Fiche d'exercices n$^{\text{o}}$ 8

Structures algébriques usuelles

Groupes

Exercice 1.

Soit G un groupe, H un sous-groupe, et A une partie non vide de G. On pose $AH = \{ah\,,\,(a,h) \in A \times H\}$. Montrer que $AH = H$ si, et seulement si, $A \subset H$.

Exercice 2. ⋆ *sous-groupe distingué*

Un sous-groupe H d'un groupe G est dit *distingué* lorsque

$$\forall x \in H, \quad \forall a \in G, \quad axa^{-1} \in H$$

a) Montrer que le noyau d'un morphisme de groupe est distingué.

b) Soient H et K deux sous-groupes d'un groupe G, avec H distingué. Montrer que $HK = \{xy\,,\,(x,y) \in H \times K\}$ est un sous-groupe de G.

Exercice 3. *automorphismes intérieurs*

Soit G un groupe multiplicatif. On note $\mathrm{Aut}(G)$ l'ensemble de ses automorphismes.

a) Montrer que $\mathrm{Aut}(G)$ est un groupe pour la loi $\circ$.

b) Déterminer $\mathrm{Aut}(\mathbb{Z})$.

c) Pour $a \in G$ on note $\phi_a : G \to G$ définie par $\phi_a : x \mapsto axa^{-1}$. Montrer que $\phi_a \in \mathrm{Aut}(G)$, et que l'application $a \mapsto \phi_a$ est un morphisme de groupes.

Exercice 4. ⋆ *théorème de Lagrange*

Soit G un groupe fini et H un sous-groupe de G. On définit une relation sur G par :

$$\forall\ x, y \in G,\ x \sim y \iff \exists\ h \in H,\ x = hy.$$

a) Montrer que $\sim$ est une relation d'équivalence. Quelle est la classe de e ?

b) Soit $a \in G$. Montrer que $\overline{a}$ est équipotent à H.

c) En déduire que $\mathrm{card}(H)$ divise $\mathrm{card}(G)$.

Exercice 5.

Soient H et K deux sous-groupes d'un groupe abélien $(G, +)$. Montrer que le sous-groupe engendré par $H \cup K$ est

$$\langle H \cup K \rangle = H + K = \{h + k\,,\,(h,k) \in H \times K\}$$

Exercice 6. ⋆

Soit A une partie non vide d'un groupe G. Montrer que

$$\langle A \rangle = \{a_1 \cdots a_n\,;\, n \in \mathbb{N}^*, a_1, \ldots, a_n \in A \cup A'\},$$

où $A' = \{a^{-1}\,,\, a \in A\}$.

Exercice 7.

Montrer que $\dfrac{2}{3}\mathbb{Z} + \dfrac{4}{5}\mathbb{Z}$ est un sous-groupe monogène de $(\mathbb{Q}, +)$.

Exercice 8.

Dans $(\mathbb{C}^*, \times)$ déterminer le sous-groupe $\langle \mathcal{P} \rangle$ engendré par l'ensemble $\mathcal{P}$ des nombres premiers.

Exercice 9. ⋆

Soit G un groupe fini de cardinal n. Montrer qu'il existe une partie génératrice de G de cardinal inférieur ou égal à $\log_2(n)$.

Exercice 10. ⋆

Sans le groupe $(\mathcal{S}_E, \circ)$ des permutations de $E = \mathbb{R}\backslash\{0, 1\}$, déterminer le sous groupe engendré par les fonctions f et g définies par

$$f(x) = 1 - x \qquad \text{et} \qquad g(x) = \frac{1}{x}$$

Exercice 11. ⋆⋆

Montrer que le groupe symétrique $\mathcal{S}_n$ est engendré par $\tau = (1 \quad 2)$ et $\sigma = (1 \quad 2 \quad \cdots \quad n)$.

Exercice 12. ⋆

Soient deux groupes H et K.

a) Montrer que si h est un élément d'ordre p de H, et k un élément d'ordre q de K, alors (h, k) est un élément d'ordre $\mathrm{ppcm}(p, q)$ de $H \times K$.

b) On suppose H et K cycliques. Montrer que $H \times K$ est un groupe cyclique si, et seulement si, les ordres de H et K sont premiers entre eux.

Exercice 13. ⋆

Soit p un entier naturel premier. On note $\mathbb{U}_{p^\infty}$ l'ensemble des $z \in \mathbb{C}$ pour lesquels existe $n \in \mathbb{N}$ tel que $z^{p^n} = 1$.

a) Montrer que $\mathbb{U}_{p^\infty}$ est un groupe multiplicatif infini où tout élément est d'ordre fini.

b) Montrer que tout sous-groupe H de $\mathbb{U}_{p^\infty}$, distinct de $\mathbb{U}_{p^\infty}$, est cyclique.
(on pourra considérer un élément z_0 de $G\backslash H$ et montrer que l'ordre des éléments de H n'excède pas celui de z_0).

Exercice 14. ⋆

Déterminer le plus petit entier n pour lequel il existe un groupe non commutatif de cardinal n.

Exercice 15. ⋆

Pour tout $(a, b) \in \mathbb{C}^* \times \mathbb{C}$, on considère la fonction $f_{a,b} : \mathbb{C} \to \mathbb{C}$ définie par

$$f_{a,b}(z) = az + b$$

a) Montrer que l'ensemble $\{f_{a,b}\ ,\ a \in \mathbb{C}, b \in \mathbb{C}^*\}$ est muni d'une structure de groupe pour la loi de composition $\circ$.

b) Déteterminer les éléments d'ordre fini de ce groupe.

Exercice 16. *sous-groupes de $\mathbb{Z}/n\mathbb{Z}$*

Soit $n \in \mathbb{N}^*$ et $G = \mathbb{Z}/n\mathbb{Z}$. On note $\varphi : \mathbb{Z} \to G$ la surjection canonique. Soit H un sous-groupe de G.

a) Montrer que $\varphi^{-1}(H)$ est de la forme $d\mathbb{Z}$, avec $d \in \mathbb{N}^*$ un diviseur de n.

b) Montrer que H est cyclique, engendré par $\overline{d}$. Quel est le cardinal de H ?

c) Décrire tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 17.

Soit G et G' deux groupes additifs et $f : G \to G'$ un morphisme de groupes.

a) Montrer que pour tout sous-groupe H de G on a : $f^{-1}(f(H)) = H + \operatorname{Ker} f$.

b) Montrer que pour tout sous-groupe H' de G' on a : $f(f^{-1}(H')) = H' \cap \operatorname{Im} f$.

Exercice 18.

Soit G un groupe cyclique engendré par a d'ordre n, G' un deuxième groupe, et $a' \in G'$.

a) Montrer qu'il existe un morphisme $\phi : G \to G'$ tel que $\phi(a) = a'$ si et seulement si a' est d'ordre fini divisant n

b) Application : déterminer tous les morphismes : $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$, $\quad \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$, $\quad \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.

Exercice 19.

Soient a, b deux éléments d'un groupe multiplicatif G tels que : $\begin{cases} a \text{ est d'ordre } \alpha \\ b \text{ est d'ordre } \beta \\ \alpha \wedge \beta = 1 \\ ab = ba \end{cases}$.

Déterminer l'ordre de ab.

Exercice 20.

Soit G un groupe fini tel que : $\forall\, x \in G,\ x^2 = e$.

a) Montrer que G est commutatif (considérer $(xy)(xy)$).

b) Soit H un sous-groupe de G et $x \in G \backslash H$. On note K le sous groupe engendré par $H \cup \{x\}$. Montrer que $\mathrm{card}(K) = 2\mathrm{card}(H)$.

c) En déduire que $\mathrm{card}(G)$ est une puissance de 2.

Exercice 21.

On considère le groupe $G = \mathbb{Z}^2$. Une *base* de G est une famille $(\alpha = (a, a'), \beta = (b, b'))$ engendrant G.

a)
- a) Montrer que (α, β) est une base de G si et seulement si $\det(\alpha, \beta) = \pm 1$.
- b) Montrer que $\alpha = (a, a')$ appartient à une base de G si et seulement si $a \wedge a' = 1$.

b) Soit H un sous-groupe non trivial de G. On note $H' = \{ux + vy \text{ tq } u \in \mathbb{Z},\ v \in \mathbb{Z}, (x, y) \in H\}$, n le plus petit élément de H' strictement positif et $u \in \mathbb{Z}$, $v \in \mathbb{Z}$, $(x, y) \in H$ tels que $ux + vy = n$.
- a) Montrer que $u \wedge v = 1$ et que x et y sont divisibles par n.
- b) On pose $\alpha = (x/n, y/n)$ et $\beta = (-v, u)$. Montrer que (α, β) est une base de G et qu'il existe $p \in \mathbb{N}$ tel que $(n\alpha, np\beta)$ engendre H.

Anneaux

Exercice 22.

Soient a, b deux éléments d'un anneau A tels que ab soit inversible et b non diviseur de zéro. Montrer que a et b sont inversibles.

Exercice 23.

Soit A un anneau commutatif non nul dont les seuls idéaux sont $\{0\}$ et A. Montrer que A est un corps.

Exercice 24. ⋆

Soit A un anneau intègre et G une partie finie non vide de $A \backslash \{0\}$ stable par multiplication. Montrer que G est un sous-groupe de $A^\times$.

Exercice 25.

Soit A un anneau commutatif, et $a \in A$. On dit que a est *nilpotent* s'il existe $n \in \mathbb{N}$ tel que $a^n = 0$.

a) Déterminer les éléments nilpotents de $\mathbb{Z}/36\mathbb{Z}$.

b) Montrer que l'ensemble des éléments nilpotents est un idéal de A.

c) Soit $a \in A$ nilpotent. Montrer que $1 - a$ est inversible (remarquer que $1 = 1^n - a^n$).

d) Soient a nilpotent et b inversible. Montrer que $a + b$ est inversible.

Exercice 26. *Caractéristique d'un anneau*

Soit A un anneau. On appelle *caractéristique* de A l'ordre de 1 dans le groupe additif $(A, +)$. On suppose A de caractéristique finie n.

a) Montrer que : $\forall\, x \in A,\ nx = 0$.

b) Si A est intègre, montrer que n est un nombre premier.

c) Si A est intègre et commutatif, montrer que $x \mapsto x^n$ est un morphisme d'anneau.

Exercice 27. ⋆

On rappelle qu'un idéal I d'un anneau A est *principal* lorsqu'il est de la forme aA pour un certain $a \in A$. Montrer que les idéaux de tous les sous-anneaux de $\mathbb{Q}$ sont principaux.

Exercice 28. ⋆ *Idéal premier*

Un idéal I d'un anneau A est dit *premier* lorsque $I \neq A$ et $\forall\, x, y \in A,\ xy \in I \Rightarrow x \in I$ ou $y \in I$.

a) Quels sont les idéaux premiers de $\mathbb{Z}$?

b) Montrer que si A est commutatif non nul et si tous les idéaux de A sont premiers alors A est un corps.

Exercice 29. ⋆ *produit d'idéaux*

Soit A un anneau commutatif et I, J deux idéaux de A.
On note $IJ = \{a_1 b_1 + \cdots + a_n b_n \text{ tq } a_i \in I,\ b_i \in J\}$.

a) Montrer que IJ est un idéal de A.

b) Montrer que $I(J + K) = IJ + IK$.

c) On suppose $I + J = A$. Montrer que $IJ = I \cap J$.

d) Pour $A = \mathbb{Z}$, $I = n\mathbb{Z}$, $J = p\mathbb{Z}$, déterminer IJ.

Exercice 30. ⋆ *nilradical*

On appelle *nilradical* d'un anneau commutatif A l'ensemble N des éléments nilpotent de A.

a) Montrer que N est un idéal de A.

b) Déterminer N lorsque $A = \mathbb{Z}/n\mathbb{Z}$.

Exercice 31. ⋆ *radical d'un idéal*

On appelle *radical* d'un idéal I d'un anneau commutatif A l'ensemble $R(I)$ des éléments $x \in A$ pour lesquels il existe $q \in \mathbb{N}^*$ tel que $x^q \in I$.

a) Si I est un idéal de A, montrer que $R(I)$ est un idéal de A contenant I.

b) Soient deux idéaux I et J deux idéaux de A. Montrer que $R(I \cap J) = R(I) \cap R(J)$.

c) Déterminer le radical de $n\mathbb{Z}$ dans l'anneau $\mathbb{Z}$, pour $n \in \mathbb{N}$.

Exercice 32. ⋆ *anneau local*

On appelle *anneau local* un anneau commutatif A dans lequel l'ensemble $V(A)$ des éléments non inversibles est un idéal.

a) Montrer que dans un anneau local A, $V(A)$ est un idéal *maximal*, c'est-à-dire qu'il n'est strictement contenu dans aucun idéal autre que A.

b) Soit $m = p^n$, avec p premier et $n \in \mathbb{N}^*$. Montrer que $\mathbb{Z}/mZ$ est un anneau local.

c) Plus généralement, déterminer tous les anneaux locaux parmi les $\mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{N}$.

Exercice 33.

On considère ici $\mathbb{Z}^2$ muni de sa structure d'anneau produit.

a) Soit $d \in \mathbb{N}$. On pose $A_d = \{(x, y) \in \mathbb{Z}^2 \text{ tq } x \equiv y[d]\}$ ($x = y$ pour $d = 0$).
Montrer que A_d est un sous-anneau de $\mathbb{Z}^2$

b) Montrer que l'on obtient ainsi tou

c) Soit I un idéal de $\mathbb{Z}^2$. On note : $\begin{cases} I_1 = \{x \in \mathbb{Z} \text{ tq } (x, 0) \in I\} \\ I_2 = \{y \in \mathbb{Z} \text{ tq } (0, y) \in I\}. \end{cases}$

Montrer que I_1 et I_2 sont des idéaux de $\mathbb{Z}$, et que $I = I_1 \times I_2$.

d) En déduire que I est un idéal principal, c'est-à-dire engendré par un seul élément.

Exercice 34.

Soient A et B deux anneaux commutatifs et soit $K \subset A \times B$. Démontrer que K est un idéal de $A \times B$ si, et seulement si $K = I \times J$, où I est un idéal de A et J est un idéal de B.

Exercice 35.

Soit G un groupe additif et A l'ensemble tous les morphismes de G dans G.

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

b) On prend $G = \mathbb{Z}/n\mathbb{Z}$, avec $n \geqslant 2$. Montrer que A est l'ensemble des applications de la forme $x \mapsto kx$ avec $k \in G$ et que $A \simeq \mathbb{Z}/n\mathbb{Z}$.

Exercice 36. *Entiers de Gauss*

Soit $A = \{a + bi\,, (a, b) \in \mathbb{Z}^2\}$.

a) Montrer que A est un sous-anneau de $\mathbb{C}$. Quels sont les éléments inversibles ?

b) Soient $u, v \in A$ avec $v \neq 0$. Montrer qu'il existe $q, r \in A$ tels que $u = qv + r$ et $|r| < |v|$.

c) Montrer que A est *principal*, c'est-à-dire que tout idéal de A est engendré par un seul élément.

Exercice 37.

Soit A un anneau non nul, commutatif et intègre.

a) Montrer que si A est fini, alors c'est un corps.

b) Montrer que si A n'a qu'un nombre fini d'idéaux, alors c'est un corps (considérer les idéaux $I_n = x^n A$ pour $x \in A$ non nul).

Exercice 38.

On considère l'ensemble $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}\,,\ (a, b) \in \mathbb{Q}^2\}$. Montrer qu'il s'agit d'un sous-corps de $\mathbb{R}$.

Exercice 39. ⋆

Soit A un anneau commutatif fini non nul. Montrer que A est intègre si, et seulement si, A est un corps.

Exercice 40. ⋆

Soit p un nombre premier supérieur ou égal à 3.

a) Montrer que pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$

b) En déduire que $f : \overline{x} \mapsto \overline{x}^p$ est un morphisme d'anneaux sur $\mathbb{Z}/p\mathbb{Z}$.

c) En déduire le petit théorème de Fermat.

Exercice 41. ⋆ *théorème de Wilson*

Soit p un nombre premier.

a) Quels sont les éléments de $\mathbb{Z}/p\mathbb{Z}$ égaux à leur inverse ?

b) En déduire que p divise $(p-1)! + 1$

c) Inversement, montrer que si un entier n supérieur à 2 divise $(n-1)!+1$, alors celui-ci est premier.

Exercice 42. ⋆⋆

Soit p un nombre premier supérieur ou égal à 3.

a) Quel est le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$?

b) On suppose $p \equiv 1$ [4]. Justifier que $\overline{-1}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ en calculant de deux façons la classe de congruence de $(p-1)!$

c) On suppose $p \equiv 3$ [4]. Montrer que $\overline{-1}$ n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.