Chapitre 19

Structures algébriques

Compétences attendues.

- ✓ Reconnaître une structure algébrique.
- ✓ Utiliser une caractérisation d'une sous-structure.
- ✓ Effectuer des calculs dans un groupe, dans un anneau.

Anthony Mansuy - Professeur en MP2I au Lycée Roosevelt (Reims)
Page personnelle : `anthony-mansuy.fr/`
E-mail : `mansuy.anthony@hotmail.fr`

1 Loi de composition interne

1.1 Définitions

Définition.

Soit E un ensemble. On appelle *loi de composition interne sur E* toute application de $E \times E$ dans E.

✎ **Notation.**

Une telle loi sera en général notée sous l'une des formes suivantes :

- $+$ en notation additive ;
- $*$, $\star$, $\cdot$, $\circ$, ... en notation multiplicative.

Au lieu d'utiliser la notation standard $+(x, y)$ pour l'image du couple (x, y) par l'application $+$, on note plutôt $x + y$ (ou $x * y$, $x \star y$, $x \cdot y$, $x \circ y$, ...).

Exemples.

- La somme $(x, y) \mapsto x + y$ et le produit $(x, y) \mapsto x \times y$ sont des lois de composition internes sur $\mathbb{R}$, mais aussi sur $\mathbb{C}$, sur $\mathbb{Z}$, sur $\mathbb{Q}$ ou sur $\mathbb{N}$.
- La différence $(x, y) \mapsto x - y$ est une loi de composition interne sur $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ et $\mathbb{Z}$, mais pas sur $\mathbb{N}$ puisque la différence de deux entiers naturel peut être négative.
- Sur l'ensemble $\mathscr{P}(E)$ des parties de E, on a deux lois de composition internes qui sont $(A, B) \mapsto A \cap B$ et $(A, B) \mapsto A \cup B$.
- L'ensemble $\mathscr{M}_n(\mathbb{K})$ est muni de deux lois de composition internes, qui sont la somme et le produit.
- Sur l'ensemble $\mathscr{F}(\mathbb{R}, \mathbb{R})$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, la somme $(f, g) \mapsto f + g$ et la composition $(f, g) \mapsto f \circ g$ sont deux lois de composition internes.

Définition.

Soit E un ensemble muni d'une loi de composition interne $*$. On dit que la loi $*$ est :

- *commutative* si pour tout $(x, y) \in E^2$, $x * y = y * x$;
- *associative* si pour tout $(x, y, z) \in E^3$, $x * (y * z) = (x * y) * z$.

Exemples.

- Sur $\mathbb{C}$ (et donc sur $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ et $\mathbb{N}$), la somme et le produit sont à la fois associatifs et commutatifs.
- La différence n'est pas commutative sur $\mathbb{Z}$ car $2 - 3 \neq 3 - 2$. Elle n'est pas non plus associative car $1 - (1 - 1) \neq (1 - 1) - 1$.
- L'union et l'intersection sont commutatives et associatives sur $\mathscr{P}(E)$.
- Sur $\mathscr{F}(\mathbb{R}, \mathbb{R})$ la composition est associative, mais elle n'est pas commutative.
- La somme de matrices est associative et commutative, le produit est associatif mais n'est pas commutatif si $n \geq 2$.

Définition.

Soit E un ensemble muni d'une loi de composition interne $*$, et soit $A \subset E$.
On dit que A est *stable* par $*$ si pour tout $(x, y) \in A^2$, $x * y$ appartient à A.
Dans ce cas, on appelle *restriction de la loi $*$ à A* la loi de composition interne définie sur A par $(x, y) \mapsto x * y$.

Remarque. Si $*$ est associative (resp. commutative), alors sa restriction à A l'est également.

Définition.

Soit E un ensemble muni de deux lois de composition internes $\oplus$ et $*$. On dit que $*$ est distributive par rapport à $\oplus$ si

$$\forall (x,y,z) \in E^3,\ x*(y\oplus z) = (x*y)\oplus(x*z) \ \text{ et } \ (x\oplus y)*z = (x*z)\oplus(y*z).$$

Exemples.

- Dans $\mathbb{R}$ ou $\mathbb{C}$, le produit est distributif par rapport à la somme. De même dans $\mathscr{M}_n(\mathbb{R})$ ou $\mathscr{M}_n(\mathbb{C})$.
- Dans $\mathscr{P}(E)$, $\cup$ est distributif par rapport à $\cap$ et $\cap$ est distributif par rapport à $\cup$.

1.2 Élément neutre, inversibilité

Définition.

Soit E un ensemble muni d'une loi de composition interne $*$. On dit que $e \in E$ est un élément neutre pour $*$ si :

$$\forall x \in E,\ x*e = e*x = x.$$

Propriété 1

Soit E un ensemble muni d'une loi de composition interne $*$. Si un élément neutre existe, alors il est unique.

Exemples.

- Dans $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ ou $\mathbb{Z}$, 0 est l'élément neutre pour l'addition et 1 est l'élément neutre pour la multiplication.
- $\mathrm{id}_{\mathbb{R}}$ est l'élément neutre de $\mathscr{F}(\mathbb{R},\mathbb{R})$ pour la composition $\circ$.
- I_n est l'élément neutre de $\mathscr{M}_n(\mathbb{K})$ pour la multiplication, et la matrice nulle est l'élément neutre pour l'addition.

✎ **Notation.**

L'élément neutre de E, s'il existe, sera plutôt noté 0_E ou 0 en notation additive, 1_E ou 1 en notation multiplicative.

Définition.

Soit E un ensemble muni d'une loi de composition interne $*$ possédant un élément neutre e.

Un élément $x \in E$ est dit *symétrisable* ou *inversible* s'il existe $y \in E$ tel que $x*y = y*x = e$.

Exemples.

- Dans $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, tout élément est symétrisable, car on a toujours $x+(-x) = (-x)+x = 0$. Dans $(\mathbb{N},+)$, seul 0 est symétrisable.
- Dans $(\mathbb{N},\times)$, seul 1 est symétrisable. Dans $(\mathbb{Z},\times)$ seuls 1 et -1 sont symétrisables.

  Dans $(\mathbb{Q},\times)$, $(\mathbb{R},\times)$, $(\mathbb{C},\times)$, tout élément non nul est symétrisable. En revanche, 0 n'est pas symétrisable car pour tout élément y, $0\times y = y\times 0 = 0 \neq 1$.

Exercice 1. On considère $\mathscr{P}(E)$ muni de l'intersection $\cap$. Existe-t-il un élément neutre ? Quels éléments sont symétrisables ? Mêmes questions pour $(\mathscr{P}(E),\cup)$.

Propriété 2

Soit E un ensemble muni d'une loi **associative** $*$ possédant un élément neutre e.
Si $x \in E$ est symétrisable, alors il existe un unique $y \in E$ tel que $x * y = y * x = e$.
Cet élément est appelé **le** *symétrique de* x.

Notation.

On note le symétrique de x (s'il existe) :

- $-x$ en notation additive, et on parle plutôt de **l'***opposé de* x dans ce cas ;
- x^{-1} en notation multiplicative, et on parle alors plutôt de **l'***inverse de* x.

Remarque. L'élément neutre e est toujours symétrisable, et égal à son propre symétrique puisque $e * e = e$.

Exemples.

- Dans $\mathscr{F}(\mathbb{R}, \mathbb{R})$, un élément f est symétrisable pour $\circ$ si, et seulement si, f est une bijection, et alors son symétrique est la bijection réciproque f^{-1} de f.
- Dans $\mathscr{M}_n(\mathbb{K})$ muni de la multiplication, on retrouve exactement la définition d'une matrice inversible.

Propriété 3

Soit E un ensemble muni d'une loi associative $*$, d'élément neutre e.

(1) Si x est symétrisable, alors x^{-1} l'est aussi, et $(x^{-1})^{-1} = x$.

(2) Si x et y sont symétrisables, alors $x * y$ l'est aussi, et $(x * y)^{-1} = y^{-1} * x^{-1}$.

Propriété 4 (Simplification par un élément inversible)

Soit E un ensemble muni d'une loi de composition interne associative $*$, et soit x un élément symétrisable. Alors :

- $\forall (y, z) \in E^2, \quad x * y = x * z \;\Rightarrow\; y = z.$
- $\forall (y, z) \in E^2, \quad y * x = z * x \;\Rightarrow\; y = z.$

On dit alors que x est un élément *régulier*.

Danger.

Dans $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$ ou $(\mathbb{C}, \times)$, tout élément non nul est inversible, et on peut donc « simplifier » par tout élément **non nul**. Attention, cela n'est pas aussi simple dans d'autres situations :

- dans $(\mathscr{F}(\mathbb{R}, \mathbb{R}), \circ)$ par exemple, si $f : x \mapsto 0$, $g : x \mapsto x$ et $h : x \mapsto |x|$, alors :

$$f \circ g = f \circ h \quad \text{et} \quad g \circ f = h \circ f$$

mais $g \neq h$. L'élément f n'est donc pas régulier, et on ne peut pas « simplifier » par f. Il est cependant possible de « simplifier » par une fonction si celle-ci est **bijective**.

- autre exemple dans $(\mathscr{M}_n(\mathbb{K}), \times)$:

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}\times\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix}\times\begin{pmatrix}0&0\\0&2\end{pmatrix}\quad\text{et}\quad\begin{pmatrix}0&0\\0&1\end{pmatrix}\times\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&2\end{pmatrix}\times\begin{pmatrix}1&0\\0&0\end{pmatrix}$$

mais $\begin{pmatrix}0&0\\0&1\end{pmatrix}\neq\begin{pmatrix}0&0\\0&2\end{pmatrix}$. On ne peut donc pas « simplifier » par $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ qui n'est pas régulier. On peut cependant « simplifier » par toute matrice **inversible**.

1.3 Itérés d'un élément

Dans cette section, E désigne un ensemble muni d'une loi interne associative $*$ et d'élément neutre e.

Définition.

Soit $x \in E$. On définit les *puissances de* x en posant $x^0 = e$ et pour tout $n \in \mathbb{N}$:

$$x^{n+1} = x^n * x.$$

Ainsi, pour tout $n \in \mathbb{N}^*$: $x^n = \underbrace{x * x * \cdots * x}_{n \text{ fois}}$.

✎ **Notation.**

Si la loi de E est notée additivement $+$, on note $0\,x = 0$ et pour tout $n \in \mathbb{N}^*$:

$$n\,x = \underbrace{x + x + \cdots + x}_{n \text{ fois}},$$

et on parle plutôt des *multiples de* x.

Propriété 5

(1) Soit $x \in E$. Alors pour tout $(m, n) \in \mathbb{N}^2$, $x^m * x^n = x^{m+n}$.

(2) Soient $x, y \in E$ des éléments qui commutent, c'est-à-dire tels que $x * y = y * x$.
Alors pour tout $n \in \mathbb{N}$:

$$x^m * y^n = y^n * x^m \quad \text{et} \quad (x * y)^n = x^n * y^n.$$

Propriété 6

Soit $x \in E$ un élément inversible. Alors pour tout $n \in \mathbb{N}$, x^n est inversible, et $(x^n)^{-1} = \left(x^{-1}\right)^n$.
On note alors x^{-n} au lieu de $\left(x^{-1}\right)^n$

Propriété 7

Soit $x \in E$ un élément inversible. Alors pour tout $(m, n) \in \mathbb{Z}^2$, $x^{m+n} = x^m * x^n$.

Remarque. Toutes les puissances de x commutent entre elles puisque $m + n = n + m$.

2 Groupes

2.1 Définitions et exemples

Définition.

Soit G un ensemble muni d'une loi de composition interne $*$.
On dit que $(G,*)$ est un *groupe* si :

- la loi $*$ est associative : $\forall (x,y,z)\in G^3,\ x*(y*z)=(x*y)*z$;
- la loi $*$ possède un élément neutre : $\exists e\in G,\ \forall x\in G,\ x*e=e*x=x$;
- tout élément de G est symétrisable pour $*$: $\forall x\in G,\ \exists y\in G,\ x*y=y*x=e$.

Si de plus la loi $*$ est commutative, on dira que $(G,*)$ est un *groupe commutatif* ou *abélien*.
Si G est fini, son cardinal $\mathrm{Card}(G)$ s'appelle *l'ordre de* G.

Rappel. D'après les résultats précédemment obtenus, l'élément neutre d'un groupe $(G,*)$ est unique, de même que le symétrique d'un élément.

✎ **Notation.**

Par convention, on note généralement multiplicativement $x*y$ la loi d'un groupe non commutatif, et on note alors 1_G ou plus simplement 1 son élément neutre.
Pour les groupes abéliens, on note plutôt la loi additivement $x+y$. Dans ce cas, on note 0_G ou 0 l'élément neutre, $-x$ le symétrique de x et $n\,x$ au lieu de x^n.

Exemples.

- $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ sont des groupes abéliens. $(\mathbb{N},+)$ n'est pas un groupe.
- $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes abéliens.
- Pour tout $n\geq 1$, $(\mathbb{U}_n,\times)$ est un groupe abélien fini d'ordre n.
- $(\mathscr{M}_{n,p}(\mathbb{K}),+)$ est un groupe abélien.
- $(\mathrm{GL}_n(\mathbb{K}),\times)$ est un groupe, non abélien dès que $n\geq 2$.

Propriété 8

Soit X un ensemble. On note $\mathfrak{S}(X)$ (ou $S(X)$) l'ensemble des bijections de X dans X.
Alors $(\mathfrak{S}(X),\circ)$ est un groupe, non commutatif dès que X contient au moins trois éléments distincts.
Si de plus X est fini de cardinal n, alors $\mathfrak{S}(X)$ est un groupe fini d'ordre $n!$.
Ce groupe est appelé *groupe symétrique de* X, et ses éléments sont nommés *permutations de* X.

✎ **Notation.**

Si $X=[\![1,n]\!]$ avec $n\geq 1$, on notera le groupe symétrique de X plus simplement $\mathfrak{S}_n$, et on l'appellera *groupe symétrique d'indice* n. Un élément $\sigma\in\mathfrak{S}_n$ se représente communément sous forme d'un tableau :

$$\sigma=\begin{pmatrix}1 & 2 & \dots & n\\ \sigma(1) & \sigma(2) & \dots & \sigma(n)\end{pmatrix}.$$

Le saviez-vous ?

Il est fréquent de trouver des propriétés communes dans des situations qui au départ semblent totalement sans rapport. Une des grandes découvertes (et réussites) des mathématiques du $19^{ème}$ siècle a été de parvenir à unifier ces problèmes en apparence distincts, en faisant ressortir de ces différents problèmes des structures ensemblistes et opératoires ayant des propriétés similaires.

C'est Évariste Galois le premier à mettre en avant ces études de structures à l'occasion de ses travaux visant à étudier la résolubilité des équations polynomiales par radicaux. Il y parle de groupes de permutations des solutions d'une équation, et est amené à étudier des propriétés de certains sous-ensembles de ces groupes de permutations. C'est lui qui introduit la terminologie de « groupe », même si la formalisation précise de cette notion est beaucoup plus tardive.

Propriété 9

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. On définit sur le produit cartésien $G_1 \times G_2$ la loi de composition interne $\star$ suivante :

$$\forall (g_1, g_2), (g_1', g_2') \in G_1 \times G_2,\ (g_1, g_2) \star (g_1', g_2') = (g_1 *_1 g_1', g_2 *_2 g_2')$$

Alors $(G_1 \times G_2, \star)$ est un groupe, appelé le *produit direct des groupes* G_1 *et* G_2.
De plus, $(G_1 \times G_2, \star)$ est abélien si, et seulement si, $(G_1, *_1)$ et $(G_2, *_2)$ le sont.

Table de Cayley d'un groupe fini.
Lorsque G est un groupe fini dont on note $a_1, a_2, \dots, a_n$ les éléments, on peut résumer la loi $*$ dans un tableau à n lignes et n colonnes dans lequel on fait figurer à l'intersection de la ligne i et de la colonne j le résultat $a_i * a_j$.

$*$	a_1	$\dots$	a_j	$\dots$	a_n
a_1	$a_1 * a_1$	$\dots$	$a_1 * a_j$	$\dots$	$a_1 * a_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_i	$a_1 * a_i$	$\dots$	$a_i * a_j$	$\dots$	$a_i * a_n$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_n	$a_n * a_1$	$\dots$	$a_n * a_j$	$\dots$	$a_n * a_n$

Exercice 2. Dresser la table des groupes $\mathbb{U}_3$, $\mathbb{U}_2 \times \mathbb{U}_2$ et $\mathfrak{S}_3$.

Remarque. Dans la table d'un groupe fini, chaque élément apparaît une et une seule fois sur chaque ligne et chaque colonne. On peut le justifier pour les colonnes en notant que pour tout $g \in G$, l'application $\varphi_g : x \mapsto x * g$ est une bijection de G sur G, d'inverse $\varphi_{g^{-1}}$. Et de même pour les lignes en considérant l'application $\psi_g : x \mapsto g * x$.

2.2 Sous-groupes

Définition.

Soit $(G, *)$ un groupe, et soit H une partie non vide de G.
On dit que H est *un sous-groupe de* G si H est stable par $*$ et que $(H, *)$ est un groupe.

Exemple. Pour tout groupe G, G et $\{e_G\}$ sont des sous-groupes de G, appelés *sous-groupes triviaux de* G. À l'inverse, on appelle *sous-groupe propre de* G tout sous-groupe non trivial de G.

Propriété 10 (Première caractérisation d'un sous-groupe)

Soit $(G, *)$ un groupe, et $H \subset G$. H est un sous-groupe de G si, et seulement si :

(1) $e_G \in H$; (2) $\forall (x, y) \in H^2$, $x * y \in H$; (3) $\forall x \in H$, $x^{-1} \in H$.

Corollaire 11 (Deuxième caractérisation d'un sous-groupe)

Soit G un groupe, et $H \subset G$. H est un sous-groupe de G si, et seulement si :

(1) $e_G \in H$; (2) $\forall (x, y) \in H^2$, $x * y^{-1} \in H$.

Exemples.

- $(\mathbb{R}_+^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$. En revanche, $(\mathbb{R}_-^*, \times)$ n'est pas un sous-groupe de $(\mathbb{R}^*, \times)$.
- L'ensemble $\mathbb{U}$ des nombres complexes de module 1 est un sous-groupe de $(\mathbb{C}^*, \times)$.
- Pour tout $n \in \mathbb{N}^*$, l'ensemble $\mathbb{U}_n$ des racines n-èmes de l'unité est un sous-groupe de $(\mathbb{C}^*, \times)$ (et de $(\mathbb{U}, \times)$ aussi).
- Soit $n \in \mathbb{N}^*$. Notons $\mathscr{D}_n^*(\mathbb{K})$ (resp. $\mathscr{T}_n^*(\mathbb{K})$) l'ensemble des matrices de taille $n \times n$ diagonales inversibles (resp. triangulaires supérieures inversibles). Alors $\mathscr{D}_n^*(\mathbb{K})$ et $\mathscr{T}_n^*(\mathbb{K})$ sont des sous-groupes de $(\mathrm{GL}_n(\mathbb{K}), \times)$.

Méthode. Comment montrer qu'un ensemble est un groupe ?

Pour montrer qu'un ensemble est un groupe, on commencera par se demander s'il ne serait pas un sous-groupe d'un groupe déjà connu. En effet, il sera alors bien plus rapide de prouver les points qui caractérisent un sous-groupe que ceux qui caractérisent un groupe.

Exercice 3. Montrer que $U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{K} \right\}$ muni du produit matriciel est un groupe.

Propriété 12

Soit $(H_i)_{i \in I}$ une famille de sous-groupes de $(G, *)$. Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

Propriété 13

Soient $(G, *)$ un groupe, et $g \in G$. Alors :

$$\langle g \rangle = \{g^n, n \in \mathbb{Z}\}$$

est un sous-groupe de G, appelé *sous-groupe engendré par* g.

De plus, $\langle g \rangle$ est le plus petit sous-groupe (au sens de l'inclusion) qui contient g : si H est un sous-groupe de G contenant g, alors $\langle g \rangle \subset H$.

Définition.

On dit qu'un groupe $(G, *)$ est *monogène* s'il existe $g \in G$ tel que $G = \langle g \rangle$. S'il est de plus fini, on dit que $(G, *)$ est *cyclique*.

Exemples.

- $(\mathbb{Z}, +)$ est monogène, engendré par 1 (ou -1).
- Pour tout $n \geq 1$, $\mathbb{U}_n$ est un groupe cyclique, engendré par $\xi_n = e^{\frac{2i\pi}{n}}$.

Propriété 14

Un groupe monogène est abélien.

Exercice 4. Les groupes $(\mathbb{R}, +)$ et $(\mathfrak{S}_n, \circ)$ sont-ils monogènes ?

2.3 Morphismes de groupes

Définition.

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. On appelle *morphisme (de groupes)* de G_1 dans G_2 toute application $\varphi : G_1 \to G_2$ telle que :

$$\forall x, y \in G, \quad \varphi(x *_1 y) = \varphi(x) *_2 \varphi(y).$$

Exemples.

- Pour tout groupe G, id_G est un morphisme de G dans lui-même.
- Si G_1 et G_2 sont deux groupes, l'application constante égale à e_{G_2} est un morphisme de G_1 dans G_2.
- Le module $z \mapsto |z|$ est un morphisme de $(\mathbb{C}^*, \times)$ dans $(\mathbb{R}_+^*, \times)$.
- L'exponentielle complexe est un morphisme de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$.
- Pour tout groupe $(G, *)$ et pour tout $g \in G$, $\varphi_g : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & G \\ n & \mapsto & g^n \end{array} \right.$ est un morphisme de $(\mathbb{Z}, +)$ dans $(G, *)$.

Propriété 15

Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes, et soit $\varphi : G_1 \to G_2$ un morphisme de groupes. Alors :

(1) $\varphi(e_{G_1}) = e_{G_2}$; (2) $\forall x \in G_1, \quad \varphi(x^{-1}) = \varphi(x)^{-1}$.

Propriété 16

Soient $(G_1, *_1)$, $(G_2, *_2)$ et $(G_3, *_3)$ trois groupes.
Si $\varphi : G_1 \to G_2$ et $\psi : G_2 \to G_3$ sont deux morphismes de groupes, alors $\psi \circ \varphi$ est un morphisme de groupes de G_1 dans G_3.

Propriété 17

Soit φ un morphisme de groupes entre $(G_1, *_1)$ et $(G_2, *_2)$.

(1) Pour tout sous-groupe H_1 de G_1, $\varphi(H_1) = \{\varphi(h),\ h \in H_1\}$ est un sous-groupe de G_2.

(2) Pour tout sous-groupe H_2 de G_2, $\varphi^{-1}(H_2) = \{h \in G_1 \mid \varphi(h) \in H_2\}$ est un sous-groupe de G_1.

Définition.

Soit φ un morphisme de groupes entre $(G_1, *_1)$ et $(G_2, *_2)$.

- On appelle *noyau de* φ, et on note $\mathrm{Ker}(\varphi)$ (provient de l'allemand *Kern*) le sous-groupe de G_1 défini par :
$$\mathrm{Ker}(\varphi) = \varphi^{-1}(\{e_{G_2}\}) = \{g \in G_1 \mid \varphi(g) = e_{G_2}\}.$$
- On appelle *image de* φ, et on note $\mathrm{Im}(\varphi)$ le sous-groupe de G_2 défini par :
$$\mathrm{Im}(\varphi) = \varphi(G_1) = \{\varphi(g),\, g \in G_1\} = \{h \in G_2 \mid \exists g \in G_1,\, \varphi(g) = h\}.$$

Propriété 18 (Caractérisations de l'injectivité et de la surjectivité)

Soit φ un morphisme de groupes entre $(G_1, *_1)$ et $(G_2, *_2)$.

(1) φ est injective si, et seulement si, $\mathrm{Ker}(\varphi) = \{e_{G_1}\}$.

(2) φ est surjective si, et seulement si, $\mathrm{Im}(\varphi) = G_2$.

Exemples.

- Le module $z \mapsto |z|$ est un morphisme surjectif de $\mathbb{C}^*$ dans $\mathbb{R}_+^*$, de noyau $\{z \in \mathbb{C}^* \mid |z| = 1\} = \mathbb{U}$.
- L'exponentielle complexe est un morphisme surjectif de $\mathbb{C}$ dans $\mathbb{C}^*$, de noyau $\{z \in \mathbb{C} \mid e^z = 1\} = 2i\pi\mathbb{Z}$.

Définition.

On appelle *isomorphisme (de groupes)* de G_1 sur G_2 tout morphisme de groupes bijectif de G_1 sur G_2.
Lorsque $G_1 = G_2$, on parle d'*automorphisme (de groupe)* de G_1.
On dit que deux groupes G_1 et G_2 sont *isomorphes* lorsqu'il existe un isomorphisme de G_1 sur G_2.

Exemple. Les groupes $(\mathbb{R}_+^*, \times)$ et $(\mathbb{R}, +)$ sont isomorphes, et le logarithme est un isomorphisme de $(\mathbb{R}_+^*, \times)$ sur $(\mathbb{R}, +)$.

Exercice 5. Montrer que $\varphi : a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ est un isomorphisme de $(\mathbb{K}, +)$ sur $(U, \times)$.

Propriété 19

(1) Soient G_1 et G_2 deux groupes et $\varphi : G_1 \to G_2$ un isomorphisme de groupes de G_1 sur G_2. Alors φ^{-1} est un isomorphisme de groupes de G_2 sur G_1.

(2) Soit G un groupe. L'ensemble $\mathrm{Aut}(G)$ des automorphismes de groupe de G est un groupe pour la composition.

Remarque. Deux groupes finis G_1 et G_2 sont isomorphes si, et seulement si, la table du groupe G_2 est identique à celle du groupe G_1 à « renumérotation » près des éléments de G_2 à l'aide des éléments de G_1.

Exercice 6. Déterminer à isomorphisme près tous les groupes de cardinal 2 et 3.

Le saviez-vous ?

Un résultat remarquable est la classification à isomorphisme près des groupes finis dits « simples » (l'équivalent des nombres premiers en théorie des groupes), achevée en 1981. C'est en fait un ensemble de travaux, comprenant des dizaines de milliers de pages publiées dans 500 articles par plus de 100 auteurs. On trouve dans cette classification des groupes qui vous sont déjà familiers, les groupes cycliques $\mathbb{U}_p$ avec p premier, mais également des structures bien plus complexes, tel que le Monstre de Fischer, de cardinal :

$$2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71 \ (\simeq 8 \times 10^{53}).$$

3 Généralités sur les anneaux

3.1 Définitions et exemples

Définition.

Soit A un ensemble muni de deux lois internes notées $+$ et $\times$.
On dit que $(A, +, \times)$ est un *anneau (unitaire)* si :

(i) $(A, +)$ est un groupe abélien, dont l'élément neutre est noté 0_A ;

(ii) la loi $\times$ est associative et possède un élément neutre 1_A ;

(iii) la loi $\times$ est distributive par rapport à la loi $+$.

Si de plus la loi $\times$ est commutative, on dit que $(A, +, \times)$ est un *anneau commutatif*.

Exemples.

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
- $(\mathscr{M}_n(\mathbb{K}), +, \times)$ est un anneau non commutatif si $n \geq 2$.
- Soit $(A, +, \times)$ un anneau, et soit E un ensemble. On définit sur l'ensemble $\mathscr{F}(E, A) = A^E$ des applications de E dans A deux lois de compositions internes encore notées $+$ et $\times$ en posant pour tout $f, g \in \mathscr{F}(E, A)$:

  – $\forall x \in E,\ (f + g)(x) = f(x) + g(x)$;
  – $\forall x \in E,\ (f \times g)(x) = f(x) \times g(x)$.

  On vérifie que $\mathscr{F}(E, A)$ muni de ces deux opérations $+$ et $\times$ est un anneau, et qu'il est commutatif si, et seulement si, A l'est.

  En particulier, les ensembles $(\mathscr{F}(I, \mathbb{R}), +, \times)$ et $(\mathscr{F}(I, \mathbb{C}), +, \times)$, où I est un intervalle non vide, sont des anneaux commutatifs, de même que $(\mathbb{R}^{\mathbb{N}}, +, \times)$ et $(\mathbb{C}^{\mathbb{N}}, +, \times)$.

Propriété 20 (Règles de calcul dans un anneau)

Soit $(A, +, \times)$ un anneau, et soient $a, b \in A$. Alors :

(1) $a \times 0_A = 0_A \times a = 0_A$;

(2) $a \times (-b) = (-a) \times b = -(a \times b)$;

(3) Plus généralement, pour tout $n \in \mathbb{Z}$, $a \times (nb) = (na) \times b = n(a \times b)$.

Remarque. Dans la définition d'anneau, rien n'interdit que $1_A = 0_A$. Si c'est le cas, alors pour tout $a \in A$, $a = a \times 1_A = a \times 0_A = 0_A$, et donc $A = \{0_A\}$ est l'*anneau nul*, qui n'a pas un gros intérêt.

Propriété 21

Soit $(A,+,\times)$ un anneau, et soient $a,b\in A$ deux éléments qui **commutent**, c'est-à-dire tels que $a\times b=b\times a$. Alors pour tout $n\in\mathbb{N}$:

- $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}$;
- $a^n-b^n=(a-b)\times\sum_{k=0}^{n-1}a^kb^{n-1-k}$.

3.2 Sous-anneaux

Définition.

Soit $(A,+,\times)$ un anneau et soit B une partie non vide de A. On dit que B est un *sous-anneau de* A si B contient 1_A, B est stable à la fois pour $+$ et pour $\times$, et que $(B,+,\times)$ est un anneau.

Propriété 22 (Caractérisation d'un sous-anneau)

Une partie B d'un anneau $(A,+,\times)$ est un sous-anneau de A si, et seulement si :

(1) $1_A\in B$;

(2) B est un sous-groupe de $(A,+)$: $\forall(x,y)\in B^2,\quad x-y\in B$;

(3) B est stable par multiplication : $\forall(x,y)\in B^2,\quad x\times y\in B$.

Exemples.

- $(\mathbb{Z},+,\times)$ est un sous-anneau de $(\mathbb{Q},+,\times)$, qui est lui-même un sous-anneau de $(\mathbb{R},+,\times)$, qui est lui-même un sous-anneau de $(\mathbb{C},+,\times)$.
- L'ensemble $2\mathbb{Z}$ des entiers pairs n'est pas un sous-anneau de $(\mathbb{Z},+,\times)$: bien qu'il en soit un sous-groupe et qu'il soit stable par multiplication, il ne contient pas le neutre multiplicatif 1 de $\mathbb{Z}$.
- Soit $n\in\mathbb{N}^*$ L'ensemble $\mathscr{T}_n(\mathbb{K})$ des matrices triangulaires supérieures de $\mathscr{M}_n(\mathbb{K})$ est un sous-anneau de $(\mathscr{M}_n(\mathbb{K}),+,\times)$.
- L'ensemble $\mathscr{C}(\mathbb{R},\mathbb{R})$ est un sous-anneau de $(\mathscr{F}(\mathbb{R},\mathbb{R}),+,\times)$.

Mise en garde.

Ne pas oublier la condition $1_A\in B$ dans la caractérisation des sous-anneaux : par exemple, $B=\left\{\begin{pmatrix}x&0\\0&0\end{pmatrix},\ x\in\mathbb{R}\right\}$ est un sous-groupe additif de $\mathscr{M}_2(\mathbb{R})$, stable par produit et admet $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ pour élément neutre multiplicatif. Ainsi, $(B,+,\times)$ est un anneau, mais ce n'est pas un sous-anneau de $(\mathscr{M}_2(\mathbb{R}),+,\times)$: ils n'ont pas le même élément neutre, et leurs inversibles (qu'on définit dans la section suivante) n'ont aucun rapport.

Exercice 7. Montrer que l'ensemble $\mathbb{Z}[i]=\left\{a+ib,\ (a,b)\in\mathbb{Z}^2\right\}$ est un sous-anneau de $(\mathbb{C},+,\times)$.

3.3 Diviseurs de zéro

Définition.

Soit $(A,+,\times)$ un anneau et $a\in A$ différent de 0_A. On dit que a est un *diviseur de zéro* s'il existe $b\in A$ différent de 0_A tel que $a\times b=0_A$ ou $b\times a=0_A$.

Exemple. L'anneau non commutatif $(\mathscr{F}(\mathbb{R},\mathbb{R}),+,\circ)$ possède des diviseurs de zéro, par exemple la fonction $f:x\mapsto\max(x,0)$, puisque si $g:x\mapsto-x^2$, alors pour tout $x\in\mathbb{R}$:

$$f\circ g(x)=\max(-x^2,0)=0.$$

Exercice 8. Montrer que si $A \in \mathscr{M}_n(\mathbb{K})$ n'est pas inversible, alors A est un diviseur de zéro.

Définition.

Un anneau commutatif $(A, +, \times)$ est dit *intègre* s'il est non nul et ne possède pas de diviseurs de zéro.
Autrement dit, $(A, +, \times)$ est intègre si $A \neq \{0_A\}$ et si

$$\forall (a, b) \in A^2, \quad a \times b = 0_A \;\Rightarrow\; (a = 0_A \text{ ou } b = 0_A)\,.$$

Exemples.

- Si $(A, +, \times)$ est un anneau intègre, alors tout sous-anneau de A est un anneau intègre.
- $(\mathbb{C}, +, \times)$ est intègre, de même que $(\mathbb{R}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{Z}, +, \times)$.

Exercice 9. Soient $(A, +, \times)$ un anneau intègre et E un ensemble non vide. Donner une condition nécessaire et suffisante sur E pour que $(\mathscr{F}(E, A), +, \times)$ soit un anneau intègre.

3.4 Éléments inversibles

Définition.

Soit $(A, +, \times)$ un anneau. On dit qu'un élément $a \in A$ est *inversible* s'il possède un inverse pour la loi $\times$, c'est-à-dire s'il existe $b \in A$ tel que $a \times b = b \times a = 1_A$.

Notation.

Si $a \in A$ est inversible, son inverse est unique par associativité de $\times$. On le note x^{-1}.
L'ensemble des éléments inversibles de A se note A^*, ou encore $\mathscr{U}(A)$ (on parle parfois d'*unités* au lieu d'inversibles).

Exemples.

- 1_A est toujours inversible, de sorte que $1_A \in \mathscr{U}(A)$.
  En revanche, si A n'est pas l'anneau nul, 0_A n'est pas inversible (car $a \times 0_A = 0_A$ ne peut jamais être égal à 1_A), et donc $\mathscr{U}(A) \subset A \setminus \{0\}$.
- $\mathscr{U}(\mathbb{Z}) = \{-1, 1\}$, $\mathscr{U}(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$, $\mathscr{U}(\mathbb{R}) = \mathbb{R} \setminus \{0\}$, $\mathscr{U}(\mathbb{C}) = \mathbb{C} \setminus \{0\}$.
- Dans $(\mathscr{M}_n(\mathbb{K}), +, \times)$ les éléments inversibles sont bien les matrices que nous avons appelées inversibles. Et nous avons alors noté $\mathrm{GL}_n(\mathbb{K})$ l'ensemble $\mathscr{U}(\mathscr{M}_n(\mathbb{K}))$.

Mise en garde.

Ne pas confondre A^*, l'ensemble des inversibles de $(A, +, \times)$, et $A \setminus \{0_A\}$. Comme dit précédemment, on a l'inclusion $A^* \subset A \setminus \{0_A\}$, mais l'inclusion réciproque est en générale fausse (elle sera vraie si, et seulement si, A est un corps, ce que nous définirons ci-dessous).
Pour éviter cette confusion, on privilégiera la notation $\mathscr{U}(A)$ pour l'ensemble des inversibles de A.

Propriété 23

Si $a \in A$ est inversible, alors a n'est pas un diviseur de zéro.

Propriété 24

Soit $(A, +, \times)$ un anneau.
$(\mathscr{U}(A), \times)$ est un groupe, appelé *groupe des inversibles* (ou *groupe des unités*) de A.
Ce groupe est commutatif si A est un anneau commutatif.

3.5 Morphismes d'anneaux

Définition.

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ des anneaux d'éléments neutres multiplicatifs 1_A et 1_B.
Une application $\varphi : A \to B$ est un *morphisme d'anneaux* si :

- $\forall (x, y) \in A^2$, $\varphi(x +_A y) = \varphi(x) +_B \varphi(y)$;
- $\forall (x, y) \in A^2$, $\varphi(x \times_A y) = \varphi(x) \times_B \varphi(y)$;
- $\varphi(1_A) = 1_B$.

Lorsque φ est bijective, on parle d'*isomorphisme d'anneaux*.

Remarques.

- On pensera à bien vérifier la condition $\varphi(1_A) = 1_B$. En effet, elle ne découle pas directement du second point. Et par exemple, si B n'est pas l'anneau nul, l'application nulle vérifie les deux premiers points, mais pas le troisième et n'est donc pas un morphisme d'anneaux.
- Le premier point nous dit notamment que φ est un morphisme de groupes entre les groupes abéliens $(A, +_A)$ et $(B, +_B)$. Et donc $\varphi(0_A) = 0_B$ et pour tout $x \in A$, $\varphi(-x) = -\varphi(x)$. Et comme tous les morphismes de groupes, φ est injectif si, et seulement si, son noyau est réduit à $\{0_A\}$.
- En revanche, φ n'est pas un morphisme de groupes pour la multiplication car A et B ne sont même pas des groupes pour le produit. On a cependant le résultat suivant.

Propriété 25

Soit $\varphi : A \to B$ un morphisme d'anneaux.
$\varphi(\mathscr{U}(A)) \subset \mathscr{U}(B)$ et pour tout $x \in \mathscr{U}(A)$, $\varphi(x)^{-1} = \varphi(x^{-1})$.
Ainsi, $\varphi_{|\mathscr{U}(A)}$ est un morphisme de groupes de $(\mathscr{U}(A), \times)$ dans $(\mathscr{U}(B), \times)$.

Remarque. Comme dans le cas des groupes, la composée de deux morphismes d'anneaux est un morphisme d'anneaux et l'image directe/réciproque d'un sous-anneau par un morphisme d'anneau est un sous-anneau. On définit également les notions d'*isomorphisme d'anneaux*, d'*automorphisme d'anneau* et d'*anneaux isomorphes*. Il reste vrai que la composée de deux isomorphismes est un isomorphisme et que la réciproque d'un isomorphisme est un isomorphisme.

Exemple. La conjugaison complexe $z \mapsto \bar{z}$ est un automorphisme d'anneau de $(\mathbb{C}, +, \times)$.

Exercice 10. Soit $f : \mathbb{C} \to \mathscr{M}_2(\mathbb{R})$ l'application qui à $z = a + ib \in \mathbb{C}$ associe $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. Montrer que f est un morphisme d'anneaux injectif.

4 Corps commutatifs

Définition.

Un anneau commutatif $(\mathbb{K}, +, \times)$ est un *corps* si tout élément non nul de $\mathbb{K}$ est inversible.

Remarques.

- Un anneau commutatif $(\mathbb{K}, +, \times)$ est un corps si, et seulement si, $\mathscr{U}(\mathbb{K}) = \mathbb{K} \setminus \{0_\mathbb{K}\}$.
- Dans un corps, tout élément non nul étant inversible, il n'y a pas de diviseur de zéro : un corps est intègre.

Exemples.

- $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis des opérations habituelles sont des corps.
- $(\mathbb{Z}, +, \times)$ n'est pas un corps car $\mathscr{U}(\mathbb{Z}) = \{-1, 1\} \neq \mathbb{Z} \setminus \{0\}$.

Définition.

Soit $\mathbb{L} \subset \mathbb{K}$ un sous-ensemble d'un corps $\mathbb{K}$. On dit que $\mathbb{L}$ est un *sous-corps de* $\mathbb{K}$ si $\mathbb{L}$ est stable par $+$ et $\times$, si $1_{\mathbb{K}}$ appartient à $\mathbb{L}$, et si les lois induites sur $\mathbb{L}$ par celles de $\mathbb{K}$ le munissent d'une structure de corps.

Propriété 26 (Caractérisation d'un sous-corps)

Une partie $\mathbb{L}$ d'un corps $\mathbb{K}$ est un sous-corps de $\mathbb{K}$ si, et seulement si :

(1) $1_{\mathbb{K}} \in \mathbb{L}$;

(2) pour tout $(x, y) \in \mathbb{L}^2$, $x - y \in \mathbb{L}$;

(3) pour tout $(x, y) \in \mathbb{L}^2$ avec $y \neq 0$, $x \times y^{-1} \in \mathbb{L}$.

Exercice 11. Montrer que l'ensemble $\mathbb{Q}(i) = \{a + ib,\ a, b \in \mathbb{Q}\}$ est un corps.

Remarque. Les corps seront le bon cadre pour faire de l'algèbre linéaire, et par exemple, tout ce que nous avons dit sur les matrices à coefficients dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$ reste valable dans un corps quelconque.