14 Structures algébriques

14.1 Loi de composition interne

14.1.1 Définitions

Définition 14.1 – Soit E un ensemble. On appelle **loi de composition interne sur** E toute application de $E \times E$ dans E.
Une telle loi est souvent notée $*, \star, +$ ou encore $\times$. Et 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 alors $x \star y, x + y$ ou $x \times y$).

Remarque

L'aspect application est généralement peu important, ce qu'il faut retenir c'est qu'une loi de composition interne est un moyen de définir, à partir de deux éléments de E, un troisième élément de E.

Exemples 14.2

► La somme $(x, y) \mapsto x + y$ et le produit $(x, y) \mapsto xy$ sont des lois de composition interne sur $\mathbf{R}$, mais aussi sur $\mathbf{C}$, sur $\mathbf{Z}$, sur $\mathbf{Q}$ ou sur $\mathbf{N}$.
► La différence $(x, y) \mapsto x - y$ est une loi de composition interne sur $\mathbf{C}, \mathbf{R}, \mathbf{Q}$ et $\mathbf{Z}$ mais pas sur $\mathbf{N}$ 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 qui sont $(A, B) \mapsto A \cap B$ et $(A, B) \mapsto A \cup B$.
► L'ensemble $\mathscr{M}_n(\mathbf{K})$ est muni de deux lois de composition internes, qui sont la somme et le produit.
► Sur l'ensemble $\mathscr{F}(\mathbf{R}, \mathbf{R})$ des fonctions de $\mathbf{R}$ dans $\mathbf{R}$, la somme $(f, g) \mapsto f + g$ et la composition $(f, g) \mapsto f \circ g$ sont deux lois de composition internes.

⚠ Attention !

Ceci ne signifie pas que toute loi nommée + est automatiquement

Définition 14.3 – Soit E un ensemble muni d'une loi de composition interne $*$.
On dit que la loi $*$ est :

1. **commutative** si $\forall (x, y) \in E^2,\ x * y = y * x$
2. **associative** si $\forall (x, y, z) \in E^3,\ x * (y * z) = (x * y) * z$.

Exemples 14.4

► Sur $\mathbf{C}$ (et donc sur $\mathbf{R}, \mathbf{Q}, \mathbf{Z}$ et $\mathbf{N}$), la somme et le produit sont à la fois associatifs et commutatifs.
► La différence n'est pas commutative sur $\mathbf{Z}$ 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 $\mathscr{F}(\mathbf{R}, \mathbf{R})$ la composition est associative[1], mais elle n'est pas commutative. Par exemple, si $f : x \mapsto x + 1$ et $g : x \mapsto x^2$, alors $f \circ g \neq g \circ f$.
► La somme de matrices est associative et commutative, le produit est associatif mais n'est pas commutatif.

[1] Ceci a déjà été prouvé plus tôt.

Dans le cas où un ensemble est fini, on peut représenter la loi de composition par un tableau

à double entrée :

	a	b	c
a	$a*a$	$a*b$	$a*c$
b	$b*a$	$b*b$	$b*c$
c	$c*a$	$c*b$	$c*c$

ou

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

La commutativité est alors facile à lire sur le tableau : il faut[2] qu'il y ait une symétrie par rapport à la diagonale.
L'associativité en revance ne s'y lit pas de manière simple.

[2] Sous réserve qu'on ait bien mis les éléments de E dans le même ordre sur les lignes et les colonnes.

Définition 14.5 – Soit E un ensemble muni de deux lois de composition internes $\oplus$ et $*$. On dit que $*$ est **distributive** par rapport à $\oplus$ si

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

Remarque

Ces deux propriétés sont appelées distributivité à gauche et distributivité à droite, mais nous n'aurons pas besoin de les distinguer.

Exemples 14.6

Dans $\mathbf{R}$ ou dans $\mathbf{C}$, le produit est distributif par rapport à la somme.
De même dans $\mathcal{M}_n(\mathbf{R})$ ou $\mathcal{M}_n(\mathbf{C})$.
Dans $\mathcal{P}(E)$, $\cup$ est distributif par rapport à $\cap$ et $\cap$ est distributif par rapport à $\cup$: ce sont les lois de De Morgan.

Une récurrence facile prouve que lorsque $*$ est distributive par rapport à $\oplus$, alors pour tout $y_1,\dots,y_n \in E^n$, et tout $x \in E$,

$$x*(y_1\oplus y_2\oplus\cdots\oplus y_n) = (x*y_1)\oplus\cdots\oplus(x*y_n).$$

14.1.2 Éléments neutres, inversibilité

Définition 14.7 – Soit E un ensemble muni d'une loi de composition interne $*$. On dit que $e \in E$ est un **élément neutre** pour $*$ si

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

Commutativité

Bien entendu, si la loi $*$ est commutative, on peut se contenter de vérifier une seule des deux égalités $e*x = x$ ou $x*e = x$.

Proposition 14.8 : *Soit E un ensemble muni d'une loi de composition interne $*$. Si un élément neutre existe, alors il est unique.*

Démonstration. Supposons qu'il existe deux éléments neutre e_1 et e_2. Alors, puisque e_1 est neutre, $e_1 * e_2 = e_2$.
Mais puisque e_2 est neutre, $e_1 * e_2 = e_1$. Et donc $e_1 = e_2$. □

Exemples 14.9

► Dans $\mathbf{C}$, $\mathbf{R}$, $\mathbf{Q}$ ou $\mathbf{Z}$, 0 est l'élément neutre pour l'addition et 1 est l'élément neutre pour la multiplication.
► Dans $\mathcal{P}(E)$, E est l'élément neutre pour l'intersection et $\emptyset$ est l'élément neutre pour l'union.
► $\mathrm{id}_{\mathbf{R}}$ est l'élément neutre de $\mathcal{F}(\mathbf{R},\mathbf{R})$ pour la composition $\circ$.
► I_n est l'élément neutre de $\mathcal{M}_n(\mathbf{R})$ pour la multiplication, et la matrice nulle est l'élément neutre pour l'addition.

Remarque

Cet exemple nous montre que pour un ensemble muni de plusieurs lois, il est important de préciser de quelle loi on parle lorsqu'on parle d'élément neutre.

Définition 14.10 – Soit E un ensemble muni d'une loi de composition interne $*$ possédant un élément neutre e.
Un élément $x \in E$ est dit **inversible** si il existe $y \in E$ tel que $x * y = y * x = e$.

Commutativité
Encore une fois, si la loi $*$ est commutative, il suffit de prouver l'une des deux égalités
$$y * x = e \text{ ou } x * y = e.$$

Exemple 14.11

► Dans $\mathbf{C}$, tout élément est inversible pour l'addition, car on a toujours $x + (-x) = (-x) + x = 0$.
Et de même, tout élément non nul est inversible pour la multiplication car $x \times \frac{1}{x} = \frac{1}{x} \times x = 1$.
En revanche, 0 n'est pas inversible pour la multiplication car pour tout $y \in \mathbf{C}$, $0 \times y = y \times 0 = 0 \neq 1$.
► Dans $\mathcal{F}(\mathbf{R}, \mathbf{R})$ un élément est inversible pour $\circ$ si et seulement si c'est une bijection.

Plus généralement
Ceci reste valable dans $\mathcal{F}(E, E)$, où E est un ensemble non vide quelconque, muni de la composition des applications.

Proposition 14.12 : *Soit E un ensemble muni d'une loi de composition interne **associative** $*$ possédant un élément neutre e.*
*Si $x \in E$ est inversible, alors il existe un **unique** $y \in E$ tel que $x * y = y * x = e$. Cet élément y est alors appelé **l'inverse de** x, et on le note x^{-1}.*

Démonstration. Supposons que $y_1 * x = y_2 * x = e$ et $x * y_1 = x * y_2 = e$.
Alors $(y_1 * x) * y_2 = e * y_2 = y_2$.
Mais d'autre part, la loi étant associative, $(y_1 * x) * y_2 = y_1 * (x * y_2) = y_1 * e = y_1$.
Et donc $y_1 = y_2$. □

Remarques. ► Si x est inversible, alors on a $x * x^{-1} = x^{-1} * x = e$, de sorte que x^{-1} est inversible, et son inverse est x. Autrement dit : $\left(x^{-1}\right)^{-1} = x$.
► L'élément neutre e est toujours inversible et égal à son propre inverse puisque $e * e = e$.
► Dans $\mathcal{M}_n(\mathbf{K})$ muni de la multiplication, on retrouve exactement la définition de matrice inversible.

Proposition 14.13 : *Soit E un ensemble muni d'une loi associative $*$, d'élément neutre e.*
Si x et y sont inversibles, alors $x * y$ est encore inversible et $(x * y)^{-1} = y^{-1} * x^{-1}$.

Démonstration. Il suffit de vérifier que $y^{-1} * x^{-1}$ est bien l'inverse de $x * y$. Or on a
$$(y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * e * y = y^{-1} * y = e.$$
Et de même, $(x * y) * (y^{-1} * x) = e$. □

Proposition 14.14 : *Soit E un ensemble muni d'une loi de composition interne associative $*$, et soit x un élément inversible. Alors*
$$\forall (y, z) \in E^2,\ x * y = x * z \Rightarrow y = z \text{ et } y * x = z * x \Rightarrow y = z.$$
On dit alors que x est régulier, ce qui signifie qu'on peut «simplifier» par x.

«Mais j'ai le droit ?»
J'entends souvent cette question : ai-je le droit de multiplier (à gauche) par x^{-1} des deux côtés de l'égalité ? Bien entendu : dire que deux élément sont égaux, c'est que ce sont les mêmes ! Et donc si vous leur appliquez la même transformation, vous obtenez encore les mêmes éléments !

Démonstration. Si $x * y = x * z$, alors en multipliant à gauche par x^{-1}, il vient
$$x^{-1} * (x * y) = x^{-1} * (x * z) \Leftrightarrow (x^{-1} * x) * y = (x^{-1} * x) * z \Leftrightarrow e * y = e * z \Leftrightarrow y = z.$$
On prouve de même que $y * x = z * x \Rightarrow y = z$. □

Exemple 14.15

Soit $A \in \mathscr{P}(E)$ non vide[3]. Alors $A \cup \emptyset$ et $A \cup A$ sont égaux.
Puisque $A \neq \emptyset$, la proposition précédente prouve donc que A n'est pas inversible pour l'union (car il n'est pas régulier).
Et donc $\emptyset$ est le seul élément de $\mathscr{P}(E)$ inversible pour la loi $\cup$.

[3] Ce qui suppose bien entendu E non vide.

14.1.3 Partie stable, itérées d'un élément

Définition 14.16 – Soit E un ensemble muni d'une loi de composition interne $*$, et soit $A \subset E$.
On dit que A est stable par $*$ si $\forall (x,y) \in A^2$, $x * y \in A$.
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 (mais la réciproque est fausse).
En revanche, si $*$ possède un élément neutre dans E, il se peut que ce ne soit pas le cas dans A. Par exemple, dans $\mathscr{M}_2(\mathbf{R})$, l'ensemble des matrices non inversibles est stable par la multiplication, mais ne contient pas d'élément neutre.
Enfin, un élément de A peut avoir un inverse pour la loi $*$, mais si cet inverse n'est pas dans A, x n'a pas d'inverse pour la restriction de $*$ à A.

Rappel
Nous avons prouvé qu'un produit AB de deux matrices de $\mathscr{M}_2(\mathbf{K})$ est inversible si et seulement si A et B le sont.

Définition 14.17 – Soit E un ensemble muni d'une loi interne associative $*$ et d'élément neutre e, et soit $x \in E$. On note alors

$$x^0 = e \text{ et pour tout } n \in \mathbf{N},\ x^{n+1} = x^n * x.$$

Plus simplement, pour tout $n \in \mathbf{N}^*$, $x^n = \underbrace{x * x * \cdots * x * x}_{n \text{ fois}}$.
S'il y a ambiguïté sur la loi, on note parfois x^{*n} au lieu de x^n.

Proposition 14.18 : *Soit $x \in E$, inversible. Alors pour tout $n \in \mathbf{N}$, x^n est inversible, et $(x^n)^{-1} = (x^{-1})^n$.*
On note alors x^{-n} au lieu de $(x^{-1})^n$

Proposition 14.19 : *Soit $x \in E$. Alors pour tout $(m,n) \in \mathbf{N}^2$, $x^{m+n} = x^m * x^n$.*
Si de plus x est inversible, alors cette relation reste valable pour $(m,n) \in \mathbf{Z}^2$.

Démonstration. Prouvons par récurrence sur $n \in \mathbf{N}$ la proposition $\mathscr{P}(n)$: « $\forall m \in \mathbf{N}$, $x^{m+n} = x^m * x^n$ ».
Pour $n = 0$, c'est évident.
Supposons donc $\mathscr{P}(n)$ vraie, et soit $m \in \mathbf{N}$. Alors

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

Donc par récurrence, $\forall (m,n) \in \mathbf{N}^2$, $x^{m+n} = x^m * x^n$.
Si de plus x est inversible, soient alors $(m,n) \in \mathbf{Z}^2$:

- si $(m,n) \in \mathbf{N}^2$, c'est déjà fait.
- si m et n sont négatifs : alors

$$x^m * x^n = \left(x^{-1}\right)^{-m} * \left(x^{-1}\right)^{-n} = \left(x^{-1}\right)^{-n-m} = x^{m+n}.$$

- si $m \geqslant 0$ et $n \leqslant 0$. Si $m + n \geqslant 0$, on a

$$x^m * x^n = x^{m+n} * x^{-n} * x^n = x^{m+n}.$$

Et si $m+n \leqslant 0$, alors

$$x^m * x^n = x^m * \left(x^{-1}\right)^{-n} = x^m * \left(x^{-1}\right)^m * \left(x^{-1}\right)^{-n-m} = \left(x^{-1}\right)^{-n-m} = x^{n+m}.$$

► On traite de manière similaire le cas $m \leqslant 0, n \geqslant 0$.

□

Remarques. Notons que cette preuve justifie, a posteriori, la validité de ces formules pour les composées de bijections ou pour les puissances de matrices inversibles.
► Une conséquence immédiate est que toutes les puissances[4] de x commutent entre elles puisque $m+n = n+m$.

[4] Négatives ou positives.

Proposition 14.20 : *Soit E un ensemble muni d'une loi de composition associative $*$, possédant un élément neutre, et soit $x \in E$.*
Alors $\{x^n,\ n \in \mathbf{N}\}$ est une partie de E stable par $*$.
Si de plus x est inversible, alors $\{x^n,\ n \in \mathbf{Z}\}$ est également stable.

Démonstration. La proposition qui précède nous dit que le produit de deux puissances de x est encore une puissance de x. □

14.2 Groupes

14.2.1 Définition

Définition 14.21 – Soit G un ensemble et $*$ une loi de composition interne sur G.
On dit que $(G,*)$ est un **groupe** si :

1. La loi $*$ est associative : $\forall (x,y,z) \in G^3,\ x*(y*z) = (x*y)*z$
2. Il existe un élément neutre e pour la loi $*$: $\exists e \in G,\ \forall x \in G,\ x*e = e*x = x$
3. Tout élément de G est inversible pour $*$: $\forall x \in G,\ \exists y \in G,\ x*y = y*x = e$.

Rappelons que nous avons prouvé précédemment qu'alors l'élément neutre e et l'inverse x^{-1} de x sont nécessairement uniques.
Si de plus la loi $*$ est commutative, on dit que G est un **groupe commutatif**, ou un **groupe abélien**[5].

Notation

S'il n'y a pas de confusion possible sur la loi de composition (notamment lorsqu'on n'a défini qu'une loi sur G), on dit plus simplement que G est un groupe.

[5] En référence à Niels Henrik Abel, mathématicien norvégien (1802–1829).

Exemples 14.22

► $(\mathbf{Z},+)$, $(\mathbf{Q},+)$, $(\mathbf{R},+)$ et $(\mathbf{C},+)$ sont des groupes abéliens.
► $(\mathbf{Q}^*,\times)$, $(\mathbf{R}^*,\times)$ et $(\mathbf{C}^*,\times)$ sont des groupes abéliens.
► $(\mathcal{M}_{n,p}(\mathbf{K}),+)$ est un groupe abélien. $(GL_n(\mathbf{K}),\times)$ est un groupe, non abélien dès que $n \geqslant 2$.

Remarque. Notons que lorsqu'on travaille dans un groupe G, si $x \in G$ et si on a $y \in G$ tel que $x*y = e_G$, alors automatiquement[6] $y = x^{-1}$, pas besoin de vérifier que $y*x = e$.
Pour autant, et bien que $GL_n(\mathbf{K})$ soit un groupe, cette remarque ne saurait suffire à prouver qu'une matrice est inversible.
Pour une matrice A que l'on sait déjà inversible, c'est-à-dire que l'on sait déjà être dans $GL_n(\mathbf{K})$, alors la remarque s'applique, et si $AB = I_n$, alors $B = A^{-1}$.
En revanche, si on n'a pas encore prouvé l'inversibilité de A, rien ne garantit[7] que $AB = I_n \Rightarrow BA = I_n$.

[6] Tout élément d'un groupe est régulier.

[7] Pour l'instant...

Par convention, on note généralement multiplicativement la loi d'un groupe non commutatif (c'est-à-dire $x \cdot y$), 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, $-x$ l'inverse de x et nx au lieu de x^n.
Ces notations ne sont pas généralement source de confusion, et si un tel risque existe, le

Remarque

Noter additivement un groupe abélien n'est pas une obligation. Mais en revanche, on évitera de noter + une loi de composition qui n'est pas commutative.

contexte sera très clair (notamment dans un énoncé).

L'étude systématique des groupes, qu'on abordera à peine[8] en prépa, est en réalité un gros morceau des mathématiques du XX$^{\text{ème}}$ siècle.
Un résultat fameux est le théorème de classification des groupes finis[9] dits «simples», dont la preuve complète tient quelques milliers à quelques dizaines de milliers de pages, et surtout est trop complexe pour qu'une seule personne puisse en comprendre l'intégralité.

[8] Pas du tout en sup et guère plus en spé.

[9] C'est-à-dire de cardinal fini.

Proposition 14.23 : *Si E est un ensemble, on note $\mathfrak{S}(E)$ (ou $S(E)$) l'ensemble des bijections de E dans E.*
Alors $(\mathfrak{S}(E), \circ)$ est un groupe, non commutatif dès que E contient au moins trois éléments.
*Ce groupe est appelé **groupe symétrique sur** E, et ses éléments sont nommés **permutations** de E.*
Pour $n \in \mathbf{N}^*$, on note $\mathfrak{S}_n$ (ou S_n) le groupe symétrique sur $E = [\![1, n]\!]$.

S ou $\mathfrak{S}$?

Mais quelle est donc cette drôle de lettre ? C'est un *S* majuscule dans une écriture gothique appelée *Fraktur*, très usitée en Allemagne au XIX$^{\text{ème}}$ et au début du XX$^{\text{ème}}$, époque où l'école mathématique allemande s'est montrée très prolifique, et à qui nous devons un certain nombre de notations.
Par ailleurs, vous avez certainement déjà rencontré cette écriture : elle est intensivement utilisée dans *Astérix et les Goths.*

Démonstration. Il est clair que $\circ$ est une loi de composition interne sur $\mathfrak{S}(E)$, la composée de deux bijections étant encore une bijection.
La composition des applications est toujours associative, et id_E est clairement l'élément neutre pour $\circ$.
Enfin, pour $\sigma \in \mathfrak{S}(E)$, la bijection réciproque σ^{-1} de σ est bien l'inverse de σ, puisque, par définition, $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id}_E$.
Donc $(\mathfrak{S}(E), \circ)$ est bien un groupe.

Si E contient au moins trois éléments distincts x, y et z, notons $f : E \to E$ l'application qui échange x et y et laisse fixe tous les autres éléments de E, et notons de même g la bijection qui permute y et z.
Les deux applications f et g sont bijectives, car $f \circ f = \mathrm{id}_E$ et $g \circ g = \mathrm{id}_E$.
Or, $(f \circ g)(x) = f(x) = y$ et $(g \circ f)(x) = g(y) = z$, donc $f \circ g \neq g \circ f$.
On en déduit donc que $\mathfrak{S}(E)$ n'est pas commutatif. □

Exercice

Prouver qu'en revanche, si E est de cardinal 1 ou 2, alors $\mathfrak{S}(E)$ est commutatif.

Par abus de langage, s'il n'y a pas de confusion possible sur la loi, on dit que G est un groupe (au lieu de «$(G, *)$ est un groupe»).
Généralement, la loi d'un groupe est notée multiplicativement, et on note xx' le produit de x et x' (plutôt que $x \times x'$, $x * x'$, etc).
Pour le groupes commutatifs, on préfère généralement utiliser la notation additive : $x + x'$.
Et dans ce cas, pour $x \in G$ et $n \in \mathbf{Z}$, on note $n \cdot x$ (ou tout simplement nx) au lieu de x^n.

Notons également que tout ce qui a été dit sur l'inverse dans un ensemble muni d'une loi de composition associative et admettant un élément neutre reste valable dans un groupe.
Si $(G, \cdot)$ est un groupe, alors pour tout $g \in G$, l'application $f_g : \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & g \cdot x \end{array} \right.$ est bijective.
En effet, si $g \cdot x = g \cdot y$, alors après multiplication par g^{-1}, il vient $x = y$, donc f_g est injective.
Et pour $y \in G$, on a $y = gg^{-1}x = f_g(g^{-1}x)$, donc f_g est surjective.
De même, $x \mapsto xg$ est bijective.
Ceci signifie que dans la table de multiplication d'un groupe fini, sur chaque ligne et chaque colonne se trouve une et une seule fois chaque élément.

Exemple 14.24 **Groupes de cardinal 2 et 3**

Soit $E = \{e, a\}$ un groupe à deux éléments, d'élément neutre e. Alors sa table de multiplication est nécessairement donnée par

	e	a
e	e	a
a	a	e

De même, si $G = \{e, a, b\}$ est un groupe de cardinal 3 et d'élément neutre e, alors

sa table de multiplication est :

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Notons que nous connaissons déjà cette table : c'est celle de $\mathbf{U}_3 = \{1, j, j^2\}$ muni de la multiplication :

	1	j	j^2
1	1	j	j^2
j	j	j^2	$j^3 = 1$
j^2	j^2	1	$j^4 = j$

Définition 14.25 – Soient $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes. Alors, on définit une loi de composition interne $*$ sur $G_1 \times G_2$ en posant

$$\forall (g_1, g_2) \in G_1 \times G_2,\ \forall (g_1', g_2') \in G_1 \times G_2,\ (g_1, g_2) * (g_1', g_2') = (g_1 \star_1 g_1', g_2 \star_2 g_2').$$

Proposition 14.26 : *Muni de la loi de composition ci-dessus, $G_1 \times G_2$ est un groupe, qu'on appelle* ***produit direct de*** G_1 ***et*** G_2.
De plus, $(G_1 \times G_2, *)$ est abélien si et seulement si $(G_1, \star_1)$ et $(G_2, \star_2)$ le sont.

Démonstration. Soit $(x_1, x_2), (y_1, y_2)$ et (z_1, z_2) trois éléments de $G_1 \times G_2$. Alors □

14.2.2 Sous-groupe

Définition 14.27 – 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.

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

A priori, pour prouver qu'une partie H de G est un sous-groupe, il faudrait de nouveau prouver les trois axiomes définissant un groupe (et notamment l'associativité, qui est généralement de loin le moins plaisant des trois). Les propositions qui suivent nous disent qu'on peut faire mieux :

Proposition 14.28 : *Soit $(G, *)$ un groupe et $H \subset G$. Alors H est un sous-groupe de G si et seulement si :*

1. $\forall (h, h') \in H^2,\ h * h' \in H$
2. $e_G \in H$
3. $\forall h \in H,\ h^{-1} \in H$.

Terminologie
On dit que H est stable par passage à l'inverse.

Démonstration. $\boxed{\Rightarrow}$ Supposons que H soit un sous-groupe de G.
Alors par définition, H est stable pour le produit, donc le point 1) est évident.
De plus, H possède un élément neutre e_H. La définition ne demande pas à ce qu'il s'agisse de l'élément neutre de e_G, mais en réalité, puisque $e_H \in G$, $e_H * e_G = e_H$.
D'autre part, e_H étant élément neutre de H, $e_H * e_H = e_H = e_G * e_H$. Et donc par régularité de e_H, $e_G = e_H$.

De même, si $h \in H$, alors h possède un inverse $h' \in H$, qui est donc nécessairement un inverse de h dans le groupe G, puisqu'il vérifie $h * h' = h' * h = e_G$.
Mais un tel inverse est unique dans G, donc $h^{-1} = h' \in H$.

$\boxed{\Leftarrow}$ Réciproquement, si H satisfait aux conditions 1), 2) et 3), montrons que c'est un sous-groupe de G.

La condition 1) traduit la stabilité de H pour la loi $*$.
L'associativité de loi loi $*$ restreinte à H est évidente.
Si $e_G \in H$, alors on a toujours, $\forall h \in H$, $e_G * h = h * e_G = h$, et donc e_G est l'élément neutre de H.
Enfin, pour tout $h \in H$, l'élément h^{-1}, qui est bien dans H vérifie $h * h^{-1} = h^{-1} * h = e_G$, et donc h est inversible.
Ainsi, H satisfait bien à toutes les hypothèse de groupe. □

Remarque. On peut remplacer la condition $e_G \in H$ par «H non vide».
En effet dans ce cas, si les deux points 1) et 3) sont vérifiés, alors dès que H contient un élément h, il contient aussi h^{-1} et donc $hh^{-1} = e$.
Sauf qu'en pratique, pour prouver qu'une partie est non vide, le plus simple est de prouver qu'elle contient e_G (qui appartient donc à tous les sous-groupes de G).

On peut donner un énoncé un peu plus court, mais en pratique pas beaucoup plus facile à utiliser :

Corollaire 14.29 (Caractérisation des sous-groupes) : *Soit G un groupe et $H \subset G$. Alors H est un sous-groupe de G si et seulement si :*

1. *H est non vide*
2. *$\forall (x, y) \in H^2$, $x * y^{-1} \in H$.*

Méthode
En général, pour prouver que H est non vide, le plus simple est de prouver qu'il contient e_G, qui doit appartenir à tout sous-groupe.

Démonstration. Si H est un sous-groupe de G, alors il est non vide car $e_G \in H$ et pour tout $(x, y) \in H^2$, $y^{-1} \in H$ et donc $x * y^{-1} \in H$.

Inversement, supposons que les points 1) et 2) sont vérifiés.
Soit alors $h \in H$. Alors en prenant $(x, y) = (h, h)$, on a $h * h^{-1} \in H \Leftrightarrow e_G \in H$.
Et par conséquent, en prenant $(x, y) = (e_G, h)$, il vient $e_G * h^{-1} \in H \Leftrightarrow h^{-1} \in H$. Ainsi, H est stable par passage à l'inverse.
Enfin, pour $h, h' \in H$, en prenant $(x, y) = (h, h'^{-1})$, il vient $h * \left(h'^{-1}\right)^{-1} = h * h' \in H$. Et donc H est stable par produit.
Par la proposition précédente, H est un sous-groupe de G. □

Exemples 14.30

- $\{-1, 1\}$ est un sous-groupe de $(\mathbf{R}^*, +)$.
- $\mathbf{R}_+^*$ est un sous-groupe de $(\mathbf{R}^*, \times)$ puisque le produit de deux réels strictement positifs est strictement positif, et que l'inverse d'un réel strictement positif est strictement positif. En revanche, $\mathbf{R}_-^*$ n'est pas un sous-groupe de $(\mathbf{R}^*, \times)$.
- $\mathbf{U} = \{z \in \mathbf{C} \mid |z| = 1\}$ est un sous-groupe de $(\mathbf{C}^*, \times)$.
- Pour tout $n \in \mathbf{N}^*$, $\mathbf{U}_n = \{z \in \mathbf{C} \mid z^n = 1\}$ est un sous-groupe de $(\mathbf{C}^*, \times)$.
- $(\mathbf{Z}, +)$ est un sous-groupe de $(\mathbf{R}, +)$.
- $U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbf{K} \right\}$ est un sous-groupe de $GL_2(\mathbf{K})$.
  En effet, le produit de deux matrices triangulaires à coefficients diagonaux égaux à 1 est encore triangulaire, à coefficients diagonaux égaux à 1, et de même pour l'inverse.

De manière générale, si on vous demande de prouver qu'un ensemble est un groupe, commencez par vous demander s'il n'aurait pas le bon goût d'être un sous-groupe d'un groupe déjà connu. Il est bien plus rapide de prouver les trois points qui caractérisent un sous-groupe que ceux qui caractérisent un groupe.

Proposition 14.31 : *Soit $(H_i)_{i \in I}$ une famille[10] de sous-groupes de $(G, \cdot)$. Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.*

[10] Finie ou infinie.

Démonstration. Puisque l'élément neutre e_G de G est dans chaque sous-groupe, $e_G \in \bigcap_{i\in I} H_i$.

Soient alors $x, y \in \bigcap_{i\in I} H_i$. Alors pour tout $i \in I$, $x \in H_i$ et $y \in H_i$.

Puisque H_i est un sous-groupe, $x \cdot y \in H_i$, et ceci étant vrai pour tout $i \in I$, $x \cdot y \in \bigcap_{i\in I} H_i$.

De même, chacun des H_i étant stable par passage à l'inverse, $\forall i \in I$, $x^{-1} \in \bigcap_{i\in I} H_i$.

Et donc $\bigcap_{i\in I} H_i$ est un sous-groupe de G. □

Définition 14.32 – Soit G un groupe, et soit $g \in G$. Alors $\langle g\rangle = \{g^n,\ n \in \mathbf{Z}\}$ est un sous-groupe de G, qu'on appelle **sous-groupe engendré par g.**

Démonstration. Déjà, $\langle g\rangle$ est non vide puisqu'il contient $g = g^1$ et $e = g^0$.
De plus, si n et k sont deux entiers, de sorte que g^n et g^k sont deux éléments de G, alors $g^n \cdot (g^k)^{-1} = g^n \cdot g^{-k} = g^{n-k} \in \langle g\rangle$.
Donc $\langle g\rangle$ est bien un sous-groupe de G. □

Proposition 14.33 : *Soit $g \in G$. Alors $\langle g\rangle$ est le plus petit[11] sous-groupe de G qui contient g : si H est un sous-groupe de G qui contient G, alors $\langle g\rangle \subset H$.*
Mieux : $\langle g\rangle = \bigcap_{\substack{H \text{sous-groupe de } G \\ g\in H}} H$.

[11] Au sens de l'inclusion.

Démonstration. Soit H un sous-groupe de G contenant g. Alors $g^2 = g \cdot g \in H$, puis $g^3 = g^2 \cdot g \in H$, et une récurrence facile prouve que pour tout $n \in \mathbf{N}$, $g^n \in H$.
Et donc par passage à l'inverse, pour tout $n \in \mathbf{Z}$, $g^n \in H$.
Donc $\langle g\rangle \subset H$.

Puisque $\bigcap_{\substack{H \text{ sous-groupe de } G \\ g\in H}} H$ est un sous-groupe de G, et qu'il contient g par définition, alors il contient $\langle g\rangle$.
Mais $\langle g\rangle$ est lui-même un sous-groupe contenant g, donc est inclus dans $\bigcap_{\substack{H \text{ sous-groupe de } G \\ g\in H}} H$ puisqu'il s'agit de l'un des ensembles dont on prend l'union. □

14.2.3 Morphismes de groupes

Définition 14.34 – Soient $(G_1, \star), (G_2, \cdot)$ deux groupes. On appelle morphisme du groupe G_1 dans le groupe G_2 (ou plus simplement morphisme de G_1 dans G_2) toute application $\varphi : G_1 \to G_2$ telle que :

$$\forall (g, g') \in G_1^2,\ \varphi(g \star g') = \varphi(g) \cdot \varphi(g').$$

Autrement dit, un morphisme est une application qui préserve la structure de groupe.

Exemples 14.35

- Pour tout groupe G, id_G est un morphisme de G dans lui-même.
- Si G_1 et G_2 sont deux groupes, alors l'application constante égale à e_{G_2} est un morphisme de G_1 dans G_2.
- Le logarithme népérien réalise un morphisme de $(\mathbf{R}_+^*, \times)$ vers $(\mathbf{R}, +)$. De même, exp réalise un morphisme de $(\mathbf{R}, +)$ dans $(\mathbf{R}_+^*, \times)$.

► L'application det : $GL_2(\mathbf{K}) \to \mathbf{K}^*$ est un morphisme.

► Pour tout groupe G et pour tout $g \in G$, $\varphi_g : \left|\begin{array}{ccc} \mathbf{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}\right.$ est un morphisme de $(\mathbf{Z}, +)$ dans G.

Proposition 14.36 : *Soient $(G_1, *)$ et $(G_2, \cdot)$ deux groupes, et soit $\varphi : G_1 \to G_2$ un morphisme de groupes. Alors :*

1. $\forall n \in \mathbf{N}, \forall (g_1, g_2, \cdots, g_n) \in G_1^n, \varphi(g_1 * g_2 * \cdots * g_n) = \varphi(g_1) \cdot \cdots \cdot \varphi(g_n)$
2. $\varphi(e_{G_1}) = e_{G_2}$
3. $\forall g \in G_1, \varphi\left(g_1^{-1}\right) = \varphi(g_1)^{-1}$.

Démonstration.

1. Par récurrence sur n.
2. On a $\varphi(e_{G_1}) = \varphi(e_{G_1} * e_{G_1}) = \varphi(e_{G_1}) \cdot \varphi(e_{G_1})$.
   Et donc en simplifiant[12] par $\varphi(e_{G_1})$, il vient $e_{G_2} = \varphi(e_{G_1})$.
3. Soit $g \in G_1$. Alors
$$\varphi(g) \cdot \varphi\left(g^{-1}\right) = \varphi\left(g * g^{-1}\right) = \varphi(e_{G_1}) = e_{G_2}.$$
   Et donc $\varphi\left(g^{-1}\right)$ est l'inverse de $\varphi(g)$.

□

[12] Tout élément de G_2 est régulier.

Proposition 14.37 : *Soient $(G_1, *), (G_2, \star)$ et $(G_3, \cdot)$ trois groupes.*
Si $f : G_1 \to G_2$ et $g : G_2 \to G_3$ sont deux morphismes, alors $g \circ f$ est un morphisme de G_1 dans G_3.

Démonstration. Soient $x, y \in G_1$. Alors

$$(g \circ f)(x * y) = g(f(x * y)) = g(f(x) \star f(y)) = g(f(x)) \cdot g(f(y)) = (g \circ f)(x) \cdot (g \circ f)(y).$$

□

Définition 14.38 – Soit φ un morphisme de groupes entre $(G_1, *)$ et $(G_2, \cdot)$. On appelle alors **noyau de** φ et on note $\operatorname{Ker}\varphi$ la partie de G_1 définie par

$$\operatorname{Ker}\varphi = \{g \in G_1 \mid \varphi(g) = e_{G_2}\} = \varphi^{-1}\left(\{e_{G_2}\}\right).$$

Notons que puisque $\varphi(e_{G_1}) = e_{G_2}$, le noyau d'un morphisme de groupe n'est jamais vide, et contient toujours l'élément neutre de G_1.

Étymologie
La notation Ker vient de l'allemand *Kern* (noyau) et pas de l'anglais *kernel* (noyau également).

Proposition 14.39 : *Soit φ un morphisme entre deux groupes $(G_1, *)$ et $(G_2, \cdot)$. Alors φ est injectif si et seulement si* $\operatorname{Ker}\varphi = \{e_{G_1}\}$.

Démonstration. Si φ est injectif, alors e_{G_2} possède au plus un antécédent par φ.
Mais e_{G_1} est un tel antécédent, donc il est le seul : $\operatorname{Ker}\varphi = \{e_{G_1}\}$.
Inversement, supposons que $\operatorname{Ker}\varphi = \{e_{G_1}\}$, et soient $g, h \in G_1$ tels que $\varphi(g) = \varphi(h)$.
Alors $\varphi(g)\varphi(h)^{-1} = e_{G_2} \Leftrightarrow \varphi(g)\varphi\left(h^{-1}\right) = e_{G_2} \Leftrightarrow \varphi\left(gh^{-1}\right) = e_{G_2}$.
Don $gh^{-1} \in \operatorname{Ker}\varphi$. Par conséquent, $gh^{-1} = e_{G_1} \Rightarrow g = h$.
Et donc φ est injective. □

Remarque. Ce résultat est très fort : il dit qu'un morphisme de groupe est injectif si et seulement si l'élément neutre de G_2 possède au plus un[13] antécédent. Et donc il n'est pas nécessaire de vérifier que tout élément possède un unique antécédent, il suffit de le faire pour e_{G_2}.

[13] Et donc un unique.

Proposition 14.40 : *Si $f : G_1 \to G_2$ est un morphisme de groupes bijectif, alors $f^{-1} : G_2 \to G_1$ est également un morphisme de groupe.*

Démonstration. Soient $(y_1, y_2) \in G_2^2$, et soient $x_1 = \varphi^{-1}(y_1)$ et $x_2 = \varphi^{-1}(y_2)$.
Alors $\varphi(x_1 * x_2) = \varphi(x_1) \cdot \varphi(x_2) = y_1 \cdot y_2$.
Donc $x_1 * x_2 = \varphi^{-1}(y_1 \cdot y_2)$, de sorte que $\varphi^{-1}(y_1 \cdot y_2) = \varphi^{-1}(y_1) * \varphi^{-1}(y_2)$.
Donc φ^{-1} est bien un morphisme de $(G_2, \cdot)$ dans $(G_1, *)$. □

Définition 14.41 – Un morphisme de groupes bijectif est appelé un **isomorphisme**.

On dit que deux groupes G_1 et G_2 sont isomorphes lorsqu'il existe un isomorphisme de G_1 dans G_2 (ou, ce qui revient au même par la proposition précédente, un isomorphisme de G_2 dans G_1).
Nous savons déjà ce que signifie la bijectivité : qu'à tout élément de G_1 correspond un unique élément de G_2, autrement dit que nous sommes face aux «mêmes ensembles», une bijection étant juste un moyen de changer le nom des éléments de G_1.
L'aspect morphisme nous dit alors que la structure de groupe est préservée par la bijection, c'est-à-dire que si dans la table de multiplication de G_2, on «renumérote» les éléments de G_2 à l'aide des éléments de G_1, alors on obtient la table de multiplication de G_1.

Exemples 14.42

Dans $\mathfrak{S}_3$, soit σ définie par $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$.
Alors $\sigma^2(1) = 3$, $\sigma^2(3) = 2$ et $\sigma^2(1) = 3$, puis $\sigma^3 = \mathrm{id}$. En particulier, $\sigma - 1 = \sigma^2$.
Alors $\langle\sigma\rangle = (\mathrm{id}, \sigma, \sigma^2)$ est un sous-groupe de $\mathfrak{S}_3$.

Sa table est donnée par

$\circ$	id	σ	σ^2
id	id	σ	σ^2
σ	σ	σ^2	id
σ^2	σ^2	id	σ

C'est celle de $\mathbf{U}_3$, où on remplace 1 par id, j par σ et j^2 par σ^2.
Autrement dit, l'application $f : \langle\sigma\rangle \to \mathbf{U}_3$ définie par $f(\mathrm{id}) = 1$, $f(\sigma) = j$ et $f(\sigma^2) = j^2$ est un isomorphisme de $\langle\sigma\rangle$ sur $\mathbf{U}_3$. Lorsqu'on a dit qu'il n'y avait pas de choix pour la table de multiplication d'un groupe de cardinal 2 ou 3, nous avons en fait prouvé[14] que deux groupes de cardinal 2 (ou deux groupes de cardinal 3) sont toujours isomorphes. Ou encore qu'«à isomorphisme près, il n'y a qu'un groupe de cardinal 2 (ou de cardinal 3)».

Terminologie
Un tel σ est appelé permutation circulaire.

[14] Ou presque prouvé, mais nous n'écrirons pas les détails.

14.3 Anneaux

Définition 14.43 – Un anneau $(A, +, \times)$ est un ensemble A muni de deux lois de composition internes, notées + et × telles que :

1. $(A, +)$ est un groupe commutatif[15], dont l'élément neutre est noté 0_A
2. la loi × est associative et possède un élément neutre noté 1_A
3. × est distributive sur +

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

[15] En particulier, + est associative et commutative.

Remarque
Certaines conventions n'imposent pas l'existence d'un neutre pour la multiplication, et appellent anneau unitaire ce que nous appelons anneau. Le programme de MPSI est clair : pour nous, un anneau possède un élément neutre pour ×.

En pratique, il y a donc un certain nombre de propriétés à vérifier pour prouver qu'un ensemble A muni de deux lois de composition internes + et · est un anneau :

1. $\forall (x, y, z) \in A^3$, $(x + y) + z = x + (y + z)$ (associativité de l'addition)
2. $\forall (x, y) \in A^2$, $x + y = y + x$ (commutativité de l'addition)
3. $\exists 0_A \in A$, $\forall x \in A$, $x + 0_A = x$ (existence d'un élément neutre pour l'addition)

4. $\forall x \in A, \exists y \in A, x + y = 0_A$ (existence d'un inverse pour l'addition)
5. $\forall (x, y, z) \in A^3, x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (associativité de la multiplication)
6. $\exists 1_A \in A, \forall x \in A, x \cdot 1_A = 1_A \cdot x = x$ (existence d'un élément neutre pour la multiplication)
7. $\forall (x, y, z) \in A^3, x \cdot (y + z) = x \cdot y + x \cdot z$ et $(x + y) \cdot z = x \cdot z + y \cdot z$ (distributivité)

Exemples 14.44

► L'ensemble $\{0\}$, muni des seules lois qu'on peut lui mettre est un anneau, appelé **anneau nul**.
► $(\mathbf{Z}, +, \times)$, $(\mathbf{Q}, +, \times)$, $(\mathbf{R}, +, \times)$ et $(\mathbf{C}, +, \times)$ sont des anneaux commutatifs.
► $(\mathcal{M}_n(\mathbf{K}), +, \times)$ est un anneau, non commutatif si $n \geqslant 2$.

⚠ Attention aux notations : si $a \in A$ et $n \in \mathbf{N}$, alors na désigne l'élément $\underbrace{a + a + \cdots + a}_{n \text{ fois}}$, alors que a^n désigne l'élément $\underbrace{a \cdot a \times \cdots \times a}_{n \text{ fois}}$.
Enfin, pour $n \in \mathbf{Z} \setminus \mathbf{N}$, na désigne l'élément $\underbrace{-a + (-a) + \cdots + (-a)}_{|n| \text{ fois}}$ et a^n n'est défini que si a possède un inverse pour le produit, et dans ce cas, $a^n = \left(a^{-1}\right)^{|n|}$, où a^{-1} désigne l'inverse de a pour le produit (l'inverse de a pour la somme, appelé opposé de a, étant noté $-a$).

Proposition 14.45 (Règles de calcul dans un anneau) : *Soit $(A, +, \cdot)$ un anneau, et soient $a, b, c \in A$. Alors :*

1. $x \cdot 0_A = 0_A \cdot x = 0_A$
2. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.
3. *Plus généralement, pour tout $n \in \mathbf{Z}$, $a \cdot (nb) = (na) \cdot b = n(a \cdot b)$.*

Démonstration.
1. On a $a \cdot 0_A + a \cdot 0_A = a \cdot (0_A + 0_A) = a \cdot 0_A$.
Donc en simplifiant par $a \cdot 0_A$ il reste $a \cdot 0_A = 0_A$.
2. On a $a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot 0_A = 0_A$, donc $a \cdot (-b)$ est l'opposé[16] de $a \cdot b$, donc égal à $-(a \cdot b)$.
On prouve de même l'autre égalité.
3. Si $n \in \mathbf{N}$, on a
$$a \cdot (nb) = a \cdot (b + \cdots + b) = (a \cdot b) + (a \cdot b) + \cdots + (a \cdot b) = n(a \cdot b).$$
Et de même, $(na) \cdot b = (a + a + \cdots + a) \cdot b = (a \cdot b) + \cdots + (a \cdot b) = n(a \cdot)$.
Et si $n < 0$, alors par définition, $a \cdot (nb) = a \cdot (\underbrace{(-n)}_{\in \mathbf{N}}(-b)) = -n(a \cdot (-b)) = n(a \cdot b)$.
□

Simplification
Cette simplification est possible car $(A, +)$ est un groupe. Donc il s'agit de la proposition 14.14.

[16] C'est-à-dire l'inverse pour la loi $+$.

Remarque. Dans la définition d'anneau, rien n'empêche 1_A et 0_A d'être égaux.
Cela dit, si c'est le cas, on a, pour tout $a \in A$, $a \cdot 0_A = 0_A$ comme nous venons de le montrer, mais également $a \cdot 0_A = a \cdot 1_A = a$, de sorte que $a = 0_A$.
Autrement dit, un tel anneau est nécessairement l'anneau nul qui, soyons honnêtes, n'est pas très intéressant.

Proposition 14.46 : *Soit $(A, +, \cdot)$ un anneau, et soient $a, b \in A$ deux éléments de A tels que $ab = ba$ (on dit que a et b commutent). Alors, pour $n \in \mathbf{N}$, on a :*

1. $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ *(formule du binôme de Newton)*
2. $a^n - b^n = (a - b) \cdot \sum_{k=0}^{n-1} a^k b^{n-k-1}$.

Démonstration. Les preuves sont exactement les mêmes que dans **C**. □

Commutativité
Pour bien comprendre en quoi la commutativité de a et b est importante, vous pouvez regarder les preuves données dans le cas de $\mathcal{M}_n(\mathbf{K})$ (en cours pour le binôme, en TD pour la seconde).

14.3.1 Sous-anneau

Définition 14.47 – Soit $(A,+,\cdot)$ un anneau et soit B une partie non vide de A.. On dit que B est un sous-anneau de A si B est stable à la fois pour $+$ et pour $\cdot$, et que $(B,+,\cdot)$ est un anneau.

Proposition 14.48 : *Une partie B d'un anneau $(A,+,\cdot)$ est un sous-anneau de A si et seulement si :*

1. $1_A \in B$
2. $\forall (x,y) \in B^2,\ x-y \in B$
3. $\forall (x,y) \in B^2,\ x\cdot y \in B$.

Démonstration. Très similaire à celle de sous-groupe. Notons d'ailleurs que les deux premiers points garantissent que $(B,+)$ est un sous-groupe de $(A,+)$. □

Exemples 14.49

► L'ensemble $2\mathbf{Z}$ des nombres pairs n'est pas un sous-anneau de $\mathbf{Z}$. Bien qu'il en soit un sous-groupe et qu'il soit stable par multiplication, il ne contient pas le neutre multiplicatif de $\mathbf{Z}$, qui est 1.
► $\mathbf{Q}(\sqrt{2}) = \{a+b\sqrt{2},\ (a,b)\in\mathbf{Q}^2\}$ est un sous-anneau de $\mathbf{R}$.
En effet, $1 = 1+0\cdot\sqrt{2} \in \mathbf{Q}(\sqrt{2})$, si $x = a+b\sqrt{2}$ et $y = c+d\sqrt{2}$ sont deux éléments de $\mathbf{Q}(\sqrt{2})$ (avec $a,b,c,d\in\mathbf{Q}$), alors $x-y = (a-c)+\sqrt{2}(b-d) \in \mathbf{Q}(\sqrt{2})$.
Et de même, $xy = (a+b\sqrt{2})(c+d\sqrt{2}) = \underbrace{ac+2bd}_{\in\mathbf{Q}} + \underbrace{(bc+ad)}_{\in\mathbf{Q}}\sqrt{2} \in \mathbf{Q}(\sqrt{2})$

14.3.2 Un exemple fondamental

Soit $(A,+,\cdot)$ un anneau et soit E un ensemble.
Alors, sur l'ensemble $\mathcal{F}(E,A) = A^E$ des fonctions de E dans A, on définit deux lois de composition internes, encore notées $+$ et $\cdot$, de la manière suivante :

- $\forall x\in E,\ (f+g)(x) = f(x)+g(x)$
- $\forall x\in E,\ (f\cdot g)(x) = f(x)\cdot g(x)$.

Proposition 14.50 : *Muni des deux opérations $+$ et $\cdot$, $\mathcal{F}(E,A)$ est un anneau, commutatif si et seulement si A l'est.*

Démonstration. ► L'associativité des deux lois découle assez facilement de l'associativité des lois de A.
Ainsi, pour f,g,h dans $\mathcal{F}(E,A)$, on a, pour tout $x\in E$,

$$((f+g)+h)(x) = (f+g)(x)+h(x) = (f(x)+g(x))+h(x) = f(x)+(g(x)+h(x)) = (f+(g+h))(x).$$

Ceci étant vrai pour tout $x\in E$, $f+(g+h) = (f+g)+h$.
De même, l'addition dans $\mathcal{F}(E,A)$ est commutative car l'addition de A l'est.
► La fonction nulle $\widetilde{0}$, définie par : $\forall x\in E,\ \widetilde{0}(x) = 0_A$ est élément neutre pour l'addition car pour $f\in\mathcal{F}(E,A)$, et pour tout $x\in E$,

$$(f+\widetilde{0})(x) = f(x)+\widetilde{0}(x) = f(x)+0_A = f(x)$$

et donc $f+\widetilde{0} = f$.
On prouve de même que la fonction constante égale à 1_A, notée $\widetilde{1}$ est l'élément neutre

pour la multiplication.
► L'inverse de f pour l'addition est la fonction $-f : x \mapsto -(f(x))$ puisque $\forall x \in E$,

$$(f + (-f))(x) = f(x) + (-f(x)) = f(x) - f(x) = 0_A = \widetilde{0}(x)$$

et donc $f + (-f) = \widetilde{0}$.
► Enfin, pour $f, g, h \in \mathcal{F}(E, A)$, et pour $x \in E$, on a

$$(f \cdot (g + h))(x) = f(x) \cdot (g(x) + h(x)) = f(x) \cdot g(x) + f(x) \cdot h(x) = (f \cdot g + f \cdot h)(x)$$

de sorte que $f \cdot (g + h) = f \cdot g + f \cdot h$.
On prouve de même que $(f + g) \cdot h = f \cdot h + g \cdot h$. □

Notons que ce résultat ne suppose aucune hypothèse sur l'ensemble de départ E, seul l'ensemble d'arrivée doit être muni d'une structure d'anneau[17].
En particulier, les ensembles $\mathcal{F}(I, \mathbf{R})$, $\mathcal{F}(I, \mathbf{C})$, où I est un intervalle, ainsi que les ensembles de suites $\mathbf{R}^{\mathbf{N}}$ et $\mathbf{C}^{\mathbf{N}}$.
L'intérêt de ce résultat est qu'il évite bien souvent de prouver qu'un ensemble de suites ou de fonctions est un anneau en vérifiant tous les points de la définition. En effet, on peut se contenter de prouver qu'il s'agit d'un sous-anneau d'un anneau de référence, ce qui demande bien moins d'efforts que de prouver de nouveau toutes les propriétés définissant un anneau.

[17] En général, on l'utilisera avec $A = \mathbf{R}$ ou $A = \mathbf{C}$.

Exemple 14.51

L'ensemble des suites convergentes est un sous-anneau de $\mathbf{R}^{\mathbf{N}}$.
En effet, la suite constante égale à 1 est convergente, la différence de deux suites convergentes est convergente, et le produit de deux suites convergentes est convergente.

14.3.3 Diviseurs de zéro

Définition 14.52 – Soit A 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 $a \cdot b = 0_A$ ou $b \cdot a = 0_A$.

Remarque. Un diviseur de zéro est un élément qui viole la sacro-sainte règle apprise à la maternelle : «un produit est nul si et seulement si l'un de des facteurs est nul».
Bien entendu, cette règle reste valable dans l'anneau $(\mathbf{R}, +, \times)$, ainsi que dans l'anneau $(\mathbf{C}, +, \times)$ (autrement dit dans le cadre où vous l'avez apprise), mais ne découle pas directement des axiomes définissant un anneau.

Exemple 14.53

Plaçons nous dans l'anneau $\mathbf{R}^{\mathbf{N}}$ des suites réelles.
Soit alors $(u_n)_{n\in\mathbf{N}}$ la suite définie par $\forall n \in \mathbf{N}$, $u_n = n$, et soit (v_n) la suite définie par

$$v_n = \begin{cases} 1 & \text{si } n = 0 \\ 0 & \text{sinon} \end{cases}$$

Alors (u_n) et (v_n) ne sont pas nulles, mais pourtant, on a $u_0 v_0 = 0 \times 1 = 0$ et pour tout $n \in \mathbf{N}^*$, $u_n v_n = n \times 0 = 0$, de sorte que $(u_n v_n)_n$ est la suite nulle.
Et donc $(u_n)_n$ et $(v_n)_n$ sont deux diviseurs de zéro.

Définition 14.54 – Un anneau commutatif A est dit **intègre** si il est non nul et ne possède pas de diviseurs de zéro.
Autrement dit si $A \neq \{0_A\}$ et si

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

Exemples 14.55

► $(\mathbf{C}, +, \times)$ et tous ses sous-anneaux $(\mathbf{R}, \mathbf{Q}, \mathbf{Z})$ sont intègres.
► $\mathcal{M}_n(\mathbf{K})$ n'est pas intègre si $n \geqslant 2$, car il existe des matrices nilpotentes[18], qui sont des diviseurs de zéro.

[18] Par exemple celle qui a des zéros partout et un 1 en haut à droite.

14.3.4 Éléments inversibles

Définition 14.56 – Soit $(A, +, \cdot)$ un anneau. On dit que $a \in A$ est inversible s'il possède un inverse pour la loi $\cdot$, c'est-à-dire s'il existe $b \in A$ tel que $a \cdot b = b \cdot a = 1_A$. L'ensemble des éléments inversibles de A se note $A^\times$, ou encore $U(A)$ (on parle parfois d'unités au lieu d'inversibles).

Exemples 14.57

► 1_A est toujours inversible, de sorte que $\{1_A\} \subset A^\times$.
► En revanche, si A n'est pas l'anneau nul, alors 0_A n'est pas inversible (car $a \cdot 0_A = 0_A$ ne peut jamais être égal à 1_A), et donc $A^\times \subset A \setminus \{0\}$.
► Dans $(\mathbf{Z}, +, \times)$, les seuls inversibles sont 1 et -1.

Proposition 14.58 : *Si $a \in A$ est inversible, alors a n'est pas un diviseur de zéro.*

Démonstration. Si $b \in A$ est tel que $a \cdot b = 0_A$, alors en multipliant à gauche par a^{-1}, il vient $a^{-1} \cdot a \cdot b = a^{-1} \cdot 0_A \Leftrightarrow b = 0_A$.
Et de même, si $b \cdot a = 0_A$, alors $b = 0_A$. □

Proposition 14.59 : *Soit $(A, +, \times)$ un anneau. L'ensemble $A^\times$ des éléments inversibles de A est un groupe pour la loi $\times$.*
Ce groupe est commutatif si A est un anneau commutatif.

Démonstration. Par définition d'un anneau, la loi $\times$ est associative.
Puisque 1_A est inversible, il est bien dans $A^\times$ et donc est l'élément neutre de $A^\times$.
Enfin, par définition de $A^\times$ tout élément possède un inverse. □

14.4 Corps

Définition 14.60 – On appelle corps tout anneau commutatif dans lequel tout élément non nul est inversible.

Exemples 14.61

► $\mathbf{Q}, \mathbf{R}$ et $\mathbf{C}$, munis de leurs opérations habituelles sont des corps.
► $\{0, 1\}$, muni des lois suivantes est aussi un corps :

$+$	0	1
0	0	1
1	1	0

et

$\times$	0	1
0	0	0
1	0	1

► $\mathbf{Q}(\sqrt{2})$ est un corps. Nous avons déjà prouvé qu'il s'agit d'un anneau, reste à prouver que tout élément non nul de $\mathbf{Q}(\sqrt{2})$ possède un inverse dans $\mathbf{Q}(\sqrt{2})$.
Mais dans $\mathbf{R}$, l'inverse de $a + b\sqrt{2} \neq 0$ est $\dfrac{1}{a+b\sqrt{2}} = \dfrac{a-b\sqrt{2}}{a^2-2b^2} = \dfrac{a}{a^2-2b^2} +$

$$\sqrt{2}\left(-\frac{b^2}{a^2-2b^2}\right)) \in \mathbf{Q}(\sqrt{2}).$$

Notons en particulier que dans un corps, tout élément non nul étant inversible, il n'y a pas de diviseurs de zéro : un corps est intègre.
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 $\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$ reste valable dans un corps quelconque.