TD n°4 : Quotients et groupes usuels

13 et 17/10/2023

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 $(\mathbb{Z}/392\mathbb{Z})^\times$.

Correction de l'exercice 1 :

1. Cela correspond aux suites d'entiers se divisant mutuellement, de produit 8 (resp. 500). Nous listons en commençant par le plus grand facteur invariant possible. La liste des groupes abéliens d'ordre 8 à isomorphisme près est donc

$$\mathbb{Z}/8\mathbb{Z}$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
$$(\mathbb{Z}/2\mathbb{Z})^3$$

De même, la liste des groupes abéliens d'ordre 500 à isomorphisme près est

$$\mathbb{Z}/500\mathbb{Z}$$
$$\mathbb{Z}/250\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
$$\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$\mathbb{Z}/50\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$$
$$\mathbb{Z}/20\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$$
$$(\mathbb{Z}/10\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z}$$

Remarque : avec l'exercice 2, nous pouvons réécrire cette liste en distinguant les parties 2-primaires et 5-primaires, ce qui classe les groupes par leurs diviseurs élémentaires.

$$\mathbb{Z}/125\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$
$$\mathbb{Z}/125\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$$
$$\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$
$$\mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$$
$$(\mathbb{Z}/5\mathbb{Z})^3 \times \mathbb{Z}/4\mathbb{Z}$$
$$(\mathbb{Z}/5\mathbb{Z}))^3 \times (\mathbb{Z}/2\mathbb{Z})^2$$

2. Décomposons en facteurs premiers $392 = 7^2 \times 2^3$. Nous utilisons l'exercice 17 du TD n°2 pour écrire

$$(\mathbb{Z}/392\mathbb{Z})^\times \cong (\mathbb{Z}/49\mathbb{Z})^\times \times (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/42\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2.$$

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.

Correction de l'exercice 2 :

1. L'existence est un conséquence du théorème de structure des groupes abéliens finis, version facteurs invariants, et du théorème des restes chinois. Explicitement, soient $a_1|\dots|a_n$ les facteurs invariants de G. Nous écrivons pour chaque entier i :
$$a_i = \prod_{p\in\mathbb{P}} p^{k_{p,i}}.$$
En posant $n_{p,k} = |\{i \,|\, k_{p,i} = k\}|$, nous obtenons
$$\begin{aligned} G &\cong \prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z} \\ &\cong \prod_{i=1}^{n}\prod_{p\in\mathbb{P}} \mathbb{Z}/p^{k_{p,i}}\mathbb{Z} \\ &\cong \prod_{p\in\mathbb{P},\,k\geq 1} \left(\mathbb{Z}/p^k\mathbb{Z}\right)^{n_{p,k}} \end{aligned}$$
Pour l'unicité, nous proposons deux méthodes. La première consiste à recomposer les facteurs invariants à partir d'une décomposition par les $(n_{p,k})$. Pour garantir la divisibilité, nous recomposons par lemme chinois les plus gros facteurs pour chaque premier, puis les plus gros restants, etc. Formalisons. Pour tout entier p, nous construisons une suite $k_{p,1} \geq k_{p,2} \geq \dots$ d'entiers décroissante qui contienne exactement $n_{p,k}$ fois l'entiers k. Prenons n maximal tel que l'un des $k_{p,n}$ est non nul puis $a_i = \prod_{p\in\mathbb{P}} p^{k_{p,n-i+1}}$. Puisque chaque suite $(k_{p,j})_{j\geq 1}$ est croissante, les a_i se divisent les uns les autres. Nous obtenons
$$\begin{aligned} G &\cong \prod_{p\in\mathbb{P},\,k\geq 1} \left(\mathbb{Z}/p^k\mathbb{Z}\right)^{n_{p,k}} \\ &\cong \prod_{j\geq 1}\prod_{p\in\mathbb{P}} \mathbb{Z}/p^{k_{p,j}}\mathbb{Z} \\ &\cong \prod_{j\geq 1} \mathbb{Z}/a_i\mathbb{Z} \end{aligned}$$
et on identifie donc chaque $k_{p,j}$ par unicité des facteurs invariants de G.

Une autre méthode consisterait à constater que pour $G_{\underline{n}}$ associé à $(n_{p,k})$, nous avons l'égalité
$$\begin{aligned} G[q^j] &= \prod_{p\in\mathbb{P},\,k\geq 1} \left(\left(\mathbb{Z}/p^k\mathbb{Z}\right)[q^j]\right)^{n_{k,p}} \\ &\cong \left[\prod_{k<j} \left(\mathbb{Z}/q^k\mathbb{Z}\right)^{n_{q,k}}\right] \times \left[\prod_{k\geq j} \left(q^{k-j}\mathbb{Z}/q^k\mathbb{Z}\right)^{n_{q,k}}\right] \end{aligned}$$

Il en découle que

$$|G[q^j]| = \left(\prod_{k<j} n_{q,k}q^k\right)(\sum_{k\geq j} n_{q,k})q^j$$

ce qui permet d'identifier les $n_{q,k}$ comme invariants de la classe d'isomorphisme de G, par récurrence sur k.

Les p^k comptés avec multiplicité $n_{k,p}$ s'appellent diviseurs élémentaires de G.

2. Pour tout premier p, soit p^{v_p} la puissance de p qui apparaît dans la décomposition en facteurs premiers de $|G|$. La première question démontre qu'il existe un sous-groupe de G d'ordre p^{v_p}. En décomposant également d en facteurs premiers, on peut se ramener au cas où $G \cong \prod_{k\geq 1} (\mathbb{Z}/p^k\mathbb{Z})^{n_{p,k}}$ et où $d = p^v$ avec $v \leq \sum_k kn_{p,k}$. Nous prenons des facteurs tant que le cardinal du produit reste inférieur à p^v ce qui nous ramène à démontrer le résultat pour le diviseur élémentaire suivant. Explicitement, considérons le couple (K, N) minimal pour l'ordre lexicographique tel que $N \leq n_{p,K}$ et que $\sum_{k<K} kn_{p,k} + KN \leq v$. En faisant ceci, on se ramène à prouver que le facteurs suivant, isomorphe à $\mathbb{Z}/p^K\mathbb{Z}$ ou $\mathbb{Z}/p^{K+1}\mathbb{Z}$, contient un sous-groupe d'ordre $p^{v-\sum_{k<K} kn_{p,k}-KN}$ où la puissance est inférieure à K ou $K+1$. Autrement dit, on s'est ramené au cas où $G \cong \mathbb{Z}/p^k\mathbb{Z}$ auquel cas le résultat est évident.

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.

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

Correction de l'exercice 5 :

1. FAUX. Prenons la famille $(2, 3)$ dans $\mathbb{Z}$. Nous avons effectivement $\langle 2, 3\rangle = 2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$ sans que 2 ni 3 n'engendre $\mathbb{Z}$. Le même exemple fonctionne même dans le groupe fin $\mathbb{Z}/6\mathbb{Z}$.
2. FAUX. La même famille dans $\mathbb{Z}$ n'est pas libre puisque $3 * 2 - 2 * 3 = 0$.
3. VRAI. Si G est sans torsion, abélien et de type fini, le théorème de structure des groupes abéliens de type fini affirme que G est isomorphe à $\mathbb{Z}^n$ pour un certain n. Les éléments correspondants à la base canonique de $\mathbb{Z}^n$ fournissent une famille génératrice et libre.
4. FAUX. Regardons la famille (2) dans $\mathbb{Z}$. Elle est libre, maximale puisque pour tout entier n, la relation $n * 2 - 2 * n = 0$ fournit une relation de liaison sur $(2, n)$. C'est encore moins vrai dans un groupe fini non trivial, où une famille libre est vide.
5. FAUX. Toujours dans $\mathbb{Z}$, soit $(p_1, \ldots, p_n)$ les premiers nombres premiers. La famille $(\prod_{j\neq i} p_j)_i$ est génératrice puisque ses éléments sont globalement premiers entre eux. Mais dès que nous enlevons le i-ième terme, le sous-groupe engendré est contenu dans $p_i\mathbb{Z}$. Ceci exhibe des familles génératrices minimales de tout cardinal.
6. VRAI. Une famille libre de cardinal n équivaut à une injection de groupes $\mathbb{Z}^n \hookrightarrow G$. Puisque son image intersecte trivialement la partie de torsion de G, nous en déduisons une injection

$$\mathbb{Z}^n \hookrightarrow G/G_{\text{tors}} \cong \mathbb{Z}^r$$

pour un certain entier r ne dépendant que de G. Nous pouvons ensuite utiliser la dernière question de l'exercice 4 du présent TD pour conclure que $n \geq r$. Un argument plus simple est possible : injectons $\mathbb{Z}^r$ dans $\mathbb{Q}^n$. Une relation sur $\mathbb{Q}$ entre les images de la base canonique de $\mathbb{Z}^n$ fournit, quitte à la multiplier par un entier assez grand, une relation sur la base canonique. Par contraposée, la base canonique de $\mathbb{Z}^n$ est envoyée sur une famille $\mathbb{Q}$-libre ; elle est de cardinal inférieur à r.

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 [1] et $f : H \to D$ un morphisme de groupes.

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 en retrouver que pour tout groupe abélien fini G, nous avons

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

Correction de l'exercice 7 :

1. Le groupe G étant possiblement énorme, nous nous trouvons typiquement dans le cas où le lemme de Zorn sera utile et il faut considérer le bon ensemble de "constructions à faire grossir". Posons

$$\mathcal{E} = \big\{(K, j) \,|\, H \leq K \leq G,\ j : K \to D \text{ tel que } j_{|H} = f\big\}$$

muni de l'ordre tel que $(K, j) \leq (K', j')$ si $K \subseteq K'$ et $j'_{|K} = j$. Il est non vide puisqu'il contient (H, f). Toute chaîne admet un majorant en considérant l'union des sous-groupes et le morphisme vers D correctement défini par la famille des morphismes. Soit (K, j) un élément tel que K est sous-groupe strict de G et soit $g \in G\backslash K$. L'idée est de prolonger j à g en tenant compte des puissances de g qui tombent dans K. L'ensemble $\{n \in \mathbb{Z} \,|\, ng \in K\}$ est un sous-groupe de $\mathbb{Z}$; il s'écrit donc $m\mathbb{Z}$. Soit d tel que $md = j(mg)$. Montrons que $j'(ng + k) = nd + j(k)$ est correctement définie sur $\langle g, K\rangle$. Si $n_1 g + k_1 = n_2 g + k_2$ alors $(n_2 - n_1)g = k_1 - k_2 \in K$. Nous écrivons alors $n_2 = n_1 + ml$ et il en découle

$$\begin{aligned} n_2 d + j(k_2) &= n_1 d + mld + j(k_2) \\ &= n_1 d + lj(mg) + j(k_2) \\ &= n_1 d + j(lmg + k_2) \\ &= n_1 d + j(k_1) \end{aligned}$$

Le couple $(\langle g, K\rangle, j')$ prouve alors que (H, j) n'est pas maximal. Puisque le lemme de Zorn affirme que $\mathcal{E}$ possède un élément maximal, ce doit être une extension à G.

2. Utiliser la première question avec $H = \langle g\rangle$ et n'importe quel isomorphisme avec les racines $\mathrm{ord}(g)$-ièmes de l'unité

$$\langle g\rangle \cong \mathbb{Z}/\mathrm{ord} g \cong \mathbb{U}_{\mathrm{ord}(g)} \hookrightarrow \mathbb{U}.$$

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