CHAPITRE N°13
STRUCTURES ALGÉBRIQUES USUELLES

Nous introduisons des notions élémentaires relatives aux groupes, anneaux et corps afin de traiter de manière unifiée un certain nombre de situations.

§ 1. LOI DE COMPOSITION INTERNE

DÉFINITION C13.1 (LOI DE COMPOSITION INTERNE)
Soit E un ensemble. Toute application $*$ de $E \times E$ dans E

$$* \left| \begin{array}{ccc} E \times E & \longrightarrow & E \\ (x,y) & \longmapsto & x * y \end{array} \right.$$

est appelée loi de composition interne sur E.

EXEMPLE C13.2 — L'addition et la multiplication sur $\mathbf{Z}$

$$+ \left| \begin{array}{ccc} \mathbf{Z} \times \mathbf{Z} & \longrightarrow & \mathbf{Z} \\ (x,y) & \longmapsto & x+y \end{array} \right. \qquad \times \left| \begin{array}{ccc} \mathbf{Z} \times \mathbf{Z} & \longrightarrow & \mathbf{Z} \\ (x,y) & \longmapsto & x \times y \end{array} \right.$$

sont deux lois de composition internes sur $\mathbf{Z}$.

EXEMPLE C13.3 — L'exponentiation sur $\mathbf{N}^*$

$$\left| \begin{array}{ccc} \mathbf{N}^* \times \mathbf{N}^* & \longrightarrow & \mathbf{N}^* \\ (x,y) & \longmapsto & x^y \end{array} \right.$$

est une loi de composition interne sur $\mathbf{N}^*$.

EXEMPLE C13.4 — Si E est un ensemble alors les applications

$$\cup \left| \begin{array}{ccc} \mathscr{P}(E) \times \mathscr{P}(E) & \longrightarrow & \mathscr{P}(E) \\ (A,B) & \longmapsto & A \cup B \end{array} \right. \qquad \cap \left| \begin{array}{ccc} \mathscr{P}(E) \times \mathscr{P}(E) & \longrightarrow & \mathscr{P}(E) \\ (A,B) & \longmapsto & A \cap B \end{array} \right.$$

sont des lois de composition internes sur $\mathscr{P}(E)$ et l'application

$$\circ \left| \begin{array}{ccc} \mathscr{F}(E,E) \times \mathscr{F}(E,E) & \longrightarrow & \mathscr{F}(E,E) \\ (f,g) & \longmapsto & f \circ g \end{array} \right.$$

est une loi de composition interne sur $\mathscr{F}(E,E)$.

DÉFINITION C13.5 (ASSOCIATIVITÉ)
Soit E un ensemble muni d'une loi de composition interne $*$. La loi de composition $*$ est dite associative si

$$x * (y * z) = (x * y) * z$$

pour tout triplet $(x,y,z) \in E^3$.

Remarque C13.6 — Si x, y, z sont trois éléments d'un ensemble E muni d'une loi de composition interne $*$ associative on note simplement $x * y * z$ l'élément $x * \big(y * z\big)$ de E qui égale l'élément $\big(x * y\big) * z$ de E. Ôter les parenthèses n'induit aucune ambiguïté.

Exemple C13.7 — L'addition et la multiplication sur $\mathbf{Z}$ sont associatives.

Exemple C13.8 — L'exponentiation sur $\mathbf{N}^*$ n'est pas associative. En effet $2^{(3^2)} = 512$ et $\big(2^3\big)^2 = 64$.

Exemple C13.9 — Si E est un ensemble alors les lois de compositions $\cup$ et $\cap$ sur $\mathscr{P}(E)$ et la loi de composition $\circ$ sur $\mathscr{F}(E,E)$ sont associatives.

Définition C13.10 (commutativité)
Soit E un ensemble muni d'une loi de composition interne $*$. La loi de composition $*$ est dite commutative si

$$x * y = y * x$$

pour tout couple $(x, y) \in E^2$.

Exemple C13.11 — L'addition et la multiplication sur $\mathbf{Z}$ sont commutatives.

Exemple C13.12 — L'exponentiation sur $\mathbf{N}^*$ n'est pas commutative. En effet $2^3 = 8$ et $3^2 = 9$.

Exemple C13.13 — Si E est un ensemble alors les lois de compositions $\cup$ et $\cap$ sur $\mathscr{P}(E)$ sont commutatives.

Exercice C13.14 — Soient E un ensemble possédant au moins trois éléments a, b, c deux-à-deux distincts. Démontrer que la loi de composition $\circ$ sur $\mathscr{F}(E,E)$ n'est pas commutative.

Définition C13.15 (existence d'un élément neutre)
Soit E un ensemble muni d'une loi de composition interne $*$. La loi de composition $*$ possède un élément neutre s'il existe un élément $e \in E$ tel que

$$x * e = x = e * x$$

pour tout $x \in E$.

Proposition C13.16 (unicité de l'élément neutre)
Soit E un ensemble muni d'une loi de composition interne $*$. Si la loi de composition $*$ possède un élément neutre alors celui-ci est unique.

Démonstration — Soient e_1 et e_2 deux éléments neutres pour la loi de composition $*$. Comme e_1 est neutre pour la loi de composition $*$

$$e_1 * e_2 = e_2$$

et comme e_2 est neutre pour la loi de composition $*$

$$e_1 * e_2 = e_1 \,.$$

Ainsi $e_1 = e_2$.

Exemple C13.17 — L'élément 0 est l'élément neutre de l'addition sur $\mathbf{Z}$ et l'élément 1 est l'élément neutre de la multiplication sur $\mathbf{Z}$.

Exemple C13.18 — L'exponentiation sur $\mathbf{N}^*$ ne possède pas d'élément neutre. En effet, si cette loi possédait un élément neutre $e \in \mathbf{N}^*$ alors on aurait

$$2^e = 2 = e^2 .$$

Or 2 n'est le carré d'aucun élément de $\mathbf{N}^*$ (cf. théorème fondamental de l'arithmétique).

Exemple C13.19 — Si E est un ensemble alors $\emptyset$ est l'élément neutre de la loi de composition $\cup$ sur $\mathscr{P}(E)$, E est l'élément neutre de la loi de composition $\cap$ sur $\mathscr{P}(E)$ et id_E est l'élément neutre de la loi de composition $\circ$ sur $\mathscr{F}(E,E)$.

Exercice C13.20 — Démontrer que la division sur $\mathbf{C}^*$

$$\left| \begin{array}{ccc} \mathbf{C}^* \times \mathbf{C}^* & \longrightarrow & \mathbf{C}^* \\ (z_1, z_2) & \longmapsto & \dfrac{z_1}{z_2} \end{array} \right.$$

n'est pas associative et qu'elle ne possède pas d'élément neutre.

Définition C13.21 (inversibilité)
Soit E un ensemble muni d'une loi de composition interne $*$ possédant un élément neutre noté e. Un élément $x \in E$ est dit inversible s'il existe un élément $y \in E$ tel que

$$x * y = e = y * x .$$

Exercice C13.22 — On considère la loi de composition $*$ définie sur $\mathbf{R}$ par

$$* \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ (x,y) & \longmapsto & x \cdot y + \left(x^2 - 1\right) \cdot \left(y^2 - 1\right) \end{array} \right.$$

où $\cdot$ désigne la multiplication usuelle sur $\mathbf{R}$.
1) Démontrer que la loi $*$ est commutative, non associative et qu'elle possède un élément neutre.
2) Démontrer que 2 est inversible pour la loi $*$ et déterminer tous les éléments $y \in \mathbf{R}$ tels $2 * y = 2 = y * 2$.

Proposition-Définition C13.23 (inverse d'un élément inversible)
Soit E un ensemble muni d'une loi de composition interne $*$ associative et possédant un élément neutre noté e. Si un élément $x \in E$ est inversible alors il existe un unique élément $y \in E$ tel que

$$x * y = e = y * x .$$

Cet élément y est appelé inverse de E et est noté x^{-1}.

Démonstration — L'existence de l'élément y de E tel que $x * y = e = y * x$ est assurée par l'inversibilité de x. Soient y_1 et y_2 deux éléments de x tels que $x * y_1 = e = y_1 * x$ et $x * y_2 = e = y_2 * x$. Alors :

$$\left(y_1 * x\right) * y_2 = e * y_2 = y_2 \qquad \text{et} \qquad y_1 * \left(x * y_2\right) = y_1 * e = y_1 .$$

Comme la loi de composition $*$ est associative, nous en déduisons $y_1 = y_2$.

Remarque C13.24 — Lorsque la loi de composition est notée additivement $(+)$:
1) on ne parle pas de l'inverse d'un élément mais de son opposé ;
2) l'opposé d'un élément x est noté $-x$ et non pas x^{-1}.

Exemple C13.25 — Si $\mathbf{Z}$ est muni de la loi de composition interne donnée par l'addition, d'élément neutre 0, alors tout élément de $\mathbf{Z}$ possède un opposé.

Exemple C13.26 — Si $\mathbf{Z}$ est muni de la loi de composition interne donnée par la multiplication, d'élément neutre 1, alors seul 1 est inversible et $1^{-1} = 1$.

Exemple C13.27 — Si $\mathbf{C}$ est muni de la loi de composition interne donnée par la multiplication, d'élément neutre 1, alors un nombre complexe est inversible si et seulement s'il est non nul. De plus, si $a + ib$ (a, b réels) est non nul alors :

$$(a+ib)^{-1} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}\,.$$

Exemple C13.28 — Si E est un ensemble non vide et $\mathscr{F}(E,E)$ est muni de la loi de composition $\circ$, d'élément neutre id_E, alors une application de E dans E est inversible si et seulement si elle est bijective. De plus, si $f \in \mathscr{F}(E,E)$ est bijective alors f^{-1} est son application réciproque définie par

$$f^{-1} \left| \begin{array}{ccc} E & \longrightarrow & E \\ y & \longmapsto & \text{l'unique élément } x \in E \text{ tel que } f(x) = y. \end{array} \right.$$

Exercice C13.29 — Soit E un ensemble.
1) On munit $\mathscr{P}(E)$ de la loi de composition $\cup$. Déterminer les éléments $A \in \mathscr{P}(E)$ inversibles.
2) Même question si $\mathscr{P}(E)$ de la loi de composition $\cap$.

Exercice C13.30 — Soit E un ensemble muni d'une loi de composition interne $*$ associative, commutative et possédant un élément neutre noté e. À tout élément $x \in E$, on associe l'application « translation par x » définie par

$$\tau_x \left| \begin{array}{ccc} E & \longrightarrow & E \\ y & \longmapsto & x * y\,. \end{array} \right.$$

Démontrer que, pour tout $x \in E$, x est inversible si et seulement si l'application τ_x est bijective.

Exercice C13.31 — On considère l'ensemble $\mathscr{F}(\mathbf{N},\mathbf{N})$ muni de la loi de composition $\circ$, d'élément neutre $\mathrm{id}_{\mathbf{N}}$. Soit l'application f définie par :

$$f \left| \begin{array}{ccc} \mathbf{N} & \longrightarrow & \mathbf{N} \\ n & \longmapsto & n+1\,. \end{array} \right.$$

1) Construire une application $g : \mathbf{N} \longrightarrow \mathbf{N}$ tel que $g \circ f = \mathrm{id}_{\mathbf{N}}$.
2) L'application f est-elle inversible ?

PROPOSITION C13.32 (PROPRIÉTÉS DES ÉLÉMENTS INVERSIBLES)
Soit E un ensemble muni d'une loi de composition interne $*$ associative et possédant un élément neutre noté e.
1) L'élément e est inversible et $e^{-1} = e$.
2) Pour tout élément $x \in E$ inversible, x^{-1} est inversible et $\left(x^{-1}\right)^{-1} = x$.
3) Pour tout couple $(x, y) \in E^2$ d'éléments inversibles, $x * y$ est inversible et $(x * y)^{-1} = y^{-1} * x^{-1}$.

Démonstration — 1) L'assertion résulte de $e * e = e$.
2) Soit $x \in E$ inversible. Comme

$$x * x^{-1} = e = x^{-1} * x$$

l'élément x^{-1} de E est inversible et son inverse est x.
3) Soient x et y des éléments inversibles de E. Comme

$$(x * y) * \left(y^{-1} * x^{-1}\right) = x * \left(y * y^{-1}\right) * x^{-1} = x * e * x^{-1} = x * x^{-1} = e$$

et

$$\left(y^{-1} * x^{-1}\right) * (x * y) = y^{-1} * \left(x^{-1} * x\right) * y = y^{-1} * e * y = y^{-1} * y = e$$

l'élément $x * y$ de E est inversible et son inverse est $y^{-1} * x^{-1}$.

EXERCICE C13.33 — Soit E un ensemble muni d'une loi de composition interne $*$ associative, commutative et possédant un élément neutre noté e. Soit (x, y) un couple d'éléments de E tels que x et $z := x * y$ sont inversibles. Démontrer que y est inversible et exprimer y^{-1} à l'aide de x^{-1} et z^{-1}.

EXERCICE C13.34 — Soit E un ensemble muni d'une loi de composition interne $*$ associative et possédant un élément neutre e. Soit x un élément inversible de E. Démontrer que l'application

$$f \left| \begin{array}{ccc} E & \longrightarrow & E \\ y & \longmapsto & x * y * x^{-1} \end{array} \right.$$

est bijective et expliciter son application réciproque.

DÉFINITION C13.35 (PARTIE STABLE)
Soit E un ensemble muni d'une loi de composition interne $*$. Une partie A de E est dite stable pour la loi $*$ si, pour tout couple $(a_1, a_2) \in A^2$

$$a_1 * a_2 \in A\,.$$

EXEMPLE C13.36 — Si $\mathbf{Z}$ est muni de la loi de composition $+$ et si $a \in \mathbf{Z}$, alors la partie

$$a\mathbf{Z} := \{na \,:\, n \in \mathbf{Z}\}$$

formée des multiples de a est stable pour la loi $+$. En effet, soient x_1 et x_2 deux éléments de $a\mathbf{Z}$. Alors il existe des entiers n_1 et n_2 tels que $x_1 = an_1$ et $x_2 = an_2$. Ainsi

$$x_1 + x_2 = a(n_1 + n_2)$$

et comme $n_1 + n_2 \in \mathbf{Z}$, $x_1 + x_2 \in a\mathbf{Z}$.

Exemple C13.37 — Si $\mathbf{C}$ est muni de la loi de composition interne $\times$, alors

$$\mathbf{U} := \{z \in \mathbf{C} \,:\, |z| = 1\}$$

est stable pour la loi $\times$. En effet, si z_1 et z_2 sont deux éléments de $\mathbf{U}$ alors, comme le module est multiplicatif

$$|z_1 \times z_2| = |z_1| \times |z_2| = 1 \times 1 = 1$$

et donc $z_1 \times z_2 \in \mathbf{U}$.

Exemple C13.38 — On considère $\mathscr{F}(\mathbf{R},\mathbf{R})$ muni de la loi de composition $\circ$ et les parties

$$A := \left\{f \in \mathscr{F}(\mathbf{R},\mathbf{R}) \,:\, f \text{ est croissante}\right\} \qquad \text{et} \qquad B := \left\{f \in \mathscr{F}(\mathbf{R},\mathbf{R}) \,:\, f \text{ est décroissante}\right\}.$$

Comme une composée d'applications croissantes est croissante, A est stable pour la loi $\circ$. L'application

$$f \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & -x \end{array} \right.$$

est décroissante mais $f \circ f = \mathrm{id}_{\mathbf{R}}$ n'est pas décroissante. Ainsi B n'est pas stable pour la loi $\circ$.

Exemple C13.39 — Soient E un ensemble et A une partie de E. La partie $\left\{\emptyset, A, \overline{A}, E\right\}$ de $\mathscr{P}(E)$ est stable pour les lois de composition $\cup$ et $\cap$.

Exercice C13.40 — On munit $\mathscr{F}(\mathbf{R},\mathbf{R})$ de la loi de composition $\circ$. Démontrer que l'ensemble des fonctions affines

$$A := \left\{ f_{a,b} \left| \begin{array}{ccc} \mathbf{R} & \longrightarrow & \mathbf{R} \\ x & \longmapsto & ax+b \end{array} \right. \,:\, (a,b) \in \mathbf{R}^2 \right\}$$

est stable pour la loi $\circ$.

Proposition C13.41 (intersection de parties stables)
Soient E un ensemble muni d'une loi de composition interne $*$ et $(A_i)_{i\in I}$ une famille de parties stables pour la loi $*$. Alors

$$\bigcap_{i\in I} A_i = \{x \in E \,:\, \forall\, i \in I \quad x \in A_i\}$$

est stable pour la loi de composition.

Démonstration — Considérons deux éléments x_1 et x_2 de $\bigcap_{i\in I} A_i$. Soit $i \in I$. Comme $x_1 \in A_i$, $x_2 \in A_i$ et A_i est stable pour la loi $*$, $x_1 * x_2 \in A_i$. Cette appartenance valant pour un élément i de I quelconque, il vient $x_1 * x_2 \in \bigcap_{i\in I} A_i$.

Remarque C13.42 — Une réunion de parties stables n'est pas nécessairement stable. En effet, considérons $\mathbf{Z}$ muni de l'addition $+$. Les parties $2\mathbf{Z} := \{2n \,:\, n \in \mathbf{Z}\}$ et $3\mathbf{Z} := \{3n \,:\, n \in \mathbf{Z}\}$ sont stables pour la loi $+$ mais la partie $A := 2\mathbf{Z} \cup 3\mathbf{Z}$ formée des entiers multiples de 2 ou 3 n'est pas stable pour la loi $+$. En effet, 2 et 3 appartiennent à A, mais pas $2+3=5$.

Exercice C13.43 — On munit $\mathbf{C}$ de la loi de composition interne $\times$.
1) Démontrer que pour tout $n \in \mathbf{N}^*$, l'ensemble $\mathbf{U}_n$ des racines n-ièmes de l'unité complexes est stable pour la loi $\times$.
2) Démontrer que $\mathbf{U}_\infty := \bigcup_{n\in\mathbf{N}^*} \mathbf{U}_n$ est également stable pour la loi $\times$.

§ 2. Groupes

Définition C13.44 (groupe)
Un groupe est un couple $(G, *)$ où G est un ensemble et $*$ est une loi de composition sur G telle que
1) la loi $*$ est associative ;
2) la loi $*$ possède un élément neutre (noté e_G) ;
3) tout élément de G est inversible.
Si en outre la loi $*$ est commutative, on dit que le groupe $(G, *)$ est commutatif ou abélien.

Exemple C13.45 — Sont des groupes abéliens $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$, $(\mathbf{C}, +)$, $(\mathbf{Q}^*, \times)$, $\left(\mathbf{Q}_+^*, \times\right)$, $(\mathbf{R}^*, \times)$, $\left(\mathbf{R}_+^*, \times\right)$, $(\mathbf{C}^*, \times)$, $(\mathbf{U}, \times)$, $(\mathbf{U}_n, \times)$, où $n \in \mathbf{N}^*$.

Exemple C13.46 — On munit $\mathbf{N}$ de la loi de composition $+$. La loi $+$ est associative, possède un élément neutre (0) mais $(\mathbf{N}, +)$ n'est pas un groupe. En effet, 1 ne possède pas d'opposé dans $\mathbf{N}$.

Exemple C13.47 — On munit $\mathbf{Z} \setminus \{0\}$ de la loi de composition $\times$. La loi $\times$ est associative, possède un élément neutre (1) mais $(\mathbf{Z} \setminus \{0\}, \times)$ n'est pas un groupe. En effet, 2 ne possède pas d'inverse dans $\mathbf{Z} \setminus \{0\}$.

Exercice C13.48 — Nous définissons deux lois de compositions internes $+$ et $\times$ sur $\mathbf{R}^\mathbf{N}$ par

$$+ \left| \begin{array}{ccc} \mathbf{R}^\mathbf{N} \times \mathbf{R}^\mathbf{N} & \longrightarrow & \mathbf{R}^\mathbf{N} \\ ((a_n)_{n\in\mathbf{N}}, (b_n)_{n\in\mathbf{N}}) & \longmapsto & (a_n + b_n)_{n\in\mathbf{N}} \end{array} \right. \quad \text{et} \quad \times \left| \begin{array}{ccc} \mathbf{R}^\mathbf{N} \times \mathbf{R}^\mathbf{N} & \longrightarrow & \mathbf{R}^\mathbf{N} \\ ((a_n)_{n\in\mathbf{N}}, (b_n)_{n\in\mathbf{N}}) & \longmapsto & (a_n \times b_n)_{n\in\mathbf{N}}. \end{array} \right.$$

1) Démontrer que $\left(\mathbf{R}^\mathbf{N}, +\right)$ est un groupe abélien.
2) Démontrer que la loi $\times$ est associative, qu'elle possède un élément neutre, puis que $\left(\mathbf{R}^\mathbf{N}, \times\right)$ n'est pas un groupe.

Exercice C13.49 — Soit $(G, *)$ un groupe à trois éléments e_G, x, y. Compléter la table suivante.

$*$	e_G	x	y
e_G	$e_G * e_G =$	$e_G * x =$	$e_G * y =$
x	$x * e_G =$	$x * x =$	$x * y =$
y	$y * e_G =$	$y * x =$	$y * y =$

Exercice C13.50 — Démontrer qu'il n'existe que deux tables possibles pour un groupe à quatre éléments.

Notation C13.51 — Soit $(G,*)$ un groupe dont la loi est notée multiplicativement. Pour tout $x \in G$ et pour tout $n \in \mathbf{Z}$, on définit l'élément x^n par

$$x^n := \begin{cases} \overbrace{x * x * \ldots * x}^{n \text{ termes}} & \text{si } n \geqslant 1 ; \\ e_G & \text{si } n = 0 ; \\ \underbrace{x^{-1} * x^{-1} * \ldots * x^{-1}}_{-n \text{ termes}} & \text{si } n \leqslant -1. \end{cases}$$

Notation C13.52 — Soit $(G,+)$ un groupe dont la loi est notée additivement. Pour tout $x \in G$ et pour tout $n \in \mathbf{Z}$, on définit l'élément nx par

$$nx := \begin{cases} \overbrace{x + x + \ldots + x}^{n \text{ termes}} & \text{si } n \geqslant 1 ; \\ e_G & \text{si } n = 0 ; \\ \underbrace{(-x) + (-x) + \ldots + (-x)}_{-n \text{ termes}} & \text{si } n \leqslant -1. \end{cases}$$

Proposition C13.53 (propriétés de la notation puissance)
Soit $(G,\times)$ un groupe dont la loi est notée multiplicativement.
1) Pour tout triplet $(x,n,m) \in G \times \mathbf{Z} \times \mathbf{Z}$

$$x^n * x^m = x^{n+m} \qquad \text{et} \qquad \left(x^n\right)^m = x^{nm}.$$

2) Si la loi $*$ est de plus commutative alors pour tout triplet $(x,y,n) \in G \times G \times \mathbf{Z}$

$$x^n * y^n = (x * y)^n.$$

Proposition-Définition C13.54 (groupe des permutations d'un ensemble)
Soit E un ensemble.
1) L'ensemble

$$S_E := \left\{ f \in \mathscr{F}(E,E) \,:\, f \text{ est bijective} \right\}$$

est appelé ensemble des permutations de E.
2) L'application

$$\circ \left| \begin{array}{ccc} S_E \times S_E & \longrightarrow & S_E \\ (f,g) & \longmapsto & f \circ g \end{array} \right.$$

est bien définie.
3) La loi $\circ$ sur S_E est associative.
4) La loi $\circ$ possède un élément neutre, id_E.
5) Tout élément $f \in S_E$ est inversible pour la loi $\circ$ et son inverse est son application réciproque

$$f^{-1} \left| \begin{array}{ccc} E & \longrightarrow & E \\ y & \longmapsto & \text{l'unique élément } x \in E \text{ tel que } f(x) = y. \end{array} \right.$$

Notation C13.55 — Si $n \in \mathbf{N}^*$, on note simplement S_n l'ensemble $S_{[\![1,n]\!]}$ des bijections de l'ensemble $[\![1,n]\!]$ dans lui-même.

Remarque C13.56 — Si $n \in \mathbf{N}^*$, alors S_n possède $n!$ éléments. En effet pour construire une bijection f de $[\![1,n]\!]$ dans lui-même
- l'image $f(1)$ de 1 par f doit être choisie dans $[\![1,n]\!]$, d'où n choix;
- l'image $f(2)$ de 2 par f doit être choisie dans $[\![1,n]\!] \setminus \{f(1)\}$ pour que f pour que f soit injective, d'où $n-1$ choix;
- ...
- l'image $f(n)$ de n par f doit être choisie dans $[\![1,n]\!] \setminus \{f(1), f(2), \dots, f(n-1)\}$ pour que f soit injective (elle sera alors également surjective), d'où 1 choix.

Au final, on dispose de $n \times (n-1) \times \dots \times 1 = n!$ choix pour construire une bijection de $[\![1,n]\!]$ dans lui-même.

Exemple C13.57 — L'ensemble $S_2 := \{f \in [\![1,2]\!]^{[\![1,2]\!]} : f \text{ est bijective}\}$ possède $2! = 2$ éléments

$$\mathrm{id}_{[\![1,2]\!]} := \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \tau_{1,2} := \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

et la table du groupe $(S_2, \circ)$ est la suivante.

$\circ$	$\mathrm{id}_{[\![1,2]\!]}$	$\tau_{1,2}$
$\mathrm{id}_{[\![1,2]\!]}$	$\mathrm{id}_{[\![1,2]\!]} \circ \mathrm{id}_{[\![1,2]\!]} = \mathrm{id}_{[\![1,2]\!]}$	$\mathrm{id}_{[\![1,2]\!]} \circ \tau_{1,2} = \tau_{1,2}$
$\tau_{1,2}$	$\tau_{1,2} \circ \mathrm{id}_{[\![1,2]\!]} = \tau_{1,2}$	$\tau_{1,2} \circ \tau_{1,2} = \mathrm{id}_{[\![1,2]\!]}$

Exercice C13.58 — L'ensemble $S_3 := \{f \in [\![1,3]\!]^{[\![1,3]\!]} : f \text{ est bijective}\}$ possède $3! = 6$ éléments listés ci-dessous.

$$\mathrm{id}_{[\![1,3]\!]} := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \tau_{1,2} := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \tau_{1,3} := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\tau_{2,3} := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad c_1 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad c_2 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Construire la table du groupe $(S_3, \circ)$.

Remarque C13.59 — Si E est un ensemble possédant au moins trois éléments a, b, c distincts alors le groupe $(S_E, \circ)$ n'est pas abélien. En effet, les deux bijections dans E dans E suivantes

$$\tau_{a,b} \left| \begin{array}{ccc} E & \longrightarrow & E \\ a & \longmapsto & b \\ b & \longmapsto & a \\ x & \longmapsto & x \text{ si } x \notin \{a,b\} \end{array} \right. \qquad \tau_{b,c} \left| \begin{array}{ccc} E & \longrightarrow & E \\ b & \longmapsto & c \\ c & \longmapsto & b \\ x & \longmapsto & x \text{ si } x \notin \{b,c\} \end{array} \right.$$

ne commutent pas puisque $\tau_{a,b} \circ \tau_{b,c}(b) = c$ et $\tau_{b,c} \circ \tau_{a,b}(b) = a$.

PROPOSITION-DÉFINITION C13.60 (PRODUIT DE DEUX GROUPES)
Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes.
1) L'application
$$* \left| \begin{array}{ccc} (G_1 \times G_2) \times (G_1 \times G_2) & \longrightarrow & (G_1 \times G_2) \\ ((x_1, x_2), (y_1, y_2)) & \longmapsto & (x_1 *_1 y_1, x_2 *_2 y_2) \end{array} \right.$$
définit une loi de composition interne sur $G_1 \times G_2$.
2) $(G_1 \times G_2, *)$ est un groupe, appelé produit des groupes $(G_1, *_1)$ et $(G_2, *_2)$.
3) L'élément neutre du groupe $(G_1 \times G_2, *)$ est (e_{G_1}, e_{G_2}).
4) Si $(x_1, x_2) \in G_1 \times G_2$ alors l'inverse de (x_1, x_2) pour la loi $*$ est $\left(x_1^{-1}, x_2^{-1}\right)$ où x_1^{-1} (resp. x_2^{-1}) désigne l'inverse de x_1 (resp. x_2) pour la loi $*_1$ (resp. $*_2$).

REMARQUE C13.61 — La notion de produit de groupes, présentée ci-dessus pour deux groupes, se généralise à une famille quelconque $((G_i, *_i))_{i \in I}$ de groupes ($I \neq \emptyset$). L'application
$$* \left| \begin{array}{ccc} \left(\prod_{i \in I} G_i\right) \times \left(\prod_{i \in I} G_i\right) & \longrightarrow & \prod_{i \in I} G_i \\ \left((x_i)_{i \in I}, (y_i)_{i \in I}\right) & \longmapsto & (x_i *_i y_i)_{i \in I} \end{array} \right.$$
définit une loi de composition interne sur $\prod_{i \in I} G_i$ et $\left(\prod_{i \in I} G_i, *\right)$ est un groupe, appelé groupe produit de la famille de groupes $((G_i, *_i))_{i \in I}$. L'élément neutre du groupe $\left(\prod_{i \in I} G_i, *\right)$ est $\left(e_{G_i}\right)_{i \in I}$ et l'inverse d'un élément $(x_i)_{i \in I} \in \left(\prod_{i \in I} G_i, *\right)$ est $\left(x_i^{-1}\right)_{i \in I}$.

EXERCICE C13.62 — Soit $(p, q) \in \mathbf{N}^* \times \mathbf{N}^*$. On considère les deux groupes $\left(\mathbf{U}_p, \times\right)$, $\left(\mathbf{U}_q, \times\right)$ et leur groupe produit $\left(\mathbf{U}_p \times \mathbf{U}_q, \times\right)$.
1) Préciser le neutre e du groupe $\left(\mathbf{U}_p \times \mathbf{U}_q, \times\right)$.
2) Donner un entier naturel non nul n tel que, pour tout $(z_1, z_2) \in \mathbf{U}_p \times \mathbf{U}_q$, $(z_1, z_2)^n = e$.
3) Soit $n \in \mathbf{N}^*$ tel que, pour tout $(z_1, z_2) \in \mathbf{U}_p \times \mathbf{U}_q$, $(z_1, z_2)^n = e$. Démontrer que $p \vee q$ divise n.

§ 3. SOUS-GROUPES

DÉFINITION C13.63 (SOUS-GROUPE)
Soit $(G, *)$ un groupe. Une partie H de G est appelée sous-groupe de $(G, *)$ si
1) $e_G \in H$ (H contient l'élément neutre de G) ;
2) pour tout couple $(h_1, h_2) \in H^2$, $h_1 * h_2 \in H$ (H est stable pour la loi $*$) ;
3) pour tout $h \in H$, $h^{-1} \in H$ (H est stable par passage à l'inverse).

EXEMPLE C13.64 — Si $(G, *)$ est un groupe, alors $\{e_G\}$ et G sont des sous-groupes de G.

EXEMPLE C13.65 — $(\mathbf{Z}, +)$ est un sous-groupe de $(\mathbf{R}, +)$.

Exemple C13.66 — $(\mathbf{U},\times)$ est un sous-groupe de $(\mathbf{C}^*,\times)$.

Exemple C13.67 — Pour tout $n\in\mathbf{N}^*$, $(\mathbf{U}_n,\times)$ est un sous-groupe de $(\mathbf{U},\times)$.

Remarque C13.68 — Soit $(G,*)$ est un groupe et H un sous-groupe de $(G,*)$. Comme H est stable par la loi $*$, l'application

$$*_H \left| \begin{array}{ccc} H\times H & \longrightarrow & H \\ (h_1,h_2) & \longmapsto & h_1*h_2 \end{array} \right.$$

est bien définie et $(H,*_H)$ est un groupe.

Proposition C13.69 (caractérisation des sous-groupes)
Soit $(G,*)$ un groupe. Une partie H de G est un sous-groupe si et seulement si
a) $H\neq\emptyset$ (H est non vide) ;
b) pour tout couple $(h_1,h_2)\in H^2$, $h_1*h_2^{-1}\in H$ (H est stable par produit tordu).

Démonstration — Supposons que les propriétés 1,2,3 soient vérifiés.
a) D'après 1, $e_G\in H$ donc $H\neq\emptyset$.
b) Soit un couple $(h_1,h_2)\in H^2$. D'après 3, $h_2^{-1}\in H$. Alors 2 livre $h_1*h_2^{-1}\in H$.
Supposons que les propriétés a,b soient vérifiés.
1) D'après a, H contient un élément h. La propriété b livre alors $e_G=h*h^{-1}\in H$.
3) Soit $h\in H$. D'après 1 et b, $h^{-1}=e_G*h^{-1}\in H$.
2) Soit un couple $(h_1,h_2)\in H^2$. D'après 3, h_2^{-1}. La propriété b livre alors $h_1*h_2=h_1*\left(h_2^{-1}\right)^{-1}\in H$.

Remarque C13.70 — Lorsque la loi du groupe G est notée additivement $(+)$, alors la Proposition C13.69 se reformule comme suit. Une partie H de G est un sous-groupe de $(G,+)$ si
a) $H\neq\emptyset$ (H est non vide) ;
b) pour tout couple $(h_1,h_2)\in H^2$, $h_1-h_2\in H$ (H est stable par somme tordue).

Exemple C13.71 — Soit $a\in\mathbf{Z}$. Alors l'ensemble

$$a\mathbf{Z}:=\{an\ :\ n\in\mathbf{Z}\}$$

des multiples de a est un sous-groupe de $(\mathbf{Z},+)$. En effet, $0\in a\mathbf{Z}$ et si $(h_1,h_2)\in a\mathbf{Z}\times a\mathbf{Z}$ alors il existe $(n_1,n_2)\in\mathbf{Z}^2$ tel que $h_1=an_1$ et $h_2=an_2$, d'où :

$$h_1-h_2=an_1-an_2=a(n_1-n_2)\,.$$

Comme $n_1-n_2\in\mathbf{Z}$, $h_1-h_2\in a\mathbf{Z}$.

Exercice C13.72 — Soit H un sous-groupe de $(\mathbf{Z},+)$ distinct du sous-groupe trivial $\{0\}$.
1) Justifier que $H\cap\mathbf{N}^*$ est non vide.
2) D'après la propriété de bon ordre, l'élément $a:=\min(H\cap\mathbf{N}^*)$ est bien défini. Démontrer $H=a\mathbf{Z}$.

Exercice C13.73 — Soient $(G,*)$ un groupe et g un élément de G. On définit la partie $< g >$ de G par

$$< g >= \left\{g^n \,:\, n \in \mathbf{Z}\right\} .$$

1) Démontrer que $< g >$ est un sous-groupe de $(G,*)$.
2) Démontrer que $< g >$ est le plus petit sous-groupe de $(G,*)$ qui contient g (au sens de l'inclusion).

Exercice C13.74 — On considère le plan euclidien $\mathscr{P}$ usuel et un triangle équilatéral ABC (non réduit à un point). On considère l'ensemble des isométries du triangle ABC défini par

$$\text{Isom}(ABC) = \left\{f \in S_{\mathscr{P}} \,:\, \forall\,(M_1,M_2) \in \mathscr{P}^2 \quad f(M_1)f(M_2) = M_1M_2 \quad \text{et} \quad f(ABC) = ABC\right\} .$$

Démontrer que $\text{Isom}(ABC)$ est un sous-groupe de $(S_{\mathscr{P}},\circ)$ possédant 6 éléments, dresser sa table et la comparer à celle de $(S_3,\circ)$.

Proposition C13.75 (intersection de sous-groupes)
Soient $(G,*)$ un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de $(G,*)$. Alors

$$\bigcap_{i\in I} H_i = \left\{g \in G \,:\, \forall\, i \in I \quad g \in H_i\right\}$$

est un sous-groupe de $(G,*)$.

Exercice C13.76 — Soient $(G,*)$ un groupe et H_1, H_2 deux sous-groupes de $(G,*)$. Démontrer que $H_1 \cup H_2$ est un sous-groupe de $(G,*)$ si et seulement si $H_1 \subset H_2$ ou $H_2 \subset H_1$.

§ 4. Morphismes de groupes

Définition C13.77 (morphisme de groupes)
Soient $(G_1,*_1)$ et $(G_2,*_2)$ deux groupes. Un morphisme de groupes de $(G_1,*_1)$ dans $(G_2,*_2)$ est une application $f : G_1 \longrightarrow G_2$ telle que

$$f\left(x_1 *_1 y_1\right) = f(x_1) *_2 f(y_1)$$

pour tout couple $(x_1,y_1) \in G_1^2$.

Exemple C13.78 — Si $(G,*)$ est un groupe alors id_G est un morphisme de groupes.

Exemple C13.79 — L'application

$$f \left|\begin{array}{ccc} (\mathbf{R},+) & \longrightarrow & (\mathbf{U},\times) \\ \theta & \longmapsto & e^{i\theta} \end{array}\right.$$

est un morphisme de groupes. En effet, pour tout $(\theta_1,\theta_2) \in \mathbf{R}^2$

$$f(\theta_1+\theta_2) = e^{i(\theta_1+\theta_2)} = e^{i\theta_1} \times e^{i\theta_2} = f(\theta_1) \times f(\theta_2) .$$

Exemple C13.80 — Soit $a \in \mathbf{Z}$. L'application

$$f \left| \begin{array}{ccc} (\mathbf{Z},+) & \longrightarrow & (\mathbf{Z},+) \\ n & \longmapsto & an \end{array} \right.$$

est un morphisme de groupes. En effet, pour tout $(n_1,n_2) \in \mathbf{Z}^2$

$$f(n_1+n_2) = a(n_1+n_2) = an_1 + an_2 = f(n_1) + f(n_2)\,.$$

Exemple C13.81 — L'application

$$f \left| \begin{array}{ccc} (S_3,\circ) & \longrightarrow & (S_3,\circ) \\ \sigma & \longmapsto & \sigma^2 \end{array} \right.$$

n'est pas un morphisme de groupes. En effet

$$\tau_{1,2}\circ\tau_{2,3} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \text{et} \qquad f(\tau_{1,2}\circ\tau_{2,3}) = \left(\tau_{1,2}\circ\tau_{2,3}\right)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

alors que $f(\tau_{1,2})\circ f(\tau_{2,3}) = \tau_{1,2}^2 \circ \tau_{2,3}^2 = \mathrm{id}_{[\![1,3]\!]} \circ \mathrm{id}_{[\![1,3]\!]} = \mathrm{id}_{[\![1,3]\!]}$.

Proposition C13.82 (composée de deux morphismes de groupes)
Si $f : (G_1,*_1) \longrightarrow (G_2,*_2)$ et $f : (G_2,*_2) \longrightarrow (G_3,*_3)$ sont des morphismes de groupes alors

$$g\circ f \left| \begin{array}{ccc} (G_1,*_1) & \longrightarrow & (G_3,*_3) \\ x & \longmapsto & g(f(x)) \end{array} \right.$$

est un morphisme de groupes.

Proposition C13.83 (propriétés d'un morphisme de groupes)
Soit $f : (G_1,*_1) \longrightarrow (G_2,*_2)$ un morphisme de groupes.
1) $f(e_{G_1}) = e_{G_2}$
2) Pour tout $x \in G_1$, $f\left(x^{-1}\right) = f(x)^{-1}$.
3) Pour tout couple $(x,n) \in G_1 \times \mathbf{Z}$, $f\left(x^n\right) = f(x)^n$.

Exemple C13.84 — Si $f : (\mathbf{Z},+) \longrightarrow (G,*)$ est un morphisme de groupes alors, pour tout $n \in \mathbf{Z}$, $f(n) = f(1)^n$.

Exercice C13.85 — Soit $f : (\mathbf{Q},+) \longrightarrow (\mathbf{R}^*,\times)$ un morphisme de groupes. Démontrer que $f(1) > 0$ puis que, pour tout $r \in \mathbf{Q}$, $f(r) = f(1)^r$.

Exercice C13.86 — Soient $n \in \mathbf{N}$ et $f : (\mathbf{U}_{2n+1},\times) \longrightarrow (\mathbf{R}^*,\times)$ un morphisme de groupes. Démontrer que, pour tout $\zeta \in \mathbf{U}_{2n+1}$, $f(\zeta) = 1$.

Exercice C13.87 — Soient a,b des entiers naturels premiers entre eux et $f : (\mathbf{U}_a,\times) \longrightarrow (\mathbf{U}_b,\times)$ un morphisme de groupes. Démontrer que, pour tout $\zeta \in \mathbf{U}_a$, $f(\zeta) = 1$.

PROPOSITION C13.88 (IMAGE ET IMAGE RÉCIPROQUE D'UN SOUS-GROUPE PAR UN MORPHISME)
Soit $f : (G_1, *_1) \longrightarrow (G_2, *_2)$ un morphisme de groupes.
1) Si H_1 est un sous-groupe de $(G_1, *_1)$ alors $f(H_1) := \{f(h_1) \,:\, h_1 \in H_1\}$ est un sous-groupe de $(G_2, *_2)$.
2) Si H_2 est un sous-groupe de $(G_2, *_2)$ alors $f^{-1}(H_2) := \{h_1 \in H_1 \,:\, f(h_1) \in H_2\}$ est un sous-groupe de $(G_1, *_1)$.

DÉFINITION C13.89 (NOYAU ET IMAGE D'UN MORPHISME DE GROUPES)
Soit $f : (G_1, *_1) \longrightarrow (G_2, *_2)$ un morphisme de groupes.
1) Le noyau de f, noté $\mathrm{Ker}(f)$, est le sous-groupe de $(G_1, *_1)$ défini par

$$\mathrm{Ker}(f) := \{x \in G_1 \,:\, f(x) = e_{G_2}\} = f^{-1}(\{e_{G_2}\}).$$

2) L'image de f, noté $\mathrm{Im}(f)$, est le sous-groupe de $(G_2, *_2)$ défini par

$$\mathrm{Im}(f) := \{f(x) \,:\, x \in G_1\} = f(G_1).$$

EXEMPLE C13.90 — Le noyau du morphisme de groupes

$$f \left| \begin{array}{ccc} (\mathbf{R}, +) & \longrightarrow & (\mathbf{U}, \times) \\ \theta & \longmapsto & e^{i\theta} \end{array} \right.$$

est $2\pi\mathbf{Z} := \{2k\pi \,:\, k \in \mathbf{Z}\}$ et son image est $\mathbf{U}$ (f est donc surjective).

EXERCICE C13.91 — Soient a, b des entiers naturels premiers entre eux et l'application

$$f \left| \begin{array}{ccc} \mathbf{Z}^2 & \longrightarrow & \mathbf{Z} \\ (u, v) & \longmapsto & au + bv. \end{array} \right.$$

1) Démontrer que f est un morphisme du groupe $(\mathbf{Z}, +) \times (\mathbf{Z}, +)$ dans $(\mathbf{Z}, +)$.
2) Déterminer le noyau et l'image de f.

PROPOSITION C13.92 (CRITÈRE D'INJECTIVITÉ POUR UN MORPHISME DE GROUPES)
Un morphisme de groupes $f : (G_1, *_1) \longrightarrow (G_2, *_2)$ est injective si et seulement si $\mathrm{Ker}(f) = \{e_{G_1}\}$.

DÉFINITION C13.93 (ISOMORPHISME DE GROUPES)
Un morphisme de groupes $f : (G_1, *_1) \longrightarrow (G_2, *_2)$ bijectif est appelé isomorphisme de groupes.

EXEMPLE C13.94 — Démontrer que

$$f_1 \left| \begin{array}{ccc} (\mathbf{Z}, +) & \longrightarrow & (\mathbf{Z}, +) \\ n & \longmapsto & n \end{array} \right. \quad \text{et} \quad f_{-1} \left| \begin{array}{ccc} (\mathbf{Z}, +) & \longrightarrow & (\mathbf{Z}, +) \\ n & \longmapsto & -n \end{array} \right.$$

sont les seuls isomorphismes de groupes de $(\mathbf{Z}, +)$ dans lui-même. Tout d'abord, f_1 et f_{-1} sont des morphismes de groupes bijectifs ($f_1 = \mathrm{id}_{\mathbf{Z}}$ et $f_{-1} \circ f_{-1} = \mathrm{id}_{\mathbf{Z}}$). Ensuite, si $f : (\mathbf{Z}, +) \longrightarrow (\mathbf{Z}, +)$ est un isomorphisme de groupes et $a := f(1)$ alors f coïncide avec l'application

$$f_a \left| \begin{array}{ccc} (\mathbf{Z}, +) & \longrightarrow & (\mathbf{Z}, +) \\ n & \longmapsto & an \end{array} \right.$$

et, puisque $1 \in f_a(\mathbf{Z})$, a divise 1 et donc $a \in \{-1, 1\}$.

Exercice C13.95 — Les groupes $(\mathbf{U}_2,\times)\times(\mathbf{U}_2,\times)$ et $(\mathbf{U}_4,\times)$ sont deux groupes à 4 éléments. Démontrer qu'il n'existe aucun isomorphisme de groupes de $(\mathbf{U}_2,\times)\times(\mathbf{U}_2,\times)$ dans $(\mathbf{U}_4,\times)$.

Exercice C13.96 — Les groupes $(S_3,\circ)$ et $(\mathbf{U}_6,\times)$ sont deux groupes à 6 éléments. Démontrer qu'il n'existe aucun isomorphisme de groupes de $(S_3,\circ)$ dans $(\mathbf{U}_6,\times)$.

Exercice C13.97 — Démontrer qu'il n'existe aucun isomorphisme de groupes de $(\mathbf{Q},+)$ dans $(\mathbf{Q}^*,\times)$.

Proposition C13.98 (application réciproque d'un isomorphisme de groupes)
Considérons un isomorphisme de groupes $f:(G_1,*_1)\longrightarrow(G_2,*_2)$. Alors

$$f^{-1}\left|\begin{array}{ccc}(G_2,*_2) & \longrightarrow & (G_1,*_1)\\ g_2 & \longmapsto & \text{l'unique } g_1\in G_1 \text{ tel que } f(g_1)=g_2\end{array}\right.$$

est un isomorphisme de groupes.

§ 5. Anneaux et corps

Définition C13.99 (distributivité)
Soit E un ensemble muni de deux lois de composition internes notées $+$ et $\times$. Si

$$(x+y)\times z=x\times z+y\times z \qquad \text{et} \qquad x\times(y+z)=x\times y+x\times z$$

pour tout triplet $(x,y,z)\in E^3$ alors on dit que la loi $\times$ est distributive par rapport à la loi $+$.

Définition C13.100 (anneau)
Un anneau A est un ensemble muni de deux lois de compositions internes $+$ et $\times$ telles que
1) $(A,+)$ est un groupe abélien (dont l'élément neutre est noté 0_A) ;
2) La loi $\times$ est associative et possède un élément neutre (noté 1_A) ;
3) La loi $\times$ est distributive par rapport à la loi $+$.
L'anneau est dit commutatif si la loi $\times$ est commutative.

Exemple C13.101 — $\mathbf{Z},\mathbf{Q},\mathbf{R},\mathbf{C}$ munis de leurs additions et multiplications usuelles sont des anneaux.

Proposition C13.102 (multiplication par 0_A et par -1_A dans un anneau)
Soient $(A,+,\times)$ un anneau et a un élément de A. Alors

$$0_A\times a=0_A=a\times 0_A \qquad \text{et} \qquad (-1_A)\times a=-a=a\times(-1_A)\ .$$

Démonstration — De $(0_A+0_A)\times a=0_A\times a$ et de la distributivité de $\times$ par rapport à $+$, nous déduisons

$$0_A\times a+0_A\times a=0_A\times a\,.$$

En ajoutant l'opposé de $0_A\times a$ à chacun des membres à gauche, nous obtenons finalement $0_A\times a=0_A$. L'identité $a\times 0_A=0_A$ peut être obtenue de manière analogue.

De $(-1_A+1_A)\times a = 0_A \times a$ et de la distributivité de $\times$ par rapport à $+$, nous déduisons

$$(-1_A)\times a + 1_A \times a = 0_A \times a$$

puis $(-1_A)\times a + a = 0_A$. En ajoutant l'opposé de a à chacun des membres à gauche, nous obtenons finalement $(-1_A)\times a = -a$. L'identité $a\times(-1_A) = -a$ peut être obtenue de manière analogue.

Notation C13.103 — Soit $(A,+,\times)$ est un anneau. Si n est un entier naturel non nul, l'élément de A

$$\underbrace{1_A+1_A+\ldots+1_A}_{n \text{ termes}}$$

que nous devrions noter $n1_A$ est plus simplement noté n.

Proposition C13.104 (une formule de factorisation dans un anneau)
Soit $(A,+,\times)$ un anneau. Si a et b sont deux éléments de A tels que $a\times b = b\times a$ alors, pour tout $n\in\mathbf{N}^*$

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}\,.$$

Proposition C13.105 (formule du binôme de Newton dans un anneau)
Soit $(A,+,\times)$ un anneau. Si a et b sont deux éléments de A tels que $a\times b = b\times a$ alors, pour tout $n\in\mathbf{N}$

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

Définition C13.106 (éléments inversible dans un anneau)
Soit $(A,+,\times)$ un anneau.
1) Un élément $a\in A$ est dit inversible s'il existe un élément $b\in A$ tel que

$$a\times b = 1_A = b\times a\,.$$

2) Si un élément $a\in A$ est inversible alors, comme la loi $\times$ est associative, il existe un unique élément $b\in A$ $a\times b = 1_A = b\times a$. Cet élément b est appelé inverse de a et est noté a^{-1}.

Notation C13.107 — L'ensemble des unités d'un anneau $(A,+,\times)$ est noté $U(A)$

$$U(A) := \{a\in A : \exists b\in A \quad a\times b = 1_A = b\times a\}\,.$$

Proposition C13.108 (groupe des unités d'un anneau)
Soit $(A,+,\times)$ un anneau. Alors l'application

$$\left|\begin{array}{ccc} U(A)\times U(A) & \longrightarrow & U(A) \\ (a_1,a_2) & \longmapsto & a_1\times a_2 \end{array}\right.$$

définit une loi de composition interne sur $U(A)$, qui confère à $U(A)$ une structure canonique de groupes.

Exemple C13.109 — L'ensemble des unités de $(\mathbf{Z},+,\times)$ est $U(\mathbf{Z}) = \{-1,1\}$.

DÉFINITION C13.110 (ANNEAU INTÈGRE)
Un anneau $(A,+,\times)$ est dit intègre s'il est commutatif et si

$$a_1 \times a_2 = 0_A \quad \Longrightarrow \quad (a_1 = 0_A \text{ ou } a_2 = 0_A)$$

pour tout couple $(a_1,a_2) \in A^2$.

EXEMPLE C13.111 — Les anneaux $(\mathbf{Z},+,\times)$, $(\mathbf{Q},+,\times)$, $(\mathbf{R},+,\times)$ et $(\mathbf{C},+,\times)$ sont intègres.

PROPOSITION C13.112 (SIMPLIFICATION DANS UN ANNEAU INTÈGRE)
Soit $(A,+,\times)$ un anneau. Pour tout couple $(a_1,a_2) \in A^2$, pour tout élément $b \in A \setminus \{0_A\}$

$$(a_1 \times b = a_2 \times b \text{ ou } b \times a_1 = b \times a_2) \quad \Longrightarrow \quad a_1 = a_2\,.$$

DÉFINITION C13.113 (CORPS)
Un anneau $(A,+,\times)$ commutatif est un corps si $1_A \neq 0_A$ et tout élément de $A \setminus \{0_A\}$ est inversible.

DÉFINITION C13.114 (SOUS-ANNEAU)
Soit $(A,+,\times)$ un anneau. Une partie B de A est un sous-anneau de A si
1) 0_A et 1_A appartiennent à B ;
2) pour tout $(b_1,b_2) \in B^2$, $b_1+b_2 \in B$ et $b_1 \times b_2 \in B$ (B est stable pour les lois $+$ et $\times$) ;
3) pour tout $b \in B$, $-b \in B$ (B est stable par passage à l'opposé).

REMARQUE C13.115 — Soient $(A,+,\times)$ un anneau et B un sous-anneau de A. Alors les applications

$$+_B \left| \begin{array}{ccc} B\times B & \longrightarrow & B \\ (b_1,b_2) & \longmapsto & b_1+b_2 \end{array} \right. \quad \text{et} \quad \times_B \left| \begin{array}{ccc} B\times B & \longrightarrow & B \\ (b_1,b_2) & \longmapsto & b_1\times b_2 \end{array} \right.$$

sont bien définies et $(B,+_B,\times_B)$ est un anneau.

EXERCICE C13.116 — Démontrer que $\mathbf{Z}[i] := \{a+ib \,:\, (a,b) \in \mathbf{Z}^2\}$ est un sous-anneau de $(\mathbf{C},+,\times)$.

EXEMPLE C13.117 — $\mathbf{Q}[i] := \{a+ib \,:\, (a,b) \in \mathbf{Q}^2\}$ est un sous-anneau de $(\mathbf{C},+,\times)$ qui est un corps.
1) Clairement 0 et 1 appartiennent à $\mathbf{Q}[i]$.
2) Considérons deux éléments x_1 et x_2 de $\mathbf{Q}[i]$ que nous écrivons $x_1 = a_1+ib_1$ et $x_2 = a_2+ib_2$ où $(a_1,b_1,a_2,b_2) \in \mathbf{Q}^4$. Comme

$$x_1+x_2 = (a_1+a_2)+i\,(b_1+b_2)$$

et a_1+a_2, b_1+b_2 sont rationnels, le nombre complexe x_1+x_2 appartient à $\mathbf{Q}[i]$. Comme

$$x_1 \times x_2 = (a_1a_2-b_1b_2)+i\,(a_1b_2+a_2b_1)$$

et $a_1a_2-b_1b_2$, $a_1b_2+a_2b_1$ sont rationnels, le nombre complexe $x_1 \times x_2$ appartient à $\mathbf{Q}[i]$.
3) Soit $x \in \mathbf{Q}[i]$ que nous écrivons $x = a+ib$ où $(a,b) \in \mathbf{Q}^2$. Comme

$$-x = (-a)+i\,(-b)$$

et $-a$, $-b$ sont rationnels, le nombre complexe $-x$ appartient à $\mathbf{Q}[i]$.

D'après 1,2,3, $\mathbf{Q}[i]$ est un sous-anneau de $(\mathbf{C},+,\times)$. Donc l'addition et la multiplication sur $\mathbf{C}$ induisent des lois de composition internes sur $\mathbf{Q}[i]$, toujours notées (abusivement) $+$ et $\times$. On observe qu'alors $(\mathbf{Q}[i],+,\times)$ est un anneau commutatif (la multiplication sur $\mathbf{C}$ est commutative) dans lequel $1\neq 0$ (puisque cette propriété vaut dans $\mathbf{C}$).

4) Soit x un élément non nul de $\mathbf{Q}[i]$, que nous écrivons $x=a+ib$ où $(a,b)\in\mathbf{Q}^2$. Le nombre complexe

$$y:=\frac{a}{a^2+b^2}+i\,\frac{-b}{a^2+b^2}$$

est bien défini et, comme $\dfrac{a}{a^2+b^2}$ et $\dfrac{-b}{a^2+b^2}$ sont rationnels, $y\in\mathbf{Q}[i]$. Nous vérifions $x\times y=1=y\times x$ et donc x est inversible pour $\times$ dans $\mathbf{Q}[i]$.

DÉFINITION C13.118 (MORPHISME D'ANNEAUX)
Soient $(A_1,+_1,\times_1)$ et $(A_2,+_2,\times_2)$ deux anneaux. Une application $f\colon A_1\longrightarrow A_2$ est un morphisme d'anneaux si

1) pour tout $(a_1,b_1)\in A_1^2$, $f(a_1+_1 b_1)=f(a_1)+_2 f(b_1)$;
2) pour tout $(a_1,b_1)\in A_1^2$, $f(a_1\times_1 b_1)=f(a_1)\times_2 f(b_1)$;
3) $f(1_{A_1})=1_{A_2}$.

PROPOSITION C13.119 (INTÉGRITÉ D'UN CORPS)
Un corps est intègre.

EXERCICE C13.120 — Démontrer que $\mathbf{Z}[\sqrt{2}]:=\{a+b\sqrt{2}\,:\,(a,b)\in\mathbf{Z}^2\}$ est un sous-anneau de $(\mathbf{R},+,\times)$ et déterminer tous les morphismes d'anneaux de $\mathbf{Z}[\sqrt{2}]$ dans lui-même.

EXERCICE C13.121 — Soit $(K,+,\times)$ un corps. Démontrer qu'il existe un unique morphisme d'anneaux $f\colon(\mathbf{Q},+,\times)\longrightarrow(K,+,\times)$ et que, pour tout $(p,q)\in\mathbf{Z}\times\mathbf{N}^*$

$$f\left(\frac{p}{q}\right)=\left(p1_K\right)\times\left(q1_K\right)^{-1}$$

EXERCICE C13.122 — Soient $(K,+_K,\times_K)$ un corps, $(A,+_A,\times_A)$ un anneau et $f\colon K\longrightarrow A$ un morphisme d'anneaux. Démontrer que f est injective.

PROPOSITION C13.123 (COMPOSÉE DE DEUX MORPHISMES D'ANNEAUX)
Soient $(A_1,+_1,\times_1)$, $(A_2,+_2,\times_2)$ et $(A_3,+_3,\times_3)$ des anneaux. Si $f\colon A_1\longrightarrow A_2$ et $g\colon A_2\longrightarrow A_3$ sont des anneaux alors

$$g\circ f\;\left|\begin{array}{ccc}A_1&\longrightarrow&A_3\\x&\longmapsto&g(f(x))\end{array}\right.$$

est un morphisme d'anneaux.

DÉFINITION C13.124 (ISOMORPHISME D'ANNEAUX)
Soient $(A_1,+_1,\times_1)$ et $(A_2,+_2,\times_2)$ deux anneaux. Si une application $f\colon A_1\longrightarrow A_2$ est un morphisme d'anneaux bijectif alors on dit que f est un isomorphisme d'anneaux.

Exemple C13.125 — L'application

$$f \left| \begin{array}{ccc} (\mathbf{C},+,\times) & \longrightarrow & (\mathbf{C},+,\times) \\ z & \longmapsto & \overline{z} \end{array} \right.$$

est un morphisme d'anneaux.

Proposition C13.126 (application réciproque d'un isomorphisme d'anneaux)
Soient $(A_1,+_1,\times_1)$, $(A_2,+_2,\times_2)$ deux anneaux et $f\colon A_1 \longrightarrow A_2$ un isomorphisme d'anneaux. Alors l'application

$$f^{-1} \left| \begin{array}{ccc} (A_2,+_2,\times_2) & \longrightarrow & (A_1,+_1,\times_1) \\ a_2 & \longmapsto & \text{l'unique } a_1 \in A_1 \text{ tel que } f(a_1)=a_2 \end{array} \right.$$

est un isomorphisme d'anneaux.

Exercice C13.127 — Démontrer qu'il existe une bijection de $\mathbf{Z}\left[\sqrt{2}\right]$ dans $\mathbf{Z}[i]$ mais qu'il n'existe aucun isomorphisme d'anneaux de $\mathbf{Z}\left[\sqrt{2}\right]$ dans $\mathbf{Z}[i]$.