École Normale Supérieure, Année 2021-2022

1$^{\text{e}}$ année, Algèbre 1

TD n° 4 : Groupes abéliens

`À faire en priorité : 1.1-3 ; 2.1 ; 4 ; 5.1 ; 7 ; 8.1`

La fin de la feuille comprend quelques définitions qui sont en italiques dans le texte.

0.1 Groupes abéliens finis

Exercice 1. Échauffements

Les questions sont indépendantes.

1. Montrer que les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ et $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ sont isomorphes.
2. Faire la liste des groupes abéliens de cardinal 360.
3. Déterminer tous les sous-groupes de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
4. Déterminer, à isomorphisme près, tous les groupes abéliens G possédant un sous-groupe H tel que $H \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong G/H$.

Exercice 2.

Soit G un groupe abélien.

1. Soient $m, n \in \mathbb{Z}$ premiers entre eux. Montrer $G[mn] = G[n] \oplus G[m]$.
2. Supposons G fini. Montrer que si G n'est pas cyclique, il existe un nombre premier p tel que G contienne un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
3. Calculer $\mathrm{g}(n)$, le nombre de groupe abéliens non-isomorphes d'ordre $n \in \mathbb{N}$. On pourra commencer par montrer $\forall n, m \in \mathbb{N}$, $(n, m) = 1 \implies \mathrm{g}(nm) = \mathrm{g}(n)\mathrm{g}(m)$ puis obtenir pour p premier $\mathrm{g}(p^k) = \mathrm{p}(k)$, le *nombre de partitions* de l'entier k.

Exercice 3. Cercle modulo p

Soit p un nombre premier $\neq 2$, soit $C = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid x^2 + y^2 = 1\}$. Montrer $\mathrm{J}(\chi, \chi^{-1}) = -\chi(-1)$ pour tout $\chi \in \widehat{(\mathbb{Z}/p\mathbb{Z})^\times}$ tel que $\chi \neq 1$. En déduire $|C| = p - (-1)^{\frac{p-1}{2}}$.

Exercice 4.

Soit G un groupe abélien fini. Soit $d \mid |G|$, montrer que G contient un sous-groupe d'ordre d.

0.2 Groupes abéliens non nécessairement finis

Exercice 5.

1. Soit G un groupe tel que $g^2 = 1$ pour tout $g \in G$. Montrer que G est abélien, puis $G \cong (\mathbb{Z}/2\mathbb{Z})^{(I)}$ pour un certain ensemble I.
2. Montrer que le sous-ensemble des *matrices unipotentes* $\mathrm{U}_n(k)$ est un sous-groupe de $\mathrm{GL}_n(k)$ pour $n \geqslant 1$ et k un corps.
3. Soit p un nombre premier. On suppose $p \geq n$. Montrer $g^p = 1$ pour tout $g \in \mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$.
4. En déduire que pour $p > 3$ premier, il existe un groupe non abélien G d'ordre p^3 tel que $g^p = 1$ pour tout $g \in G$.

Exercice 6.

1. Montrer que si G_1 et G_2 sont deux groupes, on a un isomorphisme naturel $\widehat{G_1 \times G_2} \xrightarrow{\sim} \widehat{G_1} \times \widehat{G_2}$.
2. En déduire que si G est un groupe abélien fini, alors $\widehat{G}$ est isomorphe à G.

Exercice 7. Exemples de groupes divisibles

1. Montrer que $\mathbb{Q}$ est un groupe injectif. De même, Justifier que $\mathbb{Q}/\mathbb{Z}$ est injectif mais de torsion.
2. Montrer que pour les *p-groupes de Prüfer* on a un isomorphisme $\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z} \cong \mu_{p^\infty}$.
3. Montrer la décomposition $\mathbb{Q}/\mathbb{Z} \cong \bigoplus_{p\in\mathcal{P}} \mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z}$. Conclure que $\mathbb{Q}/\mathbb{Z} \cong \mathbb{U}(1)_{\mathrm{tors}}$.
4. Montrer que tout groupe abélien fini se *plonge* dans une somme de $\mathbb{Q}/\mathbb{Z}$.

Exercice 8. Objets injectifs et groupes divisibles

Soit G un groupe abélien.

1. Montrer qu'un groupe abélien est *injectif* si, et seulement s'il est *divisible*.
2. Montrer que tout groupe abélien se plonge dans un groupe injectif.
3. Montrer que tout groupe abélien divisible est somme directe de copies de $\mathbb{Q}$ et de *p-groupes de Prüfer*. En déduire le théorème de classification des groupes abéliens de type finis.

Exercice 9. Le groupe des entiers p-adiques

Soit p un nombre premier. On note $\mathbb{Z}_p$ le sous-ensemble du produit $\prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ défini par

$$\mathbb{Z}_p \coloneqq \{(x_n)_{n\geqslant 1} \mid \forall n \in \mathbb{N}^*,\ x_{n+1} \equiv x_n \bmod p^n\},$$

Une suite de $\mathbb{Z}_p$ est appelée un *entier p-adique*.

1. Montrer que $\mathbb{Z}_p \subset \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$ est un sous-groupe puis que l'application $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ définie par $(x_n)_{n\geqslant 1} \mapsto x_n$, est un morphisme surjectif.
2. Montrer que $\mathbb{Z}_p$ est en bijection avec $\mathbb{R}$.
3. Montrer que $\mathbb{Z}_p$ n'a aucun élément non trivial d'ordre fini.
4. Montrer que pour tout caractère $\chi \in \widehat{\mu_{p^\infty}}$ il existe un unique entier p-adique $(\overline{k_n}) \in \mathbb{Z}_p$ vérifiant $\chi(e^{2i\pi/p^n}) = e^{2i\pi k_n/p^n}$ pour tout $n \geq 1$.
5. Montrer $\widehat{\mu_{p^\infty}} \simeq \mathbb{Z}_p$.

0.3 Notations et définitions pour les exercices

- On note $\mathcal{P}$ l'ensemble des nombres premiers, supposés positifs.
- On dit qu'un groupe H *se plonge* dans un groupe G s'il admet un morphisme injectif.
- On rappel que pour G un groupe abélien, $m \in \mathbb{Z}$, on note $G[m] = \{x \in G \mid m \cdot x = 0\}$ les éléments de m-torsion. De plus, G sera dit *de torsion* si tout élément est de torsion
- On notera $\mathrm{p}(k)$ le nombre de partitions d'un entier k.
- On dit qu'un groupe abélien G est *divisible* si pour tout $x \in G$ et $n \in \mathbb{N}^*$ il existe $y \in G$ tel que $ny = x$.
- On dit qu'un groupe abélien G est *injectif* si pour tout morphisme injectif de groupes abéliens $\iota\colon X \hookrightarrow Y$, tout morphisme $\psi\colon X \to G$ s'étend en un morphisme $\tilde{\psi}\colon Y \to G$ (i.e. tel que $\tilde{\psi} \circ \iota = \psi$).
- Si k est un corps et $n \geq 1$ est un entier, on note $\mathrm{U}_n(k)$ le sous-ensemble de $\mathrm{M}_n(k)$ des *unipotentes*, constitué des matrices de la forme $\mathrm{I}_n + N$ avec $N_{ij} = 0$ pour $i \geq j$ (autrement dit, N est triangulaire supérieure nilpotente).
- On note $\mu_{p^\infty} \coloneqq \bigcup_{n\geq 1} \mu_{p^n}$ le sous-groupe du cercle unité $\mathbb{U}(1) \subset \mathbb{C}^\times$ constitué des racines de l'unité d'ordre une puissance de p.
- Le *p-groupe de Prüfer* est le sous-groupe de $\mathbb{Q}/\mathbb{Z}$, *le cercle rationnel*, de la forme

$$\mathbb{Z}\left[\frac{1}{p}\right]/\mathbb{Z} \coloneqq \left\{\frac{a}{p^n} \in \mathbb{Q}/\mathbb{Z}\ ;\ n \in \mathbb{N},\ a \in \mathbb{Z}\right\}.$$