Chapitre 3

Anneaux, algèbres

3.1 Structures

Un **anneau** est un ensemble $\mathbb{A}$ muni de deux opérations internes $+$ et $\times$ et d'éléments $0_{\mathbb{A}}$ et $1_{\mathbb{A}}$ qui vérifient :

associativité de l'addition :

$$\forall a \in \mathbb{A}\ \forall b \in \mathbb{A}\ \forall c \in \mathbb{A} \quad a + (b + c) = (a + b) + c\ ,$$

commutativité de l'addition :

$$\forall a \in \mathbb{A}\ \forall b \in \mathbb{A} \quad a + b = b + a\ ,$$

$0_{\mathbb{A}}$ **est élément neutre de l'addition :**

$$\forall a \in \mathbb{A} \quad a + 0_{\mathbb{A}} = a\ ,$$

tout élément de $\mathbb{A}$ a un opposé :

$$\forall a \in \mathbb{A}\ \exists b \in \mathbb{A} \quad a + b = 0_{\mathbb{A}}\ ,$$

associativité de la multiplication :

$$\forall a \in \mathbb{A}\ \forall b \in \mathbb{A}\ \forall c \in \mathbb{A} \quad a \times (b \times c) = (a \times b) \times c\ ,$$

distributivité de la multiplication par rapport à l'addition :

$$\forall a \in \mathbb{A}\ \forall b \in \mathbb{A}\ \forall c \in \mathbb{A} \quad a \times (b+c) = (a \times b) + (a \times c) \quad \text{et} \quad (b+c) \times a = (b \times a) + (c \times a)\ ,$$

1 **est élément neutre de la multiplication :**

$$\forall a \in \mathbb{A} \quad 1_{\mathbb{A}} \times a = a \times 1_{\mathbb{A}} = a\ .$$

Un anneau est dit **commutatif** quand, en plus des propriétés ci-dessus, la multiplication est commutative :

$$\forall a \in \mathbb{A}\ \forall b \in \mathbb{A} \quad a \times b = b \times a\ .$$

L'opposé d'un élément a d'un anneau est unique et noté $-a$.

On dit que a est **inversible** dans $\mathbb{A}$ quand il existe b dans $\mathbb{A}$ tel que $a \times b = b \times a = 1_{\mathbb{A}}$. Un tel élément b est unique ; on l'appelle **l'inverse de** a, et on le note a^{-1}.

Un **corps** $\mathbb{K}$ est un anneau commutatif tel que $0_{\mathbb{K}} \neq 1_{\mathbb{K}}$ et que tout élément différent de $0_{\mathbb{K}}$ a un inverse dans $\mathbb{K}$.

Un anneau $\mathbb{A}$ est dit **intègre** quand $0_{\mathbb{A}} \neq 1_{\mathbb{A}}$ et que

$$\forall a \in \mathbb{A}\ \forall b \in \mathbb{A} \quad a \times b = 0 \Rightarrow (a = 0 \text{ ou } b = 0)\ .$$

Un corps est un anneau intègre.

Soit $\mathbb{K}$ un corps. Une **$\mathbb{K}$-algèbre** est un anneau $\mathbb{A}$ muni en plus d'une opération externe (multiplication par un scalaire) :

$$\begin{array}{ccc} \mathbb{K} \times \mathbb{A} & \longrightarrow & \mathbb{A} \\ (\lambda, a) & \longmapsto & \lambda \cdot a \end{array}$$

telle que l'addition de $\mathbb{A}$ et la multiplication par un scalaire font de $\mathbb{A}$ un $\mathbb{K}$-espace vectoriel, et que

$$\lambda \cdot (a \times b) = (\lambda \cdot a) \times b = a \times (\lambda \cdot b)\ .$$

Notations habituelles : Le plus souvent, on note simplement 0 et 1 au lieu de $0_{\mathbb{A}}$ et $1_{\mathbb{A}}$. On note $a-b$ au lieu de $a+(-b)$, et on ne parenthèse pas les additions et soustractions (ceci est justifié par l'associativité de l'addition). On note la multiplication (aussi bien la multiplication interne que la multiplication par un scalaire) sans symbole, et sans parenthésage (ce qui est justifié par l'associativité et les propriétés de compatibilité entre la multiplication interne et la multiplication par un scalaire). Le produit $a \times a \times \cdots \times a$ (n facteurs a) est noté a^n.

Exercice 3.1

Une liste d'exemples à méditer, avec quelques questions.

1. $\mathbb{Z}$ est un anneau commutatif. Montrer que $\mathbb{N}$ n'est pas un anneau.
2. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.
3. $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif. Montrer que c'est un corps si n est un nombre premier. Montrer que $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre si n n'est pas premier.
4. Soit $\mathbb{K}$ un corps. Alors $M_n(\mathbb{K})$ (l'espace vectoriel des matrices carrées à n lignes et colonnes, avec le produit matriciel) est une $\mathbb{K}$-algèbre. Montrer qu'elle n'est ni commutative ni intègre pour $n \geq 2$.
5. Soit $\mathbb{K}$ un corps. Alors $\mathbb{K}[X]$ est une $\mathbb{K}$-algèbre commutative intègre.
6. L'ensemble des suites de nombres réels, avec l'addition $(a_n)+(b_n) = (a_n+b_n)$, la multiplication $(a_n)\times(b_n) = (a_n b_n)$ et la multiplication par un scalaire réel $\lambda\cdot(a_n) = (\lambda a_n)$ est une $\mathbb{R}$-algèbre. Préciser les éléments neutres pour l'addition et la multipication.

Exercice 3.2

Dans un anneau intègre, on peut simplifier par un élément non nul : montrer que si $a \times b = a \times c$ avec $a \neq 0_{\mathbb{A}}$, alors $b = c$.

Exercice 3.3

Que se passe-t-il si $0_{\mathbb{A}} = 1_{\mathbb{A}}$ dans l'anneau $\mathbb{A}$?

Exercice 3.4

Si $\mathbb{A}$ est une $\mathbb{K}$-algèbre telle que $0_{\mathbb{A}} \neq 1_{\mathbb{A}}$, alors, pour tous λ et μ de $\mathbb{K}$ on a $\lambda 1_{\mathbb{A}} = \mu 1_{\mathbb{A}}$ si et seulement $\lambda = \mu$. (On peut alors, en identifiant λ et $\lambda 1_{\mathbb{A}}$, considérer que $\mathbb{K}$ est contenu dans $\mathbb{A}$.)

Exercice 3.5

Dans un anneau commutatif $\mathbb{A}$, on a la formule du binôme :

$$\forall a \in \mathbb{A}\ \forall b \in \mathbb{A} \quad (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} \quad \text{(les coefficients binomiaux sont aussi notés } C_n^i\text{)} .$$

Est-ce qu'elle vaut toujours si l'anneau n'est pas commutatif ?

Exercice 3.6

Quels sont les éléments inversibles de $\mathbb{Z}$? de $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps) ?

3.2 Homomorphismes. Evaluation d'un polynôme.

Soient $\mathbb{A}$ et $\mathbb{B}$ des anneaux. Un **homomorphisme d'anneaux** de $\mathbb{A}$ dans $\mathbb{B}$ est une application $f : \mathbb{A} \to \mathbb{B}$ qui vérifie :

1. $\forall a \in \mathbb{A}\ \forall b \in \mathbb{A} \quad f(a+b) = f(a) + f(b)$,
2. $\forall a \in \mathbb{A}\ \forall b \in \mathbb{A} \quad f(a \times b) = f(a) \times f(b)$,
3. $f(1_{\mathbb{A}}) = 1_{\mathbb{B}}$.

La première propriété entraîne $f(0_{\mathbb{A}}) = 0_{\mathbb{B}}$.

Supposons maintenant que $\mathbb{A}$ et $\mathbb{B}$ sont des $\mathbb{K}$-algèbres ($\mathbb{K}$ un corps). Un **homomorphisme de $\mathbb{K}$-algèbres** de $\mathbb{A}$ dans $\mathbb{B}$ est un homomorphisme d'anneaux qui est en plus $\mathbb{K}$-linéaire : la propriété à vérifier en plus est $f(\lambda \cdot a) = \lambda \cdot f(a)$.

Théorème 3.1 *Soit $\mathbb{K}$ un corps, b un élément d'une $\mathbb{K}$-algèbre $\mathbb{B}$. Il existe un unique homomorphisme de $\mathbb{K}$-algèbres $f : \mathbb{K}[X] \to \mathbb{B}$ tel que $f(X) = b$. Cet homomorphisme est donné par*

$$f(a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n) = a_0 \cdot 1_{\mathbb{B}} + a_1 \cdot b + a_2 \cdot b^2 + \cdots + a_n \cdot b^n .$$

L'homomorphisme f ainsi défini est appelé l'évaluation en b, et l'élément $f(P)$ est noté $P(b)$.

Des exemples de la situation du théorème : $\mathbb{B} = \mathbb{K}$, $\mathbb{B} = \mathbb{K}[X]$ (substitution d'un polynôme à l'indéterminée), $\mathbb{B} = M_n(\mathbb{K})$ (polynôme de matrice).

Un **sous-anneau** d'un anneau $\mathbb{A}$ est un sous-ensemble $\mathbb{B}$ stable par addition, par passage à l'opposé, par multiplication, qui contient $0_{\mathbb{A}}$ et $1_{\mathbb{A}}$. Les opérations de $\mathbb{A}$ induisent alors une structure d'anneau sur $\mathbb{B}$. Si $\mathbb{A}$ est une $\mathbb{K}$-algèbre, alors $\mathbb{B}$ est une **sous-$\mathbb{K}$-algèbre** quand c'est un sous-anneau et un sous-$\mathbb{K}$-espace vectoriel.

Exercice 3.7

Montrer que l'application $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ qui envoie un entier sur sa classe de congruence modulo n est un homomorphisme d'anneaux.

Exercice 3.8

Montrer que les suites convergentes forment une sous-algèbre de la $\mathbb{R}$-algèbre des suites de nombres réels. Montrer que l'application à valeurs dans $\mathbb{R}$ qui envoie une suite convergente sur sa limite est un homomorphisme de $\mathbb{R}$-algèbres.

Exercice 3.9

On désigne par $\mathbb{Q}[\sqrt{2}]$ l'ensemble des nombres réels qui s'écrivent sous la forme $a + b\sqrt{2}$, où a et b sont des nombres rationnels. Montrer que $\mathbb{Q}[\sqrt{2}]$ est une sous-$\mathbb{Q}$-algèbre de $\mathbb{R}$. Montrer que si a et b sont des rationnels non tous les deux nuls, alors $(a + b\sqrt{2})(a - b\sqrt{2})$ est un nombre rationnel non nul. En déduire que $\mathbb{Q}[\sqrt{2}]$ est un corps.

3.3 Polynômes sur un anneau commutatif

On peut définir les polynômes sur un anneau commutatif $\mathbb{A}$ comme on l'a fait pour les polynômes sur un corps, en prenant les suites $(a_i)_{i\in\mathbb{N}}$ d'éléments de $\mathbb{A}$ où il n'y a qu'un nombre fini de a_i différents de $0_{\mathbb{A}}$ (mais on utilise bien sûr la notation habituelle $a_0 + a_1X + \cdots + a_nX^n$). Les opérations se définissent de la même manière, et font de $A[X]$ un anneau commutatif. On définit aussi le degré d'un polynôme comme le plus grand n tel que a_n soit différent de zéro (ou $-\infty$ pour le polynôme nul).

Si $\mathbb{A}$ est une $\mathbb{K}$-algèbre commutative, alors $\mathbb{A}[X]$ a aussi une structure de $\mathbb{K}$-algèbre si l'on pose, pour $\lambda \in \mathbb{K}$:

$$\lambda \cdot (a_0 + a_1X + \cdots + a_nX^n) = \lambda \cdot a_0 + (\lambda \cdot a_1)X + \cdots + (\lambda \cdot a_n)X^n \ .$$

On a pour les polynômes à coefficients dans un anneau commutatif un théorème d'évaluation qui se formule ainsi : Soit $\varphi : \mathbb{A} \to \mathbb{B}$ un homomorphisme d'anneaux commutatifs, et b un élément de $\mathbb{B}$. Alors il existe un unique homomorphisme d'anneaux (appelé évaluation en b) $f : \mathbb{A} \to \mathbb{B}$ tel que $f(X) = b$ et que $f(a) = \varphi(a)$ pour tout élément $a \in \mathbb{A}$. On a

$$f(a_0 + a_1X + \cdots + a_nX^n = \varphi(a_0) + \varphi(a_1)b + \cdots + \varphi(a_n)b^n \ .$$

On notera encore souvent $f(P) = P(b)$ (si φ est clair dans le contexte). Par exemple, si P appartient à $\mathbb{Z}[X]$ et b appartient à $\mathbb{Z}/n\mathbb{Z}$, alors $P(b)$ est bien défini dans $\mathbb{Z}/n\mathbb{Z}$.

On n'a pas en général de division euclidienne pour les polynômes à coefficients dans un anneau commutatif. Cependant, on peut tout de même diviser par un polynôme unitaire.

Proposition 3.2 *Soient S et T des polynômes à coefficients dans un anneau commutatif $\mathbb{A}$. On suppose que T est non nul et unitaire. Alors il existe un unique couple de polynômes (Q, R) dans $\mathbb{A}[X]$ tel que $S = TQ + R$ et $\deg(R) < \deg(T)$.*

Si $a \in \mathbb{A}$, on obtient pour $T = X - a$ le résultat suivant : S est divisible par $X - a$ dans $\mathbb{A}[X]$ si et seulement si $P(a) = 0$.

Exercice 3.10

Montrer que si $\mathbb{A}$ est intègre, alors $\mathbb{A}[X]$ est intègre et $\deg(PQ) = \deg(P) + \deg(Q)$.

Exercice 3.11

Trouver le nombre de racines de $X^2 - 1$ dans $\mathbb{Z}/8\mathbb{Z}$.

3.4 Polynômes à plusieurs indéterminées

Nous ne parlons ici que de polynômes à deux indéterminées X et Y, mais on peut généraliser au cas de n indéterminées $X_1, \ldots, X_n$. Un polynôme en X et Y à coefficients dans un anneau commutatif $\mathbb{K}$ est une expression

$$\sum_{0\leq i,j\leq n} a_{i,j}X^iY^j \ ,$$

où les coefficients $a_{i,j}$ sont dans $\mathbb{K}$. Formellement, on peut donner un polynôme par le "tableau" $(a_{i,j})$ (avec i et j parcourant l'ensemble des entiers naturels) de ses coefficients, dont seulement un nombre fini est non nul. Par exemple $4 + 3X - Y + X^2 - 2XY + X^2Y + 2XY^2 - Y^3$ est codé par le tableau

$$\begin{array}{cccccc} 4 & -1 & 0 & -1 & 0 & \ldots \\ 3 & -2 & 2 & 0 & \ldots & \\ 1 & 1 & 0 & \ldots & & \\ 0 & 0 & \ldots & & & \\ \vdots & \vdots & & & & \end{array}$$

La réarrangement de termes

$$\begin{aligned} & 4+3X-Y+X^2-2XY+X^2Y+2XY^2-Y^3 \\ = \; & (4-Y-Y^3)+(3-2Y+2Y^2)X+(1+Y)X^2 \\ = \; & (4+3X+X^2)+(-1-2X+X^2)Y+(2X)Y^2-Y^3 \end{aligned}$$

illustre le fait que l'on peut considérer un polynôme en X et Y à coefficients dans $\mathbb{K}$ soit comme un polynôme en X à coefficients dans l'anneau $\mathbb{K}[Y]$ (en lisant le tableau des $a_{i,j}$ comme la suite de ses lignes), soit comme un polynôme en Y à coefficients dans l'anneau $\mathbb{K}[X]$ (en lisant le tableau comme la suite de ses colonnes). L'une ou l'autre façon de voir donnent les mêmes opérations d'addition et de multiplication, et mettent une structure de $\mathbb{K}$-algèbre commutative sur l'ensemble des polynômes en X et Y à coefficients dans $\mathbb{K}$, que l'on note $\mathbb{K}[X,Y]$. Cette $\mathbb{K}$-algèbre est intègre.

Un polynôme $A = \sum_{i,j} a_{i,j} X^i Y^j$ de $\mathbb{K}[X,Y]$ a un degré en X noté $\deg_X(A)$ (pour l'exemple ci-dessus, c'est 2) un degré en Y noté $\deg_Y(A)$ (3 dans l'exemple) et un degré total $\deg(A)$ qui est le maximum des entiers $i+j$ pour l'ensemble des couples (i,j) tels que $a_{i,j} \neq 0$, ou $-\infty$ si $A = 0$ (le degré total est 3 dans l'exemple).

Exercice 3.12

Soient A et B dans $\mathbb{K}[X,Y]$. Quelles relation y a-t-il entre $\deg(A+B)$ (respectivement $\deg(AB)$) et $\deg(A)$ et $\deg(B)$ (degré total) ?

Exercice 3.13

Donner une base et la dimension du $\mathbb{K}$-espace vectoriel des polynômes de $\mathbb{K}[X,Y]$ de degré total inférieur ou égal à n.

Exercice 3.14

Montrer que $X-Y$ divise $A(X,Y)$ dans $\mathbb{K}[X,Y]$ si et seulement si $A(X,X)=0$.

Exercice 3.15

Etudier la divisibilité de X^n-Y^n, X^n+Y^n par $X-Y$ ou $X+Y$ dans $\mathbb{K}[X,Y]$.