Olivier Debarre

ANNEAUX ET CORPS

PRÉPARATION À L'AGRÉGATION EXTERNE

UNIVERSITÉ PARIS CITÉ

2025–2026

Olivier Debarre

6 janvier 2026

ANNEAUX ET CORPS

PRÉPARATION À L'AGRÉGATION EXTERNE

UNIVERSITÉ PARIS CITÉ

2025–2026

Olivier Debarre

TABLE DES MATIÈRES

CHAPITRE I

ANNEAUX

1. Définitions

Définition 1.1. — *Un* anneau *(unitaire) est un triplet $(A, +, \times)$, où $+$ (l'« addition ») et $\times$ (la « multiplication ») sont des lois internes sur A telles que*

- *$(A, +)$ est un groupe abélien, dont l'élément neutre est noté 0_A (ou simplement 0);*
- *la multiplication est associative et possède un élément neutre est noté 1_A (ou simplement 1);*
- *la multiplication est distributive par rapport à l'addition :*

$$\forall a, b, c \in A \qquad a \times (b + c) = a \times b + a \times c \qquad (b + c) \times a = b \times a + c \times a.$$

L'anneau $(A, +, \cdot)$ est commutatif *si la multiplication est commutative.*

On note souvent ab au lieu de $a \times b$. On note aussi $-a$ l'opposé de A, c'est-à-dire que $a + (-a) = 0_A$. On a, pour tout a dans A,

$$0_A a = (0_A + 0_A)a = 0_A a + 0_A a,$$

d'où, en ajoutant des deux côtés $-0_A a$,

$$0_A a = 0_A.$$

De même,

$$a 0_A = 0_A.$$

Pour tous éléments a et b de A, on a alors

$$ab + (-a)b = (a + (-a))b = 0_A b = 0_A,$$

donc

$$(-a)b = -ab,$$

ainsi que (« règle des signes »)

$$a(-b) = -ab \qquad (-a)(-b) = -(-a)b = -(-ab) = ab.$$

Si $a \in A$ et $m \in \mathbf{Z}$, on définit ma (comme dans tout groupe abélien) par récurrence sur m en posant

$$0a \coloneqq 0_A \quad , \quad \forall m \in \mathbf{Z} \quad (m + 1)a = ma + a.$$

On a ainsi, pour tout $m, n \in \mathbf{Z}$,

$$(m + n)a = ma + na.$$

Si $a \in A$ et $m \in \mathbf{N}$, on définit a^m par récurrence sur m en posant

$$a^0 \coloneqq 1_A \quad , \quad \forall m \in \mathbf{N} \quad a^{m+1} = a^m \times a.$$

On a ainsi, pour tout $m, n \in \mathbf{N}$,

$$a^{m+n} = a^m a^n.$$

Exemple 1.2. — L'anneau nul $A = \{0_A\}$ est un anneau commutatif. Un anneau A est nul si et seulement si $0_A = 1_A$.

Exemple 1.3. — Les triplets $(\mathbf{Z}, +, \times)$ et $(\mathbf{Z}/n\mathbf{Z}, +, \times)$ sont des anneaux commutatifs.

Étant donnés un ou des anneaux, on peut en fabriquer d'autres.

***Construction 1.4* (Produit d'anneaux).** — Le produit direct $\prod_{i\in I} A_i$ d'une famille d'anneaux $(A_i, +, \times)_{i\in I}$ est un anneau (pour les lois d'addition et de multiplication terme à terme).

***Construction 1.5* (Matrices).** — Soit A un anneau *commutatif* et soit n un entier strictement positif. On définit l'anneau $\mathscr{M}_n(A)$ des *matrices carrées d'ordre n à coefficients dans A* comme l'ensemble A^{n^2} des tableaux $(a_{ij})_{1\leqslant i,j\leqslant n}$ d'éléments de A muni de l'addition terme à terme, la multiplication de matrices $(a_{ij})_{1\leqslant i,j\leqslant n}$ et $(b_{ij})_{1\leqslant i,j\leqslant n}$ étant définie comme la matrice $(c_{ij})_{1\leqslant i,j\leqslant n}$, où

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

L'anneau $\mathscr{M}_n(A)$ n'est commutatif que si A est l'anneau nul ou si $n = 1$.

Définition 1.6. — *Soit A un anneau.*

(a) *Un élément de A est* inversible *(on dit aussi que c'est une* unité *de A) s'il admet un inverse pour la multiplication. L'ensemble des éléments inversibles, muni de la multiplication, est un groupe noté habituellement $A^\times$.*

(b) *L'anneau A est* intègre *s'il est commutatif, non nul et si le produit de deux éléments non nuls de A est encore non nul. C'est un* corps *s'il est commutatif, non nul et que tout élément non nul de A est inversible.*

Un corps est un anneau intègre.

Exemple 1.7. — L'anneau $\mathbf{Z}$ est intègre et ses unités sont $\{-1, 1\}$.

Exemple 1.8. — Si n est un entier strictement positif, les unités de l'anneau $\mathbf{Z}/n\mathbf{Z}$ sont les classes des entiers premiers à n. On a

$$\mathbf{Z}/n\mathbf{Z} \text{ est un corps} \Leftrightarrow \mathbf{Z}/n\mathbf{Z} \text{ est un anneau intègre} \Leftrightarrow n \text{ est un nombre premier.}$$

Exemple 1.9. — Soit A un anneau commutatif et soit n un entier strictement positif. Les unités de l'anneau $\mathscr{M}_n(A)$ sont les matrices dont le déterminant est une unité de A.

En effet, si $M \in \mathscr{M}_n(A)$ est inversible, il existe une matrice $N \in \mathscr{M}_n(A)$ telle que $MN = I_n$. En prenant les déterminants, on obtient $\det(MN) = \det(M)\det(N) = 1$ (le déterminant d'un produit est le produit des déterminants, dans n'importe quel anneau), de sorte que $\det(M)$ est inversible dans A (d'inverse $\det(N)$).

Inversement, pour toute matrice $M \in \mathscr{M}_n(A)$, on a ${}^t\mathrm{com}(M)\, M = M\, {}^t\mathrm{com}(M) = \det(M) I_n$, où $\mathrm{com}(M)$ est la comatrice de M (dont les coefficients sont les cofacteurs de M). Si $\det(M)$ est inversible dans A, la matrice M est inversible dans $\mathscr{M}_n(A)$, d'inverse $(\det(M))^{-1}\, {}^t\mathrm{com}(M)$.

***Remarque 1.10* (Simplification dans les anneaux intègres).** — Soit A un anneau intègre et soient $a, b, c \in A$ tels que $ab = ac$. Si $a \neq 0_A$, alors $b = c$. En effet, on peut réécrire l'hypothèse $a(b - c) = 0_A$. Comme $a \neq 0_A$ et que l'anneau A est intègre, on a $b - c = 0_A$, c'est-à-dire $b = c$.

Définition 1.11. — *Un sous-anneau d'un anneau A est un sous-ensemble B de A contenant 1_A, stable par addition, opposé et multiplication. Muni de la restriction de l'addition et de la multiplication, B est un anneau.*

Définition 1.12. — *Soient A et B des anneaux. Un* morphisme *(d'anneaux) entre A et B est une application $f\colon A \to B$ qui vérifie $f(1_A) = 1_B$ et*

$$\forall x, y \in A \qquad f(x + y) = f(x) + f(y) \quad f(xy) = f(x)f(y).$$

Un isomorphisme *entre A et B est un morphisme qui est bijectif (son inverse est alors automatiquement aussi un morphisme).*

Si $f\colon A \to B$ est un morphisme d'anneaux, $f(A)$ est un sous-anneau de B. Si f est injectif, il induit un isomorphisme de A sur $f(A)$. On dit parfois qu'on *identifie A à un sous-anneau de B*.

Exemple 1.13. — Soit A un anneau. Il existe un unique morphisme $\mathbf{Z} \to A$: il envoie tout entier n sur $n1_A$.

Si un anneau A est intègre, on construit son *corps des quotients* (ou *corps des fractions*) K_A comme l'ensemble des classes d'équivalence (appelées « fractions ») des paires (a, b), avec $a \in A$ et $b \in A \smallsetminus \{0\}$, pour la relation d'équivalence

$$(a, b) \sim (a', b') \iff ab' = a'b.$$

La classe d'équivalence de (a, b) est notée $\frac{a}{b}$. Muni des opérations (addition et multiplication) habituelles sur les fractions, on vérifie que K_A est bien un corps.

2. Anneaux de polynômes

2.1. Polynômes en une indéterminée. — Soit A un anneau *commutatif*. On définit l'anneau des *polynômes à coefficients dans A* de la façon suivante. Considérons l'ensemble $A[X]$ (aussi noté $A^{(\mathbf{N})}$) des suites $(a_i)_{i\in\mathbf{N}}$ d'éléments de A dont tous les termes, sauf un nombre fini, sont nuls. On définit l'addition en additionnant terme à terme. Pour la multiplication, c'est plus compliqué : le produit des polynômes $(a_i)_{i\in\mathbf{N}}$ et $(b_j)_{j\in\mathbf{N}}$ est le polynôme $(c_k)_{k\in\mathbf{N}}$ défini par $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. On vérifie que ces deux opérations vérifient les axiomes requis et font de $A[X]$ un anneau commutatif, avec $0_{A[X]} = (0_A, 0_A, \dots)$ et $1_{A[X]} = (1_A, 0_A, 0_A, \dots)$.

On note X la suite $(0_A, 1_A, 0_A, \dots)$. Tout polynôme non nul s'écrit alors de façon unique comme

$$P(X) = a_d X^d + \cdots + a_1 X + a_0,$$

avec $d \in \mathbf{N}$, $a_d, \dots, a_1, a_0 \in A$ et $a_d \neq 0_A$. L'entier d s'appelle le *degré* du polynôme P et a_d est son *coefficient dominant ;* on dit que P est *unitaire* si son coefficient dominant est 1_A. Il est pratique de décréter que le degré du polynôme nul est $-\infty$.

L'application $A \to A[X]$ qui envoie a sur la suite $(a, 0_A, 0_A, \dots)$ est un morphisme injectif d'anneaux. On identifie donc A à un sous-anneau de $A[X]$ (celui des polynômes nul ou de degré 0).

Proposition 2.1. — *Soit A un anneau intègre.*

(a) *Si $P, Q \in A[X]$, on a $\deg(P + Q) \leqslant \max\{\deg(P), \deg(Q)\}$.*

(b) *Si $P, Q \in A[X]$ sont non nuls, le produit PQ est non nul et on a $\deg(PQ) = \deg(P) + \deg(Q)$. En particulier, l'anneau $A[X]$ est intègre.*

(c) *Les unités de l'anneau $A[X]$ sont les unités de l'anneau A (vues comme polynômes de degré 0).*

Démonstration. — Le point (a) est facile à vérifier.

Si $P(X) = a_d X^d + \cdots + a_1 X + a_0$, avec $a_d \neq 0_A$ et $d = \deg(P)$, et $Q(X) = b_e X^e + \cdots + b_1 X + b_0$, avec $b_e \neq 0_A$ et $e = \deg(Q)$, on a $(PQ)(X) = a_d b_e X^{d+e} + \cdots$. Comme A est intègre, on a $a_d b_e \neq 0_A$, donc $\deg(PQ) = d + e = \deg(P) + \deg(Q)$. Cela montre (b).

Montrons (c). Si $u \in A$ est une unité, son inverse u^{-1} dans A est aussi son inverse dans $A[X]$. Inversement, si $P \in A[X]^\times$, on a $PP^{-1} = 1_{A[X]} = 1_A$ et, en prenant les degrés et en appliquant (b), on trouve

$\deg(P)\deg(P^{-1}) = \deg(1_A) = 0$, donc $\deg(P) = \deg(P^{-1}) = 0$. Les polynômes P et P^{-1} sont ainsi constants, donc éléments de A, et P^{-1} est l'inverse de P dans A, de sorte que P est une unité de A. □

Remarque 2.2. — Attention, le point (c) ci-desssus n'est plus vrai si A n'est pas intègre. Le polynôme $P(X) = \bar{2}X + \bar{1} \in (\mathbf{Z}/4\mathbf{Z})[X]$ est inversible dans l'anneau $(\mathbf{Z}/4\mathbf{Z})[X]$, d'inverse lui-même (puisque $P(X)^2 = \bar{4}X^2 + \bar{4}X + \bar{1} = \bar{1}$), mais il n'est pas constant.

Remarque 2.3. — Si K est un corps, l'anneau $K[X]$ est intègre (prop. 2.1(b)). On note $K(X)$ son corps des fractions. Ses éléments sont les *fractions rationnelles* à coefficients dans K.

2.2. Polynômes en plusieurs indéterminées. — Soit A un anneau *commutatif* et soit n un entier strictement positif. On définit plus généralement l'anneau commutatif $A[X_1, \dots, X_n]$ des *polynômes en n indéterminées à coefficients dans A* de façon analogue : c'est l'ensemble des suites $(a_I)_{I\in\mathbf{N}^n}$ d'éléments de A dont tous les termes, sauf un nombre fini, sont 0_A. On définit l'addition en additionnant terme à terme et le produit de polynômes $(a_I)_{I\in\mathbf{N}^n}$ et $(b_J)_{J\in\mathbf{N}^n}$ comme le polynôme $(c_K)_{K\in\mathbf{N}^n}$ défini par $c_K = \sum_{I,J\in\mathbf{N}^n,\, I+J=K} a_I b_J$.

Pour $i \in \{1, \dots, n\}$, on note X_i la suite dont tous les éléments sont 0_A sauf celui correspondant à l'élément I de $\mathbf{N}^n$ dont toutes les coordonnées sont nulles sauf la i-ième qui vaut 1. Tout élément de $A[X_1, \dots, X_n]$ s'écrit alors comme une somme finie

$$P(X_1, \dots, X_n) = \sum_{0\leqslant i_j\leqslant d_j} a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n},$$

avec $a_{i_1,\dots,i_n} \in A$. On identifie encore A à un sous-anneau de $A[X_1, \dots, X_n]$.

On a des isomorphismes canoniques

$$A[X_1, \dots, X_n] = (A[X_1])[X_2, \dots, X_n] = (A[X_1, \dots, X_{n-1}])[X_n].$$

En appliquant la prop. 2.1 n fois, on en déduit que si l'anneau A est intègre, il en est de même de l'anneau $A[X_1, \dots, X_n]$ et que ses unités sont celles de A.

3. Algèbres

Définition 3.1. — *Soit A un anneau commutatif. Une* A-algèbre *(unitaire associative) est un quadruplet $(E, +, \times, \cdot)$, où $+$ et $\times$ (l'addition et la multiplication) sont des lois internes sur E et $\cdot$ est une loi externe $A \times E \to E$ telles que*

- *$(E, +, \times)$ est un anneau (unitaire) ;*
- *on les relations*

$$\forall a, b \in A \ \forall x, y \in E \qquad \begin{aligned} &1_A \cdot x = x, \\ &a \cdot (x + y) = a \cdot x + a \cdot y \quad (a + b) \cdot x = a \cdot x + b \cdot x, \\ &a \cdot (x \times y) = (a \cdot x) \times y = x \times (a \cdot y). \end{aligned}$$

La A-algèbre $(E, +, \times, \cdot)$ est commutative *si la multiplication de E est commutative.*

On définit de façon évidente les morphismes entre A-algèbres.

On peut donner une définition alternative des A-algèbres en disant qu'elles correspondent à la donnée d'un anneau E et d'un morphisme d'anneaux $\rho\colon A \to E$. L'application ρ est définie par

$$\forall a \in A \qquad \rho(a) \coloneqq a \cdot 1_E$$

et elle doit satisfaire

$$\forall a \in A \ \forall x \in E \qquad \rho(a) \times x = x \times \rho(a) \tag{1}$$

(en effet, $(a \cdot 1_E) \times x = a \cdot (1_E \times x) = a \cdot x$ et $x \times (a \cdot 1_E) = a \cdot (x \times 1_E) = a \cdot x$).

Inversement, on retrouve la multiplication externe à partir d'un morphisme $\rho\colon A \to E$ vérifiant la propriété (1) par la formule

$$\forall a \in A \ \forall x \in E \qquad a \cdot x \coloneqq \rho(a) \times x.$$

Un morphisme entre des A-algèbres $\rho_E\colon A \to E$ et $\rho_F\colon A \to F$ est alors un morphisme d'anneaux $f\colon E \to F$ tel que $\rho_F = f \circ \rho_E$.

Nous nous bornerons à donner des exemples d'algèbres. Dans tous ces exemples, A est un anneau commutatif.

Exemple 3.2. — L'anneau $A[X_1, \ldots, X_n]$ des polynômes à n indéterminées à coefficients dans A est une A-algèbre commutative. Elle a la propriété (universelle) suivante : pour toute A-algèbre commutative E et tout $x_1, \ldots, x_n \in E$, il existe un unique morphisme de A-algèbres $f\colon A[X_1, \ldots, X_n] \to E$ tel que $f(X_i) = x_i$ pour tout $i \in \{1, \ldots, n\}$.

Exemple 3.3. — L'anneau $\mathscr{M}_n(A)$ des matrices carrées d'ordre n à coefficients dans A défini dans l'ex. 1.5 est une A-algèbre, qui n'est en général pas commutative.

4. Idéaux

Soit A un anneau commutatif. Un *idéal* de A est une partie I de A qui est un sous-groupe additif tel que, pour tout $a \in A$ et tout $x \in I$, on a $ax \in I$. C'est exactement la propriété qu'il faut pour pouvoir mettre sur le groupe additif A/I une structure d'anneau qui fait de la projection canonique $A \to A/I$ un morphisme d'anneaux [1].

On notera le fait évident mais utile qu'un idéal I de A est égal à A si et seulement si $1_A \in I$.

Exemple 4.1. — Un anneau commutatif A est un corps si et seulement s'il n'est pas nul et que ses seuls idéaux sont $\{0_A\}$ et A.

L'intersection d'une famille quelconque d'idéaux de A est encore un idéal de A. Si S est une partie de A, l'intersection de tous les idéaux de A contenant S est donc un idéal de A que l'on notera (S), ou AS. C'est l'ensemble des sommes finies $\sum_{i=1}^{n} a_i s_i$, pour $n \in \mathbf{N}$, $a_i \in A$ et $s_i \in S$.

Si I et J sont des idéaux d'un anneau commutatif A, on note $I + J$ l'idéal de A engendré par $I \cup J$ et IJ l'idéal de A engendré par $\{xy \mid x \in I, y \in J\}$. On a

$$\begin{aligned} I + J &= \{x + y \mid x \in I, y \in J\} \\ IJ &= \{\sum_{i=1}^{n} x_i y_i \mid n \in \mathbf{N}, x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J\}. \end{aligned}$$

Proposition 4.2. — *Soit $f\colon A \to B$ un morphisme d'anneaux commutatifs.*

(a) *Le noyau de f est un idéal de A. Plus généralement, l'image réciproque par f d'un idéal de B est un idéal de A.*

(b) *Si I est un idéal de A, le morphisme f se factorise par la projection $A \to A/I$ si et seulement si $I \subseteq \mathrm{Ker}(f)$. Dans le cas $I = \mathrm{Ker}(f)$, le morphisme induit $A/\mathrm{Ker}(f) \to B$ est injectif.*

L'image de f n'est en général pas un idéal de B.

1. Pour que la projection canonique soit un morphisme d'anneaux, il faut définir le produit de classes $\bar{a}, \bar{b} \in A/I$ comme la classe de ab, mais il faut aussi vérifier que cette classe $\overline{ab}$ ne dépend pas des représentants a et b. Si on change a en $a + x$ et b en $b + y$, avec $x, y \in I$, alors $(a + x)(b + y) = ab + xb + ay + xy$, qui est bien dans la même classe que ab par définition des idéaux.

Définition 4.3. — *Soit A un anneau commutatif et soit I un idéal de A.*

(a) *L'idéal I est* premier *s'il est distinct de A et qu'il vérifie la propriété*

$$\forall a, b \in A \qquad ab \in I \Rightarrow (a \in I \text{ ou } b \in I).$$

(b) *L'idéal I est un* maximal *s'il est distinct de A et que l'unique idéal de A contenant strictement I est A.*

Exemple 4.4. — On rappelle que les idéaux de l'anneau $\mathbf{Z}$ sont les $n\mathbf{Z}$, avec $n \in \mathbf{N}$. L'idéal $n\mathbf{Z}$ est maximal si et seulement si l'entier n est premier ; il est premier si et seulement si l'entier n est premier ou nul.

Proposition 4.5. — *Soit A un anneau commutatif et soit I un idéal de A.*

(a) *L'idéal I est premier si et seulement si l'anneau A/I est intègre.*

(b) *L'idéal I est maximal si et seulement si l'anneau A/I est un corps.*

En particulier, tout idéal maximal est premier.

Démonstration. — Pour le premier point, il suffit de réécrire la définition en tenant compte du fait que $a \in I$ si et seulement si la classe $\bar{a}$ dans A/I est nulle.

Pour le second point, supposons I maximal et soit $\bar{a}$ un élément non nul de A/I. On a $a \notin I$, donc l'idéal $I + (a)$ de A engendré par I et a contient strictement I. La maximalité de I entraîne qu'il est égal à A, c'est-à-dire qu'il contient 1_A. On peut donc écrire $1_A = x + ab$, avec $x \in I$ et $b \in A$. En prenant les classes dans A/I, on obtient $1_{A/I} = \bar{a}\bar{b}$: l'élément $\bar{a}$ de A/I est bien inversible dans A/I. Ceci montre que l'anneau A/I est un corps.

Inversement, supposons que l'anneau A/I est un corps. Soit J un idéal de A contenant strictement I et soit a un élément de J qui n'est pas dans I. Sa classe $\bar{a}$ dans A/I est alors non nulle et, comme A/I est un corps, elle a un inverse $\bar{b}$. On a ainsi $1_{A/I} = \bar{a}\bar{b}$, ce qui est équivalent à $1_A - ab \in I$. En écrivant $1_A = ab + (1_A - ab) \in J + I = J$, on voit que $J = A$. Ceci montre que l'idéal I est maximal. □

Exemple 4.6. — L'anneau commutatif A est intègre si et seulement si $\{0_A\}$ est un idéal premier de A. C'est un corps si et seulement si $\{0_A\}$ est un idéal maximal de A.

5. Divisibilité, éléments irréductibles

Soit A un anneau *intègre* et soient a et b des éléments de A. On dit que a *divise* b (ou que a est *un diviseur de* b, ou que b est *multiple de* a), et on écrit $a \mid b$, s'il existe $q \in A$ tel que $b = aq$ (si $a \neq 0$, on écrit parfois $q = b/a$). En termes d'idéaux, c'est équivalent à $(a) \supseteq (b)$. En particulier, 0 ne divise que lui-même, tout élément divise 0, et un élément de A est une unité si et seulement s'il divise tous les éléments de A.

On a ($a \mid b$ et $b \mid a$) si et seulement s'il existe $u \in A^\times$ tel que $a = ub$; c'est aussi équivalent à l'égalité d'idéaux $(a) = (b)$. On dit alors que a et b sont *associés.*

On dit que des éléments de A sont *premiers entre eux* si leurs seuls diviseurs communs sont les unités de A.

Un élément a de A est *irréductible* si a n'est pas inversible et que si $a = xy$, alors soit x, soit y est inversible (il n'y a donc pas d'éléments irréductibles dans un corps). La seconde condition signifie que a est non nul et que les seuls diviseurs de a sont ses associés et les unités de A.

Exemple 5.1. — Les éléments irréductibles de $\mathbf{Z}$ sont les $\pm p$, avec p nombre premier. Ceux de $\mathbf{C}[X]$ sont les polynômes de degré 1. Ceux de $\mathbf{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle, c'est-à-dire les polynômes $aX^2 + bX + c$ avec $b^2 - 4ac < 0$.

Soit a un élément non nul de A. Si l'idéal (a) est premier, a est irréductible :

- a n'est pas inversible, puisque $(a) \neq A$;
- si $a = xy$, on a $xy \in (a)$, donc
  – soit $x \in (a)$, c'est-à-dire $a \mid x$, et comme $x \mid a$, les éléments x et a sont associés et comme ils sont non nuls, y est une unité ;
  – soit $y \in (a)$ et, de la même façon, x est une unité.

La réciproque est fausse en général, comme le montre l'ex. 5.3 ci-dessous.

Exemple 5.2. — Si $n \geqslant 1$, l'anneau $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si l'entier n est premier. C'est alors un corps. On a

$$n \text{ est un nombre premier } \Leftrightarrow \text{ l'idéal } (n) \text{ est premier } \Leftrightarrow \ n \text{ est irréductible.}$$

Exemple 5.3. — Dans le sous-anneau $\mathbf{Z}[i\sqrt{5}]$ de $\mathbf{C}$, le nombre 3 est irréductible (pourquoi ?) mais l'idéal (3) n'est pas premier, car 3 divise le produit $(1 + i\sqrt{5})(1 - i\sqrt{5})$ mais aucun des facteurs.

Noter que la « bonne façon » de voir l'anneau $\mathbf{Z}[i\sqrt{5}]$ est de le considérer comme l'anneau quotient $\mathbf{Z}[X]/(X^2 + 5)$: inutile de construire $\mathbf{C}$ pour cela ! On le note d'ailleurs plutôt $\mathbf{Z}[\sqrt{-5}]$.

6. Anneaux principaux

Un anneau A est *principal* si A est intègre et que tout idéal de A est principal, c'est-à-dire qu'il peut être engendré par un élément (alors uniquement déterminé à multiplication par un élément inversible de A près). L'anneau $\mathbf{Z}$ est donc principal (ex. 4.4), mais pas l'anneau $\mathbf{Z}[X]$ des polynômes à coefficients entiers, ni l'anneau $K[X, Y]$ des polynômes à deux indéterminées à coefficients dans un corps K (pourquoi ?).

Dans un anneau principal, les équivalences de l'ex. 5.2 restent vraies.

Proposition 6.1. — *Soit A un anneau principal et soit a un élément non nul de A. Les propriétés suivantes sont équivalentes :*

(i) *l'idéal (a) est premier, c'est-à-dire que l'anneau quotient $A/(a)$ est intègre ;*

(ii) *l'élément a est irréductible ;*

(iii) *l'idéal (a) est maximal, c'est-à-dire que l'anneau quotient $A/(a)$ est un corps.*

En d'autres termes, dans un anneau principal, le seul idéal premier non maximal est l'idéal nul.

En particulier, l'anneau $\mathbf{Z}[\sqrt{-5}]$ de l'ex. 5.3 n'est pas principal. Nous verrons dans le § 8 que les propriétés (i) et (ii) (mais pas (iii) en général) restent équivalentes pour une classe bien plus vaste d'anneaux, celle des anneaux factoriels.

Démonstration. — On sait qu'en général (iii) $\Rightarrow$ (i) $\Rightarrow$ (ii). Supposons (ii), c'est-à-dire que a est irréductible. Tout d'abord, comme a n'est pas inversible, on a $(a) \neq A$.

Soit maintenant I un idéal de A contenant (a). Comme A est principal, on peut écrire $I = (x)$, de sorte qu'il existe $y \in A$ tel que $a = xy$. Comme a est irréductible, soit x est inversible et $I = A$, soit y est inversible et $I = (a)$. L'idéal (a) est donc maximal. □

***Définition 6.2* (pgcd et ppcm).** — *Soient a et b des éléments d'un anneau principal A.*

L'idéal $\langle a, b\rangle$ est engendré par un élément de A, uniquement déterminé à multiplication par un élément inversible de A près. On l'appelle un pgcd *(« plus grand commun diviseur ») de a et b, parfois noté $a \wedge b$.*

L'idéal $\langle a\rangle \cap \langle b\rangle$ est engendré par un élément de A, uniquement déterminé à multiplication par un élément inversible de A près, le ppcm *(« plus grand commun multiple ») de a et b, parfois noté $a \vee b$.*

Les pgcd (ou les ppcm) ne sont en général pas uniques, mais ils sont tous associés.

On a par exemple $a \wedge 0 = a$ et $a \vee 0 = 0$, et $a \wedge b = 0$ si et seulement si $a = b = 0$.

Le lemme suivant justifie la terminologie employée.

Proposition 6.3. — *Soit A un anneau principal et soient a et b des éléments de A.*

(a) *Le pgcd $a \wedge b$ divise a et b et tout élément d de A qui divise a et b divise $a \wedge b$. En particulier, a et b sont premiers entre eux si et seulement si $a \wedge b = 1$. Si d est un élément non nul de A qui divise a et b, on a de plus $\frac{a}{d} \wedge \frac{b}{d} = \frac{a\wedge b}{d}$.*

(b) *Le ppcm $a \vee b$ est divisible par a et par b et tout élément de A qui est divisible par a et b est divisible par $a \vee b$. En particulier, $a \vee b$ divise ab. Si d est un élément non nul de A qui divise a et b, on a de plus $\frac{a}{d} \vee \frac{b}{d} = \frac{a\vee b}{d}$.*

Démonstration. — On a $\langle a\rangle \subseteq \langle a, b\rangle = \langle a \wedge b\rangle$, donc $a \wedge b$ divise a. Il divise b pour la même raison. Inversement, si un élément d de A divise a et b, on a $\langle d\rangle \supseteq \langle a\rangle$ et $\langle d\rangle \supseteq \langle b\rangle$, donc $\langle d\rangle \supseteq \langle a, b\rangle = \langle a \wedge b\rangle$ et d divise $a \wedge b$. Ceci montre la première partie du point (a). Pour la seconde, on remarque que si d est non nul, on a $x \in \langle \frac{a}{d}, \frac{b}{d}\rangle$ si et seulement si $dx \in \langle a, b\rangle$, donc $\frac{a}{d} \wedge \frac{b}{d} = \frac{a\wedge b}{d}$.

On a $\langle a \vee b\rangle \subseteq \langle a\rangle$, donc a divise $a \vee b$ et de même, b divise $a \vee b$. Inversement, si un élément e de A est divisible par a et b, on a $\langle e\rangle \subseteq \langle a\rangle$ et $\langle e\rangle \subseteq \langle b\rangle$, donc $\langle e\rangle \subseteq \langle a\rangle \cap \langle b\rangle = \langle a \vee b\rangle$ et e est divisible par $a \wedge b$. Ceci montre la première partie du point (b). Pour la seconde, on remarque que comme d est non nul, on a $x \in \langle \frac{a}{d}\rangle \cap \langle \frac{b}{d}\rangle$ si et seulement si $dx \in \langle a\rangle \cap \langle b\rangle$, donc $\frac{a}{d} \vee \frac{b}{d} = \frac{a\vee b}{d}$.

□

On peut définir la notion de pgcd et de ppcm dans les anneaux intègres généraux (mais ils n'existent pas toujours) en copiant les conclusions du lemme : on dit que d est un pgcd de a et de b si d divise a et b et que tout diviseur commun de a et de b divise d ; on dit que m est un ppcm de a et de b si m est un multiple de a et de b et que tout multiple commun de a et de b est un multiple de m. Nous montrerons dans la prop. 8.4 que pgcd et ppcm existent dans la classe plus générale des anneaux factoriels.

On dira aussi que des éléments d'un anneau intègre sont *premiers entre eux* si leurs seuls diviseurs communs sont les unités ; autrement dit, leur pgcd existe et est égal à 1.

***Théorème 6.4* (« Théorème de Bézout »).** — *Soit A un anneau principal. Des éléments a et b de A sont premiers entre eux si et seulement s'il existe x et y dans A tels que*

$$xa + yb = 1.$$

Démonstration. — L'existence de x et y équivaut à dire $1 \in (a, b)$, c'est-à-dire $a \wedge b = 1$. □

Voici maintenant un résultat classique.

***Proposition 6.5* (« Lemme de Gauss »).** — *Soit A un anneau principal. Si a, b et c sont des éléments de A tels que a divise bc mais est premier avec b, alors a divise c.*

De façon équivalente, si a et b sont premiers entre eux et qu'un élément de A est divisible par a et par b, il est divisible par ab; en d'autres termes, on a $a \vee b = ab$.

Démonstration. — Écrivons $bc = ad$ (puisque a divise bc) et $xa + yb = 1$ (puisque a et b sont premiers entre eux). On a alors $c = (xa + yb)c = xac + yad$, qui est bien divisible par a.

Pour la deuxième formulation, si x est divisible par a et par b, on écrit $x = bc$ (puisque b divise x). Comme a aussi divise x, il divise c par la première formulation, donc ab divise x. □

Corollaire 6.6. — *Soient a et b des éléments d'un anneau principal A. On a $(a \wedge b)(a \vee b) = ab$.*

Démonstration. — Le corollaire est évident si $a = b = 0$. Sinon, $a \wedge b \neq 0$ et il résulte de la prop. 6.3(a) que $\frac{a}{a\wedge b}$ et $\frac{b}{a\wedge b}$ sont premiers entre eux. Le lemme de Gauss entraîne donc $\frac{a}{a\wedge b} \vee \frac{b}{a\wedge b} = \left(\frac{a}{a\wedge b}\right)\left(\frac{b}{a\wedge b}\right)$. On applique alors la prop. 6.3(b), qui donne $\frac{a}{a\wedge b} \vee \frac{b}{a\wedge b} = \frac{a\vee b}{a\wedge b}$, d'où $\left(\frac{a}{a\wedge b}\right)\left(\frac{b}{a\wedge b}\right) = \frac{a\vee b}{a\wedge b}$ et le résultat cherché en multipliant les deux membres de cette égalité par $(a \wedge b)^2$. □

Proposition 6.7. — *Soit A un anneau principal et soient $a, b_1, \ldots, b_r$ des éléments de A.*

(a) *Si a est premier avec chacun des b_i, alors a est premier avec $b_1 \cdots b_r$.*

(b) *Si les b_i sont premiers entre eux deux à deux et que a est divisible par chacun des b_i, il est divisible par $b_1 \cdots b_r$.*

Démonstration. — Pour (a), on écrit le théorème de Bézout pour chacune des paires (a, b_i) : on a $x_i a + y_i b_1 = 1$. En prenant le produit de toutes ces identités, on obtient

$$(x_1 a + y_1 b_1) \cdots (x_r a + y_r b_r) = 1.$$

Le membre de gauche s'écrit $xa + y_1 \cdots y_r b_1 \cdots b_r = 1$ pour un certain $x \in A$, ce qui montre que a est premier avec $b_1 \cdots b_r$.

Pour (b), on procède par récurrence sur r, le cas $r = 1$ étant trivial. Supposons $r \geqslant 2$. Le point (a) nous dit que b_1 est premier avec $b_2 \cdots b_r$ et l'hypothèse de récurrence que a est divisible par $b_2 \cdots b_r$ (et par b_1). La deuxième version du lemme de Gauss entraîne que a est divisible par $b_1 \cdots b_r$. □

***Théorème 6.8* (« Théorème chinois des restes »)**. — *Soit A un anneau principal et soient $a_1, \ldots a_r$ des éléments de A premiers entre eux deux à deux. L'application*

$$\begin{array}{ccc} A & \longrightarrow & A/(a_1) \times \cdots \times A/(a_r) \\ x & \longmapsto & (\bar{x}, \ldots, \bar{x}) \end{array}$$

est un morphisme d'anneaux surjectif et son noyau est l'idéal $(a_1 \cdots a_r)$. Il induit donc un isomorphisme d'anneaux

$$A/(a_1 \cdots a_r) \xrightarrow{\sim} A/(a_1) \times \cdots \times A/(a_r).$$

Démonstration. — Il est clair que l'application en question est un morphisme d'anneaux. Posons $a = a_1 \cdots a_r$ et montrons que son noyau est l'idéal (a). Il est clair que cet idéal est contenu dans le noyau. Inversement, si x est dans le noyau, il est divisible par $a_1, \ldots, a_r$ donc par a (prop. 6.7(b)). Le théorème de factorisation donne donc un morphisme injectif

$$A/(a_1 \cdots a_r) \hookrightarrow A/(a_1) \times \cdots \times A/(a_r).$$

Notons que lorsqu'on a $A = \mathbf{Z}$, on peut abréger le reste de la démonstration en remarquant que ces deux ensembles sont finis (on peut supposer qu'aucun des a_i n'est nul) et de même cardinal. L'application est donc bijective.

Revenons au cas général pour montrer que l'application est surjective. Procédons par récurrence sur r. Si $r = 2$, on écrit $1 = x_1a_1 + x_2a_2$. Si $b_1, b_2 \in A$, l'image de $x_1a_1b_2 + x_2a_2b_1$ dans $A/(a_1) \times A/(a_2)$ est alors $(\bar{b}_1, \bar{b}_2)$. L'application est donc surjective.

Pour passer de $r-1$ à r, on remarque que a_1 est premier avec $a_2 \cdots a_r$ (prop. 6.7(a)). On a donc (cas $r = 2$) une surjection

$$A \twoheadrightarrow A/(a_1) \times A/(a_2 \cdots a_r)$$

et on conclut avec l'hypothèse de récurrence, qui donne un isomorphisme $A/(a_2 \cdots a_r) \xrightarrow{\sim} A/(a_2) \times \cdots \times A/(a_r)$: par composition, on obtient que le morphisme $A \to A/(a_1) \times \cdots \times A/(a_r)$ est bien surjectif. □

Le théorème chinois des restes nous permet d'analyser la structure du groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$ des unités de l'anneau $\mathbf{Z}/n\mathbf{Z}$. Commençons par un lemme.

Lemme 6.9. — *Soit n un entier strictement positif. Le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ des unités de l'anneau $\mathbf{Z}/n\mathbf{Z}$ est formé des classes d'entiers premiers avec n. On note $\varphi(n)$ son cardinal.*

Démonstration. — Les éléments inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$ sont les classes $\bar{x}$ telles qu'il existe une classe $\bar{y}$ vérifiant $\bar{x}\bar{y} = \bar{1}$ dans $\mathbf{Z}/n\mathbf{Z}$, c'est-à-dire $xy \equiv 1 \pmod{n}$. Par le théorème de Bézout (th. 6.4), c'est équivalent à dire que x et n sont premiers entre eux. □

On appelle φ la *fonction indicatrice d'Euler*. Une première conséquence du théorème chinois des restes est que si m et n sont des entiers premiers entre eux, on a

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Théorème 6.10. — *Soit n un entier strictement positif et soit $n = p_1^{v_1} \cdots p_r^{v_r}$ sa décomposition en produit de facteurs premiers.*

(a) *On a un isomorphisme d'anneaux*

$$\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/p_1^{v_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/\mathbf{Z}p_r^{v_r}.$$

(b) *On a un isomorphisme de groupes*

$$(\mathbf{Z}/n\mathbf{Z})^\times \simeq (\mathbf{Z}/p_1^{v_1}\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/p_r^{v_r}\mathbf{Z})^\times.$$

(c) *On a*

$$\varphi(n) = n(1 - 1/p_1) \cdots (1 - 1/p_r).$$

Démonstration. — Les points (1a) et (b) résultent du théorème chinois des restes, puisque les $p_i^{v_i}$ sont premiers entre eux deux à deux. Pour le point (c), il suffit de remarquer que le cardinal de $(\mathbf{Z}/p_i^{v_i}\mathbf{Z})^\times$, qui est le nombre d'entiers m premiers à $p_i^{v_i}$ et tels que $1 \leqslant m \leqslant p_i^{v_i}$, est $p_i^{v_i} - p_i^{v_i-1}$ (il suffit de retirer les multiples de p_i). □

On peut aller plus loin dans cette analyse et étudier la structure du groupe multiplicatif $(\mathbf{Z}/p^v\mathbf{Z})^\times$ pour p premier et $v \geqslant 1$. Le cas $p \geqslant 3$ est assez simple : les groupes $(\mathbf{Z}/p^v\mathbf{Z})^\times$ sont tous cycliques ; mais ce n'est plus le cas pour les groupes $(\mathbf{Z}/2^v\mathbf{Z})^\times$ lorsque $v \geqslant 3$. Nous laissons ça en exercice (voir th. II.2.18 pour le cas de $(\mathbf{Z}/p\mathbf{Z})^\times$).

Exemple 6.11. — On a $(\mathbf{Z}/8\mathbf{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ et un isomorphisme de groupes $(\mathbf{Z}/8\mathbf{Z})^\times \simeq (\mathbf{Z}/2\mathbf{Z})^2$, puisque $\bar{3}^2 = \bar{9} = \bar{1}$, $\bar{5}^2 = \overline{25} = \bar{1}$ et $\bar{7}^2 = (-\bar{1})^2 = \bar{1}$.

On a $(\mathbf{Z}/9\mathbf{Z})^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$ et un isomorphisme de groupes $(\mathbf{Z}/9\mathbf{Z})^\times \simeq \mathbf{Z}/6\mathbf{Z}$, puisque c'est le seul groupe abélien d'ordre 6. Remarquons que les puissances successives de $\bar{2}$ sont $\bar{2}, \bar{4}, \bar{8}, \bar{7}, \bar{5}, \bar{1}$, donc $\bar{2}$ engendre le groupe multiplicatif $(\mathbf{Z}/9\mathbf{Z})^\times$.

7. Anneaux euclidiens

Dans la pratique, on montre souvent qu'un anneau intègre A est principal en exhibant une *division euclidienne sur A,* c'est-à-dire une fonction $\varphi\colon A \smallsetminus \{0_A\} \to \mathbf{N}$ telle que pour tous éléments a et b de A, avec $b \neq 0$, on puisse écrire $a = bq+r$ avec $r = 0$, ou $r \neq 0$ et $\varphi(r) < \varphi(b)$ (on ne demande pas l'unicité). Un anneau est *euclidien* s'il est intègre et qu'il existe une telle fonction φ (appelée « stathme euclidien »).

L'anneau $\mathbf{Z}$ est euclidien pour la fonction $\varphi(n) = |n|$. Un autre exemple fondamental est celui de l'anneau des polynômes à une indéterminée à coefficients dans un corps (cor. 7.2). C'est une conséquence du résultat suivant.

***Théorème 7.1* (Division euclienne des polynômes).** — *Soit A un anneau intègre. Soient $P, Q \in A[X]$, où Q est un polynôme non nul dont le coefficient dominant est une unité de A. Alors, il existe un unique couple $B, R \in A[X]$ tel que $P = BQ + R$ et $\deg(R) < \deg(Q)$.*

Démonstration. — Montrons l'existence. On procède par récurrence sur $\deg(P)$, en commençant par le cas $\deg(P) = -\infty$, c'est-à-dire $P = 0$: on prend alors $B = R = 0$. Si $P \neq 0$, on écrit $P(X) = a_dX^d + \cdots + a_1X + a_0$, avec $a_d \neq 0_A$ et $d = \deg(P)$, et $Q(X) = b_eX^e + \cdots + b_1X + b_0$, avec $b_e \in A^\times$ et $e = \deg(Q)$. Si $d < e$, on prend $B = 0$ et $R = Q$. Si $d \geqslant e$, le polynôme

$$\begin{aligned} P_1(X) &\coloneqq P(X) - a_db_e^{-1}X^{d-e}Q(X) \\ &= a_dX^d + \cdots + a_1X + a_0 - a_db_e^{-1}X^{d-e}(b_eX^e + \cdots + b_1X + b_0) \\ &= a_dX^d + \cdots + a_1X + a_0 - (a_dX^d + \cdots + a_db_e^{-1}b_1X^{d-e+1} + a_db_e^{-1}b_0X^{d-e}) \\ &= (a_{d-1} - a_db_e^{-1}b_{d-1})dX^{d-1} + \ldots \end{aligned}$$

est de degré $< d$. On peut donc lui appliquer l'hypothèse de récurrence : il existe $B_1, R_1 \in A[X]$ tels que $P_1 = B_1Q + R_1$ et $\deg(R_1) < \deg(Q)$. On a ainsi

$$\begin{aligned} P(X) &= P_1(X) + a_db_e^{-1}X^{d-e}Q(X) \\ &= B_1(X)Q(X) + R_1(X) + a_db_e^{-1}X^{d-e}Q(X) \\ &= (B_1(X) + a_db_e^{-1}X^{d-e})Q(X) + R_1(X), \end{aligned}$$

ce qui montre ce que l'on voulait.

Montrons l'unicité. Si $P = BQ + R = B'Q + R'$, on a $(B - B')Q = R - R'$. Si $B \neq B'$, on a $R \neq R'$ et, en prenant les degrés et en utilisant la prop. 2.1(b),

$$\deg(R - R') = \deg(B - B')\deg(Q) \geqslant \deg(Q).$$

Mais cela contredit la prop. 2.1(a), puisque $\max\{\deg(R), \deg(R')\} < \deg(Q)$.

On a ainsi $B = B'$, donc $R = R'$. □

***Corollaire 7.2*.** — *Si K est un corps, l'anneau $K[X]$ est euclidien pour la fonction degré.*

Nous montrons maintenant le résultat principal de ce paragraphe.

***Théorème 7.3*.** — *Tout anneau euclidien est principal.*

Démonstration. — Soit A un anneau intègre muni d'un stathme euclidien $\varphi\colon A \smallsetminus \{0_A\} \to \mathbf{N}$. Soit I un idéal de A. Si I est nul, il est engendré par 0_A. Sinon, soit x un élément non nul de I tel que $\varphi(x)$ soit minimal. Nous allons montrer que I est engendré par x.

Soit a un élément quelconque non nul de I. On écrit $a = xq + r$ avec $r = 0$, ou $r \neq 0$ et $\varphi(r) < \varphi(x)$. Comme a et x sont dans I, il en est de même pour $r = a - xq$. Si $r \neq 0$, on a $\varphi(r) < \varphi(x)$, ce qui est impossible puisque $\varphi(x)$ est minimal. On a donc $r = 0$ et $a \in (x)$. □

Il existe des anneaux principaux non euclidiens, mais ils sont difficiles à construire (c'est le cas de l'anneau $\mathbf{Z}[(1+\sqrt{-19})/2]$).

Dans un anneau euclidien A, la division permet d'écrire un algorithme (dit « d'Euclide ») qui, étant donnés des éléments a et b non nuls de A, fournit un pgcd. Il fonctionne ainsi :

- on fait la division $a = bq + r$;
  - — si $r = 0$ (c'est-à-dire si b divise a), on arrête : $a \wedge b = b$;
  - — si $r \neq 0$, on remplace le couple (a, b) par le couple (b, r) (avec $\varphi(r) < \varphi(b)$).

Comme la suite des entiers naturels $\varphi(b)$ est strictement décroissante, l'algorithme s'arrête en temps fini. À chaque étape, le pgcd de a et b ne change pas (puisqu'on remplace (a, b) par $(b, a-bq)$) : on aboutit donc au couple $(a \wedge b, 0)$. D'autre part, l'algorithme fournit aussi des éléments x et y de A tels que $xa+yb = a \wedge b$: si on note (a_i, b_i) la paire obtenue à l'étape i, avec $(a_0, b_0) = (a, b)$ et $(a_{n+1}, b_{n+1}) = (a \wedge b, 0)$, on a $a_i = b_{i-1}$ et $b_i = a_{i-1} - b_{i-1}q_{i-1}$, donc $a_{i+1} = a_{i-1} - a_i q_{i-1}$, d'où

$$\begin{aligned} a \wedge b &= a_{n+1} \\ &= a_{n-1} - a_n q_{n-1} =: x_{n-1}a_{n-1} + y_{n-1}a_n \\ &= x_{n-1}a_{n-1} + y_{n-1}(a_{n-2} - a_{n-1}q_{n-2}) =: x_{n-2}a_{n-2} + y_{n-2}a_{n-1} \\ &\vdots \\ &= x_1 a_0 + y_1 a_1 = x_1 a_0 + y_1 b_0. \end{aligned}$$

Exemple 7.4. — Calculons le pgcd de deux nombres de Fibonacci consécutifs (c'est là où l'algorithme est le plus long), par exemple $8 \wedge 13$. On écrit

$$\begin{aligned} 8 &= 13 \cdot 0 + 8 && (8,13) \mapsto (13,8) \\ 13 &= 8 \cdot 1 + 5 && (13,8) \mapsto (8,5) \\ 8 &= 5 \cdot 1 + 3 && (8,5) \mapsto (5,3) \\ 5 &= 3 \cdot 1 + 2 && (5,3) \mapsto (3,2) \\ 3 &= 2 \cdot 1 + 1 && (3,2) \mapsto (2,1) \\ 2 &= 1 \cdot 2 + 0 && (2,1) \mapsto (1,0), \end{aligned}$$

de sorte que $8 \wedge 13 = 1$. Pour calculer les coefficients de Bézout, on écrit

$$1 = 3 - 2 = 3 - (5-3) = 2 \cdot 3 - 5 = 2 \cdot (8-5) - 5 = 2 \cdot 8 - 3 \cdot 5 = 2 \cdot 8 - 3 \cdot (13-8) = 5 \cdot 8 - 3 \cdot 13.$$

La division euclidienne est aussi utile pour décomposer une matrice à coefficients dans un anneau euclidien comme produit de matrices élémentaires (ce qu'on ne peut pas toujours faire pour les matrices à coefficients dans un anneau principal).

8. Anneaux factoriels

La notion de factorialité généralise la propriété de décomposition unique des nombres entiers en produit de nombres premiers. Le résultat principal de cette section est que tous les anneaux principaux sont factoriels. Commençons par la définition formelle.

Définition 8.1. — *Soit A un anneau. On dit que A est* factoriel *s'il vérifie les propriétés suivantes*

(I) *A est un anneau intègre ;*

(E) *tout élément non nul de A s'écrit sous la forme $up_1 \cdots p_r$, avec $u \in A^\times$, $r \in \mathbf{N}$ et $p_1, \ldots, p_r$ irréductibles ;*

(U) *cette décomposition est unique, « à permutation et à multiplication par des inversibles près » : si $up_1 \cdots p_r = vq_1 \cdots q_s$, avec $u, v \in A^\times$ et $p_1, \ldots, p_r, q_1, \ldots, q_s$ irréductibles, on a $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ tel que p_i et $q_{\sigma(i)}$ soient associés pour tout $i \in \{1, \ldots, r\}$.*

Exemple 8.2. — Dans l'anneau $\mathbf{Z}[\sqrt{-5}]$ vu dans l'ex. 5.3, on a les décompositions $6 = 3 \cdot 2 = (1+\sqrt{-5})(1-\sqrt{-5})$ et tous les facteurs de ces produits sont irréductibles dans l'anneau $\mathbf{Z}[\sqrt{-5}]$ (exerc. 11.17(3)). Cet anneau ne vérifie donc pas la propriété (U) (alors qu'il vérifie (I) et (E)).

Il est pratique d'introduire un système de représentants $\mathscr{P}$ des éléments irréductibles de A, c'est-à-dire un sous-ensemble $\mathscr{P}$ de A qui contient un et un seul élément irréductible par classe d'associés. Lorsque $A = \mathbf{Z}$, on peut prendre pour $\mathscr{P}$ l'ensemble des nombres premiers positifs. Lorsque A est l'anneau des polynômes à une indéterminée à coefficients dans un corps, on peut prendre pour $\mathscr{P}$ l'ensemble des polynômes irréductibles unitaires. Tout élément a d'un anneau factoriel s'écrit alors de façon unique comme

$$a = u \prod_{p \in \mathscr{P}} p^{v_p(a)}, \tag{2}$$

où les $v_p(a)$ (la *valuation p-adique* de a) sont des entiers naturels presque tous nuls. On a la propriété

$$\forall a, b \in A \smallsetminus \{0_A\} \quad \forall p \in \mathscr{P} \qquad v_p(ab) = v_p(a) + v_p(b).$$

Proposition 8.3. — *Soit A un anneau factoriel et soient a et b des éléments non nuls de A qu'on écrit comme dans* (2)*. Alors a divise b si et seulement si $v_p(a) \leqslant v_p(b)$ pour tout $p \in \mathscr{P}$.*

Démonstration. — Si $v_p(a) \leqslant v_p(b)$ pour tout $p \in \mathscr{P}$, il est clair que $a \mid b$. Inversement, si $a \mid b$, on écrit

$$b = ac = \Big(u \prod_{p \in \mathscr{P}} p^{v_p(a)}\Big)\Big(v \prod_{p \in \mathscr{P}} p^{v_p(c)}\Big) = uv \prod_{p \in \mathscr{P}} p^{v_p(a)+v_p(c)}.$$

On en déduit $v_p(b) = v_p(a)+v_p(c)$ par la propriété d'unicité (U), d'où $v_p(b) \geqslant v_p(a)$ pour tout $p \in \mathscr{P}$. □

Les pgcd et les ppcm, qu'on a définis dans tout anneau intègre (§ 6), mais dont on n'a montré l'existence que dans les anneaux principaux, existent aussi dans les anneaux factoriels.

Proposition 8.4. — *Soit A un anneau factoriel et soient a et b des éléments de A. Alors le pgcd $a \wedge b$ et le ppcm $a \vee b$ existent : si a et b sont non nuls et que*

$$a = u \prod_{p \in \mathscr{P}} p^{v_p(a)} \quad , \quad b = v \prod_{p \in \mathscr{P}} p^{v_p(b)},$$

on a

$$a \wedge b = \prod_{p \in \mathscr{P}} p^{\min\{v_p(a), v_p(b)\}} \quad , \quad a \vee b = \prod_{p \in \mathscr{P}} p^{\max\{v_p(a), v_p(b)\}}.$$

En particulier, on a, dans un anneau factoriel, $(a \wedge b)(a \vee b) = ab$, une propriété qu'on avait déjà établie dans les anneaux principaux (exerc. 6.6).

On peut bien sûr définir de façon analogue définir le pgcd $a_1 \wedge \cdots \wedge a_m$ et le ppcm $a_1 \vee \cdots \vee a_m$ d'une famille finie quelconque $a_1, \ldots, a_m$ d'éléments d'un anneau factoriel.

Démonstration. — Si $a = 0$, on a $0 \wedge b = b$ et $0 \vee b = 0$. Supposons a et b non nuls. Avec les notations de l'énoncé de la proposition, $d := \prod_{p \in \mathscr{P}} p^{\min\{v_p(a), v_p(b)\}}$ divise a et b. Si x divise a et b, on a $v_p(x) \leqslant v_p(a)$ et $v_p(x) \leqslant v_p(b)$ pour tout $p \in \mathscr{P}$ (prop. 8.3), donc $v_p(x) \leqslant v_p(d)$, et $x \mid d$ (prop. 8.3). Ceci montre que d est bien un pgcd de a et b. On procède de façon analogue pour le ppcm. □

Remarque 8.5. — Attention ! Dans un anneau factoriel, on n'a pas nécessairement $(a, b) = (a \wedge b)$ et $(a) \cap (b) = (a \vee b)$ (comme c'est le cas dans les anneaux principaux). Par exemple, si K est un corps, l'anneau $K[X, Y]$ est factoriel (th. 9.5). On a $X \wedge Y = 1$, mais $(X, Y) = \{P \in K[X, Y] \mid P(0, 0) = 0\} \neq (1)$.

Dans la déf. 8.1, c'est la propriété (U) qui est la plus contraignante (*cf.* ex. 8.2) ; la propriété (E) est en fait satisfaite dans une classe beaucoup plus vaste d'anneaux. Expliquons pourquoi. Soit A un anneau intègre et soit a un élément de A ne pouvant s'écrire comme dans (E). Il n'est alors ni inversible, ni irréductible, donc on peut l'écrire $a = a_1 b_1$, où ni a_1, ni b_1 n'est une unité, c'est-à-dire $(a) \subsetneq (a_1)$ et $(a) \subsetneq (b_1)$. Remarquons que a_1 et b_1 ne peuvent s'écrire tous les deux comme dans (E) (sinon, a le pourrait aussi) ; on peut supposer que a_1 ne peut s'écrire comme dans (E) et recommencer le processus, ce qui construit une suite infinie strictement croissante d'idéaux

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

Il s'avère que de telles chaînes infinies d'idéaux (pas nécessairement principaux) n'existent pas dans les anneaux *noethériens* (on peut prendre ça comme leur définition), une classe très vaste d'anneaux (qui contient celle des anneaux principaux) nommés ainsi en l'honneur d'Emmy Noether, mathématicienne allemande du début du XX$^{\text{e}}$ siècle, qui les a beaucoup étudiés. C'est par ailleurs clair dans l'anneau $\mathbf{Z}$ (puisqu'on a alors $|a_{i+1}| < |a_i|$), ou dans l'anneau des polynômes à une indéterminée à coefficients dans un corps (puisqu'on a alors $\deg(a_{i+1}) < \deg(a_i)$), ou plus généralement dans un anneau euclidien.

Théorème 8.6. — *Tout anneau principal est factoriel.*

Démonstration. — Nous allons procéder en deux temps, en montrant d'abord que les anneaux principaux vérifient la propriété (E), puis en donnant une caractérisation des anneaux factoriels parmi les anneaux intègres vérifiant (E).

Lemme 8.7. — *Tout anneau principal vérifie la propriété (E).*

Démonstration. — Comme on l'a remarqué plus haut, il suffit de montrer qu'il n'existe pas de suite infinie $(I_n)_{n\in\mathbf{N}}$ strictement croissante d'idéaux d'un anneau principal A. Soit $I \coloneqq \bigcup_{n\in\mathbf{N}} I_n$; c'est un idéal de A : si $x, y \in I$, il existe $m, n \in \mathbf{N}$ tels que $x \in I_m$ et $y \in I_n$. Si $a \in A$, on a bien $ax \in I_m \subseteq I$. On a aussi $x, y \in I_{\max\{m,n\}}$, donc $x + y \in I_{\max\{m,n\}} \subseteq I$.

Comme A est principal, l'idéal I est engendré par un élément a de I. Il existe un entier $r \in \mathbf{N}$ tel que $a \in I_r$, de sorte que $I = (a) \subseteq I_r \subseteq I$, et $I_r = I_s = I$ pour tout $s \geqslant r$, ce qui contredit l'hypothèse que la suite $(I_n)_{n\in\mathbf{N}}$ est strictement croissante. □

Lemme 8.8. — *Soit A un anneau intègre et soit p un élément irréductible de A. Tout élément a de A est ou bien premier avec p, ou bien divisible par p.*

Démonstration. — Supposons a non divisible par p. Soit x un diviseur commun de p et de a ; on écrit $p = xy$. Remarquons que y n'est pas une unité : sinon, p diviserait x, donc a. Comme p est irréductible, on en déduit que x est une unité : tout diviseur commun à p et a est donc une unité. □

Lemme 8.9. — *Soit A un anneau intègre vérifiant la propriété (E). Les propriétés suivantes sont équivalentes :*

(i) *l'anneau A est factoriel ;*
(ii) *pour tout élément irréductible p de A, l'idéal (p) est premier ;*
(iii) *le lemme de Gauss (prop. 6.5) est vrai dans A : si a, b et c sont des éléments de A tels que a divise bc mais est premier avec b, alors a divise c.*

Démonstration. — Supposons (iii). Soit p un élément irréductible de A. On a $(p) \neq A$ car p n'est pas inversible. Si $ab \in (p)$, alors $p \mid ab$. Par le lemme 8.8, soit p divise a, auquel cas $a \in (p)$, soit p est premier avec a, auquel cas p divise b par le lemme de Gauss, c'est-à-dire $b \in (p)$. Donc (iii) ⇒ (ii).

Supposons (ii). Pour montrer que A est factoriel, il suffit de comparer des décompositions $a = u\prod_{p\in\mathscr{P}} p^{v_p} = v\prod_{p\in\mathscr{P}} p^{w_p}$. Si $w_{p_0} \neq v_{p_0}$ pour un $p_0 \in \mathscr{P}$, on a par exemple $w_{p_0} > v_{p_0}$ et p_0 divise

$\prod_{p\in\mathscr{P},p\neq p_0} p^{v_p}$. Comme l'idéal (p_0) est premier, p_0 divise un $p \neq p_0$. Ces deux éléments irréductibles sont alors associés, ce qui contredit le choix de $\mathscr{P}$. On a donc une contradiction, de sorte que $w_{p_0} = v_{p_0}$ pour tout $p_0 \in \mathscr{P}$, ce qui montre (ii) $\Rightarrow$ (i).

Enfin, supposons l'anneau A factoriel et que a divise bc, avec a premier avec b. Si $c = 0$, alors a divise c. Supposons donc $c \neq 0$. Si $b = 0$, alors a divise a et b, donc a est une unité : il divise bien c. On peut donc supposer aussi $b \neq 0$, soit $bc \neq 0$. Comme a divise bc, on a aussi $a \neq 0$. On a alors $v_p(a) \leqslant v_p(b) + v_p(c)$ pour tout $p \in \mathscr{P}$ (par la prop. 8.3, car a divise bc). Comme a est premier avec b, on a, pour tout p, soit $v_p(a) = 0$, soit $v_p(b) = 0$ (prop. 8.4). Dans les deux cas, on obtient $v_p(a) \leqslant v_p(c)$, c'est-à-dire $a \mid c$. Donc (i) $\Rightarrow$ (iii). □

Le théorème résulte alors de l'implication (ii) $\Rightarrow$ (i) et de la prop. 6.1. □

9. Factorialité des anneaux de polynômes

Soit A un anneau factoriel. Nous allons montrer que l'anneau $A[X]$ des polynômes à une variable à coefficients dans A est encore factoriel. Pour cela, nous identifions tout d'abord les éléments irréductibles de l'anneau $A[X]$ en les comparant à ceux de l'anneau principal $K_A[X]$, puis nous utilisons la factorialité de l'anneau $K_A[X]$ (th. 8.6). On rappelle que, comme A est intègre, les unités de l'anneau $A[X]$ sont celles de A.

Définition 9.1. — *Soit A un anneau factoriel. Le* contenu *d'un élément P de $A[X]$, noté $c(P)$, est le pgcd (dans A) de ses coefficients. On dit que P est* primitif *si $c(P) = 1$.*

Le contenu n'est défini qu'à multiplication par une unité près. On a $c(P) = 0$ si et seulement si $P = 0$. Si P est un polynôme non nul, $c(P)$ est non nul et $P/c(P)$ est un polynôme primitif.

Lemme 9.2 **(Gauss)**. — *Soit A un anneau factoriel. Si $P, Q \in A[X]$, on a $c(PQ) = c(P)c(Q)$.*

Démonstration. — On peut supposer P et Q non nuls et il suffit, en considérant $P/c(P)$ et $Q/c(Q)$, de montrer que le produit de polynômes P et Q primitifs est encore primitif.

Or si $c(PQ) \neq 1$, il est divisible par un élément irréductible p. Cela signifie que dans l'anneau intègre $A/(p)[X]$, on a $\bar{P}\bar{Q} = 0$ donc, par exemple $\bar{P} = 0$. Tous les coefficients de P sont donc divisibles par p, c'est-à-dire $p \mid c(P)$, ce qui contredit l'hypothèse que P est primitif [2]. □

Théorème 9.3. — *Soit A un anneau factoriel de corps des fractions K_A. Les éléments irréductibles de l'anneau $A[X]$ sont :*

- *les éléments irréductibles de A ;*
- *les polynômes primitifs de degré au moins 1 qui sont irréductibles dans $K_A[X]$.*

Démonstration. — Soit $P \in A[X]$ un polynôme constant non nul (c'est-à-dire de degré 0, ou encore dans A). S'il s'écrit $P = QR$, les polynômes Q et R sont aussi de degré 0, donc dans A. Comme $A[X]^\times = A^\times$ (prop. 2.1(c)), cela revient donc au même, pour un polynôme constant, d'être irréductible dans A ou dans $A[X]$.

Supposons maintenant P de degré au moins 1. Si P est irréductible dans $A[X]$, il est primitif puisqu'on peut toujours le décomposer en produit $P = c(P)(P/c(P))$ de deux éléments de $A[X]$. Montrons qu'il est

2. On peut aussi, pour éviter de considérer l'anneau $A/(p)[X]$, regarder le coefficient de a_i de X^i dans P non divisible par p avec i minimal (il existe car, P étant primitif, tous ses coefficients ne peuvent pas être divisibles par p) et le coefficient analogue b_j de Q. Le coefficient de X^{i+j} dans PQ est alors congru à $a_i b_j$ modulo p : il n'est donc pas divisible par p. Aucun élément irréductible de A ne divise donc tous les coefficients de PQ, ce qui montre que ce polynôme est primitif.

irréductible dans $K_A[X]$. Si $P = QR$, avec $Q, R \in K_A[X]$, on peut écrire $Q = Q_1/q$ et $R = R_1/r$, avec $q, r \in A$ non nuls et $Q_1, R_1 \in A[X]$, soit encore $qrP = Q_1R_1$. En prenant les contenus, on obtient, par le lemme de Gauss,

$$qr = c(Q_1)c(R_1) \pmod{A^\times},$$

soit encore

$$P = QR = \frac{Q_1R_1}{qr} = \frac{Q_1R_1}{c(Q_1)c(R_1)} = \Big(\frac{Q_1}{c(Q_1)}\Big)\Big(\frac{R_1}{c(R_1)}\Big) \pmod{A^\times}.$$

Comme P est irréductible dans $A[X]$, l'un de ces facteurs est une unité dans $A[X]$, donc est de degré 0. L'un des facteurs Q ou R est alors de degré 0, donc inversible dans $K_A[X]$. On a donc bien montré que P est irréductible dans $K_A[X]$.

Supposons inversement P primitif et irréductible dans $K_A[X]$. Si $P = QR$, avec $Q, R \in A[X]$, l'un des facteurs, par exemple Q, est une unité dans $K_A[X]$, donc de degré 0. Comme $c(P) = c(Q)c(R)$ est une unité, Q et R sont tous deux primitifs, et Q est inversible dans $A[X]$. On a ainsi montré que P est irréductible dans $A[X]$. □

Exemple 9.4. — Les polynômes 3 et $2X^2 + 1$ sont donc irréductibles dans $\mathbf{Z}[X]$ et dans $\mathbf{Q}[X]$.

Le th. 9.3 dit que pour un polynôme primitif de $A[X]$, il revient au même d'être irréductible dans $A[X]$ que dans l'anneau principal $K_A[X]$ (ce n'est pas du tout évident, puisqu'il y a a priori plus de décompositions possibles dans $K_A[X]$ que dans $A[X]$).

Théorème 9.5. — *Soit A un anneau factoriel. Les anneaux de polynômes $A[X_1, \dots, A_n]$ sont aussi factoriels.*

Démonstration. — Il suffit bien sûr de traiter le cas $n = 1$, c'est-à-dire de montrer que l'anneau $A[X]$ est factoriel.

Comme A est factoriel, il est intègre, donc $A[X]$ est aussi intègre (prop. 2.1(b)). Montrons la propriété (E) d'existence d'une décomposition de $P \in A[X]$ non nul en produit d'irréductibles. En écrivant $P = c(P)(P/c(P))$ et en décomposant $c(P)$ en produit d'irréductibles de A (qui sont irréductibles dans $A[X]$ par le th. 9.3), on voit qu'il suffit de traiter le cas où P est un polynôme primitif non constant.

L'anneau $K_A[X]$ étant principal, donc factoriel, il existe une décomposition de P en produit de polynômes irréductibles de $K_A[X]$. En chassant les dénominateurs, on peut écrire cette décomposition comme

$$aP = P_1 \cdots P_r \quad \text{où } a \in A \text{ et } P_1, \dots, P_r \in A[X], \text{ irréductibles dans } K_A[X].$$

En prenant les contenus, on obtient, par le lemme de Gauss, $a = c(P_1) \cdots c(P_r)$, d'où

$$P = \frac{P_1}{c(P_1)} \cdots \frac{P_r}{c(P_r)}.$$

Les $P_i/c(P_i)$ sont des polynômes primitifs de $A[X]$ associés aux P_i dans $K_A[X]$, donc encore irréductibles dans cet anneau. Ils sont donc irréductibles dans $A[X]$ par le th. 9.3. Ceci établit bien la propriété (E).

Par le lemme 8.9, il suffit maintenant de montrer que si $P \in A[X]$ est irréductible, alors l'idéal (P) est premier.

Si P est constant, c'est un élément irréductible de A ; comme A est factoriel, il engendre un idéal premier dans A. Si P divise QR, avec $Q, R \in A[X]$, on a $P = c(P) \mid c(QR) = c(Q)c(R)$ (lemme de Gauss). Comme P engendre un idéal premier de A, on a par exemple $P \mid c(Q) \mid Q$. L'idéal (P) est donc bien premier dans l'anneau $A[X]$.

Supposons maintenant P de degré au moins 1. Il est alors primitif, et irréductible dans $K_A[X]$ (th. 9.3). Si P divise QR, avec $Q, R \in A[X]$, il divise par exemple Q dans $K_A[X]$ (puisque P est irréductible dans cet anneau principal). On peut donc écrire comme d'habitude $aQ = PS$, avec $a \in A$ et $S \in A[X]$; en

prenant les contenus, on obtient $ac(Q) = c(S)$, donc $a \mid c(S)$ et $S/a \in A[X]$. Comme $Q = P \cdot (S/a)$, on en déduit que P divise Q dans $A[X]$. Ceci montre que l'idéal (P) est bien premier dans $A[X]$. □

Le théorème suivant est un critère d'irréductibilité bien pratique pour les polynômes à coefficients dans un anneau factoriel.

***Théorème 9.6* (Critère d'Eisenstein).** — *Soit A un anneau factoriel de corps des fractions K_A et soit $P = a_n X^n + \cdots + a_0 \in A[X]$ un polynôme non constant. On suppose qu'il existe un élément irréductible p de A tel que*

(a) *p ne divise pas a_n ;*
(b) *p divise $a_{n-1}, \ldots, a_0$;*
(c) *p^2 ne divise pas a_0.*

Alors P est irréductible dans $K_A[X]$ (et donc dans $A[X]$ s'il est primitif).

Démonstration. — La propriété (a) entraîne que le contenu $c(P)$ n'est pas divisible par p. Le polynôme primitif $P/c(P)$ vérifie donc les propriétés (a), (b) et (c) et on peut supposer P primitif, de degré au moins 2 (puisqu'un polynôme de degré 1 est toujours irréductible dans $K_A[X]$).

Si P n'est pas irréductible dans $K_A[X]$, il ne l'est pas non plus dans $A[X]$ par le th. 9.3, donc il s'écrit

$$P = QR = (b_r X^r + \cdots + b_0)(c_s X^s + \cdots + c_0),$$

avec $Q, R \in A[X]$ et $Q, R \notin A^\times$, et $n = r + s$ et $a_n = b_r c_s$. En prenant les contenus, on obtient $1 = c(Q)c(R)$, donc Q et R sont aussi primitifs et ne peuvent donc être constants (puisque ce ne sont pas des unités). On a donc $r, s \geqslant 1$.

Réduisons cela modulo p, c'est-à-dire que l'on regarde cette égalité dans l'anneau intègre $(A/(p))[X]$. On a par hypothèse $\bar{P} = \bar{a}_n X^n$, avec $\bar{a}_n \neq 0$, de sorte que $\bar{b}_r, \bar{c}_s \neq 0$. Comme X est irréductible dans l'anneau principal $K_{A/(p)}[X]$, c'est la décomposition de $\bar{P}$ en produit d'irréductibles dans cet anneau. Le seul facteur irréductible de $\bar{Q}$ et de $\bar{R}$ est donc X, de sorte que $\bar{Q} = \bar{b}_r X^r$ et $\bar{R} = \bar{c}_s X^s$. On en déduit $0 = \bar{b}_0 = \bar{c}_0$, ce qui signifie que b_0 et c_0 sont tous les deux divisibles par p. Mais $a_0 = b_0 c_0$ est alors divisible par p^2, ce qui contredit (c). On a donc bien montré que P est irréductible dans $K_A[X]$ [3]. □

***Exemple 9.7*.** — Pour tout entier $n \geqslant 1$ et tout nombre premier p, les polynômes $X^n \pm p$ sont irréductibles dans $\mathbf{Q}[X]$.

10. Compléments

10.1. Racines d'un polynôme à une variable. — Soit A un anneau commutatif et soit

$$P(X) = a_n X^n + \cdots + a_0$$

un élément de $A[X]$. Soit x un élément de A. On pose

$$P(x) \coloneqq a_n x^n + \cdots + a_0 \in A.$$

L'application

$$\begin{aligned} \mathrm{ev}_x \colon A[X] &\longrightarrow A \\ P &\longmapsto P(x) \end{aligned}$$

est un morphisme d'anneaux appelé *évaluation en x*.

3. On peut aussi utiliser l'argument plus terre-à-terre suivant : comme $a_0 = b_0 c_0$ n'est pas divisible par p^2, les éléments b_0 et c_0 de A ne peuvent être tous les deux divisibles par p. Supposons donc $p \nmid b_0$. Comme p ne divise pas a_n, il ne divise pas non plus c_s ; on peut donc considérer le plus petit entier $t \in \{0, \ldots, s\}$ tel que $p \nmid c_t$, de sorte que $c_{t-1}, c_{t-2}, \ldots$ sont divisibles par p. Alors, $a_t = b_0 c_t + b_1 c_{t-1} + \cdots \equiv b_0 c_t \not\equiv 0 \pmod{p}$, ce qui contredit l'hypothèse (b), puisque $t \leqslant s < n$.

On a pour tout entier $m \geqslant 1$ l'identité remarquable

$$X^m - x^m = (X-x)\Big(\sum_{i=0}^{m-1} x^i X^{m-1-i}\Big).$$

En particulier, le polynôme $X^m - x^m$ est divisible par $X - x$. Il s'ensuit que le polynôme

$$P(X) - P(x) = (a_n X^n + \cdots + a_0) - (a_n x^n + \cdots + a_0) = a_n(X^n - x^n) + \cdots + a_1(X - x)$$

est aussi divisible par $X - x$ [4].

On dit qu'un élément x de A est une *racine* de P si $P(x) = 0_A$. Nous avons donc démontré le résultat suivant.

Proposition 10.1. — *Soit A un anneau commutatif, soit P un élément de $A[X]$ et soit x un élément de A. On a équivalence entre*

(i) *x est racine de P, c'est-à-dire $P(x) = 0_A$;*

(ii) *le polynôme P est divisible par $X - x$ dans $A[X]$.*

Définition 10.2. — *Soit A un anneau commutatif, soit P un élément* non nul *de $A[X]$ et soit x un élément de A. On appelle* multiplicité *de x comme racine de P le plus grand entier m tel que P est divisible par $(X - x)^m$.*

Cette définition a un sens même si A n'est pas intègre : le polynôme $(X - x)^m$ étant unitaire, on a $m \leqslant \deg(P)$ s'il divise P ; la multiplicté de toute racine de P est donc $\leqslant \deg(P)$. On peut décider que la multiplicité de n'importe quel élément de A comme racine du polynôme nul est infinie.

Proposition 10.3. — *Soit A un anneau* intègre*. Soit P un élément non nul de $A[X]$ et soient $x_1, \ldots, x_r \in A$ des racines* distinctes *de P, de multiplicités respectives $m_1, \ldots, m_r$. Alors P est divisible par le polynôme $(X - x_1)^{m_1} \ldots (X - x_r)^{m_r}$. En particulier, $\deg(P) \geqslant m_1 + \cdots + m_r$.*

Un polynôme à coefficients dans un anneau intègre qui a un nombre infini de racines est donc nul.

La conclusion de la proposition ne subsiste pas dans un anneau non intègre : dans $\mathbf{Z}/8\mathbf{Z}$, le polynôme $4X$, de degré 1, a 4 racines (simples), 0, 2, 4, et 6, tandis que le polynôme X^3, de degré 3, a comme racines 0 (triple), 2, 4 (double), et 6.

Démonstration. — Plaçons-nous dans l'anneau principal $K_A[X]$. Soit $i \neq j$; comme $X - x_i$ et $X - x_j$ sont premiers entre eux (une relation de Bézout est $\frac{1}{x_j - x_i}\big((X - x_i) - (X - x_j)\big) = 1$), il en est de même de $(X - x_i)^{m_i}$ et $(X - x_j)^{m_j}$, par deux applications de la prop. 6.7(a). Comme P est divisible par chaque $(X - x_i)^{m_i}$, il est divisible par leur produit (prop. 6.7(b)), dans l'anneau $K_A[X]$. Mais le quotient de P par $\prod_i (X - x_i)^{m_i}$ est en fait dans $A[X]$, puisque $\prod_i (X - x_i)^{m_i}$ est un polynôme unitaire (th. 7.1). □

10.2. Polynôme dérivé et formule de Taylor. —

Définition 10.4. — *Soit A un anneau commutatif et soit $P = a_n X^n + \cdots + a_0$ un élément de $A[X]$. On appelle* polynôme dérivé *de P le polynôme*

$$P'(X) := n a_n X^{n-1} + \cdots + a_1.$$

4. On peut aussi raisonner ainsi : comme le polynôme $X - x$ est unitaire, on peut diviser P par $X - x$ dans $A[X]$ (th. 7.1). On obtient $P(X) = (X - x)Q(X) + R(X)$, avec $R = 0$ ou $\deg(R) < \deg(X - x) = 1$, c'est-à-dire que R est une constante. En « faisant $X = x$ » (il faudrait dire « en prenant les images des deux membres de cette égalité par le morphisme d'anneaux ev_x »), on obtient $R(X) = P(x)$, d'où $P(X) = (X - x)Q(X) + P(x)$: le polynôme $P(X) - P(x)$ est donc bien divisible par $X - x$.

Il est clair que la dérivation est linéaire (c'est un morphisme de groupes abéliens de $A[X]$ dans $A[X]$) : on a $(P+Q)' = P' + Q'$. On vérifie par un calcul direct la formule de Leibniz

$$\forall P, Q \in A[X] \qquad (PQ)' = P'Q + PQ',$$

ainsi que

$$\forall P, Q \in A[X] \qquad (P \circ Q)' = (P' \circ Q)Q'.$$

Lorsque $A = \mathbf{R}$, la fonction polynomiale $x \mapsto P'(x)$ est bien la dérivée (au sens des fonctions réelles de variable réelle) de la fonction polynomiale $x \mapsto P(x)$, mais notre définition générale est purement formelle et ne fait pas intervenir de notion de limite (qui n'aurait aucun sens dans un anneau général).

La dérivée d'un polynôme constant est nulle mais un polynôme de dérivée nulle peut ne pas être constant : si p est un nombre premier, c'est le cas du polynôme X^p dans $(\mathbf{Z}/p\mathbf{Z})[X]$.

On peut itérer l'opération de dérivation en posant $P'' \coloneqq (P')'$, etc. On définit ainsi $P^{(r)}$, la dérivée r-ième de P, pour tout entier naturel r. Noter que $P^{(r)} = 0$ pour tout $r > \deg(P)$.

***Proposition 10.5* (Formule de Taylor).** — *Soit A un anneau commutatif, soit $P \in A[X]$ un polynôme de degré inférieur ou égal à n, et soit $x \in A$.*

(a) *Si $n! \cdot 1_A$ est inversible dans A, on a* [5]

$$P(X) = P(x) + \frac{P'(x)}{1!}(X-x) + \cdots + \frac{P^{(n)}(x)}{n!}(X-x)^n.$$

(b) *Soit m un entier positif. On a*

$$x \text{ est racine de } P \text{ de multiplicité } > m \implies P(x) = \cdots = P^{(m)}(x) = 0.$$

La réciproque est vraie si $m! \cdot 1_A$ est inversible dans A.

En particulier, dans tous les cas, x est racine multiple (c'est-à-dire de multiplicité > 1) de P si et seulement si $P(x) = P'(x) = 0$ (on applique (b) avec $m = 1$).

Démonstration. — Il suffit de montrer la proposition pour $x = 0_A$ puis de l'appliquer au polynôme $Q(X) \coloneqq P(X+x)$, en notant que $P^{(r)}(x) = Q^{(r)}(0)$ pour tout entier positif r.

Le point (a) résulte alors du fait que, si $Q = a_n X^n + \cdots + a_0$, on a $Q^{(r)}(0) = r! a_r$.

Pour le point (b), si 0_A est racine de Q de multiplicité $> m$, on a $a_m = \cdots = a_0 = 0$; inversement, si $Q(0_A) = \cdots = Q^{(m)}(0_A) = 0$, on a $m! a_m = \cdots = 0! a_0 = 0$, d'où $a_m = \cdots = a_0 = 0$ si $m! \cdot 1_A$ est inversible dans A (il en est alors de même de $r! \cdot 1_A$ pour tout $r \leqslant m$). □

Exemple 10.6. — Soit p un nombre premier, de sorte que l'anneau $\mathbf{Z}/p\mathbf{Z}$ est intègre (c'est même un corps). Considérons le polynôme $P(X) = X^p - X \in (\mathbf{Z}/p\mathbf{Z})[X]$. Comme $(\mathbf{Z}/p\mathbf{Z})^\times$ est un groupe (multiplicatif) d'ordre $p-1$, on a (théorème de Lagrange) $x^{p-1} = 1$ pour tout $x \in (\mathbf{Z}/p\mathbf{Z})^\times$, donc $x^p = x$ pour tout $x \in \mathbf{Z}/p\mathbf{Z}$. Le polynôme P a donc au moins p racines distinctes. Comme il est de degré p, ce sont toutes ses racines, elles sont simples et (prop. 10.3)

$$X^p - X = \prod_{x \in \mathbf{Z}/p\mathbf{Z}} (X-x) \in (\mathbf{Z}/p\mathbf{Z})[X].$$

On vérifie dans ce cas la prop. 10.5(b) : on a $P'(X) = -1$, donc P' n'a aucune racine et toutes les racines de P sont simples.

5. Dans cette relation, $\frac{P^{(n)}(x)}{n!}$ signifie $P^{(n)}(x)(n! \cdot 1_A)^{-1}$.

10.3. Décomposition en éléments simples des fractions rationnelles. — Soit K un corps. Une fraction rationnelle (à coefficients dans K) est un élément du corps des fractions $K(X)$ de l'anneau de polynômes $K[X]$. Elle s'écrit donc P/Q, avec $P, Q \in K[X]$ et Q non nul. Comme l'anneau $K[X]$ est factoriel, on peut toujours supposer P et Q premiers entre eux.

Le théorème suivant est parfois utile pour trouver des primitives des fractions rationnelles. C'est un classique des programmes de classes préparatoires dont la vraie utilité mathématique est marginale. Il est aussi au programme de l'agrégation. L'énoncé théorique est simple à démontrer ; la mise en œuvre pratique de la décomposition donne lieu à des myriades d'astuces (mais les ordinateurs font ça très bien).

Théorème 10.7. — *Soit K un corps. Soient P et Q des éléments non nuls de $K[X]$ premiers entre eux et soit*

$$Q = \prod_{i=1}^{r} Q_i^{v_i}$$

la décomposition de Q en produit de facteurs irréductibles dans $K[X]$. Il existe une unique décomposition

$$\frac{P}{Q} = E + \sum_{i=1}^{r} \Big(\frac{A_{i,1}}{Q_i} + \cdots + \frac{A_{i,v_i}}{Q_i^{v_i}} \Big)$$

avec $E, A_{i,j} \in K[X]$ et $\deg(A_{i,j}) < \deg(Q_i)$.

Le polynôme E est appelé *partie entière* de la fraction rationnelle P/Q. Il est obtenu comme quotient de la division euclidienne de P par Q (th. 7.1).

Dans la pratique, on est souvent dans $\mathbf{C}$, de sorte que les Q_i sont des polynômes de degré 1 et les $A_{i,j}$ des constantes, ou dans $\mathbf{R}$, auquel cas les Q_i sont des polynômes de degré 1 ou 2 (il est souvent utile de commencer par décomposer sur $\mathbf{C}$: on regroupe ensuite les fractions dont les dénominateurs sont conjugués).

Je ne donnerai qu'une seule astuce : si $Q_1(X) = X - x$ et $v_1 = 1$ (c'est-à-dire x est racine simple de Q), il est facile de déterminer la constante $a = A_{1,1}$. Écrivons $Q(X) = (X - x)R(X)$, avec $R(x) \neq 0$; on peut alors écrire

$$\frac{P}{Q} = E + \frac{a}{X - x} + \frac{P_1}{R},$$

On en déduit, en réduisant au même dénominateur,

$$P(X) = E(X)Q(X) + aR(X) + (X - x)P_1(X)$$

d'où on tire, « en faisant $X = x$ », la relation $a = P(x)/R(x)$. On obtient d'autre part par dérivation $Q'(X) = R(X) + (X - x)R'(X)$, soit $R(x) = Q'(x)$, d'où finalement

$$a = \frac{P(x)}{Q'(x)}.$$

Exemple 10.8. — Soit $P \in \mathbf{C}[X]$ et soit $n > \deg(P)$; on pose $\omega \coloneqq e^{2i\pi/n}$. Cherchons la décomposition en éléments simples

$$\frac{P(X)}{X^n - 1} = \sum_{k=0}^{n-1} \frac{a_k}{X - \omega^k}.$$

D'après ce qui précède, on a

$$a_k = \frac{P(\omega^k)}{n(\omega^k)^{n-1}} = \frac{1}{n}\omega^k P(\omega^k).$$

Si $P \in \mathbf{R}[X]$, on peut en déduire la décomposition en éléments simples sur $\mathbf{R}[X]$: si on suppose pour simplifier n impair (de sorte que -1 n'est pas racine), on a

$$\begin{aligned}\frac{P(X)}{X^n-1} &= \sum_{k=0}^{n-1} \frac{1}{n}\frac{\omega^k P(\omega^k)}{X-\omega^k} \\ &= \frac{1}{n(X-1)} + \sum_{k=1}^{(n-1)/2} \frac{1}{n}\Big(\frac{\omega^k P(\omega^k)}{X-\omega^k} + \frac{\bar\omega^k P(\bar\omega^k)}{X-\bar\omega^k}\Big) \\ &= \frac{1}{n(X-1)} + \sum_{k=1}^{(n-1)/2} \frac{1}{n}\Big(\frac{\omega^k P(\omega^k)(X-\bar\omega^k) + \bar\omega^k P(\bar\omega^k)(X-\omega^k)}{(X-\omega^k)(X-\bar\omega^k)}\Big) \\ &= \frac{1}{n(X-1)} + \sum_{k=1}^{(n-1)/2} \frac{2}{n}\Big(\frac{\mathrm{Re}(\omega^k P(\omega^k))X - \mathrm{Re}(P(\omega^k))}{X^2 - 2(\cos\frac{2k\pi}{n})X + 1}\Big).\end{aligned}$$

10.4. Polynômes homogènes à plusieurs indéterminées. — Soit A un anneau commutatif et soit n un entier naturel. On a construit dans l'ex. 2.2 l'anneau commutatif $A[X_1, \dots, X_n]$ des polynômes à n indéterminées à coefficients dans A.

Un *monôme* est un polynôme du type $X_1^{i_1} \cdots X_n^{i_n}$, avec $i_1, \dots, i_n \in \mathbf{N}$. Son *degré* (total) est l'entier naturel $i_1 + \cdots + i_n$. Le degré (total) d'un polynôme est le plus grand des degrés des monômes qui le composent.

Un polynôme P est *homogène de degré* d s'il est combinaison linéaire à coefficients dans A de monômes de même degré d (le polynôme nul est donc homogène de tous les degrés). C'est équivalent à dire qu'on a l'égalité

$$P(YX_1, \dots, YX_n) = Y^d P(X_1, \dots, X_n)$$

dans l'anneau $A[X_1, \dots, X_n, Y]$.

Tout polynôme P non nul s'écrit de façon unique comme somme

$$P = P_0 + \cdots + P_d,$$

où d est le degré de P et P_i est un polynôme homogène de degré i.

Le produit de deux polynômes homogènes de degré respectifs d et e est un polynôme homogène de degré $d + e$. Toute somme de polynômes homogènes de *même degré* d est un polynôme homogène de degré d.

Si K est un corps, les polynômes homogènes de degré d en n variables forment un K-espace vectoriel de dimension $\binom{n+d-1}{d}$.

Remarque 10.9. — On peut très bien affecter aux indéterminées des degrés (entiers) différents, $\deg(X_i) = d_i$. Le degré du monôme $X_1^{i_1} \cdots X_n^{i_n}$ est alors $i_1 d_1 + \cdots + i_n d_n$.

Dans le cas $\deg(X_i) = i$, on appelle ce degré le *poids* du polynôme.

10.5. Polynômes symétriques à plusieurs indéterminées. — Soit A un anneau commutatif et soit n un entier naturel. On dit qu'un polynôme $P \in A[X_1, \dots, X_n]$ est *symétrique* si, pour toute permutation $\sigma \in \mathfrak{S}_n$, on a

$$P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n).$$

L'ensemble des polynômes symétriques forme une sous-A-algèbre de la A-algèbre $A[X_1, \dots, X_n]$.

Définition 10.10. — *Soit A un anneau commutatif et soient n et r des entiers strictement positifs. On appelle r-ième* polynôme symétrique élémentaire *le polynôme*

$$\Sigma_r(X_1,\dots,X_n) \coloneqq \sum_{1\leqslant i_1<\cdots<i_r\leqslant n} X_{i_1}\cdots X_{i_r}.$$

On a en particulier

$$\Sigma_1(X_1,\dots,X_n) = X_1+\cdots+X_n\,,\quad \Sigma_n(X_1,\dots,X_n) = X_1\cdots X_n\,,\quad \Sigma_r(X_1,\dots,X_n) = 0 \text{ pour } r>n.$$

La notation n'est pas entièrement satisfaisante car il y manque l'entier n, mais ça ne pose en général pas de problème en pratique : une remarque essentielle est que si on annule un certain nombre des indéterminées $X_1,\dots,X_n$ dans un polynôme Σ_r, le polynôme qu'on obtient sera encore le polynôme Σ_r en les indéterminées restantes.

Ces polynômes sont à coefficients entiers. Le polynôme Σ_r est symétrique, homogène de degré r. On peut aussi définir ces polynômes par l'identité

$$\prod_{i=1}^{n}(Y-X_i) = Y^n - \Sigma_1(X_1,\dots,X_n)Y^{n-1}+\cdots+(-1)^n\Sigma_n(X_1,\dots,X_n) \tag{3}$$

ou encore

$$\prod_{i=1}^{n}(YX_i+1) = \Sigma_n(X_1,\dots,X_n)Y^n+\cdots+\Sigma_1(X_1,\dots,X_n)Y+1$$

dans l'anneau $A[X_1,\dots,X_n,Y]$ (avec toujours $\Sigma_r=0$ pour $r>n$). On peut aussi poser $\Sigma_0=1$.

Théorème 10.11. — *Soit A un anneau commutatif et soit n un entier naturel. Pour tout polynôme symétrique $P\in A[X_1,\dots,X_n]$, il existe un unique polynôme $Q\in A[Y_1,\dots,Y_n]$ tel que*

$$P = Q(\Sigma_1,\dots,\Sigma_n).$$

De plus, on a

$$\operatorname{poids}(Q) = \deg(P).$$

Démonstration. — On va montrer l'existence de Q satisfaisant à $\operatorname{poids}(Q)\leqslant\deg(P)$, en procédant par récurrence sur le nombre n de variables, puis par une seconde récurrence sur le degré total de P. L'autre inégalité $\deg(P)\leqslant\operatorname{poids}(Q)$ est évidente, puisque les monômes composant P proviennent de la décomposition de polynômes $\Sigma_1^{i_1}\cdots\Sigma_n^{i_n}$ provenant de Q : ils sont donc de degré $\sum_k ki_k\leqslant\operatorname{poids}(Q)$.

Lorsque $n=1$, tous les polynômes sont symétriques. Comme $\Sigma_1=X_1$, le théorème est évident.

Supposons la conclusion du théorème vraie pour les polyômes en au plus $n-1$ variables. On fait une seconde récurrence sur $\deg(P)$. Si P est un polynôme constant, on prend pour Q la même constante. Soit $P\in A[X_1,\dots,X_n]$ symétrique non nul de degré total $d>0$.

Si $X_n\mid P$, on peut écrire $P=X_nP_1$ et comme P est symétrique, on a

$$P(X_1,\dots,X_n) = P(X_{\sigma(1)},\dots,X_{\sigma(n)}) = X_{\sigma(n)}P_1(X_{\sigma(1)},\dots,X_{\sigma(n)})$$

pour toute permutation $\sigma\in\mathfrak{S}_n$. On a donc $X_i\mid P$ pour tout $i\in\{1,\dots,n\}$: tous les monômes composant P sont divisibles par chacun des X_i, donc par $X_1\cdots X_n=\Sigma_n$, donc P aussi. On peut donc écrire $P=\Sigma_nP_2$, avec P_2 symétrique et $\deg(P_2)=\deg(P)-n<d$. On conclut en appliquant l'hypothèse de récurrence (sur le degré) à P_2 : on écrit $P_2=Q_2(\Sigma_1,\dots,\Sigma_n)$, avec $\operatorname{poids}(Q_2)\leqslant\deg(P_2)=d-n$, d'où $P=Q(\Sigma_1,\dots,\Sigma_n)$, avec $Q=Q_2Y_n$ et $\operatorname{poids}(Q)=\operatorname{poids}(Q_2)+n\leqslant d$.

Traitons maintenant le cas général et posons $\bar{P}(X_1,\dots,X_{n-1})\coloneqq P(X_1,\dots,X_{n-1},0)$, polynôme symétrique de $A[X_1,\dots,X_{n-1}]$. Par hypothèse de récurrence (sur le nombre n de variables), on peut donc

l'écrire

$$\bar{P} = \bar{Q}(\bar{\Sigma}_1, \dots, \bar{\Sigma}_{n-1}),$$

où $\bar{\Sigma}_1, \dots, \bar{\Sigma}_{n-1}$ sont les polynômes symétriques élémentaires en $n-1$ variables, dont on remarque que ce sont aussi les polynômes $\Sigma_1(X_1, \dots, X_{n-1}, 0), \dots, \Sigma_{n-1}(X_1, \dots, X_{n-1}, 0)$. On a aussi (par hypothèse de récurrence) $\mathrm{poids}(\bar{Q}) \leqslant \deg(\bar{P})$.

Considérons le polynôme symétrique

$$P_3 \coloneqq P - \bar{Q}(\Sigma_1, \dots, \Sigma_{n-1}) \in A[X_1, \dots, X_n].$$

Le polynôme $\bar{Q}(\Sigma_1, \dots, \Sigma_{n-1})$ est combinaison linéaire de polynômes de type $\Sigma_1^{d_1} \cdots \Sigma_{n-1}^{d_{n-1}}$ avec $d_1 + \cdots + (n-1)d_{n-1} \leqslant \mathrm{poids}(\bar{Q})$; vu comme polynôme en $X_1, \dots, X_n$, il est donc de degré au plus $\mathrm{poids}(\bar{Q}) \leqslant \deg(\bar{P}) \leqslant \deg(P)$, donc $\deg(P_3) \leqslant \deg(P)$.

Par construction, $P_3(X_1, \dots, X_{n-1}, 0) = 0$ donc, d'après le cas déjà traité, on peut l'écrire $P_3 = Q_3(\Sigma_1, \dots, \Sigma_n)$, avec $\mathrm{poids}(Q_3) \leqslant \deg(P_3)$. On a donc finalement

$$P = \bar{Q}(\Sigma_1, \dots, \Sigma_{n-1}) + Q_3(\Sigma_1, \dots, \Sigma_n),$$

avec $\mathrm{poids}(\bar{Q} + Q_3) \leqslant \max(\mathrm{poids}(\bar{Q}), \mathrm{poids}(Q_3)) \leqslant \deg(P)$. Ceci conclut la preuve de l'existence d'un Q de poids convenable.

Pour montrer l'unicité, il suffit de montrer que tout polynôme $Q \in A[Y_1, \dots, Y_n]$ non nul vérifie $Q(\Sigma_1, \dots, \Sigma_n) \neq 0$. On procède encore par récurrence sur n (le cas $n = 1$ étant trivial), puis par récurrence sur $\deg(Q)$ (le cas $\deg(Q) = 0$ étant trivial). Si $Y_n \mid Q$, on écrit $Q = Y_n Q_1$, avec Q_1 non nul de degré $\deg(Q) - 1$. Par hypothèse de récurrence, on a $Q_1(\Sigma_1, \dots, \Sigma_n) \neq 0$, donc $Q(\Sigma_1, \dots, \Sigma_n) = \Sigma_n Q_1(\Sigma_1, \dots, \Sigma_n) \neq 0$.

Supposons donc $Y_n \nmid Q$, c'est-à-dire $\bar{Q}(Y_1, \dots, Y_{n-1}) \coloneqq Q(Y_1, \dots, Y_{n-1}, 0) \neq 0$. L'hypothèse de récurrence (sur n) entraîne $\bar{Q}(\bar{\Sigma}_1, \dots, \bar{\Sigma}_{n-1}) \neq 0$. On a alors

$$Q(\Sigma_1, \dots, \Sigma_n)(X_1, \dots, X_{n-1}, 0) = Q(\bar{\Sigma}_1, \dots, \bar{\Sigma}_{n-1}, 0) = \bar{Q}(\Sigma_1, \dots, \bar{\Sigma}_{n-1}) \neq 0,$$

donc en particulier $Q(\Sigma_1, \dots, \Sigma_n) \neq 0$. □

Certaines preuves fournissent un algorithme plus efficace pour trouver le polynôme Q. L'exercice 11.53 propose une telle preuve.

Exemple 10.12. — Considérons le polynôme $P(X_1, X_2) = X_1^3 + X_2^3$. On a $\bar{P}(X_1) = P(X_1, 0) = X_1^3 = \bar{\Sigma}_1^3$. On considère alors

$$P - \Sigma_1^3 = X_1^3 + X_2^3 - (X_1 + X_2)^3 = -3X_1X_2(X_1 + X_2) = -3\Sigma_2\Sigma_1.$$

On a donc $Q(Y_1, Y_2) = Y_1^3 - 3Y_1Y_2$, qui est de poids $3 = \deg(P)$.

10.6. Sommes de Newton. — Soit A un anneau commutatif et soit n un entier naturel. Les sommes de Newton sont les polynômes symétriques

$$S_d(X_1, \dots, X_n) \coloneqq X_1^d + \cdots + X_n^d$$

pour $d > 0$ (on ne définit pas S_0). D'après le th. 10.11, ce sont des polynômes à coefficients entiers en les polynômes symétriques élémentaires. On a par exemple $S_1 = \Sigma_1$ et $S_2 = \Sigma_1^2 - 2\Sigma_2$.

Pour le théorème suivant, on rappelle que $\Sigma_r = 0$ pour $r > n$.

Théorème 10.13 **(Formules de Newton–Girard–Waring)**. — *On a, pour tout* $d \in \mathbf{N}^*$,

$$S_d - \Sigma_1 S_{d-1} + \cdots + (-1)^{d-1}\Sigma_{d-1}S_1 + (-1)^d d\Sigma_d = 0.$$

Ces relations permettent d'exprimer de proche en proche les S_d comme polynômes à coefficients entiers en $\Sigma_1, \dots, \Sigma_d$ (comme prédit par le th. 10.11). On remarque que la formule ne dépend pas du nombre n de variables. Cela peut se comprendre en remarquant que toute formule de ce type pour n variables entraîne la même formule pour $m \leqslant n$ variables en évaluant simplement en $X_{m+1} = \cdots = X_n = 0$ (en utilisera une démarche inverse dans la preuve).

Pour $d > n$, la formule se réduit à

$$S_d - \Sigma_1 S_{d-1} + \cdots + (-1)^n \Sigma_n S_{d-n} = 0.$$

tandis que pour $d = n$, on a

$$S_n - \Sigma_1 S_{n-1} + \cdots + (-1)^n n\Sigma_n = 0.$$

Démonstration. — En substituant $Y = X_i$ dans (3), on obtient

$$X_i^n - \Sigma_1 X_i^{n-1} + \cdots + (-1)^n \Sigma_n = 0.$$

Si $d \geqslant n$, on multiplie par X_i^{d-n} et on somme sur i, ce qui nous donne la formule cherchée.

Supposons maintenant $d < n$. Il s'agit de montrer que le polynôme $S_d - \Sigma_1 S_{d-1} + \cdots + (-1)^d d\Sigma_d$ est nul. Or, chaque monôme qui pourrait apparaître dans ce polynôme est de degré d ; il implique donc au plus d des variables $X_1, \dots, X_n$. On voit aussi qu'il ne change pas si on annule les autres variables. Si on écrit, en degré d, l'identité de Newton (qu'on vient de démontrer) pour ces d variables, on voit que le coefficient de ce monôme est en fait nul. □

On a par exemple

$$S_2 - \Sigma_1 S_1 + 2\Sigma_2 = 0$$

et on retrouve $S_2 = \Sigma_1^2 - 2\Sigma_2$. On a ensuite

$$S_3 - \Sigma_1 S_2 + \Sigma_2 S_1 - 3\Sigma_3 = 0,$$

d'où on déduit

$$\begin{aligned} S_3 &= \Sigma_1 S_2 - \Sigma_2 S_1 + 3\Sigma_3 \\ &= \Sigma_1(\Sigma_1^2 - 2\Sigma_2) - \Sigma_2 \Sigma_1 + 3\Sigma_3 \\ &= \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3. \end{aligned}$$

On trouvera dans l'exerc. 11.54 un moyen général d'exprimer S_n comme polynôme en $\Sigma_1, \dots, \Sigma_n$ en utilisant des déterminants.

10.7. Relations entre coefficients et racines d'un polynôme à une indéterminée. — Soit A un anneau intègre. On dit qu'un élément P de $A[X]$ est *scindé* (dans $A[X]$) si

$$P(X) = a(X - x_1) \cdots (X - x_n),$$

avec $a, x_1, \dots, x_n \in A$ (pas nécessairement distincts).

Proposition 10.14. — *Soit A un anneau intègre. Soit $P(X) = a_n X^n + \cdots + a_0$ un polynôme scindé de degré n dans $A[X]$, de racines $x_1, \dots, x_n$ (pas nécessairement distinctes). Pour tout $r \in \{1, \dots, n\}$, on a*

$$a_n \Sigma_r(x_1, \dots, x_n) = (-1)^r a_{n-r}.$$

Démonstration. — Il suffit de développer l'expression $P(X) = a_n(X - x_1) \cdots (X - x_n)$ et d'identifier les coefficients de X^r. □

Par exemple, si $n = 3$, que A est un corps et que et $a_0 a_3 \neq 0$, on a

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = \frac{x_2x_3 + x_1x_3 + x_1x_2}{x_1x_2x_3} = \frac{a_1/a_3}{-a_0/a_3} = -\frac{a_1}{a_0}$$

ainsi que

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1) = (a_1/a_3)^2 - 2(-a_2/a_3) = \frac{a_1^2 + 2a_2a_3}{a_3^2}.$$

On peut ainsi calculer ces expressions, qui sont symétriques en les racines, sans effectivement connaître celles-ci.

11. Exercices

Les étoiles signalent des questions ou exercices un peu plus difficiles.

11.1. Généralités. —

Exercice 11.1. — Montrer qu'il y a exactement (à isomorphisme près) seulement quatre anneaux (commutatifs unitaires) de cardinal 4 :
- un dont le groupe additif est $\mathbf{Z}/4\mathbf{Z}$ (c'est l'anneau $\mathbf{Z}/4\mathbf{Z}$) ;
- un dont le groupe additif est $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et qui a trois éléments inversibles (c'est le corps $\mathbf{F}_4$ à quatre éléments) ;
- un dont le groupe additif est $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et qui a deux éléments inversibles (c'est l'anneau $(\mathbf{Z}/2\mathbf{Z})[X]/(X^2)$) ;
- un dont le groupe additif est $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et qui n'a qu'un élément inversible (c'est l'anneau $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$).

Exercice 11.2. — Soit A un anneau commutatif.

(1) Soit I un idéal de A. Relier les idéaux de l'anneau A/I à ceux de A. Même question pour les idéaux premiers et maximaux.

(2) Soit $f\colon A \to B$ un morphisme d'anneaux. Montrer que l'image réciproque par f d'un idéal premier est un idéal premier. Que se passe-t-il pour les idéaux maximaux ?

(3) Soient $I \subseteq J$ des idéaux de A. Montrer que l'anneau A/J est canoniquement isomorphe au quotient de l'anneau A/I par l'idéal J/I.

(4) Soient I et J des idéaux de A. Montrer que IJ est inclus dans $I \cap J$. A-t-on toujours égalité ?

(5) Soient m et n des entiers naturels et soient $I = m\mathbf{Z}$ et $J = n\mathbf{Z}$ les idéaux qu'ils engendrent dans l'anneau $\mathbf{Z}$. Déterminer les idéaux IJ, $I \cap J$ et $I + J$.

Exercice 11.3 **(Généralisation du théorème chinois des restes (th. 6.8))**. — Soit A un anneau commutatif et soient $I_1, \dots, I_r$ des idéaux de A, avec $r \geqslant 2$, qui vérifient $I_i + I_j = A$ pour tout $1 \leqslant i < j \leqslant r$.

(1) Montrer l'égalité $I_1 + I_2 \cdots I_r = A$.

(2) Montrer l'égalité $I_1 \cdots I_r = I_1 \cap \cdots \cap I_r$.

(3) Montrer qu'on a un isomorphisme d'anneaux

$$A/(I_1 \cap \cdots \cap I_r) \xrightarrow{\sim} A/I_1 \times \cdots \times A/I_r.$$

Exercice 11.4. — Montrer qu'un anneau intègre fini est un corps.

Exercice 11.5. — Soit A un anneau commutatif.

(1) Soit n un entier naturel. Établir la formule

$$\forall a, b \in A \qquad (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

dite du « binôme de Newton ».

(2) On dit qu'un élément a de A est *nilpotent* s'il existe un entier naturel n tel que $a^n = 0_A$. Montrer que l'ensemble des éléments nilpotents de A est un idéal de A.

(3) Quels sont les éléments nilpotents de l'anneau $\mathbf{Z}/1000\mathbf{Z}$?

Exercice 11.6. — Montrer qu'un nombre réel est rationnel si et seulement si son développement décimal est périodique à partir d'un certain rang.

Inversement, si $x = p/q = p'/(10^a q') > 0$ avec $10 \wedge q' = 1$, on a $10^a x = b + p''/q'$ avec $b \in \mathbf{N}$ et $0 \leqslant p'' < q'$. Comme $10 \wedge q' = 1$, 10 est une unité dans $\mathbf{Z}/q'\mathbf{Z}$ et il existe $n > 0$ tel que $10^n = 1$ dans $\mathbf{Z}/q'\mathbf{Z}$. On peut écrire $10^n - 1 = q'q''$ et $p''/q' = \frac{p''q''}{10^n-1}$ est < 1 donc s'écrit $\frac{c}{10^n-1}$ avec $0 \leqslant c < 10^n$.

Exercice 11.7 **(MG2023)**. — Soit q un entier naturel non nul. On considère le groupe $G = (\mathbf{Z}/4q\mathbf{Z})^\times$ des éléments inversibles de l'anneau $\mathbf{Z}/4q\mathbf{Z}$.

(1) Déterminer les ordres respectifs dans G des classes modulo $4q$ de $2q - 1$ et $2q + 1$.

(2) Le groupe G est-il cyclique ?

Exercice 11.8 **(MG2023)**. — (1) Déterminer l'ensemble des couples (x, y) dans $(\mathbf{Z}/3\mathbf{Z})^2$ tels que $x^2 + y^2 = 0$.

(2) Déterminer l'ensemble des couples (x, y) dans $\mathbf{Z}^2$ tels que $x^2 - 5y^2 = 33$.

(2) Déterminer l'ensemble des couples (x, y) dans $\mathbf{Q}^2$ tels que $x^2 - 5y^2 = 33$.

11.2. Anneaux principaux et euclidiens. —

Exercice 11.9 **(Entiers de Gauss)**. — Le but de cet exercice est de montrer que

$$\mathbf{Z}[i] \coloneqq \{a + ib \mid a, b \in \mathbf{Z}\}$$

est un anneau enclidien (donc principal) [6].

(1) Vérifier que $\mathbf{Z}[i]$ est un anneau intègre.

(2) On définit une fonction $\varphi \coloneqq \mathbf{Z}[i] \smallsetminus \{0\} \to \mathbf{N}$ en posant $\varphi(a + ib) = a^2 + b^2$. Montrer que φ est un stathme euclidien (*Indication :* si $x, y \in \mathbf{Z}[i]$, avec $y \neq 0$, on pourra considérer le complexe $z \coloneqq x/y \in \mathbf{C}$ et l'élément $a + ib$ de $\mathbf{Z}[i]$, où a est l'entier le plus proche de la partie réelle de z et b l'entier le plus proche de sa partie imaginaire).

Exercice 11.10 **(Suite de Fibonacci)**. — Soit $(F_n)_{n\in\mathbf{N}}$ la suite d'entiers définie par les relations

$$F_0 = 0\,, \quad F_1 = 1\,, \quad \forall n \in \mathbf{N} \quad F_{n+2} = F_{n+1} + F_n.$$

(1) Calculer $F_0, \ldots, F_{10}$.

(2) On pose $A \coloneqq \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Montrer que pour tout $n \geqslant 1$, on a

$$A^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix}.$$

En déduire que pour tout $n \in \mathbf{N}$, les entiers F_n et F_{n+1} sont premiers entre eux.

(3) Montrer que pour tout $m, n \in \mathbf{N}$, on a

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_m F_n.$$

En déduire

$$F_m \wedge F_n = F_{m\wedge n}.$$

6. On peut le définir comme $\mathbf{Z}^2$ muni de l'addition terme à terme et de la multiplication $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

Exercice 11.11. — Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également et de donner le reste au cuisinier. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?

Exercice 11.12. — Soit A un anneau commutatif qui n'est pas un corps. Montrer que l'anneau $A[X]$ n'est pas principal.

Exercice 11.13. — Soient m et n des entiers naturels et soit q un entier strictement positif. Montrer l'égalité $(q^m-1)\wedge(q^n-1)=q^{m\wedge n}-1$.

***Exercice 11.14* (Nombres de Mersenne)**. — (1) Soient m et n des entiers avec $m,n\geqslant 2$, tels que m^n-1 est premier. Montrer que $m=2$ et que n est premier [7].

(2) Soit p un entier premier et soit q un diviseur premier de 2^p-1. Montrer que p divise $q-1$.

***Exercice 11.15* (Nombres de Fermat)**. — (1) Soit n un entier strictement positif tel que 2^n+1 est un nombre premier. Montrer que n est une puissance de 2. On pose $F_m \coloneqq 2^{2^m}+1$.

(2) Soient m et n des entiers strictement positifs distincts. Montrer que F_m et F_n sont premiers entre eux [8].

Exercice 11.16. — Soit n un entier strictement positif. Si φ est l'indicatrice d'Euler, montrer la relation

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

11.3. Anneaux factoriels. —

Exercice 11.17. — On considère l'anneau

$$\mathbf{Z}[\sqrt{-5}]\coloneqq\{a+b\sqrt{-5}\mid a,b\in\mathbf{Z}\}.$$

Si $x=a+b\sqrt{-5}$, on note $\bar{x}=a-b\sqrt{-5}$.

(1) Montrer que les unités de l'anneau $\mathbf{Z}[\sqrt{-5}]$ sont ±1 (*Indication :* si x est une unité, d'inverse y, on pourra calculer $x\bar{x}y\bar{y}$).

(2) Montrer que 3 est irréductible dans l'anneau $\mathbf{Z}[\sqrt{-5}]$.

(3) Montrer que l'idéal (3) n'est pas premier et que l'anneau $\mathbf{Z}[\sqrt{-5}]$ n'est pas factoriel (*Indication :* on pourra considérer l'égalité $(1+\sqrt{-5})(1-\sqrt{-5})=2\cdot 3$).

(4) On considère maintenant l'anneau

$$\mathbf{Z}[\sqrt{5}]\coloneqq\{a+b\sqrt{5}\mid a,b\in\mathbf{Z}\}.$$

Montrer que $2+\sqrt{5}$ en est une unité et que le groupe des unités de l'anneau $\mathbf{Z}[\sqrt{5}]$ est infini.

(5) Montrer que l'anneau $\mathbf{Z}[\sqrt{5}]$ n'est pas factoriel.

---

7. Les nombres de Mersenne sont les entiers de la forme 2^n-1. Si ce nombre est premier, n est donc premier. La réciproque est fausse car $2^{11}-1=23\cdot 89$. Seuls 51 nombres de Mersenne premiers sont connus, le plus grand étant $2^{282\,589\,933}-1$. On ne sait pas s'il en existe une infinité.

8. On sait que $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$ et $F_4=65537$ sont premiers (on n'en connaît aucun autre !) mais que 641 divise F_5 (Euler). On sait aussi que $F_6,\dots,F_{32}$, $F_{2543548}$ et $F_{2747497}$ ne sont pas premiers.

Exercice 11.18. — (1) Soit A un anneau factoriel de corps des fractions K_A. Soit $x \in K_A$ tel que $P(x) = 0$, où $P \in A[X]$ est unitaire. Montrer que $x \in A$ (on dit que A est *intégralement clos*).

(2) En déduire que l'anneau $\mathbf{Z}[\sqrt{5}]$ n'est pas factoriel (*Indication :* on pourra considérer le polynôme $X^2 + X - 1$). Généraliser aux anneaux $\mathbf{Z}[\sqrt{d}]$ avec $d \in \mathbf{Z}$ non carré parfait et $d \equiv 1 \pmod 4$.

***Exercice 11.19* (Bézout)**. — * Soit K un corps et soient P et Q des éléments de $K[X, Y]$ sans facteur irréductible commun.

(1) Montrer qu'il existe $A, B \in K[X, Y]$ et $D \in K[X]$ non nul tels que $D = AP + BQ$ (*Indication :* on pourra travailler dans l'anneau principal $K(X)[Y]$).

(2) En déduire que l'ensemble

$$\{(x, y) \in K^2 \mid (P(x, y) = Q(x, y) = 0\}$$

est fini.

(3) Montrer que le K-espace vectoriel $K[X, Y]/(P, Q)$ est de dimension finie.

11.4. Polynômes. —

Exercice 11.20. — Si le polynôme $a_n X^n + \cdots + a_1 X + a_0 \in \mathbf{Z}[X]$, avec $a_n \neq 0$, a une racine rationnelle, que l'on écrit sous forme de fraction réduite a/b, alors $a \mid a_0$ et $b \mid a_n$.

Exercice 11.21. — Montrer que le polynôme $X^{163} + 24X^{57} - 6$ a exactement une racine réelle. Est-elle rationnelle ? Montrer que ce polynôme est en fait irréductible dans $\mathbf{Q}[X]$.

Exercice 11.22. — Soit K un corps. Montrer qu'il y a un infinité de polynômes irréductibles dans $K[X]$ (*Indication :* on pourra copier la preuve qu'il existe une infinité de nombres premiers).

Exercice 11.23. — Factoriser le polynôme $X^4 + 4$ en produit de facteurs irréductibles dans $(\mathbf{Z}/5\mathbf{Z})[X]$.

Exercice 11.24. — Montrer que le polynôme $X^4 + 1$ est irréductible dans $\mathbf{Q}[X]$.

Exercice 11.25. — Soit a un entier non nul. Montrer que le polynôme $X^4 + aX - 1$ est irréductible dans $\mathbf{Q}[X]$.

Exercice 11.26. — Factoriser le polynôme $X^6 + 1$ en produit de facteurs irréductibles dans $\mathbf{C}[X]$, dans $\mathbf{R}[X]$, puis dans $\mathbf{Q}[X]$.

Exercice 11.27. — Trouver toutes les racines complexes du polynôme $2X^3 - X^2 + 5X + 3$.

Exercice 11.28. — Soient $p, q \in \mathbf{R}$. Montrer que le polynôme $X^n + pX + q$ a au plus 3 racines réelles.

Exercice 11.29. — Soit $a_n X^n + \cdots + a_{k+1} X^{k+1} + a_{k-1} X^{k-1} + \cdots + a_0$ un polynôme à coefficients réels avec $0 < k < n$ et $a_{k+1} a_{k-1} > 0$. Montrer que ses n racines ne sont pas toutes réelles.

Exercice 11.30. — Soit $P \in \mathbf{R}[X]$ tel que $P(x) \geqslant 0$ pour tout $x \in \mathbf{R}$. Montrer qu'il existe des polynômes Q et R dans $\mathbf{R}[X]$ tels que $P = Q^2 + R^2$.

Exercice 11.31. — Soit $\theta \in \mathbf{R}$. Déterminer le reste de la division euclidienne du polynôme $((\sin\theta)X + \cos\theta)^n$ par le polynôme $X^2 + 1$.

Exercice 11.32. — Factoriser le polynôme $X^n - 1$ en produit de facteurs irréductibles dans $\mathbf{C}[X]$ puis dans $\mathbf{R}[X]$.

Exercice 11.33. — Soient m et n des entiers positifs.

(1) Calculer les pgcd des polynômes $X^m - 1$ et $X^n - 1$.

(2) Calculer le pgcd des polynômes $X^{m-1} + \cdots + X + 1$ et $X^{n-1} + \cdots + X + 1$.

Exercice 11.34. — Soit q un entier strictement positif. Pour tout $m \in \mathbf{N}$, on pose $P_m(X) = X^{q^m} - X$. Montrer $P_m \wedge P_n = P_{m \wedge n}$.

Exercice 11.35. — (1) Déterminer tous les polynômes irréductibles de degré 2 dans $(\mathbf{Z}/2\mathbf{Z})[X]$.

(2) Déterminer tous les polynômes irréductibles de degré 3 dans $(\mathbf{Z}/2\mathbf{Z})[X]$.

(3) Déterminer tous les polynômes irréductibles de degré 4 dans $(\mathbf{Z}/2\mathbf{Z})[X]$.

(4) Montrer que le polynôme $X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$, où a_3 et a_2 sont des entiers pairs et a_1 et a_0 des entiers impairs, est irréductible dans $\mathbf{Q}[X]$.

Exercice 11.36. — Soit p un nombre premier.

(1) Montrer que le polynôme $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ est irréductible dans $\mathbf{Q}[X]$ (*Indication :* on pourra appliquer le critère d'Eisenstein (th. I.9.6) au polynôme $\Phi_p(X + 1)$).

(2) Soit r un entier positif. Montrer plus généralement que le polynôme

$$\Phi_{p^{r+1}}(X) \coloneqq \Phi_p(X^{p^r}) = X^{p^r(p-1)} + X^{p^r(p-2)} + \cdots + X^{p^r} + 1$$

(voir ex. II.2.20) est irréductible dans $\mathbf{Q}[X]$ (*Indication :* on pourra appliquer le critère d'Eisenstein au polynôme $\Phi_{p^{r+1}}(X + 1)$).

Exercice 11.37. — Montrer que le polynôme $X^6 + Y^2X^5 + Y$ est irréductible dans $\mathbf{C}[X, Y]$.

Exercice 11.38 **(Ram Murty)**. — Soit $P(X) = a_nX^n + \cdots + a_0$ un polynôme de degré $n \geqslant 1$ à coefficients entiers. On pose

$$M \coloneqq \frac{1}{|a_n|} \max\{|a_{n-1}|, \ldots, |a_0|\}.$$

(1) Soit x une racine complexe de P. Montrer l'inégalité $|x| < M + 1$.

(2) On suppose qu'il existe un nombre entier $m \geqslant M + 2$ tel que $P(m)$ soit un nombre premier. Montrer que le polynôme P est irréductible dans $\mathbf{Q}[X]$.

(3) Montrer que le polynôme $P(X) = X^4 + 6X^2 + 1$ est irréductible dans $\mathbf{Q}[X]$ (*Indication :* on pourra calculer $P(8)$).

(4) Montrer que le polynôme $P(X) = 4X^4 + 7X^3 + 7X^2 + 1$ est irréductible dans $\mathbf{Q}[X]$ (*Indication :* on pourra calculer $P(10)$).

Exercice 11.39. — (1) Soit r un entier positif. Montrer que le polynôme

$$P_r(X) \coloneqq \binom{X}{r} \coloneqq \frac{X(X-1)\cdots(X-r+1)}{r!} \in \mathbf{Q}[X]$$

prend des valeurs entières sur tous les entiers.

* (2) Soit $P \in \mathbf{Q}[X]$ un polynôme qui prend des valeurs entières sur tous les entiers assez grands. Montrer que P est combinaison linéaire *à coefficients entiers* des polynômes $P_0, P_1, \ldots$ (*Indication :* on pourra procéder par récurrence sur le degré de P et considérer le polynôme $P(X + 1) - P(X)$).

Exercice 11.40. — Soit A un anneau intègre. Montrer qu'un polynôme $P \in A[X]$ *non constant* est de dérivée nulle si et seulement s'il existe un nombre premier p tel que $p \cdot 1_A = 0_A$ (on dit que l'anneau A est de caractéristique p ; *cf.* § II.1.1) et un polynôme $Q \in A[X]$ tels que $P(X) = Q(X^p)$.

Exercice 11.41. — Soit $P \in \mathbf{C}[X]$. Exprimer $P \wedge P'$ en fonction des racines de P et de leur multiplicité.

Exercice 11.42. — Décomposer en éléments simples la fraction rationnelle $\frac{1}{X(X-1)(X^3-2)}$ dans $\mathbf{C}(X)$, dans $\mathbf{R}(X)$, puis dans $\mathbf{Q}(X)$.

Exercice 11.43. — Décomposer en éléments simples la fraction rationnelle $\frac{1}{X^2+1}$ et en déduire sa dérivée $n$ième pour tout entier $n > 0$.

Exercice 11.44. — * (1) Soit A un anneau intègre et soient $F, G \in A[X_1, \ldots, X_n]$ des polynômes premiers entre eux, homogènes de degrés respectifs d et $d+1$. Montrer que le polynôme $F+G$ est irréductible dans $A[X_1, \ldots, X_n]$.

(2) À quelle condition nécessaire et suffisante sur les entiers naturels m et n le polynôme $X^m - Y^n$ est-il irréductible dans $\mathbf{C}[X, Y]$? (*Indication :* on pourra attribuer à X et à Y des degrés bien choisis pour pouvoir appliquer (1) ; *cf.* rem. 10.9.)

Exercice 11.45. — Soit A un anneau intègre et soit $F \in A(X_1, \ldots, X_n)$ une fraction rationnelle symétrique. Montrer qu'il existe des polynômes symétriques $P, Q \in A[X_1, \ldots, X_n]$ tels que $F = P/Q$.

Exercice 11.46. — Exprimer à l'aide des polynômes symétriques élémentaires, lorsque cela est possible, les expressions suivantes :

- $X_1X_2 + X_2X_3 + X_3X_4 + X_4X_1$;
- $\sum_{i,j=1}^{n} X_i^3 X_j$;
- $\sum_{i=1}^{n} \frac{1}{X_i}$.

Exercice 11.47. — Soit p un nombre premier impair.

(1) Montrer que

$$\prod_{x \in \mathbf{Z}/p\mathbf{Z},\ 1 \leqslant x \leqslant p-1} x = -1.$$

(2) En déduire

$$\prod_{x \in \mathbf{Z}/p\mathbf{Z},\ 1 \leqslant x \leqslant \frac{p-1}{2}} x^2 = (-1)^{\frac{p+1}{2}}$$

puis que, si $p \equiv 1 \pmod 4$, alors -1 est un carré (explicite) modulo p.

Exercice 11.48. — Soit p un nombre premier impair.

(1) Montrer que si x est un carré non nul dans $\mathbf{Z}/p\mathbf{Z}$, il vérifie $x^{\frac{p-1}{2}} = 1$.

(2) En déduire que si $x \in \mathbf{Z}/p\mathbf{Z}^\times$, on a

$$x \text{ est un carré } \iff x^{\frac{p-1}{2}} = 1$$

et

$$x \text{ n'est pas un carré } \iff x^{\frac{p-1}{2}} = -1.$$

En déduire que -1 est un carré modulo p si et seulement si $p \equiv 1 \pmod 4$.

(3) On suppose maintenant $p \equiv 1 \pmod 4$ et soit x un entier tel que $x^2 + 1$ soit divisible par p. Soit $\mathbf{Z}[i]$ l'anneau des entiers de Gauss ; on admettra le résultat montré dans l'exerc. 11.9 que cet anneau est principal. Montrer que p n'est pas irréductible dans $\mathbf{Z}[i]$ (*Indication :* on pourra remarquer que $p \mid (x+i)(x-i)$) et qu'il se décompose en $p = (a+ib)(a-ib)$, avec $a, b \in \mathbf{Z}$. Cela montre que p est somme de deux carrés [9].

(4) Montrer que si des entiers sont sommes de deux carrés, il en est de même de leur produit. En déduire qu'un entier positif tel que tous les nombres premiers p qui apparaissent dans sa décomposition en produit d'irréductibles avec une puissance impaire vérifient $p \equiv 1 \pmod 4$ sont somme de deux carrés.

9. Cette preuve n'est pas constructive : elle ne dit pas comment trouver explicitement les entiers a et b tels que $p = a^2 + b^2$. L'algorithme d'Euclide donne un tel moyen : l'entier x tel que $p \mid x^2 + 1$ est premier avec p et on peut le choisir $< p/2$; on exécute l'algorithme d'Euclide pour trouver le pgcd de p et de x (qui est bien sûr 1) et on peut prendre pour a et b les deux premiers restes qui sont $< \sqrt{p}$. Si par exemple $p = 73$, on peut prendre $x = 27$, puis $73 = 2 \times 27 + 19$, $27 = 1 \times 19 + 8$, $19 = 2 \times 8 + 3$ et on a bien $73 = 8^2 + 3^2$. La preuve que cet algorithme fonctionne, bien qu'élémentaire, n'est pas triviale (Wagon, S., Editor's Corner : The Euclidean Algorithm Strikes Again, *The American Mathematical Monthly* **97** (1990), 125–129).

(5) Montrer qu'un entier $n \equiv 3 \pmod 4$ n'est pas somme de deux carrés.

Exercice 11.49. — Résoudre le système

$$\begin{cases} x & + & y & + & z & = & 1, \\ x^2 & + & y^2 & + & z^2 & = & 21, \\ 1/x & + & 1/y & + & 1/z & = & 1. \end{cases}$$

Exercice 11.50. — Soit P un polynôme scindé qui n'a que des racines simples x_j. Calculer $\sum_j \frac{1}{P'(x_j)}$.

Exercice 11.51. — Trouver un polynôme unitaire dont les racines sont les carrés de celles du polynôme $X^3 + aX^2 + bX + c$.

Exercice 11.52. — Soient p et q des nombres complexes et soient x_1, x_2 et x_3 les racines du polynôme $X^3 + pX + q$. Trouver un polynôme unitaire dont les racines sont $x_1^2 + x_2^2$, $x_2^2 + x_3^2$ et $x_3^2 + x_1^2$.

Exercice 11.53. — Soient $\mathbf{i}, \mathbf{j} \in \mathbf{N}^n$. Nous dirons que $\mathbf{i} = (i_1, \dots, i_n)$ est *plus petit* que $\mathbf{j} = (j_1, \dots, j_n)$ si

- soit $\sum_{k=1}^n i_k < \sum_{k=1}^n j_k$,
- soit $\sum_{k=1}^n i_k = \sum_{k=1}^n j_k$ et il existe $k \in \{1, \dots, n\}$ tel que $i_1 = j_1, \dots, i_{k-1} = j_{k-1}$ et $i_k < j_k$.

(1) Montrer que si $\mathbf{i}, \mathbf{j} \in \mathbf{N}^n$ sont distincts, alors soit $\mathbf{i}$ est plus petit que $\mathbf{j}$, soit $\mathbf{j}$ est plus petit que $\mathbf{i}$.

(2) On se donne $\mathbf{i} \in \mathbf{N}^n$. Montrer que l'ensemble des $\mathbf{j} \in \mathbf{N}^n$ qui sont plus petits que $\mathbf{i}$ est fini.

Soit A un anneau commutatif. Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique non nul et soit $\mathbf{i} =: \mathrm{ht}(P)$ le plus grand (au sens de la définition précédente) élément de $\mathbf{N}^n$ tel que le coefficient de $X_1^{i_1} \cdots X_n^{i_n}$ dans P soit non nul ; on note ce coefficient $\mathrm{dom}(P)$.

(3) Montrer $i_1 \geq \cdots \geq i_n$.

(4) On pose

$$d_1 = i_1 - i_2,\ d_2 = i_2 - i_3, \dots, d_{n-1} = i_{n-1} - i_n,\ d_n = i_n.$$

Montrer que

- soit $P = \mathrm{dom}(P)\Sigma_1^{d_1} \cdots \Sigma_n^{d_n}$;
- soit $\mathrm{ht}(P - \mathrm{dom}(P)\Sigma_1^{d_1} \cdots \Sigma_n^{d_n})$ est plus petit que $\mathrm{ht}(P)$.

(5) En déduire le th. 10.11.

Exercice 11.54. — On garde les notations du § 10.6. Montrer les relations

$$S_n = \begin{vmatrix} \Sigma_1 & 1 & 0 & 0 & \cdots & 0 \\ 2\Sigma_2 & \Sigma_1 & 1 & 0 & \cdots & 0 \\ 3\Sigma_3 & \Sigma_2 & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ (n-1)\Sigma_{n-1} & \Sigma_{n-2} & \cdots & \Sigma_2 & \Sigma_1 & 1 \\ n\Sigma_n & \Sigma_{n-1} & \Sigma_{n-2} & \cdots & \Sigma_2 & \Sigma_1 \end{vmatrix}$$

et

$$n!\Sigma_n = \begin{vmatrix} S_1 & 1 & 0 & 0 & \cdots & 0 \\ S_2 & S_1 & 2 & 0 & \cdots & 0 \\ S_3 & S_2 & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ S_{n-1} & S_{n-2} & \cdots & S_2 & S_1 & n-1 \\ S_n & S_{n-1} & S_{n-2} & \cdots & S_2 & S_1 \end{vmatrix}.$$

CHAPITRE II

CORPS

1. Généralités

On rappelle qu'un corps est un anneau K commutatif non nul (c'est-à-dire que $1_K \neq 0_K$) dans lequel tout élément non nul est inversible. Ses seuls idéaux sont donc $\{0_K\}$ et K, et tout morphisme d'anneaux d'origine K vers un anneau (unitaire) non nul est injectif.

Si K et L sont des corps, un *morphisme (de corps)* de K vers L est un morphisme d'anneaux (unitaires) de K vers L ; il est nécessairement injectif et l'on dit que L est une *extension* de K. On identifiera souvent une extension $K \hookrightarrow L$ avec une inclusion $K \subseteq L$.

1.1. Caractéristique d'un corps. — Soit K un corps. Il existe un plus petit sous-corps de K, appelé *sous-corps premier* de K : c'est le sous-corps engendré par 1_K. Il est isomorphe soit à $\mathbf{Q}$, auquel cas on dit que K est de caractéristique 0, soit à un corps de la forme $\mathbf{Z}/p\mathbf{Z}$ (que l'on note le plus souvent $\mathbf{F}_p$) ; l'entier p est alors premier et l'on dit que K est de caractéristique p. Dans ce dernier cas, on a $p \cdot 1_K = 0_K$ et la formule magique [1]

$$\forall x, y \in K \qquad (x+y)^p = x^p + y^p. \tag{4}$$

Autrement dit, l'application de Frobenius

$$\begin{array}{rccc} \mathrm{Fr}_K \colon & K & \longrightarrow & K \\ & x & \longmapsto & x^p \end{array}$$

est un morphisme de corps (injectif, car $x^p = 0$ entraîne $x = 0$, mais pas nécessairement surjectif). On note en général K^p son image. Si $K = \mathbf{F}_p$, le morphisme de Frobenius est l'identité et $K^p = K$. Plus généralement, si K est un corps fini, on a $K^p = K$ (puisque Fr_K est une application injective entre ensembles de même cardinal, donc surjective). En revanche, si K est le corps $\mathbf{F}_p(X)$ (infini de caractéristique p), on a $K^p = \mathbf{F}_p(X^p) \subsetneq K$.

2. Extensions de corps

Soit $K \subseteq L$ une extension de corps. Son *degré* est la dimension du K-espace vectoriel L, notée $[L : K]$. L'extension est dite *finie* si ce degré l'est, *infinie* sinon.

1. On peut l'obtenir en remarquant que la dérivée du polynôme $(X+y)^p \in K[X]$ est nulle, de sorte que le coefficient de X^i, pour chaque $0 < i < p$, est nul (puisque la dérivée de X^i ne l'est pas). Il ne reste donc que le terme de degré p, qui est X^p, et le terme de degré 0, qui est y^p. On a donc montré $(X+y)^p = X^p + y^p$.

Exemple 2.1. — On a $[\mathbf{C} : \mathbf{R}] = 2$, $[K(X) : K] = \infty$ et $[\mathbf{C} : \mathbf{Q}] = \infty$ (*cf.* ex. 2.8) [(2)].

Théorème 2.2. — *Soient $K \subseteq L$ et $L \subseteq M$ des extensions de corps. On a*

$$[M : K] = [M : L][L : K]. \tag{5}$$

En particulier, l'extension $K \subseteq M$ est finie si et seulement si les extensions $K \subseteq L$ et $L \subseteq M$ le sont.

Démonstration. — Soit $(l_i)_{i\in I}$ une base du K-espace vectoriel L et soit $(m_j)_{j\in J}$ une base du L-espace vectoriel M. Nous allons montrer que la famille $(l_i m_j)_{(i,j)\in I\times J}$ est une base du K-espace vectoriel M.

Cette famille est libre. Supposons que l'on ait une relation $\sum_{(i,j)\in I\times J} k_{i,j} l_i m_j = 0$, avec des $k_{i,j} \in K$ presque tous nuls. On a

$$0 = \sum_{(i,j)\in I\times J} k_{i,j} l_i m_j = \sum_{j\in J} \Big(\sum_{i\in I} k_{i,j} l_i \Big) m_j.$$

Comme la famille $(m_j)_{j\in J}$ est libre, on en déduit que pour chaque $j \in J$, on a

$$\sum_{i\in I} k_{i,j} l_i = 0.$$

Comme la famille $(l_i)_{i\in I}$ est libre, on en déduit que pour chaque $i \in I$ et chaque $j \in J$, on a $k_{i,j} = 0$.

Cette famille est génératrice. Soit y un élément de M. Comme la famille $(m_j)_{j\in J}$ est génératrice, il existe des $x_j \in L$ presque tous nuls tels que $y = \sum_{j\in J} x_j m_j$. Comme la famille $(l_i)_{i\in I}$ est génératrice, il existe pour chaque $j \in J$ des $k_{i,j} \in K$ presque tous nuls tels que $x_j = \sum_{i\in I} k_{i,j} l_i$. On a donc $y = \sum_{j\in J} \sum_{i\in I} k_{i,j} l_i$.

On en déduit

$$[M : K] = \mathrm{Card}(I \times J) = \mathrm{Card}(I)\,\mathrm{Card}(J) = [M : L][L : K],$$

ce qui termine la démonstration du théorème. □

Remarque 2.3. — L'existence de bases pour un espace vectoriel n'est au programme de l'agrégation que pour les espaces vectoriels de dimension finie. Pour le théorème, il est donc sage de se restreindre, dans le cadre d'une leçon, au cas où les extensions $K \subseteq L$ et $L \subseteq M$ sont finies. On montre alors par la preuve ci-dessus que l'extension $K \subseteq M$ est finie et l'égalité (5). Inversement, si l'extension $K \subseteq M$ est finie, l'extension $K \subseteq L$ l'est aussi (puisque L est alors un sous-K-espace vectoriel du K-espace vectoriel de dimension finie M), ainsi que l'extension $L \subseteq M$, puisque toute partie génératrice finie du K-espace vectoriel M est encore génératrice de M comme L-espace vectoriel.

2.1. Éléments algébriques et transcendants. —

Définition 2.4. — *Soit $K \subseteq L$ une extension de corps et soit x un élément de L. On dit que x est* algébrique sur K *s'il existe un polynôme non nul $P \in K[X]$ tel que $P(x) = 0$. Dans le cas contraire, on dit que x est* transcendant sur K.

L'extension $K \subseteq L$ est dite algébrique *si tous les éléments de L sont algébriques sur K.*

Exemple 2.5. — Le corps $\mathbf{C}$ est une extension algébrique de $\mathbf{R}$. Le réel $\sqrt{2}$ est algébrique sur $\mathbf{Q}$. L'ensemble des nombres réels algébriques sur $\mathbf{Q}$ est dénombrable (pourquoi ?) : il existe donc des nombres réels transcendants sur $\mathbf{Q}$ (on dit souvent simplement « transcendants »). Le nombre réel $\sum_{n\geqslant 0} 10^{-n!}$ est transcendant (Liouville, 1844 ; *cf.* exerc. 5.18), ainsi que π (Lindemann, 1882). L'extension $\mathbf{Q} \subseteq \mathbf{R}$ n'est donc pas algébrique.

2. On ne se préoccupera pas ici des différentes « sortes » d'infini dans ce cours ; mais ce degré devrait bien sûr être considéré comme un cardinal.

Soit $K \subseteq L$ une extension de corps et soit S une partie de L. L'intersection de tous les sous-anneaux de L contenant K et S est un sous-anneau de L que l'on notera $K[S]$, appelé *sous-K-algèbre de L engendrée par S*. Ses éléments sont tous les éléments de L de la forme $P(s_1, \ldots, s_n)$, où $n \in \mathbf{N}$, $P \in K[X_1, \ldots, X_n]$ est un polynôme à coefficients dans K, et $s_1, \ldots, s_n \in S$. De même, l'intersection des sous-corps de L contenant K et S est un sous-corps de L, noté $K(S)$; c'est le corps des fractions de $K[S]$.

Si $x \in L$, la sous-K-algèbre $K[x]$ de L engendrée par x est donc l'image du morphisme d'anneaux K-linéaire

$$\begin{array}{rccc} \varphi_x : & K[X] & \longrightarrow & L \\ & P & \longmapsto & P(x). \end{array}$$

Le théorème suivant est fondamental.

Théorème 2.6. — *Soit $K \subseteq L$ une extension de corps et soit x un élément de L.*

(a) *Si x est transcendant sur K, le morphisme φ_x est injectif, le K-espace vectoriel $K[x]$ est de dimension infinie et l'extension $K \subseteq K(x)$ est infinie.*

(b) *Si x est algébrique sur K, il existe un polynôme unitaire $P \in K[X]$ de degré minimal vérifiant $P(x) = 0$. Ce polynôme est irréductible et c'est l'unique polynôme unitaire, irréductible dans $K[X]$, dont x est racine dans L. On appelle P le* polynôme minimal *de x sur K. On a $K[x] = K(x)$ et cette extension de K est finie de degré $\deg(P)$. La famille $(1, x, \ldots, x^{\deg(P)-1})$ forme une base du K-espace vectoriel $K[x]$.*

Démonstration. — La transcendance de x est équivalente par définition à l'injectivité de φ_x. Si φ_x est injectif, le sous-anneau $K[x]$ de L engendré par x est isomorphe à $K[X]$ donc c'est un K-espace vectoriel de dimension infinie. De même, le sous-corps $K(x)$ de L engendré par x est isomorphe à l'anneau des fractions rationnelles $K(X)$ (corps des fractions de $K[X]$) donc c'est un K-espace vectoriel de dimension infinie. Ceci montre (a).

Si x est algébrique sur K, le noyau de φ_x est un idéal non nul de $K[X]$, qui est donc principal (§ I.6), engendré par un polynôme non nul de degré minimal P qui annule x (c'est-à-dire $P(x) = 0$). Il est unique si on le prend unitaire. L'anneau $K[x]$ est alors isomorphe à l'anneau quotient $K[X]/(P)$ (§ I.4). Or l'anneau $K[x]$ est intègre car c'est un sous-anneau de L ; il s'ensuit que l'idéal (P) est premier, donc P est un polynôme irréductible. De plus, l'anneau $K[X]/(P)$ est un corps (prop. I.6.1) et il en est de même pour $K[x]$, donc $K[x] = K(x)$. On termine la preuve en montrant que la famille $(1, x, \ldots, x^{\deg(P)-1})$ forme une base du K-espace vectoriel $K[x]$.

C'est une famille libre : toute combinaison linéaire nulle non triviale de $1, x, \ldots, x^{\deg(P)-1}$ fournirait un polynôme annulateur de degré $< \deg(P)$, ce qui contredit le choix de P.

C'est une famille génératrice : si $y = Q(x) \in K[x]$, on fait la division euclidienne $Q = PS + R$ de Q par P, avec $\deg(R) < \deg(P)$. Comme $P(x) = 0$, on a $y = Q(x) = R(x)$, qui est bien combinaison linéaire de $1, x, \ldots, x^{\deg(P)-1}$. □

Exemple 2.7. — Si $a + ib$ est un nombre complexe avec $b \neq 0$, son polynôme minimal sur $\mathbf{R}$ est $(X - a)^2 + b^2$. Le polynôme minimal de $\sqrt{2}$ sur $\mathbf{Q}$ est $X^2 - 2$. Le sous-anneau $\mathbf{Q}[\sqrt{2}] = \{x + y\sqrt{2} \mid x, y \in \mathbf{Q}\}$ de $\mathbf{R}$ est un corps ; l'inverse de $x + y\sqrt{2}$, si x et y ne sont pas tout deux nuls, est $\frac{x - y\sqrt{2}}{x^2 + 2y^2}$.

Plus généralement, pour tout entier $n \geqslant 1$, le polynôme minimal de $\sqrt[n]{2}$ sur $\mathbf{Q}$ est $X^n - 2$ (ex. I.9.7) et le sous-anneau $\mathbf{Q}[\sqrt[n]{2}] = \{x_0 + x_1 \sqrt[n]{2} + \cdots + x_{n-1} \sqrt[n]{2^{n-1}} \mid x_0, \ldots, x_{n-1} \in \mathbf{Q}\}$ de $\mathbf{R}$ est un corps.

Exemple 2.8. — Soit p un nombre premier. Le polynôme minimal de $\omega := e^{2i\pi/p}$ sur $\mathbf{Q}$ est $P(X) := X^{p-1} + \cdots + X + 1$, de sorte que ω est de degré $p - 1$ sur $\mathbf{Q}$. En effet, P est irréductible (exerc. I.11.44) et ω en est racine. Si $p \geqslant 3$, le polynôme minimal de ω sur $\mathbf{R}$ est $(X - \omega)(X - \bar{\omega}) = X^2 - 2X \cos \frac{2\pi}{p} + 1$

et c'est aussi son polynôme minimal sur le corps $\mathbf{Q}(\cos\frac{2\pi}{p})$; en particulier, $[\mathbf{Q}(\cos\frac{2\pi}{p}) : \mathbf{Q}(\omega)] = 2$ et le th. 2.2 entraîne alors $[\mathbf{Q}(\cos\frac{2\pi}{p}) : \mathbf{Q}] = \frac{p-1}{2}$.

Comme il existe des nombres premiers arbitrairement grands, on en déduit $[\mathbf{R} : \mathbf{Q}] = \infty$. On peut aussi déduire cette égalité du fait qu'une extension finie d'un corps dénombrable est dénombrable (alors que $\mathbf{R}$ n'est pas dénombrable).

Corollaire 2.9. — *Toute extension finie de corps est algébrique.*

Attention ! La réciproque est fausse (*cf.* ex. 2.14).

Démonstration. — Soit $K \subseteq L$ une extension finie de corps et soit $x \in L$. Le K-espace vectoriel $K[x]$ est un sous-espace vectoriel de L, donc est de dimension finie. Le th. 2.6 entraîne que x est algébrique sur K. □

On peut aussi facilement démontrer le corollaire directement : si $K \subseteq L$ est une extension finie de corps de degré n et si $x \in L$, alors la famille $1, x, \ldots, x^n$ a $n+1$ éléments donc est une famille liée dans le K-espace vectoriel L, et une combinaison linéaire nulle non triviale de ces éléments est un polynôme non nul de $K[X]$ dont x est racine. Donc L est une extension algébrique de K.

Corollaire 2.10. — *Toute extension de corps $K \subseteq L$ engendrée par un nombre fini d'éléments $x_1, \ldots, x_n$ algébriques sur K est finie, donc algébrique. On a de plus $L = K[x_1, \ldots, x_n]$.*

Démonstration. — On procède par récurrence sur n.

Si $n = 0$, c'est évident. Si $n \geqslant 1$, on pose $L' = K(x_2, \ldots, x_n)$. L'hypothèse de récurrence entraîne que l'extension $K \subseteq L'$ est finie et $L' = K[x_2, \ldots, x_n]$. Comme x_1 est algébrique sur K, il l'est sur L', donc l'extension $L' \subseteq L = L'(x_1)$ est finie par le th. 2.6 et $L = L'[x_1]$. Le corollaire résulte alors du th. 2.2 et du cor. 2.9. □

Théorème 2.11. — *Soit $K \subseteq L$ une extension de corps. L'ensemble des éléments de L algébriques sur K est un sous-corps de L contenant K. C'est une extension algébrique de K.*

Démonstration. — Soient x et y des éléments non nuls de L algébriques sur K. Le cor. 2.10 entraîne que l'extension $K \subseteq K(x, y)$ est finie, donc algébrique. Les éléments $x - y$ et x/y de L sont donc algébriques sur K. □

Corollaire 2.12. — *Toute extension de corps $K \subseteq L$ engendrée par des éléments algébriques sur K est algébrique.*

Démonstration. — Soit $S \subseteq L$ un ensemble d'éléments de L algébriques sur K et engendrant L. Par le théorème, l'ensemble des éléments de L algébriques sur K est un sous-corps de L, et il contient S. Comme S engendre L, c'est donc L, qui est ainsi une extension algébrique de K, de nouveau par le théorème. □

Exemple 2.13. — Le réel $\sqrt{2} + \sqrt{3} + \sqrt{5}$ est algébrique (sur $\mathbf{Q}$), de même que le nombre complexe $\sqrt{2} + \sqrt{3} + i\sqrt{5}$.

Exemple 2.14. — L'ensemble $\bar{\mathbf{Q}} \subseteq \mathbf{C}$ des nombres algébriques (sur $\mathbf{Q}$) est un corps qui est une extension algébrique de $\mathbf{Q}$. Elle est de degré infini parce qu'il existe des polynômes irréductibles dans $\mathbf{Q}[X]$ de degré arbitrairement grand (exerc. I.11.44 et ex. 2.8).

Théorème 2.15. — *Soient $K \subseteq L$ et $L \subseteq M$ des extensions de corps. Si un élément x de M est algébrique sur L et que L est une extension algébrique de K, alors x est algébrique sur K.*

En particulier, si L est une extension algébrique de K et que M est une extension algébrique de L, alors M est une extension algébrique de K.

Démonstration. — Si un élément x de M est algébrique sur L, il est racine d'un polynôme $P \in L[X]$. Si l'extension $K \subseteq L$ est algébrique, l'extension $L' \subseteq L$ de K engendrée par les coefficients de P est alors finie (cor. 2.10). Comme x est algébrique sur L', l'extension $L' \subseteq L'(x)$ est finie (th. 2.6). Le th. 2.2 entraîne que l'extension $K \subseteq L'(x)$ est finie, donc algébrique (cor. 2.9), et x est algébrique sur K. □

Remarque 2.16. — Si $K \subseteq L$ et $L \subseteq M$ sont des extensions de corps, on a donc (th. 2.2 et th. 2.15)

$$\begin{aligned} K \subseteq L \text{ et } L \subseteq M \text{ finies} &\iff K \subseteq M \text{ finie}, \\ K \subseteq L \text{ et } L \subseteq M \text{ algébriques} &\iff K \subseteq M \text{ algébrique}. \end{aligned}$$

2.2. Racines de l'unité. — Soit K un corps et soit n un entier $\geqslant 1$. On appelle groupe des *racines n-ièmes de l'unité* dans K le groupe multiplicatif

$$\mu_n(K) = \{\zeta \in K \mid \zeta^n = 1\}.$$

C'est l'ensemble des racines du polynôme $P(X) = X^n - 1$ et il a donc au plus n éléments (prop. I.6.9). Un élément ζ de $\mu_n(K)$ est dit *racine primitive n-ième de l'unité* si $\zeta^d \neq 1$ pour tout $d \in \{1, \dots, n-1\}$; en d'autres termes, si ζ est d'ordre n dans le groupe $\mu_n(K)$. *S'il existe une racine primitive n-ième de l'unité ζ dans K,* elle engendre le groupe $\mu_n(K)$, qui est alors isomorphe à $\mathbf{Z}/n\mathbf{Z}$. Il y a alors

$$\varphi(n) = \mathrm{Card}((\mathbf{Z}/n\mathbf{Z})^\times) = \mathrm{Card}\{d \in \{0, \dots, n-1\} \mid d \wedge n = 1\}$$

différentes racines primitives n-ièmes de l'unité, à savoir les ζ^d pour $d \wedge n = 1$.

Exemple 2.17. — On a

$$\mu_n(\mathbf{R}) = \mu_n(\mathbf{Q}) = \begin{cases} \{1\} & \text{si } n \text{ est impair} ; \\ \{1, -1\} & \text{si } n \text{ est pair.} \end{cases}$$

Il n'y a donc de racines primitives n-ièmes de l'unité dans $\mathbf{R}$ ou dans $\mathbf{Q}$ que si $n \in \{1, 2\}$. En revanche, on a

$$\mu_n(\mathbf{C}) \simeq \mathbf{Z}/n\mathbf{Z}$$

pour tout $n \geqslant 1$.

Théorème 2.18. — *Pour tout corps K et tout entier $n \geqslant 1$, le groupe $\mu_n(K)$ est cyclique d'ordre un diviseur de n. Plus généralement, tout sous-groupe fini de $(K^\times, \times)$ est cyclique.*

En particulier, le groupe multiplicatif d'un corps fini est cyclique.

Démonstration. — Posons $m = \mathrm{Card}(\mu_n(K))$. Tout élément ζ de $\mu_n(K)$ est d'ordre un diviseur d de m (par le théorème de Lagrange) et de n (puisque $\zeta^n = 1$) ; c'est alors une racine primitive d-ième de l'unité. On a vu plus haut que l'ensemble $P_d \subseteq \mu_n(K)$ des racines primitives d-ièmes de l'unité est soit vide, soit de cardinal $\varphi(d)$. Comme

$$\mu_n(K) = \bigcup_{d \mid m \wedge n} P_d,$$

on a donc $m \leqslant \sum_{d \mid m \wedge n} \varphi(d)$. Or (exerc. I.11.16), pour tout entier $e \geqslant 1$, on a $\sum_{d \mid e} \varphi(d) = e$. On en déduit $m \leqslant m \wedge n$, donc $m \mid n$, et $P_m \neq \varnothing$. Il existe donc un élément d'ordre m dans $\mu_n(K)$, qui est ainsi un groupe cyclique d'ordre un diviseur de n. Ceci montre le premier point.

Si G est un sous-groupe de $(K^\times, \times)$ de cardinal m, il est contenu par le théorème de Lagrange dans le groupe cyclique $\mu_m(K)$, qui est de cardinal au plus m. On a donc $G = \mu_m(K) \simeq \mathbf{Z}/m\mathbf{Z}$. Ceci termine la démonstration de la proposition. □

2.3. Polynômes cyclotomiques complexes. — Soit n un entier strictement positif. On définit le n-ième *polynôme cyclotomique* (complexe) par

$$\Phi_n(X) = \prod_{\substack{\zeta \text{ racine primitive} \\ n\text{-ième de 1 dans } \mathbf{C}}} (X - \zeta). \tag{6}$$

D'après ce qui précède, c'est un polynôme unitaire de degré $\varphi(n)$ à coefficients complexes. On a par exemple

$$\begin{aligned} \Phi_1(X) &= X - 1, \\ \Phi_2(X) &= X + 1, \\ \Phi_3(X) &= X^2 + X + 1, \\ \Phi_4(X) &= X^2 + 1. \end{aligned}$$

Pour tout entier premier p, on a

$$\Phi_p(X) = \prod_{k=1}^{p-1} (X - e^{2ik\pi/p}) = \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1.$$

Proposition 2.19. — *Pour tout entier $n \geqslant 1$, on a*

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{7}$$

Le polynôme Φ_n est unitaire à coefficients entiers.

Démonstration. — On a $X^n - 1 = \prod_{\zeta \in \mu_n(\mathbf{C})} (X - \zeta)$. Comme dans la preuve du th. 2.18, on remarque que $\mu_n(\mathbf{C})$ est la réunion disjointe de ses parties P_d, pour $d \mid n$. On a donc

$$X^n - 1 = \prod_{d|n} \prod_{\zeta \in P_d} (X - \zeta) = \prod_{d|n} \Phi_d(X).$$

Pour montrer que le polynôme unitaire Φ_n est à coefficients entiers, on procède par récurrence sur n : par (7), Φ_n est le quotient de $X^n - 1$ par le polynôme unitaire $\prod_{d|n,\, d \neq n} \Phi_d(X)$, qui est à coefficients entiers par hypothèse de récurrence. C'est donc un polynôme à coefficients entiers (th. I.7.1). □

Exemple 2.20. — Pour tout entier premier p, on a $X^{p^2} - 1 = \Phi_{p^2}(X)\Phi_p(X)\Phi_1(X) = \Phi_{p^2}(X)(X^p - 1)$, donc

$$\Phi_{p^2}(X) = \frac{X^{p^2} - 1}{X^p - 1} = X^{p(p-1)} + X^{p(p-2)} + \cdots + X^p + 1.$$

Plus généralement, pour tout entier $r \geqslant 1$, on a

$$\Phi_{p^r}(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1 = \Phi_p(X^{p^{r-1}}).$$

En particulier, on a

$$\Phi_{2^r}(X) = X^{2^{r-1}} + 1.$$

Théorème 2.21. — *Pour tout entier $n \geqslant 1$, le polynôme Φ_n est irréductible dans $\mathbf{Q}[X]$. En particulier,*

$$[\mathbf{Q}(e^{2i\pi/n}) : \mathbf{Q}] = \varphi(n).$$

La preuve de ce théorème (qu'on ne donnera pas ici) est un peu compliquée mais reste du niveau de l'agrégation. C'est un développement classique pour l'oral.

Exercice 2.22. — Montrer qu'une extension finie de $\mathbf{Q}$ ne contient qu'un nombre fini de racines de l'unité.

2.4. Constructions à la règle et au compas. — Ce paragraphe est un classique de l'agrégation et les problèmes qui y sont traités ont un intérêt historique, même si leur intérêt mathématique est très limité.

Définition 2.23. — *Soit Σ un sous-ensemble de $\mathbf{R}^2$. On dit qu'un point $P \in \mathbf{R}^2$ est* constructible (à la règle et au compas) à partir de Σ *si on peut obtenir P à partir des points de Σ par une suite finie d'opérations de l'un des types suivants :*

- *prendre l'intersection de deux droites non parallèles passant chacune par deux points distincts déjà construits ;*
- *prendre l'un des points d'intersection d'une droite passant par deux points distincts déjà construits et d'un cercle de rayon joignant deux points distincts déjà construits ;*
- *prendre l'un des points d'intersection de deux cercles distincts dont les rayons joignent chacun deux points distincts déjà construits.*

On dira qu'une droite est constructible (à partir de Σ) si elle passe par deux points constructibles distincts, et qu'un cercle est constructible si son centre l'est et qu'il passe par un point constructible. On montre que la perpendiculaire et la parallèle à une droite constructible passant par un point constructible sont constructibles, et que le cercle de centre un point constructible et de rayon la distance entre deux points constructibles est constructible.

Si Σ est un sous-ensemble de $\mathbf{R}$ contenant 0 et 1, on dit qu'un réel x est constructible à partir de Σ si c'est l'abcisse d'un point P constructible à partir de $\Sigma \times \{0\}$ au sens de la définition ci-dessus. Cela revient au même de dire que les points $(x, 0)$ et $(0, x)$ sont constructibles à partir de $\Sigma \times \{0\}$.

Théorème 2.24. — *Soit Σ un sous-ensemble de $\mathbf{R}$ contenant 0 et 1. L'ensemble $\mathscr{C}_\Sigma$ des réels constructibles à partir de Σ est un sous-corps de $\mathbf{R}$ tel que, si $x \in \mathscr{C}_\Sigma$, alors $\sqrt{|x|} \in \mathscr{C}_\Sigma$.*

Démonstration. — L'addition et l'opposé sont évidents (utiliser des cercles). Le produit xy est l'ordonnée de l'intersection de la droite joignant l'origine au point $(1, x)$ avec la verticale passant par $(y, 0)$; l'inverse de x non nul est l'ordonnée de l'intersection de la droite joignant l'origine au point $(x, 1)$ avec la verticale passant par $(1, 0)$. La racine carrée d'un élément positif x de $\mathscr{C}_\Sigma$ s'obtient par le théorème de Pythagore en construisant un triangle rectangle dont un des côtés est $\frac{1}{2}|x - 1|$ et dont l'hypothénuse est $\frac{1}{2}(x + 1)$. □

En particulier, être constructible à partir de $\{0, 1\}$ est la même chose qu'être constructible à partir de $\mathbf{Q}$; on dit simplement « constructible ».

***Théorème 2.25* (Wantzel, 1837)**. — *Soit K un sous-corps de $\mathbf{R}$. Un réel x est constructible à partir de K si et seulement s'il existe une suite d'extensions*

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbf{R}$$

telle que $[K_i : K_{i-1}] = 2$ et $x \in K_n$.

Avant de démontrer le théorème, on va décrire en général les extensions de degré 2.

Lemme 2.26. — *Soit K un corps de caractéristique différente de 2 et soit $K \subseteq L$ une extension de degré 2. Il existe $x \in L \smallsetminus K$ tel que $x^2 \in K$ et $L = K[x]$.*

Démonstration. — Si $y \in L \smallsetminus K$, la famille $(1, y)$ est K-libre, donc c'est une base du K-espace vectoriel L. Il existe donc a et b dans K tels que

$$y^2 = ay + b.$$

Comme la caractéristique de K est différente de 2, on peut poser $x = y - \frac{a}{2}$. On a alors

$$x^2 = y^2 - ay + \frac{a^2}{4} = b + \frac{a^2}{4} \in K,$$

et $L = K[y] = K[x]$. □

Démonstration du théorème. — Soit L un sous-corps de $\mathbf{R}$. On vérifie par des calculs directs que :

- les coordonnées du point d'intersection de deux droites non parallèles passant chacune par deux points distincts à coordonnées dans L, sont dans L ;
- les coordonnées de chacun des points d'intersection d'une droite passant par deux points à coordonnées dans L et d'un cercle de rayon joignant deux points distincts à coordonnées dans L sont solutions d'une équation de degré 2 à coefficients dans L ;
- les coordonnées de chacun des points d'intersection de deux cercles distincts, chacun de rayon joignant deux points distincts à coordonnées dans L, sont solutions d'une équation de degré 2 à coefficients dans L.

Par récurrence, on voit que les coordonnées d'un point constructible à partir de K sont dans un corps du type K_n décrit dans l'énoncé du théorème.

Inversement, pour montrer que tout point dans un corps de type K_n est constructible à partir de K, il suffit de montrer que tout réel dans une extension quadratique d'un corps L contenue dans $\mathbf{R}$ est constructible à partir de L. Une telle extension est engendrée par un réel x tel que $x^2 \in L$ (lemme 2.26). Mais alors $x = \pm\sqrt{x^2}$ est constructible à partir de L (th. 2.24). □

Corollaire 2.27. — *Soit x un réel constructible sur un sous-corps K de $\mathbf{R}$. Alors x est algébrique sur K de degré une puissance de 2.*

Démonstration. — Si x est un réel constructible, il est dans une extension K_n du type décrit dans le théorème de Wantzel (th. 2.25), pour laquelle $[K_n : K] = 2^n$ (th. 2.2). En considérant la suite d'extensions $K \subseteq K(x) \subseteq K_n$, on voit que $[K(x) : K]$ est une puissance de 2 (th. 2.2). □

Remarque 2.28. — Attention, la réciproque du corollaire est fausse telle quelle (exerc. 5.19). On peut montrer qu'un nombre réel x est constructible si et seulement s'il vérifie la propriété suivante : x est algébrique sur $\mathbf{Q}$ et si P est son polynôme minimal (sur $\mathbf{Q}$) et si $x_1, \ldots, x_d$ sont toutes les racines (complexes) de P, alors le degré de l'extension $\mathbf{Q} \subseteq \mathbf{Q}(x_1, \ldots, x_d)$ est une puissance de 2.

Corollaire 2.29 **(Duplication du cube)**. — *Le réel $\sqrt[3]{2}$ n'est pas constructible (sur $\mathbf{Q}$).*

Démonstration. — C'est une racine du polynôme $X^3 - 2$. Si ce dernier est réductible sur $\mathbf{Q}$, il a un facteur de degré 1, donc une racine rationnelle que l'on écrit sous forme de fraction réduite a/b. On a alors $a^3 = 2b^3$, donc a est pair. On écrit $a = 2a'$ avec $4a'^3 = b^3$, donc b est pair, contradiction (voir aussi l'exerc. I.11.20 ou appliquer le critère d'Eisenstein (th. I.9.6)).

Ainsi, le degré de $\sqrt[3]{2}$ sur $\mathbf{Q}$ est 3 : il n'est donc pas constructible par cor. 2.27. □

Corollaire 2.30 **(Quadrature du cercle)**. — *Le réel $\sqrt{\pi}$ n'est pas constructible.*

Démonstration. — Ici, on triche : il faut savoir que π est transcendant (ex. 2.5), donc aussi $\sqrt{\pi}$. □

On dit qu'un angle α est constructible à partir d'un angle θ si le point $(\cos\alpha, \sin\alpha)$ est constructible à partir de $\{(0,0), (0,1), (\cos\theta, \sin\theta)\}$. Comme $\sin\alpha$ est constructible à partir de $\cos\alpha$, c'est équivalent à dire que $\cos\alpha$ est constructible à partir de $\{0, 1, \cos\theta\}$.

***Corollaire 2.31* (Trisection de l'angle).** — *L'angle $\theta/3$ est constructible à partir de l'angle θ si et seulement si le polynôme $X^3 - 3X - 2\cos\theta$ a une racine dans $\mathbf{Q}(\cos\theta)$.*

En particulier, l'angle $2\pi/9$ n'est pas constructible à la règle et au compas.

Démonstration. — Comme $\cos 3u = 4\cos^3 u - 3\cos u$, le réel $\cos\theta/3$ est racine du polynôme

$$P(X) = 4X^3 - 3X - \cos\theta.$$

Si P est irréductible sur $\mathbf{Q}(\cos\theta)$, il n'a pas de racine dans ce corps, le réel $\cos\theta/3$ est de degré 3 sur ce corps et ne peut y être constructible par cor. 2.27.

Si P est réductible sur $\mathbf{Q}(\cos\theta)$, étant de degré 3, il doit avoir une racine dans ce corps et se factoriser sur ce corps en le produit d'un polynôme de degré 1 et d'un polynôme de degré 2. Le réel $\cos\theta/3$ est racine de l'un de ces deux polynômes, donc est constructible sur $\mathbf{Q}(\cos\theta)$ (lemme 2.26 et th. 2.25). Comme $2P(X/2) = X^3 - 3X - 2\cos\theta$, cela montre la première partie de l'énoncé.

On a $\mathbf{Q}(\cos 2\pi/3) = \mathbf{Q}$, donc l'angle $2\pi/9$ est constructible si et seulement si le polynôme $X^3 - 3X - 1$ a une racine dans $\mathbf{Q}$, ce qui n'est pas le cas (exerc. I.11.20). □

On peut aussi s'intéresser plus généralement, après Fermat, aux polygones réguliers constructibles à la règle et au compas. Soit $\mathscr{N}$ l'ensemble des nombres entiers $n \geqslant 1$ tels que le polygone régulier à n côtés, inscrit dans le cercle unité et dont l'un des sommets est $(0, 1)$, soit constructible à la règle et au compas, c'est-à-dire tels que $e^{2i\pi/n}$ (ou, de façon équivalente, l'angle $2\pi/n$) soit constructible. On vient de voir que 9 n'est pas dans $\mathscr{N}$.

Rappelons qu'un *nombre premier de Fermat* est un nombre premier de la forme $F_m := 2^{2^m} + 1$.

***Théorème 2.32*.** — *Si un polygone régulier à n côtés est constructible à la règle et au compas, n est le produit d'une puissance de 2 et de nombres premiers de Fermat distincts.*

La réciproque est vraie, mais sa preuve nécessite de connaître la théorie de Galois. En particulier, le polygone régulier à 17 côtés est constructible à la règle et au compas (Gauss, 1796).

Démonstration. — Si $n \in \mathscr{N}$, le degré de $e^{2i\pi/n}$ sur $\mathbf{Q}$ est une puissance de 2 (cor. 2.31). De plus, $2n \in \mathscr{N}$ (on peut bissecter n'importe quel angle constructible) et tout diviseur de n est dans $\mathscr{N}$. Il suffit donc de montrer que si un nombre premier impair p appartiennent à $\mathscr{N}$, c'est un nombre premier de Fermat, et que le carré d'un nombre premier impair n'est pas dans $\mathscr{N}$.

Soit p un nombre premier impair. Le degré de $\exp(2i\pi/p)$ sur $\mathbf{Q}$ est $p - 1$ (ex. 2.8). Si $p \in \mathscr{N}$, l'entier $p - 1$ est donc une puissance de 2, et p est un nombre premier de Fermat (exerc. I.11.15).

Pour montrer que p^2 n'est jamais dans $\mathscr{N}$, rappelons (ex. 2.20 et th. 2.21) que le degré de $\exp(2i\pi/p^2)$ sur $\mathbf{Q}$ est $\varphi(p^2) = p(p-1)$, qui n'est pas une puissance de 2 (il est divisible par p). □

3. Construction d'extensions

On prend maintenant le problème dans l'autre sens : au lieu de se donner une extension d'un corps K et de regarder si les éléments de cette extension sont, ou non, racines de polynômes à coefficients dans K, on part d'un polynôme $P \in K[X]$ et l'on cherche à *construire* une extension de corps de K dans laquelle P aura une racine, ou même, sera *scindé* (produit de facteurs du premier degré).

3.1. Corps de rupture. — Étant donné un polynôme irréductible, on commence par construire une extension dans lequel P a une racine.

Définition 3.1. — *Soit K un corps et soit $P \in K[X]$ un polynôme irréductible. On appelle* corps de rupture *de P sur K une extension $K \subseteq L$ telle que $L = K(x)$, avec $x \in L$ et $P(x) = 0$.*

Exemple 3.2. — Le corps $\mathbf{C}$ est un corps de rupture du polynôme irréductible $X^2 + 1 \in \mathbf{R}[X]$. De même, le polynôme $X^2 + X + 1$ est aussi irréductible sur $\mathbf{R}$ et $\mathbf{C}$ est encore un corps de rupture. Plus généralement, $\mathbf{C}$ est le corps de rupture de n'importe quel polynôme de $\mathbf{R}[X]$ de degré deux sans racine réelle (*cf.* ex. 5.1).

Exemple 3.3. — Le corps $\mathbf{Q}(\sqrt[3]{2})$ est un corps de rupture du polynôme irréductible $X^3 - 2 \in \mathbf{Q}[X]$; le corps $\mathbf{Q}(j\sqrt[3]{2})$ en est un autre. Remarquons que le polynôme $X^3 - 2$ n'est pas scindé dans ces corps.

Théorème 3.4. — *Soit K un corps et soit $P \in K[X]$ un polynôme irréductible. Il existe un corps de rupture de P sur K.*

Démonstration. — L'anneau $K[X]$ étant principal, l'anneau quotient $K_P := K[X]/(P)$ est un corps (prop. 6.1). Soit $x_P \in K_P$ l'image de X dans K_P. On a alors $P(x_P) = 0$ et $K_P = K(x_P)$, donc K_P est un corps de rupture de P sur K. □

Nous allons maintenant nous intéresser à l'unicité du corps de rupture.

Définition 3.5. — *Soient $K \subseteq L$ et $K \subseteq L'$ des extensions de corps. On appelle* K-morphisme de L dans L' *un morphisme de corps $L \hookrightarrow L'$ qui est l'identité sur K.*

Proposition 3.6. — *Soit $P \in K[X]$ un polynôme irréductible. Pour toute extension $K \subseteq L$ et toute racine x de P dans L, il existe un unique K-morphisme $K_P \hookrightarrow L$ qui envoie x_P sur x.*

Démonstration. — Le morphisme $K[X] \to L$ qui envoie X sur x est nul sur P, donc définit par passage au quotient l'unique K-morphisme de K_P vers L qui envoie x_P sur x. □

Corollaire 3.7. — *Soit $P \in K[X]$ un polynôme irréductible. Deux corps de rupture de P sont K-isomorphes.*

On remarquera que l'isomorphisme entre deux corps de rupture n'est en général pas unique. Plus précisément, étant donnés des corps de rupture $K \subseteq L$ et $K \subseteq L'$ de P, et des racines $x \in L$ et $x' \in L'$ de P, il existe un unique K-isomorphisme $\sigma\colon L \xrightarrow{\sim} L'$ tel que $\sigma(x) = x'$.

3.2. Corps de décomposition. — Étant donné un polynôme P à coefficients dans K, on cherche maintenant à construire une extension de K dans laquelle P est scindé, c'est-à-dire produit de facteurs du premier degré.

Théorème 3.8. — *Soit K un corps et soit $P \in K[X]$ un polynôme non nul de degré d.*

(a) *Il existe une extension $K \subseteq L$ dans laquelle le polynôme P est scindé, de racines $x_1, \ldots, x_d$, telle que $L = K(x_1, \ldots, x_d)$.*

(b) *Deux telles extensions sont K-isomorphes.*

Une telle extension s'appelle un *corps de décomposition* de P. C'est une extension finie de K (cor. 2.10).

Démonstration. — On procède par récurrence sur le degré d de P. Si $d = 0$, le corps $L = K$ est le seul qui convient.

Si $d \geqslant 1$, soit Q un facteur irréductible de P dans $K[X]$ (*cf.* th. I.8.6) et soit K_Q le corps de rupture de Q construit plus haut. Le polynôme P admet la racine x_Q dans K_Q, donc s'écrit

$$P(X) = (X - x_Q)R(X),$$

avec $R \in K_Q[X]$ de degré $d-1$. L'hypothèse de récurrence appliquée à R fournit un corps de décomposition $K_Q \subseteq L$ de R sur K_Q. Alors R est scindé dans $L[X]$, de racines $x_1, \ldots, x_{d-1}$, donc aussi P, de racines $x_Q, x_1, \ldots, x_{d-1}$. De plus, $L = K_Q(x_1, \ldots, x_{d-1}) = K(x_Q, x_1, \ldots, x_{d-1})$, donc L est un corps de décomposition de P, et ceci montre (a).

Soient $K \subseteq L$ et $K \subseteq L'$ des corps de décomposition de P, et soient x une racine de Q (un facteur irréductible de P dans $K[X]$) dans L et x' une racine de Q dans L'. Le corps $K(x) \subseteq L$ est un corps de rupture pour Q sur K, et il en est de même pour le corps $K(x') \subseteq L'$. Il existe donc (cor. 3.7) un K-isomorphisme $K(x) \xrightarrow{\sim} K(x')$ qui envoie x sur x'. Il permet de considérer L' comme une extension de $K(x)$ via le morphisme composé $K(x) \xrightarrow{\sim} K(x') \subseteq L'$.

Écrivons comme plus haut $P(X) = (X-x)R(X)$ avec $R \in K(x)[X]$ de degré $d-1$. Les extensions L et L' de $K(x)$ sont alors des corps de décomposition de R sur $K(x)$. L'hypothèse de récurrence appliquée à R entraîne que L et L' sont $K(x)$-isomorphes, donc K-isomorphes. Ceci prouve (b). □

Exemple 3.9. — Pour tout $d \geqslant 3$, le corps $\mathbf{C}$ est un corps de décomposition pour le polynôme $X^d - 1 \in \mathbf{R}[X]$.

Exemple 3.10. — Le corps $\mathbf{Q}(\sqrt[3]{2}, j)$ est un corps de décomposition pour le polynôme $X^3 - 2 \in \mathbf{Q}[X]$. En considérant la suite d'extensions $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2}) \subseteq \mathbf{Q}(\sqrt[3]{2}, j)$, on voit que c'est une extension de degré 6 de $\mathbf{Q}$.

Remarque 3.11. — Soit K un corps de caractéristique 0 et soit $P \in K[X]$ un polynôme irréductible. Son polynôme dérivé P' est alors non nul et est donc premier avec P. En particulier, P n'a que des racines simples dans un corps de décomposition (prop. I.10.5).

Cela n'est plus nécessairement vrai en caractéristique $p > 0$ (voir cependant la rem. 4.3). Posons $L = \mathbf{F}_p(Y)$, vu comme extension de $K = L^p = \mathbf{F}_p(Y^p)$. Le polynôme $P(X) = X^p - Y^p \in K[X]$ est irréductible (Eisenstein). Un corps de décomposition est L et dans ce corps, il se décompose en $P(X) = (X-Y)^p$. Il a donc une unique racine, d'ordre p.

3.3. Clôture algébrique. —

Définition 3.12. — *On dit qu'un corps Ω est* algébriquement clos *si tout polynôme non constant de $\Omega[X]$ a une racine dans Ω.*

Une clôture algébrique *d'un corps K est une extension algébrique de corps $K \subseteq \Omega$ telle que Ω est un corps algébriquement clos.*

Si Ω est un corps algébriquement clos, tout polynôme non constant de $\Omega[X]$ est scindé dans Ω, comme on le voit facilement en raisonnant par récurrence sur le degré du polynôme.

Exemple 3.13. — Le corps $\mathbf{C}$ est algébriquement clos (c'est le théorème de d'Alembert–Gauss, qui est au programme de l'agrégation). C'est une clôture algébrique de $\mathbf{R}$, mais pas de $\mathbf{Q}$ (car l'extension $\mathbf{Q} \subseteq \mathbf{C}$ n'est pas algébrique : il existe des nombres complexes transcendants).

Proposition 3.14. — *Soit $K \subseteq L$ une extension algébrique de corps. On suppose que tout polynôme de $K[X]$ est scindé dans L. Alors L est une clôture algébrique de K.*

La conclusion subsiste si on suppose seulement que tout polynôme de $K[X]$ a une racine dans L, mais c'est beaucoup plus difficile à montrer.

Démonstration. — Soit $Q \in L[X]$ un polynôme irréductible et soit x une racine de Q dans une extension de L, de sorte que Q est le polynôme minimal de x sur L. Alors x est algébrique sur L donc sur K (th. 2.15). Soit $P \in K[X]$ son polynôme minimal sur K ; on a alors $Q \mid P$ dans $L[X]$. Mais par hypothèse faite dans la proposition, P est scindé dans L, donc $x \in L$, et Q a donc une racine dans L.

Comme tout élément de $L[X]$ est produit de polynômes irréductibles (th. I.8.6), on a montré que tout polynôme de $L[X]$ a une racine dans L, donc que L est un corps algébriquement clos. C'est donc une clôture algébrique de K. □

À partir d'un corps algébriquement clos, il est facile de construire une clôture algébrique pour n'importe quel sous-corps.

Proposition 3.15. — *Soit Ω un corps algébriquement clos et soit $K \subseteq \Omega$ un sous-corps. L'ensemble des éléments de Ω qui sont algébriques sur K est une clôture algébrique de K.*

Démonstration. — On a déjà vu que l'ensemble $\bar{K}$ des éléments de Ω qui sont algébriques sur K est un sous-corps de Ω (th. 2.11), extension algébrique de K. Montrons qu'il est algébriquement clos. Soit $P \in \bar{K}[X]$ un polynôme non constant et soit x une racine de P dans Ω. Alors x est algébrique sur $\bar{K}$, donc aussi sur K (th. 2.15), de sorte que $x \in \bar{K}$ [3]. □

Exemple 3.16. — Le corps $\bar{\mathbf{Q}} \subseteq \mathbf{C}$ des nombres algébriques (*cf.* ex. 2.14) est une clôture algébrique de $\mathbf{Q}$. C'est un corps dénombrable (pourquoi ?).

Théorème 3.17 **(Steinitz, 1910)**. — *Soit K un corps. Il existe une clôture algébrique de K. Deux clôtures algébriques de K sont K-isomorphes.*

Démonstration. — La construction d'une clôture algébrique en général utilise l'axiome du choix (par exemple sous la forme de l'existence d'un idéal maximal dans un anneau que l'on construit). *Pour simplifier la démonstration, nous nous limiterons donc au cas où le corps K est (au plus) dénombrable et nous ne démontrons que l'existence d'une clôture algébrique.* L'ensemble $K[X]$ est alors dénombrable. On peut donc numéroter ses éléments en une suite $(P_n)_{n\in\mathbf{N}}$. On construit une suite $(K_n)_{n\in\mathbf{N}}$ de corps emboîtés en posant $K_0 = K$ et en prenant pour K_{n+1} un corps de décomposition du polynôme P_n, vu comme élément de $K_n[X]$. Posons

$$L = \bigcup_{n\in\mathbf{N}} K_n.$$

Il existe sur L une (unique) structure de corps faisant de chaque K_n un sous-corps de L et $K \subseteq L$ est une extension algébrique.

Tout polynôme de $K[X]$ est un des P_n donc est par construction scindé dans L. Ce dernier est donc une clôture algébrique de K par la prop. 3.14.

Nous ne démontrerons pas que deux clôtures algébriques de K sont K-isomorphes (même dans le cas $K = \mathbf{Q}$, on utilise l'axiome du choix). □

3. Pour prouver que $\bar{K}$ est algébriquement clos, on peut aussi utiliser la prop. 3.14 : tout polynôme $P \in K[X]$ non constant a une racine dans Ω, et cette racine est dans $\bar{K}$ par définition de $\bar{K}$.

4. Corps finis

On dit qu'un corps K est *fini* s'il n'a qu'un nombre fini d'éléments. Sa caractéristique est alors un nombre premier p et son sous-corps premier le corps $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$. L'extension $\mathbf{F}_p \hookrightarrow K$ est de degré fini n, de sorte que K est de cardinal p^n.

Théorème 4.1. — *Soient p un entier premier et n un entier $\geqslant 1$.*

(1) *Il existe un corps fini à p^n éléments.*

(2) *Tout corps fini à p^n éléments est un corps de décomposition du polynôme $X^{p^n} - X$ sur le corps $\mathbf{F}_p$. En particulier, deux tels corps sont isomorphes.*

On parlera souvent *du* corps à p^n éléments, noté $\mathbf{F}_{p^n}$.

Démonstration. — Soit $\mathbf{F}_p \subseteq K$ un corps de décomposition du polynôme $P(X) := X^{p^n} - X$ sur $\mathbf{F}_p$ et soit $K' \subseteq K$ l'ensemble des racines de P dans K. Par la formule magique (4), c'est un sous-corps de K, qui lui est donc égal puisque K est engendré par ces racines. Ces racines sont toutes distinctes car sa dérivée étant -1, le polynôme P n'a pas de racine multiple (prop. I.10.5(2)). En particulier, $\mathrm{Card}(K) = p^n$. Ceci montre (1).

Soit K un corps fini à p^n éléments. Le groupe $(K^\times, \times)$ étant d'ordre $p^n - 1$, tout élément non nul x de K vérifie $x^{p^n-1} = 1$ (théorème de Lagrange). En particulier, les p^n éléments de K sont exactement les racines de P, qui est ainsi scindé dans K. Le corps K est donc un corps de décomposition de P sur $\mathbf{F}_p$. Par le th. 3.8, ceci montre (2). □

Remarque 4.2. — Si $P \in \mathbf{F}_p[X]$ est irréductible et de degré 2, son corps de rupture (qui est aussi un corps de décomposition) est une extension de degré 2 de $\mathbf{F}_p$, donc est de cardinal p^2 : c'est $\mathbf{F}_{p^2}$. Il s'ensuit que dans $\mathbf{F}_{p^2}$, tous les polynômes de degré 2 à coefficients dans $\mathbf{F}_p$ sont scindés (de la même façon que dans $\mathbf{C}$, tous les polynômes à coefficient réels sont scindés).

Si -1 n'est pas un carré dans $\mathbf{F}_p$ (cela arrive si et seulement si $p \equiv 3 \pmod 4$), le polynôme $X^2 + 1$ est irréductible dans $\mathbf{F}_p[X]$ et on a $\mathbf{F}_{p^2} = \mathbf{F}_p[i]$, avec $i^2 = -1$. Cela peut être utile pour faire des calculs dans $\mathbf{F}_{p^2}$.

Remarque 4.3. — Soit $P \in \mathbf{F}_{p^n}[X]$. Si $P' = 0$, on peut écrire $P(X) = \sum_i a_i X^{ip}$. Comme le morphisme de Frobenius $\mathrm{Fr}_{\mathbf{F}_{p^n}}$ est bijectif (§ 1.1), on peut écrire

$$P(X) = \big(\sum_i \mathrm{Fr}^{-1}_{\mathbf{F}_{p^n}}(a_i) X^i\big)^p.$$

En particulier, P ne peut être irréductible. Autrement dit, le polynôme dérivé d'un polynôme irréductible $P \in \mathbf{F}_{p^n}[X]$ est non nul et est donc premier avec P. En particulier, comme dans la rem. 3.11, P n'a que des racines simples dans un corps de décomposition.

4.1. Théorème de l'élément primitif. —

Le résultat suivant permet de simplifier la vision que l'on a des extensions finies. Mais il n'est pas valable en toute généralité (voir ex. 4.6).

Théorème 4.4. — *Soit K un corps qui est soit fini, soit de caractéristique 0 et soit $K \subseteq L$ une extension finie. Il existe $x \in L$ tel que $L = K(x)$.*

Démonstration. — Si le corps K est fini, le corps L est aussi fini. Par le th. 2.18, le groupe multiplicatif $(L^*, \times)$ est engendré par un élément x. On a alors $L = K(x)$.

Supposons maintenant K de caractéristique 0 (donc infini). Comme L est une extension finie de K, on peut faire une récurrence sur le nombre de générateurs de L sur K et on voit qu'il suffit de montrer le

théorème pour $L = K(x, y)$. Le fait fondamental qu'on va utiliser est qu'un polynôme irréductible n'a que des racines simples dans un corps de décomposition (rem. 3.11).

Soit P le polynôme minimal de x sur K, soit Q le polynôme minimal de y sur K et soit M un corps de décomposition du polynôme PQ. La rem. 3.11 entraîne que P et Q sont scindés à racines simples dans M. On les écrit

$$P(X) = \prod_{i=1}^{m}(X - x_i) \quad , \quad Q(X) = \prod_{j=1}^{n}(X - y_j),$$

où les x_i (resp. les y_j) sont distincts deux à deux, avec $x_1 = x$ et $y_1 = y$. Comme K est infini, on peut choisir $t \in K$ qui n'est égal à aucun des éléments $\frac{x_i - x}{y - y_j}$ de M, pour $i \in \{1, \dots, m\}$ et $j \in \{2, \dots, n\}$, de sorte que $z \coloneqq x + ty \in L$ n'est égal à aucun des $x_i + ty_j$.

On a bien sûr $K(z) \subseteq K(x, y)$. Montrons qu'il y a égalité en prouvant $y \in K(z)$ (donc aussi $x = z - ty \in K(z)$). Notons que y est racine de $Q(X) \in K[X]$ et de $R(X) \coloneqq P(z - tX) \in K(z)[X]$, donc aussi de leur pgcd $S(X) \in K(z)[X]$. Comme $S \mid Q$, il est produit dans $M[X]$ de facteurs distincts $X - y_j$. Si $X - y_j \mid S$ avec $j \in \{2, \dots, n\}$, alors $0 = S(y_j) = R(y_j) = P(z - ty_j)$. Ceci entraîne que $z - ty_j$ est l'un des x_i, ce qui contredit le choix de t. Comme $S(y) = 0$, on en déduit $S(X) = X - y_1$, donc $y = y_1 \in K(z)$ et $K(x, y) = K(z)$. □

Corollaire 4.5. — *Soit K un corps qui est soit fini, soit de caractéristique 0 et soit $K \subseteq L$ une extension finie. Il n'existe qu'un nombre fini d'extensions intermédiaires $K \subseteq M \subseteq L$.*

L'énoncé est bien sûr évident lorsque K est fini puisqu'il n'y a alors qu'un nombre fini de sous-ensembles de L.

Démonstration. — Écrivons $L = K(x)$ (th. 4.4) et soit $P \in K[X]$ le polynôme minimal de x sur K. À chaque extension intermédiaire $K \subseteq M \subseteq L$, associons le polynôme minimal $P_M \in M[X]$ de x sur M. Il est unitaire et divise P dans $L[X]$, donc il n'y a qu'un nombre fini de polynômes possibles P_M.

Il suffit maintenant de montrer que la sous-extension M est entièrement déterminée par le polynôme $P_M = X^e + a_{e-1}X^{e-1} + \cdots + a_1X + a_0$. On a tout d'abord $a_{e-1}, \dots, a_0 \in M$, donc $K(a_{e-1}, \dots, a_0) \subseteq M$. De plus, comme $P_M(x) = 0$ et $L = K(x) = K(a_{e-1}, \dots, a_0)(x)$, on a $[L : K(a_{e-1}, \dots, a_0)] \leqslant e$. Comme $e = [L : M]$ (puisque $L = M(x)$), on en déduit $M = K(a_{e-1}, \dots, a_0)$, ce qui montre ce qu'on voulait : M est le sous-corps de L engendré par les coefficients du polynôme P_M. □

Exemple 4.6 **(Une extension finie avec une infinité de sous-extensions)**. — Soit p un nombre premier. Considérons le corps $L \coloneqq \mathbf{F}_p(X, Y)$ comme extension du corps $K = L^p = \mathbf{F}_p(X^p, Y^p)$ (infini de caractéristique p). C'est une extension finie de K de degré p^2 (X et Y sont algébriques de degré p sur K). Mais il n'existe pas d'élément F de L tel que $L = K(F)$. En effet, pour tout $F \in L$, on a $F^p \in K$, donc $[K(F) : K] \leqslant p$.

Par ailleurs, considérons, pour chaque $n \in \mathbf{N}$, les extensions $L_n \coloneqq K(X + YX^{np})$ de K, toutes de degré p et contenues dans L. Si $L_m = L_n$, alors $X + YX^{mp}$ et $X + YX^{np}$ sont dans L_m, donc aussi leur différence $Y(X^{np} - X^{mp})$. Si $m \neq n$, la différence $X^{np} - X^{mp}$ est non nulle dans K, donc inversible. On en déduit $Y \in L_m$, puis $X \in L_m$, donc $L_m = L$, ce qui est absurde. Les sous-extensions $(L_n)_{n \in \mathbf{N}}$ de L sont donc distinctes deux à deux et il y en a une infinité.

Corollaire 4.7. — *Soit K un corps qui est soit fini, soit de caractéristique 0 et soit $K \subseteq L$ une extension algébrique. On suppose qu'il existe un entier C tel que le degré sur K de tout élément de L est $\leqslant C$. Alors $K \subseteq L$ est une extension finie (de degré $\leqslant C$).*

Démonstration. — Soit x un élément de L de degré maximal d sur K (on a $d \leqslant C$). Soit $y \in L$; l'extension $K \subseteq K(x, y)$ est finie donc, par le th. 4.4, elle est engendrée par un élément z. Par choix de x,

le degré de z sur K, c'est-à-dire le degré de l'extension $K \subseteq K(z) = K(x,y)$, est $\leqslant d$. Comme elle contient l'extension $K \subseteq K(x)$, qui est de degré d, ces extensions sont égales et $y \in K(x)$. On a donc $L = K(x)$. □

Exemple 4.8. — Soit p un nombre premier et soit I un ensemble infini. Considérons le corps $L \coloneqq \mathbf{F}_p((X_i)_{i\in I})$ comme extension du corps $K = L^p = \mathbf{F}_p((X_i^p)_{i\in I})$. Tout élément F de L est de degré $\leqslant p$ sur K, puisque $F^p \in K$, mais L est une extension infinie de K.

5. Exercices

5.1. Généralités. —

Exercice 5.1. — Soit K un corps de caractéristique 3. Montrer que les médianes de tout triangle dans K^2 sont parallèles.

Exercice 5.2. — Pour tous nombres réels positifs a et b, montrer

$$\mathbf{Q}(a, b, \sqrt{a}, \sqrt{b}) = \mathbf{Q}(a, b, \sqrt{a} + \sqrt{b}).$$

5.2. Extensions finies. —

Exercice 5.3. — Trouver le polynôme minimal de $\sqrt{3} + i$ sur $\mathbf{Q}$.

Exercice 5.4. — (1) Calculer le degré de l'extension $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ de $\mathbf{Q}$.

(2) Calculer le degré de l'extension $\mathbf{Q}(\sqrt{2} + \sqrt{3})$ de $\mathbf{Q}$.

(3) Calculer le degré de l'extension $\mathbf{Q}(\sqrt{2}, \sqrt[3]{2})$ de $\mathbf{Q}$.

Exercice 5.5. — Soit $K \subseteq L$ une extension de corps finie de degré premier. Pour tout $x \in L \smallsetminus K$, montrer que $L = K(x)$.

Exercice 5.6. — Soit $K \subseteq L$ une extension de corps finie de degré impair. On suppose qu'il existe $x \in L$ tel que $L = K(x)$. Montrer que $L = K(x^2)$.

Exercice 5.7. — Soit $K \subseteq M$ une extension finie de corps et soient $K \subseteq L \subseteq M$ et $K \subseteq L' \subseteq M$ des extensions intermédiaires. Notons LL' le sous-corps de M engendré par L et L'. Montrer $[LL' : L'] \leqslant [L : K]$ (*Indication :* on pourra prendre une base de L sur K et montrer qu'elle engendre LL' sur L').

5.3. Racines de l'unité. —

Exercice 5.8. — Soit K un corps de caractéristique $p > 0$ et soit r un entier $\geqslant 1$. Quels sont les groupes $\mu_{p^r}(K)$?

Exercice 5.9. — Soit p un nombre premier. Déterminer selon les valeurs de l'entier $n \geqslant 1$ le groupe $\mu_n(\mathbf{Z}/p\mathbf{Z})$.

Exercice 5.10. — Soit K un corps infini. Montrer que le groupe $(K^\times, \times)$ n'est pas engendré par un élément.

Exercice 5.11. — Montrer que pour tout $n \geqslant 2$, on a $\Phi_n(0) = 1$ et que le polynôme cyclotomique Φ_n est réciproque : $X^{\varphi(n)}\Phi_n(1/X) = \Phi_n(X)$.

Exercice 5.12. — Montrer l'égalité $\mathbf{Q}(e^{2i\pi/8}) = \mathbf{Q}(\sqrt{2}, i)$.

Exercice 5.13. — Pour tout entier k strictement positif, on pose $\zeta_k := e^{2i\pi/k}$. Soient m et n des entiers strictement positifs. On veut montrer l'égalité

$$\mathbf{Q}(\zeta_m) \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}(\zeta_{m\wedge n}).$$

On pose $K := \mathbf{Q}(\zeta_m) \cap \mathbf{Q}(\zeta_n)$.

(1) Montrer que si $m \mid n$, on a $\mathbf{Q}(\zeta_m) \subseteq \mathbf{Q}(\zeta_n)$. En déduire $K \supseteq \mathbf{Q}(\zeta_{m\wedge n})$.

(2) Montrer qu'on a $K(\zeta_m) = \mathbf{Q}(\zeta_m)$, $K(\zeta_n) = \mathbf{Q}(\zeta_n)$ et $K(\zeta_{m\vee n}) = \mathbf{Q}(\zeta_{m\vee n})$.

(3) Montrer $\mathbf{Q}(\zeta_m, \zeta_n) = \mathbf{Q}(\zeta_{m\vee n})$.

(4) En déduire $[\mathbf{Q}(\zeta_m, \zeta_n) : \mathbf{Q}(\zeta_m)] = \varphi(m \vee n)/\varphi(m)$ puis, en utilisant l'exerc. 5.7, $[\mathbf{Q}(\zeta_n) : K] \geqslant \varphi(m \vee n)/\varphi(m)$.

(5) Démontrer la formule $\varphi(m)\varphi(n) = \varphi(m \vee n)\varphi(m \wedge n)$ et conclure.

(6) En déduire tous les entiers strictement positifs n tels que $\sqrt{2} \in \mathbf{Q}(\zeta_n)$ (*Indication :* on pourra utiliser l'exerc. 5.12).

5.4. Extensions algébriques. —

Exercice 5.14. — Trouver toutes les extensions algébriques du corps $\mathbf{C}$.

Exercice 5.15. — Montrer que tout corps algébriquement clos est infini.

Exercice 5.16. — On considère le corps $K = \mathbf{Q}(T)$ et ses sous-corps $K_1 = \mathbf{Q}(T^2)$ et $K_2 = \mathbf{Q}(T^2 - T)$. Montrer que les extensions $K_1 \subseteq K$ et $K_2 \subseteq K$ sont algébriques, mais pas l'extension $K_1 \cap K_2 \subseteq K$ (*Indication :* on pourra montrer $K_1 \cap K_2 = \mathbf{Q}$).

Exercice 5.17. — Soit K un corps et soit L un corps tel que $K \subseteq L \subseteq K(T)$.

(1) Si L est une extension algébrique de K, montrer que $L = K$.

(2) Si $L \neq K$, montrer que $K(T)$ est une extension finie de L.

Exercice 5.18 **(Nombres de Liouville)**. — Le but de cet exercice est de donner un exemple explicite de nombre transcendant.

(1) Soit α un nombre réel algébrique irrationel. Montrer qu'il existe un réel C strictement positif et un entier positif n tels que

$$\forall p \in \mathbf{Z} \quad \forall q \in \mathbf{N} \smallsetminus \{0\} \qquad \left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^n}$$

(*Indication :* on pourra introduire un polynôme à coefficients entiers qui annule α et appliquer judicieusement l'inégalité des accroissements finis).

(2) Montrer que le nombre réel $\sum_{n\geq 1} 10^{-n!}$ est transcendant (sur $\mathbf{Q}$).

5.5. Nombres constructibles. —

Exercice 5.19. — Considérons le polynôme $P(X) = X^4 - X - 1 \in \mathbf{Q}[X]$.

(1) Montrer que P a exactement deux racines réelles distinctes x_1 et x_2.

(2) On écrit $(X - x_1)(X - x_2) = X^2 + aX + b$ avec a, $b \in \mathbf{R}$. Montrer $[\mathbf{Q}(a^2) : \mathbf{Q}] = 3$.

(3) Montrer que x_1 et x_2 ne peuvent être tous les deux constructibles, bien qu'ils soient de degré 4 sur $\mathbf{Q}$.

5.6. Corps de décomposition. —

Exercice 5.20. — Déterminer le corps de décomposition du polynôme $X^3 - 3$ sur $\mathbf{Q}$ et en donner une base sur $\mathbf{Q}$.

Exercice 5.21. — Montrer que le corps de décomposition d'un polynôme de degré d est une extension de degré au plus $d!$.

Exercice 5.22. — Soit p un nombre premier, soit K un corps et soit $a \in K$. Montrer que le polynôme $X^p - a$ est irréductible dans $K[X]$ si et seulement s'il n'a pas de racines dans K (*Indication :* on pourra montrer que si $X^p - a = PQ$, avec $n \coloneqq \deg(P)$ et $P \in K[X]$ unitaire, on a $a^n = ((-1)^n P(0))^p$, en décomposant $X^p - a$ en produit de facteurs de degré 1 dans un corps de décomposition).

5.7. Corps finis. —

Exercice 5.23. — Écrire les tables d'addition et de multiplication du corps $\mathbf{F}_4$ [4].

Exercice 5.24. — Montrer que le polynôme $P(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ est irréductible dans $\mathbf{F}_3[X]$ (*Indication :* on pourra considérer le corps de rupture d'un facteur irréductible de P).

Exercice 5.25. — Quel est le groupe additif $(\mathbf{F}_{p^n}, +)$?

Exercice 5.26. — Soit p un nombre premier.

(1) Comparer les trois groupes additifs $(\mathbf{F}_{p^2}, +)$, $(\mathbf{F}_p^2, +)$ et $(\mathbf{Z}/p^2\mathbf{Z}, +)$: lesquels sont isomorphes ?

(2) Comparer les trois anneaux correspondants : lesquels sont isomorphes ?

(3) Pour les trois anneaux précédents, déterminer les groupes (multiplicatifs) formés des éléments inversibles : lesquels sont isomorphes ?

Exercice 5.27. — Soient p et q des nombres premiers. Montrer que $\mathbf{F}_{p^m}$ est isomorphe à un sous-corps de $\mathbf{F}_{q^n}$ si et seulement si $p = q$ et m *divise* n.

Exercice 5.28. — (1) Montrer que le polynôme $X^4 - X - 1$ n'a pas de racine dans le corps $\mathbf{F}_{25}$.

(2) Montrer que le polynôme $X^4 - X - 1$ est irréductible dans $\mathbf{F}_5[X]$.

Exercice 5.29. — Factoriser le polynôme $X^4 - 2X^2 + 9$ dans $\mathbf{R}[X]$, dans $\mathbf{Q}[X]$ et dans $\mathbf{F}_p[X]$ (où p est un nombre premier quelconque) (*Indication :* on pourra utiliser les identités

$$X^4 - 2X^2 + 9 = (X^4 - 2X^2 + 1) + 8 = (X^4 + 6X^2 + 9) - 8X^2 = (X^4 - 6X^2 + 9) + 4X^2$$

pour montrer que ce polynôme est réductible modulo tout p).

4. Voir exerc. I.11.1.