ALGÈBRE GÉNÉRALE

DOSSIER D'EXERCICES (1)

Thème : théorie des groupes

1 Soit $(G,*)$ un groupe et f une bijection de G dans G. On définit une nouvelle loi interne sur G, notée $*_f$, définie par la relation

$$a *_f b = f^{-1}(f(a) * f(b)).$$

Montrer que $(G,*_f)$ est un groupe.

---

2 On note $\mathcal{A}$ l'ensemble des applications affines non constantes de $\mathbb{R}$ dans $\mathbb{R}$, autrement dit,

$$\mathcal{A} = \left\{ f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & ax+b \end{array} : a \in \mathbb{R}^\star, b \in \mathbb{R} \right\}.$$

Montrer que la loi de composition des fonctions est une loi interne sur $\mathcal{A}$ et que $(\mathcal{A},\circ)$ est un groupe. Le groupe $(\mathcal{A},\circ)$ est-il commutatif?

Montrer que l'ensemble $\mathcal{H}$ formé des éléments $f \in \mathcal{A}$ tels que $|f(x) - f(y)| = |x - y|$ pour tous $x,y \in \mathbb{R}$ forme un sous-groupe de $\mathcal{A}$. En préciser les éléments.

---

3 Soit G un sous-ensemble non vide, fini de $\mathbf{GL}_n$. Montrer que les assertions suivantes sont équivalentes :

(1) G est un sous-groupe de $\mathbf{GL}_n$,

(2) G est stable pour la multiplication des matrices.

4

a — [Etude du *groupe diédral* $\mathbf{D}_3$].

Dans le plan euclidien P on place les points M_j, $j = 0,1,2$ d'affixe respectif $z_i = \exp(2ij\pi/3)$. Ce sont les sommets d'un triangle équilatéral. On note $T = \{M_0,M_1,M_2\}$ et on appelle $\mathbf{D}_3$ l'ensemble des isométries du plan qui conservent T :

$$\mathbf{D}_3 =_{def} \{f \in \mathbf{Is}(P) : f(T) = T\}.$$

i) Montrer que $\mathbf{D}_3$ est un sous-groupe de $(\mathbf{Is}(P),\circ)$.

ii) Montrer que $\mathbf{D}_3$ est formé de 6 éléments. Donner deux éléments a et b tels que $\mathbf{D}_3 = \langle a,b \rangle$.

iii) Faire une table de $\mathbf{D}_3$. (C'est un tableau à double entrée, avec la liste des éléments de D_3 et leur produit — comme dans une table de multiplication élémentaire.)

b — [Etude du *groupe diédral* $\mathbf{D}_4$]

On considère maintenant les points N_j, $j = 0,1,2,3$ d'affixe respectif $z_i = \exp(2ij\pi/4)$. Ce sont les sommets d'un carré. On note $C = \{N_0,N_1,N_2,N_3\}$ et on appelle $\mathbf{D}_4$ l'ensemble des isométries du plan qui conservent C :

$$\mathbf{D}_4 =_{def} \{f \in \mathbf{Is}(P) : f(C) = C\}.$$

i) Montrer que $\mathbf{D}_4$ est un sous-groupe de $(\mathbf{Is}(P),\circ)$.

ii) Montrer que $\mathbf{D}_4$ est formé de 8 éléments. Donner deux éléments a et b tels que $\mathbf{D}_4 = \langle a,b \rangle$.

iii) Faire une table de $\mathbf{D}_4$.

Pour aller plus loin → Plus généralement, si P_n désigne le polygone régulier à n sommets, d'affixes respectifs $z_j = \exp(2ij\pi/n)$, $j = 0,\ldots,n-1$, on appelle $\mathbf{D}_n$ le sous-groupe de $\mathbf{Is}(P)$ formé des isométries qui laissent P_n *globalement* invariant. $\mathbf{D}_n$ contient $2n$ éléments, il est engendré par une rotation a d'ordre n et une réflexion b vérifiant $abab = e$. (e est l'isométrie identique.)

---

5 Soit $(G,*)$ un groupe. On définit le sous-ensemble $Z(G)$ par

$$Z(G) = \{u \in G : gu = ug \text{ pour tout } g \in G\}$$

Autrement dit, u est un élément de $Z(G)$ s'il commute avec *tous* les éléments de G.

a — Montrer que $Z(G)$ est un sous-groupe de G. (On l'appelle *le centre* de G.) A quelle(s) condition(s) a-t-on G=Z(G)?

b — Dans cette partie, on cherche $Z(\mathbf{GL}_2(\mathbb{R}))$.

i) Soit

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(\mathbf{GL}_2(\mathbb{R})).$$

En utilisant le fait que A commute avec les matrices J et K données par

$$I = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

montrer qu'on a nécessairement $a = d$ et $b = 0 = c$.

ii) En déduire $Z(\mathbf{GL}_2(\mathbb{R}))$.

c — Déterminer les centres des groupes *diédraux* $\mathbf{D}_3$ et $\mathbf{D}_4$.

d — Montrer que si ϕ est un isomorphisme de $(G,*)$ sur $(G',.)$ alors $\phi(Z(G)) = Z(G')$.

Pour aller plus loin → Déterminer, par exemple en utilisant une récurrence, le centre de $\mathbf{GL}_n(\mathbb{R})$.

---

6 Déterminer le sous-groupe de $\mathbf{GL}_2$ engendré par $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

---

7 Déterminer le sous-groupe de $\mathbf{GL}_2$ engendré par les matrices $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

---

8 On rappelle que $\mathbb{Z}^2 = \{(n,m) : n \in \mathbb{Z}, m \in \mathbb{Z}\}$ et que $(\mathbb{Z}^2,+)$ est un groupe avec $(n_1,m_1) + (n_2,m_2) = (n_1 + n_2, m_1 + m_2)$. Trouver une condition nécessaire et suffisante sur les éléments $a = (a_1,a_2)$ et $b = (b_1,b_2)$ pour que $\mathbb{Z}^2 = \langle a,b\rangle$. Donner une méthode générale pour construire de tels éléments.

---

9 Montrer que si m et n sont premiers entre eux alors $\mathbf{U}_{nm} \simeq \mathbf{U}_n \times \mathbf{U}_m$. Le résultat demeure-t-il si m et n ne sont plus supposés premiers entre eux?

---

10 Soient A et B deux groupes et $G = A \times B$ le produit (direct) de ces deux groupes. On considère A_1 un sous-groupe distingué de A et B_1 un sous-groupe distingué de B.

a — Montrer que $A_1 \times B_1$ est un sous-groupe distingué de G.

b — Montrer en utilisant un morphisme bien choisi que

$$G/(A_1 \times B_1) \simeq (A/A_1) \times (B/B_1).$$

c — Est-il légitime d'écrire $G/A \simeq B$?

---

11 Montrer que $\mathbf{S}_3 \simeq \mathbf{D}_3$. A-t-on $\mathbf{S}_4 \simeq \mathbf{D}_4$?

---

12 Dans $\mathbf{S}_9$ on considère les permutations σ_1 et σ_2 suivantes :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 6 & 8 & 5 & 4 & 3 & 7 & 1 & 9 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 2 & 4 & 5 & 7 & 6 & 9 & 1 \end{pmatrix}$$

a — Décomposer chacune des permutations en produit de cycles, calculer leur ordre et leur signature.

b — calculer σ_1^{50} et σ_2^{121}.

---

13 [Générateurs des groupes symétriques et alternés]
Soit $n \geq 2$.

a — Montrer que tout cycle $(a_1,a_2,\cdots,a_p)$ $(p \geq 2)$ s'écrit comme un produit de transpositions.

b — Montrer que toute permuation (i,j) avec $i < j$ vérifie

$$(i,j) = (i,i+1)(i+1,i+2)\cdots(j-1,j)(j-2,j-1)(j-3,j-2)\cdots(i,i+1).$$

c — Montrer que

$$(k,k+1) = (1,k)(1,k+1)(1,k).$$

d — Montrer les égalités suivantes

(1) $\mathbf{S}_n = \langle (1,2),(1,3),\ldots,(1,n) \rangle$.

(2) $\mathbf{S}_n = \langle (1,2),(1,2,\ldots,n) \rangle$

Indication : Posant $\sigma = (1,2,\ldots,n)$, on pourra montrer que

$$\sigma^k(12)\sigma^{-k} = (k+1,k+2).$$

e — Soit $n \geq 3$. Montrer que $(a,b)(a,c) = (a,c,b)$ et $(a,b)(c,d) = (a,c,b)(a,c,d)$. En déduire

(3) $\mathbf{A}_n$ est engendré par l'ensemble des 3-cycles.

---

14 Montrer que pour tout $n \geq 2$ on a $\mathbf{S}_n/\mathbf{A}_n \simeq \mathbb{Z}/2\mathbb{Z}$.

---

15 [Le théorème de Cayley] Soit $(G,*)$ un groupe à n éléments, $G = \{a_1,\ldots,a_n\}$. Pour tout $a \in G$, on définit l'application σ_a de $\{1,\ldots,n\}$ dans lui-même par la relation

$$\sigma_a(i) = j \iff a * a_i = a_j.$$

a — Montrer que $\sigma_a \in \mathbf{S}_n$.

b — Dans cette partie, on prend $(G,*) = (\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}, \bar{+})$ dont les quatre éléments sont $a_1 = (\bar{0},\bar{0})$, $a_2 = (\bar{1},\bar{0})$, $a_3 = (\bar{0},\bar{1})$ et $a_4 = (\bar{1},\bar{1})$. Déterminer σ_a pour tout $a \in G$.

c — Montrer dans le cas général que l'application $\Sigma : (G,*) \to (\mathbf{S}_n,\cdot)$ définie par $\Sigma(a) = \sigma_a$ est un morphisme de groupe.

d — En déduire que tout groupe d'ordre n est isomorphe à un sous-groupe de $\mathbf{S}_n$.

Thème : Anneaux et corps

16 Soient $a < b$ deux réels I, on note $C([a,b])$ l'ensemble des fonctions continues sur $[a,b]$.

a — Expliquer (rapidement) pourquoi $(C([a,b]), +, \cdot)$ est un anneau commutatif unitaire. Est-il intègre ?

b — Déterminer le groupe des éléments inversibles $C([a,b])^*$.

c — Démontrer que $C([a,b]) \simeq C([0,1])$.

---

17 Soit p un nombre premier. Montrer que $\mathbb{Q}_p$ est un sous-anneau de $(\mathbb{Q}, +, \cdot)$. On rappelle que $\mathbb{Q}_p =_{def} \left\{ \frac{m}{p^n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\}$. Déterminer $(\mathbb{Q}_p)^*$.

---

18 On définit $\mathbb{Z}[i] =_{def} \{m + in : m,n \in \mathbb{Z}\} \subset \mathbb{C}$.

a — Montrer que $(\mathbb{Z}[i], +, \cdot)$ est un anneau commutatif unitaire (on montrera que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \cdot)$).

b — On définit sur $\mathbb{Z}[i]$ l'application N par $N(n+im) = n^2 + m^2$. Montrer que pour tous α et β dans $\mathbb{Z}[i]$, on a $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$. Montrer que si α est inversible alors $N(\alpha) = 1$ en déduire $(\mathbb{Z}[i])^*$, le groupe des éléments inversibles de $\mathbb{Z}[i]$. A quel groupe déjà rencontré $((\mathbb{Z}[i])^*, \cdot)$ est-il isomorphe ?

---

19 Soit $d \in \mathbb{Z}$ tel que $\sqrt{|d|} \notin \mathbb{Q}$. Lorsque $d < 0$ on pose $\sqrt{d} =_{def} i\sqrt{|d|}$. On définit $\mathbb{Q}(\sqrt{d})$ par

$$\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} : x,y \in \mathbb{Q}\}.$$

a — Montrer que $\mathbb{Q}(\sqrt{d})$ est un sous-corps de $\mathbb{C}$.

b — Déterminer tous les isomorphismes f de $\mathbb{Q}(\sqrt{d})$ qui coïncident avec l'identité sur $\mathbb{Q}$, autrement dit tels que $f(x) = x$ pour tout $x \in \mathbb{Q}$.

c — Justifier l'assertion suivante : $\mathbb{Q}(\sqrt{d})$ *est le plus petit sous-corps de* $\mathbb{C}$ *qui contienne à la fois* $\mathbb{Q}$ *et* $\sqrt{d}$.

d — Les corps $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{5})$ sont-ils isomorphes ?

---

20 Soient $(A, +, \cdot)$ un anneau commutatif unitaire et I un idéal de A. Montrer que si $I \cap A^* \neq \emptyset$ alors $I = A$.

---

21 Soient $(A, +, \cdot)$ et $(B, +, \cdot)$ deux anneaux commutatifs (unitaires) et $\phi : A \to B$ un morphisme d'anneaux. Est-il vrai que si I est un idéal de A alors $\phi(I)$ est un idéal de B ? Est-il vrai que si J est un idéal de B alors $\phi^{-1}(J)$ est un idéal de A ?

---

22 Soit $(A, +, \cdot)$ un anneau commutatif unitaire et I un idéal de A. le radical de I, noté $\sqrt{I}$ est défini par

$$a \in \sqrt{I} \iff {}_{def}\text{il existe } m \in \mathbb{N}^\star \text{ tel que } a^m \in I$$

a — Montrer que $\sqrt{I}$ est un idéal de A. (On utilisera convenablement la formule du binôme de Newton.)

b — On prend $A = \mathbb{Z}$ et $I = 36\mathbb{Z}$. Déterminer $\sqrt{I}$. Plus généralement, comment peut-on déterminer $\sqrt{m\mathbb{Z}}$ pour tout $m \in \mathbb{Z}$?

---

23 Soit $a \in \mathbb{Z}$. Résoudre le système suivant dans $\mathbb{Z}/7\mathbb{Z}$ en fonction du paramètre $\overline{a}$.

$$\begin{cases} \overline{1}x & + & \overline{3}y & = & \overline{1} \\ \overline{2}x & + & \overline{a}y & = & \overline{6} \end{cases}.$$

24 Soit p un nombre premier > 1.

a — Montrer que pour $k = 1, \ldots, p-1$, C_p^k est divisible par p.

b — Montrer que pour tous x,$y \in \mathbb{Z}/p\mathbb{Z}$ on a $(x+y)^p = x^p + y^p$.

---

25 Soit $m \in \mathbb{N}/\{0,1\}$. Montrer que $\overline{r} \in (\mathbb{Z}/m\mathbb{Z})^*$ si et seulement si m et r sont premiers entre eux. On note $\phi(m)$ le cardinal de $(\mathbb{Z}/m\mathbb{Z})^*$. Calculer $\phi(m)$ pour $m = 2,3,4,5,6$. Que vaut $\phi(p)$ lorsque p est un nombre premier ? Que vaut $\phi(m)$ lorsque $m = p^s$ avec p premier ?

Remarque. L'application ϕ s'appelle l'indicatrice d'Euler.

Pour aller plus loin → Déduire une généralisation du petit théorème de Fermat qui fasse intervenir la fonction ϕ.

26

a — Soient $(A, \oplus_A, \odot_A)$ et $(B, \oplus_B, \odot_B)$ deux anneaux commutatifs unitaires. On définit sur $A \times B$ les lois $+$ et $\cdot$ de la manière suivante

$$(a,b) + (a',b') = (a \oplus_A a', b \oplus_B b') \quad \text{et} \quad (a,b).(a',b') = (a \odot_A a', b \odot_B b').$$

1) Montrer que $(A \times B, +, \cdot)$ est un anneau commutatif unitaire. Est-il intègre ?

2) Déterminer les éléments inversibles de $A \times B$ en fonction des éléments inversibles de A et de B.

b — Dans cette partie on prend $A = \frac{\mathbb{Z}}{m\mathbb{Z}}$ et $B = \frac{\mathbb{Z}}{n\mathbb{Z}}$ où m et n sont deux entiers premiers entre eux.

1) Montrer que l'application f ci-dessous est bien définie :

$$f : \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \mathbf{cl}_{mn}(a) & \longmapsto & (\mathbf{cl}_m(a), \mathbf{cl}_n(a)) \end{array}$$

où on utilise la notation $\mathbf{cl}_s(a)$ pour représenter la classe de a dans $\mathbb{Z}/s\mathbb{Z}$.

2) L'application f est-elle un isomorphisme d'anneau ?

3) Utiliser f, la partie a — et l'exercice précédent pour démontrer que lorsque m et n sont premiers entre eux on a $\phi(mn) = \phi(m)\phi(n)$.

4) En déduire, en utilisant l'exercice précédent, une formule générale pour le calcul de $\phi(m)$, m entier positif quelconque.

27

a — On travaille avec $(\mathbb{R}[X], +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ et on considère l'application

$$f : \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ P & \longmapsto & P(i) \end{array}$$

où i désigne le nombre complexe habituel. Montrer que f est un morphisme d'anneau. Déterminer l'idéal $\ker f$.

b — En déduire $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$.

c — Que peut-on dire de $\mathbb{Q}[X]/(X^2+1)$?

d — Pouvez-vous trouver un anneau quotient qui soit isomorphe au corps $\mathbb{Q}(\sqrt{d})$?

e — Soit $P \in \mathbb{R}[X]$. On considère l'idéal principal $I = (P)$ engendré par P. Montrer que si P s'écrit $P = P_1P_2$ avec $\deg P_i \geq 1$ alors l'anneau $\mathbb{R}[X]/I$ n'est pas intègre. A quelle(s) condition(s) l'anneau quotient $\mathbb{R}[X]/I$ sera-t-il un corps ?

---

28 Soit p un nombre premier (≥ 2). On considère les anneaux $\mathbb{Z}[X]$ et $\frac{\mathbb{Z}}{p\mathbb{Z}}[X]$. On définit l'application ϕ par

$$\phi : \begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \frac{\mathbb{Z}}{p\mathbb{Z}}[X] \\ P & \longmapsto & \overline{P} \end{array}$$

où $\overline{P} = \sum_{i=0}^n \overline{a_i} X^i$ si $P = \sum_{i=0}^n a_i X^i$. (On rappelle que $\overline{a}$ désigne la classe de $a \in \mathbb{Z}$ dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$.)

a — On prend $p = 5$. Soit $f = 5X^6 + X^5 + 3x^4 + X^3 + 4X^2 - 3X - 1$ et $g = X^2 + X + 1$. Déterminer $\overline{f}$ et $\overline{g}$. Montrer que $\overline{g}$ divise $\overline{f}$. Est-il vrai que f est divisible par g ?

b — On revient au cas p premier quelconque. Montrer que ϕ est un morphisme d'anneau. Déterminer son noyau. En déduire un isomorphisme d'anneau. Pouvez-vous généraliser le résultat (que dire si on remplace $\mathbb{Z}$ par A et $p\mathbb{Z}$ par un ideal I de A) ?

c — Soient f et g deux polynômes de $\mathbb{Z}[X]$. On suppose que $\mathrm{dom}(g) \in \mathbb{Z}^* = \{-1,1\}$. Déterminer $Q(\overline{f},\overline{g})$ (resp. $R(\overline{f},\overline{g})$) le quotient (resp. le reste) de la division de $\overline{f}$ par $\overline{g}$ en fonction de $Q(f,g)$ (resp. de $R(f,g)$).