Dernière édition : 8 avril 2020

Notes prises par Téofil Adamski

ANNEAUX ET ARITHMÉTIQUES

(ANAR)

David Bourqui

L3 maths recherche Université de Rennes 1

Chapitre 1 – Notions de base de théorie des anneaux 1
1.1 Définition, notations, règles de calcul . . . 1
1.2 Sous-anneaux d'un anneau . . . 2
1.3 Groupe des éléments inversibles d'un anneau . . . 2
1.4 Morphismes d'anneaux, noyau, image, notion d'idéal 2
1.5 Produits, polynômes et séries formelles . . . 5
1.6 Anneaux quotients . . . 7
1.7 Théorème chinois . . . 8
1.8 Diviseurs de zéros, anneaux intègres, corps . . . 9
1.9 Élément irréductibles d'un anneaux intègre . . . 10
1.10 Notion de structure d'algèbre sur un anneau . . . 11

Chapitre 2 – Étude de $\mathbb{Z}/n\mathbb{Z}$ et $K[X]/PK[X]$ 12
2.1 Étude du quotient $\mathbb{Z}/n\mathbb{Z}$ . . . 12
2.2 Étude du quotient $\mathbb{K}[X]/P\mathbb{K}[X]$ . . . 13

Chapitre 3 – Corps finis et applications 14
3.1 Introduction et premières propriétés . . . 14
3.2 Caractéristique et cardinal d'un corps fini . . . 14
3.3 Un exemple de calcul explicite dans un corps fini . . 14
3.4 Le morphisme de Frobenius . . . 14
3.5 Le groupe des inversible d'un corps fini est cyclique 14
3.6 Deux corps finis de même cardinal sont isomorphes 15
3.7 Toute puissance d'un nombre premier est le cardinal d'un corps fini . . . 16

Chapitre 4 – Localisation, corps des fractions 17
4.1 Un exemple . . . 17
4.2 Définition et propriétés élémentaires du localisé . . . 17
4.3 Le corps des fractions d'un anneau intègre . . . 19

Chapitre 5 – Anneaux euclidiens, principaux, factoriels 21
5.1 Lemme d'Euclide, lemme de Gauss, théorème de Bézout et factorisation unique . . . 21
5.2 Anneaux factoriels, principaux, euclidiens . . . 22
5.3 Valuations dans un anneau factoriel . . . 23
5.4 PGCD, PPCM et relations de Bézout . . . 24
5.5 Valuations, PGCD et PPCM dans le corps des fractions . . . 26
5.6 Factorialité des anneaux polynômes, critères d'irréductibilité . . . 26
5.7 Démonstration des théorèmes . . . 28

Chapitre 1

Notions de base de théorie des anneaux

1.1 Définition, notations, règles de calcul 1
1.2 Sous-anneaux d'un anneau 2
1.3 Groupe des éléments inversibles d'un anneau 2
1.4 Morphismes d'anneaux, noyau, image, notion d'idéal . 2
1.5 Produits, polynômes et séries formelles 5
1.6 Anneaux quotients 7
1.7 Théorème chinois 8
1.8 Diviseurs de zéros, anneaux intègres, corps 9
1.9 Élément irréductibles d'un anneaux intègre 10
1.10 Notion de structure d'algèbre sur un anneau 11

1.1 Définition, notations, règles de calcul

▷ Exemples. Les ensembles $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{R}(X)$, $\mathbb{C}(X)$ sont des anneaux. Pour tout $n \in \mathbb{Z}$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est un anneau. Pour tout $n \in \mathbb{Z} \setminus \{0\}$, l'ensemble $\mathbb{Z}[1/n]$ est un anneau.

Définition 1.1. Un anneau est un triplet $(A, *, \perp)$ où A est un ensemble et $*$ et $\perp$ deux lois de composition interne sur A vérifiant les propriétés suivantes :

(i) le couple $(A, *)$ est un groupe commutatif ;

(ii) le loi $\perp$ est associative, commutative et possède un élément neutre ;

(iii) le loi $\perp$ est distribution par rapport à la loi $*$ ce qui signifie

$$\forall a, b, c \in A, \quad a \perp (b * c) = (a \perp b) * (a \perp c).$$

Notation. La loi $*$ est quasi systématiquement notée additivement, *i. e.* avec le symbole $+$: pour tous $a, b \in A$, on note $a + b$ pour $a * b$ et $-a$ le symétrique de a pour la loi $*$. On note 0 ou 0_A l'élément neutre de la loi $+$.

Loi loi $\perp$ est souvent notée multiplicativement : pour tous $a, b \in A$, on note $a \times b$ ou ab pour $a \perp b$. On note 1 ou 1_A l'élément neutre pour la loi $\perp$.

On écrit très souvent « Soit A un anneau » plutôt que « Soit $(A, +, \times)$ un anneau », les lois seront toujours désignées par les symboles $+$ et $\times$ quand le contexte sera clair.

Règles de propriétés d'écriture. Soit $(A, +, \times)$ un anneau. La loi $\times$ est prioritaire sur la loi $+$. Ainsi, pour tous $a, b \in A$, l'écriture $a + b \times c$ désigne $a + (b \times c)$.

Règles de calcul élémentaires. Soit $a \in A$. Pour tout $n \in \mathbb{Z}$, on peut définir la « somme itérée n fois » de a, notée $n \cdot a$ ou na (comme dans n'importe quel groupe commutatif noté additivement). Pour tout $n \in \mathbb{Z}$, on peut définir la puissance n-ième de a, notée a^n, et on a les règles usuelles de calculs suivantes.

Proposition 1.2. Soit $(A, +, \times)$ un anneaux. Alors

1. pour tout $a \in A$, on a $a \times 0_A = 0_A \times a = 0_A$;
2. pour tous $a, b \in A$, on a $a \times (-b) = (-a) \times b = -(a \times b)$;
3. pour tous $a, b \in A$, on a $(-a) \times (-b) = a \times b$;
4. pour tous $a, b \in A$ et $m \in \mathbb{Z}$, on a $(ma) \times b = a \times (mb) = m(a \times b)$.

Preuve 1. Soit $a \in A$. Par commutativité de la loi $\times$, on a $a \times 0_A = 0_A \times a$. De plus, on a $a \times 0_A = a \times (0_A + 0_A)$, donc $a \times 0_A = a \times 0_A + a \times 0_A$ par distributivité. En ajoutant $-(a \times 0_A)$ aux deux membres de la dernière égalité, on obtient que $0_A = a \times 0_A$. □

◇ Remarques. 1. Le dernier point n'est pas une conséquence directe de l'associativité de la loi $\times$.

2. Soient $(A, +, \times)$ un anneaux, I un ensemble fini et $(a_i)_{i \in I}$ une famille d'éléments de A indexée par I. On peut donner un sens naturel à $\sum_{i \in I} a_i$ et $\prod_{i \in I} A_i$ avec les propriétés attendues. Par convention, si I est vide, on note $\sum_{i \in I} a_i = 0_A$ et $\prod_{i \in I} A_i = 1_A$.

Proposition 1.3 *(formule du binôme de Newton).* Soient $(A, +, \times)$ un anneaux, $a, b \in A$ et $n \in \mathbb{N}$. Alors

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

Proposition 1.4. Soient A un anneau, $n \in \mathbb{N}$ et $a, b \in A$. Alors

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

1.2 Sous-anneaux d'un anneau

Définition 1.5. Soit A un anneau. Un sous-anneau de A est une partie B de A vérifiant les propriétés suivantes :
(i) la partie B est un sous-groupe de $(A, +)$;
(ii) elle est stable par la loi $\times$;
(iii) $1_A \in B$.

Proposition 1.6. Soient A un anneaux et B un sous-anneau de A. Alors les loi $+$ et $\times$ de A induisent sur B des lois $+$ et $\times$ et, muni de ces loi, B est un anneau.

▷ Exemples. – On considère les anneaux $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$. Toute inclusion de l'un de ces anneaux dans un autre (par exemple $\mathbb{Z} \subset \mathbb{C}[X]$) fait du premier un sous-anneau du second.
– Soit I un intervalle de $\mathbb{R}$. Alors $\mathbb{R}^I$ est muni d'une structure naturelle d'anneau. Alors l'ensemble des éléments de $\mathbb{R}^I$ constitué des fonctions continues, dérivables et de classe $\mathscr{C}^\infty$ constitue un sous-anneau de $\mathbb{R}^I$.
– Soit A un anneau. Alors $B \coloneqq \{n1_A \mid n \in \mathbb{Z}\}$ est un sous-anneau de A.

Proposition 1.7. Soient A un anneau, E un ensemble et $(B_e)_{e\in E}$ une famille de sous-anneaux de A. Alors l'intersection $\bigcup_{e\in E} B_e$ est un sous-anneau de A.

Définition-proposition 1.8. Soient A un anneau et S une partie de A. Alors il existe un unique sous-anneau B de A contenant S et minimal au sens de l'inclusion pour cette propriété, *i. e.* pour tout sous-anneau C de A contenant S, on a $B \subset C$. On appelle cet anneau B le sous-anneau de A engendré par S.

Preuve Nécessairement, la partie B est l'intersection de tous les sous-anneaux de A contenant S et cette intersection est un sous-anneau de A (d'après la proposition précédente) contenant S. □

1.3 Groupe des éléments inversibles d'un anneau

Définition 1.9. Soit A un anneau. Un élément a de A est dit inversible dans A s'il existe un symétrique de a pour la seconde loi. On note $A^\times$ l'ensemble des éléments inversibles de A.

◇ Remarque. Si $a \in A$ est inversible, alors son inverse est unique et on le note a^{-1}.

▷ Exemple. On a $\mathbb{R}[X]^\times = \mathbb{R}^\times$.

Théorème 1.10. Soit A un anneau. Alors $A^\times$ est stable par multiplication. Muni de la loi de composition interne induit, c'est un groupe commutatif.

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

Définition 1.11. Soient A et B deux d'anneaux. Un morphisme d'anneaux de A vers B est une application $\varphi\colon A \to B$ vérifiant
1. pour tous $a, a' \in A$, on a $\varphi(a + a') = \varphi(a) + \varphi(a')$;
2. pour tous $a, a' \in A$, on a $\varphi(a \times a') = \varphi(a) \times \varphi(a')$;
3. $\varphi(1_A) = 1_B$.

On note $\mathrm{Hom}_{\mathrm{ann}}(A, B)$ l'ensemble des morphismes d'anneaux de A vers B.

◇ Remarque. Étant données deux anneaux A et B, il n'existe pas toujours de morphismes d'anneaux de A vers b. Il suffit de prendre l'exemple de $A = \mathbb{Q}$ et $B = \mathbb{Z}$.

Proposition 1.12. Soit $\varphi\colon A \to B$ 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.

Définition 1.13. La noyau d'un morphisme d'anneaux $\varphi\colon A \to B$ est l'ensemble

$$\operatorname{Ker}\varphi \coloneqq \varphi^{-1}(0_B) = \{a \in A \mid \varphi(a) = 0_B\}.$$

Proposition 1.14. 1. L'application réciproque d'un morphisme d'anneaux bijectif et encore un morphisme d'anneaux.
2. La composée de deux morphismes d'anneaux est un morphisme d'anneaux.
3. Un morphisme d'anneaux est injectif si et seulement si son noyau est le groupe trivial.
4. Soit $\varphi\colon A \to B$ un morphisme d'anneaux. Alors $\varphi(A^\times) \subset B^\times$ et l'application induite $\check{\varphi}\colon A^\times \to B^\times$ est un morphisme de groupes.

Théorème 1.15. Soit A un anneau. Alors il existe un unique morphisme d'anneaux $\mathbb{Z} \to A$: c'est l'application $n \longmapsto n \cdot 1_A$.

Définition 1.16. Un isomorphisme d'anneaux est un morphisme d'anneaux bijectif. Deux anneaux sont dits isomorphes s'il existe un isomorphisme d'anneaux entre les deux.

Proposition 1.17. Un morphisme d'anneaux $\varphi\colon A \to B$ est un isomorphisme d'anneaux si et seulement s'il existe un morphisme d'anneaux $\psi\colon B \to A$ tel que $\varphi \circ \psi = \mathrm{Id}_B$ et $\psi \circ \varphi = \mathrm{Id}_B$.

Définition 1.18. Soit A un anneau. Un idéal de A est une partie I de A telle que
1. I est un sous-groupe de $(A, +)$;
2. pour tous $a \in I$ et $b \in A$, on a $ab \in I$.

Proposition 1.19. Soient A un anneau et I un idéal de A. Alors les propositions suivantes sont équivalentes :
(i) $I = A$;
(ii) $1_A \subset I$;
(iii) $I \cap A^\times \neq \emptyset$.

Proposition 1.20. 1. Le noyau d'un morphisme d'anneaux est un idéal.
2. Plus généralement, l'image réciproque d'un idéal par un morphisme d'anneaux est un idéal.
3. Soit $\varphi\colon A \to B$ un morphisme d'anneaux surjectif. Alors l'image d'une idéal de A par φ est un idéal de B. En autre, l'application $I \longmapsto \varphi(I)$ est une bijection de l'ensemble des idéaux de A contenant $\operatorname{Ker}\varphi$ dans l'ensemble des idéaux de B. Sa bijection réciproque est $I' \longmapsto \varphi^{-1}(I')$.

Définition 1.21. Soient A un anneau et I et J deux idéaux de A. On note

$$I + J = \{a + b \mid a \in I, b \in J\},$$
$$I \cdot J = \{a_1 b_1 + \cdots + a_n b_n \mid n \in \mathbb{N}^*, (a_1, \ldots, a_n) \in A^n, (b_1, \ldots, b_n) \in B^n\}.$$

On peut généraliser ces définitions à une famille finie d'idéaux $(I_e)_{e\in E}$ et on note $\sum_{e\in E} I_e \subset A$ et $\bigodot_{e\in E} I_e \subset A$ respectivement la somme et le produit.

Proposition 1.22. Soit A un anneaux et $(I_e)_{e\in E}$ une famille d'idéaux de E. Alors $\bigcup_{e\in E} I_e$ est un idéal de A. Si E est fini, alors $\sum_{e\in E} I_e$ et $\bigodot_{e\in E} I_e$ en sont aussi.

Attention. En général, si I est un idéal, on n'a pas $I + I = 2I$.

Définition-proposition 1.23. Soient A un anneau et $S \subset A$. Alors il existe un unique idéal minimal de A contenant S. On le note $S \cdot A$ ou $\langle S \rangle$ et on l'appelle l'idéal engendré par S. On a

$$S \cdot A = \left\{ \sum_{s\in S} a_s \cdot s \;\middle|\; (a_s)_{s\in S} \in A^{(S)} \right\}.$$

Si $T \subset A$, alors

$$(S \cdot A) + (T \cdot A) = (S \cup T) \cdot A \quad \text{et} \quad (S \cdot A)(T \cdot A) = (ST) \cdot A.$$

Preuve • *Unicité.* Soient I et J deux tels anneaux. Alors $I \cap J$ est un idéal qui contient S. Par minimalité, on a donc $I \cap J = I$ et $I \cap J = J$, donc $I = J$.

• *Existence.* On considère I l'intersection de tous les idéaux contenant S. Alors I est aussi un idéal contenant S et, par définition, il est minimum et *a fortiori* minimal. Montrons que $S \cdot A = I$. Pour simplifier, supposons

que S est de cardinal fini $n \in \mathbb{N}$ et notons $S = \{s_1, \dots, s_n\}$. On pose

$$E = \Big\{ \sum_{i=1}^{n} a_i s_i \;\Big|\; a_1, \dots, a_n \in A \Big\}.$$

On veut montrer que E est l'idéal engendré par S. L'ensemble E contient clairement S et est un idéal de A. Montrons que tout idéal I de A contenant S est contient E. Soient $x \in E$ qu'on note $x = \sum_{i=1}^{n} a_i s_i$. Pour tout $i \in [\![1, n]\!]$, comme I est un idéal, on a $a_i x_i \in I$. Comme I est un sous-groupe additif de $(A, +)$, on a $x \in I$. D'où $E \subset I$. D'où $E = S \cdot A$.

On procède de même pour les deux autres identités. □

◇ Remarque. Si un idéal I contient deux idéal J et $\mathbb{K}$, il contient $J + \mathbb{K}$.

Notation. Si $S = \{s_1, \dots, s_n\}$ est une partie finie de cardinal $n \in \mathbb{N}^*$, l'idéal $S \cdot A$ peut être noté $\langle s_1, \dots, s_n \rangle$ et on a $S \cdot A = s_1 A + \cdots + s_n A$.

Définition 1.24. On dit qu'un idéal I de A est *premier* si

1. I est un idéal propre,
2. pour tous $x, y \in A$, si $xy \in I$, alors $x \in I$ ou $y \in I$.

On dit qu'un idéal I de A est *maximal* si

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

Proposition 1.25. Un idéal maximal de A est premier.

Preuve Soit I un idéal maximal de A. Alors I est propre. Soient $x, y \in A$ tels que $xy \in I$. Supposons que $x \notin I$. L'idéal J engendré par I et x est un idéal contenant strictement I. Comme I est maximal, on a $J = A$. Or $J = I + xA$ et 1 appartient à J, donc il s'écrit sous la forme $1 = z + xw$ avec $z \in I$ et $w \in A$. Comme $yz \in I$, on a $y = yz + yxw \in I$. On en déduit que I est premier. □

▷ Exemples. – L'idéal $\{0\}$ de $\mathbb{Z}$ est premier, mais il n'est pas maximal. En effet, pour $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$, l'idéal $n\mathbb{Z}$ est propre et contient strictement $\{0\}$.
– L'idéal $X\mathbb{Z}[X]$ de $\mathbb{Z}[X]$ est premier et non nul, mais il n'est pas maximal puisque $\langle 2, X \rangle$ est un idéal propre de $\mathbb{Z}[X]$ contenant strictement $X\mathbb{Z}[X]$.

Théorème 1.26 *(lemme de Zorn).* Tout idéal propre de A est inclus dans un idéal maximal. En particulier, un anneau non nul possède au moins un idéal premier.

◇ Remarque. Il vient que $\operatorname{Card} A = 1$ si et seulement si $0_A = 1_A$. En particulier, de tels anneaux sont tous isomorphes et on les appelle des anneaux nuls.

Proposition 1.27. L'image réciproque d'un idéal premier par un morphisme d'anneaux est un idéal premier.

Proposition 1.28. 1. Soit I un idéal de $\mathbb{Z}$. Alors il existe $n \in \mathbb{Z}$ tel que $I = n\mathbb{Z}$.
2. Soient $m, n \in \mathbb{Z}$. Alors $n\mathbb{Z} \subset m\mathbb{Z}$ si et seulement si $m \mid n$. Ainsi, on a $n\mathbb{Z} = m\mathbb{Z}$ si et seulement si $|n| = |m|$.
3. Un idéal de $\mathbb{Z}$ est premier si et seulement s'il s'écrit $n\mathbb{Z}$ où $n \in \mathbb{Z}$ tel que $n = 0$ ou $|n|$ est premier.
4. Un idéal de $\mathbb{Z}$ est maximal si et seulement s'il s'écrit $n \in \mathbb{Z}$ où $|n|$ est premier.

Preuve 1. Si $I = \{0\}$, alors $I = 0\mathbb{Z}$. Supposons que $I \neq \{0\}$. On considère $n_0 := \min(I \cap \mathbb{N}^*)$. On a $n_0 \in I$, donc $n\mathbb{Z} \subset I$. Réciproquement, soit $n \in I$. Comme $n_0 \neq 0$, on écrit $n = n_0 q + r$ avec $q \in \mathbb{Z}$ et $r \in [\![0, n_0 - 1]\!]$ la division euclidienne de n par n_0. On a $n \in I$ et $n_0 q \in I$, donc $r \in I$. Or $0 \leqslant r < n_0$, donc $r = 0$. On en déduit que $n = n_0 q \in n_0\mathbb{Z}$. D'où $I = n_0\mathbb{Z}$.

3 & 4. Soit $n \in \mathbb{Z}$ tel que $n\mathbb{Z}$ soit propre, *i. e.* $n \notin \{\pm 1\}$. La condition « un produit d'élément de $\mathbb{Z}$ est dans $n\mathbb{Z}$ si et seulement si l'un des deux facteurs est dedans » se traduit par « n divise un produit de deux entiers relatifs si et seulement si n divise l'un des deux facteurs ». Par le lemme d'Euclide, ceci est vrai si $|n|$ est premier ou si $n = 0$.

Soit $n \in \mathbb{N}$ premier. Montrons que $n\mathbb{Z}$ est maximal. Il est propre. Soit J un idéal de $n\mathbb{Z}$ contenant $n\mathbb{Z}$. On le note $J = m\mathbb{Z}$. Alors $m \mid n$. Or n est premier, donc $|m| \in \{1, n\}$, donc $m\mathbb{Z} = \mathbb{Z}$ ou $m\mathbb{Z} = n\mathbb{Z}$. □

Définition 1.29. La *caractéristique* d'un anneau A est l'unique entier $c \in \mathbb{N}$ tel que l'unique morphisme $\mathbb{Z} \to A$ ait pour noyau $c\mathbb{Z}$.

▷ Exemples. – Les anneaux $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$ sont de caractéristique 0.
– Soit $n \in \mathbb{N}$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n. L'anneau $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est de caractéristique 4 et l'anneau $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est de caractéristique 6.

Définition 1.30. Soit $\mathbb{K}$ un corps. Un polynôme $P \in \mathbb{K}[X]$ est dit *irréductible* s'il est non nul, non constant et

$$\forall Q, R \in \mathbb{K}[X], \quad P = QR \quad \Longrightarrow \quad \deg Q = 0 \text{ ou } \deg R = 0.$$

Proposition 1.31. Soit $\mathbb{K}$ un corps.

1. Si I est un idéal de $\mathbb{K}[X]$, alors il existe $P \in \mathbb{K}[X]$ tel que $I = P\mathbb{K}[X]$.
2. Soient $P, Q \in \mathbb{K}[X]$. Alors $P\mathbb{K}[X] \subset Q\mathbb{K}[X]$ si et seulement si $Q \mid P$. Ainsi, on a $P\mathbb{K}[X] = Q\mathbb{K}[X]$ si et seulement s'il existe $\alpha \in \mathbb{K}^\times$ tel que $Q = \alpha P$.
3. Un idéal de $\mathbb{K}[X]$ est premier si et seulement s'il est engendré par un polynôme nul ou irréductible.
4. Un idéal de $\mathbb{K}[X]$ est maximal si et seulement s'il est engendré par un polynôme irréductible.

1.5 Produits, polynômes et séries formelles

Définition-proposition 1.32. Soit $(A_e)_{e\in E}$ une famille d'anneaux. On munit le produit cartésien $\prod_{e\in E} A_e$ des additions et multiplications terme à terme. Alors c'est un anneau.

Proposition 1.33. 1. Alors

$$\Big(\prod_{e\in E} A_e\Big)^\times = \prod_{e\in E} A_e^\times.$$

2. Soit $f \in E$. Alors la projection

$$\pi_f : \left| \begin{array}{l} \displaystyle\prod_{e\in E} A_e \longrightarrow A_f, \\ (a_e)_{e\in E} \longmapsto a_f \end{array} \right.$$

est un morphisme d'anneaux. Soit C un anneaux. Alors l'application

$$\left| \begin{array}{l} \mathrm{Hom}_{\mathrm{ann}}\Big(C, \displaystyle\prod_{e\in E} A_e\Big) \longrightarrow \displaystyle\prod_{e\in E} \mathrm{Hom}_{\mathrm{ann}}(C, A_e), \\ \qquad\qquad \varphi \longmapsto (\pi_e \circ \varphi)_{e\in E} \end{array} \right.$$

est une bijection.

Notation. Soit $(\varphi_e)_{e\in E} \in \prod_{e\in E} \mathrm{Hom}_{\mathrm{ann}}(C, A_e)$. On note $\prod_{e\in E} \varphi_e$ l'élément de $\mathrm{Hom}_{\mathrm{ann}}(C, \prod_{e\in E} A_e)$ correspondant par la proposition précédente.

Proposition 1.34. 1. On munit $A^{\mathbb{N}}$ des lois définies par, pour toutes $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$,

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}} \quad \text{et} \quad (a_n)_{n\in\mathbb{N}} \times (b_n)_{n\in\mathbb{N}} = \Big(\sum_{\substack{k,\ell\in\mathbb{N} \\ k+\ell=n}} a_k b_\ell \Big)_{n\in\mathbb{N}}.$$

Alors $A^{\mathbb{N}}$ est un anneau.
2. L'ensemble $A^{(\mathbb{N})}$ des suites presque nulles de A est un sous-anneau de $A^{\mathbb{N}}$. On note $X = (X_n)_{n\in\mathbb{N}} \in A^{(\mathbb{N})}$ définie par $X_1 = 1_A$ et $X_n = 0_A$ pour tout $n \neq 1$.
3. Le sous-ensemble de $A^{\mathbb{N}}$ constitué des suites nulles sauf en indice 0 est un sous-anneau de $A^{\mathbb{N}}$ isomorphe à A.
4. Pour tout $N \in \mathbb{N}$, on a $X^N = (\mathbb{1}_{\{N\}}(n))_{n\in\mathbb{N}}$.
5. Soit $(a_n)_{n\in\mathbb{N}} \in A^{(\mathbb{N})}$. Alors $(a_n X^n)_{n\in\mathbb{N}}$ est une suite presque nulle de $A^{(\mathbb{N})}$ et

$$(a_n)_{n\in\mathbb{N}} = \sum_{n\in\mathbb{N}} a_n X^n.$$

Notation. Un élément $(a_n)_{n\in\mathbb{N}} \in A^{\mathbb{N}}$ est vu comme un élément de $(A^{\mathbb{N}}, +, \times)$ et sera noté $\sum_{n=0}^{+\infty} a_n X^n$. On utilisera systématiquement ce genre de notation. Par exemples, si $N \in \mathbb{N}$ et $\sum_{n=0}^{+\infty} a_n X^n \in A^{\mathbb{N}}$, 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 $A^{\mathbb{N}}$ muni des lois définies précédemment, appelé l'anneau des *séries formelles* à une indéterminée à coefficients dans A. On note $A[X]$ le sous-anneau $A^{(\mathbb{N})}$, appelée l'anneau des *polynôme* à une

indéterminée à coefficients dans A.

On va adopter les conventions classiques suivantes. On ajoute un élément $-\infty \notin \mathbb{N}$ tel que $-\infty \leqslant n$ et $n + (-\infty) = (-\infty) + n = -\infty$ pour tout $n \in \mathbb{N}$.

DÉFINITION 1.35. Le *degré* d'un polynôme $P \coloneqq \sum_{n=0}^{+\infty} a_n X^n \in A[X]$ est l'entier

$$\deg P \coloneqq \sup \{n \in \mathbb{N} \mid a_n \neq 0\} \in \mathbb{N} \cup \{-\infty\}.$$

Si $\deg P \in \mathbb{N}$, le *coefficient dominant* de P est l'élément $ta_{\deg P}$.

PROPOSITION 1.36. Soient $P, Q \in A[X]$. Alors

1. $\deg P = -\infty$ si et seulement si $P = 0$;
2. $\deg(P + Q) \leqslant \max(\deg P, \deg Q)$ avec égalité si $\deg P \neq \deg Q$;
3. $\deg(PQ) \leqslant \deg P + \deg Q$ avec égalité si $P = 0$ ou si $P \neq 0$ et le coefficient dominant de P n'est pas un diviseur de zéro.
4. Soit $\alpha \in A$. On note $P = \sum_{n=0}^{+\infty} a_n X^n$. Alors $P(\alpha) \coloneqq \sum_{n=0}^{+\infty} a_n \alpha^n$ est bien définie et l'application

$$\mathrm{ev}_\alpha : \left| \begin{array}{l} A|X] \longrightarrow A, \\ \quad P \longmapsto P(\alpha) \end{array} \right.$$

est un morphisme d'anneaux.
5. Si A est intègre, alors $A[X]$ est intègre.

Preuve L'ensemble $\{n \in \mathbb{N} \mid a_n \neq 0\}$ est une partie majorée de $\mathbb{N}$, donc il admet une borne supérieure. Donc le degré de P existe.

Justifions le point 4. Comme $(a_n)_{n\in\mathbb{N}}$ est une suite presque nulle, la suite $(a_n\alpha^n)_{n\in\mathbb{N}}$ est aussi presque nulle, donc la somme $\sum_{n=0}^{+\infty} a_n\alpha^n$ à un sens. On montre alors que l'évaluation ev_α définit bien un morphisme d'anneaux.

Justifions le point 5. Soient $P, Q \in A[X] \setminus \{0\}$. Montrons que $PQ \neq 0$. Comme A est intègre, tout élément non nul n'est pas un diviseur de zéro, donc $\deg(PQ) = \deg P + \deg Q$. Comme P et Q ne sont pas nuls, leurs degrés appartiennent à $\mathbb{N}$, donc $\deg(PQ) \in \mathbb{N}$, donc $PQ \neq 0$. □

On adopte des conventions similaires pour l'ajout d'un symbole $+\infty \notin \mathbb{N}$.

DÉFINITION 1.37. Le *valuation* d'une série formelle $P \coloneqq \sum_{n=0}^{+\infty} a_n X^n \in A[\![X]\!]$ est l'entier

$$\nu(P) \coloneqq \inf \{n \in \mathbb{N} \mid a_n \neq 0\} \in \mathbb{N} \cup \{+\infty\}.$$

Si $\nu(P) \in \mathbb{N}$, la *composante angulaire* de P est l'élément $a_{\nu(P)}$.

PROPOSITION 1.38. Soient $P, Q \in A[\![X]\!]$.

1. $\nu(P) = +\infty$ si et seulement si $P = 0$;
2. $\nu(P + Q) \leqslant \min(\nu(P), \nu(Q))$ avec égalité si $\nu(P) \neq \nu(Q)$;
3. $\nu(PQ) \geqslant \nu(P) + \nu(Q)$ avec avec égalité si $P = 0$ ou si $P \neq 0$ la composante angulaire de P n'est pas un diviseur de zéro ;
4. si A est intègre, alors $A[\![X]\!]$ est intègre.

PROPOSITION 1.39. Soient $P_1, P_2 \in A[X]$ tels que $P_2 \neq 0$. On suppose que le coefficient dominant de P_2 est inversible. Alors il existe un unique couple $(Q, R) \in A[X] \times A[X]$ tel que $P_1 = QP_2 + R$ et $\deg R < \deg P_2$.

◇ REMARQUE. L'hypothèse d'inversibilité du coefficient dominant de P_2 est nécessaire. En effet, il suffit de considérer $P_1 = X$ et $P_2 = 2X$ dans $\mathbb{Z}[X]$.

Preuve • *Unicité.* Supposons l'existence de deux tels couples (Q, R) et (Q', R'). Alors $(Q - Q')P_2 = R' - R$. Or comme le coefficient dominant de P_2 est inversible, on a $\deg(R - R') = \deg(Q - Q') + \deg P_2$. Or $\deg(R - R') \leqslant \max(\deg R, \deg R') < \deg P_2$, donc $\deg(Q - Q') = -\infty$, donc $Q = Q'$. On en déduit ainsi que $R = R'$.

• *Existence.* On procède par récurrence sur le degré n de P_1. Si $n < \deg P_2$, alors on prend $Q = 0$ et $R = P_1$. On suppose que $n \geqslant \deg P_2$ et qu'il existe une division euclidienne de P_1 de degré inférieur à $n - 1$ par P_2. On écrit $P_1 = a_n X^n + \tilde{P}_1$ avec $\deg \tilde{P}_1 < n$ et $P_2 = \alpha_{\deg P_2} X^{\deg P_2} + \tilde{P}_2$ avec $\deg \tilde{P}_1 < \deg P_2$. Par hypothèse, l'élément $\alpha_{\deg P_2}$ est inversible. On considère

$$\overline{P}_1 \coloneqq P_1 - a_n \alpha_{\deg P_2}^{-1} X^{n - \deg P_2} P_2.$$

Alors $\deg \overline{P}_1 \leqslant n - 1$. Par hypothèse, il existe une division euclidienne de $\overline{P}_1$ par P_2. Soit (Q, R) un couple adéquat. 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. Si A est un corps, ce résultat permet de montrer que tout idéal de $A[X]$ est engendré par un seul élément.

Définition 1.40. On appelle *zéro* ou *racine* d'un polynôme $P \in A[X]$ tout élément $\alpha \in A$ tel que $P(\alpha) = 0$.

Corollaire 1.41. Soient $P \in \mathbb{K}[X]$ et $\alpha \in A$. Alors α est une racine de P si et seulement s'il existe $Q \in A[X]$ tel que $P = (X - \alpha)Q$.

Preuve Le sens réciproque est trivial. On suppose que α est une racine de P. Comme $X - \alpha$ admet un coefficient dominant inversible, il existe $(Q, R) \in A[X] \times A[X]$ tel que $P = (X - \alpha)Q + R$ et $\deg R < \deg(X - \alpha) = 1$. On en déduit alors que $R(\alpha) = 0$. Comme R est de degré inférieur à zéro, il est constant égal à $R(\alpha) = 0$, donc $R = 0$. D'où $P = (X - \alpha)Q$. □

Corollaire 1.42. Soient A un anneau intègre et $P \in A[X] \setminus \{0\}$. Alors P a au plus $\deg P$ racines dans A. En particulier, si $P \in A[X]$ admet une infinité de racines dans A, alors $P = 0$.

Théorème 1.43. Soient $\iota \colon A \to A[X]$ l'injection naturelle et B un anneau. Alors l'application

$$\left|\begin{aligned} \mathrm{Hom}_{\mathrm{ann}}(A[X], B) &\longrightarrow \mathrm{Hom}_{\mathrm{ann}}(A, B) \times B, \\ \varphi &\longmapsto (\varphi \circ \iota, \varphi(X)) \end{aligned}\right.$$

est une bijection.

Soit $N \geqslant 2$. Il y a deux façons naturelles de définir l'anneau $A[X_1, \dots, X_N]$ des polynômes à N indéterminées à coefficients dans A : soit on définit

$$A[X_1, \dots, X_N] \coloneqq (A[X_1])[X_2, \dots, X_N]$$

par induction sur N, soit on pose $A[X_1, \dots, X_N] \coloneqq A^{(\mathbb{N}^N)}$ et on définit l'addition et la multiplication de manière *ad hoc*. Par la première construction, on voit que, si A est intègre, alors $A[X_1, \dots, X_N]$ est intègre. Un élément de $A[X_1, \dots, X_N]$ se met sous la forme

$$\sum_{\substack{n \in \mathbb{N}^N \\ n = (n_1, \dots, n_N)}} a_n X_1^{n_1} \cdots X_N^{n_N} \quad \text{avec} \quad (a_n)_{n \in \mathbb{N}^N} \in A^{(\mathbb{N}^N)}.$$

Théorème 1.44. Soient A et B deux anneaux et $N \geqslant 1$ un entier. On note $\iota \colon A \to A[X_1, \dots, X_N]$ le morphisme d'anneaux injectif naturel. Alors l'application

$$\left|\begin{aligned} \mathrm{Hom}(A[X_1, \dots, X_N], B) &\longrightarrow \mathrm{Hom}(A, B) \times B^N, \\ \varphi &\longmapsto (\varphi \circ \iota, \varphi(X_1), \dots, \varphi(X_N)) \end{aligned}\right.$$

est bijective.

1.6 Anneaux quotients

Théorème 1.45. Soient A un anneau et I un idéal de A. Alors il existe un anneau B et un morphisme surjectif $\pi \colon A \to B$ tels que $\operatorname{Ker} \varphi = I$. De plus, le couple (B, π) est unique à isomorphisme près : si (B', π') est un autre tel couple, alors il existe un unique isomorphisme d'anneaux $\varphi \colon B \to B'$ tel que $\varphi \circ \pi = \pi'$.

L'anneau B est appelé l'*anneau quotient* de A par I et on le note A/I. Le morphisme π est appelé le *morphisme quotient*. L'énoncé d'unicité nous permet de parler de l'anneau quotient de A par I.

Théorème 1.46 *(propriété universelle).* Soient A un anneau et I un idéal de A. On note $\pi \colon A \to A/I$ le morphisme quotient. Soient B un anneau et $\varphi \colon A \to B$ un morphisme d'anneaux tel que $\operatorname{Ker} \varphi \supset I$. Alors il existe un unique morphisme d'anneaux $\psi \colon A/I \to B$ tel que $\psi \circ \pi = \varphi$. En outre,

– le morphisme ψ est surjectif si et seulement si le morphisme φ l'est ;
– le morphisme ψ est injectif si et seulement si $\operatorname{Ker} \varphi = I$.

Preuve Plus généralement considérons un morphisme d'anneaux surjectif $\pi \colon A \to \mathbb{C}$ de noyau I. Ceci montrera l'unicité dans le théorème précédent. Soit $s \colon C \to A$ une section ensemble de φ, *i. e.* telle que $\pi \circ s = \mathrm{Id}_C$.

Montrons l'unicité de tel morphisme ψ. On a $\varphi \circ s = \psi \circ \pi \circ = \psi$ ce qui montre l'unicité. Montrons son existence. Montrons que $\psi \coloneqq \varphi \circ s$ est bien un morphisme d'anneaux. Soit $c, c' \in C$. On a $\varphi(s(c + c')) = \varphi(s(c) + s(c'))$, donc $s(c + c') - (s(c) + s(c')) \in I$. Comme $I \in \operatorname{Ker} \varphi$, on a $\varphi(s(c + c')) = \varphi(s(c) + s(c')) = \varphi(s(c)) + \varphi(s(c'))$.

De même, on montre que $\varphi(s(cc')) = \varphi(s(c))\varphi(s(c'))$. Enfin, les éléments $s(1_C)$ et 1_A ont la même image 1_B par π, donc $\varphi(s(1_C)) = \varphi(1_A) = 1_B$. On en déduit que l'application ψ est un morphisme. Montrons que $\psi \circ \pi = \varphi$. Pour tout $a \in A$, on a $\pi \circ s \circ \varphi(a) = \varphi(a)$, donc $s \circ \varphi(a) - a \in \operatorname{Ker} \pi = I$, donc $\varphi(s \circ \varphi(a)) = \varphi(a)$.

Si φ est surjectif, alors ψ est surjectif car $\psi \circ \pi = \varphi$. Réciproquement, si ψ est surjectif, alors φ est surjectif car $\psi \circ \pi = \varphi$ et π est surjectif.

On remarque que $\operatorname{Ker} \psi = \pi(\operatorname{Ker} \varphi)$, donc le morphisme ψ est injectif si et seulement si $\pi(\operatorname{Ker} \varphi) = \{0\}$ si et seulement si $\operatorname{Ker} \varphi \subset \operatorname{Ker} \varphi$ si et seulement si $\operatorname{Ker} \varphi = 1$. La dernière équivalence est vraie puisque les hypothèses donnent $\operatorname{Ker} \varphi = I$ et $I \subset \operatorname{Ker} \varphi$. □

Comme corollaire immédiat du théorème précédent, on obtient divers « théorèmes d'isomorphisme ». Basiquement, un théorème d'isomorphisme identifie sous certaines hypothèses deux quotients construits « différemment ».

THÉORÈME 1.47 *(d'isomorphisme).* 1. Soit $\varphi\colon A \to B$ un morphisme d'anneaux.

(a) Le morphisme φ induit un isomorphisme de $A/\operatorname{Ker} \varphi$ dans $\operatorname{Im} \varphi$.

(b) On suppose que φ est surjectif. Soit J un idéal de B. Alors la composition du morphisme φ avec le morphisme quotient $B \to B/J$ induit un isomorphisme de $A/\varphi^{-1}(J)$ dans B/J.

(c) On suppose que φ est surjectif. Soit I un idéal de A. Alors la composition du morphisme φ avec le morphisme quotient $B \to B/\varphi(I)$ induit un isomorphisme de $A/(I + \operatorname{Ker} \varphi)$ dans $B/\varphi(I)$.

2. Soit I un idéal de A. On note $\pi_I\colon A[X] \to (A/I)[X]$ l'unique morphisme d'anneaux tel que $\pi_I(X) = X$. Ce dernier induit un morphisme $A \to (A/I)[X]$. Soit J un idéal de $A[X]$. Alors la composition du morphisme π_I avec le morphisme quotient $(A/I)[X] \to (A/I)[X]/\pi_I(J)$ induit un isomorphes

$$A[X]/(I \cdot A[X] + J) \longrightarrow (A/I)[X]/\pi_I(J).$$

◇ REMARQUE. La définition du morphisme π_I utilise la propriété universelle de l'anneau des polynômes à une indéterminée. Concrètement, il s'obtient en réduisant modulo I les coefficients d'un polynôme de $A[X]$. Cela montre sa surjectivité.

Preuve Le point 1a découle de la propriété universelle. Les points 1b et 1c se déduisent du point 1a en calculant les noyaux des compositions des morphismes considérées.

Montrons le point 2. Le morphisme π_I est surjective d'après la remarque précédente. Par le point 1c, il suffit de montrer que $\operatorname{Ker} \pi_I = I \cdot A[X]$. On vérifie que l'ensemble des polynômes $I[X]$ à coefficients dans I est un idéal de $A[X]$ contenant I et que tout idéal de $A[X]$ contenant I contient $I[X]$. Par conséquent, on a $I \cdot A[X] = I[X]$. Le fait que le noyau de π_I soit $I[X]$ découle alors de la remarque précédente. □

1.7 Théorème chinois

THÉORÈME 1.48. Soient $n, m \geqslant 1$ des entiers. On note $\pi_n\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ et $\pi_m\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ les morphismes quotients. On note $\pi_n \times \pi_m\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ le morphisme produit. Alors

$$\operatorname{Ker} \pi_n \times \pi_m = n\mathbb{Z} \cap m\mathbb{Z} = \operatorname{ppcm}(n, m)\mathbb{Z}.$$

Si n et m sont premiers entre eux, alors $\pi_n \times \pi_m$ est surjectif et il induit un isomorphisme d'anneaux de $\mathbb{Z}/nm\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Preuve Voir le cours de sup/spé. □

THÉORÈME 1.49. Soient A un anneau et $I_1, \ldots, I_n$ des idéaux de A. Pour $i \in [\![1, n]\!]$, on note $\pi_i\colon A \to A/I_i$ le morphisme quotient. On note $\prod_{i=1}^n \pi_i\colon A \to \prod_{i=1}^n A/I_i$ le morphisme produit. Alors

$$\operatorname{Ker}\Big(\prod_{i=1}^n \pi_i\Big) = \bigcap_{i=1}^n I_i.$$

On suppose que, pour tous $i, j \in [\![1, n]\!]$ tels que $i \neq j$, on a $I_i + I_j = A$. Alors

$$\bigcap_{i=1}^n I_i = \bigodot_{i=1}^n I_i$$

et le morphisme $\prod_{i=1}^n \pi_i$ est surjectif et induit un isomorphisme

$$A/\prod_{i=1}^n I_i \longrightarrow \prod_{i=1}^n A/I_i.$$

Preuve La démonstration se fait par récurrence sur n. □

◇ Remarque. L'hypothèse que les idéaux I_i soient deux à deux étrangers est importante, on ne peut pas se contenter d'avoir $\sum_{i=1}^{n} I_i = A$. Un contre exemple est le cas $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$.

1.8 Diviseurs de zéros, anneaux intègres, corps

Définition 1.50. Soit A un anneau. Un *diviseur de zéro* dans A est un élément $a \in A$ tel qu'il existe $b \in A \setminus \{0_A\}$ tel que $ab = 0_A$.

◇ Remarque. Cette terminologie peut être source de confusion. Par exemple, dans $\mathbb{Z}$, n'importe quel entier divise 0, mais seul 0 est un diviseur de zéro.

▷ Exemples. – Un élément de $A^\times$ n'est jamais un diviseur de zéro.
– Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, ... n'ont aucun diviseur de zéro non trivial.
– Soient p et q deux nombres premiers. Alors $[p]_{pq}$ et $[q]_{pq}$ sont des diviseurs de zéro non triviaux de $\mathbb{Z}/pq\mathbb{Z}$.
– L'anneau nul n'a pas de diviseur de zéro et c'est le seul anneau vérifiant cette propriété.

Définition 1.51. Un anneau est dit *intègre* s'il est non nul et ne possède pas de diviseurs de zéro non triviaux, *i. e.* non nuls.

◇ Remarque. On peut reformuler cette définition. Un anneau A est intègre si et seulement s'il est non nul et

$$\forall x, y \in A, \quad xy = 0_A \quad \Longrightarrow \quad (x = 0_A \text{ ou } y = 0_A). \tag{$*$}$$

Proposition 1.52. Un anneau est intègre si et seulement si l'idéal nul est premier.

Preuve L'anneau est non nul si et seulement si l'idéal nul est un idéal propre. Ainsi, vu la définition d'un idéal premier, cette proposition n'est qu'une reformulation de la remarque précédente. □

Proposition 1.53. Un sous-anneau d'un anneau intègre est intègre.

Preuve La relation $(*)$ est évidemment vraie sur tout sous-anneau. Il suffit donc de montrer qu'un sous-anneau d'un anneau non nul est non nul. Ceci vient du faire que l'anneau nul est caractérisé par l'égalité $0 = 1$ et qu'un sous-anneau possède les mêmes neutres que l'anneau. □

Définition 1.54 *(corps).* Un *corps* est un anneau A tel que $A^\times = A \setminus \{0_A\}$. Un sous-corps d'un corps est un sous-anneau de ce corps qui est également un corps. Un morphisme de corps entre deux corps est un morphisme d'anneaux entre ces deux corps.

▷ Exemples. Les anneaux $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{Z}/p\mathbb{Z}$ sont des corps, l'anneau $\mathbb{K}[X]/\langle P \rangle$ est un corps si $\mathbb{K}$ est un corps et le polynôme $P \in \mathbb{K}[X]$ est irréductible.

Proposition 1.55. Soit A un anneau. Alors les propositions suivantes sont équivalentes :
(i) l'anneau A est un corps ;
(ii) l'anneau A possède deux idéaux ;
(iii) l'anneau A est non nul et les ensembles A et $\{0_A\}$ sont les seuls idéaux de A ;
(iv) l'ensemble $\{0_A\}$ est un idéal maximal de A.

Théorème 1.56. Soient A un anneau et I un idéal de A. Alors l'idéal I est premier (resp. maximal) si et seulement si le quotient A/I est intègre (resp. un corps).

◇ Remarque. On retrouve en particulier qu'un anneau est intègre si et seulement si son idéal nul est premier et est un corps si et seulement si son idéal nul est maximal.

Théorème 1.57. – Soit $n \geqslant 1$ un entier. Alors $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
– Soient $\mathbb{K}$ un corps et $P \in \mathbb{K}[X] \setminus \{0\}$. Alors $\mathbb{K}[X]/P\mathbb{K}[X]$ est un corps si et seulement si P est irréductible.

Preuve Cela découle du théorème précédent. □

Corollaire 1.58. Le caractéristique d'un corps est zéro ou un nombre premier.

◇ Remarque. Un anneau dont la caractéristique est un nombre premier n'est pas nécessairement un corps : il suffit de considérer $\mathbb{Z}/p\mathbb{Z}[X]$.

1.9 Élément irréductibles d'un anneaux intègre

On va généraliser, dans le cadre des anneaux intègres, la notion de nombre premier d'une part et de polynôme irréductible d'autre part. Dans tout ce qui suit, l'ensemble A est un anneau intègre fixé.

Définition 1.59. On dit qu'un élément $a \in A$ divise un élément $b \in A$ s'il existe $c \in A$ tel que $b = ca$. On note alors $a \mid b$.

◇ Remarque. Un élément inversible $a \in A^\times$ divise n'importe quel élément de A.

Lemme 1.60. Soient $a, b \in A$. Alors $a \mid b \Leftrightarrow bA \subset aA$. De plus, les propositions suivantes ont équivalentes :
(i) on a $a \mid b$ et $b \mid a$;
(ii) on a $aA = bA$;
(iii) il existe $c \in A^\times$ tel que $b = ca$;
(iv) il existe $c \in A^\times$ tel que $a = cb$.

Définition 1.61. On dit que deux éléments a et b de A sont associés s'ils satisfont une des quatre propositions du lemme précédent.

◇ Remarque. Les propriétés des éléments d'un anneau intègre liées à la notion de divisibilités sont « invariants par association ».

Définition 1.62. On dit qu'un élément $a \in A$ est *irréductible* s'il est non inversible et, pour tout $b, c \in A$ tels que $a = bc$, on a $b \in A^\times$ ou $c \in A^\times$.

◇ Remarque. Un élément irréductible est nécessairement non nul. Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés. Cette notion d'irréductibilité coïncident bien avec celle sur $\mathbb{K}[X]$ pour un corps $\mathbb{K}$.

Définition 1.63. On dit que deux éléments $a, b \in A$ sont *premiers entre eux* si les seuls éléments de A qui divisent a et b sont les inversibles de A.

Proposition 1.64. Soient $a \in A$ un élément irréductible et $b \in A$. Alors a et b ne sont pas premier entre eux si et seulement si $a \mid b$.

Théorème 1.65. Soit $a \in A$ tel que l'idéal $a \cdot A$ soit premier et non nul. Alors a est irréductible.

Le réciproque est fausse : un élément irréductible n'engendre pas toujours un idéal premier, mais les contre-exemples ne sont pas immédiats. On peut montrer que, dans $\mathbb{Z}[i\sqrt{3}]$, l'élément 2 est irréductible mais n'engendre pas un idéal premier.

Notation. Pour un corps $\mathbb{K}$, on note $\mathrm{Irr}(\mathbb{K}[X])$ l'ensemble des polynômes unitaires irréductibles de $\mathbb{K}[X]$.

Théorème 1.66. Soient $\mathbb{K}$ un corps et $Q \in \mathbb{K}[X]$ un polynôme non nul. Alors il existe une unique famille presque nulle $(\nu_P(Q))_{P \in \mathrm{Irr}(\mathbb{K}[X])}$ d'entiers positifs et un unique élément $a \in \mathbb{K}^\times$ tel que

$$Q = \alpha \prod_{P \in \mathrm{Irr}(\mathbb{K}[X])} P^{\nu_P(Q)}.$$

On donnera plus tard une démonstration générale de ce théorème pour tous les anneaux dits principaux. En fait, en anticipant sur les notions introduites ultérieurement, on montrera que tout anneau principal est factoriel.

Définition 1.67. Soit $\mathbb{K}$ un corps. On dit qu'un polynôme $P \in \mathbb{K}[X]$ non nul est *sans facteur multiple* si, pour tout $Q \in \mathrm{Irr}(\mathbb{K}[X])$, on a $\nu_Q(P) \leqslant 1$.

◇ Remarque. Cette définition est équivalente à demander que, pour tout polynôme non constant $Q \in \mathbb{K}[X]$, le polynôme Q^2 ne divise pas P.

Proposition 1.68. Soit $P \in \mathbb{K}[X]$. Si $\mathrm{pgcd}(P, P') = 1$, alors P est sans facteur multiple.

La réciproque est fausse en général. Elle est vrai si la caractéristique de $\mathbb{K}$ est nulle ou, plus général, si $\mathbb{K}$ est un corps parfait.

Définition 1.69. Un corps $\mathbb{K}$ est dit *algébriquement close* si tout polynôme de $\mathbb{K}[X]$ non constant admet au moins une racine dans $\mathbb{K}$.

Proposition 1.70. Soient $\mathbb{K}$ un corps algébriquement clos et $P \in \mathbb{K}[X] \setminus \{0\}$ un polynôme sans facteur multiple. Alors P a exactement $\deg P$ racines dans $\mathbb{K}$.

1.10 Notion de structure d'algèbre sur un anneau

Définition 1.71. Une *algèbre* sur un anneau A est un couple (B, φ) où B est un anneau et $\varphi\colon A \to B$ est un morphisme d'anneaux.

Soit (B, φ) une A-algèbre, *i. e.* un algèbre sur A. Alors l'application

$$\left|\begin{array}{l} A \times B \longrightarrow B, \\ (a, b) \longmapsto a \cdot b \coloneqq \varphi(a)b \end{array}\right.$$

est un loi de composition externe naturelle, correspondant à une multiplication par un scalaire (un élément de l'anneau A). Elle vérifie les propriétés suivantes :
- pour tout $b \in B$, on a $0_A \cdot b = 0_B$ et $1_A \cdot b = b$;
- pour tous $a \in A$ et $b_1, b_2 \in A$, on a $a \cdot (b_1 + b_2) = a \cdot b_1 + a \cdot b_2$;
- pour tous $a_1, a_2 \in A$ et $b \in B$, on a $a_1 \cdot (a_2 \cdot b) = (a_1 a_2) \cdot b$;
- pour tous $a_1, a_2 \in A$ et $b_1, b_2 \in A$, on a $(a_1 \cdot b_1)(a_2 \cdot b_2) = (a_1 a_2) \cdot (b_1 b_2)$.

En particulier, si A est un corps, toute A-algèbre est naturellement munie d'une structure de A-espace vectoriel. Réciproquement, si un anneau B est muni du loi de composition externe $(a, b) \in A \times B \longmapsto a \cdot b \in B$ vérifiant les quatre points ci-dessus, on peut munir B d'une structure de A-algèbre par le morphisme $\varphi\colon a \in A \longmapsto a \cdot 1_B \in B$.

▷ Exemples. – Tout anneau est muni d'une structure de $\mathbb{Z}$-algèbre ;
– Si A est un sous-anneau de B, alors B est naturellement muni d'une structure de A-algèbre. En particulier, les anneaux $A[X]$ et $A[\![X]\!]$ sont naturellement munis de structures de A-algèbres.
– Si B est une A-algèbre, tout quotient de B par un idéal est naturellement muni d'une structure de A-algèbre.
– Un anneau de caractéristique $n \in \mathbb{N}$ possède une unique structure de $\mathbb{Z}/n\mathbb{Z}$-algèbre.

Définition 1.72 *(sous-algèbre).* Soit (B, φ_B) une A-algèbre. Une sous-A-algèbre de B est un sous-anneau B' de B tel que le morphisme d'anneaux $\iota\colon B' \to B$ se factorise par le morphisme φ_B, *i. e.* il existe un morphisme d'anneaux $\varphi_{B'}\colon A \to B'$ tel que $\varphi_B = \iota \circ \varphi_{B'}$.

Soit (B, φ_C) un A-algèbre. Un morphisme de A-algèbres de B vers C est un morphisme d'anneaux $\psi\colon B \to C$ tel que $\psi \circ \varphi_B = \varphi_C$.

La plupart des propriétés et notions relatives aux anneaux, sous-anneaux et morphismes d'anneaux, correctement adaptés, s'étendent facilement aux A-algèbres et à leur morphismes et sous-algèbres. Par exemple, la composée de deux morphismes de A-algèbres est un morphisme de A-algèbres. On définit de manière évidente la notion d'isomorphisme de A-algèbres et un morphisme de A-algèbres est un isomorphisme si et seulement si c'est une application bijective.

Théorème 1.73 *(propriété universelle de l'algèbre des polynômes).* Soient A un anneau et $\iota\colon A \to A[X]$ le morphisme d'anneaux injectif naturel (qui munit $A[X]$ d'une structure de A-algèbre). Alors l'application

$$\left|\begin{array}{l} \mathrm{Hom}_{A\text{-alg}}(A[X], B) \longrightarrow B, \\ \qquad\qquad\qquad \varphi \longmapsto \varphi(X) \end{array}\right.$$

est bijective.

Définition 1.74. – Soient B une A-algèbre et $b \in B$. L'unique élément de $\mathrm{Hom}_{A\text{-alg}}(A[X], B)$ qui envoie X sur b est appelé le *morphisme d'évaluation* en b. On le note ev_b. De plus, on note $A[b]$ l'image de $A[X]$ par ev_b.
– On appelle *racine* d'un polynôme $P \in B[X]$ tout élément $b \in B$ tel que $\mathrm{ev}_b(P) = P(b) = 0$.

Théorème 1.75. Soient A un anneau, (B, ι) une A-algèbre et I un idéal de B. On note $\pi\colon B \to B/I$ le morphisme quotient. Alors $(B/I, \pi \circ \iota)$ est une A-algèbre et, en particulier, l'application π est un morphisme de A-algèbres. Soient C une A-algèbre et $\varphi\colon B \to C$ un morphisme de A-algèbres. Alors l'unique morphisme d'anneaux $\psi\colon B/I \to C$ tel que $\psi \circ \pi = \varphi$ est un morphisme de A-algèbres.

En particulier, les théorèmes 1.45 à 1.47 restent vrais en remplaçant partout dans les énoncés « anneau » (y compris dans « morphisme d'anneaux ») par « algèbre » (sur un anneau de base fixé).

Chapitre 2

Étude de $\mathbb{Z}/n\mathbb{Z}$ et $K[X]/PK[X]$

2.1 Étude du quotient $\mathbb{Z}/n\mathbb{Z}$ 12
2.1.1 Éléments inversibles 12
2.1.2 Endomorphismes 12
2.1.3 Les carrés dans $\mathbb{Z}/p\mathbb{Z}$ 12
2.2 Étude du quotient $\mathbb{K}[X]/P\mathbb{K}[X]$ 13

Notation. Soit $n \in \mathbb{N}$. Il existe un morphisme d'anneaux surjectif $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ et de noyau $n\mathbb{Z}$. Pour $a \in \mathbb{Z}$, on note $[a]_n$ l'image de a par ce morphisme. On notera de même avec le quotient $\mathbb{K}[X]/P\mathbb{K}[X]$.

2.1 Étude du quotient $\mathbb{Z}/n\mathbb{Z}$

2.1.1 Éléments inversibles

Théorème 2.1. Soit $n \geqslant 1$. Alors l'application

$$\begin{vmatrix} \{m \in [\![0, n-1]\!] \mid \operatorname{pgcd}(n,m) = 1\} & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times, \\ m & \longmapsto & [m]_n \end{vmatrix}$$

est une bijection. Pour $m \in \mathbb{N}$, l'élément $[m]_n$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\operatorname{pgcd}(n,m) = 1$.

Preuve Montrons la deuxième assertion. Soit $m \in \mathbb{Z}$. Alors $[m]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement s'il existe $r \in \mathbb{Z}$ tel que $[r]_n[m]_n = [1]_n$, *i. e.* $[rm-1]_n = 0$, si et seulement s'il existe $r, s \in \mathbb{Z}$ tels que $mr - 1 = ns$ si et seulement si $\operatorname{pgcd}(n,m) = 1$ par le théorème de Bézout.

Montrons la première assertion. Il suffit de montrer que l'application $\varphi\colon m \in [\![0, n-1]\!] \longmapsto [m]_n \in \mathbb{Z}/n\mathbb{Z}$ est une bijection. Elle est clairement injective. Soit $y \in \mathbb{Z}/n\mathbb{Z}$. Il existe $m \in \mathbb{Z}$ tel que $y = [m]_n$. Soit $m = qn + r$ la division euclidienne de m par n. Alors $y = [m]_n = [r]_n$ et $r \in [\![0, m-1]\!]$, donc $y = \varphi(r)$. L'application φ est donc surjective. □

2.1.2 Endomorphismes

Théorème 2.2. Soient $n \geqslant 1$ et A un anneau de caractéristique c. Alors l'ensemble $\operatorname{Hom}_{\text{ann}}(\mathbb{Z}/n\mathbb{Z}, A)$ est non vide si et seulement si c divise n et, dans ce cas, c'est un singleton.

◇ Remarque. En particulier, on a $\operatorname{Hom}_{\text{ann}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \{\mathrm{Id}_{\mathbb{Z}/n\mathbb{Z}}\}$.

Preuve Soit $\varphi_A\colon \mathbb{Z} \to A$ l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A. Par définition, on a $\operatorname{Ker}\varphi_A = c\mathbb{Z}$. Par la propriété universelle de l'anneau quotient, l'ensemble $\operatorname{Hom}_{\text{ann}}(\mathbb{Z}/n\mathbb{Z}, A)$ est en bijection avec l'ensemble

$$\{\varphi \in \operatorname{Hom}_{\text{ann}}(\mathbb{Z}, A) \mid n\mathbb{Z} \subset \operatorname{Ker}\varphi\}.$$

Or $\operatorname{Hom}_{\text{ann}}(\mathbb{Z}, A) = \{\varphi_A\}$, donc l'ensemble $\operatorname{Hom}_{\text{ann}}(\mathbb{Z}/n\mathbb{Z}, A)$ est non vide si et seulement si $\operatorname{Ker}\varphi_A \supset n\mathbb{Z}$, *i. e.* $c \mid n$. Dans ce cas, il s'agit bien d'un singleton. □

2.1.3 Les carrés dans $\mathbb{Z}/p\mathbb{Z}$

Définition 2.3. Un élément $a \in A$ est un *carré* dans A s'il existe $b \in A$ tel que $b^2 = a$.

Théorème 2.4. Soit $p \geqslant 3$ un nombre premier. Alors

1. l'application $x \in (\mathbb{Z}/p\mathbb{Z})^\times \longmapsto x^2 \in (\mathbb{Z}/p\mathbb{Z})^\times$ est un morphisme de groupes de noyau $\{[1]_p, [-1]_p\}$;
2. un élément $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ est un carré dans $\mathbb{Z}/p\mathbb{Z}^\times$ si et seulement si $x^{(p-1)/2} = 1$;
3. il y a $(p+1)/2$ carré dans $\mathbb{Z}/p\mathbb{Z}$.

Plus généralement, le théorème suivant est vrai pour tout corps dont la caractéristique est différente de 2.

Théorème 2.5. Soit $\mathbb{K}$ un corps de caractéristique différente de 2. Alors

1. on a $1_\mathbb{K} \neq -1_\mathbb{K}$;
2. l'application $x \in \mathbb{K}^\times \longmapsto x^2 \in \mathbb{K}^\times$ est un morphisme de groupes de noyau $\{1_\mathbb{K}, -1_\mathbb{K}\}$.
3. si $\mathbb{K}$ est fini de cardinal impair q, alors il y a exactement $(q+1)/2$ carrés dans $\mathbb{K}$ et un élément $x \in \mathbb{K}^\times$ est un carré dans $\mathbb{K}$ si et seulement si $x^{(q-1)/2} = 1_\mathbb{K}$.

Preuve 1. Si $1_\mathbb{K} = -1_\mathbb{K}$, alors le corps $\mathbb{K}$ est de caractéristique au plus 2 et, comme $\mathbb{K}$ est un corps, ce n'est pas l'anneau nul, donc sa caractéristique vaut 2.

2. On vérifie facilement qu'il s'agit d'un morphisme $\varphi\colon \mathbb{K}^\times \to \mathbb{K}^\times$ dont le noyau vaut $\{\pm 1_\mathbb{K}\}$.

3. Comme $\mathbb{K}^\times$ est un groupe fini de cardinal q, l'image $\varphi(\mathbb{K}^\times)$ est isomorphe à $\mathbb{K}^\times/\operatorname{Ker}\varphi$ et son cardinal vaut donc $(q-1)/2$. Or $\varphi(\mathbb{K}^\times)$ est l'ensemble des éléments non nuls de $\mathbb{K}$ qui sont des carrés. Par ailleurs, le neutre $0_\mathbb{K}$ est un carré. Au final, il y a $(q-1)/2+1 = (q+1)/2$ carrés dans $\mathbb{K}$.

Soit $x \in \mathbb{K}^\times$. On suppose que x est un carré dans $\mathbb{K}$. Il existe $y \in \mathbb{K}^\times$ tel que $y^2 = x$. Alors $x^{(q-1)/2} = y^{q-1} = 0_\mathbb{K}$. Soit $P \coloneqq X^{(q-1)/2} - 1_\mathbb{K} \in \mathbb{K}[X]$. Alors $\varphi(\mathbb{K}^\times) \subset R \coloneqq \{x \in \mathbb{K} \mid P(x) = 0\}$. Comme $\mathbb{K}$ est un corps, on a $\sharp R \leqslant (q-1)/2$. Or $\sharp\varphi(\mathbb{K}^\times) = (q-1)/2$, donc $\varphi(\mathbb{K}^\times) = R$. □

2.2 Étude du quotient $\mathbb{K}[X]/P\mathbb{K}[X]$

Soit $\mathbb{K}$ un corps. On note $\iota\colon \mathbb{K} \to \mathbb{K}[X]$ le morphisme d'inclusion naturelle de $\mathbb{K}$ dans $\mathbb{K}[X]$. Ce morphisme munit l'anneau $\mathbb{K}[X]$ d'une structure de $\mathbb{K}$-algèbre. De même, soient $P \in \mathbb{K}[X]$ et $\pi_P\colon \mathbb{K}[X] \to \mathbb{K}[X]/P\mathbb{K}[X]$ la projection. Alors le morphisme $\pi_P \circ \iota$ munit l'anneau $\mathbb{K}[X]/P\mathbb{K}[X]$ d'une structure de $\mathbb{K}$-algèbre.

Théorème 2.6. Soit $P \in \mathbb{K}[X]$ non constant. On pose $x \coloneqq [X]_p$. Alors le $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]/P\mathbb{K}[X]$ est de dimension $\deg P$ et la famille $(1, x, \dots, x^{\deg P - 1})$ en est une base.

Théorème 2.7. Soient $P, Q \in \mathbb{K}[X]$. Alors $[Q]_P \in (\mathbb{K}[X]/P\mathbb{K}[X])^\times$ si et seulement si $\operatorname{pgcd}(P,Q) = 1$.

Rappel. Soient $\mathbb{K}$ un corps, A une $\mathbb{K}$-algèbre et $a \in A$. On note $\operatorname{ev}_a\colon \mathbb{K}[X] \longrightarrow A$ l'unique morphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[X]$ vers A qui envoie X sur a.

Théorème 2.8. L'application

$$\begin{vmatrix} A \longrightarrow \operatorname{Hom}_{\mathbb{K}\text{-alg}}(\mathbb{K}[X], A), \\ a \longmapsto \operatorname{ev}_a \end{vmatrix}$$

est une bijection. Pour tout $P \in \mathbb{K}[X]$, cette application induit une bijection

$$\{a \in A \mid P(a) = 0\} \longrightarrow \operatorname{Hom}_{\mathbb{K}\text{-alg}}(\mathbb{K}[X]/P\mathbb{K}[X], A).$$

Preuve La première assertion n'est qu'une reformulation de la propriété universelle de la $\mathbb{K}$-algèbre $\mathbb{K}[X]$. Soit $P \in \mathbb{K}[X]$. Alors la propriété uniforme dit que l'ensemble $\operatorname{Hom}_{\mathbb{K}\text{-alg}}(\mathbb{K}[X]/\langle P\rangle, A)$ est en bijection naturelle avec l'ensemble $\{\varphi \in \operatorname{Hom}_{\mathbb{K}\text{-alg}}(\mathbb{K}[X], A) \mid \operatorname{Ker}\varphi \supset \langle P\rangle\}$. Soit $\varphi \in \operatorname{Hom}_{\mathbb{K}\text{-alg}}(\mathbb{K}[X], A)$. Dire que $\operatorname{Ker}\varphi \supset \langle P\rangle$ est équivalent à dire que $\operatorname{Ker}\varphi \ni P$. Soit $a \in A$ tel que $\varphi = \operatorname{ev}_a$. Alors $\operatorname{Ker}\varphi \ni P$ si et seulement si $\operatorname{ev}_A(P) = 0$. □

Définition 2.9. Un élément $a \in A$ est dit *algébrique* sur $\mathbb{K}$ si $\operatorname{Ker}\operatorname{ev}_a \neq \{0\}$. Dans le cas contraire, on dit qu'il est *transcendant*. Pour un élément algébrique $a \in A$, l'unique polynôme unitaire engendrant l'idéal $\operatorname{Ker}\operatorname{ev}_a \subset \mathbb{K}[X]$ est appelé le *polynôme minimal* de a sur $\mathbb{K}$.

▷ Exemple. Le réel $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ et son polynôme minimal est $X^2 - 2$. Il est algébrique sur $\mathbb{R}$ et son polynôme minimal est $X - \sqrt{2}$. Si $\mathbb{K}$ est un corps, le monôme $X \in \mathbb{K}[X]$ est transcendant sur $\mathbb{K}$.

Proposition 2.10. Soit A une $\mathbb{K}$-algèbre qui est un $\mathbb{K}$-espace vectoriel de dimension finie. Alors tout élément de A est algébrique sur $\mathbb{K}$.

▷ Exemple. Par exemple, on peut prendre $A = \mathbb{K}[X]/\langle P\rangle$ avec $P \in \mathbb{K}[X] \setminus \{0\}$.

Proposition 2.11. Soit $P \in \mathbb{K}[X] \setminus \{0\}$ un polynôme irréductible. Alors l'image de X par le morphisme quotient $\mathbb{K}[X] \to \mathbb{K}[X]/\langle P\rangle$ est algébrique sur $\mathbb{K}$ et son polynôme minimal est P.

Proposition 2.12. Soient A une $\mathbb{K}$-algèbre intègre et $a \in A$ algébrique sur $\mathbb{K}$. Alors le polynôme minimal de a sur $\mathbb{K}$ est irréductible.

Définition 2.13. Soit $\mathbb{K}$ un corps. Une $\mathbb{K}$-*extension* est une $\mathbb{K}$-algèbre $\mathbb{L}$ qui soit un corps. Le degré d'une telle extension, noté $[\mathbb{L} : \mathbb{K}]$, est la dimension de $\mathbb{L}$ comme $\mathbb{K}$-espace vectoriel.

▷ Exemples. La $\mathbb{R}$-algèbre $\mathbb{C}$ est une extension de $\mathbb{R}$ de degré 2. La $\mathbb{Q}$-algèbre $\mathbb{C}$ est une extension de $\mathbb{Q}$ de degré infini. Si $\mathbb{K}$ est un corps et $P \in \mathbb{K}[X]$ est un polynôme irréductible, alors la $\mathbb{K}$-algèbre $\mathbb{K}[X]/\langle P\rangle$ est une extension de $\mathbb{K}$ de degré $\deg P$.

Chapitre 3

Corps finis et applications

3.1 Introduction et premières propriétés 14
3.2 Caractéristique et cardinal d'un corps fini 14
3.3 Un exemple de calcul explicite dans un corps fini . . . 14
3.4 Le morphisme de Frobenius 14
3.5 Le groupe des inversible d'un corps fini est cyclique . 14
3.6 Deux corps finis de même cardinal sont isomorphes . 15
3.7 Toute puissance d'un nombre premier est le cardinal d'un corps fini 16

3.1 Introduction et premières propriétés

Proposition 3.1. Soient $\mathbb{K}$ un corps fini, $n \geqslant 1$ un entier et $P \in \mathbb{K}[X]$ un polynôme irréductible de degré n. Alors $\mathbb{L} \coloneqq \mathbb{K}[X]/\langle P \rangle$ est un corps fini de cardinal $\sharp\,\mathbb{K}^n$.

Preuve Comme P est irréductible, la $\mathbb{K}$-algèbre $\mathbb{L}$ est un corps. Sa dimension en tant que $\mathbb{K}$-espace vectoriel vaut n. En particulier, elle est isomorphe comme $\mathbb{K}$-espace vectoriel à $\mathbb{K}^n$ ce qui montre la proposition. □

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

3.2 Caractéristique et cardinal d'un corps fini

Théorème 3.3. Soit $\mathbb{K}$ un corps fini. Alors sa caractéristique est un nombre premier p. En particulier, il existe une unique structure de $\mathbb{Z}/p\mathbb{Z}$-algèbre sur $\mathbb{K}$ qui fait de $\mathbb{K}$ un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie $n \in \mathbb{N}$. Alors $\sharp\,\mathbb{K} = p^n$.

Preuve Soit $\varphi_{\mathbb{K}} \colon \mathbb{Z} \to \mathbb{K}$ l'unique morphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{K}$. Si $\operatorname{Ker}\varphi_{\mathbb{K}} = \{0\}$, alors $\mathbb{K}$ contient un sous-anneau isomorphe à $\mathbb{Z}$ ce qui est impossible. Donc il existe $c \in \mathbb{N}^*$ tel que $\operatorname{Ker}\varphi_k = c\mathbb{Z}$. Le théorème d'isomorphisme assure que $\mathbb{K}$ contient un sous-anneau isomorphe à $\mathbb{Z}/c\mathbb{Z}$. Or $\mathbb{K}$ est un corps, donc il est intègre, donc $\mathbb{Z}/c\mathbb{Z}$ est intègre, *i. e.* l'entier c est premier.

On sait alors que l'ensemble $\operatorname{Hom}_{\text{ann}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{K})$ est réduit à un élément. Or $\mathbb{K}$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel fini, donc c'est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie. □

Notation. Pour un nombre premier p, on a $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

3.3 Un exemple de calcul explicite dans un corps fini

Prenons $p \coloneqq 2$. Le polynôme $X^2 + X + [1]_2$ est irréductible dans $\mathbb{F}_2[X]$. En effet, on a $P([0]_2) \neq 0$ et $P([1]_2) \neq 0$, donc il n'a pas de racines dans $\mathbb{F}_2$. Or il est de degré 2, donc il est irréductible dans $\mathbb{F}_2[X]$. Alors le quotient $\mathbb{K} \coloneqq \mathbb{F}_2[X]/\langle P \rangle$ est un corps fini de cardinal $2^2 = 4$.

Notons $x \in \mathbb{F}_2[X]/\langle P \rangle$ l'image de X par le morphisme quotient $\pi \colon \mathbb{F}_2[X] \to \mathbb{F}_2[X]/\langle P \rangle$. Alors $P(x) = 0_{\mathbb{K}}$. On sait que la famille $([1]_2, x)$ est un base du $\mathbb{F}_2$-espace vectoriel $\mathbb{K}$.

3.4 Le morphisme de Frobenius

Théorème 3.4. Soient p un nombre premier et A un anneau de caractéristique p. Alors l'application

$$F_A \colon \left| \begin{array}{l} A \longrightarrow A, \\ x \longmapsto x^p \end{array} \right.$$

est un morphisme d'anneaux, appelé le *morphisme de Frobenius* de A. Si $\mathbb{K}$ est un corps fini, alors ce morphisme $F_{\mathbb{K}}$ est un automorphisme de corps.

3.5 Le groupe des inversible d'un corps fini est cyclique

Soit G un groupe. Pour $d \geqslant 1$, on pose

- $\varphi(d) \coloneqq \sharp(\mathbb{Z}/d\mathbb{Z})^\times$ le cardinal de l'ensemble des éléments inversibles de $\mathbb{Z}/d\mathbb{Z}$,
- $\Delta_d(G) \coloneqq \{x \in G \mid x^d = e\}$ l'ensemble des racines du polynôme $X^d - e$,

– $\Omega_d(G) \coloneqq \{x \in G \mid \mathrm{o}(x) = d\}$ l'ensemble des éléments d'ordre d de G,
– $\omega_d(G) \coloneqq \sharp\,\Omega_d(G)$ le nombre d'éléments d'ordre d de G.

D'après le théorème de Lagrange, si G est un groupe fini d'ordre $n \geqslant 1$ et $d \geqslant 1$ est un entier tel que $d \nmid n$, alors $\omega_d(G) = 0$. La classe $\{\Omega_d(G) \mid d \mid n\}$ est alors une partition de G ce qui conduit à la relation

$$\sum_{d|n} \omega_d(G) = n. \tag{$*$}$$

Par ailleurs, rappelons que, si G est un groupe cyclique d'ordre n et $d \geqslant 1$ un diviseur de n, alors $\sharp\,\Delta_d(G) = d$ et $\omega_d(G) = \varphi(d)$. Comme il existe des groupes cycliques d'ordre n, par exemple $G = \mathbb{Z}/n\mathbb{Z}$, la relation $(*)$ donne

$$\sum_{d|n} \varphi(d) = n. \tag{$**$}$$

Proposition 3.5. Soient $n \geqslant 1$ un entier et G un groupe fini d'ordre n. Alors les propositions suivantes sont équivalentes :

(i) le groupe G est cyclique ;
(ii) pour tout diviseur $d \geqslant 1$ de n, on a $\sharp\,\Delta_d(G) \leqslant d$;
(iii) pour tout diviseur $d \geqslant 1$ de n, on a $\omega_d(G) \leqslant \varphi(d)$.

Preuve L'implication (i) ⇒ (ii) vient de ce qui précède.

• *(iii) ⇒ (i).* On suppose (iii). Alors

$$\sum_{d|n} \omega_d(G) \leqslant \sum_{d|n} \varphi(d).$$

D'après les relations précédentes $(*)$ et $(**)$, cette dernière inégalité est une égalité. Alors pour tout $d \mid n$, on a $\omega_d(G) = \varphi(d)$. En particulier, on a $\omega_n(G) > 0$, *i. e.* le groupe G a un élément d'ordre n, donc il est cyclique.

• *(ii) ⇒ (iii).* On suppose (ii). Soit $d \geqslant 1$ un diviseur de n. Si $\omega_d(G) = 0$, c'est évident. On suppose que $\omega_d(G) > 0$. Soit $x \in G$ un élément d'ordre d. Alors le groupe $\langle x \rangle$ est cyclique d'ordre d. En particulier, tout élément de $\langle x \rangle$ possède un ordre qui divise d, donc $\langle x \rangle \subset \Delta_d(G)$. Comme $\sharp\,\Delta_d(G) \leqslant d$, on en déduit que $\langle x \rangle = \Delta_d(G)$. D'où $\Omega_d(G) = \Omega_d(\langle x \rangle)$, donc $\omega_d(G) = \omega_d(\langle x \rangle) = \varphi(d)$. □

Théorème 3.6. Soit $\mathbb{K}$ un corps fini. Alors le groupe $\mathbb{K}^\times$ est cyclique.

Preuve Appliquons la proposition précédente au groupe $\mathbb{K}^\times$. Soit $d \geqslant 1$ un diviseur de $|G|$. L'ensemble $\Delta_d(\mathbb{K}^\times)$ est l'ensemble des racines dans $\mathbb{K}$ du polynôme $X^d - 1_\mathbb{K}$. Comme $\mathbb{K}$ est un corps, on en déduit que $\sharp\,\Delta_d(\mathbb{K}^\times) \leqslant d$. Ainsi le groupe $\mathbb{K}^\times$ est cyclique. □

Théorème 3.7. Soit $\mathbb{K}$ un corps fini. On note $p \in \mathbb{N}$ la caractéristique de $\mathbb{K}$. Alors il existe un polynôme irréductible $P \in \mathbb{F}_p[X]$ tel que $\mathbb{K} \simeq \mathbb{F}_p[X]/\langle P \rangle$.

Preuve Le corps $\mathbb{K}$ est naturellement muni d'une structure de $\mathbb{F}_p$-algèbre. Soit $x \in \mathbb{K}^\times$ un générateur du groupe cyclique $\mathbb{K}^\times$. On note $\varphi\colon \mathbb{F}_p[X] \to \mathbb{K}$ l'unique morphisme de $\mathbb{F}_p$-algèbres envoyant X sur x. Comme $\mathbb{K} = \{0\} \cup \{x^n \mid n \in \mathbb{N}\}$, le morphisme φ est surjectif. Soit $P \in \mathbb{F}_p[X]$ un générateur de $\operatorname{Ker}\varphi$. Le théorème de factorisation induit un isomorphisme $\mathbb{F}_p[X]/\langle P \rangle \simeq \mathbb{K}$. Comme $\mathbb{K}$ est un corps, le polynôme P est nécessairement irréductible. □

3.6 Deux corps finis de même cardinal sont isomorphes

Lemme 3.8. Soient $\mathbb{K}$ un corps fini de cardinal $N \geqslant 1$ et $x \in \mathbb{K}$. Alors $x^N = x$.

Preuve Le cas $x = 0_\mathbb{K}$ est évident. Sinon l'élément x appartient au groupe $\mathbb{K}^\times$ qui est de cardinal $N - 1$. Il vient alors que $x^{N-1} = 1_\mathbb{K}$, donc $x^N = x$. □

Lemme 3.9. Soient p un nombre premier et $P \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n. Alors $P \mid X^{p^n} - X$.

Preuve On note $\mathbb{K} \coloneqq \mathbb{F}_p[X]/\langle P \rangle$ et $x \in \mathbb{K}$ l'image de X par la projection canonique $\mathbb{F}_p[X] \to \mathbb{K}$. Alors le polynôme minimal de x sur $\mathbb{F}_p$ est P. Or $\sharp\,\mathbb{K} = p^n$. Par le lemme précédent, on a $x^{p^n} = x$, *i. e.* l'élément x est une racine du polynôme $X^{p^n} - X$. On en déduit le résultat. □

THÉORÈME 3.10. Soient p un nombre premier, $n \geqslant 1$ un entier et $\mathbb{K}$ et $\mathbb{L}$ deux corps finis de cardinal p^n. Alors les corps $\mathbb{K}$ et $\mathbb{L}$ sont isomorphes.

Preuve Il existe un polynôme irréductible $P \in \mathbb{F}_p[X]$ tel que $\mathbb{K} \simeq \mathbb{F}_p[X]/\langle P\rangle$. Montrons que $\mathbb{L} \simeq \mathbb{F}_p[X]/\langle P\rangle$. Notons que tout élément de $\mathrm{Hom}_{\mathbb{F}_p\text{-alg}}(\mathbb{F}_p[X]/\langle P\rangle, \mathbb{L})$ est un isomorphisme. En effet, un élément de cet ensemble est injectif[§1] et, pour des raisons de cardinalité, il est bijectif. Par ailleurs, cet ensemble est en bijection avec l'ensemble des racines de P dans $\mathbb{L}$. Il suffit donc de montrer que ce dernier est non vide. Par le lemme précédent, il existe $R \in \mathbb{F}_p[X]$ tel que $X^{p^n} - X = PR$. En particulier, on a $\deg R < p^n$. Comme $\sharp\,\mathbb{L} = p^n$, il existe $y \in \mathbb{L}$ tel que $R(y) \neq 0$. Comme $y^{p^n} - y = 0$ et $\mathbb{L}$ est intègre, on en déduit que $P(y) = 0$. Ceci conclut la preuve. □

3.7 Toute puissance d'un nombre premier est le cardinal d'un corps fini

THÉORÈME 3.11. Soient p un nombre premier et $n \geqslant 1$ un entier. À isomorphisme près, il existe un unique corps fini de cardinal p^n.

Pour démontrer ce théorème, on va admette le théorème suivant.

THÉORÈME 3.12. Soit p un nombre premier. Alors il existe un corps algébriquement clos contenant $\mathbb{F}_p$.

Preuve On considère un corps algébriquement clos $\mathbb{L}$ contenant $\mathbb{F}_p$. On note $\mathbb{K} \subset \mathbb{L}$ l'ensemble des racines du polynôme $P \coloneqq X^{p^n} - X$. Comme $\mathbb{L}$ est de caractéristique p, on a $P' = p^n X^{p^n-1} - 1 = 0 - 1 = -1$. En particulier, les polynômes P et P' sont premiers entre eux, donc le polynôme P n'a pas de facteurs multiples. Comme $\mathbb{L}$ est algébriquement clos, il se décompose dans $\mathbb{L}[X]$ en produit de facteurs unitaires de degré un deux à deux distincts. On en déduit que $\sharp\,\mathbb{K} = p^n$. □

THÉORÈME 3.13. Soient p un nombre premier, $n \geqslant 1$ un entier et $\mathbb{K}$ un corps fini de cardinal p^n. Soit $d \geqslant 1$ un diviseur de n et

$$\mathbb{L} \coloneqq \{x \in \mathbb{K} \mid x^{p^d} = x\}.$$

Alors $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ de cardinal p^d. C'est l'unique sous-corps de $\mathbb{K}$ de cardinal p^d

Preuve En utilisant le morphisme de FROBENIUS, l'ensemble $\mathbb{L}$ est un sous-corps de $\mathbb{K}$. Le groupe $\mathbb{L}^\times$ est le sous-groupe du groupe cyclique $\mathbb{K}^\times$ des éléments dont l'ordre divise $p^d - 1$. En particulier, il est d'ordre $p^d - 1$, donc le corps $\mathbb{L}$ est de cardinal p^d. Comme deux corps de cardinal p^n sont isomorphes, on en déduit que le sous-corps $\mathbb{L}$ est unique. □

Le théorème 3.11 montre que, pour tout entier $n \geqslant 1$, il existe une extension de $\mathbb{F}_p$ dont le cardinal vaut q^n. Le théorème suivant généralise ce résultat.

THÉORÈME 3.14. Soient p un nombre premier, $n, N \geqslant 1$ deux entiers et $\mathbb{K}$ un corps de cardinal p^n. Alors il existe un sous-corps de $\mathbb{K}$ de cardinal N si et seulement s'il existe un diviseur $d \geqslant 1$ de n tel que $N = p^d$.

En particulier, si $\mathbb{K}$ est un corps fini de cardinal q, alors il existe une extension de $\mathbb{K}$ de cardinal N si et seulement si N est une puissance de q.

Preuve Le sens réciproque est évident. Réciproquement, soit $\mathbb{L}$ un sous-corps de $\mathbb{K}$. D'après le théorème précédent, il suffit de montrer qu'il existe $d \mid n$ tel que $\sharp\,\mathbb{L} = p^d$. Comme $\mathbb{K}$ est un $\mathbb{L}$-espace vectoriel de dimension finie r, on a $p^n = \sharp\,\mathbb{K} = \sharp\,\mathbb{L}^r$. Ceci assure qu'il existe un entier $d \geqslant 1$ tel que $\sharp\,\mathbb{L} = p^d$ avec $dr = n$. □

§1. Soit $\varphi \in \mathrm{Hom}_{\mathbb{F}_p\text{-alg}}(\mathbb{F}_p[X]/\langle P\rangle, \mathbb{L})$. Soit $x \in \mathrm{Ker}\,\varphi$. Raisonnons par l'absurde et supposons que $x \neq 0$. Comme $\mathbb{K}$ est un corps, on a $x \in \mathbb{K}^\times$. Il vient alors que $1 = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) = 0$ ce qui est impossible. D'où $\mathrm{Ker}\,\varphi = \{0\}$ ce qui montre l'injectivité.

Chapitre 4
Localisation, corps des fractions

4.1 Un exemple 17
4.2 Définition et propriétés élémentaires du localisé 17
4.3 Le corps des fractions d'un anneau intègre 19

La localisation est un procédé algébrique très général qui consiste en deux mots à « forcer » certains éléments d'un anneau à devenir inversibles, de façon notamment à obtenir un « calcul des fractions généralisé » aux propriétés similaires à celles du calcul des fractions classique que l'on connaît depuis notre plus tendre enfance. Le cas particulier le plus connu de ce procédé est la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$, qui se généralise en la notion de corps des fractions d'un anneau intègre : dans ce cas, on force en un sens tous les éléments non nuls à devenir inversibles. Mais la localisation est un procédé bien plus général que la construction du corps des fractions d'un anneau intègre et cette généralité, loin d'être gratuite, rend des services considérables notamment en algèbre commutative et en géométrie algébrique.

4.1 Un exemple

Commençons par un exemple destiné à éclaircir la dénomination même du procédé de localisation, laquelle est d'inspiration géométrique, voire topologique.

Soit $x_0 \in \mathbb{R}$ et mettons que l'on souhaite étudier uniquement des propriétés de nature locale des fonctions continues au voisinage de x_0, par exemple décider si une telle fonction est dérivable en x_0. L'ensemble des fonctions continues au voisinage de x_0 est-il un objet d'étude naturel pour ce type de propriétés ? Pas vraiment et au moins pour deux raisons. Tout d'abord, cet ensemble n'a pas de structure algébrique naturelle (on ne peut pas *a priori* ajouter ou multiplier deux fonctions continues au voisinage de x_0 car elles ne sont pas nécessairement définies sur le même ensemble) ce qui ne le rend pas très pratique à manipuler. Ensuite, les objets de cet ensemble restent en un sens de nature trop globale. Ainsi si I est un intervalle ouvert de $\mathbb{R}$ contenant x_0 (aussi « petit » soit-il) et $f\colon I \to \mathbb{R}$ est une fonction continue, alors f contient encore une énorme quantité d'informations dont on n'a que faire si on s'intéresse uniquement aux propriétés de nature locale en x_0. Plus précisément, ce que fait f sur le complémentaire de n'importe quel intervalle ouvert K, aussi « petit » soit-il, contenant x_0 et contenu dans I, ne nous intéresse absolument pas.

On peut cependant retrouver à la fois une structure algébrique et une localité « authentique » *via* la construction suivante : on considère l'ensemble des couples (I, f) où I est un intervalle ouvert de $\mathbb{R}$ contenant x_0 et $f\colon I \to \mathbb{R}$ est une fonction continue. On le munit d'une relation d'équivalence $\sim$ en décrétant que $(I, f) \sim (J, g)$ si et seulement s'il existe un intervalle ouvert $K \subset I \cap J$ contenant x_0 tel que $f|_K = g|_K$. On vérifie que c'est bien une relation d'équivalence. On note $\overline{(I, f)}$ la classe d'un couple (I, f) dans l'ensemble quotient. Sur l'ensemble quotient, on définit une addition et une multiplication ainsi : pour tous couples (I, f) et (J, g), on pose

$$\overline{(I, f)} + \overline{(J, g)} \coloneqq \overline{(I \cap J, f|_{I\cap J} + g|_{I\cap J})} \quad \text{et} \quad \overline{(I, f)} \times \overline{(J, g)} \coloneqq \overline{(I \cap J, f|_{I\cap J} \times g|_{I\cap J})}.$$

Cela munit le quotient d'une structure d'anneau et même de $\mathbb{R}$-algèbre. On le note $\mathscr{C}(x_0, \mathbb{R})$ et on l'appelle l'anneau des germes de fonctions continues en x_0.

Pour tout intervalle I de $\mathbb{R}$ contenant x_0, l'application

$$\varphi_I\colon \left|\begin{array}{c} \mathscr{C}(I, \mathbb{R}) \longrightarrow \mathscr{C}(x_0, \mathbb{R}), \\ f \longmapsto \overline{(I, f)} \end{array}\right.$$

est un morphisme d'anneaux. Par ailleurs, tout élément $f \in \mathscr{C}(I, \mathbb{R})$ tel que $f(x_0) \neq 0$ s'envoie sur un élément inversible par φ_I. En effet, si $f(x_0) \neq 0$, alors il existe un intervalle ouvert $J \subset I$ contenant x_0 tel que $g \coloneqq f|_J$ ne s'annule pas, donc l'élément $\overline{(I, f)} = \overline{(J, g)}$ est inversible d'inverse $\overline{(J, 1/g)}$.

Ceci montre que, dans cet anneau « local » des germes $\mathscr{C}(x_0, \mathbb{R})$, certains éléments d'anneaux plus « globaux » vont devenir inversibles. En fait, en un sens qui sera rendu précis dans ce qui suit, construire $\mathscr{C}(x_0, \mathbb{R})$, ce qui du point de vue topologique revient à « localiser » les fonctions continues au voisinage de x_0, revient exactement, du point de vue algébrique, à « forcer » toutes les fonctions de $\mathscr{C}(I, \mathbb{R})$ qui ne s'annulent pas en x_0 à devenir inversibles. Ceci est à l'origine du nom de localisation attribué au procédé purement algébrique décrit plus en détails ci-dessous et consistant à « forcer » certains éléments d'un anneau à devenir inversibles.

4.2 Définition et propriétés élémentaires du localisé

DÉFINITION 4.1. Soit A un anneau. Une partie S de A est dite *multiplicative* si $1_A \in S$ et, pour tous $s, s' \in S$, on a $ss' \in S$.

▷ EXEMPLES. – Pour tout $a \in A$, la partie $\{a^n \mid n \in \mathbb{N}\}$ est multiplicative.
– Pour tout idéal premier de A, son complémentaire $A \setminus$ est multiplicatif. En particulier, si A est intègre, alors la partie $A \setminus \{0_A\}$ est multiplicative.
– L'ensemble des éléments de A qui ne sont pas des diviseurs de zéro est multiplicatif.
– L'image d'une partie multiplicative par un morphisme d'anneaux est multiplicative.

◇ REMARQUE. Pour tout partie multiplicative S, l'ensemble $I_S := \{a \in A \mid \exists s \in S, as = 0\}$ est un idéal de A.

Localiser A par rapport à une partie multiplicative S, c'est construire un nouvel anneau où tous les éléments de A deviennent inversibles de sorte que cet anneau soit « le plus petit possible » en un sens pour cette propriété. Dans de nombreux cas d'applications, ce nouvel anneau contiendra A comme sous-anneau, mais ça n'est pas non plus systématique et, de manière générale, cela vaudra si et seulement si l'idéal I_S ci-dessus est nul.

Noter aussi qu'on ne demande pas *a priori* qu'une partie multiplicative S de A ne contienne pas 0_A. Cependant, dans ce cas, le localisé sera l'anneau nul (ce qui se comprend bien intuitivement : l'anneau nul est le seul anneau A où 0_A est inversible).

THÉORÈME 4.2. Soient A un anneau et S une partie multiplicative. Alors

1. il existe un anneau B et un morphisme d'anneaux $\varphi\colon A \to B$ tels que
– $\varphi(S) \subset B^\times$,
– pour tout anneau C et tout morphisme d'anneaux $\psi\colon A \to C$ tel que $\psi(S) \subset C^\times$, il existe un unique morphisme d'anneaux $\theta\colon B \to C$ tel que $\psi = \theta \circ \varphi$;

2. un tel couple (B, φ) est unique à isomorphisme près, *i. e.* pour tout couple (B', φ') vérifiant les deux points précédents, il existe un unique isomorphisme d'anneaux $\gamma\colon B \to B'$ tel que $\gamma \circ \varphi = \varphi'$.

◇ REMARQUE. Soit (B, φ) un tel couple. Alors $I_S \subset \operatorname{Ker}\varphi$. En effet, si $a \in A$ et $s \in S$ vérifient $\varphi(a)\varphi(s) = 0_A$, donc $\varphi(a) = \varphi(s)^{-1}0_A = 0$, donc $a \in \operatorname{Ker}\varphi$. Plus généralement, cela montre que, si C est un anneau et $\psi\colon A \to C$ est un morphisme d'anneaux tel que $\psi(S) \subset C^\times$, alors $I_S \subset \operatorname{Ker}\psi$.

On note $\tilde{A} := A/I_S$ et $\pi\colon A \to \tilde{A}$ le morphisme quotient. La propriété universelle de l'anneau quotient assure que, pour montrer l'existence d'un tel couple (B, φ), il suffit de le faire pour le quotient $\tilde{A}$ en prenant pour partie multiplicative $\pi(S)$. Alors $(B, \varphi \circ \varphi)$ sera un couple convenable pour A.

DÉFINITION 4.3. Soit (B, φ) un couple vérifiant le théorème précédent. On dira que l'anneau B est le *localisé de A par rapport à S*, noté $S^{-1}A$, et que le morphisme φ est le *morphisme de localisation*.

Les articles définis sont justifiés par le résultat d'unicité à isomorphisme unique près. Il est à noter qu'on aurait pu énoncer le théorème sous une forme équivalente en utilisant le langage des A-algèbres (rappelons que la donnée d'un anneau B et d'un morphisme d'anneaux $\varphi\colon A \to B$ correspond exactement à la donnée d'une A-algèbre). En particulier, le localisé $S^{-1}A$ est naturellement muni d'une structure de A-algèbre. On peut alors reformuler une partie du théorème précédent de la façon suivante.

THÉORÈME 4.4 *(propriété universelle de l'anneau localisé).* Soient A un anneau et S une partie multiplicative. On note $\varphi\colon A \to S^{-1}A$ le morphisme de localisation. Soient C un anneau et $\psi\colon A \to C$ un morphisme d'anneaux tel que $\psi(S) \subset C^\times$. Alors il existe un unique morphisme d'anneaux $\theta\colon S^{-1}A \to C$ tel que $\psi = \theta \circ \varphi$.

Preuve du théorème 4.2 • *Unicité à isomorphisme près.* Soient (B, φ) et (B', φ') deux tels couples. Appliquons la propriété vérifiée par le couple (B, φ) avec $C = B$ et $\psi = \varphi$. Il existe un unique morphisme d'anneaux $\iota\colon B \to B$ tel que $\iota \circ \varphi = \varphi$. On en déduit que $\iota = \mathrm{Id}_B$. De même pour le couple (B', φ').

Appliquons ensuite la propriété vérifie par le couple (B, φ) avec $C = B'$ et $\psi = \varphi'$. Il existe un unique morphisme d'anneaux $\theta\colon B \to B'$ tel que $\theta \circ \varphi = \varphi'$. Montrons que θ est un isomorphisme. En échangeant les rôles de B et B', il existe un unique morphisme $\theta'\colon B' \to B$ tel que $\theta' \circ \varphi' = \varphi$. Alors $\theta' \circ \theta \circ \varphi = \varphi$. D'après le paragraphe précédent, on en déduit $\theta' \circ \theta = \mathrm{Id}_B$. De même, on a $\theta \circ \theta' = \mathrm{Id}_{B'}$. Cela montre que θ est un isomorphisme.

• *Existence.* On munit l'ensemble $A \times S$ de la relation d'équivalence $\sim$ définie par

$$(a, s) \sim (a', s') \quad \iff \quad \exists t \in S,\ t(as' - a's) = 0$$

pour tous $(a, s), (a', s') \in A \times S$. On vérifie qu'il s'agit bien d'une relation d'équivalence. Notons B l'ensemble quotient et $\frac{a}{s}$ la classe d'équivalence d'un élément $(a, s) \in A \times S$ dans B. Pour $(a, s), (a', s') \in A \times S$, on pose

$$\frac{a}{s} + \frac{a}{s'} = \frac{as' + a's}{ss'} \quad \text{et} \quad \frac{a}{s} \times \frac{a'}{s'} = \frac{aa'}{ss'}.$$

On vérifie que ces définitions ne dépendent pas des représentants choisis et que ces deux lois munissent l'ensemble B d'une structure d'anneaux : les éléments neutres pour l'addition et la multiplication sont $\frac{0_A}{1_A}$ et $\frac{1_A}{1_A}$. De plus, on vérifie que l'application

$$\varphi\colon \begin{vmatrix} A \longrightarrow B, \\ a \longmapsto \dfrac{a}{1_A} \end{vmatrix}$$

est bien un morphisme d'anneaux vérifiant $\varphi(S) \subset B^\times$ puisque, pour tout $s \in S$, on a $\varphi(s) \times \frac{1_A}{s} = \frac{1_A}{1_A}$.

Soient C un anneau et $\psi\colon A \to C$ un morphisme d'anneaux tel que $\psi(S) \subset C^\times$. Montrons qu'il existe un unique morphisme d'anneaux $\theta\colon B \to C$ tel que $\theta \circ \varphi = \psi$. Supposons qu'un tel morphisme θ existe. Nécessairement, pour tout $a \in A$, on doit avoir $\theta(a/1_A) = \psi(a)$. De plus, pour tout $s \in S$, l'inverse $1_A/s$ dans B est $s/1_A$, donc $\theta(1_A/s) = \psi(s)^{-1}$. Finalement, pour tout $(a, s) \in A \times S$, on a

$$\theta\Big(\frac{a}{s}\Big) = \theta\Big(\frac{a}{1_A} \times \frac{1_A}{s}\Big) = \theta\Big(\frac{a}{1_A}\Big)\,\theta\Big(\frac{1_A}{s}\Big) = \psi(a)\psi(s)^{-1}.$$

ce qui montre l'unicité. Pour l'existence, il reste ensuite à vérifier que l'application $a/s \longmapsto \psi(a)\psi(s)^{-1}$ est bien définie et donne un morphisme d'anneaux. □

▷ Exemple. On reprend l'exemple introductif. Soient $x_0 \in \mathbb{R}$ et I un intervalle ouvert de $\mathbb{R}$ contenant x_0. L'ensemble

$$I_{x_0} \coloneqq \{f \in \mathscr{C}(I, \mathbb{R}) \mid f(x_0) = 0\}$$

est un idéal maximal de $\mathscr{C}(I, \mathbb{R})$. On note $S \coloneqq \mathscr{C}(I, \mathbb{R}) \setminus I_{x_0}$. Alors l'anneau localisé $S^{-1}\mathscr{C}(I, \mathbb{R})$ est isomorphe à l'anneau $\mathscr{C}(x_0, \mathbb{R})$ et le morphisme de localisation s'écrit $f \longmapsto \overline{(I, f)}$

Théorème 4.5. Soient A un anneau et S une partie multiplicative. On note $\varphi\colon A \to S^{-1}A$ le morphisme de localisation. Alors $\operatorname{Ker}\varphi = I_S$. En particulier,

1. si A est intègre et S ne contient pas 0_A, alors φ est injectif ;
2. l'anneau $S^{-1}A$ est nul si et seulement si S contient 0_A.

▷ Exemple. Soient A et B deux anneaux. La partie $S \coloneqq A^\times \times \{0_B, 1_B\}$ est multiplicative et vérifie $I_S = \{0_A\} \times B$. Le morphisme de localisation est le morphisme de projection de $A \times B$ dans A. En fait, dans ce qui précède, on peut remplacer $\{0_B, 1_B\}$ par n'importe quelle partie multiplicative de B contenant 0_B.

Théorème 4.6. Soient A un anneau intègre, S une partie multiplicative de A ne contenant pas 0_A et $\mathbb{K}$ un corps contenant A comme sous-anneau. On note $B \coloneqq S^{-1}A = \{a/s \mid (a, s) \in A \times S\} \subset \mathbb{K}$. Alors B est un sous-anneau de $\mathbb{K}$ contenant A. En outre, le morphisme de localisation est le morphisme déduit de l'inclusion de A dans B.

▷ Exemples. – Soit p un nombre premier. On note

$$\mathbb{Z}_{(p)} \coloneqq \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus p\mathbb{Z}\} \subset \mathbb{Q}.$$

Alors $\mathbb{Z}_{(p)} = (\mathbb{Z} \setminus p\mathbb{Z})^{-1}\mathbb{Z}$.
– Soit $x \in \mathbb{N} \setminus \{0\}$. On note

$$\mathbb{Z}[1/x] \coloneqq \{a/x^n \mid a \in \mathbb{Z}, n \in \mathbb{N}\} \subset \mathbb{Q}.$$

Alors $\mathbb{Z}[1/x] = \{x^n \mid n \in \mathbb{N}\}^{-1}\mathbb{Z}$.

4.3 Le corps des fractions d'un anneau intègre

Théorème 4.7. Soit A un anneau intègre. Alors le localisé $(A \setminus \{0_A\})^{-1}A$ est un corps, appelé le *corps des fractions* de A et noté $\operatorname{Frac} A$.

▷ Exemple. Soient p un nombre premier et $x \in \mathbb{N} \setminus \{0\}$. On a $\operatorname{Frac}\mathbb{Z} = \operatorname{Frac}\mathbb{Z}_{(p)} = \operatorname{Frac}\mathbb{Z}[1/x] = \mathbb{Q}$. Par ailleurs, on a $\operatorname{Frac}\mathbb{Z}[i] = \mathbb{Q}[i]$.

◇ Remarque. Soit $\mathbb{K}$ un corps. Le corps des fractions de $\mathbb{K}[X]$ s'appelle le *corps des fractions rationnelles* à une indéterminées à coefficients dans $\mathbb{K}$ et on le note $\mathbb{K}(X)$. Le corps des fractions de $\mathbb{K}[\![X]\!]$ s'appelle le *corps des séries de Laurent* à coefficients dans $\mathbb{K}$ et on le note $\mathbb{K}((X))$.

Les corps des fractions d'anneaux intègres sont des exemples particuliers de localisés et, à ce titre, vérifient la propriété universelle du localisé. Cependant, dans le cas des corps des fractions, cette propriété universelle peut se reformuler de la manière légèrement différente suivante.

THÉORÈME 4.8 *(propriété universelle du corps des fractions).* Soit A un anneau.

1. Soient $\mathbb{L}$ un corps et $\psi\colon A \to \mathbb{L}$ un morphisme d'anneaux injectif. On note $\varphi\colon A \to \operatorname{Frac} A$ le morphisme de localisation. Alors il existe un unique morphisme d'anneaux $\theta\colon \operatorname{Frac} A \to \mathbb{L}$ tel que $\psi = \theta \circ \varphi$.

2. Soient $\mathbb{K}$ un corps et $\varphi\colon A \to \mathbb{K}$ un morphisme d'anneaux injectif tels que, pour tout corps $\mathbb{K}$ et tout morphisme d'anneaux injectif $\psi\colon A \to \mathbb{L}$, il existe un unique morphisme d'anneaux $\theta\colon \mathbb{K} \to \mathbb{L}$ tel que $\psi = \theta \circ \varphi$. Alors le corps $\mathbb{K}$ est le corps $\operatorname{Frac} A$ et le morphisme φ est le morphisme de localisation.

Preuve 1. Comme ψ est un morphisme, on a $\psi(A \setminus \{0\}) \subset \mathbb{L} \setminus \{0_A\} = \mathbb{L}^\times$. La propriété universelle du localisé donne la conclusion.

2. Montrons que le couple (K, φ) vérifie la propriété universelle du localisé. Soient C un anneau et $\psi\colon A \to C$ un morphisme d'anneaux telle que $\varphi(A \setminus \{0_A\}) \subset C^\times$. Si C est l'anneau nul, on prend $\theta\colon x \in \operatorname{Frac} A \longmapsto 0_C \in C$. On suppose que C n'est pas l'anneau nul. En particulier, on a $\psi(A \setminus \{0_A\}) \subset C \setminus \{0\}$ ce qui assure l'injectivité du morphisme ψ. L'ensemble $B \coloneqq \psi(A)$ est un sous-anneau de C et, comme $\psi(A \setminus \{0_A\}) \subset C^\times$, l'ensemble

$$B' \coloneqq \{\psi(a)\psi(r)^{-1} \mid a, r \in A, r \neq 0_A\} \supset B$$

est un sous-corps de C. On note $\tilde{\psi}\colon A \to B'$ le morphisme induit. Par hypothèse, il existe un unique morphisme d'anneaux $\theta\colon \mathbb{K} \to B'$ tel que $\tilde{\psi} = \tilde{\theta} \circ \varphi$. On note $\iota\colon B' \to C$ le morphisme d'inclusion. En posant $\theta \coloneqq \iota \circ \tilde{\theta}$, on obtient $\psi = \theta \circ \varphi$. Mais tout morphisme $\theta'\colon \mathbb{K} \to C$ vérifiant $\theta' \circ \varphi = \psi$ a son image incluse dans $\psi(A) = B'$, donc il existe un morphisme $\tilde{\theta'}\colon \mathbb{K} \to B$ tel que $\theta' = \iota \circ \tilde{\theta'}$ et $\tilde{\theta'} \circ \varphi = \tilde{\psi}$. Ceci montre l'unicité de θ. □

◇ REMARQUE *(sur les usages des notations).* Nous terminons par quelques remarques concernant les notations pour les anneaux localisés. Outre la notation générique $S^{-1}A$, d'autres notations peuvent être utilisées lorsque S a une forme particulière.

On a déjà vu la notation $\operatorname{Frac} A$ lorsque A est intègre et $S = A \setminus \{0\}$. Cette notation est parfois aussi utilisée lorsque S est l'ensemble des éléments de A qui ne sont pas diviseurs de zéro (ici, l'anneau A n'est plus nécessairement intègre). Attention, dans ce cas plus général, l'anneau $\operatorname{Frac} A$ n'est pas nécessairement un corps : on l'appelle l'anneau total des fractions de A.

Lorsque I est un idéal premier de A et $S = A \setminus I$, le localisé $S^{-1}A$ est souvent noté A_I. Ceci se retrouve dans la notation $\mathbb{Z}_{(p)}$ où la notation (p) peut être vue comme une notation condensée de l'idéal $\langle p \rangle = p\mathbb{Z}$ (on aurait pu aussi utiliser la notation $\mathbb{Z}_{\langle p \rangle}$).

Lorsque S est de la forme $\{a^n \mid n \in \mathbb{N}\}$ où $a \in A$, le localisé $S^{-1}A$ est souvent noté A_a. Attention, cette notation peut entrer en conflit avec d'autres. Par exemple, si p est un nombre premier, la notation $\mathbb{Z}_p$ désigne déjà l'anneau des entiers p-adiques qui est distinct du localisé de $\mathbb{Z}$ par rapport à $\{p^n \mid n \in \mathbb{N}\}$. On peut également trouver la notation $A[\frac{1}{a}]$. Cette notation se justifie par le fait que, lorsque A est intègre et $a \neq 0$, le localisé $S^{-1}A$ s'identifie à l'image de l'unique morphisme de A-algèbre de $A[X]$ dans $\operatorname{Frac} A$ envoyant X sur $\frac{1}{a}$.

Chapitre 5

Anneaux euclidiens, principaux, factoriels

5.1 Lemme d'Euclide, lemme de Gauss, théorème de Bézout et factorisation unique 21
5.2 Anneaux factoriels, principaux, euclidiens 22
5.3 Valuations dans un anneau factoriel 23
5.4 PGCD, PPCM et relations de Bézout 24
5.4.1 PGCD et PPCM 24
5.4.2 Relations de Bézout 25
5.4.3 Algorithme d'Euclide étendu dans un anneau euclidien 25
5.4.4 PGCD et PPCM d'une famille finie d'éléments . 25
5.5 Valuations, PGCD et PPCM dans le corps des fractions 26
5.6 Factorialité des anneaux polynômes, critères d'irréductibilité 26
5.7 Démonstration des théorèmes 28
5.7.1 Tout anneau factoriel vérifie les lemmes de Gauss 28
5.7.2 Tout anneau principal est factoriel 29
5.7.3 Tout anneau factoriel vérifiant le théorème de Bézout est principal 30

5.1 Lemme d'Euclide, lemme de Gauss, théorème de Bézout et factorisation unique

Définition 5.1. On dit qu'un anneau intègre A vérifie

– la *propriété irréductible/premier* si, pour $a \in A\setminus\{0_A\}$, l'idéal aA est premier si et seulement si a est irréductible ;

– le *lemme d'Euclide* si, pour $a, b, c \in A$ tels que a soit irréductible et divise bc, alors $a \mid b$ ou $a \mid c$.

– le théorème de Bézout si, pour $a, b \in A$, les éléments a et b sont premiers entre eux si et seulement si $aA + bA = A$;

– le *lemme de Gauss* si, pour $a, b, c \in A$ tels que $a \mid bc$ et a et b soient premiers entre eux, on a $a \mid c$;

– le *théorème de factorisation unique en produit d'irréductibles* si, pour $a \in A\setminus(\{0_A\}\cup A^\times)$, il existe des éléments irréductibles $p_1, \dots, p_r \in A$ tels que $a = p_1 \cdots p_r$ et, de plus, cette décomposition est unique à l'ordre des facteurs et à associations près.

▷ Exemples. Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ vérifient toutes ces propriétés.

Proposition 5.2. Un anneau intègre A vérifie

1. la propriété « premier entraîne irréductible » : pour tout $a \in A \setminus \{0_A\}$, si l'idéal aA est premier, alors a est irréductible.
2. le lemme d'Euclide faible : pour tous $a, b, c \in A$, si l'idéal aA est premier non nul et $a \mid bc$, alors $a \mid b$ ou $a \mid c$;
3. le théorème de Bézout faible : pour tous $a, b \in A$, si $aA + bA = A$, alors a et b sont premier entre eux.
4. le lemme de Gauss faible : pour tous $a, b, c \in A$, si $a \mid bc$ et $aA + bA = A$, alors $a \mid c$.

Preuve 1. Déjà vu au chapitre 1.
2. Soient $a, b, c \in A$ tels que aA soit premier non nul et $a \mid bc$. Comme $a \mid bc$, on a $bc \in aA$. Comme l'idéal aA est premier, on a soit $b \in aA$ soit $c \in aA$, donc soit $a \mid b$ soit $a \mid c$.
3. Soient $a, b \in A$ tels que $aA + bA = A$. Soit $d \in A$ un diviseur commun de a et b. Comme $aA + bA = A$, on a $1_A \in aA + bA$, donc il existe $u, v \in A$ tels que $au + bv = 1_A$. Ainsi l'élément d divise 1_A, donc il est inversible, donc a et b sont premier entre eux.
4. Soient $a, b \in A$ tels que $aA + bA = A$ et $a \mid bc$. Comme précédemment, il existe $u, v \in A$ tel que $au + bv = 1_A$, donc $acu + bcv = c$. Or $a \mid bc$ et $a \mid acu$, donc $a \mid c$. □

Proposition 5.3. Soit A un anneau intègre. Alors

1. la propriété irréductible/premier est équivalente au lemme d'Euclide ;
2. le lemme de Gauss implique le lemme d'Euclide ;
3. le théorème de Bézout implique le lemme de Gauss.

Preuve 1. Compte tenu de la proposition précédente, il s'agit de montrer que le lemme d'Euclide est équivalent à la propriété « irréductible entraîne premier ». Mais on constate facilement que, pour un élément irréductible $a \in A$, le lemme d'Euclide exprime exactement le fait que l'idéal aA est premier.
2. Supposons que A vérifie le lemme de Gauss. Soient $a, b, c \in A$ tels que a soit irréductible et divise bc. Supposons que $a \nmid b$. Alors a et b sont premiers entre eux. Comme A vérifie le lemme de Gauss, on a $a \mid c$. Donc A vérifie bien le lemme d'Euclide.
3. Comme A vérifie le lemme de Gauss faible, s'il vérifie le théorème de Bézout, alors il vérifie le lemme de Gauss. □

5.2 Anneaux factoriels, principaux, euclidiens

Définition 5.4. Un anneau intègre A est dit
- *factoriel* s'il vérifie le théorème de factorisation unique en produit d'irréductibles ;
- *principal* si tout idéal de A est engendré par un élément, *i. e.* tout idéal I de A est de la forme aA avec $a \in A$.

Les anneaux principaux forment une classe importante d'anneaux factoriels. De plus, les anneaux sur lesquels une division euclidienne est possible forment une classe importante d'anneaux principaux.

Définition 5.5. Un anneau intègre A est dit *euclidien* s'il existe une application $\nu \colon A \setminus \{0_A\} \to \mathbb{N}$ vérifiant que, pour tous $a, b \in A$ avec $b \neq 0_A$, il existe $q, r \in A$ tels que $a = bq + r$ et soit $r = 0_A$ soit $\nu(r) < \nu(b)$.

◇ Remarque. Une telle application ν est appelée un *stathme euclidien*. Pour tous $a, b \in A$ tels que $b \neq 0$, une écriture $a = bq + r$ avec $r = 0_A$ ou $\nu(r) < \nu(b)$ est appelée une *division euclidienne* de a par b (par rapport à ν).

Théorème 5.6. 1. Il existe des anneaux intègres non factoriels.
2. Tout anneau principal est factoriel.
3. Il existe des anneaux factoriels non principaux.
4. Tout anneau euclidien est principal.
5. Il existe des anneaux principaux non euclidiens.

Preuve Le point 2 est montré dans la section 5.7.2

Montrons le point 4. Soient A un anneau euclidien et ν un stathme euclidien sur A. Par définition, l'anneau A est intègre. Soit I un idéal de A. Si I est nul, alors $I = 0_A A$. On suppose que I est non nul. On considère l'entier $\nu_0 \coloneqq \min \nu(I \setminus \{0_A\})$. Soit $a \in I \setminus \{0_A\}$ tel que $\nu(a) = \nu_0$. Montrons que $I = aA$. Comme a appartient à l'idéal I, on a $aA \subset I$. Réciproquement, soit $b \in I$. Il existe $q, r \in A$ tel que $b = aq + r$ et soit $r = 0_A$ soit $\nu(r) < \nu(a)$. Comme $a, b \in I$, on a $r = b - aq \in I$. Si $r \neq 0_A$, alors $r \in I \setminus \{0_A\}$ et $\nu(r) < \nu_0$ ce qui est impossible par minimalité de ν_0. Donc $r = 0_A$ et $b = aq \in aA$. D'où $I \subset aA$ ce qui termine la preuve. □

Théorème 5.7. Soit A un anneau factoriel. Alors $A[X]$ est un anneau factoriel.

Preuve La preuve sera faite à la page 27 □

Théorème 5.8. Un anneau factoriel vérifie le lemme de Gauss. Cela implique qu'il vérifie le lemme d'Euclide et la propriété irréductible/premier.

Preuve La preuve sera faite dans la section 5.7.1. □

Théorème 5.9. Un anneau principal vérifie le théorème de Bézout. Cela implique qu'il vérifie la propriété irréductible/premier, le lemme d'Euclide et le lemme de Gauss.

Preuve Soit A un anneau principal. Montrons qu'il vérifie le théorème de Bézout. Il vérifie déjà sa version faible. Soient $a, b \in A$ deux éléments premiers entre eux. Montrons que $aA + bA = A$. Comme A est principal, il existe $d \in A$ tel que $aA + bA = dA$. En particulier, on a $aA \subset dA$ et $bA \subset dA$, donc l'élément d divise a et b. Comme a et b sont premiers entre eux, l'élément d est inversible ce qui assure l'égalité $dA = A$. □

Théorème 5.10. Un anneau factoriel vérifiant le théorème de Bézout est principal.

Preuve Le preuve sera faite dans la section 5.7.3. □

◇ Remarque. Comme il existe des anneaux factoriels non principaux, ceci montre, en particulier, qu'il existe des anneaux intègres vérifiant le lemme de Gauss mais pas le théorème de Bézout.

▷ Exemples. – Soit $\mathbb{K}$ un corps. Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ muni des stathmes respectifs $n \longmapsto |n|$ et $P \longmapsto \deg P$ sont euclidiens. Dans ces deux cas, la division euclidien est unique.
– En vertu du théorème 5.7, on en déduit que les anneaux $\mathbb{Z}[X_1, \dots, X_n]$ et $\mathbb{K}[X_1, \dots, X_n]$ sont factoriel. Cependant, on verra que le premier n'est pas principal et que, si $n \geqslant 2$, le second ne l'est pas non plus.
– L'anneau $\mathbb{Z}[i]$ des entiers de Gauss muni du stathme $z \longmapsto z\overline{z}$ est euclidien (cf. proposition suivante).
– La valuation ν sur $\mathbb{K}[\![X]\!]$ est un stathme sur $\mathbb{K}[\![X]\!]$. En particulier, cet anneau $\mathbb{K}[\![X]\!]$ est euclidien, donc principal et factoriel.
– Soit p un nombre premier. Alors la valuation p-adique ν_p est un stathme sur l'anneau $\mathbb{Z}_{(p)}$.

– L'anneau $\mathbb{Z}[i\sqrt{3}]$, isomorphe au quotient $\mathbb{Z}[X]/\langle X^2+3\rangle$ est intègre mais n'est pas factoriel.
– L'anneau $A \coloneqq \mathbb{K}[X,Y]/\langle X^2-Y^3\rangle$ est intègre mais n'est pas factoriel. Intuitivement, cela vient du fait que l'on a forcé, dans le quotient, la factorisation non unique $X^2 = Y^2$. Cet exemple et le précédent montrent qu'un quotient intègre d'un anneau factoriel n'est pas nécessairement factoriel.
– Soit A un anneau intègre. On peut montrer que l'anneau $A[X]$ est principal si et seulement si l'anneau A est un corps. En vertu du théorème 5.7, les anneaux $\mathbb{Z}[X]$ et $\mathbb{K}[X,Y]$ sont des anneaux factoriels non principaux. De ce fait, on en déduit que l'idéal $\langle 2, X\rangle$ de $\mathbb{Z}[X]$ n'est pas principal et l'idéal $\langle X, Y\rangle$ de $\mathbb{K}[X,Y]$ ne l'est pas aussi.

PROPOSITION 5.11. L'application

$$N\colon \left|\begin{array}{l}\mathbb{Z}[i] \longrightarrow \mathbb{Z},\\ \quad z \longmapsto z\overline{z}\end{array}\right.$$

induit sur $\mathbb{Z}[i]\setminus\{0\}$ un stathme. En particulier, l'anneau $\mathbb{Z}[i]$ est euclidien.

Preuve Faisons d'abord un remarque d'ordre géométrique. Pour tout point $x \in \mathbb{R}^2$, il existe un élément $y \in \mathbb{Z}^2$ à distance strictement inférieure à 1 de y. En identifiant $\mathbb{C}$ au plan $\mathbb{R}^2$, l'anneau $\mathbb{Z}[i]$ s'identifie à $\mathbb{Z}^2$ et la remarque assure que, pour tout $z \in \mathbb{C}$, il existe $y \in \mathbb{Z}[i]$ tel que $N(x-y) < 1$.

Soient $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$. Considérons $a/b \in \mathbb{C}$. Alors il existe $q \in \mathbb{Z}[i]$ tel que $N(a/b - q) < 1$. Comme l'application N est multiplicative, en multipliant par $N(b)$, on obtient $N(r) < N(b)$ avec $r \coloneqq a - bq \in \mathbb{Z}[i]$. □

▷ EXEMPLE. Dans $\mathbb{Z}[i]$, calculons des divisions euclidiennes de $5+10i$ par $-1+7i$. On effectue le calcul

$$\frac{5+10i}{-1+7i} = \frac{13}{10} - \frac{9}{10i}.$$

Par exemple, on peut prendre $q \in \{1, 1-i, 2-i\}$ et on obtient les divisions euclidiennes

$$\begin{aligned} 5+10i &= 1(-1+7i) + 6 + 3i \\ &= (1-i)(-1+7i) - 1 + 2i \\ &= (2-i)(-1+7i) - 5i. \end{aligned}$$

Une application

L'anneau $\mathbb{Z}[i]$ est euclidien. En particulier, il vérifie la propriété irréductible/premier. Donnons-en une application : quels sont les nombres premiers qui s'écrivent comme une somme de deux carrés ? L'application N induit une application $N\colon \mathbb{Z}[i] \to \mathbb{N}$.

THÉORÈME 5.12. Soit p un nombre premier. Alors les propositions suivantes sont équivalentes :
(i) l'élément p n'est pas irréductible dans $\mathbb{Z}[i]$;
(ii) l'idéal $p\mathbb{Z}[i]$ de $\mathbb{Z}[i]$ n'est pas premier ;
(iii) l'élément -1 est un carré modulo p, *i. e.* la classe $[-1]_p$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$;
(iv) l'entier p est une somme de carrés d'entiers, *i. e.* il existe $a, b \in \mathbb{Z}$ tels que $a^2 + b^2 = p$.

Preuve L'équivalence (ii) ⇔ (iii) a déjà été montrée. L'implication (i) ⇒ (ii) est même vraie dans n'importe quel anneau intègre. L'implication (iv) ⇒ (iii) est relativement facile.

Montrons l'implication (i) ⇒ (iv). On suppose (i). Alors il existe des éléments non associés $w, z \in \mathbb{Z}[i]$ tels que $p = wz$. En passant à la norme, on obtient $p^2 = N(w)N(z)$. Si $N(w) = 1$, alors w serait associé à p ce qui est impossible. Donc $N(w) = N(z) = p$. On peut écrire $z = a + ib$ avec $a, b \in \mathbb{Z}$ et on obtient finalement $p = a^2 + b^2$. D'où (iv).

Il suffit alors de montrer l'implication (ii) ⇒ (i) ce qui est une conséquence du fait que l'anneau $\mathbb{Z}[i]$ est euclidien et donc vérifie la propriété irréductible/premier. Cela termine la preuve. □

5.3 Valuations dans un anneau factoriel

Soit A un anneau intègre. La relation d'association, notée $\sim$, est une relation d'équivalence sur A. Notons que, pour tous $a, b \in A/\!\sim$, on peut donner un sens à la condition « a divise b ». La relation $\sim$ induit une relation d'équivalence sur l'ensemble des éléments irréductibles I de A. Soit $\mathscr{I}(A) \coloneqq I/\!\sim$. Dans la pratique, il est utile de travailler avec un système de représentants $\operatorname{Irr} A \subset A$ de $\mathscr{I}(A)$ que l'on pourra identifier à $\mathscr{I}(A)$.

▷ EXEMPLES. – Pour $A = \mathbb{Z}$, on peut prendre $\operatorname{Irr}\mathbb{Z}$ l'ensemble des nombres premiers.
– Pour $A = \mathbb{K}[X]$, on peut prendre $\operatorname{Irr}\mathbb{K}[X]$ l'ensemble des polynômes irréductibles et unitaires.
– Pour $A = \mathbb{K}[\![X]\!]$, on peut prendre $\operatorname{Irr}\mathbb{K}[\![X]\!]$ le singleton $\{X\}$.

– Pour $A = \mathbb{Z}_{(p)}$, on peut prendre $\operatorname{Irr} \mathbb{Z}_{(p)}$ le singleton $\{p\}$.
– Pour $A = \mathbb{Z}[1/x]$ avec $x \in \mathbb{N}^*$, on peut prendre $\operatorname{Irr} \mathbb{Z}[1/x]$ l'ensemble des nombres premiers ne divisant pas x.

THÉORÈME 5.13. Soient A un anneau factoriel et $a \in A \setminus \{0_A\}$. Alors il existe une unique famille presque nulle d'entiers $(v_\pi(a))_{\pi \in \mathscr{I}(A)} \in \mathbb{N}^{(\mathscr{I}(A))}$ tels que, pour tout système $\operatorname{Irr} A$ de représentants d'irréductibles de A, on ait

$$a \sim \prod_{\pi \in \operatorname{Irr} A} \pi^{v_\pi(a)}.$$

Preuve Ce n'est qu'une traduction de la propriété d'unicité de la factorisation en irréductibles. □

DÉFINITION 5.14. Soit $\pi \in \mathscr{I}(A)$. En posant $v_\pi(0_A) = +\infty$, le théorème précédent permet de définir une fonction $v_\pi \colon A \longrightarrow \mathbb{N} \cup \{+\infty\}$, appelée *valuation π-adique*.

THÉORÈME 5.15. Soient A un anneau factoriel et $a, b \in A$. Alors
1. a et b sont associés si et seulement si $v_\pi(a) = v_\pi(b)$ pour tout $\pi \in \mathscr{I}(A)$;
2. a est inversible si et seulement si $v_\pi(a) = 0$ pour tout $\pi \in \mathscr{I}(A)$;
3. pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(ab) = v_\pi(a) + v_\pi(b)$;
4. a divise b si et seulement si $v_\pi(a) \leqslant v_\pi(b)$ pour tout $\pi \in \mathscr{I}(A)$;
5. si $a \neq 0_A$ et $\pi \in \mathscr{I}(A)$, on a $v_\pi(a) = \max\{n \in \mathbb{N} \mid \pi^n \mid a\}$.

Preuve Les trois premiers points découlent du théorème précédent et le point 5 se déduit du point 4.

Montrons le point 4. Le résultat est trivial si $b = 0_A$. On suppose donc $b \neq 0_A$. Directement, on suppose que a divise b. Il existe $c \in A$ tel que $b = ca$. Comme $b \neq 0_A$, on a $c \neq 0_A$. Soit $\pi \in \mathscr{I}(A)$. Alors $v_\pi(b) = v_\pi(c) + v_\pi(a)$. Comme $v_\pi(c) \in \mathbb{N}$, on a bien $v_\pi(b) \geqslant v_\pi(a)$. Réciproquement, on suppose que $v_\pi(a) \leqslant v_\pi(b)$ pour tout $\pi \in \mathscr{I}(A)$. Avec cette hypothèse, comme $b \neq 0_A$, on peut écrire $a \neq 0_A$. Alors, pour tout système $\operatorname{Irr} A$ de représentants d'irréductibles de A, on a

$$a \sim \prod_{\pi \in \operatorname{Irr} A} \pi^{v_\pi(a)} \quad \text{et} \quad b \sim \prod_{\pi \in \operatorname{Irr} A} \pi^{v_\pi(b)},$$

donc

$$b \sim a \prod_{\pi \in \operatorname{Irr} A} \pi^{v_\pi(b) - v_\pi(a)}$$

ce qui montre que a divise b. □

5.4 PGCD, PPCM et relations de Bézout

5.4.1 PGCD et PPCM

DÉFINITION 5.16. Soient A un anneau intègre et $a, b \in A$. Un *plus grand commun diviseur* (abrégé PGCD) de la paire $\{a, b\}$ est un élément $\delta \in A$ tel que
– δ divise a et b ;
– tout élément $d \in A$ divisant a et b divise δ.

Un *plus petit commun multiple* (abrégé PPCM) de la paire $\{a, b\}$ est un élément $\mu \in A$ tel que
– a et b divisent μ ;
– tout élément $m \in A$ divisible par a et b est divisible par μ.

▷ EXEMPLES. – Pour tous $a, b \in A$ premiers entre eux, tout élément de $A^\times$ est un PGCD de a et b.
– Pour tous $a, b \in A$ associés, tout élément associé à a et b est un PGCD de a et b.
– Pour tout $a \in A$, tout élément associé à a est un PGCD de a et 0.

PROPOSITION 5.17. Soient A un anneau intègre et $a, b \in A$. On suppose que a et b admettent un PGCD $\delta \in A$ (resp. un PPCM $\mu \in A$).
1. Soit $c \in A$. Alors c est un PGCD (resp. un PPCM) de a et b si et seulement si c est associé à δ (resp. à μ).
2. Soit $\alpha \in A$. Alors $\alpha\delta$ et $\alpha\mu$ sont resp. des PGCD et PPCM de αa et αb.
3. Soit $\alpha \in A \setminus \{0_A\}$ un diviseur commun de a et b. Alors δ/α et μ/α sont resp. des PGCD et PPCM de a/α et b/α. En particulier, si $\delta \neq 0$, alors a/δ et b/δ sont premiers entre eux.

Le théorème suivant garantit l'existence de PGCD et PPCM dans un anneau factoriel.

THÉORÈME 5.18. Soient A un anneau factoriel et $a, b \in A$.

1. Soit $c \in A$. Alors c est un PGCD (resp. un PPCM) de a et b si et seulement si, pour tout $\pi \in \mathscr{I}(A)$, on a

$$v_\pi(c) = \min(v_\pi(a), v_\pi(b)) \quad (\text{resp. } v_\pi(c) = \min(v_\pi(a), v_\pi(b))).$$

En particulier, les éléments a et b admettent un PGCD et un PPCM.

2. On suppose que A est principal. Alors c est un PGCD (resp. PPCM) de a et b si et seulement s'il engendre l'idéal $aA + bA$ (resp. $aA \cap bA$).

Preuve Le point 1 découle du point 4 du théorème précédent. Montrons le point 2 et traitons uniquement le cas du PGCD. Comme A est principal, le sens direct est évident. Réciproquement, on suppose que c engendre $aA + bA$. En particulier, l'idéal cA contient aA et bA, donc c divise a et b. Soit $d \in A$ divisant a et b. Alors l'idéal dA contient aA et bA, donc il contient $aA + bA = cA$, donc d divise c. On en déduit que c est un PGCD de a et b. □

5.4.2 Relations de Bézout

DÉFINITION 5.19. Soient A un anneau intègre et $a, b \in A$. Une *relation de Bézout* pour a et b est un couple $(u, v) \in A^2$ tels que $au + bv$ soit un PGCD de a et b.

◇ REMARQUE. En divisant une relation de Bézout $au + bv = \delta$ par δ, on obtient $uA + vA = A$ ce qui implique que les éléments u et v sont premiers entre eux.

PROPOSITION 5.20. Soient A un anneau intègre et $a, b \in A$. Alors il existe une relation de Bézout pour a et b si et seulement si l'idéal $aA + bA$ est principal.

Ainsi pour tout anneau principal A, toute paire d'élément admet une relation de Bézout. Cependant, dans la pratique, trouver une telle relation est difficile.

5.4.3 Algorithme d'Euclide étendu dans un anneau euclidien

LEMME 5.21. Soient A un anneau intègre et $a, b \in A$. On suppose qu'il existe $q, r \in A$ tels que $a = qb + r$. Alors a et b admettent un PGCD si et seulement si b et r admettent un PGCD. Dans ce cas, ces deux paires ont le même PGCD.

Preuve La relation $a = qb + r$ entraîne que tout diviseur commun de a et b divise r et que tout diviseur commun de b et r divise a. Ainsi, les paires $\{a, b\}$ et $\{q, r\}$ ont exactement les mêmes diviseurs communs. La définition d'un PGCD permet de conclure. □

ALGORITHME. Soit A un anneau muni d'un stathme ν. On initialise l'algorithme d'Euclide en posant $r_{-1} = a$ et $r_0 = b$. Ensuite, pour $n \in \mathbb{N}$ et tant que r_n est non nul, on écrit une division euclidienne de r_{n-1} par r_n

$$r_{n-1} = q_n r_n + r_{n+1}.$$

En particulier, on a r_{n+1} ou $\nu(r_{n+1}) < \nu(r_n)$. On définit ainsi une suite $(r_n)_{n \geqslant 1}$ d'éléments de A qui est nécessairement une suite finie car la suite $(\nu(r_n))_{n \geqslant 0}$, définie tant que r_n n'est pas nul, est une suite strictement décroissant d'entiers positifs. D'après le lemme précédent, une récurrence immédiate montre que, pour $n \geqslant -1$ tel que r_{n+1} soit défini, les paires $\{a, b\}$ et $\{r_n, r_{n+1}\}$ ont les mêmes PGCD. Ainsi si on note $N \in \mathbb{N}$ le plus grand entier $n \in \mathbb{N}$ tel que $r_n = 0$, les paires $\{a, b\}$ et $\{r_N, r_{N+1}\} = \{r_N, 0_A\}$ ont le même PGCD. En particulier, l'élément r_N est un PGCD de a et b.

5.4.4 PGCD et PPCM d'une famille finie d'éléments

DÉFINITION 5.22. Soient A un anneau intègre et $\{a_i\}_{i \in I}$ une famille finie de A. Un PGCD de la famille $\{a_i\}_{i \in I}$ est un élément $\delta \in A$ tel que

- δ divise a_i pour tout $i \in I$;
- tout $d \in A$ divisant les éléments a_i divise δ ;

Un PPCM de la famille $\{a_i\}_{i \in I}$ est un élément $\mu \in A$ tel que

- a_i divise μ pour tout $i \in I$;
- tout $m \in A$ divisible par les éléments a_i est divisible par μ ;

De même, les propositions 5.17 à 5.20 sont également valables pour les PGCD et PPCM d'une famille finie d'éléments, les démonstrations étant analogues.

5.5 Valuations, PGCD et PPCM dans le corps des fractions

Lemme 5.23. Soient A un anneau factoriel, $x \coloneqq a/b \in \operatorname{Frac} A$ et $\pi \in \mathscr{I}(A)$. Alors l'élément $v_\pi(a) - v_\pi(b)$ ne dépend que de x et coïncide avec $v_\pi(x)$ si $x \in A$.

Preuve On écrit $x = c/d$. Alors $ad = bc$, donc $v_\pi(a) + v_\pi(d) = v_\pi(b) + v_\pi(c)$. Comme $v_\pi(b)$ et $v_\pi(d)$ ne valent pas l'infini, on obtient $v_\pi(a) - v_\pi(b) = v_\pi(c) - v_\pi(d)$. □

Définition 5.24. Pour $x \coloneqq a/b \in \operatorname{Frac} A$, on pose $v_\pi(x) \coloneqq v_\pi(a) - v_\pi(b)$. On a ainsi prolongé la valuation π-adique $v_\pi \colon A \to \mathbb{N} \cup \{+\infty\}$ en une application $v_\pi \colon \operatorname{Frac} A \to \mathbb{Z} \cup \{+\infty\}$.

◇ Remarque. Pour tout $x \in \operatorname{Frac} A$ et $\pi \in \mathscr{I}(A)$, on a $v_\pi(x) = +\infty \Leftrightarrow x = 0_A$.

◇ Remarque. Soit A un anneau intègre. La relation d'association s'étend aux éléments de $\operatorname{Frac} A$: deux fractions x et y seront dites A-associés s'il existe un élément $\alpha \in A^\times$ tel que $x = \alpha y$ et on notera $x \sim_A y$. Il faut bien préciser l'anneau puisque, en général, il n'y a pas l'unicité de l'anneau A dont le corps des fractions est $\operatorname{Frac} A$. Les exemples, les éléments $1/2$ et $-1/2$ sont $\mathbb{Z}$-associés tandis que les éléments $1/2$ et 2 sont $\mathbb{Q}$-associés mais pas $\mathbb{Z}$-associés.

Théorème 5.25. Soient A un anneau factoriel et $x, y \in \operatorname{Frac} A$. Alors

1. l'ensemble $\{\pi \in \mathscr{I}(A) \mid v_\pi(x) \neq 0\}$ est fini. Par ailleurs, pour tout système $\operatorname{Irr} A$ de représentants d'irréductibles de A, on a
$$x \sim \prod_{\pi \in \operatorname{Irr} A} \pi^{v_\pi(x)}.$$
Cette dernière formule s'étend au cas $x = 0_{\operatorname{Frac} A}$ en posant $\pi^{+\infty} = 0$.
2. x et y sont A-associés si et seulement si $v_\pi(x) = v_\pi(y)$ pour tout $\pi \in \mathscr{I}(A)$;
3. $x \in A$ si et seulement si $v_\pi(x) \geqslant 0$ pour tout $\pi \in \mathscr{I}(A)$;
4. pour tout $\pi \in \mathscr{I}(A)$, on a $v_\pi(xy) = v_\pi(x) + v_\pi(y)$.

Définition 5.26. Soient A un anneau factoriel et $\{a_i\}_{i \in I}$ une famille finie de $\operatorname{Frac} A$. Pour $\pi \in \mathscr{I}(A)$, on pose
$$m_\pi \coloneqq \min_{i \in I} v_\pi(a_i) \quad \text{et} \quad M_\pi \coloneqq \min_{i \in I} v_\pi(a_i).$$
On appelle A-PGCD (resp. A-PPCM) de la famille $\{a_i\}_{i \in I}$ tout élément de $\operatorname{Frac} A$ qui soit A-associés au produit
$$\prod_{\pi \in \mathscr{I}(A)} \pi^{m_\pi} \quad (\text{resp. } \prod_{\pi \in \mathscr{I}(A)} \pi^{M_\pi}).$$

Proposition 5.27. Soient A un anneau factoriel et $\{a_i\}_{i \in I}$ une famille finie de $\operatorname{Frac} A$. Si les éléments a_i sont dans A, alors tout A-PGCD (resp. A-PPCM) de $\{a_i\}_{i \in I}$ est un PGCD (resp. PPCM) de $\{a_i\}_{i \in I}$. De plus, les propositions suivant sont équivalentes :

(i) pour tout $i \in I$, on a $a_i \in A$;
(ii) tout A-PGCD de $\{a_i\}_{i \in I}$ appartient à A ;
(iii) un A-PGCD de $\{a_i\}_{i \in I}$ appartient à A.

Proposition 5.28. Soient A un anneau factoriel, $\{a_i\}_{i \in I}$ une famille finie de $\operatorname{Frac} A$ et $\delta \in \operatorname{Frac} A$ un A-PGCD (resp. A-PPCM) de $\{a_i\}_{i \in I}$.

1. Soit $\alpha \in \operatorname{Frac} A$. Alors $\alpha\delta$ est un A-PGCD (resp. A-PPCM) de $\{\alpha a_i\}_{i \in I}$.
2. Soit $\alpha \in \operatorname{Frac} A \setminus \{0_{\operatorname{Frac} A}\}$. Alors δ/α est un A-PGCD (resp. A-PPCM) de $\{a_i/\alpha\}_{i \in I}$;
3. L'élément δ est un A-PGCD de la famille $\{a_i\}_{i \in I} \cup \{0_{\operatorname{Frac} A}\}$.

5.6 Factorialité des anneaux polynômes, critères d'irréductibilité

Dans cette section, on veut montrer le théorème 5.7. On va également donne, pour un anneau factoriel A, des critères d'irréductibilité dans $A[X]$ et $(\operatorname{Frac} A)[X]$. Dans toute la suite de cette section, on considérera un anneau factoriel A.

Définition 5.29. On appelle *contenu* d'un polynôme $P \in (\operatorname{Frac} X)[X]$ tout A-PGCD des coefficients de P. On le note $c(P) \in \operatorname{Frac} A$. On dit qu'un polynôme $P \in (\operatorname{Frac} A)[X]$ est *primitif* si $c(P) \sim_A 1_{\operatorname{Frac} A}$.

◇ Remarque. Plus précisément, voici ce qu'on entend par « A-PGCD des coefficients ». On note $P = \sum_{n\in\mathbb{N}} a_n X_n$ avec $(a_n)_{n\in\mathbb{N}} \in (\operatorname{Frac} A)^{(\mathbb{N})}$. Soit $E \subset \mathbb{N}$ une partie finie telle que $a_n = 0$ pour tout $n \in \mathbb{N} \setminus E$. Alors $c(P)$ est un A-PGCD de la famille $\{a_n\}_{n\in E}$. D'après le dernier point de la proposition précédente, l'élément $c(P)$ ne dépend pas, à A-association près, du choix du d'une telle partie E.

Proposition 5.30. 1. Un polynôme de $A[X]$ est nul si et seulement si son contenu est nul.
2. Un polynôme unitaire de $A[X]$ est primitif. Plus généralement, pour tout $P \in (\operatorname{Frac} A)[X]$, on a $1/c(P) \in A$.
3. Pour tout $P \in (\operatorname{Frac} A)[X]$, on a $P \in A[X] \Leftrightarrow c(P) \in A$. En particulier, tout polynôme primitif de $(\operatorname{Frac} A)[X]$ est un élément de $A[X]$.
4. Pour tous $P \in A[X]$ et $a \in \operatorname{Frac} A$, on a $c(aP) \sim_A ac(P)$.
5. Pour tout $P \in A[X] \setminus \{0_{A[X]}\}$, on a $c(P) \neq 0_{\operatorname{Frac} A}$ et le polynôme $P/c(P)$ est primitif.

Preuve Cela découle des propositions 5.27 et 5.28. □

Proposition 5.31. Soient $P, Q \in (\operatorname{Frac} A)[X]$. Alors $c(PQ) \sim_A c(P)c(Q)$.

Preuve Tout d'abords, montrons que le produit de deux polynômes primitifs est primitif. Soient $P, Q \in A[X]$ deux polynômes primitifs. Il suffit de montrer que, pour tout élément irréductible π de A, il existe un coefficient de PQ qui ne soit pas divisible par π. On se place dans la quotient $B \coloneqq A/\langle\pi\rangle$. Il s'agit de montrer que $\overline{PQ}$ est non nul. Comme P et Q sont primitifs, les éléments $\overline{P}$ et $\overline{Q}$ sont non nuls. Comme π est irréductible et A est factoriel, l'idéal $\langle\pi\rangle$ est premier, donc l'anneau B est intègre, donc l'anneau $B[X]$ est intègre. On en déduit que l'élément $\overline{PQ} = \overline{P} \times \overline{Q}$ est non nul ce qui conclut.

Soient $P, Q \in (\operatorname{Frac} A)[X]$. Si $P = 0$ ou $Q = 0$, alors $c(PQ) = 0 = c(P)c(Q)$ ce qui rend triviale la proposition. On suppose que $P \neq 0$ et $Q \neq 0$. Alors $c(P) \neq 0$ et $c(Q) \neq 0$. Par la proposition précédente, les polynômes $P/c(P)$ et $Q/c(Q)$ sont primitifs, donc

$$1 \sim_A c\Big(\frac{PQ}{c(P)c(Q)}\Big) \sim_A \frac{c(PQ)}{c(P)c(Q)}$$

ce qui montre le résultat. □

Lemme 5.32. Soient $P \in A[X]$ un polynôme primitif et $Q, R \in (\operatorname{Frac} A)[X]$ tels que $P = QR$. Alors il existe des polynômes primitifs $\tilde{Q}, \tilde{R} \in A[X]$ associés respectivement à Q et R dans $(\operatorname{Frac} A)[X]$ tels que $P \sim_A \tilde{Q}\tilde{R}$

Preuve Par hypothèse, on a $c(Q)c(R) \sim_A 1$, donc $c(Q)c(R) \in A^\times$. Alors $\tilde{Q} \coloneqq Q/c(Q)$ et $\tilde{R} \coloneqq R/c(R)$ sont primitifs et vérifient $P \sim_A \tilde{Q}\tilde{R}$. □

Théorème 5.33. L'ensemble des éléments irréductibles de $A[X]$ est la réunion disjointes des deux ensembles suivants :
– l'ensemble des polynômes constants qui sont des éléments irréductibles de A ;
– l'ensemble des polynômes qui sont primitifs et irréductibles dans $(\operatorname{Frac} A)[X]$.

Preuve du théorème 5.7 Montrons que $A[X]$ est factoriel. Pour cela, montrons d'abord l'existence d'une décomposition en irréductibles. Soit $P \in A[X]$ un polynôme non nul et non inversible. Le polynôme $Q \coloneqq P/c(P)$ est un élément primitif de $A[X]$. Soit $Q = P_1 \cdots P_r$ une décomposition de Q en produit de polynômes irréductibles de $(\operatorname{Frac} A)[X]$. Par le lemme précédente, quitter à remplacer les polynômes P_i par des polynômes associés dans $(\operatorname{Frac} A)[X]$, on peut supposer qu'ils sont primitifs. De telle sorte, ils sont irréductibles dans $A[X]$. Comme $P = c(P)Q$, en décomposant la fraction $c(P) \in \operatorname{Frac} A$ en irréductible dans A, par le théorème précédent, on obtient une décomposition de P en produits d'irréductibles de $A[X]$.

Montrons l'unicité de la décomposition à permutation et association près. Supposons qu'il existe des éléments irréductibles $a_1, \ldots, a_{r_1}, b_1, \ldots, b_{s_1} \in A$ et des polynômes irréductibles $P_1, \ldots, P_{r_2}, Q_1, \ldots, Q_{s_2} \in A[X]$ primitifs dans $(\operatorname{Frac} A)[X]$ tels que

$$a_1 \cdots a_{r_1} P_1 \cdots P_{r_2} = b_1 \cdots b_{s_1} Q_1 \cdots Q_{s_2}.$$

L'unicité de la décomposition dans $(\operatorname{Frac} A)[X]$ donne $r_2 = s_2$ et, quitte à renuméroter, les polynômes P_i et Q_i sont associés pour tout $i \in [\![1, s_1]\!]$. Soit $i \in [\![1, s_1]\!]$. Il existe $\alpha_i \in (\operatorname{Frac} A)^\times$ tel que $P_i = \alpha_i Q_i$. En passant au contenu, on a $\alpha_i \sim_A 1$, donc $\alpha_i \subset A^\times \subset A[X]^\times$. Quitte à remplacer Q_i par $\alpha_i Q_i$, on a $P_i = Q_i$. D'où $a_1 \cdots a_{r_1} = b_1 \cdots b_{s_1}$. On conclut en utilisant l'unicité de la factorisation dans l'anneau factoriel A. □

COROLLAIRE 5.34. L'anneau $A[X_1, \dots, X_n]$ est factoriel. En particulier, l'anneau $\mathbb{K}[X_1, \dots, X_n]$ est factoriel.

THÉORÈME 5.35. Soit $\pi \in A$ un élément irréductible. On note $B \coloneqq A/\pi A$ et $\varphi\colon A \to B$ le morphisme quotient. On note encore φ l'unique morphisme d'anneau de $A[X]$ dans $B[X]$ prolongeant φ et envoyant X sur lui-même. Soit $P \in A[X]$. On suppose que $\deg \varphi(P) = \deg P$. Si $\varphi(P)$ est irréductible dans $(\operatorname{Frac} B)[X]$, alors P est irréductible dans $(\operatorname{Frac} A)[X]$.

Preuve On suppose que $\varphi(P)$ est irréductible dans $(\operatorname{Frac} B)[X]$. L'hypothèse $\deg \varphi(P) = \deg P$ assure que π ne divise pas le coefficient dominant de P. En particulier, il ne divise pas $c(P)$. De cela, pour tout polynôme primitif $Q \in A[X]$ tels que $P = c(P)Q$, on en déduit les points suivants :

- $\deg \varphi(Q) = \deg Q$;
- P et Q sont associés dans $(\operatorname{Frac} A)[X]$;
- $\varphi(P)$ et $\varphi(Q)$ sont associés dans $(\operatorname{Frac} B)[X]$.

Vu l'énoncé à montrer, on peut donc supposer $Q = P$, *i. e.* P est primitif.

Raisonnons par contraposée. On suppose qu'il existe deux polynômes non constants $Q, R \in (\operatorname{Frac} A)[X]$ tels que $P = QR$. D'après le lemme, quitte à remplacer Q et R par des éléments associés, on peut supposer que ce sont des éléments de $A[X]$. Alors $\varphi(P) = \varphi(Q)\varphi(R)$, donc $\deg \varphi(P) = \deg \varphi(Q) + \deg \varphi(R)$, donc

$$\deg P + \deg Q = \deg \varphi(P) + \deg \varphi(Q).$$

Comme φ ne peut que diminuer le degré, les polynômes $\varphi(Q)$ et $\varphi(R)$ sont non constant, ce qui montre que le polynôme $\varphi(P)$ n'est pas irréductible dans $(\operatorname{Frac} B)[X]$. □

THÉORÈME 5.36 *(critère d'EISENSTEIN).* Soient $n \geqslant 1$ un entier et $P \coloneqq \sum_{i=0}^{n} a_i X^i \in A[X]$ un polynôme de degré n. On suppose que, pour tout $i \in [\![0, n-1]\!]$, on a $\pi \mid a_i$ et $\pi^2 \nmid a_0$. Alors P est irréductible dans $(\operatorname{Frac} A)[X]$.

Preuve On considère le polynôme primitif $Q \coloneqq P/c(P) \in A[X]$. Il suffit de montrer qu'il est irréductible dans $(\operatorname{Frac} A)[X]$. Par hypothèse, l'élément π ne divise pas $c(P)$. Ainsi le polynôme Q vérifie les mêmes hypothèses que P vis-à-vis des valuations π-adiques des coefficients.

Par le lemme précédent, il suffit de montrer qu'une écriture $Q = RS$ avec $R, S \in A[X]$ entraîne qu'un des deux polynômes R ou S est constant. Soient $R, S \in A[X]$ tels que $Q = RS$. Par hypothèse, il existe $\alpha \in B \setminus \{0\}$ tel que $\varphi(P) = \alpha X^n$. Par ailleurs, on a $\varphi(P) = \varphi(R)\varphi(S)$. Comme π est irréductible, l'anneau B est intègre, donc il existe $m, r \in [\![0, n]\!]$ avec $m + r = n$ tels que $\varphi(R) = \beta X^m$ et $\varphi(S) = \alpha X^r$. Si $(m, r) \neq 0$, alors π divise $R(0)$ et $S(0)$, donc φ^2 divise $R(0)S(0) = P(0) = a_0$ ce qui est impossible. Ainsi, on a $m = n$ et $r = 0$ par exemple. Comme $\deg R \geqslant m = n$ et $\deg S \geqslant r = 0$ avec $\deg R + \deg S = n$, on a $\deg R = n$ et $\deg S = 0$, donc le polynôme S est constant ce qu'on voulait démontrer. □

▷ EXEMPLES. – Soient p un nombre premier et $n \geqslant 1$ un entier. Le polynôme $X^n - p$ est irréductible dans $\mathbb{Q}[X]$. En effet, il suffit d'appliquer le théorème d'EISENSTEIN avec $\pi = p$. Ainsi il existe des polynômes irréductibles de tout degré dans $\mathbb{Q}[X]$.

– Soient $n \geqslant 1$ un entier et $P \in \mathbb{K}[Y]$ tel que $P(0) \neq 0$. En appliquant le critère d'EISENSTEIN avec $A = \mathbb{K}[Y]$ et $\pi = Y$, le polynôme $X^n - YP(Y)$ est irréductible dans $(\operatorname{Frac} A)[X] \supset \mathbb{K}[X, Y]$

5.7 Démonstration des théorèmes

5.7.1 Tout anneau factoriel vérifie les lemmes de Gauss

On veut démontrer le théorème 5.8 qui énonce qu'un anneau factoriel vérifie le lemme de GAUSS. Pour cela, démontrons le résultat suivant, un peu plus général.

THÉORÈME 5.37. Soit A un anneau intègre. On suppose que tout élément de A non nul et non inversibles s'écrit comme un produit d'éléments irréductibles de A. Alors les propositions suivantes sont équivalentes :

(i) l'anneau A est factoriel ;
(ii) il vérifie le lemme de GAUSS ;
(iii) il vérifie le lemme d'EUCLIDE.

Preuve L'implication (ii) ⇒ (iii) a déjà été montré.

• *(i) ⇒ (ii).* On suppose que A est factoriel. Soient $a, b, c \in A$ tels que a divise bc et a et b soient premiers entre eux. Montrons que a divise c. Le résultat est immédiat si a est nul ou inversible. Soit $\pi \in \mathscr{I}(A)$. Il suffit de montrer que $v_\pi(a) \leqslant v_\pi(c)$. Distinguons deux cas.

– On suppose $v_\pi(b) > 0$. Comme les éléments a et b sont premiers entre eux et $v_\pi(1_A) = 0$, le théorème 5.18 assure $v_\pi(a) = 0 \leqslant v_\pi(c)$.
– On suppose $v_\pi(b) = 0$. Alors $v_\pi(bc) = v_\pi(b) + v_\pi(c) = v_\pi(c)$. Comme a divise bc, on a $v_\pi(a) \leqslant v_\pi(bc) = v_\pi(c)$.

Dans les deux cas, on a bien $v_\pi(a) \leqslant v_\pi(c)$ ce qui implique que a divise c. D'où le lemme de Gauss.

• *(iii) ⇒ (i).* On suppose que A vérifie le lemme d'Euclide. Il s'agit de montrer l'unicité de la décomposition en irréductibles à l'ordre et l'association près. Soient $\{p_i\}_{i\in I}$ et $\{q_i\}_{i\in I}$ deux familles finies d'éléments irréductibles de A telles que $\prod_{i\in I} p_i = \prod_{j\in J} q_i$. On veut montrer qu'il existe une bijection $\psi\colon I \to J$ telle que les éléments p_i et $q_{\psi(i)}$ soient associés pour tout $i \in I$.

Soit $A \subset I$ une partie maximale pour l'inclusion telle qu'il existe une bijection $\psi\colon A \to B$ telle que les éléments p_i et $q_{\psi(i)}$ soient associés pour tout $i \in A$. Raisonnons par l'absurde et supposons que $A \neq I$ ou $B \neq J$. Comme $\prod_{i\in A} p_i$ et $\prod_{j\in B} q_j$ sont associés et on a $\prod_{i\in I} p_i = \prod_{j\in J} q_i$, les éléments $\prod_{i\in I\setminus A} p_i$ et $\prod_{j\in J\setminus B} q_j$ sont associés. Distinguons trois cas.
– On suppose $A \neq I$ et $B = J$. Alors $\prod_{i\in I\setminus A} p_i$ est associés à 1_A, donc il est inversible. Cela implique que, pour tout $i \in I \setminus A$, l'élément p_i est inversible ce qui est impossible car ce sont des irréductibles.
– De même, on ne peut pas avoir $A = I$ et $B \neq J$.
– On suppose $A \neq I$ et $B \neq J$. Soit $i_0 \in A \setminus I$. Comme $\prod_{i\in I\setminus A} p_i$ divise $\prod_{j\in J\setminus B} q_j$, l'élément irréductible p_{i_0} divise $\prod_{j\in J\setminus B} q_j$. Comme le lemme d'Euclide est vérifié, il existe $j_0 \in J$ tel que p_{i_0} divise q_{j_0}. Comme les éléments p_{i_0} et q_{j_0} sont irréductibles, ils sont associés. On peut donc étendre l'application $\psi\colon A \to B$ en une bijection de $A \cup \{i_0\}$ dans $B \cup \{j_0\}$ en posant $\psi(i_0) = j_0$ce qui contredit la maximalité de A.
Ces trois cas sont donc impossibles. On en déduit $A = I$ et $B = J$ ce qui assure la conclusion. □

5.7.2 Tout anneau principal est factoriel

On va utiliser le théorème précédent pour montrer le point 2 du théorème 5.6, *i. e.* tout anneau principal est factoriel. On sait déjà que tout anneau principal vérifie le lemme d'Euclide. Il suffit alors de montrer que, dans un anneau principal, tout élément non nul et non inversible est un produit d'éléments irréductibles.

Soit A un anneau principal. Montrons d'abord que tout élément $a \in A$ non nul et non inversible est divisible par un élément irréductible de A. Comme a est non inversible, l'idéal aA est propre et il est donc contenu dans un idéal maximal $\mathfrak{M}$ de A. Comme A est principal, il existe $\pi \in A$ tel que $\mathfrak{M} = \pi A$. Comme l'idéal $\mathfrak{M}$ est maximal contenant $a \neq 0_A$, il est premier et non nul, donc π est irréductible. Comme $aA \subset \pi A$, l'élément π divise a.

Lemme 5.38. Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. Alors elle est stationnaire, *i. e.* il existe $n \in \mathbb{N}$ tel que

$$\forall m \geqslant n, \quad I_m = I_n.$$

Preuve Comme A est principal, pour tout $n \in \mathbb{N}$, il existe $a_n \in A$ tel que $I_n = a_n A$. Par ailleurs, comme la suite est croissante, on peut montrer que l'ensemble $I \coloneqq \bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A, donc il existe $a \in A$ tel que $I = aA$. En particulier, on a $a \in I$, donc il existe $n \in \mathbb{N}$ tel que $a \in I_n$. Montrons que $I_m = I$ pour tout $m \geqslant n$ ce qui conclura. Soit $m \geqslant n$. Comme la suite est croissante, on a $b \in I_m = a_m A$. Comme I est l'idéal engendre par b, on obtient $I \subset I_m$. L'autre inclusion étant évidente, on a $I_m = I$. □

Reprenons la preuve du théorème. Soit $a \in A$ un élément non nul et non inversible. D'après le résultat précédent, il existe un élément irréductible $\pi_1 \in A$ tel que π_1 divise a. On pose $a_1 \coloneqq a/\pi_1 \in A \setminus \{0_A\}$. Si a_1 est inversible, alors a est irréductible et on a terminé. Sinon il existe un élément irréductible $\pi_2 \in A$ divisant a_1. Si $a_2 \coloneqq a_1/\pi_2$ est inversible, on a terminé. Sinon on recommence le procédé… Il s'agit de voir que ce procédé se termine nécessairement.

Pour récurrence, construisons deux suites $(\pi_n)_{n\geqslant 1}$ et $(a_n)_{n\geqslant 0}$ de A telle que $a_0 = a$ et, pour tout $n \geqslant 1$, l'élément π_n est irréductible ou vaut 1_A et

$$a = a_n \pi_1 \cdots \pi_n \quad \text{et} \quad a_{n+1}\pi_{n+1} = a_n.$$

On construit le couple (a_1, π_1) comme indique ci-dessus. Soit $n \geqslant 1$. Supposons qu'une telle suite $(a_i, \pi_i)_{i\leqslant n}$ soit construite. Si a_n est inversible, on pose $\pi_{n+1} \coloneqq 1_A$ et $a_{n+1} \coloneqq a_n s$ Sinon il existe un élément irréductible $\pi_{n+1} \in A$ divisant a_n et on pose $a_{n+1} \coloneqq a_n/\pi_{n+1}$.

Montrons que la suite $(a_n, \pi_n)_{n\geqslant 0}$ est stationnaire. Pour $n \geqslant 0$, on pose $I_n \coloneqq a_n A$. Alors pour tout $n \geqslant 0$, comme $a_{n+1}\pi_{n+1} = a_n$, on a $a_n \in a_{n+1}A$, donc $I_n \subset I_{n+1}$. La suite $(I_n)_{n\geqslant 0}$ est donc croissante. D'après le lemme, il existe $n \geqslant 0$ tel que $I_n = I_{n+1}$. Les éléments a_n et a_{n+1} sont donc associés. Comme $a_{n+1}\pi_{n+1} = a_n$ et un élément irréductible ne peut être inversible, l'élément π_{n+1} n'est pas irréductible. Ceci montre que l'élément a_n est inversible. Finalement, on a $a = a_n\pi_1 \cdots \pi_n$ où les éléments π_1, …, φ_n sont irréductibles et l'élément a_n est inversible ce qui achève la preuve.

5.7.3 Tout anneau factoriel vérifiant le théorème de Bézout est principal

Soit A un anneau factoriel vérifiant le théorème de Bézout. Comme A est factoriel, il est intègre. Il reste à montrer que tout idéal de A est principal.

Commençons par montre que tout idéal de A engendré par un nombre fini d'éléments est principal. Il suffit de le faire pour deux éléments, une récurrence immédiate montre le résultat. Soient $a, b \in A$. On note $I \coloneqq \langle a, b\rangle$. Si $a = b = 0_A$, alors $I = 0_A$. On suppose $a \neq 0_A$ et $b \neq 0_A$. Alors les éléments a et b admettent un PGCD non nul $\delta \in A$. Montrons que $I = \delta A$. Comme δ divise a et b, on a $aA \subset \delta A$ et $bA \subset \delta A$, donc $I = aA + bB \subset \delta A$. Réciproquement, les éléments $\alpha \coloneqq a/\delta$ et $\beta \coloneqq b/\delta$ sont premiers entre eux, donc le théorème de Bézout donne $\alpha A + \beta A = A$. En particulier, il existe $u, v \in A$ tel que $\alpha u + \beta v = 1_A$. En multipliant cette relation par δ, on obtient $\delta \in aA + bA$, donc $\delta A \subset I$. D'où $I = \delta A$.

Lemme 5.39. Dans un anneau factoriel, toute suite croissante d'idéaux principaux est stationnaire.

Preuve Soit $(a_n)_{n\geqslant 0}$ une suite de A telle que $(a_nA)_{n\geqslant 0}$ soit croissante, *i. e.* telle que a_{n+1} divise a_n pour $n \geqslant 0$. Alors pour tout élément irréductible $\pi \in A$, la suite $(v_\pi(a_n))_{n\geqslant 0}$ est une suite d'entiers décroissante, donc elle est stationnaire. Par ailleurs, pour tout élément irréductible $\pi \in A$ ne divisant pas a_0, la suite $(v_\pi(a_n))_{n\geqslant 0}$ est nulle. Comme a_0 n'a qu'un nombre fini de diviseurs, on en déduit qu'il existe $N_0 \geqslant 0$ tel que, pour tout élément irréductible $\pi \in A$, la suite $(v_\pi(a_n))_{n\geqslant N_0}$ est constante égale à un certain élément $\nu_\pi \in A$. On pose

$$a \coloneqq \prod_{\pi\in\mathscr{I}(A)} \pi^{\nu_\pi} \in A.$$

Pour tout $n \geqslant N_0$, les éléments a_n et a ont les mêmes valuations adiques, donc ils sont associés ce qui assure l'égalité $a_nA = aA$. □

Montrons enfin que tout idéal de A est principal. Soit I un idéal de A. Construisons, par récurrence, une suite d'idéaux $(I_n)_{n\geqslant 0}$ contenus dans I. Soit $a_0 \in I$. On pose $I_0 \coloneqq a_0A$. Soit $n \geqslant 0$. On suppose que l'on a construit l'idéal I_n. Si ce dernier vaut I, on pose $I_{n+1} \coloneqq I$. Sinon on pose $I_{n+1} \coloneqq I_n + a_{n+1}A \supsetneq I$ avec $a_{n+1} \in I \setminus I_n$.

La suite ainsi construite est croissante et on montre facilement que les idéaux I_n sont engendrés par un nombre fini d'éléments et, par conséquent, sont principal. Par le lemme, cette suite est stationnaire. Par construction, elle ne peut qu'être stationnaire égale à I ce qui montre la principalité de I.

Récapitulatif. Pour un anneau intègre A, le schéma suivant résume les implications et équivalences entre les diverses notions et propriétés que vérifie A de ce chapitre.

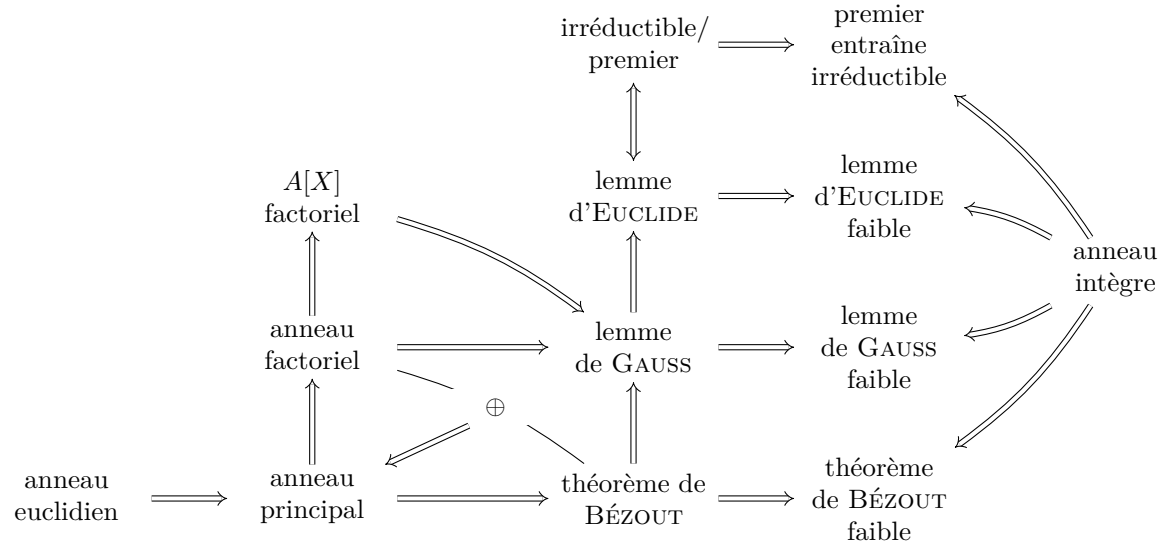

Figure 5.1 – Récapitulatif