Exercice 1.2.11 Soit A un anneau (unitaire). Montrer qu'il existe un et un seul homomorphisme d'anneaux $\mathbb{Z} \to A$.

Inversement, soit R un anneau tel que pour tout anneau A il existe un unique homomorphisme d'anneaux $R \to A$. Montrer qu'il existe un (unique) isomorphisme d'anneaux $\mathbb{Z} \to R$.

Dans la suite, on ne considérera que des anneaux unitaires et commutatifs.

Nous allons donner quelques procédés de construction d'anneaux.

Définition 1.2.12 Soient A, B deux anneaux. Le produit $A \times B$, muni de l'addition et de la multiplication termes à termes est un anneau appelé *le produit des anneaux* A, B. On définit similairement le produit d'un ensemble d'anneaux indexé par un ensemble quelconque. Si les anneaux en question sont commutatifs et unitaires, il en sera de même du produit.

Un cas particulier est l'ensemble A^X des applications d'un ensemble X vers un anneau donné A. L'addition et le produit se font sur les valeurs des applications. Quand $X = \mathbb{N}$, c'est l'ensemble des suites à valeurs dans A.

Remarque 1.2.13 La projection $A \times B \to A$, $(a, b) \mapsto a$ est un homomorphisme d'anneaux. Mais l'application naturelle $A \to A \times B$, $a \mapsto (a, 0)$ n'en est pas un si $B \neq \{0\}$ puisqu'il n'envoie pas 1 sur 1.

Définition 1.2.14 Un *sous-anneau* R d'un anneau A est un sous-groupe de A qui est stable par multiplication et qui contient l'unité 1_A. Cela revient à dire que :

1. $0_A, 1_A \in R$;
2. $x - y, xy \in R$ pour tous $x, y \in R$.

Par exemple, $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$. Mais $\mathbb{N}$ n'est pas un sous-anneau de $\mathbb{Z}$.

Exemple 1.2.15 Soit A l'ensemble des suites de Cauchy rationnelles $(r_n)_{n\geq 0}$. C'est un sous-anneau de $\mathbb{Q}^{\mathbb{N}}$. Soit $\varphi : A \to \mathbb{R}$ l'application qui à $(r_n)_n$ associe sa limite dans $\mathbb{R}$. Alors, parce que la limite commute avec la somme et le produit, φ est un homomorphisme d'anneaux. Il est surjectif car $\mathbb{Q}$ est dense dans $\mathbb{R}$.

Cet exemple suppose l'existence du corps $\mathbb{R}$ comme un corps archimédien complet dans lequel $\mathbb{Q}$ est dense. On reviendra plus tard à cette question.

Exercice 1.2.16 Montrer que l'image d'un homomorphisme d'anneaux $A \to B$ est un sous-anneau de B.

Exercice 1.2.17 Soit I un intervalle ouvert de $\mathbb{R}$. Soit $A(I, \mathbb{R})$ l'anneau des fonctions de I dans $\mathbb{R}$. Montrer que $C^0(I, \mathbb{R})$, $C^1(I, \mathbb{R})$, $C^{+\infty}(I, \mathbb{R})$ sont des sous-anneaux de $A(I, \mathbb{R})$.

Nous connaissons bien les anneaux de polynômes à une variable à coefficients dans un corps. Nous allons maintenant aborder les polynômes à plusieurs variables. Une des applications importantes de la théorie des anneaux et corps commutatifs est la résolution d'équations polynômiales du type $x^5+y^5=z^5$ ou $y^2=x^3+1$ dans $\mathbb{Z}$ ou dans $\mathbb{Q}$.

Pour cela nous allons introduire la notion des polynômes à coefficients dans un anneau.

Définition 1.2.18 Soit A un anneau (commutatif unitaire). Soit $A[X]$ l'ensemble des suites finies à coefficients dans A (c'est-à-dire des suites $(a_0, a_1, ...)$ nulles à partir d'un certain rang). On note X la suite $(0,1,0,0....)$. C'est clairement un groupe commutatif pour l'addition des suites termes à termes. La multiplication est donnée par

$$(a_n)_{n\geq 0} \times (b_m)_{m\geq 0} = (c_k)_{k\geq 0}$$

avec

$$c_k = \sum_{n,m\geq 0, n+m=k} a_n b_m.$$

On vérifie que $(A[X], +, \times)$ est un anneau commutatif dont l'élément nul (pour l'addition) est la suite nulle et dont l'unité pour la multiplication est la suite $(1,0,...)$, et que l'application $A \to A[X]$, $a \mapsto (a,0,0,...)$ est un homomorphisme d'anneaux injectif, ce qui permet d'identifier A à un sous-anneau de $A[X]$. La suite $(a_0, a_1, \ldots, a_n, 0, ...)$ est alors égale à $a_0 + a_1 X + \cdots + a_n X^n$ si on identifie $a_k \in A$ à son image dans $A[X]$.

Les éléments de $A[X]$ sont appelés des *polynômes à coefficients dans A*. Les coefficients $a_0, a_1, ...$ sont les coefficients du polynôme $P(X) = a_0 + a_1 X + \cdots + a_n X^n$. Le *degré* d'un polynôme non nul $P(X)$ est le plus grand entier $d \geq 0$ tel que $a_d \neq 0$ et que $a_k = 0$ pour tous $k \geq d+1$. Le coefficient a_d est alors appelé le *coefficient dominant* de $P(X)$.

Par convention, le degré du polynôme nul est $-\infty$.

On vérifie immédiatement les inégalités pour $P(X), Q(X) \in A[X]$

$$\deg(P(X)+Q(X)) \leq \max\{\deg P(X), \deg Q(X)\},$$

$$\deg(P(X)Q(X)) \leq \deg P(X) + \deg Q(X).$$

Ces inégalités sont strictes en général. Considérer par exemple $P(X) = X$ et $Q(X) = -X+1$ pour la première inégalité et $P(X) = Q(X) = \bar{2}X + 1$ dans $(\mathbb{Z}/4\mathbb{Z})[X]$ pour la seconde.

Définition 1.2.19 On dit que $a \in A$ est un *diviseur de zéro* dans A s'il existe $b \in A$ non nul (i.e. $\neq 0$) tel que $ab = 0$. On dit qu'un élément $a \in A$ est *régulier* si la relation $ax = ay$ ou dans A implique $x = y$. Il est immédiat de voir que $a \in A$ est régulier si et seulement s'il n'est pas diviseur de 0.

Définition 1.2.20 On dit qu'un anneau A est *intègre* si $A \neq \{0\}$ et s'il n'existe pas de diviseur de 0 non-nul. Autrement dit, si tout élément non-nul de A est régulier, ou encore que si $ab = 0$ avec $a, b \in A$, alors a ou b est nul.

Exemple 1.2.21 Les anneaux $\mathbb{Z}$, $\mathbb{R}[X]$ sont intègres. L'anneau de fonctions continues $\mathrm{C}^0(\mathbb{R}, \mathbb{R})$ n'est pas intègre. Les diviseurs de 0 dans $\mathbb{Z}/n\mathbb{Z}$ sont les classes $\bar{m}$ de $m \in \mathbb{Z}$ avec $\mathrm{pgcd}(m, n) > 1$. En particulier $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier. Quand $n = 1$ on obtient l'anneau nul qui n'est pas intègre par définition.

Exercice 1.2.22 Montrer que tout sous-anneau d'un anneau intègre est intègre. Donner un exemple d'un anneau non-intègre qui contient un sous-anneau intègre.

Proposition 1.2.23. *Si A est intègre, alors $A[X]$ est intègre et on a alors*

$$\deg(P(X)Q(X)) = \deg P(X) + \deg Q(X)$$

si $P(X), Q(X) \neq 0$.

Preuve: Soient $P(X), Q(X) \in A[X]$ non-nuls. Alors on peut écrire

$$P(X) = a_0 + a_1 X + \cdots + a_d X^d,\ Q(X) = b_0 + b_1 X + \cdots + b_e X^e,$$

avec $d, e \geq 0$ et $a_d, b_e \neq 0$. Il suit que $a_d b_e \neq 0$ puisque A est intègre, et

$$P(X)Q(X) = a_0 b_0 + (a_1 b_0 + a_0 b_1)X + \cdots + a_d b_e X^{d+e} \neq 0.$$

Enfin, $A[X] \neq \{0\}$ car $A \neq \{0\}$.

Exercice 1.2.24 Si $A = \{0\}$ est l'anneau nul. Quel est l'anneau $A[X]$?

Remarque 1.2.25 Un certain nombre de propriétés d'anneaux se transmettent de A à $A[X]$. On voit de voir c'est le cas de la propriété d'intégrité. Cependant, si A est un anneau principal, $A[X]$ ne sera jamais pas principal excepté si A est un corps (définition 1.4.5). L'objet du prochain chapitre sera d'introduire la notion d'anneaux factoriels et de montrer que cette propriété se transmet à $A[X]$.

Définition 1.2.26 Soit A un anneau (commutatif unitaire). L'anneau $A[X, Y]$ des polynômes à deux variables est défini comme étant

$$A[X, Y] = A[X][Y],$$

c'est-à-dire l'anneau des polynômes à une variable Y et à coefficients dans l'anneau $A[X]$. C'est un anneau commutatif unitaire. Concrètement les éléments de $A[X, Y]$ s'écrivent comme des sommes finies

$$P(X, Y) = \sum_{j \geq 0} a_j(X) Y^j$$

avec $a_j(X) \in A[X]$. Á leur tour, les $a_j(X)$ s'écrivent comme des sommes finies $a_j(X) = \sum_{i\geq 0} a_{ij}X^i$ avec $a_{ij} \in A$. On a donc

$$P(X,Y) = \sum_{i,j\geq 0} a_{ij}X^iY^j, \quad a_{ij} \in A$$

avec les a_{ij} tous nuls sauf un nombre fini. Du coup on a aussi

$$P(X,Y) = \sum_i (\sum_j a_{ij}Y^j)X^i \in A[Y][X].$$

On voit ainsi que $A[X,Y]$ est aussi égal à $A[Y][X]$.

Une troisième manière d'écrire les éléments de $A[X,Y]$ est la décomposition en "composantes homogènes" :

$$P(X,Y) = P_0(X,Y) + P_1(X,Y) + \cdots + P_d(X,Y) + \cdots,$$

où $P_r(X,Y) = \sum_{i+j=r} a_{ij}X^iY^j$. On définit le *degré total* de $P(X,Y) \neq 0$ comme étant le plus grand d tel qu'il existe $i,j \geq 0$ avec $i+j=d$ et $a_{ij} \neq 0$. Cela revient à dire que $P_d(X,Y) \neq 0$ et $P_m(X,Y) = 0$ pour tous $m \geq d+1$.

Il arrive aussi que l'on utilise la notion des degrés partiels. Le degré de $P(X,Y)$ en X, noté $\deg_X P(X,Y)$ est le degré de $P(X,Y) \in A[Y][X]$ vu comme un polynôme en X avec coefficients dans $A[Y]$. On définit symétriquement le degré en Y.

Considérons par exemple le polynôme

$$P(X,Y) = 1 + X + Y^2 + XY + 2X^4 + X^3Y^2 + Y^4 \in \mathbb{Q}[X,Y].$$

Il s'écrit

$$P(X,Y) = (1 + X + 2X^4) + XY + (1 + X^3)Y^2 + Y^4 \in \mathbb{Q}[X][Y]$$

mais aussi

$$P(X,Y) = (1 + Y^2 + Y^4) + (1 + Y)X + Y^2X^3 + 2X^4 \in \mathbb{Q}[Y][X],$$

ou en composantes homogènes :

$$P(X,Y) = 1 + X + (XY + Y^2) + (2X^4 + Y^4) + X^3Y^2.$$

Ainsi $\deg_Y P = 4 = \deg_X P$, et le degré total est 5.

On définit par récurrence l'anneau des polynômes à n-variables $A[X_1, \ldots, X_n]$. Par convention c'est l'anneau A si $n = 0$.

Théorème 1.2.27 (Propriété universelle)**.** *Soit $\phi : A \to B$ un homomorphisme d'anneaux. Fixons un élément $b_0 \in B$. Alors il existe un unique homomorphisme d'anneaux $\tilde{\phi} : A[X] \to B$ tel que $\tilde{\phi}(a) = \phi(a)$ pour tout $a \in A$ et que $\tilde{\phi}(X) = b_0$.*

Preuve: Si un tel homomorphisme $\tilde{\phi} : A[X] \to B$ existe, alors

$$\tilde{\phi}(\sum_i a_i X^i) = \sum_i \tilde{\phi}(a_i)\tilde{\phi}(X^i) = \sum_i \phi(a_i) b_0^i.$$

Ce qui implique l'unicité. Inversement, définissons une application f par

$$f(\sum_i a_i X^i) = \sum_i \phi(a_i) b_0^i.$$

(Par convention $b_0^0 = 1_B$). On vérifie aisément que c'est un homomorphisme d'anneaux.

Il faut voir ce théorème comme l'analogue de l'énoncé en algèbre linéaire qui dit qu'une application linéaire est uniquement déterminée par les images d'une base de l'espace de départ.