Corrigé de la Série 1 : Structures algébriques

Groupes, morphismes, groupes cycliques et anneaux

Énoncés et corrigés détaillés

Consigne. Justifier toutes les réponses. Pour les permutations, la composition se lit de droite à gauche. Les anneaux et les sous-anneaux sont unitaires ; un sous-anneau contient l'unité de l'anneau ambiant.

Exercice 1 — Vrai ou faux ?

Pour chaque affirmation, indiquer si elle est vraie ou fausse, puis donner une démonstration ou un contre-exemple.

1) Dans tout groupe, $(ab)^{-1} = a^{-1}b^{-1}$.

2) Un groupe dans lequel $x^2 = e$ pour tout élément x est abélien.

3) La réunion de deux sous-groupes est toujours un sous-groupe.

4) Un morphisme de groupes est injectif si et seulement si son noyau est réduit au neutre.

5) Tout groupe fini d'ordre premier est cyclique.

6) Tout groupe abélien fini est cyclique.

7) Dans tout anneau, $ab = 0$ implique $a = 0$ ou $b = 0$.

8) Tout anneau intègre fini est un corps.

9) $2\mathbb{Z}$ est un sous-anneau unitaire de $\mathbb{Z}$.

10) La classe $\overline{5}$ est inversible dans $\mathbb{Z}/12\mathbb{Z}$.

Correction du vrai/faux

1) **Fausse**. La formule générale est $(ab)^{-1} = b^{-1}a^{-1}$. Dans S_3, prendre $a = (1\ 2)$ et $b = (2\ 3)$: $ab = (1\ 2\ 3)$, alors que $(ab)^{-1} = (1\ 3\ 2) \neq a^{-1}b^{-1} = ab$.

2) **Vraie**. L'hypothèse donne $x^{-1} = x$ pour tout x. Ainsi $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

3) **Fausse**. Dans $(\mathbb{Z}, +)$, $2\mathbb{Z} \cup 3\mathbb{Z}$ contient 2 et 3, mais ne contient pas leur somme 5.

4) **Vraie**. Si f est injectif, $f(x) = e_H = f(e_G)$ impose $x = e_G$. Réciproquement, si $\ker f = \{e_G\}$, alors $f(x) = f(y)$ donne $f(xy^{-1}) = e_H$, d'où $xy^{-1} = e_G$ et $x = y$.

5) **Vraie**. Si $|G| = p$ est premier et $a \neq e$, Lagrange donne $\mathrm{ord}(a) \mid p$. Comme $\mathrm{ord}(a) > 1$, on a $\mathrm{ord}(a) = p$, donc $G = \langle a \rangle$.

6) **Fausse**. Le groupe $(\mathbb{Z}/2\mathbb{Z})^2$ est abélien d'ordre 4, mais chacun de ses éléments vérifie $2x = 0$; aucun n'a ordre 4.

7) **Fausse**. Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{2}\,\overline{3} = \overline{0}$ alors que les deux facteurs sont non nuls.

8) **Vraie**. Pour $a \neq 0$, l'application $x \mapsto ax$ est injective par intégrité, donc surjective puisque l'anneau est fini. Il existe b avec $ab = 1$. La commutativité donne $ba = 1$.

9) **Fausse**. L'ensemble $2\mathbb{Z}$ ne contient pas 1, l'unité de $\mathbb{Z}$.

10) **Vraie**. On a $5 \times 5 = 25 \equiv 1 \pmod{12}$; ainsi $\overline{5}^{-1} = \overline{5}$.

Exercice 2 — Une loi de groupe sur $\mathbb{R} \setminus \{-1\}$

On pose $E = \mathbb{R} \setminus \{-1\}$ et, pour $x, y \in E$,

$$x \star y = x + y + xy.$$

1) Vérifier que $\star$ est une loi interne sur E.

2) Montrer qu'elle est associative et commutative.

3) Déterminer son neutre et le symétrique de chaque $x \in E$. En déduire que $(E, \star)$ est un groupe abélien.

4) Montrer que $\varphi : E \to \mathbb{R}^*$, $\varphi(x) = 1 + x$, est un isomorphisme vers $(\mathbb{R}^*, \times)$.

5) Résoudre $2 \star x = 5$ dans E.

1) Stabilité

L'identité

$$1 + (x \star y) = (1 + x)(1 + y)$$

est fondamentale. Puisque $x, y \neq -1$, le produit de droite est non nul ; donc $x \star y \neq -1$ et $x \star y \in E$.

2) Propriétés de la loi

La commutativité résulte de $x + y + xy = y + x + yx$. De plus,

$$(x \star y) \star z = x + y + z + xy + xz + yz + xyz = x \star (y \star z).$$

La loi est donc associative.

3) Neutre et symétrique

Pour tout $x \in E$, $x \star 0 = 0 \star x = x$; le neutre est 0. L'équation $x \star y = 0$ devient $(1 + x)y = -x$, donc

$$\boxed{y = -\frac{x}{1 + x}.}$$

Ce réel appartient à E, car $1 + y = 1/(1 + x) \neq 0$. Par commutativité, il est un symétrique des deux côtés. Tous les axiomes d'un groupe abélien sont vérifiés.

4) Isomorphisme

On a $\varphi(x \star y) = \varphi(x)\varphi(y)$. L'application est bijective, de réciproque $u \mapsto u - 1$ sur $\mathbb{R}^*$. C'est donc un isomorphisme de groupes.

5) Résolution

$2 \star x = 5$ équivaut à $2 + 3x = 5$, d'où $\boxed{x = 1}$, qui appartient bien à E.

Exercice 3 — Sous-groupes de $\mathbb{Z}$: intersection, somme et réunion

Dans le groupe $(\mathbb{Z}, +)$, on considère $H = 6\mathbb{Z}$ et $K = 10\mathbb{Z}$.

1) Vérifier que H et K sont des sous-groupes de $\mathbb{Z}$.

2) Déterminer $H \cap K$.

3) On pose $H + K = \{h + k : h \in H,\ k \in K\}$. Montrer que $H + K = 2\mathbb{Z}$.

4) La réunion $H \cup K$ est-elle un sous-groupe ?

5) Déterminer le sous-groupe $\langle 6, 10\rangle$ engendré par 6 et 10.

1) Critère de sous-groupe

$0 \in H$ et, si $x = 6a$, $y = 6b$, alors $x - y = 6(a - b) \in H$. Le critère additif montre que $H \leq \mathbb{Z}$. Le même raisonnement vaut pour K.

2) Intersection

Un entier est dans $H \cap K$ si et seulement s'il est divisible par 6 et 10, donc par leur ppcm, égal à 30. Ainsi $\boxed{H \cap K = 30\mathbb{Z}}$.

3) Somme

Tout entier $6a + 10b$ est pair, donc $H + K \subset 2\mathbb{Z}$. Inversement, $2 = 2 \cdot 6 - 10$, si bien que, pour tout $r \in \mathbb{Z}$,

$$2r = 6(2r) + 10(-r) \in H + K.$$

D'où $\boxed{H + K = 2\mathbb{Z}}$, qui est en particulier un sous-groupe.

4) Réunion

Les entiers 6 et 10 sont dans $H \cup K$, mais 16 n'est divisible ni par 6 ni par 10. La réunion n'est donc pas stable par addition.

5) Sous-groupe engendré

Le sous-groupe $2\mathbb{Z}$ contient 6 et 10, donc $\langle 6, 10\rangle \subset 2\mathbb{Z}$. Tout sous-groupe contenant 6 et 10 contient $2 = 2 \cdot 6 - 10$, puis tous ses multiples. Par conséquent, $\boxed{\langle 6, 10\rangle = 2\mathbb{Z}}$.

Exercice 4 — Un morphisme entre deux groupes de classes

On note $[x]_n$ la classe de l'entier x modulo n et l'on considère

$$f : (\mathbb{Z}/12\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/8\mathbb{Z}, +), \qquad f([x]_{12}) = [2x]_8.$$

1) Montrer que f est bien définie et que c'est un morphisme de groupes.

2) Déterminer $\ker f$ et $\operatorname{Im} f$.

3) Le morphisme est-il injectif ? surjectif ? Vérifier $|\mathbb{Z}/12\mathbb{Z}| = |\ker f|\,|\operatorname{Im} f|$.

4) Résoudre $f([x]_{12}) = [6]_8$, puis $f([x]_{12}) = [1]_8$.

1) Indépendance du représentant et additivité

Si $[x]_{12} = [y]_{12}$, alors $x - y = 12k$, d'où $2x - 2y = 24k$, multiple de 8. Ainsi $[2x]_8 = [2y]_8$ et f est bien définie. De plus,

$$f([x]_{12} + [y]_{12}) = [2(x + y)]_8 = [2x]_8 + [2y]_8.$$

2) Noyau et image

On a

$$f([x]_{12}) = [0]_8 \iff 8 \mid 2x \iff 4 \mid x.$$

Par conséquent,

$$\boxed{\ker f = \{[0]_{12}, [4]_{12}, [8]_{12}\}.}$$

Les images sont des classes paires modulo 8 ; chacune est atteinte en prenant $x = 0, 1, 2, 3$. Ainsi

$$\boxed{\operatorname{Im} f = \{[0]_8, [2]_8, [4]_8, [6]_8\}.}$$

3) Injectivité et surjectivité

Le noyau contient trois éléments, donc f n'est pas injectif. L'image ne contient pas $[1]_8$, donc f n'est pas surjectif. Les cardinaux vérifient bien $12 = 3 \times 4$.

4) Antécédents

$2x \equiv 6 \pmod 8$ équivaut à $x \equiv 3 \pmod 4$; les solutions dans $\mathbb{Z}/12\mathbb{Z}$ sont

$$\boxed{[3]_{12},\ [7]_{12},\ [11]_{12}.}$$

La classe $[1]_8$ n'appartient pas à l'image : la seconde équation n'a aucune solution.

Exercice 5 — Racines de l'unité, groupes cycliques et Lagrange

On pose $\zeta = e^{2\pi i/12}$ et $U_{12} = \{z \in \mathbb{C} : z^{12} = 1\}$.

1) Montrer que U_{12} est un sous-groupe de $(\mathbb{C}^*, \times)$ et que $U_{12} = \langle \zeta \rangle$ est d'ordre 12.

2) Établir $\operatorname{ord}(\zeta^k) = 12/\operatorname{pgcd}(12, k)$ pour tout entier k.

3) Déterminer tous les générateurs de U_{12}, puis les ordres de ζ^3, ζ^4 et ζ^8.

4) Pour chaque diviseur positif d de 12, montrer qu'il existe un unique sous-groupe d'ordre d, à savoir $\langle \zeta^{12/d} \rangle$.

5) Résoudre $z^4 = 1$ dans U_{12}.

1) Structure cyclique

$1 \in U_{12}$ et, pour $z, w \in U_{12}$, $(zw^{-1})^{12} = z^{12}/w^{12} = 1$. Le critère de sous-groupe s'applique. Les douze racines sont les nombres ζ^k pour $0 \le k \le 11$. Ils sont distincts car $\zeta^k = \zeta^\ell$ équivaut à $12 \mid (k - \ell)$. Ainsi $U_{12} = \langle \zeta \rangle$ et $|U_{12}| = 12$.

2) Ordre d'une puissance

Posons $g = \operatorname{pgcd}(12, k)$, $12 = gn$ et $k = gq$, avec $\operatorname{pgcd}(n, q) = 1$. Pour $m \ge 1$,

$$(\zeta^k)^m = 1 \iff 12 \mid km \iff n \mid qm \iff n \mid m.$$

Le plus petit entier positif possible est donc $n = 12/g$.

3) Générateurs et ordres

Un élément engendre U_{12} si et seulement si son ordre est 12. Les exposants premiers à 12 donnent

$$\boxed{\zeta,\ \zeta^5,\ \zeta^7,\ \zeta^{11}.}$$

La formule précédente donne

$$\boxed{\operatorname{ord}(\zeta^3) = 4, \qquad \operatorname{ord}(\zeta^4) = 3, \qquad \operatorname{ord}(\zeta^8) = 3.}$$

4) Sous-groupes

D'après Lagrange, l'ordre d'un sous-groupe divise 12. Pour $d \mid 12$, l'élément $\zeta^{12/d}$ a ordre d, donc le sous-groupe $H_d = \langle \zeta^{12/d} \rangle$ a bien d éléments. Si H est un sous-groupe d'ordre d, Lagrange appliqué à H donne $z^d = 1$ pour tout $z \in H$. En écrivant $z = \zeta^k$, on obtient $12 \mid kd$, c'est-à-dire $(12/d) \mid k$. Donc $H \subset H_d$. Comme leurs cardinaux sont égaux, $H = H_d$: l'unicité est démontrée.

d	1	2	3	4	6	12
H_d	$\{1\}$	$\langle \zeta^6 \rangle$	$\langle \zeta^4 \rangle$	$\langle \zeta^3 \rangle$	$\langle \zeta^2 \rangle$	$\langle \zeta \rangle$

5) Une équation dans le groupe

Pour $z = \zeta^k$, $z^4 = 1$ équivaut à $12 \mid 4k$, donc à $3 \mid k$. Ainsi $\boxed{z \in \{1, i, -1, -i\} = \langle \zeta^3 \rangle}$.

Exercice 6 — Calculs dans le groupe des permutations S_3

On pose $\sigma = (1\ 2\ 3)$ et $\tau = (1\ 2)$.

1) Calculer σ^2, σ^{-1}, τ^{-1}, $\sigma\tau$ et $\tau\sigma$. Le groupe S_3 est-il abélien ?

2) Déterminer les ordres et les signatures de σ et τ.

3) Montrer que $\langle \sigma, \tau \rangle = S_3$.

4) Déterminer le sous-groupe alterné A_3 et calculer $\tau\sigma\tau^{-1}$.

5) Résoudre $\sigma x = \tau$ dans S_3.

1) Produits et inverses

En suivant les images de 1, 2, 3, on trouve

$$\sigma^2 = (1\ 3\ 2) = \sigma^{-1}, \qquad \tau^{-1} = \tau,$$

$$\boxed{\sigma\tau = (1\ 3), \qquad \tau\sigma = (2\ 3).}$$

Les deux produits sont différents, donc S_3 n'est pas abélien.

2) Ordres et signatures

Un cycle de longueur r a ordre r et signature $(-1)^{r-1}$. Ainsi

$$\operatorname{ord}(\sigma) = 3, \quad \operatorname{ord}(\tau) = 2, \qquad \operatorname{sgn}(\sigma) = 1, \quad \operatorname{sgn}(\tau) = -1.$$

3) Générateurs de S_3

Le sous-groupe engendré contient les six permutations distinctes

$$\mathrm{id}, \quad \sigma, \quad \sigma^2, \quad \tau, \quad \sigma\tau = (1\ 3), \quad \tau\sigma = (2\ 3).$$

Comme $|S_3| = 3! = 6$, ces éléments constituent tout S_3.

4) Permutations paires et conjugaison

Les permutations paires sont l'identité et les deux cycles de longueur 3 :

$$\boxed{A_3 = \{\mathrm{id}, \sigma, \sigma^2\} = \langle \sigma \rangle.}$$

La conjugaison remplace les entrées du cycle par leurs images sous τ :

$$\tau\sigma\tau^{-1} = (\tau(1)\ \tau(2)\ \tau(3)) = (2\ 1\ 3) = (1\ 3\ 2) = \sigma^{-1}.$$

5) Équation

En multipliant à gauche par σ^{-1}, on obtient l'unique solution

$$\boxed{x = \sigma^{-1}\tau = \sigma^2\tau = (2\ 3).}$$

Exercice 7 — Un sous-anneau de $\mathbb{R}$ et ses éléments inversibles

On admet que $\sqrt{2}$ est irrationnel et l'on considère

$$A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}.$$

1) Montrer que l'écriture $a + b\sqrt{2}$ est unique.

2) Montrer que A est un sous-anneau unitaire de $\mathbb{R}$.

3) L'anneau A est-il intègre ? Est-ce un corps ?

4) Montrer que $s : A \to A$, $s(a + b\sqrt{2}) = a - b\sqrt{2}$, est un automorphisme d'anneaux.

5) Montrer que $a + b\sqrt{2}$ est inversible dans A si et seulement si $a^2 - 2b^2 \in \{-1, 1\}$. En déduire les inverses de $1 + \sqrt{2}$ et $3 + 2\sqrt{2}$.

1) Unicité

Si $a + b\sqrt{2} = c + d\sqrt{2}$ et $b \neq d$, alors $\sqrt{2} = (c - a)/(b - d) \in \mathbb{Q}$, contradiction. Donc $b = d$, puis $a = c$.

2) Critère de sous-anneau

On a $1 = 1 + 0\sqrt{2} \in A$. Pour $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$,

$$x - y = (a - c) + (b - d)\sqrt{2} \in A,$$

$$xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in A.$$

Le critère de sous-anneau unitaire est vérifié.

3) Intégrité et propriété de corps

L'anneau A est commutatif, non nul et inclus dans le corps $\mathbb{R}$. Si $xy = 0$ dans A, la même égalité dans $\mathbb{R}$ impose $x = 0$ ou $y = 0$; A est donc intègre. Il n'est pas un corps : l'inverse réel de 2 est $1/2$, qui n'appartient pas à A. En effet, $1/2 = a + b\sqrt{2}$ impose $b = 0$ par irrationalité, puis $a = 1/2 \notin \mathbb{Z}$.

4) Conjugaison

L'unicité de l'écriture rend s bien définie. On vérifie $s(1) = 1$, $s(x + y) = s(x) + s(y)$ et, grâce à la formule du produit,

$$s(xy) = (ac + 2bd) - (ad + bc)\sqrt{2} = s(x)s(y).$$

Enfin $s(s(x)) = x$, donc s est bijective : c'est un automorphisme.

5) Critère d'inversibilité

Pour $x = a + b\sqrt{2}$, on a $xs(x) = a^2 - 2b^2 \in \mathbb{Z}$. Si $xy = 1$ avec $y = c + d\sqrt{2} \in A$, alors

$$(a^2 - 2b^2)(c^2 - 2d^2) = xs(x)ys(y) = (xy)s(xy) = 1.$$

Ces deux facteurs étant entiers, chacun vaut 1 ou -1. Réciproquement, si $a^2 - 2b^2 = \varepsilon \in \{-1, 1\}$, alors

$$x(\varepsilon(a - b\sqrt{2})) = \varepsilon^2 = 1.$$

L'inverse appartient donc à A. En particulier,

$$\boxed{(1+\sqrt{2})^{-1} = \sqrt{2} - 1, \qquad (3+2\sqrt{2})^{-1} = 3 - 2\sqrt{2}.}$$

Exercice 8 — L'anneau $\mathbb{Z}/12\mathbb{Z}$: unités et équations

Dans cet exercice, $\overline{a}$ désigne la classe de a modulo 12.

1) Déterminer les éléments inversibles de $\mathbb{Z}/12\mathbb{Z}$ et leurs inverses. Le groupe multiplicatif des inversibles est-il cyclique ?

2) Déterminer les diviseurs de zéro non nuls. L'anneau est-il intègre ? Est-ce un corps ?

3) Résoudre $\overline{8}\,x = \overline{4}$, puis $\overline{8}\,x = \overline{3}$.

4) Résoudre $x^2 = \overline{1}$ et $x^2 = x$ dans $\mathbb{Z}/12\mathbb{Z}$.

5) Résoudre dans $\mathbb{Z}$ le système $u \equiv 2 \pmod 3$, $u \equiv 3 \pmod 4$.

1) Groupe des unités

La classe $\overline{a}$ est inversible si et seulement si $\gcd(a, 12) = 1$. Ainsi

$$\boxed{(\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}.}$$

Les carrés de ces quatre classes valent $\overline{1}$: les représentants ont pour carrés 1, 25, 49 et 121, tous congrus à 1 modulo 12. Chaque unité est donc son propre inverse. Le groupe a quatre éléments mais aucun d'ordre 4 ; il n'est pas cyclique.

2) Diviseurs de zéro

Les classes non nulles restantes sont

$$\boxed{\overline{2},\ \overline{3},\ \overline{4},\ \overline{6},\ \overline{8},\ \overline{9},\ \overline{10}.}$$

Chacune est un diviseur de zéro, comme le montrent

$$\overline{2}\,\overline{6} = \overline{3}\,\overline{4} = \overline{8}\,\overline{3} = \overline{9}\,\overline{4} = \overline{10}\,\overline{6} = \overline{0}.$$

Les classes $\overline{4}$ et $\overline{6}$ figurent aussi dans ces produits de deux facteurs non nuls. Aucune unité ne peut être un diviseur de zéro : on pourrait sinon multiplier un produit nul par son inverse. L'anneau n'est donc ni intègre ni un corps.

3) Équations du premier degré

En écrivant $x = \overline{a}$, on obtient

$$8a \equiv 4 \pmod{12} \iff 12 \mid (8a-4) \iff 3 \mid (2a-1) \iff a \equiv 2 \pmod 3.$$

Donc

$$\boxed{x \in \{\overline{2}, \overline{5}, \overline{8}, \overline{11}\}.}$$

Il ne faut pas conserver le module 12 après division par 4. L'équation $8a \equiv 3 \pmod{12}$ n'a pas de solution : elle donnerait $8a - 12k = 3$, impossible puisque le membre de gauche est divisible par 4.

4) Deux équations du second degré

Si $x^2 = \overline{1}$, x est inversible d'inverse x. D'après la première question, les solutions sont exactement

$$\boxed{x \in \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}.}$$

Pour $x^2 = x$, un calcul des douze classes donne :

a	0	1	2	3	4	5	6	7	8	9	10	11
$a^2 - a \pmod{12}$	0	0	2	6	0	8	6	6	8	0	6	2

Ainsi $\boxed{x \in \{\overline{0}, \overline{1}, \overline{4}, \overline{9}\}}$. On ne peut pas déduire de $x(x - \overline{1}) = \overline{0}$ que $x = \overline{0}$ ou $x = \overline{1}$, car l'anneau n'est pas intègre.

5) Deux congruences simultanées

Écrivons $u = 3 + 4k$. La condition modulo 3 devient $k \equiv 2 \pmod 3$. Donc $k = 2 + 3t$, avec $t \in \mathbb{Z}$, et

$$\boxed{u = 11 + 12t, \quad t \in \mathbb{Z}.}$$

Ces entiers vérifient les deux congruences. On retrouve l'unicité de la classe solution modulo 12, annoncée par le théorème chinois puisque $\text{pgcd}(3, 4) = 1$.