Anneaux et corps abstraits

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Introduction

2. Anneaux généraux

Motivés par $\mathbb{Z}$ et ses quotients $\mathbb{Z}/n\mathbb{Z}$, nous avons introduit dans une définition du chapitre précédent la notion d'*anneau commutatif unitaire*. Mais la commutativité de la multiplication n'est pas toujours satisfaite, ou « naturelle ».

Exemple 2.1. Soit l'espace vectoriel des matrices 2×2 :

$$\mathscr{M}_{2\times 2}(\mathbb{R}) \;:=\; \Big\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) :\;\; a,\, b,\, c,\, d \in \mathbb{R} \text{ quelconques} \Big\},$$

muni de l'addition :

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) + \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \;:=\; \left(\begin{smallmatrix} a+a' & b+b' \\ c+c' & d+d' \end{smallmatrix}\right), \qquad \text{d'élément neutre } \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right),$$

et muni de la multiplication dite *matricielle* qui correspond à la *composition* des applications linéaires :

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \times \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \;:=\; \left(\begin{smallmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{smallmatrix}\right), \qquad \text{d'élément neutre } I_{2\times 2} \;:=\; \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

Le cours d'Algèbre Linéaire a démontré que $\mathscr{M}_{2\times 2}(\mathbb{R})$, muni de $+$, $\times$, satisfait toutes les propriétés attendues, à l'exception de deux propriétés.

☐ Pour $M \in \mathscr{M}_{2\times 2}$, il n'existe pas toujours $M' \in \mathscr{M}_{2\times 2}$ satisfaisant $M \times M' = I_{2\times 2} = M' \times M$.

☐ Deux matrices quelconques $A, B \in \mathscr{M}_{2\times 2}$ ne satisfont pas toujours :

$$A \times B \overset{?}{=} B \times A \qquad \text{(souvent faux)}.$$

Par exemple :

$$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \;=\; \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right) \overset{!}{\neq} \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right) \;=\; \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \times \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right).$$

Ceci motive une définition générale d'*anneau* (mathématiques, pas olympique), dans laquelle on ne demande pas forcément que la multiplication $\times$ soit commutative.

Définition 2.2. Soit A un ensemble muni de deux *lois de composition internes* $+$ et $\times$, c'est-à-dire $a+b \in A$ et $a \times b \in A$ pour tous $a, b \in A$. On dit que A est un *anneau* s'il vérifie les propriétés suivantes.

(1) Le couple $\big(A, +\big)$ est un *groupe abélien*, au sens d'une définition vue au chapitre précédent, d'élément neutre 0_A.

(2) La loi de multiplication $\times$ est associative.

(3) La loi $\times$ est distributive, à gauche et à droite, par rapport à $+$:

$$a \times (b+c) \;=\; a \times b + a \times c \qquad (\forall\, a, b, c \in A),$$
$$(a+b) \times c \;=\; a \times c + b \times c \qquad (\forall\, a, b, c \in A).$$

On dit qu'un anneau $\big(A, +, \times\big)$ est *commutatif* lorsque la loi $\times$ satisfait de plus $a \times b = b \times a$, pour tous $a, b \in A$.

Proposition 2.3. *Dans un anneau $\big(A, +, \times\big)$, les trois propriétés suivantes sont satisfaites.*

(1) $a \times 0_A = 0_A = 0_A \times a$*, pour tout* $a \in A$*.*

(2) $a \times (-b) = -\,a \times b = (-a) \times b$*, pour tous* $a, b \in A$*.*

(3) $(-a) \times (-b) = a \times b$*, pour tous* $a, b \in A$*.*

Démonstration. **(1)** Comme 0_A est un élément neutre pour la loi $+$, on a $0_A = 0_A + 0_A$. Ainsi, en multipliant cette égalité par a et en utilisant la distributivité, on a :

$$0_A \times a \;=\; (0_A + 0_A) \times a \;=\; (0_A \times a) + (0_A \times a).$$

Enfin, comme $(A, +)$ est un groupe, on en déduit que $0_A = 0_A \times a$. On montre de manière similaire que $a \times \times 0_A = 0_A$.

(2) Si a et b sont dans A, alors on a :

$$(a \times b) + (a \times (-b)) \;=\; a \times (b-b) \;=\; a \times 0_A \;=\; 0_A,$$

grâce à **(1)** que nous venons de voir. On en déduit que $a \times (-b)$ est l'inverse de $a \times b$ pour la loi $+$, c'est-à-dire :

$$a \times (-b) \;=\; -\,(a \times b).$$

On montre de façon similaire que $(-a) \times b = -\,(a \times b)$.

(3) Si a et b sont dans A, utilisons deux fois la propriété **(2)**, pour conclure :

$$(-a) \times (-b) \;=\; -\,(a \times (-b)) \;=\; -\,\big(-\;(a \times b)\big) \;=\; a \times b. \qquad \square$$

Le cas d'un anneau dans lequel $0_A = 1_A$ est très dégénéré : l'Exercice 1 propose de vérifier qu'alors tous les éléments $a \in A$ sont égaux à 0_A, de telle sorte que $A = \{0_A\}$. On dit alors que A est l'*anneau nul*. Mais comme tout ce qui est nul ne vaut rien, on supposera toujours à partir de maintenant que :

$$0_A \;\neq\; 1_A.$$

Clairement :

$$\big(\mathbb{Z}, +, \times\big), \qquad \big(\mathbb{Z}/n\mathbb{Z}, +, \times\big), \qquad \big(\mathbb{Q}, +, \times\big), \qquad \big(\mathbb{R}, +, \times\big), \qquad \big(\mathbb{C}, +, \times\big),$$

sont des anneaux, commutatifs qui plus est. En fait, il y a des inclusions qui respectent les structures d'anneau.

Définition 2.4. Soit $\big(A, +_A, \times_A\big)$ un anneau. On dit qu'un sous-ensemble $B \subset A$ est un *sous-anneau* de A lorsque :

(1) $\big(B, +_A\big)$ est un *sous-groupe abélien* de $\big(A, +_A\big)$, c'est-à-dire que :

$$b,\, b' \,\in\, B \qquad\qquad \Longrightarrow \qquad\qquad b +_A b' \,\in\, B,$$

où l'addition est prise dans A, de telle sorte que $\big(B, +_A\big)$ est un groupe abélien en lui-même.

(2) pour tous $b, b' \in B$, on a $b \times_A b' \in B$ aussi ;

(3) $1_A \in B$.

On vérifie, en jouant avec la logique, que $\big(B, +, \times\big)$ est alors un anneau en lui-même.

Proposition 2.5. *Si $B \subset A$ est un sous-anneau de $\big(A, +_A, \times_A\big)$, alors le triplet $\big(B, +_A, \times_A\big)$ est un anneau.* □

On notera souvent $+$, $\times$, sans les indices $+_A$, $\times_A$.

Par exemple, les inclusions suivantes sont des inclusions de sous-anneaux :

$$\mathbb{Z} \,\subset\, \mathbb{Q} \,\subset\, \mathbb{R} \,\subset\, \mathbb{C},$$

pour l'addition $+$ et la multiplication $\times$ classiques.

Dans le chapitre précédent, nous avons comparé :

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \overset{?}{=} \mathbb{Z}/mn\mathbb{Z},$$

où m, n sont deux entiers *premiers entre eux*. À cette occasion, nous avons introduit la notion d'*isomorphisme* entre anneaux commutatifs. Voici une définition générale valable dans un anneau quelconque.

Définition 2.6. Étant donné deux anneaux $\big(A, +_A, \times_A\big)$ et $\big(B, +_B, \times_B\big)$, l'*anneau produit* $\big(A \times B, +, \times\big)$ est l'ensemble produit constitué de couples d'éléments :

$$A \times B \,:=\, \big\{(a, b)\colon\ a \in A \text{ quelconque},\ b \in B \text{ quelconque}\big\},$$

pour lequel les deux lois de compositions internes $+$ et $\times$ sont définies par :

$$\begin{aligned}
(a, b) + (a', b') \,&:=\big(a + a',\, b + b'\big) && \text{d'élément neutre } \big(0_A, 0_B\big),\\
(a, b) \times (a', b') \,&:=\big(a \times_A a',\, b \times_B b'\big) && \text{d'élément neutre } \big(1_A, 1_B\big).
\end{aligned}$$

On vérifie par le raisonnement (tauto)logique que $\big(A \times B, +, \times\big)$ est effectivement un anneau, au sens de la Définition 2.2. Si A et B sont commutatifs, $A \times B$ l'est également.

Plus généralement, étant donné un nombre $\nu \,\geqslant\, 1$ d'anneaux $A_1, \ldots, A_\nu$, on peut construire l'*anneau-produit :*

$$A_1 \times \cdots \times A_\nu \,:=\, \Big\{\big(a_1, \ldots, a_\nu\big)\colon\ a_1 \in A_1 \text{ quelconque},\ \ldots,\ a_\nu \in A_\nu \text{ quelconque}\Big\},$$

muni des opérations :

$$\begin{aligned}
\big(a_1, \ldots, a_\nu\big) + \big(a'_1, \ldots, a'_\nu\big) \,&:=\, \big(a_1 + a'_1, \ldots, a_\nu + a'_\nu\big),\\
\big(a_1, \ldots, a_\nu\big) \times \big(a'_1, \ldots, a'_\nu\big) \,&:=\, \big(a_1 \times a'_1, \ldots, a_\nu \times a'_\nu\big).
\end{aligned}$$

Par exemple, avec :

$$\begin{aligned}
\mathbb{Z}/2\mathbb{Z} \,&=\, \big\{0,\, 1\big\} \ \mathsf{mod}\, 2,\\
\mathbb{Z}/3\mathbb{Z} \,&=\, \big\{0,\, 1,\, 3\big\} \ \mathsf{mod}\, 3,
\end{aligned}$$

on a :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \,=\, \big\{(0,0),\ (0,1),\ (0,2),\ (1,0)\ (1,1),\ (1,2)\big\}.$$

3. Morphismes d'anneaux et idéaux

Soient deux anneaux quelconques A et B.

Définition 3.1. Un *morphisme d'anneaux* de A vers B est une application $f\colon A \longrightarrow B$ satisfaisant :

(1) $f(a+b) = f(a) + f(b)$, pour tous $a, b \in A$, et $f(0_A) = 0_B$;

(2) $f(a \times b) = f(a) \times f(b)$, pour tous $a, b \in A$, et $f(1_A) = 1_B$.

Par (contre-)exemple, avec un entier fixé $\lambda \in \mathbb{Z}$, l'application $n \longmapsto \lambda\, n$ de $\mathbb{Z}$ dans $\mathbb{Z}$ est un morphisme de groupes $(\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$, mais cependant, dès que $\lambda \neq \lambda^2$, ce n'est pas un morphisme d'anneaux, car :

$$f(m\,n) \,=\, \lambda\, m\, n \,\neq\, \lambda\, m\, \lambda\, n \,=\, f(m)\, f(n) \qquad\qquad (m, n \in \mathbb{Z}).$$

Terminologie 3.2. Un *endomorphisme d'anneau* est un morphisme $A \longrightarrow A$ d'un anneau A vers lui-même.

Un *isomorphisme d'anneaux* est un morphisme $A \longrightarrow B$ d'anneaux qui est *bijectif*, c'est-à-dire simultanément injectif et surjectif.

Un *automorphisme d'anneau* est un isomorphisme d'un anneau A sur lui-même.

Par exemple, l'application de conjugaison complexe :

$$z \,=\, x + i\, y \ \longmapsto\ x - i\, y \,=\, \overline{z},$$

est un automorphisme de l'anneau $\big(\mathbb{C}, +, \times\big)$.

Définition 3.3. Si $f\colon A \longrightarrow B$ est un morphisme d'anneaux, on appelle *noyau* de f l'ensemble :

$$\mathsf{Ker}\, f \,:=\, \big\{a \in A\colon\ f(a) = 0\big\},$$

et on appelle *image* de f l'ensemble :

$$\mathsf{Im}\, f \,:=\, \big\{b \in B\colon\ \exists\, a \in A,\ f(a) = b\big\} \,=\, f(A).$$

Nous laissons en exercice la démonstration de la

Proposition 3.4. *L'image $f(A)$ d'un morphisme d'anneaux $f\colon A \longrightarrow B$ est toujours un sous-anneau de B.* □

Toutefois, le noyau $\mathsf{Ker}\, f$ d'un tel morphisme $f\colon A \longrightarrow B$ n'est en général *pas* un sous-anneau de A, car il ne contient pas toujours 1_A.

Pour terminer cette section, introduisons brièvement une notion qui sera utile ultérieurement, et que nous présentons ici seulement dans le cas où la multiplication $\times$ est commutative.

Définition 3.5. Un sous-ensemble non vide $I \subset A$ d'un anneau commutatif A est appelé un *idéal* s'il vérifie les deux propriétés suivantes :

$$\Big(\ a \in I \quad \text{et} \quad b \in I\ \Big) \qquad \Longrightarrow \qquad a - b \in I,$$

$$\Big(\ a \in I \quad \text{et} \quad p \in A \text{ quelconque}\ \Big) \qquad \Longrightarrow \qquad p\, a \in I.$$

Cette notion absolument fondamentale dans toutes les mathématiques interviendra naturellement lorsque nous étudierons les *polynômes* à une indéterminée x, dans le prochain chapitre.

4. Groupe des inversibles dans un anneau

Si un anneau A n'est *pas* un corps, en général, l'ensemble $A\backslash\{0\}$ de ses éléments non nuls n'est *pas* un groupe pour la loi $\times$ de multiplication. Dans ce cas, on peut introduire un ensemble plus petit, qui lui, est un groupe.

Définition 4.1. Un élément $a \in A$ est dit *inversible* (à gauche et à droite) s'il existe un élément, noté $a^{-1} \in A$, tel que :

$$a^{-1}\, a \;=\; 1_A \;=\; a\, a^{-1}.$$

On note alors $A^\times$ l'ensemble des éléments inversibles de A pour la loi $\times$.

Attention ! Il ne faudra pas confondre $A^\times$ avec $A^* = A\backslash\{0\}$!

Proposition 4.2. *Si $a, b \in A^\times$ sont inversibles, alors leur produit $a\, b \in A^\times$ l'est aussi.*

Preuve. En effet, $b^{-1}\, a^{-1} \in A$ fonctionne :

$$b^{-1}a^{-1}\, a\, b \;=\; b^{-1}\, b \;=\; 1_A \;=\; a\, a^{-1} \;=\; a\, b\, b^{-1}a^{-1}. \qquad \square$$

Théorème 4.3. *Le couple $\big(A^\times, \times\big)$ est un groupe.*

Démonstration. Comme la loi $\times$ est associative sur A, elle l'est également sur $A^\times$. L'élément 1_A est tautologiquement inversible, et donc, on a $1_A \in A^\times$, et 1_A est un élément neutre pour la multiplication $\times$.

Enfin, nous affirmons que tout élément de $A^\times$ est inversible. En effet, il suffit de vérifier que si $a \in A^\times$, alors $a^{-1} \in A^\times$ aussi.

Mais cela est clair, car l'identité *symétrique* qui exprime que a^{-1} est un inverse pour a :

$$a^{-1}\, a \;=\; 1_A \;=\; a\, a^{-1},$$

peut être lue comme une identité qui exprime que a est un inverse pour a^{-1}.

$$a\, a^{-1} \;=\; 1_A \;=\; a^{-1}\, a. \qquad \square$$

Terminologie 4.4. Le groupe $\big(A^\times, \times\big)$ est appelé *groupe des inversibles* de l'anneau A.

Enfin, on vérifie aisément (exercice) la

Proposition 4.5. *Si A et B sont deux anneaux quelconques, alors :*

$$\big(A \times B\big)^\times \;=\; A^\times \times B^\times. \qquad \square$$

5. Intégrité et structure de corps

En supposant que notre anneau A n'est pas commutatif, voici la notion d'intégrité, que nous avons déjà présentée dans le cas commutatif.

Définition 5.1. Un anneau $\big(A, +, \times\big)$ est dit *intègre* si, pour tous $a, b \in A$, la relation $a\, b = 0_A$ implique que $a = 0_A$ ou $b = 0_A$.

Autrement dit, par contraposition, dans un anneau intègre, si $a \neq 0_A$ et si $b \neq 0_A$, alors $a\, b \neq 0_A$ aussi.

Proposition 5.2. *Dans un anneau intègre, les deux règles de simplification suivantes sont vraies.*

(1) *si* $a \neq 0_A$*, alors* $a\,b = a\,c$ *implique* $b = c$*;*

(2) *si* $c \neq 0$*, alors* $a\,c = b\,c$ *implique* $a = b$*.*

Démonstration. Prouvons seulement la règle **(1)**, l'autre étant symétrique.

Supposons donc que $a\,b = a\,c$. Alors comme $(A, +)$ est un groupe (commutatif), on a $a\,b - a\,c = 0$. Comme $-\,a\,c = a\,(-c)$, la distributivité de la multiplication par rapport à l'addition donne :

$$a\,(b - c) \;=\; 0_A.$$

Enfin, comme $a \neq 0_A$ et comme A est par hypothèse intègre, cela force $b - c = 0_A$, donc nous concluons bien que $b = c$. □

L'anneau $\big(\mathbb{Z}, +, \times\big)$ est intègre, c'est bien connu, tandis que l'anneau $\big(\mathscr{M}_{2\times 2}(\mathbb{R}), +, \times\big)$ des matrices carrées de taille 2×2 à coefficients dans $\mathbb{R}$ n'est *pas* intègre, comme le montre la matrice non nulle :

$$M \;:=\; \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

qui satisfait :

$$M \;\neq\; \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{mais} \qquad M \cdot M \;=\; \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0\cdot 0 + 1 \cdot 0 & 0 \cdot 1 + 1 \cdot 0 \\ 0 \cdot 0 + 0 \cdot 0 & 0 \cdot 1 + 0 \cdot 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Voici encore une notion que nous avons déjà introduite, dans un chapitre qui précède, dans le cadre commutatif.

Définition 5.3. Un *corps* $\big(\mathbb{K}, +, \times\big)$ est un anneau $\big(A, +, \times\big)$ avec $1_A \neq 0_A$ tel que $\big(A^*, \times\big)$ est un *groupe*.

Ici, $A^* = A \backslash \{0\}$. De façon équivalente, un corps est un anneau ayant au moins deux éléments tel que tout élément non nul admet un inverse multiplicatif.

Par exemple, les anneaux $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, sont des corps. Par contre, l'anneau $\mathbb{Z}$ n'est pas un corps, car tout entier $n \neq -1, 1$ n'a pas d'inverse multiplicatif dans $\mathbb{Z}$.

Proposition 5.4. *Tout corps est un anneau intègre.*

Démonstration. Soit donc un corps $\mathbb{K}$ — êtes vous d'accorps ? Soient $a, b \in \mathbb{K}$ tels que :

$$a\,b \;=\; 0.$$

Pour satisfaire l'intégrité au sens de la Définition 5.1, nous devons montrer que $a = 0$ ou $b = 0$.

Supposons premièrement que $a \neq 0$ et cherchons à montrer que $b = 0$. Puisque $\mathbb{K}$ est un corps, l'élément $a \in \mathbb{K}^*$ est inversible dans $\mathbb{K}$, c'est-à-dire qu'il existe un élément, noté a^{-1}, tel que $a\,a^{-1} = 1 = a^{-1}\,a$.

Multiplions alors l'égalité $0 = a\,b$ à gauche par a^{-1}, ce qui nous donne :

$$0 \;=\; a^{-1}\,(a\,b) \;=\; a^{-1}\,a\,b \;=\; b,$$

et donc nous obtenons bien $0 = b$.

Deuxièmement, si nous supposons $b \neq 0$, le même argument (symétrisé) donne $a = 0$. □

Y a-t-il une réciproque à cette proposition ? Pas toujours, mais voici au moins une réciproque « partielle », valable avec l'hypothèse supplémentaire de cardinalité finie.

Théorème 5.5. *Pour un anneau A de cardinal fini avec $1_A \neq 0_A$, on a équivalence entre :*

(i) *A est un corps.*

(ii) *A est intègre ;*

Rappelons que la théorie des ensembles élémentaire nous a appris que si E est un ensemble fini et si $f : E \longrightarrow E$ est une application quelconque, les trois propriétés suivantes sont équivalentes :

- f est injective ;
- f est surjective ;
- f est bijective.

Démonstration. **(i)** $\Longrightarrow$ **(ii)**. Cette implication est évidente, grâce à la Proposition 5.4.

(ii) $\Longrightarrow$ **(i)** Soit donc $(A, +, \times)$ un anneau intègre de cardinal fini, avec $1_A \neq 0_A$. Il y a donc au moins deux éléments dans A. Notre objectif est d'établir que tout élément non nul fixé $a \in A\backslash\{0\}$ admet un inverse dans A, c'est-à-dire un élément $x \in A$ tel que $a\,x = 1_A = x\,a$, ce qui justifiera que A est un corps.

À cette fin, introduisons l'application de multiplication à gauche par a :

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & A \\ & x & \longmapsto & a\,x. \end{array}$$

Cette application φ est un endomorphisme du *groupe* $(A, +)$, car pour $x, y \in A$ quelconques, on a :

$$\varphi(x + y) \,=\, a\,(x + y) \,=\, a\,x + a\,y \,=\, \varphi(x) + \varphi(y).$$

Assertion 5.6. *Le morphisme φ est injectif.*

Preuve. Comme φ est un morphisme de groupes pour l'addition, il suffit de vérifier que son noyau est réduit à $\{0_A\}$. C'est bien le cas, puisque $a \neq 0_A$ dans A intègre donne :

$$\varphi(x) \,=\, 0_A \qquad \Longleftrightarrow \qquad a\,x \,=\, 0_A \qquad \Longleftrightarrow \qquad x \,=\, 0_A. \qquad \square$$

Le point-clé de l'argumentation, c'est que la finitude du cardinal (nombre d'éléments) de A *transmutation de l'injectivité en de la surjectivité*, comme nous l'avons rappelé plus haut.

Par conséquent, φ est surjective !

Cela entraîne que 1_A est dans l'image de A, et fournit donc comme par magie un $x \in A$ tel que $x\,a = 1_A$. Mais attention ! Nous n'avons pas supposé que A était commutatif !

En utilisant l'application $\psi : x \longmapsto x\,a$ de multiplication à droite par a, on établit de même qu'il existe un élément $y \in A$ tel que $y\,a = 1_A$.

Pour conclure que a est inversible, il reste encore à vérifier que $x = y$, ce que l'on peut faire en procédant comme suit :

$$y \,=\, y \cdot 1_A \,=\, y\,(a\,x) \,=\, (y\,a)\,x \,=\, 1_A \cdot x \,=\, x. \qquad \square$$

6. Corps des fractions d'un anneau commutatif intègre

Soit un anneau commutatif intègre A. On note $A^* := A\backslash\{0\}$.

Proposition 6.1. *La relation binaire définie sur $A \times A^*$ par :*

$$(a,b) \sim (c,d) \qquad \overset{déf}{\iff} \qquad a\,d = b\,c,$$

est une relation d'équivalence.

Démonstration. Réflexivité. Puisque l'anneau est commutatif, on a $a\,b = b\,a$, ce qui donne $(a,b) \sim (a,b)$.

Symétrie. De nouveau grâce à la commutativité de la loi $\times$:

$$(a,b) \sim (c,d) \iff a\,d = b\,c \iff c\,b = d\,a \iff (c,d) = (a,b).$$

Transitivité. Toujours grâce à la commutativité de la loi $\times$, si :

$$(a,b) \sim (c,d) \qquad \text{et} \qquad (c,d) \sim (e,f),$$

c'est-à-dire si $a\,d = b\,c$ et $c\,f = d\,e$, il vient :

$$a\,d\,f = b\,c\,f = b\,d\,e, \qquad \text{donc} \qquad (a\,f)\,d = (b\,e)\,d,$$

et comme $d \neq 0$ dans A intègre, on peut diviser par d pour obtenir $a\,f = b\,e$, c'est-à-dire $(a,b) \sim (e,f)$. □

Notation 6.2. L'ensemble des classes d'équivalences de $A \times A^*$ pour $(a,b) \sim (c,d)$ sera noté $\mathsf{Frac}\,A$.

La classe d'équivalence d'un élément (a,b) sera noté $\frac{a}{b}$ et appelée *fraction.*

Les raisons de cette notation $\frac{a}{b}$ vont vite devenir très claires.

Ensuite, définissons deux lois naturelles d'addition $+$ et de multiplication $\times$ sur $\mathsf{Frac}\,A$. Pour deux représentants (a,b) et (c,d) de deux fractions $\frac{a}{b}$ et $\frac{c}{d}$, avec $b \neq 0 \neq d$, on pose :

$$\frac{a}{b} + \frac{c}{d} := \frac{a\,d + b\,c}{b\,d},$$

et :

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{a\,c}{b\,d}.$$

Observons qu'en dessous de la barre (de fraction), l'élément $b\,d$ est encore non nul, puisque $b \neq 0 \neq d$ et puisque A est intègre. Notons aussi que cette multiplication entre fractions est commutative, puisque la multiplication dans A est commutative.

Proposition 6.3. *Les deux éléments ainsi définis $\frac{a\,d+b\,c}{b\,d}$ et $\frac{a\,c}{b\,d}$ ne dépendent que des classes de (a,b) et de (c,d).*

Démonstration. Prenons donc deux paires équivalentes $(a,b) \sim (a',b')$ et $(c,d) \sim (c',d')$, et vérifions pour l'addition que l'on a :

$$\big(a\,d + b\,c,\ b\,c\big) \ \sim\ \big(a'\,d' + b'\,c',\ b'\,c'\big).$$

En effet, comme $a\,b' = a'\,b$ et $c\,d' = c'\,d$ par hypothèse, il vient :

$$\begin{aligned}(a\,d + b\,c)\,b'\,c' &= a\,d\,b'\,c' + b\,c\,b'\,c' \\ &= a\,b'\,d\,c' + b'\,c'\,b\,c \\ &= a'\,b\,c\,d' + b'\,c'\,b\,c \\ &= \big(a'\,d' + b'\,c'\big)\,b\,c.\end{aligned}$$

On fait de même pour la loi de multiplication $\times$. □

Théorème 6.4. *Le triplet ainsi défini* $\big(\mathsf{Frac}\, A, +, \times\big)$ *est un corps commutatif d'élément neutre* $\frac{0}{1}$ *pour l'addition et d'élément neutre* $\frac{1}{1}$ *pour la multiplication.*

En particulier, une fraction $\frac{a}{b} \neq 0$ (avec $b \neq 0$) est non nulle dans ce corps si et seulement si $a \neq 0$.

Démonstration. Les arguments détaillés sont laissés en exercice. Le point-clé, c'est qu'une fraction (classe d'équivalence) non nulle $\frac{a}{b}$ avec $a \neq 0 \neq b$ a pour inverse multiplicatif $\frac{b}{a}$, puisque :

$$\frac{a}{b} \cdot \frac{b}{a} \;=\; \frac{a\,b}{b\,a} \;=\; \frac{1}{1},$$

car $a\,b = b\,a$ dans A commutatif. □

Autrement dit, $\mathsf{Frac}\, A$ crée un nouvelle structure algébrique dans laquelle la multiplication devient une loi de *groupe*.

Terminologie 6.5. Le corps $\mathsf{Frac}\, A$ est appelé *corps des fractions* de l'anneau commutatif intègre A.

Enfin, introduisons une application :

$$\begin{array}{rccc} \varphi\colon & A & \longrightarrow & \mathsf{Frac}\, A \\ & a & \longmapsto & \dfrac{a}{1}. \end{array}$$

Proposition 6.6. *L'application* $\varphi(a) := \frac{a}{1}$ *est un morphisme* injectif *de l'anneau* A *dans l'anneau (corps)* $\mathsf{Frac}\, A$.

Démonstration. La vérification du fait que φ est un morphisme d'anneaux (tout corps est un anneau) est laissée en exercice.

Quant à l'injectivité, elle est immédiate :

$$\frac{a}{1} \;=\; \frac{0}{1} \qquad\qquad \Longleftrightarrow \qquad\qquad a \cdot 1 \;=\; 1 \cdot 0 \;=\; 0. \qquad\qquad \square$$

Grâce à cette application naturelle φ, nous pouvons *identitifier* l'anneau A à son image :

$$A \;\hookrightarrow\; \varphi(A) \;\subset\; \mathsf{Frac}\, A,$$

dans son corps des fractions.

7. Caractéristique d'un anneau intègre

En algèbre, la caractéristique d'un anneau (unitaire) A est par définition l'ordre pour la loi additive de l'élément neutre de la loi multiplicative si cet ordre est fini ; si cet ordre est infini, la caractéristique de l'anneau est par définition 0.

Pour un anneau unitaire $(A, +, \times)$, rappelons que l'on note 0_A l'élément neutre de l'addition $+$, que l'on note 1_A celui de la multiplication $\times$, et que l'on suppose :

$$1_A \;\neq\; 0_A,$$

ce qui exclut le cas extrêmement dégénéré où $A = \{0_A\}$ est l'anneau nul.

Définition 7.1. La *caractéristique* d'un anneau A est le plus petit entier $n \geqslant 1$ tel que :

$$\begin{aligned} n\,1_A &= \underbrace{1_A + 1_A + \cdots + 1_A}_{n \text{ fois}} \\ &= 0_A, \end{aligned}$$

si un tel entier existe. Dans le cas contraire — autrement dit si 1_A est d'ordre infini —, on dit que la caractéristique de A est ***nulle***, ou est 0.

Il existe un morphisme naturel d'anneaux unitaires $f\colon \mathbb{Z} \longrightarrow A$, défini, pour un entier $n \geqslant 1$ quelconque, par :

$$f(n) := 1_A + \cdots + 1_A,$$

où 1_A est répété n fois, c'est-à-dire :

$$f(n) := n\,1_A.$$

On sait (ou on vérifie) que le noyau de f :

$$\mathsf{Ker}\, f = \big\{n \in \mathbb{Z}\colon\ n\,1_A = 0_A\big\},$$

est un *idéal* de $\mathbb{Z}$, c'est-à-dire est stable par addition-soustraction, et est stable par multiplication par un élément quelconque.

Or grâce à la division euclidienne dans $\mathbb{Z}$, nous avons démontré que tout idéal de $\mathbb{Z}$ est *principal*, *i.e.* de la forme $c\,\mathbb{Z}$ avec un certain entier $c \in \mathbb{N}$ fixé.

Donc par définition, la *caractéristique* de A est le générateur positif c de :

$$\mathsf{Ker}\, f = c\,\mathbb{Z}.$$

Lorsque $\mathsf{Ker}\, f = \{0\}$, ce qui correspond à $c = 0$, la caractéristique de A est 0.

Explicitement, la caractéristique de A est l'unique entier naturel $c \geqslant 1$ tel que :

$$\mathsf{Ker}\, f = c\,\mathbb{Z}.$$

Sans difficulté, on démontre que la caractéristique d'un anneau A est aussi l'unique entier $c \geqslant 0$ tel que $\mathbb{Z}/c\mathbb{Z}$ soit un sous-anneau unitaire de A.

On en déduit en particulier que si B est un sous-anneau unitaire de A, alors A et B ont même caractéristique. Ainsi, les anneaux de caractéristique nulle sont ceux dont $\mathbb{Z}$ est un sous-anneau unitaire. Ils sont donc de cardinal infini.

C'est le cas du corps $\mathbb{C}$ des nombres complexes et de tous ses sous-anneaux unitaires, comme le corps $\mathbb{R}$ des nombres réels ou le corps $\mathbb{Q}$ des nombres rationnels.

Le seul anneau dont la caractéristique vaut 1 est l'anneau nul $A = \{0_A\}$, que nous avons d'ailleurs exclu en supposant $1_A \neq 0_A$.

Proposition 7.2. *La caractéristique d'un anneau intègre est soit égale à 0, soit égale à un nombre premier p.*

Démonstration. En effet, soit comme ci-dessus $f\colon \mathbb{Z} \longrightarrow A$ l'application :

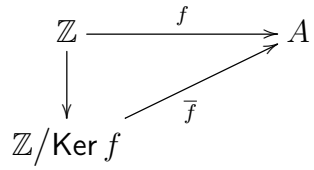
$$n \longmapsto n \cdot 1_A.$$

Son noyau est nécessairement de la forme $\mathsf{Ker}\, f = c\mathbb{Z}$, pour un certain $c \in \mathbb{N}$ fixé.

Grâce au théorème de factorisation vu dans le chapitre consacré à la théorie abstraite des groupes, nous en déduisons l'existence d'un morphisme d'anneaux :

$$\overline{f}\colon\quad \mathbb{Z}/c\mathbb{Z} \longrightarrow A,$$

provenant d'un diagramme de factorisation :



de telle sorte que $\overline{f}$ est *injectif*. Ainsi nous avons une bijection de $\mathbb{Z}/c\mathbb{Z}$ sur son image :

$$\mathbb{Z}/c\mathbb{Z} \ \xrightarrow{\sim}\ \overline{f}\big(\mathbb{Z}/c\mathbb{Z}\big) \qquad (\subset A).$$

Ainsi, l'image par $\overline{f}$ de notre anneau unitaire concret $\mathbb{Z}/c\,\mathbb{Z}$ est un sous-anneau unitaire de l'anneau unitaire A, lequel est par hypothèse *intègre*.

Comme tout sous-anneau unitaire d'un anneau unitaire intègre est aussi intègre (exercice), nous en déduisons que $\mathbb{Z}/c\,\mathbb{Z}$ est aussi *intègre*. Ça va, quand la Police l'interrogera, il n'aura rien à se reprocher !

Or dans le chapitre consacré à l'arithmétique, nous avons démontré que $\mathbb{Z}/c\,\mathbb{Z}$ est intègre si et seulement si ou bien $c = 0$ est nul, ou bien $c = p$ est un nombre premier. Monsieur l'agent, ceci conclut ! □

Proposition 7.3. *Si A est un anneau commutatif (unitaire), et si sa caractéristique est un nombre premier p, alors pour tous éléments x, y dans A, on a :*

$$(x+y)^p \ = \ x^p + y^p.$$

Démonstration. Le résultat découle de la formule du binôme de Newton et de ce que p divise les coefficients binomiaux apparaissant dans le développement, comme nous l'avons déjà vu dans le chapitre consacré à l'arithmétique sur $\mathbb{Z}$. □

L'application $x \longmapsto x^p$ est un endomorphisme de l'anneau A, appelé *endomorphisme de Frobenius*.

8. Caractéristique d'un corps

Soit maintenant $\mathbb{K}$ un corps commutatif, dans lequel $1 \neq 0$, sinon $\mathbb{K} = \{0\}$ est le corps à un élément seulement. Répétons en partie ce que nous venons de dire au sujet des anneaux, et additionnons 1 plusieurs fois :

$$1, \quad 1+1, \quad 1+1+1, \quad \ldots, \quad \underbrace{1+1+\cdots+1}_{m \text{ fois}}, \quad \ldots.$$

Écrivons alors en abrégé $m\,1$, ou $m \cdot 1$.

Comme $\mathbb{K}$ est un corps, on a ou bien $m \cdot 1 = 0$, ou bien $m \cdot 1 \neq 0$ possède un inverse dans $\mathbb{K}$. Il est possible que $m \cdot 1 \neq 0$ pour tout $m \geqslant 2$. Il est possible, aussi, qu'il existe $m \in \mathbb{N}_{\geqslant 2}$ tel que $m \cdot 1 = 0$.

L'énoncé suivant est en fait contenu dans la Proposition 7.2, mais nous le re-démontrons.

Proposition 8.1. *S'il existe, l'entier :*

$$p \ := \ \mathsf{min}\,\big\{m \in \mathbb{N}_{\geqslant 2} \colon \ m \cdot 1 = 0\big\}$$

est un nombre premier.

Preuve. Sinon, $p = q_1\, q_2$ avec $q_2, q_2 \geqslant 2$ premiers entre eux $1 = q_1 \wedge q_2$.

Mais alors, comme tout corps $\mathbb{K}$ est intègre, cela contredirait la minimalité de p :

$$0 \,=\, q_1\, q_2 \cdot 1 \,=\, q_1 \cdot 1\; q_2 \cdot 1 \qquad \Longrightarrow \qquad \Big(\; q_1 \cdot 1 = 0 \quad \text{ou} \quad q_2 \cdot 1 = 0 \;\Big). \qquad \square$$

Théorème 8.2. *Soit $\mathbb{K}$ un corps commutatif quelconque, dans lequel $1 \neq 0$. Alors l'une et l'une seulement des deux circonstances suivantes se produit.*

(1) *Ou bien il existe un entier minimal premier $p \in \mathbb{N}_{\geqslant 2}$ tel que :*

$$p \cdot 1 \,=\, 0 \qquad \Longrightarrow \qquad \Big(\; p \cdot \alpha \,=\, p \cdot 1\, \alpha \,=\, 0 \qquad \forall\, \alpha \,\in\, \mathbb{K} \;\Big).$$

(2) *Ou bien $m \cdot 1 \neq 0$ pour tout entier $m \in \mathbb{N}_{\geqslant 1}$. Dans ce cas, les deux applications :*

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{K} \\ m & \longmapsto & m \cdot 1 \end{array} \qquad \textit{et} \qquad \begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{K} \\ \frac{p}{q} & \longmapsto & p\, q^{-1} \cdot 1 \end{array}$$

sont injectives, et réalisent deux plongements *de $\mathbb{Z}$ et de $\mathbb{Q}$ dans $\mathbb{K}$.*

Par exemple, on sait que pour tout entier premier $p \geqslant 2$, les anneaux quotients $\mathbb{Z}/p\mathbb{Z}$ sont des corps.

Terminologie 8.3. Dans le cas **(2)**, on dit que $\mathbb{K}$ est de *caractéristique zéro*, ou *nulle*.

Dans le cas **(1)**, on dit que $\mathbb{K}$ est de *caractéristique* p.

Démonstration. Le cas **(1)** ayant déjà été expliqué, supposons donc comme en **(2)** que $m \cdot 1 \neq 0$ pour tout entier $m \in \mathbb{N}_{\geqslant 1}$. Alors $-\,m \cdot 1 \neq 0$ aussi, donc $m \cdot 1 \neq 0$ pour tout $m \in \mathbb{Z}^*$.

L'injectivité de l'application $m \longmapsto m \cdot 1$ est alors claire :

$$m \cdot 1 \,=\, m' \cdot 1 \qquad \Longrightarrow \qquad (m - m') \cdot 1 \,=\, 0 \qquad \Longrightarrow \qquad m \,=\, m'.$$

Ensuite, soit une fraction irréductible $\frac{p}{q} \in \mathbb{Q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}_{\geqslant 1}$. Comme $q \cdot 1 \neq 0$ par hypothèse, il en existe un inverse dans le corps $\mathbb{K}$, que l'on note $q^{-1} \cdot 1 \neq 0$. Puis, pour tout $p \in \mathbb{Z}$, on introduit $p \cdot q^{-1} \cdot 1$ la somme de p fois le même terme $q^{-1} \cdot 1$.

Assertion 8.4. *En caractéristique zéro, pour $p \neq 0 \neq q$ entiers, on a $p\, q^{-1} \cdot 1 \neq 0$.*

Preuve. Sinon, si $p\, q^{-1} \cdot 1 = p \cdot q^{-1} \cdot 1 = 0$, en multipliant par q, c'est à dire en additionnant q fois $p\, q^{-1} \cdot 1$, on obtiendrait $p \cdot 1 = 0$, contrairement à l'hypothèse **(2)**. $\square$

Enfin, ceci implique que l'application $\frac{p}{q} \longmapsto p\, q^{-1} \cdot 1$ est injective :

$$\begin{aligned} p\, q^{-1} \cdot 1 \,=\, p'\, q'^{-1} \cdot 1 \qquad &\Longrightarrow \qquad \big(p\, q' - q\, p'\big) \cdot 1 \,=\, 0 \\ &\Longrightarrow \qquad pq' - qp' \,=\, 0 \qquad \Longrightarrow \qquad \frac{p}{q} \,=\, \frac{p'}{q'}. \end{aligned} \qquad \square$$

9. Exercices

Exercice 1. Soit un anneau $\big(A, +, \times\big)$ dans lequel $1_A = 0_A$. Montrer que $A = \{0_A\}$.

Exercice 2. Soit $\big(A, +, \times\big)$ un anneau général, au sens de la Définition 2.2, d'éléments neutres 0_A pour l'addition $+$, et 1_A pour la multiplication $\times$.

(a) Montrer que $a \times 0_A = 0_A = 0_A \times a$, pour tout $a \in A$.

(b) Montrer que $a \times (-b) = -(a \times b) = (-a) \times b$, pour tous $a, b \in A$.

(c) Montrer que $(-a) \times (-b) = a \times b$, pour tous $a, b \in A$.

Exercice 3. On rappelle la formule du binôme, valable pour $x, y \in \mathbb{R}$, et pour un exposant entier $n \in \mathbb{N}$:

$$\big(x+y\big)^n \;=\; \sum_{k=0}^{n} \binom{n}{k} x^k \, y^{n-k},$$

où :

$$\binom{n}{k} \;:=\; \frac{n!}{k!\,(n-k)!} \qquad (0 \leqslant k \leqslant n).$$

L'objectif est de généraliser cette formule à des anneaux quelconques.

(a) Montrer les relations de récurrence :

$$\binom{n+1}{k+1} \;=\; \binom{n}{k} + \binom{n}{k+1}.$$

(b) Soit un anneau $\big(A, +, \times\big)$, pas forcément commutatif. Pour deux éléments $a, b \in A$, est-il légitime d'écrire :

$$\big(a+b\big)^2 \;\overset{?}{=}\; a^2 + 2\,ab + b^2 \,?$$

(c) Pour $m \in \mathbb{N}$ et $a \in A$, on pose $m\,a := a + \cdots + a$, avec m termes, ainsi que $a^m := a \times \cdots \times a$, de nouveau avec m termes. Vérifier que :

$$\big(a+b\big)^2 \;=\; a^2 + 2\,ab + b^2 \qquad\qquad \Longleftrightarrow \qquad\qquad a\,b \;=\; b\,a.$$

(d) On suppose dorénavant que deux éléments donnés $a, b \in A$ *commutent*, au sens où $a \times b = b \times a$, c'est-à-dire $a\,b = b\,a$. Montrer que :

$$\begin{aligned}
\big(a+b\big)^3 \;&=\; a^3 + 3\,a^2\,b + 3\,a\,b^2 + b^3, \\
\big(a+b\big)^4 \;&=\; a^4 + 4\,a^3\,b + 6\,a^2\,b^2 + 4\,a\,b^3 + b^4.
\end{aligned}$$

(e) Montrer, pour $k, \ell \in \mathbb{N}$, que :

$$a^k\,b^\ell\,a \;=\; a^{k+1}\,b^\ell \qquad\qquad \text{et} \qquad\qquad b\,a^k\,b^\ell \;=\; a^k\,b^{\ell+1}.$$

(f) Établir la formule du binôme :

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

Exercice 4. EE

Exercice 5. EE