Chapitre III — Anneaux et corps

1. Définition d'un anneau

Définition 3.1. *On appelle anneau un triplet formé d'un ensemble A et de deux lois de composition sur A, une addition $(x, y) \mapsto x + y$ et une multiplication $(x, y) \mapsto xy$, tels que les conditions suivantes soient vérifiées :*

1) le couple $(A, +)$ est un groupe commutatif.

2) La multiplication est associative et possède un élément neutre.

3) La multiplication est distributive par rapport à l'addition, ce qui signifie que l'on a

$$x(y + z) = xy + xz \quad et \quad (x + y)z = xz + yz \quad quels\ que\ soient\ x, y, z \in A.$$

Si de plus la multiplication est commutative, autrement dit, si l'on a $xy = yx$ quels que soient $x, y \in A$, on dit que A est un anneau commutatif.

On notera 0 l'élément neutre de $(A, +)$ et 1, ou 1_A, l'élément neutre de A pour la multiplication. Rappelons que pour tout $x \in A$, il existe un élément de A, noté $-x$, tel que l'on ait $x + (-x) = 0$ ($-x$ est l'opposé de x).

Lemme 3.1. *Quels que soient $x, y, z \in A$, on a*

$$x(y - z) = xy - xz \quad et \quad (y - z)x = yx - zx.$$

Démonstration : D'après la condition 3, on a $x(y - z) + xz = x(y - z + z) = xy$ et $(y - z)x + zx = (y - z + z)x = yx$, d'où le lemme.

Corollaire 3.1. *Quels que soient $x, y \in A$, on a*

$$x0 = 0x = 0, \quad x(-y) = -xy \quad et \quad (-y)x = -yx.$$

En particulier, on a $(-1)x = -x$.

Par convention, on a

$$x^0 = 1 \quad \text{pour tout } x \in A.$$

Un anneau réduit à un élément, i.e. pour lequel on a $1 = 0$, est dit nul.

Exemples 3.1.

1) **L'anneau $\mathbb{Z}$.** En munissant $\mathbb{Z}$ des deux lois de composition usuelles (addition et multiplication) on obtient l'anneau des entiers relatifs, qui est évidemment commutatif. Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition de la multiplication usuelles sont aussi des anneaux commutatifs.

2) **L'anneau $F(X, A)$.** Soient X un ensemble et A un anneau. Notons $F(X, A)$ l'ensemble des applications de X à valeurs dans A. On définit la somme et le produit de deux éléments $f, g \in F(X, A)$ par les égalités

$$(f + g)(x) = f(x) + g(x) \quad \text{et} \quad (fg)(x) = f(x)g(x) \quad \text{pour tout } x \in A.$$

L'ensemble $F(X, A)$ muni de ces deux lois est un anneau, qui est commutatif si A l'est, et s'appelle l'anneau des applications de X dans A.

3) **L'anneau $\mathbb{M}_n(A)$.** Soient A un anneau, n un entier ≥ 1 et $\mathbb{M}_n(A)$ l'ensemble des matrices carrées de taille (n, n) (on dit aussi d'ordre n) à coefficients dans A. Rappelons que l'on définit sur $\mathbb{M}_n(A)$ une addition et une multiplication comme suit. Soient $M = (a_{ij})$ et $N = (b_{ij})$ deux matrices de $\mathbb{M}_n(A)$. Par définition, le coefficient de la i-ème ligne et de la j-ième colonne de $M + N$ est $a_{ij} + b_{ij}$, et celui de MN est donné par la somme

$$\sum_{k=1}^{n} a_{ik} b_{kj}.$$

Muni de ces deux lois de composition, $\mathbb{M}_n(A)$ est un anneau, qui n'est pas commutatif si $n \geq 2$ et si A n'est pas nul. En effet, soit x un élément de A distinct de 1. Soit $U = (a_{ij})$ la matrice de $\mathbb{M}_n(A)$ définie par

$$a_{11} = x, \quad a_{22} = 1 \quad \text{et} \quad a_{ij} = 0 \quad \text{pour tout } (i, j) \text{ distinct de } (1, 1) \text{ et } (2, 2).$$

Soit $V = (b_{ij}) \in \mathbb{M}_n(A)$ la matrice définie par

$$b_{11} = 1, \quad b_{12} = 1, \quad b_{22} = 1 \quad \text{et} \quad b_{ij} = 0 \quad \text{pour tous les autres termes de } V.$$

On vérifie que l'on a $UV \neq VU$.

4) **L'anneau $A[X]$.** Soit A un anneau commutatif. Rappelons que les polynômes à une indéterminée à coefficients dans A sont les suites $(a_n)_{n \geq 0}$ d'éléments de A qui sont nulles à partir d'un certain rang. Les a_n sont appelés les coefficients du polynôme. Sur cet ensemble de polynômes, on définit les deux lois de compositions suivantes : si $P = (p_0, p_1, \cdots)$ et $Q = (q_0, q_1, \cdots)$, alors l'addition et la multiplication de P et Q sont définies respectivement par les égalités

$$P + Q = (p_0 + q_0, p_1 + q_1, \cdots) \quad \text{et} \quad PQ = (s_0, s_1, \cdots) \quad \text{avec} \quad s_n = \sum_{i+j=n} p_i q_j.$$

On vérifie que l'ensemble des polynômes à coefficients dans A est ainsi muni d'une structure d'anneau, qui est commutatif si A l'est. Pour tout $a \in A$, on note a le polynôme $(a, 0, \cdots, 0, \cdots)$. Posons $X = (0, 1, 0, \cdots, 0, \cdots)$. Pour tout entier $n \geq 1$, et tout $a \in A$, on

vérifie que $aX^n = (0, \cdots, 0, a, 0, \cdots)$, où le $n+1$-ième terme de la suite est a et où tous les autres sont nuls. Avec ces notations, tout polynôme $P = (p_0, p_1, \cdots, p_n, 0, \cdots)$, dont les coefficients sont nuls pour les entiers $> n$, s'écrit alors

$$P = p_0 + p_1 X + \cdots p_n X^n,$$

qui est la notation polynômiale de P et que l'on utilise exclusivement. On note $A[X]$ l'anneau ainsi obtenu. Il s'appelle l'anneau des polynômes en une indéterminée à coefficients dans A. Bien entendu, on peut désigner le polynôme $(0, 1, 0, \cdots)$ par d'autres lettres que X, par exemple Y, Z ou T, à condition que la lettre choisie n'ait pas été utilisée par ailleurs.

5) **Produit direct d'anneaux.** Soient $A_1, \cdots, A_n$ des anneaux. Il existe sur le produit cartésien

$$A = A_1 \times \cdots \times A_n$$

une structure d'anneau, l'addition et la multiplication étant données par les formules

$$(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + y_n), \tag{1}$$

$$(x_1, \cdots, x_n)(y_1, \cdots, y_n) = (x_1 y_1, \cdots, x_n y_n). \tag{2}$$

Si tous les anneaux A_i sont commutatifs, il en est de même de A. On dit que A est le produit direct des A_i, ou encore l'anneau produit des A_i. Notons que l'élément neutre multiplicatif de A est $(1_{A_1}, \cdots, 1_{A_n})$, où 1_{A_i} l'élément neutre multiplicatif de A_i.

Exercice 1. Soit A un anneau tel que pour tous $a, b \in A$, on ait $(ab)^2 = a^2 b^2$. Montrer que A est commutatif.

2. Sous-anneaux - Idéaux

Soient A un anneau et B une partie de A.

Définition 3.2. *On dit que B est un sous-anneau de A si les conditions suivantes sont vérifiées :*

1) B est un sous-groupe additif de A.

2) Quels que soient x et y dans B, le produit xy est dans B.

3) L'élément neutre multiplicatif 1 appartient à B.

On vérifie que si B est un sous-anneau de A, alors B muni des deux lois de composition induites par celles de A est un anneau.

Exemples 3.2.

1) $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$, lui-même étant un sous-anneau de $\mathbb{C}$.

2) L'ensemble des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ est un sous-anneau de $F(\mathbb{R},\mathbb{R})$.

3) Soit i une racine carrée de -1 dans $\mathbb{C}$. L'ensemble $\mathbb{Z}[i]$ des éléments de la forme $a+ib$ avec $a,b\in\mathbb{Z}$ est sous-anneau de $\mathbb{C}$. On l'appelle l'anneau des entiers de Gauss.

Définissons maintenant la notion d'idéal de A dans le cas où A est commutatif.

Définition 3.3. *Supposons A commutatif. On dit que B est un idéal de A si les deux conditions suivantes sont vérifiées :*

1) B est un sous-groupe additif de A.

2) Quels que soient $x\in B$ et $y\in A$, le produit xy est dans B.

Exemples 3.3.

1) **Idéaux de $\mathbb{Z}$.** Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, où n parcourt $\mathbb{Z}$ (ou $\mathbb{N}$). En effet, ce sont exactement les sous-groupes de $\mathbb{Z}$, et ils vérifient la condition 2 de la définition.

2) Soient X un ensemble et Y une partie de X. Le sous-ensemble de $F(X,\mathbb{R})$ formé des applications qui s'annulent sur Y est un idéal de $F(X,\mathbb{R})$.

3) **Idéaux principaux.** Supposons A commutatif. Soit a un élément de A. L'ensemble des éléments de la forme ax, où x parcourt A, est un idéal de A. On l'appelle l'idéal principal engendré par a. On le note aA ou (a). En particulier, les parties $\{0\}$ et A sont des idéaux de A. Tous les idéaux de $\mathbb{Z}$ sont principaux.

4) L'ensemble $\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$ (ni de $\mathbb{R}$, ni de $\mathbb{C}$).

5) **Idéaux d'un anneau produit.** Soient K et L des anneaux commutatifs.

Lemme 3.2. *Les idéaux de l'anneau produit $K\times L$ (qui est commutatif) sont exactement les $I\times J$, où I est un idéal de K et J un idéal de L.*

Démonstration : Soient I et J deux idéaux de K et L respectivement. Il est immédiat de vérifier que $I\times J$ est un sous-groupe additif de $K\times L$. Par ailleurs, si (a,b) est un élément de $K\times L$, alors pour tout $(i,j)\in I\times J$, on a $(a,b)(i,j)=(ai,bj)$ qui appartient à $I\times J$, donc $I\times J$ est un idéal de $K\times L$. Considérons maintenant un idéal $\mathfrak{I}$ de $K\times L$. Soit I l'image de $\mathfrak{I}$ par la première projection $K\times L\to K$ qui à (u,v) associe u. De même, soit J l'image de $\mathfrak{I}$ par l'application $K\times L\to L$ qui à (u,v) associe v. On vérifie que I (resp. J) est un idéal de K (resp. de L). Montrons que l'on a $\mathfrak{I}=I\times J$. Par définition, $\mathfrak{I}$ est contenu dans $I\times J$. Inversement, soit (x,y) un élément de $I\times J$. Il existe $r\in K$ et $s\in L$ tels que (x,s) et (r,y) soient dans $\mathfrak{I}$. Si 1_K (resp. 1_L) désigne l'élément neutre multiplicatif de K (resp. de L), l'égalité

$$(x,y)=(1_K,0)(x,s)+(0,1_L)(r,y)$$

entraîne alors que (x, y) est dans $\mathfrak{I}$, d'où l'assertion[22].

Exercice 2. Un idéal $\mathfrak{p}$ d'un anneau commutatif A est dit premier s'il vérifie les deux conditions suivantes :

1) on a $\mathfrak{p} \neq A$.

2) Quels que soient $x, y \in A$, si xy est dans $\mathfrak{p}$, alors x ou bien y est dans $\mathfrak{p}$.

Quels sont les idéaux premiers de $\mathbb{Z}$?

3. Anneau quotient d'un anneau commutatif

Considérons un anneau commutatif A et I un idéal de A. Compte tenu du chapitre II, puisque I est un sous-groupe de A et que $(A, +)$ est un groupe abélien, on peut associer à I la relation d'équivalence $\mathcal{R}$ définie pour tous $x, y \in A$ par la condition

$$x\mathcal{R}y \Longleftrightarrow x - y \in I.$$

L'ensemble quotient A/I, muni de la loi de composition définie pour tous $x, y \in A$ par l'égalité

$$(x + I) + (y + I) = (x + y) + I, \tag{3}$$

est alors un groupe abélien, d'élément neutre I i.e. la classe de 0. On va définir une seconde loi de composition sur A/I, appelée multiplication, de sorte que A/I soit, avec l'addition précedente, muni d'une structure d'anneau commutatif. Soient $x+I$ et $y+I$ deux éléments de A/I. On définit la multiplication par la formule

$$(x + I)(y + I) = xy + I. \tag{4}$$

Pour que cette définition ait sens, il convient de vérifier qu'elle ne dépend pas des représentants x et y de $x + I$ et de $y + I$. Soient x' et y' dans A tels que l'on ait $x + I = x' + I$ et $y + I = y' + I$. Il existe r et t dans I tels que $x = x' + r$ et $y = y' + t$. On a

$$xy = x'y' + (x't + ry' + rt).$$

Puisque r et t sont dans I, il en est de même de $x't+ry'+rt$, par suite, $xy-x'y'$ appartient à I, ce qui établit notre assertion.

[22] L'assertion analogue obtenue en remplaçant «anneau produit» par «groupe produit» est fausse. Autrement dit, les sous-groupes d'un groupe produit $G_1 \times G_2$ ne sont pas exclusivement les produits $H_1 \times H_2$, où H_1 et H_2 sont des sous-groupes de G_1 et G_2 respectivement. Il y en a d'autres en général. Par exemple, soit G un groupe d'ordre 2. Posons $G = \{e, a\}$, où e est l'élément neutre de G. Alors, $H = \{(e, e), (a, a)\}$ est un sous-groupe de $G \times G$ et n'est pas de la forme $H_1 \times H_2$, où H_1 et H_2 sont des sous-groupes de G, vu que les sous-groupes de G sont $\{e\}$ et G.

Théorème 3.1. *L'ensemble A/I muni de l'addition et la multiplication définies par les formules* (3) *et* (4) *est un anneau commutatif. On l'appelle l'anneau quotient de A par I.*

Démonstration : On sait déjà que $(A/I, +)$ est un groupe abélien. La multiplication dans A étant associative et commutative, il en est de même dans A/I comme on le constate directement. Par ailleurs, $1+I$ est l'élément neutre multiplicatif de A/I (car 1 est l'élément neutre multiplicatif de A). Il reste à vérifier que la multiplication est distributive par rapport à l'addition. Soient x, y, z des éléments de A. On a les égalités

$$(x+I)\big((y+I)+(z+I)\big) = (x+I)\big((y+z)+I\big) = x(y+z)+I = xy+xz+I = (xy+I)+(xz+I),$$

par suite, on a

$$(x+I)\big((y+I)+(z+I)\big) = (x+I)(y+I)+(x+I)(z+I).$$

La deuxième égalité de définition de la distributivité se vérifie de la même façon. D'où le résultat.

Exemples 3.4.

1) **L'anneau quotient $\mathbb{Z}/n\mathbb{Z}$.** Soit n un entier naturel non nul. On a vu que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. D'après le théorème 3.1, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est donc muni d'une structure d'anneau commutatif, pour laquelle l'addition et la multiplication sont données par les égalités

$$\overline{a}+\overline{b} = \overline{a+b} \quad \text{et} \quad \overline{a}\overline{b} = \overline{ab} \quad \text{quels que soient } a, b \in \mathbb{Z}. \tag{5}$$

Rappelons que l'élément neutre additif est $\overline{0} = n\mathbb{Z}$. L'élément neutre multiplicatif est $\overline{1} = 1 + n\mathbb{Z}$, i.e. l'ensemble des entiers a tels que n divise $a-1$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ s'appelle l'anneau des entiers modulo n.

2) Soit $F \in A[X]$ un polynôme à coefficients dans un anneau commutatif A. On peut considérer l'anneau quotient $A[X]/(F)$, où (F) est l'idéal principal de $A[X]$ engendré par F. Nous étudierons plus loin ces anneaux, par exemple si $A = \mathbb{Z}/p\mathbb{Z}$, où p est premier.

4. Groupe des éléments inversibles - Corps - Anneaux intègres

Soit A un anneau.

Définition 3.4. *Soit x un élément de A. On dit que x est un élément inversible de A s'il possède un inverse pour la multiplication, autrement dit, s'il existe un élément $b \in A$ tel que l'on ait $ab = ba = 1$. On notera A^* l'ensemble des éléments inversibles de A.*

Rappelons que si $a \in A$ est inversible, il existe un unique élément $b \in A$ tel que $ab = ba = 1$ et on le note a^{-1}. Par ailleurs, si x et y sont deux éléments de A^* alors le

produit xy est aussi dans A^* et son inverse est $y^{-1}x^{-1}$. En particulier, la multiplication induit sur A^* une loi de composition.

Proposition 3.1. *L'ensemble A^*, muni de la multiplication induite par celle de A, est un groupe. On l'appelle le groupe des éléments inversibles de A, ou le groupe des unités de A.*

Démonstration : C'est une conséquence directe des définitions 2.1 et 3.4, l'élément neutre de A^* étant l'élément neutre multiplicatif 1 de A.

Par exemple, le groupe des élements inversibles de l'anneau $\mathbb{Z}$ est $\{\pm 1\}$. On étudiera en détails dans le chapitre suivant l'anneau $\mathbb{Z}/n\mathbb{Z}$ et l'on décrira en particulier le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ de ses éléments inversibles.

Exercice 3. Démontrer que le groupe des éléments inversibles de l'anneau $\mathbb{Z}[i]$ est $\{\pm 1, \pm i\}$. Montrer qu'il est cyclique d'ordre 4.

Exercice 4. Soient x et y deux éléments de A tels que $1 - xy$ soit inversible. Montrer que $1 - yx$ est aussi inversible.

Exercice 5. Soient X un ensemble et f un élément de $F(X, A)$. Montrer que f est inversible si et seulement si $f(X)$ est contenu dans A^*.

Le résultat suivant décrit le groupe des éléments inversibles d'un anneau produit, on l'utilisera plus loin.

Lemme 3.3. *Soient A et B deux anneaux. Le groupe des éléments inversibles de l'anneau produit $A \times B$ est $A^* \times B^*$. Autrement dit, on a $(A \times B)^* = A^* \times B^*$. En particulier, si A et B sont finis, on a $|(A \times B)^*| = |A^*||B^*|$.*

Démonstration : Soit (a, b) un élément inversible de $A \times B$. Il existe $(c, d) \in A \times B$ tel que $(a, b)(c, d) = (c, d)(a, b) = (1_A, 1_B)$ où 1_A (resp. 1_B) est l'élément neutre multiplicatif de A (resp. de B). D'après la formule (2), on obtient ainsi les égalités $ac = ca = 1_A$ et $bd = db = 1_B$, ce qui prouve que $a \in A^*$ et que $b \in B^*$. Inversement, si (a, b) est un élément de $A^* \times B^*$, il existe $c \in A$ et $d \in B$ tels que $ac = ca = 1_A$ et $bd = db = 1_B$. Par suite, on a $(a, b)(c, d) = (c, d)(a, b) = (1_A, 1_B)$ donc $(a, b) \in (A \times B)^*$, d'où le résultat.

Lemme 3.4. *Supposons A commutatif. Soit I un idéal de A. Alors, $I = A$ si et seulement si il existe un élément inversible dans I.*

Démonstration : Supposons qu'il existe $x \in I \cap A^*$. Dans ce cas, $xx^{-1} = 1$ est dans I, par suite, pour tout $y \in A$, l'élément $y.1 = y$ est aussi dans I, d'où $I = A$.

Définition 3.5. *On dit que A est un corps si l'on a $1 \neq 0$, et si tout élément non nul de A est inversible i.e. si l'on a $A^* = A - \{0\}$.*

Par définition, un corps possède donc au moins deux éléments, à savoir 0 et 1. Si A est un anneau commutatif et est un corps, on dit que A est un corps commutatif.

Exemples 3.5.

1) Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps commutatifs.

2) On peut démontrer que tout corps fini est commutatif. Ce résultat a été établi en 1905 par le mathématicien écossais J. Wedderburn (1882-1948).

3) Il existe des corps non commutatifs. Historiquement, le premier corps non commutatif a été découvert vers 1843 par le mathématicien irlandais W. Hamilton (1805-1865). On l'appelle le corps des quaternions d'Hamilton. On le note souvent $\mathbb{H}$. On peut le décrire comme suit. Soit $\mathbb{M}_2(\mathbb{C})$ l'ensemble des matrices ayant deux lignes et deux colonnes à coefficients dans $\mathbb{C}$. Alors $\mathbb{H}$ est le sous-ensemble de $\mathbb{M}_2(\mathbb{C})$ formé des matrices

$$\begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix} \quad \text{où } u, v \in \mathbb{C}.$$

La notation $\overline{u}$ désigne le nombre complexe conjugué de u. On peut démontrer que $\mathbb{H}$ est un corps. Il n'est pas commutatif, car par exemple en posant (avec $i^2 = -1$)

$$P = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{et} \quad Q = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

on a

$$PQ = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \quad \text{et} \quad QP = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

en particulier, PQ est distinct de QP.

Définition 3.6. *Soit K un corps. On appelle sous-corps de K tout sous-anneau L de K qui est un corps. On dit alors que K est un surcorps de L.*

Compte tenu de la définition 3.5, une partie L de K est un sous-corps de K si et seulement si L est un sous-anneau de K dont tous les éléments non nuls sont inversibles.

Exemples 3.6.

1) $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, lui même étant un sous-corps de $\mathbb{C}$.

2) L'ensemble $\left\{a + ib \mid a, b \in \mathbb{Q}\right\}$ est un sous-corps de $\mathbb{C}$. C'est le plus petit sous-corps de $\mathbb{C}$ contenant l'anneau $\mathbb{Z}[i]$ (cf. exemples 3.2).

3) L'ensemble $\left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ est un sous-corps de $\mathbb{R}$.

Exercice 6. Soit A un anneau commutatif non nul. Montrer que A est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A.

Le produit de deux éléments non nuls dans un corps est non nul. Les corps, tout au moins ceux qui sont commutatifs, font partie de certains anneaux plus généraux, les anneaux intègres :

Définition 3.7. *Un anneau A est dit intègre s'il est commutatif, non réduit à 0 i.e. on a $1 \neq 0$, et si le produit de deux éléments non nuls de A est non nul.*

Par exemple, $\mathbb{Z}$ est un anneau intègre, et plus généralement, tout sous-anneau d'un corps commutatif est un anneau intègre. On utilisera le résultat suivant :

Proposition 3.2. *Soit A un anneau intègre fini. Alors, A est un corps.*

Démonstration : Soit a un élément non nul de A. Il s'agit de montrer que a est inversible. On considère pour cela l'application de A à valeurs dans A qui à x associe ax. Elle est injective, car pour tout $x, y \in A$, si l'on a $ax = ay$, alors, $a(x - y) = 0$ et puisque A est intègre, cela entraîne $x = y$. L'anneau A étant fini, cette application est donc aussi une surjection, en particulier, 1 possède un antécédent, autrement dit, il existe $b \in A$ tel que $ab = 1$ (et $ba = 1$ car A est commutatif), d'où le résultat.

Exemples 3.7. (anneaux non intègres)

1) Soit $n \geq 2$ un entier non premier. Alors, l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. En effet, on a $n = ab$ avec a et b strictement plus grands que 1, de sorte que l'on a $\overline{a}\overline{b} = \overline{n} = \overline{0}$, bien que $\overline{a}$ et $\overline{b}$ ne soient pas nuls.

2) Si A et B sont deux anneaux non nuls, l'anneau produit $A \times B$ n'est jamais intègre, comme le montre l'égalité $(1, 0)(0, 1) = (0, 0)$.

3) L'anneau $F(\mathbb{R}, \mathbb{R})$ des applications de $\mathbb{R}$ dans $\mathbb{R}$ n'est pas intègre. Considérons en effet les deux éléments f et g définis comme suit.

$$f(x) = \begin{cases} x & \text{si } x \geq 0 \\ 0 & \text{si } x \leq 0 \end{cases} \quad \text{et} \quad g(x) = \begin{cases} 0 & \text{si } x \geq 0 \\ x & \text{si } x \leq 0 \end{cases}.$$

On a alors $fg = 0$ i.e. fg est l'application qui en tout $x \in \mathbb{R}$ prend la valeur 0, bien que f et g ne soient pas nuls.

Exercice 7. Soient A un anneau commutatif et I un idéal de A. Montrer que A/I est intègre si et seulement si I est un idéal premier (voir l'exercice 2 pour la définition d'un idéal premier).

Exercice 8. Démontrer qu'un anneau intègre qui ne possède qu'un nombre fini d'idéaux est un corps (étant donné un élément x non nul, afin de montrer qu'il est inversible, on pourra considérer la suite des idéaux principaux (x^n) pour $n \geq 1$).

5. Homomorphismes d'anneaux

Définition 3.8. *Soient A et B des anneaux. On appelle homomorphisme d'anneaux, ou morphisme d'anneaux, de A dans B toute application f de A dans B vérifiant les conditions suivantes :*

1) on a les égalités

$$f(x+y) = f(x) + f(y) \quad et \quad f(xy) = f(x)f(y) \quad quels\ que\ soient\ x, y \in A.$$

2) On a $f(1_A) = 1_B$ (en notant 1_A et 1_B les éléments neutres respectifs de A et B).

Si A et B sont des corps, toute application de A dans B vérifiant ces deux conditions s'appelle un homomorphisme, ou morphisme, de corps.

Exemples 3.8.

1) Pour tout $n \geq 1$, la surjection canonique $s : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $s(x) = x + n\mathbb{Z}$ est un homomorphisme.

2) Soient X un ensemble et A un anneau. Pour tout $x \in X$, l'application $F(X, A) \to A$ qui à $f \in F(X, A)$ associe $f(x)$ est un homomorphisme.

Lemme 3.5. *Soient $f : A \to B$ un homomorphisme d'anneaux et A', B' des sous-anneaux de A et B respectivement.*

1) L'image $f(A')$ est un sous-anneau de B.

2) L'image réciproque $f^{-1}(B')$ est un sous-anneau de A.

Démonstration : 1) On sait déjà que $f(A')$ est un sous-groupe additif de B. Par ailleurs, on a $f(1_A) = 1_B$ et $1_A \in A'$ d'où $1_B \in f(A')$. Si x et y sont dans $f(A')$, il existe u et v dans A' tels que $x = f(u)$ et $y = f(v)$, de sorte que $xy = f(u)f(v) = f(uv)$ appartient à $f(A')$.

2) On a vu que $f^{-1}(B')$ est un sous-groupe de A. L'égalité $f(1_A) = 1_B \in B'$, entraîne que $1_A \in f^{-1}(B')$. Si x et y sont dans $f^{-1}(B')$, alors $f(x)$ et $f(y)$ sont dans B', et $f(xy) = f(x)f(y) \in B'$ d'où $xy \in f^{-1}(B')$.

De façon analogue aux homomorphismes de groupes, on démontre que l'application composée de deux homomorphismes d'anneaux est encore un homomorphisme d'anneaux, et que si un homomorphisme d'anneaux est une bijection, son application réciproque est aussi un homomorphisme d'anneaux.

Définition 3.9. *Soient A et B deux anneaux. On appelle isomorphisme de A sur B tout homomorphisme d'anneaux bijectif de A sur B. S'il existe un isomorphisme entre A et B, on dit que A et B sont isomorphes.*

Exemple 3.9. L'application $\mathbb{C} \to \mathbb{H}$ qui à $z \in \mathbb{C}$ associe la matrice $\begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix}$ est un homomorphisme de corps. Elle permet d'identifier $\mathbb{C}$ à un sous-corps de $\mathbb{H}$.

Lemme 3.6. *Soient A et B deux anneaux commutatifs, $f : A \to B$ un homomorphisme et I un idéal de B. Alors, $f^{-1}(I)$ est un idéal de A.*

Démonstration : Considérons deux éléments $x \in A$ et $y \in f^{-1}(I)$. L'élément $f(x)f(y)$ est dans I i.e. $f(xy) \in I$, donc $xy \in f^{-1}(I)$. L'assertion en résulte puisque $f^{-1}(I)$ est un sous-groupe additif de A.

Remarque 3.1. L'image par un homomorphisme d'un idéal n'est pas en général un idéal, comme le montre l'injection $\mathbb{Z} \to \mathbb{Q}$ (car $\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$). Cela étant :

Exercice 9. Soient A et B deux anneaux commutatifs, $f : A \to B$ un homomorphisme surjectif de A sur B, et I un idéal de A. Alors, $f(I)$ est un idéal de B.

Définition 3.10. *Soient A et B deux anneaux et $f : A \to B$ un homomorphisme. On appelle noyau de f, et on note* $\mathrm{Ker}(f)$*, l'ensemble des éléments $x \in A$ tels que $f(x) = 0$. Le sous-anneau $f(A)$ de B s'appelle l'image de f.*

On a l'énoncé suivant, analogue au théorème 2.7 :

Théorème 3.2. *Soient A un anneau commutatif, B un anneau et $f : A \to B$ un homomorphisme. Alors,* $\mathrm{Ker}(f)$ *est un idéal de A, et l'anneau quotient $A/\mathrm{Ker}(f)$ est isomorphe à $f(A)$ via l'application qui à $x + \mathrm{Ker}(f)$ associe $f(x)$.*

Démonstration : Le fait que $\mathrm{Ker}(f)$ soit un idéal de A résulte directement des définitions. Notons $h : A/\mathrm{Ker}(f) \to f(A)$ l'application définie par

$$h\big(x + \mathrm{Ker}(f)\big) = f(x).$$

Compte tenu du théorème 2.7, on sait que h est bien définie et que c'est un isomorphisme de groupes. Par ailleurs, si $x + \mathrm{Ker}(f)$ et $y + \mathrm{Ker}(f)$ sont dans $A/\mathrm{Ker}(f)$, on a

$$h\big((x + \mathrm{Ker}(f))(y + \mathrm{Ker}(f))\big) = h\big((xy + \mathrm{Ker}(f))\big) = f(xy) = f(x)f(y),$$

qui n'est autre que $h\big((x + \mathrm{Ker}(f))\big)h\big((y + \mathrm{Ker}(f))\big)$. Puisque l'on a

$$h\big(1_A + \mathrm{Ker}(f)\big) = f(1_A) = 1_B,$$

h est donc un homomorphisme d'anneaux, d'où le résultat.

En illustration de ce qui précède, démontrons l'énoncé suivant qui caractérise, à isomorphisme près, les anneaux quotients de $\mathbb{Z}$.

Proposition 3.3. *Soit A un anneau. Les deux conditions suivantes sont équivalentes :*

1) l'anneau A ne possède pas de sous-anneaux autres que lui-même.

2) Il existe un entier $n \geq 0$ tel que A soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Démonstration : Pour tout entier $n \geq 0$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'a pas de sous-anneaux autres que lui-même. En effet, si B est un sous-anneau de $\mathbb{Z}/n\mathbb{Z}$, alors $\overline{1}$ est dans B, donc le sous-groupe engendré par $\overline{1}$, i.e. $\mathbb{Z}/n\mathbb{Z}$, est contenu dans B, d'où $B = \mathbb{Z}/n\mathbb{Z}$. En particulier, tout anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$, pour un certain $n \geq 0$, possède cette propriété. Inversement, supposons la condition 1 réalisée. Considérons l'application $f : \mathbb{Z} \to A$ définie par $f(n) = n1_A$. C'est un homomorphisme d'anneaux. Son image est un sous-anneau de A (lemme 3.5). D'après l'hypothèse faite, on a donc $f(\mathbb{Z}) = A$. Par ailleurs, il existe un entier $n \geq 0$ tel que l'on ait $\mathrm{Ker}(f) = n\mathbb{Z}$. D'après le théorème 3.2, A est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exercice 10. Soient K un corps commutatif, A un anneau non nul et $f : K \to A$ un homomorphisme. Montrer que f est injectif.

6. La formule du binôme de Newton

On va démontrer ici l'énoncé suivant, connu sous le nom de formule du binôme, qui est très utile dans la théorie des anneaux.

Théorème 3.3. *Soient A un anneau et a, b deux éléments de A tels que $ab = ba$. Alors, pour tout entier $n \geq 0$, on a l'égalité*

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

Démonstration : Le calcul de $(a+b)^n$ s'obtient en choisissant dans chacun des n facteurs $a+b$, ou bien a ou bien b, en effectuant ensuite le produit des termes ainsi choisis et en additionnant tous les résultats obtenus (il y en a 2^n). Pour tout $k = 0, \cdots, n$, si l'on choisit k fois a et donc $n-k$ fois b, on obtient ainsi, puisque a et b commutent, le terme $a^k b^{n-k}$. Tous les termes du développement de $(a+b)^n$ sont donc de cette forme pour un certain k entre 0 et n. Il reste alors à remarquer que, pour k fixé, le nombre de tels termes est le nombre de façons de choisir k fois a parmi les n possibles, qui n'est autre que le nombre $\binom{n}{k}$ de parties à k éléments dans un ensemble à n éléments. D'où le résultat.

Exercice 11. Soit A un anneau commutatif. Un élément $x \in A$ est dit nilpotent s'il existe un entier $n \geq 1$ tel que $x^n = 0$. Montrer que l'ensemble des éléments nilpotents de A, qui est appelé le nilradical de A, est un idéal de A.