Algébre 2

Filière: LE-Math

2024/2025

Définition 1.1.1 (Loi de composition interne)

Toute application $*$ de $E \times E$ dans E est appelée une loi de composition interne ou une opération dans E.
On dit que E est muni de la loi de composition interne $*$.

Exemple 1.1.2 (Premiers exemples).

1. La multiplication et l'addition usuelles sont des lois sur $\mathbb{R}$.
2. L'union et l'intersection des parties d'un ensemble A sont des lois sur l'ensemble $P(A)$ des parties de A.
3. La division (des nombres) peut être ou non une loi selon l'ensemble de nombres considéré : Elle n'est pas une loi de composition interne dans $\mathbb{Z}^*$, mais elle l'est dans $\mathbb{R}^*$ (ensemble des réels non nuls).
4. Aussi, la soustraction n'est pas une loi de composition interne dans $\mathbb{N}$, mais elle l'est dans $\mathbb{Z}$.

Définition 1.1.2 (Magma)

Si un ensemble E est muni d'une loi $*$, le couple $(E, *)$ est appelé un magma.

Par abus de langage, on peut dire simplement "le magma E " au lieu de dire "le magma $(E, *)$ " lorsqu'il n'y a pas d'ambiguité sur la loi $*$.

Définition 1.1.3 (Associativité)

Soit $(E, *)$ un magma. La loi $*$ est dite associative si, pour tout $(x, y, z) \in E^3$,

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

On dit aussi que le magma $(E, *)$, ou simplement E, est associatif.

Définition 1.1.5 (Commutativité)

Soit $(E, *)$ un magma. La loi $*$ est dite commutative si, pour tout $(x, y) \in E^2, x * y = y * x$.
On dit aussi que le magma $(E, *)$, ou simplement E, est commutatif.

Exemple 1.1.2

1. La multiplication et l'addition usuelles dans $\mathbb{R}$ sont des lois à la fois associatives et commutatives .
2. L'union et l'intersection des parties d'un ensemble A sont des lois commutatives et associatives sur l'ensemble $P(A)$ des parties de A. Cependant, la différence est une loi sur $P(A)$ qui n'est ni associative, ni commutative.
3. La soustraction est une loi dans $\mathbb{Z}$ qui n'est ni commutative, ni associative.
4. La composition des applications o est une loi dans l'ensemble E^E des applications de E dans E qui est associative mais pas commutative en générale.

Définition 1.1.6 (Elément neutre)

Soit $(E, *)$ un magma. On appelle élément neutre de $(E, *)$ tout élément $e \in E$ vérifiant $x * e = e * x = x$ pour tout $x \in E$.
Il est claire que si $(E, *)$ est un magma commutatif, alors $e \in E$ est un élément neutre de E si seulement $x * e = x$ pour tout $x \in E$.

Proposition 1.1.1

Si un magma admet un élément neutre, alors il est unique.

Définition 1.1.6 (Elément neutre)

Soit $(E, *)$ un magma. On appelle élément neutre de $(E, *)$ tout élément $e \in E$ vérifiant $x * e = e * x = x$ pour tout $x \in E$.
Il est claire que si $(E, *)$ est un magma commutatif, alors $e \in E$ est un élément neutre de E si seulement $x * e = x$ pour tout $x \in E$.

Proposition 1.1.1

Si un magma admet un élément neutre, alors il est unique.

Preuve

Preuve. Supposons q'un un magma $(E, *)$ admet deux éléments neutres e et e'. Alors, $e = e' * e$ (car e' est un élément neutre). Or e est aussi un élément neutre de E, donc $e * e' = e'$. Par suite, $e = e'$. (c.q.f.d)

Exemple

1. Soit $(E_1, \perp_1), \ldots, (E_n, \perp_n)$ (où $n \in \mathbb{N}^*$) des magmas d'éléments neutres, respectivement, $e_1, \ldots, e_n$. Alors, il est facile de montrer que $(e_1, \ldots, e_n)$ est l'élément neutre du magma produit $E = E_1 \times \cdots \times E_n$.
2. Pour tout $n \in \mathbb{N}$, il est facile de voir que $\overline{0}$ (resp., $\overline{1}$) est l'élément neutre du magma $(\mathbb{Z}/n\mathbb{Z}, +)$ (resp., $(\mathbb{Z}/n\mathbb{Z}, \times)$).
3. Il est claire que la fonction constante $x \mapsto 0$ (resp., $x \mapsto 1$) est l'élément neutre du magma des fonctions réelles $(\mathcal{F}(\mathbb{R}), +)$ (resp., $(\mathcal{F}(\mathbb{R}), \times)$.
4. L'application identité de E, $\mathrm{id}_E : x \mapsto x$, est l'élément neutre du monoïde $\left(E^E, \circ\right)$.

Définition 1.1.7 (Symétrique d'un élément)

Soit $(E, *)$ un magma admettant un élément neutre e.
Un élément x est dit symétrisable dans E, s'il existe un élément $y \in E$ vérifiant : $x * y = y * x = e$. Dans ce cas, y est appelé un symétrique de x dans E.

Il est claire que si $(E, *)$ est un magma commutatif, alors $x \in E$ est symétrisable dans E s'il existe un élément $y \in E$ vérifiant seulement l'un des égalités $x * y = e$ ou $y * x = e$.

Définition 1.1.6

Un magma associatif $(E, *)$ admettant un élément neutre sera appelé un monoïde.

Définition 1.1.8

Un élément x d'un monoïde $(E, *)$ est dit régulier (ou aussi simplifiable) s'il vérifie les deux assertions suivantes :

- Pour tout $(y, z) \in E^2, x * y = x * z \Rightarrow y = z$ (simplification à gauche).
- Pour tout $(y, z) \in E^2, y * x = z * x \Rightarrow y = z$ (simplification à droite).

Proposition 1.1.2

Dans un monoïde tout élément symétrisable est régulier.

Noter qu'un élément régulier n'est pas nécessairement symétrisable. Par exemple, dans $(\mathbb{Z}, \times)$, tout élément non nul est régulier, alors que seuls 1 et -1 sont inversibles dans $(\mathbb{Z}, \times)$.

Dans la suite, sauf mention contraire, on utilisera la notation multiplicative.

Définition 1.2.1 (Groupe)

On appelle groupe tout monoïde $(G, *)$ tel que tout élément est inversible.

Par abus de langage, on peut dire simplement "le groupe G " au lieu de "le groupe $(G, *)''$ lorsqu'il n'y a pas d'ambiguité sur la loi $*$

Notation et vocabulaire

- Si la loi de G est commutative, G est dit un groupe commutatif ou un groupe abélien.
- Si G est fini, on dit que G est d'ordre fini et son cardinal sera noté par $|G|$ et appelé l'ordre de G.

Example 1.2.1

1. $(\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$ sont des groupes abéliens.
2. $(\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$ et $(\mathbb{Q}^*, \times)$ sont des groupes abéliens.
3. Pour tout $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien.
4. $(\mathbb{Z}^*, \times)$ n'est pas un groupe car, par exemple, 2 n'est pas inversible (en fait, seuls 1 et -1 sont inversibles).
5. $(\mathbb{R}, \times)$ n'est pas un groupe car, par exemple, 0 n'est pas inversible.
6. $(\mathbb{N}, +)$ n'est pas un groupe. En effet, aucun élément non nul n'est inversible.

Proposition et Définition 1.2.3 (Groupe produit)

Soit $(G_1, \ldots, G_n)$ (où $n \in \mathbb{N}^*$) une famille finie de groupes.
Alors, le monoïde produit est un groupe qui est commutatif si et seulement si G_i est commutatif pour tout $i \in \{1, \ldots, n\}$.
Le groupe G est appelé le groupe produit des groupes G_i.
Dans le cas où $G_1 = \cdots = G_n = G$, le groupe produit sera noté simplement G^n.

Exercice 1.2.1

Soit $n \in \mathbb{N}^*$. On désigne par $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble $(\mathbb{Z}/n\mathbb{Z})\backslash\{\overline{0}\}$.
Montrer que $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ est un groupe si et seulement si n est premier.

Pour aborder la notion de sous-groupe, il faut d'abord savoir ce qu'est une partie stable d'une loi.

Définition 1.3.1

Une partie non vide H d'un magma $(E, *)$ est dite stable pour la loi de E si, pour tout $(x, y) \in H^2$, $x * y \in H$. Dans ce cas, la restriction de la loi de E à H est une loi de composition interne sur H appelée la loi induite sur H. Cette loi sera notée par le même symbole que celui de la loi de E.

Pour aborder la notion de sous-groupe, il faut d'abord savoir ce qu'est une partie stable d'une loi.

Définition 1.3.1

Une partie non vide H d'un magma $(E, *)$ est dite stable pour la loi de E si, pour tout $(x, y) \in H^2$, $x * y \in H$. Dans ce cas, la restriction de la loi de E à H est une loi de composition interne sur H appelée la loi induite sur H. Cette loi sera notée par le même symbole que celui de la loi de E.

Exemple 1.3.1

1. L'ensemble des entiers naturels pairs est stable pour l'addition, cependant l'ensemble des entiers naturels impairs n'est pas stable pour l'addition. Les deux ensembles sont stables pour la multiplication.
2. L'ensemble des matrices triangulaires supérieures à diagonale unité est stable pour le produit mais pas pour la somme.
3. L'ensemble $\mathbb{U}$ des nombres complexes de module 1 est

Définition 1.3.5 (Sous-groupe)

Soit H une partie d'un groupe G. On dit que H est un sous-groupe de G si les assertions suivantes sont vérifiées :

1. $H \neq \emptyset$,
2. H est stable pour la loi de G, et
3. H muni de la loi induite est un groupe.

Exemple 1.3.2

1. Pour tout groupe G d'élément neutre e, les deux ensembles G et $\{e\}$ sont des sous-groupes de G, appelés sous-groupes triviaux de G.
2. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$.
3. $(\mathbb{Q}, +)$ est un sous-groupe de $(\mathbb{R}, +)$.
4. Pour tout $n \in \mathbb{N}$, $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$. On verra que seuls les $n\mathbb{Z}$ sont des sous-groupes de $(\mathbb{Z}, +)$.

Proposition 1.3.7

Soit H un sous-groupe d'un groupe G. Alors,

1. l'élément neutre de H est celui de G.
2. L'inverse d'un élément $a \in H$ dans H est celui de a dans G.

En pratique, pour montrer qu'une partie non vide est un sous-groupe on utilise le résultat important suivant :

Théorème 1.3.1 (Caractérisation des sous-groupes)

Soit H une partie non vide d'un groupe G. Alors, les assertions suivantes sont équivalentes :

1. H est un sous-groupe de G.
2. Les assertions suivantes sont vérifiées :
   (a) H est stable pour la loi de G.
   (b) H est stable par passage à l'inverse (i.e., pour tout $x \in H$, $x^{-1} \in H$).
3. Pour tout $(x, y) \in H^2$, $xy^{-1} \in H$.

Exercice

On munit $E = \mathbb{R}^* \times \mathbb{R}$ de la loi de composition interne $\star$ définie par : $(a, e) \star (b, f) = (ab, af + e)$ pour tout $((a, e), (b, f)) \in E^2$.

1. Montrer que $(E, \star)$ est un groupe non commutatif.
2. Soit H un sous-groupe de $(\mathbb{R}^*, \times)$. Montrer que $H \times \mathbb{R}$ est un sousgroupe de E.

Définition 1.4.1 (Morphisme de groupes)

Soient $(G, *)$ et (G', T) deux groupes. On appelle morphisme de groupes ou homomorphisme de groupes de G dans G' toute application $\phi : G \longrightarrow G'$ vérifiant : pour tout $(x, y) \in G^2, \phi(x * y) = \phi(x) T \phi(y)$.

e

Notation et vocabulaire

Soit $\phi : G \longrightarrow G'$ un morphisme de groupes.

- Lorsque les lois de G et G' sont notées multiplicativement on écrit simplement $\phi(xy) = \phi(x)\phi(y)$.
- L'ensemble $\phi(G)$ est appelé l'image de ϕ et il sera noté $\mathrm{Im}(\phi)$.
- Si $G = G'$, alors le morphisme ϕ est appelé endomorphisme de G.
- Si ϕ est bijectif, il sera appelé un isomorphisme de groupes. Dans ce cas, on dit que G et G' sont isomorphes et on écrit $G \cong G'$.

Exemples :

1. L'application identité d'un groupe G est un automorphisme de G. Rappelons l'application identité d'un ensemble E (ou application identique de E) est l'application de E dans E, notée Id_E, définie par $\mathrm{Id}_E(x) = x$ pour tout $x \in E$.
2. Soit $(G, *)$ un groupe d'élément neutre e. L'application $\phi : x \mapsto e$ est un endomorphisme de G.
   En particulier, si la loi de G est notée additivement, alors on écrit $\phi(x) = 0$ pour tout $x \in G$ et dans ce cas, ϕ est appelé l'endomorphisme nul de G.
3. L'application exponentielle est un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}^{+*}, \times)$.
4. L'application logarithme est un isomorphisme de $(\mathbb{R}^{+*}, \times)$ dans $(\mathbb{R}, +)$.

Proposition 1.4.1

Pour tout morphisme de groupes $\phi : G \longrightarrow G'$, on a :

1. $\phi(1_G) = 1_{G'}$.
2. Pour tout $p \in \mathbb{Z}$ et tout $x \in G, \phi(x^p) = \phi(x)^p$. En particulier, $\phi\left(x^{-1}\right) = \phi(x)^{-1}$.
3. Pour tout sous-groupe H de $G, \phi(H)$ est un sous-groupe de G'. Autrement dit, toute image directe d'un sous-groupe de G est un sous-groupe de G'.
   En particulier, $\mathrm{Im}(\phi)$ est un sous-groupe de G'.
4. Pour tout sous-groupe K de $G', \phi^{-1}(K)$ est un sous-groupe de G. Autrement dit, toute image inverse d'un sous-groupe de G' est un sous-groupe de G.

Proposition 1.4.2

1. La composée de deux morphismes de groupes est un morphisme de groupes.
2. L'inverse d'un isomorphisme de groupes est un isomorphisme de groupes.
3. La relation d'isomorphisme de groupes est une relation d'équivalence.

Il est facile de noter qu'un homomorphisme de groupes $f : G \longrightarrow G'$ est surjectif si et seulement si $\mathrm{Im}(f) = G'$ (ce qui est en fait vrai pour n'importe quelle application). Nous allons voir que dans le cas des homomorphismes de groupes, l'injectivité est peut être étudiée en utilisant aussi un ensemble particulier défini comme suit.

Définition 1.4.6 (Noyau)

Soit $f : G \longrightarrow G'$ un homomorphisme de groupes. L'ensemble $f^{-1}(\{1_{G'}\})$ est appelé le noyau de f et noté $\mathrm{Ker}(f)$.

Proposition 1.4.3

Pour tout homomorphisme de groupes $f : G \longrightarrow G'$, le noyau de f est un sous-groupe de G.

Preuve

Puisque $\{1_{G'}\}$ est un sous-groupe de G', $\mathrm{Ker}(f) = f^{-1}(\{1_{G'}\})$ est un sous-groupe de G (d'après la proposition 1.4.4). (c.q.f.d)
Parfois pour montrer qu'une partie d'un groupe est un sous-groupe il suffit de le montrer un noyau d'un homomorphisme de groupes.

Proposition 1.4.8

Soit $f : G \longrightarrow G'$ un homomorphisme de groupes. Alors, f est injectif si et seulement si $\mathrm{Ker}(f) = \{1_G\}$.

Preuve

Preuve. $\Rightarrow$. Supposons que f est injectif et montrons que $\mathrm{Ker}(f) = \{1_G\}$. Puisque $\mathrm{Ker}(f)$ est un sous-groupe de $G, \{1_G\} \subset \mathrm{Ker}(f)$. Alors, il reste à montrer l'inclusion inverse. Soit $g \in \mathrm{Ker}(f)$. Alors, $f(g) = 1_{G'}$. Puisque, f est un homomorphisme de groupes, $f(1_G) = 1_{G'}$, en particulier $f(g) = f(1_G)$. Or, f est injectif, donc $g = 1_G$. D'où la deuxième inclusion et par suite le résultat. $\Leftarrow$. On suppose que $\mathrm{Ker}(f) = \{1_G\}$ et on montre que f est injectif. Soit $(a, b) \in G^2$ tel que $f(a) = f(b)$. Alors,

$$f\left(ab^{-1}\right) = f(a)f\left(b^{-1}\right) = f(a)(f(b))^{-1} = 1_{G'}$$

Alors, $ab^{-1} \in \mathrm{Ker}(f) = \{1_G\}$, c'est-à-dire $ab^{-1} = 1_G$, et par suite $a = b$. Cela montre que f est injectif. (c.q.f.d)

Définition 2.1.1 (Anneau)

Soit A un ensemble muni des deux lois internes Δ et $*$ (addition et multiplication). Le triplet $(A, \Delta, *)$ (ou simplement A) est dit un anneau si les assertions suivantes sont vérifiées :

1. (A, Δ) est un groupe abélien.
2. $(A, *)$ est un monoïde.
3. Distributivité. Pour tout $(x, y, z) \in A^3$,

$$\begin{cases} x * (y \Delta z) = (x * y) \Delta (x * z) \\ (x \Delta y) * z = (x * z) \Delta (y * z) \end{cases}$$

On dit que la loi $*$ est distributive par rapport à loi Δ.
Si de plus la loi $*$ est commutative, alors l'anneau A est dit commutatif.

On convient souvent de noter la première loi d'un anneau additivement et la deuxème loi multiplicativement. Ainsi, dans la suite, lorsqu'il n'y a pas d'ambiguïté sur les lois, on adopte cette convention.

Exemple 2.1.1

1. Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, muni des lois d'addition et de multiplication usuelles, sont des anneaux commutatifs.
2. L'ensemble des entiers naturels $\mathbb{N}$ n'est pas un anneau.
3. On montre facilement que, pour tout $n \in \mathbb{N}, \mathbb{Z}/n\mathbb{Z}$, muni des lois d'addition et de multiplication usuelles, est un anneau commutatif.
4. L'ensemble des fonctions réelles (resp., complexes) muni de l'addition et de la multiplication usuelles est un anneau commutatif appelé l'anneau des fonctions réelles (resp., l'anneau des fonctions complexes) et noté $(\mathcal{F}(\mathbb{R}), +, \times)$(resp.,$(\mathcal{F}(\mathbb{C}), +, \times)$) ou simplement $\mathcal{F}(\mathbb{R})$(resp.,$(\mathcal{F}(\mathbb{C}))$).

Exercice 2.1.1

On définit deux nouvelles lois $\oplus$ et $\otimes$ sur $\mathbb{R}$ de la manière suivante : $\forall (x, y) \in \mathbb{R}^2$, on pose

$$x \oplus y = x + y - 2 \quad \text{et} \quad x \otimes y = xy - 2x - 2y + 6$$

1. Montrer que $(\mathbb{R}, \oplus)$ est un groupe abélien.
2. Montrer que $(\mathbb{R}, \oplus, \otimes)$ est un anneau commutatif.

Proposition 2.1.1 (Règles de calcul dans un anneau)

Soit A un anneau.

1. Pour tout $a \in A, 0 \times a = a \times 0 = 0$ (on dit que 0 est un élément absorbant pour la loi $\times$).
2. Pour tout $(a, b) \in A^2, (-a)b = -(ab) = a(-b)$.
3. Soit $(a, b, c) \in A^3$. On pose $a - b := a + (-b)$. Alors, $a(b - c) = ab - ac$ et $(b - c)a = ba - ca$.
4. (Transformation de somme en produit) Pour tout $(a, b) \in A^2$ et tout $n\mathbb{Z}, n(ab) = (na)b = a(nb)$.
   En particulier, $na = (n1_A)\, a$ et $(nm)a = (n1_A)\,(ma)$ pour tout $a \in A$ et tout $(n, m) \in \mathbb{Z}^2$.

Définition 2.1.2 (Diviseurs de zéro et anneaux intègres)

Soit A un anneau non nul et commutatif. Un élément x de A est dit un diviseur de zéro s'il existe $y \in A$ tel que $y \neq 0$ et $xy = 0$.
L'ensemble des diviseur de zéro dans A sera noté $Z(A)$.
Si $Z(A) = \{0\}$, alors A est dit intègre.
Autrement dit, A est intègre si, pour tout $(x, y) \in A^2$, $xy = 0$ implique $x = 0$ ou $y = 0$.
Autrement dit, par la contraposée de l'implication précédente, A est intègre si l'ensemble $A^* := A\backslash\{0\}$ est stable pour la multipilication.

Définition 2.1.3 (Anneau intègre)

Soit A un anneau non nul et commutatif. L'anneau A est dit intègre si $Z(A) = \{0\}$. Autrement dit, A est intègre si, pour tout $(x, y) \in A^2$, $xy = 0$ implique $x = 0$ ou $y = 0$.

Remarque et exemples 2.1

Par la contraposée de l'implication précédente, on peut voir qu'un anneau non nul et commutatif A est intègre si l'ensemble $A^* := A\backslash\{0\}$ est stable pour la multipilication.

1. Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, muni des lois d'addition et de multiplication usuelles, sont des anneaux commutatifs et intègres.
2. On montre facilement que, pour tout $n \in \mathbb{N}, \mathbb{Z}/n\mathbb{Z}$, muni des lois d'addition et de multiplication usuelles, est un anneau intègre si et seulement si n est un nombre premier.

On a vu dans le chapitre des groupes, que tout élément symétrisable est régulier. Dans les anneaux, l'intégrité d'un anneau suffira pour que tout élément non nul soit régulier.

Proposition 2.1.2

Si A est un anneau intègre, alors tout élément non nul de A est régulier pour la multiplication.

Proposition 2.1.3

Soient a et b deux éléments d'un anneau A. Si a et b commutent (i.e., $ab = ba$), alors, pour tout $n \in \mathbb{N}^*$, on a les deux identités remarquables suivantes :

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k} \qquad \text{(Formule du binôme de Newton)}$$

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

Définition 2.1.4

Un élément x d'un anneau A est dit inversible s'il est inversible pour la loi $\times$ (i.e., s'il existe $y \in A$ tel que $xy = yx = 1$). L'ensemble des éléments inversibles de A est noté par $U(A)$ (qui est bien un groupe multiplicatif) est appelé le groupe des inversibles (ou parfois, des unités) de A.

Exemple 2.1.3

1. Pour les anneaux $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, on a $U(\mathbb{Z}) = \{-1; 1\}$, $U(\mathbb{Q}) = \mathbb{Q}^*$, $U(\mathbb{R}) = \mathbb{R}^*$ et $U(\mathbb{C}) = \mathbb{C}^*$.
2. Dans un anneau non nul l'élément 0 n'est pas inversible.

Exercice

Soit A un anneau commutatif non nul. On pose $B = A \times A$. On munit B des lois suivantes : pour tout $((x, e), (y, f)) \in B^2$, on pose

$$\begin{cases} (x, e) + (y, f) = (x + y, e + f) \\ (x, e)(y, f) = (xy, xf + ey) \end{cases}$$

1. Montrer que B est un anneau commutatif.
2. Montrer que B n'est pas intègre.
3. Déterminer l'ensemble des éléments inversibles de B.
4. Soient $(x, e) \in B$ et $n \in \mathbb{N}^*$. Montrer que $(x, e)^n = \left(x^n, nx^{n-1}e\right)$.

Définition 2.1.5 (Corps)

Un anneau commutatif et non nul K est dit un corps si tout élément non nul de K est inversible (i.e., $A^* = U(A)$).

Exemples

1. L'anneau $\mathbb{Z}$ n'est pas un corps.
2. Les anneaux $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des corps.
3. Pour tout $n \in \mathbb{N}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

De la définition on déduit facilement la caractérisation suivante des corps.

Proposition 2.1.3

Un ensemble K muni des deux lois internes + et $\times$ est un corps si et seulement s'il satisfait les trois assertions suivantes :

1. $(K, +)$ est un groupe abéliens.
2. $(K^*, \times)$ est un groupe abéliens.
3. la loi $\times$ est distributive par rapport à + .

Corollaire 2.1.1

Tout corps est un anneau intègre.

Définition 2.2.6 (Sous-anneau)

1. Une partie B non vide d'un anneau A est dit un sous-anneau de A si les assertions suivantes sont vérifiées :
   (a) B est stable pour les deux lois + et $\times$.
   (b) $(B, +, \times)$ est un anneau.
   (c) $1_A \in B$.

Remarque 2.2.2

1. Si B est un sous-anneau d'un anneau A, alors $1_B = 1_A$.
2. Les auteurs qui excluent la condition qu'un anneau contient l'élément neutre pour la deuxième loi n'exigent pas que le sous-anneau B d'un anneau A partage l'élément neutre 1_A avec A.

Définition 2.2.3 (Sous-corps)

Uun sous-anneau K' d'un corps K est dit un sous-corps de K si, pour tout $x \in K' \backslash \{0\}, x^{-1} \in K'$ (i.e., $(K', +, \times)$ est un corps).

Exemple 2.2.4

1. $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ (et ainsi de $\mathbb{R}$ et de $\mathbb{C}$).
2. $\mathbb{Q}$ est un sous-corps du corps $\mathbb{R}$.
3. $\mathbb{R}$ est un sous-corps du corps $\mathbb{C}$.

Proposition 2.2.5

Une partie B non vide d'un anneau A est un sous-anneau de A si et seulement si les assertions suivantes sont vérifiées :

1. $(B, +)$ est un sous-groupe de $(A, +)$,
2. B est stable pour la loi $\times$.
3. $1_A \in B$.

Remarque 2.2.3

Soit K une partie stable pour l'addition et la multiplication d'un anneau A. Pour montrer que K, muni des lois induites, est un corps, il suffit de montrer les assertions suivantes :

1. K est un sous-anneau de A,
2. le monoïde $(K, \times)$ est commutatif (autrement dit, K est un sousanneau commutatif de A), et
3. tout élément non nul de K est inversible (autrement dit, le monoïde $(K \setminus \{0_A\}, \times)$ est un groupe ou aussi $U(K) = K \setminus \{0_A\}$).

Définition 2.4.1

Soient A et B deux anneaux. Une application $f : A \longrightarrow B$ est dite un morphisme ou homomorphisme d'anneaux, si les assertions suivantes sont vérifiées :

1. $f(1_A) = 1_B$.
2. Pour tout $(x, y) \in A^2, f(x + y) = f(x) + f(y)$.
3. Pour tout $(x, y) \in A^2, f(xy) = f(x)f(y)$.

Proposition 2.4.1

Soit $f : A \longrightarrow A'$ un morphisme d'anneaux commutatifs.

1. Pour tout $x \in A$ et tout $n \in \mathbb{N}$, $f(x^n) = f(x)^n$.
2. Si x est un élément inversible dans A, alors $f(x)$ est inversible dans A' et on a $f\left(x^{-1}\right) = f(x)^{-1}$. Ainsi, $f(x^n) = f(x)^n$ pour tout $n \in \mathbb{Z}$.
3. L'image directe d'un sous-anneau de A est un sous-anneau de A'. En particulier, l'image de f, $\mathrm{Im}(f)$, est un sous-anneau de A'.
4. L'image réciproque d'un sous-anneau de A' est un sous-anneau de A.
5. Si f est un isomorphisme, alors f^{-1} est aussi un isomorphisme d'anneaux.