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

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

Corrections détaillées

Boîte à outils

Ordre et groupes cycliques.

— x d'ordre d : $x^k = e \Leftrightarrow d \mid k$; $\mathrm{ord}(x^k) = \frac{d}{d \wedge k}$.

— **Lagrange** : dans G fini, $\mathrm{ord}(x) \mid \mathrm{card} G$, donc $x^{\mathrm{card} G} = e$.

— Dans $\mathbb{Z}/n\mathbb{Z}$: $\mathrm{ord}(\overline{k}) = \frac{n}{n \wedge k}$; $\overline{k}$ engendre $\Leftrightarrow k \wedge n = 1$ ($\varphi(n)$ générateurs).

— Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $\langle \overline{n/d} \rangle$, un et un seul pour chaque diviseur d de n (d'ordre d), et

$$\sum_{d \mid n} \varphi(d) = n$$

— **Permutations** : l'ordre d'une permutation est le ppcm des longueurs de ses cycles.

— $\mathrm{U}_n = \{z \in \mathbb{C} \mid z^n = 1\} \simeq \mathbb{Z}/n\mathbb{Z}$, engendré par $\mathrm{e}^{2i\pi/n}$.

— Un sous-groupe d'indice 2 est distingué ; un groupe où $x^2 = e$ pour tout x est abélien.

Correction de l'exercice 1 – Générateurs de Z/12Z

a) L'ordre de $\overline{k}$ est le plus petit $d \geq 1$ tel que $12 \mid dk$, soit

$$\mathrm{ord}(\overline{k}) = \frac{12}{12 \wedge k}$$

— $\overline{0} : 1$; $\overline{6} : 2$; $\overline{4}, \overline{8} : 3$; $\overline{3}, \overline{9} : 4$; $\overline{2}, \overline{10} : 6$; $\overline{1}, \overline{5}, \overline{7}, \overline{11} : 12$.

b) Générateurs : les éléments d'ordre 12, soit $\overline{1}, \overline{5}, \overline{7}, \overline{11}$. Il y en a $4 = \varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$.

c) $\overline{k}$ engendre si et seulement si $\overline{1} \in \langle \overline{k} \rangle$, c'est-à-dire s'il existe u avec $uk \equiv 1 \pmod{n}$: il existe u, v entiers tels que $uk + vn = 1$, ce qui équivaut à $k \wedge n = 1$ (Bézout).

Réponse. Ordres $\frac{12}{12 \wedge k}$; générateurs $\overline{1}, \overline{5}, \overline{7}, \overline{11}$; $\overline{k}$ générateur ssi $k \wedge n = 1$.

Correction de l'exercice 2 – Sous-groupes d'un groupe cyclique

a) Image réciproque d'un sous-groupe par un morphisme : c'est un sous-groupe de $\mathbb{Z}$, donc de la forme $a\mathbb{Z}$ ($a \geq 0$). Il contient $\pi^{-1}(\{\overline{0}\}) = n\mathbb{Z}$, donc $a \mid n$ (et $a \geq 1$). Comme π est surjective, $H = \pi(a\mathbb{Z}) = \langle \overline{a} \rangle$.

b) $\langle \overline{a} \rangle$ (avec $a \mid n$) a pour ordre $\frac{n}{a}$. Pour $d \mid n$, le seul sous-groupe d'ordre d est donc

$$H_d = \left\langle \overline{n/d} \right\rangle$$

c) Diviseurs de 12 : $1, 2, 3, 4, 6, 12$. Sous-groupes : $\{\overline{0}\}$, $\langle \overline{6} \rangle$, $\langle \overline{4} \rangle$, $\langle \overline{3} \rangle$, $\langle \overline{2} \rangle$, $\mathbb{Z}/12\mathbb{Z}$. $H_d \subset H_{d'}$ si et seulement si $d \mid d'$: par exemple $\langle \overline{6} \rangle \subset \langle \overline{3} \rangle \cap \langle \overline{2} \rangle$, et $\langle \overline{4} \rangle \subset \langle \overline{2} \rangle$.

Réponse. Un sous-groupe par diviseur : $H_d = \langle \overline{n/d} \rangle$; pour 12 : 6 sous-groupes.

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).

Correction de l'exercice 3 – La formule de Gauss pour l'indicatrice

a) Un élément d'ordre d engendre un sous-groupe d'ordre d, nécessairement H_d (unicité). Les éléments d'ordre d sont donc les générateurs de $H_d \simeq \mathbb{Z}/d\mathbb{Z}$: il y en a $\varphi(d)$.

b) On partitionne $\mathbb{Z}/n\mathbb{Z}$ selon l'ordre des éléments, qui divise n (Lagrange) :

$$n = \sum_{d \mid n} \operatorname{card}\{x \mid \operatorname{ord}(x) = d\} = \sum_{d \mid n} \varphi(d)$$

c) $n = 12$: $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$. $n = 30$: diviseurs $1, 2, 3, 5, 6, 10, 15, 30$, valeurs $1, 1, 2, 4, 2, 4, 8, 8$, somme 30.

Réponse. $\varphi(d)$ éléments d'ordre d ; $\sum_{d \mid n} \varphi(d) = n$.

Correction de l'exercice 4 – Ordre d'une permutation

a) Un ℓ-cycle c envoie chaque élément de son support sur le suivant ; c^k le déplace de k crans : $c^k = \mathrm{id} \Leftrightarrow \ell \mid k$. Des cycles à supports disjoints commutent, donc $(c_1 \cdots c_r)^k = c_1^k \cdots c_r^k$, qui vaut id si et seulement si chaque $c_i^k = \mathrm{id}$ (supports disjoints), c'est-à-dire $\ell_i \mid k$ pour tout i :

$$\operatorname{ord}(\sigma) = \operatorname{ppcm}(\ell_1, \ldots, \ell_r)$$

b) $\operatorname{ord}(\sigma) = \operatorname{ppcm}(3, 4) = 12$, et $\operatorname{ord}(\sigma^2) = \frac{12}{12 \wedge 2} = 6$ (en effet $\sigma^2 = (1\,3\,2)(4\,6)(5\,7)$, de ppcm $\operatorname{ppcm}(3, 2, 2) = 6$).

c) On maximise ppcm des parts d'une partition de 7 : $7 \to 7$, $6 + 1 \to 6$, $5 + 2 \to 10$, $4 + 3 \to 12$, $3 + 2 + 2 \to 6$, $4 + 2 + 1 \to 4$, et les autres types donnent moins Le maximum est 12, atteint par le type $(4, 3)$.

Réponse. Ordre = ppcm des longueurs ; $\operatorname{ord}(\sigma) = 12$, $\operatorname{ord}(\sigma^2) = 6$; maximum 12 dans S_7.

Correction de l'exercice 5 – Le groupe diédral D4

a) Dans un repère orthonormé centré en O dont l'axe des abscisses est l'axe de s : $s = \operatorname{diag}(1, -1)$, $r = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, et $srs = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = r^{-1}$. Par récurrence, $sr^k s = (srs)^k = r^{-k}$ (car $s^2 = \mathrm{id}$).

b) id : 1 ; r, r^3 : 4 ; r^2 : 2 ; les 4 réflexions : 2.

c) Non abélien : $sr = r^{-1}s \neq rs$. Non cyclique : aucun élément d'ordre 8. Centre : r^2 commute avec tout ($sr^2 = r^{-2}s = r^2 s$), et c'est le seul élément non trivial : r ne commute pas avec s, une réflexion sr^k ne commute pas avec r.

$$Z(D_4) = \{\mathrm{id}, r^2\}$$

d) $\langle r \rangle$ est d'indice 2 dans D_4 (cardinal 4 sur 8) : ses deux classes à gauche et à droite sont $\langle r \rangle$ et son complémentaire, donc $g\langle r \rangle = \langle r \rangle g$ pour tout g.

Réponse. $sr^k s = r^{-k}$; ordres $1, 4, 2, 4$ et 2 (réflexions) ; non abélien, non cyclique ; $Z = \{\mathrm{id}, r^2\}$.

Correction de l'exercice 6 – Le centre de S3

a) id (ordre 1), trois transpositions $(1\,2), (1\,3), (2\,3)$ (ordre 2), deux 3-cycles $(1\,2\,3), (1\,3\,2)$ (ordre 3).

b) $(1\,2)(1\,3)$: $1 \mapsto 3$, $3 \mapsto 1 \mapsto 2$, $2 \mapsto 1$: c'est $(1\,3\,2)$. $(1\,3)(1\,2) = (1\,2\,3)$. Les deux produits diffèrent : S_3 n'est pas abélien.

c) Une transposition ne commute pas avec une autre transposition (b), un 3-cycle ne

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).

commute pas avec une transposition (par exemple $(1\,2\,3)(1\,2) = (1\,3)$ et $(1\,2)(1\,2\,3) = (2\,3)$). Seule l'identité commute avec tout.

d) Si σ commute avec $\tau = (a\,b)$, alors $\sigma\tau\sigma^{-1} = (\sigma(a)\,\sigma(b)) = (a\,b)$, donc σ stabilise $\{a, b\}$. Pour a fixé et deux autres éléments $b \neq c$ (possible si $n \geq 3$), $\sigma(a) \in \{a, b\} \cap \{a, c\} = \{a\}$: $\sigma(a) = a$ pour tout a.

Réponse. S_3 non abélien ($(1\,2)(1\,3) = (1\,3\,2)$) ; centre trivial ; pour $n \geq 3$, $Z(S_n) = \{\mathrm{id}\}$.

Correction de l'exercice 7 – Un élément d'ordre 2 dans un groupe d'ordre pair

a) $x \mapsto x^{-1}$ est une involution de G ; ses orbites ont 1 ou 2 éléments, les orbites à un élément étant les x tels que $x = x^{-1}$, soit $x^2 = e$.

b) Les paires contribuent pour un nombre pair d'éléments ; comme $\mathrm{card} G$ est pair, le nombre N de solutions de $x^2 = e$ est pair. e en fait partie, donc $N \geq 2$: il existe $x \neq e$ avec $x^2 = e$, d'ordre 2.

c) Les solutions de $x^2 = e$ dans S_4 : l'identité, les $\binom{4}{2} = 6$ transpositions, les 3 doubles transpositions, soit 10 (pair). Éléments d'ordre 2 : $10 - 1 = 9$, impair.

Réponse. Involution $x \mapsto x^{-1}$; nombre pair de solutions de $x^2 = e$; 9 éléments d'ordre 2 dans S_4.

Correction de l'exercice 8 – Un groupe où tout élément est d'ordre au plus 2

a) $(xy)^2 = e$ donne $xyxy = e$, donc $yx = x^{-1}y^{-1} = xy$ (car $x^{-1} = x$ et $y^{-1} = y$).

b) En notation additive, G est un groupe abélien où $x + x = 0$. Les axiomes d'espace vectoriel sur F_2 se vérifient : seule la distributivité $(\overline{1} + \overline{1}) \cdot x = \overline{1} \cdot x + \overline{1} \cdot x$ demande quelque chose, et elle s'écrit $0 = x + x$, ce qui est vrai.

c) Un F_2-espace de dimension finie k est isomorphe à F_2^k (choix d'une base) :

$$G \simeq (\mathbb{Z}/2\mathbb{Z})^k, \qquad \mathrm{card} G = 2^k$$

— Exemple : le groupe de Klein $\{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$, de dimension 2.

Réponse. G abélien ; F_2-espace vectoriel ; $G \simeq (\mathbb{Z}/2\mathbb{Z})^k$, cardinal 2^k.

Correction de l'exercice 9 – Sous-groupe d'indice deux

a) Les classes à gauche xH partitionnent G et ont toutes le cardinal de H : il y en a 2, à savoir H et $G \setminus H$. Si $g \notin H$, $gH \neq H$ (car $g \in gH$), donc $gH = G \setminus H$. De même pour les classes à droite.

b) Si $g \in H$, $gHg^{-1} = H$. Sinon, $gH = Hg$ par a), d'où $gHg^{-1} = Hgg^{-1} = H$.

c) La signature ε est un morphisme surjectif sur $\{\pm 1\}$ (pour $n \geq 2$) : $A_n = \ker \varepsilon$ est distingué comme tout **noyau**, et d'indice 2 par le théorème d'isomorphisme ($S_n/A_n \simeq \{\pm 1\}$), ce qui redonne b). Directement : $\varepsilon(g\sigma g^{-1}) = \varepsilon(g)\varepsilon(\sigma)\varepsilon(g)^{-1} = \varepsilon(\sigma)$.

Réponse. $gH = G \setminus H = Hg$; indice 2 $\Rightarrow$ distingué ; $A_n = \ker \varepsilon$.

Correction de l'exercice 10 – Racines de l'unité

a) $\varphi(k) = \mathrm{e}^{2ik\pi/n}$ est un morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{C}^*, \times)$, d'image U_n et de noyau $n\mathbb{Z}$ ($\mathrm{e}^{2ik\pi/n} = 1 \Leftrightarrow n \mid k$). Par le théorème d'isomorphisme :

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathrm{U}_n$$

b) Générateurs : $\varphi(n)$. Pour $n = 6$: $k \in \{1, 5\}$, soit $\mathrm{e}^{i\pi/3}$ et $\mathrm{e}^{-i\pi/3}$.

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).

c) Si $G \subset \mathbb{C}^*$ est un sous-groupe de cardinal n, Lagrange donne $z^n = 1$ pour tout $z \in G$: $G \subset \mathrm{U}_n$, et les cardinaux sont égaux.

Réponse. $\mathrm{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$; $\varphi(n)$ racines primitives ($e^{\pm i\pi/3}$ pour $n = 6$) ; unique sous-groupe d'ordre n.

Correction de l'exercice 11 – Les isométries du triangle équilatéral

a) Une isométrie conserve les distances, donc envoie les points de T les plus éloignés du centre (les sommets) sur des sommets : elle induit une permutation $\Phi(f)$ des indices. $\Phi(f \circ g) = \Phi(f) \circ \Phi(g)$.

b) Si $\Phi(f) = \mathrm{id}$, f fixe A_1, A_2, A_3 ; une isométrie affine fixant trois points non alignés est l'identité (elle fixe un repère).

c) Rotations de centre O et d'angles $0, \frac{2\pi}{3}, \frac{4\pi}{3}$: identité et 3-cycles. Réflexions d'axes les trois médianes : transpositions (chacune fixe un sommet et échange les deux autres). Φ est injective et $\mathrm{card} D_3 = 6 = \mathrm{card} S_3$:

$$D_3 \simeq S_3$$

Réponse. Φ morphisme injectif ; 3 rotations (identité, 3-cycles) et 3 réflexions (transpositions) ; $D_3 \simeq S_3$.

Correction de l'exercice 12 – Image d'un groupe cyclique

a) $f(g^k) = f(g)^k$: tout élément de $f(G)$ est une puissance de $f(g)$.

b) Si $g^d = e$, alors $f(g)^d = f(g^d) = e$, donc l'ordre de $f(g)$ divise $d = \mathrm{ord}(g)$.

c) Le quotient est l'image de $\mathbb{Z}/12\mathbb{Z}$ par la projection : il est cyclique, engendré par la classe de $\overline{1}$, de cardinal $\frac{12}{3} = 4$:

$$(\mathbb{Z}/12\mathbb{Z})/\langle\overline{4}\rangle \simeq \mathbb{Z}/4\mathbb{Z}$$

d) Non : l'image serait cyclique de cardinal 5, engendrée par $f(g)$ d'ordre 5, qui devrait diviser 12. Seul le morphisme trivial existe vers $\mathbb{Z}/5\mathbb{Z}$.

Réponse. Image cyclique ; $\mathrm{ord} f(g) \mid \mathrm{ord} g$; quotient $\simeq \mathbb{Z}/4\mathbb{Z}$; pas de surjection $\mathbb{Z}/12 \to \mathbb{Z}/5$.

Correction de l'exercice 13 – Sous-groupes de Z et pgcd

a) $a\mathbb{Z} + b\mathbb{Z}$ contient 0, est stable par somme et opposé : c'est un sous-groupe, égal à $d\mathbb{Z}$ avec $d \geq 0$. $a, b \in d\mathbb{Z}$, donc d divise a et b ; et $d = au + bv$: tout diviseur commun de a et b divise d. Donc $d = a \wedge b$, et l'on obtient au passage Bézout.

b) $a\mathbb{Z} \cap b\mathbb{Z}$ est l'ensemble des multiples communs, sous-groupe $m\mathbb{Z}$; m est un multiple commun qui divise tous les autres : $m = a \vee b$.

c) Euclide : $120 = 84 + 36$, $84 = 2 \times 36 + 12$, $36 = 3 \times 12$. Donc $84\mathbb{Z} + 120\mathbb{Z} = 12\mathbb{Z}$, et en remontant :

$$12 = 84 - 2 \times 36 = 84 - 2(120 - 84) = 3 \times 84 - 2 \times 120$$

Réponse. $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$, $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$; $12 = 3 \times 84 - 2 \times 120$.

Correction de l'exercice 14 – Exposant d'un groupe abélien fini

a) Chaque ordre divise $\mathrm{card} G$ (Lagrange), donc leur ppcm aussi.

b) Soient a d'ordre m, b d'ordre n, et $L = \mathrm{ppcm}(m, n)$. On écrit $L = m'n'$ avec $m' \mid m$, $n' \mid n$, $m' \wedge n' = 1$ (on répartit les facteurs premiers : chaque p^α de L est pris dans m ou dans 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).

Alors $a^{m/m'}$ est d'ordre m' et $b^{n/n'}$ d'ordre n', et leur produit est d'ordre $m'n' = L$. Par récurrence sur les éléments de G, on obtient un élément d'ordre $e(G)$.

c) G est cyclique si et seulement s'il a un élément d'ordre card$G$, c'est-à-dire (par b) et a)) si et seulement si $e(G) = \mathrm{card}G$.

$$e((\mathbb{Z}/8\mathbb{Z})^\times) = 2 < 4, \qquad e((\mathbb{Z}/9\mathbb{Z})^\times) = 6$$

— Le premier n'est pas cyclique, le second l'est.

Réponse. $e(G) \mid \mathrm{card}G$; il existe un élément d'ordre $e(G)$; cyclique $\Leftrightarrow e(G) = \mathrm{card}G$.

Correction de l'exercice 15 – Synthèse : x² = 1 modulo p et le théorème de Wilson

a) $x^2 - 1 = (x-1)(x+1)$, et un corps est intègre : $x = \overline{1}$ ou $x = -\overline{1}$ (distincts car $p \neq 2$).

b) $x \mapsto x^{-1}$ est une involution de G, dont les points fixes sont les solutions de $x^2 = \overline{1}$, soit $\pm\overline{1}$. Les autres éléments se groupent en paires $\{x, x^{-1}\}$ de produit $\overline{1}$. Le produit de tous les éléments vaut donc $\overline{1} \times (-\overline{1}) = -\overline{1}$:

$$(p-1)! \equiv -1 \pmod{p}$$

c) $p = 7$: paires $\{2,4\}$ ($8 \equiv 1$), $\{3,5\}$ ($15 \equiv 1$), et 1, 6 seuls. $6! = 720 = 7 \times 103 - 1$.

d) Si $n = ab$ avec $1 < a < n$, alors a divise $(n-1)!$; si l'on avait $(n-1)! \equiv -1 \pmod{n}$, a diviserait aussi $(n-1)! + 1$, donc 1 : absurde. Ainsi n est premier si et seulement si $n \mid (n-1)! + 1$ — critère exact, mais inutilisable en pratique (calcul de $(n-1)!$).

Réponse. $x^2 = 1 \Rightarrow x = \pm 1$; $(p-1)! \equiv -1 \pmod{p}$; Wilson caractérise les nombres premiers.

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).