Anneaux et corps

Cornou Jean-Louis

6 décembre 2023

À la différence des groupes, nous considérons à présent des ensembles munis de **deux** lois de composition interne. Celles-ci auront des rôles distincts et il convient de repérer les propriétés des groupes applicables, et celles qui ne le sont pas dans le cadre des anneaux. Le chapitre est assez court et s'illustrera notamment dans le cadre de $\mathbb{C}$. On dispose de peu d'anneaux non commutatifs à ce stade de l'année pour les illustrations.

1 Notion d'anneau

Définition 1 *Soit* E *un ensemble,* $\star$ *et* $\dashv$ *deux lois de composition interne sur* E*. On dit que* $\star$ *est distributive par rapport à* $\dashv$ *lorsque*

$$\forall (x,y,z) \in E^3, \quad x \star (y \dashv z) = (x \star y) \dashv (x \star z), \quad (x \dashv y) \star z = (x \star z) \dashv (y \star z)$$

Définition 2 *On appelle anneau un triplet* $(A,+,\times)$ *formé d'un ensemble* A *et de deux lois de composition interne* $+$ *et* $\times$ *sur* A *vérifiant les conditions suivantes :*

- $(A,+)$ *est un groupe commutatif.*
- $(A,\times)$ *est un magma associatif unifère (ou encore un monoïde).*
- *La loi* $\times$ *est distributive par rapport à la loi* $+$*.*

Lorsque le magma $(A,\times)$ *est de plus commutatif, on dit que* A *est un anneau commutatif.*

⚠ **Attention**
On ne requiert pas que $(A,\times)$ *soit un groupe ! Autrement dit, l'inversibilité pour la loi* $\times$ *n'est pas requise pour tous les éléments de* A*.*

Notation
Pour la suite du cours, on notera 0_A *le neutre de* $(A,+)$ *et* 1_A *le neutre de* $(A,\times)$*. Leurs existences viennent de la définiton d'anneau, leurs unicités ont été prouvées dans le début du cours sur les groupes, chapitre sur les monoïdes. Pour tout* a *dans* A*, son inverse pour la loi* $+$ *(on dira plutôt son opposé), est noté* $-a$*. On raccourcit l'écriture* $b+(-a)$ *en* $b-a$*. Pour tout* n *dans* $\mathbb{N}^*$*, tout* a *dans* A*, on note* $na = \underbrace{a+a+\cdots+a}_{n \text{ fois}}$*,* $0_{\mathbb{Z}}a = 0_A$*, pour tout* n *dans* $\mathbb{Z}\backslash\mathbb{N}$*, on note* $na = (-n)(-a) = \underbrace{(-a)+(-a)+\cdots+(-a)}_{-n \text{ fois}}$*. Pour tout* n *dans* $\mathbb{N}^*$*, tout* a *dans* A*, on note* $a^n = \underbrace{a \times a \times \cdots \times a}_{n \text{ fois}}$*. On convient que* $a^{0_{\mathbb{N}}} = 1_A$*. Attention, comme on ne suppose pas que* a *possède un inverse dans* $(A,\times)$*, on ne peut pas manipuler a priori la notation* a^n *avec* $n \in \mathbb{Z}\backslash\mathbb{N}$*.*

Exemple 1 *L'exemple fondamental d'anneau est l'anneau* $(\mathbb{Z},+,\times)$*. Notez que seuls les éléments* 1 *et* -1 *de cet anneau sont inversibles pour la loi* $\times$*. Vous connaissez également* $(\mathbb{Q},+,\times)$*,* $(\mathbb{R},+,\times)$*,* $(\mathbb{C},+,\times)$*. Ceux-ci ont la particularité que tout élément non nul est inversible pour la loi* $\times$*.*

A présent quelques propriétés classiques de calcul dans un anneau :

Propriété 1 *Soit* $(A,+,\times)$ *un anneau. Alors*

$$\forall x \in A, \quad x \times 0_A = 0_A \times x = 0_A, \quad x \times (-1_A) = (-1_A) \times x = -x.$$

On dit que 0_A *est absorbant pour la loi* $\times$*.*

Démonstration. Soit $x \in A$.

$$\begin{aligned} x \times 0_A &= x \times (0_A + 0_A) && 0_A \text{ neutre de } + \\ &= x \times 0_A + x \times 0_A && \text{distributivité} \end{aligned}$$

On additionne l'opposé de $x \times 0_A$ à cette égalité, ce qui fournit $x \times 0_A - x \times 0_A = x \times 0_A + x \times 0_A - x \times 0_A$, soit encore par associativité de $+$, $0_A = x \times 0_A + 0_A$. Comme 0_A est le neutre de $+$, on en déduit $0_A = x \times 0_A$.
Pour l'autre sens, on procède de même :

$$0_A \times x = (0_A + 0_A) \times x = 0_A \times x + 0_A \times x$$

Après addition de l'opposé de $0_A \times x$, on obtient

$$0_A = 0_A \times x - 0_A \times x = 0_A \times x + 0_A \times x - 0_A \times x = 0_A \times x + 0_A = 0_A \times x$$

$$\begin{aligned} x \times (-1_A) + x &= x \times (-1_A) + x \times 1_A && 1_A \text{ neutre de } \times \\ &= x \times (-1_A + 1_A) && \text{distributivité} \\ &= x \times 0_A && -1_A \text{ est l'opposé de } 1_A \\ &= 0 && \text{car } 0_A \text{ est absorbant} \end{aligned}$$

On procède de même pour l'autre sens

$$x + x \times (-1_A) = x \times 1_A + x \times (-1_A) = x \times (1_A - 1_A) = x \times 0_A = 0_A$$

Ces deux égalités prouvent que $x \times (-1_A)$ est l'opposé de x, i.e $-x$. L'égalité $(-1_A) \times x = -x$ résulte des mêmes manipulations en exploitant la distributivité à gauche.

Exercice 1 *En déduire que si* $(A, +, \times)$ *est un anneau vérifie que* $(A, \times)$ *est un groupe, alors* A *est réduit à un seul élément.*

Propriété 2 (Binôme) *Soit* $(A, +, \times)$ *un anneau, a et b deux éléments de* A *tels que* $a \times b = b \times a$ *(on dit que a et b commutent). Alors pour tout entier naturel n,*

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

Démonstration. On procède par récurrence comme dans le cas classique des réels ou des complexes. Pour tout entier naturel n, on note $\mathcal{P}(n)$ l'assertion : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$. Initialisons : pour $n = 0$, on a convenu que $(a+b)^0 = 1_A$. D'autre part, $\sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k} = \binom{0}{0} a^0 b^0 = 1_{\mathbb{Z}} 1_A 1_A = 1_A$, donc $\mathcal{P}(0)$ est vraie.
Hérédité : soit $n \in \mathbb{N}$, supposons $\mathcal{P}(n)$ vraie et démontrons que $\mathcal{P}(n+1)$ l'est. La distributivité et l'assertion $\mathcal{P}(n)$ donnent

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

Comme a et b commutent, pour tout k dans $[\![0, n]\!]$, $b a^k b^{n-k} = a^k b^{n+1-k}$. Dans la première somme, on effectue le changement d'indice $j = k + 1$, ce qui entraîne

$$\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} = \sum_{j=1}^{n+1} \binom{n}{j-1} a^j b^{n+1-j}$$

Comme l'addition dans un anneau est commutative, on peut regrouper les deux sommes

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

puisque l'indice de sommation est muet, et on a les conventions $\binom{n}{-1} = 0$ et $\binom{n}{n+1} = 0$. On utilise alors la formule de Pascal :

$$\forall k \in [\![0, n+1]\!], \binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

et on obtient

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

ce qui démontre l'assertion $\mathcal{P}(n+1)$.

⚠ **Attention**
Sans hypothèse de commutation entre a et b, ce résultat est faux. Cela sera capital lors du calcul matriciel par exemple. On développera à la main $(a+b)^2 = a^2 + ab + ba + b^2$.

Propriété 3 *Soit $(A, +, \times)$ un anneau, a et b deux éléments de A tels que $a \times b = b \times a$ (on dit que a et b commutent). Alors pour tout entier naturel n,*

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

Démonstration. Pour $n = 0$, la somme est vide et vaut alors par convention 0_A. Comme 0_A est absorbant, cette égalité revient à vérifier $0_A = 1_A - 1_A = 0_A$, qui est vraie. Soit à présent $n \in \mathbb{N}^*$.

$$\begin{aligned}
(a-b)\sum_{k=0}^{n-1} a^k b^{n-k-1} &= a\sum_{k=0}^{n-1} a^k b^{n-k-1} - b\sum_{k=0}^{n-1} a^k b^{n-k-1} && \text{distributivité}\\
&= \sum_{k=0}^{n-1} a^{k+1} b^{n-k-1} - \sum_{k=0}^{n-1} a^k b^{n-k} && \text{car } a \text{ et } b \text{ commutent}\\
&= \sum_{j=1}^{n} a^j b^{n-k} - \sum_{k=0}^{n-1} a^k b^{n-k} && \text{changement d'indice } j = k+1 \text{ dans la première somme}\\
&= a^n b^{n-n} - a^0 b^{n-0} && \text{télescopage}\\
&= a^n - b^n
\end{aligned}$$

Exercice 2 *Soit E un ensemble, on examine la structure $(\mathcal{P}(E), \Delta, \bigcap)$. Montrer qu'il s'agit d'un anneau. Vérifier la cohérence des propriétés calculatoires précédentes.*

2 Construction d'anneaux

Propriété 4 *Soit $(A, +, \times)$ et $(B, +\times)$ deux anneaux. Leurs lci sont notées avec les mêmes symboles pour alléger les notations. Les applications $(A \times B)^2 \to A \times B, (a_1, b_1, a_2, b_2) \mapsto (a_1 + a_2, b_1 + b_2)$ et $(A\times B)^2 \to A\times B, (a_1, b_1, a_2, b_2) \mapsto (a_1 \times a_2, b_1 \times b_2)$ munissent l'ensemble $A\times B$ d'une structure d'anneau. Le triplet $(A \times B, +, \times)$ est appelé anneau produit de A et B.*

Démonstration. On propose une démonstration allégée pour ne pas crouler sous 3 pages de trivialités.

- La structure $(A\times B, +)$ est un groupe d'après ce qui a été établi sur les groupes produits. D'autre part, comme $(A, +)$ et $(B, +)$ sont commutatifs, $(A \times B, +)$ est un groupe commutatif.
- La structure $(A \times B, \times)$ est un monoïde en reprenant la même démonstration que celle des groupes produits en enlevant l'étape sur les déterminations d'inverses. Le neutre multiplicatif de $A \times B$ est en particulier, $(1_A, 1_B)$.
- La distributivité se vérifie composante par composante via celles de A et B, donc est valide sur $A \times B$.

Exemple 2 *Pour tout entier n non nul, $(\mathbb{Z}^n, +, \times)$ est un anneau, $(\mathbb{C}^n, +, \times)$ est un anneau.*

Définition 3 *Soit X un ensemble et $(A, +\times)$ un anneau. Pour tout couple (f, g) de $\mathcal{F}(X, A)$, on définit*

- $f + g : X \to A, x \mapsto f(x) + g(x)$.
- $f \times g : X \to A, x \mapsto f(x) \times g(x)$.

Propriété 5 *Avec les mêmes notations que précédemment, la structure $(\mathcal{F}(X, A), +, \times)$ est un anneau. Son neutre additif est l'application constante égale à 0_A, son neutre multiplicatif est l'application constante égale à 1_A.*

Démonstration. Adapter la preuve sur les groupes $\mathcal{F}(X, G)$. Vérifier plus spécifiquement la commutativité de $(\mathcal{F}(X, A), +)$ et la distributivité.

Exemple 3 *On peut voir $\mathbb{C}^{n^2}$ comme l'ensemble $\mathcal{F}([\![1, n]\!]^2, \mathbb{C})$ et ainsi le munir de la structure d'anneau découlant de celle de $(\mathbb{C}, +, \times)$.*

Exercice 3 *Montrer que ces structures héritent de la commutativité des anneaux* A, B *le cas échéant.*

Exemple 4 *Afin de disposer d'exemples pertinents, on va donner des exemples d'anneaux de cardinal* 4. *Comme dans le cas des groupes, on peut décrire leurs lois de composition interne via des tables de Cayley. Comme ces anneaux sont non réduits à un élément, on sait que leurs neutres additifs et multiplicatifs sont distincts. Soit* A *un tel anneau, on le liste sous la forme* $A = \{0, 1, a, b\}$. *On dispose d'entre autres deux façons de construire des tables pour cet ensemble*

$+$	0	1	a	b
0	0	1	a	b
1	1	a	b	0
a	a	b	0	1
b	b	0	1	a

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	0	a
b	0	b	a	1

Ceci définit une structure d'anneau commutatif sur A, *souvent notée* $\mathbb{Z}/4\mathbb{Z}$. *Nous la retrouverons en arithmétique à l'aide des congruences. Il existe une autre structure d'anneau sur* A *donnée par les tables suivantes :*

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Cette dernière structure est encore commutative, mais tout élément non nul possède un inverse multiplicatif à la différence de $\mathbb{Z}/4Z$ *pour lequel a n'a pas d'inverse multiplicatif. Cette structure est souvent notée* $\mathbb{F}_4$.

Exemple 5 *Considérons l'ensemble* $A = \mathbb{R}^{[[1,2]]^2}$. *Il s'agit des familles de réels indexés par les couples de* $[[1,2]]^2$. *On note typiquement un élément de* A *sous la forme* $\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$. *On le munit des deux lois suivantes :*

$$+ : \left(\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}, \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} \right) \mapsto \begin{pmatrix} a_{1,1} + b_{1,1} & a_{1,2} + b_{1,2} \\ a_{2,1} + b_{2,1} & a_{2,2} + b_{2,2} \end{pmatrix}$$

$$\times \left(\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}, \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} \right) \mapsto \begin{pmatrix} a_{1,1}b_{1,1} + a_{1,2}b_{2,1} & a_{1,1}b_{1,2} + a_{1,2}b_{2,2} \\ a_{2,1}b_{1,1} + a_{2,2}b_{2,1} & a_{2,2}b_{1,2} + a_{2,2}b_{2,2} \end{pmatrix}$$

On peut montrer qu'il s'agit d'un anneau de neutre additif $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ *et de neutre multiplicatif* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Attention, ce n'est pas la même structure que la structure produit où l'on multiplie les n^2*-uplets composante par composante. Une façon de s'en rendre compte est d'examiner la commutativité de la loi* $\times$.

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \quad \textit{tandis que} \quad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

On note cette structure $(\mathcal{M}_2(\mathbb{R}), +, \times)$.

3 Sous-anneaux

On fixe $(A, +, \times)$ un anneau dans cette partie.

Définition 4 *Soit* B *une partie de* A. *On dit que* B *est un sous-anneau de* A *lorsque*

— B *est stable par* $+$ *et* $\times$

— $1_A \in B$.

— $(B, +_B, \times_B)$ *est un anneau.*

☞ **Remarque**
Le critère $1_A \in B$ *est nécessaire pour disposer de bonnes structures. En effet, avec l'exemple des matrices* 2×2 *précédent, on peut considérer l'élément* $M = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. *Celui-ci vérifie* $M^2 = M$ *et la partie* $\{M\}$ *est stable par multiplication, mais il n'y a pas de bonnes interactions avec la structure « cadre »* $\mathcal{M}_2(\mathbb{R})$.

Propriété 6 *Si* B *est un sous-anneau de* A, *alors son neutre multiplicatif* 1_B *est égal à* 1_A.

Démonstration. En effet, 1_A appartient à B et est un neutre pour la loi induite $\times_B$. Par unicité du neutre, $1_B = 1_A$.

Théorème 1 (Caractérisation des sous-anneaux) *Soit* B *une partie de* A. *On a l'équivalence :* B *est un sous-anneau de* A *si et seulement si*

- $(B, +)$ *est un sous-groupe de* $(A, +)$,
- $\forall (x, y) \in B^2, x \times y \in B$.
- $1_A \in B$.

Démonstration. Supposons que B est un sous-anneau et montrons que les trois critères annoncés sont vérifiés.

- D'une part, B est bien stable par $+$. D'autre part, $(B, +_B, \times_B)$ est un anneau, donc $(B, +_B)$ est un groupe. Conclusion, $(B, +)$ est un sous-groupe de $(A, +)$.
- D'après la définition d'un sous-anneau, B est stable par $\times$, donc $\forall (x, y) \in B^2, x \times y \in B$.
- Le troisième critère fait partie de la définition de sous-anneau.

Réciproquement, supposons que B vérifie les trois critères précédents et démontrons que B est un sous-anneau de A.

- $(B, +)$ est un sous-groupe de $(A, +)$, donc B est stable par $+$. D'autre part, le second critère donne la stabilité de B par $\times$.
- Comme $(B, +)$ est un sous-groupe de $(A, +)$, $(B, +_B)$ est un groupe. D'autre part, soit $(x, y) \in B^2$, comme $(A, +)$ est commutatif, $x +_B y = x + y = y + x = y +_B x$, donc $(B, +_B)$ est un groupe commutatif. $(B, \times_B)$ contient 1_A qui est un neutre pour $\times_B$ donc $(B, \times_B)$ est unifère. D'autre part, il hérite de l'associativité de $\times$ dans A, donc $(B, \times_B)$ est un monoïde. La distributivité de $\times_B$ sur $+_B$ découle de la distributivité de $\times$ sur $+$. Conclusion, $(B, +_B, \times_B)$ est un anneau.
- $1_A \in B$ est vérifié.

⚠ **Attention**
Ne pas oublier le critère $1_A \in B$. *La partie* $2\mathbb{Z}$ *des entiers relatifs pairs est un sous-groupe additif de* $\mathbb{Z}$ *stable par multiplication, mais ce n'est pas un sous-anneau de* $\mathbb{Z}$ *car il ne contient pas* 1. *C'est la grande différence par comparaison avec les sous-groupes.*

On dispose d'une caractérisation plus maniable des sous-anneaux.

Théorème 2 *Soit* $(A, +, \times)$ *un anneau et* B *une partie de* A. *Alors* B *est un sous-anneau de* A *si et seulement si*

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

Démonstration. Supposons que B est un sous-anneau de A. Alors B contient 1_A. Comme $(B, +_B)$ est un sous-groupe, B contient -1_A. De plus, B est stable par $+$ et $\times$.
Réciproquement, supposons que B vérifie les trois critères précédents et montrons que c'est un sous-anneau de A. B est non vide car il contient -1_A et pour tous éléments x, y de B, $x - y = x + (-1_A) \times y$ d'après les règles de calcul dans les anneaux. Comme B est stable par $+, \times$ et contient -1_A, $x - y \in B$. On en déduit que $(B, +)$ est un sous-groupe de $(A, +)$. De plus, B est stable par $\times$. Enfin, $(-1_A) \times (-1_A) = 1_A$, donc $1_A \in B$. Ainsi, B vérifie tous les critères de la première caractérisation des sous-anneaux, donc est un sous-anneau de A.

Exemple 6 *Sous-anneaux quadratiques de* $\mathbb{C}$.
On fixe ω *un complexe et on note* $\mathbb{Z}[\omega] = \{n + m\omega | (n, m) \in \mathbb{Z}^2\}$. *On cherche une condition nécessaire et suffisante sur* ω *pour que* $\mathbb{Z}[\omega]$ *soit un sous-anneau de* $\mathbb{C}$. *Supposons que cet ensemble le soit, alors il est stable par produit. Comme* $\omega = 0 + 1 \times \omega \in \mathbb{Z}[\omega]$, *on en déduit que* $\omega^2 \in \mathbb{Z}[\omega]$, *i.e* $\exists (\alpha, \beta) \in \mathbb{Z}^2, \omega^2 =$

$\alpha\omega+\beta$. On va chercher à savoir si cela suffit. Supposons donc $\exists(\alpha,\beta)\in\mathbb{Z}^2, \omega^2=\alpha\omega+\beta$ et montrons que $\mathbb{Z}[\omega]$ est un sous-anneau de $\mathbb{C}$. On remarque que $-1=-1+0\times\omega\in\mathbb{Z}[\omega]$. Soit $(x,y)\in\mathbb{Z}[\omega]^2$. On dispose d'entiers relatifs (n,m,p,q) tels que $x=n+m\omega$ et $y=p+q\omega$. On en déduit $x+y=(n+p)+(m+q)\omega$ où $n+p\in\mathbb{Z}$ et $m+q\in\mathbb{Z}$, soit $x+y\in\mathbb{Z}[\omega]$. D'autre part, $xy=(np+mq\beta)+(qn+mp+mq\alpha)\omega$ où $np+mq\beta\in\mathbb{Z}$ et $qn+mp+mq\alpha\in\mathbb{Z}$, ce qui démontre $xy\in\mathbb{Z}[\omega]$.
Ces anneaux d'apparence anodine sont la source de toute l'arithmétique moderne. On peut prouver le théorème des deux carrés via $\mathbb{Z}[i]$ l'anneau des entiers de Gauss, la résolution de $x^3+y^3=z^3$ passe entre autres par l'anneau $\mathbb{Z}[j]$ des entiers d'Eisenstein. Certains possèdent des propriétés arithmétiques similaires à $\mathbb{Z}$ comme la division euclidienne. D'autres présentent des propriétés arithmétiques très distinctes : $\mathbb{Z}[i\sqrt{5}]$ ne possède pas de factorisation unique en facteurs premiers comme $\mathbb{Z}$: $(2+i\sqrt{5})(2-i\sqrt{5})=9=3^2$ donne deux factorisations distinctes de 9 dans cet anneau.

Propriété 7 *Soit $(A,+,\times)$ un anneau et B un sous-anneau de A. Si A est commutatif, alors B est commutatif.*

Démonstration. Laissée à titre d'exercice.

⚠ **Attention**
La réciproque est fausse. Un anneau non commutatif peut contenir des sous-anneaux commutatifs. Dans l'exemples des matrices 2×2 sur $\mathbb{R}$, la partie

$$\left\{\begin{pmatrix}a&0\\0&a\end{pmatrix}\,|\,a\in\mathbb{R}\right\}$$

est un sous-anneau commutatif, bien que l'anneau cadre ne le soit pas!

4 Morphismes d'anneaux

On fixe $(A,+_A,\times_A)$ et $(B,+_B,\times_B)$ deux anneaux dans cette partie du cours.

Définition 5 *Soit $f:A\to B$ une application. On dit que c'est un morphisme d'anneaux lorsque*

- $\forall(a_1,a_2)\in A^2, f(a_1+_A a_2)=f(a_1)+_B f(a_2)$.
- $\forall(a_1,a_2)\in A^2, f(a_1\times_A a_2)=f(a_1)\times_B f(a_2)$.
- $f(1_A)=1_B$.

⚠ **Attention**
Il ne faut pas oublier le dernier critère de conservation du neutre « multiplicatif ». L'application $\mathbb{Z}\to\mathbb{Z}, n\mapsto 0$ est additive et multiplicative, mais ne conserve pas 1. Ce n'est pas un morphisme d'anneaux. A l'inverse, il ne faut pas rajouter ce critère de conservation du neutre dans les morphismes de groupes car c'est une conséquence de la structure de groupe.

Propriété 8 *Soit $(A,+,\times)$ un anneau. L'application $\varphi:\mathbb{Z}\to A, n\mapsto n1_A$ est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A. Il est parfois appelé morphisme caractéristique de A. (On dit que $\mathbb{Z}$ est un objet initial dans la catégorie des anneaux)*

Démonstration. On rappelle que pour tout entier naturel n, la notation $n1_A$ désigne $\underbrace{1_A+1_A+\dots1_A}_{n\text{ termes}}$, que $0_\mathbb{Z}1_A$ désigne 0_A et que pour tout entier relatif strictement négatif, $n1_A$ désigne $(-n)(-1_A)$. Il s'ensuit via des récurrences classiques : $\forall(n,m)\in\mathbb{Z}^2, (n+m)1_A=n1_A+m1_A$ et $(nm)1_A=n1_A\times m1_A$. Enfin, $\varphi(1_\mathbb{Z})=1_A$, ce qui démontre que φ est un morphisme d'anneau.
Soit ψ un morphisme d'anneau de $\mathbb{Z}$ dans A. Alors $\psi(1_\mathbb{Z})=1_A$. On mène alors une récurrence pour prouver $\forall n\in\mathbb{N}^*, \psi(n)=n1_A$. Comme ψ est un morphisme de groupe additif, $\psi(0_\mathbb{Z})=0_A$, ce qui permet de prouver $\forall n\in\mathbb{Z}, \psi(n)=n1_A$. Il reste encore des récurrences à traiter pour vérifier $\forall(n,m)\in\mathbb{Z}^2, \psi(nm)=n1_A\times m1_A$. Conclusion, ψ est nécessairement égal à φ.

Propriété 9 *La composée de morphisme d'anneaux est un morphisme d'anneaux.*

Définition 6 *On appelle isomorphisme d'anneaux tout morphisme d'anneaux bijectif.*

Propriété 10 *Soit $f : A \to B$ un isomorphisme d'anneaux. Alors sa réciproque $f^{-1} : B \to A$ est un morphisme d'anneaux.*

Démonstration. Comme f est un morphisme d'anneaux, c'est en particulier un morphisme de groupes de $(A,+)$ vers $(B,+)$. On a déjà prouvé que sa réciproque est un morphisme de groupes de $(B,+)$ vers $(A,+)$. D'autre part, $f(1_A) = 1_B$, donc $f^{-1}(1_B) = 1_A$. Il reste à prouver la multiplicativité. Soit $(b_1, b_2) \in B^2$. On note $a_1 = f^{-1}(b_1)$ et $a_2 = f^{-1}(b_2)$. Comme f est un morphisme d'anneaux,

$$f(a_1 \times a_2) = f(a_1) \times f(a_2)$$

En appliquant f^{-1}, on obtient

$$a_1 \times a_2 = f^{-1}(b_1 \times b_2)$$

soit encore

$$f^{-1}(b_1) \times f^{-1}(b_2) = f^{-1}(b_1 \times b_2)$$

Les morphismes d'anneaux héritent des caractérisations d'injectivité et de surjectivité de celles des morphismes de groupes additifs.

Définition 7 *Soit $f : A \to B$ un morphisme d'anneaux. On appelle image de f l'ensemble $f(A)$, et noyau de f, l'ensemble $f^{-1}(\{0_B\})$.*

⚠ **Attention**
Le noyau de f est l'image réciproque du neutre additif de B, et non de son neutre multiplicatif.

Propriété 11 *Soit $f : A \to B$ un morphisme d'anneaux. Alors f est surjective si et seulement si son image vaut B. f est injective si et seulement si son noyau est réduit à $\{0_A\}$.*

Démonstration. Comme f est un morphisme de groupes de $(A,+)$ dans $(B,+)$, cette caractérisation a déjà été établie.

Propriété 12 *Soit $f : A \to B$ un morphisme d'anneaux, C un sous-anneau de A et D un sous-anneau de B. Alors $f(C)$ est un sous-anneau de B et $f^{-1}(D)$ est un sous-anneau de A.*

Démonstration. La partie sur les sous-groupes a déjà été traitée. Calquer la preuve des morphismes de groupes pour la partie multiplicative. Le seul critère nouveau porte sur le neutre multiplicatif. Comme C est un sous-anneau de A, il contient 1_A, mais alors $f(C)$ contient $f(1_A) = 1_B$. De manière similaire, D est un sous-anneau de B, donc contient 1_B. Comme $f(1_A) = 1_B$, on en déduit que $1_A \in f^{-1}(D)$.

5 Eléments particuliers d'un anneau

On fixe $(A,+,\times)$ un anneau. Faisons un peu de zoologie dans A.

Définition 8 *Soit $a \in A$. On dit que a est*

- *nilpotent lorsque $\exists n \in \mathbb{N}^*, a^n = 0_a$.*
- *idempotent lorsque $a^2 = a$.*

Exemple 7 *Dans $\mathbb{Z}/4\mathbb{Z}$, l'élément a est nilpotent car $a^2 = 0$. Le neutre multiplicatif 1_A est toujours idempotent. Dans $\mathcal{M}_2(\mathbb{R})$, l'élément $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ est idempotent.*

Définition 9 *Soit $a \in A$. On dit que a est un élément central lorsque*

$$\forall b \in A, b \times a = a \times b$$

i.e lorsque a commute avec tous les éléments de A.

Exemple 8 *Les neutres additifs et multiplicatifs sont centraux.*

Définition 10 *Soit $a \in A$. On dit que a est un diviseur de zéro lorsqu'il est non nul et*

$$\exists b \in A \backslash \{0_A\}, a \times b = 0_A \wedge b \times a = 0_A$$

Un élément de A qui est ni nul, ni un diviseur de zéro est appelé régulier.

Exemple 9 *Dans* $\mathcal{M}_2(\mathbb{R})$*, l'élément* $P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ *est un diviseur de zéro car l'élément non nul* $Q = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ *vérifie* $PQ = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ *et* $QP = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Définition 11 *Soit* $(A, +, \times)$ *un anneau. On dit que* A *est intègre lorsqu'il est non réduit à* 0_A*, commutatif (rappellons que cela concerne la loi* $\times$*) et quand tous ses éléments non nuls sont réguliers. Autrement dit,* A *ne possède pas de diviseurs de zéro.*

Exemple 10 $(\mathbb{C}, +, \times)$ *et tous ses sous-anneaux sont intègres.*

Propriété 13 *La règle du produit nul est valable dans les anneaux intègres, i.e*

$$\forall (a, b) \in A^2, (a \times b = 0_A \iff [a = 0_A \vee b = 0_A])$$

Démonstration. Soit $(a, b) \in A^2$. Si $a = 0_A$ ou $b = 0_A$ alors $a \times b = 0_A$ car le neutre 0_A est absorbant. Réciproquement, supposons $a \times b = 0_A$ et $a \neq 0_A$. Comme A est intègre, a n'est pas un diviseur de zéro, donc $b = 0_A$.

Propriété 14 *Soit* $(A, +, \times)$ *un anneau intègre et* B *un sous-anneau non nul de* A*. Alors* B *est intègre.*

Démonstration. Laissée à titre d'exercice.

Définition 12 *Soit* $x \in A$*.* x *est dit inversible s'il est inversible pour la loi* $\times$*, i.e*

$$\exists y \in A, y \times x = x \times y = 1_A$$

⚠ **Attention**
Il s'agit bien de symétrique pour la loi $\times$*. La structure* $(A, +)$ *est un groupe donc tout élément* a *de* A *admet un symétrique pour la loi* $+$*, que l'on a noté* $-a$*.*

Notation
Comme $(A, \times)$ *est un magma associatif unifère, il y a unicité de l'inverse en cas d'existence, celui-ci est alors noté* x^{-1}*.*

Théorème 3 *L'ensemble des éléments inversibles de* A*, muni de la loi* $\times$ *est un groupe. Il est noté* $A^\times$*.*

Démonstration. On ne dispose pas de grande structure de groupe dans laquelle « plonger » $(A^\times, \times)$. Il faut revenir à la définition d'un groupe.

- Démontrons que $A^\times$ est stable par $\times$, ce qui légitime l'écriture de la structure $(A^\times, \times)$. On a vu dans le début du cours sur les groupes que dans un magma associatif unifère, le produit de deux éléments inversibles $x \star y$ est inversible (d'inverse $y^{-1} \star x^{-1}$).
- Comme $(A, +, \times)$ est un anneau, $(A, \times)$ est associatif. Ainsi, $(A^\times, \times)$ est associatif.
- Comme 1_A est le neutre de $(A, \times)$, $1_A \times 1_A = 1_A \times 1_A = 1_A$, ce qui prouve que 1_A est inversible (d'inverse 1_A), il appartient à $A^\times$.
- Il nous reste à montrer que tout élément de $A^\times$ admet un inverse pour $\times$. Soit $x \in A^\times$. Comme x est inversible dans l'anneau, il admet un inverse y dans A qui vérifie

  $$y \times x = x \times y = 1_A$$

  Cela démontre que l'élément y est inversible d'inverse x, i.e $y \in A^\times$. Résumons : tout élément de $A^\times$ possède un inverse dans $A^\times$ pour la loi $\times$.

Exemple 11 $\mathbb{Z}^\times = \{-1, 1\}$ *est le groupe à deux éléments,* $\mathbb{C}^\times = \mathbb{C}^*$*. Examinons le cas de* $A = \mathbb{Z}[i] = \{a + bi | (a, b) \in \mathbb{Z}^2\}$*. L'application* $N : A \to \mathbb{Z}, a + bi \mapsto a^2 + b^2$*. Cette application a la propriété remarquable d'être multiplicative, i.e* $\forall (z_1, z_2) \in A^2, N(zz') = N(z)N(z')$*. On en déduit que si* z *est inversible dans* A*, on dispose d'un inverse* z' *dans* A*, mais alors* $zz' = 1$*, ce qui entraîne* $N(z)N(z') = N(1) = 1$*, donc* $N(z) = 1$ *puisque* $(N(z), N(z')) \in \mathbb{N}^2$*. Mais alors* $|\mathfrak{Re}(z)| \leqslant 1$ *et* $|\mathfrak{Im}(z)| \leqslant 1$*, il ne reste alors que quatre possibilités* $1, i, -1, -i$*. Réciproquement, ces quatre éléments de* A *sont inversibles, i.e* $\mathbb{Z}[i]^\times = \mathbb{U}_4$*.*

Propriété 15 *Dans* A *anneau unitaire, tout élément inversible de* A *est régulier.*

Démonstration. Soit x un élément inversible de A, alors $xx^{-1} = 1_A$, par conséquent, x n'est pas nul, puisque $1_A \neq 0_A$. Soit $b \in A$ tel que $xb = 0_A$. En mutlipliant à gauche par x^{-1}, on obtient $x^{-1}xb = x^{-1}0_A$. Comme 0_A est absorbant, on en déduit $1_A b = 0_A$, i.e $b = 0$. Ainsi, x n'est pas un diviseur de zéro, il est régulier.

⚠ **Attention**
Il existe des éléments réguliers non inversibles dans certains anneaux. Certains anneaux sont mêmes intègres alors qu'ils ne possèdent que très peu d'inversibles ! Penser par exemple à $\mathbb{Z}$

6 Corps

Définition 13 *On appelle corps tout triplet* $(K,+,\times)$ *où* K *désigne un ensemble,* $+$ *et* $\times$ *sont deux lois de composition interne sur* K *vérifiant*

— $(K,+,\times)$ *est un anneau commutatif.*

— $(K\backslash\{0_K\},\times)$ *est un groupe commutatif.*

Il revient au même de dire que K n'est pas réduit à 0_K et que tout élément non nul de K est inversible, ou encore que $1_K \neq 0_K$ et $K^\times = K\backslash\{0\}$.

☞ **Remarque**
Ne pas oublier la commutativité de $\times$*. On trouve dans de vieilles conventions les corps non commutatifs, qui sont désormais appéles « algèbres à division ». On pourra en construire une via les quaternions. On peut toutefois prouver que toute algèbre à division de cardinal finie est commutative, donc un corps.*

Exemple 12 *Les exemples fondamentaux de corps sont* $(\mathbb{C},+,\times)$*,* $(\mathbb{R},+,\times)$ *et* $(\mathbb{Q},+,\times)$*. Nous travaillerons dans l'immense majorité des cas dans* $\mathbb{R}$ *ou* $\mathbb{C}$*. Parmi les structures d'anneau* $\mathbb{Z}/4\mathbb{Z}$ *et* $\mathbb{F}_4$*, seul* $\mathbb{F}_4$ *est un corps. Soit* K, L *deux corps. L'anneau produit* $K\times L$ *n'est pas un corps, car* $(1_K,0_L)\neq(0_K,0_L)$ *n'est pas inversible.*

Exemple 13 *Une vieille promesse : on peut construire* $(\mathbb{C},+,\times)$ *de la manière suivante : on munit* $\mathbb{R}^2$ *de deux lois de compositions internes via*

$$+ : (\mathbb{R}^2)^2 \to \mathbb{R}^2, ((a_1,b_1),(a_2,b_2)) \mapsto (a_1+a_2, b_1+b_2)$$

$$\times : (\mathbb{R}^2)^2 \to \mathbb{R}^2, ((a_1,b_1),(a_2,b_2)) \mapsto (a_1a_2-b_1b_2, a_1b_2+a_2b_1)$$

Un autre possibilité est de considérer le sous-anneau $\left\{\begin{pmatrix} a & -b \\ b & a\end{pmatrix} | (a,b)\in\mathbb{R}^2\right\}$ *de* $\mathcal{M}_2(\mathbb{R})$.

Propriété 16 *Soit* $(K,+,\times)$ *un corps. Alors* K *est un anneau intègre.*

⚠ **Attention**
La réciproque est fausse. $\mathbb{Z}$ *est intègre, mais n'est pas un corps (2 n'a pas d'inverse multiplicatif dans* $\mathbb{Z}$*).*

Exercice 4 *Soit* A *un anneau intègre fini. Montrer que* A *est un corps.*

☞ **Remarque**
Si l'on dispose d'un anneau intègre A*, on dispose d'un moyen de construire un corps qui « contient » cet anneau. On l'appelle le corps des fractions de* A*, on utilisera cette méthode pour construire le corps des fractions rationnelles à l'aide de l'anneau des polynômes.*

Définition 14 *Soit* $(K,+,\times)$ *un corps et* L *une partie de* K*. On dit que* L *est un sous-corps de* K *lorsque*

— L *est stable par* $+$ *et* $\times$*.*

— $(L,+_L,\times_L)$ *est un corps.*

Théorème 4 (Caractérisation des sous-corps) *Soit* L *une partie de* K*. C'est un sous-corps de* K *si et seulement si*

— L *est un sous-anneau de* K*,*

— $\forall x\in L\backslash\{0\}, x^{-1}\in L$*. (stabilité par inverse multiplicatif)*

Théorème 5 *Soit* L *une partie de* K*. C'est un sous-corps de* K *si et seulement si*

— $-1_L\in K$.

— $\forall (x,y)\in L^2, x+y\in L$.

— $\forall (x,y)\in L^2, x\times y\in L$.

— $\forall (x,y)\in (L\backslash\{0\})^2, x^{-1}\in L$.

Exemple 14 *$\mathbb{Q}[\sqrt{2}] = \{p + q\sqrt{2} | (p,q) \in \mathbb{Q}^2\}$ est un sous-corps de $\mathbb{C}$, idem pour $\mathbb{Q}[\sqrt[3]{2}] = \{p + q2^{1/3} + r2^{2/3} | (p,q,r) \in \mathbb{Q}^3\}$.*

Définition 15 *Soit K, L deux corps et $f : K \to L$ une application. On dit que f est un morphisme de corps lorque c'est un morphisme d'anneau des structures sous-jacentes i.e*

- $\forall (x,y) \in K^2, f(x+y) = f(x) + f(y)$.
- $\forall (x,y) \in K^2, f(xy) = f(x)f(y)$.
- $f(1_K) = 1_L$.

☞ **Remarque**
Comme vu dans le cas des morphismes de groupes, la compatibilité avec la loi de composition interne suffit à assurer la compatibilité avec l'inverse, ce qui explique qu'aucune condition supplémentaire n'est rajoutée par rapport au cas des morphismes d'anneaux.

Exemple 15 *La conjugaison $\mathbb{C} \to \mathbb{C}, z \mapsto \overline{z}$ est un morphisme de corps. Dans $K = \mathbb{Q}[j] = \{p + qj | (p,q) \in \mathbb{Q}^2\}$, l'application $\sigma : K \to K, p + qj \mapsto p - qj$ est un morphisme de corps.*

Propriété 17 *Soit K, L deux corps et $f : K \to L$. Il suffit que*

- $\forall (x,y) \in K^2, f(x+y) = f(x) + f(y)$.
- $\forall (x,y) \in K^2, f(xy) = f(x)f(y)$.

pour que f soit un morphisme de corps.

Démonstration. La multiplicativité est valide sur $K^\times$, donc f est un morphisme de groupes de $(K^\times, \times)$ dans $(L^\times, \times)$, donc $f(1_K) = 1_L$.

Propriété 18 *Soit $f : K \to L$ un morphisme de corps. Alors $\forall x \in K \backslash \{0\}, f(x^{-1}) = f(x)^{-1}$. En particulier, f est injectif.*

Démonstration. On vient de remarquer que f induit un morphisme de groupes entre $K^\times$ et $L^\times$, donc la compatibilité avec l'inverse des éléments non nuls. Soit $x \in K$ tel que $f(x) = 0_L$. Si x est non nul, alors on peut multiplier par $f(x^{-1})$, ce qui entraîne $f(x^{-1})f(x) = f(x^{-1})0_L$, soit encore $f(1_K) = 0_L$, i.e $1_L = 0_L$, ce qui est exclu dans les corps . Conclusion, $x = 0_K$, d'où $\ker(f) = \{0_K\}$ et f est injectif.

Propriété 19 *Soit K, L deux corps et $f : K \to L$ un morphisme de corps. A un sous-corps de L et B un sous-corps de L, alors $f(A)$ est un sous-corps de L, et $f^{-1}(B)$ est un sous-corps de K.*

☞ **Remarque**
En s'aidant du morphisme $\varphi : \mathbb{Z} \to K, n \mapsto n1_K$ et d'outils d'algèbre linéaire, on peut démontrer que tout corps fini est nécessairement de cardinal p^n avec p un entier premier. En particulier, il n'existe pas de corps de cardinal 6. La réciproque (i.e la construction de tels corps) nécessite bien plus de travail.

Exemple 16 *Examinons le cas des morphismes de corps de $(\mathbb{R}, +, \times)$ dans $(\mathbb{R}, +, \times)$. Soit f un tel morphisme. Alors $\forall x \in \mathbb{R}^+, f(x) = f\left(\sqrt{x}^2\right) = f(\sqrt{x})^2 \geqslant 0$. Soit à présent deux réels x, y tels que $x \leqslant y$. Alors $f(y) - f(x) = f(y - x) \geqslant 0$, d'après ce qui précède puisque $y - x \geqslant 0$. On en déduit $f(y) \geqslant f(x)$, donc f est croissante. On est alors ramené à l'étude des fonctions additives croissantes de $\mathbb{R}$ dans $\mathbb{R}$. On sait qu'il s'agit des fonctions linéaires $x \mapsto ax$. Le critère $f(1) = 1$, impose alors $a = 1$, soit $f = Id_{\mathbb{R}}$. Réciproquement, l'identité est bien un morphisme de corps.*

Exercice 5 *Soit $K \subset L$ deux corps (i.e K est un sous-corps de L). On considère l'ensemble des automorphismes de L (i.e morphismes de corps bijectifs de L dans L) suivant*

$$G = \{\varphi \in Aut(L) | \forall x \in K, \varphi(x) = x\}$$

Montrer que G est un groupe. Le déterminer dans le cas de l'extension $\mathbb{R} \subset \mathbb{C}$.