Plaquette 2 – Groupes, sous-groupes et théorème de Lagrange

Structures algébriques — Prépa MPSI / MP2I (1re année)

Corrections détaillées

Boîte à outils

Groupes et sous-groupes.

— **Sous-groupe** : $H \subset G$ est un sous-groupe si et seulement si

$$e \in H \quad \text{et} \quad \forall x, y \in H,\ xy^{-1} \in H$$

— **Sous-groupe engendré** par a : $\langle a \rangle = \{a^k,\ k \in \mathbb{Z}\}$; son cardinal est l'**ordre** de a.

— **Ordre** : $a^m = e \Leftrightarrow \mathrm{ord}(a) \mid m$. Dans $\mathbb{Z}/n\mathbb{Z}$, $\overline{k}$ est d'ordre $\frac{n}{k \wedge n}$; il engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.

— **Lagrange** : si H est un sous-groupe du groupe fini G, les classes xH partitionnent G et ont toutes $\mathrm{card}H$ éléments, donc

$$\mathrm{card}H \text{ divise } \mathrm{card}G$$

— **Corollaires** : $\mathrm{ord}(a) \mid \mathrm{card}G$; $a^{\mathrm{card}G} = e$; un groupe d'ordre premier est cyclique.

— **Groupe produit** : $G \times G'$ avec la loi composante par composante ; $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique si et seulement si $m \wedge n = 1$.

Correction de l'exercice 1 – Reconnaître un groupe

On teste dans l'ordre : loi **interne**, **associativité**, **neutre**, **inverses**.

— **a)** Loi interne, associative, neutre 0 ; mais 1 n'a pas d'opposé dans $\mathbb{N}$: **non**.

— **b)** La soustraction n'est pas associative : $(1-2)-3 = -4$ et $1-(2-3) = 2$: **non**.

— **c)** C'est un sous-groupe de $(\mathbb{R}^*, \times)$: $1 \in \mathbb{Q}^*$ et, pour $x, y \in \mathbb{Q}^*$, $xy^{-1} \in \mathbb{Q}^*$: **oui**.

— **d)** max est associative et $\max(x,y) \geq x$; un neutre e vérifierait $\max(e,x) = x$ pour tout x, donc $e \leq x$ pour tout réel x : impossible. **Non**.

— **e)** Sous-groupe de $(\mathbb{R}^*, \times)$: 1 est dedans et $(\pm 1)(\pm 1)^{-1} = \pm 1$: **oui** (c'est U_2).

— **f)** $\overline{2} \times \overline{3} = \overline{0}$: la loi n'est pas interne sur $\mathbb{Z}/6\mathbb{Z} \setminus \{\overline{0}\}$. **Non**.

La caractérisation utilisée en c) et e) :

$$H \text{ sous-groupe de } G \Leftrightarrow e \in H \text{ et } \forall x, y \in H,\ xy^{-1} \in H$$

Réflexe : dès qu'un ensemble est inclus dans un groupe connu pour la même loi, on évite de revérifier l'associativité — elle est héritée.

Réponse. Groupes : c) et e). Non-groupes : a) (inverses), b) (associativité), d) (neutre), f) (loi non interne).

Correction de l'exercice 2 – Une loi transportée

a) On développe : $(1-x)(1-y) = 1-x-y+xy = 1-(x+y-xy)$. Si $x \neq 1$ et $y \neq 1$, le produit est non nul, donc $1 - x*y \neq 0$: $x*y \in G$.

b) f est bijective de G sur $\mathbb{R}^*$, de réciproque $u \mapsto 1-u$. D'après a) :

$$f(x*y) = 1 - x*y = (1-x)(1-y) = f(x)f(y)$$

c) $*$ est la loi de $(\mathbb{R}^*, \times)$ **transportée** par la bijection f : $x*y = f^{-1}(f(x)f(y))$. Toutes les propriétés passent :

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).

— **associativité** et **commutativité** : celles du produit de réels ;
— **neutre** : $f^{-1}(1) = 0$ (en effet $x * 0 = x$) ;
— **inverse** de x : $f^{-1}\left(\frac{1}{1-x}\right) = 1 - \frac{1}{1-x} = \frac{x}{x-1}$.

Contrôle pour $x = 3$: l'inverse annoncé est $\frac{3}{2}$, et $3 * \frac{3}{2} = 3 + \frac{3}{2} - \frac{9}{2} = 0$ ✓.

Méthode : repérer une bijection qui « simplifie » la loi évite de vérifier l'associativité à la main, qui est ici pénible.

Réponse. $(G, *) \simeq (\mathbb{R}^*, \times)$ par $x \mapsto 1 - x$; neutre 0, inverse $\frac{x}{x-1}$.

Correction de l'exercice 3 – Différence symétrique

a) En un point x, $1_{A\Delta B}(x) = 1$ si et seulement si x est dans **exactement un** des deux ensembles, c'est-à-dire si $1_A(x) + 1_B(x) = 1$. Les autres cas donnent $0 + 0 = 0$ ou $1 + 1 = 2 \equiv 0$. Donc

$$1_{A\Delta B} \equiv 1_A + 1_B \pmod 2$$

b) L'application $A \mapsto 1_A$ identifie $P(E)$ aux fonctions de E dans $\mathbb{Z}/2\mathbb{Z}$, et Δ à l'**addition** de ces fonctions. Les propriétés de $(\mathbb{Z}/2\mathbb{Z}, +)$ se transportent :

— associativité et commutativité ;
— neutre : $\varnothing$ ($1_\varnothing = 0$) ;
— inverse : A lui-même, car $1_A + 1_A \equiv 0$, soit $A \Delta A = \varnothing$.

c) On « ajoute » A des deux côtés, par associativité :

$$A \Delta X = B \Leftrightarrow A \Delta (A \Delta X) = A \Delta B \Leftrightarrow X = A \Delta B$$

— solution unique $X = A \Delta B$. Contrôle avec $A = \{1, 2\}$, $B = \{2, 3\}$: $X = \{1, 3\}$ et $\{1, 2\} \Delta \{1, 3\} = \{2, 3\}$ ✓.

Réponse. $1_{A\Delta B} \equiv 1_A + 1_B$ (2) ; groupe abélien de neutre $\varnothing$, chaque A est son propre inverse ; $X = A \Delta B$.

Correction de l'exercice 4 – Le groupe des isométries du carré

a) Une isométrie qui conserve le carré conserve son centre O et permute les sommets en respectant les côtés.

— **Rotations** de centre O : id, r, r^2 (demi-tour), r^3 (angle $-\frac{\pi}{2}$).
— **Réflexions** : d'axes les deux diagonales (AC), (BD) et les deux médiatrices des côtés.

L'image de A peut être l'un des 4 sommets, puis celle de B l'un des 2 voisins de cette image : au plus 8 isométries, et on en a trouvé 8.

b) id : ordre 1 ; r et r^3 : ordre 4 ; r^2 et les quatre réflexions : ordre 2. Tous divisent 8, comme l'exige Lagrange :

$$\mathrm{ord}(g) \mid \mathrm{card} D_4 = 8$$

c) r envoie $A \to B \to C \to D \to A$ (sens direct) ; s fixe A et C et échange B et D.

— $r \circ s$: $A \mapsto A \mapsto B$ et $B \mapsto D \mapsto A$: il échange A et B, c'est la réflexion d'axe la médiatrice de $[AB]$.
— $s \circ r$: $A \mapsto B \mapsto D$ et $B \mapsto C \mapsto C$: il envoie A sur D, c'est la réflexion d'axe la médiatrice de $[AD]$.

$r \circ s \neq s \circ r$: D_4 **n'est pas abélien**.

d) $\{\mathrm{id}, r, r^2, r^3\} = \langle r \rangle$ est engendré par r, cyclique d'ordre 4. Les $r^k \circ s$ sont 4 isométries **indirectes** distinctes (composer par s est injectif), donc les 4 réflexions. Au total

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).

$D_4 = \langle r\rangle \cup \langle r\rangle \circ s$.

Réponse. 4 rotations, 4 réflexions ; ordres $1, 4, 2, 4$ et 2 pour les réflexions ; $r \circ s \neq s \circ r$; $D_4 = \{r^k, r^k s\}$.

Correction de l'exercice 5 – Sous-groupes de Z/12Z

a) On ajoute l'élément à lui-même jusqu'à revenir à $\overline{0}$:

— $\langle\overline{3}\rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$, d'ordre 4 ; $\langle\overline{9}\rangle$ est le même, car $\overline{9} = -\overline{3}$.
— $\langle\overline{4}\rangle = \{\overline{0}, \overline{4}, \overline{8}\}$, d'ordre 3 ; $\langle\overline{8}\rangle$ est le même.

Conforme à la formule du cours :

$$\operatorname{ord}(\overline{k}) = \frac{n}{k \wedge n}, \qquad \text{par exemple} \quad \operatorname{ord}(\overline{9}) = \frac{12}{3} = 4$$

b) $\overline{k}$ engendre $\mathbb{Z}/12\mathbb{Z}$ si et seulement si son ordre vaut 12, soit $k \wedge 12 = 1$: $\overline{1}, \overline{5}, \overline{7}, \overline{11}$.

c) Un sous-groupe par diviseur de 12 :

— $d = 1$: le groupe entier (ordre 12) ; $d = 2$: $\{\overline{0}, \overline{2}, \ldots, \overline{10}\}$ (ordre 6) ; $d = 3$: $\langle\overline{3}\rangle$ (ordre 4) ;
— $d = 4$: $\langle\overline{4}\rangle$ (ordre 3) ; $d = 6$: $\{\overline{0}, \overline{6}\}$ (ordre 2) ; $d = 12$: $\{\overline{0}\}$ (ordre 1).

Six sous-groupes, d'ordres $12, 6, 4, 3, 2, 1$: exactement les diviseurs de 12, comme le prévoit Lagrange — et chaque diviseur est atteint une fois.

Piège : $\langle\overline{8}\rangle$ n'est pas d'ordre $\frac{12}{8}$; l'ordre est $\frac{12}{8 \wedge 12} = \frac{12}{4} = 3$.

Réponse. $\langle\overline{3}\rangle = \langle\overline{9}\rangle$ d'ordre 4, $\langle\overline{4}\rangle = \langle\overline{8}\rangle$ d'ordre 3 ; générateurs $\overline{1}, \overline{5}, \overline{7}, \overline{11}$; six sous-groupes.

Correction de l'exercice 6 – Le cycle des quintes

a) Empiler k quintes depuis do conduit à la note $\overline{7k}$. L'ordre de $\overline{7}$ vaut

$$\operatorname{ord}(\overline{7}) = \frac{12}{7 \wedge 12} = 12$$

— donc $\langle\overline{7}\rangle = \mathbb{Z}/12\mathbb{Z}$: les douze notes sont atteintes avant le retour. Suite : $0, 7, 2, 9, 4, 11, 6, 1, 8, 3, 10, 5$, puis 0 (do, sol, ré, la, mi, si, fa♯, do♯, sol♯, ré♯, la♯, fa).

b) $\langle\overline{4}\rangle = \{\overline{0}, \overline{4}, \overline{8}\}$ (ordre 3) : trois tierces majeures ramènent au départ, ce qui découpe l'octave en trois parts égales — c'est l'**accord augmenté**.

— $\langle\overline{3}\rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ (ordre 4) : quatre tierces mineures bouclent — l'**accord de septième diminuée**.

c) Il faut un générateur de $\mathbb{Z}/12\mathbb{Z}$, donc $k \wedge 12 = 1$: 1 (demi-ton), 5 (quarte), 7 (quinte), 11 (septième majeure). Les autres intervalles restent dans un sous-groupe strict.

Remarque : en accord « naturel », douze quintes pures dépassent sept octaves ($\left(\frac{3}{2}\right)^{12} \approx 129{,}7 > 2^7 = 128$) ; le tempérament égal force le cycle à se refermer.

Réponse. $\overline{7}$ engendre $\mathbb{Z}/12\mathbb{Z}$: $0, 7, 2, 9, 4, 11, 6, 1, 8, 3, 10, 5$; tierces : sous-groupes d'ordres 3 et 4 ; intervalles générateurs $1, 5, 7, 11$.

Correction de l'exercice 7 – Démonstration du théorème de Lagrange

a) $h \mapsto xh$ est surjective sur xH par définition, et injective : $xh = xh' \Rightarrow h = h'$ en multipliant à gauche par x^{-1}. Donc $\operatorname{card}(xH) = \operatorname{card} H$.

b) Si $z \in xH$, alors $z = xh_0$ et $zH = xh_0H = xH$ (car $h_0H = H$, H étant un sous-groupe). De même $z \in yH$ donne $zH = yH$. Donc $xH \cap yH \neq \varnothing \Rightarrow xH = yH$.

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) Tout x est dans sa classe xH ($x = xe$) : les classes **recouvrent** G, et d'après b) elles forment une **partition**. Si elles sont k, chacune de cardinal card$H$ d'après a) :

$$\text{card}G = k \times \text{card}H$$

d) Soit $a \neq e$ et $H = \langle a \rangle$. Son cardinal divise p et vaut au moins 2 (il contient e et a) : il vaut p, donc $\langle a \rangle = G$.

— Exemple : $\mathbb{Z}/7\mathbb{Z}$ est engendré par chacun de ses six éléments non nuls.

Attention : la réciproque de Lagrange est fausse en général ; un groupe d'ordre 12 peut n'avoir aucun sous-groupe d'ordre 6 (c'est le cas du groupe des déplacements du tétraèdre).

Réponse. Les classes xH partitionnent G et ont card$H$ éléments : card$H$ | card$G$; ordre premier ⇒ cyclique.

Correction de l'exercice 8 – Lagrange redonne Fermat et Euler

a) Soit $k = \text{ord}(x)$. Par Lagrange appliqué à $\langle x \rangle$, $k \mid N$: $N = kq$ et

$$x^N = \left(x^k\right)^q = e^q = e$$

b) Pour p premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est formé des $p-1$ classes non nulles (toutes inversibles, car $\mathbb{Z}/p\mathbb{Z}$ est un corps). Pour $p \nmid a$, a) donne $\overline{a}^{\,p-1} = \overline{1}$, soit $a^{p-1} \equiv 1 \pmod{p}$.

c) $(\mathbb{Z}/n\mathbb{Z})^*$ est le groupe des classes inversibles, de cardinal $\varphi(n)$. Pour $a \wedge n = 1$, $\overline{a}$ est dedans et $\overline{a}^{\varphi(n)} = \overline{1}$.

d) 13 est premier et $13 \nmid 2$: $2^{12} \equiv 1 \pmod{13}$. Or $100 = 12 \times 8 + 4$, donc

— $2^{100} \equiv 2^4 = 16 \equiv 3 \pmod{13}$.

Contrôle par l'ordre : $2^6 = 64 \equiv -1 \pmod{13}$, donc l'ordre de 2 est 12 (il divise 12, ne divise ni 4 ni 6 puisque $2^4 \equiv 3$ et $2^6 \equiv -1$).

Point de vue : les théorèmes de Fermat et d'Euler ne sont que Lagrange dans un groupe particulier.

Réponse. $x^{\text{card}G} = e$; Fermat et Euler en sont des cas particuliers ; $2^{100} \equiv 3 \pmod{13}$.

Correction de l'exercice 9 – Nombres complexes vus comme matrices

a) $\det M(a,b) = a^2 + b^2 \neq 0$, donc $C \subset \text{GL}_2(\mathbb{R})$. Le produit se calcule directement :

$$M(a,b)M(c,d) = \begin{pmatrix} ac - bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} = M(ac-bd,\, ad+bc)$$

— **Neutre** : $I_2 = M(1,0) \in C$.

— **Inverse** : $M(a,b)^{-1} = \dfrac{1}{a^2+b^2} M(a,-b)$, de la même forme.

— Stabilité par produit (et $(ac-bd, ad+bc) \neq (0,0)$ car le déterminant est $(a^2+b^2)(c^2+d^2) \neq 0$) : C est un sous-groupe.

b) Le calcul de a) est **exactement** celui de $(a+\mathrm{i}b)(c+\mathrm{i}d) = (ac-bd)+\mathrm{i}(ad+bc)$: $\Phi(zw) = \Phi(z)\Phi(w)$. Φ est bijective (les coefficients a, b se lisent sur la matrice). C'est un isomorphisme.

c) $\Phi(\mathrm{U}) = \{M(a,b),\, a^2+b^2 = 1\} = \{M(\cos\theta, \sin\theta)\}$: les matrices de **rotation** d'angle θ. Multiplier par $\mathrm{e}^{\mathrm{i}\theta}$, c'est tourner de θ ; l'isomorphisme le traduit en matrices.

— Contrôle : $\Phi(\mathrm{i})^2 = M(0,1)^2 = M(-1,0) = -I_2 = \Phi(-1)$ ✓.

Réponse. C sous-groupe de $\text{GL}_2(\mathbb{R})$, isomorphe à $\mathbb{C}^*$; $\Phi(\mathrm{U})$ = matrices de rotation.

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 10 – Ordre d'un produit

a) Un élément x de $\langle a\rangle \cap \langle b\rangle$ a un ordre qui divise m et n (Lagrange dans chacun des deux sous-groupes), donc divise $m \wedge n = 1$: $x = e$.

— Comme $ab = ba$, $(ab)^k = a^k b^k$. Donc $(ab)^{mn} = (a^m)^n (b^n)^m = e$: l'ordre k de ab divise mn.

— Si $(ab)^k = e$, alors $a^k = b^{-k}$ est dans $\langle a\rangle \cap \langle b\rangle = \{e\}$. Donc $a^k = e$ et $b^k = e$, d'où $m \mid k$ et $n \mid k$, puis $mn \mid k$ par Gauss.

$$\mathrm{ord}(ab) = mn$$

b) Dans $\mathbb{Z}/4\mathbb{Z}$ (notation additive), $a = b = \overline{1}$ sont d'ordre 4, mais $a + b = \overline{2}$ est d'ordre $2 \neq 16$. Même avec $a = \overline{1}$, $b = \overline{3}$: $a + b = \overline{0}$, d'ordre 1.

c) Avec $\tau_1 = (1\ 2)$ et $\tau_2 = (2\ 3)$, d'ordre 2 : $\tau_1 \circ \tau_2$ envoie $3 \mapsto 2 \mapsto 1$, $1 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 3$, c'est le cycle $(1\ 2\ 3)$, d'ordre 3. Ici $\tau_1\tau_2 \neq \tau_2\tau_1$ (et $2 \wedge 2 \neq 1$) : sans commutativité, l'ordre d'un produit n'est lié à rien.

Réponse. $ab = ba$ et $m \wedge n = 1 \Rightarrow \mathrm{ord}(ab) = mn$; contre-exemples $\overline{1} + \overline{1}$ dans $\mathbb{Z}/4\mathbb{Z}$ et $(1\ 2)(2\ 3)$ dans S_3.

Correction de l'exercice 11 – Groupes où tout élément est d'ordre au plus 2

a) $x^2 = e$ signifie $xx = e$, donc $x^{-1} = x$. Pour $x, y \in G$, $(xy)^2 = e$ donne $xyxy = e$, soit en multipliant à gauche par x et à droite par y :

$$yx = x^{-1}y^{-1} = xy$$

— G est abélien.

b) $(\mathbb{Z}/2\mathbb{Z})^n$; le groupe de Klein ; $(P(E), \Delta)$ (tout A vérifie $A \,\Delta\, A = \varnothing$).

c) $a^2 = e$ donne la stabilité de $H = \{e, a\}$: sous-groupe d'ordre 2. Si $b \notin H$:

— $ab \notin \{e, a, b\}$ ($ab = e \Rightarrow b = a$; $ab = a \Rightarrow b = e$; $ab = b \Rightarrow a = e$) : K a 4 éléments.

— Stabilité : grâce à la commutativité et à $x^2 = e$, $a \cdot ab = b$, $b \cdot ab = a$, $ab \cdot ab = e$: K est un sous-groupe.

Par Lagrange, $2 \mid \mathrm{card} G$ et, si $\mathrm{card} G > 2$, $4 \mid \mathrm{card} G$. Pour $\mathrm{card} G \leq 8$, les multiples de 4 possibles sont 4 et 8 (le cas $\mathrm{card} G = 8$ se traite en ajoutant un $c \notin K$, qui donne un sous-groupe d'ordre 8). Dans tous les cas, $\mathrm{card} G \in \{1, 2, 4, 8\}$.

Structure : un tel groupe est un espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$, d'où son cardinal 2^n.

Réponse. $x^{-1} = x$ et G abélien ; exemples $(\mathbb{Z}/2\mathbb{Z})^n$, Klein, $(P(E), \Delta)$; cardinal puissance de 2.

Correction de l'exercice 12 – Groupes produits cycliques

a) Les multiples de $(\overline{1}, \overline{1})$: $(\overline{1}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{2}), (\overline{0}, \overline{0})$ — six pas pour revenir au neutre. Un élément d'ordre 6 dans un groupe à 6 éléments l'engendre : le groupe est cyclique, et $k \mapsto k(\overline{1}, \overline{1})$ induit un isomorphisme avec $\mathbb{Z}/6\mathbb{Z}$.

b) Tout (x, y) vérifie $2(x, y) = (\overline{0}, \overline{0})$: aucun élément d'ordre 4.

c) $k(x, y) = (kx, ky)$ est nul si et seulement si $\mathrm{ord}(x) \mid k$ et $\mathrm{ord}(y) \mid k$, c'est-à-dire si k est un multiple commun. Le plus petit est le PPCM :

$$\mathrm{ord}(x, y) = \mathrm{ppcm}(\mathrm{ord}(x), \mathrm{ord}(y))$$

— Les ordres dans $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ divisent m et n, donc l'ordre de tout élément du produit divise $\mathrm{ppcm}(m, n)$.

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).

— Le produit (de cardinal mn) est cyclique si et seulement si un élément est d'ordre mn ; c'est possible si et seulement si $\text{ppcm}(m,n) = mn$, soit $m \wedge n = 1$, et alors $(\overline{1},\overline{1})$ convient.

C'est une forme du **théorème chinois**.

Réponse. $(\overline{1},\overline{1})$ d'ordre 6 : $\mathbb{Z}/2 \times \mathbb{Z}/3 \simeq \mathbb{Z}/6$; $\text{ord}(x,y) = \text{ppcm}$; cyclique $\Leftrightarrow m \wedge n = 1$.

Correction de l'exercice 13 – Sous-groupes finis de C*

a) Par Lagrange (corollaire $x^{\text{card}G} = e$) appliqué au groupe H :

$$\forall z \in H, \qquad z^n = 1$$

— donc tout élément de H est une racine n-ième de l'unité : $H \subset U_n$.

b) U_n a exactement n éléments (les $e^{2ik\pi/n}$, $0 \leq k \leq n-1$) et $H \subset U_n$ a aussi n éléments : $H = U_n$. Les sous-groupes finis de $\mathbb{C}^*$ sont donc les U_n, tous **cycliques**.

c) $U_4 \cup U_6$ a $4 + 6 - 2 = 8$ éléments ($U_4 \cap U_6 = U_2 = \{\pm 1\}$). S'il était un sous-groupe fini, ce serait U_8 d'après b) ; or $e^{i\pi/3} \in U_6$ n'est pas une racine 8-ième de l'unité ($e^{8i\pi/3} \neq 1$). Ce n'est pas un sous-groupe.

— Un sous-groupe fini contenant U_4 et U_6 est un U_N avec $4 \mid N$ et $6 \mid N$ (car $i \in U_N$ impose $4 \mid N$, et $e^{i\pi/3} \in U_N$ impose $6 \mid N$). Le plus petit est U_{12}, avec $12 = \text{ppcm}(4,6)$.

Réponse. $H = U_n$; $U_4 \cup U_6$ n'est pas un sous-groupe ; le plus petit sous-groupe fini le contenant est U_{12}.

Correction de l'exercice 14 – Sous-groupes de R et densité

a) Si $\alpha \notin H$, par définition de la borne inférieure il existe $h_1, h_2 \in H$ avec $\alpha < h_2 < h_1 < 2\alpha$. Alors $0 < h_1 - h_2 < \alpha$ et $h_1 - h_2 \in H$: contradiction avec la définition de α. Donc $\alpha \in H$ et $\alpha\mathbb{Z} \subset H$.

— Pour $h \in H$, on écrit $h = q\alpha + r$ avec $q = \left\lfloor \frac{h}{\alpha} \right\rfloor$ et $0 \leq r < \alpha$. Alors $r = h - q\alpha \in H$, et par minimalité $r = 0$: $H = \alpha\mathbb{Z}$.

b) Soit $\varepsilon > 0$: il existe $h \in H$ avec $0 < h < \varepsilon$. Les multiples kh forment une grille de pas $h < \varepsilon$; pour x réel, avec $k = \left\lfloor \frac{x}{h} \right\rfloor + 1$,

$$x < kh \leq x + h < x + \varepsilon$$

— et $kh \in H$: H rencontre $]x, x+\varepsilon[$.

c) $\sqrt{2} - 1 = -1 + 1 \times \sqrt{2} \in H$, et H est stable par produit :
$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$. Donc $(\sqrt{2}-1)^n \in H$, avec $0 < (\sqrt{2}-1)^n \to 0$ (car $0 < \sqrt{2} - 1 < 1$) : $\alpha = 0$ et H est dense d'après b).

— Par exemple $(\sqrt{2}-1)^2 = 3 - 2\sqrt{2} \approx 0{,}172 \in H$.

Réponse. $\alpha > 0 \Rightarrow H = \alpha\mathbb{Z}$; $\alpha = 0 \Rightarrow H$ dense ; $\mathbb{Z} + \sqrt{2}\,\mathbb{Z}$ est dense car il contient les $(\sqrt{2}-1)^n \to 0$.

Correction de l'exercice 15 – Synthèse : les groupes d'ordre 4

a) Par Lagrange, l'ordre d'un élément divise 4 : 1 (seulement e), 2 ou 4.

b) Si $\text{ord}(a) = 4$, alors $\langle a \rangle = \{e, a, a^2, a^3\}$ a 4 éléments : $G = \langle a \rangle$, et $\overline{k} \mapsto a^k$ est un isomorphisme de $\mathbb{Z}/4\mathbb{Z}$ sur G (bien défini car $a^4 = e$).

c) Sinon, tout $x \neq e$ est d'ordre 2 : $x^2 = e$ pour tout x, donc G est **abélien** (exercice sur les groupes d'ordre au plus 2). Écrivons $G = \{e, a, b, c\}$; $ab \notin \{e, a, b\}$ (sinon $b = a$, $b = e$ ou $a = e$), donc $ab = c$. De même $ac = b$ et $bc = a$: la table est entièrement déterminée,

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).

$$a^2 = b^2 = c^2 = e, \qquad ab = c, \quad ac = b, \quad bc = a$$

— c'est celle du groupe de Klein. Il y a donc deux classes d'isomorphisme : $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$.

d) $U_4 = \{1, \mathrm{i}, -1, -\mathrm{i}\}$: i d'ordre 4, **cyclique**.

— $(\mathbb{Z}/5\mathbb{Z})^*$: $\overline{2}$ d'ordre 4 $(2, 4, 3, 1)$, **cyclique**.

— $(\mathbb{Z}/8\mathbb{Z})^*$: tous les éléments $\neq \overline{1}$ d'ordre 2, **Klein**.

— Rotations du carré : r d'ordre 4, **cyclique**.

— $\{\mathrm{id}, s_1, s_2, r^2\}$: trois éléments d'ordre 2 (et $s_1 s_2 = r^2$), **Klein**.

Réponse. Ordres $1, 2, 4$; deux groupes : $\mathbb{Z}/4\mathbb{Z}$ (un élément d'ordre 4) ou Klein ; U_4, $(\mathbb{Z}/5\mathbb{Z})^*$, rotations : cycliques ; $(\mathbb{Z}/8\mathbb{Z})^*$ et $\{\mathrm{id}, s_1, s_2, r^2\}$: Klein.

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).