L3 Mathématiques – Site Nancy, S5 – 2021/22

Algèbre 2 – Feuille 3

Groupes finis, groupes cycliques

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. *Montrer qu'un groupe* G *est d'ordre premier si, et seulement si, il est cyclique et simple (c-à-d que* $\{e\}$ *et* G *sont les seuls sous-groupes distingués de* G*).*

Exercice 5. *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 6. *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 7. *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 8. *Soit* $f : G \to G'$ *un morphisme de groupes. Montrer que si* $x \in G$ *est d'ordre fini* 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* $\mathbb{Z}/7\mathbb{Z}$

Exercice 9. *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 10. *Montrer que le groupe* $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ *est cyclique. Expliciter ses éléments et donner ses générateurs.*

Exercice 11. *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 12. *(a) Montrer que tout grope d'ordre* p^n *où* p *est un nombre premier et* $n \in \mathbb{N}^*$*, a un centre non réduit à* $\{e\}$.

(b) Soit G *un groupe ; montrer que si* $G/Z(G)$ *est cyclique, alors* G *est abélien.*

(c) Soit p *un nombre premier et soit* G *un groupe d'ordre* p^2*. Montrer que* G *est abélien.*

Exercice 13. *Soit* p *un nombre premier et soit* G *un groupe d'ordre* p^2.

(a) Quels sont les ordres possibles des éléments de G *? Montrer que si* G *possède un élément d'ordre* p^2*, alors* $G \simeq \mathbb{Z}/p^2\mathbb{Z}$.

(b) On suppose que G *ne possède pas d'élément d'ordre* p^2.

(i) Montrer que, pour tout $x \in G \setminus \{e\}$*,* $\langle x \rangle \simeq \mathbb{Z}/p\mathbb{Z}$.

(ii) Montrer que si H *et* K *sont deux sous-groupes de* G *distincts d'ordre* p*, alors* $H \cap K = \{e\}$ *et* $HK = G$*. En déduire que* $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$.

Exercice 14. *Soi* 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 15. *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 $d = \mathrm{pgcd}(m, n)$.

(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 16. *Soit G un groupe fini d'ordre n. Soit p le plus petit nombre premier qui divise n. On suppose que H est un sous-groupe de G d'indice p. Montrer que H est distingué dans G.*