CAPES de Mathématiques
Préparation à l'écrit
Algèbre et probabilités

Université Joseph Fourier
Année 2007-2008

Fiche 7 : Algèbre (1) Groupes

« L'être humain n'est pas un tueur. Le groupe, si. » Konrad Lorenz

1 Rappels de cours

Une loi de composition (interne) sur un ensemble E est une application $* : E \times E \to E$. On note $x * y$ l'image de (x, y) par $*$. La loi $*$ est associative si et seulement si, pour tous x, y et z éléments de E, $(x * y) * z = x * (y * z)$. La loi $*$ est commutative si et seulement si, pour tous x et y éléments de E, $x * y = y * x$. Un élément e de E est un neutre pour la loi $*$ si et seulement si, pour tout x élément de E, $x * e = e * x = x$. Quand la loi possède un élément neutre e, un inverse d'un élément x de E est un élément y de E tel que $x * y = y * x = e$. Dans ce cas, on note souvent $y = x^{-1}$.

Un groupe $(G, *)$ est un couple formé d'un ensemble G et d'une loi de composition $*$ sur G, associative, admettant un élément neutre, et telle que tout élément possède un inverse. Si de plus, la loi $*$ est commutative, on dit que $(G, *)$ est abélien ou commutatif.

Exercice 1.1. 1) Montrer que le neutre est unique, au sens où, si e et e' sont deux éléments neutres d'un groupe $(G, *)$, alors $e = e'$.

2) Montrer que l'inverse est unique, au sens où, si x est un élément d'un groupe $(G, *)$ et si y et z sont des inverses de x, alors $y = z$.

Exercice 1.2. 1) Les ensembles $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des groupes pour l'addition.

2) Pour tout ensemble E non vide, $\mathfrak{S}(E)$ est un groupe pour la composition.

3) Pour tout ensemble E, $\mathcal{P}(E)$ est un groupe pour la différence symétrique.

4) Pour tout ensemble E non vide et tout groupe $(G, *)$, l'ensemble G^E est un groupe pour la multiplication terme à terme définie comme suit : si φ et ψ sont des éléments de G^E, on pose, pour tout élément x de E, $(\varphi \cdot \psi)(x) = \varphi(x) * \psi(x)$.

Exercice 1.3. Montrer que, quand $(G, *) = (\mathbb{Z}/2\mathbb{Z}, +)$, l'exemple 4 de l'exercice 1.2 correspond à l'exemple 3.

Une partie H de G est stable par $*$ si, pour tous x et y éléments de H, $x * y$ appartient à H. On note alors de nouveau $*$ la restriction de $*$ à $H \times H$.

Une partie H de $(G, *)$ est un sous-groupe de $(G, *)$ si et seulement si H est stable par $*$ et si $(H, *)$ est un groupe.

Soit $A \subset G$. On note $\langle A \rangle$ l'intersection de tous les sous-groupes de $(G, *)$ contenant A. Alors la partie $\langle A \rangle$ est elle-même un sous-groupe de $(G, *)$, appelé le sous-groupe engendré par A. Comme toute intersection de sous-groupes d'un groupe est elle-même un sous-groupe, $\langle A \rangle$ est aussi le plus petit sous-groupe de $(G, *)$ contenant A.

Si $A = \{x_1, \ldots, x_n\}$ est fini, on note $\langle A\rangle = \langle x_1, \ldots, x_n\rangle$.
Soit x un élément de G et e l'élément neutre. On définit par récurrence x^n pour tout entier relatif n en posant $x^0 = e$ puis, pour tout $n \geqslant 0$,

$$x^{n+1} = x^n * x, \qquad x^{-(n+1)} = x^{-n} * x^{-1}.$$

Exercice 1.4. Montrer que $x^n * x^p = x^{n+p}$ pour tous n et p entiers relatifs.

Un groupe $(G, *)$ est cyclique s'il est engendré par un seul élément, donc s'il existe x élément de G tel que $G = \langle x\rangle$, c'est-à-dire $G = \{x^n\,;\, n \in \mathbb{Z}\}$.
Attention : cette écriture ne signifie pas que G est en bijection avec $\mathbb{Z}$.
L'ordre d'un élément x d'un groupe $(G, *)$ d'élément neutre e est

$$\inf\{n \geqslant 1 \,|\, x^n = e\}.$$

Exercice 1.5. L'ordre de x est le cardinal de $\langle x\rangle$ si $\langle x\rangle$ est fini, et $+\infty$ sinon.

Un morphisme (de groupes) d'un groupe $(G, *)$ dans un groupe $(H, \circ)$ est une application $\varphi : G \to H$ compatible avec les lois $*$ et $\circ$, c'est-à-dire telle que, pour tous x et y éléments de G, $\varphi(x * y) = \varphi(x) \circ \varphi(y)$. Si $G = H$, on dit que φ est un endomorphisme (de groupe) du groupe G.
L'image du morphisme $\varphi : G \to H$ est $\varphi(G) = \{z \in H\,;\, \exists x \in G,\, \varphi(x) = z\}$.
Le noyau du morphisme φ est $\ker(G) = \{x \in G\,;\, \varphi(x) = e_H\}$.

Exercice 1.6. L'image d'un morphisme de groupes $\varphi : (G, *) \to (H, \circ)$ est un sous-groupe de H et son noyau est un sous-groupe de G.

Un morphisme de groupes de G vers H est injectif si et seulement si son noyau est le sous-groupe trivial, donc réduit à $\{e_G\}$.
Enfin, si un morphisme de groupes φ de G vers H est bijectif, l'application inverse $\varphi^{-1} : H \to G$ est aussi un morphisme. Dans ce cas, on dit que φ est un isomorphisme, que φ^{-1} est l'isomorphisme inverse de φ et que les groupes G et H sont isomorphes.

2 Vrai ou faux

Prouver chacune des assertions suivantes ou en donner un contre-exemple.

1. $(\mathbb{N}, +)$ est un groupe abélien.
2. $(\mathbb{Q}^*, +)$ est un groupe.
3. $(\mathbb{Q}^*, \times)$ est un groupe.
4. $(\mathbb{Z}^*, +)$ est un groupe.
5. $(\mathbb{Z}^*, \times)$ est un groupe.
6. Soit $(G, \cdot)$ un groupe. Pour tout entier $n \geqslant 1$ et tous x et y éléments de G, $(x \cdot y)^n = x^n \cdot y^n$.
7. Soit $(G, \cdot)$ un groupe et x et y deux éléments de G d'ordres finis, notés respectivement $o(x)$ et $o(y)$. Alors $o(x \cdot y)$ est fini et divise le produit $o(x)o(y)$.
8. Même affirmation avec « groupe abélien » au lieu de « groupe ».
9. Soit $H \subset G$ une partie non vide d'un groupe $(G, \cdot)$. La condition suivante entraîne que H est un sous-groupe de G : pour tout h élément de H, h^{-1} appartient à H.

10. Même affirmation avec la condition : pour tous h et h' éléments de H, $h \cdot h'$ appartient à H.
11. Même affirmation avec la condition : pour tous h et h' éléments de H, $h^{-1} \cdot h'$ appartient à H.
12. Même affirmation avec la condition : pour tous h et h' éléments de H, $h \cdot h'$ et h^{-1} appartiennent à H.
13. L'ensemble $\mathbb{U} = \{z \in \mathbb{C}\,;\, |z| = 1\}$ des nombres complexes de module 1, muni du produit des nombres complexes, est un sous-groupe du groupe $\mathbb{C}^* = (\mathbb{C} \setminus \{0\}, \cdot)$.
14. La fonction exponentielle est un morphisme de groupes de $(\mathbb{R}, +)$ dans $\mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \cdot)$.
15. La fonction exponentielle est un morphisme de groupes de $(\mathbb{R}, +)$ dans $\mathbb{R}_+^* = (\mathbb{R}_+ \setminus \{0\}, \cdot)$.
16. Les groupes $(\mathbb{R}, +)$ et $\mathbb{R}_+^*$ sont isomorphes.
17. Les groupes $(\mathbb{R}, +)$ et $\mathbb{R}^*$ sont isomorphes.

3 Exercices

Exercice 3.1. Soit $*$ une loi sur un ensemble E, e_g un neutre à gauche et e_d un neutre à droite. On suppose donc que, pour tout x élément de E, $e_g * x = x = x * e_d$. Prouver que $e_g = e_d$.

Exercice 3.2. Soit $E =]-\frac{\pi}{2}, \frac{\pi}{2}[$ et $* : E \times E \to E$ définie par

$$x * y = \arctan(\tan x + \tan y).$$

a) Prouver que $(E, *)$ est un groupe abélien.

b) Préciser si le groupe $(E, *)$ est isomorphe à $(\mathbb{R}, +)$.

Exercice 3.3. Soit E un ensemble, $(G, \cdot)$ un groupe, $\varphi : E \to G$ une bijection et

$$* : E \times E \to E, \qquad x * y = \varphi^{-1}(\varphi(x) \cdot \varphi(y)).$$

Prouver que $(E, *)$ est un groupe et que ce groupe est isomorphe à $(G, \cdot)$.

Exercice 3.4. Soit $G = \mathbb{R}^* \times \mathbb{R}$ et $*$ la loi sur G définie par

$$(x, y) * (u, v) = (xu, xv + y).$$

a) Prouver que $(G, *)$ est un groupe. Préciser si ce groupe est commutatif.

b) Montrer que $\mathbb{R}_+^* \times \mathbb{R}$ est un sous-groupe de G.

Exercice 3.5. a) Soit E un ensemble. Prouver que l'ensemble $\mathfrak{S}(E)$ des bijections de E sur E, muni de la loi $(s, t) \mapsto s \circ t$ où $s \circ t : E \to E$ est définie par $s \circ t(x) = s(t(x))$, est un groupe.

b) Pour tous nombres réels a et b, soit $F_{a,b} : \mathbb{R} \to \mathbb{R}$ telle que $F(t) = at + b$. Soit $\mathbb{B}$ l'ensemble des fonctions $F_{a,b}$ avec a et b réels et a non nul. Soit $\mathbb{A} \subset \mathfrak{S}(\mathbb{R})$ l'ensemble des bijections affines de $\mathbb{R}$ dans $\mathbb{R}$. On rappelle que $F : \mathbb{R} \to \mathbb{R}$ appartient à $\mathbb{A}$ si et seulement si, pour tout réel u dans $[0, 1]$ et tous réels s et t,

$$F(ut + (1-u)s) = uF(t) + (1-u)F(s).$$

Montrer que $\mathbb{B} = \mathbb{A}$. On pourra distinguer le cas où t appartient à $[0, 1]$, puis le cas où $t > 1$ en écrivant $1 = (1/t)t + (1 - 1/t)0$, puis le cas où $t < 0$.

En déduire que $\mathbb{A}$ est un sous-groupe de $\mathfrak{S}(\mathbb{R})$.

c) Prouver directement que $\mathbb{A}$ est un sous-groupe de $\mathfrak{S}(\mathbb{R})$.

d) Préciser si le groupe $\mathbb{A}$ est isomorphe au groupe G de l'exercice 4.

Exercice 3.6. Soit $G_1 = \mathbb{R}^* \times \mathbb{R}$ et $*$ la loi sur G_1 définie par

$$(x, y) * (u, v) = (xu, xv + yu^{-1}).$$

a) Prouver que $(G_1, *)$ est un groupe.

b) Parmi les parties suivantes, préciser lesquelles sont des sous-groupes de G_1 :

$$\mathbb{R}^* \times \{0\},\ \{-1\} \times \mathbb{R},\ \{-1, 1\} \times \mathbb{R},\ \{1\} \times \mathbb{R},\ \mathbb{Q}^* \times \mathbb{Q},\ \mathbb{Q}^* \times \mathbb{R},\ \mathbb{Q}^* \times \mathbb{Z},\ \{-1, 1\} \times \mathbb{Z}.$$

c) Pour tout t dans $\mathbb{R}$, soit $H_t = \{(x, t\,(x - x^{-1}))\,;\, x \in \mathbb{R}^*\}$. Montrer que H_t est un sous-groupe commutatif de G_1.

Exercice 3.7. Pour tout nombre complexe a, on définit $r_a : \mathbb{C} \to \mathbb{C}$ par $z \mapsto r_a(z) = az$ et $s_a : \mathbb{C} \to \mathbb{C}$ par $z \mapsto s_a(z) = a\overline{z}$. Soit

$$D = \{r_a, s_a \,|\, a \in \mathbb{C}^*\}.$$

Pour tout entier $n \geqslant 1$, soit

$$D_n = \{r_a, s_a \,|\, a \in \mathbb{C}^*,\ a^n = 1\}.$$

a) Prouver que D est un sous-groupe de $\mathfrak{S}(\mathbb{C})$ (on appelle D le groupe diédral).

b) Prouver que D_n est un sous-groupe à $2n$ éléments de D.

c) Donner les tables de composition de D_2 et D_3.

d) Prouver que D_n est commutatif si et seulement si $n = 1$ ou $n = 2$.

e) Prouver que l'application $u : D \to (\{-1, 1\}, \cdot)$ définie par $u(r_a) = +1$ et $u(s_a) = -1$ est un morphisme de groupes.

Exercice 3.8. Soit $(G, \cdot)$ un groupe. Le centre de G, noté $Z(G)$, est l'ensemble des éléments x de G qui commutent avec G, c'est-à-dire tels que, pour tout élément y de G, $x \cdot y = y \cdot x$.

a) Prouver que $Z(G)$ est un sous-groupe de G et que $Z(G) = G$ si et seulement si le groupe G est abélien.

b) Prouver que $Z(G)$ est un groupe abélien.

c) Déterminer le centre des groupes $\mathcal{A}$ de l'exercice 5, G_1 de l'exercice 6, et D, D_{2n+1} et D_{2n} de l'exercice 7.

d) Préciser si le centre d'un groupe est son plus grand sous-groupe abélien, ou non.

Exercice 3.9. a) Soit $u : \mathbb{C}^* \to \mathbb{U}$ définie par $u(z) = z/|z|$. Montrer que u est un morphisme surjectif du groupe multiplicatif $(\mathbb{C}^*, \cdot)$ dans $(\mathbb{U}, \cdot)$.

b) Construire des isomorphismes du groupe $(\mathbb{C}^*, \cdot)$ sur chacun des groupes produits $(\mathbb{U}, \cdot) \times (\mathbb{R}_+^*, \cdot)$ et $(\mathbb{U}, \cdot) \times (\mathbb{R}, +)$.

Exercice 3.10. a) Soient $(G, \cdot)$ un groupe et φ et ψ des endomorphismes du groupe G qui commutent, c'est-à-dire tels que $\varphi \circ \psi = \psi \circ \varphi$. Montrer que $\varphi(\ker \psi) \subset \ker(\psi)$.

b) Soit $(A, \cdot)$ un groupe abélien et $n \geqslant 0$ un entier. On note p_n l'application de A dans A définie par $p_n(a) = a^n$ pour tout a dans A. Montrer que p_n est un endomorphisme de A. Montrer que si ψ est un endomorphisme de A, alors $\psi \circ p_n = p_n \circ \psi$.

c) Déduire de a) et b) que, si p_n n'est pas injectif, alors il n'existe pas d'endomorphisme s de A tel que $p_n \circ s = \mathrm{Id}_A$, puis que p_n est un isomorphisme si et seulement s'il existe une application s de A dans A telle que $p_n \circ s = \mathrm{Id}_A$.

d) Pour $A = \mathbb{C}^*$, rouver que $p_{\mathbb{C}^*}^2$ est surjectif, mais qu'il n'existe pas d'endomorphisme r de $\mathbb{C}^*$ tel que $p_{\mathbb{C}^*}^2 \circ r = \mathrm{Id}_{\mathbb{C}^*}$. En d'autres termes, il n'existe pas de morphisme « racine carrée ».

Exercice 3.11. Soit $(G, \cdot)$ un groupe, e son élément neutre et A l'ensemble des éléments x de G tels que $x^2 = e$. Prouver que A est aussi l'ensemble des éléments x de G tels que $x = x^{-1}$. En déduire que l'ensemble $B = G \setminus A$ est stable par l'application $x \mapsto x^{-1}$. Montrer les assertions suivantes.

a) Si $A = G$, alors $(G, \cdot)$ est abélien.

b) Si G est fini, alors le cardinal de B est pair.

c) Si le cardinal de G est pair, alors il existe un élément x de G différent de e tel que $x^2 = e$.

Exercice 3.12. Soit $(G, \cdot)$ un groupe cyclique de générateur a et d'élément neutre e.

a) Soit $\pi : \mathbb{Z} \to G$ définie par $\pi(n) = a^n$. Montrer que π est un morphisme surjectif de groupes.

b) Prouver que π est un isomorphisme si et seulement si G est infini.

c) Soit H un sous-groupe de $(G, \cdot)$. Prouver que si G est fini ou si $H \neq \{e\}$, alors $A = \pi^{-1}(H)$ contient un élément strictement positif, puis que A est l'ensemble des multiples entiers de son plus petit élément strictement positif. En déduire les assertions suivantes.

c1) Tout sous-groupe de $(G, \cdot)$ est cyclique.

c2) Tout sous-groupe de $(G, \cdot)$ est stable par les endomorphismes de $(G, \cdot)$.

d) Donner des contre-exemples de c1) et c2) quand $(G, \cdot)$ n'est pas cyclique.

Exercice 3.13. a) Soit A une partie finie de $\mathbb{Q}$. En considérant un dénominateur commun de tous les éléments de A, prouver que le sous-groupe $\langle A \rangle$ de $(\mathbb{Q}, +)$ est cyclique.

b) Préciser si tout sous-groupe de $(\mathbb{Q}^*, \cdot)$ engendré par une partie finie est cyclique.

c) Préciser si les groupes $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+ \setminus \{0\}, \times)$ sont isomorphes.

Exercice 3.14. Soit $\varphi : (G, \cdot) \to (K, \cdot)$ un morphisme de groupes et x un élément de G d'ordre fini. Prouver que l'ordre de $\varphi(x)$ dans K divise l'ordre de x dans G.

Exercice 3.15 (Supplément : exercice corrigé). Soit R un anneau et $GL_k(R)$ le groupe des matrices carrées de taille $k \geqslant 1$ à coefficients dans R et inversibles. L'application det envoie les éléments de $GL_k(R)$ dans le groupe R^* des éléments inversibles de R et le groupe $SL_k(R)$ est son noyau, donc

$$SL_k(R) := \{M \in \mathcal{M}_{k\times k}(R)\,;\, \det M = 1\}.$$

Le but de l'exercice est d'étudier certains sous-groupes $SL_k(\mathbb{Z}/n\mathbb{Z})$.

1) Déterminer $SL_2(\mathbb{Z}/2\mathbb{Z})$ et montrer que ce groupe est isomorphe à $\mathfrak{S}_3$.

2) Calculer l'ordre de $SL_2(\mathbb{Z}/n\mathbb{Z})$ quand n est un entier premier.

3) Trouver des sous-groupes de $SL_2(\mathbb{Z}/n\mathbb{Z})$ isomorphes à $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})^*$.

4) Calculer l'ordre de $A := \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$ dans $G := SL_2(\mathbb{Z}/3\mathbb{Z})$.

5) D'après la question précédente, l'ordre de G est 24. Montrer que pourtant, G n'est pas isomorphe à $\mathfrak{S}_4$.

Indications de solution

1) On énumère d'abord les 6 éléments de l'ensemble $SL_2(\mathbb{Z}/2\mathbb{Z})$. Ensuite, chacun de ces éléments représente une application linéaire sur $(\mathbb{Z}/2\mathbb{Z})^2$ qui préserve $(0,0)$ et correspond à une bijection de $(\mathbb{Z}/2\mathbb{Z})^2 \setminus \{(0,0)\}$ dans lui-même.

2) On choisit d'abord la première ligne de M, qui est un vecteur non nul, disons (a, b). Soit (c, d) la deuxième ligne. Si $a \neq 0$, il reste à choisir c puis $d = (1 + bc)a^{-1}$ est imposé, donc n possibilités pour b puis n possibilités pour (c, d), pour chaque a non nul. Si $a = 0$, d est libre

donc n possibilités, et b doit être non nul et $c = b^{-1}$, donc $n-1$ possibilités. En tout, on obtient $n^2(n-1) + n(n-1) = n(n^2-1)$ matrices.

3) On peut associer à tout élément a de $\mathbb{Z}/n\mathbb{Z}$ la matrice $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ et à tout élément a de $(\mathbb{Z}/n\mathbb{Z})^*$ la matrice $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$.

4) L'ordre de A est 6 car $A^2 = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}$, $A^3 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ et $A^6 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

5) Le groupe G possède un élément d'ordre 6. Soit s un élément de $\mathfrak{S}_4$. Ou bien s est un cycle de longueur 2 ou s se décompose en un produit de deux cycles de longueur 2 disjoints, alors s est d'ordre 2, ou bien s est un cycle d'ordre 3 ou 4, alors s est d'ordre 3 ou 4. En tout cas, aucun élément de $\mathfrak{S}_4$ n'est d'ordre 6 donc les deux groupes ne sont pas isomorphes.

Fiche 8 : Algèbre (2) Groupe symétrique

« La symétrie, c'est l'ennui. » Victor Hugo, Les Misérables

1 Rappels de cours

Une permutation d'un ensemble E est une bijection de E dans E. Le groupe $\mathfrak{S}(E)$ est l'ensemble des permutations de E muni de la composition des applications (notée $\circ$ ou $\cdot$). Si $n \geqslant 1$ est un entier, on note $\mathbb{N}_n = \{1, 2, \ldots, n\}$ et $\mathfrak{S}_n$ le groupe $\mathfrak{S}(\mathbb{N}_n)$ des permutations de n objets, qu'on appelle le groupe symétrique sur n éléments.

Une transposition est un élément de $\mathfrak{S}_n$ qui laisse fixe tous les points de $\mathbb{N}_n$ sauf exactement deux d'entre eux. Pour toute transposition t, il existe donc deux entiers i et j distincts dans $\mathbb{N}_n$ tels que $t(j) = i$, $t(i) = j$, et, pour tout k dans $\mathbb{N}_n \setminus \{i, j\}$, $t(k) = k$.

Les transpositions engendrent $\mathfrak{S}_n$. Le cardinal de $\mathfrak{S}_n$ vaut $n!$. Il existe un unique morphisme $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$, qu'on appelle la signature, tel que pour toute transposition t, $\varepsilon(t) = -1$.

Exercice 1.1. Montrer que, pour toute permutation s, $\varepsilon(s) = (-1)^{i(s)}$, où $i(s)$ désigne le nombre d'inversions de s, c'est-à-dire le cardinal de l'ensemble des couples (i, j) d'entiers i et j entre 1 et n tels que $i < j$ et $s(i) > s(j)$.

Le groupe alterné est le noyau du morphisme signature ε.

Pour $\ell \geqslant 2$, un cycle de longueur ℓ de $\mathfrak{S}_n$ est une permutation s dans $\mathfrak{S}_n$ telle qu'il existe une partie $S \subset \mathbb{N}_n$ de cardinal ℓ, appelée le support du cycle s, avec $S = \{i_j \,;\, 1 \leqslant j \leqslant \ell\}$, telle que $s(i_j) = i_{j+1}$ pour tout $1 \leqslant j \leqslant \ell - 1$, $s(i_\ell) = i_1$, et $s(i) = i$ pour tout i dans $\mathbb{N}_n \setminus S$.

Toute permutation s'écrit de manière unique, à l'ordre des facteurs près, comme un produit de cycles de supports disjoints.

Si H est un sous-groupe d'un groupe $(G, \cdot)$, la relation de congruence à droite, définie par

$$\text{« } x \sim y \text{ si et seulement si } x^{-1}y \text{ appartient à } H \text{ »},$$

est une relation d'équivalence sur G. Les classes d'équivalence de cette relation sont les parties $xH = \{xh \,;\, h \in H\}$ pour x dans G. On appelle xH la classe à droite de x modulo H. L'ensemble de ces classes (ou ensemble quotient) est noté G/H.

Théorème 1.2 (Théorème de Lagrange). *Si le groupe G est fini alors son cardinal est le produit du cardinal de H et du cardinal de G/H.*

Corollaire 1.1. *Le cardinal d'un sous-groupe d'un groupe fini divise celui du groupe.*

Définition 1.3. *Un sous-groupe H d'un groupe $(G, \cdot)$ est distingué, ou normal, si pour tout élément h de H et tout élément g de G, le conjugué ghg^{-1} de h par g appartient à H. On note cette propriété $H \triangleleft G$.*

Si $H \triangleleft G$, il existe une unique structure de groupe sur G/H telle que l'application quotient $\varrho : G \to G/H$ définie par $\varrho(x) = xH$ pour tout élément x de G, est un morphisme. On appelle cette structure le groupe quotient. En d'autres termes, dans G/H, on pose $(xH)(yH) = (xy)H$ pour tous éléments x et y de G.

Une action à gauche d'un groupe $(G, \cdot)$ d'élément neutre e sur un ensemble X est une application $G \times X \to X$ notée $(g, x) \mapsto g \cdot x$, telle que pour tous g et h dans G et tout x dans X, $g \cdot (h \cdot x) = (gh) \cdot x$ et $e \cdot x = x$. On dit que G agit à gauche sur X.

Pour une action à gauche $(g, x) \mapsto g \cdot x$ donnée, le stabilisateur d'un élément x de X pour cette action est l'ensemble $G_x = \{g \in G\,;\, g \cdot x = x\}$ et son orbite sous l'effet de cette action est l'ensemble $G \cdot x = \{g \cdot x\,;\, g \in G\}$. Pour toute action de G sur X et pour tout élément x de X, G_x est un sous-groupe de $(G, \cdot)$. Pour toute action de G sur X, les orbites $G \cdot x$ pour x élément de X forment une partition de X.

La conjugaison intérieure $(g, h) \mapsto ghg^{-1}$ est une action de $(G, \cdot)$ sur G.

2 Exercices

Exercice 2.1. a) Soit $c = (i_1, \ldots, i_\ell)$ un cycle de longueur ℓ dans $\mathfrak{S}_n$ et soit s un élément de $\mathfrak{S}_n$. Établir que le conjugué scs^{-1} est le cycle de longueur ℓ qui vaut $(s(i_1), \ldots, s(i_\ell))$.

En déduire que ces deux cycles éléments de $\mathfrak{S}_n$ et de longueur ℓ ont même signature.

Désormais, on fixe $2 \leqslant \ell \leqslant n$.

b) Prouver que tout cycle élément de $\mathfrak{S}_n$ de longueur ℓ est conjugué au cycle $(1, 2 \ldots, \ell)$.

c) Déterminer la permutation $(1, 2)(2, 3) \cdots (i, i+1) \cdots (\ell - 1, \ell)$ élément de $\mathfrak{S}_n$.

d) Prouver que tout cycle de longueur ℓ élément de $\mathfrak{S}_n$ est le produit de $\ell - 1$ transpositions. En déduire la signature d'un tel cycle.

Exercice 2.2. a) Pour tout ℓ, prouver que l'ordre d'un cycle de longueur ℓ vaut ℓ.

b) Déterminer l'ordre de $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ et l'ordre de $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$. Préciser pour chacune de ces permutations s'il s'agit d'un cycle et s'il s'agit d'une puissance d'un cycle.

c) Décomposer en produit de cycles de supports disjoints la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 4 & 5 & 8 & 7 & 9 & 11 & 10 & 1 & 12 & 3 & 2 \end{pmatrix}.$$

En déduire sa signature et son ordre.

d) Soit s élément de $\mathfrak{S}_n$ une permutation produit de k cycles de supports disjoints et de longueurs ℓ_i pour $1 \leqslant i \leqslant k$. Vérifier que $\ell_1 + \cdots + \ell_k \leqslant n$ et déterminer la signature et l'ordre de s en fonction des ℓ_i.

Exercice 2.3. Soit $(G, \cdot)$ un groupe fini et g un élément de G. Montrer que l'ordre de g divise le cardinal de G. En déduire qu'un groupe fini dont le nombre d'éléments est premier est cyclique.

Exercice 2.4. Soit p un nombre premier et $n \geqslant p$. Prouver qu'un élément d'ordre p de $\mathfrak{S}_n$ est un cycle.

Exercice 2.5. Soit $H = \langle u, v, w \rangle$ le sous-groupe de $\mathfrak{S}_9$ engendré par les éléments

$$u = (1, 4, 7)(2, 5, 8)(3, 6, 9),\ v = (3, 6, 9),\ w = (1, 2, 3)(4, 5, 6)(7, 8, 9).$$

a) Calculer les ordres de u, v et w.

b) Calculer wvw^{-1} et $w^{-1}vw$. En déduire la relation $u = (wv)^3$.

c) Déterminer si tout élément non trivial de H est d'ordre 3.

d) Prouver que $K = \langle v, wvw^{-1}, w^{-1}vw\rangle$ est un sous-groupe distingué de H.

e) Déterminer le nombre d'éléments de K puis celui de H.

f) Déterminer la plus grande puissance de 3 qui divise le cardinal de $\mathfrak{S}_9$.

Exercice 2.6. Soit $\mathbb{A}^+$ la partie du groupe $\mathbb{A}$ des bijections affines de $\mathbb{R}$, défini dans l'exercice 3.5 du chapitre 7, formée des bijections croissantes. Prouver que $\mathbb{A}^+$ est un sous-groupe distingué de $\mathbb{A}$. Calculer le cardinal de $\mathbb{A}/\mathbb{A}^+$, identifier le groupe quotient $\mathbb{A}/\mathbb{A}^+$ et le morphisme quotient $\mathbb{A} \to \mathbb{A}/\mathbb{A}^+$.

Exercice 2.7. a) Prouver que le centre $Z(G)$ d'un groupe $(G, \cdot)$ est un sous-groupe distingué de $(G, \cdot)$.

b) Prouver que si le groupe quotient $G/Z(G)$ est cyclique, il est trivial.

c) Déterminer si on peut remplacer « cyclique » par « abélien » dans l'assertion b). On pourra considérer la loi sur $\mathbb{Z}^3$ définie par

$$(u, v, w) * (x, y, z) = (u + x, v + y, w + uy + z).$$

Exercice 2.8. Soit $(G, \cdot)$ un groupe et H un sous-groupe de $(G, \cdot)$. On considère sur G la relation « $x \approx y$ si et seulement si $xy^{-1} \in H$ ».

a) Établir que $\approx$ est une relation d'équivalence et que ses classes d'équivalence sont les ensembles $Hy = \{hy\,;\, h \in H\}$ pour y élément de G.

b) Prouver que H est distingué si et seulement si, pour tout x élément de G, $xH = Hx$.

c) Pour deux parties A et B de G, soit $AB = \{ab\,;\, a \in A, b \in B\}$.

c1) Vérifier que si C est une troisième partie de G alors

$$(AB)C = A(BC).$$

c2) En déduire que pour tous x et y éléments de G, $(xH)(yH) = (xy)H$ si et seulement si H est distingué.

d) Conclure de c2) qu'il existe une structure de groupe sur G/H telle que l'application quotient $\varrho : G \to G/H$ est un morphisme si et seulement si H est distingué.

Exercice 2.9. On reprend les groupes G et G_1 des exercices 3.4 et 3.6 du chapitre 7.

a) Prouver que $(x, y) \mapsto (x^2, y\,x^{-1})$ est un morphisme surjectif de G_1 sur G.

b) Déduire du fait que $Z(G_1) = \{(-1, 0), (1, 0)\}$ que $G_1/Z(G_1)$ est isomorphe à G.

Exercice 2.10. a) Soit $(A, +)$ un groupe abélien dont on note 0 le neutre. Établir que l'ensemble de ses éléments d'ordre fini est un sous-groupe de $(A, +)$. On le note $T(A)$ et on l'appelle le groupe de torsion de A.

b) Prouver que $\dot{0} = T(A)$ est le seul élément d'ordre fini du groupe quotient $A/T(A)$.

c) Déterminer le sous-groupe de torsion du groupe quotient $(\mathbb{R}/\mathbb{Z}, +)$. Préciser si ce sous-groupe est fini ou non.

d) Déterminer les éléments d'ordre fini du groupe $\mathbb{A}$ des bijections affines de $\mathbb{R}$. Préciser si ces éléments forment un sous-groupe.

e) Prouver que l'application $\varphi : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ définie par

$$t \mapsto \varphi(t) = \mathrm{e}^{2\mathrm{i}\pi t} = \cos(2\pi t) + \mathrm{i}\sin(2\pi t),$$

est un morphisme de groupes et déterminer son noyau et son image.

f) Montrer que $(\mathbb{R}/\mathbb{Z}, +)$ est isomorphe au groupe $(\mathbb{U}, \times)$ des nombres complexes de module 1.

g) Prouver que toute partie finie $\{\xi_1, \ldots, \xi_n\} \subset T(\mathbb{U})$ du groupe de torsion de $\mathbb{U}$ est incluse dans un sous-groupe cyclique, c'est-à-dire qu'il existe un élément ξ de $\mathbb{U}$ tel que $\{\xi_1, \ldots, \xi_n\} \subset \langle \xi \rangle$. Préciser si un tel élément ξ est nécessairement de torsion ou non.

Exercice 2.11. Soit $(G, \cdot)$ un groupe et X un ensemble. Prouver que l'application de $G \times X$ vers X définie par $(g, x) \mapsto g \cdot x$ est une action de $(G, \cdot)$ sur X si et seulement si, pour tout élément g de G, l'application $s_g : X \to X$ définie par $s_g(x) = g \cdot x$ est bijective, et si $g \mapsto s_g$ est un morphisme de $(G, \cdot)$ dans $(\mathfrak{S}(X), \circ)$.

Exercice 2.12. Soit H un sous-groupe d'un groupe $(G, \cdot)$. Pour tout élément g de G, on note $\lambda(g)$ l'application qui à toute partie K de G associe $\lambda(g)(K) = gK$.

a) Prouver que λ induit un morphisme de $(G, \cdot)$ sur $(\mathfrak{S}(G/H), \circ)$, encore noté λ et défini par $\lambda(g)(g'H) = (gg')H$. On appelle λ le morphisme de translation à gauche sur G/H.

b) Prouver que si le cardinal de G/H vaut 2, alors $\lambda(h)(H) = H$ pour tout élément h de H. En déduire que pour tout élément g de G, $\lambda(h)(gH) = gH$, puis que H est distingué.

Exercice 2.13. Soit $(G, \cdot)$ un groupe fini non réduit à un élément et $p \geqslant 2$ le plus petit nombre premier divisant le cardinal de G. Soit H un sous-groupe de $(G, \cdot)$ d'indice p. On suppose donc que le cardinal de G/H vaut p, et on voit que $\mathfrak{S}(G/H)$ est isomorphe à $\mathfrak{S}_p$.

a) Prouver que l'image $\lambda(G)$ du morphisme λ de translation à gauche sur G/H défini dans l'exercice 2.12 est un sous-groupe d'ordre p de $\mathfrak{S}(G/H)$.

b) En déduire que si g est un élément de $G \setminus \ker(\lambda)$, $\lambda(g)$ est un cycle de longueur p dans $\mathfrak{S}(G/H)$.

On pourra utiliser l'exercice 2.4.

c) En conclure que $H = \ker(\lambda)$, donc que H est distingué dans G.

Indications

Exercice 2.5

Il s'agit d'un 3-Sylow maximal.

Exercice 2.13

a) L'ordre de $\lambda(G)$ divise l'ordre de S_p et l'ordre de G, donc leur pgcd, qui vaut p. Donc l'ordre de $\lambda(G)$ vaut 1 ou p. Si $g \in H$, $\lambda(g) = \mathrm{Id}$. Si $g \in G \setminus H$, $\lambda(g)H = gH \neq H$ donc $\lambda(g) \neq \mathrm{Id}$. Comme $\lambda(G)$ possède au moins 2 éléments, donc $\lambda(G)$ est d'ordre p.

Fiche 9 : Algèbre (3) Anneaux et corps

« Le corps est le tombeau de l'âme. » Platon, Cratyle

1 Rappels de cours

Un anneau $(A, +, \times)$ est un ensemble A muni de deux lois de composition $+$, souvent appelée l'addition de A, et $\times$, souvent appelée la multiplication de A, tel que (1) $(A, +)$ est un groupe commutatif, (2) la multiplication est associative, (3) la multiplication possède un élément neutre, et (4) la multiplication est distributive par rapport à l'addition, c'est-à-dire que, pour tous a, b et c éléments de A,

$$a \times (b + c) = (a \times b) + (a \times c), \qquad (a + b) \times c = (a \times c) + (b \times c).$$

On appelle le neutre de $+$ le zéro de A et on le note souvent 0. On appelle le neutre de $\times$ le un de A et on le note souvent 1. L'anneau A est commutatif si de plus sa multiplication est commutative.

Une partie $B \subset A$ d'un anneau $(A, +, \times)$ est un sous-anneau de A si B est stable par les deux opérations $+$ et $\times$, si le un de A appartient à B et si $(B, +)$ est un sous-groupe de $(A, +)$.

Un corps (commutatif) est un anneau (commutatif) A tel que $1 \neq 0$ et tel que tout élément non nul est inversible pour la multiplication.

Un anneau A est intègre si A est commutatif et si pour tout a et b éléments de A, $a \times b = 0$ implique que $a = 0$ ou $b = 0$.

Un morphisme d'anneaux est une application $\varphi : A \to A'$ entre deux anneaux A et A', qui préserve les lois et l'élément neutre multiplicatif, c'est-à-dire telle que, pour tous a et b éléments de A,

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(a \times b) = \varphi(a) \times \varphi(b), \quad \varphi(1_A) = 1_{A'}.$$

Un idéal (bilatère) I d'un anneau $(A, +, \times)$ est un sous-groupe de A tel que, pour tout x élément de I et tout a élément de A, ax et xa sont des éléments de I.

Le noyau $\ker(\varphi)$ (pour l'addition) d'un morphisme d'anneaux $\varphi : A \to A'$ est un idéal de A.

Si I est un idéal d'un anneau A, le groupe abélien quotient A/I possède une unique structure d'anneau telle que l'application quotient $\pi : A \to A/I$ est un morphisme d'anneaux.

Si A est un anneau, il existe un unique morphisme d'anneaux c_A de $\mathbb{Z}$ dans A. Si c_A est injectif, $\ker(c_A) = \{0\}$ et on pose $n_A = 0$. Sinon, $\ker(c_A)$ est un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$ donc il existe un entier $n_A \geqslant 1$ tel que $\ker(c_A) = n_A\mathbb{Z}$ (c'est le plus petit entier strictement positif qui appartient à $\ker(c_A)$). Si $A = K$ est de plus un corps, alors $n_K = 0$ ou n_K est un nombre premier. On appelle n_K la caractéristique du corps K.

Si A est un anneau commutatif et si x est un élément de A, l'ensemble xA des xa avec a élément de A est un idéal de A, qu'on appelle idéal principal engendré par a et que l'on note $I(a)$. Un anneau est principal s'il est commutatif intègre et si tous ses idéaux sont principaux.

Si B est une partie de A, on note $I(B)$ l'idéal engendré par B : c'est le plus petit idéal contenant B, et aussi l'intersection de tous les idéaux contenant B. Si B est une partie finie avec $B = \{x_1, \ldots, x_n\}$, on note $I(B) = I(x_1, \ldots, x_n)$.

2 Vrai ou faux

Démontrer ou donner un contre-exemple des assertions suivantes.

1. Soit A un anneau. L'application nulle $\varphi : A \to A$ telle que $\varphi(a) = 0$ pour tout a dans A est un endomorphisme d'anneau.
2. $3\,\mathbb{Z} = \{3\,n\,;\, n \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{Z}$.
3. Si $n \geqslant 1$ est un entier, l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ est un corps de caractéristique n.
4. Soit G un groupe abélien et $A = G^G$ l'ensemble des applications de G dans G, muni des lois $f + g = [x \mapsto f(x) + g(x)]$ et $f \circ g = [x \mapsto f(g(x))]$.

   a) $(A, +, \circ)$ est un anneau.

   b) L'ensemble $B \subset A$ des endomorphismes de groupe de G est stable par $+$ et $\circ$, et $(B, +, \circ)$ est un anneau commutatif.
5. L'anneau $\mathbb{Z}/6\mathbb{Z}$ des entiers modulo 6 est un anneau intègre.

3 Exercices de cours

1. Soit A un anneau. Montrer que, pour tout a dans A, $0 \times a = 0 = a \times 0$ et $-a = (-1) \times a = a \times (-1)$.

2. Soit A un anneau. Montrer que l'ensemble C des éléments c de A tels que, pour tout élément a de A, $a \times c = c \times a$, est un sous-anneau de A.

3. Soit A un annneau commutatif et a un élément de A idempotent, c'est-à-dire tel que $a \times a = a$.

a) Prouver que $+$ et $\times$ induisent sur l'idéal principal $I(a) = aA$ une structure d'anneau.

b) Prouver que aA est un sous-anneau de A si et seulement si $a = 1$.

c) Donner des exemples d'anneaux commutatifs A possédant des éléments idempotents autres que 1 et 0.

4. Montrer que l'anneau $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo un entier naturel $n \geqslant 1$ est un corps si et seulement si n est un nombre premier, c'est-à-dire que $n \geqslant 2$ et qu'il n'existe pas d'entiers p et q différents de 1 et n tels que $n = pq$.

5. Soit I un idéal d'un anneau A et $\pi : A \to A/I$ le morphisme quotient. Montrer que J est un idéal de A/I si et seulement si $\pi^{-1}(J)$ est un idéal de A contenant I. En déduire, dans le cas où A est commutatif, que l'anneau quotient A/I est un corps si et seulement si I est un idéal strict maximal de A, c'est-à-dire que $I \neq A$ et que, pour tout idéal J de A avec $I \subset J$, soit $J = I$ soit $J = A$.

6. Soit A un anneau et A^* l'ensemble des éléments de A inversibles pour la multiplication, donc un élément a de A appartient à A^* si et seulement s'il existe un élément b dans A tel que $a \times b = b \times a = 1$.

a) Prouver que A^* est stable par la multiplication et que $(A^*, \times)$ est un groupe. On appelle $(A^*, \times)$ le groupe des unités de A.

b) Déterminer le groupe des unités des anneaux $\mathbb{Z}$ et $\mathbb{Q}$. Si A est un anneau, soit $M_n(A)$ l'anneau des matrices $n \times n$ à coefficients dans A. Déterminer le groupe des unités des anneaux $M_2(\mathbb{R})$ et $M_2(\mathbb{Z})$.

7. Soit A un anneau commutatif, a et b des éléments de A, et $n \geqslant 0$ un entier. Montrer la formule du binôme

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}.$$

Rappeler pourquoi cette formule n'est plus vraie dans un anneau non commutatif.

4 Exercices

1. Soit $(A, +, \times)$ un ensemble muni de deux lois $+$ et $\times$. On suppose que la loi $\times$ est distributive par rapport à la loi $+$, que la loi $\times$ possède un élément neutre 1, et que $(A, +)$ est un groupe.

Prouver que $+$ est commutative. Indication : On pourra considérer, pour a et b dans A, l'élément $(a+b) \times (1+1)$.

2. Soit A un anneau tel que tout élément de A non nul possède un inverse à gauche : pour tout élément non nul a de A, il existe un élément b de A tel que $ba = 1$. Prouver qu'un inverse à gauche de a est aussi un inverse à droite, c'est-à-dire qu'on a aussi $ab = 1$.

3. Soit A un anneau et a, b et c des éléments de A tels que $c(1-ba) = 1$. Calculer $(1+acb)(1-ab)$. En déduire que si $1 - ba$ admet un inverse à gauche, $1 - ab$ aussi.

4. Soit A un anneau idempotent, c'est-à-dire tel que tout élément a de A vérifie $a^2 = a$.

a) Montrer que pour tout élément a de A, $a + a = 0$. En déduire que A est commutatif.

b) Montrer que pour tout a, b et c éléments de A, $(a+b)c = 0$ si et seulement si $a(b+1)c = 0$ et $(a+1)bc = 0$.

c) Soit X un ensemble et $\mathcal{P}(X)$ l'ensemble des parties de X. Montrer que $(\mathcal{P}(X), \triangle, \cap)$ est un anneau idempotent.

5. Soit p un nombre premier et $\mathbb{Z}_p$ l'ensemble des nombres rationnels que l'on peut écrire comme une fraction dont le dénominateur n'est pas divisible par p.

a) Prouver que $\mathbb{Z}_p$ est un sous-anneau de $\mathbb{Q}$.

b) Prouver que pour tout nombre rationnel x, soit x appartient à $\mathbb{Z}_p$, soit $x \neq 0$ et x^{-1} appartient à $\mathbb{Z}_p$.

c) Soit A un sous-anneau de $\mathbb{Q}$ contenant $\mathbb{Z}_p$. Prouver que les propriétés suivantes sont équivalentes.

1. $A \neq \mathbb{Z}_p$.

2. Il existe un entier $n \geqslant 1$ tel que $1/p^n$ appartient à A.
3. Pour tout entier $n \geqslant 1$, $1/p^n$ appartient à A.
4. $A = \mathbb{Q}$.

d) Etablir les équivalences des trois premières conditions de c) quand, au lieu de supposer que le sous-anneau A de $\mathbb{Q}$ contient $\mathbb{Z}_p$, on suppose que $\mathbb{Z}_p$ ne contient pas A. Donner un exemple avec $A \neq \mathbb{Q}$.

6. Un anneau non principal a) Prouver que l'équation $10\,y^2 = x^2$ n'a pas de solution (x, y) dans $\mathbb{Z}^2$ à part $x = y = 0$.

b) Déterminer l'ensemble des carrés modulo 10 : un élément y de $\mathbb{Z}/10\mathbb{Z}$ est un carré modulo 10 s'il existe un élément x de $\mathbb{Z}/10\mathbb{Z}$ tel que $y = x^2$.

c) Prouver qu'il n'existe pas de couple (x, y) dans $\mathbb{Z}^2$ tel que $10y^2 = x^2 + 3$ ou $10y^2 = x^2 - 3$.

d) Soit $v = \sqrt{10}$ et A l'ensemble des $x + yv$ pour x et y éléments de $\mathbb{Z}$. Prouver que A est un sous-anneau de $\mathbb{R}$ et que pour tout élément a de A, les entiers x et y tels que $a = x + yv$ sont uniques. On note souvent $A = \mathbb{Z}[\sqrt{10}]$.

e) Soit $c : A \to A$ définie par $c(x + yv) = x - yv$, pour tous x et y entiers. Montrer que c est un endomorphisme d'anneau et que les seuls points fixes de c sont les éléments de $\mathbb{Z}$.

f) Expliciter $ac(a)$ en fonction des « coordonnées » (x, y) de $a = x + yv$. En déduire qu'il n'existe pas d'élément a de A tel que $|ac(a)| = 3$.

g) Soit $n : A \to A$ définie par $n(a) = ac(a)$. Montrer que n est à valeurs dans $\mathbb{Z}$ et vérifie les propriétés suivantes : pour tous a et b éléments de A, $n(ab) = n(a)n(b)$; pour tout a élément de A, $n(a) = 0$ si et seulement si $a = 0$.

h) Soit I l'ensemble des $3a + (2 + v)b$ pour a et b éléments de A. Montrer que I est un idéal de A contenant 3 et $2 + v$ et déduire de ce qui précède que cet idéal n'est pas principal.

7. Soit $\mathbb{Z}[\mathrm{i}]$ l'ensemble des nombres complexes de la forme $a + \mathrm{i}b$ avec a et b éléments de $\mathbb{Z}$.

a) Montrer que $\mathbb{Z}[\mathrm{i}]$ est un sous-anneau de $\mathbb{C}$.

b) Soit z un élément de $\mathbb{Z}[\mathrm{i}]$. Montrer que le conjugué $\overline{z}$ de z appartient à $\mathbb{Z}[i]$ et que $|z|^2$ appartient à $\mathbb{N}$.

c) Soit z un élément de $\mathbb{Z}[\mathrm{i}]$. Montrer que z appartient au groupe $\mathbb{Z}[\mathrm{i}]^*$ des unités de $\mathbb{Z}[\mathrm{i}]$ si et seulement si $|z| = 1$.

d) Déterminer le groupe $\mathbb{Z}[\mathrm{i}]^*$.

e) Montrer que pour tout z élément de $\mathbb{C}$, il existe un élément z_0 de $\mathbb{Z}[\mathrm{i}]$ tel que $|z - z_0|^2 \leqslant \frac{1}{2}$.

f) Prouver que pour tous z_0 et z_1 éléments de $\mathbb{Z}[\mathrm{i}]$ avec $z_1 \neq 0$, il existe des éléments a_0 et a_1 de $\mathbb{Z}[\mathrm{i}]$ tels que $z_0 = a_0 z_1 + a_1$ avec $|a_1| < |z_1|$.

g) Montrer que $\mathbb{Z}[\mathrm{i}]$ est un anneau principal.

8. Soit K un corps de caractéristique non nulle p. Montrer que, pour tous x et y éléments de K et tout entier $n \geqslant 0$,

$$(x + y)^{p^n} = x^{p^n} + y^{p^n}.$$

Fiche 10 : Algèbre (4) Arithmétique, anneau des entiers relatifs

« One Ring to rule them all,
One Ring to find them,
One Ring to bring them all,
And in the darkness bind them. »
JRR Tolkien, The Lord of the Rings

1 Rappels de cours

L'anneau $\mathbb{Z}$ est intègre et tout sous-groupe additif de $\mathbb{Z}$ est un idéal.

Division euclidienne. Soit a et b des entiers relatifs avec $b \neq 0$. Il existe un unique élément (q, r) de $\mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leqslant r < |b|$. Les entiers q et r sont respectivement le quotient et le reste de la division euclidienne de l'entier a par l'entier non nul b.

L'anneau $\mathbb{Z}$ est ainsi euclidien donc principal : tout idéal I non nul contient des éléments positifs et, si on note n_I le plus petit élément strictement positif de I, on obtient $I = n_I\mathbb{Z}$. Pour déterminer le générateur n_I de l'idéal $I(A)$ engendré par une partie A de cardinal $n \geqslant 3$, on se ramène au cas $n = 2$ en remarquant que $I(A \cup B) = I(I(A) \cup B)$. Pour cela, on utilise l'algorithme d'Euclide.

Algorithme d'Euclide. Soit a et b des entiers avec $b \neq 0$. Si la division euclidienne de a par b est $a = bq + r$ avec $0 \leqslant r < |b|$, alors les diviseurs communs de a et b sont ceux de b et r, donc $I(a, b) = I(b, r)$: soit $r = 0$ et tout diviseur de b divise a, soit b et r sont deux entiers strictement positifs avec $r < |b|$ et les diviseurs communs de a et b sont ceux de b et r. On construit ainsi une suite $b_0 = a$, $b_1 = |b| > b_2 > \cdots b_n > 0$ telle que, pour tout $2 \leqslant i \leqslant n$, b_i, est le reste de la division de b_{i-2} par b_{i-1}, et telle que b_n divise tous les b_i.

Plus grand commun diviseur. Le pgcd d'une partie A de $\mathbb{Z}$ non vide et non réduite à $\{0\}$ est l'unique entier naturel $d \geqslant 1$ tel que $I(A) = d\mathbb{Z}$.

Un entier d est le pgcd des x_k pour $1 \leqslant k \leqslant n$ si et seulement si d divise chaque x_k et s'exprime par une identité de Bezout, c'est-à-dire qu'il existe des entiers m_k tels que $d = \sum_{k=1}^{n} m_k x_k$.

Deux entiers x et y sont premiers entre eux, ou bien x est premier avec y, si 1 est le pgcd de $\{x, y\}$.

Lemme de Gauss Si d est premier avec x et divise le produit xy, alors d divise y.

Plus petit commun multiple. Le ppcm d'un ensemble fini d'entiers A est l'unique entier naturel $m \geqslant 1$ tel que $\bigcap_{x \in A} I(x) = I(m) = m\mathbb{Z}$.

Pour tous x et y entiers relatifs, $xy = \text{pgcd}(x, y)\text{ppcm}(x, y)$.

Un nombre premier est un entier naturel $p \geqslant 2$ dont l'ensemble des diviseurs positifs est $\{1, p\}$. L'ensemble des nombres premiers est infini.

Théorème fondamental de l'arithmétique Tout entier naturel non nul n s'écrit, de manière unique à l'ordre près, comme un produit de nombres premiers. Donc

$$n = p_1 \cdots p_m = \prod_p p^{v_p(n)},$$

où le produit porte sur les nombres premiers p, chaque $v_p(n)$ appartient à $\mathbb{N}$ et l'ensemble des nombres premiers p tels que $v_p(n) \neq 0$ est fini.

Dans la première factorisation ci-dessus, il y a éventuellement des répétitions $p_i = p_j$ pour $i \neq j$, mais pas dans la seconde. Si l'ensemble des nombres premiers p tels que $v_p(n) \neq 0$ vaut $\{p_1, \ldots, p_k\}$ avec $p_i < p_{i+1}$, la factorisation réduite de l'entier n est $n = p_1^{n_1} \cdots p_k^{n_k}$ et cette décomposition est maintenant unique.

Corollaire Si m et n sont des entiers positifs non nuls,

$$\mathrm{pgcd}(m,n) = \prod_{p \in \mathcal{P}} p^{\min(v_p(m), v_p(n))}, \quad \mathrm{ppcm}(m,n) = \prod_{p \in \mathcal{P}} p^{\max(v_p(m), v_p(n))}.$$

Soit $n \geqslant 1$ un entier naturel. L'anneau $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo n possède n éléments. C'est un corps si et seulement si n est premier. Plus généralement, la classe $\overline{m}$ d'un entier m dans $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si m est premier avec n.

2 Vrai ou faux

1. Soient m et n des entiers relatifs. Les idéaux principaux $I(m)$, $I(n)$ et $I(mn)$ vérifient :
a) $I(m) \cap I(n) \subset I(mn)$; b) $I(mn) \subset I(m) \cap I(n)$; c) $I(mn) = I(m) \cap I(n)$.

2. Le reste de la division de -56 par 12 est -8.

3. L'entier 1457632916 est divisible par 4 mais ne l'est pas par 8.

4. Si n est un entier sans facteur carré, c'est-à-dire si $n = p_1 \cdots p_k$ où les p_i sont des nombres premiers deux à deux distincts, alors $\sqrt{n}$ est irrationnel.

5. Le pgcd de 585 et 286 est 13.

6. Les entiers 728145362718 et 782145326718 sont divisibles par 9.

7. Les entiers 33333333, 14327143271 et 34103025 sont divisibles par 11.

8. Les nombres 101, 103 et 107 sont premiers.

3 Exercices de cours

1. Soit m et n deux nombres premiers entre eux.

a) Pour tout entier $k \geqslant 1$, soit $f_k : \mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ défini par $f_k(a) = a$ modulo k. Déterminer le noyau de $f = (f_m, f_n) : \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.

b) En déduire que pour tout couple d'entiers (x, y), il existe un entier a tel que $a = x$ modulo m et $a = y$ modulo n (lemme chinois).

2. a) Soit p un nombre premier et $n \in \mathbb{N}$. Calculer le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/p^n\mathbb{Z}$.

b) Soit n un entier positif et $n = p_1^{n_1} \cdots p_k^{n_k}$ sa factorisation réduite. Déduire du a) de l'exercice 1 que $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à l'annneau produit

$$\mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}.$$

c) Prouver que, avec les notations de b), le nombre $\varphi(n)$ des inversibles de $\mathbb{Z}/n\mathbb{Z}$ vaut (formule d'Euler)

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

où le produit porte sur les nombres premiers p.

3. a) En utilisant l'algorithme d'Euclide, déterminer le pgcd de 525 et 231.

b) En remontant les calculs, trouver des entiers x et y tels que

$$x525 + y231 = \text{pgcd}(525, 231).$$

4. a) Soit $p_1, \ldots, p_n$ des entiers positifs avec $p_i \leqslant 2^{2^{i-1}}$, et $P = p_1 \cdots p_n + 1$. Prouver que P est premier avec chaque p_i et vérifie $1 \leqslant P \leqslant 2^{2^n}$.

b) En déduire que l'ensemble des nombres premiers est infini, que le $n$ème nombre premier p_n est majoré par $2^{2^{n-1}}$ et que le nombre $\pi(x)$ de nombres premiers $p \leqslant x$ majorés par x vérifie

$$\pi(x) \geqslant \frac{\log(\log x) - \log(\log 2)}{\log 2}.$$

Addendum En fait $\pi(x)$ est équivalent à $x/\log x$ quand $x \to \infty$ et le $n$ème nombre premier p_n est équivalent à $n \log n$. Des formules approchées encore plus précises sont obtenues en remplaçant le logarithme usuel par

$$\text{Li}(x) = \int_1^x \frac{\mathrm{d}x}{\log x}.$$

4 Exercices

1. a) Prouver qu'il existe une infinité de nombres premiers de la forme $4n + 3$.

b) Prouver qu'il existe une infinité de nombres premiers de la forme $6n + 5$.

2. a) Résoudre les équations $637x + 595y = 91$ et $637x + 595y = 143$ pour x et y entiers relatifs.

b) Préciser si l'équation $442x = 317$ modulo 495 admet une solution x entier relatif.

c) Déterminer les entiers relatifs (u, v) tels que $442u + 495v = 1$.

d) En déduire les solutions de l'équation de b).

3. a) Résoudre l'équation $x^2 + y^2 = 0$ pour x et y éléments de $\mathbb{Z}/3\mathbb{Z}$.

b) En déduire que l'ensemble des entiers relatifs (x, y, z) tels que $x^2+y^2-3z^2 = 0$ vaut $\{(0, 0, 0)\}$.

c) Préciser si le cercle de centre $(0, 0)$ et de rayon $\sqrt{3}$ comprend des points de coordonnées rationnelles.

4. a) Prouver que, pour tout entier n impair, n^2 est congru à 1 modulo 8.

b) En déduire que l'ensemble des entiers relatifs (x, y, z, t) tels que $x^2 + y^2 + z^2 - 7t^2 = 0$ vaut $\{(0, 0, 0, 0)\}$.

5. a) Soit $1 \leqslant a < b$ des entiers. Prouver qu'il existe un entier unique $n_1 \geqslant 2$ tel que $\dfrac{1}{n_1} \leqslant \dfrac{a}{b} < \dfrac{1}{n_1 - 1}$ et que si $a_1 = an_1 - b$ et $b_1 = bn_1$, alors $a_1 < a$ et $0 \leqslant \dfrac{a}{b} - \dfrac{1}{n_1} = \dfrac{a_1}{b_1} < \dfrac{1}{n_1}$.

b) Soit r un nombre rationnel strictement positif. Prouver qu'il existe $k \geqslant 1$ et des entiers $n_i \geqslant 1$ pour $1 \leqslant i \leqslant k$ avec $n_i < n_{i+1}$ et

$$r = \frac{1}{n_1} + \cdots + \frac{1}{n_k}.$$

On pourra d'abord utiliser a) pour traiter le cas où r appartient à $]0, 1[$.

6. Soit p un nombre premier et $n \geqslant 1$ un entier naturel. Soit p^{a_n} la plus grande puissance de p divisant $(p^n)!$, c'est-à-dire $(p^n)! = p^{a_n} q$ où q est premier avec p.

a) Dans le cas $p = 3$, calculer a_2.

b) En général établir que $a_0 = 0$ et que $a_{n+1} = p\, a_n + 1$ pour tout $n \geqslant 0$.

7. Soit $n \geqslant 1$ un entier naturel. Prouver qu'il existe un multiple de n de la forme $10^m - 1$ si et seulement si n est premier avec 10. On pourra considérer l'élément 10 de $\mathbb{Z}/n\mathbb{Z}$.

En déduire que :

a) 2004 possède un multiple dont l'écriture décimale ne comporte que le chiffre 4 ;

b) 2004 ne possède aucun multiple dont l'écriture décimale ne comporte que le chiffre 6.

9. a) Soit p un nombre premier et a un entier naturel non divisible par p. Prouver qu'il existe un entier naturel $k \geqslant 1$ vérifiant la propriété suivante : pour tout entier n, $a^n = 1$ modulo p si et seulement si k divise n. Montrer que k divise $p - 1$.

b) Prouver que 16 est le plus petit entier positif k tel que $5^k = 1$ modulo 17. On pourra d'abord vérifier que $5^8 = -1$ modulo 17.

c) Prouver que pour tout entier b non divisible par 17, il existe un entier positif n tel que $5^n = b$ modulo 17, et trouver tous les entiers naturels n tels que $5^n = 3$ modulo 17.

d) Dans le cas général de a), soit b un entier naturel non divisible par p. Prouver qu'il existe un entier naturel $\ell \geqslant 1$ vérifiant la propriété suivante : pour tout entier n, $a^n = b$ modulo p si et seulement si $n = \ell$ modulo k.

Supplément

Soit $M = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ une matrice 2×2 à cœfficients entiers. Pour tout entier n, soit $E_1(n) = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ et $E_2(n) = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$. Calculer $E_1(n)\, M$ et $E_2(n)M$.

Soit a et b des entiers non nuls. On définit un entier $K \geqslant 0$ et des suites $(a_k)_k$, $(b_k)_k$ et $(M_k)_k$, à valeurs dans $\mathbb{Z}$, $\mathbb{Z}$ et $M_2(\mathbb{Z})$ et indexées par $0 \leqslant k \leqslant K$, comme suit.

On pose $a_0 = a$, $b_0 = b$ et $M_0 =$ la matrice identité puis, pour tout $k \geqslant 0$, on applique les étapes suivantes.

Si $b_{2k} \neq 0$, on pose $a_{2k+1} = a_{2k} - b_{2k}q_{2k}$ avec $0 \leqslant a_{2k+1} \leqslant |b_{2k}| - 1$. Donc a_{2k+1} est le reste de la division de a_{2k} par b_{2k} et q_{2k} est le quotient. On pose $b_{2k+1} = b_{2k}$ et $M_{2k+1} = E_1(q_{2k})M_{2k}$.

Si $a_{2k+1} \neq 0$, on pose $a_{2k+2} = a_{2k+1}$, $b_{2k+2} = b_{2k+1} - a_{2k+1}q_{2k+1}$ avec $0 \leqslant b_{2k+2} \leqslant a_{2k+1} - 1$. Donc b_{2k+2} est le reste de la division de b_{2k+1} par a_{2k+1} et q_{2k+1} est le quotient. On pose $M_{2k+2} = E_2(q_{2k+1})\, M_{2k+1}$.

Si $b_{2k} = 0$ ou $a_{2k+1} = 0$, on a terminé et on pose $K = 2k$ ou $K = 2k + 1$ selon les cas.

Montrer que le pgcd de a et b vaut

$$\text{pgcd}(a, b) = a_K = x_K a + y_K b \quad \text{si } K \text{ est pair,}$$

et

$$\text{pgcd}(a, b) = b_K = z_K a + t_K b \quad \text{si } K \text{ est impair.}$$

Dans le cas $a = 525$, $b = 231$, calculer K et les suites $(a_k)_k$, $(b_k)_k$ et $(M_k)_k$, en écrivant chaque matrice M_k comme $M_k = \begin{pmatrix} x_k & y_k \\ z_k & t_k \end{pmatrix}$. Calculer $M_K \begin{pmatrix} a \\ b \end{pmatrix}$.

Supplément

a) Soit x et y deux entiers strictement positifs et premiers entre eux. Prouver qu'il existe un entier $k \geqslant 1$ tel que $x^k = 1$ modulo y.

b) Soient a et r deux entiers avec $a > r \geqslant 2$. La suite arithmétique de premier terme a et raison r vaut $(a + nr)_{n\in\mathbb{N}}$. Montrer que cette suite contient une infinité de termes ayant tous les mêmes diviseurs premiers. On pourra traiter d'abord avec a) le cas où a et r sont premiers entre eux.

Note En 2004, Ben Green et Terence Tao ont montré qu'il existe des suites arithmétiques en nombres premiers arbitrairement longues. La plus longue suite connnue est constituée de 23 termes. (Tao a reçu à 31 ans une des médailles Fields décernées au Congrès de Madrid en 2006.)