Chapter 14 Groupes

14.1 loi de composition

Exercice 14.1 *Étude de lois de composition*

Indiquer, parmi les applications suivantes, lesquelles sont des lois de composition interne. Lorsque c'est le cas, préciser l'éventuelle associativité ou commutativité.

$$\perp : \begin{array}{rcl} \mathbb{R}\times\mathbb{R} & \to & \mathbb{R} \\ (x,y) & \mapsto & x-y \end{array} \qquad \top : \begin{array}{rcl} \mathbb{R}\times\mathbb{R} & \to & \mathbb{R} \\ (x,y) & \mapsto & \frac{x+y}{4} \end{array}$$

$$\square : \begin{array}{rcl} \mathbb{R}^{\mathbb{N}}\times\mathbb{R}^{\mathbb{N}} & \to & \mathbb{R}^{\mathbb{N}} \\ \big((u_n),(v_n)\big) & \mapsto & (u_0,v_0,u_1,v_1,u_2,v_2,\dots) \end{array} \qquad \triangle : \begin{array}{rcl} [0,1]\times[0,1] & \to & [0,1] \\ (x,y) & \mapsto & \mathrm{e}^{x+y} \end{array}.$$

Exercice 14.2 *Propriétés de lois de composition*

Étudier les lois de composition interne suivantes : commutativité, élément neutre éventuel, éléments inversibles.

$$\star : \begin{array}{rcl} \mathfrak{P}(\mathbb{N})\times\mathfrak{P}(\mathbb{N}) & \to & \mathfrak{P}(\mathbb{N}) \\ (A,B) & \mapsto & A\cap B \end{array} \qquad \square : \begin{array}{rcl} \mathbb{R}_+ & \to & \mathbb{R}_+ \\ (x,y) & \mapsto & \max(x,y) \end{array}$$

$$\triangle : \begin{array}{rcl} \big(\mathbb{R}^\star\times\mathbb{R}\big)^2 & \to & \mathbb{R}^\star\times\mathbb{R} \\ \big((x,y),(x',y')\big) & \mapsto & \big(xx', xy'+x'y\big) \end{array}$$

14.2 La structure de groupes

Exercice 14.3 *Addition des vitesses en théorie de la relativité*

Soit $c > 0$ (c correspond à la vitesse de la lumière) et $I =]-c,c[$.

1. Montrer
$$\forall (x,y)\in I^2, x\star y = \frac{x+y}{1+\frac{xy}{c}} \in I.$$

2. Montrer que la loi $\star$ munit I d'une structure de groupe abélien.

Cette loi $\star$ correspond à l'addition des vitesses portées par un même axe en théorie de la relativité.

Exercice 14.4

Soit l'ensemble
$$\mathcal{J} = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}) \;\middle|\; x\in\mathbb{R}^\star \right\}.$$

Montrer que, muni de la multiplication usuelle des matrices, $\mathcal{J}$ est un groupe abélien.

Exercice 14.5

On considère les fonctions de $\mathbb{R}\setminus\{0,1\}$ dans lui-même définies par

$$f_1(x)=x, \qquad f_2(x)=\frac{1}{1-x}, \qquad f_3(x)=\frac{x-1}{x},$$
$$f_4(x)=\frac{1}{x}, \qquad f_5(x)=1-x, \qquad f_6(x)=\frac{x}{x-1}.$$

1. Montrer qu'elles forment un groupe G pour la loi $\circ$.

2. Quels sont les sous-groupes de G?

Exercice 14.6

Soit $(G,\cdot)$ un groupe tel que $x^2 = e$ pour tout $x \in G$. Montrer que G est commutatif.

Exercice 14.7

Soit $(G,.)$ un groupe dont on note e l'élément neutre.

Soit $a,b,c \in G$. On suppose que $b^6 = e$ et $ab = b^4a$. Montrer les égalités $b^3 = e$ et $ab = ba$.

Exercice 14.8

Montrer que $H = \left\{ \frac{a}{3^n} \;\middle|\; a \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$ est un sous-groupe de $(\mathbb{R},+)$.

Exercice 14.9

Soit

$$G = \left\{ \begin{pmatrix} 2^x & 0 & 0 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; x \in \mathbb{R} \right\}.$$

Montrer que G est un groupe multiplicatif.

Exercice 14.10

Montrer que

$$\left\{ \frac{1}{\sqrt{1-x^2}} \begin{pmatrix} 1 & x \\ x & 1 \end{pmatrix} \;\middle|\; x \in]-1,1[\right\}$$

est un groupe pour la multiplication matricielle.

Exercice 14.11

Sur $G = \mathbb{R}^\star \times \mathbb{R}$, on définit la loi $\square$ par $(x,y)\square(x',y') = (xx', xy' + y)$.

1. Montrer que $(G,\square)$ est un groupe.

2. Montrer que $H =]0,+\infty[\times\mathbb{R}$ est un sous-groupe de $(G,\square)$.

Exercice 14.12 *Un exemple de sous-groupe*

On pose $\mathbb{Z}[\sqrt{7}] = \left\{ a + b\sqrt{7} \;\middle|\; (a,b) \in \mathbb{Z}^2 \right\}$.

Montrer que $\mathbb{Z}[\sqrt{7}]$ est un sous-groupe de $(\mathbb{R},+)$.

Exercice 14.13

Pour la multiplication usuelle des matrices carrées, les ensembles suivants sont-ils des groupes.

1. $\mathbf{GL}_2(\mathbb{R}) \cap \mathscr{M}_2(\mathbb{Z})$.

2. $\left\{ M \in \mathscr{M}_2(\mathbb{Z}) \;\middle|\; \det M = 1 \right\}$.

Exercice 14.14 (**)

Soit $(G,\star)$ un groupe. On appelle centre de G l'ensemble

$$Z(G) = \{ x \in G \mid \forall g \in G, x \star g = g \star x \}.$$

Montrer que $Z(G)$ est un sous-groupe de G.

Exercice 14.15 (**)

Soient G un groupe commutatif d'élément neutre e et $n \in \mathbb{N}$. On pose

$$B = \{ a \in G \mid a^n = e \}.$$

Montrer que B est un sous-groupe de G.

Exercice 14.16 (***)

Soit G un groupe commutatif d'élément neutre e. On pose

$$B = \left\{ a \in G \;\middle|\; \exists n \in \mathbb{N}^\star, a^n = e \right\}.$$

Montrer que B est un sous-groupe de G.

Exercice 14.17 (**)

Soit G un groupe abélien fini (loi notée multiplicativement), de cardinal $n \geq 2$, de neutre e, et a, un élémnet de G.

1. En considérant l'ensemble des a^k, $k = 0, \dots, n$, montrer qu'il existe $d \in [\![1, n]\!]$ tel que $a^d = e$.

2. Justifier l'existence de ω, le plus petit entier supérieur ou égal à 1 vérifiant $a^\omega = e$. ω s'appelle l'**ordre** de l'élément a.

3. Vérifier que
$$< a >= \left\{ e, a, a^2, \dots, a^{\omega-1} \right\}$$
est un sous-groupe de G à ω éléments.

Exercice 14.18 (**)

Soit $(G, +)$ un groupe commutatif ; soient A et B deux parties de G. On définit la somme de A et B, notée $A + B$, par
$$A + B = \{ x \in G \mid \exists (a, b) \in A \times B, x = a + b \} .$$

1. Montrer que si A et B sont deux sous-groupes de G, $A + B$ est un sous-groupe de G.

2. On suppose maintenant que A et $A + B$ sont deux sous-groupes de G ; B est-il un sous-groupe de G ?

Exercice 14.19 (***)

Soit $(G, \cdot)$ un groupe (non commutatif) ; soient A et B deux sous-groupes de G. On définit le produit de A et B, noté $A \cdot B$, par
$$A \cdot B = \{ x \in G \mid \exists (a, b) \in A \times B, x = a.b \} .$$

Montrer les équivalences
$$(A \cdot B \text{ est un sous-groupe de } G) \iff (A \cdot B = B \cdot A) \iff (B \cdot A \subset A \cdot B) .$$

Donner un exemple (en précisant G, A, B) où $A \cdot B$ n'est pas un groupe.

Exercice 14.20 (****) *Théorème de Lagrange*

Soient $(G, \cdot)$ un groupe fini et H un sous-groupe de G. On définit la relation $\mathcal{R}$ dans G par
$$x \mathcal{R} y \iff x y^{-1} \in H .$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence dans G et que la classe d'équivalence de x modulo $\mathcal{R}$ est
$$xH = \{ xh \mid h \in H \} .$$

2. Montrer que les classe d'équivalence modulo $\mathcal{R}$ ont toutes le même cardinal que H.

3. En déduire que
$$\operatorname{card}(G) = \operatorname{card}(H) \times \operatorname{card}(G/\mathcal{R})$$
où $G/\mathcal{R}$ désigne l'ensemble des classe d'équivalences modulo $\mathcal{R}$.

On a ainsi prouvé le théorème de Lagrange:

> Dans un groupe fini, l'ordre de tout sous-groupe divise l'ordre du groupe.

Exercice 14.21

Traduire en termes d'homomorphisme de groupes les propriétés traditionnelles suivantes

1. $\ln(xy) = \ln x + \ln y$;
2. $|zw| = |z||w|$;
3. $(xy)^{\frac{1}{2}} = x^{\frac{1}{2}} y^{\frac{1}{2}}$;
4. $e^{z+w} = e^z e^w$;
5. $\overline{z+w} = \bar{z} + \bar{w}$;
6. $\overline{zw} = \bar{z}\bar{w}$.

Exercice 14.22

Soient $n \in \mathbb{N}^\star$ et $f : \begin{array}{rcl} \mathbb{R}^\star & \to & \mathbb{R}^\star \\ x & \mapsto & x^n \end{array}$. Montrer que f est un endomorphisme du groupe $(\mathbb{R}^\star, .)$. Déterminer son image et son noyau.

Exercice 14.23

Soit $f : \mathbb{R} \to \mathbb{C}^\star$ l'application qui à tout $x \in \mathbb{R}$ associe $e^{ix} \in \mathbb{C}^\star$.

1. Montrer que f est un homomorphisme de groupes.
2. Calculer son noyau et son image.
3. f est-elle injective ?

Exercice 14.24

Pour tout couple (a, b) de $\mathbb{R}^2$, on pose la matrice

$$M_{a,b} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Soit

$$\mathcal{G} = \left\{ M_{a,b} \;\middle|\; (a, b) \in \mathbb{R}^2 \setminus \{ (0,0) \} \right\} \qquad \text{et} \qquad f : \begin{array}{rcl} \mathcal{G} & \to & \mathbb{R}^\star \\ M_{a,b} & \mapsto & a^2 + b^2 \end{array}.$$

1. Montrer que $\mathcal{G}$ est un groupe pour la loi usuelle de multiplication des matrices carrées.
2. Montrer que f est un morphisme du groupe $(\mathcal{G}, \times)$ dans le groupe $\left(\mathbb{R}^\star, \times\right)$.

Exercice 14.25

Soit $(G, .)$ un groupe. Pour $a \in G$ fixé, on considère l'application

$$f_a : \begin{array}{rcl} G & \to & G \\ x & \mapsto & a.x.a^{-1} \end{array}.$$

1. Montrer que f_a est un automorphisme de $(G, .)$.
2. On note $I = \left\{ f_a \;\middle|\; a \in G \right\}$. Montrer que $(I, \circ)$ est un groupe où $\circ$ est la loi de composition des applications de G dans G.
3. Soit
$$\varphi : \begin{array}{rcl} G & \to & I \\ a & \mapsto & f_a \end{array}.$$
Montrer que φ est un morphisme de $(G, .)$ dans $(I, \circ)$.

Exercice 14.26

Montrer que

$$\left\{ \begin{pmatrix} 1 & 0 & x \\ -x & 1 & -\frac{x^2}{2} \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; x \in \mathbb{R} \right\}$$

est un groupe (pour la multiplication usuelle) isomorphe à $(\mathbb{R}, +)$.

Exercice 14.27 *Étude des groupes à faibles cardinaux*

1. (a) Soit $(G, \cdot)$ un groupe à deux éléments. Construire la table de multiplication de G.
   (b) Soit $(G, \cdot)$ et $(G', \cdot)$ deux groupes à deux éléments. Construire un isomorphisme de groupes de G dans G'.

   Ainsi, tous les groupes à deux éléments sont isomorphes. On dit qu'il n'y a qu'un groupe à deux éléments à isomorphisme près.

2. Soit $(G, \cdot)$ un groupe à trois éléments. Construire la table de multiplication de G. En déduire qu'il n'y a qu'un groupe à trois éléments à isomorphisme près.

3. Montrer que $\mathbb{U}_4$ et $\mathbb{U}_2 \times \mathbb{U}_2$ (muni de la loi de groupe produit) ne sont pas isomorphes (il y a donc plusieurs «types» de groupes à quatre éléments).

Exercice 14.28

Déterminer, à isomorphisme près, les groupes d'ordre 6.

Exercice 14.29

Soit $(G, .)$ un groupe (quelconque). On note $C(G)$ l'ensemble des caractères de G, c'est-à-dire l'ensemble des morphismes de G vers le groupe multiplicatif $\mathbb{C}^\star$.

1. Montrer que $C(G)$ est un groupe commutatif pour la loi naturelle. On l'appelle *groupe des caractères* de G.

2. Montrer que $C(\mathbb{Z})$ est isomorphe à $\mathbb{C}^\star$.

3. Soient $n \in \mathbb{N}$ et $\omega = e^{2i\pi/n}$. Montrer que $F : \begin{array}{ccc} C(\mathbb{U}_n) & \to & \mathbb{U}_n \\ f & \mapsto & f(\omega) \end{array}$ est un isomorphisme de groupes.

4. Soit $G = G_1 \times G_2$ un groupe produit. En introduisant, pour $f_1 \in C(G_1)$ et $f_2 \in C(G_2)$, l'application

$$f : \begin{array}{ccc} G & \to & \mathbb{C}^\star \\ (x_1, x_2) & \mapsto & f_1(x_1) f_2(x_2) \end{array},$$

   montrer que $C(G)$ est isomorphe à $C(G_1) \times C(G_2)$.

Exercice 14.30 (****)

Montrer que si f est une bijection de X sur Y, alors $F : \begin{array}{ccc} \mathfrak{S}(X) & \to & \mathfrak{S}(Y) \\ \sigma & \mapsto & f \sigma f^{-1} \end{array}$ est un isomorphisme.

Exercice 14.31

Le but de cet exercice est de montrer que les groupes $(\mathbb{R}^\star, \times)$ et $(\mathbb{C}^\star, \times)$ ne sont pas isomorphes. Supposons qu'il existe un isomorphisme φ de $(\mathbb{R}^\star, \times)$ sur $(\mathbb{C}^\star, \times)$.

1. Montrer que $\varphi(-1) = -1$.

2. Montrer que si $\alpha = \varphi^{-1}(i)$, alors $\alpha^2 = -1$.

3. Conclure.

Exercice 14.32

Soient p, q deux entiers naturels premiers entre eux et $n = pq$. Soit $(G, \cdot)$ un groupe fini commutatif vérifiant $x^n = 1$ pour tout $x \in G$. On forme

$$M = \{ x \in G \mid x^p = 1 \} \quad \text{et} \quad N = \{ x \in G \mid x^q = 1 \}.$$

1. Montrer que M et N sont des sous-groupes de $(G, \cdot)$.

2. Vérifier $M \cap N = \{ 1 \}$.

3. Établir que l'application

$$\begin{array}{rccc} f\ : & M \times N & \to & G \\ & (x, y) & \mapsto & xy \end{array}$$

est un isomorphisme de groupes.

Anneaux, corps

14.3 Anneaux

Exercice 14.33 *Études d'inversibilités dans un anneau*
Soit $(A,+,.)$ un anneau.

1. Soit $a \in A$ tel que $a^2 = 0$. Démontrer que $1-a$ et $1+a$ sont inversibles et expliciter leurs inverses.

2. Généraliser pour $a \in A$ tel qu'il existe $n \in \mathbb{N}^\star$ pour lequel $a^n = 0$.

Exercice 14.34 *Éléments nilpotents*
Soit $(A,+,.)$ un anneau. Un élément x de A est dit **nilpotent** s'il existe $n \in \mathbb{N}^\star$ tel que $x^n = 0$.

1. Démontrer que si xy est nilpotent, alors yx l'est aussi.

2. Démontrer que si x et y sont nilpotents et commutent, alors, xy et $x+y$ sont nilpotents.

Exercice 14.35 *Étude d'un ensemble de fonctions*
Soit A l'ensemble des fonctions définies sur $\mathbb{R}$ telles que $f(0) = f(1)$. Démontrer que A est un anneau.

Exercice 14.36
Soit a un élément d'un ensemble X. Montrer que l'application

$$E_a : \begin{array}{ccc} \mathscr{F}(X,\mathbb{R}) & \to & \mathbb{R} \\ f & \mapsto & f(a) \end{array}$$

est un morphisme d'anneaux.

Exercice 14.37 *Nilradical d'un anneau*
On appelle nilradical d'un anneau commutatif $(A,+,\times)$ l'ensemble N formé des éléments nilpotents de A, c'est-à-dire des $x \in A$ tels qu'il existe $n \in \mathbb{N}^\star$ vérifiant $x^n = 0_A$.
Montrer que N est un idéal de A.

Exercice 14.38 *Radical d'un idéal*
Soit I un idéal d'un anneau commutatif A. On appelle **radical** de l'idéal I l'ensemble $R(I)$ des éléments x de A pour lesquels il existe $q \in \mathbb{N}^\star$ tel que $x^q \in I$.

1. Montrer que $R(I)$ est un idéal de A contenant I.

2. Soient I et J deux idéaux. Vérifier

$$R(I \cap J) = R(I) \cap R(J).$$

3. On suppose que $A = \mathbb{Z}$. Déterminer le radical de $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

14.4 Corps

Exercice 14.39
Montrer que $\mathbb{Q}[i\sqrt{3}] = \left\{ a + bi\sqrt{3} \;\middle|\; (a,b) \in \mathbb{Q}^2 \right\}$ est un corps.

14.5 Algèbres