# 8 - Structures algébriques I

Jeremy Daniel

> Young man, in mathematics you don't understand things. You just get used to them.
>
> John von Neumann

## 0 Lois de composition interne

Définition 0.1 (Loi de composition interne)
Une loi de composition interne (LCI) sur un ensemble $E$ est une application $\star : E \times E \to E$.

Remarque 0.2
On note plutôt $a \star b$, au lieu de $\star(a, b)$ l'image du couple $(a, b)$ par $\star$. Quand on applique plusieurs fois l'opération $\star$, on aura recours à des parenthèses dès qu'il peut y avoir ambiguïté sur l'ordre des opérations à effectuer.

Définition 0.3 (Associativité)
Une LCI $\star$ sur $E$ est associative si $\forall x, y, z \in E, (x \star y) \star z = x \star (y \star z)$.

Remarque 0.4
Quand la loi $\star$ est associative, on peut effectuer des opérations du type $x_1 \star x_2 \star \cdots \star x_k$ dans un ordre quelconque ; on omet donc les parenthèses dans ce cas. Attention ! Il faut cependant conserver l'ordre des éléments dans l'expression.

Définition 0.5 (Élément neutre)
Une LCI $\star$ sur $E$ admet un élément neutre $e \in E$ si $\forall x \in E, x \star e = e \star x = x$.

**Proposition 0.6** (Unicité de l'élément neutre)
*Si une LCI $\star$ admet un élément neutre, celui-ci est unique.*

Définition 0.7 (Symétrique)
Soit $\star$ une LCI sur $E$, admettant un élément neutre $e$. Soit $x \in E$. On dit que

- $y \in E$ est un symétrique à droite de $x$ si $x \star y = e$.
- $y \in E$ est un symétrique à gauche de $x$ si $y \star x = e$.
- $y \in E$ est un symétrique de $x$ si c'est un symétrique et à droite de $x$.

**Proposition 0.8** (Unicité des symétriques)
*On suppose que la loi $\star$ est associative et admet un élément neutre.*
*Si $x$ admet un symétrique, celui-ci est unique.*

**Proposition 0.9** (Symétrique de $x \star y$)
*Si $\star$ admet un élément neutre et que $x$ et $y$ ont un symétrique, notés respectivement $x^s$ et $y^s$, alors $y^s \star x^s$ est le symétrique de $x \star y$.*

Définition 0.10 (Commutativité)
Une LCI $\star$ sur $E$ est commutative si $\forall x, y \in E, x \star y = y \star x$.

Remarque 0.11
Si une LCI $\star$ est associative et commutative, une expression de la forme $x_1 \star x_2 \star \cdots \star x_k$ peut être calculée en effectuant les opérations dans un ordre quelconque ET en permutant des éléments.

Définition 0.12 (Élément simplifiable)
Soit $\star$ une LCI sur $E$, soit $x \in E$. On dit que $x$ est
- simplifiable à gauche si $\forall y, z \in E, x \star y = x \star z \implies y = z$.
- simplifiable à droite si $\forall y, z \in E, y \star x = z \star x \implies y = z$.
- simplifiable s'il est simplifiable à gauche et à droite.

**Proposition 0.13** (Un élément symétrique est simplifiable)
*On suppose que la loi $\star$ est associative et admet un élément neutre. Un élément qui admet un symétrique/un symétrique à gauche/un symétrique à droite est simplifiable/simplifiable à gauche/simplifiable à droite.*

Attention !
La réciproque est fausse. Par exemple, dans $\mathbb{Z}$ muni de la LCI $\times$, 3 est un élément simplifiable mais il n'admet pas de symétrique.

Définition 0.14 (Itérés d'un élément par $\star$)
Soit $\star$ une LCI sur $E$. Soit $x \in E$. On définit récursivement les éléments $x^{\star,n}$, pour $n \in \mathbb{N}^*$ par $x^{\star,1} = x$ et $\forall n \in \mathbb{N}^*, x^{\star,n+1} = x^{\star,n} \star x$. Si $\star$ admet un élément neutre $e$, on convient de plus que $x^{\star,0} = e$.
Si $x$ admet un symétrique, noté $x^s$, on convient de plus que

$$\forall n \in \mathbb{Z} - \mathbb{N}, x^{\star,n} = (x^s)^{\star,-n}.$$

Remarque 0.15
On a alors, $\forall k, l \in \mathbb{N}^*$ (ou $\mathbb{N}$ ou $\mathbb{Z}$ suivant les cas) : $x^{\star,k} \star x^{\star,l} = x^{\star,k+l}$.

Définition 0.16 (Partie stable par une LCI)
Une partie $A \subset E$ est stable par la LCI $\star$ si $\forall x, y \in A, x \star y \in A$.

Remarque 0.17 (Convention d'écriture pour les LCI)
La plupart du temps, les LCI sont écrites $+$ ou $\times$. On dira alors que la loi est notée en convention additive ou en convention multiplicative. On dispose d'un standard de notations et un vocabulaire dans ces deux situations :

- Si la loi est notée $+$, on note généralement 0 son élément neutre (s'il existe). On parle d'opposé plutôt que de symétrique et on note $-x$ l'opposé de $x$ (s'il existe). Les itérés $x^{+,n}$ se notent simplement $nx$. Cette convention d'écriture ne s'applique en principe qu'à des LCI commutatives.
- Si la loi est notée $\times$, on note généralement 1 son élément neutre (s'il existe). On parle d'inverse plutôt que de symétrique et on note $x^{-1}$ l'inverse de $x$ (s'il existe). Les itérés $x^{\times,n}$ se notent simplement $x^n$. De plus, on omet souvent l'écriture de la loi, en écrivant $xy$ au lieu de $x \times y$. Cette convention d'écriture peut être appliquée à toutes les LCI.

L'exemple le plus important de LCI notée différemment est la composition $\circ$ entre applications. Cependant,quand il n'y a pas d'ambiguïté, on écrira cette loi en convention multiplicative ; ainsi $gf$ sera un raccourci pour $g \circ f$ et $f^n$ pourra désigner la composée itérée $n$-ème de $f$.

Exemple 0.18 (Lois de composition interne sur $\mathbb{Z}/n\mathbb{Z}$)
Soit $n \in \mathbb{N}^*$. On rappelle qu'on a défini l'ensemble $\mathbb{Z}/n\mathbb{Z}$ comme l'ensemble des classes d'équivalences de la relation d'équivalence $\mathcal{R}$ sur $\mathbb{Z}$, $\mathcal{R}$ étant définie par

$$\forall x, y \in \mathbb{Z}, x \mathcal{R} y \iff x \equiv y\,[n].$$

Pour tout $x \in \mathbb{Z}$, on note $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$ la classe d'équivalence de $x$. On a donc

- $\forall x, y \in \mathbb{Z}, \overline{x} = \overline{y} \iff x \equiv y\,[n]$ ;
- $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Dans le chapitre d'arithmétique, on a vu que la relation de congruence modulo $n$ était compatible avec les opérations $+$ et $\times$ sur $\mathbb{Z}$. On peut alors définir deux lois de composition interne $+$ et $\times$ sur $\mathbb{Z}/n\mathbb{Z}$ par : $\forall x, y \in \mathbb{Z}, \overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \times \overline{y} = \overline{xy}$.

# 1 Groupes

## 1.1 Généralités

Définition 1.1 (Groupe)
Un groupe est un couple $(G, \star)$, où $G$ est un ensemble et $\star$ est une LCI sur $G$ telle que :

- $\star$ est associative ;
- $\star$ a un élément neutre ;
- tout élément $x \in G$ admet un symétrique.

Définition 1.2 (Groupe abélien)
Un groupe $(G, \star)$ est abélien si la loi $\star$ est commutative.

Remarque 1.3
Suivant les conventions générales discutées plus haut, on notera la loi de groupe additivement quand le groupe est abélien et multiplicativement dans le cas général.

Notation 1.4
Soit $G$ un groupe, soient $A$ et $B$ deux parties de $G$, soit $x$ un élément de $G$.
- Si la loi de groupe est notée additivement, on note

$$x + A = A + x = \{x + y, y \in A\} \text{ et } A + B = \{a + b, (a, b) \in A \times B\}.$$

- Si la loi de groupe est notée multiplicativement, on note

$$xA = \{xy, y \in A\}, Ax = \{yx, y \in A\} \text{ et } AB = \{ab, (a, b) \in A \times B\}.$$

Exemples 1.5
Exemples de groupes abéliens :
- $(\mathbb{C}, +)$ ; $(\mathbb{R}, +)$ ; $(\mathbb{Z}, +)$ ;
- $(\mathbb{C}^n, +)$ ; $(\mathbb{R}^n, +)$ ; $(\mathbb{Z}^n, +)$ ;
- $(\mathbb{C}^*, \times)$ ; $(\mathbb{R}^*, \times)$ ; $(\mathbb{R}_+^*, \times)$ ;
- $(\mathbb{U}, \times)$ ; $(\mathbb{U}_n, \times)$ ;
- $(\mathbb{Z}/n\mathbb{Z}, +)$ ;
- $(\mathcal{F}(X, G), +)$, où $X$ ensemble quelconque, et $(G, +)$ groupe abélien.

Exemples de groupes non abéliens :
- $(S_E, \circ)$ (si $E$ est un ensemble, on note $S_E$ l'ensemble des permutations de $E$) ;
- $(\mathrm{GL}_n(\mathbb{R}), \times)$, $n \geq 2$ ;
- l'ensemble des similitudes de $\mathbb{C}$ (pour la composition d'applications) ;

Attention !
Les exemples suivants ne sont pas des groupes :
- $(\mathbb{N}, +)$ : un entier $n \geq 1$ n'a pas d'opposé ;
- $(\mathbb{R}, \times)$ : 0 n'a pas d'inverse ;
- $(\mathbb{R}_-^*, \times)$ ; $\times$ n'est pas une LCI puisque le produit de deux nombres strictement négatifs n'en est pas un.

**Proposition 1.6** (Produit de groupes)
*Soient $(G_1, \star_1)$ et $(G_2, \star_2)$ deux groupes.*

*Le produit cartésien $G_1 \times G_2$ est un groupe pour la loi $\star$ définie par*

$$\forall (x_1, x_2), (y_1, y_2) \in G_1 \times G_2, (x_1, x_2) \star (y_1, y_2) = (x_1 \star_1 y_1, x_2 \star_2 y_2).$$

## 1.2 Sous-groupes

Remarque 1.7
Dans un énoncé général, quand on ne précise pas la loi, il est sous-entendu qu'on adopte une convention d'écriture multiplicative.

Définition 1.8 (Sous-groupe)
Soit $G$ un groupe, d'élément neutre $e_G$. Une partie $H$ de $G$ est un sous-groupe de $G$ si
- $e_G \in H$ ;
- $\forall x, y \in H$, $xy \in H$ ;
- $\forall x \in H$, $x^{-1} \in H$.

Exercice 1.9
Montrer que $H$ est un sous-groupe de $G$ ssi $H$ est non vide et si $\forall x, y \in H, xy^{-1} \in H$.

**Théorème 1.10** (Un sous-groupe est un groupe)
*Si $H$ est un sous-groupe de $G$, alors $H$ est un groupe (avec la LCI induite), de même élément neutre.*

Exemples 1.11
- $(\mathbb{Z}, +)$ est sous-groupe de $(\mathbb{Q}, +)$, sous-groupe de $(\mathbb{R}, +)$, sous-groupe de $(\mathbb{C}, +)$.
- $(\mathbb{Z}^n, +)$ est sous-groupe de $(\mathbb{R}^n, +)$.
- $(\mathbb{R}_+^*, \times)$ est sous-groupe de $(\mathbb{R}^*, \times)$, sous-groupe de $(\mathbb{C}^*, \times)$.
- $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
- Pour tout $n \geq 1$, $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$.
- L'ensemble des similitudes de $\mathbb{C}$ est un sous-groupe de l'ensemble des permutations de $\mathbb{C}$.

**Théorème 1.12** (Caractérisation des sous-groupes de $\mathbb{Z}$)
*Les sous-groupes de $(\mathbb{Z}, +)$ sont les parties de $\mathbb{Z}$ de la forme $n\mathbb{Z}$, où $n \in \mathbb{N}$.*

**Théorème 1.13** (Caractérisation des sous-groupes de $\mathbb{R}$)
*Soit $H$ un sous-groupe de $(\mathbb{R}, +)$. On a l'alternative suivante :*
- *$\exists! a \in \mathbb{R}_+, H = a\mathbb{Z}$ ;*
- *$H$ est une partie dense de $\mathbb{R}$.*

**Proposition 1.14** (Une intersection de sous-groupes est un sous-groupe)
*Soit $G$ un groupe, 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 $G$.*

**Théorème 1.15** (Caractérisation par le haut du sous-groupe engendré par $A$)
*Soit $A$ une partie d'un groupe $G$. Il existe un plus petit (au sens de l'inclusion) sous-groupe de $G$ contenant $A$ : c'est l'intersection de tous les sous-groupes de $G$ contenant $A$.*

Définition 1.16 (Sous-groupe engendré par une partie)
Le sous-groupe précédent se note $\langle A \rangle$ ; c'est le sous-groupe de $G$ engendré par $A$.
Si $\langle A \rangle = G$, on dit que $A$ est une partie génératrice de $G$, ou que $A$ engendre $G$.

Remarque 1.17
Si $A = \{x\}$ est réduit à un élément, on note $\langle x \rangle$ le groupe engendré par $\{x\}$.

**Théorème 1.18** (Caractérisation par le bas du sous-groupe engendré par $A$)
*Soit $A$ une partie d'un groupe $G$.*

$$\langle A \rangle = \{x_1 x_2 \dots x_k,\ k \in \mathbb{N} \text{ et } \forall i \in [\![1, k]\!], x_i \in A \text{ ou } x_i^{-1} \in A.\}.$$

Exemples 1.19
- Si $A = \emptyset$, $\langle A \rangle$ est $\{e_G\}$.
- Soit $n \in \mathbb{Z}$. Dans $\mathbb{Z}$, le sous-groupe engendré par $\{n\}$ est $n\mathbb{Z}$.
- Soient $n_1, \dots, n_k \in \mathbb{Z}$. Le sous groupe engendré par $\{n_1, \dots, n_k\}$ est $(n_1 \wedge \dots \wedge n_k)\mathbb{Z}$.

## 1.3 Morphismes de groupes

Définition 1.20 (Morphisme de groupes)
Soient $(G, \star_G)$ et $(H, \star_H)$ deux groupes. Un morphisme de groupes de $G$ vers $H$ est une application $f : G \to H$ telle que

$$\forall x, y \in G, f(x \star_G y) = f(x) \star_H f(y).$$

**Proposition 1.21** (Les morphismes préservent inverse et élément neutre)
*Avec les notations précédentes, si $f$ est un morphisme :*
- $f(e_G) = e_H$ ;
- $\forall x \in G, f(x^{-1}) = f(x)^{-1}$.

Définition 1.22 (Noyau et image)
Soit $f : G \to H$ un morphisme de groupes.
- Le noyau de $f$, noté $\mathrm{Ker}(f)$, est $f^{-1}(e_H) = \{x \in G \mid f(x) = e_H\}$.
- L'image de $f$, notée $\mathrm{Im}(f)$, est $f(G)$.

**Proposition 1.23** (Noyau et image sont des sous-groupes)
*Soit $f : G \to H$ un morphisme de groupes.*

– $\mathrm{Ker}(f)$ *est un sous-groupe de* $G$*. On a* $\mathrm{Ker}(f) = \{e_G\}$ *ssi* $f$ *est injective.*
– $\mathrm{Im}(f)$ *est un sous-groupe de* $H$*. On a* $\mathrm{Im}(f) = H$ *ssi* $f$ *est surjective.*

Définition 1.24 (Endomorphisme, isomorphisme, automorphisme)
Soit $f : G \to H$ un morphisme de groupes. On dit que c'est un
– endomorphisme si $G = H$ (avec les mêmes lois de groupe) ;
– isomorphisme si c'est une application bijective ;
– automorphisme si c'est un endomorphisme et un isomorphisme.

**Proposition 1.25**
*Une composée d'isomorphismes de groupes/la bijection réciproque d'un isomorphisme de groupes est un isomorphisme de groupe.*

**Corollaire 1.26**
*L'ensemble des automorphismes d'un groupe* $G$ *est un groupe, pour la composition.*

Exercice 1.27
Montrer que $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont des groupes isomorphes. Montrer que les groupes suivants ne sont pas isomorphes :
– $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$ ;
– $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$ ;
– $(\mathbb{Z}, +)$ et $(\mathbb{Z}^2, +)$.

## 1.4 Groupes monogènes

Définition 1.28 (Groupe monogène)
Un groupe $G$ est dit monogène s'il existe $x \in G$ tel que $G = \langle x \rangle$.

**Théorème 1.29** (Caractérisation des groupes monogènes)
*Soit* $G$ *un groupe monogène.*
– *Si* $G$ *est infini,* $G$ *est isomorphe à* $\mathbb{Z}$*.*
– *Si* $G$ *est fini de cardinal* $n$*,* $G$ *est isomorphe à* $\mathbb{Z}/n\mathbb{Z}$*.*

Remarque 1.30
Dans la deuxième cas (groupe monogène fini), on dit que $G$ est cyclique.

Exemples 1.31

- Le groupe $\mathbb{U}_n$ des racines $n$-èmes de l'unité est fini de cardinal $n$ et est engendré par $\omega = e^{2i\pi/n}$. Il est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$. L'isomorphisme est donné par :

$$\phi : \left\{ \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{U}_n \\ \overline{k} & \mapsto & e^{2ik\pi/n} \end{array} \right.$$

- Dans $\mathbb{Z}/10\mathbb{Z}$, l'élément $\overline{2}$ engendre un sous-groupe $G$ de cardinal 5. Ainsi, $G$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$, l'isomorphisme étant donné par :

$$\phi : \left\{ \begin{array}{ccc} \mathbb{Z}/5\mathbb{Z} & \to & G \\ \mathrm{cl}_5(k) & \mapsto & \mathrm{cl}_{10}(2k) \end{array} \right.$$

- Les sous-groupes discrets de $\mathbb{R}$ qui ne sont pas denses sont les sous-groupes monogènes de $\mathbb{R}$. Le sous-groupe $a\mathbb{Z}$ de $\mathbb{R}$ est isomorphe à $\mathbb{Z}$.

# 2 Anneaux et corps

## 2.1 Généralités

Définition 2.1 (Anneau)
Un anneau (unitaire) est un triplet $(A, +, \times)$ où $A$ est un ensemble, $+$ et $\times$ sont des LCI sur $A$ telles que :

- $(A, +)$ est un groupe abélien ;
- La loi $\times$ est associative et a un élément neutre ;
- $\times$ est distributive par rapport à $+$ :

$$\forall x, y, z \in A, x(y+z) = xy + xz \text{ et } (y+z)x = yx + zx.$$

On dit que l'anneau est commutatif si la loi $\times$ est commutative.

Remarque 2.2
On notera systématiquement $0_A$ et $1_A$ (ou simplement 0 et 1) les éléments neutres respectifs de $+$ et $\times$.

Remarque 2.3
On peut avoir $0_A = 1_A$. Mais dans ce cas, $A$ est réduit à $\{0_A\}$.
On dit que $A$ est l'anneau nul.

**Proposition 2.4** (0 est absorbant pour $\times$)
*0 est un élément absorbant pour $\times$ :* $\forall x \in A, 0 \times x = x \times 0 = 0$.

Remarque 2.5
De façon générale, on calcule dans un anneau $A$ quelconque comme dans $\mathbb{Z}$, en prenant toutefois garde à la possible non-commutativité de $A$. Par exemple, $(-1)^2 = 1$ et

$$\forall x, y \in A, -(xy) = (-x)y = x(-y).$$

**Proposition 2.6** (Identité de Bernoulli)
*Soient $a$ et $b$ deux éléments d'un anneau $A$. Soit $n \in \mathbb{N}$.*

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

**Proposition 2.7** (Formule du binôme de Newton)
*Soient $a$ et $b$ deux éléments d'un anneau $a$. Soit $n \in \mathbb{N}$. On suppose que $ab = ba$.*

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

Exemples 2.8
On a les exemples suivants d'anneaux :
- $\mathbb{Z}$ ; $\mathbb{R}$ ; $\mathbb{C}$ ;
- l'ensemble des fonctions polynomiales à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$ (définies sur $\mathbb{R}$) ;
- $\mathcal{M}_n(\mathbb{K})$, ensemble des matrices carrées de taille $n$ à coefficients dans $\mathbb{K}$ ;
- $\mathbb{Z}/n\mathbb{Z}$.

Définition 2.9 (Anneau intègre)
Un anneau commutatif est intègre s'il est distinct de l'anneau nul et s'il satisfait :

$$\forall x, y \in A, xy = 0 \implies x = 0 \text{ ou } y = 0.$$

Remarque 2.10
La définition précédente ne s'applique pas à $\mathcal{M}_n(\mathbb{K})$, non-commutatif pour $n \geq 2$. On remarque cependant que $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_{\mathcal{M}_2(\mathbb{K})}$.
On verra plus tard que $\mathbb{Z}/n\mathbb{Z}$ est intègre ssi $n$ est premier. Remarquons par exemple, que pour $n = 6$, $\bar{2} \times \bar{3} = \bar{6} = 0_{\mathbb{Z}/6\mathbb{Z}}$.

Définition 2.11 (Élément inversible)
Soit $A$ un anneau. Un élément $x \in A$ est inversible s'il a un symétrique pour la loi $\times$ :

$$\exists y \in A, xy = yx = 1.$$

Notation 2.12
On note $A^\times$ l'ensemble des inversibles de $A$.

**Théorème 2.13** (L'ensemble des inversibles est un groupe)
*Soit $A$ un anneau. Alors, $(A^\times, \times)$ est un groupe.*

Définition 2.14 (Corps)
Un corps est un anneau commutatif $\mathbb{K}$ tel que $\mathbb{K}^\times = \mathbb{K} - \{0\}$.

Remarque 2.15
L'anneau nul n'est pas un corps.

**Proposition 2.16**
*Un corps est un anneau intègre.*

Remarque 2.17
Mais la réciproque est fausse : $\mathbb{Z}$ est intègre mais n'est pas un corps.

Exemples 2.18
- $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps ;
- $\mathbb{Z}$ n'en est pas un : 2 n'est pas inversible ;
- $\mathcal{M}_n(\mathbb{K})$ n'en est pas un si $n \geq 2$ : les matrices données dans l'exemple plus haut ne sont pas inversibles ;
- l'ensemble des applications polynomiales n'est pas un corps ; un polynôme de degré $\geq 1$ n'est pas inversible.

**Théorème 2.19**
*L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi $n$ est premier.*

Notation 2.20
Si $p$ est un nombre premier, on note souvent $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

## 2.2 Sous-anneaux et morphismes d'anneaux

Définition 2.21 (Sous-anneau)
Soit $B$ une partie d'un anneau $A$. On dit que $B$ est un sous-anneau de $A$ si
- $1_A \in B$ ;
- $(B, +)$ est un sous-groupe de $(A, +)$ ;
- $B$ est stable par $\times$.

Si $A$ est un corps, on dit que $B$ est un sous-corps de $A$.

Remarque 2.22
En pratique, pour montrer que $B$ est un sous-anneau de $A$, on montre donc qu'il contient $1_A$ et que

$$\forall x, y \in B, x - y \in B \text{ et } xy \in B.$$

**Proposition 2.23** (Un sous-anneau est un anneau.)
*Avec les lois $+$ et $\times$ induites, un sous-anneau/un sous-corps est un anneau/un corps.*

Exemples 2.24
- $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$ ;
- $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, qui est un sous-corps de $\mathbb{C}$.

Définition 2.25 (Morphisme d'anneaux)
Soient $A$ et $B$ deux anneaux. Un morphisme d'anneaux de $A$ vers $B$ est une application $f : A \to B$ telle que :

- $f(1_A) = 1_B$ ;
- $f$ est un morphisme de groupes $(A, +_A) \to (B, +_B)$ :

$$\forall x, y \in A, f(x +_A y) = f(x) +_B f(y);$$

- $\forall x, y \in A, f(xy) = f(x)f(y)$.

Si $A$ et $B$ sont des corps, on parle de morphisme de corps.

Exemples 2.26

- L'application de conjugaison $z \mapsto \overline{z}$ est un morphisme de corps de $\mathbb{C}$ dans $\mathbb{C}$ ;
- Soit $n \geq 1$ un entier. Considérons $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, définie par $\pi_n(x) = \overline{x}$ (classe de $x$ modulo $n$). Alors, par construction, $\pi_n$ est un morphisme d'anneaux ;
- Notons $A$ l'anneau des fonctions polynomiales à coefficients dans $\mathbb{K}$. Soit $x_0$ un réel. L'application $\phi : A \to \mathbb{K}$, définie par $\phi(P) = P(x_0)$ est un morphisme d'anneaux (morphisme d'évaluation en $x_0$).

**Proposition 2.27** (Un morphisme de corps est injectif)
*Si $\phi : \mathbb{K} \to \mathbb{L}$ est un morphisme de corps, alors $\phi$ est injectif.*

Définition 2.28 (Caractéristique d'un corps)
Soit $\mathbb{K}$ un corps.

- Si pour tout $n \in \mathbb{N}^*, n \times 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$, on dit que $\mathbb{K}$ est de caractéristique 0.
- Sinon, on note $n$ le plus petit entier naturel non nul tel que $n \times 1_{\mathbb{K}} = 0_{\mathbb{K}}$ et on dit que $\mathbb{K}$ est de caractéristique $n$.

**Théorème 2.29**
*La caractéristique d'un corps est* 0 *ou un nombre premier.*