer qu'il existe $(p \pm 1)/4$ carrés x dans $\mathbb{Z}/p\mathbb{Z}$ tels que $x+1$ n'est pas un carré, le signe dépendant de la congruence de p modulo 4.

3 Inclassés

Exercice 9. Groupes d'exposant fini

Nous commençons notre analyse en regardant les groupes d'exposant 2. Soit G un tel groupe, i.e. non trivial et tel que

$$\forall g \in G,\ \ g^2 = e.$$

1. Démontrer que G est abélien.
2. Démontrer qu'il existe un ensemble non vide X tel que G est isomorphe à la somme directe $(\mathbb{Z}/2\mathbb{Z})^{\oplus X}$.

Nous nous intéressons ensuite aux groupes d'exposant fini. Nous rappelons que pour un groupe dont tous les éléments sont d'ordre fini, l'exposant est défini comme le ppcm des ordres de ses éléments [6].

3. Trouver les entiers naturels $N \geq 1$ tel que tout groupe d'exposant N est abélien.

6. Cet exposant est éventuellement un entier supernaturel.

Exercice 10. Il y a beaucoup d'automorphismes, version générale

Nous avons démontré à l'exerice 3 qu'il n'existe qu'un nombre fini de groupes abéliens finis à nombre d'automophismes fixé. Cet exercice vise à démontrer l'énoncé bien plus délicat suivant : il n'existe qu'un nombre fini de classes d'isomorphismes de groupes possédant moins de N automorphismes.

3. Démontrer que $[G : Z(G)] \leq N$.

Nous fixons pour la suite m cet indice, prenons $x_1, \dots, x_m$ des représentants des classes à gauche ${}^{G}/_{Z(G)}$. Nous posons $v_1, \dots, v_k$ des éléments de $Z(G)$ d'ordres $\Omega_1, \dots, \Omega_k$, donnés par la structure des groupes abéliens de type fini, i.e. tels que les inclusions induisent un isomorphisme

$$\prod_i \langle v_i \rangle \xrightarrow[\sim]{} Z(G).$$

Nous posons également $y_{i,j} \in Z(G)$ tels que $x_i x_j = x_{l(i,j)} y_{i,j}$ et $Y(G,x) = \langle y_{i,j} \,|\, 1 \leq i,j \leq m \rangle$.

Nous posons w_i un élément engendrant un groupe cyclique d'ordre $\Omega_i m$ et définissons

$$G^* = (G \times \prod \langle w_i \rangle)/_{w_i^m = v_i}.$$

4. Démontrer que les automorphismes de $Z(G)$ qui fixent $Y(G,x)$ se relèvent des automorphismes distincts de G.
5. Démontrer que $Z(G*) = \langle w_i \rangle$ et que la famille (x_i) est encore une famille de représentants de ${}^{G^*}/_{Z(G^*)}$.
6. Nous posons $x_i^* = x_i \times \prod_j y_{i,j}^{-1/m}$ où la puissance ${}^1/_m$-ième dénote le choix d'une racine m-ième. Démontrer que les x_i^* forment encore une famille de représentants et que $Y(G^*, x^*)$ obtenu est d'exposant m.
7. Soit $1 \leq i \leq k$ et un entier s tel que $\operatorname{pgcd}(1 + sm, \Omega_i) = 1$. Démontrer que l'automorphisme $\alpha(s,i)$ de $Z(G^*)$ défini par $\alpha(s,i)(w_i) = w_i^{1+sm}$ et $\alpha(s,i)(w_j) = w_j$ si $j \neq i$ se relève en un automorphisme de G^* qui laisse stable G.
8. En examinant quelles restrictions des $\alpha(s,i)$ à G coïncident, démontrer que les Ω_i sont bornés par une constante de dépendant que de N.

Nous savons pour l'instant que les groupes cycliques dans la décomposition de $Z(G)$ sont petits. Il pourrait cependant y en avoir beaucoup. Il nous reste simplement à démontrer que la p-composante Z_p de $Z(G)$ est de cardinal borné par une constante ne dépendant que de N. Nous rappelons que le théorème de strcuture des groupes abéliens de type fini démontre en particulier que les inclusions induisent un isomorphisme

$$\prod_p Z_p \cong Z(G).$$

Nous notons Y_p la projection de $Y(G,x)$ sur Z_p.

1. Rappeler pourquoi les de Z_p laissant fixes Y_p se prolongent en automorphismes distincts de G.
2. Démontrer que si A est un p-groupe abélien avec un système de générateurs minimal à r éléments et que B en est un sous-groupe à $r' < r$ générateurs, il existe $(a_1, \dots, a_r)$ engendrant A tels que $B \subseteq \langle a_1, \dots, a_{r-1}, a_r^p \rangle$.
3. Démontrer que Z_p possède moins de m^2 générateurs et conclure que si $p^{n_p - 1} > N$, alors Z_p doit avoir moins de $\max(n_p, m^2)$ générateurs.
4. Conclure.

Exercice 11. Construction d'un morphisme singulier

Soit G le groupe abélien

$$G := \prod_{p \geq 3 \text{ premier}} \mathbb{Z}/p\mathbb{Z}$$

et pour tout entier N, on note G_N le même produit sur $\{p \text{ premier} \,|\, p \geq 3,\ p \nmid N\}$.

1. Montrer que tous les ${}^{G_N}/_{G_{N,\mathrm{tors}}}$ sont isomorphes à $\widetilde{G} := {}^{G}/_{G_{\mathrm{tors}}}$.
2. En déduire que $\widetilde{G}$ est uniquement divisible. Démontrer qu'un groupe uniquement divisible peut être muni d'une structure de $\mathbb{Q}$-espace vectoriel en décrétant que ${}^{a}/_{b} \cdot g$ est l'unique racine b-ième de ag.
3. En déduire un morphisme surjectif de G vers $\mathbb{Q}$.
4. En utilisant l'exercice 7 du TD 3, en déduire un morphisme surjectif de G vers $\mathbb{U}_{2^\infty}$ le groupe des racines de l'unité d'ordre une puissance de 2 dans $\mathbb{C}$.

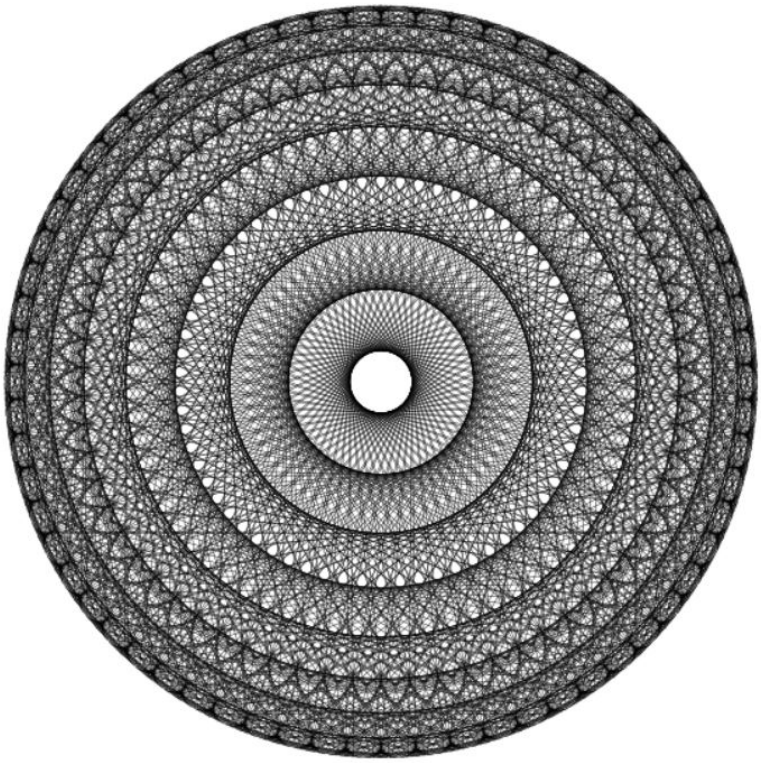


FIGURE 1 – Puissance 67e appliquée aux racines 1254-ièmes.