Université de Rennes 1

ANAR

ANNEAUX & ARITHMÉTIQUE

Propriétés élémentaires des anneaux commutatifs unitaires, anneaux des polynômes, idéaux, étude de $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{K}[X]/P\mathbb{K}[X]$, classification des corps finis, localisation, corps des fractions, anneaux euclidiens, principaux, et factoriels.

Auteur
David Bourqui

Notes de cours
Victor Lecerf

2020–2021

Table des matières

Chapitre 1

Notions de base des théories des anneaux

1.1 Définitions, notations, règles de calcul

1.1.1 Définition d'un anneau (unitaire, commutatif)

Définition 1.1.1. *Un anneau est un triplet $(A, *, \perp)$ où A est un ensemble (dit sous-jacent de l'anneau), et $*$ et $\perp$ sont deux lois de composition interne sur A telles que*

(i) *$(A, *)$ est un groupe abélien,*

(ii) *La loi $\perp$ est distributive par rapport à la loi $*$, i.e*

$$\forall (a,b,c) \in A^3,\ a \perp (b * c) = (a * b) \perp (a * c),$$
$$\forall (a,b,c) \in A^3,\ (a * b) \perp c = (a * c) \perp (b * c).$$

(iii) *La loi $\perp$ possède un élément neutre et est associative.*
L'anneau $(A, *, \perp)$ est dit commutatif si la loi $\perp$ l'est.

1.2 Sous-anneaux d'un anneau

Définition 1.2.1. *Soit $(A, +, \times)$ un anneau et soit $B \subset A$ une partie non vide. On dit que $(B, +, \times)$ est un sous-anneau de $(A, +, \times)$ si la restriction des lois de composition à B^2 induit une structure d'anneau sur B, i.e*

— *$(B, +)$ est un sous-groupe de $(A, +)$,*

— *Pour tout $x, y \in B$, $x \times y \in B$,*

— *B contient 1_A.*

Exemples.

— Pour tout anneau A, $\{n1_A \,|\, n \in \mathbb{Z}\}$ est un sous-anneau de A.

— Soit $n \in \mathbb{N}$. On considère la chaîne d'inclusion

$$\mathbb{Z} \subset \mathbb{Z}[1/n] \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{C}[X].$$

Ici, toute inclusion de la forme $A \subset B$ extraite de cette chaîne fait de A un sous-anneau de B.

— Soit I un intervalle ouvert de $\mathbb{R}$. L'ensemble $\mathbb{R}^I$ des applications de I dans $\mathbb{R}$ est naturellement muni d'une structure d'anneau. Alors, $\mathcal{C}^k(I, \mathbb{R})$ est un sous-anneau de $\mathbb{R}^I$ pour tout $k \in \mathbb{N} \cup \{\infty\}$.

Remarque. Comme en théorie des groupes, on montrera qu'un ensemble est un anneau en montrant que c'est le sous-anneau d'un anneau déjà connu.

Proposition 1.2.1. *Une intersection quelconque de sous-anneaux est un anneau.*

Remarque. On peut alors définir le sous-anneau engendré par une partie. Soit A un anneau, et S une partie de A. On définit B le sous-anneau engendré par S comme le plus petit sous-anneau de A contenant S. C'est l'intersection de tous les anneaux contenant S.

1.3 Groupe des éléments inversibles d'un anneau

Définition 1.3.1. *Soit A un anneau commutatif et $a \in A$. L'élément a est dit inversible s'il existe $b \in A$ tel que $a \times b = b \times a = 1_A$. On note $A^\times$ l'ensemble des éléments inversibles de A pour la seconde loi.*

Proposition 1.3.1. *Soit $(A, +, \times)$ un anneau. L'ensemble $A^\times$ muni de la loi $\times$ est un groupe. Entre autres, pour $a, b \in A^\times$, ab est inversible, d'inverse $(ab)^{-1} = b^{-1}a^{-1}$. Si de plus A est un anneau commutatif, alors $(A^\times, \times)$ est abélien.*

Exemples. $\mathbb{Z}^\times = \{-1, 1\}, \mathbb{R}^\times = \mathbb{R}^*, \mathbb{R}[X]^\times = \mathbb{R}^*$. Plus généralement, pour tout anneau intègre A, on a $A[X]^\times = A^\times$. Si A n'est pas intègre, on a l'inclusion (généralement stricte) $A^\times \subset A[X]^\times$.

1.4 Morphisme d'anneaux, noyau, image, idéal

Définition 1.4.1. *Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ des anneaux. On appelle **morphisme d'anneaux** toute application $\varphi : A \longrightarrow B$ telle que*

— *$\varphi : (A, +_A) \longrightarrow (B, +_B)$ est un morphisme de groupes.*

— *Pour tout $x, y \in A$, $\varphi(x \times_A y) = \varphi(x) \times_B \varphi(y)$,*

— *$\varphi(1_A) = 1_B$.*

Remarques.

— La dernière condition permet d'éviter le "morphisme nul". Entre autres, pour tout anneau A non nul, il n'existe pas de morphisme de l'anneau nul vers A. Contrairement aux groupes, il n'existe pas toujours de morphisme entre deux anneaux.

— Il n'existe aucun morphisme d'anneau de $\mathbb{Q}$ vers $\mathbb{Z}$. Plus généralement, il n'existe aucun morphisme d'anneau d'un corps quelconque vers $\mathbb{Z}$.

Proposition 1.4.1. *Soient A, B des anneaux et $\varphi : A \longrightarrow B$ un morphisme d'anneaux.*

(i) Pour tout sous-anneau $\mathcal{A}$ de A, $\varphi(\mathcal{A})$ est un sous-anneau de B.

(ii) Pour tout sous-anneau $\mathcal{B}$ de B, $\varphi^{-1}(\mathcal{B})$ est un sous-anneau de A.

Exemples.

— Si A est un anneau, et B un sous-anneau de A, alors l'application d'inclusion $B \to A$, $x \mapsto x$ est un morphisme d'anneau injectif.

— La conjugaison sur $\mathbb{C}$ est un morphisme d'anneau.

— Pour tout anneau A, id_A est un morphisme d'anneau.

— Soit A un anneau. Pour tout $a \in A$, l'application $A[X] \to A$, $P \mapsto P(a)$ est un morphisme d'anneau (appelé morphisme d'évaluation en a).

Définition 1.4.2 (noyau)**.** *Soient A et B des anneaux, et φ un morphisme d'anneaux. On note* $\ker(\varphi)$ *le noyau de φ en tant que morphisme de groupes entre A et B pour leur première loi de composition :*

$$\ker \varphi = \varphi^{-1}(0_B) = \{a \in A \,|\, \varphi(a) = 0_B\}.$$

Proposition 1.4.2. *Soient A, B des anneaux, et $\varphi : A \longrightarrow B$ des morphismes d'anneaux.*

— *φ est injectif si et seulement si* $\ker \varphi = \{0_A\}$.

— *Pour tout $a \in A$ et $n \in \mathbb{Z}$, $\varphi(na) = n\varphi(a)$ et $\varphi(a^n) = \varphi(a)^n$.*

— *Si φ est bijectif, alors l'application φ^{-1} est aussi un morphisme d'anneaux.*

— *Soit C un anneau et $\psi : B \longrightarrow C$ un morphisme d'anneaux. Alors, l'application $\psi \circ \varphi : A \longrightarrow C$ est un morphisme d'anneau.*

— *On a $\varphi(A^\times) \subset B^\times$. L'application coinduite $A^\times \to B^\times$, $x \mapsto \varphi(x)$ est un morphisme de groupes.*

Théorème 1.4.1. *Soit A un anneau. L'application $\varphi_A : \mathbb{Z} \to A$, $n \mapsto n \cdot 1_A$ est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans A.*

Démonstration. Soit $\varphi : \mathbb{Z} \longrightarrow A$ un morphisme d'anneaux. On a pour tout $n \in \mathbb{Z}$, $\varphi(n) = n\varphi(1_\mathbb{Z}) = n \cdot 1_A = \varphi_A(n)$. Il suffit alors de montrer que φ_A est bien un morphisme d'anneaux. □

Définition 1.4.3. *Soient A, B des anneaux, et $\varphi : A \longrightarrow B$ un morphisme d'anneaux. L'application φ est dit être un* ***isomorphisme*** *si elle est* ***bijective****. Deux anneaux sont dits* ***isomorphes*** *s'il existe un isomorphisme de l'un dans l'autre.*

Remarque. En théorie des groupes, le noyau est un sous-groupe du groupe de départ. Cependant, en théorie des anneaux, le noyau est un sous-groupe du groupe sous-jacent mais est rarement un sous-anneau de l'anneau de départ. Cependant, il existe bien une structure au noyau.

Définition 1.4.4 (idéal)**.** *Soit A un anneau commutatif. Un idéal de A est une partie I de A qui est un sous-groupe de $(A, +)$ et qui est tel que :*

$$\forall a \in A, \forall x \in \mathcal{I}, ax \in \mathcal{I}.$$

Remarque. À partir de maintenant, toutes les propositions concernant les idéaux d'un anneau commutatif ne feront plus mention de la commutativité des anneaux manipulés. En effet, lorsque l'anneau n'est plus commutatif, on doit parler d'idéal à gauche, à droite, ou bilatère.

Proposition 1.4.3. *Soit A un anneau et $\mathcal{I}$ un idéal de A. Alors,*

$$\mathcal{I} = A \iff 1_A \in \mathcal{I} \iff A \cap \mathcal{I} \neq \varnothing.$$

Conséquence. Un corps $\mathbb{K}$ n'a pas d'idéal non trivial : ses seuls idéaux sont $\{0_\mathbb{K}\}$ et $\mathbb{K}$.

Proposition 1.4.4. *Soit A et B des anneaux. Alors,*

(i) Soit $\varphi : A \longrightarrow B$ un morphisme d'anneaux. Alors, pour tout idéal $\mathcal{J}$ de B, $\varphi^{-1}(\mathcal{J})$ est un idéal de A. En particulier, $\ker \varphi$ est un idéal de A.

(ii) Soit $\pi : A \longrightarrow B$ un morphisme d'anneaux surjectif. Alors, pour tout idéal I de A, $\pi(A)$ est un idéal de B. L'application $\mathcal{I} \longmapsto \pi(\mathcal{I})$ est une bijection de l'ensemble des idéaux de A vers l'ensemble de ceux de B, de réciproque $\mathcal{J} \longmapsto \pi^{-1}(\mathcal{J})$.

Proposition 1.4.5. *Soit A un anneau commutatif, et S une partie de A. Il existe un unique plus petit idéal de A contenant S, noté $\langle A \rangle$ (ou $S \cdot A$). C'est l'intersection de tous les idéaux de A contenant S.*

Définition 1.4.5. *Soit A un anneau, et $\mathcal{I}$ et $\mathcal{J}$ des idéaux de A. On définit la somme $\mathcal{I}+\mathcal{J}$ de ces idéaux par l'ensemble*

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

On définit de même le produit $\mathcal{I}\cdot\mathcal{J}$ par

$$\mathcal{I}\cdot\mathcal{J}=\left\{\sum_{k\in F}a_kb_k\;\middle|\;(a_k,b_k)_{k\in K}\in(\mathcal{I}\times\mathcal{J})^K,\,K\subset\mathbb{N}\text{ fini}\right\}.$$

Plus généralement, on définit pour $(\mathcal{I}_e)_{e\in E}$ une famille d'idéaux indexé par un ensemble E l'ensemble

$$\sum_{e\in E}\mathcal{I}_e=\left\{\sum_{e\in E}a_e\;\middle|\;(a_e)_e\in I^{(E)}\right\}$$

où $I^{(E)}$ désigne l'ensemble des suites à support fini indexées par E à valeurs dans I. Enfin, on définit le produit fini d'idéaux pour $\mathcal{I}_1,\,\ldots,\mathcal{I}_n$ des idéaux de A par

$$\mathcal{I}_1\cdots\mathcal{I}_n=\left\langle\left\{\prod_{k=1}^{n}x_i\;\middle|\;(x_1,\ldots,x_n)\in\prod_{k=1}^{n}\mathcal{I}_k\right\}\right\rangle.$$

Remarque. Le produit d'idéaux est associatif, d'où la notation dans la définition.

Proposition 1.4.6. *Dans un anneau commutatif : l'intersection, la somme finie, ainsi que le produit fini d'idéaux, sont des idéaux.*

Remarque. La somme d'idéaux est un peu particulière. Par exemple, pour tout idéal $\mathcal{I}$ d'un anneau commutatif, $\mathcal{I}+\mathcal{I}=\mathcal{I}$. On peut aussi noter l'égalité $2\mathbb{Z}+3\mathbb{Z}=5\mathbb{Z}$.

Proposition 1.4.7. *Soit A un anneau commutatif, et S une partie de A. Alors,*

(i) On a

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

Cela signifie que $\langle S\rangle$ est l'ensemble des combinaisons linéaires à coefficients dans A des éléments de S.

(ii) Pour $S,T\in\mathcal{P}(A)$, on a

$$\langle S\rangle+\langle T\rangle=\langle S\cup T\rangle,$$

et

$$\langle S\rangle\langle T\rangle=\big\langle\{st\,|\,(s,t)\in S\times T\}\big\rangle.$$

Définition 1.4.6. *Soit A un anneau commutatif. Soit $\mathcal{I}$ un idéal de A.*

— *$\mathcal{I}$ est dit **premier** si :*

$$(\mathcal{I} \neq A) \wedge \Big(\forall x, y \in A,\, (xy \in \mathcal{I}) \implies \big((x \in \mathcal{I}) \wedge (y \in \mathcal{I})\big)\Big).$$

— *$\mathcal{I}$ est dit maximal s'il est propre ($\mathcal{I} \neq A$) et que pour tout idéal $\mathcal{J}$ de A, alors*

$$(\mathcal{I} \subset \mathcal{J}) \implies (\mathcal{J} \in \{\mathcal{I}, A\}).$$

Remarque. Un idéal $\mathcal{I}$ de A est dit *propre* lorsque $\mathcal{I} \neq A$. Ainsi défini, A en tant qu'idéal n'est ni premier ni maximal (ce qui évite que certains théorèmes soient triviaux).

Le lemme suivant anticipe un peu sur les notions d'anneau intègre, de corps, et de quotient d'un anneau par un idéal. [1]

Lemme 1.4.1. *Soit A un anneau et $\mathcal{I}$ un idéal de A, avec $\mathcal{I} \neq A$. Alors,*

(i) $\mathcal{I}$ est un idéal premier si et seulement si $A/\mathcal{I}$ est intègre,

(ii) $\mathcal{I}$ est un idéal maximal si et seulement si $A/\mathcal{I}$ est un corps.

Démonstration. Voir Gourdon, *Algèbre.*

□

Proposition 1.4.8. *Un idéal maximal est premier.*

Démonstration. Soit $\mathcal{I}$ un idéal maximal d'un anneau commutatif A. Alors $A/\mathcal{I}$ est un corps et est donc intègre. On en déduit que $\mathcal{I}$ est premier.

□

Théorème 1.4.2 (Krull)**.** *L'axiome du choix est vrai si et seulement si tout idéal d'un anneau commutatif est inclus dans un idéal maximal.*

Remarque. Axiome du choix considéré, tout anneau commutatif possède un idéal premier.

Démonstration. Hors-programme.

□

Proposition 1.4.9. *Soient A, B des anneaux commutatifs, $\varphi : A \longrightarrow B$ un morphisme d'anneaux, et $\mathcal{J}$ un idéal premier de B. Alors, $\varphi^{-1}(\mathcal{J})$ est un idéal premier de A.*

1. mais je suis sûr que ça ne vous dérangera pas.

Proposition 1.4.10. *On a les résultats suivants sur les idéaux de $\mathbb{Z}$.*

(i) Les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

(ii) Soit $n, m \in \mathbb{Z}$. Alors,

$$(n\mathbb{Z} \subset m\mathbb{Z}) \iff (m|n).$$

En particulier, $n\mathbb{Z} = m\mathbb{Z}$ si et seulement si $|n| = |m|$.

(iii) Un idéal de $\mathbb{Z}$ est premier si et seulement si il est nul, ou engendré par un nombre premier.

(iv) Un idéal de $\mathbb{Z}$ est maximal si et seulement si il est engendré par un nombre premier.

Remarque. Le premier point se résume à dire que $\mathbb{Z}$ est principal : tous ses idéaux sont principaux, *i.e* engendrés par un seul élément chacun.

Définition 1.4.7 (caractéristique)**.** *Soit A un anneau, et $\varphi_A : \mathbb{Z} \longrightarrow \mathbb{Z}$ l'unique morphisme d'anneaux de A vers $\mathbb{Z}$. On appelle* $\mathrm{car}(A)$ *l'unique entier naturel tel que* $\ker \varphi_A = \mathrm{car}(A)\mathbb{Z}$.

Exemples.

— $\mathrm{car}\,(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) = 4$.

— La caractéristique d'un anneau intègre est soit nulle, soit un nombre premier.

Proposition 1.4.11. *Soit $\mathbb{K}$ un corps commutatif. On a les résultats suivants.*

(i) $\mathbb{K}[X]$ est un anneau principal.

(ii) Soit $P, Q \in \mathbb{K}[X]$. L'inclusion $P\mathbb{K}[X] \subset Q\mathbb{K}[X]$ est vérifiée si et seulement s'il existe $\alpha \in \mathbb{K}^\times$ tel que $P = \alpha Q$.

(iii) Un idéal de $\mathbb{K}[X]$ est premier si et seulement s'il est nul, ou engendré par un polynôme irréductible.

(iv) Un idéal de $\mathbb{K}[X]$ est maximal si et seulement s'il est engendré par un polynôme irréductible.

1.5 Produits, polynômes, séries formelles

1.5.1 Anneau produit

Définition 1.5.1 (anneau produit)**.** *Soit I un ensemble d'indices et $(A_i)_{i\in I}$ une famille d'anneaux (on note leurs lois de compositions identiquement). Alors, on peut munir le produit cartésien $A = \prod_{i\in I} A_i$ d'une structure d'anneaux naturelle via les lois de compositions définies pour tout $a = (a_i)_i$ et $b = (b_i)_i \in A$ par*

$$a + b = (a_i + b_i)_{i\in I} \quad et \quad a \times b = (a_i \times b_i)_{i\in I}.$$

Proposition 1.5.1 (inversibles d'un anneau produit)**.** *En conservant la même quantification qu'à la définition précédente, on a*

$$\left(\prod_{i\in I} A_i\right)^\times = \prod_{i\in I} A_i^\times.$$

Proposition 1.5.2. *En reprenant encore les mêmes notations et si pour tout $i \in I$, $\pi_i : A \longrightarrow A_i$ désigne la projection sur la i-ème coordonnée, on a les deux résultats suivants.*

- *Pour tout $i \in I$, la projection $\pi_i : A_i \longrightarrow A$ est un morphisme d'anneau.*
- *Si B est anneau, alors l'application*

$$\begin{array}{ccc} \mathrm{Hom}\left(B, \prod_{i\in I} A_i\right) & \longrightarrow & \prod_{i\in I} \mathrm{Hom}(B, A_i) \\ \varphi & \longmapsto & (\pi_i \circ \varphi)_{i\in I} \end{array}$$

est une bijection.

Moralement, se donner un morphisme vers un produit d'anneaux, c'est se donner un morphisme vers chacune des composantes du produit.

Définition 1.5.2 (anneau d'applications)**.** *Soit E un ensemble et A un anneau. On peut munir A^E d'une structure naturelle d'anneau en définissant les lois de compositions internes (notées identiquement à celle de A) par*

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x) \quad \text{et} \quad (\varphi \times \psi)(x) = \varphi(x) \times \psi(x),$$

pour tout $x \in E$, et $\varphi, \psi \in A^E$.

1.5.2 Anneau des polynômes en une indéterminée

Définition 1.5.3 (somme pseudo-finie)**.** *Soit A un anneau et $(a_n)_n \in A^{\mathbb{N}}$ une suite à support fini (ou presque nulle) d'éléments de A. Soit $N \in \mathbb{N}$ tel que pour tout $n > N$, $a_n = 0$. On pose alors*

$$\sum_{n=0}^{\infty} a_n = \sum_{n=0}^{N} a_n.$$

Remarque. Cette notation est bien évidemment indépendante du choix de N.

Définition 1.5.4 (polynômes et séries formelles en une indéterminée)**.** *Soit A un anneau.*

(i) On appelle ***indéterminée*** *l'élément $X = (\delta_{1,n} \cdot 1_A)_{n\in\mathbb{N}}$*

(ii) On appelle ***anneau des séries formelles en une indéterminée à coefficients dans*** *A l'ensemble $A^{\mathbb{N}}$ munit de l'addition terme à terme, et de la multiplication définie pour tout $a, b \in A^{\mathbb{N}}$ par*

$$a \times b = \left(\sum_{k=0}^{n} a_k b_{n-k} \right)_{n\in\mathbb{N}}.$$

Cet anneau est noté $A[[X]]$.

(iii) On appelle ***anneau des polynômes en une indéterminée à coefficients dans*** *A le sous-anneau $A^{(\mathbb{N})}$ de $A^{\mathbb{N}}$. Cet anneau est noté $A[X]$.*

(iv) L'anneau $A[[X]]$ constitue un prolongement de A, via l'injection $a \longmapsto (\delta_{0,n} \cdot a)_{n\in\mathbb{N}}$ (qui est un isomorphisme d'anneaux entre A et son image).

(v) Pour tout $k \in \mathbb{N}$, on a $X^k = (\delta_{k,n} \cdot 1_A)_{n\in\mathbb{N}}$, ce qui motive la notation

$$a = \sum_{k=0}^{\infty} a_k X^k$$

pour tout $a \in A[[X]]$. Si de plus a est à support fini, alors on peut noter

$$a = \sum_{k=0}^{N} a_k X^k$$

pour $N \in \mathbb{N}$ tel que $a_n = 0$ pour tout $n > N$.

Remarques.

— Le choix de la lettre X est totalement arbitraire. On pourra trouver par exemple la lettre T dans le *cours d'algèbre* de Daniel Perrin.

— Les éléments de $A[X]$ (*resp.* $A[[X]]$) sont appelés *polynômes* (*resp. séries formelles*). Pour toute suite $\sum_{n=0}^{\infty} a_n$ est une série formelle, la suite $(a_n)_n$ est appelée la *suite des coefficients* de cette série formelle.

Convention. Dans les paragraphes suivants nous introduirons dans $\mathbb{N}$ l'élément $-\infty$. On prolonge l'ordre naturel sur $\mathbb{N}$ par les relations

$$-\infty \leq n \quad , \quad -\infty + n = -\infty \quad , \quad -\infty \times n = -\infty,$$

pour tout $n \in \mathbb{N}$. On rappelle par ailleurs que $\sup \varnothing = -\infty$ dans $\overline{\mathbb{R}}$.

Définition 1.5.5 (degré d'un polynôme)**.** *Soit A un anneau, et $P \in A[X]$ un polynôme noté $P = \sum_{n=0}^{\infty} a_n X^n$, où $(a_n)_n$ est une suite à support fini d'éléments de A. On appelle degré de P, noté* $\deg(P)$*, la quantité*

$$\sup\{n \in \mathbb{N} \,|\, a_n \neq 0_A\} \in \mathbb{N} \cup \{-\infty\}.$$

On appelle alors coefficient dominant de P l'élément $a_{\deg(P)}$.

Proposition 1.5.3. *Soit A un anneau. On a sur $A[X]$ les résultats suivants.*

(i) Soit $P \in A[X]$,

$$\deg P = -\infty \iff P = 0.$$

(ii) Pour $P, Q \in A[X]$. Alors :

- $\deg(P+Q) \leq \min(\deg P, \deg Q)$, *avec égalité si* $\deg P \neq \deg Q$.
- $\deg(PQ) \leq \deg P + \deg Q$, *avec égalité si le coefficient dominant de P ou de Q n'est pas diviseur de zéro.*
- *Si A est un anneau intègre, $A[X]$ l'est aussi.*
- *Morphisme d'évaluation. Soit $a \in A$. L'application*

$$\begin{array}{ccc} A[X] & \longrightarrow & A \\ \displaystyle\sum_{n=0}^{\infty} b_n X^n & \longmapsto & \displaystyle\sum_{n=0}^{\infty} b_n a^n \end{array}$$

est bien définie et est un morphisme d'anneau, appelé morphisme d'évaluation (en a).

Définition 1.5.6 (valuation d'une série formelle)**.** *Soit $P \in A[[X]]$ une série formelle notée $P = \sum_{n=0}^{\infty} a_n X^n$ avec $(a_n)_n \in A^{\mathbb{N}}$. On appelle* ***valuation de*** *P, notée $\nu(P)$, la quantité*

$$\inf\{n \in \mathbb{N} \,|\, a_n \neq 0\} \in \mathbb{N}/$$

Si $\nu(P) < \infty$, on appelle ***composante angulaire*** *l'élément $a_{\nu(P)} \in A$.*

Proposition 1.5.4. *Soit A un anneau commutatif.*

(i) Pour tout $P \in A[[X]]$, $\nu(P) = \infty$ si et seulement si $P = 0$.

(ii) Soient P et $Q \in A[[X]]$. Alors,

- $\nu(P+Q) \geq \min(\nu(P), \nu(Q))$, *avec égalité si* $\nu(P) \neq \nu(Q)$.
- *On a*

$$\nu(PQ) \geq \nu(P)) + \nu(Q),$$

avec égalité si la composante angulaire de P (ou de Q) n'est pas diviseur de zéro (par exemple si elle est inversible, ou si elle est non nulle et A est intègre), ou si P ou Q est nul.

(iii) Si A est intègre, alors $A[[X]]$ aussi.

Démonstration. La démonstration de (iii) se fait en utilisant le résultat suivant : soit $P \in A[[X]]$ et $n \in \mathbb{N}$, alors,

$$(\nu(P) = n) \iff (\exists b \in A \backslash \{0_A\},\ \exists Q \in A[[X]],\ P = X^n(b + XQ)).$$

□

1.5.3 Division de polynômes

Proposition 1.5.5 (division euclidienne)**.** *Soit A un anneau commutatif. Soit $P_1, P_2 \in A[X]$. On suppose P_2 non nul, de coefficient dominant inversible. Alors, il existe un unique couple $(Q, R) \in A[X]^2$ tel que*

$$\begin{cases} P_1 = P_2 Q + R \\ \deg(R) < \deg(P_2) \end{cases}$$

Démonstration. — *Unicité.* Soient (Q_1, R_1) et (Q_2, R_2) deux couples vérifiant la propriété de l'énoncé. On Peut écrire $P_2(Q_1 - Q_2) = R_1 - R_2$. Par les conditions sur les degrés, on obtient $\deg(R_1 - R_2) < \deg(P_2)$. Or, puisque P_2 est de coefficient dominant inversible, on a

$$\deg(P_2) + \deg(Q_1 - Q_2) = \deg(P_2(Q_1 - Q_2)) < \deg(P_2)$$

(car le coefficient dominant n'est pas un diviseur de zéro, voir 1.5.3, *(ii)*). Cette inégalité stricte impose alors $Q_1 - Q_2 = 0$. De même, $0 = P_2(Q_1 - Q_2) = R_1 - R_2$.

— *Existence.*

On fixe $P_2 \in A[X]$ un polynôme non nul, et de coefficient dominant inversible. Montrons par récurrence sur $n \in \mathbb{N}$ que, pour tout $n \in \mathbb{N}$, $\mathcal{P}(n)$: "Pour tout $P \in A_n[X]$, il existe un couple $(Q, R) \in A[X]^2$ tel que $P = QP_2 + R$, avec $\deg(R) < \deg(P_2)$" est vraie.

— *Initialisation.* Pour $n = 0$ (ou même $n < \deg(P_2)$), on prend $(Q, R) = (0, P)$.

— *Hérédité.* Soit $n \in \mathbb{N}^*$. On suppose $\mathcal{P}(n-1)$. Soit $P \in A[X]$ un polynôme de degré n. On note a le coeffcient dominant de P, et b celui de P_2. Soit alors

$$\widetilde{P} = P - ab^{-1}X^{n-\deg(P_2)}P_2.$$

En posant ceci, on élimine le monôme de plus haut degré de P. On a en fait $\deg(\widetilde{P}) < \deg(P)$. On applique l'hypothèse de récurrence sur $\widetilde{P}$: il existe (Q, R) un couple convenable de division euclidienne pour $\widetilde{P}$. Alors, $(Q + ab^{-1}X^{n-\deg(P_2)}, R)$ est un couple convenable pour P.

□

Remarques.

— La méthode utilisée pour l'hérédité dans cette démonstration est la base du calcul effectif de la division euclidienne.

— *Contre-exemple.* Dans $\mathbb{Z}[X]$, la division euclidienne de X par $2X$ n'existe pas, car 2 n'est pas inversible dans l'anneau $\mathbb{Z}$.

— Si $A = \mathbb{K}$ est un corps, l'hypothèse sur le coefficient dominant est toujours vérifiée. On peut alors montrer que $\mathbb{K}[X]$ est un anneau principal. Ce n'est pas toujours lorsque A n'est plus un corps. Par exemple, dans $\mathbb{Z}[X]$, l'idéal $\langle 2, X \rangle$ ne vérifie pas cette propriété.

Définition 1.5.7 (racine)**.** *Soit $P \in A[X]$. On appelle racine (ou zéro) de P (dans A) tout élément $a \in A$ tel que $P(a) = 0$.*

Corollaire 1.5.1. *Soit $P \in A[X]$, et $a \in A$. Alors, a est une racine de P si et seulement si $X - a$ divise P.*

Démonstration. Le sens réciproque est évident. Pour le sens direct, appliquer la division euclidienne.

□

Corollaire 1.5.2. *Soit A un anneau commutatif intègre, et $P \in A[X]$ un polynôme non nul. Alors, P a au plus $\deg(P)$ racines dans A. En particulier, si $A[X]$ a une infinité de racines dans A, alors $P = 0_{A[X]}$.*

Remarque. Si A n'est pas intègre, un polynôme unitaire peut avoir une *infinité* de racines A (voir l'exemple de $\mathbb{K}[X]/X^2$ dans le chapitre 3).

1.5.4 Propriété universelle

Théorème 1.5.1 (propriété universelle de l'anneaux des polynômes en une indéterminée)**.** *Soit A, B des anneaux commutatifs. Soit $i : A \longrightarrow A[X]$ le morphisme injectif naturel. L'application*

$$\begin{array}{rcl} \mathrm{Hom}(A[X], B) & \longrightarrow & \mathrm{Hom}(A, B) \times B \\ \varphi & \longmapsto & (\varphi \circ i, \varphi(X)) \end{array}$$

est bijective.

Remarques.

— Entre autres, un morphisme $A[X] \longrightarrow B$ est uniquement déterminée par l'image des polynômes constants et de l'image de l'indéterminée.

— Si $B = A$, pour tout $a \in A$, l'antécédent de (id_A, a) par l'application de l'énoncé est le morphisme d'évaluation en a.

Démonstration. Soit $(\psi, b) \in \mathrm{Hom}(A, B) \times B$. Soit

$$\theta(\psi, b) : \left| \begin{array}{rcl} A[X] & \longrightarrow & B \\ \displaystyle\sum_{n\in\mathbb{N}} a_n X^n & \longmapsto & \displaystyle\sum_{n\in\mathbb{N}} \psi(a_n) b^n \end{array} \right.$$

L'application $\theta(\psi, b)$ est un morphisme d'anneau. De plus, θ est l'application réciproque que celle de l'énoncé.

□

Définition 1.5.8. *Avec les mêmes quantifications et notations qu'à la proposition précédente, pour tout $\varphi \in \mathrm{Hom}(A, B)$ et $b \in B$, on note $\varphi(A)[b]$ (ou $A[b]$ lorsque φ est injectif et clairement indiquée dans le contexte) le sous-anneau de B image de $A[X]$ par le morphisme $\theta(\varphi, b)$.*

1.5.5 Anneau des polynômes en N indéterminées à coefficients dans A

Soit $N \geq 1$. On peut construire de deux façons l'anneau des polynômes $A[X_1, \ldots, X_N]$ en N indéterminées à coefficients dans A.

(i) On itère la construction précédente : $A[X_1, X_2] = (A[X_1])[X_2]$, $A[X_1, X_2, X_3] = (A[X_1, X_2])[X_3]$, *etc...*

(ii) On considère l'ensemble $A^{(\mathbb{N}^N)}$ l'ensemble des suites d'éléments de A à support fini indexées par $\mathbb{N}^N$. On définit une addition terme à terme et le produits de deux éléments a et $b \in A^{(\mathbb{N}^N)}$ par

$$a \times b = \left(\sum_{\substack{m,k \in \mathbb{N}^N \\ m+k=n}} a_m b_k \right)_{n \in \mathbb{N}^N}$$

Ces deux constructions conduisent à des anneaux isomorphes (et même à des A-algèbres isomorphes). Dans la seconde construction, on a pour tout $i \in [\![1, N]\!]$ que l'indéterminée X_i est l'élément de $A^{(\mathbb{N}^N)}$ nul en tout élément de $\mathbb{N}^N$, sauf en $n_i = (\delta_{i,j})_{1 \leq j \leq N} \in \mathbb{N}^N$, où il vaut 1_A. Alors, tout élément de $A[X_1, \ldots, X_N]$ s'écrit alors de manière unique sous la forme

$$\sum_{n \in \mathbb{N}^N} a_n \prod_{i=1}^{N} X_i^{n_i}.$$

où $a \in A^{(\mathbb{N}^N)}$. De la même manière, on peut construire l'anneau des séries formelles en N indéterminées à coefficients dans A (mais qui ne sera d'aucune utilité dans ce cours). On peut aussi construire un anneau de polynômes en un nombre infini (dénombrable ou non) d'indéterminées. Enfin et d'après la première construction, si A est intègre, il en est de même de $A[X_1, \ldots, X_N]$.

Théorème 1.5.2 (propriété universelle de l'anneau des polynômes en N indéterminées)**.** *Soit A et B des anneaux et $N \geq 1$ un entier. Soit $i : A \longrightarrow A[X_1, \ldots, X_N]$ le morphisme injectif d'anneaux naturel. L'application*

$$\begin{array}{rcl} \mathrm{Hom}(A[X_1, \ldots, X_N], B) & \longrightarrow & \mathrm{Hom}(A, B) \times B^N \\ \varphi & \longmapsto & (\varphi \circ i, \varphi(X_1), \ldots, \varphi(X_N)) \end{array}$$

est bijective.

1.6 Anneaux quotients

Théorème 1.6.1. *Soit A un anneau et $\mathcal{I}$ un idéal de A. À isomorphisme près, il existe une unique structure d'anneau sur $A/\mathcal{I}$.*

Remarque.

— La structure de groupe est déjà connue. Il suffit de vérifier que la multiplication sur $A/\mathcal{I}$ est bien définie.

— Si $\pi : A \longrightarrow A/I$ est la projection canonique, alors $\mathcal{J} \longmapsto \pi(\mathcal{J})$ est un bijection des idéaux de A contenant I vers ceux de $A/\mathcal{I}$. Cette dernière induit une bijection des idéaux premiers de A contenant I vers ceux de $A/\mathcal{I}$.

Proposition 1.6.1. *Soit B_1 et B_2 des anneaux, et $\pi_1 : A \longrightarrow B_1$ et $\pi_2 : A \longrightarrow B_2$ des surjections de noyau $\mathcal{I}$. Alors, il existe un unique isomorphisme d'anneaux $\varphi : B_1 \longrightarrow B_2$ tel que $\varphi \circ \pi_1 = \pi_2$.*

Théorème 1.6.2 (propriété universelle de l'anneau quotient, théorème de factorisation)**.** *Soit A un anneau, et $\mathcal{I}$ un idéal de A. Soit $\pi : A \longrightarrow A/\mathcal{I}$ la projection canonique. Soit B un anneau et $\varphi : A \longrightarrow B$ un morphisme d'anneaux dont le noyaux contient I. Alors, il existe un unique morphisme $\tilde{\varphi} : A/\mathcal{I} \longrightarrow B$ tel que $\varphi = \tilde{\varphi} \circ \pi$. De plus,*

- *$\tilde{\varphi}$ est surjectif si et seulement si φ est surjectif.*
- *$\tilde{\varphi}$ est injectif si et seulement si $\ker \varphi = \mathcal{I}$.*

Théorème 1.6.3 (théorèmes d'isomorphismes)**.** *Soient A et B des anneaux commutatifs.*

(i) Soit $\varphi : A \longrightarrow B$ un morphisme d'anneaux.

- *Le morphisme φ induit un isomorphisme de $A/\ker \varphi$ sur $\mathrm{Im}(\varphi)$.*
- *Supposons φ surjectif, et soit $\mathcal{J}$ un idéal de B. On note $\rho : B \longrightarrow B/\mathcal{J}$ la projection canonique associé. Alors, $\rho \circ \varphi$ induit un isomorphisme de $A/\varphi^{-1}(\mathcal{J})$ vers $B/\mathcal{J}$.*
- *Supposons φ surjectif, et soit $\mathcal{I}$ un idéal de A. Soit $\nu : B \longrightarrow B/\varphi(I)$ la projection canonique. Alors, $\nu \circ \varphi$ induit un isomorphisme de $A/(\mathcal{I} + \ker \varphi)$ vers $B/\varphi(I)$.*

(ii) Soit $\mathcal{I}$ un idéal de A. On note $\pi_{I,X} : A[X] \longrightarrow (A/\mathcal{I})[X]$ l'unique morphisme qui envoie $X \in A$ sur $X \in A/\mathcal{I}$ donné par la composition naturelle

$$A \longrightarrow A/\mathcal{I} \longrightarrow (A/\mathcal{I})[X].$$

Soit $\mathcal{J}$ un idéal de $(A/\mathcal{I})[X]$ et soit $\nu : (A\mathcal{I})[X] \longrightarrow (A/\mathcal{I})[X]/\pi_{\mathcal{I},X}(\mathcal{J})$ la projection canonique. Alors, $\nu \circ \pi_{\mathcal{I},X}$ induit un isomorphisme de $A[X]/(\mathcal{I} \cdot A[X] + \mathcal{J})$ vers $(A/\mathcal{I})[X]/\pi_{\mathcal{I},X}(\mathcal{J})$.

1.7 Théorème chinois

Théorème 1.7.1. *Soient $n, m \in \mathbb{N}^*$. Soit $\pi_n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ et $\pi_m : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ les projections canoniques. Soit $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, $x \mapsto (\pi_n(x), \pi_m(x))$ le morphisme d'anneaux produit associé. On a les résultats suivants.*

(i) $\ker \pi = n\mathbb{Z} \cap m\mathbb{Z} = \mathrm{ppcm}(n, m)\mathbb{Z}$.

(ii) Si n et m sont premiers entre eux, alors π est surjectif. En particulier, π induit un morphisme d'anneaux

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Théorème 1.7.2. *Soit A un anneau et $\mathcal{I}$ et $\mathcal{J}$ deux idéaux de A. Soit $\pi_{\mathcal{I}} : A \longrightarrow A/\mathcal{I}$, et $\pi_{\mathcal{J}} : A \longrightarrow A/\mathcal{J}$ les projections canoniques associées. Soit $\pi : A \to A/\mathcal{I} \times A/\mathcal{J}$, $x \mapsto (\pi_{\mathcal{I}}(x), \pi_{\mathcal{J}}(x))$ le morphisme d'anneaux produit associé. Alors,*

(i) $\ker \pi = \mathcal{I} \cap \mathcal{J}$.

(ii) Si $\mathcal{I} + \mathcal{J} = A$, alors $\mathcal{I} \cap \mathcal{J} = \mathcal{I}\mathcal{J}$ et π est surjectif. En particulier, π induit un morphisme d'anneaux

$$A/(\mathcal{I}\mathcal{J}) \cong (A/\mathcal{I}) \times (A/\mathcal{J}).$$

Théorème 1.7.3. *Soit $n \in \mathbb{N}^*$, A un anneau, et $(\mathcal{I}_i)_{1 \leq i \leq n}$ un famille finie d'idéaux de A. Pour tout $i \in [\![1, n]\!]$, on note $\pi_i : A \longrightarrow A/\mathcal{I}_i$, la projection canonique associée au quotient $A/\mathcal{I}_i$. Soit*

$$\pi : \left| \begin{array}{ccc} A & \longrightarrow & \displaystyle\prod_{i=1}^{n} A/\mathcal{I}_i \\ x & \longmapsto & (\pi_1(x), \ldots, \pi_n(x)) \end{array} \right.$$

Le morphisme d'anneaux produit associé. Alors, on a les résultats suivants.

(i) On a

$$\ker \pi = \mathcal{I}_1 \cdots \mathcal{I}_n.$$

(ii) Supposons que pour tout $i, j \in [\![1, n]\!]$ avec $i \neq j$, $\mathcal{I}_i + \mathcal{I}_j = A$. Alors $\cap_{i=1}^{n} \mathcal{I}_i = \mathcal{I}_1 \cdots \mathcal{I}_n$ et π est surjectif. En particulier, π induit un morphisme d'anneaux

$$A/\left(\mathcal{I}_1 \cdots \mathcal{I}_n\right) \cong \prod_{i=1}^{n} A/\mathcal{I}_i.$$

Remarque. L'hypothèse que $I_i + I_j = A$ dès lors que $i \neq j$ est nécessaire. En effet, la remplacer par $\sum_{i=1}^{n} \mathcal{I}_i = A$ ne suffit pas. On pourra s'en convaincre en vérifiant que $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ n'est pas isomorphe à $\mathbb{Z}/nmr\mathbb{Z}$ lorsque $(n, m, r) = (6, 10, 15)$.

1.8 Diviseurs de zéros, anneaux intègres, corps

Définition 1.8.1. *Soit A un anneau. On appelle* ***diviseur de zéro*** *tout élément $a \in A$ tel qu'il existe $b \in A$ non nul vérifiant $ab = 0_A$. On dit que a est non trivial lorsque $a \neq 0_A$.*

Exemple. Si p et q sont des nombres premiers, alors $\overline{p}$ et $\overline{q}$ sont des diviseurs de zéro dans $\mathbb{Z}/pq\mathbb{Z}$.

Définition 1.8.2 (anneaux intègre)**.** *Soit A un anneau commutatif. A est dit* ***intègre*** *lorsqu'une de ces conditions (équivalentes) est réalisée :*

(i) *A ne possède pas de diviseur de zéro non trivial.*

(ii) *le morphisme $x \mapsto ax$ est injectif pour tout $a \in A$ non nul.*

(iii) *Pour tout $a \in A$ non nul :*

$$\forall x \in A,\ (ax = 0_A) \implies (x = 0_A).$$

(iv) *Pour tout $a, b \in A$:*

$$(ab = 0_A) \implies (a = 0_A) \vee (b = 0_A).$$

Proposition 1.8.1. *Soit A un anneau commutatif et $\mathcal{I}$ un idéal. Alors, A est intègre si et seulement si $\{0_A\}$ est un idéal premier.*

Proposition 1.8.2. *Un sous-anneau d'un anneau intègre est aussi intègre.*

Définition 1.8.3 (corps)**.** *Un corps est un anneau commutatif non nul tel que tout élément non nul est inversible.*

Remarques.

— En résumé, $A \neq \{0_A\}$ et $A^\times = A \backslash \{0_A\}$.

— Un corps non commutatif est appelé anneau à division, ou corps gauche. D'ailleurs, on ne définit pas toujours les anneaux comme étant commutatifs par défaut. Cependant, nous les supposerons toujours commutatif.

— Un corps est évidemment intègre.

Exemples. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ dès lors que p est un nombre premier, ou $\mathbb{K}[X]/P\mathbb{K}[X]$ lorsque $\mathbb{K}$ est un corps commutatif et $P \in \mathbb{K}[X]$ est irréductible.

Proposition 1.8.3. *Soit A un anneau commutatif. Sont équivalents :*

(i) *A est un corps,*

(ii) *A possède deux idéaux,*

(iii) *A ne possède que des idéaux triviaux (A et $\{0_A\}$),*

(iv) *$\{0_A\}$ est un idéal de A.*

En particulier, si $\mathbb{K}$ est un corps, et que $\varphi : \mathbb{K} \longrightarrow B$ est un morphisme d'anneau (où B est un anneau commutatif), alors si φ est injectif, B possède un sous-anneau isomorphe au corps $\mathbb{K}$.

Proposition 1.8.4. *Soit A un anneau commutatif, et $\mathcal{I}$ un idéal de A.*

(i) *$\mathcal{I}$ est premier si et seulement si $A/\mathcal{I}$ est intègre.*

(ii) *$\mathcal{I}$ est maximal si et seulement si $A/\mathcal{I}$ est un corps.*

Théorème 1.8.1. *(i) Soit $n \in \mathbb{N}^*$. Alors, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est intègre, si et seulement si n est premier.*

(ii) Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme non nul. Alors $\mathbb{K}/P\mathbb{K}[X]$ est un corps si et seulement si $\mathbb{K}/P\mathbb{K}[X]$ est intègre, si et seulement si P est irréductible (dans $\mathbb{K}[X]$).

Remarque. Dans le premier cas, n est non nul car $\mathbb{Z}/0\mathbb{Z}$ est isomorphe à $\mathbb{Z}$ donc est intègre, mais n'est pas pour autant un corps.

Corollaire 1.8.1. *La caractéristique d'un corps est soit nul, soit un nombre premier.*

Remarques.

— C'est aussi le cas des anneaux intègres.

— Pour tout nombre premier p, $\mathbb{Z}/p\mathbb{Z}[X]$ est de caractéristique p, mais n'est pas un corps.

1.9 Éléments irréductibles d'un anneau intègre

Cette section a pour but de généraliser le concept de nombre premier ou de polynôme irréductible, et les théorèmes arithmétiques associés, à tout anneau intègre. Ainsi, A désignera dans cette section un anneau intègre (donc commutatif).

Définition 1.9.1. *Soient $a, b \in A$. On dit que a divise b (ou que b est un multiple de a) s'il existe $c \in A$ tel que $b = ca$. On note alors $a|b$.*

Remarques.

— Puisque A est intègre, tout le monde divise 0_A, mais 0_A ne divise que 0_A.

— Un élément inversible divise tout le monde.

Lemme 1.9.1. *Soit $a, b \in A$. Alors, a divise b si et seulement si $bA \subset aA$. De plus, on a les équivalences suivantes.*

(i) $a|b$ et $b|a$.

(ii) $bA = aA$.

(iii) Il existe $c \in A^\times$ tel que $b = ca$.

(iv) Il existe $c \in A^\times$ tel que $a = cb$.

Si l'une des quatre conditions est vérifiée, a et b sont dits ***associés****.*

Remarque. Si a et $a' \in A$ sont associés et que b et $b' \in A$ aussi, alors a divise b *si et seulement si* a' divise b'.

Définition 1.9.2 (élément irréductible)**.** *Un élément $a \in A$ est **irréductible** s'il est non inversible, et que pour tout $b, c \in A$, $a = bc$ impose que $b \in A^\times$ ou $c \in A^\times$.*

Remarque.

- Un élément irréductible est nécessairement non nul.
- Un élément $a \in A$ est irréductible *si et seulement si* , il est non nul, non inversible, et tout élément divisant a est soit irréductible, soit associé à a.
- Un élément $a \in A$ est irréductible *si et seulement si* tout élément associé à A est irréductible.

Exemples. Les irréductibles de $\mathbb{Z}$ sont les premiers et leurs opposés. Les irréductibles de $\mathbb{K}[X]$ sont bien ce qu'on appelle les polynômes irréductibles.

Définition 1.9.3 (primalité)**.** *Deux éléments $a, b \in A$ sont dits **premiers entre eux** si les diviseurs communs commun de a et b sont les éléments inversibles.*

Proposition 1.9.1. *Soit $a \in A$ un élément irréductible et $b \in A$. Alors, a et b ne sont premiers entre eux si et seulement si a ne divise pas b.*

Théorème 1.9.1. *Soit $x \in A$. Si l'idéal xA est premier et non nul, alors x est irréductible.*

Démonstration. Soient y et $z \in A$ tels que $x = yz$. Alors, y ou z est élément de xA. En particulier, les deux sont non nuls. Supposons que $y \in A$ est élément de xA. Alors, il existe $w \in A$ tel que $y = xw$. Alors par intégrité de A, $wz = 1_A$. On en conclue alors x est irréductible.

□

Contre-exemple. Dans $\mathbb{Z}[i\sqrt{3}]$, 2 est irréductible, mais n'engendre pas un idéal premier.

On termine cette section avec quelques résultats spécifiques aux polynômes en une indéterminée sur un corps $\mathbb{K}$. On notera $\mathrm{Irr}(\mathbb{K}[X])$ l'ensemble des polynômes unitaires irréductibles de $\mathbb{K}[X]$.

Théorème 1.9.2. *Soit $\mathbb{K}$ un corps. Soit $P \in \mathbb{K}[X]$ un polynôme non nul. Il existe une unique famille à support fini $(\nu_Q(P))_{Q \in \mathrm{Irr}(\mathbb{K}[X])}$ d'entiers positifs et un unique $\alpha \in \mathbb{K}^\times$, tels que*

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

Nous démontrerons ce théorème plus tard, lors de sa généralisation aux anneaux principaux (en montrant que tous les anneaux principaux sont factoriels).

Définition 1.9.4. *Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme non nul. On dit que P est* ***sans facteur multiple*** *si pour tout $Q \in \mathrm{Irr}(\mathbb{K}[X])$, $\nu_Q(P) \leq 1$.*

Remarque. Il est équivalent de demander que si Q est non constant, alors Q^2 ne divise pas P.

Proposition 1.9.2. *Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$. Si $P \wedge P' = 1$, alors P est sans facteur multiple (où P' désigne le polynôme dérivé de P).*

Attention. La remarque est généralement en fausse. Elle est vrai sur les corps **parfait**, dont les corps de caractéristique nulle font partie.

Définition 1.9.5. *Un corps $\mathbb{K}$ est dit* ***algébriquement clos*** *si tout élément de $\mathbb{K}[X]$ non constant a au moins une racine dans $\mathbb{K}$.*

Exercice. Un corps fini n'est jamais algébriquement clos.

Proposition 1.9.3. *Soit $\mathbb{K}$ un corps algébriquement clos et $P \in \mathbb{K}[X]$ un polynôme non nul sans facteur multiple. Alors, P a exactement $\deg(P)$ racines dans $\mathbb{K}$.*

1.10 Notion de structure d'algèbre sur un anneau

Définition 1.10.1. *Soit A un anneau. Une* ***algèbre sur*** *A est un couple (B, φ) où B est un anneau et $\varphi : A \longrightarrow B$ un morphisme d'anneau.*

Remarque. Par abus de langage, on dit que $\varphi : A \longrightarrow B$ est une A-algèbre. La loi de composition externe naturelle "multiplication par un scalaire"

$$\begin{array}{ccc} A \times B & \longrightarrow & B \\ (a, b) & \longmapsto & a \cdot b = \varphi(a)b \end{array}$$

vérifie les propriétés suivantes.

- Pour tout $b \in B$, $0_A \cdot b = 0_B$.
- Pour tout $b \in B$, $1_A \cdot b = b$.
- Pour tout $a \in A$, et $b, c \in B$, $a \cdot (b + c) = a \cdot b + a \cdot c$.
- Pour tout $a_1, a_2 \in A$, et $b \in B$, $a_1 \cdot (a_2 \cdot b) = (a_1 a_2) \cdot b$.

Ainsi, pour tout corps $\mathbb{K}$, toute $\mathbb{K}$-algèbre B est naturellement munie d'une structure de $\mathbb{K}$-espace vectoriel. On rappelle que si B est non nul, alors il existe un sous-anneau de B isomorphe à $\mathbb{K}$.

Réciproquement, si un anneau B est muni d'une loi de composition externe

$$\begin{array}{ccc} A \times B & \longrightarrow & B \\ (a, b) & \longmapsto & a \cdot b \end{array}$$

vérifiant les propriétés énoncés ci-dessus, alors B est naturellement muni d'une structure de A algèbre où $\varphi : A \longrightarrow B$ est donnée par le méchanisme $a \longmapsto a \cdot 1_B$.

Exemples.

— Tout anneau est muni d'une unique structure de $\mathbb{Z}$-algèbre.

— Si A est un sous-anneau de B, B est naturellement muni d'une structure de A-algèbre. En particulier, $A[X]$ et $A[[X]]$ sont muni d'une structure naturelle de A-algèbre.

— Si A est un anneau et B une A-algèbre, alors tout quotient de B par un de ses idéaux est naturellement muni d'une structure de A-algèbre.

— Si A est un anneau, l'anneau nul $\{0_A\}$ est naturellement muni d'une structure de A-algèbre [2].

— Si E est un ensemble quelconque, alors A^E est naturellement muni d'une structure de A-algèbre *via* le morphisme diagonal.

— Un anneau de caractéristique n possède une unique structure de $\mathbb{Z}/n\mathbb{Z}$-algèbre (et plus généralement une unqiue structure de $\mathbb{Z}/m\mathbb{Z}$-algèbre pour tout multiple m de n).

Définition 1.10.2 (sous-algèbre)**.** *Soit $\varphi_B : A \longrightarrow B$ une A-algèbre. Une sous-A-algèbre de B est un anneau C de B tel que le morphisme d'anneaux d'inclusion $i : C \longrightarrow B$ se factorise par φ_B. En d'autres termes, il existe une structure de A-algèbre $\varphi_C : A \longrightarrow C$ telle que $\varphi_B = i \circ \varphi_C$.*

Définition 1.10.3 (morphisme d'algèbres)**.** *Soit $\varphi_B : A \longrightarrow B$ et $\varphi_C : A \longrightarrow C$ deux A-algèbres. On appelle morphisme d'A-algèbre tout morphisme d'anneaux $\psi : B \longrightarrow C$ tel que $\psi \circ \varphi_B = \varphi_C$.*

Bien évidemment, toutes les notions relatives aux anneaux s'étendent assez facilement aux algèbres. Par exemple, la composée de morphismes d'anneaux est un morphisme d'anneaux. On définit aussi un isomorphisme d'anneaux comme on peut s'y attendre. Nous nous attarderons un instant sur l'algèbre $A[X]$.

Théorème 1.10.1 (propriété universelle de l'algèbre des polynômes en un indéterminée)**.** *Soit A un anneau, B une A-algèbre, et $i : A \longrightarrow A[X]$ le morphisme d'inclusion qui munit $A[X]$ d'une structure de A-algèbre. L'application*

$$\begin{array}{rcl} \mathrm{Hom}_{A-alg}(A[X], B) & \longrightarrow & B \\ \varphi & \longmapsto & \varphi(X) \end{array}$$

est bijective. En d'autres termes, un morphisme d'A-algèbres $A[X] \longrightarrow B$ est uniquement déterminé par l'image de l'indéterminée X.

Définition 1.10.4. *Soit A un anneau et B une A-algèbre. Soit $b \in B$. Soit $\varphi \in \mathrm{Hom}_{A-alg}(A[X], B)$ l'unique morphisme d'A-algèbre tel que $\varphi(X) = b$. On appelle φ le morphisme d'évaluation en b, noté ev_b. Il est tel que pour tout $P \in A[X]$, $\mathrm{ev}_b(P) = P(b)$. On note $A[b]$ l'image de $A[X]$ par ev_b.*

Enfin, nous terminons ce chapitre par une considération sur les quotients dans les algèbres.

2. Oui je sais, c'est totalement inintéressant.

Théorème 1.10.2. *Soit $i : A \longrightarrow B$ une A-algèbre, $\mathcal{J}$ un idéal de B, et $\pi : B \longrightarrow B/\mathcal{J}$ la surjection canonique. On considère sur $B/\mathcal{J}$ la structure de A-algèbre induite par $\pi \circ i$.*

(i) π est un morphisme d'A-algèbre.

(ii) Soit C une A-algèbre, et $\varphi : B \longrightarrow C$ un morphisme d'A-algèbres dont le noyau contient $\mathcal{J}$. Alors, l'unique morphisme d'anneaux $\psi : B/\mathcal{J} \longrightarrow C$ tel que $\psi \circ \pi = \varphi$ est un morphisme d'A-algèbres.

Chapitre 2

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

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

Soit $n \in \mathbb{N}$. On rappelle que la surjection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $m \mapsto [m]_n$ est... surjective [1]... de noyau $n\mathbb{Z}$. De plus, l'application $[\![0, n-1]\!] \to \mathbb{Z}/n\mathbb{Z}$, $m \mapsto [m]_n$ est une bijection.

2.1.1 Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Nous passons cette section en vitesse puisque tous les éléments permettant d'arriver à ce résultat se trouvent dans un quelconque cours de théorie des groupes. Entre autres, on montrant que les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les éléments $[m]_n \in \mathbb{Z}/n\mathbb{Z}$ tels que $m \wedge n = 1$. La recherche d'un inverse passe alors par la recherche d'une relation de Bézout (donc par l'algorithme d'Euclide étendu). Ces considérations sont évidemment ensemblistes puisqu'on a accès aux cardinaux des $(\mathbb{Z}/n\mathbb{Z})^\times$, mais cela ne nous dit rien sur leurs structures de groupes (en tant que groupes d'inversibles).

2.1.2 Endomorphismes de $\mathbb{Z}/n\mathbb{Z}$

Théorème 2.1.1. *Soit $n \in \mathbb{N}$ et A un anneau. Alors :*

$$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A) \neq \varnothing \iff (\mathrm{car}\, A) | n.$$

Dans ce cas, $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A)$ *possède un unique élément. On notera en particulier que*

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

Démonstration. On note φ_A l'unique morphisme de $\mathrm{Hom}(\mathbb{Z}, A)$. Notons qu'il est de noyau $\mathrm{car}(A)\mathbb{Z}$. Par la propriété universelle du quotient, les ensembles

$$\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A) \quad \text{et} \quad \{\varphi \in \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A) \,|\, n\mathbb{Z} \subset \ker \varphi\}$$

sont en bijection. Puisque $\mathrm{Hom}(\mathbb{Z}, A)$ possède un unique élément φ_A de noyau $\mathrm{car}(A)\mathbb{Z}$, on en déduit que $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, A)$ est non vide *si et seulement si* $n\mathbb{Z} \subset \mathrm{car}(A)\mathbb{Z}$.

□

Notation. Pour tout $m, n \in \mathbb{N}$ tels que $m|n$, on note $\pi_{n,m}$ l'unique élément de $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z})$.

1. La plupart des auteurs l'appellent la projection canonique, ou le morphisme quotient, ce qui fait un peu stupide comme remarque dans ce cours.

Remarque. Si $n_1, \ldots, n_r$ sont des nombres premiers entre eux deux à deux, alors le morphisme

$$(\pi_{n,n_1}, \ldots, \pi_{n,n_r}) : \mathbb{Z}/n\mathbb{Z} \longrightarrow \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$$

est l'isomorphisme décrit par le théorème chinois.

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

On rappelle que dans un anneau A, un élément $a \in A$ est dit être un carré s'il existe un $x \in A$ tel que $x^2 = a$ (non nécessairement unique).

Proposition 2.1.1. *Soit $p \geq 3$ un nombre premier. On a les résultats suivants.*

(i) L'application

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ x & \longmapsto & x^2 \end{array}$$

est un morphisme de groupes de noyau $\{[1]_p, [-1]_p\}$.

(ii) Il y a exactement $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$. En outre, si $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, alors x est un carré si et seulement si $x^{\frac{p-1}{2}} = [1]_p$.

Théorème 2.1.2. *Soit $\mathbb{K}$ un corps de caractéristique différente de 2.*

(i) On a $1_\mathbb{K} \neq -1_\mathbb{K}$.

(ii) L'application

$$C_\mathbb{K} : \left| \begin{array}{ccc} \mathbb{K}^\times & \longrightarrow & \mathbb{K}^\times \\ x & \longmapsto & x^2 \end{array} \right.$$

est un morphisme de groupes de noyau $\{-1_\mathbb{K}, 1_\mathbb{K}\}$.

(iii) En particulier, si $\mathbb{K}$ est un corps fini de cardinal q impair, il y a $\frac{q+1}{2}$ carrés dans $\mathbb{K}$. De plus, si $x \in \mathbb{K}^\times$, alors x est un carré si et seulement si $x^{\frac{q-1}{2}} = 1_\mathbb{K}$.

Démonstration. (i) Puisqu'un corps n'est jamais nul, on remarque que l'unique morphisme $\varphi_\mathbb{K} : \mathbb{Z} \to \mathbb{K}, n \mapsto n \cdot 1_\mathbb{K}$ n'a pas $\mathbb{Z}$ pour noyau. De plus, puisque $\mathrm{car}(\mathbb{K}) \neq 2$, on a $0_\mathbb{K} \neq 1_\mathbb{K} + 1_\mathbb{K} = 2 \cdot 1_\mathbb{K}$.

(ii) L'application $C_\mathbb{K}$ est clairement un morphisme de groupe. Soit $x \in \ker C_\mathbb{K}$, alors on remarque que $(x - 1_\mathbb{K})(x + 1_\mathbb{K}) = 0_\mathbb{K}$ dont par intégrité de $\mathbb{K}$ en tant que corps, on a remarque que $x \in \{1_\mathbb{K}, -1_\mathbb{K}\}$. On vérifie facilement l'inclusion réciproque.

(iii) On suppose que $\mathbb{K}$ est un corps fini de cardinal q impair. Notons $D_\mathbb{K}$ l'ensemble des carrés non nuls de $\mathbb{K}$. Puisque $D_\mathbb{K} = C_\mathbb{K}(\mathbb{K}^\times)$ et que $|\ker(C_\mathbb{K})| = 2$, on en déduit que $\mathrm{card}(D_\mathbb{K}) = \frac{q-1}{2}$. Puisque $0_\mathbb{K}$ est aussi un carré, on en déduit qu'il y a exactement $\frac{q+1}{2}$ carrés dans $\mathbb{K}$. Soit $x \in D_\mathbb{K}$ et y une racine carrée de x. Alors, par le théorème de Lagrange appliqué au groupe $\mathbb{K}^\times$ de cardinal $q - 1$, on a $y^{q-1} = 1_\mathbb{K}$. Ainsi, $x^{\frac{q-1}{2}} = 1_\mathbb{K}$. On en déduit que le polynôme $X^{\frac{q-1}{2}} - 1_\mathbb{K}$ a au moins $\mathrm{card}(D_\mathbb{K}) = \frac{q-1}{2}$ racine, mais a aussi au plus $\frac{q-1}{2}$ racine de par son degré.

□

2.2 Étude de la $\mathbb{K}$-algèbre $\mathbb{K}[X]/P\mathbb{K}[X]$

2.2.1 Structure de $\mathbb{K}$-espace vectoriel sur les quotients de $\mathbb{K}[X]$

Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$. Le morphisme d'inclusion $\mathbb{K} \longrightarrow \mathbb{K}[X]$ induit par composition avec le morphisme de projection canonique $\mathbb{K}[X] \longrightarrow \mathbb{K}[X]/P\mathbb{K}[X]$ une structure de $\mathbb{K}$-algèbre (et donc de $\mathbb{K}$-espace vectoriel) sur $\mathbb{K}[X]/P\mathbb{K}[X]$.

Théorème 2.2.1. *Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme non constant. Soit $\pi : \mathbb{K}[X] \longrightarrow \mathbb{K}[X]/P\mathbb{K}[X]$ la projection canonique, et soit $x = \pi(X)$. Alors, la famille $(1, x \ldots, x^{\deg(P)-1})$ est une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]/P\mathbb{K}[X]$. En particulier, la restriction de π à $\{Q \in \mathbb{K}[X] \mid \deg Q < \deg P\}$ est bijective.*

Démonstration. Si $A \in \mathbb{K}[X]$, et Q et $R \in \mathbb{K}[X]$ (avec $\deg R < \deg P$) sont respectivement le quotient et le reste de la division euclidienne de A par P, alors $A = PQ+R$ et donc $\pi(A) = \pi(R)$. En notant

$$R = \sum_{k=0}^{\deg(P)-1} a_k X^k,$$

on obtient que $\pi(R) = \sum_{k=0}^{\deg(P)-1} a_k x^k$. De plus, si $(b_k)_{i\in[\![0,\deg(P)-1]\!]} \in \mathbb{K}^{\deg P}$ est une famille telle que

$$\sum_{k=0}^{\deg(P)-1} a_k x_k = 0,$$

alors en notant en notant $B = \sum_{k=0}^{\deg(P)-1} a_k X_k = 0$, ce polynôme est élément de $\ker \pi$, donc est divisible par P. Or, le degré inférieur de B impose que $B = 0$, donc ses coefficients sont nuls.

□

Proposition 2.2.1. *Soit $\mathbb{K}$ un corps fini et $P \in \mathbb{K}[X]$ un polynôme irréductible de degré $n \in \mathbb{N}^*$. Alors, $\mathbb{K}[X]/P\mathbb{K}[X]$ est de cardinal fini $|\mathbb{K}|^n$ et est de caractéristique égale à celle de $\mathbb{K}$.*

Démonstration. Puisque $\mathbb{K}$ est fini, sa caractéristique (qu'on note k) est non nul. Soit $n \in \mathbb{Z}$. On remarque $n \cdot 1_{\mathbb{K}/P\mathbb{K}[X]} = n \cdot \pi(1_{\mathbb{K}})$. Ainsi, on voit que $k \cdot 1_{\mathbb{K}[X]/\mathbb{K}[X]} = 0_{\mathbb{K}[X]/\mathbb{K}[X]}$. On en déduit que k divise m. Or, k et m sont premiers (puisqu'ils sont non nuls, et sont des caractéristiques de corps). On en déduit que $k = m$.

□

2.2.2 Éléments inversibles des quotients de $\mathbb{K}[X]$

Théorème 2.2.2. *Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme non constant. Soit $\pi : \mathbb{K}[X] \longrightarrow \mathbb{K}[X]/P\mathbb{K}[X]$ le morphisme canonique, et soit $Q \in \mathbb{K}[X]$. Alors, $\pi(Q)$ est inversible dans $\mathbb{K}[X]/P\mathbb{K}[X]$ si et seulement si P et Q sont premiers entre eux. En particulier, l'application*

$$\begin{array}{rcl} \{Q \in \mathbb{K}[X] \mid \deg Q < \deg P,\ \mathrm{pgcd}(P,Q) = 1\} & \longrightarrow & (\mathbb{K}[X]/P\mathbb{K}[X])^\times \\ Q & \longmapsto & \pi(Q) \end{array}$$

induite par restriction et corestriction de π est une bijection.

Démonstration. Identique à la démonstration sur les quotients de $\mathbb{Z}$. □

2.2.3 Endormophismes des quotients de $\mathbb{K}[X]$

Théorème 2.2.3. *Soit $\mathbb{K}$ un corps, et A une $\mathbb{K}$-algèbre. Alors, l'application*

$$\begin{array}{rcl} A & \longrightarrow & \mathrm{Hom}_{\mathbb{K}-alg}(\mathbb{K}[X], A) \\ a & \longmapsto & \mathrm{ev}_a \end{array}$$

est une bijection.

Chapitre 3

Corps finis et applications

Comme son nom l'indique, ce chapitre fera l'objet de l'études corps finis. Comme pour les groupes, nous nous intéresserons à classifier ces corps par classes d'isomorphismes et donc de structure. Heureusement, la classification est beaucoup simple que celles des groupes finis.

3.1 Introduction et premières propriétés

Proposition 3.1.1. *Soit $\mathbb{K}$ un corps fini et $P \in \mathbb{K}[X]$ un polynôme irréductible. Alors, l'anneau quotient $\mathbb{L} = \mathbb{K}[X]/\langle P \rangle$ est un corps fini de cardinal $\mathrm{car}(\mathbb{K})^{\deg P}$.*

Proposition 3.1.2. *Tout anneau commutatif intègre fini est un corps.*

Démonstration. Par intégrité de A, pour tout $a \in A$, $a \neq 0_A$, l'application $A \to A$, $x \mapsto ax$ est injective donc bijective puisque A est fini.

□

3.2 Caractéristique et cardinal d'un corps fini

Théorème 3.2.1. *Soit $\mathbb{K}$ un corps fini. Alors, la caractéristique de $\mathbb{K}$ est un nombre premier p. Il existe en particulier une unique structure de $\mathbb{F}_p$-algèbre sur $\mathbb{K}$ qui fait de $\mathbb{K}$ un $\mathbb{F}_p$-espace vectoriel de dimension finie. Si $n = \dim_{\mathbb{F}_p}(\mathbb{K})$, alors $\operatorname{card} \mathbb{K} = p^n$. En particulier, le cardinal d'un corps fini est toujours fini.*

Démonstration. La caractéristique d'un corps est soit 0 soit un nombre premier, mais si $\mathbb{K}$ avait 0 pour caractéristique, il contiendrait au moins $\mathbb{Z}$. Ainsi, $\operatorname{car} \mathbb{K}$ est un nombre premier. De plus, la structure de $\mathbb{F}_p$ algèbre est donnée par la factorisation du morphisme canonique $\mathbb{Z} \longrightarrow \mathbb{K}$ par $\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{K}$. De plus, $\mathbb{K}$ étant fini, il est nécessairement de dimension finie.

□

3.3 Un exemple de calcul explicite dans un corps fini

3.4 Morphisme de Frobenius

Théorème 3.4.1. *Soit A un anneau de caractéristique p où p est un nombre premier. Alors, l'application $F_A : A \to A$, $x \mapsto x^p$ est un morphisme d'anneaux appelé* ***morphisme de*** **Frobenius**. *Si $\mathbb{K}$ est un corps fini, l'application $\mathbb{F}_K$ est un isomorphisme de corps.*

3.5 Cyclicité du du groupe des inversibles d'un corps fini

Avant de (re)démontrer ce résultat énoncé au premier semestre en théorie des groupes, rappelons quelques notations. On note φ l'indicatrice d'Euler. Soit G un groupe et $d \in \mathbb{N}^*$, on note $\Delta_d(G) = \{x \in G \,|\, x^d = e_G\}$ et $\Omega_d(G) \subset \Delta_d(G)$ les éléments de G d'ordre de d. Enfin, on note $\omega_d(G) = \text{card}(\Omega_d(G))$. On remarquera de par le théorème de Lagrange que si G est fini d'ordre n et que si d est un entier positif ne divisant pas n, alors $\omega_d(G) = 0$. On en déduit que $(\Omega_d(G))_{d|n}$ est une partition de G (où d parcourt les diviseurs positifs de n). On a alors

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

De plus, si G est un groupe cyclique d'ordre n, et si d est un diviseur positif de n, alors $\text{card}(\Delta_d(G)) = d$ et $\omega_d(G) = \varphi(d)$. Puisqu'il existe toujours des groupes cycliques d'ordre n ($\mathbb{Z}/n\mathbb{Z}$), la relation précédente devient

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

Passons maintenant à des nouveautés.

Théorème 3.5.1. *Soit $n \in \mathbb{N}^*$ et G un groupe fini d'ordre n. Sont équivalents.*

(i) G est cyclique ;

(ii) pour tout diviseur positif d de n, $\text{card}(\Delta_d(G)) \leq d$;

(iii) pour tout diviseur positif d de n, $\omega_d(G) \leq \varphi(d)$.

Démonstration. — $(i) \implies (ii)$. Le rappel précédent suffit (avec égalité par ailleurs).

— $(iii) \implies (i)$. Par hypothèse,

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

Or, d'après les deux relations démontrées dans le rappel, cette inégalité est une égalité. On en déduit que pour tout diviseur positif d de n, $\omega_d(G) = \varphi(d)$. En particulier, $\omega_n(G) = \varphi(n) > 0$ donc G contient un élément d'ordre n et est cyclique.

— ...

□

Théorème 3.5.2. *Soit $\mathbb{K}$ un corps fini. Alors, le groupe multiplicatif $\mathbb{K}^\times$ est cyclique.*

Démonstration. Remarquer que le polynôme $X^d - 1_{\mathbb{K}}$ a au plus d racines.

□

Théorème 3.5.3. *Soit $\mathbb{K}$ un corps fini de caractéristique p. Alors, il existe un élément $P \in \mathbb{F}_p[X]$ irréductible tel que $\mathbb{K}$ est isomorphe à $\mathbb{F}_p[X]/\langle P \rangle$.*

Démonstration. Soit x un générateur du groupe cyclique $\mathbb{K}^\times$, et $\varphi : \mathbb{F}_p[X] \longrightarrow \mathbb{K}$ l'unique morphisme de $\mathbb{F}_p$-algèbe qui envoie X sur x. Par définition de x, on a $\mathbb{K} = \{0\} \cup \{x^n \mid n \in \mathbb{N}\}$. On en déduit que φ est surjectif. Soit alors P un générateur du noyau de φ. On invoque alors le théorème d'isomorphisme. Puisque $\mathbb{K}$ est un corps, on en déduit *a fortiori* que P est irréductible.

□

3.6 Deux corps finis de même cardinal sont isomorphes

Lemme 3.6.1. *Soit $\mathbb{K}$ un corps fini de cardinal N et $x \in \mathbb{K}$. Alors, $x^N = x$.*

Démonstration. Si $x = 0_{\mathbb{K}}$, c'est clair. Sinon, on observe que $|\mathbb{K}^\times| = N - 1$.

□

Lemme 3.6.2. *Soit p un nombre premier et $P \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n. Alors, P divise $X^{p^n} - X$.*

Théorème 3.6.1. *Soit p un nombre premier et $n \in \mathbb{N}^*$. Soit $\mathbb{K}$ et $\mathbb{L}$ deux corps finis de cardinal p^n. Alors, $\mathbb{K} \cong \mathbb{L}$.*

Remarque. ...

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

Théorème 3.7.1. *Soit p un nombre premier. Alors, il existe un corps algébriquement clos $\mathbb{L}$ qui contient $\mathbb{F}_p$.*

Théorème 3.7.2. *Soit p un nombre premier et $n \in \mathbb{N}^*$. À isomorphisme près, il existe un unique corps fini de cardinal p^n.*

Proposition 3.7.1. *Soit p un nombre premier. On note $\mathrm{Irr}(p, n)$ l'ensemble des polynômes irréductibles unitaires de degré n dans $\mathbb{F}_p$. On a alors*

$$X^{p^n} - X = \prod_{r|n} \prod_{P \in \mathrm{Irr}(p,r)} P.$$

Théorème 3.7.3. *Soit p un nombre premier, $n \in \mathbb{N}^*$, et $\mathbb{K}$ un corps fini de cardinal p^n. Soit enfin d un diviseur positif de n, et*

$$\mathbb{L} = \left\{ x \in \mathbb{K} \,\middle|\, x^{p^d} = x \right\}.$$

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

Théorème 3.7.4. *Soit p un nombre premier et $n \in \mathbb{N}^*$. Soit $\mathbb{K}$ un corps fini de cardinal p^n et $N \in \mathbb{N}^*$. Alors, il existe un sous-corps de $\mathbb{K}$ de cardinal N si et seulement si il existe un diviseur positif de n tel que $N = p^d$. Dans ce cas, ce sous-corps est unique. En particulier, si $\mathbb{K}$ est un corps fini de cardinal q, il existe une extension de $\mathbb{K}$ de cardinal si et seulement si N est une puissance de q.*

Chapitre 4

Localisation, corps des fractions

Dans ce chapitre, nous considérons toujours des anneaux commutatifs. Nous ne mentionnerons donc plus explicitement ce caractère.

4.1 Exemple

4.2 Définition et propriétés élémentaires du localisé

Définition 4.2.1. *Soit A un anneau. Un partie de S est dite* ***multiplicative*** *si elle contient 1_A et est stable par multiplication.*

Remarque. Si S est une partie multiplicative d'un anneau A, alors

$$\mathcal{I}_S = \{a \in A \mid \exists s \in S,\, as = 0_A\}$$

est un idéal de A.

Théorème 4.2.1. *Soit A un anneau et S une partie multiplicative de A.*

(i) Il existe un anneau B et un morphisme d'anneaux $\varphi : A \longrightarrow B$ vérifiant les propriétés suivantes.

- *$\varphi(S) \subset B^\times$.*
- *$(*)$ Pour tout anneau C, et pour tout morphisme d'anneau $\psi : A \longrightarrow C$ tel que $\psi(S) \subset C^\times$. Alors, il existe un unique morphisme d'anneaux $\theta : B \longrightarrow C$ tel que $\psi = \theta \circ \varphi$.*

(ii) Un tel couple (B, φ) est unique à isomorphisme près, c'est-à-dire que si B' est un anneau et $\varphi' : A \longrightarrow B'$ est un morphisme d'anneau, et (B', φ') vérifie la propriété $(*)$, alors il existe un unique isomorphisme d'anneau $\gamma : B \longrightarrow B'$ tel que $\varphi' = \gamma \circ \varphi$.

Remarques.

- Si (B, φ) vérifie les propriétés de l'énoncé, on remarque alors que $\mathcal{I}_S \subset \ker \varphi$.
- Si (B, φ) vérifie les propriétés de l'énoncé, B est appelé *le*[1] *localisé de A par rapport à A*. On le note $S^{-1}A$. On dira que $\varphi : A \longrightarrow S^{-1}A$ est *le morphisme de localisation*. On

1. Il est unique à isomorphisme près.

remarque alors que $S^{-1}A$ est muni d'une structure de A-algèbre. On reforme le théorème précédent de la façon suivante.

Théorème 4.2.2 (propriété universelle de l'anneau localisé)**.** *Soit A un anneau et S une partie multiplicative de A et $\varphi : A \longrightarrow S^{-1}A$ le morphisme de localisation. Soit C un anneau et $\psi : A \longrightarrow C$ un morphisme d'anneaux tel que $\psi(S) \subset C^\times$. Alors, il existe un unique morphisme d'anneaux $\theta : S^{-1}A \longrightarrow C$ tel que $\psi = \theta\varphi$.*

En d'autres termes, se donner un morphisme du localisé $S^{-1}A$ vers un anneau C revient à se donner un morphisme de A vers C tel que l'image de tout élément de S est inversible dans C.

4.3 Intégrité du corps des fractions

Chapitre 5

Anneaux euclidiens, principaux, factoriels

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

Définition 5.1.1. *Soit A un anneau intègre. On dit que A vérifié*

- *la propriété **"irréductible = premier"** si pour tout $x \in A$ non nul, xA est irréductible si et seulement si il est premier ;*
- *le **lemme d'Euclide** si pour tout a, b, et $c \in A$, tels que a soit irréductible et que a divise bc, alors a divise b ou c ;*
- *le **théorème de Bézout** si pour tout $x, y \in A$, x et y sont premiers entre eux si et seulement si $xA + yA = A$;*
- *le **lemme de Gauss** si pour tout a, b, et $c \in A$ tels que a divise bc et a et b sont premiers entre eux, alors a divise c ;*
- *le **théorème de factorisation unique** si tout élément non nul de A se factorise en produit d'irréductibles, et la factorisation est unique à l'ordre des facteurs et à l'association près.*

Exemples. $\mathbb{Z}$, $\mathbb{K}[X]$, $\mathbb{Z}[i]$.

Contre-exemple. $\mathbb{Z}[i\sqrt{3}]$. Un anneau intègre ne vérifie pas nécessairement toutes ses propriétés. Cependant, tout anneau possède des propriétés plus faibles, mais semblables.

Proposition 5.1.1. *Soit A un anneau intègre. A vérifie*

- *la propriété **"premier entraîne irréductible"** si pour tout $x \in A$ non nul, xA est premier, alors x est irréductible ;*
- *le **lemme d'Euclide faible** si pour tout a, b, et $c \in A$, tels que aA soit premier et a divise bc, alors a divise b ou c ;*
- *le **théorème de Bézout faible** si pour tout $x, y \in A$, $xA + yA = A$, alors x et y sont premiers entre eux ;*
- *le **lemme de Gauss faible** si pour tout a, b, et $c \in A$ tels que a divise bc et $aA + bA = A$, alors a divise c.*

Démonstration. (i) Soit $x \in A$ tel que xA soit premier. Puisque l'idéal xA est premier, il est en particulier propre donc x n'est pas inversible. Soit a et $b \in A$ tels que $x = ab$. Puisque xA est premier, on sait que $a \in xA$ ou $b \in xA$. Par symétrie des rôles, on peut supposer que $a \in xA$ et que $a = xc$ avec $c \in A$. Alors, $x = xcb$ et donc $x(1_A - cb) = 0_A$. Par intégrité de A, b est inversible.

(ii) Soit $a \in A$ tel que aA soit premier, et b et $c \in A$ tels que a divise bc. Cela signifie que $bc \in aA$, donc par primalité de aA, $b \in aA$ ou $c \in aA$, ce qui signifie que a divise b ou c.

(iii) Soient $x, y \in A$ tels que $xA + yA = A$. Il existe $a, b \in A$ tels que $ax + by = 1_A$. Alors, si $z \in A$ divise x et y, alors z divise 1_A, ce qui signifie que z est inversible.

(iv) Soient $a, b, c \in A$, tels que a divise bc et $aA + bA = A$. Il existe $(x, y) \in A^2$ tel que $ax + by = 1_A$. Alors, $acx + bcy = c$. Puisque a divise le premier membre, on en déduit que a divise c.

□

Remarque. Il n'y a pas de version faible du théorème de factorisation unique valable dans tout anneau intègre. On appellera *anneau atomique* tout anneau intègre où tout élément est décomposable (d'au moins un façon) en produit d'irréductibles.

On remarque aussi que certaines propriétés sont redondantes, et que certains liens existent entre ces propriétés.

Proposition 5.1.2. *On a les propriétés suivantes,*

- *la propriété "irréductible = premier" et le lemme d'*Euclide *sont équivalents ;*
- *le lemme de* Gauss *implique le lemme d'*Euclide *;*
- *le théorème de* Bézout *implique le lemme de* Gauss.

5.2 Anneaux factoriels, principaux, euclidiens

Définition 5.2.1 (anneau factoriel)**.** *Un anneau intègre est dit* ***factoriel*** *s'il vérifie le théorème de factorisation unique.*

Remarque. En anglais, *unique factorization domain (UFD).*

Définition 5.2.2 (anneau principal)**.** *Un anneau intègre A est dit* ***principal*** *si tout idéal de A est engendré par un élément.*

Définition 5.2.3 (anneau euclidien)**.** *Soit A un anneau intègre. L'anneau A est dit* ***euclidien*** *s'il existe un stathme euclidien, i.e une application $\nu : A\backslash\{0_A\} \longrightarrow \mathbb{N}$ telle que pour tout $a, b \in A$ avec b non nul, il existe $(q, r) \in A^2$ tel que*

$$a = bq + r \quad et \quad r = 0 \text{ ou } \nu(r) < \nu(b).$$

Cette écriture est appelée ***division euclidienne*** *de a par b par rapport au stathme euclidien ν.*

Théorème 5.2.1. *On a les propriétés suivantes.*

(i) Il existe des anneaux non factoriels.

(ii) Il existe des anneaux factoriels non principaux.

(iii) Tout anneau euclidien est principal.

(iv) Il existe des anneaux euclidiens non principaux.

Démonstration. (i) $\mathbb{Z}[i\sqrt{3}]$ est intègre, mais $4 = 2^2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$.

(ii) $\mathbb{Z}[X]$ est principal puisque $\mathbb{Z}$ l'est (voir théorème suivant), mais l'idéal $\langle 2, X\rangle$ n'est pas principal.

(iii) Soit A un anneau euclidien muni du stathme euclidien ν. Soit $\mathcal{I}$ un idéal de A.

□

Théorème 5.2.2. *Soit A un anneau factoriel. Alors, $A[X]$ est factoriel.*

Théorème 5.2.3. *Soit A un anneau factoriel. Alors, A vérifie le théorème de* Bézout *(donc le lemme d'*Euclide *et la propriété "irréductible = premier", et le lemme de* Gauss*).*

Remarque. Toutes ces propriétés sont donc vérifiées dans un anneau euclidien.

Théorème 5.2.4. *Un anneau factoriel vérifiant le théorème de* Bézout *est principal.*

Remarque. Puisque certains anneaux factoriels ne sont pas principaux, cela signifie qu'il existe des anneaux intègres vérifiant le lemme de Gauss mais pas le théorème de Bézout.

5.2.1 Exemples sur les différentes propriétés

— Soit $\mathbb{K}$ un corps. Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ sont euclidiens (donc principaux et factoriels) avec les stathmes respectifs $|\cdot|$ et deg. Dans ces exemples, les quotients et restes sont uniques dans les divisions euclidiennes. Ce n'est pas toujours le cas comme dans l'anneau euclidien $\mathbb{Z}[i]$. Nous démontrerons ce résultat un peu plus loin.

— Si A est factoriel, alors $A[X_1, \ldots, X_n]$ et $A[X_1, \ldots, X_n, \ldots]$ aussi.

— Si A est un anneau principal, $A[X]$ ne l'est généralement pas. $\mathbb{Z}[X_1, \ldots, X_n]$ n'est pas principal, et $\mathbb{K}[X_1, \ldots, X_n]$ non plus dès lors que $n \geq 2$ (où $\mathbb{K}$ est un corps).

— Soit $\mathbb{K}$ un corps. On munit ce corps du stathme de valuation défini pour tout $P = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{K}[[X]]$ par

$$\nu(P) = \inf\{n \in \mathbb{N} \,|\, a_n \neq 0\}.$$

L'anneau $\mathbb{K}[[X]]$ est euclidien (dont factoriel et principal).

— Un quotient intègre d'un anneau factoriel n'est pas nécessairement factoriel. Soit $\mathbb{K}$ un corps. L'anneau $A = \mathbb{K}[X, Y]/\langle X^2 - Y^3\rangle$ n'est pas factoriel. En effet, si x et y désignent les images respectives de X et Y, alors on remarque que l'on obtient les factorisations $x^2 = y^3$. D'une part, x et y sont irréductibles, et le nombre de facteurs comptés avec multiplicités dans les deux décompositions diffèrent. On pourrait aussi montrer que y est irréductible et que $\langle y\rangle$ n'est pas premier.

5.3 Valuation dans un anneau factoriel

5.4 PGCD, PPCM et relation de Bézout

5.5 Valuations, PGCD et PPCM dans le corps des fractions

5.6 Factorialité des anneaux polynômes, critères d'irréductibilité

5.7 Démonstration des théorèmes