Plaquette 3 – Morphismes et isomorphismes de groupes

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

Corrections détaillées

Boîte à outils

Morphismes de groupes.

— $f:(G,\cdot)\to(G',\cdot)$ est un **morphisme** si $f(xy)=f(x)f(y)$ pour tous x,y. Alors

$$f(e)=e',\qquad f\left(x^{-1}\right)=f(x)^{-1},\qquad f\left(x^{k}\right)=f(x)^{k}\ (k\in\mathbb{Z})$$

— **Images** : si H est un sous-groupe de G, $f(H)$ est un sous-groupe de G' ; si K' est un sous-groupe de G', $f^{-1}(K')$ est un sous-groupe de G.

— **Noyau** : $\ker f=\{x\in G,\ f(x)=e'\}$, sous-groupe de G, et

$$f \text{ injectif} \Leftrightarrow \ker f=\{e\}$$

— **Fibres** : si $f(x_0)=y$, alors $f^{-1}(\{y\})=x_0\ker f$. Pour G fini : $\operatorname{card}G=\operatorname{card}(\ker f)\times\operatorname{card}(\operatorname{Im}f)$.

— **Isomorphisme** : morphisme bijectif ; sa réciproque est un morphisme. Il conserve l'ordre des éléments, la commutativité, le caractère cyclique.

— **Ordre** : pour tout morphisme, $\operatorname{ord}f(x)$ divise $\operatorname{ord}(x)$; il y a égalité si f est injectif.

— **Automorphismes intérieurs** : $i_g(x)=gxg^{-1}$; $g\mapsto i_g$ est un morphisme de G dans $(\operatorname{Aut}G,\circ)$, de noyau le centre $Z(G)$.

Correction de l'exercice 1 – Reconnaître un morphisme

On vérifie la relation de définition, en commençant par le test rapide $f(e)=e'$:

$$f(xy)=f(x)f(y)\quad\Rightarrow\quad f(e)=e'$$

— **a)** $\det(AB)=\det A\det B$: **oui** (morphisme multiplicatif du déterminant).

— **b)** $3(x+y)=3x+3y$: **oui**.

— **c)** L'image du neutre 0 est $1\neq 0$: **non**.

— **d)** $|zw|=|z|\,|w|$: **oui**.

— **e)** $(1+1)^2=4\neq 1^2+1^2=2$: **non** (et pourtant $0\mapsto 0$: le test du neutre ne suffit pas à conclure positivement).

— **f)** $(xy)^2=xyxy$ et $x^2y^2=xxyy$; en simplifiant à gauche par x et à droite par y, l'égalité équivaut à $yx=xy$. C'est un morphisme **si et seulement si** G **est abélien**.

— **g)** La transposition renverse l'ordre, $(AB)^{\mathrm{T}}=B^{\mathrm{T}}A^{\mathrm{T}}$, et l'inversion aussi :

$$\left((AB)^{\mathrm{T}}\right)^{-1}=\left(B^{\mathrm{T}}A^{\mathrm{T}}\right)^{-1}=\left(A^{\mathrm{T}}\right)^{-1}\left(B^{\mathrm{T}}\right)^{-1}$$

Les deux renversements se compensent : **oui**. En revanche $M\mapsto M^{\mathrm{T}}$ seule n'est pas un morphisme de $\mathrm{GL}_2(\mathbb{R})$, qui n'est pas commutatif.

Réponse. Morphismes : a), b), d), g), et f) si et seulement si G est abélien. Non : c) et e).

Correction de l'exercice 2 – Noyaux et images classiques

Le noyau est l'image réciproque du **neutre d'arrivée** :

$$\ker f=\{x\in G,\ f(x)=e'\}$$

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)** Noyau : $\{M,\ \det M = 1\} = \mathrm{SL}_n(\mathbb{R})$. Image : pour $a \in \mathbb{R}^*$, la matrice diagonale $\mathrm{diag}(a, 1, \ldots, 1)$ a pour déterminant a, donc det est **surjectif**. Non injectif ($n \geq 2$: $\mathrm{diag}(2, \frac{1}{2}, 1, \ldots)$ est dans le noyau).

— **b)** $|zw| = |z|\,|w|$. Noyau : le cercle unité U. Image : $|r| = r$ pour $r > 0$, donc surjectif. Non injectif.

— **c)** $\mathrm{e}^{z+w} = \mathrm{e}^z \mathrm{e}^w$. Pour $z = a + \mathrm{i}b$, $\mathrm{e}^z = \mathrm{e}^a \mathrm{e}^{\mathrm{i}b} = 1$ impose $\mathrm{e}^a = 1$ (module) et $b \in 2\mathrm{i}\pi\mathbb{Z}$ (argument) : ker $= 2\mathrm{i}\pi\mathbb{Z}$. Image : tout $w \neq 0$ s'écrit $r\mathrm{e}^{\mathrm{i}\theta} = \mathrm{e}^{\ln r + \mathrm{i}\theta}$, donc surjectif.

— **d)** $x \mapsto x^3$: $x^3 = 1 \Leftrightarrow x = 1$, noyau $\{1\}$, **injectif** ; tout réel non nul a une racine cubique : **bijectif**, c'est un automorphisme de $\mathbb{R}^*$.

— $x \mapsto x^4$: noyau $\{-1, 1\}$, image $\mathbb{R}_+^*$ (les puissances quatrièmes sont positives, et $y > 0$ vaut $\left(y^{1/4}\right)^4$) : ni injectif, ni surjectif.

Lecture : le noyau de c) est la raison pour laquelle le logarithme complexe n'est défini qu'à $2\mathrm{i}\pi$ près.

Réponse. a) ker $= \mathrm{SL}_n(\mathbb{R})$, surjectif · b) ker = U, surjectif · c) ker $= 2\mathrm{i}\pi\mathbb{Z}$, surjectif · d) x^3 bijectif ; x^4 : ker $= \{\pm 1\}$, image $\mathbb{R}_+^*$.

Correction de l'exercice 3 – Morphismes de Z dans un groupe

a) Les règles de calcul des puissances donnent, pour $k, l \in \mathbb{Z}$:

$$f_a(k+l) = a^{k+l} = a^k a^l = f_a(k) f_a(l)$$

— L'image est $\{a^k,\ k \in \mathbb{Z}\} = \langle a \rangle$, le sous-groupe engendré par a.

b) Soit f un morphisme et $a = f(1)$. Par récurrence, $f(k) = f(1 + \ldots + 1) = a^k$ pour $k \geq 1$; $f(0) = e = a^0$; et pour $k \geq 1$, $f(-k) = f(k)^{-1} = a^{-k}$. Donc $f = f_a$: un morphisme issu de $\mathbb{Z}$ est **déterminé par l'image de** 1.

c) $\ker f_a$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $m\mathbb{Z}$ avec $m \geq 0$.

— $m = 0$ signifie que $a^k \neq e$ pour tout $k \neq 0$: a est d'ordre infini, et f_a est injectif.

— Si $m \geq 1$, m est le plus petit entier $k \geq 1$ tel que $a^k = e$: c'est l'ordre de a, et $a^k = e \Leftrightarrow m \mid k$.

d) Pour $G = (\mathbb{Z}, +)$, la notation multiplicative a^k devient ka : les morphismes sont les $k \mapsto ak$, $a \in \mathbb{Z}$. Un tel morphisme est surjectif si et seulement si 1 est atteint, soit $ak = 1$ pour un entier k : $a = \pm 1$. Les automorphismes sont id et $-\mathrm{id}$.

Réponse. $f_a(k) = a^k$, d'image $\langle a \rangle$; tout morphisme est un f_a ; $\ker f_a = \mathrm{ord}(a)\,\mathbb{Z}$ (ou $\{0\}$) ; endomorphismes de $\mathbb{Z}$: $k \mapsto ak$; automorphismes $\pm\mathrm{id}$.

Correction de l'exercice 4 – Morphismes entre groupes cycliques

a) $\overline{k} = \overline{1} + \ldots + \overline{1}$ (k termes), donc $f(\overline{k}) = ka$. En particulier $\overline{0} = f(\overline{0}) = f(\overline{n}) = na$.

b) Le point délicat est que $\overline{k}$ a plusieurs représentants. Si $\overline{k} = \overline{k'}$, alors $k - k' = qn$ et

$$ka - k'a = q\,(na) = \overline{0}$$

— donc ka ne dépend que de la classe $\overline{k}$: l'application est **bien définie**. Elle est additive : $(k+l)a = ka + la$.

c) Les morphismes correspondent donc aux $a = \overline{b} \in \mathbb{Z}/m\mathbb{Z}$ tels que $m \mid nb$. En divisant par d :

$$m \mid nb \Leftrightarrow \frac{m}{d} \mid \frac{n}{d} b \Leftrightarrow \frac{m}{d} \mid b$$

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).

— la dernière équivalence par le **lemme de Gauss**, car $\frac{m}{d} \wedge \frac{n}{d} = 1$. Les multiples de $\frac{m}{d}$ dans $\{0, \dots, m-1\}$ sont $0, \frac{m}{d}, \dots, (d-1)\frac{m}{d}$: il y en a d.

d) $n = 4$, $m = 6$, $d = 2$: b multiple de 3, donc $a \in \{\overline{0}, \overline{3}\}$. Les deux morphismes sont le morphisme nul et $\overline{k} \mapsto \overline{3k}$ (contrôle : $4 \times 3 = 12 \equiv 0 \pmod 6$).

— $n = 5$, $m = 7$, $d = 1$: seul le **morphisme nul** existe. Aucun élément de $\mathbb{Z}/7\mathbb{Z}$ autre que $\overline{0}$ n'a un ordre divisant 5.

Réponse. $f(\overline{k}) = ka$ avec $na = \overline{0}$; exactement $n \wedge m$ morphismes ; $\mathbb{Z}/4 \to \mathbb{Z}/6$: $a \in \{\overline{0}, \overline{3}\}$; $\mathbb{Z}/5 \to \mathbb{Z}/7$: seulement le nul.

Correction de l'exercice 5 – Automorphismes de Z/nZ

a) $\mathbb{Z}/n\mathbb{Z}$ est fini, donc f_a est bijectif si et seulement s'il est surjectif. Il est surjectif si et seulement si $\overline{1}$ est atteint : il existe x avec $ax = \overline{1}$, c'est-à-dire a inversible. Avec $a = \overline{b}$, la condition s'écrit :

$$f_{\overline{b}} \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \Leftrightarrow b \wedge n = 1$$

b) $f_a \circ f_b(x) = a(bx) = (ab)x$, donc $f_a \circ f_b = f_{ab}$: l'application $a \mapsto f_a$ est un morphisme. Elle est injective ($f_a(\overline{1}) = a$ permet de retrouver a) et surjective d'après a) : c'est un isomorphisme.

c) Il suffit d'étudier $(\mathbb{Z}/n\mathbb{Z})^\times$, de cardinal $\varphi(n)$.

— $n = 5$: $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, et $\overline{2}$ a pour puissances $\overline{2}, \overline{4}, \overline{3}, \overline{1}$: ordre 4, groupe **cyclique**. $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ est engendré par $x \mapsto 2x$.

— $n = 8$: $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ avec $3^2 = 9$, $5^2 = 25$, $7^2 = 49$, tous $\equiv 1 \pmod 8$: trois éléments d'ordre 2, groupe de **Klein**.

— $n = 12$: $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ avec 25, 49, 121 tous $\equiv 1 \pmod{12}$: encore **Klein**.

Piège : un automorphisme de $\mathbb{Z}/n\mathbb{Z}$ n'est pas « n'importe quelle permutation » : il est imposé par l'image de $\overline{1}$, qui doit être un générateur.

Réponse. $f_{\overline{b}}$ automorphisme $\Leftrightarrow b \wedge n = 1$; $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$; $n = 5$: cyclique d'ordre 4 ; $n = 8$ et $n = 12$: Klein.

Correction de l'exercice 6 – Automorphismes intérieurs et centre

a) On insère $g^{-1}g = e$ au milieu du produit :

$$i_g(xy) = gxyg^{-1} = \left(gxg^{-1}\right)\left(gyg^{-1}\right) = i_g(x)\, i_g(y)$$

— $i_{g^{-1}}\big(i_g(x)\big) = g^{-1}gxg^{-1}g = x$, et de même dans l'autre sens : i_g est bijectif de réciproque $i_{g^{-1}}$.

b) $i_{gh}(x) = ghx(gh)^{-1} = g\left(hxh^{-1}\right)g^{-1} = i_g \circ i_h(x)$, donc $\Phi(gh) = \Phi(g) \circ \Phi(h)$.

— $g \in \ker\Phi \Leftrightarrow i_g = \mathrm{id} \Leftrightarrow \forall x,\ gxg^{-1} = x \Leftrightarrow \forall x,\ gx = xg \Leftrightarrow g \in Z(G)$.

c) Si G est abélien, $gxg^{-1} = gg^{-1}x = x$: tous les i_g sont l'identité, Φ est **triviale**.

d) On calcule $\tau\sigma\tau^{-1}$ point par point (de droite à gauche, avec $\tau^{-1} = \tau$) :

— $1 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 3 \xrightarrow{\tau} 3$; $2 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 2 \xrightarrow{\tau} 1$; $3 \xrightarrow{\tau} 3 \xrightarrow{\sigma} 1 \xrightarrow{\tau} 2$.

— Donc $i_\tau(\sigma) = (1\ 3\ 2) = \sigma^2 \neq \sigma$: $i_\tau \neq \mathrm{id}$.

Comme $\ker\Phi = Z(S_3) = \{\mathrm{id}\}$, Φ est **injectif** : les 6 automorphismes i_g sont deux à deux distincts.

Règle pratique : conjuguer un cycle revient à renommer ses éléments,

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).

$\tau(a\ b\ c)\tau^{-1} = (\tau(a)\ \tau(b)\ \tau(c))$; ici $(2\ 1\ 3) = (1\ 3\ 2)$.

Réponse. i_g automorphisme de réciproque $i_{g^{-1}}$; $\ker\Phi = Z(G)$; trivial si G abélien ; $i_\tau(\sigma) = (1\ 3\ 2)$; six automorphismes intérieurs distincts.

Correction de l'exercice 7 – Images directes et réciproques de sous-groupes

On utilise la caractérisation des sous-groupes :

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

a) $e' = f(e) \in f(H)$. Si $x' = f(x)$ et $y' = f(y)$ avec $x, y \in H$, alors $x'y'^{-1} = f(x)f(y)^{-1} = f\left(xy^{-1}\right)$, avec $xy^{-1} \in H$: $x'y'^{-1} \in f(H)$.

b) $f(e) = e' \in K'$, donc $e \in f^{-1}(K')$. Si $f(x), f(y) \in K'$, alors $f\left(xy^{-1}\right) = f(x)f(y)^{-1} \in K'$. Enfin $\ker f = f^{-1}(\{e'\}) \subset f^{-1}(K')$ puisque $\{e'\} \subset K'$.

c) On applique b) au morphisme $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$:

— $\mathrm{SL}_n(\mathbb{R}) = \det^{-1}(\{1\})$;
— $\mathrm{GL}_n^+(\mathbb{R}) = \det^{-1}(\mathbb{R}_+^*)$, car $\mathbb{R}_+^*$ est un sous-groupe de $\mathbb{R}^*$;
— $\{M,\ \det M = \pm 1\} = \det^{-1}(\{-1, 1\})$, car $\{\pm 1\}$ est un sous-groupe de $\mathbb{R}^*$.

d) Non : il ne contient pas I_n ($\det I_n = 1$), et le produit de deux de ses éléments a un déterminant positif. D'ailleurs $\mathbb{R}_-^*$ n'est pas un sous-groupe de $\mathbb{R}^*$.

Méthode : reconnaître un sous-groupe comme **image réciproque** (en particulier comme noyau) dispense de toute vérification.

Réponse. $f(H)$ et $f^{-1}(K')$ sont des sous-groupes ; SL_n, GL_n^+, $\{\det = \pm 1\}$ en sont par $\det^{-1}$; $\{\det < 0\}$ n'en est pas un.

Correction de l'exercice 8 – Montrer que deux groupes ne sont pas isomorphes

Un isomorphisme f conserve l'**ordre** des éléments, car pour f injectif :

$$f(x)^k = e' \Leftrightarrow f\left(x^k\right) = f(e) \Leftrightarrow x^k = e$$

— **a)** Dans $\mathbb{R}^*$, -1 est d'ordre 2. Dans $(\mathbb{R}, +)$, $2x = 0$ impose $x = 0$: aucun élément d'ordre 2.
— **b)** Dans $\mathbb{C}^*$, i est d'ordre 4. Dans $\mathbb{R}^*$, $x^4 = 1$ impose $x = \pm 1$, d'ordre au plus 2.
— **c)** $\mathbb{Z} = \langle 1 \rangle$ est **monogène**. Si $\mathbb{Q} = \langle r \rangle = r\mathbb{Z}$ avec $r \neq 0$, alors $\frac{r}{2} = kr$ pour un entier k, soit $k = \frac{1}{2}$: absurde. $\mathbb{Q}$ n'est pas monogène.
— **d)** Dans $(\mathbb{Q}, +)$, tout élément est un « double » : $x = \frac{x}{2} + \frac{x}{2}$. Si $f : \mathbb{Q} \to \mathbb{Q}_+^*$ était un isomorphisme, on écrirait $2 = f(x)$ et

$$2 = f\left(\frac{x}{2} + \frac{x}{2}\right) = f\left(\frac{x}{2}\right)^2$$

qui ferait de $\sqrt{2} = f\left(\frac{x}{2}\right)$ un rationnel : absurde.

— **e)** $\mathbb{Z}/6\mathbb{Z}$ est **abélien**, S_3 ne l'est pas ($(1\ 2)(2\ 3) = (1\ 2\ 3)$ et $(2\ 3)(1\ 2) = (1\ 3\ 2)$). On peut aussi dire : $\overline{1}$ est d'ordre 6, alors que les éléments de S_3 sont d'ordre 1, 2 ou 3.

Méthode : on ne prouve jamais une non-isomorphie en essayant quelques bijections ; on cherche un **invariant**.

Réponse. Invariants séparateurs : a) élément d'ordre 2 · b) élément d'ordre 4 · c) monogène · d) racines carrées (2 n'est pas un carré dans $\mathbb{Q}_+^*$) · e) commutativité.

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 9 – Morphismes continus de (R, +)

a) f est un morphisme issu de $\mathbb{Z}$ (restreint), donc $f(n) = nf(1) = na$ pour $n \in \mathbb{Z}$. Pour $r = \frac{p}{q}$ avec $q \geq 1$:

$$qf\left(\frac{p}{q}\right) = f\left(q \times \frac{p}{q}\right) = f(p) = pa$$

— d'où $f(r) = \frac{p}{q}a = ra$.

b) Soit x réel et (r_k) une suite de rationnels tendant vers x (densité de $\mathbb{Q}$). Par continuité de f en x :

— $f(x) = \lim f(r_k) = \lim r_k a = xa$.

Réciproquement, $x \mapsto ax$ est bien un morphisme continu : ce sont exactement les **homothéties**.

c) Si $g : \mathbb{R} \to \mathbb{R}_+^*$ est un morphisme continu, $\ln \circ g$ est un morphisme continu de $(\mathbb{R}, +)$ dans lui-même : $\ln g(x) = bx$, soit

$$g(x) = \mathrm{e}^{bx} = c^x \qquad \text{avec } c = g(1) > 0$$

d) Si $h : \mathbb{R}_+^* \to \mathbb{R}$ est un morphisme continu, $h \circ \exp$ est un morphisme continu de $(\mathbb{R}, +)$ dans lui-même : $h(\mathrm{e}^t) = at$, soit $h(y) = a \ln y$.

Bilan : les exponentielles sont les seuls morphismes continus de l'addition vers la multiplication, les logarithmes les seuls dans l'autre sens. **Piège** : sans l'hypothèse de continuité, a) reste vrai mais b) tombe en défaut (il existe, avec l'axiome du choix, des morphismes non linéaires).

Réponse. $f(x) = ax$; morphismes continus $\mathbb{R} \to \mathbb{R}_+^* : x \mapsto c^x$ $(c > 0)$; $\mathbb{R}_+^* \to \mathbb{R} : y \mapsto a \ln y$.

Correction de l'exercice 10 – Le groupe des similitudes directes

a) $s_{a,b} \circ s_{c,d}(z) = a(cz + d) + b$, donc

$$s_{a,b} \circ s_{c,d} = s_{ac,\, ad+b}$$

— $ac \neq 0$: S est stable par composition. $\mathrm{id} = s_{1,0} \in S$.

— $w = az + b \Leftrightarrow z = \frac{1}{a}w - \frac{b}{a}$: $s_{a,b}$ est bijective et $s_{a,b}^{-1} = s_{1/a,\, -b/a} \in S$. C'est un sous-groupe.

b) D'après a), $\varphi(s_{a,b} \circ s_{c,d}) = ac = \varphi(s_{a,b})\varphi(s_{c,d})$. Tout $a \in \mathbb{C}^*$ est atteint $(s_{a,0})$: φ est surjectif.

— $\ker \varphi = \{s_{1,b},\, b \in \mathbb{C}\}$: ce sont les **translations**, qui forment un sous-groupe isomorphe à $(\mathbb{C}, +)$ par $b \mapsto s_{1,b}$.

c) Non : $s_{2,0} \circ s_{1,1} : z \mapsto 2z + 2$ et $s_{1,1} \circ s_{2,0} : z \mapsto 2z + 1$.

d) Une rotation de centre ω et d'angle θ s'écrit $z \mapsto \mathrm{e}^{\mathrm{i}\theta}(z - \omega) + \omega$: c'est un $s_{a,b}$ avec $a = \mathrm{e}^{\mathrm{i}\theta}$. Par b), $\rho \circ \rho' = s_{A,B}$ avec $A = \mathrm{e}^{\mathrm{i}(\theta + \theta')} \neq 1$.

— Un point fixe vérifie $Az + B = z$, soit $z_0 = \frac{B}{1 - A}$: il existe et est unique.

— Alors $s_{A,B}(z) - z_0 = A(z - z_0)$: c'est la **rotation** de centre z_0 et d'angle $\theta + \theta'$.

Lecture : le morphisme φ « oublie » la position et ne garde que l'angle et le rapport ; les angles s'ajoutent quels que soient les centres.

Réponse. $s_{a,b} \circ s_{c,d} = s_{ac,\, ad+b}$; φ surjectif de noyau les translations ; non abélien ; $\rho \circ \rho'$ rotation d'angle $\theta + \theta'$.

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 11 – Isométries du triangle équilatéral

a) Une isométrie conserve les distances ; les sommets sont les seuls points du triangle à distance maximale de O, donc une isométrie qui conserve le triangle (et son centre) envoie un sommet sur un sommet, et bijectivement. La restriction d'une composée est la composée des restrictions :

$$\Phi(g \circ h) = (g \circ h)_{|\{A,B,C\}} = \Phi(g) \circ \Phi(h)$$

b) Si $\Phi(g) = \mathrm{id}$, alors g fixe A, B, C. Une isométrie fixant A et B fixe la droite (AB) point par point, donc c'est l'identité ou la réflexion d'axe (AB) ; cette dernière ne fixe pas C. Donc $g = \mathrm{id}$: $\ker\Phi = \{\mathrm{id}\}$.

c) On dispose de six isométries du triangle :

— l'identité $\mapsto$ id ;

— les rotations de centre O d'angles $\pm\frac{2\pi}{3} \mapsto$ les 3-cycles $(A\ B\ C)$ et $(A\ C\ B)$;

— les réflexions d'axes les médianes (figure) : celle qui passe par A fixe A et échange B et C, d'où $(B\ C)$; de même $(A\ C)$ et $(A\ B)$.

Φ est surjectif, et injectif par b) : c'est un **isomorphisme** $D_3 \simeq S_3$; en particulier $\mathrm{card} D_3 = 3! = 6$.

d) Un isomorphisme conserve la commutativité et les ordres : S_3 n'est pas abélien, D_3 non plus. Les ordres sont ceux des permutations correspondantes :

— id : 1 ; les deux rotations (3-cycles) : 3 ; les trois réflexions (transpositions) : 2.

Remarque : pour le carré, le même morphisme vers S_4 est injectif mais **pas** surjectif ($8 < 24$: une isométrie ne peut pas séparer deux sommets voisins).

Réponse. Φ morphisme injectif et surjectif : $D_3 \simeq S_3$; rotations d'ordre 3, réflexions d'ordre 2 ; non abélien.

Correction de l'exercice 12 – Ordre et morphismes : les morphismes de S3 dans C*

a) $f(x)^m = f(x^m) = f(e) = e'$. Or une puissance vaut le neutre exactement aux multiples de l'ordre :

$$y^m = e' \Leftrightarrow \mathrm{ord}(y) \mid m$$

— donc $\mathrm{ord}\, f(x) \mid m$.

b) Une transposition est d'ordre 2, donc $f(\tau)^2 = 1$ dans $\mathbb{C}^*$: $f(\tau) = \pm 1$.

c) On compose de droite à gauche. Pour $(1\ 2)(2\ 3)(1\ 2)$: $1 \mapsto 2 \mapsto 3 \mapsto 3$, $2 \mapsto 1 \mapsto 1 \mapsto 2$, $3 \mapsto 3 \mapsto 2 \mapsto 1$: c'est $(1\ 3)$. Le second calcul est analogue. Comme $\mathbb{C}^*$ est **commutatif** :

— $f((1\ 3)) = f((1\ 2))\,f((2\ 3))\,f((1\ 2)) = f((1\ 2))^2 f((2\ 3)) = f((2\ 3))$, et de même $f((2\ 3)) = f((1\ 3))$.

d) $(1\ 2)(2\ 3)$: $1 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 3$, $3 \mapsto 2 \mapsto 1$, soit $(1\ 2\ 3)$. Donc $f((1\ 2\ 3)) = \varepsilon^2 = 1$, idem pour $(1\ 3\ 2)$. Tout f est déterminé par $\varepsilon \in \{\pm 1\}$:

— $\varepsilon = 1$: le morphisme **trivial** ;

— $\varepsilon = -1$: $f = -1$ sur les transpositions, $+1$ sur l'identité et les 3-cycles — la **signature**.

e) Un élément non nul de $\mathbb{Z}/3\mathbb{Z}$ est d'ordre 3 ; son image a un ordre qui divise 3 et (Lagrange dans $\mathbb{Z}/4\mathbb{Z}$) divise 4, donc vaut 1. Seul le morphisme **nul** existe (conforme à la formule $3 \wedge 4 = 1$ morphisme).

Réponse. $\mathrm{ord}\, f(x) \mid \mathrm{ord}(x)$; deux morphismes $S_3 \to \mathbb{C}^*$: le trivial et la signature ; aucun morphisme non nul $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$.

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 13 – Le sous-groupe engendré par 2 et 3

a) Par les règles des puissances :

$$\varphi((a,b)+(a',b')) = 2^{a+a'}3^{b+b'} = 2^a3^b \times 2^{a'}3^{b'}$$

b) Si $2^a3^b = 1$, alors $2^a = 3^{-b}$. La valuation 2-adique (exposant de 2, étendue aux rationnels) vaut a à gauche et 0 à droite : $a = 0$. Il reste $3^{-b} = 1$, donc $b = 0$. Ainsi $\ker\varphi = \{(0,0)\}$.

c) L'image de φ est $\{2^a3^b,\ (a,b) \in \mathbb{Z}^2\}$, le plus petit sous-groupe de $\mathbb{Q}^*$ contenant 2 et 3. φ réalise un isomorphisme de $\mathbb{Z}^2$ sur cette image.

d) Supposons $\mathbb{Z}^2 = \langle (p,q)\rangle$. Alors $(1,0) = k(p,q)$ et $(0,1) = l(p,q)$ pour des entiers k, l :

— $kp = 1$ impose $k \neq 0$, puis $kq = 0$ impose $q = 0$; mais alors $lq = 0 \neq 1$. Contradiction.

e) $\left(\frac{3}{2}\right)^k = 2^m$ s'écrit $\varphi(-k-m,k) = \varphi(0,0)$; par injectivité $k = 0$ (et $m = 0$). Aucun empilement de quintes pures ne retombe exactement sur des octaves : c'est le **comma pythagoricien**, que le tempérament égal fait disparaître (voir le cycle des quintes de la plaquette précédente).

— Contrôle numérique : $\left(\frac{3}{2}\right)^{12} \approx 129{,}75$ et $2^7 = 128$, proches mais distincts.

Réponse. φ morphisme injectif : $\langle 2,3\rangle \simeq \mathbb{Z}^2$, non monogène ; $\left(\frac{3}{2}\right)^k = 2^m \Rightarrow k = 0$.

Correction de l'exercice 14 – Puissances dans le groupe des racines de l'unité

a) U_n est un sous-groupe de $\mathbb{C}^*$, et $(zw)^k = z^k w^k$ car la multiplication est commutative. De plus $\left(z^k\right)^n = (z^n)^k = 1$: f_k est à valeurs dans U_n.

b) Si $z^n = 1$ et $z^k = 1$, avec une relation de Bézout $un + vk = d$:

$$z^d = (z^n)^u\left(z^k\right)^v = 1$$

— donc $z \in U_d$. Réciproquement, si $z^d = 1$, comme $d \mid n$ et $d \mid k$, on a $z^n = z^k = 1$. Donc $\ker f_k = U_d$.

c) Avec $\omega = \mathrm{e}^{2\mathrm{i}\pi/n}$, $U_n = \{\omega^j\}$ et $\mathrm{Im}f_k = \{\omega^{jk}\} = \langle\omega^k\rangle$. L'ordre de ω^k est $\frac{n}{d}$ (formule de l'ordre de $\overline{k}$ dans $\mathbb{Z}/n\mathbb{Z} \simeq U_n$). Donc $\mathrm{Im}f_k$ est un sous-groupe à $\frac{n}{d}$ éléments de $\mathbb{C}^*$: c'est $U_{n/d}$ (sous-groupes finis de $\mathbb{C}^*$).

d) f_k est injectif $\Leftrightarrow U_d = \{1\} \Leftrightarrow d = 1$; il est alors bijectif (U_n fini). Condition : $n \wedge k = 1$.

e) $d = 12 \wedge 8 = 4$: $\ker f_8 = U_4 = \{1, \mathrm{i}, -1, -\mathrm{i}\}$ et $\mathrm{Im}f_8 = U_3 = \{1, j, j^2\}$.

— Contrôle : $4 \times 3 = 12$. Par exemple $\left(\mathrm{e}^{\mathrm{i}\pi/6}\right)^8 = \mathrm{e}^{4\mathrm{i}\pi/3} = j^2 \in U_3$.

Réponse. $\ker f_k = U_{n\wedge k}$, $\mathrm{Im}f_k = U_{n/(n\wedge k)}$; automorphisme $\Leftrightarrow n \wedge k = 1$; $n = 12$, $k = 8$: noyau U_4, image U_3.

Correction de l'exercice 15 – Synthèse : les carrés modulo p

a) $f(x) = f(x_0) \Leftrightarrow f\left(x_0^{-1}x\right) = e' \Leftrightarrow x_0^{-1}x \in \ker f \Leftrightarrow x \in x_0\ker f$. La fibre de chaque $y \in \mathrm{Im}f$ a donc $\mathrm{card}(\ker f)$ éléments ($h \mapsto x_0h$ est injectif), et ces fibres partitionnent G :

$$\mathrm{card}G = \mathrm{card}(\ker f) \times \mathrm{card}(\mathrm{Im}f)$$

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).

b) G est commutatif, donc f est un morphisme. $x^2 = \overline{1} \Leftrightarrow (x-\overline{1})(x+\overline{1}) = \overline{0} \Leftrightarrow x = \pm\overline{1}$, car $\mathbb{Z}/p\mathbb{Z}$ est un **corps** (donc intègre). De plus $\overline{1} \neq -\overline{1}$ car $p \neq 2$. Donc $\text{card}(\ker f) = 2$ et, par a),

— il y a $\dfrac{p-1}{2}$ carrés non nuls modulo p.

c) $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16 \equiv 5$, $5^2 = 25 \equiv 3$ (et $(11-x)^2 \equiv x^2$) : les carrés non nuls sont $\{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}$, soit $\dfrac{11-1}{2} = 5$ éléments.

d) Si $x = y^2$ avec $y \neq \overline{0}$, le petit théorème de Fermat (Lagrange dans G d'ordre $p-1$) donne

$$x^{\frac{p-1}{2}} = y^{p-1} = \overline{1}$$

— $p = 11$: $2^5 = 32 = 33 - 1 \equiv -1$, donc $\overline{2}$ n'est **pas** un carré ; $3^5 = 243 = 242 + 1 \equiv 1$, donc $\overline{3}$ en est un ($\overline{3} = \overline{5}^2$, cohérent avec c)).

e) Par le critère, $-\overline{1}$ est un carré $\Leftrightarrow (-1)^{(p-1)/2} = 1 \Leftrightarrow \dfrac{p-1}{2}$ pair $\Leftrightarrow p \equiv 1 \pmod 4$ (dans $\mathbb{Z}/p\mathbb{Z}$, $-\overline{1} \neq \overline{1}$, donc l'égalité est bien une égalité d'entiers ± 1).

— $p = 13 \equiv 1 \pmod 4$: $5^2 = 25 = 26 - 1 \equiv -1 \pmod{13}$ ✓ ; pour $p = 11 \equiv 3 \pmod 4$, $\overline{10} = -\overline{1}$ n'est pas dans la liste de c).

Réponse. $\text{card}G = \text{card}(\ker f) \times \text{card}(\text{Im} f)$; $\dfrac{p-1}{2}$ carrés non nuls ; modulo 11 : $\{1, 3, 4, 5, 9\}$; $\overline{2}$ non carré, $\overline{3}$ carré ; -1 carré $\Leftrightarrow p \equiv 1$ (4).

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).