Table des matières

Partie I. Anneaux, idéaux, algèbres 3
1. Les principaux objets algébriques 3
2. Idéaux 7
3. Localisation 16
4. Anneaux intègres 19
5. Anneaux de polynômes 26
6. Algèbres 39

Partie II. Modules 41
7. Le langage des catégories 41
8. Modules 48
9. Anneaux et modules noetheriens 53
10. Modules sur un anneau principal 56
11. Produit tensoriel 60
12. Cohomologie 67

Partie III. Géométries 73
13. Rappel de topologie 73
14. Ensembles algébriques affines, topologie de Zariski 76
15. Spectre maximal 80
16. Spectre premier 82

Partie IV. Corps 85
17. Extension de corps, degré 85
18. Extensions algébriques et transcendantes 88
19. Corps de décomposition, séparabilité 91
20. Corps finis 96
21. Théorie de Galois 101
22. Groupes de Galois 111

Partie V. Compléments de géométrie arithmétique 120
23. Anneaux de Dedekind 120
24. Lemme de Hensel. Anneau des vecteurs de Witt 129
25. Anneaux de valuation 141
26. Perfectoïdes 148

L'objet de ce cours est l'étude des anneaux commutatifs et de leurs modules. Nous traitons plus spécifiquement les extensions de corps via la théorie de Galois et introduisons les notions de base de l'algèbre commutative. Il s'agit de considérer les objets algébriques non seulement d'un point de vue abstrait mais surtout en lien avec des questions arithmétiques et géométriques. Nous abordons donc les notions suivantes :
– Principaux exemples d'anneaux commutatifs : anneaux de polynômes, de séries formelles, anneaux d'entiers algébriques.
– Divisibilité, factorisation et idéaux dans les anneaux commutatifs. Applications arithmétiques et géométriques.
– Opérations sur les anneaux commutatifs et leurs modules : localisation, produit tensoriel. Modules projectifs. Homologie.
– Structure des modules sur un anneau noetherien ou principal. Application à la réduction des endomorphismes.
– Extensions de corps. Nullstellensatz. Théorie de Galois. Applications.
– Constructions locales et globales en géométrie arithmétique. Lemme de Hensel. Vecteurs de Witt. Valuations.
– Introduction à la géométrie algébrique.

La géométrie arithmétique motive l'essentiel des partis pris dans ce cours. Il s'agit de mettre en place les outils de géométrie algébrique pour s'attaquer à des problèmes arithmétiques.

La conjecture de Weil est une illustration des liens profonds et mystérieux entre la géométrie algébrique et l'arithmétique. En effet pour $f \in \mathbb{Z}[X_1, \ldots, X_n]$, nous pouvons considérer d'une part l'espace topologique X des solutions de $f = 0$ dans $\mathbb{C}$ et d'autre part l'ensemble des solutions dans $\mathbb{F}_{p^m}$ de l'équation réduite modulo p. La conjecture de Weil, démontrée par Deligne, établit un lien entre les nombres de Betti de X et les cardinalités des ensembles de solutions en caractéristique p.

PARTIE I

ANNEAUX, IDÉAUX, ALGÈBRES

L'objet de ce cours est l'étude des anneaux et des corps et leurs premières propriétés. Nous rappelons ici les concepts de base de l'algèbre commutative qui sont étudiés en détail tout au long de ce cours.

1. Les principaux objets algébriques

Dans ce paragraphe, nous définissons les objets algébriques élémentaires : anneaux, corps, idéaux, modules et algèbres.

1.1. Anneaux, idéaux. —

Définition 1.1. — *Un* **anneau** *unitaire* $(A, +, \cdot)$ *est la donnée d'un ensemble et de deux lois internes* $+$ *et* $.$ *vérifiant :*
i. $(A, +)$ *est un groupe commutatif d'élément neutre 0,*
ii. la multiplication $\cdot$ *est associative et possède un élément neutre, noté 1,*
iii. la multiplication $\cdot$ *est distributive par rapport à l'addition :*

$$\forall x, y, z \in A, \quad x(y+z) = xy + xz, \quad (y+z)x = yx + zx.$$

Si la multiplication est commutative, l'anneau A *est dit* **commutatif**.

Dans ce cours, sauf mention explicite du contraire, le mot "anneau" désigne un anneau unitaire commutatif.

Exemples 1.2. — *i. L'anneau nul* $\{0\}$ *est le seul anneau dans lequel* $1 = 0$.
ii. Les entiers relatifs $(\mathbb{Z}, +, \cdot)$*, les entiers modulo* n $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ *sont des anneaux commutatifs. Les nombres décimaux* $(\mathbb{Z}[1/10], +, \cdot)$ *sont munis d'une structure d'anneau commutatif.*
iii. L'ensemble $P(E)$ *des parties d'un ensemble* E *muni de la différence symétrique* $(A \Delta B = A \cup B - A \cap B)$ *et de l'intersection est un anneau dit anneau de Boole.*
iv. Si A *est un anneau non nul (commutatif), l'ensemble des matrices* $(M_n(A), +, \cdot)$ *muni de l'addition et de la multiplication est un anneau qui est non commutatif si* $n \geq 2$.
v. D'après le théorème de Jacobson, tout anneau A *tel que*

$$\forall a \in A, \exists n \geq 2, a^n = a$$

est commutatif.

Certains anneaux apparaissent naturellement comme anneaux de fonctions.

Exemples 1.3. — *v. Si A est un anneau (commutatif), l'anneau $A[X]$ des polynômes en la variable X est l'ensemble des sommes de la forme $\sum_{i\in\mathbb{N}} a_i X^i$ avec $a_i \in A$ presque tous nuls et dont l'addition et la multiplication sont définies par*

$$(\sum_{i\geq 0} a_i X^i) + (\sum_{j\geq 0} b_j X^j) = \sum_{k\geq 0}(a_k + b_k)X^k,$$

$$(\sum_{i\geq 0} a_i X^i)(\sum_{j\geq 0} b_j X^j) = \sum_{k\geq 0}(\sum_{i+j=k} a_i b_j)X^k.$$

Par induction, nous définissons l'anneau $A[X_1, \ldots, X_n]$ des polynômes à n variables (voir Exemple 1.5 ii.).
vi. Si A est un anneau commutatif, nous pouvons définir l'anneau commutatif des séries formelles $A[[X]]$ dont les éléments sont les séries $\sum_{i\geq 0} a_i X^i$ avec $a_i \in A$ les lois internes étant données par la somme et le produit de convolution des séries formelles. Par induction, nous définissons également l'anneau commutatif des séries formelles à n variables $A[[X_1, \ldots, X_n]]$.
vii. Munissons $\mathbb{R}$ de sa topologie standard, i.e. engendrée par la base

$$\{]a, b[, a, b \in \mathbb{R}, a < b\}.$$

Pour tout espace topologique T, l'ensemble des fonctions continues à valeurs réelles $T \longrightarrow \mathbb{R}$ est un anneau noté $\mathcal{C}(T, \mathbb{R})$. En effet l'addition, la soustraction et le produit de deux fonctions continues sont continus ; les fonctions constantes à 0 et 1 sont les éléments neutres respectifs de l'addition et de la multiplication.

Plus généralement, la géométrie algébrique apporte l'intuition géométrique dans des situations de nature algébrique car permet de penser à n'importe quel anneau comme un anneau de fonctions sur un objet géomébrique (§14).

Définition 1.4. — *Un* **morphisme** *d'anneaux $f : A \longrightarrow B$ est une application entre les deux anneaux A et B satisfaisant pour tous $(x, y) \in A^2$,*
i. $f(x + y) = f(x) + f(y)$,
ii. $f(xy) = f(x)f(y)$,
iii. $f(1) = 1$.

Exemples 1.5. — *i. Un isomorphisme (d'anneaux) est un morphisme d'anneaux $f : A \longrightarrow B$ qui admet un inverse à droite et à gauche :*

$$\exists g : B \longrightarrow A, \quad f \circ g = \mathrm{id}_B, g \circ f = \mathrm{id}_A.$$

Un sous-anneau B de A est un sous-groupe de A stable par la multiplication, ayant le même élément neutre. L'inclusion $B \longrightarrow A$ est alors un morphisme d'anneaux. L'image d'un morphisme d'anneaux $f : A \longrightarrow B$ est un sous-anneau

de B.
ii. Nous avons un isomorphisme d'anneaux canonique

$$A[X_1, \dots, X_n] \longrightarrow A[X_1, \dots, X_{n-1}][X_n]$$

ce qui justifie que la définition (et la notation) de l'anneau des polynômes à n variables ne dépend pas de l'ordre des variables dans la construction par induction. Cette propriété est utile pour transfèrer des propriétés d'un anneau A à l'anneau $A[X_1, \dots, X_n]$ (par exemple la factorialité Corollaire 5.25).
iii. L'application nulle n'est pas un morphisme d'anneaux $f : A \longrightarrow B$ avec $B \neq 0$ (car $f(1) \neq 1$). L'application $f : \mathbb{Z}/6\mathbb{Z} \longrightarrow \mathbb{Z}/6\mathbb{Z}$, $f(x) = 3x$ n'est pas un morphisme d'anneaux (bien que $3xy = 3x3y$).
iv. Soit p un nombre premier et A un anneau de caractéristique $p > 0$ (i.e. $p \cdot 1 = \underbrace{1 + \cdots + 1}_{p \text{ fois}} = 0$). Alors l'application de Frobenius $\varphi : A \longrightarrow A$, $a \mapsto a^p$ est un morphisme d'anneaux.
En effet, d'une part,

$$\forall a, b \in A, \varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b), \quad \varphi(1) = 1^p = 1.$$

D'autre part, comme p est premier, il divise les coefficients du binôme $\binom{p}{k}$ pour $0 < k < p$; donc

$$\forall a, b \in A, \quad \varphi(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + b^p = \varphi(a) + \varphi(b).$$

v. Le seul morphisme d'anneaux $f = \mathbb{R} \longrightarrow \mathbb{R}$ est l'identité. En effet, le morphisme f est l'identité sur $\mathbb{Z}$ donc sur $\mathbb{Q}$. Les éléments de $\mathbb{R}_+$ étant les carrés, $f(\mathbb{R}_+) \subset \mathbb{R}_+$. Nous en déduisons que f est croissante et par densité de $\mathbb{Q}$, $f = \mathrm{Id}_{\mathbb{R}}$.
Le lemme d'Hensel permet de généraliser cette propriété à d'autres complétés topologiques du corps des nombres rationnels $\mathbb{Q}$ (voir Exemple 24.5 ii.).

Définition 1.6. — *Un* **idéal** *d'un anneau (commutatif) A est un sous-groupe additif I de $(A, +)$ stable par multiplication par A.*

Exemples 1.7. — *i. Le noyau d'un morphisme d'anneaux est un idéal. Réciproquement, tous les idéaux de A s'obtiennent comme noyau de morphismes d'anneaux de source A (voir 2.7). Le morphisme f est injectif si et seulement si $\ker f = \{0\}$. Il est surjectif si et seulement si $\mathrm{Coker}\, f = B/\operatorname{im} f = \{0\}$.*
ii. Dans l'anneau $\mathbb{Z}$, tous les sous-groupes additifs sont des idéaux. Mais dans $\mathbb{Z}[1/10]$, $\mathbb{Z}[1/2]$ est un sous-groupe qui n'est pas un idéal car $1/10 = 1/5 \cdot 1/2 \notin \mathbb{Z}[1/2]$.

1.2. Anneaux intègres, corps. —

Définition 1.8. — *L'ensemble des éléments inversibles d'un anneau A*

$$A^* = \{x \in A | \exists y \in A, xy = 1\}$$

est un groupe pour la multiplication induite de celle de A.
Un anneau $A \neq 0$ et commutatif est dit **intègre** *si $x, y \in A - \{0\}$ implique que $xy \in A - \{0\}$.*
Si $A^* = A - \{0\}$ (et A unitaire et commutatif), nous disons que A est un **corps**.
Un morphisme de corps est un morphisme d'anneaux entre deux corps.

Exemples 1.9. — *i. Les éléments du groupe $(\mathbb{Z}/n\mathbb{Z})^*$ sont les classes des éléments premiers à n. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps, i.e. si et seulement si n est un nombre premier.*
ii. Si K est un corps, $K[X_1, \ldots, X_n]^*$ est l'ensemble des polynômes constants non nuls. Ce n'est plus vrai si nous remplaçons le corps K par un anneau A. En effet si A contient un élément ε tel que $\varepsilon^2 = 0$, alors $1 + \varepsilon X$ n'est pas constant mais est inversible d'inverse $1 - \varepsilon X$ dans $A[X]$.
iii. Une série formelle $f \in A[[X]]$ est inversible si et seulement si son terme constant est inversible $f(0) \in A^*$.
iv. Soit A un anneau de cardinal fini ou tel qu'il existe un corps K, sous-anneau de A tel que A s'identifie à un K-espace vectoriel de dimension finie. Alors A est intègre si et seulement si A est un corps.
En effet, supposons que A est intègre et montrons que tout élément $a \in A - \{0\}$ admet un inverse dans A : l'application

$$A \longrightarrow A, \quad x \mapsto ax$$

est injective car A est intègre. Donc elle est surjective (car K-linéaire ou bien A est fini). Donc il existe $b \in A$ avec $ab = 1$.

1.3. Modules, algèbres. — La notion de K-espace vectoriel K^n, centrale en algèbre linéaire, se généralise pour A anneau de la façon suivante :

Définition 1.10. — *Soit A un anneau. Un A-***module** *$(M, +, \cdot)$ est un ensemble muni d'une loi interne $+$ et d'une loi externe $A \times M \longrightarrow M, (\alpha, m) \mapsto \alpha m$ vérifiant :*
i. $(M, +)$ est un groupe commutatif,
ii. Pour tous $\alpha, \beta \in A$ et $m, m' \in M$ les propriétés suivantes sont satisfaites :
- (distributivité) $\alpha(m + m') = \alpha m + \alpha m'$, $(\alpha + \beta)m = \alpha m + \beta m$,
- (associativité) $(\alpha\beta)m = \alpha(\beta m)$,
- (élément neutre) $1 \cdot m = m$.
Un morphisme de A-modules est un morphisme A-linéaire $f : M \longrightarrow M'$ entre deux A-modules

$$f(\alpha m + \beta n) = \alpha f(m) + \beta f(n), \alpha, \beta \in A, m, n \in M.$$

Dans le cadre des modules, la notion et l'existence de bases sont plus subtiles que pour les espaces vectoriels et conduisent à mettre en exergue certaines familles particulières d'anneaux, tels que les anneaux euclidiens, principaux, factoriels

(§4), noethériens (§9)... Un A-module muni d'une structure d'anneau est dit A-algèbre :

Définition 1.11. — *Soit A un anneau. Une A-**algèbre** est un couple (B, ι) composé d'un anneau B et d'un morphisme d'anneaux $\iota : A \longrightarrow B$ (qui est souvent sous-entendu). Un morphisme de A-algèbres $(B, \iota) \longrightarrow (B', \iota')$ est un morphisme d'anneaux $f : B \longrightarrow B'$ tel que $f \circ \iota = \iota'$. L'ensemble des morphismes de A-algèbres est noté* $\mathrm{Hom}_{A-\mathrm{Alg}}(B, B')$.

En particulier, pour K un corps, les K-algèbres jouent un rôle central pour décrire les solutions d'équations polynomiales à coefficients dans K ; c'est l'objet de la théorie de Galois (§21).

2. Idéaux

Les idéaux apparaissent naturellement en algèbre comme noyaux de morphismes d'anneaux. En géométrie, tout système d'équations polynômiales est équivalent à la donnée d'un idéal. En théorie des nombres, les idéaux apparaissent pour palier à la non unicité de la factorisation.
Dans cette section, nous définissons (§2.1) différentes opérations sur les idéaux (addition, produit, intersection, radical...). Nous démontrons une version étendue du théorème chinois (§2.2). Ensuite (§2.3) nous caractérisons les idéaux qui conduisent à des anneaux quotients ayant de bonnes propriétés (intègres, réduits, corps...).

2.1. Idéaux, anneau quotient. —

Définition 2.1. — *Un* **idéal** *d'un anneau A est un sous-groupe additif $I \subset (A, +)$ tel que $AI \subset I$, i.e*

$$\forall a \in A, x \in I, ax \in I.$$

Un idéal I distinct de A est dit **propre**.

Proposition 2.2. — *Soit $S \subset A$ un ensemble non vide d'un anneau A. Nous notons (S) l'intersection de tous les idéaux de A contenant S. C'est un idéal et*

$$(S) = \{\sum_{s \in S} a_s s | a_s \in A \text{ presque tous nuls } \}.$$

Démonstration. — D'une part $I = \{\sum_{s \in S} a_s s | a_s \in A$ presque tous nuls $\}$ est inclus dans tout idéal contenant S. D'autre part I est un idéal. Donc $(S) = I$. □

Définition 2.3. — *Soit $S \subset A$ un ensemble non vide d'un anneau A. L'idéal (S) est dit* **idéal engendré** *par S. Les éléments de S sont dits* **générateurs** *de l'idéal (S).*

Pour $x \in A$, $(x) := (\{x\}) = Ax = \{ax | a \in A\}$ est dit idéal **principal** *engendré par x.*
Un idéal est dit **de type fini** *si $I = (S)$ avec S un ensemble fini.*

Exemples 2.4. — *i. Les idéaux $(0) = \{0\}$, $(1) = A$.*
Plus généralement $x \in A^* \Longleftrightarrow (x) = A$.
ii. Si $I \subset J$ sont deux idéaux de A avec J engendré par n éléments. Alors I n'est pas forcément engendré par n éléments. Par exemple dans $K[X_1, X_2]$ nous avons $(X_1) \subset (X_1, X_2) \subset (1)$.
iii. Soit K un corps. Le théorème de la base d'Hilbert (Théorème 9.8) établit que les idéaux de $K[X_1, \ldots, X_n]$ sont de type fini, ce qui n'est pas le cas dans $K[X_i, i \in \mathbb{N}]$.

Définition-Proposition 2.5. — *Soient I, J deux idéaux de A. Les opérations suivantes conduisent à la définition d'un idéal de A :*
- intersection $I \cap J$ et l'intersection d'une famille d'idéaux de A,
- somme $I + J = \{x + y | x \in I, y \in J\}$,
- produit $IJ =< \{xy | x \in I, y \in J\} >= \{\sum_{\alpha=1}^{r} x_\alpha y_\alpha | x_\alpha \in I, y_\alpha \in J, r \geq 1\}$,
- radical $\mathrm{rad}(I) = \{x \in A | \exists n \geq 1, x^n \in I\}$.

Démonstration. — Montrons que $\mathrm{rad}(I)$ est un idéal de A. Soit $f, g \in A$ et $n \in \mathbb{N}$ tels que $f^n, g^n \in I$. Alors

$$(f+g)^{2n-1} = \sum_{k=0}^{2n-1} \binom{2n-1}{k} f^k g^{2n-1-k} \in I$$

car $\max(k, 2n-1-k) \geq n$. □

Lorsque les idéaux sont de type fini, ces opérations s'expriment en termes de générateurs de I et J et mettent en évidence des propriétés arithmétiques de l'anneau A.

Exemples 2.6. — *i. Si $I = (x_1, \ldots, x_n)$ et $J = (y_1, \ldots, y_m)$ alors*

$$I + J = (x_1, \ldots, x_n, y_1, \ldots, y_m) \text{ et } IJ = (x_1y_1, \ldots, x_1y_m, x_2y_1, \ldots, x_ny_m).$$

ii. Soit $A = \mathbb{Z}$, $I = (m)$, $J = (n)$ pour $n, m \geq 1$. Alors

$$(m) + (n) = (m, n) = (\mathrm{PGCD}(n, m)), \quad (m) \cap (n) = (\mathrm{PPCM}(n, m)),$$

$$(m)(n) = (mn), \ \mathrm{rad}\,(m) = (m_0)$$

où m_0 est le produit des nombres premiers distincts divisant m.

Les idéaux d'un anneau A permettent de construire les anneaux quotients de A :

Définition 2.7. — *Pour tout idéal I de A, le groupe abélien quotient A/I a une unique structure d'anneau, dite* **anneau quotient**, *pour laquelle la projection canonique*

$$\pi : A \longrightarrow A/I, \quad x \mapsto x + I$$

est un morphisme d'anneaux. Son noyau est l'idéal $\ker \pi = I$.

Démonstration. — Le produit $\pi(x)\pi(y) = \pi(xy)$ est bien défini car si $\pi(x) = \pi(x')$ et $\pi(y) = \pi(y')$ alors $x - x' \in I$, $y - y' \in I$ et

$$xy - x'y' = x(y - y') + y'(x - x') \in AI + AI \subset I + I = I,$$

i.e $\pi(xy) = \pi(x'y')$. □

Exemples 2.8. — *i. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est l'anneau quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.*
ii. L'anneau quotient A/I est l'anneau des classes d'équivalence $x \equiv y \mod I \Longleftrightarrow x - y \in I$.

Proposition 2.9. — *i. (Propriété universelle). Pour tout morphisme d'anneaux $f : A \longrightarrow B$ et tout idéal I de A tel que $I \subset \ker f$, il existe un unique morphisme d'anneaux $\bar{f} : A/I \longrightarrow B$ tel que $\bar{f} \circ \pi = f$.*
ii. (Théorème d'isomorphisme). Pour tout morphisme d'anneaux, $f : A \longrightarrow B$, le morphisme $\bar{f}$ induit un isomorphisme $\bar{f} : A/\ker f \longrightarrow \mathrm{im}(f)$.

Démonstration. — i. Nous définissons $\bar{f}(\pi(x)) := f(x)$.
ii. Le morphisme $\bar{f} : A/\ker f \longrightarrow \mathrm{im}(f)$ est bijectif, c'est donc un isomorphisme. □

Exemples 2.10. — *i. Si A est un anneau et $f = X^d + a_1X^{d-1} + \cdots + a_d \in A[X]$ un polynôme unitaire de degré $d \geq 1$, l'anneau quotient*

$$A[X]/(f) = \{g \mod f | g \in A[X], \deg(g) < d\}.$$

En particulier, pour $f = X - a$ ($a \in A$), l'idéal $(X - a)$ coïncide avec le noyau de l'évaluation

$$\mathrm{ev}_a : A[X] \longrightarrow A, \quad g(X) \mapsto g(a)$$

qui induit un isomorphisme

$$\overline{\mathrm{ev}}_a : A[X]/(X - a) \longrightarrow A.$$

iv. De même, l'application surjective d'évaluation

$$\mathrm{ev}_i : \mathbb{R}[X] \longrightarrow \mathbb{R}[i] = \mathbb{C}, \quad g(X) \mapsto g(i),$$

a pour noyau $\ker \mathrm{ev}_i = (X^2 + 1)\mathbb{R}[X]$ *et induit un isomorphisme*

$$\overline{\mathrm{ev}}_i : \mathbb{R}[X]/(X^2 + 1) \xrightarrow{\simeq} \mathbb{C}.$$

Sa restriction à $\mathbb{Z}[X] \subset \mathbb{R}[X]$ induit un isomorphisme

$$\overline{\mathrm{ev}}_i : \mathbb{Z}[X]/(X^2 + 1) \longrightarrow \mathbb{Z}[i].$$

v. Si $f : A \longrightarrow B$ est un morphisme d'anneaux et I est un idéal de B alors l'image réciproque $f^{-1}(I)$ est un idéal de A. En effet,

$$f^{-1}(I) = \ker(\pi \circ f : A \longrightarrow B \longrightarrow B/I).$$

vi. Passer au quotient permet de montrer que certaines équations n'ont pas de solution dans A en montrant qu'elles n'ont pas de solution dans A/I. Par exemple $x^2 - 10y^2 = 2$ n'a pas de solution $(x, y) \in \mathbb{Z}^2$ car n'a pas de solution dans l'anneau quotient $\mathbb{Z}/5\mathbb{Z}$ (en effet 2 n'est pas un carré modulo 5). Déduire des solutions dans A de solutions dans A/I peut s'avérer plus subtile (voir §24).

2.2. Théorème des restes chinois. — L'objet de ce paragraphe est la généralisation du lemme chinois : pour $m, n \in \mathbb{Z}$ premiers entre eux,

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Définition 2.11. — *Soient $A_1, \ldots, A_n$, $n \geq 2$ des anneaux. L'ensemble produit $A = A_1 \times \cdots \times A_n$ est muni d'une structure naturelle d'anneau via*

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$

$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n),$$

avec $1_A = (1, \ldots, 1) = (1_{A_1}, \ldots, 1_{A_n})$.

Proposition 2.12. — *Soit A un anneau, I, J des idéaux de A avec $I + J = (1) = A$. Alors $I \cap J = IJ$ et l'application*

$$A/(I \cap J) \xrightarrow{\simeq} A/I \times A/J, \quad x + I \cap J \mapsto (x + I, x + J)$$

est un isomorphisme d'anneaux.

Démonstration. — L'application $\alpha : A \longrightarrow A/I \times A/J$, $\alpha(x) = (x + I, x + J)$ est un morphisme d'anneaux de noyau $\ker \alpha = I \cap J$ qui induit un isomorphisme $\overline{\alpha} : A/(I \cap J) \xrightarrow{\simeq} \mathrm{im}(\alpha)$. Il suffit donc de vérifier que α est surjective. Par hypothèse, il existe $i \in I$ et $j \in J$ tel que $i + j = 1$. Ainsi $\alpha(i) = (0, 1)$ et $\alpha(j) = (1, 0)$. Donc $\alpha(yi + xj) = (x + I, y + J)$ pour tous $x, y \in A$.
L'inclusion $IJ \subset I \cap J$ est toujours vérifiée. Réciproquement si $a \in I \cap J$, $a = ai + aj \in JI + IJ = IJ$. □

Corollaire 2.13. — *(Théorème des restes chinois).*
Soit A un anneau et $I_1, \ldots, I_n$ des idéaux de A tels que $I_j + I_k = (1)$ pour $j \neq k$. Alors $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ et l'application

$$A/(I_1 \cap \cdots \cap I_n) \xrightarrow{\simeq} A/I_1 \times \cdots \times A/I_n, \quad x + (I_1 \cap \cdots \cap I_n) \mapsto (x + I_1, \ldots, x + I_n)$$

est un isomorphisme d'anneaux.

Exemple 2.14. — *Soit $n \geq 2$ et $\zeta \in \mathbb{C}$ une racine complexe primitive n-ième de l'unité. Le n-ième polynôme cyclotomique est le polynôme irréductible de $\mathbb{Z}[X]$ défini par $\Phi_n = \Pi_{1 \leq k \leq n, (k,n)=1}(X - \zeta^k)$. Nous avons $X^n - 1 = \Pi_{d|n}\Phi_d$ et les Φ_d sont premiers entre eux deux à deux. Ainsi d'après le lemme chinois*

$$\mathbb{Q}[X]/(X^n - 1) = \Pi_{d|n}\mathbb{Q}[X]/(\Phi_d).$$

Définition 2.15. — *Un élément e d'un anneau A est dit* **idempotent** *s'il vérifie $e^2 = e$. Deux idempotents e_1, e_2 sont dits* **orthogonaux** *si $e_1 e_2 = 0$.*

Exemples 2.16. — *i. Les éléments neutres 0,1 sont les idempotents triviaux de A. Dans $\mathbb{Z}/6\mathbb{Z}$, 3,4 sont les seuls idempotents non triviaux.*
ii. Soit T un espace topologique et $\mathcal{C}(T, \mathbb{R})$ l'anneau des fonctions continues de T dans $\mathbb{R}$. Un idempotent de $\mathcal{C}(T, \mathbb{R})$ est une fonction à valeurs dans $\{0, 1\}$. Donc si T est connexe, il n'y a pas d'idempotent non trivial.
iii. L'ensemble des idempotents de A muni des lois $*, \cdot$ ($a*b = a+b-2ab, a \cdot b = ab$) est un anneau.
iv. Si e est un idempotent de A, $1-e$ aussi et A s'identifie au produit des anneaux Ae et $A(1-e)$: l'isomorphisme d'anneaux

$$A \longrightarrow Ae \times A(1-e), \quad a \mapsto (ae, a(1-e))$$

a pour réciproque $(x, y) \mapsto x + y$.
v. Soient m, n deux entiers premiers entre eux. Soit $u, v \in \mathbb{Z}$ avec $mu + nv = 1$. Par conséquent $(mu)^2 \equiv mu \mod nm$. Donc $e \equiv mu \mod nm$ est un élément nilpotent de $\mathbb{Z}/nm\mathbb{Z}$, $(\mathbb{Z}/nm\mathbb{Z})e = mu\mathbb{Z}/nm\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$, $(1-e)(\mathbb{Z}/nm\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}$. Nous retrouvons le lemme chinois $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Lemme 2.17. — *Avec les notations de la définition 2.11, les projections*

$$\pi_k : A \longrightarrow A_k, \quad \pi_k(x_1, \ldots, x_n) = x_k, \ 1 \leq k \leq n$$

sont des morphismes d'anneaux.
Les inclusions

$$i_k : A_k \longrightarrow A, \quad i_k(x_k) = (0, \ldots, x_k, \ldots, 0), \quad 1 \leq k \leq n$$

ne sont pas des morphismes d'anneaux car $e_k = i_k(1_{A_k}) = (0, \ldots, 1, \ldots, 0) \neq 1_A$. Les éléments e_k, $1 \leq k \leq n$ satisfont les propriétés suivantes pour tous $1 \leq j < k \leq n$:
i. $e_k^2 = e_k$ (idempotent),
ii. $e_j e_k = 0$ (orthogonalité),
iii. $e_1 + \cdots + e_n = 1$.

Proposition 2.18. — *Soit A un anneau et $e_1, \ldots, e_n \in A$ des idempotents orthogonaux tels que $e_1 + \cdots + e_n = 1$. Alors pour tout $1 \leq k \leq n$, le sous-ensemble $A_k = e_k A = \{e_k a | a \in A\} \subset A$ muni des opérations induites de l'addition et de la multiplication de A, est un anneau d'unité $1_{A_k} = e_k$. Les applications*

$\pi_k : A \longrightarrow A_k, \pi_k(a) = e_k a$ sont des morphismes d'anneaux qui induisent un isomorphisme

$$\pi = (\pi_1, \dots, \pi_n) : A \xrightarrow{\simeq} A_1 \times \cdots \times A_n, \quad \pi(a) = (e_1 a, \dots, e_n a),$$

qui a pour inverse $\pi^{-1}(a_1, \dots, a_n) = e_1 a_1 + \cdots + e_n a_n$. Pour tout idéal I de A, l'image $I_k = e_k(I) = e_k I$ est un idéal de A_k et $\pi(I) = I_1 \times \cdots \times I_n$.

2.3. Idéaux premiers, idéaux maximaux. —

2.3.1. Idéaux premiers et maximaux. —

Définition 2.19. — *Soit I un idéal propre ($I \neq A$) d'un anneau A.*
L'idéal I est dit **maximal**, *s'il est maximal pour l'inclusion parmi les idéaux propres de A.*
L'idéal I est dit **premier**, *si*

$$\forall x, y \in A, xy \in I \Longrightarrow \Big(x \in I \text{ ou } y \in I\Big).$$

L'ensemble des idéaux premiers de A est noté $\operatorname{Spec} A$. *L'ensemble des idéaux maximaux de A est noté* $\operatorname{Spm} A$.

Exemples 2.20. — *i. L'idéal* (0) *est premier si et seulement si A est intègre.*
ii. La terminologie "spectre premier" (pour Spec*) ou "spectre maximal" (pour* Spm*) qui justifie les notations introduites est réservée à ces ensembles munis de topologie de Zariski (§15,16).*

Proposition 2.21. — *Soit I un idéal propre d'un anneau A.*
i. L'idéal I est premier si et seulement si A/I est intègre.
ii. L'idéal I est maximal si et seulement si A/I est un corps.

Démonstration. — i. Soit $\pi : A \longrightarrow A/I$ la projection canonique. Soient $x, y \in A$ avec $\pi(x), \pi(y) \neq 0$. Alors $x, y \notin I$.
Si I est premier, alors $xy \notin I$, donc $\pi(x)\pi(y) \neq 0$, donc A/I intègre.
Réciproquement si A/I intègre, $\pi(x)\pi(y) \neq 0$ donc $xy \notin I$, donc I est premier.
ii. De même, $I \neq A$ est maximal parmi les idéaux propres de A si et seulement si

$$\forall x \notin I,\ I + (x) = A \Longleftrightarrow \forall x \notin I, (\pi(x)) = A/I \Longleftrightarrow$$
$$\forall x \notin I, \pi(x) \in (A/I)^* \Longleftrightarrow (A/I)^* = A/I - \{0\}.$$

□

Exemples 2.22. — *i. Si K est un corps,* $\operatorname{Spec} K = \{(0)\}$. *Si ces ensembles (topologiques) sont identiques pour tous les corps, ils sont munis d'une structure supplémentaire, dite schéma (espace topologique muni d'un anneau de fonctions sur cet espace topologique) qui permet de les différencier.*
ii. L'ensemble $\operatorname{Spm} \mathbb{Z} = \{(p), p \text{ nombre premier}\}$, $\operatorname{Spec} \mathbb{Z} = \operatorname{Spm} \mathbb{Z} \cup \{(0)\}$.
iii. Soit $\mathbb{C}$ le corps des nombres complexes. Alors $\operatorname{Spm} \mathbb{C}[X] = \{(X - a), a \in \mathbb{C}\}$ *et* $\operatorname{Spec} \mathbb{C}[X] = \operatorname{Spm} \mathbb{C}[X] \cup \{(0)\}$ *(voir Ex. 4.15).*

iv. L'ensemble $\operatorname{Spm}\mathbb{Z}[X]$ *est l'ensemble des couples* (p, P) *où* $p \in \mathbb{N}$ *est nul ou premier et* $P \in \mathbb{Z}[X]$ *est un polynôme irréductible modulo* p *(voir Exemples 4.3).*

Lemme 2.23. — *Soit* I *un idéal de* A *et* $\pi : A \longrightarrow A/I$ *la projection canonique. Il y a une bijection naturelle entre*

$$\{\textit{idéaux } \overline{J} \textit{ de } A/I\} \longleftrightarrow \{\textit{idéaux } J \textit{ de } A \textit{ contenant } I\},$$

via $\bar{J} \mapsto \pi^{-1}(\overline{J})$ *et* $J/I \leftarrow J$ *si* $I \subset J$. *De plus* $(A/I)/\overline{J} = A/J$.
Cette bijection induit par restriction des bijections :

$$\{\mathfrak{p} \in \operatorname{Spec} A | I \subset \mathfrak{p}\} \longleftrightarrow \operatorname{Spec} A/I,$$
$$\{\mathfrak{m} \in \operatorname{Spm} A | I \subset \mathfrak{m}\} \longleftrightarrow \operatorname{Spm} A/I.$$

Démonstration. — Si $\mathfrak{p}$ est un idéal de A et $I \subset \mathfrak{p}$, nous avons $A/\mathfrak{p} = (A/I)/(\mathfrak{p}/I)$. Donc $A/\mathfrak{p}$ est intègre si et seulement si $(A/I)/(\mathfrak{p}/I)$ est intègre. Le cas des idéaux maximaux est identique. □

Lemme 2.24. — *Soit* A *un anneau.*
i. Soit $I_1, \ldots, I_k$ *des idéaux et* $\mathfrak{p} \in \operatorname{Spec} A$ *tels que* $\cap_{j=1}^k I_j \subset \mathfrak{p}$. *Alors il existe* j *tel que* $I_j \subset \mathfrak{p}$.
ii. Soit $I, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *des idéaux de* A, $n \geq 1$, $\mathfrak{p}_i \in \operatorname{Spec} A$ *et* $I \subset \bigcup_{j=1}^n \mathfrak{p}_i$. *Alors il existe* j *tel que* $I \subset \mathfrak{p}_j$.

Démonstration. — i. Raisonnons par l'absurde en supposant pour tout i, $I_i \not\subset \mathfrak{p}$. Alors, pour tout i, il existe $a_i \in I_i - \mathfrak{p}$ et $a_1 \cdots a_k \in \cap_{i=1}^k I_i - \mathfrak{p}$ car $\mathfrak{p}$ est premier.
ii. Nous pouvons supposer que si $i \neq j$, $\mathfrak{p}_i \not\subset \mathfrak{p}_j$. Raisonnons par induction et contraposition : supposons que $I \not\subset \mathfrak{p}_i$ pour $i = 1, \ldots, n$ et montrons que pour tout $m = 1, \ldots, n$, il existe $x_m \in I - \cup_{i=1}^m \mathfrak{p}_i$.
Supposons $m \geq 2$ et qu'il existe $x_{m-1} \in I - \cup_{i=1}^{m-1} \mathfrak{p}_i$ (induction). Comme $I, \mathfrak{p}_1, \ldots, \mathfrak{p}_{m-1} \not\subset \mathfrak{p}_m$, il existe $a_i \in \mathfrak{p}_i - \mathfrak{p}_m$ pour tout $i = 1, \ldots, m-1$ et $a_m \in I - \mathfrak{p}_m$. Ainsi $z = a_1 \cdots a_m \in I \cap \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{m-1} - \mathfrak{p}_m$ et $x_m = x_{m-1}$ ou $x_m = x_{m-1} + z$ convient (suivant que $x_{m-1} \notin \mathfrak{p}_m$ ou $x_{m-1} \in \mathfrak{p}_m$). □

Lemme 2.25. — *(Fonctorialité).*
i. Tout morphisme d'anneaux $f : A \longrightarrow B$ *induit une application*

$$f^* : \operatorname{Spec} B \longrightarrow \operatorname{Spec} A$$

définie par $f^*(\mathfrak{p}) = f^{-1}(\mathfrak{p})$.
ii. Si f *est surjectif, alors* f^* *est injectif et* $f^*(\operatorname{Spec} B) = \{\mathfrak{q} \in \operatorname{Spec} A, \ker f \subset \mathfrak{q}\}$.
iii. En général, $f^*(\operatorname{Spm} B) \not\subset \operatorname{Spm} A$.

Démonstration. — i. Si $I \subset B$ est un idéal (quelconque) de B alors f induit un homomorphisme injectif d'anneaux $A/f^{-1}(I) \longrightarrow B/I$. Si $\mathfrak{p} \in \operatorname{Spec} B$, alors $B/\mathfrak{p}$ est intègre donc $A/f^{-1}(\mathfrak{p})$ est intègre (il est non nul car $1 \notin f^{-1}(\mathfrak{p})$) et $f^{-1}(\mathfrak{p}) \in \operatorname{Spec} A$. Par conséquent f^* est bien définie.
ii. L'application surjective f induit une bijection entre $A/\ker f$ et B. D'après

le lemme 2.23, nous avons une bijection naturelle (croissante pour l'inclusion) entre $\mathrm{Spec}(A/\ker f)$ et $\{\mathfrak{q} \in \mathrm{Spec}\, A, \ker f \subset \mathfrak{q}\}$. Donc f^* injective d'image $f^*(\mathrm{Spec}\, B) = \{\mathfrak{q} \in \mathrm{Spec}\, A, \ker f \subset \mathfrak{q}\}$.
iii. Soit l'inclusion $f : \mathbb{Z} \longrightarrow \mathbb{Q}$. Alors $(0) \in \mathrm{Spm}\,\mathbb{Q}$ mais $f^{-1}((0)) = (0) \notin \mathrm{Spm}\,\mathbb{Z}$. □

Exemple 2.26. — *Si $f : A \longrightarrow B$ et $g : B \longrightarrow C$ sont des morphismes d'anneaux, nous avons $(g \circ f)^* = f^* \circ g^*$. Nous avons ainsi construit un foncteur contravariant de la catégorie des anneaux dans la catégorie des ensembles (§7.2).*

2.3.2. Existence d'un idéal maximal. — Dans ce cours, nous considérons le lemme de Zorn comme un axiome de la théorie axiomatique des ensembles. Cependant, nous prendrons soin de préciser explicitement dans ce texte lorsque nous y aurons recours. Admettre le lemme de Zorn est équivalent à admettre l'axiome du choix qui postule qu'un produit d'ensembles non vides est non vide.

Lemme 2.27. — *(Zorn) Soit $(E, \leq)$ un ensemble partiellement ordonné non vide, inductif (i.e. tel que pour toute partie $E' \subset E$ totalement ordonnée, il existe $x \in E$ tel que $x' \leq x$, pour tout $x' \in E'$). Alors E a un élément maximal.*

Théorème 2.28. — *Si l'anneau A est non nul, alors* $\mathrm{Spm}\, A \neq \emptyset$.

Démonstration. — Soit S l'ensemble des idéaux propres de A. L'ensemble S est non vide car contient (0), il est partiellement ordonné pour l'inclusion et il est inductif : tout sous-ensemble totalement ordonné $\{I_\alpha\} \subset S$ admet une borne supérieure (l'union de tous ses éléments). D'après le lemme de Zorn, l'ensemble S contient un élément maximal. □

Corollaire 2.29. — *Soit A un anneau.*
i. Tout idéal I propre de A est contenu dans un idéal maximal.
ii. $A - A^* = \cup_{\mathfrak{m} \in \mathrm{Spm}\, A} \mathfrak{m}$.

Démonstration. — i. Soit $\pi : A \longrightarrow A/I$, $\bar{\mathfrak{m}} \in \mathrm{Spm}\, A/I$. Il suffit alors de prendre $\mathfrak{m} = \pi^{-1}(\bar{\mathfrak{m}})$.
ii. Si $x \in A^*$ alors pour tout $\mathfrak{m} \in \mathrm{Spm}\, A$, $x \mod \mathfrak{m} \in (A/\mathfrak{m})^* = (A/\mathfrak{m}) - \{0\}$, donc $x \notin \mathfrak{m}$. Réciproquement si $x \notin A^*$, alors $(x) \neq A$ donc il existe $\mathfrak{m} \in \mathrm{Spm}\, A$ avec $(x) \subset \mathfrak{m}$. □

Lemme 2.30. — *Soit $A \neq 0$ un anneau. Tout idéal premier $\mathfrak{p}$ de A contient un idéal premier minimal.*

Démonstration. — En effet, l'ensemble $E = \{\mathfrak{q} \text{ premier}, \mathfrak{q} \subset \mathfrak{p}\}$ (non vide car $\mathfrak{p} \in E$) est muni de l'ordre partiel $\mathfrak{q} < \mathfrak{q}' \Longleftrightarrow \mathfrak{q}' \subsetneq \mathfrak{q}$. Soit $(\mathfrak{p}_\lambda)_{\lambda \in \Lambda}$ une partie de E totalement ordonnée par inclusion avec $\Lambda \neq \emptyset$. Par le lemme de Zorn, il suffit de montrer que $\mathfrak{p}_0 = \cap_{\lambda \in \Lambda} \mathfrak{p}_\lambda$ est un idéal premier. Soit $x, y \in A$ avec $xy \in \mathfrak{p}_0$. Si $y \notin \mathfrak{p}_0$, il existe $\lambda \in \Lambda$ avec $y \notin \mathfrak{p}_\lambda$, donc $y \notin \mathfrak{p}_\mu$ pour tout $\mathfrak{p}_\mu \subset \mathfrak{p}_\lambda$. Par

primalité des idéaux, $x \in \mathfrak{p}_\mu$ pour tout $\mathfrak{p}_\mu \subset \mathfrak{p}_\lambda$ et comme la famille d'idéaux est totalement ordonnée $x \in \mathfrak{p}_\mu$ pour tout $\mu \in \Lambda$. Ainsi $x \in \mathfrak{p}_0$ et $\mathfrak{p}_0$ est premier. $\square$

2.3.3. Radicaux. —

Définition 2.31. — *Soit A un anneau. L'idéal*

$$\mathcal{J}(A) = \cap_{\mathfrak{m} \in \operatorname{Spm} A} \mathfrak{m}$$

est dit **radical de Jacobson** *de A.*

Théorème 2.32. — *Soit $A \neq 0$ un anneau et $\mathcal{J}(A)$ son radical de Jacobson. Soit $f \in A$. Alors $f \in \mathcal{J}(A)$ si et seulement si $1 - af \in A^*$ pour tout $a \in A$.*

Démonstration. — Si $f \in \mathcal{J}(A)$ et $a \in A$, l'élément $1 - af$ n'est contenu dans aucun idéal maximal (car si $1 - af \in \mathfrak{m} \in \operatorname{Spm} A$, $1 = (1 - af) + af \in \mathfrak{m}$ exclu.) Donc $1 - af$ est inversible.
Réciproquement, soit $f \notin \mathcal{J}(A)$. Il existe $\mathfrak{m} \in \operatorname{Spm} A$ avec $f \notin \mathfrak{m}$. Alors $\overline{f} \in A/\mathfrak{m}$ et $\overline{f} \neq 0$. Comme $A/\mathfrak{m}$ est un corps, il existe $a \in A$ tel que $\overline{a}\overline{f} = \overline{1}$ donc $1 - af \in \mathfrak{m}$ et $1 - af$ n'est pas inversible. $\square$

Soit A un anneau et I un idéal. Nous rappelons que

$$\operatorname{rad}(I) = \{a \in A | \exists n \geq 1, a^n \in I\}.$$

Définition 2.33. — *Soit A un anneau.*
i. L'ensemble $\operatorname{rad}(0)$ *des éléments* **nilpotents** *de A est dit* **nilradical** *de A.*
ii. L'anneau A est dit **réduit** *si* $\operatorname{rad}(0) = (0)$.
Nous notons $A^{\mathrm{red}} = A/\operatorname{rad}(0)$ le plus grand anneau réduit quotient de A.

Exemples 2.34. — *i. Soit p un nombre premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est intègre donc réduit. Si $n \geq 2$, l'anneau $\mathbb{Z}/p^n\mathbb{Z}$ n'est pas réduit et* $\operatorname{rad}(0) = p\mathbb{Z}/p^n\mathbb{Z}$.
ii. L'anneau $(A/I)^{\mathrm{red}} = A/\operatorname{rad}(I)$ est le plus grand anneau réduit quotient de A/I.
iii. Le morphisme $\pi : A \longrightarrow A^{\mathrm{red}}$ vérifie la propriété universelle suivante : pour tout morphisme d'anneaux $f : A \longrightarrow B$ où B est réduit, il existe un unique morphisme $\bar{f} : A^{\mathrm{red}} \longrightarrow B$ tel que $f = \bar{f} \circ \pi$.
iv. La projection canonique $\pi : A \longrightarrow A^{\mathrm{red}}$ induit des bijections

$$\pi^* : \operatorname{Spec} A^{\mathrm{red}} \longrightarrow \operatorname{Spec} A, \quad \operatorname{Spm} A^{\mathrm{red}} \longrightarrow \operatorname{Spm} A.$$

v. Nous avons $A[X]^* = A^* + \operatorname{rad}(0)[X]$.
vi. Dans le langage des catégories, le foncteur $A \longrightarrow A^{\mathrm{red}}$ de la catégorie des anneaux vers la catégorie des anneaux réduits est un adjoint à gauche du foncteur d'oubli (§7.4).

Proposition 2.35. — *Soit A un anneau.*
i. Le nilradical $\operatorname{rad}(0) = \cap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$.
ii. Plus généralement, si I idéal de A, $\operatorname{rad}(I)$ *est l'intersection des idéaux premiers de A qui contiennent I.*

Démonstration. — i. Si $f \in A$ est nilpotent, il existe $n \in \mathbb{N}$ avec $f^n = 0$, donc $f^n \in \mathfrak{p}$ pour tout $\mathfrak{p} \in \operatorname{Spec} A$ donc $f \in \mathfrak{p}$ et $f \in \cap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$.
Réciproquement, si $f \in A$ n'est pas nilpotent, notons

$$S_f = \{f^n, n \in \mathbb{N}\}$$

et E l'ensemble des idéaux de A tels que $I \cap S_f = \emptyset$, muni de la relation d'ordre donnée par l'inclusion d'idéaux. Comme $0 \notin S_f$, $(0) \in E$, donc E n'est pas vide. Si $(I_\lambda)_{\lambda \in \Lambda}$ est une famille totalement ordonnée non vide d'éléments de E, alors $\cup_{\lambda \in \Lambda} I_\lambda \in E$. Par le lemme de Zorn, E possède un élément maximal I. Montrons que $I \in \operatorname{Spec} A$. Soit $x, y \in A - I$. Par maximalité de I, nous avons $I + xA, I + yA \notin E$, donc il existe $n, m \in \mathbb{N}$, $a, a' \in A$, $b, b' \in I$ tels que $f^n = ax + b$ et $f^m = a'y + b'$. Donc $f^{n+m} = aa'xy + axb' + ba'y + bb' \notin I$. Donc $aa'xy \notin I$, donc $xy \notin I$, donc I est premier. Comme $f \notin I$, $f \notin \cap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$.
ii. Pour $\pi : A \longrightarrow A/I$, nous avons

$$\operatorname{rad}(I) = \pi^{-1}(\operatorname{rad}(0)) = \cap_{\{\mathfrak{p} \in \operatorname{Spec} A/I\}} \pi^{-1}\mathfrak{p}.$$

Or $\{\pi^{-1}\mathfrak{p}, \mathfrak{p} \in \operatorname{Spec} A/I\}$ est l'ensemble des idéaux premiers de A qui contiennent I. □

Exemple 2.36. — *i. Soit I, J deux idéaux de A alors*

$$\operatorname{rad}(I) \cap \operatorname{rad}(J) = \operatorname{rad}(I \cap J) = \operatorname{rad}(IJ).$$

ii. Soit $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ des idéaux maximaux distincts de A. Ainsi $\mathfrak{m}_i + \mathfrak{m}_j = A$ pour $i \neq j$ et $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r = \mathfrak{m}_1 \cdots \mathfrak{m}_r$. Soit $I = \mathfrak{m}_1^{n_1} \cdots \mathfrak{m}_r^{n_r}$. D'après le théorème chinois 2.13,

$$(A/I)^{\mathrm{red}} = A/\operatorname{rad}(I) = A/\mathfrak{m}_1 \cdots \mathfrak{m}_r = A/(\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r) \xrightarrow{\simeq} A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_r.$$

Donc $(A/I)^{\mathrm{red}}$ est un produit de corps.
iii. Pour $t \in [0,1]$, notons $I_t \subset \mathcal{C}([0,1], \mathbb{R})$ l'ensemble des fonctions $f : [0,1] \longrightarrow \mathbb{R}$ telles que $f^{-1}(0)$ est un voisinage de t. Alors I_t est un idéal de $\mathcal{C}([0,1], \mathbb{R})$ et il existe des idéaux premiers non maximaux $\mathfrak{p}$, tels que $I_t \subset \mathfrak{p}$. En effet I_t est un idéal qui vérifie $\operatorname{rad}(I_t) = I_t$. Donc I_t est l'intersection des idéaux premiers qui le contiennent. Le seul idéal maximal qui contient I_t est l'idéal $\mathfrak{m}_t$ des fonctions qui s'annulent au point t. Comme $I_t \neq \mathfrak{m}_t$, la propriété annoncée est démontrée. En particulier $\mathcal{C}([0,1], \mathbb{R})$ a des idéaux premiers non maximaux, cependant il n'est pas facile de les décrire directement.
iv. Les idéaux radiciels, i.e égaux à leur radical, sont les objets élémentaires de la géométrie algébrique (Corollaire 14.9). L'idéal de Jacobson donne un critère utile de nullité de certains A-modules de type fini (Lemme de Nakayama 11.17).

3. Localisation

La localisation d'un anneau en une partie multiplicative (§3.1) permet de construire des anneaux ayant un unique idéal maximal (§3.2) et de plonger tout

anneau intègre dans son corps de fractions. Nous précisons également l'opération induite par la localisation sur les spectres d'idéaux premiers (§3.2).

3.1. Parties multiplicatives. —

Définition 3.1. — *Une* **partie multiplicative** *d'un anneau A est un sous-ensemble S de A stable par multiplication, contenant 1.*

Définition-Proposition 3.2. — *Soit A un anneau et S une partie multiplicative de A. La relation*

$$(a, s) \sim (a', s') \Longleftrightarrow \exists u \in S \text{ tel que } uas' = ua's$$

est une relation d'équivalence sur $A \times S$. Notons $\frac{a}{s}$ la classe d'équivalence de (a, s). L'ensemble des classes d'équivalence $S^{-1}A$ est muni d'une structure d'anneau, dit anneau localisé, via les opérations

$$\frac{a}{s} + \frac{b}{r} = \frac{ar + bs}{sr}, \quad \frac{a}{s}\frac{b}{r} = \frac{ab}{sr}.$$

L'application de localisation $j : A \longrightarrow S^{-1}A$, $a \mapsto \frac{a}{1}$ est un morphisme d'anneaux.

Démonstration. — Les opérations sont bien définies, associatives et commutatives. Montrons que l'addition est bien définie, les autres propriétés sont analogues. Pour $(a, s) \sim (a', s')$ et $(b, r) \sim (b', r')$, alors il existe $u, v \in S$ avec $u(as' - a's) = 0 = v(br' - b'r)$. Donc $uv(ar + bs)s'r' = uv(a'r' + b's')sr$ d'où $(ar + bs, sr) \sim (a'r' + b's', s'r')$.
L'élément neutre de l'addition est $\frac{0}{s}$ pour tout $s \in S$ et l'unité est $\frac{1}{1}$. La multiplication est distributive par rapport à l'addition. □

Exemple 3.3. — *i Si $0 \in S$ alors $S^{-1}A = 0$. Ceci explique que, dans la littérature, la définition des ensembles multiplicatifs impose parfois qu'ils ne contiennent pas 0.*
ii. Soit A un anneau et S une partie multiplicative. L'élément $a/s \in S^{-1}A$ satisfait $a/s = 0/1$ si et seulement si il existe $u \in S$ tel que $ua = 0$ dans A. Par conséquent, pour $A \neq 0$, l'application de localisation $j : A \longrightarrow S^{-1}A$ est injective si et et seulement si aucun élément de S n'est diviseur de 0.
iii. Soit $t \in A$. Alors la partie

$$S_t = \{1, t, t^2, \ldots\}$$

est un sous-ensemble multiplicatif de A.
Si $d \in N^*$ alors $S_d^{-1}\mathbb{Z}$ consiste en les éléments de $\mathbb{Q}$ dont les dénominateurs divise une puissance de d :

$$S_d^{-1}\mathbb{Z} = \{a/d^n \in \mathbb{Q} | a \in \mathbb{Z}, n \in \mathbb{N}\}.$$

Nous construisons ainsi le corps des nombres décimaux et la décomposition en base ≥ 2 .
vi. Si $A = K[X_1, \ldots, X_n]$ est un anneau de polynômes à n variables à coefficients

dans un corps K. Soit $P \in A$, un polynôme arbitraire. Alors $S_P^{-1}A$ est l'anneau des fractions

$$S_P^{-1}A = \left\{ \frac{Q}{P^m}, Q \in A, m \in \mathbb{N} \right\}.$$

3.2. Idéaux des anneaux localisés. —

Lemme 3.4. — *Soit A un anneau, I un idéal de A, $S \subset A$ une partie multiplicative et $j : A \longrightarrow S^{-1}A$ l'application de localisation. Alors*

$$S^{-1}I = \{a/s \in S^{-1}A, a \in I, s \in S\}$$

est un idéal de $S^{-1}A$ et tout idéal $J \subset S^{-1}A$ est de cette forme : $J = S^{-1}(j^{-1}J)$.

Démonstration. — L'inclusion $S^{-1}(j^{-1}J) \subset J$ est claire. Réciproquement soit $a/s \in J$. Alors $a/1 = (a/s)(s/1) \in J$ donc $a \in j^{-1}J$ et $a/s \in S^{-1}(j^{-1}J)$. □

Proposition 3.5. — *Soit A un anneau, $S \subset A$ une partie multiplicative, $j : A \longrightarrow S^{-1}A$ l'application de localisation. L'application*

$$j^* : \operatorname{Spec} S^{-1}A \longrightarrow \operatorname{Spec} A$$

est injective et son image est $\{\mathfrak{p} \in \operatorname{Spec} A, S \cap \mathfrak{p} = \emptyset\}$.

Démonstration. — D'après le lemme 3.4, l'application j^* est injective.
Soit $\mathfrak{q} \in \operatorname{Spec} S^{-1}A$ et $\mathfrak{p} = j^*\mathfrak{q}$. Si $t \in S \cap \mathfrak{p}$ alors $1 = t/t \in S^{-1}\mathfrak{p} = \mathfrak{q}$, donc $\mathfrak{q}$ n'est pas propre, ce qui est absurde. Donc $S \cap \mathfrak{p} = \emptyset$ et $j^*(\operatorname{Spec} S^{-1}A) \subset \{\mathfrak{p} \in \operatorname{Spec} A, \mathfrak{p} \cap S = \emptyset\}$.
Réciproquement si $\mathfrak{p} \in \{\mathfrak{p} \in \operatorname{Spec} A, S \cap \mathfrak{p} = \emptyset\}$. Alors $S^{-1}\mathfrak{p}$ est un idéal premier. En effet si $(a/s) \cdot (b/r) = ab/rs \in S^{-1}\mathfrak{p}$ alors il existe $u \in S$ et $c \in \mathfrak{p}$ avec $ab/rs = c/u$. Donc il existe $v \in S$ tel que $abuv = crsv$ dans A donc $abuv \in \mathfrak{p}$. Comme $uv \in S$, $ab \in \mathfrak{p}$ donc a/s ou b/r dans $S^{-1}\mathfrak{p}$ qui est donc premier. L'idéal $S^{-1}\mathfrak{p}$ est propre car si $1 \in S^{-1}\mathfrak{p}$, il existe $c \in \mathfrak{p}$ et $u \in S$ tels que $1/1 = c/u$. Donc il existe $v \in S$ avec $uv = cv$ dans A ce qui est exclu car $uv \in S$ et $S \cap \mathfrak{p} = \emptyset$. □

La définition suivante explique le choix de la terminologie.

Définition-Proposition 3.6. — *Un anneau* **local** *est un anneau n'admettant qu'un idéal maximal.*
Si $\mathfrak{p}$ est un idéal premier $S = A - \mathfrak{p}$ est multiplicative. Le localisé $S^{-1}A = A_\mathfrak{p}$ de A en $\mathfrak{p}$ est un anneau local d'idéal maximal $S^{-1}\mathfrak{p}$.

Démonstration. — Soit $\mathfrak{p} \in \operatorname{Spec} A$. D'après la proposition 3.5 l'application de localisation $A \longrightarrow A_\mathfrak{p}$ induit une bijection

$$\operatorname{Spec} A_\mathfrak{p} \simeq \{\mathfrak{q} \in \operatorname{Spec} A, \mathfrak{q} \subset \mathfrak{p}\}.$$

L'idéal $S^{-1}\mathfrak{p} \subset A_\mathfrak{p}$ est l'unique idéal maximal de l'anneau local $A_\mathfrak{p}$. □

Exemples 3.7. — *i. Un corps est un anneau local d'idéal maximal* (0).
ii. L'anneau des séries formelles $K[[X_1, \ldots, X_n]]$ *est un anneau local d'idéal maximal engendré par* $X_1, \ldots, X_n$.

3.3. Corps des fractions. — Le corps des fractions d'un anneau intègre "rend inversible" tout élément non nul de A dans une extension canonique $\mathrm{Frac}(A)$ de A. Il s'agit du prototype de la localisation.

Définition 3.8. — *Soit* A *intègre et* $S = A - \{0\}$ *(multiplicative). Les éléments non nuls de* $S^{-1}A$ *sont de la forme* $\frac{a}{b}$, $a, b \neq 0$ *d'inverse* $\frac{b}{a}$. *L'anneau* $S^{-1}A$ *est un corps noté* $\mathrm{Frac}(A)$ *et appelé* **corps des fractions** *de* A. *C'est le plus petit corps contenant* A.

Exemples 3.9. — *i. Le corps des fractions des entiers relatifs est le corps des rationnels :* $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$. *Les sous-anneaux propres de* $\mathbb{Q}$ *sont les localisés de* $\mathbb{Z}$ *en* $S \subset \operatorname{Spec} \mathbb{Z}$.
ii. Les corps des fonctions rationnelles à n *variables sur le corps* K *est le corps des fractions de l'anneau des polynômes à* n *variables* $\mathrm{Frac}(K[X_1, \ldots, X_n]) = K(X_1, \ldots, X_n)$.
iii. Soit K *un corps. Le corps des fractions de l'anneau des séries formelles* $K[[X]]$ *est le corps des séries de Laurent :*

$$K((X)) = \mathrm{Frac}(K[[X]]) = \bigcup_{n \in \mathbb{N}} \left\{ \sum_{i=-n}^{\infty} a_i X^i, a_i \in K \right\}.$$

Lemme 3.10. — *Soit* A *un anneau intègre de corps des fractions* K. *Alors* $\mathrm{Frac}(A[X]) = K(X)$.

Démonstration. — Tout élément non nul de $A[X]$ est inversible dans $K(X)$, ce qui fournit un morphisme de corps injectif $\mathrm{Frac}(A[X]) \longrightarrow K(X)$. Montrons qu'il est surjectif. Soit $Q = \frac{f}{g} \in K(X)$. Quitte à multiplier par les dénominateurs des coefficients de f et g, nous pouvons écrire $Q = \frac{\tilde{f}}{\tilde{g}}$ avec $\tilde{f}, \tilde{g} \in A[X]$. □

4. Anneaux intègres

Dans l'anneau $\mathbb{Z}$, il y a unicité de la factorisation (à l'ordre près) en produit de nombres premiers. Cette propriété est la clé de nombreuses stratégies de résolutions d'équations diophantiennes.

Exemples 4.1. — *i. L'équations* $x^2 = 2$ *n'a pas de solution dans* $\mathbb{Q}$.
ii. L'équation $x^2 - 1 = y^3$ *a pour solution dans* $\mathbb{Q}^2$, $\{(0, -1), (\pm 1, 0), (\pm 3, 2)\}$.

Lorsque cette propriété d'unicité de la factorisation n'est plus satisfaite, les idéaux premiers remplacent les éléments irréductibles. En effet les idéaux d'un anneau A peuvent être additionnés et multipliés. Si, de plus, A est un anneau de Dedekind, les idéaux propres non nuls admettent une factorisation unique en produit d'idéaux premiers (voir §23.3).

L'objet de ce paragraphe est de caractériser certains anneaux qui ont des propriétés similaires à l'anneau $\mathbb{Z}$ et d'en déduire des propriétés arithmétiques. Nous étudions ici quatre classes d'anneaux intègres :
- les anneaux de Bézout,
- les anneaux euclidiens,
- les anneaux principaux,
- les anneaux factoriels.

Les anneaux euclidiens sont principaux. Les anneaux principaux sont factoriels. Les anneaux factoriels sont les anneaux intègres dans lesquels il y a unicité de la factorisation en produit d'éléments irréductibles. Les anneaux factoriels de Bézout sont les anneaux principaux.

4.1. Arithmétique dans un anneau intègre, anneau de Bézout. — Le PGCD et le PPCM sont des outils efficaces pour calculer dans l'anneau des entiers $\mathbb{Z}$. La généralisation de ces notions dans un anneau intègre quelconque fait apparaitre des difficultés nouvelles qu'il convient de contourner.

Définition 4.2. — *Soit A un anneau intègre.*
i. Pour a, b deux éléments non nuls de A, nous disons que b **divise** *a (et nous notons $b|a$) s'il existe $c \in A$ tel que $a = bc$.*
En particulier ($b|a$ et $a|b$) si et seulement si $a = bu$ pour $u \in A^*$.
ii. Un élément $a \in A$ est dit **irréductible** *si $a \notin A^* \cup \{0\}$ et si $a = bc$ avec $b, c \in A$ alors $b \in A^*$ ou $c \in A^*$ (mais pas les deux).*
Autrement dit $a \notin A^* \cup \{0\}$ est réductible (non irréductible) s'il existe $b, c \in A - A^*$ avec $a = bc$.

Exemples 4.3. — *i. Les éléments irréductibles de $\mathbb{Z}$ sont les $\pm p$ avec p premier.*
ii. Soit $a \in A - \{0\}$. Si l'idéal (a) est premier, alors a est irréductible, mais la réciproque est fausse : dans le sous-anneau $\mathbb{Z}[i\sqrt{5}]$ de $\mathbb{C}$ le nombre 3 est irréductible. En effet l'application norme $N : \mathbb{Z}[i\sqrt{5}] \longrightarrow \mathbb{N}$, $N(x + i\sqrt{5}y) = x^2 + 5y^2$ est multiplicative : $N(ab) = N(a)N(b)$. Comme 3 n'est pas une norme, donc ses seuls diviseurs sont $\pm 1, \pm 3$, donc 3 est irréductible. Cependant, l'idéal (3) n'est pas premier car 3 divise le produit $(2 + i\sqrt{5})(2 - i\sqrt{5})$ mais aucun de ses facteurs.
iii. Les idéaux premiers de $\mathbb{Z}[X]$ sont l'idéal nul (0), les idéaux principaux (P) avec P élément irréductible de $\mathbb{Z}[X]$ et les idéaux maximaux (p, P) où p est nul ou est un nombre premier et P irréductible modulo p.

iv. Soit $\overline{\mathbb{Z}}$ le sous-anneau de $\mathbb{C}$ des entiers algébriques, i.e. des racines des polynômes unitaires à coefficients dans $\mathbb{Z}$ (voir 23.13). Cet anneau n'est pas un corps, car pour $n \geq 2$, $1/n$ n'est pas entier. Soit $z \in \overline{\mathbb{Z}}$ non nul non inversible et $z^{1/2}$ une racine de z dans $\mathbb{C}$. Alors $z^{1/2}$ est un élément non nul et non inversible de $\overline{\mathbb{Z}}$ et $z = z^{1/2}z^{1/2}$. Donc z n'est pas irréductible. Donc $\overline{\mathbb{Z}}$ n'admet aucun élément irréductible.

Définition 4.4. — *Soit A un anneau intègre. La relation $\mathcal{R}$ de double divisibilité $a\mathcal{R}b \Longrightarrow a|b$ et $b|a$ est une relation d'équivalence et l'ensemble quotient $A/\mathcal{R}$ est ordonné par la relation induite par la divisibilité.*
Soit $a, b, d, m \in A - \{0\}$.
L'élément d est dit PGCD *de a et b, noté $d = \mathrm{PGCD}(a, b)$ si d est la borne inférieure de a et b dans $A/\mathcal{R}$.*
L'élément m est dit PPCM *de a et b noté $m = \mathrm{PPCM}(a, b)$ si m est la borne supérieure de a et b dans $A/\mathcal{R}$.*
Si $\mathrm{PGCD}(a, b) = 1$, nous disons que a et b sont **premiers entre eux**.

Ecrire $d = \mathrm{PGCD}(a, b)$, signifie que d divise a et b et que si c divise a et b, alors $c|d$. Ecrire $m = \mathrm{PPCM}(a, b)$ signifie que a et b divisent m et que si a et b divisent c alors m divise c.
Le PGCD et le PPCM sont définis dans $A/\mathcal{R}$ donc à un élément inversible près.

Lemme 4.5. — *Si $m = \mathrm{PPCM}(a, b)$ alors*
i. $(m) = (a) \cap (b)$,
ii. les éléments a et b ont un PGCD*, $d = \mathrm{PGCD}(a, b)$ et $ab = dm$ aux inversibles près.*

Démonstration. — i. Comme a, b divise $m = \mathrm{PPCM}(a, b)$, nous avons $(m) \subset (a)$ et $(m) \subset (b)$, donc $(m) \subset (a) \cap (b)$. Réciproquement si $c \in (a) \cap (b)$, nous avons $c = aa' = bb'$ donc c est un multiple de a et b donc de m et $(c) \subset (m)$.
ii. Comme ab est un multiple de a et b, c'est un multiple de m : $ab = md$. Montrons que d est un PGCD de a et b. Nous avons $m = aa'$, donc $ab = aa'd$ et $b = a'd$ donc d divise b et de même d divise a.
Soit c un diviseur de a et b, $a = ca''$, $b = cb''$ donc $ca''b''$ est un multiple de m. Par conséquent mc divise $c^2a''b'' = ab = md$ donc c divise d. □

Exemple 4.6. — *La réciproque du lemme précédent est fausse. En effet dans $\mathbb{Z}[i\sqrt{5}]$, 3 et $2 + i\sqrt{5}$ ont 1 pour* PGCD *mais n'ont pas de* PPCM.
Comme 3 irréductible ne divise pas $2 + i\sqrt{5}$, et $\mathrm{PGCD}(3, 2 + i\sqrt{5}) = 1$. Si 3 et $2 + i\sqrt{5}$ avaient un PPCM *m, alors $m = ab = 3(2 + i\sqrt{5})$. Mais 3 et $2 + i\sqrt{5}$ divisent 9, alors $m = 3(2 + i\sqrt{5})$ devrait diviser 9 et $2 + i\sqrt{5}$ diviserait 3 ce qui est absurde.*

Lemme 4.7. — *Soient $a, b \in A - \{0\}$ et d un diviseur de a et b. Les propriétés suivantes sont équivalentes :*
i. $(d) = (a) + (b)$,

ii. Il existe $u, v \in A$ tels que $au + bv = d$.
Si ces propriétés sont vérifiées alors d est un PGCD *de a et b. De plus a et b ont ab/d comme* PPCM.

Démonstration. — Comme d divise a et b, $(a) \subset (d)$ et $(b) \subset (d)$, donc $(a)+(b) \subset (d)$ et l'inclusion réciproque est équivalente à ii.
Si ces propriétés sont vérifiées et si c divise a, b alors c divise d ; donc d est un PGCD de a et b.
Ecrivons $a = da'$, $b = db'$ et $m = da'b'$; ainsi $a'u + b'v = 1$. Soit c un multiple de a et b, alors $c = al = da'l = bl' = db'l'$, donc $c = c(a'u+b'v) = db'l'a'u+da'lb'v = da'b'(l'u + lv)$ donc c est un multiple de m. □

Remarque 4.8. — *Si tous les idéaux de A sont principaux,* $(\mathrm{PGCD}(a, b)) = (a) + (b)$ *(§4.2) . Mais cette égalité est fausse en général par exemple dans $K[X, Y]$, où* $\mathrm{PGCD}(X, Y) = 1$ *et* $(X, Y) \neq (1)$.

Définition 4.9. — *Un anneau intègre est* **de Bézout** *si et seulement si tout idéal de type fini est principal.*

Dans un anneau de Bézout, tout couple d'éléments non nuls admet un PGCD. Pourtant la propriété "de Bézout" ne garantit pas l'existence et l'unicité de la factorisation en éléments irréductibles (factorialité) qui permettent la mise en œuvre des stratégies de preuves ou de calculs analogues à celles sur l'anneau des entiers relatifs $\mathbb{Z}$. Il convient alors de définir des propriétés plus fortes sur les anneaux intègres (euclidiens, principaux, factoriels).

Remarque 4.10. — *Les anneaux de valuation sont des anneaux de Bézout (§25). L'anneau des fonctions holomorphes sur $\mathbb{C}$ et l'anneau des entiers algébriques $\overline{\mathbb{Z}}$ (23.13) sont de Bézout mais ne sont pas factoriels.*

4.2. Anneaux principaux et euclidiens. —

Définition 4.11. — *Un anneau intègre A est un anneau* **euclidien** *pour la fonction*

$$\varphi : A \longrightarrow \mathbb{N}$$

si les propriétés suivantes sont satisfaites :
i. $\varphi(a) = 0 \Longleftrightarrow a = 0$,
ii. pour tous $a, b \in A$, avec $b \neq 0$, il existe $q, r \in A$ tels que $a = qb + r$ et $\varphi(r) < \varphi(b)$.

Exemples 4.12. — *i. L'anneau $A = \mathbb{Z}$ est euclidien pour $\varphi(n) = |n|$.*
ii. Les sous-anneaux de $\mathbb{Q}$ sont euclidiens (voir Ex. 3.9).
iii. L'anneau $A = K[X]$, où K est un corps, est euclidien pour $\varphi(f) = \deg(f)+1$ (avec la convention $\deg(0) = -1$*).*
iv. L'anneau $A = \mathbb{Z}[i] = \{x + iy | x, y \in \mathbb{Z}\}$ est euclidien pour $\varphi(x + iy) = (x + iy)(x - iy) = |x + iy|^2 = x^2 + y^2$.

En effet, pour $a, b \in A$ et $b \neq 0$, alors nous écrivons $a/b = u + iv \in \mathbb{Q}[i]$ et nous prenons $q = x + iy \in \mathbb{Z}[i]$ avec x (resp. y) l'entier le plus proche de u (resp. v). Dans ce cas $|x - u|, |y - v| \leq 1/2$ donc

$$|a/b - q|^2 = |u - x|^2 + |y - v|^2 \leq (1/2)^2 + (1/2)^2 \leq 1/2 < 1.$$

Donc $a = bq + r$ avec $r \in \mathbb{Z}[i]$ et $\varphi(r) = |r|^2 = |a - qb|^2 < |b|^2 = \varphi(b)$.
v. De la même façon, $A = \mathbb{Z}[i\sqrt{2}] = \{x + iy\sqrt{2} | x, y \in \mathbb{Z}\}$ est euclidien pour $\varphi(x + iy\sqrt{2}) = x^2 + 2y^2$.
vi. Le même argument ne s'applique pas à $A = \mathbb{Z}[i\sqrt{d}]$ pour d entier ≥ 3 et $\varphi(a) = |a|^2$. En fait aucun de ces anneaux n'est euclidien ni même n'admet unicité de la factorisation en produit d'éléments irréductibles.
vii. L'anneau $\mathbb{Z}[(1 + i\sqrt{d})/2]$ est euclidien pour $\varphi(a) = |a|^2$ si $d = 3, 7, 11$.

Remarque 4.13. — *L'anneau des entiers (23.13) d'un corps quadratique $\mathbb{Q}(\sqrt{d})$ est euclidien pour sa norme algébrique si et seulement si*

$$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Les cinq valeurs $-11, -7, -3, -2, -1$ sont les seules valeurs négatives de d pour lesquelles cet anneau est euclidien. Conjecturalement, il existe une infinité de valeurs positives, pour lesquelles il est euclidien pour une autre norme (conjecture dûe à Gauss).

Définition 4.14. — *Un anneau* **principal** *est un anneau intègre dans lequel tous les idéaux sont principaux.*

Exemples 4.15. — *i. Si A est principal,* $\operatorname{Spm} A = \{(\pi), \pi$ *irréductible* $\}$ *et* $\operatorname{Spec} A = \operatorname{Spm} A \cup \{(0)\}$. *Par exemple* $\operatorname{Spm} \mathbb{C}[X] = \{(X - a), a \in \mathbb{C}\}$.
ii. Les anneaux locaux ne sont pas tous principaux. Par exemple, soit K un corps. Alors $A = K[X, Y]/(X, Y)^2$ est un anneau local non principal.

Proposition 4.16. — *Si A est un anneau euclidien alors il est principal.*

Démonstration. — Soit I un idéal de A. Si $I = 0$ alors $I = (0)$ sinon il existe $b \in I - \{0\}$ tel que $\varphi(b) \geq 1$ est minimal. Alors $(b) = bA \subset I$. Réciproquement si $a \in I$, il existe $q, r \in A$ tels que $a = bq + r$ avec $r = a - bq \in I$ et $\varphi(r) < \varphi(b)$ donc $r = 0$ et $a = qr \in (b)$. Donc $I \subset (b)$ et $I = (b)$. □

Exemples 4.17. — *i. (Equations diophantiennes) Les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation $y^2 + 2 = x^3$ sont $x = 3$ et $y = \pm 5$. En effet dans l'anneau euclidien $\mathbb{Z}[i\sqrt{2}]$ (pour $\varphi(x + i\sqrt{2}y) = x^2 + 2y^2$), nous avons*

$$(y + i\sqrt{2})(y - i\sqrt{2}) = x^3.$$

Or $\operatorname{PGCD}(y + i\sqrt{2}, y - i\sqrt{2}) = 1$ *car si $\pi \in \mathbb{Z}[i\sqrt{2}]$ divise $y \pm i\sqrt{2}$, π divise $2y, 2i\sqrt{2}$ et x^3. Donc $\varphi(\pi) = \pi\overline{\pi} \in \mathbb{N}$ divise le* PGCD *dans $\mathbb{Z}$ de $(\varphi(2y), \varphi(2\sqrt{2}), \varphi(x^3)) = (4y^2, 8, x^3)$. Or si 2 divise x alors 2 divise y et $2 = x^3 - y^2$ est divisible par 4, ce qui est exclu.*
Par conséquent $y + i\sqrt{2} = \pm d^3$ pour $d \in \mathbb{Z}[i\sqrt{2}]$ donc il existe $a, b \in \mathbb{Z}$ avec

$y + i\sqrt{2} = (a + ib\sqrt{2})^3$ donc $y = a(a^2 - bb^2)$ et $1 = b(3a^2 - 2b^2)$. Donc $b = \pm 1$ et $3a^2 = 2b^2 \pm 1 = 2 \mp 1$. Donc $b = 1$ et $a = \pm 1$. Soit encore $x = 3$ et $y = \pm 5$.
ii. L'anneau $\mathbb{Z}[(1 + i\sqrt{19})/2]$ est principal mais n'est pas euclidien.

4.3. Anneaux factoriels. —

Définition 4.18. — *Un anneau est dit* **factoriel** *s'il est intègre et s'il satisfait les deux propriétés suivantes :*
i. Tout élément $a \in A - \{0\}$ s'écrit de la forme $a = ux_1 \cdots x_r$ avec $u \in A^*$, x_i irréductibles et $r \geq 0$;
ii. Si $ux_1 \cdots x_r = vy_1 \cdots y_s$ avec $u, v \in A^*$ et x_i, y_j irréductibles, alors $r = s$ et il existe des éléments inversibles $u_1, \ldots, u_r \in A^*$ et une permutation $\sigma \in \mathfrak{S}_r$ telle que $x_i = u_i y_{\sigma(i)}$, $1 \leq i \leq r$.

Exemple 4.19. — *Soit $A = \mathbb{Z}[i\sqrt{5}]$. La norme $N : A \longrightarrow \mathbb{N}$, $N(x + i\sqrt{5}y) = |x + i\sqrt{5}y|^2 = x^2 + 5y^2$ est multiplicative $N(ab) = N(a)N(b)$, $N(1) = 1$. Donc $A^* \subset \{a \in A, N(a) = 1\}$ or $x^2 + 5y^2 = 1$ et $x, y \in \mathbb{Z}$ impliquent $x^2 = 1$ et $y = 0$ donc $A^* = \{\pm 1\}$. Il n'y a pas d'élément $a \in A$ avec $N(A) = 3$ ou $N(a) = 7$. Les éléments $3, 7, 4 \pm i\sqrt{5} \in A$ sont donc irréductibles. Or*

$$21 = 3 \cdot 7 = (4 - i\sqrt{5})(4 + i\sqrt{5}).$$

Donc $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

Les anneaux factoriels ne sont pas de Bézout (sauf s'ils sont principaux). Pourtant, nous pouvons définir les notions de PGCD et de PPCM dans un anneau factoriel :

Lemme 4.20. — *Soit P un système de représentants des éléments irréductibles de A anneau factoriel. Alors tout $a \in A - \{0\}$, s'écrit de façon unique $a = u\Pi_{x \in \mathrm{P}} x^{v_x(a)}$, $u \in A^*$, $v_x(a) \in \mathbb{N}$ presque tous nuls. Pour $a, b \in A - \{0\}$, le plus grand commun diviseur et le plus petit commun multiple de a et b sont*

$$\mathrm{PGCD}(a, b) = \Pi_{x \in \mathrm{P}} x^{\min(v_x(a), v_x(b))}, \quad \mathrm{PPCM}(a, b) = \Pi_{x \in \mathrm{P}} x^{\max(v_x(a), v_x(b))}.$$

Les notions de plus grand commun diviseur et de plus petit commun multiple, dépendent du choix d'un système de représentants d'éléments irréductibles, donc sont bien définies à multiplication par un élément inversible près.

Démonstration. — Nous avons $b|a$ si et seulement si $\forall x \in \mathrm{P}$, $v_x(b) \leq v_x(a)$. □

Exemples 4.21. — *i. L'anneau $\mathbb{Z}$ est factoriel. Il suffit de prendre pour P l'ensemble des nombres premiers positifs.*
ii. Soit K un corps. L'anneau $K[X]$ est factoriel, nous pouvons prendre pour P l'ensemble des polynômes unitaires irréductibles.
iii. La décomposition d'un polynôme $f \in \mathbb{Q}[X]$ à racines simples en facteurs irréductibles s'interprète en termes d'action du groupe de Galois du corps de décomposition de f sur $\mathbb{Q}$ (voir Proposition 22.10).

Lemme 4.22. — *Un anneau intègre est factoriel si et seulement si les deux conditions suivantes sont satisfaites :*
- tout élément s'écrit comme produit d'irréductibles (i. 4.18)
- si un élément irréductible $x \in A$ divise ab $(a, b \in A)$ alors x divise a ou b (Lemme de Gauss).

Démonstration. — $\Longrightarrow$ Ecrivons $ab = xc$ et factorisons a, b, c sous forme de produits d'éléments irréductibles. Alors x coincide (à un élément inversible près) avec un facteur irréductible de a ou b.
$\Longleftarrow$ Supposons $ux_1 \cdots x_r = vy_1 \cdots y_s$ avec $r \leq s$. Si $r = 0$ alors $s = 0$. Si $r \geq 1$, alors $x_1 | vy_1 \cdots y_s$ donc divise l'un des y_j d'après le lemme de Gauss. Quitte à renuméroter, nous pouvons supposer $j = 1$ et $y_1 = u_1 x_1$. Nous simplifions par x_1 et nous recommençons par induction. Ainsi $y_j = u_j x_j$, $1 \leq j \leq r$, $u_j \in A^*$ et $u = vu_1 \cdots u_r y_{r+1} \cdots y_s$ qui implique finalement que $r = s$. □

Proposition 4.23. — *Un anneau principal est factoriel.*

Démonstration. — Si $a \in A - \{0\}$ ne peut pas s'écrire sous la forme d'un produit d'irréductibles, alors $a \notin A^* \cup \{0\}$ n'est pas irréductible, donc $a = a_1 b_1$ avec $a_1, b_1 \notin A^*$ et $(a) \subsetneq (a_1)$. Ainsi au moins l'un des deux (disons a_1) ne peut pas s'écrire sous forme d'un produit. Par induction, nous construisons ainsi une suite $a_n = a_{n+1} b_{n+1}$ d'éléments ayant les mêmes propriétés. D'où une suite infinie d'idéaux

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

L'union de tous ces idéaux est un idéal engendré par un élément $c \in A$ car A est principal. Il existe donc $n \geq 1$ avec $c \in (a_n)$, donc $(a_n) = (a_{n+1})$ ce qui est exclu donc l'existence d'une décomposition en produit d'irréductibles (i. 4.22) est vérifiée.
Nous vérifions à présent le lemme de Gauss. Supposons que x est un élément irréductible de A divisant ab. Alors $(x, b) = (c)$ pour $c \in A - \{0\}$. Ainsi $c | x$ et $x = cd$ pour un $d \in A$. Comme x est irréductible, nous avons ou bien $d \in A^*$ (et alors $x | c | b$) ou bien $c \in A^*$ (et $(x, b) = (1)$ donc $1 = xu + bv$ pour $u, v \in A$ et donc $a(1 - bv) = xau$ et $x | a$). Ainsi le lemme de Gauss est satisfait. □

Exemples 4.24. — *i. Le lemme de Gauss exprime également que pour tout élément irréductible $x \in A$, l'anneau quotient $A/(x)$ est intègre, donc (x) est premier.*
ii. L'anneau $K[X_1, \ldots, X_n]$, $n \geq 2$, K corps, n'est pas principal car l'idéal (X_1, X_2) n'est pas principal. Nous verrons qu'il est factoriel (Théorème 5.24). Plus généralement, $A[X]$ est principal si et seulement si A est un corps.

5. Anneaux de polynômes

L'objet de ce paragraphe est d'adapter plusieurs stratégies classiques de calcul sur les polynômes à une variable à coefficients dans un corps K aux polynômes à plusieurs variables : d'abord une version étendue de l'algorithme d'Euclide (§5.1). Ensuite, nous étudions plus généralement les anneaux de polynômes à coefficients dans un anneau factoriel (§5.2) et nous déterminons leurs éléments irréductibles. Enfin nous décrivons les polynômes symétriques à coefficients dans un anneau quelconque (§5.3).

5.1. Algorithme de division euclidienne étendue. — Dans ce paragraphe, $K[X]$ désigne l'anneau des polynômes en une indéterminée à coefficients dans un corps K.

Définition 5.1. — *Soit $f \in K[X]$. Si $f \neq 0$, alors $f = a_0X^m + \cdots + a_m$, $a_i \in k$ et $a_0 \neq 0$. Alors le terme $LT(f) = a_0X^m$ est dit* **terme dominant** *de f.*

L'anneau $K[X]$ est un anneau euclidien pour l'application degré. En effet, dans $K[X]$, nous avons l'algorithme de division euclidienne :

Proposition 5.2. — *Soit $g \in K[X]$, $g \neq 0$. Pour tout $f \in K[X]$, il existe un unique couple d'éléments $q, r \in K[X]$ tel que $f = qg + r$, avec $r = 0$ ou $\deg r < \deg g$.*

Démonstration. — L'algorithme d'Euclide s'écrit en pseudo-code :
Entrée : g, f
Sortie : q, r
$q := 0; r := f$
Tant que $r \neq 0$ et que $LT(g)$ divise $LT(r)$ faire
$q := q + LT(r)/LT(g)$
$r := r - (LT(r)/LT(g))g$

En effet, nous avons toujours

$$f := qg + r = (q + LT(r)/LT(g))g + (r - (LT(r)/LT(g))g).$$

L'algorithme s'arrête quand la proposition ($r \neq 0$ et $LT(g)|LT(r)$) est fausse. Donc en sortie d'algorithme, $r = 0$ ou $LT(g)$ ne divise pas $LT(r)$, donc $r = 0$ ou $\deg r < \deg g$.
L'algorithme s'arrête car à chaque étape le degré de r diminue par substitution à $r - (LT(r)/LT(g))g$.
Il y a unicité de l'écriture. En effet si nous avons deux écritures

$$f = qg + r = q'g + r'$$

satisfaisant les hypothèses de la proposition, alors $\deg(r - r') < \deg g$. Si $r \neq r'$ alors $(q - q')g = r' - r$ donc $q - q' \neq 0$ et $\deg r - r' > \deg g$, absurde ! Donc $r = r'$ et, par suite, $q = q'$. $\square$

Soient $X_1, \ldots, X_n$, n variables.

Définition 5.3. — *Un* **monôme** *en $X_1, \ldots, X_n$ est un produit de la forme*

$$X_1^{\alpha_1} \cdots X_n^{\alpha_n} \text{ où } \alpha_i \in \mathbb{N}, 1 \leq i \leq n$$

Nous notons aussi $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, où $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. Le **degré total** *de X^α est $|\alpha| = \alpha_1 + \cdots + \alpha_n$.*

Définition 5.4. — *Un* **polynôme** *f en $X_1, \ldots, X_n$ à coefficients dans K est une combinaison linéaire finie de monômes :*

$$f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X^\alpha$$

où les $a_\alpha \in K$ sont presque tous nuls ; l'élément a_α est dit **coefficient** *du monôme X^α dans f. Le* **degré total** *de f est le maximum de $|\alpha|$ pour $a_\alpha \neq 0$.*
Un polynôme est dit **homogène** *si tous les monômes qui apparaissent avec un coefficient non nul ont même degré total.*

Définition 5.5. — *Un* **ordre admissible** *sur $K[X_1, \ldots, X_n]$ est une relation $>$ sur l'ensemble des monômes X^α de $K[X_1, \ldots, X_n]$ (ou, de façon équivalente sur les exposants $\alpha \in \mathbb{N}^n$) telle que*
a. La relation $>$ est compatible avec la multiplication de $K[X_1, \ldots, X_n]$:

$$\text{Si } X^\alpha > X^\beta, \text{ alors } \forall X^\gamma, X^\alpha X^\gamma = X^{\alpha+\gamma} > X^\beta X^\gamma = X^{\beta+\gamma}.$$

b. La relation $>$ est bien ordonnée : tout ensemble non vide de monômes a un élément minimal pour $>$.

Dans le cas où $n = 1$, ce sont précisément les propriétés du degré qui permettent d'établir l'algorithme d'Euclide. Remarquons enfin que le degré est le seul ordre admissible sur les polynômes à une variable. En revanche, il y a plusieurs ordres admissibles sur $K[X_1, \ldots, X_n]$.

Exemples 5.6. — *i. L'***ordre lexicograpique** *est l'ordre "du dictionnaire" : soit $X^\alpha, X^\beta \in K[X_1, \ldots, X_n]$*

$$X^\alpha >_{lex} X^\beta \iff \text{dans } \alpha - \beta \in \mathbb{Z}^n \text{ le premier coefficient non nul est } > 0.$$

Par exemple, dans $K[x, y, z]$, $x^3y^2z > x^2y^6z^{12}$ car $(3, 2, 1) - (2, 6, 12) = (1, -4, -11)$.
*ii. L'***ordre lexicographique gradué** *est l'ordre défini par : $X^\alpha, X^\beta \in K[X_1, \ldots, X_n]$*

$$X^\alpha >_{grlex} X^\beta \iff \begin{cases} |\alpha| > |\beta|, \\ \text{ou} \\ |\alpha| = |\beta| \text{ et } X^\alpha >_{lex} X^\beta. \end{cases}$$

Par exemple, dans $K[x,y,z]$, $x^2y^6z^{12} >_{grlex} x^3y^2z$.
*iii. L'***ordre lexicographique inverse gradué** *est l'ordre défini par :* $X^\alpha, X^\beta \in K[X_1,\dots,X_n]$

$$X^\alpha >_{grevlex} X^\beta \Longleftrightarrow \begin{cases} |\alpha| > |\beta|, \\ ou \\ |\alpha| = |\beta|, \text{ et } \alpha - \beta \in \mathbb{Z}^n \\ \text{et le premier coefficient non nul en partant de la droite est } < 0. \end{cases}$$

Par exemple, dans $K[x,y,z]$, $x^3y^5z^2 >_{grlex} x^2y^7z$ *mais* $x^2y^7z >_{grevlex} x^3y^5z^2$.
iv. Les ordres $lex, grlex, grevlex$ *sont des ordres admissibles.*

Nous supposons maintenant que $K[X_1,\dots,X_n]$ est muni d'un ordre admissible noté $>$.

Définition 5.7. — *Le* **terme dominant** *de* $f = \sum_\alpha c_\alpha X^\alpha$ *non nul est* $c_\alpha X^\alpha$ *où* X^α *est le plus grand monôme pour l'ordre* $>$. *Nous notons* $LT(f) = c_\alpha X^\alpha$.
Le **multidegré** *de* f *est multidegré*$(f) := \max\{\alpha \in \mathbb{N}^n, c_\alpha \neq 0\}$.

Le terme dominant dépend de l'ordre admissible choisi.

Lemme 5.8. — *(Lemme de Dickson) Soit* $\Lambda \subset \mathbb{N}^n$ *et* $I =< X^\alpha, \alpha \in \Lambda >$ *un idéal monomial. Alors il existe un nombre fini d'éléments* $\gamma(1),\dots,\gamma(s) \in \Lambda$ *tels que* $I =< X^{\gamma(1)},\dots,X^{\gamma(s)} >$. *En particulier* I *a une base finie.*

Démonstration. — Par induction sur le nombre n de variables. Si $\Lambda = \emptyset$, le résultat est clair.
Si $n = 1$, soit $I =< X_1^\alpha, \alpha \in \Lambda >$. Posons $\beta = \min\{\alpha \in \Lambda\}$ (ici $\Lambda \subset \mathbb{N}$). Pour tout $\alpha \in \Lambda$, $\alpha \geq \beta$ donc $X_1^\beta | X_1^\alpha$ et $I =< X_1^\beta >$.
Supposons le théorème vrai pour $n-1 \geq 1$. Nous écrivons les variables $X_1,\dots,X_{n-1},y$ et les monômes de $K[X_1,\dots,X_{n-1},y]$ sous la forme

$$X^\alpha y^m, \alpha \in \mathbb{N}^{n-1}, m \in \mathbb{N}.$$

Soit $I \subset K[X_1,\dots,X_{n-1},y]$ un idéal monomial. Soit

$$J =< X^\alpha \text{ tel que } \exists m \text{ avec } X^\alpha y^m \in I >$$

la projection de I sur $K[X_1,\dots,X_{n-1}]$. Par hypothèse $J =< X^{\alpha(1)},\dots,X^{\alpha(s)} >$. Pour tout $1 \leq i \leq s$, il existe m_i avec $X^{\alpha(i)}y^{m_i} \in I$. Soit $m = \max\limits_{1\leq i\leq s} m_i$ et pour $0 \leq \ell \leq m-1$,

$$J_\ell =< X^\beta \text{ tel que } X^\beta y^\ell \in I >=< X^{\alpha_\ell(1)},\dots,X^{\alpha_\ell(s_\ell)} > .$$

Montrons que

$$(1) \qquad I =< X^{\alpha_\ell(i)}y^\ell, 0 \leq \ell \leq m-1, 1 \leq i \leq s_\ell, X^{\alpha(i)}y^m, 1 \leq i \leq s > .$$

Soit $X^\alpha y^p$ avec $(\alpha, p) \in \Lambda$. Si $p \geq m$ alors $\exists i$ avec $X^{\alpha(i)} y^m | X^\alpha y^p$. D'où (1).
Montrons que nous pouvons de plus choisir les $(\alpha_\ell(i), \ell)$ et $(\alpha(i), m) \in \Lambda$. En effet

$$I =< X^{\beta(1)}, \ldots, X^{\beta(s)} >=< X^\alpha, \alpha \in \Lambda >$$

Ainsi chaque $X^{\beta(i)}$ est divisible par un $X^{\gamma(i)}$ avec $\gamma(i) \in \Lambda$. Donc $I =< X^{\gamma(1)}, \ldots, X^{\gamma(s)} >$. □

Définition 5.9. — *Soit $I \subset K[X_1, \ldots, X_n]$ un idéal non nul.*
L'ensemble des termes dominants de I est

$$LT(I) = \{cX^\alpha \text{ s'il existe } f \in I \text{ tel que } LT(f) = cX^\alpha\}$$

Nous notons $< LT(I) >$ l'idéal engendré par les éléments de $LT(I)$.
Pour $I = 0$, nous posons $LT(I) = \{0\}$.

Exemple 5.10. — *Soit $I =< f_1, f_2 >$ avec $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$.*
Remarquons que $< LT(I) > \neq < LT(f_1), LT(f_2) >$. En effet

$$x(x^2y - 2y^2 + x) - y(x^3 - 2xy) = x^2$$

Donc $x^2 \in I$ et $x^2 = LT(x^2) \in < LT(I) >$ mais $x^2 \notin < x^3, x^2y >$.

Proposition 5.11. — *Soit $I \subset K[X_1, \ldots X_n]$ un idéal. Alors $< LT(I) >$ est un idéal monomial et $\exists g_1, \ldots, g_s \in I$ tels que $< LT(I) >=< LT(g_1), \ldots, LT(g_s) >$.*

Démonstration. — D'après le lemme de Dickson, nous pouvons écrire

$$< LT(I) >=< LT(g_1), \ldots, LT(g_s) > .$$

□

Théorème 5.12. — *(Théorème de la base d'Hilbert) Tout idéal I de $K[X_1, \ldots, X_n]$ est de type fini.*

Démonstration. — Si $I = \{0\}$, le résultat est clair.
Sinon, écrivons $< LT(I) >=< LT(g_1), \ldots, LT(g_s) >$. Montrons que $I =< g_1, \ldots, g_s >$. L'inclusion $< g_1, \ldots, g_s > \subset I$ est claire.
Montrons l'inclusion $I \subset < g_1, \ldots, g_s >$. Soit $f \in I$, écrivons

$$f = a_1 g_1 + \cdots + a_s g_s + r.$$

Supposons $r \neq 0$ et aucun terme de r n'est divisible par un terme $LT(g_i)$. Or $r = f - a_1 g_1 - \cdots - a_s g_s \in I$. Donc $LT(r) \in < LT(I) >$ donc il existe i avec $LT(g_i)$ divise $LT(r)$. Absurde !
Donc $r = 0$ et $f =< g_1, \ldots, g_s >$. □

Soit $>$ un ordre admissible de $K[X_1, \ldots, X_n]$. Nous allons définir une division algorithmique dans $K[X_1, \ldots, X_n]$ analogue à la division euclidienne.

Proposition 5.13. — *Soit $F = (f_1, \ldots, f_s)$ un s-uplet ordonné de polynômes de $K[X_1, \ldots, X_n]$. Alors pour tout $f \in K[X_1, \ldots, X_n]$, nous pouvons écrire*

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

où $a_i, r \in K[X_1, \ldots, X_n]$ et
- pour tout $i \in \{1, \ldots, s\}$, $a_i f_i = 0$ ou $LT(f) \geq LT(a_i f_i)$,
- $r = 0$ ou r est une combinaison linéaire de monômes dont aucun n'est divisible par $LT(f_1), \ldots, LT(f_s)$.
Le terme r est alors appelé le **reste** *de la division de f par F et est noté $r = \overline{f}^F$.*

Démonstration. — Algorithme de division :
Entrée : $f_1, \ldots, f_s, f$
Sortie $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots, a_s := 0; r := 0$
$p := f$
Tant que $p \neq 0$ faire
  $i := 1$
  division:=faux
  Tant que $i \leq s$ et division=faux faire
    Si $LT(f_i)$ divise $LT(p)$ alors (nous divisons p par f_i et nous arrêtons)
      $a_i := a_i + LT(p)/LT(f_i)$
      $p := p - (LT(p)/LT(f_i))f_i$
      division=vrai
    sinon $i := i + 1$ (nous essayons la variable suivante)
  Si division=faux alors
  $r := r + LT(p)$
  $p := p - LT(p)$

Dans cet algorithme, p désigne le polynôme intermédiaire des divisions à chaque étape, $a_1, \ldots, a_s$ sont les quotients et r est le reste.
• Montrons qu'à chaque étape, nous avons

$$f = a_1 f_1 + \ldots + a_s f_s + p + r.$$

C'est vrai au début de l'algorithme. Supposons que c'est vrai à une étape de la division alors
- Si $LT(f_i)|LT(p)$, $a_i f_i + p = (a_i + LT(p)/LT(f_i))f_i + p - (LT(p)/LT(f_i))f_i$.
- Sinon $p + r = p - LT(p) + r + LT(p)$.
• Lorsque l'algorithme s'arrête, $p = 0$, donc $f = a_1 f_1 + \cdots + a_s f_s + r$.
• Montrons que l'algorithme s'arrête. Pour cela, nous établissons qu'à chaque étape le multidegré de p diminue :
- Si $LT(f_i)|LT(p)$, $p' = p - (LT(p)/LT(f_i))f_i$. Or $LT\left(\frac{LT(p)}{LT(f_i)} f_i\right) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p)$. Donc p et $\frac{LT(p)}{LT(f_i)} f_i$ ont même terme dominant, d'où, multidegré$(p') <$ multidegré(p).

- Sinon $p' = p - LT(p)$ et multidegré$(p') <$ multidegré(p).
Ainsi le multidegré est une fonction strictement décroissante et l'algorithme se termine.
• Il reste à montrer que $LT(f) \geq LT(a_i f_i)$ si $a_i f_i \neq 0$. Par construction, tous les termes de a_i sont de la forme $\frac{LT(p)}{LT(f_i)}$ où p varie en décroissant son terme dominant. Nous commençons à $p = f$, ainsi $LT(p) \leq LT(f)$ et à chaque étape $LT(a_i f_i) \leq LT(f)$. □

Exemples 5.14. — *Soit $k[x, y]$ muni de l'ordre lexicographique, $f_1 = xy + 1$, $f_2 = y^2 - 1$ et $f = xy^2 - x$.*
• *Si $F = (f_1, f_2)$, alors $xy^2 - x = y(xy + 1) + 0 \cdot (y^2 - 1) + (-x - y)$.*
• *Si $F = (f_2, f_1)$, alors $xy^2 - x = x(y^2 - 1) + 0 \cdot (xy + 1) + 0$.*

L'exemple 5.14 montre que $\overline{f}^F$ dépend de l'ordre de la famille ordonnée F. La nullité du reste $r = 0$ est une condition suffisante mais pas nécessaire pour établir l'appartenance

$$f \in < f_1, \ldots, f_s >= I.$$

Les bases de Gröbner fournissent un "bon système" de générateurs de I tels que
- la condition $r = 0$ est équivalente à $f \in I$
- l'ordre de la division n'a pas d'importance.

Définition 5.15. — *Un sous-ensemble fini $G := \{g_1, \ldots, g_s\}$ d'un idéal $I \subset K[X_1, \ldots, X_n]$ est dit* **base de Gröbner** *si*

$$< LT(g_1), \ldots, LT(g_s) >=< LT(I) >$$

D'après la démonstration du théorème de la base de Hilbert

Corollaire 5.16. — *i. Tout idéal $I \subset K[X_1, \ldots, X_n]$ a une base de Gröbner.*
ii. Toute base de Gröbner de I est une base de I.

Proposition 5.17. — *Soit $G = \{g_1, \ldots, g_s\}$ une base de Gröbner de l'idéal I et $f \in K[X_1, \ldots, X_n]$. Alors il existe un unique $r \in K[X_1, \ldots, X_n]$ tel que*
i. aucun terme de r ne soit divisible par $LT(g_1), \ldots, LT(g_r)$,
ii. il existe $g \in I$ avec $f = g + r$.
En particulier, $r = \overline{f}^G$ est le reste de la division de f par G indépendamment de l'ordre des g_i en utilisant l'algorithme de division. De plus $f \in I$ si et seulement si le reste de f par G est nul.

Démonstration. — L'existence de r satisfaisant i. et ii. est assurée par l'algorithme de division. Son unicité résulte du calcul suivant : soit $f = g + r = g' + r'$ sont deux écritures satisfaisant les hypothèses i. et ii. Alors $r - r' = g' - g \in I$. Si $r \neq r'$, alors $LT(r - r') \in < LT(I) >=< LT(g_1), \ldots, LT(g_s) >$. Donc il existe i avec $LT(g_i)$ divise $LT(r - r')$ ce qui est exclu ! Donc $r = r'$ et $g = g'$. □

Remarque 5.18. — *Les propriétés de la proposition 5.17 caractérisent les bases de Gröbner (Becke et Weispfenning (1993)).*

Exemples 5.19. — *i. Considérons le système* $(*)$ *d'équations dans* $\mathbb{C}^3$

$$\begin{cases} x^2+y^2+z^2=1 \\ x^2+z^2=y \\ x=z \end{cases}$$

Considérons l'idéal $I =< x^2+y^2+z^2-1, x^2+z^2-y, x-z >$. *Déterminons une base de Gröbner de* I *pour l'ordre lexicographique :* $G := \{g_1 = x-z, g_2 = -y+2z^2, g_3 = z^4+(1/2)z^2-1/4\}$. *Le système* $(*)$ *est équivalent au système* $g_1 = g_2 = g_3 = 0$. *Or* $g_3 = 0$ *est équivalent à*

$$z = \pm 1/2\sqrt{\pm\sqrt{5}-1}$$

Ce qui permet de résoudre le système $(*)$.
ii. Soit le système

$$\begin{cases} x^2+y+z=1 \\ x+y^2+z=1 \\ x+y+z^2=1 \end{cases}$$

Notons $I =< x^2+y+z-1, x+y^2+z-1, x+y+z^2-1 >$, *l'idéal associé. Une base de Gröbner pour* I *(ordre* $>_{lex}$*) est*

$$\begin{array}{rcl} g_1 & = & x+y+z^2-1 \\ g_2 & = & y^2-y-z^2+z \\ g_3 & = & 2yz^2+z^4-z^2 \\ g_4 & = & z^6-4z^4+4z^3-z^2 \end{array}$$

Or $g_4 = z^2(z-1)^2(z^2+2z-1)$. *Donc* $z \in \{0, 1, -1 \pm \sqrt{2}\}$. *Nous remplaçons dans* g_2 *et* g_3, *nous déterminons les* y *possibles et nous remplaçons le tout dans* g_1. *D'où les solutions du système*

$$(1,0,0), (0,1,0), (0,0,1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}).$$

Nous constatons que nous sommes passés par les mêmes deux étapes pour résoudre le système polynomial que pour les systèmes linéaires. Après une étape de triangularisation, nous avons obtenu $g_4 \in I \cap k[z]$, $g_2, g_3 \in I \cap k[y,z]$ *puis nous résolvons le système d'équations par une étape de report des solutions des équations du bas en haut.*

5.2. Anneau de polynômes sur un anneau factoriel. — Dans ce paragraphe A est un anneau factoriel.

5.2.1. Éléments irréductibles. — L'objet de ce paragraphe est de montrer que si A est factoriel alors $A[X]$ aussi.

Définition 5.20. — *Soit A un anneau factoriel de corps des fractions K. Le* **contenu** $\mathrm{ct}(f)$ *d'un polynôme non nul $f \in A[X]$ est le* PGCD *de ses coefficients. Un polynôme $f \in A[X]$ est dit* **primitif**, *s'il est non nul et si* $\mathrm{ct}(f) = 1$.

Lemme 5.21. — *Pour tous $f, g \in A[X] - \{0\}$, $\mathrm{ct}(fg) = \mathrm{ct}(f)\,\mathrm{ct}(g)$ (à un élément inversible près).*

Démonstration. — Quitte à remplacer f par $f/\mathrm{ct}(f)$ et g par $g/\mathrm{ct}(g)$, nous pouvons supposer $f, g \in A[X]$ primitifs. Montrons que fg est primitif. Sinon il existe un élément irréductible p de A qui divise tous les coefficients de fg. Comme f et g sont primitifs, chacun a au moins un coefficient non divisible par p. Soit a_i (resp. b_j) le coefficient de f (resp. de g) d'indice minimal non divisible par p. Alors le coefficient c_{i+j} d'indice $i+j$ de fg est $c_{i+j} = a_i b_j + pd$, avec $d \in A$. Donc c_{i+j} n'est pas divisible par p (p irréductible et A est factoriel). Absurde ! □

Corollaire 5.22. — *Soit A un anneau factoriel de corps de fractions K. Alors les éléments irréductibles de $A[X]$ sont :*
i. les polynômes $f = p$ constants avec p irréductible de A,
ii. les polynômes primitifs de degré ≥ 1 qui sont irréductibles dans $K[X]$.

Démonstration. — Comme A est intègre, $A[X]^* = A^*$ et un polynôme constant est irréductible si et seulement il est irréductible dans A.
Soit $f \in A[X]$ est primitif de degré ≥ 1 irréductible dans $K[X]$. Si $f = gh$ avec $g, h \in A[X]$ alors $\mathrm{ct}(g) = \mathrm{ct}(h) = 1$ et g ou h est constant, donc une constante inversible. Donc f est irréductible dans $A[X]$.
Montrons enfin qu'un polynôme f de degré ≥ 1 irréductible dans $A[X]$ est primitif et irréductible dans $K[X]$. Or comme $\mathrm{ct}(f)$ divise f, nous avons f primitif. Si $f = gh$ avec $g, h \in K[X] - K$ alors il existe $a, b \in A$ et $g_1, h_1 \in A[X] - A$ avec $g = g_1/a$ et $h = h_1/b$. Donc $abf = g_1 h_1$ et $ab = \mathrm{ct}(g_1)\,\mathrm{ct}(h_1)$. Ainsi $f = \frac{g_1}{\mathrm{ct}(g_1)} \frac{h_1}{\mathrm{ct}(h_1)}$ est une décomposition de f dans $A[X] - A$ ce qui est exclu. Donc f est irréductible dans $K[X]$.

□

Exemple 5.23. — *Si $f \in A[X] - \{0\}$ est primitif, alors $fK[X] \cap A[X] = fA[X]$, i.e. le morphisme d'anneaux $A[X]/(f) \longrightarrow K[X]/(f)$ est injectif.*

Théorème 5.24. — *Si A est factoriel alors $A[X]$ aussi.*

Démonstration. — Montrons d'abord que tout polynôme $f \in A[X]$ admet une décomposition en produit d'éléments irréductibles. Quitte à écrire $f = \mathrm{ct}(f) f_1$ et à décomposer $\mathrm{ct}(f)$ en produit d'éléments irréductibles, nous pouvons supposer f primitif non constant. Quitte à multiplier f par $a \in A - \{0\}$, nous pouvons décomposer $af = f_1 \cdots f_n$ dans l'anneau principal $K[X]$ avec

$f_i \in A[X]$ irréductible dans $K[X]$. En passant aux contenus, nous obtenons $a = \mathrm{ct}(f_1)\cdots\mathrm{ct}(f_n)$ et $f = \prod_{i=1}^n \frac{f}{\mathrm{ct}(f_i)}$ est une décomposition de f en produit d'éléments irréductibles de $A[X]$.
Il suffit alors de montrer que $A[X]$ satisfait le lemme de Gauss. Soit $f \in A[X]$ irréductible. Si f est constant, alors $A[X]/(f) = (A/(f))[X]$ est intègre, donc (f) est premier dans $A[X]$. Supposons f primitif de degré ≥ 1 irréductible dans $K[X]$. Alors si f divise le produit gh de deux polynômes de $A[X]$, il divise g ou h dans $K[X]$, anneau principal donc factoriel. Quitte à échanger g et h, il existe $a \in A$ tel que $ah = qf$ avec $q \in A[X]$. Donc $\mathrm{ct}(ah) = a\,\mathrm{ct}(h) = \mathrm{ct}(q)$ car f est primitif et a divise $\mathrm{ct}(q)$. Ainsi $h = (q/a)f$ avec $q/a \in A[X]$ donc f divise h dans $A[X]$.

□

Corollaire 5.25. — *Si I est un ensemble (fini ou infini) et si A est factoriel alors $A[X_i, i \in I]$ est factoriel.*

Démonstration. — Le cas infini découle du cas fini. □

Théorème 5.26. — *(Critère d'Eisenstein)*
Soit A un anneau factoriel, $f \in A[X]$ non constant et $p \in A$ irréductible. Nous posons $f = \sum_{i=0}^n a_i X^i$ et nous supposons :
i. p ne divise pas a_n,
ii. p divise a_i pour $0 \leq i \leq n-1$,
iii. p^2 ne divise pas a_0.
Alors f est irréductible dans $K[X]$ (et aussi dans $A[X]$ s'il est primitif).

Démonstration. — Comme $f/\mathrm{ct}(f)$ vérifie les mêmes hypothèses que f, nous pouvons supposer f primitif de degré ≥ 2. Si f n'est pas irréductible $f = gh$ avec $g = b_r X^r + \cdots + b_0$, $h = c_s X^s + \cdots + c_0$ polynômes non constants de $A[X]$. L'anneau $B = A/(p)$ est intègre et $A[X]/pA[X]$ est isomorphe à $B[X]$. Dans $A[X]/pA[X] = B[X]$, nous avons $\bar{f} = \bar{a}_n X^n = \bar{g}\bar{h}$. Comme $\bar{a}_n = \bar{b}_r \bar{c}_s \neq 0$, les polynômes $\bar{g}$ et $\bar{h}$ ne sont pas constants et l'égalité dans l'anneau principal (donc factoriel) $\mathrm{Frac}(B)[X]$ implique que $\bar{g}$ et $\bar{h}$ sont divisibles par l'élément irréductible X dans $\mathrm{Frac}(B)[X]$. Donc p divise b_0 et c_0 ce qui contredit le fait que a_0 n'est pas divisible par p^2. □

Exemples 5.27. — *i. Le polynôme $X^8 - 9X^6 - 3$ est irréductible dans $\mathbb{Q}[X]$.*
ii. Si p est premier, $P(X) = 1 + X + \cdots + X^{p-1}$ est irréductible dans $\mathbb{Q}[X]$ (appliquer le critère d'Eisenstein à $P(X+1)$).
iii. Soit $a(y) \in \mathbb{C}[y]$ un polynôme non constant ayant au moins une racine simple. Alors pour tout $n \geq 1$, $x^n + a(y)$ est un élément irréductible de $\mathbb{C}[x, y]$.

5.2.2. Résultant. — Soit K un corps. Les anneaux $A = K[X_2, \ldots, X_n]$ et $A[X_1]$ sont factoriels. Ainsi les stratégies mises en place dans le paragraphe précédent

(§5.2.1) conduisent à une autre méthode de triangularisation des systèmes d'équations polynômiales, via le calcul de résultants dans $\mathrm{Frac}(A)[X_1]$.

Lemme 5.28. — *Soit $f, g \in K[X_1, \ldots, X_n]$ ayant des degrés en X_1 strictement positifs. Alors f et g ont un facteur commun dans $K[X_1, \ldots, X_n]$ de degré strictement positif en X_1 si et seulement si ils ont un facteur commun non constant dans $K(X_2, \ldots, X_n)[X_1]$.*

Démonstration. — $\Longrightarrow$ Clair.
$\Longleftarrow$ $f = \tilde{h}\tilde{f}_1$, $g = \tilde{h}\tilde{g}_1$ avec $\tilde{h}, \tilde{f}_1, \tilde{g}_1 \in K(X_2, \ldots, X_n)[X_1]$. Soit $d \in K[X_2, \ldots, X_n]$ le dénominateur commun de $\tilde{h}, \tilde{f}_1, \tilde{g}_1$. Alors $d^2 f = h f_1$ et $d^2 g = h g_1$ dans $K[X_1, \ldots, X_n]$ (avec des notations naturelles $f_1 = d\tilde{f}_1$...). Soit $h_1 \in K[X_1, \ldots, X_n]$ un facteur irréductible de h de degré strictement positif en X_1 (comme $\tilde{h} = h/d$ a un degré strictement positif en X_1, h_1 existe). Alors h_1 divise $d^2 f$. Mais $d^2 \in K[X_2, \ldots, X_n]$ donc h_1 divise f. De même h_1 divise g. □

Lemme 5.29. — *Soit $f, g \in K[X]$ des polynômes d'une variable X de degré $\ell > 0$ et $m > 0$. Alors f et g ont un facteur commun si et seulement si il existe des polynômes $A, B \in K[X]$ tels que :*
i. A et B ne sont pas tous les deux nuls
ii. A est de degré au plus $m - 1$ et B est de degré au plus $\ell - 1$,
iii. $Af + Bg = 0$.

Démonstration. — Si f, g ont un facteur commun $f = hf_1$ et $g = hg_1$ alors $A = g_1$ et $B = -f_1$ conviennent.
Réciproquement si f, g n'ont pas de facteur commun $uf + vg = 1$. S'il existe A, B avec $Bg = -Af$, alors

$$B = (uf + vg)B = uBf + vBg = (uB - vA)f$$

et $\deg B > \ell$ absurde. □

Rappelons la notion de résultant qui permet d'établir de façon calculatoire si deux polynômes de $K[X]$ sont premiers entre eux :

Définition 5.30. — *Soient $f, g \in K[X]$ de degrés strictement positifs avec*

$$f = a_0 X^\ell + \cdots + a_\ell, \quad g = b_0 X^m + \cdots + b_m.$$

La matrice de Sylvester de f, g est la matrice $(\ell+m)\times(\ell+m)$ (avec m colonnes (a_i) et ℓ colonnes (b_j))

$$Syl(f,g,X) = \begin{pmatrix} a_0 & 0 & \cdots & 0 & b_0 & \cdots & 0 \\ \vdots & a_0 & \ddots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & 0 & \vdots & \cdots & b_0 \\ a_\ell & \vdots & \cdots & a_0 & \vdots & \cdots & \vdots \\ 0 & a_\ell & \cdots & \vdots & b_m & \cdots & \vdots \\ \vdots & 0 & \ddots & \vdots & 0 & \ddots & \vdots \\ 0 & \vdots & \cdots & a_\ell & \vdots & \cdots & b_m \end{pmatrix}$$

Le résultant est le déterminant de la matrice de Sylvester $Res(f,g,X) = \det Syl(f,g,X)$.

Proposition 5.31. — *Soit $f, g \in K[X]$ de degré strictement positif. Alors $Res(f,g,X)$ est un polynôme à coefficients entiers en les coefficients de f et g. Les polynômes f, g ont un facteur commun dans $K[X]$ si et seulement si $Res(f,g,X) = 0$.*
De plus, il existe des polynômes $A, B \in K[X]$ entiers en les coefficients de f et g avec $Af + Bg = Res(f,g,X)$.

Démonstration. — Il s'agit de résoudre le système $fu + gv = 1$ en utilisant la formule de Cramer qui fait intervenir $Res(f,g,X)$ en dénominateur. □

Pour $f, g \in K[X_1,\ldots,X_n]$ de degré strictement positif en X_1, nous pouvons écrire :

$$f = a_0X_1^\ell + \cdots + a_\ell, \quad g = b_0X_1^m + \cdots + b_m$$

avec $a_i, b_j \in K[X_2,\ldots,X_n]$. La définition précédente donne un résultant $Res(f,g,X_1) \in K[X_2,\ldots,X_n]$. Ainsi

Proposition 5.32. — *Soit $f, g \in K[X_1,\ldots,X_n]$ de degré strictement positif en X_1. Alors*
i. $Res(f,g,X_1) \in < f, g > \cap K[X_2,\ldots,X_n]$.
ii. $Res(f,g,X_1) = 0$ si et seulement si f et g ont un facteur commun dans $K[X_1,\ldots,X_n]$ de degré strictement positif en X_1.

Démonstration. — i. D'après la proposition 5.31, le résultant est un polynôme entier en les a_i, b_j. Donc $Res(f,g,X_1) \in K[X_2,\ldots,X_n]$ et il existe A, B des polynômes en X_1 entiers en les a_i, b_j tels que $Af + Bg = Res(f,g,X_1)$. Donc $A, B \in K[X_2,\ldots,X_n][X_1]$, donc $Res(f,g,X_1) \in < f, g >$.
ii. D'après proposition 5.31 appliquée à $f, g \in K(X_2,\ldots,X_n)[X_1]$, $Res(f,g,X_1) = 0$ ssi f, g ont un facteur commun dans $K(X_2,\ldots,X_n)[X_1]$, donc dans $K[X_1,\ldots,X_n]$. □

Sous cette forme le résultant permet de résoudre par induction certains systèmes d'équations polynômiales, comme nous procèdons par triangularisation des systèmes linéaires. Nous nous nous contentons ici d'une application élémentaire à l'extension de solutions partielles de systèmes d'équations polynômiales complexes à plusieurs variables :

Corollaire 5.33. — *Soit* $f, g \in \mathbb{C}[X_1, \ldots, X_n]$, *avec*

$f = a_0 X_1^\ell + \cdots + a_\ell, \quad g = b_0 X_1^m + \cdots + b_m, \ \text{où } a_i, b_j \in K[X_2, \ldots, X_n], \ell, m \geq 1.$

Supposons que $Res(f, g, X_1) \in \mathbb{C}[X_2, \ldots, X_n]$ *s'annule en* $(c_2, \ldots, c_n) \in \mathbb{C}^{n-1}$. *Alors*
ou bien a_0 *ou* b_0 *s'annulent en* $(c_2, \ldots, c_n)$,
ou bien il existe $c_1 \in \mathbb{C}$ *tels que* f *et* g *s'annulent en* $(c_1, \ldots, c_n) \in \mathbb{C}^n$.

Démonstration. — Notons $c = (c_2, \ldots, c_n)$. Il s'agit de montrer que $f(X_1, c)$ et $g(X_1, c)$ ont une racine commune lorsque $a_0(c)$ et $b_0(c)$ ne sont pas tous les deux nuls. Supposons $a_0(c) \neq 0$ et $b_0(c) \neq 0$. Par hypothèses $h(c) = Res(f, g, X_1)(c) = 0$. Remarquons que $0 = h(c) = Res(f(X_1, c), g(X_1, c), X_1)$. Donc $f(X_1, c)$ et $g(X_1, c)$ ont une racine commune. □

5.3. Polynômes symétriques. — Soit A un anneau. Le groupe symétrique $\mathfrak{S}_n$ agit sur l'anneau $A[X_1, \ldots, X_n]$ via l'unique A-automorphisme tel que $\sigma(X_i) = X_{\sigma(i)}$:

$$\sigma(f) = \sum_{\nu \in \mathbb{N}^n} a_\nu X^{\sigma(\nu)} = \sum_{\nu \in \mathbb{N}^n} a_{\sigma^{-1}\nu} X^\nu \text{ pour } f = \sum_{\nu \in \mathbb{N}^n} a_\nu X^\nu, \sigma \in \mathfrak{S}_n$$

où $X^\nu = X_1^{\nu_1} \cdots X_n^{\nu_n}$ et $X^{\sigma(\nu)} = X_{\sigma(1)}^{\nu_1} \cdots X_{\sigma(n)}^{\nu_n}$.

Définition-Proposition 5.34. — *Pour* $j \in \{1, \ldots, n\}$, *les polynômes*

$$\Sigma_j = \sum_{1 \leq i_1 < \cdots < i_j \leq n} X_{i_1} \cdots X_{i_j} \in A[X_1, \ldots, X_n]$$

sont invariants par $\mathfrak{S}_n$ *et sont dits* **polynômes symétriques élémentaires**.

Exemple 5.35. — *Les polynômes symétriques élémentaires encodent les relations entre racines et coefficients des polynômes. Nous établissons par induction, dans* $\mathbb{Z}[X_1, \ldots, X_n][T]$,

$$(T - X_1) \cdots (T - X_n) = T^n - \Sigma_1 T^{n-1} + \cdots + (-1)^n \Sigma_n.$$

Théorème 5.36. — *L'unique morphisme d'anneaux*

$$\varphi : A[Y_1, \ldots, Y_n] \longrightarrow A[X_1, \ldots, X_n] \text{ avec } \varphi(Y_i) = \Sigma_i, 1 \leq i \leq n$$

est injectif et son image est $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$:

$$A[X_1, \ldots, X_n]^{\mathfrak{S}_n} = A[\Sigma_1, \ldots, \Sigma_n].$$

Démonstration. — Nous munissons $A[X_1, \ldots, X_n]$ de l'ordre lexicographique gradué.
• Soit $f \in A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ et $X_1^{i_1} \cdots X_n^{i_n}$ le plus grand monôme de f ayant un coefficient non nul. Comme f est symétrique, il contient tous les monômes obtenus à partir de $X_1^{i_1} \cdots X_n^{i_n}$ en permutant les variables, par conséquent $i_1 \geq i_2 \geq \cdots \geq i_n$ et

$$f = cX_1^{i_1} \cdots X_n^{i_n} + \text{ termes de degrés inférieurs}, c \neq 0.$$

• Le monôme de plus haut degré de Σ_i est $X_1 \cdots X_i$ donc le monôme de plus haut degré de $\Sigma_1^{d_1} \cdots \Sigma_n^{d_n}$ est

$$X_1^{d_1+d_2+\cdots+d_n} X_2^{d_2+\cdots+d_n} \cdots X_n^{d_n}.$$

Donc le terme de plus haut degré de

$$f - c\Sigma_1^{i_1-i_2}\Sigma_2^{i_2-i_3} \cdots \Sigma_n^{i_n}$$

est strictement inférieur au terme de plus haut degré de f. Par induction, nous obtenons donc une écriture de $f \in A[\Sigma_1, \ldots, \Sigma_n]$.
• Si l'écriture de $f \in A[\Sigma_1, \ldots, \Sigma_n]$ n'était pas unique, en soutrayant les deux polynômes, nous obtiendrions un polynôme non trivial $g(\Sigma_1, \ldots, \Sigma_n)$ qui serait nul comme polynôme en $X_1, \ldots, X_n$. Considérons le polynôme non nul

$$g(Y_1, \ldots, Y_n) = \sum_{\mu \in \mathbb{N}^n} g_{\mu_1,\ldots,\mu_n} Y_1^{\mu_1} \cdots Y_n^{\mu_n} = \sum_{\mu \in \mathbb{N}^n} g_\mu Y^\mu.$$

L'ensemble $\{\mu | g_\mu \neq 0\}$ est non vide, fini donc contient un unique élément maximal μ'. Donc $g(\Sigma_1, \ldots, \Sigma_n)$ contient le monôme $g_{\mu'} X_1^{\mu'_1+\cdots+\mu'_n} X_2^{\mu'_2+\cdots+\mu'_n} \cdots X_n^{\mu'_n}$ donc $g(\Sigma_1, \ldots, \Sigma_n) \neq 0$. D'où l'absurdité. □

Exemples 5.37. — *i. Pour $n \geq 2$ et $f = (T - X_1) \cdots (T - X_n) \in \mathbb{Z}[X_1, \ldots, X_n][T]$ le discriminant de f est défini par*

$$D(f) = \Pi_{i<j}(X_i - X_j)^2 \in \mathbb{Z}[X_1, \ldots, X_n]^{\mathfrak{S}_n} = \mathbb{Z}[\Sigma_1, \ldots, \Sigma_n].$$

Ainsi,

$$D(f) = (-1)^{n(n-1)/2} \Pi_{i=1}^n f'(X_i).$$

ii. Si K est un corps $K(X_1, \ldots, X_n)^{\mathfrak{S}_n} = K(\Sigma_1, \ldots, \Sigma_n)$. En effet, pour $f/g \in K(X_1, \ldots, X_n)^{\mathfrak{S}_n}$ nous posons $h_1 = \Pi_{\sigma \in \mathfrak{S}_n} \sigma g$ et $h_2 = h_1 f/g$. Alors $h_1, h_2 \in K[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ et $f/g = h_2/h_1$.
iii. (Formule de Newton) Les polynômes $S_k = X_1^k + \cdots + X_n^k$, $k \geq 1$ satisfont la récurrence

$$S_k - \Sigma_1 S_{k-1} + \cdots + (-1)^{k-1} \Sigma_{k-1} S_1 + (-1)^k k \Sigma_k = 0$$

avec la convention $\Sigma_k = 0$ pour $k > n$.

6. Algèbres

Soit A un anneau. Nous définissons ici la notion de A-algèbre qui généralise la notion de polynômes à coefficients dans un anneau A. Nous donnons quelques exemples de nature géométrique et arithmétique qui seront développés dans la suite de ce cours.

6.1. Définitions. —

Définition 6.1. — *Soit A un anneau. Une A-***algèbre** *est un couple (B, ι) composé d'un anneau B et d'un morphisme d'anneaux $\iota : A \longrightarrow B$ (qui est souvent sous-entendu). Un morphisme de A-algèbres $(B, \iota) \longrightarrow (B', \iota')$ est un morphisme d'anneaux $f : B \longrightarrow B'$ tel que $f \circ \iota = \iota'$. L'ensemble des morphismes de A-algèbres est noté* $\mathrm{Hom}_{A-\mathrm{Alg}}(B, B')$.

Exemples 6.2. — *i. Si A est un sous-anneau de B alors B est un A-algèbre pour l'inclusion ι.*
ii. Tout anneau B est une $\mathbb{Z}$-algèbre via $\iota : \mathbb{Z} \longrightarrow B, n \mapsto 1_B + \cdots + 1_B$ (somme de n termes) pour $n > 0$, $\iota(0) = 0_B$ et $\iota(n) = -\iota(-n)$ si $n < 0$. Les morphismes d'anneaux coincident avec les morphismes de $\mathbb{Z}$-algèbres.
iii. L'évaluation $\mathrm{ev}_i : \mathbb{R}[X] \longrightarrow \mathbb{C}, P(X) \mapsto P(i)$ *est un morphisme de $\mathbb{R}$-algèbres.*

Proposition 6.3. — *Soit A un anneau et B une A-algèbre. Alors l'application*

$$\mathrm{Hom}_{A-\mathrm{Alg}}(A[X_1, \ldots, X_n], B) \longrightarrow B^n, \quad \alpha \mapsto (\alpha(X_1), \ldots, \alpha(X_n)),$$

est bijective.

Démonstration. — Son inverse est donné par

$$b = (b_1, \ldots, b_n) \in B^n \mapsto \mathrm{ev}_b \in \mathrm{Hom}_{A-\mathrm{Alg}}(A[X_1, \ldots, X_n], B) : g \mapsto g(b_1, \ldots, b_n).$$

En effet $(\mathrm{ev}_b(X_1), \ldots, \mathrm{ev}_b(X_n)) = b$ et si $(\alpha(X_1), \ldots, \alpha(X_n)) = b$ alors, pour tout $g \in A[X_1, \ldots, X_n]$,

$$\mathrm{ev}_b(g) = g(\alpha(X_1), \ldots, \alpha(X_n)) = \alpha(g(X_1, \ldots, X_n)) = \alpha(g).$$

□

Définition 6.4. — *Une A-algèbre B est dite* **de type fini**, *s'il existe un momorphisme surjectif de A-algèbres $\pi : A[X_1, \ldots, X_n] \longrightarrow B$, i.e un système fini $(b_1, \ldots, b_n) \in B^n$ tel que tout b s'écrive sous la forme $b = P(b_1, \ldots, b_n)$ pour un $P \in A[X_1, \ldots, X_n]$. Nous disons alors que $(b_1, \ldots, b_n)$ est un* **système de générateurs**.
Une A-algèbre B est dite **de présentation finie** *si elle est de type fini pour un homomorphisme surjectif de A-algèbres $\pi : A[X_1, \ldots, X_n] \longrightarrow B$ de noyau un idéal de type fini.*

Exemples 6.5. — *i. Si K est un corps, tout anneau B intermédiaire $K \subset B \subset K[x]$ est une K-algèbre de type fini. En revanche $B = K[x^i y, i \in \mathbb{N}] \subset K[x, y]$ n'est pas une K-algèbre de type fini.*
ii. Soit A un anneau et $n \in \mathbb{N}^*$. L'algèbre des polynômes de Laurent à n indéterminées est l'algèbre $A[\mathbb{Z}^n]$ dont une base est donnée par la famille des monômes de Laurent $X^\nu = X_1^{\nu_1} \cdots X_n^{\nu_n}$, pour $\nu \in \mathbb{Z}^n$. Nous la notons également $A[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$.
iii. $K[X_1, \ldots, X_n]^{\mathfrak{S}_n} = K[\Sigma_1, \ldots, \Sigma_n]$ est une K-algèbre de type fini (Théorème 5.36). Plus généralement si G est un groupe fini qui agit via des morphismes de K-algèbres sur $K[X_1, \ldots, X_n]$, alors $K[X_1, \ldots, X_n]^G$ est une K-algèbre de type fini (Corollaire 23.11).
iv. Si G est un groupe fini et K un corps, la K-algèbre $K[G]$ de groupe G est le K-espace vectoriel K^G des applications de G dans K muni du produit de convolution

$$\left(\sum_{g \in G} a_g \delta_g\right)\left(\sum_{h \in G} b_h \delta_h\right) = \sum_{g,h \in G} a_g b_h \delta_{gh}.$$

Les résultats de la théorie des K-représentations de dimension finie de G s'obtiennent directement via l'étude de cette algèbre.
v. Si $A = K$ est un corps, les K-algèbres de type fini sont de présentation finie car tout idéal de $K[X_1, \ldots, X_n]$ est de type fini (voir Théorème de la base d'Hilbert 9.8).
vi. Pour K un corps, les K-algèbres de type fini jouent un rôle important en géométrie algébrique (voir §14).

PARTIE II

MODULES

Considérer des familles d'objets algébriques de même nature partageant des propriétés similaires demande un peu d'abstraction. Le langage des catégories permet d'unifier certaines constructions, de définir des objets ou des propriétés universelles, d'abstraire les stratégies de démonstration pour mieux les comprendre et pour les généraliser.

7. Le langage des catégories

Nous présentons un peu de langage des catégories, très pratique pour formuler des "propriétés universelles" et définir des objets "canoniques". Les objets algébriques ou géométriques représentant des foncteurs et leurs propriétés algébriques ou géométriques, correspondent aux propriétés des foncteurs qu'ils représentent.

7.1. Catégories. — Il s'agit de présenter brièvement ici un langage commode unificateur. Il permet de dégager un certain nombre de propriétés formelles qui se retrouvent dans des domaines divers.

Définition 7.1. — *Une* **catégorie** $\mathcal{C}$ *est la donnée d'une classe d'objets* $\mathrm{Ob}\mathcal{C}$ *et pour tout couple* (A, B) *d'objets de* $\mathcal{C}$*, d'un ensemble* $\mathrm{Hom}_{\mathcal{C}}(A, B)$ *de morphismes de* A *vers* B*, dont,*
- pour tout $A \in \mathrm{Ob}\mathcal{C}$*, un élément* $\mathrm{Id}_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$,
- pour tout triplet (A, B, C) *d'objets de* $\mathcal{C}$*, une application*

$$\mathrm{Hom}_{\mathcal{C}}(A, B) \times \mathrm{Hom}_{\mathcal{C}}(B, C) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, C), \quad (f, g) \mapsto g \circ f,$$

satisfaisant les propriétés suivantes :
(Associativité) : $(h \circ g) \circ f = h \circ (g \circ f)$ *pour tout triplet* (f, g, h) *de morphismes tel que ces compositions aient un sens.*
(Neutralité des identités) : pour tout couple (A, B) *d'objets de* $\mathcal{C}$ *et tout morphisme* f *de* A *vers* B*, nous avons* $f \circ \mathrm{Id}_A = \mathrm{Id}_B \circ f = f$.

Dans cette définition, nous ne précisons pas la notion de classes qui n'est pas une notion usuelle de théorie des ensembles (en particulier, la notation $A \in \mathrm{Ob}\mathcal{C}$ est abusive). Notons que $\mathrm{Ob}\mathcal{C}$ n'est pas, en général, un ensemble.

Exemples 7.2. — *i. La catégorie* Ens *est la catégorie dont les objets sont les ensembles et les morphismes, les applications.*
ii. La catégorie Gp *est la catégorie dont les objets sont les groupes et les morphismes, les morphismes de groupes.*
iii. La catégorie Ab *est la catégorie dont les objets sont les groupes abéliens et les morphismes, les morphismes de groupes. Il s'agit d'une sous-catégorie pleine de* Gp *: pour tous A, B objets de* Ab*, alors A, B sont des objets de* Gp *et les morphismes de A vers B coïncident dans ces deux catégories :* $\mathrm{Hom}_{\mathrm{Gp}}(A, B) = \mathrm{Hom}_{\mathrm{Ab}}(A, B)$.
iv. La catégorie Ann *est la catégorie dont les objets sont les anneaux et les morphismes, les morphismes d'anneaux.*
v. La catégorie Top *est la catégorie dont les objets sont les espaces topologiques et les morphismes sont les applications continues.*
*vi. Soit A un anneau, la catégorie A-*Alg *est la catégorie des A-algèbres dont les morphismes sont des morphismes de A-algèbres.*
*vii. Soit A un anneau, la catégorie A-*Mod *est la catégorie des A-modules dont les morphismes sont des morphismes de A-modules.*

Définition 7.3. — *A toute catégorie $\mathcal{C}$, nous pouvons associer la catégorie $\mathcal{C}^{\mathrm{op}}$* **opposée** *dont les objets sont les objets de $\mathcal{C}$ et les morphismes* $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(B, A)$.

7.2. Foncteurs. —

Définition 7.4. — *Un* **foncteur covariant** *F de la catégorie $\mathcal{C}$ dans la catégorie $\mathcal{C}'$ est une loi qui à chaque objet A de $\mathcal{C}$ associe un objet $F(A)$ de $\mathcal{C}'$ et à chaque morphisme $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ de $\mathcal{C}$ associe un morphisme $F(f) \in \mathrm{Hom}_{\mathcal{C}'}(F(A), F(B))$ de sorte que :*
i. pour tout objet A de $\mathcal{C}$, $F(\mathrm{Id}_A) = \mathrm{Id}_{F(A)}$,
ii. pour tous morphismes $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ et $g \in \mathrm{Hom}_{\mathcal{C}}(B, C)$: $F(g \circ f) = F(g) \circ F(f)$.

Pour définir la notion de foncteur contravariant, il suffit de renverser le sens des flèches : pour $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, alors $F(f) \in \mathrm{Hom}_{\mathcal{C}'}(F(B), F(A))$ et pour tous morphismes $f : A \longrightarrow B$ et $g : B \longrightarrow C$: $F(g \circ f) = F(f) \circ F(g)$.

Exemples 7.5. — *i. Le foncteur d'oubli est un foncteur covariant qui consiste à oublier certaines des structures des objets. Par exemple, l'oubli de la topologie induit un foncteur de* Top *dans* Ens.
ii. Si $F : \mathcal{C} \longrightarrow \mathcal{C}'$ et $G : \mathcal{C}' \longrightarrow \mathcal{C}''$ sont deux foncteurs, nous définissons naturellement le foncteur composé $G \circ F : \mathcal{C} \longrightarrow \mathcal{C}''$.
iii. A une catégorie $\mathcal{C}$ et un objet A de $\mathcal{C}$, nous associons un foncteur h_A covariant de $\mathcal{C}$ dans Ens *qui envoie un objet de B de $\mathcal{C}$ sur* $\mathrm{Hom}_{\mathcal{C}}(A, B)$ *et un morphisme*

$f \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ sur l'application $\mathrm{Hom}_{\mathcal{C}}(A,B) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(A,C)$, $g \mapsto f \circ g$.
iv. A une catégorie $\mathcal{C}$ et un objet A de $\mathcal{C}$, nous associons un foncteur h^A contravariant de $\mathcal{C}$ dans Ens *qui envoie un objet de B de $\mathcal{C}$ sur $\mathrm{Hom}_{\mathcal{C}}(B,A)$ et un morphisme $f \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ sur l'application $\mathrm{Hom}_{\mathcal{C}}(C,A) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(B,A)$, $g \mapsto g \circ f$.*

Définition 7.6. — *Soit $F, G : \mathcal{C} \longrightarrow \mathcal{C}'$ deux foncteurs. Un* **morphisme de foncteurs** *$\varphi : F \longrightarrow G$ est la donnée pour tout objet A de $\mathcal{C}$ d'un morphisme*

$$\varphi(A) : F(A) \longrightarrow G(A)$$

de la catégorie $\mathcal{C}'$ de telle sorte que pour tout morphisme $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ le diagramme suivant est commutatif :

$$\begin{array}{ccc} F(A) & \stackrel{\varphi(A)}{\longrightarrow} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \stackrel{\varphi(B)}{\longrightarrow} & G(B) \end{array}$$

Exemple 7.7. — *L'identité Id_F du foncteur F est le morphisme de F dans lui-même induit par la collection des $\mathrm{Id}_{F(A)}$ où A parcourt $\mathrm{Ob}\mathcal{C}$. Les morphismes de foncteurs se composent de façon naturelle.*

Définition 7.8. — *Un morphisme de foncteurs $\varphi : F \longrightarrow G$ est un* **isomorphisme** *s'il existe un morphisme $\psi : G \longrightarrow F$ tel que $\psi \circ \varphi = \mathrm{Id}_F$ et $\varphi \circ \psi = \mathrm{Id}_G$.*

Définition 7.9. — *Soit $\mathcal{C}$ une catégorie. Un foncteur covariant $F : \mathcal{C} \longrightarrow$* Ens *est dit* **représentable** *s'il existe $A \in \mathrm{Ob}\mathcal{C}$ et un isomorphisme $h_A \simeq F$.*

Exemples 7.10. — *i. Soit A un anneau commutatif. Soit le foncteur*

$$F : A - \mathrm{Alg} \longrightarrow \mathrm{Ens}, B \mapsto B.$$

La A-algèbre des polynômes $A[X]$ munie de son élément X représente le foncteur F : pour toute A-algèbre B et tout élément $b \in B$, il existe un unique morphisme de A-algèbres $\varphi : A[X] \longrightarrow B$, tel que $\varphi(X) = b$. En d'autres termes, pour A-algèbre B, l'application $\varphi \mapsto \varphi(X)$ est une bijection $\mathrm{Hom}_{A-\mathrm{Alg}}(A[X], B) \longrightarrow B$. Sa bijection réciproque associe à un élément $b \in B$ le morphisme d'évaluation en b : $\mathrm{ev}_b : A[X] \longrightarrow B$, $f \mapsto f(b)$.
ii. Plus généralement, soit A un anneau commutatif et $n \in \mathbb{N}^*$. Le foncteur qui envoie une A-algèbre B sur l'ensemble B^n est représentable. En effet l'application $f \mapsto (f(X_1), \ldots, f(X_n))$ établit une bijection fonctorielle en B entre $\mathrm{Hom}_{A-Alg}(A[X_1, \ldots, X_n], B)$ et B^n.
iii. Soit A un anneau et S un sous-ensemble de A. Le foncteur covariant

$$F : Ann \longrightarrow \mathrm{Ens}, \quad B \mapsto \{f \in \mathrm{Hom}(A,B) | \forall s \in S, f(s) \in B^*\}$$

est représentable : il existe un anneau C et un morphisme $g : A \longrightarrow C$ tels que :
- $g(S) \subset C^*$,

- pour tout $f : A \longrightarrow B$, tel que $f(S) \subset B^*$, il existe un unique $h : C \longrightarrow B$ faisant commuter le diagramme

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ g\downarrow & \nearrow & \\ C & & \end{array}.$$

En effet, il s'agit de montrer $C = A[T_s]_{s\in S}/(sT_s - 1)_{s\in S}$ et $g : a \mapsto \bar{a}$ représentent F. En général, il est difficile de dire si $C = 0$. Pour S une partie multiplicative (contenant 1), nous identifions (C, g) au localisé de A en S : $(S^{-1}A, g : a \mapsto \frac{a}{1})$.
iv. Soit $\mathcal{C}$ une catégorie. La flèche $\mathcal{C} \longrightarrow$ Ens qui envoie un objet A sur un singleton $\{*\}$ est un foncteur covariant F. Nous pouvons aussi le voir comme un foncteur contravariant G.
Si F est représentable, un représentant de F est dit objet initial de $\mathcal{C}$. Ainsi un objet A de $\mathcal{C}$ est initial si et seulement si $\mathrm{Hom}_{\mathcal{C}}(A, B)$ est un singleton pour tout objet B de $\mathcal{C}$.
Si G est représentable, un représentant de G est dit objet final de $\mathcal{C}$. Ainsi un objet A de $\mathcal{C}$ est final si et seulement si $\mathrm{Hom}_{\mathcal{C}}(B, A)$ est un singleton pour tout objet B de $\mathcal{C}$.
Par exemple, dans la catégorie Ens, *$\emptyset$ est initial et $\{*\}$ est final.*
Dans la catégorie Gp, *$\{e\}$ est initial et final.*
Dans la catégorie Ann *des anneaux, $\mathbb{Z}$ est initial et $\{0\}$ est final. L'objet initial $\mathbb{Z}$ dans la catégorie des anneaux permet de définir la caractéristique d'un anneau comme le générateur positif du noyau de l'unique morphisme d'anneaux (unitaires) $f : \mathbb{Z} \longrightarrow A$.*
La catégorie des corps n'a ni objet final, ni objet initial.

Montrer qu'un foncteur F est représentable revient à exhiber un objet A et un isomorphisme $h_A \simeq F$. Ce dernier point peut sembler délicat. Le lemme de Yoneda en donne une description concrète simple.

Lemme 7.11. — *(Lemme de Yoneda). Soit $\mathcal{C}$ une catégorie et A un objet de $\mathcal{C}$. Soit $F : \mathcal{C} \longrightarrow$ Ens un foncteur covariant et $\xi \in F(A)$. Alors ξ définit un morphisme de h_A vers F :*

$$\varphi_\xi : h_A \longrightarrow F, \quad h_A(B) = \mathrm{Hom}_{\mathcal{C}}(A, B) \longrightarrow F(B),\ f \mapsto F(f)(\xi).$$

Pour tout ψ morphisme de h_A dans F, il existe un unique $\xi \in F(A)$ tel que $\psi = \varphi_\xi$ à savoir $\psi(A)(\mathrm{Id}_A)$.
Par conséquent le foncteur $F : \mathcal{C} \longrightarrow$ Ens est représentable si et seulement si il existe un objet A de $\mathcal{C}$ et un élément $\xi \in F(A)$ tel que φ_ξ soit un isomorphisme.

Démonstration. — En effet, soit $\xi = \psi(A)(\mathrm{Id}_A)$, montrons que $\psi = \varphi_\xi$. Soit $B \in \mathrm{Ob}\mathcal{C}$ et $f : A \longrightarrow B$ un élément de $h_A(B)$. Par définition d'un morphisme

de foncteurs, nous disposons d'un diagramme commutatif

$$\begin{array}{ccc} h_A(A) & \xrightarrow{\psi(A)} & F(A) \\ h_A(f)\downarrow & & \downarrow F(f) \\ h_A(B) & \xrightarrow{\psi(B)} & F(B) \end{array}$$

Comme $h_A(f)$ est la composition avec f, nous avons $h_A(f)(\mathrm{Id}_A) = f$. L'image de Id_A par $\psi(A)$ est égale à ξ par définition. Par commutativité du diagramme nous obtenons $\psi(B)(f) = F(f)(\xi) = \varphi_\xi(B)(f)$. D'où l'égalité attendue.
Remarquons enfin que si ξ satisfait $\psi = \varphi_\xi$, alors

$$\psi(A)(\mathrm{Id}_A) = \varphi_\xi(A)(\mathrm{Id}_A) = F(\mathrm{Id}_A)(\xi) = \mathrm{Id}_{F(A)}(\xi) = \xi.$$

D'où l'unicité de ξ. □

Définition 7.12. — *Un couple (A, ξ) est dit caractérisé par une* **propriété universelle** *s'il représente un foncteur F. Le couple (A, ξ) est un* **représentant** *de F et ξ est dit* **objet universel relativement** *au foncteur F.*

Lemme 7.13. — *Soit $F : \mathcal{C} \longrightarrow \mathrm{Ens}$ un foncteur covariant représentable. Si (A, ξ) et (A', ξ') sont deux représentants de F alors il existe un unique $f \in \mathrm{Hom}_{\mathcal{C}}(A', A)$ tel que $F(f)(\xi') = \xi$. De plus f est un isomorphisme.*

Démonstration. — Comme A' représente F, il existe un unique $f \in \mathrm{Hom}_{\mathcal{C}}(A', A)$ tel que $F(f)(\xi') = \xi$. De même il existe un unique $f' \in \mathrm{Hom}_{\mathcal{C}}(A, A')$ tel que $F(f')(\xi) = \xi'$. Alors $f' \circ f \in \mathrm{Hom}_{\mathcal{C}}(A', A')$ avec $F(f' \circ f)(\xi') = \xi'$. Or $h_{A'}(A') \xrightarrow{\sim} F(A')$, $h \mapsto F(h)(\xi')$ et $F(\mathrm{Id}_{A'})(\xi') = \xi'$. Donc $f' \circ f = \mathrm{Id}_{A'}$. De même $f \circ f' = \mathrm{Id}_A$ donc f est unique et c'est un isomorphisme. □

7.3. Limites injectives et projectives. —

Définition 7.14. — *Soit $\mathcal{C}$ une catégorie. Un* **diagramme** *de $\mathcal{C}$ est la donnée d'une famille $(A_i)_{i \in I}$ d'objets de $\mathcal{C}$ et pour tout $(i, j) \in I \times I$ d'un ensemble E_{ij} de morphismes de A_i vers A_j. Un diagramme $((A_i), (E_{ij}))$ est* **commutatif** *si pour tout triplet (i, j, k) et tout $f \in E_{ij}$, $g \in E_{jk}$, $h \in E_{ik}$, nous avons $h = g \circ f$.*

Définition 7.15. — *Soit $\mathcal{D} = ((A_i), (E_{ij}))$ un diagramme dans $\mathcal{C}$ et B un objet de $\mathcal{C}$.*
Un **morphisme** *de $\mathcal{D}$ dans B est une famille $(a_i : A_i \longrightarrow B)$ de morphismes telle que l'on ait pour tout couple (i, j) et tout tout $f \in E_{ij}$, $a_j \circ f = a_i$. Nous notons $\mathrm{Hom}_{\mathcal{C}}(\mathcal{D}, B)$ l'ensemble des morphismes de $\mathcal{D}$ dans B.*
Un morphisme de B dans $\mathcal{D}$ est une famille $(b_i : B \longrightarrow A_i)$ de morphismes telle que l'on ait pour tout couple (i, j) et tout tout $f \in E_{ij}$, $f \circ b_i = b_j$. Nous notons $\mathrm{Hom}_{\mathcal{C}}(B, \mathcal{D})$ l'ensemble des morphismes de B dans $\mathcal{D}$.

Définition 7.16. — *Soit $\mathcal{D}$ un diagramme de $\mathcal{C}$. Si le foncteur covariant de $\mathcal{C}$ dans Ens qui envoie un objet B sur $\mathrm{Hom}_{\mathcal{C}}(\mathcal{D}, B)$ est représentable, son représentant est dit* **limite inductive** *du diagramme $\mathcal{D}$ et est noté $\varinjlim \mathcal{D}$.*

Soit $\mathcal{D}$ un diagramme de $\mathcal{C}$. Si le foncteur contravariant de $\mathcal{C}$ dans Ens *qui envoie un objet B sur $\mathrm{Hom}_{\mathcal{C}}(B, \mathcal{D})$ est représentable, son représentant est dit* **limite projective** *du diagramme $\mathcal{D}$ et est noté $\varprojlim \mathcal{D}$.*

Exemples 7.17. — *i. Soit $\mathcal{D} = ((A_i), (\emptyset))$ un diagramme de $\mathcal{C}$ constitué d'une famille d'objets sans morphisme. La limite inductive $\varinjlim \mathcal{D}$ existe si et seulement si le foncteur*

$$F : \mathcal{C} \longrightarrow \mathrm{Ens}, B \mapsto \prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(A_i, B)$$

est représentable. Si c'est le cas, la limite inductive est dite somme (disjointe ou directe) des $(A_i)_{i \in I}$ et notée $\bigsqcup_{i \in I} A_i$ ou $\bigoplus_{i \in I} A_i$ suivant le contexte.
La limite projective $\varprojlim \mathcal{D}$ existe si et seulement si le foncteur

$$F : \mathcal{C} \longrightarrow \mathrm{Ens}, B \mapsto \prod_{i \in I} \mathrm{Hom}_{\mathcal{C}}(B, A_i)$$

est représentable. Si c'est le cas, la limite projective est dite produit des $(A_i)_{i \in I}$ et notée $\prod_{i \in I} A_i$. Il existe des produits dans Ens, Gp, Ann *mais pas dans la catégorie des corps (un produit de corps n'est pas un corps).*
Il existe aussi des produits dans la catégorie Top *des espaces topologiques : la topologie produit sur $\prod_{i \in I} A_i$ est la topologie la moins fine pour laquelle les projections $\prod_{i \in I} A_i \longrightarrow A_i$ sont continues. Les ouverts de la forme*

$$\{\prod_{j=1}^{n} U_{i_j} \times \prod_{i \in I - \{i_1, \ldots, i_n\}} A_i, U_{i_j} \text{ ouvert de } A_{i_j}\}$$

forment une base de la topologie produit.
ii. Soit $(A_i)_{i \in \mathbb{N}}$ des ensembles (resp. groupes, anneaux) et des applications (resp. des morphismes de groupes, d'anneaux)

$$A_1 \xleftarrow{f_1} A_2 \xleftarrow{f_2} A_3 \xleftarrow{f_3} \ldots$$

La limite projective de ce diagramme (où les morphismes sont les morphismes Id_{A_i} et les compositions des morphismes f_i) est l'ensemble des suites compatibles d'éléments :

$$A = \varprojlim_n A_n = \{a = (a_n)_{n \geq 1} | a_n \in A_n, f_n(a_{n+1}) = a_n, \forall n \geq 1\}.$$

Il s'identifie au sous-objet du produit direct $\prod_{i \in \mathbb{N}} A_i$ par les relations induites par les morphismes du diagramme. C'est un ensemble (resp. un groupe, un anneau pour les opérations termes à termes). De plus si chaque f_n est une application continue entre les espaces topologiques A_{n+1} et A_n, alors $A \subset \Pi_{n=1}^{\infty} A_n$ admet une topologie naturelle induite par la topologie produit des A_n.
iii. Soit A un anneau. La limite projective $\varprojlim_n A[X]/(X^n)$ (i.e. du diagramme $(A[X]/(X^n), \pi_{m,n})$ où les $\pi_{m,n}$ sont les projections canoniques) s'identifie naturellement avec l'anneau des séries formelles $A[[X]]$.
iv. Soit A un anneau. Pour $t \in A$, nous notons $S_t = \{t^i, i \in \mathbb{N}\}$. Pour tout

ensemble multiplicatif S contenant 1, $S^{-1}A = \varinjlim S_t^{-1}A$ où t décrit les éléments de S partiellement ordonnés par la division.
En effet si $t', t \in S$ avec $t' = st$ alors

$$\varphi_{tt'} : S_t^{-1}A \longrightarrow S_{t'}^{-1}A, \quad \frac{a}{t} \mapsto \frac{as}{t'}$$

donc $((S_t^{-1}A), \varphi_{tt'})$ est un diagramme $\mathcal{D}$. Pour $t \in S$, le morphisme $A \longrightarrow S^{-1}A$ s'étend de façon unique en un morphisme d'anneaux $S_t^{-1}A \longrightarrow S^{-1}A$, $\frac{a}{t} \mapsto \frac{a}{t}$ et ce morphisme est compatible avec les applications du diagramme. Enfin $S^{-1}A = \varinjlim \mathcal{D}$ représente le foncteur Ann *dans* Ens *qui envoie un objet B sur* $\mathrm{Hom}_{\mathcal{C}}(\mathcal{D}, B)$.
v. Pour tout entier $b > 1$, si $n \leq m$, l'inclusion des idéaux de $\mathbb{Z}$, $b^m\mathbb{Z} \subset b^n\mathbb{Z}$, induit un morphisme d'anneaux $\mathbb{Z}/b^n\mathbb{Z} \longleftarrow \mathbb{Z}/b^m\mathbb{Z}$. L'anneau des entiers b-adiques est défini comme

$$\mathbb{Z}_b = \varprojlim_n \mathbb{Z}/b^n\mathbb{Z} = \{(a_n)_{n\geq 1} | a_n \in \mathbb{Z}/b^n\mathbb{Z}, a_{n+1} \equiv a_n \mod b^n\}$$

Les éléments de $\mathbb{Z}_b$ s'écrivent comme des sommes

$$x = \sum_{i=0}^{\infty} x_i b^i, \quad x_i \in \{0, \ldots, b-1\}.$$

La topologie discrète sur les anneaux finis $\mathbb{Z}/b^n\mathbb{Z}$ induit une topologie sur $\mathbb{Z}_b$ (induite par la topologie produit) dont une base d'ouverts est donnée par les ensembles $x + b^n\mathbb{Z}_b$.
Si $b = p_1^{r_1} \cdots p_k^{r_k}$ avec $r_i \geq 1$ et p_i des nombres premiers distincts. Alors le théorème des restes chinois (Théorème 2.13)

$$\mathbb{Z}/b^n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p_1^{nr_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{nr_k}\mathbb{Z}$$

donne l'isomorphisme

$$\mathbb{Z}_b \xrightarrow{\sim} \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}.$$

C'est pourquoi, il suffit d'étudier l'anneau des entiers p-adiques $\mathbb{Z}_p$ pour p nombre premier (voir §24).
vi. Notons $\overline{K}$ une clôture algébrique de K. Le groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ de $\overline{K}$ sur K s'obtient comme limite projective des groupes de Galois des extensions algébriques finies (voir §21.3).

7.4. Foncteurs adjoints. —

Définition 7.18. — *Soit $F : \mathcal{C} \longrightarrow \mathcal{C}'$ et $G : \mathcal{C}' \longrightarrow \mathcal{C}$ deux foncteurs covariants. Nous disons que F est un* **adjoint à gauche** *de G, ou que G est un* **adjoint à droite** *de F, ou que (F, G) est un* **couple de foncteurs adjoints**, *s'il existe une collection d'isomorphismes*

$$\iota_{(A,B)} : \mathrm{Hom}_{\mathcal{C}'}(F(A), B) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(A, G(B))$$

paramétrée par $(A, B) \in \mathrm{Ob}\mathcal{C} \times \mathrm{Ob}\mathcal{C}'$ *et fonctorielle en* (A, B)*, ie. pour tout morphisme* $u : A \longrightarrow A'$ *de* $\mathcal{C}$ *et toute flèche* $v : B \longrightarrow B'$ *de* $\mathcal{C}'$*, le diagramme suivant est commutatif*

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{C}'}(F(A'), B) & \underset{\iota_{(A',B)}}{\xrightarrow{\sim}} & \mathrm{Hom}_{\mathcal{C}}(A', G(B)) \\
\downarrow^{\circ F(u)} & & \downarrow^{\circ u} \\
\mathrm{Hom}_{\mathcal{C}'}(F(A), B) & \underset{\iota_{(A,B)}}{\xrightarrow{\sim}} & \mathrm{Hom}_{\mathcal{C}}(A, G(B)) \\
\downarrow^{v\circ} & & \downarrow^{G(v)\circ} \\
\mathrm{Hom}_{\mathcal{C}'}(F(A), B') & \underset{\iota_{(A,B')}}{\xrightarrow{\sim}} & \mathrm{Hom}_{\mathcal{C}}(A, G(B'))
\end{array}$$

Exemples 7.19. — *i. Le foncteur* $F : \mathrm{Gp} \longrightarrow \mathrm{Ab}$*,* $G \mapsto G/D(G)$ *admet un adjoint à droite le foncteur oubli* $\mathrm{Ab} \longrightarrow \mathrm{Gp}$*.*
ii. Soit K *un corps et* Vect_K *la catégorie des* K*-espaces vectoriels. Le foncteur* $F : \mathrm{Ens} \longrightarrow \mathrm{Vect}_K$ *qui à un ensemble* B *associe le* K*-espace vectoriel de base* $(e_b)_{b\in B}$ *est l'adjoint du foncteur oubli* $G : \mathrm{Vect}_K \longrightarrow \mathrm{Ens}$*.*
iii. Le foncteur oubli $\mathrm{Top} \longrightarrow \mathrm{Ens}$ *admet un adjoint à gauche et à droite. Son adjoint à gauche est le foncteur qui associe à un ensemble le même ensemble muni de la topologie discrète. Son adjoint à droite associe à un ensemble le même ensemble muni de la topologie grossière.*
iv. Supposons que le foncteur covariant $G : \mathcal{C}' \longrightarrow \mathcal{C}$ *admette un adjoint à gauche* F *et fixons* A *de* $\mathcal{C}$*. Alors le foncteur covariant*

$$\mathcal{C}' \longrightarrow \mathrm{Ens}, \quad B \mapsto \mathrm{Hom}_{\mathcal{C}}(A, G(B))$$

est isomorphe à $B \mapsto \mathrm{Hom}_{\mathcal{C}'}(F(A), B)$*. Il est donc représentable.*
v. Soit $F : \mathcal{C} \longrightarrow \mathcal{C}'$ *un foncteur covariant et* $\mathcal{D} = ((A_i), (E_{ij}))$ *un diagramme dans* $\mathcal{C}$*. Supposons que* F *admette un adjoint à droite* G *et que* $\varinjlim \mathcal{D}$ *existe dans* $\mathcal{C}$*. Alors* $\varinjlim F(\mathcal{D})$ *existe et est égal à* $F(\varinjlim \mathcal{D})$*.*

8. Modules

Les modules, en particulier les idéaux, sont des objets linéaires. Ils sont donc plus aisés à étudier que les anneaux eux-mêmes. Cependant ils ne sont en général pas libres, contrairement aux espaces vectoriels qui sont des modules sur des corps.

8.1. Définitions. —

Définition 8.1. — *Un* A-**module** $(M, +, \cdot)$ *est un ensemble muni d'une loi interne* $+$ *et d'une loi externe* $A \times M \longrightarrow N, (\alpha, m) \mapsto \alpha m$ *vérifiant :*
i. $(M, +)$ *est un groupe abélien,*
ii. Pour tous $\alpha, \beta \in A$ *et* $m, m' \in M$ *les propriétés suivantes sont satisfaites :*
- (distributivité) $\alpha(m + m') = \alpha m + \alpha m'$*,* $(\alpha + \beta)m = \alpha m + \beta m$*,*

- *(associativité)* $(\alpha\beta)m = \alpha(\beta m)$,
- *(élément neutre)* $1 \cdot m = m$.

Comme l'anneau A est supposé commutatif, il n'y a pas lieu de distinguer entre module à gauche et module à droite. De plus si M est un A-module $(-1)m = -m$.

Exemples 8.2. — *i. Si $A = K$ est un corps, un K-module est un K-espace vectoriel.*
ii. L'anneau A est un A-module, l'opération externe étant la multiplication dans A.
iii. Si $\iota : A \longrightarrow B$ est un morphisme d'anneaux, la multiplication externe $A \times B \longrightarrow B, (a, b) \mapsto \iota(a)b$ munit B d'une structure de A-module, autrement dit une A-algèbre est un A-module.
iv. Tout groupe abélien est un $\mathbb{Z}$-module : si $\alpha \in \mathbb{N}^*$, $\alpha m = m + \cdots + m$ (α fois), $(-\alpha)m = -\alpha m$ et $0m = 0$.
v. Soit $n > 0$ et M un groupe abélien de n-torsion, i.e. tel que $nx = 0$ pour tout $x \in M$. Alors M est un $\mathbb{Z}/n\mathbb{Z}$-module.

Définition 8.3. — *Soit M un A-module. Un* **sous-module** *N de M est un sous-groupe de $(M, +)$ qui est stable par la multiplication externe par tout élément de A :*

$$a \in A, n \in N \Longrightarrow an \in N.$$

Exemples 8.4. — *i. Une partie N de M est un sous-module si et seulement si N contient 0 et si pour tous $x, y \in N$ et $\alpha \in A$, $x + y \in N$ et $\alpha x \in N$.*
ii. Soit I une partie de A. Alors I est un sous-module de A si et seulement si c'est un idéal de A.
iii. Soit S une partie d'un A-module M. Le sous-A-module $< S >$ de M engendré par S est l'ensemble des combinaisons linéaires $\sum_{s \in S} \alpha_s s$ où $(a_s)_{s \in S}$ est une famille presque nulle d'éléments de A. C'est le plus petit sous-module de M qui contient S. Les éléments de S sont dits générateurs de $< S >$.
Remarquons que nous pouvons avoir besoin de plus de générateurs pour un sous-module N de M que pour M (prendre par exemple un idéal non principal de A). Cette difficulté disparait si A est principal (§10).
iv. Soit N un sous-A-module de M. Alors l'ensemble

$$(N : M) = \{a \in A | am \in N, \forall m \in M\}$$

est un idéal de A. Si $N = (0)$, nous notons $(0 : M) = \mathrm{Ann}_A M$, l'annulateur de M (voir Définition 8.8).
v. Si I est un idéal de A et M un A-module, l'ensemble $M[I]$ des éléments tués par I :

$$M[I] = \{m \in M | \forall a \in I, am = 0\}$$

est un sous-module de M.
Si I' est un autre idéal

$$M[I] \cap M[I'] = M[I + I'],$$

et si $A = I + I'$,

$$M[I] + M[I'] = M[I \cap I'] = M[II'].$$

Définition 8.5. — *Un* **morphisme** *de A-modules est une application $f : M \longrightarrow M'$ entre deux A-modules M et M' telle que pour tous $a, b \in A$ et $m, n \in M$, nous avons :*

$$f(am + bn) = af(m) + bf(n).$$

L'ensemble des morphismes de A-modules de M dans M' est noté $\mathrm{Hom}_A(M, M')$. *C'est un A-module pour les opérations :*

$$(f + f')(m) = f(m) + f'(m), \ \ (\alpha f)(m) = f(\alpha m) = \alpha f(m).$$

L'image $\mathrm{im}\, f$ *et le noyau* $\ker f$ *sont des sous-A-modules de M', resp. M.*
Un morphisme de A-modules de M dans M est dit **endomorphisme** *de M. Nous notons* $\mathrm{Hom}_A(M, M)$ *l'ensemble des endomorphismes.*

8.2. Opérations sur les modules. —

Définition 8.6. — *Soit M un A-module, N un sous-module de M. Alors le groupe quotient M/N équipé de la loi externe $\alpha \cdot \overline{m} = \overline{\alpha \cdot m}$, $\alpha \in A$ et $\bar{m} \in M/N$, est un A-module, dit* **module quotient** *de M par N.*

Exemples 8.7. — *i. Le module quotient $(M/N, \pi : M \longrightarrow M/N)$ satisfait la propriété universelle suivante : Pour tout $f \in \mathrm{Hom}_A(M, M')$, avec $N \subset \ker f$, il existe un unique $\tilde{f} \in \mathrm{Hom}_A(M/N, M')$ tel que $f = \tilde{f} \circ \pi$, i.e. $(M/N, \pi)$ représente le foncteur*

$$F : A - \mathrm{Mod} \longrightarrow \mathrm{Ens}, M' \mapsto \{f \in \mathrm{Hom}_A(M, M') | N \subset \ker f\}.$$

ii. Si $f \in \mathrm{Hom}_A(M, M')$, il existe un unique $\tilde{f} : M/\ker f \longrightarrow M'$ tel que $f = \tilde{f} \circ \pi$ où $\pi : M \longrightarrow M/\ker f$ est la surjection canonique. De plus $\tilde{f}$ est injective d'image $\mathrm{im}\, f$.
iii. Soit A un anneau et $f : M \longrightarrow N$ un morphisme de A-modules. Le A-module quotient $N/f(M)$ est appelé conoyau de f et noté $\mathrm{Coker}\, f$. *Nous avons* $\mathrm{Coker}\, f = 0$ *si et seulement si f est surjectif. Donc f est un isomorphisme si et seulement si* $\ker f = 0$ *et* $\mathrm{Coker}\, f = 0$.

Définition 8.8. — *Soit A un anneau, I un idéal de A et M un A-module. Nous notons $IM \subset M$ le sous-module de M engendré par $\{am | a \in I, m \in M\}$.*
*L'***annulateur** *de M dans A est l'idéal de A*

$$\mathrm{Ann}_A(M) = \{a \in A | ax = 0, \forall x \in M\}.$$

Le module M est dit **fidèle** *si* $\mathrm{Ann}_A(M) = 0$

Définition 8.9. — *(Changement d'anneau) Soit $f : B \longrightarrow A$ un morphisme d'anneaux. Tout A-module M admet une structure de B-module, via $bm = f(b)m$, $b \in B$, $m \in M$.*

Définition-Proposition 8.10. — *Soit $(M_\lambda)_{\lambda\in\Lambda}$ une famille de A-modules. Alors $\prod_{\lambda\in\Lambda} M_\lambda$ est un A-module pour les lois induites. Il est dit* **produit direct** *des M_λ. Pour tout $\mu \in \Lambda$, la projection $\pi_\mu : \prod_{\lambda\in\Lambda} M_\lambda \longrightarrow M_\mu$ est un morphisme (surjectif) de A-modules.*
Le produit direct satisfait la propriété universelle : pour tout A-module N avec, pour tout $\lambda \in \Lambda$, un morphisme $f_\lambda \in \mathrm{Hom}_A(N, M_\lambda)$, il existe un unique $f \in \mathrm{Hom}(N, \prod_{\lambda\in\Lambda} M_\lambda)$ tel que $f_\lambda = \pi_\lambda \circ f$ pour tout $\lambda \in \Lambda$, défini par $f(n) = (f_\lambda(n))_{\lambda\in\Lambda}$.
La **somme directe** *des modules $(M_\lambda)_{\lambda\in\Lambda}$ est le sous-module*

$$\bigoplus_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} M_\lambda | m_\lambda \text{ presque tous nuls}\} \subset \prod_{\lambda\in\Lambda} M_\lambda$$

Pour tout $\mu \in \Lambda$, l'inclusion $\iota_\mu : M_\mu \longrightarrow \bigoplus_{\lambda\in\Lambda} M_\lambda$, $\iota_\mu(x) = (m_\lambda)$ avec $m_\lambda = \delta_{\lambda\mu} x$ est un morphisme injectif de A-modules. La somme directe satisfait la propriété universelle : pour tout A-module N muni de morphismes $f_\lambda \in \mathrm{Hom}_A(M_\lambda, N)$ pour tout $\lambda \in \Lambda$, il existe un unique $f \in \mathrm{Hom}_A(\bigoplus_{\lambda\in\Lambda} M_\lambda, N)$ tel que $f_\lambda = f \circ \iota_\lambda$ pour tout $\lambda \in \Lambda$.

Exemples 8.11. — *i. La somme directe $\bigoplus_{\lambda\in\Lambda} M_\lambda$ munie des inclusions $(\iota_\mu : M_\mu \longrightarrow \bigoplus_{\mu\in\Lambda} M_\lambda)_{\lambda\in\Lambda}$ représente le foncteur covariant $F : A - \mathrm{Mod} \longrightarrow \mathrm{Ens}$*

$$N \mapsto \prod_{\lambda\in\Lambda} \mathrm{Hom}_A(M_\lambda, N).$$

Le produit direct $\prod_{\lambda\in\Lambda} M_\lambda$ muni des projections $(\pi_\mu : \prod_{\lambda\in\Lambda} M_\lambda \longrightarrow M_\mu)_{\mu\in\Lambda}$ représente le foncteur contravariant $F : A - \mathrm{Mod} \longrightarrow \mathrm{Ens}$

$$N \mapsto \prod_{\lambda\in\Lambda} \mathrm{Hom}_A(N, M_\lambda).$$

ii. Le produit direct et somme directe d'une famille finie de A-modules coïncident. Les applications

$$\mathrm{Hom}_A(N, \prod_{\lambda\in\Lambda} M_\lambda) \xrightarrow{\simeq} \prod_{\lambda\in\Lambda} \mathrm{Hom}_A(N, M_\lambda), \quad f \mapsto (\pi_\mu \circ f)_{\mu\in\Lambda}$$

et

$$\mathrm{Hom}_A(\bigoplus_{\lambda\in\Lambda} M_\lambda, N) \xrightarrow{\simeq} \prod_{\lambda\in\Lambda} \mathrm{Hom}_A(M_\lambda, N) \quad g \mapsto (g \circ \iota_\mu)_{\mu\in\Lambda}$$

sont des bijections. Le produit direct de n copies de M est noté M^n. Plus généralement, pour Λ un ensemble, nous notons

$$M^{(\Lambda)} = \bigoplus_{i\in\Lambda} M \subset \prod_{i\in\Lambda} M = M^\Lambda.$$

iii. Soit A un anneau. A tout ensemble Λ, associer le A-module libre $A^{(\Lambda)}$ définit un foncteur

$$A^{(-)} : \mathrm{Ens} \longrightarrow A - \mathrm{Mod}, \quad \Lambda \mapsto A^{(\Lambda)}.$$

En effet soit $\phi : \Lambda \longrightarrow \Lambda'$ une application, il s'agit de définir une application A-linéaire $A^{(\Phi)} : A^{(\Lambda)} \longrightarrow A^{(\Lambda')}$, de telle façon que $A^{(1_\Lambda)} = \mathrm{Id}_{A^{(\Lambda)}}$ pour tout ensemble

Λ et $A^{(\phi')} \circ A^{(\phi)} = A^{(\phi' \circ \phi)}$ pour toutes applications $\phi : \Lambda \longrightarrow \Lambda'$ et $\phi' : \Lambda' \longrightarrow \Lambda''$. Notons $(e_\lambda)_{\lambda \in \Lambda}$ et $(e'_{\lambda'})_{\lambda' \in \Lambda'}$ les bases canoniques de $A^{(\Lambda)}$ et $A^{(\Lambda')}$ respectivement. Il suffit de poser $A^{(\phi)}(e_\lambda) = e'_{\varphi(e_\lambda)}$, $\lambda \in \Lambda$.

Définition-Proposition 8.12. — *Soit A un anneau non nul. Un A-module M est* **libre** *s'il existe un isomorphisme de A-modules $f : A^{(\Lambda)} \longrightarrow M$ pour un ensemble Λ. Une* **base** *de M est l'image de la base canonique $(e(\lambda))_{\lambda \in \Lambda}$ d'éléments $e(\lambda)_\mu = \delta_{\lambda\mu}$ de $A^{(\Lambda)}$ par un tel isomorphisme f. Le* **rang** *du module libre M est le cardinal de Λ. Il ne dépend que de M.*

Démonstration. — Supposons que $f : A^{(\Lambda)} \longrightarrow A^{(\Lambda')}$ soit un isomorphisme de A-modules. Il s'agit de montrer que Λ et Λ' ont le même cardinal. D'après 2.28, A admet un idéal maximal $\mathfrak{m}$. Alors f induit un isomorphisme $(A/\mathfrak{m})^{(\Lambda)} \longrightarrow (A/\mathfrak{m})^{(\Lambda')}$ de $A/\mathfrak{m}$-espaces vectoriels. Le fait que deux espace vectoriels isomorphes ont même dimension permet alors de conclure. □

Exemples 8.13. — *i. Dire que $(x_\lambda)_{\lambda \in \Lambda}$ est une base équivaut au fait que la famille (x_λ) est génératrice et libre, i.e. $\sum_{\lambda \in \Lambda} a_\lambda x_\lambda = 0$ implique que la famille presque nulle (a_λ) est nulle.*
ii. Soit A un anneau commutatif non nul. Si $f : A^r \longrightarrow A^s$ est un morphisme surjectif de A-modules, alors $r \geq s$.

Définition 8.14. — *Un A-module M est dit de* **type fini** *s'il existe une partie finie S de M telle que M soit engendré par S, i.e. il existe $n \in \mathbb{N}$ et un morphisme surjectif de A-modules $f : A^n \longrightarrow M$.*
Le A-module M est dit de **présentation finie**, *s'il existe $f : A^n \longrightarrow M$ surjectif avec $\ker f$ de type fini.*
Le A-module M est dit **cyclique** *s'il existe un morphisme surjectif $f : A \longrightarrow M$ (i.e. s'il existe un idéal I de A tel que $M \simeq A/I$).*

Exemples 8.15. — *i. Un A-module M est de type fini si et seulement s'il s'écrit comme quotient de A^n pour un certain $n > 0$. Il ne faut pas confondre cette notion avec celle de A-algèbre de type fini qui correspond à être un quotient de l'anneau de polynômes $A[X_1, \ldots, X_n]$.*
ii. Un quotient d'un module de type fini est de type fini.
iii. En général, un idéal de A qui n'est pas engendré par un nombre fini d'éléments n'est pas de type fini comme A-module bien que ce soit un sous-module de A (qui est engendré par 1). Nous verrons que si A est noetherien, un sous-module d'un module de type fini sur A est encore de type fini.

Un module qui n'est pas libre admet des éléments de torsion au sens suivant :

Définition 8.16. — *Soit M un module sur un anneau A intègre. Un élément $m \in M$ est dit* **de torsion**, *s'il existe $a \in A - \{0\}$ tel que $am = 0$. L'union de tous les éléments de torsion de M est le* **sous-module de torsion** *de M :*

$$M_{\text{tors}} = \cup_{a \neq 0} M[a] = \cup_{I \neq 0} M[I] \subset M,$$

où I décrit l'ensemble des idéaux non nuls de A. Le module M est dit **de torsion** *si $M = M_{\text{tors}}$. Il est dit* **sans torsion** *si $M_{\text{tors}} = 0$. Pour tout module M, M/M_{tors} est sans torsion.*

Exemples 8.17. — *i. Un module libre M sur un anneau intègre A est sans torsion : si $a \in A$ et $x \in M$, $ax = 0$ implique $a = 0$ ou $x = 0$.*
ii. L'anneau $\mathbb{Z}/n\mathbb{Z}$, $n \geq 2$ est un $\mathbb{Z}$-module de type fini qui n'est pas libre (car de torsion).
iii. Le $\mathbb{Z}$-module $\mathbb{Q}$ est sans torsion mais n'est pas libre car il est divisible : si $n > 0$, tout élément $x \in \mathbb{Q}$ s'écrit $x = ny$ pour $y \in \mathbb{Q}$, ce qui est impossible dans un $\mathbb{Z}$-module libre (prendre un élément dont l'une des composantes sur la base est 1 et $n \geq 2$). Nous verrons que sur un anneau principal, un module de type fini sans torsion est libre.

Aves des hypothèses supplémentaires sur l'anneau de base A, nous pouvons donner des informations plus fines sur la structure des A-modules. Par exemple, les idéaux d'un anneau noetherien sont de type fini (§9). Nous obtenons également un théorème de structure des modules de type fini sur un anneau principal (§10).

9. Anneaux et modules noetheriens

Dans tout ce paragraphe, A est un anneau commutatif mais pas forcément intègre. En revanche, nous supposons que A est noetherien (Définition 9.1) ce qui garantit que les A-modules de type fini sont de présentation finie (Proposition 9.7). Le théorème de la base de Hilbert (Théorème 9.8) montre en particulier que les anneaux de polynômes à un nombre fini de variables à coefficients dans un corps sont noetheriens.

Définition-Proposition 9.1. — *Un A-module M est dit* **noetherien** *s'il satisfait l'une des trois propriétés équivalentes suivantes :*
i. Tout sous-module N de M est engendré par un nombre fini d'éléments.
ii. (Condition de chaîne ascendante). Toute suite croissante (pour l'inclusion) $M_1 \subset M_2 \subset \cdots \subset M$ de sous-modules de M est stationnaire : il existe un indice j tel que $M_k = M_j$ pour tout $k \geq j$.
iii. Toute famille S non vide de sous-modules de M contient un élément maximal pour l'inclusion.

Démonstration. — i.$\Longrightarrow$ii. L'union $N = \cup_{i=1}^{\infty} M_i$ est un sous-module de M donc il est engendré par un ensemble fini d'éléments $n_1, \ldots, n_r \in M$. Il existe $j \geq 1$ tel que M_j contienne tous les $n_i, 1 \leq i \leq r$. Ainsi $N = M_j = M_k$, $k \geq j$.
ii.$\Longrightarrow$ iii. Comme S n'est pas vide, il existe $M_1 \in S$. Si S n'admet pas d'élément maximal, alors il existe $M_2 \in S$ tel que $M_1 \subsetneq M_2$. Nous construisons ainsi par induction une chaîne strictement croissante de sous-modules ce qui est en contradiction avec l'hypothèse ii.

iii.$\Longrightarrow$ i. Soit S l'ensemble des sous-modules de type fini de N sous-modules de M. Il est non vide car $0 \in S$. Donc il contient un élément maximal P. Si $P \neq N$, il existe $n \in P - N$. Le sous-module $P + An \subset N$ engendré par P et n est de type fini, donc appartient à S ce qui contredit la maximalité de P. Donc $P = N$ et N est de type fini. $\square$

Nous commençons par un lemme technique utile à la démonstration de la proposition 9.3 :

Lemme 9.2. — *Si $X \subset Y \subset M$, $N \subset M$ sont des sous-modules tels que $X \cap N = Y \cap N$ et $\pi(X + N) = \pi(Y + N)$ pour $\pi : M \longrightarrow M/N$, alors $X = Y$.*

Démonstration. — Soit $y \in Y$. Comme $\pi(X + N) = \pi(Y + N)$, il existe $x \in X$ et $n \in N$ tels que $y = x + n$. Alors $n = y - x \in N \cap Y = N \cap X$, donc $y = x + (y - x) \in X$. $\square$

Proposition 9.3. — *Si M est un A-module et N est un sous-module de M. Alors M est noetherien si et seulement si N et M/N sont noetheriens.*

Démonstration. — Soit $\pi : M \longrightarrow M/N$ la projection canonique.
Si M est noetherien alors N et M/N sont noetherien. En effet, si $X \subset M/N$, le sous-module $\pi^{-1}(X) \subset M$ est de type fini donc $X = \pi(\pi^{-1}(X))$ aussi.
Réciproquement si N et M/N sont noetheriens et $M_1 \subset M_2 \subset \cdots \subset M$ est une chaîne de sous-modules, alors les chaines de sous-modules

$$M_1 \cap N \subset M_2 \cap N \subset \cdots \subset N, \quad \pi(M_1 + N) \subset \pi(M_2 + N) \subset \cdots \subset M/N$$

se stabilisent pour $k \geq j$. Ainsi d'après le lemme 9.2, $M_k = M_j$ pour tout $k \geq j$ et M est noetherien. $\square$

Définition 9.4. — *Un anneau A est* **noetherien** *s'il est noetherien en tant que A-module, i.e si l'une des conditions équivalentes suivantes est satisfaites :*
i. Tout idéal I de A est engendré par un nombre fini d'éléments.
ii. (Condition de chaîne ascendante). Toute suite croissante (pour l'inclusion) $I_1 \subset I_2 \subset \cdots \subset A$ d'idéaux de A est stationnaire : il existe un indice j tel que $I_k = I_j$ pour tout $k \geq j$.
iii. Toute famille S non vide d'idéaux de M contient un élément maximal pour l'inclusion.

Exemples 9.5. — *i. Un anneau principal est noetherien.*
ii. L'anneau factoriel des polynômes $\mathbb{C}[X_1, X_2, \ldots] = \cup_{n=1}^{\infty} \mathbb{C}[X_1, \ldots, X_n]$ à une infinité de variables n'est pas noetherien, car la suite d'idéaux

$$(X_1) \subset (X_1, X_2) \subset \cdots$$

est croissante non stationnaire.

Proposition 9.6. — *Soit $f : A \longrightarrow B$ un morphisme d'anneaux surjectif. Si A est noetherien alors B est noethérien.*

Démonstration. — Pour toute chaîne d'idéaux de B, $J_1 \subset J_2 \subset \cdots \subset B$, la chaîne $f^{-1}(J_1) \subset f^{-1}(J_2) \subset \cdots \subset A$ est stationnaire, $f^{-1}(J_j) = f^{-1}(J_k)$ pour $j \geq k$. Par surjectivité de f, $J_k = f(f^{-1}(J_k)) = f(f^{-1}(J_j)) = J_j$, $j \geq k$. Donc B est noetherien. □

Proposition 9.7. — *Soit A un anneau noetherien. Un A-module M est noetherien si et seulement s'il est de type fini. En particulier, tout A-module de M de type fini est de présentation finie.*

Démonstration. — L'implication "$\Longrightarrow$" est immédiate. Réciproquement, l'isomorphisme de A-modules $A^n/A \xrightarrow{\simeq} A^{n-1}$ implique par induction que tout A^n $(n \geq 1)$ est un A-module noetherien. Un A-module de type fini est de la forme A^n/N, donc est noetherien. □

Théorème 9.8. — *(Théorème de la base d'Hilbert). Si A est noetherien et $n \geq 1$, alors $A[X]$ est noethérien.*

Démonstration. — Il s'agit de montrer que tout idéal $I \subset A[X]$ est de type fini. Pour tout $i \geq 0$, soit

$$I_i = \{a \in A | \exists a X^i + a_{i-1}X^{i-1} + \cdots + a_0 \in I\} \subset A.$$

Ils forment une chaîne croissante d'idéaux de A noethérien, donc il existe $k \geq 0$ tel que $I_j = I_k$, $j \geq k$. De plus $I_0, \ldots, I_k$ sont de type fini donc il existe $f_{ij} \in A[X]$, $(0 \leq i \leq k, 1 \leq j \leq m, \deg(f_{ij}) \leq i)$ tels que, pour tout $i = 0, ..., k$, l'idéal I_i est engendré par le coefficient en X^i des polynômes $f_{i1}, ..., f_{im}$. Notons $J \subset I$ l'idéal engendré par l'ensemble (fini) de polynômes f_{ij} $(0 \leq i \leq k, 1 \leq j \leq m)$. Il suffit alors de montrer que tout $f \in I - \{0\}$ est contenu dans J ($\Longrightarrow I = J$ est de type fini). Si $d = \deg(f)$, alors il existe $c_1, \ldots, c_m \in A$ tel que le polynôme $g_d = (c_1 f_{l1} + \cdots + c_m f_{lm}) X^{\max(d-k,0)} \in J$ pour $\ell = \min(k, d)$ vérifie $\deg(f - g_d) < d$. Par induction décroissante sur d, nous obtenons en au plus $d+1$ étapes $g \in J$ tel que $f - g = 0$, donc $f \in J$. □

Exemples 9.9. — *i. Si A est noetherien alors $A[X_1, \ldots, X_n]/I$ est noetherien pour tout idéal I de $A[X_1, \ldots, X_n]$.*
ii. Si A est noetherien, alors $A[[X]]$ et $A[X, X^{-1}]$ sont noetheriens.
iii. Dans un anneau noetherien, le nombre minimal de générateurs d'un idéal peut être arbitrairement grand : par exemple, soit K est un corps, considérons l'idéal $I = (X, Y)^n$ de l'anneau noetherien $K[X, Y]$. L'idéal I est engendré par les monômes $X^k Y^{n-k}$, $0 \leq k \leq n$ et tout système de générateurs de I contient une base des polynômes homogènes de degré n, donc a pour cardinal minimum $n + 1$.

Lemme 9.10. — *Soit A un anneau intègre noethérien. Alors tout élément x non nul de A s'écrit : $x = up_1 \cdots p_r$ avec $u \in A^*$ et les p_i irréductibles.*

Démonstration. — Soit S l'ensemble des idéaux de A de la forme xA avec x non inversible ne s'écrivant pas comme produit d'irréductibles. Si S n'est pas vide, il admet un élément maximal $(a) = aA$. En particulier a n'est pas irréductible. Comme il n'est pas inversible, il s'écrit $a = bc$ avec b, c dans A non associés à a. Mais les idéaux (b) et (c) contiennent strictement (a), donc par maximalité de (a), b et c se décomposent en produit d'irréductibles, ce qui contredit le fait que a ne s'écrit pas comme produit d'irréductibles. □

Rappelons qu'un anneau factoriel est un anneau intègre dans lequel tout élément non nul s'écrit de manière unique en produit d'éléments irréductibles. Cependant les notions d'anneaux noethérien et factoriel ne sont pas liées comme l'illustrent les exemples suivants.

Exemples 9.11. — *i. Si K est un corps $K[X_n, n \in \mathbb{N}]$ est factoriel non noethérien.*
ii. L'anneau $\mathbb{Z}[X]/(X^2+5)$ est noethérien non factoriel.
iii. Soit U un ouvert connexe (donc non vide) de $\mathbb{C}$. L'ensemble $\mathcal{H}(U)$ des fonctions holomorphes sur U est un anneau de Bézout intègre ni factoriel ni noethérien.
iv. L'anneau $\{f \in \mathbb{Q}[X] | f(0) \in \mathbb{Z}\}$ est aussi de Bézout, intègre non factoriel, non noetherien.

10. Modules sur un anneau principal

Soit A un anneau. En écrivant les éléments de A^n comme des matrices colonnes à coefficients dans A, un morphisme de modules $f : A^m \longrightarrow A^n$ s'identifie à une matrice $M \in \mathcal{M}_{n,m}(A) : f(x) = Mx$, $x \in A^m$. Le morphisme f est inversible si et seulement si $m = n$ et la matrice M est inversible, i.e $\det(M) \in A^*$.

Dans ce paragraphe, A est un anneau principal. Le résultat suivant, établi pour $A = \mathbb{Z}$ (euclidien) dans le cours d'Algèbre 1, permet de décrire la structure des modules de type fini sur A principal.

Théorème 10.1. — *Soit $M \in M_{n,m}(A)$ avec A un anneau principal.*
i. Il existe $P \in \mathrm{GL}_n(A)$ et $Q \in \mathrm{GL}_m(A)$ tel que

$$PMQ = \begin{pmatrix} d_1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ & 0 & 0 & d_r & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

où $0 \leq r \leq \min(n,m)$ *et* $d_1, \ldots, d_r$ *sont des éléments non nuls de* A *tels que* $d_1 | \cdots | d_r$.
ii. L'entier r *et les idéaux* $(d_1), \ldots, (d_r)$ *ne dépendent que de* M.

Démonstration. — Nous pouvons supposons $M \neq 0$. Par induction, il suffit de mettre M sous la forme

$$\begin{pmatrix} d_1 & 0 \\ 0 & d_1 N \end{pmatrix}, \quad N \in M_{n-1,m-1}(A)$$

en appliquant une successsion d'opérations élémentaires sur les lignes et les colonnes.
- Etape 1. Remarquons que si une colonne (resp. une ligne) de M contient deux éléments non nuls $a, b \in A - \{0\}$, alors on peut remplacer, par opérations élémentaires, le couple (a,b) par $(d,0)$ avec $d = \mathrm{PGCD}(a,b)$ sans changer les autres éléments de la colonne (resp. la ligne). En effet, il existe $u, v \in A$ avec $au + bv = d$. Alors

$$\begin{pmatrix} u & v \\ -b/d & a/d \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$$

permet de se ramener (après permutation et réitération) à une première colonne de la forme

$$C_1 = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad d \neq 0.$$

- Etape 2. Si d divise tous les termes de M, nous obtenons la forme attendue en soustrayant chaque colonne par un multiple de C_1. Sinon quitte à sommer la première ligne avec une autre, nous pouvons supposer qu'il existe un élément de la première ligne qui n'est pas divisible par d. Alors en appliquant l'étape 1 à la première ligne puis à la nouvelle première colonne, nous remplaçons la première colonne par

$$C_1' = \begin{pmatrix} d' \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

avec d' diviseur propre de d. Ainsi en un nombre fini d'étape, nous obtenons l'écriture attendue.
ii. Nous établissons que $d_1 \cdots d_j$ est le PGCD des mineurs de taille j de la matrice M pour tout $1 \leq j \leq r$ et $r = \mathrm{rg} M$ (voir cours d'Algèbre I). □

Corollaire 10.2. — *(Théorème de la base adaptée). Soit* A *un anneau principal,* M *un* A*-module libre de rang* n *et* N *un sous-module de* M. *Alors*
i. N *est libre de rang* $m \leq n$,
ii. Il existe des éléments $d_1, \ldots d_r$ *de* $A - \{0\}$, $d_1 | \cdots | d_r$ *et une base* $e_1, \ldots, e_n$ *de*

M tels que $d_1e_1, \ldots, d_re_r$ est une base de N.
iii. Le module quotient

$$M/N \simeq A^{n-r} \oplus A/(d_1) \oplus \cdots \oplus A/(d_r).$$

Démonstration. — Le choix d'une base de M sur A et d'un système de m générateurs de N, conduit à une matrice $B \in M_{m,n}(A)$ que nous mettons sous forme réduite via le théorème 10.1 et qui permet d'établir le corollaire. □

Corollaire 10.3. — *Soit A un anneau principal et M un module de type fini sur A. Alors, il existe $a, r \in \mathbb{N}$, $d_1, \ldots, d_r \in A - \{0\} \cup A^*$, $d_1| \cdots |d_r$ tels que*

$$M \xrightarrow{\simeq} A^a \oplus A/(d_1) \oplus \cdots \oplus A/(d_r).$$

De plus les entiers a, r et les idéaux $(d_1), \ldots, (d_r)$ ne dépendent que de la classe d'isomorphisme de M.

Démonstration. — D'après le théorème de la base adaptée, nous avons une écriture sous la forme

$$M \simeq A^a \oplus A/(d_1) \oplus \cdots \oplus A/(d_r).$$

Ainsi $M/M_{\text{tors}} \simeq A^a$ donc a ne dépend que de la classe d'isomorphisme de M. Pour l'unicité des idéaux $(d_1), \ldots, (d_r)$, nous devons considérer pour tout élément irréductible x de A, la suite des exposants de x dans les d_i :

$$0 \leq v_x(d_1) \leq \ldots \leq v_x(d_r).$$

Montrons qu'ils sont déterminés par M_{tors}. Pour $j \geq 0$, soit $r_j(x) = |\{i | v_x(d_i) \geq j\}|$. Ainsi la suite de sous-modules

$$M[x] \supset xM[x^2] \supset x^2M[x^3] \supset \cdots$$

est isomorphe à

$$(A/(x))^{r_1(x)} \supset (A/(x))^{r_2(x)} \supset (A/(x))^{r_3(x)} \supset \cdots$$

Par conséquent la suite d'exposants $(v_x(d_i))_{1 \leq i \leq r}$ ne dépend que de M_{tors}.
Enfin comme d_1 n'est pas inversible, il est divisible par un élément irréductible x_0. Donc $r = r_1(x_0)$ est déterminé. □

Comme tout groupe abélien est un $\mathbb{Z}$-module, nous retrouvons le théorème de structure des groupes abéliens :

Corollaire 10.4. — *Soit M un groupe abélien de type fini. Alors M est isomorphe à*

$$\mathbb{Z}^r \oplus \oplus_{i=1}^r \mathbb{Z}/d_i\mathbb{Z}$$

où $r \in \mathbb{N}$, $d_i \in \mathbb{N} - \{0, 1\}$, $d_1| \cdots |d_r$. De plus $r, d_1, \ldots, d_i$ sont déterminés par M.

Exemple 10.5. — *Soit $p \in \mathbb{N}$ est premier impair et $\alpha \in \mathbb{N}^*$. Le groupe des éléments inversibles $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{\alpha-1}\mathbb{Z}$ est cyclique. En revanche pour $p = 2$ et $\alpha \geq 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p^{\alpha-2}\mathbb{Z}$ n'est pas cyclique. La classe de $\bar{5} \in (\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est d'ordre $p^{\alpha-2}$.*

Une autre application importante de la théorie des modules de type fini sur un anneau principal est la réduction des endomorphismes d'un K-espace vectoriel de dimension finie (K corps) qui permet de déterminer les classes de similitude.

Définition 10.6. — *Soit $P = X^d + \sum_{i=0}^{d-1} a_i X^i \in K[X]$ un polynôme unitaire. La* **matrice compagnon** *de P est la matrice*

$$C(P) = \begin{pmatrix} 0 & \cdots & \cdots & \cdots & -a_0 \\ 1 & \cdots & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 1 & -a_{d-1} \end{pmatrix}.$$

Théorème 10.7. — *i. Pour tout endomorphisme u d'un K-espace vectoriel de dimension finie E, il existe une base de E dans laquelle la matrice de u est diagonale par blocs, de la forme*

$$\begin{pmatrix} C(P_1) & & & \\ & C(P_2) & & \\ & & \cdots & \\ & & & C(P_r) \end{pmatrix}$$

où les P_i sont des polynômes unitaires de $K[X]$ de degré au moins 1 vérifiant $P_1|P_2|\cdots|P_r$.
ii. Les P_i sont déterminés par u et sont dits invariants de similitude de u. Deux matrices de $M_n(K)$ sont semblables si et seulement si elles sont les mêmes invariants de similitude.

Démonstration. — Un $K[X]$-module est la donnée d'un K-espace vectoriel M muni d'un endomorphisme K-linéaire $u : M \longrightarrow M$ correspondant à l'action de X, via

$$K[X] \times M \longrightarrow M, (P, v) \mapsto P(u)(v).$$

Ce module M est de torsion car si π est un polynôme annulateur de u alors $\pi \cdot v = \pi(u)(v) = 0$ pour tout $v \in M$. Nous avons ainsi

$$M \xrightarrow{\simeq} K[X]/(P_1) \oplus \cdots \oplus K[X]/(P_r)$$

avec $P_1|\cdots|P_r$. Nous avons

$$\sum_{i=1}^{r} \deg(P_i) = \sum_{i=1}^{r} \dim_K K[X]/(P_i) = \dim_K M$$

Choisissons une K-base de M et considérons B la matrice de u dans cette base. L'unicité du théorème de structure des $K[X]$-modules de type fini implique que deux matrices B, B' ont la même suite de poynômes $P_1|\cdots|P_r$ si et seulement si elles sont semblables. $\square$

Exemples 10.8. — *i. Soit $B \in M_n(K)$ et $C = X\,\mathrm{Id} - B \in M_n(K[X])$ la matrice caractéristique de B. Alors la suite des facteurs invariants de C est $(1, \ldots, 1, P_1, \ldots, P_r)$ où $P_1, \ldots, P_r$ sont les invariants de similitude de B. En particulier, ces invariants sont donnés par les* PGCD *m_i des mineurs d'ordre i de C dans $K[X]$: $P_1 \ldots P_h = m_{h+n-r}$.*
En particulier le polynôme minimal de B est P_r et le polynôme caractéristique de u est $P_1 \cdots P_r$.
ii. Si $N \xrightarrow{\simeq} K[T]/(Q)$ avec $Q = T^d + a_{d-1}T^{d-1} + \cdots + a_0$. Alors $1, \ldots, T^{d-1}$ mod Q est une base de N sur K et la matrice de la multiplication par T dans cette base est $C(Q)$. Le polynôme minimal et le polynôme caractéristique de $C(Q)$ coïncident avec Q.
En décomposant $Q = Q_1^{n_1} \cdots Q_s^{n_s}$ en facteurs irréductibles distincts, nous obtenons

$$N \xrightarrow{\simeq} K[T]/(Q_1^{n_1}) \oplus \cdots \oplus K[T]/(Q_s^{n_s}).$$

Ainsi la matrice de la multiplication par T dans l'union des bases $1, T, \ldots, T^{n_i \deg Q_i}$ mod $Q_i^{n_i}$ est

$$\begin{pmatrix} C(Q_1^{n_1}) & 0 & \cdots & 0 \\ 0 & C(Q_2^{n_2}) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & C(Q_s^{n_s}) \end{pmatrix}.$$

iii. Si K est algébriquement clos, les poynômes irréductibles unitaires sont de la forme $T - \lambda$ pour $\lambda \in K$. Dans la base $1, T - \lambda, \ldots, (T - \lambda)^{n-1}$ la multiplication par T a pour matrice

$$\begin{pmatrix} \lambda & 0 & 0 & \cdots & 0 & 0 \\ 1 & \lambda & 0 & \cdots & 0 & 0 \\ 0 & 1 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 0 \\ 0 & 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}.$$

Nous retrouvons l'existence et l'unicité de la forme de Jordan pour une matrice à coefficients dans un corps algébriquement clos.

11. Produit tensoriel

11.1. Définition du produit tensoriel. — Nous généralisons la notion de produit tensoriel d'espaces vectoriels au produit tensoriel de modules sur un anneau A. C'est un procédé qui permet de passer des modules sur un anneau A

aux modules sur une A-algèbre B. Le produit tensoriel de A-modules est une solution universelle à un problème de factorisation (voir Proposition 11.2)

Définition 11.1. — *Soit A un anneau, $k > 0$ entier et $M_1, \ldots, M_k, P$ une suite de A-modules. Une application*

$$\beta : M_1 \times \cdots \times M_k \longrightarrow P$$

*est dite A-***mutilinéaire** *si pour tout $(m_1, \ldots, m_k) \in M_1 \times \cdots \times M_k$ et tout $i \in \{1, \ldots, k\}$ l'application*

$$M_i \longrightarrow P, x \mapsto \beta(m_1, \ldots, m_{i-1}, x, m_{i+1}, \ldots, m_k)$$

est A-linéaire. Nous notons $\mathcal{L}_A(M_1 \times \cdots \times M_k, P)$ l'ensemble des applications A-multilinéaires. Pour $k = 2$ les applications A-multilinéaires $\mathcal{L}_A(M_1 \times M_2, P)$ sont dites **bilinéaires**.

Nous avons défini un foncteur

$$\mathcal{L}_A(M_1 \times \cdots \times M_k, -) : A - \mathrm{Mod} \longrightarrow \mathrm{Ens}.$$

En effet si $f : P \longrightarrow P'$ est un morphisme de A-modules, alors la composition $f \circ \beta$ est A-linéaire et nous obtenons une application

$$\mathcal{L}_A(M_1 \times \cdots \times M_k, f) : \mathcal{L}_A(M_1 \times \cdots \times M_k, P) \longrightarrow \mathcal{L}_A(M_1 \times \cdots \times M_k, P') \;\; \beta \mapsto f \circ \beta.$$

Proposition 11.2. — *Soit A un anneau, M, N deux A-modules. Le foncteur $\mathcal{L}_A(M \times N, -)$ est représentable, i.e. il existe un A-module $M \otimes_A N$ appelé le produit tensoriel de M et N et une application A-bilinéaire*

$$\omega : M \times N \longrightarrow M \otimes_A N$$

tels que pour tout A-module P et toute application A-bilinéaire $\beta : M \times N \longrightarrow P$, il existe une unique application A-linéaire $\overline{\beta} : M \otimes_A N \longrightarrow P$ avec $\beta = \overline{\beta} \circ \omega$.
Si $M_1, \ldots, M_k$ sont des A-modules, le foncteur $\mathcal{L}_A(M_1 \times \cdots \times M_k, -)$ est représentable par le produit tensoriel $M_1 \otimes_A \cdots \otimes_A M_k$.

Démonstration. — Soit $(e_{m,n})_{m \in M, n \in N}$ la base canonique de $A^{(M \times N)}$ et S le A-module engendré par

$$e_{m+am',n} - e_{m,n} - ae_{m',n}, \; m, m' \in M, n \in N, a \in A,$$

$$e_{m,n+an'} - e_{m,n} - ae_{m,n'}, \; m \in M, n, n' \in N, a \in A.$$

Soit $M \otimes_A N = A^{(M \times N)}/S$ et notons $m \otimes n$ la classe de $e_{m,n}$ dans $M \otimes_A N$ pour tout $m \in M$, $n \in N$. Par construction les $m \otimes n$ engendrent le A-module $M \otimes_A N$. Alors

$$(M \otimes_A N, \omega : M \times N \longrightarrow M \otimes_A N, (m, n) \mapsto m \otimes n)$$

représente $\mathcal{L}_A(M \times N, -)$. En effet ω est A-bilinéaire et pour $\beta : M \times N \longrightarrow P$ bilinéaire, définissons $\tilde{\beta} : A^{(M \times N)} \longrightarrow P$ par $\tilde{\beta}(e_{m,n}) = \beta(m, n)$, $(m, n) \in M \times N$. Ainsi $\tilde{\beta}(S) = 0$ donc $\tilde{\beta}$ se factorise de manière unique en une application A-linéaire $\overline{\beta} : M \otimes_A N \longrightarrow P$ avec $\beta = \overline{\beta} \circ w$ et comme l'image de ω engendre le

A-module $M \otimes N$, $\overline{\beta}$ est unique.
Par induction, nous définissons $M \otimes_A (M' \otimes_A M'')$ et $(M \otimes_A M)' \otimes_A M''$ qui sont isomorphes par universalité, ce qui permet de les noter $M \otimes_A M' \otimes_A M''$. Nous constatons alors que $M_1 \otimes_A \cdots \otimes_A M_k$ avec l'application canonique construite par induction

$$\omega_k : M_1 \times \cdots \times M_k \longrightarrow M_1 \otimes \cdots \otimes M_k, (m_1, \ldots, m_k) \mapsto m_1 \otimes \cdots \otimes m_k$$

représente $\mathcal{L}_A(M_1 \times \cdots \times M_k, -)$. □

Exemples 11.3. — *i. Si M est un A-module,*

$$\{0\} \times_A M = M \otimes_A \{0\} = \{0\}.$$

Nous avons $\varphi : A[X] \otimes_A A[Y] \simeq A[X, Y]$. En effet la multiplication définit une application A-bilinéaires

$$A[X] \times A[Y] \longrightarrow A[X, Y], (P, Q) \mapsto P(X)Q(Y).$$

Les éléments $X^i \otimes Y^j$ forment une base de $A[X] \otimes_A A[Y]$ comme A-module et leurs images $X^i Y^j$ forment une base de $A[X, Y]$. De plus, φ est un ismormorphisme d'algèbres.
ii. Soient M, N deux A-modules. L'application

$$M \times N \longrightarrow N \otimes_A M, (m, n) \mapsto n \otimes m$$

est bilinéaire donc induit une application A-linéaire $u : M \otimes_A N \longrightarrow N \otimes_A M$, $m \otimes n \mapsto n \otimes m$. De même nous avons une application A-linéaire $v : N \otimes_A M \longrightarrow M \otimes_A N$, $n \otimes m \mapsto m \otimes n$. Nous avons $u \circ v = \mathrm{Id}_{N \otimes_A M}$ et $v \circ u = \mathrm{Id}_{M \otimes_A N}$, donc u et v sont des isomorphismes réciproques l'un de l'autre.
iii. Soit N un A-module et M un A-module libre de rang 1. Soit e une base de M. Alors l'application A-linéaire

$$\varphi : N \longrightarrow M \otimes_A N, n \mapsto e \otimes n$$

est un isomorphisme. En effet l'application bilinéaire $u \in \mathcal{L}_A(M \times N, N)$, $u(ae, n) \mapsto an$ induit une application A-linéaire $\psi : M \otimes_A N \longrightarrow N$, $ae \otimes n \mapsto an$, inverse de φ.
En particulier $N \simeq A \otimes_A N$. De même si $N = Af$ est aussi libre de rang 1, alors $M \otimes_A N = Ae \otimes_A Af$ est libre de rang 1 de base $e \otimes f$.
iv. Le produit tensoriel de deux modules non nuls peut être nul : $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$. En effet soit $(a, b) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Alors

$$a \otimes b = (3 - 2)a \otimes b = 3a \otimes b - 2a \otimes b = a \otimes 3b - 2a \otimes b = 0.$$

De même d'après Bézout si n, m sont premiers entres eux $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = 0$.
v. Si $f : M \longrightarrow M'$ est surjective, il en est de même de $f \otimes \mathrm{Id}_N : M \otimes N \longrightarrow M' \otimes N$. En effet si $m' = f(m)$, alors $m' \otimes n = (f \otimes \mathrm{Id}_N)(m \otimes n)$ pour tout $n \in N$.
Si $f : M \longrightarrow M'$ est injective, $f \otimes \mathrm{Id}_N$ n'est pas forcément injective. Par exemple si $A = M = M' = \mathbb{Z}$ et $f : x \mapsto 2x$ et $N = \mathbb{Z}/2\mathbb{Z}$. Alors

$$(f \otimes \mathrm{Id}_N)(x \otimes \bar{1}) = 2x \otimes \bar{1} = x \otimes 2\bar{1} = 0.$$

Mais d'après v. $M' \otimes_A N = N \neq 0$, *donc* $f \otimes \mathrm{Id}_N$ *n'est pas injective.*

Proposition 11.4. — *(Adjonction) Soit* L, M, N *trois* A*-modules. Le foncteur* $L \mapsto \mathrm{Hom}_A(M, L)$ *est adjoint à droite à* $N \mapsto M \otimes_A N$.

Démonstration. — Soit $f : N \longrightarrow \mathrm{Hom}_A(M, L)$ une application A-linéaire. L'application

$$M \times N \longrightarrow L, (m, n) \mapsto f(n)(m)$$

est bilinéaire et induit une application linéaire $M \otimes_A N \longrightarrow L$ qui dépend linéairement de f. Nous avons ainsi défini une application A-linéaire

$$\varphi : \mathrm{Hom}_A(N, \mathrm{Hom}(M, L)) \longrightarrow \mathrm{Hom}_A(M \otimes_A N, L).$$

L'application A linéaire

$$\psi : \mathrm{Hom}_A(M \otimes_A N, L) \longrightarrow \mathrm{Hom}_A(N, \mathrm{Hom}_A(M, L)), \psi(g) : n \mapsto (m \mapsto g(m \otimes n))$$

est la bijection réciproque de φ et ces constructions sont fonctorielles en L, M, N. A M fixé, nous disposons d'un isomorphisme

$$\mathrm{Hom}_A(N, \mathrm{Hom}_A(M, L)) \simeq \mathrm{Hom}_A(M \otimes_A N, L)$$

qui est fonctoriel en N et L. Ceci établit une adjonction pour le couple de foncteurs $(M \otimes_A -, \mathrm{Hom}_A(M, -))$. □

11.2. Restriction et extension des scalaires. —

Définition 11.5. — *Soit* $f : A \longrightarrow B$ *un morphisme d'anneaux et* N *un* B*-module. Nous pouvons munir* N *d'une structure de* A*-module* N_f *via*

$$a \cdot n = f(a)n, a \in A, n \in N.$$

Le A*-module* N_f *est dit obtenu par* **restriction des scalaires** *du* B*-module* N *suivant le morphisme* f.

Exemples 11.6. — *i. Soit* M *un* A*-module,* A' *un sous-anneau de* A *et* $\iota : A' \longrightarrow A$ *l'injection canonique. Ainsi la restriction à* $A' \times M$ *de la loi externe* $A \times M$ *fait de* M *un* A'*-module (restriction des scalaires).*
ii. L'injection de $\mathbb{Z} \longrightarrow \mathbb{C}$ *conduit à considérer le* $\mathbb{C}$*-espace vectoriel* $M_n(\mathbb{C})$ *comme un* $\mathbb{Z}$*-module.*

Définition 11.7. — *Soit* $f : A \longrightarrow B$ *un morphisme d'anneaux et* M *un* A*-module. Alors* $B \otimes_A M$ *est dit* B*-module obtenu par* **extension des scalaires** *du* A*-module* M *suivant le morphisme* f.

Exemples 11.8. — *i. Soit* V *un* $\mathbb{R}$*-espace vectoriel. Le complexifié* $V_{\mathbb{C}}$ *de* V *est l'extension des scalaires du* $\mathbb{R}$*-module* V *par* $\mathbb{C}$ *suivant le morphisme* $\mathbb{R} \longrightarrow \mathbb{C}, a \mapsto a$. *Ainsi* $V_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} V = \mathbb{C}^n = V \oplus iV$. *Or* $\mathbb{C} = \mathbb{R}[i]$ *comme* $\mathbb{R}$*-algèbre. La structure de* $\mathbb{C}$*-module sur* $V \oplus iV$ *est donnée par :*

$$(a + ib) \cdot (v + iv') = (av - bv') + i(bv + av').$$

ii. Si $M \simeq A^n$ est un A-module libre de type fini et $f : A \longrightarrow B$ un morphisme d'anneaux. Alors $B \otimes_A M \simeq B^n$.
iii. Nous avons défini deux foncteurs adjoints

$$(-)_f : B - \mathrm{Mod} \longrightarrow A - \mathrm{Mod}, N \mapsto N_f,$$
$$B \otimes_A - : A - \mathrm{Mod} \longrightarrow B - \mathrm{Mod}, M \mapsto B \otimes_A M.$$

Corollaire 11.9. — *Soit M un A-module, B une A-algèbre et C une B-algèbre. Alors les C-modules suivants sont isomorphes :*

$$C \otimes_B (B \otimes_A M) \simeq C \otimes_A M.$$

Démonstration. — Soit $c \in C$. L'application A-bilinéaire

$$B \times M \longrightarrow C \otimes_A M, (b, m) \mapsto cb \otimes m$$

induit une application A-linéaire $m_c : B \otimes_A M \longrightarrow C \otimes_A M$.
L'application B-bilinéaire

$$C \times (B \otimes_A M) \longrightarrow C \otimes_A M, (c, u) \mapsto m_c(u)$$

induit une application B-linéaire $\varphi : C \otimes_B (B \otimes_A) \longrightarrow C \otimes_A M$. L'application A-bilinéaire

$$C \times M \longrightarrow C \otimes_B (B \otimes_A M), (c, m) \mapsto c \otimes (1 \otimes m)$$

induit une application A-linéaire $\psi : C \otimes_A M \longrightarrow C \otimes_B (B \otimes_A M)$. Enfin les applications φ et ψ sont des bijections C-linéaires réciproques l'une de l'autre. □

11.3. Produit tensoriel, localisations et quotients. — Soit M un A-module. Nous décrivons l'extension des scalaires de M aux quotients et aux localisés de A.

Proposition 11.10. — *Soit I un idéal de A et M un A-module. Alors*

$$(A/I) \otimes_A M \simeq M/IM.$$

Démonstration. — La structure de A-module du quotient M/IM est induite par la structure de A/I-module (car la multiplication externe par a ne dépend que de la classe de a modulo I.).
La surjection $M \longrightarrow M/IM$ est A-linéaire donc induit un morphisme de A/I-modules

$$\varphi : (A/I) \otimes_A M \longrightarrow M/IM.$$

Par ailleurs l'application A-linéaire

$$M \longrightarrow (A/I) \otimes_A M, m \mapsto 1 \otimes m$$

s'annule sur IM car pour tout $a_i \in I, m_i \in M$, $1 \otimes \sum a_i m_i = \sum \overline{a_i} \otimes m_i = 0$. Elle induit donc une application A-linéaire $\psi : M/IM \longrightarrow (A/I) \otimes_A M$. Toute application A-linéaire entre A/I-modules est A/I-linéaire. Enfin φ et ψ sont des isomorphismes inverses l'un de l'autre. □

Proposition 11.11. — *Soit S une partie multiplicative de A et M un A-module. Le quotient $S^{-1}M$ de $M \times S$ par la relation d'équivalence $(m,s) \simeq (n,t) \iff \exists r \in S, r(tm - sb) = 0$ est canoniquement muni d'une structure de $S^{-1}A$-modules. De plus nous avons un isomorphisme de $S^{-1}A$-modules*

$$\psi : S^{-1}M \longrightarrow S^{-1}A \otimes_A M, m/s \mapsto 1/s \otimes m.$$

Démonstration. — Les formules

$$((m,s),(n,t)) \mapsto (tm + sn, st), ((aa,s),(m,t)) \mapsto (am, st)$$

passent au quotient et définissent une loi interne $+$ sur $S^{-1}M$ et une loi externe $\times : S^{-1}A \times S^{-1}M \longrightarrow S^{-1}M$ qui font de $S^{-1}M$ un $S^{-1}A$-module. Nous notons m/s la classe de $(m,s) \in M \times S$ dans $S^{-1}M$.
L'application $M \longrightarrow S^{-1}M$, $m \mapsto m/1$ est A-linéaire donc induit une application $S^{-1}A$-linéaire $\varphi : S^{-1}A \otimes_A M \longrightarrow S^{-1}M$ inverse de ψ. □

Nous avons ainsi défini un foncteur $A - \mathrm{Mod} \longrightarrow S^{-1}A - \mathrm{Mod}, M \mapsto S^{-1}M$. En effet si $f \in \mathrm{Hom}_A(M,N)$ alors $(m,s) \mapsto f(m)/s$ passe au quotient par $\simeq$ et induit $\tilde{f} \in \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$ avec $\tilde{f}(m/s) = f(m)/s$.

Exemple 11.12. — *Si $f \in \mathrm{Hom}_A(M,N)$ est une application injective entre deux A-modules et S est une partie multiplicative de A, alors l'application $S^{-1}M \longrightarrow S^{-1}N$ induite par f est injective.*
En effet supposons que $f(m)/s = 0$. Alors il existe $r \in S$ tel que $rf(m) = 0 = f(rm)$. Comme f est injective, $rm = 0$ et $m/s = 0$.

Lemme 11.13. — *Soit M un A-module. Pour $\mathfrak{p}$ idéal premier de A, nous notons $M_{\mathfrak{p}} = (A - \mathfrak{p})^{-1}M$ le localisé de A en l'idéal $\mathfrak{p}$. Alors*

$$M = 0 \iff \forall \mathfrak{p} \in \mathrm{Spec}\, A, M_{\mathfrak{p}} = 0 \iff \forall \mathfrak{m} \in \mathrm{Spm}\, A, M_{\mathfrak{m}} = 0.$$

Démonstration. — Il suffit de montrer que l'application $\varphi : M \longrightarrow \Pi_{\mathfrak{m}} M_{\mathfrak{m}}$ est injective. Soit $x \in \ker \varphi$ et $I = \{a \in A | ax = 0\}$. Alors I est un idéal et pour tout $\mathfrak{m}$, il existe $b \in A - \mathfrak{m}$ tel que $bx = 0$. Donc I n'est inclus dans aucun idéal maximal. Donc $I = A$. Par conséquent $1 \in I$ et $1.m = 0$ pour tout $m \in M$ donc $M = 0$. □

11.4. Lemme de Nakayama. —

Définition-Proposition 11.14. — *(Cayley-Hamilton) Soit A un anneau et $f \in \mathrm{Hom}_A(A^n, A^n)$. Le polynôme caractéristique de f est*

$$\chi_f(T) = \det(f - T\,\mathrm{Id}) \in A[T].$$

Il satisfait $\chi_f(f) = 0$.

Démonstration. — Si A est un corps, il s'agit du théorème de Cayley-Hamilton classique. Si A est intègre, en prolongeant f au K-espace vectoriel K^n pour $K = \mathrm{Frac}(A)$, nous avons encore $\chi_f(f) = 0$.
Supposons A anneau commutatif arbitraire, notons $(a_{ij})_{1\leq i,j\leq n}$ l'écriture matricielle de f dans la base canonique de A^n. Posons $R = \mathbb{Z}[Y_{ij}, 1 \leq i, j \leq n]$ et $(e_i)_{1\leq k\leq n}$ la base canonique de R^n. Nous définissons un morphisme d'anneaux

$$g : R \longrightarrow A, Y_{ij} \mapsto a_{ij}.$$

Par extension des scalaires, $A \otimes_R R^n$ est ainsi muni d'une structure de A-module et $A \otimes_R R^n \simeq A^n$. L'endomorphisme de R^n

$$h : R^n \longrightarrow R^n, \quad e_j \mapsto \sum_{i=1}^{n} Y_{ij} e_i, 1 \leq j \leq n.$$

Le diagramme suivant d'applications A-linéaires est alors commutatif :

$$\begin{array}{ccc} A \otimes_R R^n & \xrightarrow{\simeq} & A^n \\ \mathrm{Id} \otimes_R h \downarrow & & \downarrow f \\ A \otimes_R R^n & \xrightarrow{\simeq} & A^n \end{array}$$

Comme R est intègre $\chi_h(h) = 0$ donc $\chi_f(f) = A \otimes_R \chi_h(h) = 0$. □

Proposition 11.15. — *Soit A un anneau. Soit M un A-module de type fini, I un idéal de A et $f \in \mathrm{Hom}_A(M, M)$ tel que $f(M) \subset IM$. Alors il existe $k \in \mathbb{N}$, $a_1, \ldots, a_k \in I$ tels que*

$$f^k + a_1 f^{k-1} + \cdots + a_k \,\mathrm{Id} = 0.$$

Démonstration. — Nous montrons que nous pouvons nous ramener au cas M libre de type fini. La proposition de Cayley-Hamilton permet alors de conclure dans ce cas.
Notons $(m_i)_{1\leq i\leq k}$ un système de générateurs de M, $(e_i)_{1\leq i\leq k}$ la base canonique de A^k et $\pi : A^k \longrightarrow M$ la surjection A-linéaire $e_i \mapsto m_i$, $1 \leq i \leq k$. Comme $f(M) \subset IM$, $f(m_i) = \sum_{j=1}^{k} b_{ij} m_j$ avec $B = (b_{ij})_{1\leq i,j\leq k}$ matrice à coefficients dans I. Ainsi B détermine un endomorphisme ψ de A^k tel que $\pi \circ \psi = f \circ \pi$. Comme π est surjectif et $\chi_\psi(\psi) = 0$ (d'après la proposition de Cayley-Hamilton), nous obtenons le résultat annoncé. □

Exemple 11.16. — *Soit M un A-module de type fini. Si $f \in \mathrm{Hom}_A(M, M)$ est surjectif alors il est bijectif. En effet, M est muni d'une structure de $A[X]$-module via $X \cdot m = f(m)$. Comme f est surjectif, $M = IM$ pour $I = XA[X]$. D'après le théorème de Cayley-Hamilton appliqué à $g = \mathrm{Id}_M$, nous avons*

$$g^k + a_1 g^{k-1} + \cdots + a_{k-1} g + a_k \,\mathrm{Id}_M = 0 \in \mathrm{Hom}_A(M, M)$$

avec $a_i = Xb_i \in XA[X]$. Par conséquent pour tout $m \in M$

$$0 = (g^k + a_1 g^{k-1} + \cdots + a_{k-1} g + a_k \,\mathrm{Id}_M)(m)$$

$$0 = m + a_1(f)(m) + \cdots + a_{k-1}(f)(m) + a_k(f)(m) = m + f(b_1(f) + \cdots + b_k(f))(m).$$

Donc $-(b_1(f) + \cdots b_k(f)) \in \mathrm{Hom}_A(M, M)$ *est l'inverse de* f.

Corollaire 11.17. — *(Lemme de Nakayama) Soit* M *un* A*-module de type fini,* $\mathfrak{J}(A) = \cap_{\mathfrak{m} \in \mathrm{Spm}\, A} \mathfrak{m}$ *le radical de Jacobson de* A*,* I *un idéal de* A *tel que* $IM = M$*. Si* $I \subset \mathfrak{J}(A)$ *alors* $M = 0$*.*

Démonstration. — D'après la proposition 11.15 appliquée à $f = \mathrm{Id}_M$, il existe $a_1, \ldots, a_k \in I$ avec $f^k + \cdots + a_k \mathrm{Id}_M = 0$. Soit $(1 + a_1 + \cdots + a_k)M = 0$. Or $a_1 + \cdots + a_k \in I \subset \mathfrak{J}(A)$ donc $1 + a_1 + \cdots + a_k \in A^*$ (Théorème 2.32). D'où $M = 0$. □

Corollaire 11.18. — *Soit* A *un anneau et* $\mathfrak{J}(A)$ *son radical de Jacobson. Soit* M *un* A*-module,* $N \subset M$ *un sous-module et* I *un idéal de* A *tel que* $M = IM + N$*. Supposons que l'une des conditions suivantes soit satisfaite :*
i. $I \subset \mathfrak{J}(A)$ *et* M *est de type fini,*
ii. I *est nilpotent (*$\exists n \in \mathbb{N}$*,* $I^n = 0$*).*
Alors $M = N$*.*

Démonstration. — Supposons i. Alors $I(M/N) = (IM + N)/N = M/N$. Le lemme de Nakayama implique donc $M/N = 0$.
Supposons ii. Comme $I^k(M/N) = M/N$ pour tout $k \in \mathbb{N}$, nous obtenons encore $M/N = 0$. □

Exemple 11.19. — *Dans le lemme de Nakayama, l'hypothèse de finitude est nécessaire. En effet soit* K *un corps et* $K((X))$ *l'anneau des séries de Laurent vu comme module sur l'anneau local* $K[[X]]$ *des séries formelles. Alors* $XK((X)) = K((X))$ *mais* $K((X)) \neq 0$*.*

Concluons par un corollaire très utile dans les applications pratiques.

Corollaire 11.20. — *Soit* A *un anneau local d'idéal maximal* $\mathfrak{m}$*,* M *un* A*-module et* $(m_\lambda)_{\lambda \in \Lambda}$ *une famille d'éléments de* M *dont les classes* $(\overline{m_\lambda})_{\lambda \in \Lambda}$ *forment une base du* $A/\mathfrak{m}$*-espace vectoriel* $M/\mathfrak{m}M$*. Supposons* M *de type fini ou* $\mathfrak{m}$ *nilpotent. Alors* $(m_\lambda)_{\lambda \in \Lambda}$ *est un système de générateurs du* A*-module* M*.*

Démonstration. — Posons $N = \sum_{\lambda \in \Lambda} A m_\lambda$. Nous avons $M = N + \mathfrak{m}M$ et $\mathfrak{J}(A) = \mathfrak{m}$. Il suffit alors d'appliquer le corollaire 11.18. □

12. Cohomologie

Introduisons les bases de la cohomologie algébrique pour des complexes de A-modules où A est un anneau (commutatif). Outre ses applications importantes, le formalisme algébrique est source d'inspiration dans différents domaines des mathématiques tels la topologie algébrique, la géométrie algébrique, la théorie des groupes, la théorie des nombres...

12.1. Suites exactes. —

Définition 12.1. — *Soient $a, b \in \mathbb{Z}$. Une suite de morphismes de A-modules*

$$M^a \xrightarrow{f^a} \cdots \longrightarrow M^{i-1} \xrightarrow{f^{i-1}} M^i \xrightarrow{f^i} M^{i+1} \longrightarrow \cdots \longrightarrow M^b$$

est dite **exacte** *en M^i si $\operatorname{im} f^{i-1} = \ker f^i$ (ce qui implique que $f^i \circ f^{i-1} = 0$ et $\operatorname{Coker}(f^{i-1}) \xrightarrow{\simeq} \operatorname{im} f^i$). La suite est dite* **exacte** *si elle est exacte en M^i pour tout $a < i < b$. Un* **morphisme** *(resp. un isomorphisme) entre deux suites exactes $(M^i, f^i)_{a \leq i \leq b}$ et $(N^i, g^i)_{a \leq i \leq b}$ est donné par des morphismes (resp. isomorphismes) de A-modules $u^i : M^i \longrightarrow N^i$, $(a \leq i \leq b)$ tels que $g^i \circ u^i = u^{i+1} \circ f^i$ pour tout $i = a, \ldots, b-1$.*

Exemples 12.2. — *i. Une suite de A-modules*

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{p} P \longrightarrow 0$$

est exacte si et seulement si i est injectif, $\ker p = \operatorname{im} \iota$ et p est surjectif.
Alors i induit un isomorphisme de N sur le sous-A-module $\iota(N)$ de M et p induit un isomorphisme $M/\iota(N) \simeq P$.
ii. Pour tout morphisme de A-modules $f : M \longrightarrow N$, la suite

$$0 \longrightarrow \ker f \longrightarrow M \longrightarrow N \longrightarrow \operatorname{Coker} f \longrightarrow 0$$

est exacte.

Nous rappelons le lemme du serpent :

Lemme 12.3. — *(Lemme du serpent). Etant donné un diagramme commutatif de A-modules ($\iota' \circ f = g \circ \iota$, $p' \circ g = h \circ p$)*

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \xrightarrow{\iota} & M & \xrightarrow{p} & P & \longrightarrow 0 \\ & & f \downarrow & & g \downarrow & & h \downarrow & \\ 0 & \longrightarrow & N' & \xrightarrow{\iota'} & M' & \xrightarrow{p'} & P' & \longrightarrow 0 \end{array}$$

avec des lignes exactes, alors il existe une suite exacte

$$0 \longrightarrow \ker f \xrightarrow{\iota_*} \ker g \xrightarrow{p_*} \ker h \xrightarrow{\delta} \operatorname{Coker} f \xrightarrow{\iota'_*} \operatorname{Coker} g \xrightarrow{p'_*} \operatorname{Coker} h \longrightarrow 0.$$

Démonstration. — La construction des applications de la suite exacte est immédiate sauf pour $\delta : \ker\ h \to \operatorname{Coker} g$. Soit $q \in \ker h$ et m un relèvement de q dans M. Par commutativité du diagramme, $g(m)$ s'envoie sur 0 dans P' donc provient d'un unique $n' \in N'$. Nous définissons $\delta(q)$ comme l'image de n' dans $\operatorname{Coker} f$. Deux choix de relèvements m, m' diffèrent par un élément $n \in N$ qui s'envoie sur 0 dans $\operatorname{Coker} f$ donc δ est bien défini. Il suffit alors de vérifier l'exactitude de la suite obtenue. □

Corollaire 12.4. — *Avec les notations du lemme du serpent,*
i. si f, h sont injectives, g aussi. Si f, h sont surjectives, g aussi.
ii. Si f est surjective et g injective, h est injective. Si g est surjective et h injective, f est surjective.

Définition-Proposition 12.5. — *Une suite exacte courte de A-modules*

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{p} P \longrightarrow 0$$

est dite **scindée** *si elle vérifie l'une des condtions équivalentes suivantes :*
i. Il existe $q : P \longrightarrow M$ tel que $p \circ q = \mathrm{Id}_P$.
ii. Il existe $j : M \longrightarrow N$ tel que $j \circ \iota = \mathrm{Id}_N$.
iii. L'image $i(N)$ a un supplémentaire dans M.

Démonstration. — i.$\Longrightarrow$ iii. Montrons que $Q = q(P) \subset M$ est un supplémentaire de $\iota(N)$. En effet Q et $\iota(N)$ sont en somme directe : Si $\iota(x) = q(y)$ avec $x \in N$ et $y \in P$ alors $0 = p(\iota(x)) = p(q(y)) = y$. Donc si $y = 0$ et $\iota(x) = 0$ donc $x = 0$ et $\iota(N) \cap Q = \{0\}$. De plus Q est supplémentaire de $\iota(N)$: pour $m \in M$, soit $y = p(m)$. Alors $p(m - q(y)) = p(m) - p(q(p(m))) = 0$ donc $m - q(y) \in \iota(N)$.
iii.$\Longrightarrow$ i. Soit Q un supplémentaire de $\iota(N)$ dans M. Nous avons $\ker p_{|Q} = \ker p \cap Q = \iota(N) \cap Q = \{0\}$, donc $p_{|Q}$ est injectif. Pour $x \in P$, soit $y \in M$, tel que $x = p(y)$. Ecrivons $y = \iota(z) + z'$ avec $z \in N$ et $z' \in Q$. Ainsi $x = p(\iota(z)) + p_{|Q}(z') = p_{|Q}(z')$. Donc $p_{|Q}$ est surjectif, donc bijectif, soit $q : P \longrightarrow Q$ sa réciproque. L'application q satisfait i.
ii.$\Longrightarrow$ iii. Soit $Q = \ker j$, montrons que Q et $\iota(N)$ sont en somme directe. Si $x \in Q \cap \iota(N)$, il existe $n \in N$ avec $x = \iota(n)$ et $0 = j(x) = j(\iota(n)) = 0$, donc $x = 0$. Montrons que $M = Q \oplus \iota(N)$. Soit $m \in M$ et $y = m - \iota(j(m))$. Alors $j(y) = j(m) - j(\iota(j(m))) = 0$ donc $y \in Q$.
iii.$\Longrightarrow$ ii. Soit Q un supplémentaire de $\iota(N)$ dans M. Soit $j : M \longrightarrow N$, qui à $m = x + \iota(y)$ $(x \in Q, y \in N)$ associe $y \in N$. Cette application est un morphisme bien défini car i est injectif. Et $\iota(y) \in \iota(N)$ s'écrit $\iota(y) = 0 + \iota(y)$, donc $j(\iota(y)) = y$ et $j \circ \iota = \mathrm{Id}_N$. □

Exemple 12.6. — *Une suite exacte courte de $\mathbb{Z}$-modules*

$$0 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 0$$

est scindée si et seulement le groupe G est le produit semi-direct de H et G/H.

12.2. Modules projectifs, injectifs. —

Définition 12.7. — *Un A-module P est dit* **projectif** *si toute suite exacte courte*

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{p} P \longrightarrow 0$$

est scindée.

Théorème 12.8. — *Soit P un A-module. Les propriétés suivantes sont équivalentes :*
i. P est projectif.
ii. P est facteur direct (sous-module admettant un supplémentaire) d'un A-module libre.
iii. Pour tout morphisme surjectif $p : M \longrightarrow N$ et tout morphisme $f : P \longrightarrow N$, il existe un morphisme $g : P \longrightarrow M$ tel que $f = p \circ g$.

Démonstration. — i.$\Longrightarrow$ii. Supposons que P est projectif. Soit S une famille génératrice de P, $L = A^{(S)}$ le A-module libre de base S et $p : L \longrightarrow P$, $e_s \mapsto s$. Notons $N = \ker p$, ainsi nous disposons d'une suite exacte courte

$$0 \longrightarrow N \xrightarrow{i} L \xrightarrow{p} P \longrightarrow 0$$

Comme P est projectif, N admet un supplémentaire Q dans L et $p_{|Q} : Q \longrightarrow P$ est un isomorphisme. Donc P est isomorphe à un facteur direct du A-module libre L.
ii.$\Longrightarrow$iii. Supposons que $L = P \oplus Q$ avec L A-module libre de base S. Soit $p : M \longrightarrow N$ morphisme surjectif, $f : P \longrightarrow N$ morphisme quelconque. Montrons qu'il existe $g : P \longrightarrow M$ tel que $p \circ g = f$.
Soit $\varphi : L \longrightarrow N$ défini par $\varphi(x + y) = f(x)$ si $x \in P$ et $y \in Q$; ainsi $\varphi_{|P} = f$. Pour tout $s \in S$ soit $m_s \in M$ tel que $p(m_s) = \varphi(s)$ (qui existe car p est surjectif). La propriété universelle des modules libres implique qu'il existe un unique morphisme $\gamma : L \longrightarrow M$ tel que $\gamma(s) = m_s$. Alors $p \circ \gamma(s) = p(m_s) = \varphi(s)$, $s \in S$. Comme S est une base de L, $p \circ \gamma = \varphi$. Le morphisme $g = \varphi_{|P}$ satisfait $p \circ g = \varphi_{|P} = f$.
iii.$\Longrightarrow$i. Soit $p : M \longrightarrow P$ un morphisme surjectif. D'après iii. avec $N = P$ et $f = \mathrm{Id}_P$, il existe $g : P \longrightarrow M$ tel que $p \circ g = \mathrm{Id}_P$. Donc P est projectif. □

Exemple 12.9. — *Les modules libres sont projectifs.*

Définition 12.10. — *Un foncteur covariant F est dit* **exact à gauche** *si pour toute suite exacte*

$$0 \longrightarrow N \longrightarrow M \longrightarrow P$$

la suite

$$0 \longrightarrow F(N) \longrightarrow F(M) \longrightarrow F(P)$$

est exacte.
Un foncteur covariant F est dit **exact à droite** *si pour toute suite exacte*

$$N \longrightarrow M \longrightarrow P \longrightarrow 0$$

la suite

$$F(N) \longrightarrow F(M) \longrightarrow F(P) \longrightarrow 0$$

est exacte.
Le foncteur covariant F est **exact** *s'il est exact à droite et à gauche.*

Exemples 12.11. — *i. Soit Q un A-module. Le foncteur* $\mathrm{Hom}_A(Q,\cdot)$ *est exact à gauche. Il est exact si seulement si Q est projectif.*
ii. Soit M un A-module. Le foncteur $N \mapsto M \otimes_A N$ est exact à droite. En général il n'est pas exact à gauche. En effet la multiplication par 2 $\mathbb{Z} \longrightarrow \mathbb{Z}$ est injective mais coïncide avec l'application nulle sur $M = \mathbb{Z}/2\mathbb{Z}$.
iii. Nous avons des définitions analogues pour les foncteurs contravariants.

Nous avons une définition analogue des modules injectifs :

Définition 12.12. — *Un A-module I est* **injectif** *si toute suite exacte courte*

$$0 \longrightarrow I \longrightarrow M \longrightarrow N \longrightarrow 0$$

est scindée.

Exemples 12.13. — *i. Le A-module I est injectif si et seulement si le foncteur contravariant* $\mathrm{Hom}_A(-,I)$ *est exact.*
ii. (Critère de Baer) Le A-module I est injectif si et seulement si pour tout idéal $J \subset A$, toute application A-linéaire $J \longrightarrow I$ se prolonge en une application A-linéaire $A \longrightarrow I$.

12.3. Cohomologie. —

Définition 12.14. — *Un* **complexe** (M,δ) *de A-modules est une suite de morphismes de A-modules*

$$\cdots \longrightarrow M^{i-1} \xrightarrow{\delta^{i-1}} M^i \xrightarrow{\delta^i} \cdots \longrightarrow$$

telle que $\delta^i \circ \delta^{i-1} = 0$ pour tout $i \in \mathbb{Z}$.
Un **morphisme de complexes** $(M,\delta) \to (M',\delta')$ *est une collection d'homomorphismes $\phi^i : M^i \longrightarrow M^{i'}$, $i \in \mathbb{Z}$ tels que le diagramme suivant est commutatif*

$$\begin{array}{ccc} M^{i-1} & \xrightarrow{\delta^{i-1}} & M^i \\ {\scriptstyle \phi^{i-1}}\downarrow & & \downarrow{\scriptstyle \phi^i} \\ M'^{i-1} & \xrightarrow{\delta'^{i-1}} & M'^i \end{array}$$

Une **suite exacte de complexes** *est une suite de morphismes de complexes*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

telle que pour tout $i \in \mathbb{Z}$, la suite de A-modules suivantes est exacte :

$$0 \longrightarrow A^i \longrightarrow B^i \longrightarrow C^i \longrightarrow 0.$$

Définition 12.15. — *Le i-ème groupe de cohomologie du complexe (M,δ) de A-modules est*

$$H^i(M) = \ker \delta^i / \operatorname{im} \delta^{i-1}, i \in \mathbb{Z}.$$

Un morphisme de complexes $(M,\delta) \longrightarrow (M',\delta')$ induit donc des applications $H^i(M) \longrightarrow H^i(M')$ pour $i \in \mathbb{Z}$.

Théorème 12.16. — *(Suite exacte longue de cohomologie). Soit*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

une suite exacte courte de complexes de A-modules. Alors nous avons une suite exacte longue de cohomologie

$$\cdots \longrightarrow H^i(A) \longrightarrow H^i(B) \longrightarrow H^i(C) \longrightarrow H^{i+1}(A) \longrightarrow H^{i+1}(B) \longrightarrow \cdots$$

Démonstration. — Il suffit d'appliquer le lemme du serpent au diagramme

$$\begin{array}{ccccccc} & A^i/\operatorname{im}\delta^{A^{i-1}} & \longrightarrow & B^i/\operatorname{im}\delta^{B^{i-1}} & \longrightarrow & C^i/\operatorname{im}\delta^{C^{i-1}} & \longrightarrow 0 \\ & \alpha\downarrow & & \beta\downarrow & & \gamma\downarrow & \\ 0 \longrightarrow & \ker\delta^{A^i} & \longrightarrow & \ker\delta^{B^i} & \longrightarrow & \ker\delta^{C^i} & \end{array}.$$

□

Théorème 12.17. — *(Caractéristique d'Euler-Poincaré). Supposons que (M, δ) est un complexe de K-espaces vectoriels de dimension finie et que les M^i sont presque tous nuls. Alors la caractéristique d'Euler-Poincaré*

$$\chi(M) = \sum_{i\in\mathbb{Z}} (-1)^i \dim_K M^i \in \mathbb{Z}$$

du complexe (M, δ) ne dépend que des groupes de cohomologie $H^i(M)$.

Démonstration. — La suite exacte

$$0 \longrightarrow H^i(M) \longrightarrow M^i/\operatorname{im}\delta^{i-1} \xrightarrow{\bar{\delta}^i} \operatorname{im}\delta^i \longrightarrow 0$$

et l'égalité

$$\dim_K M^i = \dim_K \operatorname{im}\delta^{i-1} + \dim_K M^i/\operatorname{im}\delta^{i-1}$$

donnent $\dim_K M^i = \dim_K \operatorname{im}\delta^{i-1} + \dim_K \operatorname{im}\delta^i + \dim_K H^i(M)$. Donc

$$\sum_{i\in\mathbb{Z}} (-1)^i (\dim_K M^i - \dim_K H^i(M)) = \sum_{i\in\mathbb{Z}} \dim_K \operatorname{im}\delta^{i-1}((-1)^i + (-1)^{i+1}) = 0.$$

□

PARTIE III

GÉOMÉTRIES

Comme en algèbre 1, où nous considérons l'action d'un groupe sur un ensemble, les anneaux s'identifient à des anneaux de fonctions sur des espaces adaptés. Suivant le contexte, il s'agit de fonctions continues (en topologie), fonctions lisses (en géométrie différentielle), des fonctions holomorphes (en géométrie complexe) ou des fonctions polynomiales (en géométrie algébrique). Par exemple, l'anneau quotient $\mathbb{C}[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$ est un anneau de fonctions sur le sous-ensemble de l'espace affine défini par le système d'équations polynomiales $f(X_1, \ldots, X_n) = \cdots = f_m(X_1, \ldots, X_n) = 0$.
Il y a une dualité naturelle entre points et fonctions. Dans l'équation

$$f(x) = 0 \quad (f \text{ fonction } x \text{ point})$$

nous considérons habituellement f fixe et x variable, mais il s'agit également de considérer x fixe et f variable. Cette dualité conduit à un dictionnaire naturel entre les concepts géométriques (points, applications, dimension, réductibilité, multiplicité, localisation au voisinage d'un point) et leurs analogues algébriques.

13. Rappel de topologie

Définition 13.1. — *Soit X un ensemble. Nous appelons* **topologie** *sur X la donnée d'un ensemble $\mathcal{O}$ de parties de X possédant les propriétés suivantes :*
i. $\mathcal{O}$ contient $\emptyset$ et X,
ii. la réunion quelconque d'éléments de $\mathcal{O}$ est encore dans $\mathcal{O}$,
iii. l'intersection finie d'éléments de $\mathcal{O}$ est encore dans $\mathcal{O}$.
Les éléments de $\mathcal{O}$ sont appelés **ouverts** *et les complémentaires sont appelés* **fermés**. *Le couple $(X, \mathcal{O})$ est appelé* **espace topologique**.

En absence d'ambiguïté, nous notons simplement X un espace topologique $(X, \mathcal{O})$.

Exemples 13.2. — *i. Un espace métrique X (i.e un ensemble X muni d'une distance) est un espace topologique.*
ii. Si $\mathcal{O} = \{\emptyset, X\}$, X est dit muni de la topologie grossière.
iii. Si $\mathcal{O} = \{Y \subset X\}$, X est muni de la topologie discrète. Tous les sous-ensembles de X sont ouverts et fermés, X est dit espace discret. Toutes les applications de X dans lui-même sont continues. La topologie discrète est métrisable par la distance discrète : $d(x, y) = 1$ si $x \neq y$.
iv. Nous pouvons définir de façon duale une topologie sur X en donnant l'ensemble de ses fermés.

Définition 13.3. — *Soit $(X, \mathcal{O})$ un espace topologique. Une* **base d'ouverts** *de $\mathcal{O}$ est un sous-ensemble $\mathcal{O}'$ de $\mathcal{O}$ tel que $\mathcal{O}$ soit le plus petit ensemble contenant $\mathcal{O}'$ qui soit une topologie (nous disons encore que $\mathcal{O}'$ engendre la topologie $\mathcal{O}$).*

Exemples 13.4. — *i. L'ensemble $\{\{x\}, x \in X\}$ est une base de la topologie discrète de X.*
ii. Les carrés ouverts de sommets dans $\mathbb{Z}[1/2, i]$ forment une base d'ouverts de $\mathbb{C}$.

Définition 13.5. — *Un* **groupe topologique** *est un groupe muni d'une topologie telle que la loi de groupe et son inverse soient continues.*
Un **anneau topologique** *est un anneau muni d'une topologie telle que l'addition et la multiplication soient continues (comme l'anneau est unitaire, l'application opposée est alors continue).*
Un **corps topologique** *est un anneau topologique dont l'application d'inversion est continue.*

Exemples 13.6. — *i. Un groupe (anneau, corps) muni de la topologie discrète est un groupe (anneau, corps) topologique. C'est la topologie naturelle lorsque l'ensemble sous-jacent est fini.*
ii. Pour définir un groupe (anneau, corps) topologique, il suffit de se donner un groupe (anneau, corps) et une base de voisinages de 0.
iii. Lorsque A et B sont des anneaux munis d'une topologie, nous considérons des morphismes d'anneaux continus. Un morphisme continu bijectif est un isomophisme d'anneaux topologiques si et seulement si son inverse est continu.

Lemme 13.7. — *Soit G un groupe topologique et $\mathcal{O}$ une base de voisinage de $e \in G$. Alors*
i. Pour tout $V, V' \in \mathcal{O}$, il existe $V'' \in \mathcal{O}$ tel que $e \in V'' \subset V \cap V'$.
ii. Pour tout $V \in \mathcal{O}$, il existe $V' \in \mathcal{O}$ tel que $V'V' \subset V$.
iii. Pour tout $V \in \mathcal{O}$, il existe $V' \in \mathcal{O}$ tel que $V'^{-1} \subset V$.
iv. Pour tout $V \in \mathcal{O}$ et $g \in G$, il existe $V' \in \mathcal{O}$ tel que $V' \subset gVg^{-1}$.
v. Pour tout $g \in G$, $\{gV, V \in \mathcal{O}\}$ est une base de voisinages de g.
Réciproquement si G est un groupe et $\mathcal{O}$ est un ensemble non vide de sous-ensembles de G satisfaisant i.-iv. alors il existe une unique structure de groupe topologique sur G telle que v. soit satisfaite.

Démonstration. — Si $\mathcal{O}$ est une base de voisinage de e dans G groupe topologique. Alors i. est clair. Les propriétés ii.-iv. sont conséquence de la continuité de la loi, l'inversion et la conjugaison. Enfin v. s'obtient en considérant l'homéomorphisme de multiplication par g dans G.
Réciproquement supposons que $\mathcal{O}$ satisfait i.-iv. Alors $e \in V$, pour tout $V \in \mathcal{O}$. Notons

$$\mathcal{O}' = \{U \subset G | \forall g \in U, \exists V \in \mathcal{O} \text{ tel que } gV \subset U\}.$$

Alors $\emptyset, G \in \mathcal{O}'$ et $\mathcal{O}'$ est stable par réunion. Soit $U_1, U_2 \in \mathcal{O}'$ et $g \in U_1 \cap U_2$. Alors il existe $V_1, V_2 \in \mathcal{O}$ tels que $gV_1 \subset U_1, gV_2 \subset U_2$. En appliquant i. nous

obtenons $V' \in \mathcal{O}$ avec $gV' \subset U_1 \cap U_2$ donc $U_1 \cap U_2 \in \mathcal{O}'$. Par conséquent $\mathcal{O}'$ définit une topologie sur G qui satisfait v.
Les propriétés ii. et iv. donnent la continuité de la loi de G. En effet, soit $(g_1, g_2) \in G \times G$ et $U \in \mathcal{O}'$ avec $g_1 g_2 \in \mathcal{O}'$. Alors il existe $V \in \mathcal{O}$ tel que $g_1 g_2 V \subset U$. Donc d'après ii., il existe $V' \in \mathcal{O}$ tel que $V'V' \subset V$, donc $g_1 g_2 V'V' = g_1(g_2 V' g_2^{-1}) g_2 V' \subset U$. D'après iv, il existe $V'' \in \mathcal{O}$ tel que $V'' \subset g_2 V' g_2^{-1}$ et $g_1 V'' \times g_2 V'$ est un voisinage de (g_1, g_2).
Les propriétés iii. et iv. donnent la continuité de l'inversion. En effet soit $U \in \mathcal{O}'$ et $g \in G$ tel que $g^{-1} \in U$. Il existe $V \in \mathcal{O}$ tel que $g^{-1}V \subset U$, donc $V^{-1}g \subset U^{-1}$. D'après iii., il existe $V' \in \mathcal{O}$ avec $V'g \subset U^{-1}$. Enfin, d'après iv., il existe $V'' \in \mathcal{O}$ avec $gV'' \subset g(g^{-1}V'g) \subset U^{-1}$.

□

Définition 13.8. — *Soit X et X' deux espaces topologiques.*
i. L'espace X est dit **séparé** *si pour tout $x, y \in X$ distincts, il existe un voisinage U_x (resp. U_y) de x (resp. de y) tels que $U_x \cap U_y = \emptyset$.*
ii. L'espace X est dit **compact** *si pour toute famille $(U_i)_{i \in I}$ d'ouverts de X avec $\cup_{i \in I} U_i = X$, il existe une partie finie $J \subset I$ avec $\cup_{i \in J} U_i = X$.*
iii. L'espace X est dit **normal**, *s'il est séparé et pour tout couple de parties fermées $Z, Z' \subset X$ avec $Z \cap Z' = \emptyset$, il existe des parties ouvertes U, U' de X avec*

$$Z \subset U, Z' \subset U', U \cap U' = \emptyset.$$

iv. L'espace topologique X est **irréductible** *si $\forall F_1, F_2$ fermés propres de X, $F_1 \cup F_2 \neq X$. Une partie $Z \subset X$ est dite irréductible, si le sous-espace topologique Z est irréductible.*

Exemple 13.9. — *Un espace topologique X est irréductible si et seulement si tout ouvert non vide est partout dense.*

Lemme 13.10. — *Un espace topologique X compact séparé est normal.*

Démonstration. — Soit $Z, Z' \subset X$ deux parties fermées disjointes.
Cas $Z = \{z\}$. Pour tout $z' \in Z'$, il existe des ouverts disjoints $U_{z'}$ et $U'_{z'}$ avec $z \in U_{z'}$ et $z' \in U'_{z'}$. Les ouverts $(U'_{z'})_{z' \in Z'}$ recouvrent Z' qui est fermé dans un compact donc compact. Nous pouvons extraire un sous-recouvrement fini $Z' \subset \cup_{z' \in S'} U'_{z'}$ et les ouverts $U'_z = \cup_{z' \in S'} U'_{z'}$, $U_z = \cap_{z' \in S'} U_{z'}$ satisfont $Z \subset U_z$ et $Z' \subset U'_z$ et $U_z \cap U'_z = \emptyset$.
Cas général. D'après l'étude précédente, pour tout $z \in Z$, il existe des ouverts U_z, U'_z disjoints avec $z \in U_z$ et $Z' \subset U'_z$. Nous pouvons extraire un recouvrement fini $Z \subset \cup_{z \in S} U_z$ du recouvrement de Z par $5U_z)_{z \in Z}$. Alors $U = \cup_{z \in S} U_z$ et $U' = \cap_{z \in S} U'_z$ satisfont $Z \subset U$ et $Z' \subset U'$ et $U \cap U' = \emptyset$. Donc X est normal. □

Lemme 13.11. — *(Urysohn) Un espace topologique $(X, \mathcal{O})$ est normal si et seulement si il est séparé et pour tout couple de parties fermées $A, B \subset X$ telles que $A \cap B = \emptyset$, il existe une fonction continue $f : X \longrightarrow [0, 1]$ telle que $f(A) = \{0\}$ et $f(B) = \{1\}$.*

Démonstration. — $\Longleftarrow$. Soient A, B deux parties fermées disjointes et $f : X \longrightarrow [0,1]$ continue avec $f(A) = \{0\}$ et $f(B) = \{1\}$. Alors les parties ouvertes $f^{-1}([0,1/2[)$ et $f^{-1}(]1/2,1])$ sont disjointes et contiennent A et B respectivement. Donc X est normal.
$\Longrightarrow$ Réciproquement si X est normal, soit

$$\Lambda_n = \{k/2^n | k \in \mathbb{N}, 0 \leq k \leq 2^n\}, n \in \mathbb{N} \text{ et } \Lambda = \cup_{n\in\mathbb{N}}\Lambda_n.$$

Pour toute partie $S \in X$, nous notons $\overline{S}$ l'adhérence de S (i.e. le plus petit fermé de X contenant S) dans X. Construisons une application $g : \Lambda \longrightarrow \mathcal{O}$ telle que :

$$A \subset g(0), B \cap g(1) = \emptyset, \overline{g(\lambda)} \subset g(\lambda'), \lambda, \lambda' \in \Lambda, \lambda < \lambda'.$$

Nous définissons la restriction de g à Λ_n, par induction sur $n \in \mathbb{N}$. Pour $n = 0$, nous posons $g(1) = X - B$. Comme X est normal, il existe $U \in \mathcal{O}$ tel que $A \subset U \subset X - B = g(1)$. Comme $X - B$ est fermé, $A \subset \mathrm{U} \subset \overline{U} \subset g(1)$. Nous posons $g(0) = U$. Supposons que la restriction de g à Λ_n soit connue pour $n \in \mathbb{N}$. Ainsi pour $0 \leq k \leq 2^n - 1$, nous avons $\overline{g(k/2^n)} \subset g((k+1)/2^n)$ et comme X est normal, il existe $U \in \mathcal{O}$ tel que $\overline{g(k/2^n)} \subset U \subset \overline{U} \subset g((k+1)/2^n)$. Nous posons $g((2k+1)/2^{n+1}) = U$, ce qui achève la construction par induction de g.
Posons $U(\lambda) = g(\lambda)$, pour $\lambda \in \Lambda - \{1\}$ et $U(1) = X$ et définissons pour $x \in X$

$$f(x) = \inf\{\lambda \in \Lambda | x \in U(\lambda)\}.$$

Alors $f(A) = \{0\}$ et $f(B) = \{1\}$. Il suffit alors de vérifier la continuité de f : soit $x \in X$, $r = f(x)$ et $\varepsilon \in]0,1]$. Si $r = 0$ nous avons $x \in g(\lambda) \subset f^{-1}([0,\varepsilon[)$ pour tout $\lambda \in \Lambda \cap]0,\varepsilon[$. Si $r = 1$, nous avons $x \in X - \overline{g(\lambda)} \subset f^{-1}(]1-\varepsilon, 1[$. Si $0 < r < 1$, choisissons $\lambda, \lambda' \in \Lambda$ tels que $r - \varepsilon < \lambda < r < \lambda' < r + \varepsilon$; ainsi $x \in g(\lambda') - \overline{g(\lambda)} \subset f^{-1}(]r-\varepsilon, r+\varepsilon[)$. □

14. Ensembles algébriques affines, topologie de Zariski

14.1. Topologie de Zariski. — Les anneaux qui interviennent le plus souvent en géométrie algébrique sont des K-algèbres de présentation finie pour K un corps arbitraire. Pour simplifier, nous commençons par supposer que le corps $K = \overline{k}$ désigne un corps algébriquement clos (par exemple le corps $\mathbb{C}$ des nombres complexes).

Définition 14.1. — *Le n-espace affine (sur $\overline{k}$) est l'ensemble des n-uplets*

$$\mathbb{A}^n = \mathbb{A}^n(\overline{k}) = \{P = (x_1, \ldots, x_n), x_i \in \overline{k}\}.$$

Définition 14.2. — *A toute partie S de $\overline{k}[X] = \overline{k}[X_1, \ldots, X_n]$, nous associons le sous-ensemble de $\mathbb{A}^n$,*

$$V(S) = \{P \in \mathbb{A}^n, f(P) = 0, f \in S\}.$$

Un **ensemble algébrique** *(affine) est un ensemble de la forme $V(S)$.*
Si V est un ensemble algébrique affine, **l'idéal de** *V est défini par*

$$I(V) = \{f \in \overline{k}[X] | f(P) = 0, P \in V\}.$$

Avec les notations précédentes, $I(V)$ est un idéal qui admet un nombre fini de générateurs (Théorème de la base d'Hilbert) et $V = V(I(V))$. En effet si $V = V(S)$ alors $S \subset I(V)$ et $V(I(V)) \subset V$. Réciproquement si $P \in V(S)$, $f(P) = 0$ pour tout $f \in I(V)$ donc $P \in V(I(V))$. Donc $V \subset V(I(V))$.

Exemples 14.3. — *i. $V(1) = \emptyset$ et $V(0) = \overline{k}[X]$ sont des ensembles algébriques.*
ii. Pour $n = 1$, un idéal I de $\overline{k}[X_1]$ est principal donc $V(I(V))$ est fini ou égal à $\overline{k}$.
iii. Pour $\overline{k} = \mathbb{C}$, $V(X_1^4 - 2) = \{\pm 2^{1/4}, \pm i 2^{1/4}\}$.
iv. Un point de $\overline{k}$ est un ensemble algébrique car $V(X_1 - x_1, \ldots, X_n - x_n) = \{(x_1, \ldots, x_n)\}$.
v. Dans $\overline{k}^2$, $V(X_1^2) = V(X_1)$ c'est l'axe des x_2. Nous avons $I(V) = (X_1)$.
vi. Tout sous-espace affine de $\mathbb{A}^n$ est un ensemble algébrique.
vii. Soit S une partie de $\overline{k}[X]$. Nous avons $V(S) = V(< S >)$. Mais en général $I(V(S))$ n'est pas l'idéal engendré par S (voir v.)
vii. Soit $S = \{f_1, \ldots, f_d\} \subset \overline{k}[X]$. Alors V est vide si et seulement si 1 est combinaison des f_i (Nullstellenstatz 14.8).

Proposition 14.4. — *i. Toute intersection d'ensembles algébriques est un ensemble algébrique.*
ii. Toute réunion finie d'ensembles algébriques est un ensemble algébrique.

Démonstration. — i. $\cap_\alpha V(S_\alpha) = V(< \cup_\alpha I(V(S_\alpha)) >) = V(\sum_\alpha I(V(S_\alpha)))$.
ii. Nous avons $V(S_1) \cup V(S_2) = V(S_1 S_2)$ où $S_1 S_2$ est l'ensemble des produits d'un élément de S_1 et d'un élément de S_2. En effet si $x \notin V(S_1) \cup V(S_2)$, $\exists F_1 \in S_1$ et $F_2 \in S_2$ avec $F_1(x) F_2(x) \neq 0$ donc $x \notin V(S_1 S_2)$. □

La proposition 14.4 permet de définir une topologie dite de Zariski sur $\mathbb{A}^n(\overline{k})$:

Définition 14.5. — *La* **topologie de Zariski** *sur $\mathbb{A}^n(\overline{k})$ est la topologie dont les fermés sont les ensembles algébriques. Plus généralement, nous munissons tout ensemble algébrique de la topologie induite par la topologie de Zariski.*

La topologie de Zariski sur $\mathbb{A}^n(\overline{k})$ n'est pas séparée. De façon imagée, les ouverts sont très gros, et les fermés très petits. Par exemple, dans $\overline{k}$, les fermés sont $\emptyset$, $\overline{k}$ et les ensembles finis.

14.2. Nullstellensatz. — L'étude des extensions algébriques et transcendantes d'un corps fait l'objet du paragraphe §18 mais par souci de cohérence de l'exposé, nous présentons ici le lemme technique suivant.

Lemme 14.6. — *Soit $\bar{k}$ un corps algébriquement clos non dénombrable et K une extension de $\bar{k}$ de dimension au plus dénombrable. Alors $K = \bar{k}$.*

Démonstration. — Il suffit de démontrer que K est algébrique sur $\bar{k}$. Sinon il contiendrait un élément transcendant donc un sous-corps isomorphe au corps des fractions rationnelles $\bar{k}(T)$. Mais ce corps contient la famille non dénombrable des $1/(T-a)$ avec $a \in \bar{k}$ et cette famille est libre : si nous avons une relation

$$\sum_{i=1}^{n} \frac{\lambda_i}{T - a_i} = 0$$

en multipliant par $T - a_i$ et en faisant $T = a_i$, nous obtenons $\lambda_i = 0$. □

Théorème 14.7. — *(Nullstellensatz faible)*
Soit I un idéal propre de $\bar{k}[X_1, \ldots, X_n]$. Alors $V(I)$ est non vide.

Démonstration. — Quitte à plonger I dans un idéal maximal, nous pouvons supposer I maximal. Notons $K = \bar{k}[X_1, \ldots, X_n]/I$ le corps résiduel. Or $\bar{k}[X_1, \ldots, X_n]$ est un $\bar{k}$-espace vectoriel de dimension au plus dénombrable sur $\bar{k}$, donc K aussi. D'après le lemme 14.6, $K = \bar{k}$. Notons a_i les images de X_i dans K. Si $P(X_1, \ldots, X_n) \in I$ alors $P(a_1, \ldots, a_n) = 0$ donc $(a_1, \ldots, a_n) \in V(I)$, non vide. □

Théorème 14.8. — *(Nullstellensatz)*
Soit I un idéal de $\bar{k}[X_1, \ldots, X_n]$. Nous avons $I(V(I)) = \mathrm{rad}(I)$.

Démonstration. — $I =< f_1, \ldots, f_s >$ et $V = V(I)$. Il est clair que $\mathrm{rad}(I) \subset I(V(I))$.
Réciproquement soit $f \in I(V(I))$, montrons que $f^m \in I$ pour m assez grand.
Soit $A_{(f)}$ l'anneau localisé en f. Il suffit de montrer que l'idéal $IA_{(f)}$ engendré par I dans $A_{(f)}$ est égal à $(1) = A_{(f)}$ car alors

$$1 = \sum_i \frac{f_i P_i}{f^m}$$

donc en chassant le dénominateur, nous obtenons $f^m \in I$.
Mais l'anneau $A_{(f)}$ est isomorphe à $\bar{k}[X_1, \ldots, X_n, T]/(1 - Tf)$, donc la condition $IA_{(f)} = (1)$ signifie que $1 = \sum_i f_i P_i + Q(1 - Tf)$ avec $Q, P_i \in \bar{k}[X_1, \ldots, X_n, T]$.
Soit $J = (f_1, \ldots, f_s, 1 - Tf)$ l'idéal de $\bar{k}[X_1, \ldots, X_n, T]$. Nous avons $V(J) = \emptyset$ dans $\bar{k}^{n+1}$ car si $(c_1, \ldots, c_n, t) \in V(J)$, le point $(c_1, \ldots, c_n)$ annulerait les f_i et serait dans V donc annulerait f et ne pourrait pas annuler $1 - Tf$. Il résulte du Nullstellensatz faible que $J = (1)$. □

Corollaire 14.9. — *(Version géométrique du Nullstellensatz) Sur un corps $\overline{k}$ algébriquement clos, les applications*

$$I : \{\textit{Ensembles algébriques de } \mathbb{A}^n(\overline{k})\} \longrightarrow \{\textit{Idéaux de } \overline{k}[X_1, \ldots, X_n]\}$$

$$V : \{\textit{ Idéaux de } \overline{k}[X_1, \ldots, X_n]\} \longrightarrow \{\textit{Ensembles algébriques de } \mathbb{A}^n(\overline{k})\}$$

satisfont $I(V(I)) = \operatorname{rad} I$ et $V(I(V)) = V$. Elles induisent des bijections inverses l'une de l'autre

$$\{\textit{Ensembles algébriques de } \mathbb{A}^n(\overline{k})\} \xrightarrow{\simeq} \{\textit{ Idéaux radiciels de } \overline{k}[X_1, \ldots, X_n]\}$$

14.3. Algèbre et géométrie. — Soit K un corps (pas forcément algébriquement clos). Il est naturel d'étendre les définitions précédentes aux K-algèbres.

Définition 14.10. — *Soit K un corps et I un idéal de $K[X_1, \ldots, X_n]$. Nous notons $Z(K) = \{(x_1, \ldots, x_n) \in K^n | \forall f \in I, f(x) = 0\}$ l'ensemble algébrique associé à I. L'***anneau des fonctions régulières*** sur $Z(K)$ est la K-algèbre*

$$\mathcal{O}(Z(K)) = K[X_1, \ldots, X_n]/I.$$

Plus généralement, pour toute K-algèbre B, l'ensemble des B-points de Z :

$$Z(B) = \{b = (b_1, \ldots, b_n) \in B^n | \forall f \in I, f(b) = 0\}.$$

Exemples 14.11. — *i. La conique Z définie par $I = (x^2 + y^2 + 1)$ vérifie $Z(\mathbb{R}) = \emptyset$, mais pour la $\mathbb{R}$-algèbre $\mathbb{C}$, nous avons $Z(\mathbb{C}) \neq \emptyset$.*
ii. Sur $\mathbb{C}^2$, Z défini par $I = (y)$ est la droite horizontale et l'ensemble Z' défini par $I = (y^2)$ est la même droite avec multiplicité deux. Ce sont deux objets différents dont les points complexes coïncident

$$Z(\mathbb{C}) = Z'(\mathbb{C}) = \{(x, 0), x \in \mathbb{C}\}$$

d'anneaux de fonctions régulières respectifs

$$\mathcal{O}(Z) = \mathbb{C}[x, y]/(y) = \mathbb{C}[x], \quad \mathcal{O}(Z') = \mathbb{C}[x, y]/(y^2) = \mathbb{C}[x] + \varepsilon\mathbb{C}[x]$$

où $\varepsilon = y \mod y^2 \neq 0 \in \mathcal{O}(V')$ et $\varepsilon^2 = 0$. Il s'agit d'un élément infinitésimal.
iii. Soit k un corps et $\overline{k}$ une clôture algébrique (voir §18). Soit V un ensemble algébrique sur $\overline{k}$. Notons

$$I(V/k) = \{f \in k[X], f(P) = 0, P \in V\} = I(V) \cap k[X]$$

Nous disons que V est définie sur k si

$$I(V) = I(V/k)\overline{k}[X].$$

Si V est définie sur k, alors $\mathrm{Gal}(\overline{k}/k)$ agit sur V et

$$V(k) = \{P \in V, P^\sigma = P, \sigma \in \mathrm{Gal}(\overline{k}/k)\}.$$

Déterminer $V(k)$ c'est résoudre les équations polynômiales et c'est un problème central en arithmétique.
iv. Pour $I = (Y^2 - X^3 - 17)$ idéal de $\mathbb{Q}[X, Y]$, l'ensemble algébrique $Z(\mathbb{Q})$ a une

infinité de points (courbe elliptique).
v. Le théorème de Fermat dit que si $n \geq 3$

$$V((X^n + Y^n - 1))(\mathbb{Q}) = \begin{cases} \{(1,0),(0,1)\} & n \text{ impair,} \\ \{(\pm 1,0),(0,\pm 1)\} & n \text{ pair.} \end{cases}$$

Proposition 14.12. — *Pour toute* K*-algèbre* B*, les applications*

$$\mathrm{Hom}_{K-\mathrm{Alg}}(\mathcal{O}(Z), B) \longrightarrow Z(B), \quad \beta \mapsto (\beta \circ \mathrm{pr}(X_1), \ldots, \beta \circ \mathrm{pr}(X_n))$$

et

$$Z(B) \longrightarrow \mathrm{Hom}_{K-\mathrm{Alg}}(\mathcal{O}(Z), B), \quad b = (b_1, \ldots, b_n) \mapsto \overline{\mathrm{ev}}_b$$

sont des bijections réciproques l'une de l'autre ($\mathrm{pr} : K[X_1, \ldots, X_n] \longrightarrow \mathcal{O}(Z)$ *est la projection canonique et* $\mathrm{ev}_b = \overline{\mathrm{ev}}_b \circ \mathrm{pr}$*).*

Démonstration. — Soit un homomorphisme de K-algèbres $\alpha = \mathrm{ev}_b$ ($b \in B^n$). Il se factorise en $\alpha = \beta \circ \mathrm{pr}$ pour un unique $\beta = \overline{\mathrm{ev}}_b$ si et seulement si

$$\mathrm{ev}_b(I) = \alpha(I) = 0 \Longleftrightarrow \forall g \in I, 0 = \alpha(g(X_1, \ldots, X_n)) = g(\alpha(X_1), \ldots, \alpha(X_n)) = g(b)$$

$$\Longleftrightarrow b = (\alpha(X_1), \ldots, \alpha(X_n)) \in Z(B).$$

□

Corollaire 14.13. — *Soit deux* K*-algèbres de type fini*

$$\mathcal{O}(Z_1) = K[X_1, \ldots, X_n]/I_1 \text{ et } \mathcal{O}(Z_2) = K[Y_1, \ldots, Y_m]/I_2$$

correspondant respectivement aux ensembles affines $Z_1 = V(I_1)$ *et* $Z_2 = V(I_2)$*. Alors tout morphisme de* K*-algèbres* $\alpha : \mathcal{O}(Z_1) \longrightarrow \mathcal{O}(Z_2)$ *induit des applications*

$$\alpha_B^* : Z_2(B) \xrightarrow{\simeq} \mathrm{Hom}_{K-\mathrm{Alg}}(\mathcal{O}(Z_2), B) \longrightarrow \mathrm{Hom}_{K-\mathrm{Alg}}(\mathcal{O}(Z_1), B) \xrightarrow{\simeq} Z_1(B)$$

via $\alpha_B^*(b) = b \circ \alpha$*.*

15. Spectre maximal

15.1. Toplogie de Zariski. — Pour A un anneau, en nous inspirant du paragraphe précédent, nous munissons $\mathrm{Spm}\, A$ de la topologie de Zariski engendrée par les ouverts

$$D(f) = \{\mathfrak{m} \in \mathrm{Spm}\, A | f \notin \mathfrak{m}\}, \forall f \in A.$$

Ainsi tout idéal I de A définit une partie fermée de $\mathrm{Spm}\, A$:

$$V(I) = \{\mathfrak{m} \in \mathrm{Spm}\, A | I \subset \mathfrak{m}\}.$$

Proposition 15.1. — *La topologie de Zariski sur* $\mathrm{Spm}\, A$ *est compacte.*

Démonstration. — Soit $(U_\lambda)_{\lambda\in\Lambda}$ une famille de parties ouvertes de $\operatorname{Spm} A$ dont la réunion est $\operatorname{Spm} A$. Nous pouvons supposer que pour tout $\lambda \in \Lambda$, il existe $f_\lambda \in A$ tel que $U_\lambda = D(f_\lambda)$. Donc pour tout $\mathfrak{m} \in \operatorname{Spm} A$, il existe $\lambda \in \Lambda$ tel que $f_\lambda \notin \mathfrak{m}$. Donc l'idéal $I = \sum_{\lambda\in\Lambda} Af_\lambda$ n'est contenu dans aucun idéal maximal donc $I = A$. Ainsi il existe une partie finie $S \subset \Lambda$ et une écriture $1 = \sum_{\lambda\in S} a_\lambda f_\lambda$. Par conséquent $(U_\lambda)_{\lambda\in S}$ est un sous-recouvrement ouvert de $\operatorname{Spm} A$. □

15.2. Espace topologique et spectre maximal. — L'objet de ce paragraphe est d'identifier tout espace topologique X compact séparé au spectre maximal de l'anneau des fonctions continues sur X à valeurs réelles.

Définition-Proposition 15.2. — *Soit X un espace topologique. Nous notons $\mathcal{C}(X)$ l'anneau des fonctions continues à valeurs réelles $f : X \longrightarrow \mathbb{R}$, où $\mathbb{R}$ est muni de la topologie standard engendrée par la base $\{]a, b[, a, b \in \mathbb{R}, a < b\}$.*
i. Les éléments inversibles de $\mathcal{C}(X)$ sont

$$\mathcal{C}(X)^* = \{f \in \mathcal{C}(X) | f(x) \neq 0, \text{ pour tout } x \in X\}.$$

ii. Pour $x \in X$, l'idéal

$$\mathfrak{m}_x = \{f \in \mathcal{C}(X) | f(x) = 0\}$$

est maximal, ce qui permet de définir une application

$$\phi_X : X \longrightarrow \operatorname{Spm}(\mathcal{C}(X)), x \mapsto \mathfrak{m}_x.$$

Démonstration. — i. Si $f \in \mathcal{C}(X)$ est inversible, $\exists g \in \mathcal{C}(X)$ tel que $fg = 1$ et nous avons $f(x) \neq 0$ pour tout $x \in X$. Réciproquement, l'application $i : \mathbb{R}^* \longrightarrow \mathbb{R}^*$, $x \mapsto 1/x$ est continue et si $f(X) \subset \mathbb{R}^*$, alors $i \circ f = 1/f \in \mathcal{C}(X)$ et $f \in \mathcal{C}(X)^*$.
ii. En effet $\mathfrak{m}_x$ est le noyau du morphisme surjectif d'évaluation

$$\mathcal{C}(X) \longrightarrow \mathbb{R}, x \mapsto f(x)$$

donc $\mathfrak{m}_x$ est un idéal. Comme $\mathcal{C}(X)/\mathfrak{m}_x \simeq \mathbb{R}$, $\mathfrak{m}_x$ est maximal. □

Exemple 15.3. — *Nous avons défini un foncteur*

$$\mathrm{Top}^{\mathrm{op}} \longrightarrow \mathbb{R} - \mathrm{Alg}, X \mapsto \mathcal{C}(X).$$

En effet, à toute application continue $f : X \longrightarrow X'$, nous associons un morphisme d'anneaux $f : \mathcal{C}(X') \longrightarrow \mathcal{C}(X)$, $g \mapsto g \circ f$. Il s'agit alors de vérifier que $(g \circ f)^* = f^* \circ g^*$.

Théorème 15.4. — *(Gelfand-Naimark) Si X est un espace topologique compact et séparé, l'application ϕ_X est bijective.*

Démonstration. — Soit $\mathfrak{m} \in \operatorname{Spm}(\mathcal{C}(X))$. Notons

$$V(\mathfrak{m}) = \{x \in X, f(x) = 0 \text{ pour tout } f \in \mathfrak{m}\}.$$

Montrons que $V(\mathfrak{m})$ est non vide. Sinon pour tout $x \in X$, il existe $f_x \in \mathfrak{m}$ avec $f_x(x) \neq 0$. Posons $U_x = f_x^{-1}(\mathbb{R} - \{0\})$. La partie U_x est ouverte dans X et

$X = \cup_{x \in X} U_x$. Comme X est compact , il existe une partie finie $S \subset X$ telle que $\cup_{s \in S} U_s = X$. Soit $g = \sum_{s \in S} f_s^2$. Nous avons $g(x) > 0$ pour tout $x \in X$, donc g est inversible dans $\mathcal{C}(X)$. Mais $g \in \mathfrak{m}$ conduit à une absurdité.
ϕ_X est surjective : si $x \in V(\mathfrak{m})$, nous avons $\mathfrak{m} \subset \phi_X(x)$, donc $\mathfrak{m} = \phi_X(x)$ car ces deux idéaux sont maximaux.
ϕ_X est injective : si $x, y \in X$ sont distincts, d'après le théorème d'Uryson (X séparé compact est normal) il existe $f \in \mathcal{C}(X)$ telle que $f \in \phi_X(x)$ et $f \notin \phi_X(y)$ d'où $\phi_X(x) \neq \phi_X(y)$. □

Proposition 15.5. — *Soit X espace topologique compact séparé. Munissons* $\operatorname{Spm} \mathcal{C}(X)$ *de la topologie de Zariski, i.e. la topologie engendrée par*

$$D(f) = \{\mathfrak{m} \in \operatorname{Spm}(\mathcal{C}(X)) | f \notin \mathfrak{m}\}, f \in \mathcal{C}(X).$$

Alors $\phi_X : X \longrightarrow \operatorname{Spm}(\mathcal{C}(X))$ est un homéomorphisme.

Démonstration. — Pour tout $x \in X$, $\mathfrak{m}_x \in D(f)$ si et seulement si $f(x) \neq 0$. Donc $\phi_X^{-1}(D(f)) = f^{-1}(\mathbb{R} - \{0\})$ est une partie ouverte de X et ϕ_X est continue. Comme ϕ_X est bijective continue, X est compact et $\operatorname{Spm}(\mathcal{C}(X))$ est séparé, ϕ_X est un homéomorphisme. □

Exemple 15.6. — *En général, la topologie de Zariski sur le spectre maximal n'est pas séparée. Par exemple, la topologie sur* $\operatorname{Spm} \mathbb{Z}$ *est engendrée par les parties $D(n)$, $n \in \mathbb{Z}$. Si $p_1, \ldots, p_k$ sont les diviseurs premiers de n, nous avons $D(n) = \operatorname{Spm} \mathbb{Z} - \{p_1\mathbb{Z}, \ldots, p_k\mathbb{Z}\}$. Ainsi les parties fermées de* $\operatorname{Spm} \mathbb{Z}$ *sont* $\operatorname{Spm} \mathbb{Z}$ *et les parties finies de* $\operatorname{Spm} \mathbb{Z}$. *Donc* $\operatorname{Spm} \mathbb{Z}$ *n'est pas séparé.*

Remarque 15.7. — *Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Alors f induit une application*

$$\operatorname{Spec} f : \operatorname{Spec} B \longrightarrow \operatorname{Spec} A, \mathfrak{p} \mapsto f^{-1}(\mathfrak{p}).$$

Cependant f n'induit pas en général d'application (voir Lemme 2.25)

$$\operatorname{Spm} f : \operatorname{Spm} B \longrightarrow \operatorname{Spm} A.$$

C'est l'une des raisons pour lesquelles, il est en général préférable de considérer le spectre premier plutôt que le spectre maximal (voir §16).

16. Spectre premier

La discussion précédente (§15) s'applique au spectre premier $\operatorname{Spec} A$. La topologie de Zariski engendrée par les parties ouvertes

$$D(f) = \{\mathfrak{p} \in \operatorname{Spec} A | f \notin \mathfrak{p}\}, \forall f \in A$$

confère à $\operatorname{Spec} A$ la structure d'un espace topologique compact.

Exemple 16.1. — *Pour tout idéal $I \subset A$, la partie*

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec} A, I \subset \mathfrak{p}\}$$

est fermée et toute partie fermée est de cette forme. De plus

$$I \subset J \Longrightarrow \operatorname{rad}(I) \subset \operatorname{rad}(J) \Longrightarrow V(J) \subset V(I).$$

Plus généralement, pour toute suite finie d'idéaux $I_1, \ldots, I_k$ de A,

$$\cup_{i=1}^k V(I_i) = V(\cap_{i=1}^k I_i).$$

En effet si l'idéal premier $\mathfrak{p} \in V(\cap_{i=1}^k I_i)$, alors $\cap_{i=1}^k I_i \subset \mathfrak{p}$ et le lemme 2.24 implique qu'il existe i tel que $I_i \subset \mathfrak{p}$, i.e $\mathfrak{p} \in V(I_i)$.

Exemples 16.2. — *i. Soit K un corps algébriquement clos, alors* $\operatorname{Spec} K[T] = \operatorname{Spm} K[T] \cup \{0\}$ *et* $\operatorname{Spm} K[T] = \{(T-a), a \in K\}$ *car K algébriquement clos. Ainsi l'application naturelle*

$$K \longrightarrow \operatorname{Spm} K[T], a \mapsto T - a$$

est une bijection.
ii. Supposons K est parfait (voir Définition 19.9) et notons $\overline{K}$ une cloture algébrique de K. Alors $\overline{K}/K$ est galoisienne de groupe $G = \operatorname{Gal}(\overline{K}/K)$. Les polynômes irréductibles unitaires de $K[T]$ sont en bijection naturelle avec les orbites $\overline{K}/G$ sous G de $\overline{K}$ et $\operatorname{Spec} K[T] = \{(0)\} \cup \overline{K}/G$. *Par exemple, nous avons une identification naturelle du spectre maximal de $\mathbb{R}[T]$ et du demi-plan supérieur complexe :*

$$\operatorname{Spm} \mathbb{R}[T] \simeq \{z \in \mathbb{C}, \operatorname{Im}(z) \geq 0\}.$$

Lemme 16.3. — *Tout morphisme d'anneaux $f : A \longrightarrow B$ induit une application continue*

$$\operatorname{Spec} f : \operatorname{Spec} B \longrightarrow \operatorname{Spec} A, \ \ \mathfrak{p} \mapsto f^{-1}\mathfrak{p}.$$

Démonstration. — L'application $\operatorname{Spec} f$ est bien définie d'après le lemme 2.25. La continuité s'obtient en remarquant que pour tout $a \in A$,

$$(\operatorname{Spec} f)^{-1} D(a) = D(f(a)).$$

□

Exemple 16.4. — *Nous avons défini un foncteur* $\operatorname{Spec} : \mathbb{Z} - \operatorname{Alg}^{\operatorname{op}} \longrightarrow \operatorname{Top}$, $A \mapsto \operatorname{Spec} A$. *En revanche l'association $A \mapsto \operatorname{Spm} A$ n'est pas fonctorielle.*

Lemme 16.5. — *Soit A un anneau, I un idéal, $\pi : A \longrightarrow A/I$ la projection. L'espace topologique* $\operatorname{Spec} A/I$ *s'identifie au sous-espace fermé $V(I)$ de* $\operatorname{Spec} A$, *via*

$$\operatorname{Spec} \pi : \operatorname{Spec} A/I \longrightarrow \operatorname{Spec} A.$$

Ainsi Specπ est un homéomorphisme si et seulement si $I \subset \cap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p} = \operatorname{rad}(0)$.

Démonstration. — L'application $\operatorname{Spec}\pi$ est injective et son image est la partie fermée $V(I) = \{\mathfrak{p} \in \operatorname{Spec} A | I \subset \mathfrak{p}\}$ (Lemme 2.25). Montrons que la topologie de Zariski sur $\operatorname{Spec} A/I$ coïncide avec la topologie induite sur $\operatorname{Spec} A$ via $\operatorname{Spec}\pi$. En effet toute partie ouverte de $\operatorname{Spec} A/I$ est réunion de parties de la forme $D(\overline{a})$ avec $\overline{a} \in A/I$ la classe d'un élément $a \in A$. Comme $D(\overline{a}) = (\operatorname{Spec}\pi)^{-1}(D(a))$, toute partie ouverte de $\operatorname{Spec} A/I$ est image réciproque d'une partie ouverte de $\operatorname{Spec} A$. Autrement dit l'espace topologique $\operatorname{Spec} A/I$ s'identifie canoniquement au sous-espace fermé $V(I)$ de $\operatorname{Spec} A$.
L'application $\operatorname{Spec}\pi$ est un homéomorphisme si et seulement si, il est surjectif, i.e. $V(I) = \operatorname{Spec} A$, i.e. $I \subset \operatorname{rad}(0)$. □

Remarque 16.6. — *Hochster caractérise en termes purement topologiques les spectres premiers des anneaux ; ce sont les espaces topologiques spectraux au sens suivant :*
Un espace topologique T est dit **spectral** *si :*
i. T est compact,
ii. T admet une base d'ouverts compacts et est stable par intersections finies,
iii. toute partie fermée irréductible Z de T est l'adhérence d'un point unique $z \in Z$, appelé point générique de Z.

PARTIE IV

CORPS

Soit f un polynôme à coefficients dans un corps K. L'étude de la résolution de l'équation $f = 0$, conduit à considérer non seulement l'ensemble des racines $\alpha_1, \ldots, \alpha_n$ de f mais surtout le corps $K(\alpha_1, \ldots, \alpha_n)$ engendré sur K par l'ensemble des racines de f. Il s'agit alors d'étudier les extensions de corps de degré fini $K \hookrightarrow L$.

17. Extension de corps, degré

Définition-Proposition 17.1. — *Soient K, L deux corps. Un morphisme d'anneaux $f : K \longrightarrow L$ est dit* **morphisme de corps**. *Son noyau* $\ker f \neq (1)$ *est un idéal de K, donc égal à* (0), *ce qui implique que f est injectif. Le morphisme $f : K \hookrightarrow L$ est appelé* **plongement** *ou une* **extension de corps** *et est noté L/K.*

Exemple 17.2. — *Pour des corps K, L fixés, il y a en général plusieurs plongements différents $K \hookrightarrow L$. Par exemple, l'identité et la conjugaison complexe sont deux plongements de $\mathbb{C}$ dans $\mathbb{C}$. En général, le sous-corps $f(K) \subset L$ dépend de f et pas seulement de K et L.*

Tout corps est une extension de $\mathbb{Q}$ ou d'un corps $\mathbb{F}_p$ de cardinal $p > 0$ premier. En effet,

Définition 17.3. — *Soit K un corps. Le noyau de l'application canonique $i : \mathbb{Z} \longrightarrow K$ est un idéal principal* $\ker i \subset \mathbb{Z}$.
Si $\ker i = (0)$, *alors $\mathbb{Z} \subset K$ et* $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q} \subset K$. *Le corps K est dit* **de caractéristique zéro**. *Nous notons* $\mathrm{car} K = 0$.
Si $\ker i = (n)$ *pour $n \geq 1$ alors $n = p$ est un nombre premier (car* $\mathrm{im}\, i \simeq \mathbb{Z}/n\mathbb{Z} \subset K$ *est intègre). Le corps K est dit* **de caractéristique** *p. Nous notons* $\mathrm{car} K = p$. *Dans ce cas, le corps K est un extension du corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

Définition 17.4. — *Une* **base** *de l'extension de corps L/K est une base de L comme K-espace vectoriel. Le* **degré** *de L/K est la dimension $[L : K] = \dim_K(L) \in \mathbb{N} \cup \{\infty\}$. Si $[L : K] < \infty$, l'extension L/K est dite* **finie**.

Exemples 17.5. — *i.* $[\mathbb{C} : \mathbb{R}] = 2$ *et $\{1, i\}$ est une base de $\mathbb{C}/\mathbb{R}$.*
ii. $[\mathbb{C} : \mathbb{Q}] = \infty$,
iii. $[K(X) : K] = \infty$ *pour tout corps K.*

Proposition 17.6. — *(Multiplicativité du degré).*
Soit $K \longrightarrow L \longrightarrow M$ des extensions de corps et $\{\ell_i\}_{i\in I}$ (resp. $\{m_j\}_{j\in J}$) une base de L/K (resp. de M/L). Alors $\{\ell_i m_j\}_{(i,j)\in I\times J}$ est une base de M/K et

$$[M : K] = |I \times J| = |I| \cdot |J| = [L : K][M : L].$$

En particulier, l'extension M/K est finie si et seulement si les extensions L/K et M/L sont finies.

Démonstration. — La famille $S = \{\ell_i m_j\}_{(i,j)\in I\times J}$ engendre M comme K-espace vectoriel et est libre. □

Lemme 17.7. — *Soit K un corps. Soit $f \in K[X]$ un polynôme unitaire irréductible de degré n. Alors $K[x] = K[X]/(f)$ est une extension de degré n de K.*

Démonstration. — Notons x l'image de X dans $K[x] = K[X]/(f)$. L'applicaton

$$\mathrm{ev}_x : K[X] \longrightarrow K[x],\ P \mapsto P(x)$$

est un morphisme surjectif qui envoie f sur 0, donc $f(x) = 0$.
D'après l'algorithme de division euclidienne, nous savons que tout élément g de $K[X]/(f)$ est représenté par un unique polynôme r de degré $< n$. Donc tout élément de $K[x]$ s'écrit de façon unique sous la forme

$$\alpha = g(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},\ \ a_i \in K,$$

forme sous laquelle il convient d'additionner deux éléments. Pour multiplier deux éléments sous cette forme, il suffit de les multiplier et d'utiliser la relation $f(x) = 0$ pour exprimer les termes de degré $\geq n$ en expression de plus bas degré.
Comme f est irréductible et $\deg g \leq n-1$, alors $\mathrm{PGCD}(f, g) = 1$ et il existe $a, b \in K[X]$ tels que $af + bg = 1$. Ainsi $b(x)g(x) = 1$ et $b(x)$ est l'inverse de $g(x)$. □

Exemples 17.8. — *i. Soit $f = X^2+1 \in \mathbb{R}[X]$, alors $\mathbb{R}[x] = \mathbb{R}[X]/(f) = \mathbb{R}[i] = \mathbb{C}$.*
ii. Soit $f = X^2 + X + 1 \in \mathbb{F}_2[X]$. Ce polynôme quadratique n'a pas de racine dans $\mathbb{F}_2[X]$ donc est irréductible. Ainsi $\mathbb{F}_2[X]/(X^2 + X + 1)$ est un corps à 4 élèments : $0, 1, x, x + 1$.
iii. Soit $f = X^3 - 3X - 1 \in \mathbb{Q}[X]$. Si $r \in \mathbb{Q}$ est racine alors $r = \pm 1$ et $f(1) \neq 0$, $f(-1) \neq 0$. Donc f est irréductible. Ainsi $\mathbb{Q}[x]$ est un corps de base $\{1, x, x^2\}$ comme $\mathbb{Q}$-espace vectoriel. Soit

$$\beta = x^4 + 2x^3 + 3 = 3x^2 + 7x + 5 \in \mathbb{Q}[x].$$

L'algorithme d'Euclide donne

$$(X^3 - 3X - 1)(\frac{-7}{37}X + \frac{29}{111}) + (3X^2 + 7X + 5)(\frac{7}{111}X^2 - \frac{26}{111}X + \frac{28}{111}) = 1.$$

Ainsi

$$\beta^{-1} = \frac{7}{111}x^2 - \frac{26}{111}x + \frac{28}{111} \in \mathbb{Q}[x].$$

iv. Le polynôme $f = X^3 - 2 \in \mathbb{Q}[X]$ *a trois racines distinctes* $\alpha_1 = \sqrt[3]{2} \in \mathbb{R}$, $\alpha_2 = \rho\alpha_1$, $\alpha_3 = \rho^2\alpha_1$ *pour* $\rho = e^{2i\pi/3}$.
Les trois corps $\mathbb{Q}(\alpha_i)$ *sont distincts mais ils sont tous les trois isomorphes au corps* $\mathbb{Q}[X]/(X^3 - 2)$ *via l'évaluation* $\overline{\mathrm{ev}}_{\alpha_i}$. *Le corps* $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha_1, \rho)$ *est de degré* $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha_1)][\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 6$.

Définition 17.9. — *Soit* K *un sous-corps d'un corps* L *et* $S \subset L$. *Le sous-anneau* $K[S]$ *de* L *engendré par* K *et* S, *est l'intersection de tous les sous-anneaux de* L *contenant* K *et* S. *Ces éléments s'expriment comme des sommes finies*

$$K[S] = \sum_{(i_1,\dots,i_n)\in\mathbb{N}^n} a_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n}, \quad a_{i_1\cdots i_n} \in F \text{ presque tous nuls }, \alpha_i \in S.$$

L'intersection de tous les sous-corps contenant K *et* S, *est le corps* $K(S)$ *des fractions de* $K[S]$.

Exemples 17.10. — *i. Pour tout* $n \geq 1$ *le polynôme* $X^n - 2 \in \mathbb{Q}[X]$ *est irréductible (d'après le critère d'Eisenstein 5.26). Soit* $\sqrt[n]{2}$ *son unique racine réelle positive. Alors*

$$\mathbb{Q}(\sqrt[n]{2}) = \mathbb{Q}[\sqrt[n]{2}] = \{a_0 + a_1\sqrt[n]{2} + \cdots + a_{n-1}(\sqrt[n]{2})^{n-1} | a_j \in \mathbb{Q}\}$$

est un sous-corps de $\mathbb{R}$ *de degré* $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ *sur* $\mathbb{Q}$.
ii. Si $S = \{\alpha_1, \dots, \alpha_n\}$, *nous notons* $K[S] = F[\alpha_1, \dots, \alpha_n]$ *et* $K(S) = K(\alpha_1, \dots, \alpha_n)$. *L'anneau* $K[S]$ *(resp. le corps* $K(S)$*) est l'ensemble des éléments de* L *qui peuvent s'écrire comme polynômes (resp. fractions rationnelles) en* $\alpha_1, \dots, \alpha_n$. *Une extension de corps* L/K *est dite de* **type fini**, *s'il existe un nombre fini d'éléments* $\alpha_1, \dots, \alpha_n \in L$ *tel que* $L = K(\alpha_1, \dots, \alpha_n)$.
iii. Si $K[S]$ *est un corps, alors* $K[S] = K(S)$.
vi. Si K, K' *sont des sous-corps de* L, *nous notons* $KK' = K(K') = K'(K)$ *le composé de* K *et* K'. *C'est le plus petit sous-corps de* L *qui contient* K *et* K'.
iv. Une extension L *de* K *est dite* **simple** *si* $L = K(\alpha)$ *pour* $\alpha \in L$. *Par exemple* $\mathbb{Q}(\pi)$ *et* $\mathbb{Q}[i]$ *sont des extensions simples de* $\mathbb{Q}$.
v. Soit L/K *une extension de corps et* $\alpha \in L$. *Alors* $K[\alpha]$ *est l'image de l'unique morphisme de* K*-algèbres* $K[X] \longrightarrow L$. *Cependant* $K(\alpha)$ *n'est pas toujours l'image d'un morphisme de corps* $K(X) \longrightarrow L$. *En effet prenons* $K = \mathbb{Q}$, $L = \mathbb{C}$ *et* $\alpha = i$. *Ainsi* $\mathbb{Q}[i] = \mathbb{Q} \oplus i\mathbb{Q}$ *est un corps, donc* $\mathbb{Q}[i] = \mathbb{Q}(i)$ *est un* $\mathbb{Q}$*-espace vectoriel de dimension 2. Cependant* $\mathbb{Q}(X)$ *est de dimension infinie et comme tout morphisme de corps est injectif, il n'y a pas de morphisme de corps* $\mathbb{Q}(X) \longrightarrow \mathbb{Q}(i)$.

18. Extensions algébriques et transcendantes

18.1. Polynôme minimal d'un élément algébrique. —

Définition 18.1. — *Soit L/K une extension de corps. Un élément $\beta \in L$ est dit* **algébrique** *(resp.* **transcendant***) sur K, s'il existe un (resp. il n'existe aucun) polynôme $f \in K[X]$ non nul tel que $f(\beta) = 0$. L'extension L/K est dite* **algébrique** *si tous les éléments de L sont algébriques sur K, sinon elle est dite* **transcendante**.
Si $\beta \in L$ est algébrique sur K, l'ensemble $I = \{g \in K[X] | g(\beta) = 0\}$ est un idéal principal de $K[X]$. Le générateur unitaire de I est dit polynôme minimal de β.

La définition 18.1 ne donne pas de moyen explicite pour déterminer le polynôme minimal d'un élément algébrique. Soit L une extension finie de K. Soit $\alpha_1, \ldots, \alpha_n$ une K-base de L et $\beta \in L$. Soit $M_\beta \in M_n(K)$ la matrice dans la base $\alpha_1, \ldots, \alpha_n$ de l'application K-linéaire

$$L \longrightarrow L, \quad x \mapsto \beta x.$$

Alors le poynôme caractéristique de M_β, $\chi_{L/K,\beta}(X) = \det(X \operatorname{Id} - M_\beta) \in K[X]$ est un polynôme unitaire de degré n annulateur de β indépendant du choix de la base de L/K.

Théorème 18.2. — *Soit L/K une extension finie, $\beta \in L$ et f le polynôme minimal de β sur K. Alors $\chi_{L/K,\beta} = f^{[L:K(\beta)]}$.*

Démonstration. — Soit $\alpha_1, \ldots, \alpha_d$ (resp. $\gamma_1, \ldots, \gamma_r$) une base de $K(\beta)/K$ (resp. de $L/K(\beta)$). La matrice M_β dans la base $\alpha_i\gamma_j$ de L/K est une matrice bloc

$$M_\beta = \begin{pmatrix} \Lambda & 0 & \cdots & 0 \\ 0 & \Lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \Lambda \end{pmatrix},$$

où Λ est la matrice de la multiplication par β dans la base $\alpha_1, \ldots, \alpha_d$ de $K(\beta)/K$. Ainsi

$$\chi_{L/K,\beta} = \chi^r_{K(\beta)/K,\beta}.$$

Par conséquent, le polynôme unitaire $\chi_{K(\beta)/K,\beta}$ de degré $[K(\beta)/K]$ annulateur de β est le polynôme minimal f de β et $\chi_{L/K,\beta} = f^{[L:K(\beta)]}$. □

Définition 18.3. — *Soit L/K une extension de degré $n < \infty$. La* **norme** *et la* **trace** *d'un élément $\beta \in L$ est définie comme*

$$N_{L/K}(\beta) = \det M_\beta \in K, \quad \operatorname{Tr}_{L/K} \beta = \operatorname{Tr}(M_\beta) \in K.$$

Corollaire 18.4. — *Soit L/K une extension finie et $f \in K[X]$ le polynôme minimal de $\alpha \in L$. Notons $\alpha_1, \ldots, \alpha_d$ les racines de f et $r = [L : K(\alpha)]$. Alors*

$$\mathrm{Tr}_{L/K}(\alpha) = r \sum_{i=1}^{d} \alpha_i, \quad N_{L/K}\alpha = (\Pi_{i=1}^{d} \alpha_i)^r.$$

Définition 18.5. — *Soit L une extension du corps K. Le* **degré de transcendance** *$degtr_{L/K}$ de L sur K est le plus petit n tel que L soit une extension algébrique d'un corps $K(x_1, \ldots, x_n)$.*

Exemples 18.6. — *i. Si L/K est algébrique $degtr_{L/K} = 0$.*
ii. Soit L une extension de K, nous appelons base de transcendance de L sur K toute famille d'élements algébriquement indépendants maximale pour l'inclusion. D'après l'axiome de Zorn, il existe une base de transcendance et toutes les bases de transcendance ont le même cardinal, appelé degré de transcendance.

18.2. Extensions algébriques et transcendantes. —

Proposition 18.7. — *Une extension de corps L/K est finie si et seulement si L est algébrique et de type fini sur K.*

Démonstration. — $\Longrightarrow$ Dire que $\alpha \in L$ est transcendant signifie que les éléments $1, \alpha, \alpha^2, \ldots$ sont linéairement indépendants ce qui est exclu si L est fini sur K. Donc L est algébrique sur K. Il reste à montrer que L est de type fini sur K. Le résultat est clair si $L = K$. Sinon il existe $\alpha_1 \in L - K$. Si $L \neq K[\alpha_1]$, il existe $\alpha_2 \in L - K[\alpha_1]$, etc... Comme

$$|K(\alpha_1) : K] < [K(\alpha_1, \alpha_2) : K] < \cdots < [L : K]$$

la construction s'arrête après un nombre fini d'étapes.
$\Longleftarrow$ Soit $L = K(\alpha_1, \ldots, \alpha_n)$ avec α_i algébriques sur K. Comme les extensions $K(\alpha_1)/K$ et $K(\alpha_1, \alpha_2)/K(\alpha_1)$ sont finies (car α_1, α_2 algébriques sur K), l'extension $K(\alpha_1, \alpha_2)/K$ est finie. De même pour L/K par induction. □

Corollaire 18.8. — *i. Si L est algébrique sur K, alors tout sous-anneau A de L contenant K est un corps.*
ii. Si $K \subset E \subset L$, L algébrique sur E et E algébrique sur K, alors L est algébrique sur K.

Démonstration. — i. Si α est algébrique sur K alors $K[\alpha]$ est un corps. Ainsi pour $\alpha \in A - \{0\}$, $K[\alpha] \subset A$ donc α est inversible dans A.
ii. Tout $\alpha \in L$ est racine d'un polynôme unitaire $X^m + a_1 X + \cdots + a_m \in E[X]$. Les extensions $K[a_1, \ldots, a_m, \alpha]/K[a_1, \ldots, a_m]/K$ sont finies. Donc $K[a_1, \ldots, a_m, \alpha]$ est finie (donc algébrique) sur K. □

Définition 18.9. — *Un nombre complexe $\alpha \in \mathbb{C}$ est dit* **algébrique** *(resp.* **transcendant***) s'il est algébrique (resp. transcendant) sur $\mathbb{Q}$.*

Exemples 18.10. — *i. (Lindemann, 1882) π est transcendant.*
ii. (Gelfond, Schneider, 1934) α^β est transcendant si α, β algébriques, $\alpha \neq 0, 1$, $\beta \notin \mathbb{Q}$ (7ième problème de Hilbert).
iii. Nous ne savons pas à ce jour si la constante d'Euler

$$\gamma = \lim_{n\to\infty} \Big(\sum_{k=1}^{n} 1/k - \log n \Big)$$

est transcendante (ni même irrationnelle). De même pour $\pi + e$.
iv. L'ensemble des nombres algébriques de $\mathbb{C}$ sur $\mathbb{Q}$

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} | \alpha \text{ algébrique sur } \mathbb{Q}\}$$

est un sous-corps de $\mathbb{C}$ de degré infini sur $\mathbb{Q}$ (d'après l'exemple i. 17.10).

Proposition 18.11. — *L'ensemble $\overline{\mathbb{Q}}$ des nombres algébriques est dénombrable.*

Démonstration. — La hauteur $h(r)$ d'un nombre rationnel $r \in \mathbb{Q}$ est $\max\{|p|, |q|\}$ pour $r = p/q$ son écriture irréductible. Il n'y a qu'un nombre fini de nombres rationnels de hauteur inférieure à $n \in \mathbb{N}$. Soit $A(n)$ l'ensemble des nombres algébriques dont le polynôme minimal est de degré $\leq n$ et dont les coefficients sont de hauteur $< n$. Alors $A(n)$ est fini pour tout n et la réunion $\cup A(n)$ est dénombrable. □

Définition 18.12. — *Un corps K est dit* **algébriquement clos** *si tout polynôme non constant de $K[X]$ admet une racine dans K.*
Une **clôture algébrique** *de K est une extension algébrique L de K qui est algébriquement close.*

Remarque 18.13. — *La construction d'une clôture algébrique pour tout corps K nécessite le lemme de Zorn.*

Théorème 18.14. — *Le nombre*

$$\alpha = \sum \frac{1}{2^{n!}}$$

est transcendant.

Démonstration. — Supposons que α soit algébrique et notons

$$f = X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbb{Q}[X]$$

son polynôme minimal. Alors $[\mathbb{Q}[\alpha] : \mathbb{Q}] = d$ et il existe $D \in \mathbb{N}^*$ tel que $Df \in \mathbb{Z}[X]$. Posons $\sigma_N = \sum_{n=0}^{N} \frac{1}{2^{n!}}$ et $x_N = f(\sigma_N)$. Comme $\alpha \notin \mathbb{Q}$ et f est irréductible, il n'admet pas de racine dans $\mathbb{Q}$. Donc $x_N = f(\sigma_N) \neq 0$ et $x_N \in \mathbb{Q}$. Nous avons même $(2^{N!})^d D x_N \in \mathbb{Z}$ donc

$$|2^{N!d} D x_N| \geq 1.$$

Le polynôme $f = \Pi_{i=1}^{d}(X - \alpha_i)$, $\alpha_i \in \mathbb{C}$ ($\alpha_1 = \alpha$) est scindé dans $\mathbb{C}[X]$. Donc

$$|x_N| = \Pi_{i=1}^{d} |\sigma_N - \alpha_i| \leq |\sigma_N - \alpha_1| (\sigma_N + M)^{d-1}, \text{ où } M = \max_{i\neq 1}(1, |\alpha_i|).$$

Or

$$|\sigma_N - \alpha_1| = \sum_{n \geq N+1} \frac{1}{2^{n!}} \leq \frac{1}{2^{(N+1)!}} \sum_{n=0}^{\infty} \frac{1}{2^n} = \frac{2}{2^{(N+1)!}}.$$

Donc $|x_N| \leq \frac{2}{2^{(N+1)!}}(\sigma_N + M)^{d-1}$ et

$$|(2^{N!})^d D x_N| \leq 2\frac{2^{N!d} D}{2^{(N+1)!}}(\sigma_N + M)^{d-1}$$

ce qui est absurde car le terme de droite tend vers 0 quand N tend vers $+\infty$. □

19. Corps de décomposition, séparabilité

19.1. Corps de décomposition. — L'objet de ce paragraphe est de définir le corps L engendré par les racines d'un polynôme $f \in K[X]$ donné.

Définition 19.1. — *Soit K un corps et $f \in K[X]$ un polynôme de degré $n \geq 0$. Le corps de décomposition de f sur K est la plus petite (pour l'inclusion) extension L/K telle que f est scindé dans $L[X]$:*

$$f(X) = c(X - \alpha_1) \cdots (X - \alpha_n), \text{ avec } c \in K^*, \alpha_i \in L.$$

Ainsi $L = K(\alpha_1, \ldots, \alpha_n)$.

Exemples 19.2. — *i. Pour $r \in \mathbb{N}^*$, $f \in K[X]$, les corps de décomposition de f et de f^r coïncident.*
ii. Si f a $\deg(f) - 1$ racines dans E alors il est scindé dans $E[X]$.
iii. Soit $f = aX^2 + bX + c \in \mathbb{Q}[X]$ et $\alpha = (b^2 - 4ac)^{1/2}$. Alors le sous-corps $\mathbb{Q}[\alpha]$ de $\mathbb{C}$ est le corps de décomposition de f.

La proposition suivante montre l'existence et l'unicité du corps de décomposition (à isomorphisme près).

Proposition 19.3. — *Tout polynôme $f \in K[X]$ de degré $n \geq 1$ admet un corps de décomposition K_f et $[K_f : K] \leq n!$. Deux corps de décomposition sont isomorphes comme K-algèbres.*

Démonstration. — Soit f_1 un facteur irréductible unitaire de f et $K_1 = K[\alpha_1] = K[X]/(f_1)$. Alors $f(\alpha_1) = 0$ et nous posons $K_2 = K_1[\alpha_2]$ le quotient de $K_1[X]$ par un facteur irréductible unitaire de $f/(X - \alpha_1)$ de $K_1[X]$. Par induction, nous obtenons un corps de décomposition K_f.
Nous avons $[K_1 : K] = \deg f_1 \leq n, [K_2 : K_1] \leq n - 1, \ldots$ donc $[K_f : K] \leq n!$.
Soient L/K et L'/K deux corps de décomposition de f sur K. Soit $g \in K[X]$ un facteur irréductible de f. Par conséquent g est scindé sur L et L' donc il existe $\alpha \in L$ et $\alpha' \in L'$ tels que $g(\alpha) = 0$ et $g(\alpha') = 0$. Les évaluations ev_α et $\mathrm{ev}_{\alpha'}$ induisent des isomorphismes de K-algèbres :

$$\overline{\mathrm{ev}}_\alpha : K[X]/(g) \xrightarrow{\simeq} K(\alpha) = K_1 \subset L, \quad \overline{\mathrm{ev}}_{\alpha'} : K[X]/(g) \xrightarrow{\simeq} K(\alpha') = K_1' \subset L'$$

et $\sigma = \overline{\mathrm{ev}}_{\alpha'} \circ \overline{\mathrm{ev}}_{\alpha}^{-1} : K_1 \xrightarrow{\simeq} K_1'$. Nous pouvons alors considérer K_1 comme sous-corps de L et L' (via σ et l'inclusion) et écrire $f = (X - \alpha)f_1$ pour $f_1 \in K_1[X]$ et L, L' des corps de décomposition de f_1 sur K_1. Par induction en remplaçant (K, f) par (K_1, f_1), nous obtenons des tours d'extensions simples

$$K = K_0 \subset K_1 = K(\alpha_1) \subset \cdots \subset K_{i-1} \subset K_i = K_{i-1}(\alpha_i) = K(\alpha_1, \ldots, \alpha_i)$$

$$\subset \cdots \subset K_n = K(\alpha_1, \ldots, \alpha_n) \subset L$$

$$K = K_0 \subset K_1' = K(\alpha_1') \subset \cdots \subset K_{i-1}' \subset K_i' = K_{i-1}'(\alpha_i') = K(\alpha_1', \ldots, \alpha_i')$$

$$\subset \cdots \subset K_n' = K(\alpha_1', \ldots, \alpha_n') \subset L'$$

telles que $f = c(X - \alpha_1) \cdots (X - \alpha_n) \in K_n[X]$ et $f = c(X - \alpha_1') \cdots (X - \alpha_n') \in K_n'[X]$, (donc $L = K_n$ et $L' = K_n'$) et des isomorphismes de corps $\sigma_i : K_i \xrightarrow{\simeq} K_i'$ tels que $\sigma_{i|K_{i-1}} = \sigma_{i-1}$. Ainsi $\sigma_n : L \xrightarrow{\simeq} L'$ est un isomorphisme de K-algèbres. □

19.2. Exensions séparables, corps parfaits. — La proposition suivante permet de définir la notion de PGCD de deux polynômes sans référence au corps de base.

Théorème 19.4. — *Soit $f, g \in K[X]$ et L une extension de K. Soit le* PGCD *de f et g dans $K[X]$ coïncide avec le* PGCD *de f et g dans $L[X]$.*

Démonstration. — Soit $h_K = \mathrm{PGCD}(g, f) \in K[X]$ et $h_L = \mathrm{PGCD}(g, f) \in L[X]$. Nous avons h_K divise h_L. De plus d'après Bézout, il existe $a, b \in K[X]$ avec $af + bg = h_K$ donc h_L divise h_K. □

Définition 19.5. — *Soit $f \in K[X]$. Il existe une extension L de K dans laquelle f est scindé :*

$$f = a\Pi_{i=1}^{r}(X - \alpha_i)^{m_i}, \alpha_i \text{ distincts}, \quad m_i \geq 1, \sum_{i=1}^{r} m_i = \deg(f)$$

Nous disons que α_i est **racine** *de f de multiplicité m_i. Si $m_i > 1$, α_i est dit* **racine multiple**. *Sinon α_i est une* **racine simple**.
Nous disons que f est à racines multiples si au moins un des $m_i > 1$. Nous disons que f est à racines simples si tous les $m_i = 1$.

Exemple 19.6. — *Soit $K = \mathbb{F}_p(t)$. Alors le polynôme $X^p - t$ est irréductible dans $K[X]$. Dans le corps de décomposition, $X^p - t = (X - a)^p$. Donc un polynôme irréductible peut avoir des racines multiples.*

Définition 19.7. — *Soit $f = \sum_{i=0}^{n} a_i X^i \in K[X]$. Le polynôme dérivé de f est $f' = \sum_{i=1}^{n} i a_i X^{i-1} \in K[X]$.*

Proposition 19.8. — *Soit $f \in K[X]$ un polynôme irréductible non constant. Les propriétés suivantes sont équivalentes :*
i. f a une racine multiple,
ii. $\mathrm{PGCD}(f, f') \neq 1$,
iii. $\mathrm{car}K = p > 0$ *et f est un polynôme en X^p,*
iv. Toutes les racines de f sont multiples.

Démonstration. — i.$\Longrightarrow$ ii. Soit α une racine multiple de f. Alors $f = (X - \alpha)^m g(X)$, $m > 1$ dans le corps de décomposition de f. Donc

$$f'(X) = m(X - \alpha)^{m-1} g(X) + (X - \alpha)^m g'(X).$$

Donc f et f' ont $X - \alpha$ comme facteur commun.
ii$\Longrightarrow$ iii. Comme f est irréductible et $\deg(f') < \deg(f)$, $\mathrm{PGCD}(f, f') \neq 1$ implique que $f' = 0$. Mais comme f n'est pas constant, f' ne peut être nul que si K est de caractéristique $p > 0$ et f est un polynôme en X^p.
iii.$\Longrightarrow$ iv. Supposons $f(X) = g(X^p)$ et écrivons $g(X) = \Pi_i (X - \alpha_i)^{m_i}$ dans le corps de décomposition de f. Alors

$$f(X) = g(X^p) = \Pi_i (X^p - \alpha_i)^{m_i} = \Pi_i (X - a_i)^{pm_i}$$

avec $\alpha_i = a_i^p$. Donc toutes les racines de f sont à multiplicité au moins p.
iv.$\Longrightarrow$ i. est clair. □

Définition 19.9. — *Un polynôme est* **séparable** *s'il n'a que des racines simples (dans son corps de décomposition).*
Un corps K est **parfait** *si tout polynôme irréductible de $K[X]$ est séparable. L'extension L/K est dite* **séparable** *si pour tout $x \in L$, le polynôme minimal de x, $\mu_x \in K[X]$ est séparable.*

Exemples 19.10. — *i. Si la caractéristique de K est nulle, alors K est parfait (car un polynôme irréductible P est premier à P').*
ii. Si k est fini, k est parfait. En effet notons $p = \mathrm{cark}$. Soit $f(X) = \sum_{j=0}^{m} b_j X^j \in k[X]$ un polynôme irréductible inséparable. Le morphisme de Frobenius

$$\varphi : k \to k, x \mapsto x^p$$

est bijectif (car injectif) donc surjectif et il existe $a_j \in k$ avec $b_j = a_j^p$. Alors $f(X) = (\sum_j a_j X^j)^p$ qui n'est pas irréductible.
iii. Si K est algébriquement clos, alors K est parfait (même raisonnement en caractéristique $p > 0$ qu'au ii.).

Exemple 19.11. — *Soit F un corps de caractéristique $p > 0$ et $a \in F - F^p$ un élément de F qui n'est pas une racine p-ième. Alors le polynôme $f = X^{p^n} - a \in F[X]$, $n \geq 1$ est irréductible. Si α est une racine de f, alors $f(X) = (X - \alpha)^{p^n} \in F[\alpha][X]$. L'extension $F[\alpha]/F$ n'est pas séparable et $[F[\alpha] : F] = p^n$.*
En effet, pour $n = 1$, si $g \in F[X]$ est un polynôme non constant qui divise f, alors $g = (X - \alpha)^m = X^m - m\alpha X^{m-1} + \cdots$ pour $m \leq p$. Si $m < p$ alors $m \in F^*$ et $\alpha \in F$. Donc $a = \alpha^p \in F^p$, ce qui est exclu. Donc $m = p$ et f est irréductible.

Pour $n \geq 1$, nous posons $a_i = \alpha^{p^{n-i}}$ $(0 \leq i \leq n)$ et $F_i = F(a_i)$. Puis nous concluons par induction en utilisant le cas $n = 1$.

Proposition 19.12. — *Un corps F est parfait si et seulement si*
i. F est de caractéristique nulle, ou
ii. $\mathrm{car} F = p > 0$ *et tout élément de F est une puissance p-ième, i.e. le morphisme de Frobenius*

$$\varphi : F \longrightarrow F, x \mapsto x^p$$

est surjectif.

Démonstration. — Le cas i. est clair. Supposons que $\mathrm{car} F = p > 0$. Si F contient un élément a qui n'est pas une puissance p-ième, alors $X^p - a$ est irréductible non séparable. Réciproquement si tout élément de F est une racine p-ième. Alors tout polynôme en X^p :

$$\sum_{i=0}^{n} a_i X^{ip} = (\sum_{i=0}^{n} b_i X^i)^p \text{ pour } a_i = b_i^p$$

donc n'est pas irréductible. □

Exemples 19.13. — *i. Un corps qui est une union de corps parfaits est parfait. Donc tout corps algébrique sur $\mathbb{F}_p$ est parfait.*
ii. Si $\mathrm{car} F = p > 0$ *alors le corps $F(X)$ n'est pas parfait car X n'est pas une puissance p-ième.*

Théorème 19.14. — *(Théorème de l'élément primitif). Soit F un corps et $E = F(\alpha, \beta_1, \ldots, \beta_n)$ une extension finie de F. Si les éléments $\beta_1, \ldots, \beta_n$ sont séparables sur F alors il existe un élément primitif $\gamma \in E$, i.e. tel que $E = F(\gamma)$.*

Démonstration. — Si F est fini alors $E = F(\gamma)$ pour γ générateur du groupe cyclique E^*. Supposons $|F| = \infty$. Par induction, il suffit de supposer $E = F(\alpha, \beta)$ avec β séparable sur F. Notons f (resp. g) le polynôme minimal de α (resp. β). Nous avons

$$f(X) = \Pi_{i=1}^{m}(X - a_i), \quad g(X) = \Pi_{j=1}^{n}(X - b_j)$$

avec a_i, b_j dans le corps de décomposition de fg et $a_1 = \alpha$, $b_1 = \beta$, les racines de g étant distinctes.
Nous cherchons $t \in F$ pour lequel $\gamma = \alpha + t\beta \in E$ satisfait $E = F(\gamma)$. Le polynôme $h(X) = f(\gamma - tX) \in F(\gamma)[X]$ a pour racines $(\gamma - a_i)/t = \beta + (\alpha - a_i)/t$. Comme F est infini et $\beta - \beta_j \neq 0$ pour $j > 1$, nous pouvons choisir $t \in F$ tel que $t(\beta - \beta_j) \neq a_i - \alpha$ pour tout $1 \leq i \leq m$ et $2 \leq j \leq n$. Ainsi la seule racine commune de g et h est β avec multiplicité 1. Les deux polynômes g, h sont à coefficients dans $F(\gamma)$ et donc $\mathrm{PGCD}(g, h) = X - \beta$ est à coefficients dans $F(\gamma)$ et $\beta \in F(\gamma)$. Par conséquent $\alpha = \gamma - t\beta \in F(\gamma)$ et $E = F(\alpha, \beta) = F(\gamma)$. □

Corollaire 19.15. — *Soit E/F une extension de corps finie séparable. L'application*

$$E \times E \longrightarrow F, (\beta, \beta') \mapsto \mathrm{Tr}_{E/F}(\beta\beta')$$

est une forme bilinéaire symétrique non dégénérée sur le F-espace vectoriel E.

Démonstration. — L'extension finie séparable E/F est simple $E = F(\alpha)$. Nous notons $f \in F[X]$ le polynôme minimal de α, $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ ses $n = [E : F]$ racines distinctes et $1, \alpha, \cdots, \alpha^{n-1}$ est une base du F-espace vectoriel E.
La matrice M_α de la multiplication par α a pour polynôme caractéristique f, donc elle est diagonalisable à valeurs propres les α_i, $1 \leq i \leq n$. Par conséquent pour $1 \leq i, j \leq n$,

$$\mathrm{Tr}_{E/F}(\alpha^i\alpha^j) = \mathrm{Tr}\, A_\alpha^{i+j} = \sum_{k=1}^{n} \alpha_k^{i+j} \text{ et } \det \mathrm{Tr}_{E/F}(\alpha^i\alpha^j) = \det B^t B = (\det B)^2$$

où $B = (\alpha_k^i)_{1\leq i,k\leq n}$ est de déterminant non nul (matrice de Vandermonde). Donc $\det \mathrm{Tr}_{E/F}(\alpha^i\alpha^j) \neq 0$ et la trace $\mathrm{Tr}_{E/F}$ est non dégénérée. □

Théorème 19.16. — *Soit $F \subset E$ une extension finie. Il existe $\gamma \in E$ tel que $E = F(\gamma)$ si et seulement si il n'existe qu'un nombre fini de corps intermédiaires $F \subset M \subset E$.*

Démonstration. — La proposition est claire si F est un corps fini. Nous supposons dorénavant que F est infini.
$\Longrightarrow$ Soit $\mu \in F[X]$ le polynôme minimal de γ et M un corps intermédiaire $F \subset M \subset E$. Notons $\mu_M \in M[X]$ le polynôme minimal de γ dans M et $M' \subset M$ le sous-corps de M engendré sur F par les coefficients de μ_M. Comme le polynôme $\mu_M \in M[X]$ est irréductible sur M, il est irréductible sur M'. Donc $[E : M] = [M[\gamma] : M] = \deg \mu_M = [M'[\gamma] : M'] = [E : M']$, donc $M = M'$. Il n'y a qu'un nombre fini de possibilité pour μ_M (car il divise μ). D'où la finitude des extensions intermédiaires.
$\Longleftarrow$ L'extension E/F est de type fini, donc $E = F(\alpha_1, \ldots, \alpha_n)$. Par induction, il suffit de montrer que pour tous $\alpha, \beta \in E$, il existe $\gamma \in E$ tel que $F(\alpha, \beta) = F(\gamma)$. Le corps F est infini, mais il n'existe qu'un nombre fini d'extensions intermédiaires $F \subset F(\alpha + t\beta) \subset E$, pour $t \in F$. Donc il existe $t \neq t'$ tels que $F(\alpha + t\beta) = F(\alpha + t'\beta) = M$. Par conséquent $(t - t')\beta \in M$ donc $\beta, \alpha \in M$ et $F(\alpha, \beta) = M = F(\alpha + t\beta)$. □

Corollaire 19.17. — *Soit E/F une extension finie.*
Si E/F est séparable, alors pour toute extension F'/F, $L \otimes_F F'$ est un anneau réduit. C'est un produit fini d'extensions finies de F'.

Démonstration. — Soit $\gamma \in E$ tel que $E = F[\gamma]$. Notons $\mu \in F[X]$ le polynôme minimal de γ. Ainsi $E \simeq F[X]/(\mu)$. Soit F'/F une extension de F et $\mu = \Pi_i \mu_i$

la décomposition de μ en polynômes irréductibles sur $F'[X]$. Ainsi

$$E \otimes_F F' = (F[X] \otimes_F F')/(\mu \otimes 1) = F'[X]/(\mu) \simeq \Pi_i F'[X]/(\mu_i).$$

□

20. Corps finis

20.1. Existence et unicité. — La proposition suivante permet de décrire tous les corps finis à isomorphisme près.

Proposition 20.1. — *i. Un corps F est fini si et seulement si* $\mathrm{car}F = p > 0$ *et* $[F : \mathbb{F}_p] = n < \infty$. *Dans ce cas* $|F| = p^n = q$ *et les éléments de* F^* *(resp. de* F*) sont les racines du polynôme* $X^{q-1} - 1 \in \mathbb{F}_p[X]$ *(resp.* $X^q - X \in \mathbb{F}_p[X]$*).*
ii. Pour tout $n \geq 1$*, le polynôme* $X^{p^n} - X \in \mathbb{F}_p[X]$ *a des racines simples.*
iii. Si F est un corps à $|F| = p^n = q$ *éléments, alors F est le corps de décomposition du polynôme* $X^{p^n} - X$ *sur* $\mathbb{F}_p$. *En particulier, il est unique à isomorphisme près. Nous le notons* $\mathbb{F}_q$.
iv. Si $f \in \mathbb{F}_p[X]$ *est un polynôme irréductible de degré* $n \geq 1$ *alors* $F = \mathbb{F}_p[X]/(f)$ *est un corps à* p^n *éléments et le polynôme f divise* $X^{p^n} - X$ *dans* $\mathbb{F}_p[X]$.
v. Tout corps fini est isomorphe à un corps obtenu par la construction iv.

Démonstration. — i. Si $\mathrm{car}F = p > 0$ et $[F : \mathbb{F}_p] = n < \infty$, alors F est isomorphe à $\mathbb{F}_p^n$ comme $\mathbb{F}_p$ espace vectoriel, donc $|F| = p^n$. Si $\mathrm{car}F = p > 0$ et $[F : \mathbb{F}_p] = \infty$ alors F contient un $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_p^n$ de dimension n pour tout $n \geq 1$ donc $|F| = \infty$.
Si $|F| = q < \infty$, alors F^* est un groupe fini d'ordre $q-1$. Donc pour tout $a \in F^*$, $a^{q-1} = 1$ (et $a^q = a$). Si $a \in F - F^*$ alors $a = 0$ et $a^q = a$ est encore vérifié.
ii. Le polynôme $g(X) = X^{p^n} - X \in \mathbb{F}_p[X]$ a pour dérivée $g'(X) = -1 \in \mathbb{F}_p[X]$, donc $\mathrm{PGCD}(g, g') = 1$ et g n'a que des racines simples.
iii. D'après i. et ii., les éléments de F sont les p^n racines distinctes de $g(X) = X^{p^n} - X \in \mathbb{F}_p[X]$ dans son corps de décomposition E sur $\mathbb{F}_p$. Comme le corps E est engendré sur $\mathbb{F}_p$ par ces racines, $E = F$.
iv. Notons x l'image de X dans $F = \mathbb{F}_p[X]/(f)$. Alors $x^{p^n} - x = 0$ donc $f|(X^{p^n} - X)$.
v. Le groupe F^* est cyclique d'ordre $q - 1$. Soit α un générateur. Alors $F = \mathbb{F}_p[\alpha] \xrightarrow{\simeq} \mathbb{F}_p[X]/(f)$ où $f \in \mathbb{F}_p[X]$ est le polynôme minimal de α sur $\mathbb{F}_p$. □

Définition 20.2. — *Soit p un nombre premier et A une* $\mathbb{F}_p$*-algèbre (i.e.* $p \cdot 1 = 0$ *dans A). Alors*

$$\varphi : A \longrightarrow A, \varphi(x) = x^p$$

définit un morphisme de $\mathbb{F}_p$*-algèbre (*$\varphi(1) = 1$, $\varphi(xy) = \varphi(x)\varphi(y)$, $\varphi(x - y) = \varphi(x) - \varphi(y)$, $\varphi(a) = a$, $x, y \in A, a \in \mathbb{F}_p$*) dit* **morphisme de Frobenius**.
Pour $n \geq 1$ *et* $q = p^n$*, nous notons* $\varphi_q = \varphi^n : A \longrightarrow A, x \mapsto x^q$.

La proposition suivante donne l'existence d'un corps fini à p^n éléments pour tout p premier et $n \geq 1$.

Proposition 20.3. — *Soit p un nombre premier, E le corps de décomposition sur $\mathbb{F}_p$ de $g = X^q - X \in \mathbb{F}_p[X]$. Alors $E^{\varphi_q} = \{a \in E | (\varphi_q - \mathrm{Id})(a) = 0\} = E$ est un corps à q éléments.*

Démonstration. — Soit $x, y \in E^{\varphi_q}$ alors $\varphi_q(x \pm y) = \varphi_q(x) \pm \varphi_q(y)$, $\varphi_q(xy) = \varphi_q(x)\varphi_q(y)$ et si $y \neq 0$ $\varphi_q(x/y) = \varphi_q(x)/\varphi_q(y)$ car $\varphi_q : E \longrightarrow E$ est un morphisme de corps. Donc E^{φ_q} est un sous-corps de E. Par définition, ses éléments sont les racines de g contenues dans E. Comme g est un polynôme de degré q à racines simples, il admet exactement q racines distinctes dans son corps de décomposition E. Donc $|E^{\varphi_q}| = q$ est le corps de décomposition de g et $E = E^{\varphi_q}$. □

Théorème 20.4. — *Soit p un nombre premier et $n \geq 1$.*
i. Il existe un unique (à isomorphisme près) corps à p^n éléments. Nous le notons $\mathbb{F}_{p^n}$.
ii. Soit $m, n, r \in \mathbb{N}^*$ et $q = p^r$. Il existe un morphisme de corps $\sigma : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^n}$ si et seulement si $m|n$.

Démonstration. — ii. Si $m|n$ alors $q^m - 1$ divise $q^n - 1$ et le polynôme $X^{q^m} - X$ divise $X^{q^n} - X$. Donc le corps de décomposition de $X^{q^n} - X$ contient le corps de décomposition de $X^{q^m} - X$. Réciproquement s'il existe un plongement $\sigma : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^n}$, alors $K = \sigma(\mathbb{F}_{q^m})$ est un sous-corps de $\mathbb{F}_{q^n}$ et $q^n = q^{md}$ avec $d = [\mathbb{F}_{q^n} : K]$, donc $n = md$. □

Nous en déduisons le corollaire suivant :

Corollaire 20.5. — *Soit p un nombre premier, $r \geq 1$, $q = p^r$.*
i. Si $f \in \mathbb{F}_q[X]$ est un polynôme irréductible de degré $m \geq 1$, alors f divise $X^{q^n} - X$ dans $\mathbb{F}_q[X]$ si et seulement si $m|n$.
ii. Pour $m \geq 1$, nous notons A_m^q l'ensemble des polynômes unitaires irréductibles $f \in \mathbb{F}_q[X]$ de degré m. Alors l'ensemble A_m^q n'est pas vide et

$$\forall n \geq 1, X^{q^n} - X = \Pi_{m|n} \Pi_{f \in A_m^q} f, \quad q^n = \sum_{m|n} m|A_m^q|.$$

Exemples 20.6. — *i. Nous avons la décomposition $X^4 - X = X(X-1)(X^2 + X + 1) \in \mathbb{F}_2[X]$ et $\mathbb{F}_2[X]/(X^2 + X + 1) = \mathbb{F}_4$.*
ii. Soit $f \in \mathbb{F}_q[X]$ unitaire non constant sans racine multiple avec $f = f_1 \cdots f_r$ sa décomposition en polynômes unitaires irréductibles de $\mathbb{F}_q[X]$. Alors

$$\varphi_q - \mathrm{Id} : \mathbb{F}_q[X]/(f) \longrightarrow \mathbb{F}_q[X]/(f), \overline{h} \mapsto \overline{h^q - h}$$

est $\mathbb{F}_q$-linéaire, $\dim_{\mathbb{F}_q} \mathrm{Ker}(\varphi_q - \mathrm{Id}) = r$ et (f est irréductible) si et seulement si $\mathrm{Ker}(\varphi_q - \mathrm{Id}) = \mathbb{F}_q$. En effet d'après le théorème des restes chinois (§2.2):

$$\mathbb{F}_q[X]/(f) \xrightarrow{\simeq} \mathbb{F}_q[X]/(f_1) \times \cdots \times \mathbb{F}_q[X]/(f_r) = \mathbb{F}_{q^{d_1}} \times \cdots \times \mathbb{F}_{q^{d_k}}$$

$$(\mathbb{F}_q[X]/(f))^{\varphi_q-1} \longrightarrow (\mathbb{F}_{q^{d_1}})^{\varphi_q-1} \times \cdots \times (\mathbb{F}_{q^{d_k}})^{\varphi_q-1} = \Pi_{i=1}^r \mathbb{F}_q.$$

iii. Algorithme de Berlekamp. Soit $f \in \mathbb{F}_q[X]$ un polynôme unitaire de degré $n \geq 1$ sans racine multiple. Soit $B \in M_n(\mathbb{F}_q)$ la matrice de l'application $\mathbb{F}_q$-linéaire

$$\varphi_q - \mathrm{Id} : \mathbb{F}_q[X]/(f) \longrightarrow \mathbb{F}_q[X]/(f)$$

dans la base $1, \overline{X}, \cdots, \overline{X}^{n-1}$. Si l'espace des solutions $\{u \in \mathbb{F}_q^n | Bu = 0\} = \mathbb{F}_q e_1$, alors f est irréductible dans $\mathbb{F}_q[X]$. Sinon il existe une autre solution $u \in \mathbb{F}_q^n$ correspondant à un polynôme non constant $h \in \mathbb{F}_q[X]$ de degré $< n$ tel que $h^q - h = 0 \mod (f)$. Autrement dit $f | h^q - h = \Pi_{a \in \mathbb{F}_q}(h - a)$. Les polynômes $h - a$ $(a \in \mathbb{F}_q)$ sont deux à deux premiers entre eux et vérifient $\deg(h - a) < f$. D'où la factorisation

$$f = \Pi_{a \in \mathbb{F}_q} h_a, \quad h_a = \mathrm{PGCD}(f, h - a), \quad \deg h_a < \deg f.$$

iv. Notons $\mu : \mathbb{N}^* \longrightarrow \{0, 1, -1\}$ la fonction de Möbius :

$$\mu(1) = 1, \mu(n) = 0 \text{ si } n \text{ a un facteur carré, } \mu(p_1 \cdots p_r) = (-1)^r$$

si $p_1, \ldots, p_r$ sont des nombres premiers distincts. Notons $|A_m^q|$ le nombre de polynômes irréductibles unitaires de degré m dans $\mathbb{F}_q[X]$, alors

$$|A_m^q| = \frac{1}{m} \sum_{d|m} \mu(m/d) q^d.$$

Corollaire 20.7. — *Tout polynôme unitaire irréductible $f \in \mathbb{F}_p[X]$ de degré $d|n$ apparait comme facteur de multiplicité 1 de $X^{p^n} - X$. En particulier le degré du corps de décomposition de f est d.*

Démonstration. — Les facteurs de $X^{p^n} - X$ sont distincts car il n'a pas de terme commun avec sa dérivée. Si f est irréductible de degré d, alors f a un racine dans un corps de degré d sur $\mathbb{F}_p$. Mais le corps de décomposition de $X^{p^n} - X$ contient une copie de chaque corps de degré d sur $\mathbb{F}_p$ avec $d|n$. Donc $f | X^{p^n} - X$. En particulier $f | X^{p^d} - X$ donc est scindé dans le corps de décomposition de $X^{p^d} - X$ qui est de degré d sur $\mathbb{F}_p$. □

Proposition 20.8. — *Le corps $\mathbb{F}_p$ admet pour clôture algébrique $\mathbb{F} = \cup_{i \geq 1} \mathbb{F}_{p^{i!}}$.*

Démonstration. — Le corps $\mathbb{F}$ réunion d'extensions algébriques croissantes de $\mathbb{F}_p$ est algébrique sur $\mathbb{F}_p$. Tout polynôme de $\mathbb{F}_p[X]$ est scindé dans $\mathbb{F}$ donc $\mathbb{F}$ est une clôture algébrique de $\mathbb{F}_p$. □

20.2. Codes linéaires, distance de Hamming. —

Définition 20.9. — *Soit $q = p^r$, $\mathbb{F}_q^k$, $\mathbb{F}_q^n$ deux espaces vectoriels sur $\mathbb{F}_q$. Un* **codage** *est une application injective $E : \mathbb{F}_q^k \to \mathbb{F}_q^n$. L'image $C = E(\mathbb{F}_q^k) \subset \mathbb{F}_q^n$ est dite* **code**. *Un* **décodage** *est une fonction $D : \mathbb{F}_q^n \to \mathbb{F}_q^k$ telle que $D \circ E$ est l'identité de $\mathbb{F}_q^k$.*

Nous ne nous interessons ici qu'aux codes linéaires, i.e. pour lesquels E est une application linéaire. Ainsi C est un sous-espace vectoriel de $\mathbb{F}_q^n$. La matrice G de E dans les bases canoniques est dite matrice génératrice correspondant à E.

Définition 20.10. — *Un* **code linéaire**, *étant un sous-espace vectoriel de dimension r de $\mathbb{F}_q^n$ peut également être défini comme le noyau d'un système linéaire, donc par une matrice H de taille $(n-r)\times n$, dite* **matrice de vérification**. *Ainsi $xH = 0$, pour tout $x \in C$.*

Exemple 20.11. — *Soit C le code linéaire défini par $E : \mathbb{F}_2^2 \to \mathbb{F}_2^4$ avec*

$$G = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Alors $C = \{(0,0,0,0),(1,0,1,0),(1,1,1,1),(0,1,0,1)\}$. Ce code admet la matrice de vérification :

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

Nous définissons une distance sur les codes :

Définition 20.12. — *La* **distance de Hamming** *sur $\mathbb{F}_q^n$ est définie par*

$$\forall x, y \in \mathbb{F}_q^n, d(x,y) = |\{i, 1 \leq i \leq n, x_i \neq y_i\}|$$

Cette distance permet de déterminer combien d'erreurs sont admissibles dans la transmission d'un code au sens suivant :

Proposition 20.13. — *Soit C un code de distance minimum $d = \min\{d(x,y), x \neq y \in C\}$. Alors toute erreur de $d-1$ termes peut être détectée. De plus si $d \geq 2t+2$ toute erreur de $t \geq 1$ termes peut être corrigée par la fonction de décodage du plus proche voisin.*

Démonstration. — Si pour tout $x \neq y \in C$, $d(x,y) \geq d$, une erreur de transmission sur au plus $d-1$ termes pourra être détectée.
De plus si $d \geq 2t+1 \geq 3$ alors $d(x,z)+d(z,y) \geq d(x,y) \geq 2t+1$. Ainsi $d(x,z) > t$ ou $d(y,z) > t$. Or $\{y \in C, d(y,x) \leq t\} = \{x\}$, donc $D(x) = E^{-1}(c)$ où $c \in C$ minimise $d(x,c)$. □

20.3. Codes cycliques. —

Définition 20.14. — *Un* **code cyclique** *est un code linéaire $C \subset \mathbb{F}_q^n$ tel que C est stable par permutations des composantes dans $\mathbb{F}_q^n$.*

Cette définition est motivée par l'isomorphisme

$$\mathbb{F}_q^n \to A = \mathbb{F}_q[x]/(x^n - 1), \quad (a_0, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

Un code cyclique définie donc un sous-ensemble de polynômes de degré $n-1$ stable par multiplication par x dans A.

Proposition 20.15. — *Soit $A = \mathbb{F}_q[x]/(x^n - 1)$.*
i. Un sous-espace $C \subset A$ est un code cyclique si et seulement si C est un idéal de A.
ii. Les idéaux de A sont principaux engendrés par un diviseur g de $x^n - 1$.

Démonstration. — i. Un sous-espace vectoriel de A stable par multiplication par x est stable par mulplication par tout $h(x) \in A$.
ii. Les idéaux de A sont en bijection avec les idéaux de $\mathbb{F}_q[x]$ contenant $x^n - 1$. □

Définition 20.16. — *Soit $A = \mathbb{F}_q[X_1, \ldots, X_m]/(X_1^{n_1} - 1, \ldots, X_m^{n_m} - 1)$. Nous appellons code cyclique de dimension m tout idéal I de A.*

L'isomorphisme $A = \mathbb{F}_q[X_1, \ldots, X_m]/(X_1^{n_1} - 1, \ldots, X_m^{n_m} - 1) \sim \mathbb{F}_q^{n_1 \cdot n_2 \cdots n_m}$ permet de définir les codes cycliques de dimension m via un système de générateurs $\{\overline{f_1}, \ldots, \overline{f_s}\}$ d'un idéal I de A. L'idéal correspondant J dans $\mathbb{F}_q[X_1, \ldots, X_m]$ est

$$J = (f_1, \ldots, f_s) + (X_1^{n_1} - 1, \ldots, X_m^{n_m} - 1).$$

Définition 20.17. — *Soit $J \subset \mathbb{F}_q[X_1, \ldots, X_m]$ un idéal. Nous appelons* **monôme standard**, *les monômes non inclus dans $< \mathrm{LT}(J) >$.*

Théorème 20.18. — *Soit $I \subset A = \mathbb{F}_q[X_1, \ldots, X_m]/(X_1^{n_1} - 1, \ldots, X_m^{n_m} - 1)$ un code cyclique de dimension m et G une base de Gröbner pour l'idéal associé $J \subset \mathbb{F}_q[X_1, \ldots, X_m]$ pour un ordre monomial fixé. Le codage E de I est donné par :*
Input : Base de Gröbner G pour J
w une combinaison linéaire de monômes non standard
Output : $E(w) \in C$
$\overline{w} := \overline{w}^G$
$E(w) := w - \overline{w}$

Démonstration. — Soit w une combinaison linéaire de monômes non standard. Ainsi $\overline{w}^G$ est une combinaison linéaire de monômes non standard dont les symboles de w ne sont pas changés dans le calcul de $E(w) = w - \overline{w}$. Montrons que $E(w) \in I$. Ainsi $I = J/ < X_1^{n_1} - 1, \ldots, X_m^{n_m} - 1 >$ et

$$A/I \cong \mathbb{F}_q[X_1, \ldots, X_m]/J.$$

donc $h(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ représente un élément de I dans A ssi $\overline{h}^G = 0$. □

21. Théorie de Galois

21.1. Groupe d'automorphismes d'un corps. —

Définition 21.1. — *Soit une extension E/F. Un F-isomorphisme $E \longrightarrow E$ est dit F-automorphisme de E. Les F-automorphismes de E forment un groupe, noté* $\mathrm{Aut}(E/F)$.

Exemples 21.2. — *i. Il existe une infinité non dénombrable d'éléments de* $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. *L'identité et la conjugaison en sont deux particuliers.*
ii. Soit $E = \mathbb{C}(X)$. Un automorphisme de E envoie X sur un autre générateur de E sur $\mathbb{C}$. Nous verrons qu'il s'agit des éléments $\frac{aX+b}{cX+d}$, $ad - bc \neq 0$. Donc $\mathrm{Aut}(\mathbb{C}(X)/\mathbb{C}) \simeq \mathrm{PGL}_2(\mathbb{C})$ *(Théorème 21.10).*
iii. Nous ne savons pas décrire le groupe de Cremona $\mathrm{Aut}(\mathbb{C}(X_1, \ldots, X_n)/\mathbb{C})$ *pour $n \geq 3$.*

Lemme 21.3. — *Si F_f est le corps de décomposition d'un polynôme $f \in F[X]$ séparable, alors* $\mathrm{Aut}(F_f/F)$ *a pour ordre* $[F_f : F]$.

Démonstration. — Nous avons $F_f = F[\alpha_1, \ldots, \alpha_r]$ avec α_i des racines de f. Notons f_1 le polynôme minimal de α_1 dans $F[X]$. Comme f_1 divise f, les racines de f_1 sont distinctes et il existe $[F(\alpha_1) : F]$ F-morphismes $F(\alpha_1) \longrightarrow F_f$: un tel morphisme est déterminé par l'image de α_1 parmi les racines de f_1. Le polynôme minimal de α_2 sur $F(\alpha_1)$ est un facteur irréductible f_2 de f dans $F(\alpha_1)[X]$ donc est séparable. Les F-morphismes de $F(\alpha_1) \longrightarrow F_f$ se prolongent en F-morphismes de $F(\alpha_1, \alpha_2) \longrightarrow F_f$ en envoyant α_2 sur une racine de f_2. Nous obtenons ainsi $[F(\alpha_1, \alpha_2) : F]$ F-morphismes distincts. Ainsi par récurrence, nous obtenons $[F_f : F]$ F-automorphismes de F_f. □

Exemples 21.4. — *i. Soit $\sqrt[3]{2}$ une racine cubique réelle de 2. Alors* $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$ *(car $\mathbb{Q}(\sqrt[3]{2})$ ne contient qu'une racine du polynôme $X^3 - 2$). Ainsi dans le lemme 21.3, il est essentiel de supposer que E est un corps de décomposition.*
ii. Soit F un corps de caractéristique $p > 0$ et $a \in F$, qui n'est pas une puissance de p dans F. Alors $f = X^p - a$ a une unique racine dans son corps de décomposition E et $\mathrm{Aut}(E/F) = 1$. *C'est pourquoi dans le lemme 21.3, il faut supposer que f est séparable.*
iii. La preuve du Lemme 21.3 montre que si F_f est le corps de décomposition d'un polynôme $f \in F[X]$ pas forcément séparable, alors $|\mathrm{Aut}(F_f/F)| \leq [F_f : F]$.

Définition 21.5. — *Soit G un groupe d'automorphismes d'un corps E. Le sous-corps de E fixe par G est*

$$E^G = \{x \in E | \sigma(x) = x, \sigma \in G\}.$$

Théorème 21.6. — *(Artin) Soit G un groupe fini d'automorphismes de E et $F = E^G$. Alors $[E : F] \leq |G|$.*
En particulier $G = \mathrm{Aut}(E/E^G)$.

Démonstration. — Notons $G = \{\sigma_1 = \mathrm{id}, \ldots, \sigma_m\}$. Nous allons montrer que toute famille $\{\alpha_1, \ldots, \alpha_n\}$ de $n > m$ éléments de E est liée sur F. Pour cela, nous considérons le système d'équations linéaires à coefficients dans E

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_n)x_n = 0, \\ \cdots \\ \sigma_m(\alpha_1)x_1 + \cdots + \sigma_m(\alpha_n)x_n = 0, \end{cases}$$

Ce système de m équations à n inconnues ($n > m$) a des solutions dans E non triviales. Soit $(c_1, \ldots, c_n)$ une solution dans E^n ayant le minimum d'éléments non nuls. Quitte à renuméroter les coefficients, nous pouvons supposer $c_1 \neq 0$ et quitte à multiplier par un scalaire nous pouvons supposer $c_1 \in F^*$. Ainsi

$$\alpha_1 c_1 + \cdots + \alpha_n c_n = 0.$$

S'il existe un $c_i \notin F$, alors il existe $k \in [1, n]$ $\sigma_k(c_i) \neq c_i$. Nous appliquons σ_k aux équations

$$\begin{cases} \sigma_1(\alpha_1)c_1 + \cdots + \sigma_1(\alpha_n)c_n = 0, \\ \cdots \\ \sigma_m(\alpha_1)c_1 + \cdots + \sigma_m(\alpha_n)c_n = 0, \end{cases}$$

et en remarquant que $(\sigma_k\sigma_1, \ldots, \sigma_k\sigma_n)$ est une permutation de $(\sigma_1, \ldots, \sigma_n)$, nous trouvons une autre solution $(c_1, \sigma_k(c_2), \ldots, \sigma_k(c_n))$ du système. En soustrayant les deux solutions obtenues, nous obtenons une troisième solution non triviale (le terme en i est $c_i - \sigma_k(c_i)$) ayant strictement moins de coefficients non nuls (la première coordonnée est nulle), ce qui est exclu.
Comme $G \subset \mathrm{Aut}(E/E^G)$, nous avons

$$[E : E^G] \leq |G| \leq |\mathrm{Aut}(E/E^G)| \leq [E : E^G].$$

D'où $|G| = |\mathrm{Aut}(E/E^G)|$. □

Lemme 21.7. — *(Indépendance linéaire de caractères). Soit G un groupe abélien, M un corps. Tout ensemble fini de morphismes distincts de groupes abéliens $\chi_1, \ldots, \chi_n : G \longrightarrow M^*$ est linéairement indépendant sur M : si $\lambda_1, \ldots, \lambda_n \in M$ et*

$$\forall a \in G, \sum_{i=1}^{n} \lambda_i \chi_i(a) = 0$$

alors $\lambda_1 = \cdots = \lambda_n = 0$.

Démonstration. — Nous raisonnons par induction sur n. Pour $n = 1$, le résultat est clair. Si $n \geq 2$, alors pour tout $a, b \in G$,

$$\sum_{i=1}^{n} \lambda_i \chi_i(ab) = 0, \quad \chi_n(a) \sum_{i=1}^{n} \lambda_i \chi_i(b) = 0.$$

Donc $\sum_{i=1}^{n-1} \lambda_i(\chi_i(a) - \chi_n(a))\chi_i(b) = 0$ et par induction $\lambda_i(\chi_i(a) - \chi_n(a)) = 0$, $1 \leq i \leq n-1$. Comme les morphisme χ_i sont distincts, pour tout $i < n$, il existe $a \in G$ tel que $\chi_i(a) - \chi_n(a) \neq 0$. Donc $\lambda_i = 0$. □

Corollaire 21.8. — *(Indépendance linéaire des plongements de corps). Soit E/F et M/F deux extensions de F. Tout ensemble fini de morphismes distincts de F-algèbres $\sigma_1, \ldots, \sigma_n \in \mathrm{Hom}_{F-\mathrm{Alg}}(E, M)$ est linéairement indépendant sur M. Autrement dit si $\lambda_1, \ldots, \lambda_n \in M$ et*

$$\forall y \in E, \sum_{i=1}^{n} \lambda_i \sigma_i(y) = 0$$

alors $\lambda_1 = \cdots = \lambda_n = 0$.

Pour décrire le groupe des F-automorphismes de $F(X)$, nous avons besoin du lemme suivant :

Lemme 21.9. — *Soit F un corps et $R = P/Q$ une fraction rationnelle $P, Q \in F[X]$ premiers entre eux. Alors*
i. R est transcendant sur F.
ii. L'extension $F(X)/F(R)$ est finie de degré $\max(\deg P, \deg Q)$.
iii. Le polynôme minimal de X sur $F(R)$ est $\chi(T) = P(T) - Q(T)R \in F(R)[T]$.

Démonstration. — i. Nous avons $\chi(X) = 0$ donc X est algébrique sur $F(R)$ donc R est transcendant sur F.
ii. et iii. D'après i., $F[R]$ est isomorphe à un anneau de polynômes en une variable à coefficients dans F. Montrons que χ est irréductible dans $F(R)[T]$. Il est irréductible dans $F[R][T]$ car de degré 1 (en R). Donc irréductible dans $F(R)[T]$. Le pgcd de ses coefficients dans $F(R)$ est 1, donc χ est encore irréductible dans $F(R)[T]$. Nous en déduisons iii. et ii. □

Théorème 21.10. — *Nous avons un isomorphisme*

$$\mathrm{PGL}(2, F) \longrightarrow \mathrm{Aut}(F(X)/F), \quad \begin{pmatrix} a & c \\ b & d \end{pmatrix} \mapsto \left(X \mapsto \frac{aX+b}{cX+d}\right).$$

Démonstration. — Soit $\varphi \in \mathrm{Aut}(F(X)/F)$. Il est déterminé par $\varphi(X) = P/Q \in F(X)$. Comme φ est surjectif, $\max(\deg(P), \deg(Q)) = 1$ et $\varphi(X) = \frac{aX+b}{cX+d}$ avec $(c, d) \neq (0, 0)$ et (a, b) non proportionnel à (c, d). □

21.2. Extensions séparables, normales, galoisiennes. —

Définition 21.11. — *Une extension algébrique E/F est dite* **séparable** *si le polynôme minimal sur F de tout élément de E est séparable. Sinon E/F est dite* **inséparable**.
L'extension algébrique E/F est dite **normale** *si le polynôme minimal sur F de tout élément de E est scindé dans $E[X]$.*

Exemples 21.12. — *i. L'extension* $\mathbb{Q}[\sqrt[3]{2}]$ *est séparable mais pas normale sur* $\mathbb{Q}$.
ii. L'extension $\mathbb{F}_p(T)$ *est normale mais inséparable sur* $\mathbb{F}_p(T^p)$.

Définition 21.13. — *Soit* F *un corps. Une extension finie* E *de* F *est dite* **galoisienne** *si* F *est le corps fixe par le groupe de* F*-automorphismes de* E*. Ce groupe est alors dit* **groupe de Galois** *de* E *sur* F *et est noté* $\mathrm{Gal}(E/F)$.

Théorème 21.14. — *Soit* E/F *une extension de corps. Alors les propriétés suivantes sont équivalentes :*
i. E *est le corps de décomposition d'un polynôme séparable* $f \in F[X]$,
ii. E *est galoisien sur* F,
iii. $F = E^G$ *pour un groupe fini* G *d'automorphismes de* E,
iv. E *est normal, séparable, de degré fini sur* F.

Démonstration. — i.$\Longrightarrow$ ii. Notons $G = \mathrm{Aut}(E/F)$ et $F' = E^G \supset F$. Nous devons montrer $F' = F$. Le corps E est le corps de décomposition de f sur F et sur F', donc f est séparable comme polynôme à coefficients dans F'. Par conséquent

$$|\,\mathrm{Aut}(E/F')| = [E : F'] \leq [E : F] = |\,\mathrm{Aut}(E/F)|.$$

Ainsi d'après le théorème d'Artin $\mathrm{Aut}(E/F') = G = \mathrm{Aut}(E/F)$, donc $[E : F'] = [E : F]$ donc $F = F'$.
ii.$\Longrightarrow$iii. Soit $G = \mathrm{Gal}(E/F)$. Alors $F = E^G$ et G est fini car E est fini sur F.
iii. $\Longrightarrow$iv. Nous avons $[E : F] \leq |G|$, donc E est fini sur F. Soit $\alpha \in E$ et f le polynôme minimal de α dans $F[X]$. Nous devons montrer que f est scindé sans racine multiple dans $E[X]$. Soit $\{\alpha_1 = \alpha, \ldots, \alpha_m\}$ l'orbite de α sous l'action de G et

$$g(X) = \Pi_{i=1}^m (X - \alpha_i) = X^m + a_1 X^{m-1} + \cdots + a_n.$$

Les coefficients a_i sont des polynômes symétriques en α_i et chaque $\sigma \in G$ permute les α_i, donc $\sigma(a_i) = a_i$. Donc $g(X) \in F[X]$, unitaire divisible par $f(X)$, polynôme minimal de α dans $F[X]$. Si $\alpha_i = \sigma(\alpha)$, en appliquant σ à l'équation $f(\alpha) = 0$, nous obtenons que $f(\alpha_i) = 0$. Donc tous les α_i sont des racines de f. Donc g divise f. Ainsi $f = g$ et $f(X)$ est scindé à racines simples dans E.
iv.$\Longrightarrow$ i. Comme E est fini sur F, il est engendré par un nombre fini d'éléments. Ainsi $E = F[\alpha_1, \ldots, \alpha_m]$, $\alpha_i \in E$ algébrique sur F. Soit f_i le polynôme minimal de α_i et f le produit des f_i distincts. Comme E est normal sur F, les f_i sont scindés dans E, donc E est le corps de décomposition de f. Comme E est séparable sur F, chaque f_i est séparable. Donc f est séparable. □

Corollaire 21.15. — *Soit* E/F *galoisienne de groupe* $G = \mathrm{Gal}(E/F)$ *et* $\alpha \in E$. *Les éléments* $\alpha_1, \ldots, \alpha_m$ *de l'orbite de* α *sous* G *sont dits conjugués de* α. *Le polynôme minimal de* α *est* $\Pi_{i=1}^m (X - \alpha_i)$.

Corollaire 21.16. — *Toute extension finie séparable* E *de* F *est contenue dans une extension finie galoisienne.*

Démonstration. — Soit $E = F[\alpha_1, \ldots, \alpha_m]$ et f_i le polynôme minimal (séparable) de α_i sur F. Alors le produit des f_i distincts est un polynôme séparable dans $F[X]$ donc le corps de décomposition est une extension galoisienne de F contenant E. □

Lemme 21.17. — *Soit $E/F'/F$ des extensions de corps avec E/F galoisienne. Alors $\forall \alpha \in F'$,*

$$[E : F'] \operatorname{Tr}_{F'/F}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(E/F)} \sigma(\alpha) \quad \textit{et} \quad N_{F'/F}(\alpha)^{[E:F']} = \prod_{\sigma \in \mathrm{Gal}(E/F)} \sigma(\alpha).$$

Démonstration. — Soit $\alpha \in F'$ et $f \in F[X]$ son polynôme minimal dans F. D'après le Corollaire 18.4, $\operatorname{Tr}_{E/F}(\alpha) = [E : F'] \operatorname{Tr}_{F'/F}(\alpha) = [E : F(\alpha)] \sum_{i=1}^{d} \alpha_i$, où α_i, $1 \leq i \leq d$ sont les racines (distinctes) de f, donc l'orbite de α sous l'action de $\mathrm{Gal}(E/F)$. Comme le stabilisateur de α dans $\mathrm{Gal}(E/F)$ est $\mathrm{Gal}(E/F(\alpha))$, nous obtenons $[E : F(\alpha)] \sum_{i=1}^{d} \alpha_i = \sum_{\sigma \in \mathrm{Gal}(E/F)} \sigma(\alpha)$ et

$$[E : F'] \operatorname{Tr}_{F'/F}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(E/F)} \sigma(\alpha).$$

Le résultat sur la norme s'obtient de façon analogue. □

Corollaire 21.18. — *Soit $F \subset M \subset E$. Si E/F est galoisienne, alors E/M est galoisienne.*

Démonstration. — Le corps E est le corps de décomposition d'un polynôme séparable $f \in F[X]$. C'est donc le corps de décompostion de f, vu comme polynôme à coefficients dans M. □

Définition 21.19. — *Une extension finie E/F est dite cyclique, abélienne, résoluble... si elle est galoisienne de groupe de Galois cyclique, abélien, résoluble...*

Corollaire 21.20. — *(Théorème 90 d'Hilbert). Soit E/F une extension galoisienne de groupe $G = \mathrm{Gal}(E/F)$ cyclique d'ordre n de générateur σ. Alors $\beta \in E^*$ vérifie $N_{E/F}(\beta) = 1 \Longleftrightarrow$ il existe $\alpha \in E^*$ tel que $\beta = \alpha/\sigma(\alpha)$.*

Démonstration. — $\Longrightarrow$ Si $\beta = \alpha/\sigma(\alpha)$, alors $N_{E/F}(\beta) = \beta\sigma(\beta)\cdots\sigma^{n-1}(\beta) = 1$.
$\Longleftarrow$ Si $N_{E/F}(\beta) = 1$, alors pour $\gamma \in E$,

$$\alpha = \sum_{j=0}^{n-1} (\beta\sigma(\beta)\cdots\sigma^j(\beta))\sigma^j(\gamma) = \beta\gamma + \beta\sigma(\beta)\sigma(\gamma) + \cdots + N_{E/F}(\beta)\sigma^{n-1}(\gamma) \in E.$$

Nous avons

$$\sigma(\alpha) = \gamma + \sigma(\beta)\sigma(\gamma) + \cdots + \sigma(\beta)\cdots\sigma^{n-1}(\beta)\sigma^{n-1}(\gamma),$$

donc $\alpha = \beta\sigma(\alpha)$. L'indépendance linéaire des $\sigma^i \in \mathrm{Hom}_{F-\mathrm{Alg}}(E, E)$ montre l'existence d'un $\gamma \in E$ pour lequel $\alpha \neq 0$. Par conséquent $\beta = \alpha/\sigma(\alpha)$. □

Exemple 21.21. — *Le théorème 90 d'Hilbert pour l'extension quadratique* $\mathbb{Q}(i)/\mathbb{Q}$ *établit que*

$$x + iy \in \mathbb{Q}(i) \textit{vérifie } (x+iy)(x-iy) = 1$$
$$\Longleftrightarrow \exists u + iv \in \mathbb{Q}(i) \textit{ tel que } x + iy = (u+iv)/(u-iv).$$

Ainsi nous pouvons décrire tous les triplets Pythagoriciens, i.e tous les $a, b, c \in \mathbb{N}$ *avec* $a^2 + b^2 = c^2$.

Théorème 21.22. — *(Théorème fondamental de la théorie de Galois). Soit* E/F *finie galoisienne et* $G = \mathrm{Gal}(E/F)$. *Alors les applications* $H \mapsto E^H$ *et* $M \mapsto \mathrm{Gal}(E/M)$ *sont des bijections inverses l'une de l'autre entre l'ensemble des sous-groupes de* G *et l'ensemble des corps compris entre* E *et* F *:*

$$\{\textit{Sous-groupes de } G\} \longleftrightarrow \{M \textit{ corps } | F \subset M \subset E\}.$$

De plus,
i. La correspondance renverse les inclusions : $H_2 \subset H_1 \Longleftrightarrow E^{H_1} \subset E^{H_2}$,
ii. $[H_1 : H_2] = [E^{H_2} : E^{H_1}]$,
iii. $\sigma H \sigma^{-1} \longleftrightarrow \sigma M$, *i.e.* $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$; $\mathrm{Gal}(E/\sigma M) = \sigma\,\mathrm{Gal}(E/M)\sigma^{-1}$,
iv. H *est normal dans* $G \Longleftrightarrow E^H$ *est normale (donc galoisienne) sur* F *et dans ce cas*

$$\mathrm{Gal}(E^H/F) = G/H.$$

Démonstration. — Soit H un sous-groupe de G. Alors $\mathrm{Gal}(E/E^H) = H$. Soit $F \subset M \subset E$, alors E/M est galoisienne et $E^{\mathrm{Gal}(E/M)} = M$. Par conséquent les applications $H \mapsto E^H$ et $M \mapsto \mathrm{Gal}(E/M)$ sont des bijections inverses l'une de l'autre.
i. Nous avons

$$H_2 \subset H_1 \Longrightarrow E^{H_1} \subset E^{H_2} \Longrightarrow \mathrm{Gal}(E/E^{H_1}) \supset \mathrm{Gal}(E/E^{H_2})$$

Comme $H_i = \mathrm{Gal}(E/E^{H_i})$, nous obtenons i.
ii. Pour tout sous-groupe H de G, nous avons $[E : E^H] = |\,\mathrm{Gal}(E/E^H)|$, ce qui prouve ii. dans le cas $H_2 = 1$. Le cas général suit car

$$|H_1| = [H_1 : H_2]|H_2| \text{ et } [E : E^{H_1}] = [E : E^{H_2}][E^{H_2} : E^{H_1}].$$

iii. Pour $\tau \in G$ et $\alpha \in E$. Nous avons $\tau(\alpha) = \alpha \Longleftrightarrow \sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma\alpha$. Donc $\mathrm{Gal}(E/\sigma M) = \sigma\,\mathrm{Gal}(E/M)\sigma^{-1}$. Donc $\sigma\,\mathrm{Gal}(E/M)\sigma^{-1} \longleftrightarrow \sigma M$.
iv. Soit H un sous-groupe normal de G. Comme $\sigma H \sigma^{-1} = H$ pour tout $\sigma \in G$, nous avons $\sigma E^H = E^H$ pour tout $\sigma \in G$: l'action de G sur E stabilise E^H. Ainsi le morphisme

$$G \longrightarrow \mathrm{Aut}(E^H/F), \quad \sigma \mapsto \sigma_{|E^H}$$

est bien défini et a pour noyau H. Comme $(E^H)^{G/H} = F$, E^H/F est galoisienne et $G/H \simeq \mathrm{Gal}(E^H/F)$.
Réciproquement si $M = E^H$ est normal sur F, écrivons $M = F[\alpha_1, \ldots, \alpha_m]$. Pour $\sigma \in G$, $\sigma\alpha_i$ est une racine du polynôme minimal de α_i sur F donc appartient aussi à M. Donc $\sigma M = M$ et $\sigma H \sigma^{-1} = H$ (par iii.). □

Corollaire 21.23. — *Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Démonstration. — Nous définissons $\mathbb{C}$ comme le corps de décomposition sur $\mathbb{R}$ de X^2+1. Il s'agit de montrer que tout polynôme $f(X) \in \mathbb{R}[X]$ a une racine complexe.
D'après le théorème des valeurs intermédiaires, tout réel positif admet une racine carrée et tout polynôme de $\mathbb{R}[X]$ de degré impair admet une racine réelle.
• Montrons que tout $\alpha \in \mathbb{C}$ admet une racine carrée. Ecrivons $\alpha = a + ib$ avec $a, b \in \mathbb{R}$. Soit $c, d \in \mathbb{R}$ tels que cd soit du signe de b et

$$c^2 = \frac{a + \sqrt{a^2+b^2}}{2}, \quad d^2 = \frac{-a + \sqrt{a^2+b^2}}{2}.$$

Ainsi $(c+id)^2 = \alpha$ donc $c + id$ est une racine de α.
• Soit $f(X) \in \mathbb{R}[X]$ et E le corps de décomposition sur $\mathbb{R}$ de $(X^2+1)f(X)$. Comme $\mathbb{R}$ est de caractéristique 0, $E/\mathbb{R}$ est séparable donc galoisienne. Nous notons $G = \mathrm{Gal}(E/\mathbb{R})$ et H un sous-groupe de 2-Sylow de G. Notons $M = E^H$. Ainsi $[M : \mathbb{R}] = |G|/|H|$ est impair. Donc le degré du polynôme minimal de tout élément $\alpha \in M$ divise $[M : \mathbb{R}]$ donc est impair et admet une racine réelle. D'où $M = \mathbb{R}$.
• Si $E \neq \mathbb{C}$ alors $\mathrm{Gal}(E/\mathbb{C})$ est un groupe d'ordre 2^r, $r > 0$. Il admet un sous-groupe N d'indice 2. Le corps E^N, de degré 2 sur $\mathbb{C}$, est engendré par la racine carrée d'un élément de $\mathbb{C}$ donc $E = \mathbb{C}$ absurde ! Par conséquent $\mathrm{Gal}(E/\mathbb{C}) = 1$ et f est scindé sur $\mathbb{C}$. □

Proposition 21.24. — *Soit E, L des extensions de F contenues dans une même extension EL de F. Si E/F est galoisienne alors EL/L et $E/E \cap L$ aussi et l'application*

$$\sigma \mapsto \sigma_{|E} : \mathrm{Gal}(EL/L) \longrightarrow \mathrm{Gal}(E/E \cap L)$$

est un isomorphisme.
De plus

$$[EL : F] = \frac{[E : F][L : F]}{[E \cap L : F]}.$$

Démonstration. — Comme E/F est galoisienne, c'est le corps de décomposition d'un polynôme séparable $f \in F[X]$. Donc EL est le corps de décomposition de f sur L et E est le corps de décomposition de f sur $E \cap L$. Donc EL/L et $E/E \cap L$ sont galoisiennes.
Tout automorphisme $\sigma \in \mathrm{Gal}(LE/L)$ fixe les éléments de F (et de $E \cap L$) et envoie les racines de f sur des racines de f. Donc $\sigma E = E$ et nous obtenons un morphisme

$$\varphi : \mathrm{Gal}(EL/L) \longrightarrow \mathrm{Gal}(E/E \cap L), \ \sigma \mapsto \sigma_{|E}$$

- φ est injectif : si $\sigma \in \mathrm{Gal}(EL/L)$ fixe les éléments de E alors il fixe les éléments de EL donc $\sigma = \mathrm{Id}$.

- φ est surjectif : si $\alpha \in E$ est fixe par tous les $\sigma \in \mathrm{Gal}(EL/L)$, alors $\alpha \in L \cap E$. D'après le théorème fondamental de la théorie de Galois, l'image de φ est donc $\mathrm{Gal}(E/E \cap L)$.
Enfin, comme $[EL : F] = [EL : L][L : F]$ et $[EL : L] = [E : E \cap L] = \frac{[E:F]}{[E \cap L:F]}$, nous obtenons l'égalité annoncée. □

Proposition 21.25. — *Soient E_1, E_2 des extensions de F contenues dans le corps E_1E_2. Si E_1 et E_2 sont galoisiennes sur F, alors E_1E_2 et $E_1 \cap E_2$ aussi et*

$$\varphi : \mathrm{Gal}(E_1E_2/F) \longrightarrow \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F), \quad \sigma \mapsto (\sigma_{|E_1}, \sigma_{|E_2})$$

est un isomorphisme entre $\mathrm{Gal}(E_1E_2/F)$ *et le sous-groupe de* $\mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$ *:*

$$H = \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F) | \sigma_{1|E_1 \cap E_2} = \sigma_{2|E_1 \cap E_2}\}.$$

Démonstration. — Soit $a \in E_1 \cap E_2$ et $f \in F[X]$ son polynôme minimal. Alors f a $\deg f$ racines distinctes dans E_1 et E_2. Comme f a au plus $\deg f$ racines dans E_1E_2, f a $\deg f$ racines distinctes dans $E_1 \cap E_2$. Donc $E_1 \cap E_2$ est normale séparable donc galoisienne sur F.
Comme E_1 (resp. E_2) est galoisien sur F, c'est le corps de décomposition d'un polynôme séparable f_1 (resp. f_2) dans $F[X]$. Le corps E_1E_2 est le corps de décomposition de f_1f_2 donc est une extension galoisienne de F.
L'application φ est un morphisme injectif dont l'image est incluse dans H. Pour montrer la surjectivité, nous calculons les cardinaux des groupes. D'après le théorème fondamental de la théorie de Galois, $\mathrm{Gal}(E_2/E_1 \cap E_2)$ est normal dans $\mathrm{Gal}(E_2/F)$ et

$$\mathrm{Gal}(E_2/F)/\mathrm{Gal}(E_2/E_1 \cap E_2) = \mathrm{Gal}(E_1 \cap E_2/F).$$

Ainsi pour tout $\sigma_1 \in \mathrm{Gal}(E_1/F)$, $\sigma_{1|E_1 \cap E_2}$ a exactement $[E_2 : E_1 \cap E_2]$ extensions à $\mathrm{Gal}(E_2/F)$. Donc

$$|H| = [E_1 : F][E_2 : E_1 \cap E_2] = \frac{[E_1 : F][E_2 : F]}{[E_1 \cap E_2 : F]} = [E_1E_2 : F].$$

□

21.3. Extension algébrique galoisienne infinie. —

Définition 21.26. — *Une extension algébrique E/F est dite galoisienne si elle est séparable normale.*

Exemples 21.27. — *i. L'extension algébrique E/F est galoisienne si et seulement si elle est réunion d'extensions galoisiennes finies.*
ii. Notons $\zeta_{p^n} \in \mathbb{C}$ une racine primitive p^n-ième de l'unité. Ainsi l'extension algébrique $\mathbb{Q}(\zeta_{p^\infty}) = \cup_{n \geq 0} \mathbb{Q}(\zeta_{p^n})$ est galoisienne sur $\mathbb{Q}$.

Le lemme suivant généralise les résultats obtenus dans le cas galoisien fini.

Lemme 21.28. — *Soit E/F une extension algébrique galoisienne et M une extension intermédiaire $F \subset M \subset E$. Alors,*
i. E est galoisienne sur M.
ii. Tout F-morphisme $M \longrightarrow E$ se prolonge en un F-automorphisme $E \longrightarrow E$.
iii. Si M est stable sous $\mathrm{Aut}(E/F)$*, alors M/F est galoisienne.*

Démonstration. — i. Soit $g \in M[X]$ un polynôme irréductible ayant une racine $\alpha \in E$ et $f \in F[X]$ le polynôme minimal de α. Ainsi f est scindé à racines simples et g divise f dans $M[X]$. Donc g est scindé à racines simples.
ii. Le lemme de Zorn permet de montrer que tout F-morphisme $M \longrightarrow E$ se prolonge en un F-morphisme $\sigma : E \longrightarrow E$. Il s'agit de montrer que ce morphisme est sujectif. Soit $\alpha \in E$ et f son polynôme minimal sur F. Comme E contient $\deg f$ racines de f, $\sigma(E)$ aussi donc $\alpha \in \sigma(E)$ et σ est surjectif.
iii. Soit $f \in F[X]$ polynôme minimal de $\alpha \in M$. Comme E/F est galoisienne, f a $\deg f$ racines distinctes $a_i \in E$. Le F-isomorphisme $F[\alpha] \longrightarrow F[a_i] \subset E$ qui envoie α sur a_i qui s'étend en un F-automorphisme $E \longrightarrow E$. Comme M est stable sous $\mathrm{Aut}(E/F)$, nous avons $a_i \in M$. Par conséquent M est algébrique séparable normale donc galoisienne sur F. □

Proposition 21.29. — *Soit E/F une extension galoisienne et $G = \mathrm{Aut}(E/F)$ d'élément neutre e. Soit S un sous-ensemble fini de E et*

$$G(S) = \{\sigma \in G | \sigma(s) = s, \forall s \in S\}$$

Il existe une unique structure de groupe topologique sur G pour laquelle les ensembles $G(S)$ forment une base de voisinages de e. Cette topologie est dite **topologie de Krull**. *Le groupe G muni de la topologie de Krull est dit* **groupe de Galois** *de E/F et est noté* $\mathrm{Gal}(E/F)$.

Démonstration. — Nous avons $G(S_1) \cap G(S_2) = G(S_1 \cup S_2)$.
Comme $G(S)$ est un groupe, $G(S)G(S) \subset G(S)$ et $G(S) \subset G(S)^{-1}$.
Comme S est finie, $S' = \cup_{\sigma \in G} \sigma S$ est finie (l'orbite d'un élément $x \in E$ sous $\mathrm{Gal}(E/F)$ est finie) et $\sigma S' = S'$ pour tout $\sigma \in G$. Donc $G(S')$ est un sous-groupe normal de G : $\sigma G(S')\sigma^{-1} = G(S') \subset G(S)$.
D'après le lemme 13.7, ces propriétés garantissent qu'il existe une unique structure de groupe topologique sur G telle que pour tout $g \in G$,

$$\{gG(S), S \text{ sous-ensemble fini de } E\}$$

soit une base de voisinages de g. □

Exemples 21.30. — *i. Si* $\mathrm{Gal}(E/F)$ *est fini, la topologie de Krull sur* $\mathrm{Gal}(E/F)$ *est la topologie discrète.*
ii. Si S est une partie finie de E stable sous $\mathrm{Gal}(E/F)$*, alors $F(S)$ est une extension finie de F stable sous* $\mathrm{Gal}(E/F)$ *donc galoisienne sur F. Par conséquent*

$$\{\mathrm{Gal}(E/M), M \textit{ finie galoisienne sur } F\}$$

est une base de voisinages de e composée de sous-groupes ouverts normaux.
iii. Le groupe de Galois $\mathrm{Gal}(E/F)$ *est compact séparé et ses composantes connexes sont les singletons.*

Lemme 21.31. — *Soit* E/F *algébrique galoisienne, de groupe de Galois* $\mathrm{Gal}(E/F)$ *et* M *un sous-corps de* E *contenant* F*. Alors,*
i. $E^{\mathrm{Gal}(E/M)} = M$ *et* $\mathrm{Gal}(E/M)$ *est fermé.*
ii. Pour tout sous-groupe H *de* $\mathrm{Gal}(E/F)$*,* $\mathrm{Gal}(E/E^H) = \overline{H}$*.*

Démonstration. — i. L'extension E/M est galoisienne d'après le lemme 21.28. Tout élément $\alpha \in E$ appartient à une extension finie galoisienne L de M. L'application

$$\mathrm{Gal}(E/M) \longrightarrow \mathrm{Gal}(L/M), \sigma \mapsto \sigma_{|L}$$

est surjective (tout M-morphisme $L \longrightarrow E$ s'étend à E). D'où $E^{\mathrm{Gal}(E/M)} = M$.
Pour tout ensemble fini stable $S' \subset M$, la projection

$$\pi : \mathrm{Gal}(E/F) \longrightarrow \mathrm{Gal}(F(S')/F)$$

est continue car l'image réciproque d'un singleton (ouvert) est ouverte. Donc l'image réciproque $G(S')$ du singleton $\{e\}$ (fermé) est fermée. Ainsi $\mathrm{Gal}(E/M) = \cap_{S' \subset M stable} G(S')$ est fermé.
D'après le théorème de Tychonoff, le groupe $\mathrm{Gal}(E/F)$ est séparé et compact comme limite projective de groupes séparés compacts.
ii. Comme $\mathrm{Gal}(E/E^H)$ est fermé et contient H, il contient $\overline{H}$. Par ailleurs soit $\sigma \in G - \overline{H}$. Comme $\sigma \notin \overline{H}$, il existe une extension galoisienne finie M de F dans E avec $\sigma\,\mathrm{Gal}(E/M) \cap H = \emptyset$. Soit $\psi : \mathrm{Gal}(E/F) \longrightarrow \mathrm{Gal}(M/F)$, l'application surjective de restriction à M. Nous avons $\sigma_{|M} \notin \psi(H)$ donc σ ne laisse pas fixe un élément de $M^{\psi(H)} \subset E^H$. D'où $\mathrm{Gal}(E/E^H) = \overline{H}$. □

Proposition 21.32. — *Soit* $E = \cup_\alpha F_\alpha$ *une extension algébrique galoisienne avec* F_α/F *extensions galoisiennes finies.*
i. Le groupe de Galois $\mathrm{Gal}(E/F) \simeq \varprojlim \mathrm{Gal}(F_\alpha/F)$*, muni de la topologie de limite projective de groupes finis, est un groupe compact séparé dont les sous-groupes ouverts normaux* $\mathrm{Gal}(E/F_\alpha)$ *forment une base de voisinage de l'identité.*
ii. La correspondance de Galois est une bijection

$$\{M \text{ corps } |E/M/F\} \longleftrightarrow \{\text{sous-groupes fermés } H \subset \mathrm{Gal}(E/F)\},$$

via $M = E^H$ *et* $H = \mathrm{Gal}(E/M)$*.*

Démonstration. — i. Tout élément $\sigma \in \mathrm{Gal}(E/F)$ définit par restriction un système compatible d'éléments des groupe de Galois finis $\mathrm{Gal}(F_\alpha/F)$: les morphismes surjectifs

$$\mathrm{res}_{\alpha\beta} : \mathrm{Gal}(F_\beta/F) \longrightarrow \mathrm{Gal}(F_\alpha/F)$$

(pourvu que F_β/F_α soit une extension de corps) et les automorphismes $\sigma_{F_\alpha} \in \mathrm{Gal}(F_\alpha/F)$ satisfont $\mathrm{res}_{\alpha\beta}(\sigma_{F_\beta}) = \sigma_{F_\alpha}$.

L'application ainsi définie de $\mathrm{Gal}(E/F)$ sur $\varprojlim \mathrm{Gal}(F_\alpha/F)$ est injective, surjective, continue et ouverte. C'est un homéomorphisme.
Les sous-groupes ouverts de $\mathrm{Gal}(E/F)$ sont les sous-groupes fermés d'indice fini. Ils correspondent aux extensions finies M/F.
ii. Les applications $H \mapsto E^H$ et $M \mapsto \mathrm{Gal}(E/M)$ sont inverses l'une de l'autre. □

Exemples 21.33. — *i. Les énoncés du théorème fondamental de la théorie de Galois et les propositions 21.24,21.25 s'étendent sans peine dans ce contexte.*
ii. Les groupes de Galois $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ *sont cycliques d'ordre* n *engendrés par le morphisme de Frobenius* φ. *En effet le corps* $\mathbb{F}_{p^n}$ *est le corps de décomposition du polynôme séparable* $X^{p^n} - X$ *sur* $\mathbb{F}_p$ *donc* $\mathbb{F}_{p^n}/\mathbb{F}_p$ *est galoisienne. Les morphismes* $\varphi^j : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $x \mapsto x^{pj}$ *sont* n $\mathbb{F}_p$*-automorphismes de* $\mathbb{F}_{p^n}$ *distincts. Nous avons* $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \widehat{\mathbb{Z}} = \prod \mathbb{Z}_\ell$, *le produit portant sur l'ensemble des nombres premiers.*
iii. Le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *reste, à ce jour, très mystérieux. Par exemple, le problème de Galois inverse conjecture que tout groupe fini apparait comme quotient de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
iv. Les groupes de Galois d'extensions de corps se généralisent en groupes fondamentaux d'espaces de revêtements.

22. Groupes de Galois

22.1. Extensions cyclotomiques. —

Proposition 22.1. — *Soit* F *un corps de caractéristique 0 ou* p *ne divisant pas* n. *Soit* E *le corps de décomposition de* $X^n - 1$.
i. L'extension E/F *est galoisienne,* E *contient une racine primitive* n*-ième* ξ *de 1 et* $E = F[\xi]$.
ii. Pour tout $\sigma \in \mathrm{Gal}(E/F)$, *il existe* $i \in (\mathbb{Z}/n\mathbb{Z})^*$ *tel que* $\sigma(\xi) = \xi^i$. *L'application* $\sigma \mapsto i$ *est un morphisme injectif* $\mathrm{Gal}(E/F) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$.

Démonstration. — i. Le corps E est le corps de décomposition d'un polynôme séparable sur F, donc E/F est galoisienne. Les racines de $X^n - 1$ dans E et forment un sous-groupe cyclique C_n d'ordre n de E^*. Tout générateur de C_n est d'ordre n donc est une racine primitive ξ n-ième de 1. Les racines de $X^n - 1$ sont les puissances de ξ et $F[\xi]$ les contient donc toutes.
ii. Si $\sigma \in \mathrm{Gal}(E/F)$, $\sigma(\xi) = \xi^i$ avec $(i, n) = 1$ car ξ^i est une racine primitive n-ième de 1. L'application $\sigma \mapsto i \mod n$ est un morphisme injective car ξ engendre E sur F. □

Nous notons le n-ième polynôme cyclotomique $\Phi_n(X) = \Pi(X - \xi) \in \mathbb{Z}[X]$, où ξ parcourt l'ensemble des racines primitives n-ièmes de l'unité. C'est un polynôme de degré $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.

Lemme 22.2. — *Soit F un corps de caractéristique 0 ou p ne divisant pas n. Soit ξ un racine primitive n-ième de l'unité. Les propriétés suivantes sont équivalentes :*
i. le n-ième polynôme cyclotomique Φ_n est irréductible,
ii. $[F(\xi) : F] = \varphi(n)$,
iii. $\mathrm{Gal}(F(\xi)/F) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.

Démonstration. — Comme ξ est une racine primitive n-ième de l'unité, le polynôme minimal μ de ξ divise Φ_n. De plus $\mu = \Phi_n$ si et seulement si $[F(\xi) : F] = \varphi(n)$ donc si et seulement si l'injection $\mathrm{Gal}(E/F) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ est surjective. □

Proposition 22.3. — *Le polynôme cyclotomique Φ_n est irréductible sur $\mathbb{Q}[X]$.*

Démonstration. — Soit $\xi \in \mathbb{C}$ une racine primitive n-ième de l'unité et $f \in \mathbb{Q}[X]$ son polynôme minimal. Comme f est unitaire et divise le polynôme unitaire $\Phi_n \in \mathbb{Z}[X]$, nous avons $f \in \mathbb{Z}[X]$. Soit $g \in \mathbb{Z}[X]$ avec $\Phi_n = fg$. Supposons qu'il existe p premier ne divisant pas n avec ξ^p racine de g. Alors f et $g(X^p)$ ont une racine commune donc un facteur commun $h \in \mathbb{Z}[X]$ de degré supérieur à 1. Notons $\bar{f}, \bar{g}, \bar{h}$ les images de f, g, h dans $\mathbb{F}_p[X]$. Ainsi $\bar{f}$ et $\bar{g}(X^p)$ ont un facteur commun dans $\mathbb{F}_p[X]$. Comme $\bar{g}(X^p) = (\bar{g})^p$ et $\bar{g}$ ont les mêmes racines, $\bar{g}$ et $\bar{f}$ ont un facteur commun de degré ≥ 1 dans $\mathbb{F}_p[X]$. Or $X^n - 1 \in \mathbb{F}_p[X]$ n'a que des racines simples, nous obtenons une contradiction. Par conséquent pour tout p premier ne divisant pas n, ξ racine de f implique ξ^p aussi. Donc pour tout i premier avec n (donc produit de nombres premiers ne divisant pas n) ξ racine de f implique ξ^i aussi. Donc $\Phi_n = f$ est irréductible sur $\mathbb{Q}[X]$. □

Exemple 22.4. — *Soit $\zeta_{p^n} \in \mathbb{C}$ une racine primitive p^n-ième de l'unité, $p \geq 3$ premier. Nous avons* $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}$ *(voir Exemple 10.5). Donc* $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) = \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$.

22.2. Groupe de Galois, discriminant, groupe des permutations. —

Définition 22.5. — *Soit $f \in F[X]$ un polynôme unitaire*

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$$

s'écrivant $f(X) = \Pi_{i=1}^n (X - \alpha_i)$ dans un corps de décomposition. Le **discriminant** *de f est défini par*

$$D(f) = \Pi_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Ainsi $D(f) = \Delta(f)^2$ pour $\Delta(f) = \Pi_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$.

Donc $D(f) \neq 0$ si et seulement si f n'admet que des racines simples. Sous cette hypothèse, nous notons $G_f = \mathrm{Gal}(F_f/F)$ le groupe de Galois du corps F_f de décomposition de f ; il s'identifie à un sous-groupe du groupe $\mathfrak{S}_n$ des permutations de $\{\alpha_1, \ldots, \alpha_n\}$.

Exemple 22.6. — *Nous avons*

$$D(X^2+bX+c) = b^2-4c, \quad D(X^3+aX^2+bX+c) = -4a^3c+a^2b^2+18abc-4b^3-27c^2.$$

En degré supérieur, il est malcommode d'exprimer le discriminant en fonction des coefficients du polynôme.

Lemme 22.7. — *Soit $f \in F[X]$ de degré n à racines simples. Notons $A_n < \mathfrak{S}_n$ le sous-groupe alterné. Alors,*
i. $D(f) \in F$.
ii. Le sous-corps de F_f correspondant à $A_n \cap G_f$ est $F[\Delta(f)]$.
iii. $G_f \subset A_n \Longleftrightarrow \Delta(f) \in F \Longleftrightarrow D(f)$ est un carré dans F.

Démonstration. — i. Le discriminant de f est un élément de F_f fixe par G_f donc $D(f) \in F$.
ii. Comme f n'a que des racines simples, $\Delta(f) \neq 0$. Comme $\sigma\Delta(f) = \varepsilon(\sigma)\Delta(f)$, $\sigma \in G_f$, un élément de G_f fixe $\Delta(f)$ si et seulement si il appartient à A_n. Ainsi par la correspondance de Galois $G_f \cap A_n$ correspond à $F[\Delta(f)]$. D'où le corollaire. □

Exemple 22.8. — *Supposons $F \subset \mathbb{R}$. Alors $D(f)$ n'est pas un carré s'il est négatif. Or le signe de $D(f)$ est $(-1)^s$ où $2s$ est le nombre de racines complexes non réelles de f. En effet notons $\alpha_1, \ldots, \alpha_r$, les racines réelles et $\alpha_{r+1}, \overline{\alpha_{r+1}}, \ldots, \alpha_{r+s}, \overline{\alpha_{r+s}}$ les racines complexes de f. Le signe de $D(f)$ est égal au signe de $\prod_{i=1}^{s}(\alpha_{i+r} - \overline{\alpha_{i+r}})^2$, soit $(-1)^s$.*
Si s est impair alors $G_f \not\subset A_n$ (la conjugaison complexe agit sur les racines de f comme le produit de s transpositions disjointes). En revanche quand s est pair, G_f n'est pas forcement inclus dans A_n. En effet, il s'agit ensuite de voir si $\sqrt{D(f)} \in F$.

Proposition 22.9. — *Soit $f \in F[X]$ à racines simples. Alors f est irréductible si et seulement si G_f permute les racines de f transitivement.*

Démonstration. — $\Longrightarrow$ Soient α_1, α_2 deux racines distinctes de f. Alors le F-isomorphisme $F[\alpha_1] \longrightarrow F[\alpha_2], \alpha_1 \mapsto \alpha_2$ s'étend en un F-morphisme de $F_f \longrightarrow F_f$.
$\Longleftarrow$ Soit $g \in F[X]$ un facteur irréductible de f et α une racine de g. Soit β une autre racine de f. Comme l'action de G_f est transitive, il existe $\sigma \in G_f$ tel que $\beta = \sigma\alpha$. Par ailleurs comme g est à coefficients dans F,

$$g(\sigma\alpha) = \sigma g(\alpha) = 0$$

donc β est racine de g et $f = g$. □

Proposition 22.10. — *Soit $f \in F[X]$ n'ayant que des racines simples. Supposons que $G_f = \mathrm{Gal}(F_f/F)$ agit sur les racines de f suivant r orbites de cardinal respectif $m_1, \ldots, m_r$. Alors f se factorise dans $F[X]$ sous la forme $f = f_1 \cdots f_r$ avec f_i irréductible de degré m_i.*

Démonstration. — Notons $\{\alpha_1, \ldots, \alpha_m\}$ les racines de f. A toute partie $S \subset \{\alpha_1, \ldots, \alpha_m\}$ nous associons le polynôme

$$S \longleftrightarrow f_S = \Pi_{\alpha \in S}(X - \alpha).$$

Ainsi f_S est fixe sous l'action de G_f (donc est à coefficients dans F) si et seulement si S est stable sous G_f. Par conséquent les facteurs irréductibles de f dans $F[X]$ sont les polynômes f_S correspondant aux sous-ensembles minimaux de $\{\alpha_1, \ldots, \alpha_m\}$ stable par G_f, i.e les orbites de G_f dans $\{\alpha_1, \ldots, \alpha_m\}$. $\square$

Si f est irréductible de degré n, alors $[F[\alpha] : F] = n$ divise $[F_f : F] = |G_f|$. Donc G_f est un sous-groupe transitif de $\mathfrak{S}_n$ d'ordre divisible par n.

Exemples 22.11. — *i. Soit $f \in F[X]$, $\deg f = 2$. Alors f est inséparable si et seulement si $\mathrm{car} F = 2$ et $f = X^2 - a$ avec $a \in F - F^2$. Si f est séparable. Alors $G_f = 1 = A_2$ ou $G_f = \mathfrak{S}_2 = \mathbb{Z}/2\mathbb{Z}$ suivant que $D(f)$ est un carré ou non dans F.*
ii. Soit $f \in F[X]$ irréductible de degré 3. Alors f est inséparable si et seulement si $\mathrm{car} F = 3$ et $f = X^3 - a$ avec $a \in F - F^3$. Si f est séparable, G_f est un sous-groupe transitif de $\mathfrak{S}_3$ de degré divisible par 3. Donc $G_f = A_3$ ou $\mathfrak{S}_3$ suivant que $D(f)$ est un carré ou non dans F.
Par exemple pour $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$, $D(f) = -4(-3)^3 - 27 = 9^2$, donc $G_f = A_3$.
Pour $g = X^3 + 3X + 1 \in \mathbb{Q}[X]$, $D(g) = -135$ et $G_g = \mathfrak{S}_3$.

Lemme 22.12. — *Soit* $f(X) = \Pi_{i=1}^4(X - \alpha_i) \in F[X]$ *un polynôme irréductible séparable de degré 4 de groupe* G_f. *Notons*

$$V = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$$

le sous-groupe normal de $\mathfrak{S}_4$ *engendré par les bi-transpositions et*

$$\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4, \beta = \alpha_1\alpha_3 + \alpha_2\alpha_4, \gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

i. Le sous-corps fixe du corps de décomposition F_f *sous l'action de* $G_f \cap V$ *est* $F[\alpha, \beta, \gamma]$.
ii. Nous avons les possibilités suivantes pour G_f *sont déterminées par les cardinaux de* $G_f \cap V$ *et de* $G_f/G_f \cap V$ *:*

G_f	$\lvert G_f \cap V\rvert$	$\lvert G_f\rvert/\lvert G_f \cap V\rvert$
$\mathfrak{S}_4$	4	6
A_4	4	3
V	4	1
D_4	4	2
C_4	2	2

Démonstration. — i. Les éléments α, β, γ sont distincts car les α_i sont distincts et

$$\alpha - \beta = \alpha_1(\alpha_2 - \alpha_3) + \alpha_4(\alpha_3 - \alpha_2) = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3).$$

Le groupe des permutations de $\{\alpha_1, \ldots, \alpha_4\}$ permute $\{\alpha, \beta, \gamma\}$ transitivement. Le stabilisateur de chaque élément α, ou β ou γ est donc un sous-groupe d'indice 3 dans $\mathfrak{S}_4$, donc est d'ordre 8 (par exemple le stabilisateur de β est $< (1234), (13) >$). Les groupes d'ordre 8 dans $\mathfrak{S}_4$ sont les 2-Sylow. Il y en a donc 3, tous isomorphes à D_4. Or $|V| = 4$ est contenu dans un sous-groupe de 2-Sylow. Comme V est normal et que les sous-groupes de 2-Sylow sont conjugués, V est l'intersection des 3 sous-groupes de 2-Sylow de $\mathfrak{S}_4$. Ainsi chaque 2-Sylow de $\mathfrak{S}_4$ fixe exactement l'un des éléments α, β, γ et leur intersection V est le sous-groupe de $\mathfrak{S}_4$ qui fixe α, β et γ. Donc $G_f \cap V$ est le sous-groupe de G_f qui fixe $F[\alpha, \beta, \gamma]$.
ii. D'après i., $F[\alpha, \beta, \gamma]/\mathrm{F}$ est galoisienne de groupe $G_f/G_f \cap V$ et $F_f/F[\alpha, \beta, \gamma]$ galoisienne de groupe $G_f \cap V$. □

Définition 22.13. — *Soit* $f(X) = X^4 + bX^3 + cX^2 + dX + e = \Pi_{i=1}^4(X - \alpha_i) \in F[X]$ *un polynôme irréductible séparable. Nous notons* $\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4, \beta = \alpha_1\alpha_3 + \alpha_2\alpha_4, \gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3$. *Alors le polynôme cubique* g **résolvant** *de* f *est*

$$g = (X - \alpha)(X - \beta)(X - \gamma) = X^3 - cX^2 + (bd - 4e)X - b^2e + 4ce - d^2.$$

Exemples 22.14. — *i. Le polynôme irréductible séparable* $f(X) = X^4 - 4X + 2 \in \mathbb{Q}[X]$. *Le polynôme résolvant* $g(X) = (X-\alpha)(X-\beta)(X-\gamma) = X^3 - 8X + 16$ *est irréductible (car n'a pas de racine dans* $\mathbb{F}_5$*) et* $D(g) = -4864$ *qui n'est pas un carré, donc* $G_g = \mathfrak{S}_3$ *et* $G_f = \mathfrak{S}_4$.
ii. Le polynôme irréductible séparable $F(X) = X^4 - 10X^2 + 4 \in \mathbb{Q}[X]$ *a pour polynôme résolvant* $g(X) = (X + 10)(X - 4)(X + 4)$. *Donc* $G_f = V$.

Proposition 22.15. — *Soit $f \in \mathbb{Q}[X]$ irréductible de degré premier p. Si f a exactement deux racines non réelles alors $G_f = \mathfrak{S}_p$.*

Démonstration. — Soit $\alpha \in \mathbb{Q}_f$ une racine de f. Comme f est irréductible $[\mathbb{Q}[\alpha] : \mathbb{Q}] = p$ donc $p|[\mathbb{Q}_f : \mathbb{Q}]$ et G_f contient un élément d'ordre p, donc un p-cycle de $\mathfrak{S}_p$. La conjugaison complexe est un élément d'ordre deux de G_f qui permute les deux racines non réelles. Donc $G_f < \mathfrak{S}_p$ contient une permutation et un p-cycle donc $G_f = \mathfrak{S}_p$. □

22.3. Théorie de Kummer. — La théorie de Kummer permet de décrire explicitement les groupes de Galois des extensions $F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})/F$ pour $a_i \in F^*$, $\mu_n \subset F$ et car$F \not| n$.
Soit $n \geq 2$ un entier et F un corps tel que $|\mu_n(F)| = n$ (ce qui implique que la caractéristique de F ne divise pas n). Soit $a_1, \ldots, a_r \in F^*$ et E le corps de décomposition sur F du polynôme séparable

$$(T^n - a_1) \cdots (T^n - a_r) = \Pi_{\zeta \in \mu_n(F)} \Pi_{i=1}^r (T - \zeta \sqrt[n]{a_i}) \in F[T].$$

Ainsi l'extension $E = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})/F$ est galoisienne de groupe $G = \mathrm{Gal}(L/K)$.
Pour $a \in F^*$, nous notons $\bar{a}$ son image dans F^*/F^{*n}. Soit $\Delta \subset F^*/F^{*n}$ le sous-groupe engendré par $\bar{a}_1, \ldots, \bar{a}_r$. Remarquons que Δ est un sous-groupe du groupe abélien

$$\Delta' = \mathrm{Ker}(F^*/F^{*n} \longrightarrow E^*/E^{*n}) = (F^* \cap E^{*n})/F^{*n}.$$

Lemme 22.16. — *Nous avons une application bien définie*

$$(\ ,\ ) : G \times \Delta' \longrightarrow \mu_n, \ \ (g, \bar{a}) \mapsto g(\alpha)/\alpha$$

où $\alpha \in E^*$ est une racine n-ième quelconque de a. De plus, pour tous $\bar{a}, \bar{b} \in \Delta', g, g' \in G$, elle satisfait
i. $(g, \bar{a}\bar{b}) = (g, \bar{a})(g, \bar{b})$,
ii. $(gg', \bar{a}) = (g, \bar{a})(g', \bar{a})$.
Enfin $(\ ,\ )$ *est non dégénérée à droite et à gauche :*
iii. $(g, \bar{a}) = 1, \forall \bar{a} \in \Delta' \Longrightarrow g = \mathrm{Id}$,
iv. $(g, \bar{a}) = 1, \forall g \in G \Longrightarrow \bar{a} = 1$.

Démonstration. — Comme

$$(g(\alpha)/\alpha)^n = g(\alpha^n)/\alpha^n = g(a)/a = 1$$

nous avons $(g, \bar{a}) \in \mu_n$.
Soit $a, b \in F^*$ avec $\bar{a} = \bar{b} \in \Delta'$. Posons $b = \beta^n$, $a = \alpha^n, a = bc^n$ pour $\alpha, \beta \in E^*$ et $c \in F^*$. Par conséquent, $\alpha/\beta c \in \mu_n$, $\alpha/\beta \in F$ et

$$\frac{g(\alpha)}{\alpha} = \frac{g(\beta)}{\beta} \frac{g(\alpha/\beta)}{\alpha/\beta} = \frac{g(\beta)}{\beta}.$$

Donc (,) est bien définie.
i. Pour $a = \alpha^n$ et $b = \beta^n$, $\frac{g(\alpha\beta)}{\alpha\beta} = \frac{g(\alpha)}{\alpha}\frac{g(\beta)}{\beta}$.
ii. Comme $g(\zeta) = \zeta$ pour tout $\zeta \in \mu_n$, nous avons pour tout $g, h \in G$, $\alpha \in \Delta'$,

$$\frac{gh(\alpha)}{\alpha} = \frac{g(\alpha)}{\alpha} g\Big(\frac{h(\alpha)}{\alpha}\Big) = \frac{g(\alpha)}{\alpha}\frac{h(\alpha)}{\alpha}.$$

iii. Si $g(\alpha_i)/\alpha_i = 1$ pour $i = 1, \ldots, r$ ($\alpha_i^n = a_i$), alors $g = \mathrm{Id}$ sur $E = F(\alpha_1, \ldots, \alpha_r)$.
iv. Si $a = \alpha^n$ et $g(\alpha)/\alpha = 1$ pour tout $g \in G$, alors $\alpha \in (E^*)^G = F^*$ donc $a \in F^{*n}$ et $\bar{a} = 1$. □

Corollaire 22.17. — *i. L'application $g \mapsto (\overline{a} \mapsto (g, \overline{a}))$ est un morphisme de groupes injectif $G \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Delta', \mu_n)$, qui reste injectif par par restriction à $\mathrm{Hom}_{\mathbb{Z}}(\Delta, \mu_n)$.*
ii. L'application $\overline{a} \mapsto (g \mapsto (g, \overline{a}))$ est un morphisme de groupes injectif $\Delta' \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(G, \mu_n)$.
iii. Le groupe G est abélien de n-torsion et $G \simeq \mathrm{Hom}_{\mathbb{Z}}(G, \mu_n)$.

Démonstration. — i. D'après le lemme 22.16, l'application $g \mapsto (\overline{a} \mapsto (g, \overline{a}))$ est un homomorphisme de groupes injectif (idem pour ii.).
iii. D'après i., la partie de n-torsion $G[n]$ de G est abélienne et satisfait $G[n] = G$. Le groupe abélien $D(G) = \mathrm{Hom}_{\mathbb{Z}}(G, \mu_n)$ est fini et satisfait aussi $D(G)[n] = D(G)$. Si G est cyclique d'ordre $d|n$, alors $D(G)$ aussi. Comme $D(G \oplus H) = D(G) \oplus D(H)$, nous avons $G \simeq D(G)$. □

Théorème 22.18. — *(Kummer) Nous avons $\Delta = \Delta'$ et les isomorphismes de groupes abéliens suivants :*

$$G \simeq \mathrm{Hom}_{\mathbb{Z}}(\Delta, \mu_n), \quad \Delta \simeq \mathrm{Hom}_{\mathbb{Z}}(G, \mu_n).$$

En particulier, $G = \mathrm{Gal}(E/F) \simeq \Delta$ et $|\Delta| = |G| = [L : K]$.

Démonstration. — D'après le corollaire 22.17, $|G| \leq |\Delta|$ et $|\Delta'| \leq |G|$. Comme $\Delta \subset \Delta'$, $\Delta = \Delta'$ et $|G| = |\Delta|$. Les morphismes de groupes injectifs du corollaire 22.17 sont donc des isomorphismes. □

Exemple 22.19. — *i. Soit $p_1 < p_2 < p_3 < \cdots$ une suite croissante de nombres premiers et soit la suite d'extensions algébriques*

$$\mathbb{Q} = F_0 \subset \cdots \subset F_n = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) \subset E = \cup_{n=0}^{\infty} F_n = \mathbb{Q}(\sqrt{p_n}, n \geq 1).$$

D'après la théorie de Kummer, $\mathrm{Gal}(F_n/\mathbb{Q}) = \prod_{j=1}^{n}\{\pm 1\}$ *et*

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \prod_{j=1}^{\infty}\{\pm 1\}, \quad g \mapsto (g(\sqrt{p_j})/\sqrt{p_j})_{j \geq 1}.$$

22.4. Équations résolubles. —

Définition 22.20. — *Soit F un corps de caractéristique 0. Soit $f \in F[X]$. L'équation $f = 0$ est dite* **résoluble par radicaux** *s'il existe une tour de corps*

$$F = F_0 \subset F_1 \subset \cdots \subset F_m$$

telle que F_m contiennent un corps de décomposition de f, $F_i = F_{i-1}[\alpha_i]$, $\alpha_i^{m_i} \in F_{i-1}$, $m_i \in \mathbb{N}^*$, $1 \leq i \leq m$.

Exemples 22.21. — *i. Le groupe des permutations $\mathfrak{S}_n$ n'est pas résoluble pour $n \geq 5$. Par conséquent pour $f \in F[X]$ irréductible de degré n avec $G_f = \mathfrak{S}_n$, l'équation $f = 0$ n'est pas résoluble sur F.*
ii. L'équation $f = 0$ est résoluble si et seulement si ses solutions s'obtiennent par une suite d'additions, soustractions, multiplications, divisions et racines r-ième d'élements de F.

Lemme 22.22. — *Soit F un corps de caratéristique 0 contenant ζ une racine primitive n-ième de l'unité.*
i. Si $E = F[\alpha]$ avec $\alpha^n \in F$ et $\alpha^k \notin F$, $1 \leq k, \leq n-1$ alors E/F est une extension galoisienne cyclique d'ordre n.
ii. Si E est une extension (galoisienne) cyclique de degré n alors $E = F[\alpha]$ avec $\alpha^n \in F$.

Démonstration. — i. D'après la théorie de Kummer, E/F est galoisienne cyclique d'ordre n.
ii. Pour $\zeta \in K$ une racine primitive n-ième de l'unité et σ un générateur de $\mathrm{Gal}(L/K)$,

$$\sum_{i=0}^{n-1} \zeta^i \sigma^i$$

n'est pas nulle. Donc il existe $\gamma \in K^*$ tel que $\alpha = \sum_{i=0}^{n-1} \zeta^i \sigma^i(\gamma) \neq 0$. Nous avons alors $\sigma(\alpha) = \zeta^{-1}\alpha$. Ainsi $L = K[\alpha]$, $\alpha^n \in K$. □

Théorème 22.23. — *(Galois) Soit F un corps de caractéristique 0 et $f \in F[X]$. L'équation $f = 0$ est résoluble par radicaux si et seulement si le groupe de Galois du corps de décomposition F_f de f sur F est résoluble.*

Démonstration. — $\Longrightarrow$ Avec les notations de la définition 22.20, posons $r = \prod_{1 \leq i \leq m} m_i$. Soit E la plus petite extension galoisienne sur F contenant $F_m[\zeta_r]$. Alors E s'obtient comme extension de $F[\zeta_r]$ en rajoutant successivement des racines r-ièmes. Chacune de ses extensions est abelienne donc E/F est résoluble. Donc G_f quotient du groupe résoluble $\mathrm{Gal}(E/F)$ est résoluble.
$\Longleftarrow$ Notons $n = \deg f$ et ζ une racine primitive d'ordre $n!$ de l'unité et $F' = F[\zeta]$. Supposons que $\mathrm{Gal}(F_f/F)$ soit résoluble. Alors $\mathrm{Gal}(F'_f/F')$ s'identifie à un sous-groupe de $\mathrm{Gal}(F_f/F)$ est résoluble : il existe une suite de sous-groupes

$$G_m = \{e\} \subset G_{m-1} \subset \cdots \subset G_1 \subset G_0 = \mathrm{Gal}(F'_f/F')$$

avec G_i distingué dans G_{i-1} et G_{i-1}/G_i cyclique. Notons $F_i = F_f^{G_i}$. Alors

$$F \subset F' = F[\zeta] = F_0 \subset F_1 \subset \cdots \subset F_m = F'_f$$

avec $\mathrm{Gal}(F_i/F_{i-1})$ cyclique donc $F_i = F_{i-1}[\alpha_i]$ avec $\alpha_i^{[F_i:F_{i+1}]} \in F_{i-1}$. Donc f est résoluble. $\square$

PARTIE V

COMPLÉMENTS DE GÉOMÉTRIE ARITHMÉTIQUE

23. Anneaux de Dedekind

Les anneaux d'entiers de corps de nombres sont des anneaux de Dedekind. L'objet de ce chapitre est de définir ces notions et d'en déduire les propriétés de factorisations des idéaux en produit d'idéaux premiers dans un anneau d'entiers (Théorèmes 23.27).

23.1. Eléments entiers. —

Définition 23.1. — *Soit A un sous-anneau d'un anneau B. Un élément $\alpha \in B$ est dit* **entier** *sur A s'il est racine d'un polynôme unitaire à coefficients dans A.*

Exemple 23.2. — *Les entiers de $\mathbb{Q}$ sur $\mathbb{Z}$ sont les éléments de $\mathbb{Z}$. En effet si $x = r/s \in \mathbb{Q}$ (avec $\mathrm{PGCD}(r,s) = 1$) annule $X^n + a_1X^{n-1} + \cdots + a_n$. Alors $r^n + a_1r^{n-1}s + \cdots + a_ns^n = 0$ et s divise r^n donc $s = \pm 1$ et $x \in \mathbb{Z}$.*

Proposition 23.3. — *Soit $A \subset B$ deux anneaux et $x \in B$. Les affirmations suivantes sont équivalentes :*
i. x est entier sur A,
ii. $A[x] \subset B$ est un A-module de type fini,
iii. $A[x] \subset C \subset B$, pour un sous-anneau C de B qui est un A-module de type fini,
iv. il existe un $A[x]$-module fidèle M (i.e. tel que $\mathrm{Ann}_{A[x]}(M) = 0$) qui est un A-module de type fini par restriction des scalaires.

Démonstration. — i.$\Longrightarrow$ ii. En effet, comme x est entier

$$x^n \in M := A + Ax + \cdots + Ax^{n-1}.$$

Montrons par induction que $x^k \in M$ pour tout $k \in \mathbb{N}$. C'est vrai pour $k \leq n$. Soit $k > n$, supposons $x^{k-1} \in M$. Alors x^{k-1} admet une écriture sous la forme $x^{k-1} = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ avec $b_i \in A$ et $x^k \in M + Ax^n = M$. Donc $M = A[x]$ est un A-module de type fini.
ii.$\Longrightarrow$ iii. Il suffit de prendre $C = A[x]$.
iii.$\Longrightarrow$ iv. Remarquons que C est fidèle. En effet si $y \in \mathrm{Ann}_{A[x]}C$, $y \cdot 1 = 0$ donc $y = 0$. Il suffit donc de prendre $M = C$.
iv.$\Longrightarrow$ i. Soit $f \in \mathrm{Hom}_A(M,M)$ défini par $f(m) = xm$. Alors (d'après Proposition 11.15) nous avons une équation de la forme

$$f^n + a_1f^{n-1} + \cdots + a_n\,\mathrm{Id} = 0, a_i \in A.$$

Donc $x^n + a_1x^{n-1} + \cdots + a_n \in \mathrm{Ann}_{A[x]}M = 0$. D'où i. $\square$

Corollaire 23.4. — *Soit $A \subset B$ deux anneaux, $x_1, \ldots, x_n \in B$ des éléments entiers sur A. Alors le sous-anneau $A[x_1, \ldots, x_n]$ de B est un A-module de type fini.*

Démonstration. — Nous raisonnons par induction sur n. Le cas $n = 1$ a été établi (Proposition 23.3). Supposons $n > 1$ et le A-module $C = A[x_1, \ldots, x_{n-1}]$ est de type fini de générateurs $\{y_1, \ldots, y_k\}$. Comme x_n est entier sur C, il existe $z_i \in C[x_n]$ avec $C[x_n] = Cz_1 + \cdots + Cz_\ell$. Le A-module Cz_i est engendré par $\{z_i y_1, \ldots, z_i y_k\}$. Donc $\{z_i y_j, 1 \leq i \leq \ell, 1 \leq j \leq k\}$ engendre le A-module $A[x_1, \ldots, x_n]$. □

Exemple 23.5. — *Si B est entier sur A et de type fini comme A-algèbre, alors B est de type fini comme A-module.*

Définition 23.6. — *Soit $A \subset B$ deux anneaux. Alors*

$$C = \{x \in B | x \text{ est entier sur } A\}$$

est appelé la **cloture intégrale** *de A dans B. Si $C = B$, B est dit* **entier sur** *A.*

Exemple 23.7. — *Soit $A \subset B \subset C$ des anneaux. Si B est entier sur A et C est entier sur B, alors C est entier sur A.*

Lemme 23.8. — *Soit $A \subset B$ deux anneaux. La cloture intégrale de A dans B est un sous-anneau de B contenant A.*

Démonstration. — Si $x, y \in C$ alors $A[x, y]$ est un A-module de type fini (Corollaire 23.4) qui contient $x + y$ et xy, donc $x + y, xy$ sont entiers sur A. □

Lemme 23.9. — *Soit $A \subset B$ une extension entière d'anneaux avec B intègre. Alors A est un corps si et seulement si B est un corps.*

Démonstration. — Si A est un corps, alors $A[b]$ est un A-espace vectoriel de dimension finie pour tout $b \in B$. Si $b \neq 0$, la multiplication par b est un morphisme A-linéaire injectif (car B est intègre) donc surjectif. Par conséquent b est inversible dans $A[b] \subset B$.
Réciproquement si B est un corps, alors tout élément non nul $a \in A$ admet un inverse $b \in B$. Comme b est entier sur A, il est racine d'un polynôme à coefficients dans A : $b^n + a_1 b^{n-1} + \cdots + a_n = 0$. En multipliant chaque terme par a^{n-1}, nous obtenons $b = -(a_1 + a_2 a + \cdots + a_n a^{n-1}) \in A$. □

Théorème 23.10. — *(Théorème d'Artin-Tate). Soit $A \subset B \subset C$ des anneaux tels que A noethérien, C est une A-algèbre de type fini et C est une B-algèbre entière. Alors B est une A-algèbre de type fini.*

Démonstration. — Comme C est une A-algèbre de type fini, il existe $c_i \in C$ tels que $C = A[c_1, \ldots, c_m]$. Comme C est entier sur B, c_i est racine d'un polynôme $X^n + b_{1,i}X^{n-1} + \cdots + b_{n,i} \in B[X]$. Donc tous les c_i sont entiers dans le sous-anneau $B' = A[b_{ij}, i, j] \subset B$ et B' est noethérien. De plus $C = B'[c_1, \ldots, c_m]$ est un B'-module de type fini (Corollaire 23.4). L'anneau B est un sous-module du B'-module de type fini C, donc B est un B'-module de type fini : $B = B'b_1 + \cdots + B'b_r$. Comme B est un anneau, $B = B'[b_1, \ldots, b_r] = A[b_{ij}, b_k, i, j, k]$ est une A-algèbre de type fini. □

Le théorème d'Artin-Tate a pour conséquence une généralisation de l'isomorphisme de K-algèbres $K[X_1, \ldots, X_n]^{\mathfrak{S}_n} = K[\Sigma_1, \ldots, \Sigma_n]$ à tout groupe fini :

Corollaire 23.11. — *Soit K un corps et G un groupe fini agissant sur $K[X_1, \ldots, X_n]$ via des morphismes d'algèbres. Alors $K[X_1, \ldots, X_n]^G$ est une K-algèbre de type fini.*

Démonstration. — Il s'agit d'appliquer le théorème d'Artin-Tate à $K \subset K[X_1, \ldots, X_n]^G \subset K[X_1, \ldots, X_n]$. Pour cela, il faut vérifier que tout élément $f \in K[X_1, \ldots, X_n]$ est entier sur $K[X_1, \ldots, X_n]^G$. Or f est racine du polynôme unitaire $P(T) = \Pi_{g \in G}(T - g \cdot f) \in K[X_1, \ldots, X_n]^G[T]$. □

Remarque 23.12. — *(14-ième problème d'Hilbert). Pour quel $G \subset \mathrm{GL}_n(\mathbb{C})$, $\mathbb{C}[X_1, \ldots, X_n]^G$ est-il une $\mathbb{C}$-algèbre de type fini ?*

Définition 23.13. — *Soit F une extension algébrique de $\mathbb{Q}$. L'***anneau des entiers** *$\mathcal{O}_F$ de F est l'anneau des éléments de F entiers sur $\mathbb{Z}$:*

$$x \in \mathcal{O}_F \Longleftrightarrow \exists P \in \mathbb{Z}[X] \text{ unitaire tel que } P(x) = 0.$$

Exemples 23.14. — *i. Si $p \geq 3$ est premier, l'anneau des entiers de $F = \mathbb{Q}(\zeta_p)$ est $\mathbb{Z}[\zeta_p]$. L'anneau des entiers de $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ est $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.*
ii. Soit $d \in \mathbb{Z}$ sans facteur carré. Si $d \equiv 2, 3 \mod 4$ alors $\mathbb{Z}[\sqrt{d}]$ est l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$. Si $d \equiv 1 \mod 4$, l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ est $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.
iii. Si $x \in \mathcal{O}_F - \{0\}$ tel que $|\sigma(x)| < 1$ pour tout plongement $\sigma : F \longrightarrow \mathbb{C}$, alors x est une racine de l'unité.
iv. Le sous-anneau $\overline{\mathbb{Z}}$ de $\mathbb{C}$ des entiers algébriques n'est pas noethérien mais est de Bézout.
v. Soit F un corps de nombres, i.e. une extension finie F de $\mathbb{Q}$. L'anneau des entiers $\mathcal{O}_F$ de F est un $\mathbb{Z}$-module libre de rang $d = [F : \mathbb{Q}]$.

23.2. Anneaux intégralement clos. —

Définition 23.15. — *Soient $A \subset B$ deux anneaux. Si A coïncide avec la cloture intégrale de A dans B, l'anneau A est dit* **intégralement fermé** *dans B.*

Un anneau intègre intégralement fermé dans son corps de fractions est dit **intégralement clos**.

Exemples 23.16. — *i. L'anneau $\mathbb{Z}$ et intégralement clos.*
ii. Tout anneau factoriel ou intègre à PGCD *est intégralement clos (même preuve que sur $\mathbb{Z}$ voir Exemple 23.2).*
iii. L'anneau $\mathbb{Z}[\sqrt{5}]$ n'est pas intégralement clos.
iv. Soit A intègre et B la cloture intégrale de A dans une extension finie E du corps des fractions F de A. Soit S une partie multiplicative de A. Alors $S^{-1}B$ est la cloture intégrale de $S^{-1}A$ dans E. En particulier, si A est intégralement clos alors $S^{-1}A$ aussi.

Lemme 23.17. — *Soit F le corps des fractions de A intègre et E une extension finie de F. Supposons A intégralement clos. Un élément $\alpha \in E$ est entier sur A si et seulement son polynôme minimal sur F est à coefficients dans A.*

Démonstration. — $\Longrightarrow$ Soit $\alpha \in E$ entier sur A. Il existe $g \in A[X]$ non nul avec $g(\alpha) = 0$. Soit β une racine de $f \in F[X]$ polynôme minimal et σ le F-isomorphismes $F[\alpha] \longrightarrow F[\beta]$, $\alpha \mapsto \beta$. Ainsi $\sigma(g)(\beta) = 0$, donc toutes les racines de f sont entières sur A. Les coefficients de f sont des éléments de F, entiers sur A. D'où $f \in A[X]$. □

Proposition 23.18. — *La cloture intégrale d'un anneau intègre A dans une extension algébrique E de son corps des fractions est intégralement close. En particulier l'anneau des entiers $\mathcal{O}_F$ d'un corps de nombres F est intégralement clos.*

Démonstration. — Soit B la clôture intégrale de A dans E et C la clôture intégrale de B dans E. Alors C est entier sur A (voir Exemple 23.7) donc $C \subset B$. □

23.3. Anneaux de Dedekind. —

Définition 23.19. — *Un* **anneau de Dedekind** *est un anneau qui n'est pas un corps qui satisfait les trois propriétés suivantes :*
i. A est intègre et noethérien,
ii. Si I est un idéal premier non nul de A, alors I est maximal,
iii. A est intégralement clos.

Exemples 23.20. — *i. Un anneau principal est de Dedekind. En effet il est intègre et noethérien. Tout idéal premier non nul est maximal. Enfin il est factoriel donc intégralement clos.*
ii. Soit A un anneau de Dedekind et S une partie multiplicative de A. Alors $S^{-1}A$ est de Dedekind. En effet, $S^{-1}A$ est intègre, noethérien et intégralement clos. De plus, comme A est intègre, $\mathfrak{p} \mapsto \mathfrak{p}S^{-1}A$ établit une bijection de l'ensemble des idéaux premiers de A tels que $\mathfrak{p} \cap S = \emptyset$ et l'ensemble des idéaux premiers de

$S^{-1}A$. L'application réciproque est $\mathfrak{p} \mapsto \mathfrak{p} \cap A$. Donc les idéaux premiers non nuls de $S^{-1}A$ sont maximaux.
iii. L'anneau des entiers d'un corps de nombres est un anneau de Dedekind (voir Théorème 23.21).

Théorème 23.21. — *Soit A un anneau de Dedekind de corps des fractions F et B la cloture intégrale de A dans une extension finie séparable E de F. Alors B est un anneau de Dedekind.*

Démonstration. — • Montrons que B est noethérien. Tout élément $\beta \in E$ satisfait une équation de la forme

$$\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0, \quad a_j \in F.$$

Soit $d \in A$ le dénominateur commun des a_j, ainsi $da_j \in A$ pour tout j et

$$(d\beta)^n + da_1(d\beta)^{n-1} + \cdots + a_n d^n = 0$$

donc $d\beta \in B$. Si $(\beta_i)_{1\leq i\leq m}$ une base de E/F, alors il existe $d \in A$ tel que $d\beta_i \in B$, $1 \leq i \leq m$. Alors $(d\beta_i)_{1\leq i\leq m}$ est encore une base de E/F. Nous pouvons donc supposer que $(\beta_i)_{1\leq i\leq m}$ est une base de E/F composée d'éléments de B.
La trace est une forme bilinéaire non dégénérée (Corollaire 19.15), donc il existe une base $(\beta'_i)_{1\leq i\leq m}$ de E/F telle que $\mathrm{Tr}_{E/F}(\beta_i\beta'_j) = \delta_{ij}$. Soit $\beta = \sum_{j=1}^m b_j\beta'_j \in B$. Comme $\beta, \beta_i \in B$, $\mathrm{Tr}_{E/F}(\beta\beta_i) \in A$ et

$$\mathrm{Tr}_{E/F}(\beta\beta_i) = \mathrm{Tr}_{E/F}(\sum_j b_j\beta'_j\beta_i) = \sum_j b_j\delta_{ij} = b_i$$

donc $b_i \in A$ et

$$B \subset A\beta'_1 + A\beta'_2 + \cdots + A\beta'_m$$

est contenu dans un A-module de type fini. Donc tout idéal de B est de type fini comme A-module, donc de type fini comme B-module. Donc B est noethérien.
• B est intègre et intégralement clos : en effet B est la cloture intégrale de A dans une extension algébrique E du corps des fractions F de A.
• Il reste à montrer que tout idéal premier non nul $\mathfrak{p}$ de B est maximal. Soit $\beta \in \mathfrak{p}$, $\beta \neq 0$. Comme β est entier sur A, il est racine d'une équation de degré minimum

$$\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0, \quad a_i \in A.$$

Ainsi $a_n \neq 0$. Comme $a_n \in \beta B \cap A$, $\mathfrak{p} \cap A \neq (0)$. Ainsi $\mathfrak{q} = \mathfrak{p} \cap A$ est un idéal premier propre, il est donc maximal et $A/\mathfrak{q}$ est un corps. L'application

$$A/\mathfrak{q} \longrightarrow B/\mathfrak{p}, \quad a + \mathfrak{q} \mapsto a + \mathfrak{p}$$

identifie $A/\mathfrak{q}$ à un sous-corps de l'anneau intègre $B/\mathfrak{p}$. Comme B est entier sur A, $B/\mathfrak{p}$ est entier sur $A/\mathfrak{q}$ donc $B/\mathfrak{p}$ est un corps (Lemme 23.9) et $\mathfrak{p}$ est maximal. □

Nous allons donner une caractérisation des anneaux de Dedekind en termes de leurs localisations.

Définition 23.22. — *Une* **valuation discrète** *sur un corps F est une application*

$$v : F \longrightarrow \mathbb{Z} \cup \{+\infty\}$$

qui satisfait
i. (séparation) $\forall f \in F, v(f) = +\infty \Longleftrightarrow f = 0$,
ii. (compatibilité avec le produit) $\forall f, g \in F, v(fg) = v(f) + v(g)$,
iii. (inégalité ultramétrique) $v(f + g) \geq \min(v(f), v(g))$.
*L'***anneau de valuation** *de v est le sous-anneau*

$$A = \{f \in F, v(f) \geq 0\}.$$

C'est un anneau local d'idéal maximal $\mathfrak{m} = \{f \in A | v(f) > 0\} = (\pi)$ *où* $\pi \in A$ *est un élément quelconque de valuation* $v(\pi) = 1$. *Un tel élément est dit* **uniformisante** *de A.*
Un anneau intègre est dit **anneau de valuation discrète** *si c'est l'anneau d'une valuation discrète sur son corps des fractions.*

Exemples 23.23. — *i. Un anneau de valuation discrète est un anneau intègre local dont l'idéal maximal* $\mathfrak{m} = (\pi)$ *est principal et tel que* $A - \{0\} = \sqcup_{n \in \mathbb{N}} \pi^n A^*$. *Son corps des fractions est alors* $F = \sqcup_{n \in \mathbb{Z}} \pi^n A^*$ *et la valuation est* $v(\pi^n A^*) = n$.
ii. Soit A un anneau de valuation discrète v et d'uniformisante π. La valuation v confère à A la structure d'anneau topologique pour la distance définie par $d(x, y) = \rho^{v(x-y)}$, $x, y \in A$. *Cette topologie est indépendante du choix de ρ fixé dans* $]0, 1[$. *Le complété* $\hat{A} = \varprojlim A/\pi^n A$ *pour cette topologie est encore un anneau de valuation discrète pour une valuation prolongeant v.*
iii. Plus généralement, l'anneau A est dit séparé et complet pour la topologie I-adique où I est un idéal de A si l'application naturelle $A \longrightarrow \varprojlim A/I^n A$ *est un isomorphisme.*

Lemme 23.24. — *Soit A un anneau intègre. Alors A est de valuation discrète si et seulement si A est local et de Dedekind.*

Démonstration. — Si A est de valuation discrète alors il est principal donc de Dedekind. Réciproquement supposons que A est local de Dedekind et montrons que tout idéal de A est principal engendré par une puissance d'un élément π que nous commençons par construire.
• Soit $\alpha \in A$ un élément non nul non inversible, $B = A/(\alpha)$. Pour tout $b \in B - \{0\}$, nous notons

$$\mathrm{Ann}(b) = \{a \in A, ab = 0\}$$

Alors $\mathrm{Ann}(b)$ est un ideal propre de A (car $1 \notin \mathrm{Ann}(b)$ et $\alpha \in \mathrm{Ann}(b)$). Comme A est noetherien, il existe $b \in B - \{0\}$ tel que $\mathrm{Ann}(b)$ soit maximal pour l'inclusion. Nous notons $b = \beta + (\alpha)$ et $\mathfrak{p} = \mathrm{Ann}(b)$ idéal propre associé.
Montrons que $\mathfrak{p}$ est premier. Par l'absurde, supposons qu'il existe $x, y \notin \mathfrak{p}$ avec $xy \in \mathfrak{p}$. Mais alors $y\beta + (\alpha) \neq 0$ dans B car $y \notin \mathfrak{p}$. L'idéal $\mathrm{Ann}(y\beta + (\alpha))$ contient strictement $\mathfrak{p}$ (car il contient aussi x) ce qui contredit la maximalité de $\mathfrak{p}$. Donc $\mathfrak{p}$ est premier. Comme A est local de Dedekind, $\mathfrak{p}$ est l'unique idéal maximal de

A.
L'élement $\beta/\alpha \notin A$ car sinon $\beta = \alpha \cdot (\beta/\alpha) \in (\alpha)$ et $b = 0$ (exclu !).
Montrons que $\alpha/\beta \in A$ et $\mathfrak{p} = (\alpha/\beta)$. Nous avons $\beta\mathfrak{p} \subset (\alpha)$ donc $\beta\mathfrak{p}/\alpha$ est un idéal de A. Si $\beta\mathfrak{p}/\alpha\mathfrak{p}$, comme $\mathfrak{p}$ est de type fini, β/α est entier sur A donc $\beta/\alpha \in A$ ce qui est exclu. Par conséquent $\beta\mathfrak{p}/\alpha = A$ donc $\alpha/\beta \in A$ et $\mathfrak{p} = (\alpha/\beta)$. Nous notons $\pi = \alpha/\beta$.
• Montrons que pour tout idéal I propre de A, il existe $n \in N^*$ tel que $I = (\pi^n)$. En effet la suite

$$I \subset \pi^{-1}I \subset \pi^{-2}I \subset \cdots \subset \operatorname{Frac} A$$

est croissante. Cette suite est même strictement croissante car si $\pi^{-r}I = \pi^{-r-1}I$, alors $\pi^{-1}(\pi^{-r}I) = I\pi^{-r}$ donc π^{-1} est entier sur A donc $\pi^{-1} \in A$ ce qui est exclu. Comme la suite est strictement croissante et que A est noetherien, il existe $n \in N^*$ minimum tel que $\pi^{-n}I \subset A$ et $\pi^{-n-1}I \not\subset A$. Alors $\pi^{-n}I \not\subset \mathfrak{p}$. Donc $\pi^{-n}I = A$ et $I = (\pi^n)$. □

Corollaire 23.25. — *Si A est un anneau de Dedekind, $\mathfrak{m} \in \operatorname{Spm} A$. Alors le localisé $A_\mathfrak{m}$ est un anneau de valuation discrète.*

Démonstration. — D'après le Lemme 23.24, il suffit de montrer que $A_\mathfrak{m}$ est de Dedekind. Or si A est intègre et S multiplicative alors A noetherien (resp. intégralement clos) implique $S^{-1}A$ noetherien (resp. intégralement clos). Donc A de Dedekind implique que $S^{-1}A$ est un corps ou est de Dedekind. □

Corollaire 23.26. — *Un anneau intègre A qui n'est pas un corps est de Dedekind si et seulement si il est noethérien et ses localisations en tout idéal maximal $\mathfrak{m}$ sont des anneaux $A_\mathfrak{m}$ de valuation discrète.*

Démonstration. — $\Longrightarrow$ Soit A un anneau de Dedekind de corps des fractions F. Alors pour tout idéal maximal $\mathfrak{m} \in \operatorname{Spm} A$, le localisé $A_\mathfrak{m}$ de A en $\mathfrak{m}$ est de valuation discrète (Corollaire 23.25).
$\Longleftarrow$ Remarquons que $\cap_{\mathfrak{m}\in\operatorname{Spm} A} A_\mathfrak{m} = A$. En effet, pour $x \in F$, définissons l'idéal de A, $I = \{a \in A | ax \in A\}$. Alors $x \in A_\mathfrak{m} \Longleftrightarrow I \not\subset \mathfrak{m}$. Par conséquent si $x \in \cap_{\mathfrak{m}\in\operatorname{Spm} A} A_\mathfrak{m}$, $I = A$ donc $x \in A$.
Soit $x \in F$ entier sur A. Alors x est entier sur tout $A_\mathfrak{m}$ donc est inclus dans $\cap_{\mathfrak{m}\in\operatorname{Spm}(A)} A_\mathfrak{m} = A$. Donc A est intégralement clos.
Soit $\mathfrak{p}$ un idéal premier non nul de A. Si $\mathfrak{p} \subset \mathfrak{m}$, son image $\mathfrak{p}A_\mathfrak{m}$ dans $A_\mathfrak{m}$ est un idéal premier donc maximal. Donc $\mathfrak{p} = \mathfrak{m}$ est maximal. □

Théorème 23.27. — *Soit A un anneau de Dedekind. Alors les applications*

$$\psi : \{\textit{idéal non nul de } A\} \longrightarrow \oplus_{\mathfrak{m}\in\operatorname{Spm} A}\mathbb{N},$$

$$\psi(I) = (v_\mathfrak{m}(I)) \textit{ tel que } IA_\mathfrak{m} = (\mathfrak{m}A_\mathfrak{m})^{v_\mathfrak{m}(I)}, \mathfrak{m} \in \operatorname{Spm} A,$$

et

$$\psi' : \oplus_{\mathfrak{m}\in\operatorname{Spm} A}\mathbb{N} \longrightarrow \{\textit{idéaux propres de } A\}, \quad (n_\mathfrak{m}) \mapsto \Pi_{\mathfrak{m}\in\operatorname{Spm} A}\mathfrak{m}^{n_\mathfrak{m}}$$

sont inverses l'une de l'autre et $\psi(IJ) = \psi(I)+\psi(J)$ *pour tous* I, J *idéaux propres de* A.
En particulier, tout idéal propre non nul I *de* A *admet une factorisation unique en produit d'idéaux premiers.*

Démonstration. — Siot I un idéal propre de A. Comme A est noetherien, il existe des idéaux premiers $\mathfrak{m}_i$ tels que $\mathfrak{m}_1^{\alpha_1} \cdots \mathfrak{m}_r^{\alpha_r} \subset I$. En effet, notons J un idéal maximal pour la propriété de ne pas inclure un produit fini d'idéaux premiers. Nous remarquons que J n'est pas premier. Donc il existe $x, y \in A - J$ tels que $xy \in J$. Alors J est strictement inclus dans $(y) + J$ et dans $(x) + J$ qui sont donc produits finis d'idéaux premiers. Or $((x)+J)((y)+J) \subset J$ contredit la définition de J.
Nous avons

$$A/\mathfrak{m}_1^{\alpha_1} \cdots \mathfrak{m}_r^{\alpha_r} \sim A/\mathfrak{m}_1^{\alpha_1} \times \cdots \times A/\mathfrak{m}_r^{\alpha_r} \sim A_{\mathfrak{m}_1}/(\mathfrak{m}_1 A_{\mathfrak{m}_1})^{\alpha_1} \times \cdots \times A_{\mathfrak{m}_r}/(A_{\mathfrak{m}_r}\mathfrak{m}_r)^{\alpha_r}.$$

L'idéal $I/\mathfrak{m}_1^{\alpha_1} \cdots \mathfrak{m}_r^{\alpha_r}$ s'identifie à $\mathfrak{m}_1^{\beta_1} A_{\mathfrak{m}_1}/(A_{\mathfrak{m}_1}\mathfrak{m}_1)^{\alpha_1} \times \cdots \times \mathfrak{m}_r^{\beta_r} A_{\mathfrak{m}_r}/(A_{\mathfrak{m}_r}\mathfrak{m}_r)^{\alpha_r}$ dans le produit d'anneaux de valuation discrète. Donc il correspond à l'idéal $\mathfrak{m}_1^{\beta_1} \cdots \mathfrak{m}_r^{\beta_r}/\mathfrak{m}_1{}^{\alpha_1} \cdots \mathfrak{m}_r^{\alpha_r}$ dans $A/\mathfrak{m}_1^{\alpha_1} \cdots \mathfrak{m}_r^{\alpha_r}$. Donc $I = \mathfrak{m}_1^{\beta_1} \cdots \mathfrak{m}_r^{\beta_r}$ dans A. □

Le théorème 23.27 montre qu'il est possible de faire des preuves analogues à celles dans les anneaux factoriels en remplaçant éléments irréductibles par idéaux premiers. C'est la clé de la démonstration de Kummer du théorème de Fermat pour les nombres premiers réguliers. La démonstration générale demande une analyse plus fine de la structure p-adique des équations algébriques (où p un nombre premier).

23.4. Ramification. —

Définition 23.28. — *Soit* A *un anneau de Dedekind de corps des fractions* F *et* B *la cloture intégrale de* A *dans une extension finie séparable* E *de* F. *Tout idéal* $\mathfrak{p} \in A$ *se factorise dans* B *sous la forme*

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, e_i \geq 1, \mathfrak{P} \in \operatorname{Spec} B.$$

Si un des coefficients $e_i > 1$, *l'idéal* $\mathfrak{p}$ *est dit* **ramifié** *dans* B *(ou* E*). Le nombre* $e_i = e(\mathfrak{P}_i/\mathfrak{p})$ *est dit* **indice de ramification** *et le degré* $f(\mathfrak{P}_i/\mathfrak{p}) = [B/\mathfrak{P}_i : A/\mathfrak{p}]$ *est dit* **degré résiduel**.
Si aucun idéal premier de A *n'est ramifié dans* B, *nous disons que l'extension* E/F *est non ramifiée.*

Exemples 23.29. — *i. L'idéal* $(2) = (1+i)^2 \in \mathbb{Z}[i]$ *donc* (2) *est ramifié d'indice de ramification 2.*
ii. L'idéal $(5) = (2+i)(2-i)$ *est non ramifié dans* $\mathbb{Z}[i]$.

Lemme 23.30. — *Soit* A *un anneau de Dedekind de corps des fractions* K *et* B *la cloture intégrale de* A *dans une extension finie séparable* L *de* K. *Un idéal* $\mathfrak{P}$ *de* B *divise l'idéal* $\mathfrak{p}$ *de* A *si et seulement si* $\mathfrak{p} = \mathfrak{P} \cap K$.

Démonstration. — $\Longrightarrow$ Si $\mathfrak{P}$ divise $\mathfrak{p}$, alors $\mathfrak{p} \subset \mathfrak{P} \cap K$ et $\mathfrak{P} \cap K \neq A$. Comme $\mathfrak{p}$ est maximal (car A est de Dedekind), $\mathfrak{p} = \mathfrak{P} \cap K$.
$\Longleftarrow$ Si $\mathfrak{p} \subset \mathfrak{P}$, alors $\mathfrak{p}B \subset \mathfrak{P}$ donc $\mathfrak{P}$ apparait dans la factorisation de $\mathfrak{p}B$. $\square$

Théorème 23.31. — *Soit A un anneau de Dedekind de corps des fractions K et B la cloture intégrale de A dans une extension finie séparable L de K de degré m. Soit $\mathfrak{p}$ un idéal premier de A et $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ sa décomposition dans B. Alors*

$$\sum_{i=1}^{g} e_i f_i = m.$$

Si de plus L/K est galoisienne, alors les indices de ramification sont égaux $e_i = e$, $1 \leq i \leq g$ et les degrés résiduels aussi $f_i = f$, $1 \leq i \leq g$. Ainsi $efg = m$.

Démonstration. — • Montrons $\sum_{i=1}^{g} e_i f_i = [B/\mathfrak{p}B : A/\mathfrak{p}]$. D'après le théorème chinois $B/\mathfrak{p}B = B/\Pi\mathfrak{P}_i^{e_i} \simeq \Pi B/\mathfrak{P}_i^{e_i}$, donc il suffit de montrer

$$[B/\mathfrak{P}_i^{e_i} : A/\mathfrak{p}] = e_i f_i.$$

Par définition de f_i, $B/\mathfrak{P}_i$ est un corps de degré f_i sur $A/\mathfrak{p}$. De plus $\mathfrak{P}_i^r/\mathfrak{P}_i^{r+1}$ est un $B/\mathfrak{P}_i$-module et comme il n'y a pas d'idéal entre $\mathfrak{P}_i^r$ et $\mathfrak{P}_i^{r+1}$, il est de dimension 1 comme $B/\mathfrak{P}$-espace vectoriel donc de dimension f_i comme $A/\mathfrak{p}$ espace vectoriel. Donc $B/\mathfrak{P}^{e_i}$ est de dimension $e_i f_i$ sur $A/\mathfrak{p}$.
• Montrons $[B/\mathfrak{p}B : A/\mathfrak{p}] = m$ quand B est un A-module libre. L'isomorphisme de A-modules $A^n \longrightarrow B$ induit par tensorisation par K, un isomorphisme $K^n \longrightarrow L$. Donc $n = m$. Par tensorisation par $A/\mathfrak{p}$, nous obtenons un isomorphisme $(A/\mathfrak{p})^n \longrightarrow B/\mathfrak{p}B$ d'où $[B/\mathfrak{p}B : A/\mathfrak{p}] = m$.
• Montrons $[B/\mathfrak{p}B : A/\mathfrak{p}] = m$ en général. Soit $S = A - \mathfrak{p}$, $B' = S^{-1}B$ et $A' = S^{-1}A$. Alors B est la cloture intégrale de A' dans L et $\mathfrak{p}B' = \Pi(\mathfrak{P}_i B')^{e_i}$. Donc $\sum e_i f_i = [B'/\mathfrak{p}B' : A'/\mathfrak{p}A']$. Or A' est principal donc $[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = m$.
• Supposons L/K galoisienne. Soit $\sigma \in \mathrm{Gal}(L/K)$. Ainsi σ induit un isomorphisme de B et $\sigma\mathfrak{P}$ est un idéal premier. De plus si $\mathfrak{P}$ divise $\mathfrak{p}$ alors $\sigma\mathfrak{P}$ divise $\mathfrak{p}$ (Lemme 23.30), donc $e(\sigma\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$ et $f(\sigma\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$. Il suffit donc de montrer que $\mathrm{Gal}(L/K)$ agit transitivement sur les idéaux de B divisant $\mathfrak{p}$. Soit $\mathfrak{P}$ et $\mathfrak{P}'$ divisant $\mathfrak{p}$ avec $\sigma\mathfrak{P} \neq \mathfrak{P}'$ pour tout $\sigma \in \mathrm{Gal}(L/K)$. D'après le théorème chinois, il existe $\beta \in \mathfrak{P}' - \cup_\sigma \sigma\mathfrak{P}$. Soit $b = Nm_{L/K}(\beta) = \Pi_\sigma \beta$. Alors $b \in A \cap \mathfrak{P}' = \mathfrak{p}$ et pour tout $\sigma \in \mathrm{Gal}(L/K)$, $\beta \notin \sigma^{-1}\mathfrak{P}$ donc $\sigma\beta \notin \mathfrak{P}$. Or $\prod_\sigma \sigma\beta \in \mathfrak{p} \subset \mathfrak{P}$ ce qui est exclu car $\mathfrak{P}$ est premier. $\square$

23.5. Anneau de valuation discrète d'un corps de fonctions. — L'objet de ce paragraphe est d'expliciter les anneaux de valuations des corps de fonctions F/k, i.e $k(x)/k$ transcendante et $F/k(x)$ algébrique finie.

24. Lemme de Hensel. Anneau des vecteurs de Witt

Dans ce chapitre, p désigne un nombre premier fixé. Dans un anneau de valuation discrète complet, il est facile de résoudre des équations polynomiales. Le lemme de Hensel (24.1) montre qu'il suffit de relever les solutions de l'équation réduite modulo l'idéal maximal. Par exemple, pour résoudre une équation diophantienne (équation polynomiale à coefficients dans $\mathbb{Z}$) dans $\mathbb{Z}_p$, il suffit de relever ses solutions modulo les puissances p^n successives car $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. L'objet de ce paragraphe est de généraliser la construction des entiers p-adiques $\mathbb{Z}_p$ notamment pour relever les solutions appartenant à un corps fini $\mathbb{F}_q$ (pour $q = p^r$). Ceci nous conduit à définir l'anneau des vecteurs de Witt sur $\mathbb{F}_q$ qui est un anneau local $W(\mathbb{F}_q)$ de corps résiduel $\mathbb{F}_q$ non ramifié sur $\mathbb{Z}_p$ (§24.3). Il s'agit de l'anneau des entiers de l'extension non ramifiée de degré r du corps des fractions $\mathbb{Q}_p$ de $\mathbb{Z}_p$ (§24.2). Cette construction est fonctorielle, de foncteur adjoint le basculement (§24.4).

24.1. Lemme de Hensel. — Dans ce paragraphe, A un anneau de valuation discrète complet de corps résiduel k et π est une uniformisante (générateur de l'idéal maximal).

Proposition 24.1. — *A un anneau de valuation discrète complet d'uniformisante π. Soit $f \in A[X]$ et a_0 une racine simple de $f \mod \pi$. Alors il existe une unique racine $a \in A$ de f avec $a \equiv a_0 \mod \pi$.*

Démonstration. — Nous construisons une suite de Cauchy $(a_n)_{n\in\mathbb{N}}$ de A dont la limite est la racine a cherchée. Pour cela nous procédons par récurrence et nous supposons avoir construit $a_n \in A$ tel que $a_n \equiv a_0 \mod \pi$ et

$$f(a_n) \equiv 0 \mod \pi^{n+1}.$$

Posons $a_{n+1} = a_n + h\pi^{n+1}$, pour $h \in A$. En notant $f'(X)$ la dérivée de $f(X)$, nous avons

$$f(a_n + h\pi^{n+1}) = f(a_n) + h\pi^{n+1}f'(a_n) \mod \pi^{n+2}.$$

Comme $\pi^{n+1}|f(a_n)$ et $f'(a_n) \equiv f'(a_0) \mod \pi$ est non nul, nous pouvons choisir $h \equiv -\frac{f(a_n)}{\pi^{n+1}}f'(a_n)^{-1} \mod \pi$ et construire ainsi une suite $(a_n)_{n\in\mathbb{N}}$ qui converge vers une racine $a \in A$ de f avec $a \equiv a_0 \mod \pi$. La racine a satisfaisant ces propriétés est unique car $a \mod \pi^n$ est déterminé de façon unique pour chaque n. □

Lemme 24.2. — *Soit A un anneau local de corps résiduel k. Si $f, g \in A[X]$ sont tels que leurs images $\bar{f}, \bar{g} \in k[X]$ soient premières entre elles et f est unitaire, alors il existe $u, v \in A[X]$ avec $\deg u < \deg g$ et $\deg v < \deg f$ tels que $uf+vg = 1$.*

Démonstration. — Soit $M = A[X]/(f, g)$ et $\mathfrak{m}$ l'idéal maximal de A. Comme f est unitaire, M est un A-module de type fini. Comme $(\bar{f}, \bar{g}) = k[X]$, nous avons $(f, g) + \mathfrak{m}A[X] = A[X]$ donc $\mathfrak{m}M = M$. D'où, d'après le lemme de Nakayama,

$M = 0$.
Par conséquent, il existe $u, v \in A[X]$ tels que $uf + vg = 1$. Si $\deg v \geq \deg f$, écrivons $v = fq + r$ avec $\deg r < \deg f$ et $(u + qg)f + rg = 1$ convient. □

Lemme 24.3. — *Soit A un anneau local de corps résiduel k. Supposons que $f = gh = g'h' \in A[X]$ avec g, h, g', h' unitaires tels que leurs images dans $k[X]$ satisfont $\bar{g} = \bar{g}'$, $\bar{h} = \bar{h}'$ et $\bar{g}, \bar{h}$ premiers entre eux. Alors $g = g'$ et $h = h'$.*

Démonstration. — D'après le lemme 24.2, $(g, h) = A[X]$ et il existe $r, s \in A[X]$ tels que $gr + h's = 1$. Comme $g' = g'gr + g'h's = g'gr + ghs$, g divise g'. Ce sont deux polynômes unitaires de même degré donc $g = g'$. □

Théorème 24.4. — *(Lemme de Hensel). Soit k le corps résiduel de A anneau de valuation discrète complet. Pour $f \in A[X]$ unitaire, nous notons $\bar{f}$ son image dans $k[X]$. Si $\bar{f} = g_0 h_0$ avec g_0, h_0 unitaires premiers entre eux dans $k[X]$, alors $f = gh$ avec g, h unitaires tels que $\bar{g} = g_0$ et $\bar{h} = h_0$. De plus g, h sont uniquement déterminés et $(g, h) = A[X]$.*

Démonstration. — D'après le lemme 24.3, il suffit de montrer l'existence de g et h. Nous construisons par récurrence deux suites de polynômes unitaires $g_n, h_n \in A[X]$ tels que

$$f - g_n h_n \equiv 0 \mod \pi^{n+1} A[X], g_n \equiv g_0 \mod \pi A[X], h_n \equiv h_0 \mod \pi A[X].$$

Pour cela, nous cherchons $u, v \in A[X]$ avec $\deg u < \deg g_0$ et $\deg v < \deg h_0$ tels que

$$f - (g_n + \pi^{n+1} u)(h_n + \pi^{n+1} v) \equiv 0 \mod \pi^{n+2} A[X].$$

Or comme g_0, h_0 sont unitaires et premiers entre eux, d'après le lemme 24.2 il existe $u, v \in A[X]$ avec $\deg u < \deg g_0$ et $\deg v < \deg h_0$ tels que $uh_n + g_n v \equiv (f - g_n h_n)/\pi^{n+1} \mod \pi A[X]$. □

Exemples 24.5. — *i. Soit $x = 2^n u \in \mathbb{Q}_2^*$ avec $n \in \mathbb{Z}$ et $u \in \mathbb{Z}_2^*$ une unité 2-adique. Alors x est un carré dans $\mathbb{Q}_2$ si et seulement si n est pair et $u \equiv 1 \mod 8\mathbb{Z}_2$.*
ii. Le lemme de Hensel permet d'établir que le seul endomorphisme de corps de $\mathbb{Q}_p$ est l'identité.

24.2. Extension locale non ramifiée. — Dans ce paragraphe K désigne un corps parfait complet pour une valuation discrète dont le corps résiduel k est parfait. D'après le lemme de Hensel, résoudre des équations sur le corps résiduel k permet de résoudre les équations sur l'anneau de valuation discrète A de K. Ainsi les groupes de Galois des extensions L de K coïncident avec les groupes de Galois des extensions de k, pourvu que les extensions L/K soient non ramifiées.

Lemme 24.6. — *Soit K un corps complet pour une valuation discrète v d'anneau de valuation A et L une extension finie séparable de K de degré n et*

B la clôture intégrale de A dans L. Alors il existe un unique idéal premier $\mathfrak{p}$ de B qui divise l'idéal maximal $\mathfrak{p}$ de A.

Démonstration. — Notons k le corps résiduel de A. Montrons par l'absurde qu'il existe un unique idéal premier $\mathfrak{P}$ de B au dessus de l'idéal $\mathfrak{p}$ maximal de A. Supposons qu'il y en ait deux $\mathfrak{P}_1, \mathfrak{P}_2$. Soit $b \in \mathfrak{P}_1 - \mathfrak{P}_2$ et $f \in A[X]$ son polynôme minimal. D'après le lemme de Hensel, l'image de f, $\bar{f} \in k[X]$ vérifie $\bar{f} = \bar{g}^r$ avec $\bar{g} \in k[x]$ irréductible. Ainsi $A[b]/\mathfrak{p}A[b] \sim k[X]/(\bar{f})$ est un anneau local ce qui est exclu car $A[b]$ contient deux idéaux premiers distincts $\mathfrak{P}_1 \cap A[b]$ et $\mathfrak{P}_2 \cap A[b]$ contenant $\mathfrak{p}$. □

Proposition 24.7. — *Soit K un corps complet pour une valuation discrète v et L un extension finie séparable de K de degré n. Alors v s'étend de façon unique en une valuation discrète v_L sur L, le corps L est complet pour cette valuation et*

$$\forall b \in L, v_L(b) = v(\mathbb{N}_{L/k}(b))^{1/n}.$$

Démonstration. — Notons A l'anneau de valuation de K, $\mathfrak{p}$ son idéal maximal et B sa cloture intégrale dans L. L'unique idéal premier $\mathfrak{P}$ de B au-dessus de A (Lemme 24.6) permet de définir l'unique un prolongement v_L de v à L.
Notons L'/L une extension finie telle que L'/K soit galoisienne et $v_{L'}$ l'unique extension de v à L'. Alors pour tout $\sigma \in \mathrm{Gal}(L'/K)$, le pongement $L \longrightarrow L', b \mapsto \sigma(b)$ induit une valuation v' sur L, $v'(b) = v_{L'}(\sigma(b))$ qui étend v. Donc $v' = v_L$ par unicité. Donc pour $b \in L$,

$$v_{L'}(\mathbb{N}_{L'/K}(b)) = v_L(\mathbb{N}_{L/K}(b))^{[L':L]} = \Pi_{\sigma \in \mathrm{Gal}(L'/K)} v_{L'}(\sigma(b)) = v_L(b)^{[L':L]}.$$

Ainsi $\forall b \in L, v_L(b) = v(\mathbb{N}_{L/k}(b))^{1/n}$.
Le corps L est complet comme espace vectoriel de dimension finie sur K complet. □

Remarque 24.8. — *Si K un corps parfait complet pour une valuation discrète et L est une extension algébrique de K, alors v s'étend à L en une valuation (qui n'est plus discrète) par passage à la limite sur les extensions K'/K finies incluses dans L. Nous pouvons de même définir par passage à la limite, le corps résiduel l de L.*

Théorème 24.9. — *Soit K un corps parfait complet pour une valuation discrète dont le corps résiduel k est parfait. Soit L une extension algébrique de K et l son corps résiduel . L'application $K' \mapsto k'$ qui envoie une extension non ramifiée K' de K contenant L sur son corps résiduel k' est une correspondance entre les ensembles*

$$\{K' \subset L \text{ finie et non ramifiée sur } K\} \longleftrightarrow \{k' \subset l \text{ finie sur } k\}.$$

De plus K'/K est galoisienne si et seulement si k'/k est galoisienne et, dans ce cas, les groupes

$$\mathrm{Gal}(K'/K) \longrightarrow \mathrm{Gal}(k'/k)$$

sont isomorphes.

Démonstration. — • Soit k' une extension finie de k. Alors il existe $a \in k'$ tel que $k' = k[a]$ et nous notons $f_0 \in k[X]$ le polynôme minimal de a et $f \in A[X]$ un relèvement de f_0. Comme $a \in k'$ est racine simple de f_0, il existe un unique $\alpha \in L$ avec $f(\alpha) = 0$ et $\alpha \equiv a \mod \pi$ (d'après le lemme de Hensel). Soit $K' = K[\alpha]$. Le corps K' a pour corps résiduel k' et $[K' : K] = [k' : k] = \deg f_0$ est non ramifiée. Donc l'application qui à $K' \subset L$ finie et non ramifiée sur K associe son corps résiduel est une application surjective.
Supposons que K' et K'' sont deux extensions non ramifiées de K dans L de même corps résiduel. Alors $K'K''$ est une extension non ramifiée de K de corps résiduel k' et $[K'K'' : K] = [k' : k] = [K' : K]$ donc $K'' = K'$.
• Supposons K'/K galoisienne et notons A' la cloture intégrale de A dans K'. Alors $\mathrm{Gal}(K'/K)$ stabilise A' et son idéal maximal, d'où une application $\mathrm{Gal}(K'/K) \longrightarrow \mathrm{Aut}(k'/k)$. Ecrivons $k' = k[a]$ et $g \in A[X]$ tel que $\bar{g} \in k[X]$ soit le polynôme minimal de a. Soit $\alpha \in A'$ l'unique racine de g telle que $\bar{\alpha} = a$. Comme K'/K est galoisienne, g est scindé dans $A'[X]$, donc $\bar{g}$ est scindé dans $k'[X]$ donc k'/k est galoisienne. Soit $f = [k' : k] = [K' : K]$ et $\alpha_1, \ldots, \alpha_f$ les racines de $g(X)$. Alors

$$\{\alpha_1, \ldots, \alpha_f\} = \{\sigma\alpha, \sigma \in \mathrm{Gal}(K'/K)\}.$$

Comme $\bar{g}$ est séparable, les α_i sont distincts modulo π donc l'image de $\mathrm{Gal}(K'/K) \longrightarrow \mathrm{Gal}(k'/k)$ est de cardinal f, d'où l'isomorphisme.
Réciproquement si k'/k est galoisienne, écrivons encore $k' = k[a]$ et $\alpha \in A$ relèvement de a. D'après le lemme de Hensel, A' contient les conjugués de α donc K'/K est galoisienne. □

Exemple 24.10. — *Le corps $\mathbb{Q}_p$ est un corps parfait complet pour la valuation p-adique de corps résiduel $\mathbb{F}_p$ parfait. Les extensions finies non ramifiées de $\mathbb{Q}_p$ coïncident avec les corps de fractions $\mathbb{Q}_{p^r} = \mathrm{Frac}\, W(\mathbb{F}_{p^r})$, $r \in \mathbb{N}^*$. Elles sont naturellement en bijection avec les extensions F_{p^r} finies de $\mathbb{F}_p$.*

24.3. Construction des vecteurs de Witt. — Les vecteurs de Witt permettent de décrire les anneaux d'entiers des extensions non ramifiées de $\mathbb{Q}_p$: pour tout anneau parfait A de caractéristique $p > 0$, l'anneau des vecteurs de Witt $W(A)$ de A est l'unique anneau tel que
- p n'est pas nilpotent dans $W(A)$,
- $W(A)$ est séparé complet pour la topologie p-adique,
- $W(A)/pW(A) = A$.
Un tel anneau est dit p-anneau strict. Ainsi le foncteur des vecteurs de Witt est adjoint à gauche du foncteur "réduction modulo p" de la catégorie des p-anneaux stricts dans la catégorie des $\mathbb{F}_p$-algèbres parfaites.

Nous commençons par expliciter la construction des vecteurs de Witt d'un anneau quelconque (commutatif et unitaire).

Définition 24.11. — *Soit A un anneau (commutatif et unitaire). Notons $W(A)$ l'ensemble $A^{\mathbb{N}}$ des suites infinies à valeurs dans A. Les éléments de $W(A)$ sont dits* **vecteurs de Witt** *à coefficients dans A.*
A chaque vecteur $x = (x_k)_k$ de $W(A)$, nous associons la suite $x^* = (x^{(k)})_k$ de $A^{\mathbb{N}}$ définie par :

$$\forall k \geq 0, x^{(k)} = x_0^{p^k} + p x_1^{p^{k-1}} + \cdots + p^k x_k.$$

Les coefficients $x^{(k)}, k \geq 0$ de la suite x^* sont dits **composantes fantômes** *de x.*

Définition 24.12. — *A chaque morphisme d'anneaux $f : A \to B$, nous associons l'application d'ensembles $W(f) : W(A) \to W(B)$, $(a_k)_{k\in\mathbb{N}} \mapsto (f(a_k))_{k\in\mathbb{N}}$. Ainsi W définit un foncteur de la catégorie des anneaux commutatifs dans la catégorie des ensembles.*

Nous définissons l'application

$$g_A : W(A) \to A^{\mathbb{N}}, \;\; x \mapsto x^* \;\; (x_k)_k \mapsto (x^{(k)})_k.$$

Proposition 24.13. — *Si l'anneau A contient le corps $\mathbb{Q}$ des nombres rationnels, l'application g_A est bijective.*

Démonstration. — Nous avons $x_0 = x^{(0)}$ et $x_1 = (x^{(1)} - x^{(0)^p})/p$. Pour $k \geq 1$, nous avons :

$$x_k = \frac{1}{p^k}\Big(x^{(k)} - \sum_{0\leq d\leq k-1} p^d x_d^{p^{n-d}}\Big).$$

Ainsi chaque composante x_k s'écrit comme combinaison linéaire des $x^{(d)}$ avec $0 \leq d \leq k$ à coefficients rationnels. Donc g_A est bijective. □

Si A contient $\mathbb{Q}$, l'application g_A est bijective et nous posons

$$\forall a, b \in W(A) \;\; a\hat{+}b = g_A^{-1}(a^* + b^*) \text{ et } a\hat{\times}b = g_A^{-1}(a^* \times b^*).$$

Plus précisément, la somme et le produit sont définis comme les vecteurs de Witt dont les composantes fantômes sont données par :

$$\forall k \geq 0, (a\hat{+}b)^{(k)} = a^{(k)} + b^{(k)}, \;\; (a\hat{\times}b)^{(k)} = a^{(k)} \cdot b^{(k)}.$$

Exemple 24.14. — *Si $\mathbb{Q} \subset A$ et $a = (a_k)$, $b = (b_k)$ sont deux éléments de $W(A)$, alors*

$$a\hat{+}b = (a_0 + b_0, a_1 + b_1 - \sum_{k=1}^{p-1} \frac{1}{p}\binom{p}{k} a_0^k b_0^{p-k}, \cdots)$$

$$a\hat{\times}b = (a_0 b_0, a_1 b_0^p + a_0^p b_1 + p a_1 b_1, \ldots)$$

En particulier $R_{\mathbb{Q}} = \mathbb{Q}[X_0, X_1, \ldots, Y_0, Y_1, \ldots]$ contient $\mathbb{Q}$. Nous allons montrer que l'addition et la multiplication définies sur $W(R_{\mathbb{Q}})$ n'utilisent que des coefficients entiers : soit $X = (X_0, X_1, \ldots)$ et $Y = (Y_0, Y_1, \ldots)$ deux vecteurs de Witt particuliers dans $W(R_{\mathbb{Q}})$, notons

$$(X \hat{+} Y)_k = S_k(X_0, X_1, \ldots, Y_0, Y_1, \ldots), \text{ et } (X \hat{\times} Y)_k = P_k(X_0, X_1, \ldots, Y_0, Y_1, \ldots)$$

les composantes des vecteurs de Witt $X \hat{+} Y$ et $X \hat{\times} Y$. Nous allons montrer que les polynômes S_k, P_k sont à coefficients dans $\mathbb{Z}$ (Proposition 24.18).

Exemple 24.15. — *Nous avons les formules récursives suivantes pour $n \geq 0$,*

$$S_n = (X_n + Y_n) + \frac{1}{p}(X_{n-1}^p + Y_{n-1}^p - S_{n-1}^p) + \cdots + \frac{1}{p^n}(X_0^{p^n} + Y_0^{p^n} - S_0^{p^n}),$$

$$P_n = \frac{1}{p^n}\left((X_0^{p^n} + \cdots + p^n X_n)(Y_0^{p^n} + \cdots + p^n Y_n) - (P_0^{p^n} + \cdots + p^{n-1} P_{n-1}^p)\right).$$

Lemme 24.16. — *Considérons la série formelle*

$$f_Z(t) = \Pi_{k \geq 0}(1 - Z_k t^k)$$

où $(Z_\ell)_{\ell \in \mathbb{N}}$ est un ensemble d'indéterminées. Alors

$$-f_Z'(t)/f_Z(t) = \sum_{k \geq 0} g_k(Z) t^k$$

où

$$g_k(Z) = g_k(Z_1, \ldots, Z_k) \in \mathbb{Z}[Z_1, \ldots, Z_k] = \sum_{d|k} d Z_d^{k/d}$$

est un polynôme de degré 1 en Z_k de coefficient dominant -1.

Démonstration. — Nous avons

$$-t f_{\underline{Z}}'(t)/f_{\underline{Z}}(t) = -t \frac{d}{dt} \sum_{n \geq 1} \ln(1 - Z_n t^n) = t \frac{d}{dt} \sum_{n \geq 1} \sum_{k \geq 1} \frac{(Z_n t^n)^k}{k}$$

$$= \sum_{n=1}^{+\infty} \sum_{k=1}^{+\infty} n Z_n^k t^{nk} = \sum_{m=1}^{+\infty} \sum_{d|m} d Z_d^{\frac{m}{d}} t^m$$

Donc

$$-t f_Z'(t)/f_Z(t) = \sum_{k \geq 0} g_k(Z) t^k \text{ avec } g_k(Z) = \sum_{d|k} d Z_d^{k/d}.$$

□

Lemme 24.17. — *Notons $[d, k]$ le* PPCM *de d et de k. Soit*

$$g(t) = \prod_{d=1}^{+\infty} \prod_{k=1}^{+\infty} (1 - X_d^{\frac{[d,k]}{d}} Y_k^{\frac{[d,k]}{k}} t^{[d,k]})^{\frac{dk}{[d,k]}}.$$

Alors

$$-tg'(t)/g(t) = \sum_{m=1}^{+\infty} \sum_{d|m} dX_d^{\frac{m}{d}} \sum_{k|m} kY_k^{\frac{m}{k}} t^m.$$

Démonstration. — Nous avons

$$-tg'(t)/g(t) = -t\frac{d}{dt} \ln \prod_{d=1}^{+\infty} \prod_{k=1}^{+\infty} (1 - X_d^{\frac{[d,k]}{d}} Y_k^{\frac{[d,k]}{k}} t^{[d,k]})^{\frac{dk}{[d,k]}}$$

$$- = -t\frac{d}{dt} \sum_{d=1}^{+\infty} \sum_{k=1}^{+\infty} \frac{dk}{[d,k]} \ln(1 - X_d^{\frac{[d,k]}{d}} Y_k^{\frac{[d,k]}{k}} t^{[d,k]})$$

$$= t\frac{d}{dt} \sum_{d=1}^{+\infty} \sum_{k=1}^{+\infty} \frac{dk}{[d,k]} \sum_{n=1}^{+\infty} \frac{(X_d^{\frac{[d,k]}{d}} Y_k^{\frac{[d,k]}{k}} t^{[d,k]})^n}{n}$$

$$= \sum_{d=1}^{+\infty} \sum_{k=1}^{+\infty} \sum_{n=1}^{+\infty} dk(X_d^{\frac{[d,k]}{d}} Y_k^{\frac{[d,k]}{k}} t^{[d,k]})^n.$$

Notons $m = n[d,k]$.

$$-tg'(t)/g(t) = \sum_{m=1}^{+\infty} \sum_{d|m} \sum_{k|m} dkX_d^{\frac{m}{d}} Y_k^{\frac{m}{k}} t^m$$

$$= \sum_{m=1}^{+\infty} \sum_{d|m} dX_d^{\frac{m}{d}} \sum_{k|m} kY_k^{\frac{m}{k}} t^m.$$

□

Proposition 24.18. — *Pour tout $k \geq 0$, $S_k, P_k \in \mathbb{Z}[X_0, \ldots, X_k, Y_0, \ldots, Y_k]$.*

Démonstration. — De façon analogue aux vecteurs de Witt, nous pouvons associer à $z = (z_k)_k \in W'(A) = A^{\mathbb{N}}$ la suite $z_* = (z_{(k)})_k$ de $A^{\mathbb{N}}$, définie par les composantes "fantômes généralisées"

$$\forall k \geq 0, z_{(k)} = \sum_{d|k} dz_d^{k/d}$$

et donc une addition $\hat{\hat{+}}$ et une multiplication $\hat{\hat{\cdot}}$ sur $W'(S_{\mathbb{Q}}) = W(\mathbb{Q}[Z_0, Z_1, \ldots, Z'_0, Z'_1, \ldots])$. La projection

$$W'(S_{\mathbb{Q}}) \to W(S_{\mathbb{Q}}) = W(R_{\mathbb{Q}}), Z_\ell \mapsto \begin{cases} X_k & \text{si } \ell = p^k \\ 0 & \text{sinon} \end{cases}$$

est un morphisme d'anneaux. Notons $Z = (Z_\ell)_{\ell \in \mathbb{N}}$ et $Z' = (Z'_\ell)_{\ell \in \mathbb{N}}$ des intéterminées et $Z'' = (Z''_\ell)_{\ell \in \mathbb{N}}$ défini par

$$\underline{Z''} = (\underline{Z} \hat{\hat{+}} \underline{Z'}).$$

En comparant les dérivées et les valeurs prises en 0 des séries $f_Z(t)f_{Z'}(t)$ et $f_{Z''}(t)$ iva les lemmes 24.16 et 24.17, nous montrons que

$$f_Z(t)f_{Z'}(t) = f_{Z''}(t)$$

En identifiant les coefficients des t^{p^k}, et en appliquant la projection de $W'(S_{\mathbb{Q}}) \to W(R_{\mathbb{Q}})$, nous obtenons $S_k \in \mathbb{Z}[X_0, \ldots, X_k, Y_0, \ldots Y_k]$. Nous obtenons de façon analogue le résultat annoncé pour P_k. □

Nous définissons une addition et une multiplication sur $a, b \in W(A)$ pour A anneau commutatif :

Définition 24.19. — *Soit $R_{\mathbb{Z}} = \mathbb{Z}[X_0, X_1, \ldots, Y_0, Y_1, \ldots]$ et A un anneau. Pour tous $a, b \in W(A)$, notons*

$$a\hat{+}b = W(\phi_{ab})(X\hat{+}Y),\ a\hat{\times}b = W(\phi_{ab})(X\hat{\times}Y)$$

où ϕ_{ab} est l'unique morphisme d'anneaux

$$\phi_{ab} : R_{\mathbb{Z}} \to A, X_k \mapsto a_k, Y_k \mapsto b_k, \forall k \in \mathbb{N}.$$

Nous avons la propriété fonctorielle

Proposition 24.20. — *Soit A un anneau. Pour tous vecteurs de Witt a, b dans $W(A)$, les relations suivantes sont satisfaites :*

$$g_A(a\hat{+}b) = g_A(a) + g_A(b),\ g_A(a\hat{\times}b) = g_A(a)g_A(b).$$

En d'autres termes, pour tous $a, b \in W(A)$, il existe un unique vecteur de Witt dans $W(A)$ noté $a\hat{+}b$ (resp. $a\hat{\times}b$) dont les composantes fantômes sont $a^{(k)} + b^{(k)}$ (resp. $a^{(k)}b^{(k)}$).

Démonstration. — Nous avons le diagramme commutatif

$$\begin{array}{ccc} W(A_{\mathbb{Z}}) & \xrightarrow{W(\phi_{a,b})} & W(A) \\ \downarrow g_{A_{\mathbb{Z}}} & & \downarrow g_A \\ A_{\mathbb{Z}}^{\mathbb{N}} & \xrightarrow{\phi_{a,b}^{\mathbb{N}}} & A^{\mathbb{N}} \end{array}$$

Or pour tous $X, Y \in W(A_{\mathbb{Z}})$, il existe un unique vecteur de Witt dans $W(A_{\mathbb{Z}})$ noté $X\hat{+}Y$ dont les composantes fantômes sont $X^{(k)} + Y^{(k)}$ et le morphisme $\phi_{a,b}^{\mathbb{N}}$ est additif. Ainsi

$$\begin{array}{rcc} g_A(a\hat{+}b) & = & g_A \circ W(\phi_{ab})(X\hat{+}Y) \\ & = & \phi_{a,b}^{\mathbb{N}} \circ g_{A_{\mathbb{Z}}}(X\hat{+}Y) \\ & = & \phi_{a,b}^{\mathbb{N}}(g_{A_{\mathbb{Z}}}(X) + g_{A_{\mathbb{Z}}}(Y)) \\ & = & \phi_{a,b}^{\mathbb{N}} \circ g_{A_{\mathbb{Z}}}(X) + \phi_{a,b}^{\mathbb{N}} \circ g_{A_{\mathbb{Z}}}(Y) \\ & = & g_A(a) + g_A(b) \end{array}$$

De même, nous montrons $g_A(a\hat{\times}b) = g_A(a) \cdot g_A(b)$. □

La proposition 24.20 ne suffit pas, en général à définir des lois d'addition et de multiplication sur $W(A)$. C'est l'objet du théorème 24.22. Par exemple si p n'est pas inversible dans A, l'application g_A n'est plus bijective car deux vecteurs de Witt distincts peuvent avoir les mêmes composantes fantômes.
Si A contient $\mathbb{Q}$, g_A définit un isomorphisme d'anneaux. Dans le cas général, $A^{\mathbb{N}}$ et $W(A)$ se correspondent uniquement en tant qu'ensembles. Par exemple, si l'anneau A est de caractéristique $p > 0$, $A^{\mathbb{N}}$ aussi, mais $W(A)$ est de caractéristique 0. Ces anneaux ne sont pas isomorphes.

Proposition 24.21. — *Soit A, B deux anneaux. Si $f : A \to B$ est un morphisme d'anneaux, alors l'application induite :*

$$W(f) : W(A) \to W(B)$$

est additive et multiplicative pour les lois $\hat{+}$ et $\hat{\times}$.

Démonstration. —

$$W(f)(a\hat{+}b) = W(f \circ \phi_{ab})(X\hat{+}Y) = W(\phi_{W(f)(a),W(f)(b)})(X\hat{+}Y)$$
$$= W(\phi_{W(f)(a),W(f)(b)})(X)\hat{+}W(\phi_{W(f)(a),W(f)(b)})(Y) = W(f)(a) + W(f)(b)$$

de même pour le produit. □

Théorème 24.22. — *Soit A un anneau. Notons 0,1 ses éléments neutres pour l'addition et la multiplication. Alors l'ensemble $W(A)$ muni de $\hat{+}$ et $\hat{\times}$ est un anneau d'élément neutre $(0, 0, \ldots)$ et d'unité $(1, 0, \ldots)$.*

Démonstration. — Si A contient $\mathbb{Q}$, l'application g_A est bijective, additive, multiplicative donc transfère la structure d'anneau commutatif de $(A^{\mathbb{N}}, +, \times)$ à $(W(A), \hat{+}, \hat{\times})$.
Si A est un sous-anneau d'un anneau contenant $\mathbb{Q}$, $W(A)$ est encore un anneau. C'est en particulier le cas pour $R_{\mathbb{Z}} = \mathbb{Z}[X_0, X_1, \ldots, Y_0, Y_1, \ldots, Z_0, Z_1, \ldots]$ dans lequel nous notons X, Y et Z les vecteurs de Witt $(X_0, X_1, \ldots)$, $(Y_0, Y_1, \ldots)$ et $(Z_0, Z_1, \ldots)$.
Sinon, soit $a, b, c \in W(A)$. Notons $\phi_{abc} : R_{\mathbb{Z}} \to A$ l'homomorphisme d'anneaux qui envoie les composantes X_k (resp. Y_k, Z_k) sur a_k (resp. b_k, c_k) pour tout entier $k \geq 0$. L'application ϕ_{abc} est additive, multiplicative, elle transporte donc les relations d'associativité, distributivité et commutativité de l'anneau $W(R_{\mathbb{Z}})$ dans l'ensemble $W(A)$ pour les lois $\hat{+}$, $\hat{\times}$. Ainsi $W(A)$ est muni d'une structure d'anneau commutatif.
Les éléments neutre et unité : le résultat est clair si $\mathbb{Q} \subset A$ et une preuve analogue à la précédente dans le cas général conclut. □

Nous en déduisons alors :

Corollaire 24.23. — *Soient A, B deux anneaux. Pour tout morphisme d'anneaux $f : A \to B$, l'application induite $W(f) : W(A) \to W(B)$ est un morphisme d'anneaux.*

Définition 24.24. — *Pour tout entier $n \geq 1$, nous notons $W_n(A)$ l'ensemble des vecteurs de Witt de $W(A)$ tronqués $(x_0, x_1, \ldots, x_{n-1})$ de longueur n.*

Ainsi $W_n(A), \hat{+}, \hat{\times}$ est un anneau commutatif, quotient de $W(A)$. Pour $n \geq m \geq 1$, nous notons le morphisme de troncation

$$t_{nm} : W_n(A) \to W_m(A), (x_0, \ldots, x_{n-1}) \mapsto (x_0, \ldots, x_{m-1}).$$

Théorème 24.25. — *Soit A un anneau. L'anneau des vecteurs Witt $W(A)$ est isomorphe à la limite projective du système $(W_n, t_{nm})_{(n,m)\in\mathbb{N}^2}$:*

$$W(A) = \varprojlim W_n(A).$$

Démonstration. — Les morphismes de troncation t_{nm} sont des morphismes d'anneaux, la limite projective $\operatorname{proj\,lim} W_n(A)$ a une structure d'anneau. Montrons l'existence d'un isomorphisme d'anneaux entre $W(A)$ et $\varprojlim W_n(A)$. Pour $n \in N^*$, notons π_n la projection

$$\pi_n : \varprojlim W_n(A) \longrightarrow W_n(A)$$

Comme les applications de troncation sont surjectives les projections π_n aussi. La propriété universelle des limites projectives appliquée aux morphismes compatibles $t_n : W(A) \to W_n(A)$ induit l'existence d'une unique application (qui est donc un morphisme d'anneaux) $\theta : W(A) \longrightarrow \varprojlim W_n(A)$ qui factorise les t_n à travers π_n : $t_n = \theta \circ \pi_n$.
Montrons que θ est bijectif. Il est clairement injectif. Soit $z = (z^1, z^2, \ldots) \in \varprojlim W_n(A)$, nous cherchons $x \in W(A)$ tel que $\theta(x) = z$. Or

$$\theta(x) = z \Longleftrightarrow \forall n \geq 1, \pi_n \circ \theta(x) = \pi_n(z)$$

$$\Longleftrightarrow \forall n \geq 1, t_n(x) = z^n \Longleftrightarrow \forall n \geq 1, \forall k \leq n-1, x_k = (z^n)_k.$$

Pour $n \geq m$, $t_{nm} \circ \pi_n(z) = \pi_m(z)$ (système projectif). Donc pour $n \geq m$ et $k \in \{0, \ldots, m-1\}$, $(z^n)_k = (z^m)_k$. Ainsi pour $k \geq 0$ et $n \geq k+1$ les coefficients $(z^n)_k$ sont constants et égaux à $(z^{k+1})_k$. Alors le vecteur de Witt x de $W(A)$ défini par ses coefficients :

$$\forall k \geq 0, x_k = (z^{k+1})_k$$

satisfait

$$\forall n \geq 0, \forall k \leq n-1, (x)_k = (z^{(n)})_k.$$

Donc $\theta(x) = z$ et θ est surjectif. □

Corollaire 24.26. — *Si A est un anneau topologique, l'anneau des vecteurs de Witt $W(A)$ est naturellement muni de la topologie induite du produit $\Pi_n W_n(A)$, où chaque anneau $W_n(A)$ est muni de la topologie induite de A^n.*

Nous concluons ce paragraphe par une description des unités de $W(A)$.

Lemme 24.27. — *Pour tout entier $n \geq 1$, un vecteur tronqué $(x_0, \ldots, x_{n-1})$ de $W_n(A)$ est une unité de $W_n(A)$ si et seulement si x_0 est une unité de A.*

Démonstration. — Si $x = (x_0, \ldots, x_{n-1}) \in W_n^*(A)$, alors il existe $y = (y_0, \ldots, y_{n-1}) \in W_{n-1}(A)$ tel que $xy = (1, 0 \ldots)$ donc $x_0 y_0 = 1$ et $x_0 \in A^*$. Réciproquement si $x_0 \in A^*$. Soit $y = (y_0^{-1}, 0, \ldots,) \in W_n(A)$. Ainsi

$$xy = (1, *, \ldots, *) = (1, 0, \ldots, 0) - (0, *, \ldots, *) = 1 - Vz$$

pour $z \in W_{n-1}(A)$ et $V : W_{n-1}(A) \longrightarrow W_n(A)$, $(z_1, \ldots, z_{n-1}) \mapsto (0, z_1, \ldots, z_{n-1})$. Ainsi

$$xy(1 + Vz) = 1 - V^n z = 1$$

donc $x \in W_{n-1}(A)^*$ □

Proposition 24.28. — *Les unités de l'anneau de Witt $W(A)$ sont les vecteurs de Witt dont la première composante est une unité de A.*

Démonstration. —

$$\begin{aligned} x \in W(A)^* &\iff \exists y \in W(A), x \cdot y = 1 \\ &\iff \exists y \in W(A), \forall n, t_n(x \cdot y) = 1 \\ &\iff \exists y \in W(A), \forall n, t_n(x) \cdot t_n(y) = 1 \\ &\iff \forall n, t_n(x) = (x_0, \ldots, x_{n-1}) \text{ est une unité de } W_n(A) \\ &\iff x_0 \text{ est une unité de } A. \end{aligned}$$

□

24.4. Basculement. — Le foncteur de Witt sur les anneaux parfaits de caractéristique $p > 0$ est l'adjoint à gauche du foncteur de basculement sur les anneaux p-adiquement complet.

Définition-Proposition 24.29. — *Soit p un nombre premier et A un anneau. Notons $\varphi : A/p \longrightarrow A/p$, $f \mapsto f^p$ le morphisme de Frobenius. Le* **basculement** *de A est l'anneau*

$$A^\flat = \varprojlim_{\varphi} A/p.$$

L'anneau $A^\flat$ est un anneau parfait de caractéristique p muni de la topologie de limite projective induite par la topologie discrète de A/p. Si, de plus, A/p est un anneau valué, nous pouvons définir une valuation sur $A^\flat$ en prenant la valuation de la première composante.

Démonstration. — Par définition de la limite projective

$$A^\flat = \varprojlim_{\varphi} A/p = \{(a_0, a_1, \ldots) \in (A/p)^{\mathbb{N}} | \forall i \geq 1, a_i^p = a_{i-1}\}$$

est l'ensemble des suites compatibles de racines p-ièmes de A/p. Nous pouvons multiplier termes à termes deux éléments de cette suite et comme A/p est de caratéristique p, nous pouvons sommer deux telles suites. □

Exemples 24.30. — *i. Nous avons* $\mathbb{F}_p[t]^\flat = \mathbb{F}_p$, $\mathbb{Z}_p^\flat = \mathbb{F}_p$.
ii. Le basculement est fonctoriel : tout morphisme d'anneaux de caractéristique p, $f \in \mathrm{Hom}(A, B)$ *induit un morphisme* $f^\flat \in \mathrm{Hom}(A^\flat, B^\flat)$ *d'anneaux de caractéristique* $p > 0$.
iii. Si A *est un anneau parfait de caractéristique* $p > 0$ *et si* B *est un anneau* p*-adiquement complet, alors*

$$\mathrm{Hom}(W(A), B) = \mathrm{Hom}(A, B^\flat).$$

24.5. Anneaux entiers perfectoïdes. —

Définition 24.31. — *Un anneau topologique* A *est dit* **entier perfectoïde** *s'il existe un élément non diviseur de zéro* $\pi \in A$ *tel que*
i. $A \longrightarrow \varprojlim A/\pi^n A$ *est un isomorphisme d'anneaux topologiques où chaque* $A/\pi^n A$ *est muni de la topologie discrète,*
ii. $p \in \pi^p A$,
iii. le Frobenius $\Phi : A/\pi A \longrightarrow A/\pi^p A$, $a \mapsto a^p$ *est un isomorphisme.*

Exemples 24.32. — *i. L'anneau* $\mathbb{Z}_p$ *n'est pas entier perfectoïde car ne satisfait pas ii.*
ii. Soit L *une extension algébrique de* $\mathbb{Q}_p$ *et* $\mathcal{O}_L$ *la clôture intégrale de* $\mathbb{Z}_p$ *dans* L. *Supposons que tout élément de* $\mathcal{O}_L/p\mathcal{O}_L$ *admet une racine* p*-ième de l'unité et qu'il existe* $\pi \in \mathcal{O}_L - \mathcal{O}_L^*$ *tel que* $p \in \pi^p \mathcal{O}_L$. *Alors le complété* p*-adique* $\widehat{\mathcal{O}_L}$ *est un anneau entier perfectoïde (car* Φ *est un isomorphisme). Ainsi* $\widehat{\mathcal{O}_{\mathbb{Q}_p(p^{1/p^\infty})}} = \widehat{\mathbb{Z}_p[p^{1/p^\infty}]}$, $\widehat{\mathcal{O}_{\mathbb{Q}_p(\zeta_{p^\infty})}} = \widehat{\mathbb{Z}_p[\zeta_{p^\infty}]}$ *et* $\widehat{\mathcal{O}_{\overline{\mathbb{Q}_p}}}$ *sont des anneaux entiers perfectoïdes.*

Proposition 24.33. — *Le basculement d'un anneau entier perfectoïde* A

$$A^\flat = \varprojlim_{x \mapsto x^p} A/pA$$

muni de la topologie induite par la limite projective d'anneaux quotients d'un anneau topologique est un anneau entier perfectoïde.

Définition 24.34. — *L'***application de débasculement** *est*

$$\# : A^\flat \longrightarrow A, \quad b = (b_0, b_1, \ldots) \mapsto b^\# = \lim_i \tilde{b}_i^{p^i}$$

où $\tilde{b}_i \in A$ *est un relevé quelconque de* $b_i \in A/pA$.

Lemme 24.35. — *Soit* A *un anneau entier perfectoïde. Il existe un unique morphisme d'anneaux*

$$\theta : W(A^\flat) \longrightarrow A$$

tel que $\theta([b]) = b^\#$ *pour tout* $b \in A^\flat$.

Théorème 24.36. — *Soit* A *un anneau entier perfectoïde. Le basculement induit une équivalence de catégories*

$$\{\ A - \textit{algèbres perfectoïdes}\} \xrightarrow{\simeq} \{A^\flat - \textit{algèbres perfectoïdes}\}$$

$B \mapsto B^\flat$ dont la réciproque envoie une $A^\flat$-algèbre perfectoïde C sur $C^\# = W(C) \otimes_{W(A^\flat),\theta} A$.

25. Anneaux de valuation

L'objet de ce chapitre est de généraliser la notion de valuation dans un cadre topologique non discret.

25.1. Valuations. —

Définition 25.1. — *Un* **groupe ordonné** $(\Gamma, \cdot, \leq)$ *est un groupe* $(\Gamma, \cdot)$ *muni d'un ordre* $\leq$ *compatible avec le produit :*

$$\forall x, y, z \in \Gamma, x \leq y \Rightarrow (zx \leq zy \text{ et } xz \leq yz).$$

Il est **totalement ordonné** *si l'ordre est total :*

$$\forall x, y \in \Gamma, (x \leq y \text{ ou } x \leq y).$$

Lemme 25.2. — *Soient* Γ *un groupe commutatif,* H *une partie de* Γ *telle que :*
- H est stable par le produit,
- $H \cup H^{-1} = \Gamma$,
- $H \cap H^{-1} = \{e\}$.
Alors il existe un unique ordre total compatible avec le produit sur Γ *tel que* H *soit l'ensemble des éléments inférieurs ou égaux* e.

Démonstration. — Munissons Γ d'un ordre. Pour $a, b \in \Gamma$, définissons l'ordre sur Γ : $a \leq b$ si $ab^{-1} \in H$. Cet ordre satisfait les propriétés suivantes :
- Si $a, b \in \Gamma$ avec $a \leq b$ et $b \leq a$, alors $ab^{-1} \in H \bigcap H^{-1}$ donc $a = b$.
- Si $a, b, c \in \Gamma$ avec $a \leq b$ et $b \leq c$, alors $ab^{-1}bc^{-1} \in H$. Donc $a \leq c$.
- Si $a, b \in \Gamma$ alors $ab^{-1} \in H$ ou $ba^{-1} \in H$ (car $H \bigcup H^{-1} = \Gamma$), donc $a \leq b$ ou $b \leq a$.
- Si $a, b, c \in \Gamma$ avec $a \leq b$, alors $ca \leq cb$.
Pour l'unicité, considérons $\preccurlyeq$ un autre ordre compatible avec le produit tel que H soit l'ensemble des éléments inférieurs ou égaux à e. Soient $a, b \in \Gamma$. Nous avons $a \preccurlyeq b$ si et seulement si $ab^{-1} \preccurlyeq e$ i.e. si et seulement si $ab^{-1} \in H$. Donc ces deux ordres coïncident. □

Définition 25.3. — *Soit* $(\Gamma, \cdot, \leq)$ *un groupe commutatif totalement ordonné. Étendons la loi de composition interne de* Γ *à* $\Gamma \cup \{0\}$ *en posant,* $\forall \alpha \in \Gamma, 0 \cdot \alpha = \alpha \cdot 0 = 0 \cdot 0 = 0$. *L'ordre s'étend à* $\Gamma \cup \{0\}$ *via* $\forall \alpha \in \Gamma, 0 < \alpha$.
Nous appelons **valuation** *(ultramétrique) d'un anneau* A *(commutatif unitaire non nul), une application*

$$|\cdot| : A \longrightarrow \Gamma \cup \{0\}$$

qui satisfait :
i.(séparation) $\forall f \in A, |f| = 0 \Longleftrightarrow f = 0_A$,

ii. (compatibilité avec le produit) $\forall f, g \in A, |fg| = |f||g|$,
iii. (inégalité ultramétrique) $|f+g| \leq \max(|f|, |g|)$.

Exemples 25.4. — *i. La valuation triviale est définie par*

$$|\cdot| : A \longrightarrow \mathbb{R}_+, x \mapsto \begin{cases} 0 & si\ x = 0_A \\ 1 & sinon. \end{cases}$$

ii. Si $|\cdot|$ *est une valuation sur* A *alors* $|1| = |-1| = 1$,

$$\forall x, y \in A, |x| \neq |y| \Longrightarrow |x+y| = \max(|x|, |y|).$$

Si de plus A *est intègre et il existe une unique valuation sur* $\mathrm{Frac}(A)$ *qui prolonge* $|\cdot|$ *:*

$$\forall p/q \in \mathrm{Frac}(A), |p/q| = |p||q|^{-1}.$$

iii. Soit p *un nombre premier. La valuation* p*-adique sur* $\mathbb{Z}$ $|\cdot|_p : \mathbb{Z} \longrightarrow \mathbb{R}_+$ *, pour* $n \in \mathbb{Z} - \{0\}$, $n = mp^j$ *avec* $p \not| n$ *et* $|n|_p = p^{-j}$. *La valuation* p*-adique sur* $\mathbb{Z}$ *s'étend au corps des fractions* $\mathbb{Q}$ *de* $\mathbb{Z}$.
Dans le langage classique la valuation p*-adique de* n *est l'exposant* j *(une valuation discrète au sens de la définition 23.22) et* p^{-j} *est valeur absolue* p*-adique de* n. *Cependant dans les développements récents de géométrie adique, le terme de valuation a remplacé celui de valeur absolue.*
iv. La norme sur $\mathbb{R}$ *n'est pas une valuation car elle ne respecte pas l'inégalité ultramétrique.*
v. Suivant le contexte (algébrique, topologique ou géométrique), une valuation est notée $v, |\cdot|, x$.

Définition 25.5. — *Deux valuations* v *et* v' *d'un anneau* A *sont dites* **équivalentes** *si il existe* ϕ *un isomorphisme de monoïdes croissant de* $v(A-\{0\})$ *dans* $v'(A-\{0\})$ *tel que :*

$$\forall f \in A, \phi(v(f)) = v'(f).$$

Soit $(A, v), (A', v')$ *deux anneaux valués. Un* **morphisme d'anneaux valués** $\varphi : A \longrightarrow A'$ *est un morphisme d'anneaux tel que* $v' \circ \varphi = v$.

Exemple 25.6. — *Soit* $K[X]$ *l'anneau des polynômes à coefficients dans* K *corps et* $a \in K$. *L'application "ordre d'annulation en* a*"*

$$o_a : K[X] \longrightarrow \mathbb{Z} \cup \{\infty\}, P \mapsto \sup\{k \in N | \exists Q \in K[X], P(X) = (X-a)^k Q(X)\}$$

permet de définir une valuation sur $K[X]$ *pour* $\rho \in]0, 1[$ *fixé*

$$|\cdot|_a : K[X] \longrightarrow \mathbb{R}_+, \quad P \mapsto \rho^{o_a(P)}.$$

La classe d'équivalence de $|\cdot|_a$ *ne dépend pas du choix de* ρ.

D'après le cours de topologie (en étendant la terminologie classique des suites de Cauchy aux valuations qui prennent des valeurs non réelles) :

Lemme 25.7. — *La distance associée à une valuation $d(x,y) = |x-y|$ fait de A un anneau topologique.*
Les topologies associées à deux valuations équivalentes sont équivalentes.
Lorsqu'un anneau topologique est métrisable, les opérations s'étendent (de manière unique) à sa complétion métrique, qui devient ainsi son anneau complété.

Exemples 25.8. — *i. L'espace métrique $(\mathbb{Z}, |\cdot|_p)$ est un anneau topologique.*
ii. Le corps des nombres rationnels, muni de différentes topologies induites par la distance usuelle ($|x-y|$) ou la distance p-adique ($|x-y|_p$) est un corps topologique.
iii. L'ordre d'annulation en 0 sur l'anneau des polynômes $K[X]$ définit une distance, dite distance X-adique sur $K[X]$ et lui confère la structure d'anneau topologique.

Exemples 25.9. — *i. Le complété de l'anneau des polynômes $K[X]$ pour la distance X-adique est l'anneau des séries formelles $K[[X]]$.*
ii. Le complété de $\mathbb{Z}$ pour la distance p-adique est l'anneau $\mathbb{Z}_p$ des entiers p-adiques. Ses éléments sont les séries

$$\sum_{i\geq 0} a_i p^i, a_i \in \{0,\dots,p-1\}.$$

iii. Le complété de $\mathbb{Q}$ pour la distance p-adique est le corps des nombres p-adiques $\mathbb{Q}_p$. Ses éléments sont les séries

$$\sum_{i\geq -r} a_i p^i, a_i \in \{0,\dots,p-1\}.$$

Le corps des nombres p-adiques est le corps des fractions de l'anneau des entiers p-adiques. L'espace topologique $\mathbb{Q}_p$ possède une base de voisinages ouverts et fermés. Il est donc totalement discontinu (chaque élément est sa propre composante connexe).

Remarque 25.10. — *Soit A un anneau, I un idéal de A. Nous appellons topologie I-adique, l'unique topologie sur A compatible avec sa structure d'anneau dont un système de voisinage de 0 soit l'ensemble I^ℓ, $\ell \geq 0$. La topologie obtenue est séparée si $\cap I^\ell = \{0\}$. Dans ce cas, elle est métrisable par la distance ultramétrique définie par $d(x,y) = 1/2^k$ si $k \in N$ est la plus grande puissance de l'idéal qui contient la différence $x-y$. Elle est complète si pour toute famille $(a_\ell \in I_\ell)_{\ell\in\mathbb{N}}$, il existe $a \in A$ tel que pour tout $k \in \mathbb{N}$, $a - \sum_{\ell<k} a_\ell \in I^k$. Le séparé complèté de A muni de la topologie I-adique est $\hat{A} = \varprojlim A/I^\ell$.*

Plus généralement pour $(\Gamma, \cdot, \leq)$ un groupe commutatif totalement ordonné, nous pouvons considérer l'ensemble des valuations (x,Γ) sans l'hypothèse de séparation sur un anneau A. Le groupe des valeurs $\Gamma_x \subset \Gamma$ est défini comme le sous-groupe engendré par $x(A) - \{0\}$.
Le support d'une valuation x est l'idéal premier $\mathfrak{p}_x = \{f \in A : x(f) = 0\}$. Le corps résiduel associé est $k(x) = \mathrm{Frac}(A/\mathfrak{p}_x)$, sur lequel x induit une valuation

$x : k(x) \longrightarrow \Gamma \cup \{0\}$, $f/g \mapsto x(f)/x(g)$, $(f, g \in A - \mathfrak{p}_x)$ d'image $\Gamma_x \cup \{0\}$; nous notons $\mathcal{O}_x = \{f \in k(x) : x(f) \leq 1\}$ l'anneau de valuation associé. L'équivalence entre valuations s'exprime alors de la façon suivante :

Lemme 25.11. — *Soit $x : A \longrightarrow \Gamma$ et $y : A \longrightarrow \Delta$ des valuations. Alors les affirmations suivantes sont équivalentes :*
i. Pour tous $f, g \in A$, $x(f) \leq x(g) \Longleftrightarrow y(f) \leq y(g)$;
ii. $\mathfrak{p}_x = \mathfrak{p}_y$ et $\mathcal{O}_x = \mathcal{O}_y$;
iii. il existe un isomorphisme de groupes ordonnés $\iota : \Gamma_x \longrightarrow \Delta_y$ tel que $y = \iota \circ x$.
Quand ces propriétés sont satisfaites, nous disons que x et y sont des valuations équivalentes.

Démonstration. — . i.$\Longrightarrow$ ii. : Comme $x(f) = 0$ si et seulement si $x(f) \leq x(0)$ (et de même pour y), nous déduisons que $\mathfrak{p}_x = \mathfrak{p}_y$. Si $f, g \in \mathfrak{p}_x$ sont tels que f/g définit un élément de $k(x)$, alors $f/g \in \mathcal{O}_x$ si et seulement si $x(f) \leq x(g)$, si et seulement si $y(f) \leq y(g)$ donc si et seulement si $f/g \in \mathcal{O}_y$.
ii.$\Longrightarrow$ iii. : La valuation x induit un isomorphisme $x : k(x)^\times/\mathcal{O}_x \longrightarrow \mathcal{O}_x^\times$ tel que pour $f, g \in k(x)^\times$, nous avons $x(f) \leq x(g) \Longleftrightarrow gf^{-1} \in \mathcal{O}_x$. Ceci est encore vrai pour y, donc l'isomorphisme ι est donné par

$$\Gamma_x \xrightarrow{\simeq} k(x)^\times/\mathcal{O}_x^\times = k(y)^\times/\mathcal{O}_y^\times \xrightarrow{\simeq} \Delta_y,$$

(en utilisant la correspondance entre valuations sur un corps et anneau des entiers associé).
iii.$\Longrightarrow$ i. est clair. □

25.2. Anneau de valuation. — Nous rappelons qu'un corps valué est un corps topologique dont la topologie est induite par une valuation.

Définition-Proposition 25.12. — *Soit F un corps, un* **anneau de valuation de** *F est un sous-anneau A de F possédant un idéal maximal $\mathfrak{m}$ satisfaisant*

$$\forall a \in F, (a \notin A) \Rightarrow (a^{-1} \in \mathfrak{m})$$

Alors A est local d'unique idéal maximal $\mathfrak{m}$.

Démonstration. — Comme $\mathfrak{m} \neq A$, $\mathfrak{m}$ contient tous les éléments non-inversibles de A. C'est donc l'unique idéal maximal. □

Définition-Proposition 25.13. — *Soit F un corps valué. L'anneau $F^\circ = \{a \in F, |a| \leq 1\}$ est un anneau de valuation de F d'idéal maximal $F^{\circ\circ} = \{a \in F, |a| < 1\}$.*

Démonstration. — L'*inégalité ultramétrique* et la *compatibilité avec le produit* assurent que F° est un anneau. De plus $F^{\circ\circ}$ est un idéal, et si $|a| > 1$ alors $|a^{-1}| < 1$. □

Proposition 25.14. — *Soit F un corps et A un anneau de valuation de F. Il existe une unique valuation sur F à équivalence près telle que $F^\circ = A$.*

Démonstration. — Commençons par construire une valuation sur F satisfaisant les hypothèses de l'énoncé. Notons U le sous-groupe de F^* des éléments inversibles de A et $\Gamma = F^*/U$. Notons v le morphisme de groupes canonique de F^* dans Γ.
Remarquons que
- A est stable par le produit donc $v(A)$ est stable par le produit,
- $v(A) \cup v(A)^{-1} = v(A) \cup v(A^{-1}) = v(A \cup A^{-1}) = \Gamma$,
- Si $a \in v(A) \cap v(A)^{-1}$, il existe $x, y \in A$ tels que $v(x) = v(y)^{-1} = a$. Par conséquent $xy \in U$ et $x^{-1}y^{-1} \in U$, donc $x^{-1} \in A$ et $x \in U$. Enfin $a = 1_\Gamma$. Nous munissons alors Γ de l'unique ordre compatible avec le produit tel que A soit l'ensemble des éléments d'image par v inférieure ou égale à 1_Γ.
Pour établir que $v : F \to \Gamma \cup \{0\}$ est une valuation, il suffit de vérifier l'inégalité ultramétrique. Pour $x, y \in F$, nous avons $xy^{-1} \in A$ ou $yx^{-1} \in A$; donc $(xy^{-1} + 1)U \subset A$ ou $(yx^{-1} + 1)U \subset A$, donc $v(x + y) \leq \max(v(x), v(y))$. Nous avons donc défini une valuation sur F telle que $F^\circ = A$.
Soit v_1 une valuation sur F telle que $F^\circ = A$. Notons $\Gamma_1 = v_1(F^*)$. La valuation v_1 est un morphisme de groupe de F^* dans Γ_1. Il est clair que $\ker(v_1) = U$ donc Γ_1 est isomorphe $\Gamma = F^*/U$: notons $\varphi(v_1(A)) = v(A)$. Soit $a, b \in \Gamma_1$ tels que $a \leq b$. Nous avons $v_1(ab^{-1}) \in v_1(A)$, donc $\varphi(ab^{-1}) \in v(A)$, donc $\varphi(a) \leq \varphi(b)$. Les valuations v est v_1 sont équivalentes. □

Définition 25.15. — *Une valuation $|\cdot| : F \to \mathbb{R}^+$ sur un corps F est dite de classe 1 si son image $|F^\times|$ est un sous-groupe non discret de $\mathbb{R}^+$.*

Soit F est un corps topologique pour la topologie induite de la valuation $|\cdot| : F \to \mathbb{R}^+$. Notons $\mathcal{O}_F = F^\circ$ le sous-anneau des éléments $x \in F$ tels que $|x| \leq 1$.

Proposition 25.16. — *Soit F un corps topologique pour la topologie induite de la valuation multiplicative $|\cdot| : F \to \mathbb{R}^+$. Nous supposons que la caractéristique résiduelle de F est p, et que l'application de Frobenius $\mathcal{O}_F/p \to \mathcal{O}_F/p$ est surjective. Alors les affirmations suivantes sont équivalentes :*
i. il existe $\pi \in \mathcal{O}_F$ avec $|\pi| \neq 1$ tel que $p \in \pi^p \mathcal{O}_F$,
ii. la valuation est de classe 1.

Démonstration. — i. $\Longrightarrow$ ii. Soit $p = \pi^p h$ avec $h \in \mathcal{O}_F$. Comme $p \geq 2$, $1 > |\pi| > |p|$. Par surjectivité de l'application de Frobenius, il existe $\pi_1, h \in \mathcal{O}_F$ tels que $\pi = \pi_1^p + hp$. Comme $|\pi| > |hp|$, $|\pi_1|^p = \max\{|\pi|, |hp|\} = |\pi|$. Ainsi par induction, nous définissons π_n tel que $1 > |\pi_{n+1}| > |\pi_n|$ pour tout $n \geq 1$. Par conséquent $|F^\times|$ n'est pas sous-groupe discret de $\mathbb{R}^+$.
ii. $\Longrightarrow$ i. Comme l'image de la valuation n'est pas discrète, c'est un sous-groupe dense de $\mathbb{R}^+$. Donc il existe $h_1 \in F$ tel que $|p| < |h_1| < 1$. Ainsi $\left|\dfrac{p}{h_1}\right| < 1$ et il

existe $\pi \in F^{oo}$, $h_2 \in F^o$, tels que $\frac{p}{h_1} = \pi^p + ph_2$. Pour $\frac{1}{h} = \frac{1}{h_1} - h_2$, $\frac{p}{h} = \pi^p$ et $|\frac{1}{h}| = \max\{|\frac{1}{h_1}|, |h_2|\} \geq 1$. Donc $p = \pi^p h$ avec $h \in \mathcal{O}_F$. □

25.3. Prolongement des valuations. — Montrons qu'une valuation sur un corps se prolonge aux extensions de ce corps.

Lemme 25.17. — *Soit A un sous-anneau d'un corps K, $\mathfrak{m}$ un idéal propre de A et $a \in K^*$, alors $\mathfrak{m}A[a]$ est un idéal propre de $A[a]$ ou $\mathfrak{m}A[a^{-1}]$ est un idéal propre de $A[a^{-1}]$.*

Démonstration. — Raisonnons par l'absurde et écrivons

$$1 = n_0 + n_1 a + n_2 a^2 + \cdots + n_k a^k = m_0 + m_1 a^{-1} + m_2 a s^{-2} + \cdots + m_l a^{-l}$$

avec l et k minimaux et $n_0, \ldots, n_k, m_0, \ldots, m_l \in \mathfrak{m}$. Comme $\mathfrak{m}$ est un idéal propre de A, nous avons $k, l \geq 1$. Par symétrie, nous pouvons supposer $k \geq l$. Ainsi $a^l(1 - m_0) = m_1 a^{l-1} + m_2 a^{l-2} + \cdots + m_l$ et

$$1 = m_0 + (1 - m_0)n_0 + (1 - m_0)n_1 a + (1 - m_0)n_2 a^2 + \cdots + (1 - m_0)n_k a^k$$

d'où

$$\begin{aligned} 1 = m_0 + (1 - m_0)n_0 + (1 - m_0)n_1 a + \cdots + (1 - m_0)n_{k-1} a^{k-1} \\ + a^{k-l} n_k (m_1 a^{l-1} + m_2 a^{l-2} + \cdots + m_l). \end{aligned}$$

Ce qui contredit la minimalité de k. □

Lemme 25.18. — *Soit A un anneau (intègre), $\mathfrak{m}$ un idéal maximal de A, Ω un corps algébriquement clos, $\phi : A \to \Omega$ un morphisme d'anneaux de noyau $\ker(\phi) = \mathfrak{m}$. Soit a un élément d'une extension E du corps des fractions de A tel que $\mathfrak{m}A[a]$ soit un idéal propre de $A[a]$. Alors ϕ se prolonge à $A[a]$.*

Démonstration. — L'image $F = \phi(A)$ est un corps car ϕ a pour noyau $\mathfrak{m}$ qui est maximal. Le morphisme ϕ se prolonge de façon unique en un morphisme d'anneaux $\gamma : A[X] \to F[X]$ tel que $\gamma(X) = X$. Notons Z l'idéal de $A[X]$ des polynômes qui admettent a pour racine et $Z' = \gamma(Z)$. Montrons par l'absurde que $Z' \neq F[X]$:
Supposons $Z' = F[X]$. Soit $P(X) \in Z$ avec $\gamma(P(X)) = 1$:

$$P(X) = \sum_{i=0}^{n} c_i X^i, \quad \gamma(P(X)) = \sum_{i=0}^{n} \gamma(c_i) X^i = 1$$

Donc, $\gamma(c_0) = 1$ et $\gamma(c_i) = 0$ pour $i \geq 1$. Donc $c_0 - 1 \in \mathfrak{m}$ et $c_i \in \mathfrak{m}$ pour $i \geq 1$, de plus:

$$P(a) = \sum_{i=0}^{n} c_i a^i = 0, \quad 1 = (c_0 - 1) + \sum_{i=1}^{n} c_i a^i$$

ce qui est exclu car $\mathfrak{m}A[a]$ est un idéal propre de $A[a]$. Donc $Z' \neq F[X]$.
Comme F est un corps, l'idéal Z' de $F[X]$ anneau principal, est engendré par $Q(X) \in F[X]$ non constant donc admettant une racine $r \in \Omega$ algébriquement clos.

Notons $\mu_r \in F[X]$ le polynôme minimal de r. Nous avons $\gamma(Z) \subset \mu_r(X)F[X]$, $A[a] = A[X]/Z$ et $F[r] = F[X]/\mu_r(X)$. Par conséquent γ induit un unique morphisme d'anneaux φ qui fait commuter le diagramme suivant et qui prolonge ϕ :

$$\begin{array}{ccc} A[X] & \longrightarrow & F[X] \\ \downarrow & & \downarrow \\ A[a] & \longrightarrow^{\varphi} & F[r] \end{array}$$

□

Le résultat suivant nécessite le lemme de Zorn :

Lemme 25.19. — *Soit K un corps valué, K° anneau de valuation de K, $K^{\circ\circ}$ idéal maximal de K°. Soit L une extension algébrique de K et ϕ un morphisme d'anneaux de K° dans Ω une clôture algébrique de $K^\circ/K^{\circ\circ}$ tel que $\phi(K^\circ) = K^\circ/K^{\circ\circ}$. Alors le morphisme ϕ se prolonge en un morphisme φ de R anneau de valuation de L dans Ω tel que* $\ker(\varphi)$ *soit l'idéal maximal de R et que $K^\circ = K \bigcap R$.*

Démonstration. — Soit $\mathcal{E}$ l'ensemble des paires (S, φ) avec S un sous-anneau de L et φ un morphisme d'anneaux de S vers Ω d'image un corps. Nous munissons $\mathcal{E}$ de l'ordre $\preccurlyeq$ défini par $(S_1, \varphi_1) \preccurlyeq (S_2, \varphi_2)$ si S_1 est un sous-anneau de S_2 et φ_2 prolonge φ_1. Montrons que $(\mathcal{E}, \preccurlyeq)$ est inductif :
- l'ensemble $\mathcal{E}$ n'est pas vide car $(K^\circ, \phi) \in \mathcal{E}$,
- soit $(S_i, \varphi_i)_{i\in I}$ une chaine non-vide de $(\mathcal{E}, \preccurlyeq)$. Notons $S = \cup_{i\in I} S_i$. Soit $\varphi_S : S \to \Omega$ tel que pour $a \in S_i$ alors $\varphi_S(a) = \varphi_i(a)$. Nous vérifions que S est un anneau, φ_S est un morphisme d'anneaux et son image est un corps.
Donc $(\mathcal{E}, \preccurlyeq)$ est bien inductif. D'après le lemme de Zorn, $(\mathcal{E}, \preccurlyeq)$ a un élément maximal (R, φ). Soit $M = \ker(\varphi)$. Il faut vérifier que $K^\circ = K \bigcap R$ et que R est un anneau de valuation de L.
Montrons que pour $a \in L$, si $a \notin R$ alors $a^{-1} \in \ker(\varphi)$. Soit $a \in L \setminus R$. D'après le lemme 25.17, $MR[a]$ est un idéal propre de $R[a]$ ou $MR[a^{-1}]$ est un idéal propre de $R[a^{-1}]$. Si $MR[a]$ est un idéal propre de $R[a]$, le lemme 25.18 permet de prolonger φ sur $R[a]$ ce qui contredit la maximalité de R. Donc $MR[a^{-1}]$ est un idéal propre de $R[a^{-1}]$. Comme R est maximal, $R[a^{-1}] = R$, donc $a^{-1} \in R$.
Montrons que $a^{-1} \in M$. Supposons que $\varphi(a^{-1}) \neq 0$. Soit R' le localisé de R en a^{-1}. Soit $b \in R'$, $b = ra^k$ avec $r \in R$. Nous pouvons prolonger φ sur R' en posant $\varphi(a) = \varphi(a^{-1})^{-1}$. Cela contredit la maximalité de R. Donc $a^{-1} \in M$ et R est un anneau de valuation de L .
Montrons enfin que $K^\circ = K \bigcap R$. Soit $a \in (K \bigcap R) \setminus K^\circ$, nous savons que $a^{-1} \in K^{\circ\circ}$. Donc $\varphi(a)\varphi(a^{-1}) = 1$, $\phi(a^{-1}) \neq 0$, donc $a^{-1} \notin K^{\circ\circ}$. D'où $K^\circ = K \bigcap R$. □

Théorème 25.20. — *Soit K un corps valué, L une extension algébrique de K. La valuation de K s'étend à L.*

Démonstration. — Le lemme 25.19 donne un anneau de valuation R de L tel que $K^\circ = K \cap R$ et une valuation sur L telle que $L^\circ = R$. Cette valuation induit une valuation sur K et $K^\circ = K \cap L^\circ$, d'après 25.14 ces deux valuations sont équivalentes, quitte à les identifier, nous obtenons un prolongement de la valuation de K. □

Le prolongement d'une valuation à une extension n'est pas unique :

Exemple 25.21. — *Munissons $\mathbb{Q}$ de la valuation 5-adique (cf. exemple 1.3). Nous prolongeons cette valuation sur $\mathbb{Q}[i]$ de deux façons, soit avec la valuation $(2+i)$-adique soit avec la valuation $(2-i)$-adique.*

26. Perfectoïdes

Dans ce paragraphe p est un nombre premier fixé.

Définition 26.1. — *Un* **corps perfectoïde** *est un corps topologique K complet de caractéristique résiduelle p, dont la topologie est induite par une valuation non-archimédienne de classe 1 et tel que tout élément de $\mathcal{O}_K/p$ est une racine p-ième.*

Exemples 26.2. — *i. Soit $\mathbb{Q}_p(p^{\frac{1}{p^\infty}}) = \bigcup_n \mathbb{Q}_p(p^{\frac{1}{p^n}})$. Comme la valuation sur $\mathbb{Q}_p(p^{\frac{1}{p^n}})$ est unique à équivalence près, la valuation sur $\mathbb{Q}_p(p^{\frac{1}{p^\infty}})$ est également unique à équivalence près. Notons $\widehat{\mathbb{Q}_p(p^{\frac{1}{p^\infty}})}$ le complété de $\mathbb{Q}_p(p^{\frac{1}{p^\infty}})$. Alors $\widehat{\mathbb{Q}_p(p^{\frac{1}{p^\infty}})}$ est un corps perfectoïde.*
ii. Notons $\mathbb{F}_p((t^{\frac{1}{p^n}}))$ les séries de Laurent à coefficients dans $\mathbb{F}_p$, d'indéterminée $t^{\frac{1}{p^n}}$. C'est naturellement une extension de $\mathbb{F}_p((t))$ et la valuation définie par l'ordre des éléments de $\mathbb{F}_p((t^{\frac{1}{p^n}}))$ prolonge la valuation de $\mathbb{F}_p((t))$. Notons

$$\mathbb{F}_p((t^{\frac{1}{p^\infty}})) = \bigcup_{n\in\mathbb{N}} \mathbb{F}_p((t^{\frac{1}{p^n}}))$$

et $\widehat{\mathbb{F}_p((t^{\frac{1}{p^\infty}}))}$ le complété de $\mathbb{F}_p((t^{\frac{1}{p^\infty}}))$. Alors $\widehat{\mathbb{F}_p((t^{\frac{1}{p^\infty}}))}$ est un corps perfectoïde.
iii. Le corps $\widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ est perfectoïde.

Définition 26.3. — *Soit K un corps perfectoïde. Le basculement de K est le corps des fractions $K^\flat$ du basculé $\mathcal{O}_K^\flat$ de l'anneau entier perfectoïde $\mathcal{O}_K$.*

Lemme 26.4. — *Si K est un corps perfectoïde alors $K^\flat$ est un corps perfectoïde.*

Théorème 26.5. — *Soit K un corps perfectoïde. Alors toute extension finie L de K est un corps perfectoïde et $L \mapsto L^\flat$ définit une équivalence de catégories préservant le degré*

$$\{\textit{extensions finies de } K\} \longleftrightarrow \{\textit{extensions finies de } K^\flat\}$$

qui induit un isomorphisme des groupes de Galois $\mathrm{Gal}(\overline{K}/K) \simeq \mathrm{Gal}(\overline{K^\flat}/K^\flat)$.