Plaquette 2 – Groupes : ordre, groupes cycliques, sous-groupes

Structures algébriques — Prépa MP / MPI (2e année)

Exercices

Méthode

L'outil central est l'**ordre** d'un élément : x est d'ordre d si et seulement si $\{k \in \mathbb{Z} \mid x^k = e\} = d\mathbb{Z}$, et alors $\langle x \rangle \simeq \mathbb{Z}/d\mathbb{Z}$. Dans un groupe fini, **Lagrange** impose que d divise le cardinal. Les **groupes cycliques** sont entièrement décrits : $\mathbb{Z}/n\mathbb{Z}$ a $\varphi(n)$ générateurs et exactement un sous-groupe de chaque ordre $d \mid n$. Pour étudier un groupe concret (permutations, isométries, racines de l'unité), on calcule les ordres de ses éléments, on cherche des générateurs, on compare avec $\mathbb{Z}/n\mathbb{Z}$.

Exercice 1 – Générateurs de Z/12Z

a) Calculer l'ordre de chaque élément de $\mathbb{Z}/12\mathbb{Z}$.

b) Quels éléments engendrent $\mathbb{Z}/12\mathbb{Z}$? Vérifier qu'il y en a $\varphi(12)$.

c) Montrer en général que $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

Exercice 2 – Sous-groupes d'un groupe cyclique

Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ et $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la projection.

a) Montrer que $\pi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$ contenant $n\mathbb{Z}$; en déduire $\pi^{-1}(H) = a\mathbb{Z}$ avec $a \mid n$, puis $H = \langle \overline{a} \rangle$.

b) En déduire que pour chaque diviseur d de n, il existe un unique sous-groupe d'ordre d.

c) Lister les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$ et dessiner leurs inclusions (diagramme de divisibilité).

Exercice 3 – La formule de Gauss pour l'indicatrice

a) Montrer que $\mathbb{Z}/n\mathbb{Z}$ contient exactement $\varphi(d)$ éléments d'ordre d pour chaque diviseur d de n (ce sont les générateurs de H_d).

b) En déduire $\sum_{d \mid n} \varphi(d) = n$.

c) Vérifier pour $n = 12$ et $n = 30$.

Exercice 4 – Ordre d'une permutation

a) Montrer que l'ordre d'un cycle de longueur ℓ est ℓ, puis que l'ordre d'un produit de cycles à supports disjoints est le ppcm des longueurs.

b) Calculer l'ordre de $\sigma = (1\,2\,3)(4\,5\,6\,7)$ dans S_7, et de σ^2.

c) Quel est l'ordre maximal d'un élément de S_7 ?

Exercice 5 – Le groupe diédral D4

Soit D_4 le groupe des isométries du plan conservant un carré centré en O : rotations r^k (r quart de tour, $0 \le k \le 3$) et réflexions s, sr, sr^2, sr^3 (s réflexion d'axe une médiane).

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

a) Vérifier que $srs = r^{-1}$ et en déduire $sr^k s = r^{-k}$.
b) Déterminer l'ordre de chaque élément.
c) D_4 est-il abélien ? cyclique ? Déterminer son centre.
d) Montrer que $\langle r \rangle$ est distingué.

Exercice 6 – Le centre de S3

a) Lister les éléments de S_3 et leurs ordres.
b) Calculer $(1\,2)(1\,3)$ et $(1\,3)(1\,2)$. Que conclure ?
c) Montrer que le centre de S_3 est réduit à l'identité.
d) Plus généralement, montrer que si $n \geq 3$, une permutation qui commute avec toutes les transpositions est l'identité.

Exercice 7 – Un élément d'ordre 2 dans un groupe d'ordre pair

Soit G un groupe fini de cardinal pair.

a) Montrer que la relation « $y = x$ ou $y = x^{-1}$ » groupe les éléments de G en paires $\{x, x^{-1}\}$ et en singletons $\{x\}$ avec $x = x^{-1}$.
b) En déduire que le nombre d'éléments vérifiant $x^2 = e$ est pair, puis qu'il existe un élément d'ordre 2.
c) Application : montrer que dans S_4 le nombre d'éléments d'ordre 2 est impair, et le calculer.

Exercice 8 – Un groupe où tout élément est d'ordre au plus 2

Soit G un groupe tel que $x^2 = e$ pour tout $x \in G$.

a) Montrer que G est abélien (calculer $(xy)^2$).
b) On suppose G fini. En le munissant de la loi externe $\overline{0} \cdot x = e$, $\overline{1} \cdot x = x$, montrer que G est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel (notation additive).
c) En déduire que $\mathrm{card} G$ est une puissance de 2, et que $G \simeq (\mathbb{Z}/2\mathbb{Z})^k$.

Exercice 9 – Sous-groupe d'indice deux

Soit H un sous-groupe d'un groupe fini G avec $\mathrm{card} G = 2\,\mathrm{card} H$.

a) Montrer que pour $g \notin H$, $gH = G \setminus H = Hg$.
b) En déduire que H est distingué ($gHg^{-1} = H$ pour tout g).
c) Application : montrer que le groupe alterné A_n (noyau de la signature) est distingué dans S_n, de deux façons.

Exercice 10 – Racines de l'unité

Soit $\mathrm{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$.

a) Montrer que $k \mapsto \mathrm{e}^{2ik\pi/n}$ induit un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur U_n.
b) Combien y a-t-il de racines **primitives** n-ièmes (générateurs) ? Les lister pour $n = 6$.
c) Montrer que tout sous-groupe fini de $\mathbb{C}^*$ de cardinal n est égal à U_n.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Exercice 11 – Les isométries du triangle équilatéral

Soit T un triangle équilatéral de sommets A_1, A_2, A_3 et D_3 le groupe des isométries du plan qui le conservent.

a) Montrer qu'une isométrie conservant T permute ses sommets, ce qui définit un morphisme $\Phi : D_3 \to S_3$.

b) Montrer que Φ est injectif (une isométrie du plan qui fixe trois points non alignés est l'identité).

c) Décrire les 6 isométries (rotations et réflexions) et conclure que $D_3 \simeq S_3$.

Exercice 12 – Image d'un groupe cyclique

Soit $f : G \to G'$ un morphisme de groupes.

a) Montrer que si $G = \langle g \rangle$ est cyclique, $f(G) = \langle f(g) \rangle$ est cyclique.

b) Montrer que $\mathrm{ord}(f(g))$ divise $\mathrm{ord}(g)$.

c) Le quotient $(\mathbb{Z}/12\mathbb{Z})/\langle \overline{4} \rangle$ est-il cyclique ? À quel groupe est-il isomorphe ?

d) Un groupe cyclique d'ordre 12 peut-il se surjecter sur un groupe d'ordre 5 ?

Exercice 13 – Sous-groupes de Z et pgcd

a) Montrer que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$, et que $d = a \wedge b$.

b) Montrer que $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

c) Application : déterminer le sous-groupe de $\mathbb{Z}$ engendré par 84 et 120, puis une relation de Bézout.

Exercice 14 – Exposant d'un groupe abélien fini

Soit G un groupe abélien fini. Son **exposant** $e(G)$ est le ppcm des ordres de ses éléments.

a) Montrer que $e(G)$ divise $\mathrm{card} G$.

b) En utilisant l'exercice sur l'ordre d'un produit, montrer que G possède un élément d'ordre $e(G)$ (traiter d'abord deux éléments d'ordres m, n quelconques, en extrayant des éléments d'ordres premiers entre eux de produit $\mathrm{ppcm}(m, n)$).

c) En déduire que G est cyclique si et seulement si $e(G) = \mathrm{card} G$. Vérifier sur $(\mathbb{Z}/8\mathbb{Z})^\times$ et $(\mathbb{Z}/9\mathbb{Z})^\times$.

Exercice 15 – Synthèse : x² = 1 modulo p et le théorème de Wilson

Soit p un nombre premier impair et $G = (\mathbb{Z}/p\mathbb{Z})^\times$.

a) Montrer que dans le corps $\mathbb{Z}/p\mathbb{Z}$, l'équation $x^2 = \overline{1}$ n'a que les solutions $\pm\overline{1}$.

b) En regroupant chaque élément de G avec son inverse, montrer que le produit de tous les éléments de G vaut $-\overline{1}$: $(p-1)! \equiv -1 \pmod{p}$ (Wilson).

c) Vérifier pour $p = 7$ en écrivant les paires.

d) Montrer que si $n \geq 2$ n'est pas premier, $(n-1)! \not\equiv -1 \pmod{n}$, et en déduire un critère de primalité (peu efficace).

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).