Anneaux et arithmétique

Thomas Harbreteau

13 avril 2020

Notes du cours de David Bourqui.
Université de Rennes 1, année 2019/2020.

Sommaire

Chapitre 2

Notions de base de théorie des anneaux

1 Définition d'un anneau, notations, règles d'écriture et de calculs

Exemple 2.1.1 $\mathbf{Z}$; $\mathbf{R}$; $\mathbf{Q}$; $\mathbf{R}[X]$; $\mathbf{C}[X]$; $\mathbf{R}(X)$; $\mathbf{C}(X)$; $\mathbf{Z}/n\mathbf{Z}, (n \in \mathbf{Z})$;

$$\mathbf{Z}\left[\frac{1}{n}\right] = \left\{\frac{a}{n^k} \mid a \in \mathbf{Z}, k \in \mathbf{N}\right\} \subset \mathbf{Q}, \quad n \in \mathbf{Z} \setminus \{0\}.$$

$\mathbf{Z}[1/10]$ est l'anneau des nombres décimaux.

Définition 2.1.2 (Anneau) *On appelle anneau un triplet $(A, *, \perp)$, où A est un ensemble et $*$, $\perp$ des lois de composition interne sur A telles que*

1. *$(A, *)$ est un groupe abélien,*
2. *$\perp$ est associative, commutative et possède un élément neutre,*
3. *$\perp$ est distributive par rapport à $*$, i. e.*

$$\forall x, y, z \in A, \quad x \perp (y * z) = (x \perp y) * (x \perp z).$$

Remarque 2.1.3 Dans ce cours, on appelle *anneau* ce que l'on appelle régulièrement *anneau commutatif unitaire.*

Notation :

1. La loi $*$ est notée $+$.
2. La loi $\perp$ est notée $\times$.
3. On note $-a$ le symétrique de a pour $+$.
4. On note 0 le neutre de $+$.
5. On note 1 le neutre de $\times$.
6. On note « Soit A un anneau »plutôt que « Soit $(A, +, \times)$ un anneau ».

Règles de priorités d'écriture : Soit A un anneau, $\times$ est prioritaire sur $+$.

Règles de priorités de calcul élémentaires dans un anneau : Soit A un anneau.

- Pour tous $n \in \mathbf{Z}$ et $a \in A$, on peut définit la « somme itérée n fois de a », que l'on note na.
- Pour tous $n \in \mathbf{N}$, $a \in A$, on peut définir la « puissance $n^{\text{ème}}$ de a », que l'on note a^n. Les règles de calcul usuelles des puissances s'appliquent.

Proposition 2.1.4 *Soit A un anneau, alors*

- $\forall a \in A, \quad a \times 0 = 0 \times a = 0.$
- $\forall (a, b) \in A^2, \quad a \times (-b) = (-a) \times b = -(a \times b).$
- $\forall (a, b) \in A^2, \quad (-a) \times (-b) = a \times b.$
- $\forall (a, b) \in A^2, \forall m \in \mathbf{Z}, \quad (ma) \times b = a \times (mb) = m(a \times b).$

Preuve.

- $a \times 0 = a \times (0 + 0) = a \times 0 + a \times 0$, donc $a \times 0 = 0$.
- $a \times (-b) + (a \times b) = a \times (-b + b) = 0$.
- $(-a) \times (-b) = a \times (-(-b)) = a \times b$.
- $ma \times b = (a + a + \cdots + a) = a \times b + a \times b + \cdots + a \times b = m(a \times b)$.

□

Ainsi, pour un ensemble I fini, on peut donner un sens naturel à $\sum_{i\in I} a_i$ et à $\prod_{i\in I} a_i$ avec les propriétés attendues. Si $I=\emptyset$, on adopte la convention $\sum_{i\in I} a_i = 0$ et $\prod_{i\in I} a_i = 1$. On a par exemple la règle de développement : Soit J un autre ensemble fini, alors

$$\left(\sum_{i\in I} a_i\right)\left(\sum_{j\in J} b_j\right) = \sum_{(i,j)\in I\times J} a_i b_j.$$

Théorème 2.1.5 (Binôme de Newton) *Soit A un anneau, $a,b\in A$, $n\in\mathbf{N}$, alors*

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

PREUVE. Par récurrence sur $n\in\mathbf{N}$.

- L'initialisation est vraie.
- Soit $n\in\mathbf{N}$ tel que (H_n) est vraie, alors

$$\begin{aligned}
(a+b)^{n+1} &= a(a+b)^n + b(a+b)^n \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= a^{n+1} + b^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k-1} + \binom{n}{k}\right] a^k b^{n+1-k} \\
&= \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n+1-k}.
\end{aligned}$$

Donc (H_{n+1}) est vraie.

□

Proposition 2.1.6 *Soient A un anneau et $n\in\mathbf{N}$, alors*

$$\forall (a,b)\in A^2,\quad a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

PREUVE.

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

□

2 Sous-anneaux d'un anneau

Définition 2.2.1 (Sous-anneau) *Soit A un anneau, un sous-anneau de A est une partie B de A telle que*

- *B est un sous-groupe de $(A,+)$,*
- *B est stable par $\times$,*
- *$1\in B$.*

Proposition 2.2.2 *Soient A un anneau et B un sous-anneau de A, alors les lois $+$ et $\times$ de A induisent sur B des lois $+$ et $\times$ et muni de ces lois, B est un anneau.*

PREUVE. Évident. □

Intérêt : Dans la pratique, ceci permet de munir un ensemble d'une structure d'anneau en l'identifiant à un sous-anneau d'un anneau « connu ».

Exemple 2.2.3

- On considère les anneaux $\mathbf{Z}$, $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{C}$, $\mathbf{R}[X]$ et $\mathbf{C}[X]$. Toute inclusion de l'un de ces anneaux dans l'autre (comme $\mathbf{Z}\subset\mathbf{C}[X]$) fait du premier un sous-anneau du second.

- Soit I un intervalle de $\mathbf{R}$. Alors $\mathbf{R}^I$ est muni d'une structure nautrelle d'anneau, et l'ensemble des éléments de $\mathbf{R}^I$ constitué
  - — des fonctions continues,
  - — des fonctions dérivables,
  - — des fonctions de classe $\mathcal{C}^\infty$,

  est un sous-anneau de $\mathbf{R}^I$.
- Soit A un anneau, notons $B := \{n1_A \mid n \in \mathbf{Z}\}$, alors B est un sous-anneau de A.

Proposition 2.2.4 *Soient A un anneau, E un ensemble et $(B_e)_{e\in E}$ une famille de sous-anneaux de A. Alors $\cap_{e\in E}B_e$ est un sous-anneau de A.*
PREUVE. Voir TD 1, exercice 1.2. □

Proposition 2.2.5 *Soient A un anneau et S une partie de A. Il existe un unique sous-anneau minimal B de A contenant S (au sens de l'inclusion) pour cette propriété (contenir S).*

Définition 2.2.6 (Sous-anneau engendré) *Avec les mêmes notations, l'anneau B s'appelle le sous-anneau engendré par S.*
PREUVE. (esquisse) B est nécéssairement l'intersection de tous les sous-anneaux de A contenant S, et cette intersection est un sous-anneau de A contenant S. □

Exemple 2.2.7 Soit A un anneau, le sous-anneau de A engendré par $\{0_A\}$ ou $\{1_A\}$ ou $\{0_1, 1_A\}$ est $\{n1_A \mid n \in \mathbf{Z}\}$.

3 Groupe des éléments inversibles d'un anneau

Définition 2.3.1 (Élément inversible) *Soit A un anneau. Un élément de A est dit inversible dans A s'il possède un symétrique pour la seconde loi, i. e. il existe $b \in A$ tel que $ab = 1_A$.*
On note $A^\times$ l'ensemble des éléments inversibles de A.

Remarque 2.3.2
- Avec les mêmes notations, si $a \in A$ est inversible, l'élément b de l'énoncé est unique. On l'appelle l'*inverse* de a et on peut le noter a^{-1}.
- 1_A est un élément de $A^\times$, d'inverse lui-même. En particulier, $A^\times$ n'est jamais vide.
- $A^\times$ ne désigne pas l'ensemble $A \setminus \{0_A\}$. Parfois, $A \setminus \{0_A\}$ est noté A^*, mais souvent, A^* désigne aussi $A^\times$.

Exemple 2.3.3 $\mathbf{R}^\times = \mathbf{R} \setminus \{0\}$; $\mathbf{K}^\times = \mathbf{K} \setminus \{0\}$ où $\mathbf{K}$ désigne un corps ; $\mathbf{Z}^\times = \{1, -1\}$.

Théorème 2.3.4 *Soit A un anneau. Alors l'ensemble $A^\times$ est stable par multiplication. Muni de la loi de composition interne induite, $A^\times$ est un groupe (commutatif).*
PREUVE. Montrons que $A^\times$ est stable par multiplication. Soient $a, b \in A^\times$, montrons que $ab \in A^\times$. On a $(ab)(b^{-1}a^{-1}) = 1$, donc ab est inversible, d'inverse $b^{-1}a^{-1}$.
Montrons que $(A^\times, \times)$ est un groupe. Soit l'application

$$\varphi : \begin{array}{ccc} A & \longrightarrow & A^A \\ a & \longmapsto & (b \in A \longmapsto ab) \end{array}.$$

On montre les points suivants.
1. Si $a \in A^\times$, $\varphi(a)$ est une bijection de A, d'inverse $\varphi(a^{-1})$.
2. Si $a, a' \in A$, $\varphi(aa') = \varphi(a) \circ \varphi(a')$.
3. $\varphi(1_A) = \mathrm{id}_A$.

Cela montre en particulier que $\varphi(A^\times)$ est un sous-groupe du groupe S_A (groupe des bijections de A). Par ailleurs, $\varphi_{|A^\times}$ est injective. Donc φ induit un isomorphisme de $(A^\times, \times)$ sur le groupe $\varphi(A^\times)$, ce qui montre que $(A^\times, \times)$ est un groupe. □

Exemple 2.3.5
- $\mathbf{R}[X]^\times = \mathbf{R}^\times$.
- Plus généralement, si A est un anneau intègre, $A[X]^\times = A^\times$.
- Soit $n \geq 1$ un entier, $(\mathbf{Z}/n\mathbf{Z})^\times$ est un groupe fini.

4 Morphismes d'anneaux, noyau, image, notion d'idéal

Définition 2.4.1 (Morphisme d'anneaux) *Soient A et B des anneaux. Un morphisme d'anneaux est une application $\varphi : A \to B$ vérifiant les propriétés suivantes.*

1. $\varphi : (A, +_A) \to (B, +_B)$ *est un morphisme de groupes, i. e.*
$$\forall (a, a') \in A^2, \quad \varphi(a +_A a') = \varphi(a) +_B \varphi(a').$$
2. $\forall (a, a') \in A^2, \quad \varphi(a \times_A a') = \varphi(a) \times_B \varphi(a')$.
3. $\varphi(1_A) = \varphi(1_B)$.

Exemple 2.4.2
1. Si A est un anneau, id_A est un morphisme d'anneaux.
2. Si on considère $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{C}$, $\mathbf{R}[X]$, $\mathbf{C}[X]$ et parmis ces anneaux, deux anneaux A et B tels que $A \subset B$, alors l'application $A \to B$ induite par l'inclusion est un morphisme d'anneaux.
3. La conjugaison complexe.
4. Si A et B sont des anneaux, alors l'application
$$pr_B : \begin{array}{ccc} A \times B & \longrightarrow & B \\ (a, b) & \longmapsto & b \end{array}$$
est un morphisme d'anneaux.
5. Si A est un anneau et $a \in A$, alors l'application d'évaluation en a,
$$\begin{array}{ccc} A[X] & \longrightarrow & A \\ P & \longmapsto & P(a) \end{array}$$
est un morphisme d'anneaux.

Remarque 2.4.3 Étant donnés deux anneaux A et B, il n'existe pas toujours de morphisme d'anneaux de A vers B.

Exemple 2.4.4 Si $A := \mathbf{Q}$ et $B := \mathbf{Z}$, on ne peut pas trouver de morphisme d'anneaux de $\mathbf{Q}$ vers $\mathbf{Z}$.

Proposition 2.4.5 *Soit $\varphi : A \to B$ un morphisme d'anneaux.*
1. *Si A' est un sous-anneau de A, alors $\varphi(A')$ est un sous-anneau de B.*
2. *Si B' est un sous-anneau de B, alors $\varphi^{-1}(B')$ est un sous-anneau de A.*

Preuve. Voir l'exercice 1.4 du TD 1. □

Définition 2.4.6 (Noyau d'un morphisme d'anneaux) *Soit $\varphi : A \to B$ un morphisme d'anneaux. Le noyau de φ, noté $\operatorname{Ker}\varphi$, est le noyau de φ comme morphisme de groupes $(A, +) \to (B, +)$. En d'autres termes, $\operatorname{Ker}\varphi = \varphi^{-1}\{0_B\}$, i. e.*
$$\operatorname{Ker}\varphi = \{a \in A \mid \varphi(a) = 0_B\}.$$

Exemple 2.4.7
1. Si A est un anneau, $\operatorname{Ker}\mathrm{id}_A = \{0_A\}$.
2. Si $\varphi : \mathbf{Z} \to \mathbf{R}$ est le morphisme déduit de l'inclusion $\mathbf{Z} \subset \mathbf{R}$, alors $\operatorname{Ker}\varphi = \{0_{\mathbf{Z}}\}$.
3. Si φ est la conjugaison complexe, alors $\operatorname{Ker}\varphi = \{0_{\mathbf{C}}\}$.
4. Soient A, B des anneaux, ainsi que l'application
$$pr_B : \begin{array}{ccc} A \times B & \longrightarrow & B \\ (a, b) & \longmapsto & b \end{array}.$$
Alors $\operatorname{Ker} pr_B = A \times \{0_B\}$.
5. Soient A un anneau, $a \in A$ et
$$ev_a : \begin{array}{ccc} A[X] & \longrightarrow & A \\ P & \longmapsto & P(a) \end{array}.$$
Alors $\operatorname{Ker} ev_a = \{(X - a)Q \mid Q \in A[X]\}$.

Proposition 2.4.8
1. *Si φ est un morphisme d'anneaux bijectif, alors l'application réciproque est encore un morphisme d'anneaux.*
2. *La composée de deux morphismes d'anneaux (si elle est définie) est un morphisme d'anneaux.*
3. *Un morphisme d'anneaux est injectif si et seulement si son noyau est $\{0\}$.*
4. *Soit $\varphi : A \to B$ un morphisme d'anneaux. On a*
   (a) $\forall n \in \mathbf{Z}, \forall a \in A, \quad \varphi(na) = n\varphi(a)$,
   (b) $\forall n \in \mathbf{N}, \forall a \in A, \quad \varphi(a^n) = \varphi(a)^n$.
5. *Soit $\varphi : A \to B$ un morphisme d'anneaux. Alors $\varphi(A^\times) \subset B^\times$ et l'application induite $\tilde{\varphi} : A^\times \to B^\times$ est un morphisme de groupes.*

Preuve. Voir exercice 1.4 du TD 1. □

Théorème 2.4.9 *Soit A un anneau, il existe un unique morphisme d'anneaux $\varphi : \mathbf{Z} \to A$, c'est l'application $n \mapsto n1_A$.*

PREUVE. L'application $\psi : n \mapsto n1_A$ est un morphisme d'anneaux (propriétés des sommes itérées).

Soit $\varphi : \mathbf{Z} \to A$ un morphisme d'anneaux, soit $n \in \mathbf{Z}$,

$$\varphi(n) = n\varphi(1_{\mathbf{Z}}) = n\varphi 1_{\mathbf{Z}} = n1_A.$$

Ainsi, $\varphi = \psi$. □

Définition 2.4.10 (Isomorphisme d'anneaux) *Soit $\varphi : A \to B$ un morphisme d'anneaux. On dit que φ est un isomorphisme d'anneaux s'il existe un morphisme d'anneaux $\psi : B \to A$ tel que $\varphi \circ \psi = \mathrm{id}_B$ et $\psi \circ \varphi = \mathrm{id}_A$.*

Deux anneaux sont dits isomorphes s'il existe un isomorphisme de l'un sur l'autre.

Proposition 2.4.11 *Soit $\varphi : A \to B$ un morphisme d'anneaux. Alors φ est isomorphisme si et seulement si φ est une application bijective.*

PREUVE. Voir exercice 1.4 du TD 1. □

Définition 2.4.12 (Idéal) *Soit A un anneau. Une partie I de A est un idéal de A si*

1. *I est un sous-groupe de $(A, +)$,*
2. *$\forall a \in I, \forall b \in A, \quad ab \in I$.*

Exemple 2.4.13 Soit A un anneau.

- A et $\{0_A\}$ sont des idéaux de A (dits « triviaux »).
- Si $a \in A$, $aA = \{ab \mid b \in A\}$ est un idéal de A (« idéal principal »).

Proposition 2.4.14 *Soient A un anneau et I un idéal de A. Les conditions suivantes sont équivalentes.*

1. *$I = A$.*
2. *$1_A \in I$.*
3. *$I \cap A^\times \neq \emptyset$.*

PREUVE. Voir l'exercice 1.2 du TD 1. □

Proposition 2.4.15

1. *Le noyau d'un morphisme d'anneaux est un idéal de l'anneau de départ.*
2. *Plus généralement, l'image réciproque d'un idéal par un morphisme d'anneaux est un idéal de l'anneau de départ.*
3. *Soit $\varphi : A \to B$ un morphisme d'anneaux surjectif. Alors l'image d'un idéal de A par φ est un idéal de B.*

   En outre, l'application $I \mapsto \varphi(I)$ est une bijection de l'ensemble des idéaux de A contenant $\operatorname{Ker}\varphi$ sur l'ensemble des idéaux de B, de bijection réciproque $J \mapsto \varphi^{-1}(J)$.

PREUVE. Voir l'exercice 1.4 du TD 1. □

Définition 2.4.16 (Somme d'idéaux) *Soient A un anneau, I et J des idéaux de A.*

1. *La somme $I + J$ de ces idéaux est une partie de A définie comme*

$$I + J = \{a + b \mid a \in I, b \in J\}.$$

2. *Le produit IJ de ces idéaux est une partie de A définie comme l'ensemble des sommes finies d'éléments de la forme ab, où $a \in I$ et $b \in J$.*

Plus généralement, soit $(I_e)_{e\in E}$ une famille d'idéaux de A indexée par un ensemble E.

1. *La somme de cette famille d'idéaux est la partie de A définie comme*

$$\sum_{e\in E} I_e = \left\{ \sum_{e\in E} a_e \mid (a_e)_{e\in E} \in \prod_{e\in E} I_e, \text{ famille presque nulle, i. e. } \{e \in E \mid a_e \neq 0\} \text{ est fini.} \right\}.$$

2. *Le produit de cette famille d'idéaux est la partie de A définie comme l'ensemble des sommes finies d'éléments de A de la forme $\prod_{e\in E} a_e$, où $(a_e)_e \in \prod_{e\in E} I_e$. On peut le noter $\prod_{e\in E} I_e \subset A$.*

Proposition 2.4.17 *Soit A un anneau et $(I_e)_{e\in E}$ une famille d'idéaux indexée par un ensemble E. Alors $\cap_{e\in E} I_e$, $\sum_{e\in E} I_e$ et (si E est fini) $\prod_{e\in E} I_e$ sont des idéaux de A.*

PREUVE. Voir l'exercice 1.2 du TD 1. □

Remarque 2.4.18

1. Si I est un idéal de A, en général, $I + I$ est distinct de $2I$.
2. $\underbrace{2\mathbf{Z} + 3\mathbf{Z}}_{=\mathbf{Z}} \neq 5\mathbf{Z}$.

Proposition 2.4.19 *Soient A un anneau et S une partie de A. Il existe un unique idéal de A contenant S et minimal (au sens de l'inclusion) pour cette propriété. On le note $S \cdot A$, ou $\langle S \rangle$, et on l'appelle l'idéal engendré par S.*

L'idéal $S \cdot A$ est minimum (au sens de l'inclusion) parmis les idéaux contenant S.

On a

$$S \cdot A = \left\{ \sum_{s \in S} a_s s \mid (a_s)_s \in A^S \text{ presque nulle} \right\}.$$

Si T et une autre partie de A, on a $S \cdot A + T \cdot A = (S \cup T) \cdot A$ et $(S \cdot A)(S \cdot T) = (ST) \cdot A$, où $ST = \{st \mid s \in S, t \in T\}$.

PREUVE. On note $\mathcal{I}_S$ l'ensemble des idéaux de A contenant S. Un élément I de $\mathcal{I}_S$ est minimal (pour l'inclusion) si

$$\forall J \in \mathcal{I}_S, \quad J \subset I \implies J = I.$$

Il est minimum (pour l'inclusion) si

$$\forall J \in \mathcal{I}_S, \quad I \subset J.$$

Montrons l'unicité d'un élément de $\mathcal{I}_S$ minimal pour l'inclusion. Soient I et J deux tels éléments. Alors $I \cap J$ est un idéal qui contient S donc par minimalité, $I \cap J = I$ et $I \cap J = J$, donc $I = J$.

Montrons l'existence. Soit

$$I := \bigcap_{J \in \mathcal{I}_S} J \in \mathcal{I}_S.$$

Alors par définition,

$$\forall J \in \mathcal{I}_S, \quad I \subset J.$$

Donc I est minimum, donc minimal.

Montrons que $S \cdot A$ est égal à l'ensemble décrit par l'énoncé. Pour simplifier, supposons S fini, de cardinal $n \in \mathbf{N}$. Notons $S := \{s_1, \ldots, s_n\}$, ainsi que

$$\mathcal{E} := \left\{ \sum_{i=1}^{n} a_i s_i \mid (a_i)_i \in A^n \right\}.$$

On veut montrer que $\mathcal{E}$ est l'idéal engendré par S. Il suffit de montrer que

1. $\mathcal{E}$ contient S,
2. $\mathcal{E}$ est un idéal de A,
3. tout idéal de A qui contient S contient $\mathcal{E}$.

On vérifie donc ces points.

1. Soient $i_0 \in \{1, \ldots, n\}$ et $(a_i)_i \in A^n$ tels que

$$\begin{cases} a_{i_0} &= 1_A \\ a_i &= 0_A \quad \text{si} \quad i \neq i_0 \end{cases}.$$

   Alors $\sum_{i=1}^{n} a_i s_i = s_{i_0}$, donc $s_{i_0} \in \mathcal{E}$. On a bien montré que $S \subset \mathcal{E}$.
2. Montrons que $\mathcal{E}$ est un sous-groupe de $(A, +)$. Soient $(a_i)_i \in A^n$ et $(b_i)_i \in A^n$, on a

$$-\sum_{i=1}^{n} a_i s_i = \sum_{i=1}^{n} (-a_i s_i) = \sum_{i=1}^{n} (-a_i) s_i,$$

   or $(-a_i)_i \in A^n$, donc $-\sum_{i=1}^{n} a_i s_i \in \mathcal{E}$. De plus,

$$\sum_{i=1}^{n} a_i s_i + \sum_{i=1}^{n} b_i s_i = \sum_{i=1}^{n} (a_i + b_i) s_i,$$

   mais $(a_i + b_i)_i \in A^n$ donc $\sum_{i=1}^{n} a_i s_i + \sum_{i=1}^{n} b_i s_i \in \mathcal{E}$. Comme $0_A = \sum_{i=1}^{n} 0_A s_i$, $0_A \in \mathcal{E}$, donc $\mathcal{E}$ est un sous-groupe de $(A, +)$.

   Soient $x \in \mathcal{E}$ et $y \in A$. Soit $(a_i)_i \in A^n$ telle que $x = \sum_{i=1}^{n} a_i s_i$. Alors

$$xy = y \left(\sum_{i=1}^{n} a_i s_i \right) = \sum_{i=1}^{n} (a_i y) s_i,$$

   or $(a_i y)_i \in A^n$ donc $xy \in \mathcal{E}$. Donc $\mathcal{E}$ est un idéal de A.
3. Soit I un idéal de A contenant S. Montrons que I contient $\mathcal{E}$. Soient $x \in \mathcal{E}$ et $(a_i)_i \in A^n$ telle que $x = \sum_{i=1}^{n} a_i s_i$. Par hypothèse, si $i \in \{1, \ldots, n\}$, on a $s_i \in I$. Comme $a_i \in A$ et que I est un idéal de A, on a $a_i s_i \in I$. Or I est un sous-groupe de A donc est stable par somme finie. Donc $x = \sum_{i=1}^{n} a_i s_i \in I$. On a donc bien $\mathcal{E} \subset I$.

Ces trois points montrent que $\mathcal{E} = S \cdot A$.

Pour montrer l'égalité $S \cdot A + T \cdot A = (S \cup T) \cdot A$, on peut utiliser la description précédente, ou montrer que $S \cdot A + T \cdot A$

1. est un idéal,
2. contient $S \cup T$,
3. est contenu dans tout idéal qui contient $S \cup T$.

Montrons 3. Soit I un idéal contenant $S \cup T$. Montrons que I contient $S \cdot A + T \cdot A$. Comme I contient $S \cup T$, il contient S, et comme I est un idéal, il contient $S \cdot A$. De même, I contient $T \cdot A$. Donc I contient la somme des idéaux $S \cdot A$ et $T \cdot A$.

Même genre de raisonnement pour $(S \cdot A)(T \cdot A)$. □

Remarque 2.4.20 Si un idéal I d'un anneau A contient deux idéaux J et K, il contient $J + K$.

Notation : Si $S = \{a_1, \ldots, a_n\}$ est une partie finie de cardinal n, l'idéal $S \cdot A$ peut être noté $\langle a_1, \ldots, a_n \rangle$, et on a (cf. remarque)

$$S \cdot A = a_1 A + \cdots + a_n A = \sum_{i=1}^{n} a_i A.$$

Définition 2.4.21 (Idéal premier) *Soient A un anneau et I un idéal de A. On dit que I est un idéal premier de A si*

1. *I est un idéal propre (différent de A et de $\{0_A\}$),*
2. *$\forall x \in A, \forall y \in A, \quad xy \in I \implies x \in I$ ou $y \in I$.*

Définition 2.4.22 (Idéal maximal) *On dit que I est un idéal maximal de A si*

1. *I est prore,*
2. *pour tout idéal J contenant I, on a $J = I$ ou $J = A$.*

Proposition 2.4.23 *Soient A un anneau et I un idéal maximal de A, alors I est un idéal premier de A.*

Preuve. Comme I est maximal, I est propre. Soient $x, y \in A$ tels que $xy \in I$. Montrons que $x \in I$ ou $y \in I$. Supposons que $x \notin I$ et montrons que $y \in I$. Comme $x \notin I$, l'idéal J engendré par I et x est un idéal contenant strictement I. Comme I est maximal, on a $J = A$. Or $J = I + xA$, donc $1 \in I + xA$, d'où l'existence de $z \in I$ et de $w \in A$ tels que $1 = z + xw$. Ainsi, $y = zy + xyw$. Comme $z \in I$, $zy \in I$ et $xy \in I$, donc $xyw \in I$, d'où $y \in I$. □

Exemple 2.4.24

- $\{0\}$ est un idéal premier de $\mathbf{Z}$, mais ce n'est pas un idéal maximal de $\mathbf{Z}$. En effet, si $n \in \mathbf{Z} \setminus \{0, 1, -1\}$, alors $n\mathbf{Z}$ est un idéal propre de $\mathbf{Z}$ qui contient strictement $\{0\}$.
- L'idéal $X\mathbf{Z}[X]$ est un idéal premier non nul de $\mathbf{Z}[X]$, mais ce n'est pas un idéal maximal de $\mathbf{Z}[X]$: l'idéal engendré par $\langle 2, X \rangle$ est un idéal propre de $\mathbf{Z}[X]$ qui contient strictement $X\mathbf{Z}[X]$.

Théorème 2.4.25 *Soit A un anneau. Alors tout idéal propre de A est inclus dans un idéal maximal. En particulier, tout anneau non nul possède au moins un idéal premier.*

Preuve. Théorème admis. □

Remarque 2.4.26 Soit A un anneau. Les conditions suivantes sont équivalentes.

1. $\mathrm{card}(A) = A$.
2. $0_A = 1_A$.

En particulier, de tels anneaux sont tous isomorphes, on les appelle *l'anneau nul.*

Proposition 2.4.27 *L'image réciproque d'un idéal premier par un morphisme d'anneaux est un idéal premier de l'anneau de départ.*

Preuve. Voir l'exercice 1.4 du TD 1. □

Proposition 2.4.28

1. *Soit I un idéal de $\mathbf{Z}$, alors il existe $n \in \mathbf{Z}$ tel que $I = n\mathbf{Z}$.*
2. *Soient $n, m \in \mathbf{Z}$. Alors $n\mathbf{Z} \subset m\mathbf{Z}$ si et seulement si $m|n$. En particulier, $n\mathbf{Z} = m\mathbf{Z}$ si et seulement si $|m| = |n|$.*
3. *Un idéal de $\mathbf{Z}$ est premier si et seulement s'il s'écrit $n\mathbf{Z}$, où $n \in \mathbf{Z}$ est tel que $n = 0$ ou $|n|$ est un nombre premier.*
4. *Un idéal de $\mathbf{Z}$ est maximal si et seulement s'il s'écrit $n\mathbf{Z}$, où $|n|$ est un idéal premier.*

Preuve.

1. Si $I = \{0\}$, on prend $n = 0$. Sinon, on considère $A \cap (\mathbf{N} \setminus \{0\})$ qui est non vide (car $-I = I$), et on prend n_0 le plus petit élément de cet ensemble. On a $n_0 \in I$, donc $n_0\mathbf{Z} \in I$ (car $n_0\mathbf{Z}$ est l'idéal engendré par $\mathbf{Z}$).

   Montrons l'inclusion $I \subset n_0\mathbf{Z}$. Soit $m \in I$, on a $n_0 \neq 0$ donc on peut noter la division euclidienne de m par n_0, $m = n_0 q + r$, avec $q \in \mathbf{Z}$, avec $0 \leq r \leq n_0 - 1$. On a $m \in I$ et $n_0 q \in I$, donc $r = m - n_0 q \in I$. Or $0 \leq r < n_0 - 1$, et $n_0 = \min(I \cap \mathbf{N} \setminus \{0\})$, donc $r = 0$ et $m \in n_0\mathbf{Z}$.

Remarque 2.4.29 $n\mathbf{Z}$ est l'ensemble des multiples de n.

2. Exercice.

Remarque 2.4.30 Pour $n \in \mathbf{Z}$, $n\mathbf{Z}$ est l'idéal nul si et seulement si $n = 0$, et $n\mathbf{Z} = \mathbf{Z}$ si et seulement s $n \in \{-1, 1\}$.

3. Soit $n \in \mathbf{Z}$ tel que $n\mathbf{Z}$ est propre, i. e. $n \notin \{-1, 1\}$. La condition « Un produit d'élément de $\mathbf{Z}$ est dans $n\mathbf{Z}$ si et seulement si l'un des deux facteurs est dedans »se traduit par : n divise un produit de deux entiers relatids si et seulement si n divise l'un des facteurs. Elle est vérifiée si et seulement si $|n|$ est premier (lemme d'Euclide) ou si $n = 0$.
4. Soit n un nombre premier. Montrons que $n\mathbf{Z}$ est maximal. Il est en tout cas propre. Soit J un idéal de $\mathbf{Z}$ tel que $J = m\mathbf{Z}$. On a donc $m|n$, or n est premier, donc $|m| = 1$ ou $|m| = n$. Ainsi, $m\mathbf{Z} = \mathbf{Z}$ ou $m\mathbf{Z} = n\mathbf{Z}$.

□

Remarque 2.4.31 Un idéal de $\mathbf{Z}$ est toujours engendré par un élément et un idéal premier de $\mathbf{Z}$ est soit nul, soit maximal.

Définition 2.4.32 (Caractéristique d'un anneau) *Soit A un anneau. La caractéristique de A est l'unique entier positif c tel que l'unique morphisme $\varphi : \mathbf{Z} \to A$ ait pour noyau $c\mathbf{Z}$.*

Exemple 2.4.33

- $\mathbf{Z}$; $\mathbf{R}$; $\mathbf{C}$; $\mathbf{R}[X]$; $\mathbf{C}[X]$ sont de caractéristique 0.
- Soit $n \in \mathbf{N}$, alors $\mathbf{Z}/n\mathbf{Z}$ est de caractéristique n.
- $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ est de caractéristique 4.
- $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ est de caractéristique 6.

Proposition 2.4.34 *Soit K un corps.*

1. *Soit I un idéal de $K[X]$, alors il existe $P \in K[X]$ tel que $I = PK[X]$.*
2. *Soient $P, Q \in K[X]$. Alors $PK[X] \subset QK[X]$ si et seulement si Q divise P. En particulier, $PK[X] = QK[X]$ si et seulement s'il existe $\alpha \in K^\times$ tel que $P = \alpha Q$.*
3. *Un idéal de $K[X]$ est premier si et seulement s'il est engendré par un polynôme nul ou irréductible.*
4. *Un idéal de $K[X]$ est maximal si et seulement s'il est engendré par un polynôme irréductible.*

PREUVE. Exercice. □

Remarque 2.4.35 Les mêmes que pour la proposition analogue sur $\mathbf{Z}$. $\mathbf{Z}[X]$ ne vérifie pas ces proprités.

Rappel : Soit K un corps. Un élément $P \in K[X]$ est dit *irréductible* s'il est non nul, non constant, et pour toute décomposition $P = QR$, avec $Q, R \in K[X]$, Q ou R est constant.

5 Produits d'anneaux, anneaux de polynômes et séries formelles à coefficients dans un anneau

Proposition 2.5.1 *Soient E un ensemble et $(A_e)_e$ une famille d'anneaux indexée par E. On munit le produit cartésien $B := \prod_{e\in E} A_e$ des lois $+$ et $\times$ définies par*

$$\forall (a_e)_e, (b_e)_e \in B, \quad \begin{cases} (a_e)_e + (b_e)_e & := & (a_e + b_e)_e \\ (a_e)_e \times (b_e)_e & := & (a_e b_e)_e \end{cases}.$$

Alors B muni de ces lois est un anneau d'élément neutre $(0_e)_e$ pour $+$, et $(1_e)_e$ pour $\times$.

PREUVE. Voir l'exercice 1.3 du TD 1. □

Terminologie : B s'appelle l'anneau produit de $(A_e)_e$.

Proposition 2.5.2 *Sous les mêmes hypothèses que précédemment, le groupe des inversibles d'un anneau produit est le groupe produit des groupes des éléments inversibles des composantes. En d'autres termes,*

$$\left(\prod_{e\in E} A_e\right)^\times = \prod_{e\in E} E_e^\times.$$

Proposition 2.5.3 *Sous les mêmes hypothèses et notations que précédemment, si $f \in E$, alors la projection*

$$\begin{array}{rccc} \pi_f : & \prod\limits_{e\in E} A_e & \longrightarrow & A_f \\ & (a_e)_e & \longmapsto & a_f \end{array}$$

est un morphisme d'anneaux.

Soit C un anneau, alors l'application

$$\begin{array}{ccc} \mathrm{Hom}_{anneaux}\left(B, \prod_{e\in E} A_e\right) & \longrightarrow & \prod_{e\in E} \mathrm{Hom}_{anneaux}(C, A_e) \\ \varphi & \longmapsto & (\pi_e \circ \varphi)_e \end{array}$$

est une bijection.

Notation : Si $(\varphi_e)_e \in \prod_{e\in E} \mathrm{Hom}_{\text{anneaux}}(C, A_e)$, on note $\prod_{e\in E} \varphi_e$ l'élément de $\mathrm{Hom}_{\text{anneaux}}(C, \prod_{e\in E} A_e)$ qui lui correspond via la bijection précédente.

PREUVE. Voir l'exercice 2.2 du TD 2. □

Slogan : « Se donner un morphisme d'anneaux vers un produit, c'est se donner un morphisme d'anneaux vers chacune des composantes du produit. »

Notation : (Somme pseudo-infinie) Soit A un anneau et $(a_n)_n \in A^{\mathbf{N}}$ une suite presque nulle d'éléments de A, i. e. $\{n \in \mathbf{N} \mid a_n \neq 0\}$ est fini. Soit $N \in \mathbf{N}$ tel que $(a_n)_n$ soit nulle à partir du rang N. Alors sa somme $\sum_{n=0}^{N} a_n$ ne dépend pas du choix d'un tel N. On la note $\sum_{n=0}^{+\infty} a_n$, ou $\sum_{n\in\mathbf{N}} a_n$.

Proposition 2.5.4 *Soit A un anneau.*

1. *On munit l'ensemble $A^{\mathbf{N}}$ des lois suivantes :*

$$\forall (a_n)_n, (b_n)_n \in A^{\mathbf{N}}, \quad \begin{cases} (a_n)_n + (b_n)_n & := & (a_n + b_n)_n \\ (a_n)_n \times (b_n)_n & := & \displaystyle\sum_{n=0}^{+\infty} c_n, \quad \text{où} \quad \forall n \in \mathbf{N}, \quad c_n := \sum_{\substack{k,l\in\mathbf{N} \\ k+l=n}} a_k b_l = \sum_{k=0}^{n} a_k b_{n-k}. \end{cases} .$$

2. *L'ensemble $A^{(\mathbf{N})}$ des suites presque nulles d'éléments de A est un sous-anneau de $A^{\mathbf{N}}$. On note X l'élément de $A^{(\mathbf{N})}$ définie par*

$$\forall n \in \mathbf{N}, \quad \begin{cases} X(1) & = & 1_A \\ X(n) & = & 0_A \quad \text{si } n \geq 1 \end{cases} .$$

3. *Le sous-ensemble de $A^{\mathbf{N}}$ constitué des suites nulles pour tout indice n sauf $n = 0$ est un sous-anneau de $A^{\mathbf{N}}$, isomorphe à l'anneau A.*
4. *Pour tout entier naturel N, X^N est la suite qui vaut 0_A pour tout indice n sauf pour $n = N$, où elle vaut 1_A.*
5. *Soit $(a_n)_n \in A^{(\mathbf{N})}$. Alors $(a_n X^n)_n$ est une suite presque nulle d'éléments de $A^{(\mathbf{N})}$ et on a*

$$(a_n)_n = \sum_{n=0}^{+\infty} a_n X^n.$$

PREUVE. Voir l'exercice 1.5 du TD 1. □

Notation : Soit A un anneau, un élément $(a_n)_n \in A^{\mathbf{N}}$ vu comme élément de l'anneau $(A^{\mathbf{N}}, +, \times)$ défini dans la proposition précédente, sera noté $\sum_{n=0}^{+\infty} a_n X^n$.

On utilise systématiquement ce genre de notations. On a par exemple l'identité suivante : soient $N \in \mathbf{N}$ et $\sum_{n=0}^{+\infty} a_n X^{\cdot}$, avec $(a_n)_n \in A^{\mathbf{N}}$, on a

$$X^N \sum_{n=0}^{+\infty} a_n X^n = \sum_{n=0}^{+\infty} a_n X^{n+N} = \sum_{n=N}^{+\infty} a_{n-N} X^n.$$

On note $A[[X]]$ l'anneau $A^{\mathbf{N}}$ muni des lois définies précédement. On l'appelle l'anneau des séries formelles en une indeterminée à coefficients dans A. On note $A[X]$ le sous-anneau $A^{(\mathbf{N})}$ de $A[[X]]$. On l'appelle l'anneau des polynômes en une indéterminée à coefficients dans A.

On va adopter les conventions classiques suivantes :

- $\forall n \in \mathbf{N} \cup \{-\infty\}, \quad n \geq -\infty$,
- $\forall n \in \mathbf{N} \cup \{-\infty\}, \quad (-\infty) \times n = -\infty$.

Définition 2.5.5 (Degré d'un polynôme) *Soient A un anneau et $P \in A[X]$, noté $P = \sum_{n=0}^{+\infty} a_n X^n$, avec $(a_n)_n \in A^{(\mathbf{N})}$. On définit*

$$\deg P := \sup\{n \in \mathbf{N} \mid a_n \neq 0\}.$$

Remarque 2.5.6 On a $\deg P \in \mathbf{N} \cup \{-\infty\}$. Si $\deg P \in \mathbf{N}$, le coefficient dominant de P est $a_{\deg P}$.

Proposition 2.5.7 *Soit A un anneau.*

1. *Si $P \in A[X]$, $\deg P$ est bien défini et on a $\deg P = -\infty$ si et seulement si $P = 0$.*
2. *Soient $P, Q \in A[X]$.*
   (a) *On a $\deg(P+Q) \leq \max(\deg P, \deg Q)$, avec égalité si $\deg P \neq \deg Q$.*
   (b) *On a $\deg(PQ) \leq \deg P + \deg Q$ avec égalité si $P = 0$ ou si $P \neq 0$ et le coefficient dominant de P n'est pas un diviseur de 0.*
3. *Morphisme d'évaluation : Soient $\alpha \in A$ et $P = \sum_{n=0}^{+\infty} a_n X^n \in A[X]$. Alors $P(\alpha) := \sum_{n=0}^{+\infty} a_n \alpha^n$ est bien défini comme élément de A, et l'application*
$$ev_\alpha : \begin{array}{ccc} A[X] & \longrightarrow & A \\ P & \longmapsto & P(\alpha) \end{array}$$
est un morphisme d'anneau.
4. *Si A est intègre, $A[X]$ est intègre.*

PREUVE.

1. Soit $P = \sum_{n=0}^{+\infty} a_n X^n \in A[X]$.
$$\{n \in \mathbf{N} \mid a_n \neq 0\} \subset \mathbf{N}$$
est non vide si et seulement si $P \neq 0$. Elle est par ailleurs bornée (car $(a_n)_n \in A^{(\mathbf{N})}$). Ainsi, si $P \neq 0$, sa borne supérieure existe et est un maximum. Si $P = 0$, cet ensemble est vide, et sa borne supérieure est alors $-\infty$.
2. L'énoncé sur le degré de la somme est laissé en exercice.
Soient $P, Q \in A[X]$, l'énoncé sur le degré du produit est clair si $P = 0$ ou $Q = 0$. Supposons $P \neq 0$ et $Q \neq 0$. Soient $n := \deg P$ et $m := \deg Q$. Écrivons
$$\begin{cases} P &= a_n X^n + \sum_{i=1}^{n-1} a_i X^i \\ Q &= b_m Q^m + \sum_{i=0}^{m-1} b_i X^i \end{cases}.$$
On a
$$PQ = a_n b_m X^{n+m} + \underbrace{a_n X^n \sum_{i=0}^{m-1} b_i X^i + b_m X^m \sum_{i=0}^{n-1} a_i X^i + \left(\sum_{i=0}^{n-1} a_i X^i\right)\left(\sum_{i=0}^{m-1} b_i X^i\right)}_{=:R}.$$
On vérifie que R a un degré inférieur à $m+n-1$ (ce qui revient à démontrer en général $\deg(PQ) \leq \deg P + \deg Q$). On a $a_n \neq 0$ et $b_m \neq 0$. On peut avoir en général $a_n b_m = 0$. Si on fait l'hypothèse que a_n n'est pas diviseur de zéro, comme $b_n \neq 0$, on a $a_n b_m \neq 0$. Ainsi, $\deg(PQ) = n + m = \deg P + \deg Q$.
3. Comme $(a_n)_n \in A^{(\mathbf{N})}$, on a $(a_n \alpha^n)_n \in A^{(\mathbf{N})}$, donc $\sum_{n=0}^{+\infty} a_n \alpha^n$ a un sens (comme somme pseudo-finie). Montrons que ev_α est un morphisme d'anneaux. Soient $P, Q \in A[X]$ et $N \in \mathbf{N}$ tel que $N \geq \max(\deg P, \deg Q)$. On peut écrire $P = \sum_{n=0}^{+\infty} a_n X^n$ et $Q = \sum_{n=0}^{+\infty} b_n X^n$. Montrons que ev_α est un morphisme revient à montrer que
$$\left(\sum_{n=0}^{+\infty} a_n X^n\right) + \left(\sum_{n=0}^{+\infty} b_n X^n\right) = \sum_{n=0}^{+\infty} (a_n + b_n) X^n,$$
et
$$\left(\sum_{n=0}^{+\infty} a_n X^n\right)\left(\sum_{n=0}^{+\infty} b_n X^n\right) = \sum_{n=0}^{2N} c_n \alpha^n,$$
où c_n est le produit de Cauchy de $(a_0, \ldots, a_N, 0, \ldots, 0)$ et de $(b_0, \ldots b_N, 0 \ldots, 0)$, ce qui est vrai. Par ailleurs, si $P = 1_{A[X]}$, P est le polynôme constant égal à 1_A et $ev_\alpha(P) = 1_A$, ce qui conclut.
4. Si A est intègre, A n'est pas l'anneau nul, donc $1_A \neq 0_A$, et comme A est un sous-anneau de $A[X]$, $A[X]$ n'est pas l'anneau nul. Soient $P, Q \in A[X] \setminus \{0\}$. Il faut montrer que $PQ \neq 0$. Comme A est intègre, tout élément non nul n'est pas diviseur de zéro, donc $\deg(PQ) = \deg P + \deg Q$. Comme $P \neq 0$ et $Q \neq 0$, on a $\deg P \in \mathbf{N}$ et $\deg Q \in \mathbf{N}$. Ainsi, $\deg(PQ) \in \mathbf{N}$, donc $PQ \neq 0$.

□

On adopte les conventions classiques suivantes.

- $\forall n \in \mathbf{N} \cup \{+\infty\}, \quad n \leq +\infty$.
- $\forall n \in \mathbf{N} \cup \{+\infty\}, \quad n + (+\infty) = +\infty$.

Définition 2.5.8 (Valuation et composante angulaire) *Soient A un anneau et $P = \sum_{n=0}^{+\infty} a_n X^n \in A[[X]]$. On définit*

$$\nu(P) := \inf\{n \in \mathbf{N} \mid a_n \neq 0 \ \in \mathbf{N} \cup \{+\infty\}\}$$

la valuation de P. On appelle la composante angulaire de P (si $\nu(P) \in \mathbf{N}$) l'élément $a_{\nu(P)}$.

Proposition 2.5.9 *Soit A un anneau.*

1. *Soit $P \in A[[X]]$. Alors $\nu(P)$ est bien définie et $\nu(P) = +\infty$ si et seulement si $P = 0$.*
2. *Soient $P, Q \in A[[X]]$.*
   (a) *On a $\nu(P+Q) \geq \min(\nu(P), \nu(Q))$ avec égalité si $\nu(P) \neq \nu(Q)$.*
   (b) *On a $\nu(PQ) \geq \nu(P) + \nu(Q)$ avec égalité si $P = 0$ ou si $P \neq 0$ et la composante angulaire de P n'est pas un diviseur de 0.*
3. *Si A est intègre, $A[[X]]$ est intègre.*

PREUVE. Voir l'exercice 1.5 du TD 1. □

Proposition 2.5.10 (Division euclidienne dans un anneau de polynômes en une indéterminée) *Soit A un anneau. Soient $P_1, P_2 \in A[X]$ avec $P_2 \neq 0$. On suppose que le coefficient de P_2 est inversible. Alors il existe un unique couple (Q, R) d'éléments de $A[X]$ vérifiant*

1. *$P_1 = QP_2 + R$,*
2. *$\deg R < \deg P_2$.*

PREUVE. Supposons l'existence de deux tels couples (Q, R) et $(\tilde{Q}, \tilde{R})$. On a $QP_2 + R = \tilde{Q}P_2 + \tilde{R}$, soit $(Q - \tilde{Q})P_2 = \tilde{R} - R$. Or, comme le coefficient dominant de P_2 est inversible, donc on a $\deg(R - \tilde{R}) = \deg(Q - \tilde{Q}) + \deg P_2$. Mais

$$\deg(R - \tilde{R}) \leq \max(\deg R, \deg \tilde{R}) < \deg P_2.$$

Donc $\deg P_2 + \deg(Q - \tilde{Q}) < \deg P_2$. Comme $\deg(Q - \tilde{Q}) \in \mathbf{N} \cup \{-\infty\}$, donc $\deg(Q - \tilde{Q}) = -\infty$, d'où $Q - \tilde{Q} = 0$. Par conséquent, $Q = \tilde{Q}$ et $R = \tilde{R}$.

L'existence se fait par récurrence sur le degré de P_1. L'hypothèse de récurrence est (H_n) : « Pour tout polynôme P_1 de degré au plus n, il existe une division euclidienne de P_1 par P_2. »

Si $n < \deg(P_2)$, (H_n) est vraie. Pour P_1 de degré au plus n, on prend $(Q, R) = (0, P_1)$. Soit $n \geq \deg P_2$ tel que (H_{n-1}) est vérifiée. Soit P_1 de degré n. Écrivons $P_1 = a_n X^n + \tilde{P_1}$, avec $\deg \tilde{P_1} < n$, ainsi que $P_2 = \alpha_{\deg P_2} X^{\deg P_2} + \tilde{P_2}$, avec $\deg \tilde{P_2} < \deg P_2$. Par hyopthèse, $\alpha_{\deg P_2} \in A^\times$. On considère

$$\overline{P_1} := P_1 - a_n \times \alpha_{deg P_2}^{-1} X^{n - \deg P_2} P_2.$$

On a $\deg \overline{P_1} \leq n - 1$. Par hypothèse de récurrence, $\overline{P_1}$ admet une division euclidienne par P_2. Soit (Q, R) un couple adéquat correspondant, alors le couple $(Q + a_n \alpha_{\deg P_2}^{-1} X^{n - \deg P_2}, R)$ définit une division euclidienne de P_1 par P_2. □

Remarque 2.5.11 L'hypothèse de l'inversibilité du coefficient de P_2 est essentielle. Contre exemple : dans $\mathbf{Z}[X]$, $P_1 = X$, $P_2 = 2X$.

Remarque 2.5.12 Si A est un corps, ce résultat permet de montrer que tout idéal de $A[X]$ est engendré par un élément. L'idéal $\langle 2, X \rangle$ de $\mathbf{Z}[X]$ n'est pas engendré par un élément.

Définition 2.5.13 (Racine d'un polynôme) *Soient A un anneau et $P \in A[X]$. Un zéro (ou racine) de P dans A est un élément $\alpha \in A$ tel que $P(\alpha) = 0$, autrement dit tel que $P \in \mathrm{Ker}(ev_\alpha)$.*

Corollaire 2.5.14 *Soient A un anneau, $P \in A[X]$ et $\alpha \in A$. Alors α est racine de P si et seulement s'il existe $Q \in A[X]$ tel que $P = (X - \alpha)Q$.*

PREUVE. Supposons qu'il existe $Q \in A[X]$ tel que $P = (X - \alpha)Q$. Alors

$$ev_\alpha(P) = ev_\alpha((X - \alpha)Q) = ev_\alpha(X - \alpha) ev_\alpha Q = (\alpha - \alpha) ev_\alpha Q = 0.$$

Supposons que α est racine de P. Comme $X - \alpha$ a un coefficient dominant inversible, il existe $(Q, R) \in A[X]^2$ tel que $P = (X - \alpha)Q + R$ et $\deg R < \deg(X - \alpha) = 1$. On a

$$ev_\alpha(P) = ev_\alpha(X - \alpha) ev_\alpha(Q) + ev_\alpha(R) = R(\alpha).$$

Donc $R(\alpha) = 0$, mais $\deg R \leq 0$. Donc $R \in A$ et $R(\alpha) = 0$. Ainsi, $R = 0$ et $P(X - \alpha)Q$. □

Corollaire 2.5.15 *Soit A un anneau intègre. Soit $P \in A[X]$ un polynôme non nul. Alors P a au plus $\deg P$ racines dans A. En particulier si $P \in A[X]$ a une infinité de racines dans A, alors $P = 0$.*

PREUVE. Soit $n \in \mathbf{N}$, $n \geq 1$, tel qu'il existe n éléments $a_1, \ldots, a_n$ de A deux à deux distincts qui sont des racines de P. Montrons que $n \leq \deg P$. Comme a_1 est racine de P, il existe $Q_1 \in A[X]$ tel que $P = (X - a_1)Q_1$. On a $P(a_2) = 0 = (a_2 - a_1)Q_1(a_2)$. Or $a_2 - a_1 \neq 0$ et A est intègre, donc $Q_1(a_2) = 0$. De proche en proche, il existe $Q \in A[X]$ tel que $P = (X - a_1)(X - a_2) \ldots (X - a_n)Q$. Mais les $X - a_i$ sont unitaires, donc

$$\deg P = \sum_{i=1}^{n} \deg(X - a_i) + \deg Q = n + \deg Q,$$

ce qui conclut car $\deg P \neq -\infty$ par hypothèse. □

Remarque 2.5.16 Si A n'est pas intègre, même un polynôme unitaire peut avoir une infinité de racines.

Théorème 2.5.17 *Soit A un anneau. Soit $c : A \to A[X]$ le morphisme d'anneau injectif naturel. Soit B un anneau. Alors l'application*

$$\begin{array}{ccc} \mathrm{Hom}_{anneaux}(A[X], B) & \longrightarrow & \mathrm{Hom}_{anneaux}(A, B) \times B \\ \varphi & \longmapsto & (\varphi \circ c, \varphi(X)) \end{array}$$

est une bijection.

PREUVE. Voir TD 1. □

Slogan : « Se donner un morphisme d'anneaux de $A[X]$ vers B, c'est se donner un morphisme d'anneaux de A vers B et un élément de B. »

Remarque 2.5.18 Prenons $A = B$ et $\alpha \in A$. L'image réciproque de (id_A, α) par la bijection de l'énoncé est le morphisme ev_α.

Soient A un anneau et $N \geq 2$. Il y a essentiellement deux façons de définir l'anneau $A[X_1, \ldots, X_N]$.

1. De proche en proche :
$$\begin{array}{rcl} A[X_1, X_2] & := & (A[X])[X_2] \\ A[X_1, X_2, X_3] & := & (A[X_1])[X_2, X_3] \\ & \vdots & \end{array}.$$
2. On considère $A^{(\mathbf{N}^\mathbf{N})}$ l'ensemble des applications presque nulles $\mathbf{N}^\mathbf{N} \to A$, i. e. $\{n \in \mathbf{N}^\mathbf{N} \mid \varphi(n) \neq 0 \text{ est fini}\}$. On définit l'addition et la multiplication de manière ad hoc.

Par la construction 1), il est facile de voir que si A est intègre, alors $A[X_1, \ldots, X_N]$ est encore intègre.

Chapitre 3

Étude des anneaux quotients $\mathbf{Z}/n\mathbf{Z}$ et $\mathbf{K}[X]/P\mathbf{K}[X]$

1 Étude de $\mathbf{Z}/n\mathbf{Z}$

1.1 Éléments inversibles de $\mathbf{Z}/n\mathbf{Z}$

Notation : On désignera par $[m]_n$ l'élément de $\mathbf{Z}/n\mathbf{Z}$ dont un représentant est m.

Théorème 3.1.1 *Soit n un entier strictement positif, l'application*

$$\varphi : \begin{array}{ccc} \{m \in \mathbf{Z} \mid 0 \leq m \leq n-1, \operatorname{pgcd}(m,n) = 1\} & \longrightarrow & (\mathbf{Z}/n\mathbf{Z})^\times \\ m & \longmapsto & [m]_n \end{array}$$

est une bijection.

De manière plus générale, si $m \in \mathbf{Z}$, on a $[m]_n \in (\mathbf{Z}/n\mathbf{Z})^\times$ si et seulement si $\operatorname{pgcd}(m,n) = 1$.

Remarque 3.1.2 Ce résultat ne dit rien sur la structure de groupe de $(\mathbf{Z}/n\mathbf{Z})^\times$.

PREUVE. Montrons la deuxième assertion. Soit $m \in \mathbf{Z}$, alors les propriétés du morphisme d'anneaux surjectif canonique $\pi : m \in \mathbf{Z} \mapsto [m]_n \in n\mathbf{Z}$ montrent que

$$\begin{aligned} [m]_n \in (\mathbf{Z}/n\mathbf{Z})^\times &\iff \exists x \in \mathbf{Z}/n\mathbf{Z}, \quad x[m]_n = 1_{\mathbf{Z}/n\mathbf{Z}} \\ &\iff \exists r \in \mathbf{Z}, \quad [r]_n[m]_n = [1]_n \qquad \text{(surjectivité de } \pi) \\ &\iff \exists n \in \mathbf{Z}, \quad [nm-1]_n = [0]_n \qquad \text{(propriétés de morphisme de } \pi) \\ &\iff \exists n, k \in \mathbf{Z}, \quad nm - 1 = nk \qquad \text{(le noyau de } \pi \text{ étant } n\mathbf{Z}). \end{aligned}$$

D'après le théorème de Gauss, on a donc

$$[m]_n \in (\mathbf{Z}/n\mathbf{Z})^\times \iff \operatorname{pgcd}(m,n) = 1.$$

Montrons la première assertion. Soit $y \in \mathbf{Z}/n\mathbf{Z}$, il existe $m \in \mathbf{Z}$ tel que $y = [m]_n$. On note $m = qn + r$ la division euclidienne de m par n. On a

$$[m]_n = [qn+r]_n = [q]_n \underbrace{[n]_n}_{=0_{\mathbf{Z}/n\mathbf{Z}}} + [r]_n = [r]_n.$$

Or $0 \leq r \leq n-1$ et $y = [r]_n = \varphi(r)$. Donc φ est surjective. De plus, soient $m, m' \in \mathbf{Z}$ tels que $0 \leq m, m' \leq n-1$, et $\varphi(m) = \varphi(m')$. On a $\varphi(m) = \varphi(m')$, donc $[m]_n = [m']_n$, donc $[m-m']_n = 0_{Z/n\mathbf{Z}}$. Ainsi, n divise $m - m'$, mais $|m - m'| \leq n-1$, d'où $m - m' = 0$. La fonction φ est donc surjective, donc bijective. □

Remarque 3.1.3 On a montré en particulier que $\mathbf{Z}/n\mathbf{Z}$ est fini, de cardinal n.

1.2 Endomorphismes de $\mathbf{Z}/n\mathbf{Z}$

Théorème 3.1.4 *Soit n un entier positif. Soient A un anneau quelconque et c sa caractéristique. Alors* $\operatorname{Hom}_{anneaux}(\mathbf{Z}/n\mathbf{Z}, A)$ *est non vide si et seulement si c divise n, et dans ce dernier cas, cet ensemble est un singleton. En particulier,*

$$\operatorname{Hom}_{anneaux}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z}/n\mathbf{Z}) = \{\mathrm{id}_{\mathbf{Z}/n\mathbf{Z}}\}.$$

PREUVE. Soit $\varphi_A : \mathbf{Z} \to A$ l'unique morphisme d'anneaux de $\mathbf{Z}$ vers A. On a $\mathrm{Ker}(\varphi_A) \subset c\mathbf{Z}$. Par la propriété universelle de l'anneau quotient, l'ensemble $\mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}/n\mathbf{Z}, A)$ est en bijection avec l'ensemble

$$\{\varphi \in \mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}, A) \mid n\mathbf{Z} \subset \mathrm{Ker}\,\varphi\}.$$

Mais par ailleurs $\mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}, A) = \{\varphi_A\}$, donc cet ensemble est non vide si et seulement si $n\mathbf{Z} \subset \mathrm{Ker}\,\varphi_A$. Dans ce cas, c'est un singleton. Mais comme $\mathrm{Ker}\,\varphi_A = c\mathbf{Z}$, la condition $n\mathbf{Z} \subset \mathrm{Ker}\,\varphi_A$ est équivalente à la condition c divise n. □

Exemple 3.1.5 Soient $m, n \in \mathbf{N}$, la caractéristique de $\mathbf{Z}/m\mathbf{Z}$ est m. On suppose que m divise n. Soit $\pi_{m,n}$ l'unique élément de $\mathrm{Hom}_{\text{anneaux}}(\mathbf{Z}/n\mathbf{Z}, \mathbf{Z}/m\mathbf{Z})$. Soit $x \in \mathbf{Z}/n\mathbf{Z}$, soit $r \in \mathbf{Z}$ tel que $x = [r]_n$, alors $\pi_{n,m}(x) = [r]_m$.

1.3 Les carrés dans $\mathbf{Z}/p\mathbf{Z}$, où p est premier

Définition 3.1.6 (Carré) *Soit A un anneau et $a \in A$. On dit que a est un carré dans A s'il existe $b \in A$ tel que $a = b^2$.*

Théorème 3.1.7 *Soit p un nombre premier impair.*

1. *L'application*
$$\begin{array}{ccc} (\mathbf{Z}/p\mathbf{Z})^\times & \longrightarrow & (\mathbf{Z}/p\mathbf{Z})^\times \\ x & \longmapsto & x^2 \end{array}$$
est un morphisme de groupes de noyau de cardinal 2 égal à $\{[1]_p, [-1]_n\}$.
2. *Soit $x \in (\mathbf{Z}/p\mathbf{Z})^\times$. Alors x est un carré dans $\mathbf{Z}/p\mathbf{Z}$ si et seulement si $x^{(p-1)/2} = 1$.*
3. *Il y a exactement $(p+1)/2$ carrés dans $\mathbf{Z}/p\mathbf{Z}$.*

Énonçons le théorème suivant, plus général, duquel découle le théorème précédent.

Théorème 3.1.8 *Soit $\mathbf{K}$ un corps de caractéristique différente de 2.*

1. *On a $1_\mathbf{K} \neq -1_\mathbf{K}$.*
2. *L'application*
$$\begin{array}{ccc} \mathbf{K}^\times & \longrightarrow & \mathbf{K}^\times \\ x & \longmapsto & x^2 \end{array}$$
est un morphisme de groupes de noyau $\{1_\mathbf{K}, -1_\mathbf{K}\}$.
3. *Si $\mathbf{K}$ est fini, de cardinal q impair, il y a exactement $(q+1)/2$ carrés dans $\mathbf{K}$, et si $x \in \mathbf{K}^\times$, x est un carré dans $\mathbf{K}$ si et seulement si $x^{(q-1)/2} = 1_\mathbf{K}$*

PREUVE.

1. Dire que $1_\mathbf{K} = -1_\mathbf{K}$ équivaut à dire que $2 \in \mathrm{Ker}\,\varphi_\mathbf{K}$, l'unique morphisme d'anneaux de $\mathbf{Z}$ vers $\mathbf{K}$. En particulier, si c'est vrai, ce noyau contient $2\mathbf{Z}$, or $2\mathbf{Z}$ est maximal et le noyau n'est pas $\mathbf{Z}$ car $\mathbf{K}$ étant un corps, il n'est pas l'anneau nul. Donc le noyau est $2\mathbf{Z}$ et la caractéristique de $\mathbf{K}$ est 2.
2. Soient $x, y \in \mathbf{K}^\times$. On a
$$\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\varphi(y),$$
donc φ est un morphisme de groupes. Si $x \in \mathbf{K}$, on a par intégrité de $\mathbf{K}$,
$$x \in \mathrm{Ker}\,\varphi \iff x^2 = 1_\mathbf{K} \iff (x - 1_\mathbf{K})(x + 1_\mathbf{K}) = 0_\mathbf{K} \iff x = 1_\mathbf{K} \text{ ou } x = -1_\mathbf{K}.$$
3. $\mathbf{K}^\times$ est un groupe fini de cardinal $q-1$, donc $\varphi(\mathbf{K}^\times)$, qui est isomorphe à $\mathbf{K}^\times/\mathrm{Ker}\,\varphi$, est de cardinal $(q-1)/2$. Or $\varphi(\mathbf{K}^\times)$ est l'ensemble des éléments non nuls de $\mathbf{K}^\times$ qui sont des carrés. Par ailleurs, $0_\mathbf{K}$ est toujours un carré, donc il y a $(q-1)/2 + 1 = (q+1)/2$ carrés dans $\mathbf{K}$.
Montrons la dernière assertion. Soit $x \in \mathbf{K}^\times$ qui est un carré. Montrons que $x^{(q-1)/2} = 1_\mathbf{K}$. Il existe $y \in \mathbf{K}^\times$ tel que $x = y^2$, donc D'après le théorème de Lagrange dans le groupe $\mathbf{K}^\times$, de cardinal $q-1$, $x^{(q-1)/2} = y^{q-1} = 1_\mathbf{K}$. Soit $P = X^{(q-1)/2} - 1_\mathbf{K} \in \mathbf{K}[X]$. On a montré que $\varphi(\mathbf{K}^\times) \subset \{x \in \mathbf{K} \mid P(x) = 0\}$. Or $\mathbf{K}$ est un corps, donc
$$\mathrm{card}(\{x \in \mathbf{K} \mid P(x) = 0\}) \leq \deg P = \frac{q-1}{2}.$$
Or $\mathrm{card}(\varphi(\mathbf{K}^\times)) = (q-1)/2$, donc $\varphi(\mathbf{K}^\times) = \{x \in \mathbf{K} \mid P(x) = 0\}$.

□

Exemple 3.1.9 Les carrés dans $\mathbf{Z}/7\mathbf{Z}$ sont $[0]_7$, $[1]_7$, $[4]_7$ et $[2]_7$.

2 Étude de $\mathbf{K}[X]/P\mathbf{K}[X]$

Soit $\mathbf{K}$ un corps. Soit $\iota : K \to \mathbf{K}[X]$ le morphisme déduit de l'inclusion naturelle de $\mathbf{K}$ dans $\mathbf{K}[X]$. Ce morphisme munit $\mathbf{K}[X]$ d'une structure de $\mathbf{K}$-algèbre, donc de $\mathbf{K}$-espace vectoriel. Par composition ave le morphisme quotient, il induit aussi, pour tout $P \in \mathbf{K}[X]$ une structure de $\mathbf{K}$-algèbre, donc de $\mathbf{K}$-epace vectoriel sur $\mathbf{K}[X]/P\mathbf{K}[X]$.

Théorème 3.2.1 *Soient $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$ un polynôme non constant. Soit $x := [X]_P$. Alors le $\mathbf{K}$-espace vectoriel $\mathbf{K}[X]/P\mathbf{K}[X]$ est de dimension finie, et égale à $\deg P$. De plus, $\{1, x, \dots, x^{\deg P - 1}\}$ en est une base. En particulier, l'application*

$$\begin{array}{rccc} \varphi : & \{Q \in \mathbf{K}[X] \mid \deg Q \leq \deg P\} & \longrightarrow & \mathbf{K}[X]/P\mathbf{K}[X] \\ & Q & \longmapsto & [Q]_P \end{array}$$

est bijective.

PREUVE. Montrons que la famille $\{1, x, \dots, x^{\deg P - 1}\}$ est génératrice. Soit $y \in \mathbf{K}[X]/P\mathbf{K}[X]$. Soit $S \in \mathbf{K}[X]$ tel que $y = [S]_P$. Soit $S = PQ + R$ la division euclidienne de S par P (P est non constant, donc non nul). En particulier, $\deg R < \deg P$. Écrivons $R = \sum_{i=0}^{\deg P - 1} a_i X^i$, avec $(a_i)_i \in \mathbf{K}^{\deg P}$. On a

$$y = [S]_P = [PQ + R]_P = [P]_P[Q]_P + [R]_P = [R]_P.$$

Finalement, on a $y = [R]_P$. Ceci montre déjà que l'application φ de l'énoncé est surjective. De plus,

$$y = [R]_P = \sum_{i=0}^{\deg P - 1} [a_i]_P [X^i]_P = \sum_{i=0}^{\deg P - 1} a_i [X]_P^i = \sum_{i=0}^{\deg P - 1} a_i x^i.$$

Donc la famille $\{1, x, \dots, x^{\deg P - 1}\}$ engendre le $\mathbf{K}$-espace vectoriel $\mathbf{K}[X]/P\mathbf{K}[X]$. Montrer que cette famille est libre est équivalent à montrer que φ est injective. Soit $(a_i)_i \in \mathbf{K}^{\deg P}$ telle que

$$\sum_{i=0}^{\deg P - 1} a_i x^i = 0.$$

Soit $R := \sum_{i=0}^{\deg P - 1} a_i X^i$, on a

$$[R]_P = \sum_{i=1}^{\deg P - 1} a_i x^i = 0,$$

donc P divise R. Or $\deg P < \deg R$, donc $R = 0$. Ainsi,

$$\forall i \in \{0, \dots, \deg P - 1\}, \quad a_i = 0,$$

ce qui conclut. □

2.1 Endomorphismes de la K-algèbre $\mathbf{K}[X]/\langle P \rangle$

Rappel : Soit $\mathbf{K}$ un corps, A une $\mathbf{K}$-algèbre et $a \in A$. On note ev_a l'unique morphisme de $\mathbf{K}$-algèbres de $\mathbf{K}[X]$ vers A qui envoie X sur a.

Théorème 3.2.2 *Soient $\mathbf{K}$ un corps et A une $\mathbf{K}$-algèbre. Alors l'application*

$$\begin{array}{ccc} A & \longrightarrow & \mathrm{Hom}_{\mathbf{K}\text{-}algèbre}(\mathbf{K}[X], A) \\ a & \longmapsto & ev_a \end{array}$$

est une bijection qui induit pour tout $P \in \mathbf{K}[X]$ une bijection de $\{a \in A \mid ev_a(P) = 0\}$ sur $\mathrm{Hom}_{\mathbf{K}\text{-}algèbre}(\mathbf{K}[X]/\langle P \rangle, A)$.

Slogan : Se donner un morphisme de $\mathbf{K}$-algèbres de $\mathbf{K}[X]/\langle P \rangle$ vers A, c'est se donner une racine de P dans A.

PREUVE. La première assertion n'est qu'une reformulation de la propriété universelle de la $\mathbf{K}$-algèbre $\mathbf{K}[X]$.

Soit $P \in \mathbf{K}[X]$, la propriété universelle des $\mathbf{K}$-algèbres quotient dit que $\mathrm{Hom}_{\mathbf{K}\text{-algèbre}}(\mathbf{K}[X]/\langle P \rangle, A)$ sont en bijection naturelle avec

$$\{\varphi \in \mathrm{Hom}_{\mathbf{K}\text{-algèbre}}(\mathbf{K}[X], A) \mid \langle P \rangle \subset \mathrm{Ker}\, \varphi\}.$$

Soit $\varphi \in \mathrm{Hom}_{\mathbf{K}\text{-algèbre}}(\mathbf{K}[X], A)$. Dire que $\langle P \rangle \subset \mathrm{Ker}\, \varphi$ est équivalent à dire que $P \in \mathrm{Ker}\, \varphi$ (par définition de l'idéal engendré par P). Soit $a \in A$ tel que $\varphi = ev_a$, alors

$$P \in \mathrm{Ker}\, \varphi \iff ev_a(P) = 0 \iff P(a) = 0.$$

□

Définition 3.2.3 (Élément algébrique) *Soient* $\mathbf{K}$ *un corps et* A *une* $\mathbf{K}$*-algèbre. Soit* $a \in A$*. On dit que* a *est algébrique sur* $\mathbf{K}$ *si* $\operatorname{Ker} ev_a \neq \{0\}$*. De manière équivalente,* ev_a *n'est pas injectif, ou* a *est racine d'un polynôme non nul de* $\mathbf{K}[X]$*.*

Définition 3.2.4 (Polynôme minimal) *Si* a *est algébrique sur* $\mathbf{K}$*, l'unique polynôme unitaire de* $\mathbf{K}[X]$ *qui engendre* $\operatorname{Ker}(ev_a)$ *est appelé polynôme minimal de* a *sur* $\mathbf{K}$*.*

Définition 3.2.5 (Élément transcendant) *Si* $\operatorname{Ker} ev_a = \{0\}$*,* a *est dit transcendant sur* $\mathbf{K}$*.*

Exemple 3.2.6 Le nombre $\sqrt{2}$ est algébrique sur $\mathbf{Q}$, de polynôme minimal $X^2 - 2$ sur $\mathbf{Q}$, mais il est aussi algébrique sur $\mathbf{R}$ de polynôme $X - \sqrt{2}$. Si $\mathbf{K}$ est un corps, l'élément X de $\mathbf{K}[X]$ est transcendant sur $\mathbf{K}$. Le nombre π est transcendant sur $\mathbf{Q}$.

Proposition 3.2.7 *Soit* $\mathbf{K}$ *un corps et* A *une* $\mathbf{K}$*-algèbre qui est un* $\mathbf{K}$*-espace vectoriel de dimension finie. Alors tout élément de* A *est algébrique sur* $\mathbf{K}$*.*

Exemple 3.2.8 $\mathbf{K}[X]/\langle P\rangle$ avec $P \in \mathbf{K}[X] \setminus \{0\}$.

Proposition 3.2.9 *Soient* $\mathbf{K}$ *un corps,* $P \in \mathbf{K}[X] \setminus \{0\}$ *unitaire,* x *l'image de* X *par le morphisme quotient* $\mathbf{K}[X] \to \mathbf{K}[X]/\langle P\rangle$*. Alors* x *est algébrique sur* $\mathbf{K}$ *de polynôme minimal* P*.*

Proposition 3.2.10 *Soient* $\mathbf{K}$ *un corps et* A *une* $\mathbf{K}$*-algèbre intègre. Soit* $a \in A$ *algébrique sur* $\mathbf{K}$*. Alors le polynôme minimal de* a *sur* $\mathbf{K}$ *est irréductible.*

Définition 3.2.11 (Extension de corps) *Soit* $\mathbf{K}$ *un corps. Une* $\mathbf{K}$*-extension (ou une extension de* $\mathbf{K}$*) est une* $\mathbf{K}$*-algèbre* $\mathbf{L}$*, qui est un corps. Le degré d'une telle extension, noté* $[\mathbf{L} : \mathbf{K}]$ *est la dimension de* $\mathbf{L}$ *comme* $\mathbf{K}$*-espace vectoriel.*

Exemple 3.2.12 $\mathbf{C}$ est une extension de $\mathbf{R}$ de degré 2. $\mathbf{C}$ est une extension de $\mathbf{Q}$ de degré infini. Soit $\mathbf{K}$ un corps, $P \in \mathbf{K}[X]$ irréductible, $\mathbf{K}[X]/\langle P\rangle$ est une extension de $\mathbf{K}$ de degré $\deg P$.

Chapitre 4

Corps finis, applications en cryptographie et en théorie des codes correcteurs d'erreur

1 Introduction, premières propriétés

Proposition 4.1.1 *Soient* $\mathbf{K}$ *un corps fini,* $n \geq 1$ *un entier et* $P \in \mathbf{K}[X]$ *un polynôme irréductible de degré* n*. Alors* $\mathbf{L} := \mathbf{K}[X]/\langle P \rangle$ *est un corps fini, de cardinal* $\mathrm{card}(\mathbf{K})^n$*.*
PREUVE. Comme P est irréductible, la $\mathbf{K}$-algèbre $\mathbf{K}[X]/\langle P \rangle$ est un corps. Sa dimension en tant que $\mathbf{K}$-espace vectoriel est n. En particulier, $\mathbf{L}$ est isomorphe comme $\mathbf{K}$-espace vectoriel à $\mathbf{K}^n$. Donc $\mathbf{L}$ est fini, de cardinal $\mathrm{card}(\mathbf{K}^n) = \mathrm{card}(\mathbf{K})^n$. □

Proposition 4.1.2 *Soit* A *un anneau intègre fini. Alors* A *est un corps fini.*
PREUVE. Voir la feuille de TD 1. □

2 Caractéristique et cardinal d'un corps fini

Notation : Soit p un nombre premier, on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

Théorème 4.2.1 *Soit* $\mathbf{K}$ *un corps fini, alors la caractéristique de* $\mathbf{K}$ *est un nombre premier* p*. En particulier, il existe une unique structure de* $\mathbf{Z}/p\mathbf{Z}$*-algèbre (autrement dit de* $\mathbf{Z}/p\mathbf{Z}$*-extension) sur* $\mathbf{K}$*, qui fait de* $\mathbf{K}$ *un* $\mathbf{Z}/p\mathbf{Z}$*-espace vectoriel de dimension finie, notée* n*. En particulier,* $\mathbf{K}$ *est de cardinal* p^n*. En particulier, le cardinal d'un corps fini est une puissance d'un nombre premier.*
PREUVE. Soit $\varphi_{\mathbf{K}} : \mathbf{Z} \to \mathbf{K}$ l'unique morphisme d'anneaux de $\mathbf{Z}$ vers $\mathbf{K}$. Si $\mathrm{Ker}\,\varphi_{\mathbf{K}} = \{0\}$, alors $\mathbf{K}$ contient un sous-anneau isomorphe à $\mathbf{Z}$, or $\mathbf{Z}$ est infini, et $\mathbf{K}$ est fini. C'est absurde, donc il existe $c \in \mathbf{N}\backslash\{0\}$ tel que $\mathrm{Ker}\,\varphi_{\mathbf{K}} = c\mathbf{Z}$. Par un théorème d'isomorphisme, $\mathbf{K}$ contient un sous-anneau isomorphe à $\mathbf{Z}/c\mathbf{Z}$. Or $\mathbf{K}$ est un corps, donc $\mathbf{K}$ est intègre, donc tout sous-anneau de $\mathbf{K}$ également. Donc $\mathbf{Z}/c\mathbf{Z}$ est intègre, d'où c est premier. On sait alors que $\mathrm{Hom}_{\mathrm{anneaux}}(\mathbf{Z}/p\mathbf{Z}, \mathbf{K})$ est réduit à un élément. $\mathbf{K}$ est un $\mathbf{F}_p$-espace vectoriel fini, donc $\mathbf{K}$ est un $\mathbf{F}_p$-espace vectoriel de dimension finie. Soit $n \in \mathbf{N}$ sa dimension, alors $\mathbf{K}$ est isomorphe, comme $\mathbf{F}_p$-espace vectoriel, à $\mathbf{F}_p^n$. Donc $\mathrm{card}\,\mathbf{K} = \mathrm{card}\,\mathbf{F}_p^n = p^n$. □

3 Un exemple de calcul explicite dans un corps fini qui n'est pas de cardinal premier

Prenons $p := 2$. Le polynôme $P := X^2 + X + [1]_2$ est irréductible dans $\mathbf{F}_2[X]$. En effet, $P([0]_2) = [1]_2 \neq [0]_2$, et $P([1]_2) = [1]_2 \neq [0]_2$, donc P n'a pas de racine dans $\mathbf{F}_2$. or $\deg P = 2$, donc P est irréductible dans $\mathbf{F}_2$. Donc $\mathbf{K} := F_2[X]/\langle X^2 + X + [1]_2 \rangle$ est un corps fini de cardinal $2^2 = 4$.

Remarque 4.3.1 $\mathbf{Z}/4\mathbf{Z}$ n'est pas un corps de cardinal 4.

Notons x l'image de X par le morphisme quotient $\mathbf{F}_2[X] \to \mathbf{F}_2[X]/\langle P \rangle$. On a $P(x) = [0]_2$, soit $x^2 + x + [1]_2 = [0]_2$. on sait que $\{[1]_2, x\}$ est une base du $\mathbf{F}_2$-espace vectoriel $\mathbf{K}$, et que

$$\begin{array}{ccc} \mathbf{F}_2^2 & \longrightarrow & \mathbf{K} \\ (\alpha, \beta) & \longmapsto & \alpha + \beta x \end{array}$$

est une bijection. Soient $(\alpha, \beta) \in \mathbf{F}_2^2$ et $(\alpha', \beta') \in \mathbf{F}_2^2$, alors

$$(\alpha + \beta x) + (\alpha' + \beta' x) = (\alpha + \alpha') + (\beta + \beta')x.$$

On peut alors dresser les tables d'addition et de multiplication dans $\mathbf{K}$.

$+$	$[0]_2$	$[1]_2$	x	$[1]_2 + x$
$[0]_2$	$[0]_2$	$[1]_2$	x	$[1]_2 + x$
$[1]_2$		$[0]_2$	$[1]_2 + x$	x
x			$[0]_2$	$[1]_2$
$[1]_2 + x$				$[0]_2$

$\times$	$[0]_2$	$[1]_2$	x	$[1]_2 + x$
$[0]_2$	$[0]_2$	$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$		$[1]_2$	x	$[1]_2 + x$
x			$[1]_2 + x$	$[1]_2$
$[1]_2 + x$				x

4 Le morphisme de Frobenius

Théorème 4.4.1 *Soient p un nombre premier et A un anneau de caractéristique p. Alors l'application*

$$F_A : \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & x^p \end{array}$$

est un morphisme d'anneaux, appelé morphisme de Frobenius de A. Si $\mathbf{K}$ est un corps fini, $F_{\mathbf{K}}$ est un automorphisme du corps $\mathbf{K}$, i. e. un isomorphisme d'anneaux de $\mathbf{K}$ dans lui-même.

PREUVE. Soient $x, y \in A$. On a

$$F_A(xy) = (xy)^p = x^p y^p = F_A(x)F_A(y),$$

et $F_A(1_A) = 1_A$. L'anneau A étant de caractéristique p, pour tous $a \in A$ et $n \in \mathbf{Z}$ tels que p divise n, on a $na = 0_A$. De plus,

$$F_A(x+y) = (x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k},$$

or pour tout $1 \leq k \leq p-1$, p qui divise $\binom{p}{k}$. Donc $F_A(x+y) = x^p + y^p$, donc c'est un morphisme d'anneaux. Si A est intègre, F_A est injectif. En effet, $\operatorname{Ker} F_A = \{x \in A \mid x^p = 0\} = \{0_A\}$. Si $\mathbf{K}$ est un corps fini, alors $F_{\mathbf{K}} : \mathbf{K} \to \mathbf{K}$ est une application injective, donc surjective. Donc $F_{\mathbf{K}}$ est bijective, et est donc un automorphisme de corps. □