UNIVERSITÉ DE LORRAINE

L3 Mathématiques – Site Nancy, S5 – 2025-2026

Algèbre 2 – Feuille 3

Groupes abéliens finis

Exercice 1. Déterminer les générateurs du groupe additif $\mathbb{Z}/12\mathbb{Z}$ et ceux du groupe multiplicatif $\mathbb{U}_{18}$.

Exercice 2. Déterminer les éléments d'ordre 6 et ceux d'ordre 5 dans le groupe $\mathbb{U}_{30}$.

Exercice 3. Déterminer les sous-groupes de $\mathbb{Z}/20\mathbb{Z}$ et les sous-groupes de $\mathbb{U}_{12}$.

Exercice 4. Soient G un groupe fini, K et M deux sous-groupes de G d'ordres k et m. Montrer que si, k et m sont premiers entre eux, alors $K \cap M = \{e\}$.

Exercice 5. Soit G un groupe fini d'ordre $2n$, d'élément neutre e. On suppose qu'il existe deux sous-groupes distincts H, H' de G d'ordre n, tels que $H \cap H' = \{e\}$. Montrer que $n = 2$ et dresser la table de G.

Exercice 6. Soit G un goupe d'ordre $2p$, avec $p > 2$ premier. Montrer qu'il existe dans G des sous-groupes H et K d'ordres p et 2 et que l'on a $G = HK$, H distingué dans G et $H \cap K = \{e\}$.

Exercice 7. Soit $f : G \to G'$ un morphisme de groupes. Montrer que si $x \in G$ est d'ordre fini divisant un entier n, alors $f(x)$ est d'ordre fini et son ordre divise n.
Application : trouver tous les morphismes de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}$ et dans $\mathbb{Z}/7\mathbb{Z}$.

Exercice 8. Soient G et G' deux groupes cycliques d'ordres n et m. Combien existe-t-il de morphismes de G dans G' ?
Donner l'expression de tous les morphismes de $\mathbb{Z}/21\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$, de $\mathbb{Z}/18\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.

Exercice 9. Montrer que le groupe $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ est cyclique. Expliciter ses éléments et donner ses générateurs.

Exercice 10. Soient G un groupe fini et H un sous-groupe distingué de G.

(a) Soit K un sous-groupe de G tel que $[G : H]$ et $|K|$ soient premiers entre eux. Montrer que $K \subset H$.

(b) Si $[G : H]$ et $|H|$ sont premiers entre eux, montrer que le seul sous-groupe de G d'ordre m est H.

Exercice 11. Soit G un groupe d'ordre pq où p et q ont deux nombres premiers distincts. On veut montrer que G possède au moins un élément d'ordre p et au moins un élément d'ordre q sans utiliser le théorème de Cauchy. Pour cela on suppose que G ne possède aucun éléments d'ordre q.

(a) Montrer que tout élément de $G \setminus \{e\}$ est d'ordre p.

(b) Soit $x \in G \setminus \{e\}$ et soit $H = \langle x \rangle$.

(1) Montrer que si H est distingué dans G, alors le quotient G/H est cyclique d'ordre q ; soit alors $y \in G$ tel que $G/H = \langle \bar{y} \rangle$. En raisonnant sur $o(y)$ et $o(\bar{y})$ trouver une contradictions et en déduire que H n'est pas distingué dans G.

(2) Montrer que $N_G(H) = H$.

(3) Montrer que H possède exactement q conjugués aHa^{-1} quand a décrit G ; en déduire que la réunion R des conjugués de H a $1 + q(p-1)$ éléments.

(4) Montrer que $R \neq G$. On peut donc choisir $y \in G \setminus R$.

(5) Soit $K = \langle y \rangle$ et soit S la réunion des conjugués de K. Montrer que S a $1 + q(p-1)$ éléments.

(6) Montrer que $S \cap R = \{e\}$. En déduire que $\mathrm{card}(S \cup R) = 1 + 2q(p-1)$.

(7) Conclure.

Exercice 12. Pour tout entier $n \geq 2$, on note $\varphi(n)$ le cardinal de l'ensemble des entiers tels que $0 \leq k \leq n-1$ et $k \wedge n = 1$. On convient que $\varphi(1) = 1$. La fonction φ de $\mathbb{N}^*$ dans $\mathbb{N}^*$ ainsi définie est appelée la fonction d'Euler. L'entier $\varphi(n)$ est aussi le nombre de générateurs de tout groupe cyclique d'ordre n.

(a) Déterminer $\varphi(2), \varphi(3), \varphi(4)$ et $\varphi(5)$.

(b) Montrer que $\varphi(p) = p - 1$ si et seulement si p est premier.

(c) Soit $n \in \mathbb{N}^*$. Montrer que $n = \sum_{d|n} \varphi(d)$.

(d) Soient $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$. Montrer que $\varphi(mn) = \varphi(m)\varphi(n)$.

(e) Montrer que si la décomposition en facteurs premiers de $n \geq 2$ est $n = p_1^{s_1} \cdots p_k^{s_k}$, alors $\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$.

(f) En déduire que pour tout $m, n \in \mathbb{N}^*$, $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$, où $d = \text{pgcd}(m, n)$.

(g) Soit $n \geq 3$. Montrer que $\varphi(n)$ est pair.

(h) Montrer que $\varphi(2n) = \varphi(n)$ si n est impair et que $\varphi(2n) = 2\varphi(n)$ si n est pair.

Exercice 13. Pour les groupes suivants, déterminer la décomposition primaire et la décomposition cyclique :

(a) $G = (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/90\mathbb{Z})$.

(b) $G = (\mathbb{Z}/84\mathbb{Z}) \times (\mathbb{Z}/90\mathbb{Z})$.

(c) $G = (\mathbb{Z}/40\mathbb{Z}) \times (\mathbb{Z}/42\mathbb{Z}) \times (\mathbb{Z}/120\mathbb{Z})$.

Exercice 14. Donner la décomposition primaire du groupe abélien $\mathbb{Z}/851\mathbb{Z}$. En déduire la structure du groupe $Aut(\mathbb{Z}/851\mathbb{Z})$.

Exercice 15. Déterminer, à isomorphisme près, tous les groupes abéliens d'ordre :

(a) 600.

(b) 720.

(c) 3240.

Exercice 16. Parmi les groupes suivants, tous abéliens d'ordre 180, déterminer lesquels sont isomorphes entre eux :

(1) $\mathbb{Z}/180\mathbb{Z}$

(2) $(\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/15\mathbb{Z})$

(3) $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/90\mathbb{Z})$

(4) $(\mathbb{Z}/3\mathbb{Z})^2 \times (\mathbb{Z}/20\mathbb{Z})$

(5) $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/45\mathbb{Z})$

(6) $(\mathbb{Z}/15\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$

(7) $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$

(8) $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z})$

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

(10) $(\mathbb{Z}/181\mathbb{Z})^\times$

(11) $(\mathbb{Z}/19\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times$

(12) $(\mathbb{Z}/209\mathbb{Z})^\times$

Exercice 17. Montrer que dans tout groupe abélien d'ordre 40, il y a au moins un élément d'ordre 10.
Existe-t-il un groupe abélien d'ordre 40 dans lequel l'ordre de tout élément divise 10 ?

Exercice 18. (a) Soient $k \geq 2$ et $n \geq 2$ des entiers. Posons $d = \text{pgcd}(k, n)$ et $m = \text{ppcm}(k, n)$. Montrer que le groupe $G = (\mathbb{Z}/k\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ et que c'est la seule expression de G sous la forme $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ avec a divisant b (décomposition cyclique, avec (a, b) l'invariant de G).

(b) Application : déterminer la décomposition cyclique de $G = (\mathbb{Z}/18\mathbb{Z}) \times (\mathbb{Z}/45\mathbb{Z})$.