DEUX CENT TRENTE-QUATRE EXERCICES D'ALGÈBRE POUR LA LICENCE DE MATHÉMATIQUES

2008–2009

M. Audin, V. Blanlœil, G. Collinet, M. Coornaert, R. Noot, J. Poineau

Les exercices marqués d'une étoile sont les « indispensables », c'est-à-dire ceux qui ne sont pas très difficiles et qu'il est indispensable de savoir faire — ce qui ne veut pas pas dire qu'il ne faut pas savoir faire les autres, parfois un peu plus techniques, ou faisant appel à plus de connaissances mathématiques (en algèbre linéaire, en analyse ou en géométrie), voire contenant des pièges.

On trouvera d'autres exercices dans les livres [**5, 2, 3, 1, 6, 7**] (dans lesquels certains de ceux présentés ici ont été copiés) notamment.

0. Bases du raisonnement, ensembles, relations d'équivalence — exercices de vérification

Cette première série d'exercices est un « échauffement ». Assurez-vous qu'aucun des exercices (étoilés) suivants ne vous pose de problème avant de vous attaquer aux exercices d'algèbre proprement dits.

Exercice⋆ 0.1. S'il pleut, je prends un parapluie. Est-ce que cela veut dire que si vous me rencontrez dans la rue avec un parapluie, il pleut ?

***Exercice⋆ 0.2* (La nuit...)**. Nier l'assertion[(1)] « tous les chats sont gris », puis l'assertion « la nuit, tous les chats sont gris ».

Exercice⋆ 0.3. Nier les assertions suivantes :

– Tout triangle rectangle possède un angle droit.

– Dans toutes les universités, tous les étudiants détestent tous les enseignants.

– Pour tout entier x, il existe un entier y tel que pour tout entier z, la relation $z < y$ implique la relation $z < x + 1$.

***Exercice⋆ 0.4* (Cent mille milliards de théorèmes)**. Quand E est l'ensemble vide, tous les énoncés commençant par « pour tout $x \in E$ » sont vrais. Vrai ?

***Exercice⋆ 0.5* (Tous les crayons ont la même couleur)**. Démonstration par récurrence sur le nombre n de crayons : pour $n = 1$, l'assertion est trivialement vraie ; pour le passage de n à $n + 1$, parmi nos $n + 1$ crayons, choisissons-en n, ils ont tous la même couleur, par hypothèse de récurrence, de même l'ensemble formé par le dernier crayon et un de nos n premiers crayons, donc les $n + 1$ crayons ont bien la même couleur. Commentaire ?

Exercice⋆ 0.6. Soient A et B deux parties de l'ensemble E. Montrer que

$$(\complement^E A) \cap (\complement^E B) = \complement^E (A \cup B).$$

Exercice⋆ 0.7. Vrai ou faux ?

Merci de nous communiquer commentaires, corrections et suggestions. Il n'existe pas et n'existera pas de « corrigé » de cette « feuille ».

(1) Une bonne occasion de recommander la lecture de [**4**].

– Si $f : E \to F$ est une application injective, alors $|F| \geq |E|$.
– Si $f : E \to F$ est une application surjective, alors $|F| \geq |E|$.
– Si $f : E \to F$ est une application injective et si $|F| = |E|$, alors f est bijective.
– Si $f : E \to F$ est une application surjective et si $|F| \leq |E|$, alors f est bijective.
– Si E et F sont des ensembles finis et $|E| = |F|$, alors il existe une bijection de E sur F.

Exercice⋆ 0.8. Combien y a-t-il de relations d'équivalence sur un ensemble à deux éléments ? sur un ensemble à trois éléments ?

Exercice⋆ 0.9. On considère une relation binaire $\mathcal{R}$ sur $\mathbf{R}$. Quelles propriétés de son graphe

$$\Gamma(\mathcal{R}) = \left\{(x, y) \in \mathbf{R}^2 \mid x\mathcal{R}y\right\} \subset \mathbf{R}^2$$

expriment respectivement le fait que $\mathcal{R}$ est réflexive ? symétrique ?

Pour chacune des parties de $\mathbf{R}^2$ qui suivent, déterminer si elle est ou non le graphe d'une relation d'équivalence sur $\mathbf{R}$:

– $\Gamma(\mathcal{R}) = \{(s, s) \mid s \in \mathbf{R}\}$;
– $\Gamma(\mathcal{R}) = \varnothing$;
– $\Gamma(\mathcal{R}) = \{(x, y) \mid xy + 1 = 0\}$.

Dans le premier cas, de quelle relation d'équivalence s'agit-il ?

Exercice⋆ 0.10. Soit E l'ensemble des droites d'un plan affine. On rappelle que « par un point extérieur à une droite, on peut mener une unique parallèle à cette droite ». Montrer que la relation « être parallèle à » est une relation d'équivalence sur E.

Exercice 0.11. Simplifier la phrase suivante : « ... il ne se trouvera aucun sportif pour nier que le contraire n'eût été immérité... »

1. Lois de composition internes, définition d'un groupe

Exercice⋆ 1.1. Montrer que la loi de composition interne $\star$ définie sur $\mathbf{N}$ par

$$x \star y = x^y$$

n'est ni commutative ni associative et qu'en plus elle n'admet pas d'élément neutre.

Exercice⋆ 1.2. Dans cet exercice, E est un ensemble et $\mathcal{P}(E)$ désigne l'ensemble des parties de E.

(1) On munit $\mathcal{P}(E)$ de la loi de composition interne $\cap$ (intersection). Est-elle associative ? commutative ? a-t-elle un élément neutre ? est-ce une loi de groupe ?
(2) Mêmes questions pour la loi $\cup$ (réunion).
(3) On munit maintenant $\mathcal{P}(E)$ de la loi Δ « différence symétrique » définie par

$$A\Delta B = A \cup B - A \cap B.$$

Montrer que $(\mathcal{P}(E), \Delta)$ est un groupe commutatif.

Exercice⋆ 1.3. Soit $X = \{a, b\}$ un ensemble à deux éléments. Construire une loi de composition interne commutative mais non associative sur X.

Exercice⋆ 1.4. Soit $X = \{a, b\}$ un ensemble à deux éléments. Construire une loi de composition interne associative mais non commutative sur X.

Exercice⋆ 1.5. Soit $X = \{a, b\}$ un ensemble à deux éléments. Construire une loi de composition interne $\star$ sur X telle que $(X, \star)$ soit un monoïde commutatif mais pas un groupe.

Exercice⋆ 1.6. Soit X un ensemble à deux éléments. Combien de lois de composition internes $*$ existe-t-il sur X telles que $(X, *)$ soit un groupe ?

Même question, mais pour X de cardinal 3, puis de cardinal 4.

Exercice⋆ 1.7. Pour chacun des couples d'un ensemble avec loi de composition suivants, décider s'il s'agit d'une loi interne. Lorsque c'en est une, est-ce qu'elle définit une structure de groupe sur l'ensemble en question ? Lorsque c'est le cas, trouver l'élément neutre et, pour tout élément, son inverse.

(1) $(\mathbf{N}, +)$.

(2) $(\mathbf{R}, *)$, avec $x * y = x + y - 1$.
(3) $(]-\pi/2, \pi/2[, *)$, avec $x * y = \arctan(\tan(x) + \tan(y))$.
(4) $(\{f : \mathbf{R} \to \mathbf{R}\}, *)$, avec $f * g = f \circ g$.
(5) $(\{A \in M(n; \mathbf{R}) \mid \text{dét}(A) \neq 0\}, \cdot)$, avec $\cdot$ la multiplication des matrices.
(6) $(\{A \in M(n; \mathbf{Z}) \mid \text{dét}(A) \neq 0\}, \cdot)$, avec $\cdot$ la multiplication des matrices.

Exercice⋆ 1.8. Soit E un ensemble muni d'une loi de composition interne associative qui possède un élément neutre. Montrer que l'ensemble des éléments inversibles de E forme un groupe.

***Exercice⋆ 1.9* (Calcul dans les groupes)**. Dans un groupe G, montrer que l'on a
(1) $a, b \in G \Rightarrow \exists\, !x \in G \mid ax = b$;
(2) $a, b, c \in G$ et $ac = bc \Rightarrow a = b$.

***Exercice⋆ 1.10* (Calcul dans les groupes (suite))**. Soient G un groupe, $n \in \mathbf{N}$ et $g_1, \ldots, g_n \in G$.
(1) Définir $\prod_{i=1}^{n} g_i = g_1 g_2 \cdots g_n$.
(2) Montrer que pour $1 \leq m \leq n$ on a $\left(\prod_{i=1}^{m} g_i\right)\left(\prod_{i=m+1}^{n} g_i\right) = \prod_{i=1}^{n} g_i$.
(3) En déduire que $(g_1 g_2 \cdots g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$.
(4) Pour $g \in G$ et $n \in \mathbf{Z}$, définir g^n.
(5) Montrer que, pour $g \in G$ et $m, n \in \mathbf{Z}$, on a $g^m g^n = g^{m+n}$ et $(g^m)^n = g^{mn}$.
(6) Donner une condition nécessaire et suffisante pour que $(gh)^n = g^n h^n$ pour tous g, $h \in G$ et tout $n \in \mathbf{Z}$.

Exercice⋆ 1.11. Donner la table des groupes additifs $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$ et $\mathbf{Z}/4\mathbf{Z}$.

Exercice⋆ 1.12. Faire la liste (table de multiplication) de tous les groupes à deux, trois, quatre (exercice 1.6) et cinq éléments.

Exercice⋆ 1.13. Donner la table des groupes symétriques $\mathfrak{S}_2$ et $\mathfrak{S}_3$.

Exercice⋆ 1.14. Soient X un ensemble non vide et G un groupe. On note A l'ensemble des applications de X dans G. Munir A d'une structure de groupe.

***Exercice⋆ 1.15* (Le groupe diédral)**. On considère l'ensemble D_{2n} des isométries qui préservent un polygone régulier à n côtés (n est un entier ≥ 3). Montrer que c'est un groupe, le *groupe diédral*, que ce groupe a $2n$ éléments[(2)], dont la moitié sont des rotations (d'angle multiple de $2\pi/n$) et les autres des réflexions (d'ordre 2). Ce groupe est-il commutatif ?

Exercice⋆ 1.16. On considère l'ensemble G des transformations « affines » de $\mathbf{R}$ dans $\mathbf{R}$,

$$x \longmapsto ax + b \text{ avec } a, b \in \mathbf{R} \text{ et } a \neq 0.$$

Montrer que G, muni de la composition des applications, est un groupe et que ce groupe n'est pas commutatif.

Exercice⋆ 1.17. Soit G un groupe d'élément neutre e.
(1) On suppose que, que pour tout $x \in G$ on a $x^2 = e$. Montrer que G est commutatif.
(2) On suppose maintenant que pour tous x et y dans G on a $(xy)^{-1} = x^{-1}y^{-1}$. Montrer que G est commutatif.
(3) On suppose enfin que, pour tous x et y dans G on a $(xy)^2 = x^2y^2$. Peut-on conclure que G est commutatif ?

Exercice 1.18. Donner un exemple d'un groupe non commutatif G tel que pour tous x et y dans G on ait $(xy)^3 = x^3y^3$. Indication : considérer les a dans $M(3; \mathbf{Z}/3\mathbf{Z})$ tels que $a_{i,i} = 1$ pour $1 \leq i \leq 3$ et $a_{i,j} = 0$ pour $1 \leq j < i \leq 3$.

(2) d'où la notation, qui n'est pas universelle, on trouve aussi D_n pour ce même groupe

Exercice 1.19. Pour chacun des couples d'un ensemble avec loi de composition suivants, décider s'il s'agit d'une loi interne. Lorsque c'en est une, est-ce qu'elle définit une structure de groupe sur l'ensemble en question ?

(1) $(\{A \in M(100, \mathbf{Z}) \,|\, \exists\, B \in M(100, \mathbf{Z}) : AB = BA = I\}, \cdot)$, avec $\cdot$ la multiplication des matrices.
(2) $(\{A \in M(100, \mathbf{Z}) \,|\, \exists\, B \in M(100, \mathbf{Z}) : AB = I\}, \cdot)$, avec $\cdot$ la multiplication des matrices.
(3) $(\{a \in \mathrm{End}(V) \,|\, \exists\, b \in \mathrm{End}(V) : ab = \mathrm{Id}_V\}, \circ)$, avec V un espace vectoriel, éventuellement de dimension infinie, sur un corps quelconque. Est-ce qu'on peut appliquer le résultat de l'exercice 1.8 pour résoudre cette question ? Pourquoi (pas) ?

Exercice 1.20. Soient G un ensemble et $*$ une loi de composition interne associative sur G. Supposons que $(G, *)$ a un élément neutre e, et que pour tout x dans G il existe y et y' dans G tels que $yx = e = xy'$. Est-ce que $(G, *)$ est un groupe ? Est-ce que l'existence d'un inverse à gauche (y, donc) suffit ?

Exercice 1.21. Trois éléments x, y et z d'un groupe sont tels que $xyz = e$. A-t-on $yzx = e$? Et $yxz = e$?

Exercice 1.22. On suppose que X est un ensemble muni d'une loi de composition (binaire) interne, pas nécessairement associative et que $x_1, \ldots, x_5 \in X$. De combien de façons peut-on insérer trois paires de parenthèses dans le produit $x_1x_2x_3x_4x_5$ pour que ce produit soit défini ?

2. Sous-groupes

Exercice* 2.1. Parmi les sous-ensembles suivants, lesquels sont des sous-groupes ?

(1) $\mathrm{GL}(n; \mathbf{R}) \subset \mathrm{GL}(n; \mathbf{C})$ (pour $n \geq 1$).
(2) $\{1, -1\} \subset (\mathbf{R}^\star, \times)$.
(3) $\mathbf{N} \subset (\mathbf{Z}, +)$.
(4) $(\mathbf{Q}^\star, \times) \subset (\mathbf{R}^\star, \times)$.
(5) $\{-1, 0, 1\} \subset (\mathbf{Z}, +)$.
(6) Pour $n \geq 2$, $\{g \in \mathrm{GL}(n; \mathbf{R}) \,|\, {}^t g = g\}$ dans $\mathrm{GL}(n; \mathbf{R})$.
(7) Pour G un groupe d'élément neutre e, $\{x \in G \,|\, x^2 = e\}$ dans G.

Exercice* 2.2. Montrer que

$$\left\{x + y\sqrt{2}, x \in \mathbf{Z}, \quad y \in \mathbf{Z}\right\}$$

est un sous-groupe de $(\mathbf{R}, +)$.

***Exercice* 2.3* (Groupe des rotations)**. Montrer que

$$H = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \mid \theta \in \mathbf{R} \right\}$$

est un sous-groupe de $\mathrm{GL}(2; \mathbf{R})$.

***Exercice* 2.4* (Groupe orthogonal)**. Montrer que

$$\mathrm{O}(n) = \{g \in \mathrm{GL}(n; \mathbf{R}) \,|\, {}^t g^{-1} = g\} \subset \mathrm{GL}(n; \mathbf{R})$$

est un sous-groupe. Vérifier que c'est le groupe des isométries vectorielles de l'espace $\mathbf{R}^n$.

Déterminer tous les éléments de $\mathrm{O}(2)$.

Exercice* 2.5. Montrer que

$$H = \left\{ \begin{pmatrix} 2^k & \frac{n}{2^m} \\ 0 & 2^{-k} \end{pmatrix} \mid k, n, m \in \mathbf{Z} \right\}$$

est un sous-groupe de $\mathrm{GL}(2; \mathbf{R})$.

Exercice* 2.6. Montrer que

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbf{R} \right\}$$

est un sous-groupe de $\mathrm{GL}(3; \mathbf{R})$.

Exercice⋆ 2.7. Montrer que les matrices

$$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad \pm\begin{pmatrix}0&i\\i&0\end{pmatrix},\quad \pm\begin{pmatrix}i&0\\0&-i\end{pmatrix}$$

forment un sous-groupe de $\mathrm{GL}(2;\mathbf{C})$ (on appelle ce groupe à huit éléments le groupe *quaternionien*).

Exercice⋆ 2.8. Quels sont les éléments du sous-groupe engendré par $\begin{pmatrix}1&1\\-1&0\end{pmatrix}$ dans $\mathrm{GL}(2;\mathbf{R})$?

Exercice⋆ 2.9. Donner un exemple d'un groupe G et de sous-groupes H_1 et H_2 tels que $H_1 \cup H_2$ ne soit pas un sous-groupe.

Soit G un groupe, H_1 et H_2 des sous-groupes. Montrer que $H_1 \cup H_2$ est un sous-groupe si et seulement si $H_1 \subset H_2$ ou $H_2 \subset H_1$.

Exercice⋆ 2.10. Montrer que G, défini par

$$G = \left\{ \begin{pmatrix}1&a\\0&b\end{pmatrix} \in M(2;\mathbf{R}) \mid b \neq 0 \right\}.$$

est un sous-groupe de $\mathrm{GL}(2;\mathbf{R})$. Montrer que

$$H_1 = \left\{ \begin{pmatrix}1&0\\0&b\end{pmatrix} \mid b \neq 0 \right\} \text{ et } H_2 = \left\{ \begin{pmatrix}1&a\\0&1\end{pmatrix} \mid a \in \mathbf{R} \right\}$$

sont des sous-groupes de G.

Exercice⋆ 2.11. Montrer que dans le groupe $(\mathcal{P}(E), \Delta)$, considéré dans l'exercice 1.2, tous les éléments (sauf $\varnothing$) sont d'ordre 2.

Exercice⋆ 2.12. Soit G un groupe commutatif. Soit H l'ensemble des éléments d'ordre fini de G. Montrer que H est un sous-groupe de G. Montrer aussi que, pour d fixé, l'ensemble des éléments x tels que $x^d = e$ est un sous-groupe. La condition que G soit commutatif est-elle essentielle ?

Exercice⋆ 2.13. L'hypothèse de commutativité du groupe est indispensable dans l'exercice 2.12, en voici une preuve. On considère le groupe affine G comme dans l'exercice 1.16, dont on a vu qu'il n'est pas commutatif. Montrer que les éléments $x \mapsto -x$ et $x \mapsto -x+1$ sont d'ordre 2 mais que leur produit est d'ordre infini.

Exercice⋆ 2.14. Soit G un groupe. Soit $x \in G$ un élément d'ordre fini n. Soit $r \in \mathbf{N}$. Montrer que x^r est d'ordre $n' = n/d$, où $d = \mathrm{pgcd}(n, r)$.

Exercice⋆ 2.15. Soit G un groupe fini d'ordre n. Montrer que G est cyclique si et seulement si G possède un élément d'ordre n.

Exercice⋆ 2.16. Soient G_1 et G_2 des groupes. Soient $x \in G_1$ un élément d'ordre fini m et $y \in G_2$ un élément d'ordre fini n. Montrer que l'élément $(x, y) \in G_1 \times G_2$ est d'ordre $r = \mathrm{ppcm}(m, n)$.

Exercice⋆ 2.17. Soit H un sous-ensemble non vide d'un groupe G, stable par la loi de groupe. Est-ce que H est un sous-groupe ? Et si on suppose que H est fini ?

Exercice⋆ 2.18. Soit G un groupe. Soit H un sous-groupe de G d'indice fini n.

(1) Soit g un élément de G. Montrer qu'il existe un entier $k \in \{1, \ldots, n\}$ tel que $g^k \in H$.

(2) On suppose qu'il existe un entier M tel que tout élément d'ordre fini de H soit d'ordre inférieur ou égal à M. Montrer que tout élément d'ordre fini de G est d'ordre inférieur ou égal à nM.

Exercice⋆ 2.19. Dans un groupe G, on considère le sous-groupe H engendré par deux éléments a et b. Montrer que, si $ab = ba$, alors H est abélien.

Exercice⋆ 2.20. Déterminer le nombre d'éléments d'ordre 2 dans chacun des groupes suivants : $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $\mathfrak{S}_3$.

Exercice⋆ 2.21. Soit G un groupe. On considère la relation $\sim$ définie dans G par

$$(x \sim y) \Leftrightarrow (x = y \text{ ou } x = y^{-1}).$$

Montrer que $\sim$ est une relation d'équivalence.

Montrer que tout groupe fini d'ordre pair contient un nombre impair d'éléments d'ordre 2 (et en particulier qu'il en contient au moins un).

Exercice⋆ 2.22. Soient G un groupe cyclique à m éléments et x un générateur de G. Montrer que, pour que x^k soit un générateur de G, il faut et il suffit que k et m soient premiers entre eux.

Exercice⋆ 2.23. Soit G un groupe. Soient a et b dans G.

(1) Montrer que a, a^{-1}, bab^{-1} ont tous le même ordre.
(2) Montrer que ab et ba ont le même ordre.
(3) Soit n un entier. Exprimer l'ordre de a^n en termes de n et de l'ordre de a.
(4) Supposons que $ab = ba$, que $\langle a\rangle \cap \langle b\rangle = \{e\}$, et que a et b sont d'ordre fini n et m, respectivement. Exprimer l'ordre de ab en termes de n et m.
(5) Supposons que $ab = ba$, et que a et b sont d'ordre fini n et m, respectivement, avec n et m premiers entre eux. Exprimer l'ordre de ab en termes de n et m.

Exercice⋆ 2.24. Soit $n \geq 1$ un entier.

(1) Déterminer la somme des éléments du groupe $(\mathbf{Z}/n\mathbf{Z}, +)$.
(2) Notons $\mu_n(\mathbf{C})$ l'ensemble des solutions complexes de $z^n = 1$. Montrer que la multiplication des nombres complexes induit une structure de groupe sur $\mu_n(\mathbf{C})$. Déterminer le produit de tous les éléments de $\mu_n(\mathbf{C})$.

Exercice⋆ 2.25. Soit $n \in \mathbf{Z}$. Déterminer tous les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$.

Exercice⋆ 2.26. Déterminer le centre de $\mathrm{GL}(n; \mathbf{R})$ (et plus généralement de $\mathrm{GL}(n; \mathbf{K})$).

Exercice 2.27. Soit $\mathbf{K}$ un corps fini d'ordre q. Montrer que le groupe $\mathrm{GL}(n, \mathbf{K})$ est fini, d'ordre

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

Exercice 2.28. Soit G un groupe commutatif, noté additivement, tel que pour tout x dans G et tout entier n non nul il existe un unique y dans G avec $ny = x$. Montrer que G est le groupe additif sous-jacent à un $\mathbf{Q}$-espace vectoriel.

Exercice 2.29. Soit G le sous-groupe $\{e^{2\pi i x} \mid x \in \mathbf{Q}\}$ de $\mathbf{C}^*$.

(1) Montrer que tout élément de G est d'ordre fini.
(2) Montrer que G est « divisible », c'est-à-dire que, pour tout z dans G et tout entier $n \neq 0$ il existe w dans G tel que $z = w^n$.
(3) Est-ce que G est le groupe additif sous-jacent à un $\mathbf{Q}$-espace vectoriel ?

Exercice 2.30. (1) Peut-on avoir une infinité de sous-groupes distincts dans un groupe fini ?
(2) Même question dans un groupe dont le cardinal n'est pas fini.
(3) Existe-t-il un groupe infini dont le nombre de sous-groupes est fini ?

Exercice 2.31. Montrer qu'un sous-groupe de $(\mathbf{R}, +)$ est, soit dense dans $\mathbf{R}$, soit engendré par un élément a de $\mathbf{R}$.

Exercice 2.32. Le sous-groupe défini dans l'exercice 2.2 est-il un sous-groupe discret de $\mathbf{R}$? Même question en remplaçant $\sqrt{2}$ par $3/2$.

***Exercice⋆ 2.33* (Examen, janvier 2007)**. Soit p un nombre premier.

(1) **Question de cours.** Soit H un groupe d'ordre p, dont on note l'élément neutre e. Montrer que H est cyclique, engendré par n'importe lequel de ses éléments $\neq e$.
(2) Soit G un groupe. On suppose que H_1 et H_2 sont deux sous-groupes de G, tous les deux d'ordre p. Montrer que, soit $H_1 \cap H_2 = \{e\}$, soit $H_1 = H_2$.
(3) Sous les mêmes hypothèses, on suppose que $H_1 \neq H_2$. Montrer que $|G| \geq 2p$.

3. Groupe symétrique

Exercice⋆ 3.1. Pour quelles valeurs de n le groupe symétrique $\mathfrak{S}_n$ est-il commutatif ?

Exercice⋆ 3.2. Décomposer en cycles disjoints

(1) $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 2 & 7 & 9 & 6 & 10 & 3 & 1 & 4 \end{pmatrix}$;

(2) $b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix}$;

(3) $c = (12345)(159)(249)$;

(4) $d = (1867)(8675)(6751)$;

(5) $f = (12)(23)(34)(45)(56)(67)(71)$;

(6) $h = (18)(17)(16)(15)(14)(13)(12)$.

Déterminer l'ordre de ces éléments de $\mathfrak{S}_{10}$. Calculer b^{100} et c^{2005}.

Exercice⋆ 3.3. Écrire les permutations suivantes comme produit de cycles disjoints.

(1) $(3,1,4)(1,5,9,2,6)(5,3)$ dans $\mathfrak{S}_9$.

(2) σ^{-1}, où $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$ dans $\mathfrak{S}_5$.

(3) σ^{-1}, où $\sigma = (5,6,2)(1,3)$ dans $\mathfrak{S}_6$.

Pour chacune de ces permutations, quelle est sa signature ?

Exercice⋆ 3.4. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{pmatrix}$ dans $\mathfrak{S}_{12}$. Calculer σ^{2000}. Quelle est la signature de σ ?

Exercice⋆ 3.5. Pour $3 \leq n \leq 7$, déterminer l'ensemble $X_n = \{\text{ordre}(\sigma) \mid \sigma \in \mathfrak{S}_n\}$ des ordres des éléments de $\mathfrak{S}_n$.

***Exercice⋆ 3.6* (Examen, janvier 2006)**. Pour cet exercice, on se place dans le groupe symétrique $\mathfrak{S}_4$.

(1) Quels sont les ordres possibles des éléments de $\mathfrak{S}_4$?

(2) Déterminer tous les éléments d'ordre 2, d'ordre 3, d'ordre 4.

(3) Combien y a-t-il de classes de conjugaison dans $\mathfrak{S}_4$? Quel est le cardinal de chacune de ces classes ?

Exercice⋆ 3.7. Quelle est la signature d'une permutation d'ordre 12, resp. 14, resp. 15, dans $\mathfrak{S}_{10}$?

Exercice⋆ 3.8. Montrer que $\mathfrak{S}_n$ est engendré par

– les transpositions $\{(1,i) \mid 2 \leq i \leq n\}$ (indication : pour i et j des entiers tels que $2 \leq i < j \leq n$, on a $(1,i)(1,j)(1,i) = (i,j)$) ;

– ou la transposition $(1,2)$ et le cycle $(2,3,\ldots,n)$;

– ou les transpositions $\{(i,i+1) \mid 1 \leq i < n\}$;

– ou encore la transposition $(1,2)$ et le cycle $(1,2,\ldots,n)$.

Exercice 3.9. Déterminer le nombre minimal de transpositions qui engendrent $\mathfrak{S}_n$.

Exercice⋆ 3.10. Dans tout l'exercice, on fixe un entier $n > 0$, on note $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $\{1,2,\ldots,n\}$ et $\mathfrak{A}_n \subset \mathfrak{S}_n$ le groupe alterné.

(1) Soit $C \subset \mathfrak{S}_n$ une classe de conjugaison. Montrer que ou bien $C \subset \mathfrak{A}_n$ ou bien $C \cap \mathfrak{A}_n = \varnothing$.

(2) On fixe désormais $n = 5$. Déterminer le nombre de classes de conjugaison de $\mathfrak{S}_5$ et trouver un réprésentant et le cardinal de chaque classe.

(3) Déterminer quelles classes de conjugaison de $\mathfrak{S}_5$ sont contenues dans $\mathfrak{A}_5$.

(4) Déterminer le nombre de classes de conjugaison de $\mathfrak{A}_5$.

Exercice⋆ 3.11. Montrer que dans le groupe symétrique $\mathfrak{S}_n$ tout élément est conjugué à son inverse.

Exercice 3.12. (1) Trouver les σ dans $\mathfrak{S}_4$ tels que $\sigma^2 = (1,2)(3,4)$.

(2) Soit $n \geq 2$. Existe-t-il un σ dans $\mathfrak{S}_n$ tel que $\sigma^2 = (1,2)$? Même question pour $n \geq 6$ et $\sigma^2 = (1,2)(3,4,5,6)$.

Exercice 3.13. Montrer que $\mathfrak{A}_4$ n'a pas de sous-groupe d'ordre 6.

Exercice 3.14. Établir la liste des ordres des éléments de $\mathfrak{S}_8$. Montrer qu'il n'existe pas dans $\mathfrak{S}_8$ de sous-groupe cyclique d'ordre 9, de sous-groupe cyclique d'ordre 14 (mais $\mathfrak{S}_8$ contient un sous-groupe d'ordre 14, le groupe diédral D_{14}, pourquoi ?).

Exercice* 3.15. Soit G un groupe d'ordre 6. Montrer que $G \cong \mathbf{Z}/6\mathbf{Z}$ ou $G \cong \mathfrak{S}_3$.

***Exercice* 3.16* (Examen, janvier 2007)**. Pour cet exercice, on se place dans le groupe alterné $\mathfrak{A}_5$.

(1) Quel est l'ordre du groupe $\mathfrak{A}_5$? Faire la liste des diviseurs de ce nombre et dire lesquels de ces diviseurs sont effectivement des ordres d'éléments de $\mathfrak{A}_5$.

(2) Pour chacun des groupes G ci-dessous, dire si $\mathfrak{A}_5$ contient un sous-groupe isomorphe à G (si oui, exhiber un tel sous-groupe, si non, dire pourquoi) :

$$G = \mathbf{Z}/2\mathbf{Z}, \quad G = \mathbf{Z}/3\mathbf{Z}, \quad G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \quad G = \mathbf{Z}/4\mathbf{Z}, \quad G = \mathbf{Z}/5\mathbf{Z}, \quad G = \mathbf{Z}/6\mathbf{Z}.$$

***Exercice* 3.17* (Examen, septembre 2007)**. Dans chaque case des tableaux suivants, indiquer (par oui ou par non) si les groupes correspondant à la ligne et à la colonne de la case sont isomorphes. Justifier vos réponses.

(1)

$\cong$?	$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/4\mathbf{Z}$	$\mathfrak{A}_4$
$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$			
$\mathbf{Z}/4\mathbf{Z}$			
$\mathfrak{A}_4$			

(2)

$\cong$?	$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/6\mathbf{Z}$	$\mathfrak{S}_3$
$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$			
$\mathbf{Z}/6\mathbf{Z}$			
$\mathfrak{S}_3$			

(3) Y a-t-il un groupe dans le premier tableau qui est isomorphe à un groupe du deuxième tableau ?

***Exercice* 3.18* (Examen, septembre 2008)**. Pour cet exercice, on se place dans le groupe symétrique $\mathfrak{S}_4$.

(1) Déterminer les éléments de $\mathfrak{S}_4$ dont l'ordre est une puissance de 2.

(2) Soient τ_1 et τ_2 deux transpositions. Quel peut être l'ordre du produit $\tau_1\tau_2$?

(3) Soit σ un cycle d'ordre 4. Calculer σ^2 et donner sa décomposition en produit de cycles à support disjoints.

(4) Soit $H \subset \mathfrak{S}_4$ un sous-groupe d'ordre 4.

(a) On suppose que H contient un élément d'ordre 4. Montrer que H est cyclique.

(b) On suppose que H ne contient aucun élément d'ordre 4. Montrer qu'il est isomorphe au produit de deux groupes cycliques.

(c) Montrer que les deux possibilités se produisent effectivement.

(5) Soit $K \subset \mathfrak{S}_4$ un sous-groupe d'ordre 8.

(a) Quels sont les ordres possibles des éléments de K ?

(b) Montrer que K contient un élément d'ordre 4.

4. Morphismes de groupes, sous-groupes distingués

Exercice* 4.1. Montrer que la loi de composition

$$x * y = \sqrt[3]{x^3 + y^3}$$

munit $\mathbf{R}$ d'une structure de groupe et que ce groupe est isomorphe au groupe additif de $\mathbf{R}$. De même pour

$$x * y = \arctan(\tan x + \tan y) \text{ sur } \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[.$$

Généralisation ?

Exercice⋆ 4.2. Soit $f\colon G_1 \to G_2$ un isomorphisme de groupes. Soit $x \in G_1$ un élément d'ordre fini n. Montrer que $f(x)$ est d'ordre n. Que se passe-t-il si f n'est pas bijectif ?

Exercice⋆ 4.3. Soient G un groupe et $H \subset G$ un sous-groupe. Montrer que $G/H = \{\overline{e}\}$ si et seulement si $H = G$.

Exercice⋆ 4.4. Soit

$$H = \left\{(x, y) \in \mathbf{Z}^2 \mid \ x + y \text{ est pair } \right\}.$$

(1) Montrer que H est un sous-groupe d'indice 2 du groupe $\mathbf{Z}^2$.
(2) Montrer que l'application

$$\begin{aligned} \varphi : \mathbf{Z}^2 &\longrightarrow H \\ (a, b) &\longmapsto (a, 2b - a) \end{aligned}$$

est un isomorphisme de groupes.

Exercice⋆ 4.5. Soit $H = \left\{(x, y, z) \in \mathbf{Z}^3 \mid x + y + z = 0\right\}$.

(1) Montrer que H est un sous-groupe de $\mathbf{Z}^3$.
(2) Montrer que le groupe H est isomorphe à $\mathbf{Z}^2$.

Exercice⋆ 4.6. Montrer que l'application « déterminant » est un morphisme du groupe $\mathrm{GL}(n; \mathbf{R})$ (resp. $\mathrm{GL}(n; \mathbf{C})$) sur (le mot « sur » employé ici signifie bien que dét est surjective, ce qu'il faut donc montrer !) le groupe multiplicatif $\mathbf{R}^\star$ (resp. $\mathbf{C}^\star$).

Exercice⋆ 4.7. Pour chacun des triplets (G, H, f) suivants avec G et H des groupes et $f : G \to H$ une application, décider si f est un morphisme de groupes. Lorsque c'est le cas, déterminer son noyau et son image et décider si f est injective, si f est surjective et si f est un isomorphisme.

(1) $f : (M(100; \mathbf{R}), +) \to (M(100; \mathbf{R}), +)$, $a \mapsto a + {}^t a$.
(2) $f : (M(100; \mathbf{R}), +) \to (M(100; \mathbf{R}), +)$, $a \mapsto ba$, avec $b \in M(100; \mathbf{R})$ une matrice fixée.
(3) $f : \mathrm{GL}(100; \mathbf{R}) \to \mathrm{GL}(100; \mathbf{R})$, $a \mapsto {}^t a$.
(4) $f : \mathrm{GL}(100; \mathbf{R}) \to \mathrm{GL}(100; \mathbf{R})$, $a \mapsto {}^t aa$.
(5) $f : (M(100; \mathbf{R}), +) \to \mathrm{GL}(100; \mathbf{R})$, $a \mapsto \exp(a)$.
(6) $f : (\mathbf{R}, +) \to \mathrm{GL}(100; \mathbf{R})$, $t \mapsto \exp(ta)$, pour $a \in M(100; \mathbf{R})$ une matrice fixée.
(7) $f : (\mathbf{R}, +) \to (\mathbf{R}, +)$, $a \mapsto a + \arctan(1) - \pi/4$.
(8) $f : \mathbf{C}^* \to \mathbf{R}^*$, $z \mapsto |z|$.

Exercice⋆ 4.8. On considère le groupe

$$G = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \in M(2; \mathbf{R}) \mid b \neq 0 \right\}$$

(pour la multiplication des matrices) et ses deux-sous-groupes H_1 et H_2 définis dans l'exercice 2.10. Montrer que l'application

$$\begin{aligned} f_1 : G &\longrightarrow \mathbf{R}^* \\ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} &\longmapsto b \end{aligned}$$

est un morphisme et que $H_2 = \mathrm{Ker}(f_1)$, que

$$\begin{aligned} f_2 : G &\longrightarrow (\mathbf{R}, +) \\ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} &\longmapsto a \end{aligned}$$

n'est pas un morphisme, que

$$\begin{aligned} g_1 : \mathbf{R}^* &\longrightarrow H_1 \\ b &\longmapsto \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \end{aligned}$$

est un isomorphisme... et enfin que

$$\begin{array}{rcl} g_2 : (\mathbf{R}, +) & \longrightarrow & H_2 \\ a & \longmapsto & \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \end{array}$$

est, elle aussi, un isomorphisme.

Exercice⋆ 4.9. Vrai ou faux ?

(1) $\mathbf{Z}/6\mathbf{Z}$ est isomorphe à $\mathfrak{S}_3$.
(2) $\mathbf{Z}/6\mathbf{Z}$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.
(3) $\mathbf{Z}/4\mathbf{Z}$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
(4) $(\mathbf{R}^*, \cdot)$ est isomorphe à $(\mathbf{C}^*, \cdot)$.
(5) $(\mathbf{Q}^*, \cdot)$ est isomorphe à $(\mathbf{R}^*, \cdot)$.
(6) Il existe un morphisme de groupes f surjectif de $(\mathbf{C}, +)$ vers $(\mathbf{C}^*, \cdot)$.

Exercice⋆ 4.10. Montrer que le groupe $(\mathbf{R}, +)$ est isomorphe au groupe multiplicatif des réels strictement positifs.

Exercice⋆ 4.11. Soient m et n des entiers strictement positifs et soit d leur pgcd. La notation μ_n désigne le groupe des racines n-ièmes de l'unité (noté $\mu_n(\mathbf{C})$ dans l'exercice 2.24).

(1) Montrer que $\mu_n \cong \mathbf{Z}/n\mathbf{Z}$.
(2) Montrer que $\mu_m \cap \mu_n = \mu_d$.

Exercice⋆ 4.12. Montrer que le groupe des automorphismes de $\mathfrak{S}_3$ est isomorphe à $\mathfrak{S}_3$.

Exercice⋆ 4.13. Soit G un groupe fini. Montrer qu'il n'y a qu'un seul homomorphisme de G dans $\mathbf{Z}$.

Exercice⋆ 4.14. Soient G un groupe d'ordre 40 et H un groupe d'ordre 63. Montrer qu'il n'y a qu'un seul homomorphisme G dans H.

***Exercice⋆ 4.15* (Examen, septembre 2006)**. Soient n et q des entiers premiers entre eux. On se donne un groupe G contenant un sous-groupe fini H d'ordre $|H| = n$.

(1) Soient G' un groupe fini d'ordre q et $f : G \to G'$ un homomorphisme. En considérant l'ordre de $f(h)$ pour $h \in H$, montrer que H est contenu dans le noyau de f.

(2) Soit K un sous-groupe distingué de G d'indice fini $[G : K] = q$. Déduire de la première question que l'on a $H \subset K$.

(3) Dans le groupe symétrique $\mathfrak{S}_3$, on considère le sous-groupe H engendré par la transposition $\tau_1 = (1, 2)$ et le sous-groupe K engendré par la transposition $\tau_2 = (2, 3)$. Que valent $|H|$ et $[\mathfrak{S}_3 : K]$? Quelle réflexion cela vous inspire-t-il ?

Exercice⋆ 4.16. Soit $f : G_1 \to G_2$ un morphisme de groupes. On suppose que G_1 est engendré par l'ensemble de ses éléments d'ordre 2 et que G_2 est fini et d'ordre impair. Montrer que f est trivial.

Exercice⋆ 4.17. Montrer que tous les endomorphismes de $(\mathbf{Z}, +)$ (morphismes de ce groupe dans lui-même) sont de la forme $n \mapsto an$, pour un certain a dans $\mathbf{Z}$. Pour tout $a \in \mathbf{Z}$, déterminer si l'endomorphisme $n \mapsto an$ est injectif, surjectif, bijectif.

Exercice⋆ 4.18. Le groupe additif $(\mathbf{Z}, +)$ est-il isomorphe au groupe additif $(\mathbf{Q}, +)$?

Exercice⋆ 4.19. Montrer que les deux groupes quaternionien (exercice 2.7) et diédral D_8 (exercice 1.15), tous deux d'ordre 8, ne sont pas isomorphes.

Exercice⋆ 4.20. Montrer que le groupe diédral d'ordre $2n$ (exercice 1.15) est isomorphe à un sous-groupe de $\mathfrak{S}_n$. Quand a-t-on un isomorphisme $D_{2n} \to \mathfrak{S}_n$?

Exercice⋆ 4.21. Soit G un groupe et soit

$$\begin{array}{rcl} f : G & \longrightarrow & G \\ x & \longmapsto & x^{-1} \end{array}$$

l'application de passage à l'inverse. Montrer que f est bijective. À quelle condition est-ce un isomorphisme de groupes ?

Exercice 4.22. Soient G un groupe, x, y, z dans G et $N \subset G$ un sous-groupe distingué tels que $x^5 \in N$, $y^7 \in N$ et $y^{-1}zxz^{-1} \in N$. Montrer que $x \in N$ et que $y \in N$. (Indication : calculer dans G/N ; quels peuvent être ordre($\overline{x}$), ordre($\overline{y}$) et que peut-on tirer de $y^{-1}zxz^{-1} \in N$?)

Exercice* 4.23. Soient G un groupe et H un sous-groupe. Montrer que l'application $i : G \to G$, $g \mapsto g^{-1}$ induit une bijection entre $H\backslash G$ et G/H.

***Exercice* 4.24* (Groupe spécial linéaire)**. Montrer que

$$\mathrm{SL}(n;\mathbf{R}) = \{g \in \mathrm{GL}(n;\mathbf{R}) \mid \det(g) = 1\}$$

est un sous-groupe distingué de $\mathrm{GL}(n;\mathbf{R})$.

Exercice 4.25. Soit $\mathbf{K}$ un corps fini d'ordre q. En utilisant l'exercice 2.27, montrer que le groupe $\mathrm{SL}(n,\mathbf{K})$ est fini, d'ordre

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})}{q-1}.$$

Exercice* 4.26. Soient G_1 et G_2 des groupes, $H_1 \subset G_1$ et $H_2 \subset G_2$ des sous-groupes distingués. Montrer que $H_1 \times H_2$ est un sous-groupe distingué de $G_1 \times G_2$, et que $(G_1 \times G_2)/(H_1 \times H_2)$ est isomorphe à $G_1/H_1 \times G_2/H_2$.

Exercice* 4.27. On considère le groupe affine G (voir l'exercice 1.16). Soient

$$H = \{x \mapsto x+b \mid b \in \mathbf{R}\} \text{ et } K = \{x \mapsto x+b \mid b \in \mathbf{Z}\}.$$

Montrer que H et K sont des sous-groupes de G, que H est distingué dans G, que K est distingué dans H, mais que K n'est pas distingué dans G.

Exercice* 4.28. Montrer que l'ensemble

$$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbf{R} \right\}$$

est un sous-groupe isomorphe à $(\mathbf{R},+)$ de $\mathrm{SL}(2;\mathbf{R})$ et que ce sous-groupe n'est pas distingué.

Exercice* 4.29. Soient $H = \{\mathrm{Id}, (12)(34)\}$ et $K = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$ deux sous-groupes de $\mathfrak{S}_4$. Montrer que H est distingué dans K, K est distingué dans $\mathfrak{S}_4$ et que H n'est pas distingué dans $\mathfrak{S}_4$.

Exercice* 4.30. On considère les sous-groupes $H = \{e, (1,2)\}$ et $K = \{e, (2,3)\}$ du groupe symétrique $G = \mathfrak{S}_3$. Montrer que HK n'est pas un sous-groupe de G.

Soit G un groupe. Soit H un sous-groupe de G. Soit K un sous-groupe distingué de G. Montrer que HK est un sous-groupe de G.

***Exercice* 4.31* (Examen, septembre 2008)**. Soit $\varepsilon = \mathfrak{S}_n \to \{\pm 1\}$ l'homomorphisme « signature ».

(1) Quel est son noyau ? Pour simplifier, on note N ce sous-groupe.
(2) Soit $\tau \in \mathfrak{S}_n$ une transposition fixée. Montrer que $H = \{\mathrm{Id}, \tau\}$ est un sous-groupe de $\mathfrak{S}_n$.
(3) Montrer que la restriction de ε à H est un isomorphisme. Déterminer $N \cap H$.
(4) Montrer que tout élément $g \in \mathfrak{S}_n$ peut s'écrire, de façon unique, sous la forme $g = nh$, avec $n \in N$ et $h \in H$.

Exercice* 4.32. Soit G un groupe. Soient H et K des sous-groupes de G. Montrer que les conditions suivantes sont équivalentes :

(1) HK est un sous-groupe de G ;
(2) $HK = KH$.

Soit G un groupe. Soient H et K des sous-groupes distingués de G. Montrer que HK est un sous-groupe distingué de G.

***Exercice* 4.33* (Examen, janvier 2006)**. On munit l'ensemble $G = \mathbf{Z} \times \mathbf{Z}$ de la loi de composition interne définie par

$$(m,n) \star (m',n') = (m + (-1)^n m', n + n').$$

(1) Montrer que $(G, \star)$ est un groupe (dont on précisera l'élément neutre et l'inverse de chaque élément). Ce groupe est-il commutatif ?

(2) On considère les parties

$$H = \{(a, 0) \mid a \in \mathbf{Z}\} \text{ et } K = \{(0, b) \mid b \in \mathbf{Z}\}$$

de G. Montrer que H et K sont des sous-groupes et que chacun d'eux est isomorphe à $\mathbf{Z}$.

(3) Montrer que l'application $G \to \mathbf{Z}$ qui à (m, n) associe n est un homomorphisme de groupes.

(4) Montrer que H est un sous-groupe distingué de G mais que K n'est pas distingué.

(5) À quel groupe bien connu le groupe quotient G/H est-il isomorphe ?

***Exercice⋆ 4.34* (Groupe des rotations (suite))**. On considère le groupe $\mathrm{O}(n)$ défini dans l'exercice 2.4. Montrer que

$$\mathrm{O}^+(n) = \{g \in \mathrm{O}(n) \mid \text{dét}(g) = 1\}$$

est un sous-groupe distingué de $\mathrm{O}(n)$.

Déterminer tous les éléments de $\mathrm{O}^+(2)$ et montrer que ce groupe est commutatif. En est-il de même de $\mathrm{O}(2)$? De $\mathrm{O}^+(n)$ pour $n \geq 3$?

Exercice⋆ 4.35. Soit H le sous-groupe de $\mathrm{GL}(3; \mathbf{R})$ considéré dans l'exercice 2.6 et formé des matrices triangulaires supérieures dont tous les coefficients diagonaux sont égaux à 1. Montrer que l'application

$$H \longrightarrow \mathbf{R}^2$$
$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \longmapsto (a, c)$$

est un homomorphisme. Déterminer le noyau et l'image de f.

***Exercice⋆ 4.36* (Groupe diédral (suite))**. On se place dans le groupe des isométries préservant un polygone régulier à n côtés (exercice 1.15). Montrer que le sous-groupe des rotations est distingué (par exemple en l'exhibant comme noyau d'un morphisme de groupes) mais que le sous-groupe engendré par une réflexion ne l'est pas.

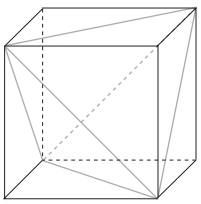
***Exercice 4.37* (Isométries d'un tétraèdre régulier)**. On considère, dans l'espace euclidien de dimension 3, un tétraèdre régulier $ABCD$. Montrer que toute isométrie qui préserve ce tétraèdre préserve l'ensemble de ses sommets. Soit G l'ensemble de toutes ces isométries. Montrer que G est un groupe, muni d'un morphisme

$$G \longrightarrow \mathfrak{S}_4$$

vers le groupe des permutations des quatre points A, B, C et D.

Montrer que ce morphisme est injectif (une isométrie est déterminée par les images des quatre sommets) et surjectif (toutes les permutations sont atteintes, par exemple parce que toutes les transpositions sont atteintes).

***Exercice 4.38* (Isométries d'un cube)**. Dans un cube, on dessine, à l'aide des diagonales des faces, un tétraèdre $\mathcal{T}$ comme sur la figure. Vérifier que ce tétraèdre est régulier. Combien y a-t-il de tétaèdres dans le cube ?



Soit φ une réflexion qui préserve le tétraèdre $\mathcal{T}$. Montrer que φ préserve le cube. Même question pour une isométrie quelconque. Montrer que le groupe des isométries de $\mathcal{T}$ apparaît ainsi comme un sous-groupe du groupe des isométries qui préservent le cube, et que ce sous-groupe est d'indice 2. Combien le groupe des isométries du cube contient-il d'éléments ?

Exercice⋆ 4.39. Soit G un groupe. Soit H un sous-groupe distingué de G tel que $|H| = 2$. Montrer que H est contenu dans le centre de G.

Exercice 4.40. Soit G un groupe. Soit $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

(1) Montrer que $(\mathrm{Aut}(G), \circ)$, où $\circ$ est la composition, est un groupe.

(2) Montrer que pour tout $x \in G$ l'application $\mathrm{Int}_x : G \to G$, $y \mapsto xyx^{-1}$ est un automorphisme de G.

(3) Montrer que $\mathrm{Int} : G \to \mathrm{Aut}(G)$, $x \mapsto \mathrm{Int}_x$ est un morphisme. Son image s'appelle le groupe des *automorphismes intérieurs* de G et se note $\mathrm{Int}(G)$.

(4) Monter que le noyau $\mathrm{Ker}(\mathrm{Int})$ de $\mathrm{Int} : G \to \mathrm{Aut}(G)$ est le centre $Z(G)$ de G.

(5) Montrer que $\mathrm{Int}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$, c'est à dire, montrer que pour $x \in G$ et $\sigma \in \mathrm{Aut}(G)$ on a $\sigma \mathrm{Int}_x \sigma^{-1} \in \mathrm{Int}(G)$.

Exercice⋆ 4.41. Un sous-groupe H d'un groupe G est dit *caractéristique* si pour tout automorphisme σ de G on a $\sigma(H) = H$.

Soient G un groupe et $H_2 \subset H_1 \subset G$ des sous-groupes.

(1) Supposons que H_1 est caractéristique dans G. Est-il distingué ?

(2) Supposons que H_1 est distingué dans G. Est-il caractéristique ?

(3) Supposons que H_1 soit distingué dans G et que H_2 soit caractéristique dans H_1. Est-ce que H_2 est distingué dans G ?

(4) Supposons que H_2 soit distingué dans G. Est-il distingué dans H_1 ?

(5) Supposons que H_2 soit distingué dans H_1 et H_1 distingué dans G, H_2 est-il distingué dans G ?

Exercice 4.42. Soit G un groupe. On considère l'application

$$\begin{aligned} f : G \times G &\longrightarrow G \times G \\ (x, y) &\longmapsto (y, x) \end{aligned}$$

(1) Montrer que f est un automorphisme du groupe $G \times G$.

(2) On suppose que G n'est pas réduit à son élément neutre. Montrer que f n'est pas un automorphisme intérieur.

Exercice⋆ 4.43. Soit $n \geq 2$ un entier. Soit α un automorphisme de $\mathfrak{S}_n$. Montrer que l'on a $\alpha(\mathfrak{A}_n) = \mathfrak{A}_n$.

Exercice⋆ 4.44. Soit G un groupe infini. Soit H un sous-groupe de G tel que $H \neq G$. Montrer que le complémentaire de H dans G est infini.

Exercice⋆ 4.45. Déterminer tous les sous-groupes du groupe symétrique $\mathfrak{S}_3$. Soient $G = \mathfrak{S}_3$ et $H = \{e, (12)\}$. Déterminer les classes à gauche (resp. à droite) de G suivant H.

Quels sont les sous-groupes distingués du groupe symétrique $\mathfrak{S}_3$?

Exercice⋆ 4.46. Montrer qu'il n'existe pas de sous-ensemble fini $A \subset \mathbf{Q}$ tel que A engendre le groupe $\mathbf{Q}$.

Exercice⋆ 4.47. On considère le groupe quotient $(\mathbf{Q}/\mathbf{Z}, +)$.

(1) Montrer que ce groupe est infini mais que tous ses éléments sont d'ordre fini.

(2) Montrer que, pour tout entier $n \geq 1$, ce groupe possède un unique sous-groupe de cardinal n.

Exercice⋆ 4.48. On considère dans cet exercice le cercle unité

$$\mathbf{U} = \{z \in \mathbf{C} \mid |z| = 1\}.$$

(1) Montrer que $\mathbf{U}$ est un sous-groupe de $\mathbf{C}^*$.

(2) Montrer que $\mathbf{R}/\mathbf{Z}$ est isomorphe à $\mathbf{U}$ (indication : considérer le morphisme de groupes $x \mapsto \exp(2\pi i x)$ de $\mathbf{R}$ dans $\mathbf{C}^*$).

(3) Montrer que $\mathbf{C}^*/\mathbf{U}$ est isomorphe à $(\mathbf{R}_+^*, \cdot\,)$.

(4) Pour tout entier $n \geq 1$, soit $\mu_n(\mathbf{C})$ le groupe de racines n-ièmes de l'unité (comme dans l'exercice 2.24). Montrer que $\mu_\infty(\mathbf{C}) = \cup_{n \geq 1} \mu_n(\mathbf{C})$ est un sous-groupe de $\mathbf{U}$ et que $\mu_\infty(\mathbf{C})$ est isomorphe à $\mathbf{Q}/\mathbf{Z}$.

Exercice⋆ 4.49. Soient G et G' deux groupes, $f : G \to G'$ un morphisme de groupes, et H' un sous-groupe distingué de G'. On appelle $H = f^{-1}(H')$. Montrer que H est distingué dans G. Soit K un sous-groupe distingué de G. Montrer que $f(K)$ est un sous-groupe de G', mais qu'il peut très bien ne pas être distingué.

Exercice⋆ 4.50. Soient m et n des entiers strictement positifs.

(1) Déterminer l'ensemble des morphismes $\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$.
(2) Déterminer $\mathrm{Aut}(\mathbf{Z}/m\mathbf{Z})$.
(3) Déterminer $\mathrm{Aut}(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z})$.

***Exercice⋆ 4.51* (Récapitulation)**. Déterminer les ensembles de morphismes de groupes

– de $\mathbf{Z}$ dans $\mathbf{Z}$ (exercice 4.17) ;
– de $\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$;
– de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{Z}$;
– de $\mathbf{Z}/m\mathbf{Z}$ dans $\mathbf{Z}/n\mathbf{Z}$ (exercice 4.50)).

Exercice⋆ 4.52. Combien de morphismes y a-t-il de $\mathbf{Z}/45\mathbf{Z}$ vers $\mathfrak{S}_3$? Et de $\mathfrak{S}_3$ vers $\mathbf{Z}/45\mathbf{Z}$? Et d'ailleurs, combien y a-t-il de morphismes de $\mathfrak{S}_n$ dans $\mathbf{Z}/m\mathbf{Z}$?

Exercice⋆ 4.53. Déterminer tous les morphismes de groupes de $\mathfrak{S}_n$ dans $\mathbf{C}^\times$.

Exercice⋆ 4.54. Soit G un groupe fini tel que $g^2 = e$ pour tout $g \in G$. Montrer que l'ordre de G est une puissance de 2. (Indication : établir d'abord que si $|G| \geq 2$, alors G admet un sous-groupe distingué d'ordre 2. Procéder ensuite par récurrence sur l'ordre de G).

***Exercice⋆ 4.55* (Groupes d'ordre 10)**. Soit G un groupe d'ordre 10.

(1) Montrer que G admet un élément ρ d'ordre 5.
(2) On fixe $\rho \in G$ d'ordre 5. Montrer que $N = \langle \rho \rangle$ est un sous-groupe distingué de G.
(3) Montrer que G contient un élément σ d'ordre 2.
(4) On fixe $\sigma \in G$ d'ordre 2. Montrer que

$$G = \{\sigma^i \rho^j \mid 0 \leq i \leq 1; 0 \leq j \leq 4\}.$$

(5) Montrer que si l'on a $\rho\sigma = \sigma\rho$, alors $G \cong \mathbf{Z}/10\mathbf{Z}$.

Dans la suite, on supposera que $\rho\sigma \neq \sigma\rho$.

(6) Montrer que $\sigma\rho^i\sigma^{-1} = \rho^{-i}$ pour tout $i \in \mathbf{Z}$. (Indication : Considérer l'application $f : \{e, \sigma\} \to \mathrm{Aut}(N)$ donnée par $f(e) = \mathrm{Id}$ et $f(\sigma) : \rho \mapsto \sigma\rho\sigma^{-1}$.)

(7) Montrer que G est isomorphe au sous-groupe de $\mathfrak{S}_5$ engendré par les permutations $(1, 4)(2, 3)$ et $(1, 2, 3, 4, 5)$.

(8) Montrer que G est isomorphe au groupe diédral D_{10} des isométries d'un pentagone régulier.

Exercice 4.56. Donner des exemples

(1) de deux groupes G et G' avec des sous-groupes distingués $H \subset G$ et $H' \subset G'$ tels que $H \cong H'$ et $G/H \cong G'/H'$ mais $G \ncong G'$;
(2) d'un groupe G avec deux sous-groupes distingués $H, H' \subset G$ avec $H \ncong H'$ mais $G/H \cong G/H'$;
(3) d'un groupe G avec deux sous-groupes distingués $H, H' \subset G$ avec $H \cong H'$ mais $G/H \ncong G/H'$.

Exercice 4.57. Soient G un groupe, H_1 et H_2 des sous-groupes distingués tels que $H_1 \cap H_2 = \{e\}$ et $G = H_1H_2$ (où H_1H_2 est le sous-groupe de G engendré par $H_1 \cup H_2$). Montrer que l'application

$$\begin{aligned} H_1 \times H_2 &\longrightarrow G \\ (h_1, h_2) &\longmapsto h_1h_2 \end{aligned}$$

est un isomorphisme (indication : on pourra montrer d'abord que pour h_1 dans H_1 et h_2 dans H_2 on a $h_2h_1 = h_1h_2$, en considérant $h_1h_2h_1^{-1}h_2^{-1}$).

Exercice 4.58. Soit $G \subset \mathbf{Q}$ un sous-groupe avec $G \neq \{0\}$. Montrer que tout élément de $\mathbf{Q}/G$ est d'ordre fini.

Montrer qu'il n'existe pas de groupes non-triviaux G_1, G_2 tels que $G_1 \times G_2 \cong \mathbf{Q}$.

Exercice 4.59. Soit G un groupe. Soient H un sous-groupe de G et K un sous-groupe distingué de G tels que $HK = G$ et $H \cap K = \{e\}$. Montrer que le groupe quotient G/K est isomorphe à H.

Exercice 4.60. Est-ce que le groupe des bijections de $\mathbf{N}$ contient des éléments d'ordre infini ? Est-ce que le produit de deux éléments d'ordre fini est lui aussi d'ordre fini ? Indication : les réponses sont les mêmes si on remplace $\mathbf{N}$ par $\mathbf{Z}$, ou par $\mathbf{Q}$, ou par $\mathbf{Q}^2$, par exemple.

Exercice 4.61. Soient G un groupe et $N \subset G$ un sous-groupe d'indice fini n.

(1) Supposons que N est distingué dans G. Montrer que pour tout x dans G on a $x^n \in N$.

(2) Donner un exemple où il existe x dans G avec x^n pas dans N.

(3) Soit H un sous-groupe d'indice fini de $\mathbf{C}^*$. Montrer que $H = \mathbf{C}^*$.

***Exercice* 4.62* (Examen, septembre 2007)**. Dans cet exercice on note $\mathbf{C} = (\mathbf{C}, +)$ le groupe additif des nombres complexes et $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\} \subset \mathbf{C}$.

(1) Montrer que $\mathbf{Z}$ et $\mathbf{Z}[i]$ sont des sous-groupes distingués de $\mathbf{C}$.

(2) Soit n un entier strictement positif. Montrer que la classe de $1/n$ dans $\mathbf{C}/\mathbf{Z}$ est un élément d'ordre n.

Montrer que les classes de $1/2$, de $i/2$ et de $1/2 + i/2$ dans $\mathbf{C}/\mathbf{Z}[i]$ sont des éléments d'ordre 2.

(3) Est-ce que $\mathbf{C}/\mathbf{Z}[i]$ est un groupe fini ? Est-ce que ce groupe contient des éléments d'ordre infini ?

(4) Combien y a-t-il d'éléments d'ordre 2 dans le groupe $\mathbf{C}/\mathbf{Z}$? Combien y a-t-il d'éléments d'ordre 2 dans le groupe $\mathbf{C}/\mathbf{Z}[i]$?

Les groupes $\mathbf{C}/\mathbf{Z}$ et $\mathbf{C}/\mathbf{Z}[i]$ sont-ils isomorphes ?

(5) Montrer que pour tout entier $n > 0$, l'ensemble des éléments $c \in \mathbf{C}/\mathbf{Z}[i]$ tels que $nc = 0$ est un sous-groupe isomorphe à $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$.

***Exercice* 4.63* (Examen, janvier 2008)**. Dans tout l'exercice on considère l'anneau $\mathbf{Z}/3\mathbf{Z}$ avec les opérations d'addition et de multiplication habituelles. Tous les morphismes $\mathbf{Z}^2 \to \mathbf{Z}/3\mathbf{Z}$ considérés sont des morphismes de groupes additifs.

(1) Soient $\alpha, \beta \in \mathbf{Z}/3\mathbf{Z}$. Montrer que l'application $f\colon \mathbf{Z}^2 \to \mathbf{Z}/3\mathbf{Z}$ donnée par $f(x, y) = \alpha\bar{x} + \beta\bar{y}$ est un morphisme de groupes.

(2) Montrer que ce morphisme f est surjectif si et seulement si $(\alpha, \beta) \neq (0, 0)$.

(3) Soit $g\colon \mathbf{Z}^2 \to \mathbf{Z}/3\mathbf{Z}$ un morphisme de groupes. Montrer qu'il existe un unique couple $\alpha, \beta \in \mathbf{Z}/3\mathbf{Z}$ tels que $g(x, y) = \alpha\bar{x} + \beta\bar{y}$ pour tout $(x, y) \in \mathbf{Z}^2$.

(4) Soit X l'ensemble des morphismes de groupes *surjectifs* $\mathbf{Z}^2 \to \mathbf{Z}/3\mathbf{Z}$. Montrer que $|X| = 8$.

(5) Quelles sont les unités de l'anneau $\mathbf{Z}/3\mathbf{Z}$?

Pour $f \in X$ et $\gamma \in (\mathbf{Z}/3\mathbf{Z})^\times$ soit l'application $\gamma f\colon \mathbf{Z}^2 \to \mathbf{Z}/3\mathbf{Z}$ donnée par $(x, y) \mapsto \gamma f(x, y)$. Montrer que $\gamma f \in X$ et que

$$\begin{aligned}(\mathbf{Z}/3\mathbf{Z})^\times \times X &\to X\\ (\gamma, f) &\mapsto \gamma f\end{aligned}$$

est une opération de $(\mathbf{Z}/3\mathbf{Z})^\times$ sur X.

(6) Déterminer les ordres des orbites pour cette opération. Combien y a-t-il d'orbites ?

(7) Soient $f, g \in X$. Montrer que f et g sont dans la même orbite pour l'opération ci-dessus si et seulement si $\mathrm{Ker}(f) = \mathrm{Ker}(g)$.

(8) Trouver le nombre de sous-groupes de $\mathbf{Z}^2$ d'indice 3.

5. Groupes opérant

Exercice* 5.1. Le groupe $\mathrm{GL}(n; \mathbf{R})$ opère sur $\mathbf{R}^n$ (naturellement, c'est-à-dire par $(A, x) \mapsto A \cdot x$). Montrer qu'il opère aussi sur l'ensemble des droites vectorielles de $\mathbf{R}^n$, par $(A, L) \mapsto A(L)$. Montrer que cette opération est transitive.

Exercice* 5.2. (1) Donner la décomposition de $\mathbf{R}^2$ en orbites sous l'action du groupe des rotations $\mathrm{O}(2)$. Déterminer le stabilisateur d'un point.

(2) Mêmes questions pour l'opération du groupe $\mathrm{O}(n)$ sur $\mathbf{R}^n$.

***Exercice⋆ 5.3* (Le groupe affine)**. On considère le groupe affine G défini dans l'exercice 1.16 comme groupe opérant sur $\mathbf{R}$. Quel est le stabilisateur de 0 pour cette action ? Montrer que cette action est transitive.

Exercice⋆ 5.4. Soit $E \subset \mathfrak{S}_4$ l'ensemble des produits de deux transpositions à supports disjoints, explicitement

$$E = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

(c'est un ensemble à trois éléments). Le groupe $\mathfrak{S}_4$ opère par conjugaison sur E. En déduire un morphisme de groupes $\mathfrak{S}_4 \to \mathfrak{S}_3$, montrer qu'il est surjectif[(3)], quel est son noyau ?

Soit N le sous-groupe de $G = \mathfrak{S}_4$ engendré par E. Combien a-t-il d'éléments ? Montrer que N est sous-groupe distingué et que G/N est isomorphe à $\mathfrak{S}_3$.

***Exercice 5.5* (Le même)**. Le groupe des isométries qui préservent un tétraèdre régulier est isomorphe à $\mathfrak{S}_4$ (exercice 4.37). Montrer que tout élément de ce groupe envoie la perpendiculaire commune à deux arêtes opposées sur la perpendiculaire commune à deux arêtes opposées. En déduire un homomorphisme surjectif

$$\mathfrak{S}_4 \longrightarrow \mathfrak{S}_3.$$

Quel est son noyau ?

Exercice⋆ 5.6. On se donne un ensemble X sur lequel agit un groupe fini d'ordre 156. On suppose qu'un élément $a \in X$ a un stabilisateur d'ordre 12. Quel est le cardinal de l'orbite de a ?

Exercice⋆ 5.7. Soit G un groupe opérant sur un ensemble X. Supposons que $|X| = 108$ et que $|G| = 143$. Montrer que G fixe au moins un point de X.

Exercice⋆ 5.8. Un groupe à 35 éléments opère sans point fixe sur un ensemble à 19 éléments. Combien y a-t-il d'orbites pour cette opération ?

Exercice⋆ 5.9. Un groupe d'ordre 63 peut-il agir transitivement sur un ensemble de cardinal 27 ?

***Exercice⋆ 5.10* (Examen, janvier 2008)**. Soit G un groupe fini d'ordre n dont l'élément neutre est noté e. On suppose que G a exactement deux classes de conjugaison.

(1) Montrer que $G \neq \{e\}$.

(2) Montrer que $G\backslash\{e\} = \{g \in G \mid g \neq e\}$ est une classe de conjugaison.

(3) Soit $g \in G$ avec $g \neq e$. Quel est l'ordre de l'orbite de g pour l'action de G sur lui-même par conjugaison ? Quel peut être l'ordre du stabilisateur de g pour cette action ?

(4) Montrer que $n = 2$ et que G est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

***Exercice⋆ 5.11* (Examen, janvier 2006)**. Soit $\mathbf{K}$ un corps. Le groupe $\mathrm{GL}(2;\mathbf{K})$ opère naturellement sur l'espace vectoriel $\mathbf{K}^2$ (c'est-à-dire par $A \cdot X = AX$).

(1) Combien cette opération a-t-elle d'orbites ?

(2) On suppose désormais que $\mathbf{K} = \mathbf{Z}/2\mathbf{Z}$, c'est-à-dire que $\mathbf{K}$ a deux éléments. Combien d'éléments non nuls y a-t-il dans $\mathbf{K}^2$? Montrer que le groupe $\mathrm{GL}(2;\mathbf{K})$ opère sur un ensemble à trois éléments, de façon que l'application $\mathrm{GL}(2;\mathbf{K}) \to \mathfrak{S}_3$ soit un isomorphisme de groupes.

***Exercice⋆ 5.12* (Examen, septembre 2006)**. Soient p un nombre premier et n un entier strictement positif. On considère un groupe fini G d'ordre p^n dont l'élément neutre sera noté e. Soit H un sous-groupe distingué de G tel que $H \neq \{e\}$. On considère l'application

$$\begin{aligned} \alpha : G \times H &\to H \\ (g,h) &\mapsto ghg^{-1}. \end{aligned}$$

(1) Montrer que α définit une opération de G sur H.

(2) Montrer que, pour cette opération, l'orbite de tout élément de H a un cardinal de la forme p^k avec k entier et $0 \leq k \leq n-1$.

(3) En déduire que H contient un élément du centre de G distinct de e.

[(3)] C'est exceptionnel ! On peut montrer que, pour $n \geq 5$, il n'existe pas de morphisme surjectif $\mathfrak{S}_n \to \mathfrak{S}_{n-1}$.

Exercice⋆ 5.13. Soit G un p-groupe (c'est-à-dire un groupe d'ordre p^n avec p premier), opérant sur un ensemble X.

(1) Montrer qui si

$$X^G = \{x \in X \mid \forall\, g \in G\ g.x = x)\,,$$

alors on a

$$|X| = |X^G| + \sum_{w(x),x\notin X^G} |w(x)|.$$

(2) Montrer que $|X| \equiv |X^G| \mod p$.

(3) Faire opérer un p-groupe sur lui-même par conjugaison et montrer que son centre n'est pas réduit à l'élément neutre.

Exercice 5.14. Soit G un groupe fini opérant sur un ensemble fini X. On désigne par N le nombre de G-orbites. Pour tout $g \in G$, on pose $\mathrm{Fix}(g) = \{x \in X \mid\ gx = x\}$. On se propose de démontrer la *formule de Burnside*

$$N = \frac{1}{|G|} \sum_{g\in G} |\mathrm{Fix}(g)|.$$

(1) Soient E et F des ensembles finis et $S \subset E \times F$. Pour tout $a \in E$ et pour tout $b \in F$, on pose

$$V_a = \{v \in F \mid\ (a, v) \in S\} \quad \text{et} \quad H_b = \{u \in E \mid\ (u, b) \in S\}.$$

Montrer que l'on a

$$\sum_{a\in E} |V_a| = \sum_{b\in F} |H_b|.$$

(2) Démontrer la formule de Burnside en appliquant le résultat de la question précédente à

$$S = \{(g, x) \in G \times X \mid\ gx = x\} \subset G \times X.$$

Exercice 5.15. On reprend les notations de l'exercice 2.10, où sont définis un sous-groupe G de $\mathrm{GL}(2;\mathbf{R})$ et un sous-groupe H_2 de celui-ci.

(1) Interpréter G comme le stabilisateur d'un élément pour une action convenable de $\mathrm{GL}(2;\mathbf{R})$ (sur un ensemble à déterminer).

(2) Montrer que H_2 est un sous-groupe distingué de G (ce qui est aussi une conséquence de l'exercice 4.8).

(3) Montrer que G/H_2 est isomorphe à $\mathbf{R}^*$ (même remarque).

Exercice 5.16. Soient G un groupe et H un sous-groupe de G. On fait agir G sur l'ensemble G/H par multiplication à gauche. Soit $\rho\colon G \to \mathrm{Bij}(G/H)$ le morphisme de groupes associé à cette action.

(1) Soit $g \in G$. Montrer que le stabilisateur de gH est gHg^{-1}.

(2) En déduire que l'on a

$$\mathrm{Ker}(\rho) = \bigcap_{g\in G} gHg^{-1}.$$

Exercice 5.17. Soit G un groupe opérant à gauche sur un ensemble X. On considère

$$F = \{f : X \to \mathbf{R}\}$$

l'ensemble des fonctions sur X à valeurs dans $\mathbf{R}$. Montrer que l'application

$$\begin{array}{ccc} F \times G & \longrightarrow & F \\ (f, a) & \longmapsto & (x \mapsto f(ax)) \end{array}$$

définit une opération (à droite) de G sur F. Le choix de $\mathbf{R}$ est-il essentiel ? Est-ce qu'on aurait pu prendre un ensemble quelconque au lieu de $\mathbf{R}$?

***Exercice⋆ 5.18* (Examen, janvier 2007)**. Soit G un groupe. On suppose que G contient un sous-groupe H d'indice n.

(1) Combien y a-t-il de classes à gauche modulo H ? En faisant opérer G par translation à gauche sur l'ensemble G/H de ces classes, montrer qu'il existe un homomorphisme de groupes non trivial

$$G \longrightarrow \mathfrak{S}_n$$

de G dans le groupe symétrique $\mathfrak{S}_n$.

(2) En déduire que G contient un sous-groupe distingué K, qui est contenu dans H, et dont l'indice $[G : K]$ dans G est un diviseur de $n!$.

Exercice 5.19. Combien y a-t-il de classes de conjugaison dans le groupe $\mathfrak{S}_3$ (resp. $\mathfrak{S}_4$, resp. $\mathfrak{S}_6$) ?

Exercice 5.20. On se donne un entier $n \geq 2$. Décrire le centralisateur de la transposition $\tau = (12)$ dans le groupe $\mathfrak{S}_n$.

Exercice 5.21. Soient p un nombre premier, $s > 0$ un entier et G un groupe d'ordre p^s.

(1) Soit $s = 1$, donc G d'ordre p. Montrer que $G \cong \mathbf{Z}/p\mathbf{Z}$.

(2) Soit $s = 2$, donc G d'ordre p^2. Montrer que G est isomorphe à $\mathbf{Z}/p^2\mathbf{Z}$ ou à $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

Indication : Utiliser le fait que le centre $Z(G)$ de G n'est pas réduit à $\{e\}$ (voir le cours ou l'exercice 5.13), puis en déduire que $G/Z(G)$ est un groupe cyclique et que cela implique que G est commutatif.

Exercice 5.22. On se propose de déterminer tous les groupes finis qui ont exactement trois classes de conjugaison. Soit donc G un groupe fini, disons d'ordre n, et supposons que G a exactement trois classes de conjugaison.

(1) En considérant l'opération de G sur lui-même par conjugaison, montrer qu'il existe des entiers $a \geq b > 0$ tels que $a|n$, $b|n$ et

$$(*) \qquad 1 = \frac{1}{n} + \frac{1}{a} + \frac{1}{b}.$$

(2) Déterminer les solutions de l'équation $(*)$ en nombres entiers $n \geq a \geq b > 0$ tels que $a|n$ et $b|n$. (Indication : on a $b \leq 3$ car $n \geq a \geq b$.)

(3) Donner la liste complète des groupes finis, à isomorphisme près, qui ont exactement trois classes de conjugaison.

Exercice 5.23. Soit $n \geq 0$. Notons Y l'ensemble des formes bilinéaires symétriques sur $\mathbf{R}^n$. On fait opérer $\mathrm{GL}(n;\mathbf{R})$ à droite sur Y comme dans l'exercice 5.17, c'est-à-dire par

$$\begin{array}{ccc} Y \times \mathrm{GL}(n;\mathbf{R}) & \longrightarrow & Y \\ (\varphi, g) & \longmapsto & ((u,v) \mapsto \varphi(g \cdot u, g \cdot v)). \end{array}$$

Combien y a-t-il d'orbites ?

Exercice 5.24. Soit G un groupe fini. Notons n l'ordre de G et p le plus petit nombre premier qui divise n. Supposons que $H \subset G$ est un sous-groupe d'indice p. Le but de l'exercice est de démontrer que H est distingué.

(1) Le groupe G opère sur G/H par translations à gauche, ce qui induit un morphisme $f : G \to \mathrm{Bij}(G/H)$. Montrer que $\mathrm{Ker}(f) \subset H$.

(2) Montrer que $|f(G)| = p$ (indication : quels sont les nombres premiers divisant $|\mathrm{Bij}(G/H)|$?).

(3) Montrer que $H = \mathrm{Ker}(f)$ et conclure.

Exercice 5.25. Soient $n \in \mathbf{N}$, $\sigma \in \mathfrak{S}_n$ et $\sigma = c_1 \cdots c_r$ une décomposition de σ comme produit de cycles à supports disjoints. On supposera dans tout l'exercice que dans une telle décomposition on écrit tous les cycles, même de longueur 1, de sorte que $\cup_{k=1}^{r} \mathrm{Supp}(c_k) = X_n = \{1, \ldots, n\}$.

(1) Montrer que pour tout sous-groupe $H \subset \mathfrak{S}_n$, l'action de $\mathfrak{S}_n$ sur X_n définit une action de H sur X_n.

(2) Soit $H = \langle \sigma \rangle$ le sous-groupe de $\mathfrak{S}_n$ engendré par σ. Montrer que si $i \in \mathrm{Supp}(c_k)$, alors $\mathrm{Supp}(c_k) = Hi$, l'orbite de i pour l'action de H.

(3) Déduire de la question précédente que r est le nombre d'orbites pour l'action de H et que les $\mathrm{Supp}(c_k)$ (pour $k = 1, \ldots, r$) sont les orbites pour cette action.

(4) Soit $\sigma = c'_1 \cdots c'_{r'}$ une autre décomposition de σ comme produit de cycles à supports disjoints. Montrer que $r' = r$ et que, à une permutation des c'_k près, on a $\mathrm{Supp}(c_k) = \mathrm{Supp}(c'_k)$ pour $k = 1, \ldots, r$.

(5) Avec les notations de la question précédente, montrer que $c_k = c'_k$ pour $k = 1, \ldots, r$.

Exercice 5.26. Soit $n \in \mathbf{N}$. Pour $\sigma \in \mathfrak{S}_n$, on note

$$\mathrm{Fix}(\sigma) = \{k \in \{1, \ldots, n\} \mid \sigma(k) = k\}$$

l'ensemble des points fixes de σ.

(1) Si $\sigma \in \mathfrak{S}_n$ avec $\sigma \neq (1)$, montrer qu'il existe un cycle c_1 de longueur $\ell_1 > 1$ et une permutation $\tau \in \mathfrak{S}_n$ tels que $\sigma = c_1\tau$ et $\mathrm{Fix}(\tau)$ est la réunion disjointe de $\mathrm{Fix}(\sigma)$ et du support de c_1.

(2) Montrer par récurrence décroissante sur $|\mathrm{Fix}(\sigma)|$ que toute permutation σ est un produit de cycles disjoints.

Exercice 5.27. Soient $n \geq 0$ et σ dans $\mathfrak{S}_n$.

(1) Soit m le nombre d'orbites de σ. Montrer que $\varepsilon(\sigma) = (-1)^{n-m}$.

(2) Soit s le nombre d'orbites de cardinal pair de σ. Montrer que $\varepsilon(\sigma) = (-1)^s$.

Exercice 5.28. Soient m et $n \geq 0$. Soit $f : \mathfrak{S}_n \to \mathfrak{S}_m$ un morphisme. Montrer que $f(\mathfrak{A}_n) \subset \mathfrak{A}_m$.

***Exercice 5.29* (Classes de conjugaison dans $\mathfrak{A}_n$)**. Soient $n \in \mathbf{N}$ et $\mathfrak{S}_n$ le groupe symétrique opérant sur l'ensemble $\{1, \ldots, n\}$. Le but de cet exercice est de déterminer les classes de conjugaison de $\mathfrak{A}_n$ en termes de celles de $\mathfrak{S}_n$.

Concernant les classes de conjugaison de $\mathfrak{S}_n$, on rappelle que $\sigma, \sigma' \in \mathfrak{S}_n$ sont conjuguées si et seulement si elles ont le même type, déterminé par leurs décomposition en cycles disjoints.

(1) Soit $\sigma \in \mathfrak{A}_n$. Montrer que la $\mathfrak{S}_n$-classe de conjugaison de σ est contenue dans $\mathfrak{A}_n$.

(2) Soit $H \subset \mathfrak{S}_n$ un sous-groupe. Montrer que $H \cap \mathfrak{A}_n \subset H$ est un sous-groupe d'indice 1 ou 2.

(3) On considère l'action de $\mathfrak{S}_n$ sur lui-même par conjugaison et pour $\sigma \in \mathfrak{S}_n$, on note C_σ le stabilisateur de σ pour cette action. Montrer que si $\sigma \in \mathfrak{A}_n$ est tel que $C_\sigma \not\subset \mathfrak{A}_n$, alors la $\mathfrak{A}_n$-classe de conjugaison de σ coïncide avec sa $\mathfrak{S}_n$-classe de conjugaison.

(4) Soit $\sigma \in \mathfrak{A}_n$ tel que $C_\sigma \subset \mathfrak{A}_n$. Montrer la $\mathfrak{S}_n$-classe de conjugaison de σ est la réunion de deux $\mathfrak{A}_n$-classes de conjugaison du même ordre.

Exercice 5.30. Soit $\mathbf{K}$ un corps fini, disons à q éléments et soit $V = \mathbf{K}^2$, espace vectoriel de dimension 2 sur $\mathbf{K}$. Le groupe $\mathrm{GL}(2;\mathbf{K})$ (des applications linéaires ou des matrices inversibles) opère sur V (par sa définition), de même que son sous-groupe $\mathrm{SL}(2;\mathbf{K})$ (des applications linéaires de déterminant 1) .

(1) Montrer que l'ordre du groupe $\mathrm{GL}(2;\mathbf{K})$ est $(q^2-1)(q^2-q)$ et que celui de $\mathrm{SL}(2;\mathbf{K})$ est $(q^2-1)(q^2-q)/(q-1)$.

(2) Soit $\mathbf{P}(V)$ l'ensemble des droites vectorielles de V. Montrer que cet ensemble a $q+1$ éléments, que $\mathrm{GL}(2;\mathbf{K})$ et son sous-groupe $\mathrm{SL}(2;\mathbf{K})$ opèrent sur cet ensemble. En déduire des homomorphismes

$$\varphi : \mathrm{SL}(2;\mathbf{K}) \longrightarrow \mathfrak{S}_{q+1} \text{ et } \widetilde{\varphi} : \mathrm{GL}(2;\mathbf{K}) \longrightarrow \mathfrak{S}_{q+1}.$$

(3) Supposons que $q = 2$, de sorte que $\mathbf{K} \cong \mathbf{Z}/2\mathbf{Z}$. Montrer que $\mathrm{GL}(2,\mathbf{K}) = \mathrm{SL}(2,\mathbf{K}) \cong \mathfrak{S}_n$.

(4) On suppose dans toute la suite que $q = 4$. Il existe un unique (à isomorphisme près) corps $\mathbf{K}$ à quatre éléments, dans lequel tous les éléments sont d'ordre 2 (pour l'addition) et le seul élément de carré 1 est 1 lui-même (voir l'exercice 6.3). Montrer que dans ce cas,

$$\varphi : \mathrm{SL}(2;\mathbf{K}) \longrightarrow \mathfrak{S}_5$$

est injective.

(5) Soit (e_1, e_2) la base canonique de V et soit $e_3 = e_1 + e_2$. Montrer qu'il existe une matrice A dans $\mathrm{SL}(2;\mathbf{K})$ qui vérifie

$$A(e_1) = e_2, \quad A(e_2) = e_3 \text{ et } A(e_3) = e_1.$$

Soient L_1, L_2 et L_3 trois droites vectorielles distinctes de V. Montrer qu'il existe des vecteurs non nuls tels que u_1, u_2 et $u_3 = u_1 + u_2$ engendrent respectivement les droites L_1, L_2 et L_3.

(6) En déduire que l'image de φ contient tous les 3-cycles et donc $\mathfrak{A}_5$. Montrer que $\mathrm{SL}(2;\mathbf{K})$ est isomorphe à $\mathfrak{A}_5$ (et donc en particulier qu'il est simple).

***Exercice 5.31* (Classes de conjugaison dans $\mathrm{GL}(2;\mathbf{C})$).** Dans tout l'exercice, on note $\mathrm{GL}(2;\mathbf{C})$ le groupe des matrices inversibles de type 2×2 à coefficients dans $\mathbf{C}$, la loi de groupe étant la multiplication des matrices. On se propose d'étudier les classes de conjugaison dans $\mathrm{GL}(2;\mathbf{C})$.

(1) Montrer que deux matrices diagonalisables $A, B \in \mathrm{GL}(2;\mathbf{C})$ sont conjuguées si et seulement si elles ont le même polynôme caractéristique.

(2) Supposons que $A \in \mathrm{GL}(2;\mathbf{C})$ ne soit pas diagonalisable. Montrer que A est alors conjuguée à une matrice de la forme $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ où $a \in \mathbf{C}$ avec $a \neq 0$. En déduire que deux matrices non diagonalisables $A, B \in \mathrm{GL}(2;\mathbf{C})$ sont conjuguées si et seulement si elles ont le même polynôme caractéristique.

(3) Soient

$$X_1 = \{P \in \mathbf{C}[X] \mid P(X) = X + a \text{ avec } a \neq 0\} \quad \text{et}$$
$$X_2 = \{P \in \mathbf{C}[X] \mid P(X) = X^2 + aX + b \text{ avec } b \neq 0\}.$$

Établir une bijection entre l'ensemble des classes de conjugaison de $\mathrm{GL}(2,\mathbf{C})$ et l'ensemble $X_1 \cup X_2$.

***Exercice 5.32* (Groupes résiduellement finis).** Si G est un groupe, on note e_G son élément neutre. On dit qu'un groupe G est *résiduellement fini* s'il vérifie la propriété suivante : pour tout $x \in G$ tel que $x \neq e_G$, il existe un groupe fini F et un homomorphisme $f\colon G \to F$ tel que $f(x) \neq e_F$.

(1) Montrer que tout groupe fini est résiduellement fini.

(2) Montrer que le groupe $\mathbf{Z}$ est résiduellement fini.

(3) Montrer que tout sous-groupe d'un groupe résiduellement fini est résiduellement fini.

(4) Soient G_1 et G_2 des groupes résiduellement finis. Montrer que le groupe $G_1 \times G_2$ est résiduellement fini.

(5) Montrer que le groupe $\mathbf{Q}$ n'est pas résiduellement fini.

***Exercice 5.33* (Groupes hopfiens).** Si G et H sont des groupes, on note $\mathrm{Hom}(G,H)$ l'ensemble des homomorphismes de G dans H. On dit qu'un groupe G est un groupe *de type fini* s'il existe un sous-ensemble fini $A \subset G$ tel que A engendre G. On dit qu'un groupe G est *hopfien* si tout endomorphisme surjectif de G est injectif.

(1) Soient G et H des groupes. On suppose qu'il existe un sous-ensemble fini $A = \{a_1, \ldots, a_n\} \subset G$ de cardinal n qui engendre G. On considère l'application $\alpha\colon \mathrm{Hom}(G,H) \to H^n$ qui associe à tout homomorphisme $h \in \mathrm{Hom}(G,H)$ l'élément $\alpha(h) \in H^n$ défini par

$$\alpha(h) = (h(a_1), \ldots, h(a_n)).$$

(a) Montrer que l'application α est injective.

(b) En déduire que si H est fini, alors l'ensemble $\mathrm{Hom}(G,H)$ est fini.

(2) Soient G et H des groupes. Soit $\rho\colon G \to G$ un homomorphisme surjectif. Montrer que l'application $\Phi\colon \mathrm{Hom}(G,H) \to \mathrm{Hom}(G,H)$ définie par $\Phi(h) = h \circ \rho$ est injective.

(3) Soient G un groupe de type fini et $\rho\colon G \to G$ un homomorphisme surjectif. Soit F un groupe fini. Montrer que pour tout $f \in \mathrm{Hom}(G,F)$, il existe $h \in \mathrm{Hom}(G,F)$ tel que $f = h \circ \rho$.

(4) Montrer que tout groupe de type fini résiduellement fini est hopfien.

6. Anneaux

Sauf mention explicite du contraire, tous les anneaux sont supposés commutatifs et unitaires.

Exercice** *6.1. Déterminer toutes les structures d'anneaux possibles sur les ensembles à deux et trois éléments.

Exercice** *6.2. On considère le groupe additif $(\mathbf{Z}/4\mathbf{Z}, +)$. On suppose que $\star$ est une multiplication sur ce groupe qui est commutative, associative, et distributive sur l'addition. L'élément $\overline{2}$ peut-il être élément neutre de $\star$? Déterminer toutes les structures d'anneau sur $\mathbf{Z}/4\mathbf{Z}$.

Exercice** *6.3. On considère le groupe additif $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. On le munit d'une loi $\star$ qui en fait un anneau. On nomme ses éléments $0, 1, a, b$ (0 et 1 sont respectivement les éléments neutres pour $+$ et $\star$).

– Montrer que $a + b = 1$.

– On suppose qu'un des éléments, disons a, est de carré nul. Montrer qu'alors $ab = a$ et $b^2 = 1$.

– On suppose que a^2 et $b^2 \neq 0$ mais que $ab = 0$. Montrer qu'alors $a^2 = a$ et $b^2 = b$. Montrer que l'anneau obtenu est isomorphe à l'anneau produit $(\mathbf{Z}/2\mathbf{Z}, +, \cdot) \times (\mathbf{Z}/2\mathbf{Z}, +, \cdot)$.

– On suppose maintenant que a^2, b^2 et ab sont non nuls. Montrer qu'alors $a^2 = b$, $b^2 = a$ et $ab = 1$. Montrer que l'anneau obtenu est un corps.

– Montrer qu'il existe un unique (à isomorphisme près) corps à quatre éléments.

Exercice⋆ 6.4. Combien d'anneaux commutatifs (unitaires) y a-t-il, à isomorphisme près, de cardinal n, pour $0 \leq n \leq 6$?

Exercice⋆ 6.5. Est-ce que $\{-1, 0, 1\}$ est un sous-anneau de $\mathbf{Z}$?

Exercice⋆ 6.6. Soit $n \geq 1$ un entier.

(1) Résoudre l'équation $M^3 = I_n$ dans l'anneau $\mathcal{M}(n, \mathbf{R})$.

(2) Résoudre la même équation dans l'anneau $\mathcal{M}(n, \mathbf{C})$.

***Exercice⋆ 6.7* (Anneaux de Boole)**. On dit qu'un anneau A est un *anneau de Boole* si, pour tout $x \in A$, on a $x^2 = x$. On ne suppose pas ici *a priori* que A est commutatif, ni qu'il est unitaire.

(1) Vérifier que $(\mathbf{Z}/2\mathbf{Z}, +, \times)$ est un anneau de Boole.

(2) Soit E un ensemble. On note $\mathcal{P}(E)$ l'ensemble des parties de E. On reprend la loi Δ de l'exercice 1.2. Vérifier que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau de Boole.

(3) Soit A un anneau de Boole. Montrer que l'on a $x + x = 0$ pour tout $x \in A$.

(4) Montrer que tout anneau de Boole est commutatif.

(5) Soit A un anneau de Boole. Soient x et y des éléments de A. Calculer $xy(x + y)$. En déduire qu'un anneau de Boole ayant au moins trois éléments ne peut pas être intègre.

Exercice⋆ 6.8. Soit A un anneau (commutatif mais pas nécessairement unitaire). On munit $B = A \times \mathbf{Z}$ des lois

$$(a, m) + (b, n) = (a + b, m + n) \text{ et } (a, m) \cdot (b, n) = (mb + na + ab, mn).$$

Montrer que B est un anneau (commutatif et unitaire).

Exercice⋆ 6.9. Soient A un anneau, a et b dans A. Montrer que ab est inversible si et seulement si a et b le sont.

Exercice⋆ 6.10. Pour tout entier n avec $0 \leq n \leq 10$, faire la liste des éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$, et de leurs inverses. Dans chacun des cas, identifier le groupe des éléments inversibles.

Exercice⋆ 6.11. Soit $A \subset \mathbf{R}$ l'ensemble des nombres décimaux, c'est-à-dire les éléments avec un développement décimal fini. Montrer que A est un sous-anneau de $\mathbf{R}$ et que $A \subset \mathbf{Q}$.

Exercice⋆ 6.12. On considère l'ensemble $\mathbf{Z}[i]$ des nombres complexes de la forme $a + ib$ avec $a, b \in \mathbf{Z}$. Montrer que $\mathbf{Z}[i]$ est un sous-anneau de $\mathbf{C}$. Quelles sont ses unités ?

Exercice⋆ 6.13. Soit A le sous-anneau (unitaire) de $\mathbf{C}$ engendré par $2i$. Montrer que A est l'ensemble des $a + 2bi$ avec a et b des entiers. Faire la liste des éléments de $A^\times$.

Exercice⋆ 6.14. Soit X un ensemble. On considère l'ensemble

$$\mathcal{F}(X) = \{f : X \to \mathbf{R}\}$$

de toutes les applications de X dans $\mathbf{R}$, muni des lois $+$ et $\cdot$ induites par celles de $\mathbf{R}$. Vérifier que $(\mathcal{F}(X), +, \cdot)$ est un anneau. À quelle condition est-il intègre ?

Exercice⋆ 6.15. Soit A un anneau fini. Montrer que tout élément qui n'est pas diviseur de zéro est inversible. Et si on ne suppose pas que A est fini ?

Exercice 6.16. Soit $\mathcal{C}(\mathbf{R}, \mathbf{R})$ l'anneau des applications continues de $\mathbf{R}$ dans $\mathbf{R}$. Montrer que les diviseurs de zéro dans $\mathcal{C}(\mathbf{R}, \mathbf{R})$ sont les $f : \mathbf{R} \to \mathbf{R}$ telles que $f^{-1}(0)$ est d'intérieur non vide.

Exercice 6.17. Soit $U \subset \mathbf{C}$ un ouvert, et soit A l'anneau des fonctions holomorphes $f : U \to \mathbf{C}$. Montrer que A est intègre si et seulement si U est connexe et non vide.

7. Morphismes d'anneaux, idéaux

***Exercice*⋆ 7.1**. L'application $f : \mathbf{R}[X] \to \mathbf{R}$ définie par $P \mapsto P'(0)$ est-elle un homomorphisme d'anneaux ? Et l'application

$$\begin{array}{rcl} g : \mathbf{R}[X] & \longrightarrow & M(2;\mathbf{R}) \\ P & \longmapsto & \begin{pmatrix} P(0) & P'(0) \\ 0 & P(0) \end{pmatrix} ? \end{array}$$

***Exercice*⋆ 7.2**. Montrer qu'il n'existe pas de morphisme d'anneau de $\mathbf{Z}/3\mathbf{Z}$ dans $\mathbf{Z}/4\mathbf{Z}$.

***Exercice*⋆ 7.3**. Soit A un anneau (pas nécessairement unitaire). Montrer que $(\mathrm{End}(A,+),+,\circ)$ est un anneau (en général pas commutatif). Pour tout élément a de A, notons m_a l'application $x \mapsto ax$ de A vers A.

(1) Montrer que l'application $A \to \mathrm{End}(A,+)$, $a \mapsto m_a$, est un morphisme d'anneaux.
(2) Montrer que si A est unitaire, ce morphisme est injectif.
(3) Donner des exemples où le morphisme $A \to \mathrm{End}(A,+)$ défini ci-dessus est un isomorphisme, et où il n'en est pas.

***Exercice*⋆ 7.4**. Soit $n \in \mathbf{Z}$. Rappeler quelles sont les unités de $\mathbf{Z}/n\mathbf{Z}$. Montrer que l'application

$$\begin{array}{rcl} \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z},+) & \longrightarrow & \mathbf{Z}/n\mathbf{Z} \\ f & \longmapsto & f(1 \bmod n) \end{array}$$

induit un isomorphisme du groupe $(\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z},+),\circ)$ sur le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ des éléments inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$.

***Exercice*⋆ 7.5**. Déterminer les automorphismes d'anneau de $\mathbf{Z}/n\mathbf{Z}$.

***Exercice*⋆ 7.6**. Soit A un anneau (commutatif). Soit I un idéal de A. Montrer que les conditions suivantes sont équivalentes :

(1) $I = A$;
(2) I contient un élément inversible de A.

***Exercice*⋆ 7.7**. Soit A un anneau commutatif intègre. Soient a et b des éléments non nuls de A. On note (a) (resp. (b)) l'idéal de A engendré par a (resp. b). Montrer que les conditions suivantes sont équivalentes :

(1) on a $(a) = (b)$;
(2) il existe un élément inversible $u \in A$ tel que $a = ub$.

***Exercice*⋆ 7.8**. Montrer que l'ensemble

$$I = \{P \in \mathbf{Z}[X] \mid P(0) \text{ est divisible par } 5\}$$

est un idéal de l'anneau $\mathbf{Z}[X]$ et que cet idéal n'est pas principal.

***Exercice*⋆ 7.9 (Examen, janvier 2008)**. Soit $A = \{m + in\sqrt{5} \mid m, n \in \mathbf{Z}\} \subset \mathbf{C}$.

(1) Montrer que A est un sous-anneau de $\mathbf{C}$.
(2) Le but de cette question est de trouver les unités de A.
   (a) Montrer que si $a \in A$, alors $|a|^2 \in \mathbf{Z}$.
   (b) Supposons que $a \in A$ est une unité, avec inverse b. Montrer que $|a|^2|b|^2 = 1$ puis que $|a|^2 = 1$.
   (c) Trouver les unités de A.
(3) Montrer que si $ab = 2$ alors $a = \pm 1, \pm 2$.
(4) Soit $I = \{2a + b(1 + i\sqrt{5}) \mid a, b \in A\}$. Montrer que $I \subset A$ est un idéal.
Montrer que $1 \notin I$ et en déduire que $I \neq A$.
(5) Montrer que I n'est pas un idéal principal.
On pourra raisonner par l'absurde et supposer que $I = (a)$. En utilisant le fait que $2 \in I$ et la question 3 on pourra alors déterminer les valeurs possibles de a et arriver à une contradiction.

***Exercice⋆ 7.10* (Examen, janvier 2006)**. Soient $\mathcal{I}$ et $\mathcal{J}$ deux idéaux d'un anneau commutatif $(A, +, \cdot)$. On définit une partie $\mathcal{I} + \mathcal{J}$ de A par

$$\mathcal{I} + \mathcal{J} = \{b + c \mid b \in \mathcal{I} \text{ et } c \in \mathcal{J}\}.$$

Montrer que $\mathcal{I} + \mathcal{J}$ et $\mathcal{I} \cap \mathcal{J}$ sont des idéaux de A.

On suppose que $A = \mathbf{Z}$, que $\mathcal{I} = (m)$ et que $\mathcal{J} = (n)$. Déterminer deux éléments r et s de $\mathbf{Z}$ tels que

$$\mathcal{I} + \mathcal{J} = (r) \text{ et } \mathcal{I} \cap \mathcal{J} = (s).$$

***Exercice⋆ 7.11* (Examen, septembre 2006)**. Soit $A = \{z \in \mathbf{C} \mid z = m + ni \text{ avec } m, n \in \mathbf{Z}\}$.

(1) Montrer que A est un sous anneau unitaire de $\mathbf{C}$.

(2) Soit $z \in \mathbf{C}$. Montrer qu'il existe $q \in A$ tel que $|z - q| \leq \sqrt{2}/2 < 1$. (Indication : Faire un dessin représentant A comme sous-ensemble du plan complexe.)

(3) Soient $a, b \in A$ avec $b \neq 0$. Montrer qu'il existe $q, r \in A$ tels que $a = bq + r$ et $|r| < |b|$. (Indication : Appliquer la question précédente à $z = a/b$.)

(4) Soit $I \subset A$ un idéal avec $I \neq \{0\}$. Montrer qu'il existe $b \in I$ avec $b \neq 0$ et tel que $|a| \geq |b|$ pour tout $a \in I$ $(a \neq 0)$. Montrer qu'un tel élément b engendre I (c'est à dire que $I = (b) = bA$).

(5) Montrer que A est un anneau principal, c'est-à-dire que tout idéal de A est principal.

***Exercice⋆ 7.12* (Examen, septembre 2008)**. Soient $\mathbf{Z}[\sqrt{2}]$ et $\mathbf{Z}[\sqrt{3}]$ les sous-anneaux de $\mathbf{C}$ engendrés par $\mathbf{Z}$ et $\sqrt{2}$, respectivement par $\mathbf{Z}$ et $\sqrt{3}$.

(1) Montrer que

$$\mathbf{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\right\}$$

et que

$$\mathbf{Z}[\sqrt{3}] = \left\{a + b\sqrt{3} \mid a, b \in \mathbf{Z}\right\}.$$

(2) On suppose que $\varphi : \mathbf{Z}[\sqrt{2}] \to \mathbf{Z}[\sqrt{3}]$ est un morphisme d'anneaux.
   (a) Que vaut $\varphi(1)$?
   (b) Que vaut $(\varphi(\sqrt{2}))^2$?

(3) Montrer qu'il n'existe pas de morphisme d'anneaux de $\mathbf{Z}[\sqrt{2}]$ dans $\mathbf{Z}[\sqrt{3}]$.

Exercice 7.13. Montrer que l'anneau des nombres décimaux (voir 6.11) est un anneau principal.

Exercice⋆ 7.14. Soit A un anneau. Un élément x de A est dit *nilpotent* s'il existe un entier $n > 0$ tel que $x^n = 0$. Soit x dans A. Montrer que si x est nilpotent, alors $1 - x$ est inversible (indication : calculer le produit $(1 - x)(1 + x + x^2 + \cdots)$).

Exercice⋆ 7.15. Soit A un anneau commutatif. On note N l'ensemble des éléments nilpotents de A. Montrer que N est un idéal de A.

Exercice⋆ 7.16. Soit A un anneau commutatif. On appelle *radical* d'un idéal I de A l'ensemble noté $R(I)$ formé des $x \in A$ tels qu'il existe un entier $n \geq 1$ vérifiant $x^n \in I$.

(1) Soit I un idéal de A. Montrer que $R(I)$ est un idéal de A. Montrer que l'on a $I \subset R(I)$ et $R(R(I)) = R(I)$.

(2) Soient I et J des idéaux de A. Montrer que l'on a $R(I \cap J) = R(I) \cap R(J)$.

(3) Quel est le radical de $\{0\}$?

Exercice⋆ 7.17. Montrer que l'anneau quotient $\mathbf{Z}[i]/(1 + 3i)$ est isomorphe à $\mathbf{Z}/10\mathbf{Z}$.

Exercice⋆ 7.18. Soient k un corps, a dans k et P dans $k[X]$.

(1) Montrer que le reste de la division euclidienne de P par $X - a$ est $P(a)$.

(2) Montrer que $P(a) = 0$ si et seulement si P appartient à l'idéal principal $(X - a)$ de $k[X]$.

(3) Supposons que $P \neq 0$. Montrer qu'il existe au plus $\deg P$ éléments $x \in k$ tels que $P(x) = 0$.

Exercice⋆ 7.19. Montrer que dans l'anneau $\mathbf{Z}[X]$ l'idéal (X) est premier mais non maximal.

Exercice 7.20. Soient A un anneau et a dans A. Notons $\varepsilon_a : A[X] \to A$ l'application $P \mapsto P(a)$ qui évalue P en a.

(1) Montrer que ε_a est un morphisme d'anneaux.
(2) Montrer que ε_a est surjectif.
(3) Montrer que $\mathrm{Ker}(\varepsilon_a)$ est l'idéal $(X-a)$ engendré par $X-a$, et que ε_a induit un isomorphisme de $A[X]/(X-a)$ vers A.

Exercice⋆ 7.21. Soient A et B des anneaux commutatifs et $f\colon A \to B$ un morphisme d'anneau. Soit J un idéal de B. On pose $I = f^{-1}(J)$. Montrer que I est un idéal de A. Montrer que si J est un idéal premier de B, alors I est un idéal premier de A.

Exercice⋆ 7.22. Soient X un ensemble et $\mathbf{K}$ un corps commutatif. On considère l'ensemble

$$\mathcal{F}(X) = \{f : X \to \mathbf{K}\}$$

de toutes les applications de X dans $\mathbf{K}$, muni de sa structure naturelle d'anneau (c'est-à-dire des lois $+$ et $\cdot$ induites par celles de $\mathbf{K}$).

(1) Déterminer les éléments inversibles de l'anneau $\mathcal{F}(X)$.
(2) Soit $x_0 \in X$. Montrer que l'ensemble M_{x_0} défini par

$$M_{x_0} = \{f \in \mathcal{F}(X) \mid f(x_0) = 0\}$$

est un idéal maximal de $\mathcal{F}(X)$.

Exercice 7.23. Soit a dans $\mathbf{R}$. Posons $A = \mathcal{C}(\mathbf{R}, \mathbf{R})$ et $I = \{f \in A \mid f(a) = 0\}$.

(1) Montrer que I est un idéal de A.
(2) Montrer que I n'est pas principal.
(3) Que se passe-t-il si on remplace A par $\mathbf{R}[X]$, ou par $\mathcal{C}^\infty(\mathbf{R}, \mathbf{R})$, ou par $\mathbf{R}^{\mathbf{R}}$?

***Exercice⋆ 7.24* (Examen, septembre 2007)**. Étant donné un anneau A, on désigne par $N(A)$ l'ensemble des éléments non inversibles de A.

(1) Déterminer $N(A)$ pour $A = \mathbf{Z}$, pour $A = \mathbf{Z}/4\mathbf{Z}$ et pour $A = \mathbf{Z}/6\mathbf{Z}$.

On dit qu'un anneau A est un *anneau local* si l'ensemble $N(A)$ est stable pour l'addition, c'est-à-dire si l'on a $a + b \in N(A)$ quels que soient $a \in N(A)$ et $b \in N(A)$.

(2) Montrer que si A est un anneau local, alors $N(A)$ est un idéal.
(3) L'anneau $\mathbf{Z}$ est-il un anneau local ?
(4) Montrer que l'anneau $\mathbf{Z}/4\mathbf{Z}$ est un anneau local mais que l'anneau $\mathbf{Z}/6\mathbf{Z}$ n'est pas un anneau local.
(5) Soit A un anneau local. Montrer que $N(A)$ est un idéal maximal de A et ensuite que $N(A)$ est l'unique idéal maximal de A.
(6) On se donne un entier $n \geq 2$. Montrer que les conditions suivantes sont équivalentes :
   (a) Il existe un nombre premier p et un entier $\alpha \geq 1$ tels que $n = p^\alpha$.
   (b) L'anneau $\mathbf{Z}/n\mathbf{Z}$ est un anneau local.

***Exercice⋆ 7.25* (Examen, septembre 2008)**. Soit A un anneau intègre. On suppose que A ne contient qu'un nombre fini d'idéaux.

Pour $a \in A$ un élément non nul et $n \in \mathbf{N}$, on considère l'idéal engendré par a^n. Montrer que ces idéaux ne sont pas tous distincts. En déduire que a est inversible dans A et que A est un corps. Combien A a-t-il d'idéaux ?

8. Corps

Exercice⋆ 8.1. Montrer que tout morphisme de corps est injectif.

Exercice⋆ 8.2. On considère l'ensemble

$$\mathbf{Z}_{(3)} = \left\{x \in \mathbf{Q} \mid x = \frac{a}{b} \text{ avec } b \text{ non divisible par } 3\right\}.$$

Montrer que $\mathbf{Z}_{(3)}$ est un sous-anneau de $\mathbf{Q}$, qu'il contient $\mathbf{Z}$, que ce n'est pas un corps et que pour tout $x \in \mathbf{Q}$, soit x, soit $x^{-1} \in \mathbf{Z}_{(3)}$. Montrer que si A est un sous-anneau de $\mathbf{Q}$ contenant $\mathbf{Z}_{(3)}$, alors $A = \mathbf{Z}_{(3)}$ ou $\mathbf{Q}$. Quelles sont les unités de cet anneau ? Quel est le corps des fractions de cet anneau ?

Mêmes questions en remplaçant 3 par n'importe quel nombre premier p.

Exercice⋆ 8.3. Notons $\mathbf{Q}(i)$ le sous-anneau (unitaire) de $\mathbf{C}$ engendré par $\mathbf{Q} \cup \{i\}$.

(1) Montrer que $\mathbf{Q}(i)$ est l'ensemble des $a + bi$ avec a et b dans $\mathbf{Q}$.
(2) Montrer que $\mathbf{Q}(i)$ est un corps.

***Exercice⋆ 8.4* (Examen, janvier 2007)**. On considère, dans l'anneau $\mathbf{R}[X]$ des polynômes à une indéterminée sur $\mathbf{R}$, la partie

$$\mathcal{I} = \left\{ A \in \mathbf{R}[X] \mid \text{il existe un polynôme } B \text{ tel que } A(X) = (X^2+1)B(X) \right\}.$$

(1) Montrer que $\mathcal{I}$ est un idéal de $\mathbf{R}[X]$.
(2) Soit $\mathcal{J}$ un idéal de $\mathbf{R}[X]$ tel que $\mathcal{J} \supset \mathcal{I}$ et $\mathcal{J} \neq \mathcal{I}$. Montrer que $\mathcal{J}$ contient un polynôme de degré 0 ou 1, puis que $\mathcal{J}$ contient un polynôme constant non nul.
(3) Montrer que l'idéal $\mathcal{I}$ est maximal. Que peut-on dire de l'anneau quotient $\mathbf{R}[X]/\mathcal{I}$?
(4) Montrer que l'anneau $\mathbf{R}[X]/\mathcal{I}$ est isomorphe à $\mathbf{C}$.

Exercice⋆ 8.5. À quel corps le quotient $\mathbf{R}[X]/(X^2 + X + 1)$ est-il isomorphe ?

Exercice⋆ 8.6. Y a-t-il une structure de corps sur $\mathbf{Z}/4\mathbf{Z}$ dont le groupe additif sous-jacent est le groupe $(\mathbf{Z}/4\mathbf{Z}, +)$?

Exercice⋆ 8.7. Faire la liste de tous les corps à cinq éléments ou moins.

Exercice⋆ 8.8. Soit $\mathbf{F}_2$ le corps à deux éléments ($\mathbf{F}_2 \cong \mathbf{Z}/2\mathbf{Z}$). Soit $L = \mathbf{F}_2[X]/(X^2 + X + 1)$. Montrer que L est un corps à quatre éléments, et écrire ses tables d'addition et de multiplication. Vérifier que L est isomorphe au corps construit dans l'exercice 6.3.

Que se passe-t-il si on remplace $X^2 + X + 1$ par $X^2 + 1$?

Exercice 8.9. Faites la division euclidienne, dans $\mathbf{F}_2[X]$, de $X^{64} + X$ par $X^{16} + X$.

Exercice 8.10. Déterminer les degrés des extensions de corps suivantes : $\mathbf{R} \subset \mathbf{C}$, $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2})$, $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2})$ et $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}, i)$.

Exercice 8.11. Montrer que $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$, $\mathbf{Q}(2^{1/6}) = \mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$ et que $[\mathbf{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbf{Q}] = 6$. (Indication : pour la dernière égalité, donner une base du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$).

Exercice 8.12. Soit $F = X^3 + 3X - 2$ dans $\mathbf{Q}[X]$.

(1) Montrer que $\mathbf{Q}[X]/(F)$ est un corps.
(2) Est-il isomorphe à un sous-corps de $\mathbf{R}$?
(3) Est-il isomorphe à un sous-corps de $\mathbf{C}$ non contenu dans $\mathbf{R}$?
(4) Combien F a-t-il de racines dans $\mathbf{Q}[X]/(F)$?
(5) Notons u la classe de X dans $\mathbf{Q}[X]/(F)$. Montrer que $(1, u, u^2)$ est une $\mathbf{Q}$-base de $\mathbf{Q}[X]/(F)$.
(6) Exprimer $(2u^2 + u - 3)(3u^2 - 4u + 1)$ et $(u^2 - u + 4)^{-1}$ dans cette base.

Références

[1] M. Artin – *Algebra*, Prentice Hall, 1990.

[2] A. Bouvier & D. Richard – *Groupes*, Actualités Scientifiques et Industrielles, Hermann, Paris, 1979, Observation, théorie pratique, édition corrigée.

[3] J. Calais – *Eléments de théorie des groupes*, Mathématiques, Presses Universitaires de France, Paris, 1984.

[4] L. Carroll – *Logique sans peine*, Hermann, Paris, 1966, Traduit et présenté par J. Gattégno et E. Coumet, illustré par Max Ernst.

[5] R. Godement – *Cours d'algèbre*, Collection Enseignement des Sciences, Hermann, Paris, 1987, troisème édition.

[6] D. Guin – *Algèbre, tome 1, Groupes et anneaux*, Espaces34 et Belin, 1998.

[7] D. Perrin – *Cours d'algèbre*, Ellipses, 1996.

Version du 9 décembre 2008

M. Audin, V. Blanlœil, G. Collinet, M. Coornaert, R. Noot, J. Poineau, Institut de Recherche Mathématique Avancée, Université Louis Pasteur et cnrs