Olivier Debarre

ALGÈBRE 2

ÉCOLE NORMALE SUPÉRIEURE

2012–2013

Olivier Debarre

ALGÈBRE 2

ÉCOLE NORMALE SUPÉRIEURE

2012–2013

Olivier Debarre

TABLE DES MATIÈRES

CHAPITRE I

EXTENSIONS DE CORPS

1. Anneaux

Nous reviendrons au chapitre III plus longuement sur la théorie des anneaux. Nous nous contentons ici des quelques préliminaires nécessaires pour aborder la théorie des extensions de corps.

Tous nos anneaux sont commutatifs unitaires (mais il se peut que $1 = 0$; cela arrive si et seulement si l'anneau est nul !). Un morphisme (d'anneaux unitaires) $f : A \to B$ doit vérifier $f(1_A) = 1_B$.

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^*.

Un anneau A est *intègre* (« anneau intègre » se dit « integral domain », ou simplement « domain » en anglais) s'il est non nul et si le produit de deux éléments non nuls de A est encore non nul. C'est un *corps* s'il est non nul et si tout élément non nul de A admet un inverse.

Si un anneau A est intègre, on définit son *corps des quotients* (ou *corps des fractions*) K_A comme l'ensemble des « fractions » $\frac{a}{b}$, avec $a \in A$ et $b \in A - \{0\}$, modulo la relation d'équivalence

$$\frac{a}{b} \sim \frac{a'}{b'} \iff ab' = a'b.$$

Muni des opérations (addition et multiplication) habituelles sur les fractions, on vérifie que K_A est bien un corps.

Exercice 1.1. — Soit A un anneau.

a) Si A est intègre, montrer que l'anneau $A[X]$ des polynômes à une indéterminée à coefficients dans A est aussi intègre.

b) Si A est intègre, quelles sont les unités de $A[X]$?

b) Si A est quelconque, caractériser les unités de $A[X]$ (c'est difficile à faire directement ! Noter que $(2X + 1)^2 = 1$ dans $(Z/4\mathbf{Z})[X]$, donc $2X + 1$ est une unité dans cet anneau).

1.1. Idéaux. — Si A est un anneau, une partie $I \subseteq A$ est un *idéal* si c'est un sous-groupe additif et si, pour tout $a \in A$ et tout $b \in I$, on a $ab \in I$. 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.

Le noyau d'un morphisme d'anneaux $f : A \to B$ est un idéal de A noté $\mathrm{Ker}(f)$ (mais l'image de f n'est en général pas un idéal de B). Plus généralement, l'image réciproque par f d'un idéal de B est un idéal de A. Si I est un idéal de A, le morphisme f se factorise par la projection $A \to A/I$ si et seulement si $I \subseteq \mathrm{Ker}(f)$.

Exemple 1.2. — L'anneau A est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A.

Exemple 1.3. — Les idéaux de l'anneau $\mathbf{Z}$ sont les $I_n = n\mathbf{Z}$, avec $n \in \mathbf{N}$.

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 $s_i \in S$.

Soit I un idéal de l'anneau A. L'anneau A/I est intègre si et seulement si I est un *idéal premier,* c'est-à-dire qu'il est distinct de A et qu'il vérifie la propriété :

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

L'anneau A/I est un corps si et seulement si I est un *idéal maximal,* c'est-à-dire qu'il est distinct de A et que l'unique idéal de A contenant strictement I est A (en particulier, tout idéal maximal est évidemment premier). Il résulte du théorème de Zorn que tout idéal de A distinct de A est contenu dans un idéal maximal [1]. En particulier, tout anneau non nul possède un idéal maximal.

Exemple 1.4. — L'anneau A est un corps si et seulement si $\{0\}$ est un idéal maximal de A.

Exercice 1.5. — Soit A un anneau. Montrer l'égalité

$$\bigcup_{\mathfrak{m} \text{ idéal maximal de } A} \mathfrak{m} = A - A^*.$$

Exercice 1.6. — Soit $\mathscr{C}$ l'anneau des fonctions continues de $[0, 1]$ dans $\mathbf{R}$.

a) Montrer que les idéaux maximaux de $\mathscr{C}$ sont les

$$I_x = \{f \in \mathscr{C} \mid f(x) = 0\},$$

pour chaque $x \in [0, 1]$ (pour lesquels $\mathscr{C}/I_x \simeq \mathbf{R}$).

b) Montrer que tout idéal premier de $\mathscr{C}$ est contenu dans un unique idéal maximal de $\mathscr{C}$, et qu'il y est dense (pour la topologie de la convergence uniforme). Tout idéal premier fermé de $\mathscr{C}$ est donc maximal [2].

1.2. Divisibilité, éléments irréductibles. — Soit A un anneau intègre et soient a et b des éléments de A. On dit que a *divise* b, et on écrit $a \mid b$, s'il existe $q \in A$ tel que $b = aq$. En termes d'idéaux, c'est équivalent à $(a) \supseteq (b)$. En particulier, 0 ne divise que lui-même, et une unité divise tous les éléments de A.

On a ($a \mid b$ et $b \mid a$) si et seulement s'il existe $u \in A^*$ tel que $a = ub$. On dit alors que a et b sont *associés.*

Un élément de A est *irréductible* si a n'est pas inversible et que si $a = xy$, alors soit x, soit y est inversible. La seconde condition signifie que les seuls diviseurs de a sont ses associés et les unités de A.

Enfin, on dit que des éléments de A sont *premiers entre eux* si leurs seuls diviseurs communs sont les unités de A. Par exemple, si a est irréductible, tout élément de A est ou bien premier avec a, ou bien divisible par a.

Exemple 1.7. — Les éléments irréductibles de $\mathbf{Z}$ sont les $\pm p$, avec p nombre premier. Ceux de $\mathbf{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Soit a un élément non nul de A. Si l'idéal (a) est premier, a est irréductible, mais la réciproque est fausse en général, comme le montre l'ex. 1.9 ci-dessous.

1. Soit I un idéal de A distinct de A. L'ensemble des idéaux de A contenant I et distincts de A est inductif car si $(I_j)_{j \in J}$ est une famille totalement ordonnée d'idéaux de A distincts de A, la réunion $\bigcup_{j \in J} I_j$ est encore un idéal (parce que la famille est totalement ordonnée) distinct de A (parce qu'elle ne contient pas 1_A). On applique alors le lemme de Zorn.

2. En revanche, la description générale des idéaux premiers de $\mathscr{C}$ est un problème très difficile ! Même montrer qu'il existe des idéaux premiers non maximaux n'est pas évident (*cf.* exerc. III.3.4).

Exemple 1.8. — Si $n \geq 1$, l'anneau $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si 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 1.9. — 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 !

1.3. Anneaux principaux, anneaux euclidiens. — Un anneau A est *principal* (« principal ideal domain », ou « PID », en anglais) si A est intègre et que tout idéal de A est principal, c'est-à-dire qu'il peut être engendré par un élément. L'anneau $\mathbf{Z}$ est donc principal (ex. 1.3), mais pas l'anneau $\mathscr{C}$ de l'ex. 1.6, ni 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.

Dans la pratique, on montre souvent qu'un anneau intègre est principal en exhibant une *division euclidienne sur A,* c'est-à-dire une fonction $\varphi : A - \{0\} \to \mathbf{N}$ 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 $\varphi(r) < \varphi(b)$. Les deux exemples fondamentaux sont :

- l'anneau $\mathbf{Z}$ est euclidien pour la fonction $\varphi(n) = |n|$;
- si K est un corps, l'anneau $K[X]$ est euclidien pour la fonction $\varphi(P) = \deg(P)$.

Si on a une telle fonction φ, on montre qu'un idéal I non nul de A est engendré par tout élément x non nul de I pour lequel $\varphi(x)$ est minimal.

Exercice 1.10. — Si K est un corps, l'anneau des séries formelles $K[[X]]$ est euclidien. Ses idéaux sont $\{0\}$ et les $I_m = (X^m)$ pour chaque $m \in \mathbf{N}$.

Exercice 1.11. — L'anneau des nombres décimaux (c'est-à-dire les nombres rationnels dont le développement décimal est fini) est principal.

Exercice 1.12. — Montrer que les idéaux maximaux de l'anneau $\mathscr{C}$ des fonctions continues de $[0,1]$ dans $\mathbf{R}$ ne sont pas principaux (*cf.* exerc. 1.6 et III.2.16). Que se passe-t-il si l'on remplace $\mathscr{C}$ par l'anneau des fonctions continues de classe $\mathscr{C}^\infty$ de $[0,1]$ dans $\mathbf{R}$?

Exercice 1.13. — Soit A un anneau intègre dans lequel tout idéal premier est principal. Montrer que l'anneau A est principal (*Indication :* on pourra considérer un élément maximal I dans la famille des idéaux non principaux de A, des éléments x et y de $A - I$ tels que $xy \in I$, un générateur z de l'idéal $I + (x)$, un générateur w de l'idéal $\{a \in A \mid az \in I\}$, et montrer que zw engendre I).

Si a et b sont des éléments d'un anneau principal A, l'idéal (a,b) 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 » ; « gcd », ou « greatest common divisor », en anglais) de a et b, parfois noté $a \wedge b$. De même, l'idéal $(a) \cap (b)$ est engendré par un élément de A, uniquement déterminé à multiplication par un élément inversible de A près, le *ppcm* (« plus grand commun multiple » ; « lcm », ou « least common multiple », en anglais) de a et b, parfois noté $a \vee b$. Dans ce contexte, le « théorème de Bézout », qui dit que a et b sont premiers entre eux si et seulement s'il existe x et y dans A tels que

$$xa + yb = 1$$

est une tautologie. Mentionnons comme conséquence un résultat classique (nous reviendrons sur ces questions dans le § III.1).

***Lemme 1.14* (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.*

Démonstration. — Écrivons $bc = ad$ et $xa + yb = 1$. On a alors $c = (xa + yb)c = xac + yad$, qui est bien divisible par a. □

Dans un anneau principal A, les équivalences de l'ex. 1.8 restent vraies.

Proposition 1.15. — *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) *a est irréductible ;*

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

En particulier, l'anneau $\mathbf{Z}[i\sqrt{5}]$ de l'ex. 1.9 n'est pas principal.

Démonstration. — On sait qu'en général (iii) ⇒ (i) ⇒ (ii). Supposons a irréductible et soit 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 $I = (a)$. Comme a n'est pas inversible, on a $(a) \neq A$, donc l'idéal (a) est maximal. □

Nous montrerons plus tard (cor. III.2.6) de façon indépendante que tout anneau principal est *factoriel*, c'est-à-dire que tout élément non nul s'écrit de façon unique comme produit d'irréductibles. Comme nous aurons besoin dans le chapitre suivant de ce résultat dans le cas particulier de l'anneau principal $K[X]$, où K est un corps, nous donnons ici une démonstration *ad hoc.*

Théorème 1.16. — *Soit K un corps. Tout élément non nul P de $K[X]$ admet une décomposition*

$$P = u \prod_{i=1}^{m} P_i^{r_i}$$

avec $u \in K^*$ et $m \geq 0$, où les polynômes $P_1, \ldots, P_m$ sont irréductibles unitaires, distincts deux à deux.

Cette décomposition est unique au sens suivant : si $P = v \prod_{i=1}^{n} Q_i^{s_i}$ est une autre telle décomposition, on a $m = n$ et il existe une permutation $\sigma \in \mathfrak{S}_m$ telle que $Q_i = P_{\sigma(i)}$ et $s_i = r_{\sigma(i)}$ pour tout $i \in \{1, \ldots, m\}$.

Démonstration. — On procède par récurrence sur le degré de P, les assertions étant claires lorsque celui-ci vaut 0.

Supposons donc P de degré ≥ 1 et montrons d'abord l'existence d'une décomposition. Si P est irréductible de coefficient directeur u, on écrit simplement $P = u(P/u)$. Sinon, il existe une décomposition $P = QR$ où Q et R sont non constants et on applique l'hypothèse de récurrence à Q et R.

C'est l'unicité qui est le point important. Comme Q_1 est irréductible, le lemme de Gauss (lemme 1.14) entraîne que Q_1 divise l'un des P_i, que l'on note $P_{\sigma(1)}$. Comme ce dernier est irréductible et que ces deux polynômes sont unitaires, ils sont égaux. Il suffit maintenant d'appliquer l'hypothèse de récurrence à $P/Q_1 = P/P_{\sigma(1)}$. □

2. Corps

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 $K \subseteq L$.

L'intersection d'une famille quelconque de sous-anneaux de L est encore un sous-anneau de L. Si A est une partie de L, l'intersection de tous les sous-anneaux de L contenant K et A est donc un sous-anneau de L que l'on notera $K[A]$; c'est une K-algèbre intègre appelée *sous-anneau de L engendré par A.*

De même, l'intersection d'une famille quelconque de sous-corps de L est encore un sous-corps de L. Il existe donc un plus petit sous-corps de L contenant K et A, que l'on appelle le *sous-corps de L engendré par A,* noté $K(A)$; c'est le corps des fractions de $K[A]$. On dit qu'une extension $K \hookrightarrow L$ est *de type fini* s'il existe une partie finie $A \subseteq L$ telle que $L = K(A)$.

2.1. 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 plus habituellement $\mathbf{F}_p$) ; 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 [3]

$$\forall x, y \in K \qquad (x+y)^p = x^p + y^p. \tag{1}$$

Autrement dit, l'application de Frobenius

$$\begin{aligned} \mathrm{Fr}_K : K &\longrightarrow K \\ x &\longmapsto x^p \end{aligned}$$

est un morphisme de corps (injectif). On note K^p son image.

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

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

Il a au plus n éléments. Un élément ζ de $\mu_n(K)$ est dit *racine primitive n-ième de l'unité* si $\zeta^d \neq 1$ pour tout $d \in \{1, \ldots, n-1\}$; 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 dans K,* elle engendre le groupe $\mu_n(K)$, qui est alors isomorphe à $\mathbf{Z}/n\mathbf{Z}$. Il y a alors

$$\varphi(n) := \mathrm{Card}((\mathbf{Z}/n\mathbf{Z})^*) = \mathrm{Card}\{d \in \{1, \ldots, n-1\} \mid d \wedge n = 1\}.$$

différentes racines primitives n-ièmes de l'unité.

Exercice 2.1. — Soit K un corps de caractéristique $p > 0$ et soit r un entier ≥ 1. Quels sont les groupes $\mu_{p^r}(K)$?

Proposition 2.2. — *Pour tout corps K et tout entier $n \geq 1$, le groupe $\mu_n(K)$ est cyclique d'ordre un diviseur de n. Plus généralement, tout sous-groupe fini de $(K^*, \times)$ est cyclique.*

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

3. 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).

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

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

on a donc $m \leq \sum_{d|m\wedge n} \varphi(d)$. On vérifie (exercice !) que pour tout entier $e \geq 1$, on a $\sum_{d|e} \varphi(d) = e$. On en déduit $m \leq m \wedge n$, donc $m \mid n$, et $P_m \neq \varnothing$. Il existe donc un élément d'ordre m dans $\mu_n(K)$, qui est ainsi cyclique. Ceci montre le premier point.

Si G est un sous-groupe de $(K^*, \times)$ 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. Extensions de corps. — Le *degré* d'une extension de corps $K \hookrightarrow L$ est la dimension du K-espace vectoriel L, notée $[L : K]$. L'extension est dite *finie* si ce degré l'est.

Exemple 2.3. — On a $[\mathbf{C} : \mathbf{R}] = 2$, $[\mathbf{C} : \mathbf{Q}] = \infty$ et $[K(X) : K] = \infty$ [4].

Théorème 2.4. — *Soient $K \hookrightarrow L$ et $L \hookrightarrow M$ des extensions de corps. On a*

$$[M : K] = [M : L][L : K].$$

En particulier, l'extension $K \hookrightarrow M$ est finie si et seulement si les extensions $K \hookrightarrow L$ et $L \hookrightarrow M$ 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. □

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

2.4. Éléments algébriques et transcendants. —

Définition 2.5. — Soit $K \hookrightarrow L$ 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 $K \hookrightarrow L$ est dite *algébrique* si tous les éléments de L sont algébriques sur K.

Exemple 2.6. — Le corps $\mathbf{C}$ est une extension algébrique de $\mathbf{R}$. Le réel $\sqrt{2}$ est algébrique sur $\mathbf{Q}$. L'ensemble des réels algébriques sur $\mathbf{Q}$ est dénombrable : il existe donc des nombres réels transcendants sur $\mathbf{Q}$ (on dit souvent simplement « transcendants »). Le nombre réel $\sum_{n\geq 0} 10^{-n!}$ est transcendant (Liouville, 1844), ainsi que π (Lindemann, 1882).

Soit $K \hookrightarrow L$ une extension de corps et soit $x \in L$. Le sous-anneau $K[x]$ de L engendré par x est l'image du morphisme de K-algèbres

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

Théorème 2.7. — *Soit $K \hookrightarrow L$ 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 $K \hookrightarrow K(x)$ est infinie.*

b) *Si x est algébrique sur K, il existe un unique polynôme unitaire P de degré minimal vérifiant $P(x) = 0$. Ce polynôme est irréductible, on a $K[x] = K(x)$ et cette extension de K est finie de degré* $\deg(P)$. *On appelle P le* polynôme minimal *de x sur K.*

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 (§ 1.3), 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 $K[X]/(P)$ (§ 1.1). 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 que l'anneau $K[X]/(P)$ est un corps (prop. 1.15) et il en est de même pour $K[x]$. Enfin, les K-espaces vectoriels $K[x]$ et $K[X]/(P)$ sont aussi isomorphes, et on vérifie que ce dernier admet comme base les classes de $1, X, \ldots, X^{d-1}$, où $d = \deg(P)$. Ils sont donc de dimension d. □

Exemple 2.8. — 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.

Exercice 2.9. — Soit $K \hookrightarrow L$ une extension de corps. Montrer qu'un élément x de L est algébrique sur K si et seulement si l'anneau $K[x]$ est un corps.

Attention ! La réciproque est fausse (*cf.* ex. 2.15).

Corollaire 2.10. — *Toute extension finie de corps est algébrique.*

Démonstration. — Soit $K \hookrightarrow L$ une extension finie de corps et soit $x \in L$. Le K-espace vectoriel $K[x]$ est contenu dans L, donc est de dimension finie. Le th. 2.7 entraîne que x est algébrique sur K. □

Corollaire 2.11. — *Toute extension $K \hookrightarrow L$ engendrée par un nombre fini d'éléments algébriques sur K est finie, donc algébrique. En particulier, toute extension de corps algébrique et de type fini est finie.*

Démonstration. — On procède par récurrence sur le cardinal d'une partie finie $A \subseteq L$ telle que $L = K(A)$.

Si A est vide, c'est évident. Sinon, on prend $x \in A$ et l'on pose $L' = K(A - \{x\})$. L'hypothèse de récurrence entraîne que l'extension $K \hookrightarrow L'$ est finie. Comme x est algébrique sur K, il l'est sur L', donc $L' \hookrightarrow L$ est finie par le th. 2.7. Le corollaire résulte alors du th. 2.4 (et du cor. 2.10). □

Théorème 2.12. — *Soit $K \hookrightarrow L$ une extension de corps. L'ensemble des éléments de L algébriques sur K est un sous-corps de L contenant K appelé* clôture algébrique de K dans L. *C'est une extension algébrique de K.*

Attention à ne pas confondre cette notion avec celle de clôture algébrique de K, qui sera définie dans le § 3.3. Sous les hypothèses du théorème, on dit que K *est algébriquement clos dans* L si sa clôture algébrique dans L est K (attention à ne pas confondre avec la définition de corps algébriquement clos (tout court) donnée dans la déf. 3.9).

Démonstration. — Soient x et y des éléments non nuls de L algébriques sur K. Le cor. 2.11 entraîne que l'extension $K \hookrightarrow K(x, y)$ est finie, donc algébrique. Les éléments $x - y$ et x/y de L sont donc algébriques sur K. □

Corollaire 2.13. — *Toute extension $K \hookrightarrow L$ engendrée par des éléments algébriques sur K est algébrique.*

Démonstration. — Soit $A \subseteq L$ un ensemble d'éléments de L algébriques sur K et engendrant L. La clôture algébrique de K dans L contient A, donc c'est L, qui est donc une extension algébrique de K par le théorème. □

Exemple 2.14. — 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 2.15. — Le corps $\bar{\mathbf{Q}} \subseteq \mathbf{C}$ des nombres algébriques (sur $\mathbf{Q}$) est une extension algébrique de $\mathbf{Q}$. Elle n'est pas finie (parce que, comme on le verra plus tard, par exemple dans l'exerc. III.1.13, il existe des polynômes irréductibles dans $\mathbf{Q}[X]$ de degré arbitrairement grand).

Théorème 2.16. — *Soient $K \hookrightarrow L$ et $L \hookrightarrow M$ 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 $K \hookrightarrow L$ est algébrique, l'extension $L' \subseteq L$ de K engendrée par les coefficients de P est alors finie (cor. 2.11). Comme x est algébrique sur L', l'extension $L' \hookrightarrow L'(x)$ est finie (th. 2.7). Le th. 2.4 entraîne que l'extension $K \hookrightarrow L'(x)$ est finie, donc algébrique (cor. 2.10), et x est algébrique sur K. □

Soit $K \hookrightarrow L$ une extension de corps et soient $x_1, \ldots, x_n$ des éléments de L. On montrera plus tard (th. III.10.2) que l'extension $K \hookrightarrow K(x_1, \ldots, x_n)$ est algébrique si et seulement si l'anneau $K[x_1, \ldots, x_n]$ est un corps (cela généralise l'exerc. 2.9, mais c'est bien plus difficile !).

Remarque 2.17. — Si $K \hookrightarrow L$ et $L \hookrightarrow M$ sont des extensions de corps, on a donc (th. 2.4 et th. 2.16)

$$K \hookrightarrow L \text{ et } L \hookrightarrow M \text{ finies} \iff K \hookrightarrow M \text{ finie},$$
$$K \hookrightarrow L \text{ et } L \hookrightarrow M \text{ algébriques} \iff K \hookrightarrow M \text{ algébrique}.$$

L'équivalence

$$K \hookrightarrow L \text{ et } L \hookrightarrow M \text{ de type fini} \iff K \hookrightarrow M \text{ de type fini}$$

est aussi vraie, mais plus difficile à montrer (*cf.* exerc. III.12.3).

Exercice 2.18. — 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 $K_1 \cap K_2 \subseteq K$.

2.5. Constructions à la règle et au compas. —

Définition 2.19. — 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, chacun de rayon joignant deux points distincts déjà construits.

Exercice 2.20. — 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. Montrer que la perpendiculaire et la parallèle à une droite constructible passant par un point constructible sont constructibles. Montrer que le cercle de centre un point constructible et de rayon la distance entre deux points constructibles est constructible.

Exercice 2.21. — Soit K un corps de caractéristique 3. Montrer que les médianes de tout triangle dans K^2 sont parallèles.

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. Par l'exerc. 2.20, cela revient au même de dire que le point $(x, 0)$ est constructible à partir de $\Sigma \times \{0\}$.

Théorème 2.22. — *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. La multiplication et l'inverse s'obtiennent à partir du théorème de Thalès et la racine carrée à partir de celui de Pythagore. □

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 2.23* (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 2.24. — *Soit K un corps de caractéristique différente de 2 et soit $K \hookrightarrow L$ une extension de degré 2. Il existe $x \in L - K$ tel que $x^2 \in K$ et $L = K[x]$.*

On remarquera que l'extension $\mathbf{Z}/2\mathbf{Z} \hookrightarrow (\mathbf{Z}/2\mathbf{Z})[X]/(X^2 + X + 1)$, de degré 2 entre corps de caractéristique 2, ne peut être engendrée par un élément dont le carré est dans $\mathbf{Z}/2\mathbf{Z}$.

Démonstration. — Si $y \in L - K$, 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 l'un 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 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 2.24). Mais alors $x = \pm\sqrt{x^2}$ est constructible à partir de L (th. 2.22). □

Corollaire 2.25. — *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.*

Attention, la réciproque est fausse telle quelle (exerc. 2.28) ; *cf.* th. 8.4 pour une caractérisation des nombres constructibles.

Démonstration. — Si x est un réel constructible, il est dans une extension K_n du type décrit dans le théorème de Wantzel (th. 2.23), pour laquelle $[K_n : K] = 2^n$ (th. 2.4). 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. 2.4). □

Corollaire 2.26 **(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 exerc. 2.27).

Le degré de $\sqrt[3]{2}$ sur $\mathbf{Q}$ est donc 3 : il n'est donc pas constructible par cor. 2.25. □

Exercice 2.27. — Si le polynôme $a_nX^n + \cdots + a_1X + a_0 \in \mathbf{Z}[X]$, 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 2.28. — Considérons le polynôme $P(X) = X^4 - X - 1 \in \mathbf{Q}[X]$.

a) Montrer que P a exactement deux racines réelles distinctes x_1 et x_2.
b) On écrit $(X - x_1)(X - x_2) = X^2 + aX + b$ avec $a, b \in \mathbf{R}$. Montrer $[\mathbf{Q}(a^2) : \mathbf{Q}] = 3$.
c) Montrer que x_1 et x_2 ne peuvent être tous les deux constructibles (en fait, aucun des deux ne l'est ; *cf.* exerc. 8.5).

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 2.29 **(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 $\pi/9$ 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 $\mathbf{Q}(\cos\theta)$, le réel $\cos\theta/3$ est de degré 3 sur ce corps et ne peut y être constructible par cor. 2.25.

Si P est réductible sur $\mathbf{Q}(\cos\theta)$, étant de degré 3, il doit avoir une racine dans ce corps et se factorise 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 2.24 et th. 2.23). Comme $2P(X/2) = X^3 - 3X - 2\cos\theta$, cela montre la première partie de l'énoncé.

On a $\mathbf{Q}(\cos\pi/3) = \mathbf{Q}$, donc l'angle $\pi/9$ 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. 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 (Exemple 2.6), donc aussi $\sqrt{\pi}$. □

3. Polynômes et racines

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 K dans laquelle P aura une racine, ou même, sera *scindé* (produit de facteurs du premier degré).

3.1. Corps de rupture. — Les unités de l'anneau $K[X]$ sont les polynômes constants non nuls (c'est-à-dire les éléments de K^*).

Soit $P \in K[X]$ un polynôme irréductible. L'anneau $K[X]$ étant principal, l'anneau quotient $K_P := K[X]/(P)$ est un corps (prop. 1.15). Soit $x_P \in K_P$ l'image de X dans K_P. On a alors $P(x_P) = 0$, de sorte que l'on a construit une extension K_P de K dans laquelle P a une racine, x_P ; de plus, $K_P = K[x_P]$. On appelle K_P un *corps de rupture* de P.

Exemple 3.1. — 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. 1.7).

Exemple 3.2. — 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.

Définition 3.3. — *Soient $\iota : K \hookrightarrow L$ et $\iota' : K \hookrightarrow L'$ des extensions de corps. On appelle* K-morphisme de L dans L' *un morphisme de corps $\sigma : L \hookrightarrow L'$ qui est l'identité sur K, c'est-à-dire qui vérifie $\sigma \circ \iota = \iota'$.*

Proposition 3.4. — *Soit $P \in K[X]$ un polynôme irréductible. Pour toute extension $K \hookrightarrow L$ 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 s'annule en P, donc définit par passage au quotient l'unique K-morphisme de K_P vers L qui envoie x_P sur x. □

Corollaire 3.5. — *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 $K \hookrightarrow L$ et $K \hookrightarrow L'$ de P, et des racines $x \in L$ et $x' \in L'$ de P, il existe un unique K-isomorphisme $\sigma : L \xrightarrow{\sim} L'$ 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 3.6. — *Soit K un corps et soit $P \in K[X]$.*

a) *Il existe une extension $K \hookrightarrow L$ 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 isomorphes.*

Une telle extension s'appelle un *corps de décomposition* de P (« splitting field » en anglais). C'est une extension algébrique de type fini, donc finie de K (cor. 2.11).

Démonstration. — On procède par récurrence sur le degré d de P. Si $d = 1$, le corps $L = K$ est le seul qui convient.

Si $d > 1$, soit Q un facteur irréductible de P dans $K[X]$ (*cf.* th. 1.16) 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 $K_Q \hookrightarrow L$ 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 $K \hookrightarrow L$ et $K \hookrightarrow L'$ des corps de décomposition de P, et soient x une racine de Q 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. 3.5) 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 $K(x) \xrightarrow{\sim} K(x') \hookrightarrow L'$.

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

Exemple 3.8. — Le corps $\mathbf{Q}(\sqrt[3]{2}, j)$ est un corps de décomposition pour le polynôme $X^3 - 2 \in \mathbf{Q}[X]$.

3.3. Clôture algébrique. —

Définition 3.9. — 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 $K \hookrightarrow \Omega$ telle que Ω est un corps algébriquement clos.

Exemple 3.10. — Le corps $\mathbf{C}$ est algébriquement clos. C'est une clôture algébrique de $\mathbf{R}$, mais pas de $\mathbf{Q}$.

Exercice 3.11. — Montrer que tout corps algébriquement clos est infini.

Proposition 3.12. — *Soit $K \hookrightarrow L$ 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 (exerc. 5.26).

Démonstration. — Soit $Q \in L[X]$ un polynôme irréductible et soit x une racine de Q dans une extension de L. Alors x est algébrique sur L donc sur K (th. 2.16). Soit $P \in K[X]$ son polynôme minimal ; puisque Q est irréductible sur L, on a $Q \mid P$ dans $L[X]$. Mais par hypothèse, 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. 1.16), on a montré que L est 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 3.13. — *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.*

En d'autres termes (*cf.* th. 2.12), la clôture algébrique d'un corps dans une extension algébriquement close est une clôture algébrique (tout court) !

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. 2.12), 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. 2.16), de sorte que $x \in \bar{K}$. □

Exemple 3.14. — Le corps $\bar{\mathbf{Q}} \subseteq \mathbf{C}$ des nombres algébriques (*cf.* ex. 2.15) est une clôture algébrique de $\mathbf{Q}$. C'est un corps dénombrable (pourquoi ?).

Théorème 3.15 **(Steinitz, 1910)**. — *Soit K un corps. Il existe une clôture algébrique de K. Deux clôtures algébriques de K sont K-isomorphes.*

Démonstration. — Nous donnerons, un fois n'est pas coutume, deux démonstrations de l'existence d'une clôture algébrique. La première suppose que K est dénombrable, mais elle est plus transparente. La seconde est générale, mais un peu obscure.

Supposons donc tout d'abord le corps K (au plus) dénombrable. 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 $K \hookrightarrow L$ 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. 3.12.

Donnons maintenant une démonstration dans le cas général. On considère tout d'abord la K-algèbre de polynômes à beaucoup d'indéterminées $A := K[X_{P,i}]$, où P parcourt l'ensemble $\mathscr{P}$ de tous les polynômes unitaires de $K[X]$ et $0 \leq i \leq \deg(P)$. Pour $P \in \mathscr{P}$ de degré n, on note $a_{P,0}, \ldots, a_{P,n} \in A$ les coefficients du polynôme

$$P(X) - \prod_{i=1}^{n}(X - X_{P,i}) \in A[X].$$

Soit I l'idéal de A engendré par tous les $a_{P,i}$ lorsque P décrit $\mathscr{P}$ et $0 \leq i \leq \deg(P)$. Montrons $I \neq A$. Dans le cas contraire, on a une relation

$$1 = a_{P_1,i_1}b_1 + \cdots + a_{P_r,i_r}b_r, \tag{2}$$

avec $b_1, \ldots, b_r \in A$ et $P_1, \ldots, P_r \in \mathscr{P}$. Soit $K \subseteq K'$ une extension de corps dans laquelle chaque polynôme P_j est scindé, de racines $(x_{j,i})_{1\leq i\leq \deg(P_j)}$ dans K'. On définit un morphisme de K-algèbres $\varphi : A \to K'$ en envoyant chaque $X_{P_j,i}$ sur $x_{j,i}$, pour $j \in \{1, \ldots, r\}$ et $0 \leq i \leq \deg(P_j)$, et les autres indéterminées sur 0. Le morphisme φ induit un morphisme $\Phi : A[X] \to K'[X]$ qui envoie chaque

$$P_j(X) - \prod_{i=1}^{\deg(P_j)} (X - X_{P_j,i})$$

sur

$$P_j(X) - \prod_{i=1}^{\deg(P_j)} (X - x_{j,i}) = 0.$$

de sorte que $\varphi(a_{P_j,i}) = 0$ pour $0 \leq i \leq \deg(P_j)$. En prenant l'image de la relation (2) par φ, on obtient la contradiction $1 = 0$.

Soit donc $\mathfrak{m}$ un idéal maximal de A contenant I. Montrons que $L := A/\mathfrak{m}$ est une extension algébrique de K. Soit $P \in \mathscr{P}$ de degré $n \geq 0$. Notons $\bar{X}_{P,i}$ la classe de $X_{P,i}$ dans L. Les coefficients du polynôme

$$P(X) - \prod_{i=1}^{n}(X - X_{P,i})$$

sont par définition dans I, donc

$$P(X) = \prod_{i=1}^{n}(X - \bar{X}_{P,i})$$

dans $L[X]$. Ceci montre d'une part que tous les $\bar{X}_{P,i}$ sont algébriques sur K ; comme ils engendrent L, l'extension $K \hookrightarrow L$ est algébrique (cor. 2.13). D'autre part, tout polynôme unitaire de $K[X]$ est scindé dans L, donc L est une clôture algébrique de K par la prop. 3.12.

Pour montrer l'unicité, commençons par montrer deux lemmes fondamentaux qui nous serviront de nouveau dans le § 5.3.

Lemme 3.16. — *Soit $K \hookrightarrow L$ une extension de corps telle que L est engendré par un élément x algébrique sur K, de polynôme minimal $P \in K[X]$. Toute extension $K \hookrightarrow \Omega$, où Ω est un corps algébriquement clos, se prolonge en*[5] *$L \hookrightarrow \Omega$ et le nombre de ces extensions est égal au nombre de racines distinctes de P dans son corps de décomposition.*

Démonstration. — On a $L \simeq K[X]/(P)$, de sorte que se donner un K-morphisme σ de L dans Ω est équivalent à se donner un élément $\sigma(x)$ de Ω qui vérifie $P(\sigma(x)) = 0$. Il y a donc exactement autant de tels morphismes que de racines de P dans Ω, ou encore dans le sous-corps de Ω que ces racines engendrent ; ce sous-corps est un corps de décomposition de P, ce qui montre le lemme. □

Lemme 3.17. — *Soit $K \hookrightarrow L$ une extension algébrique de corps. Toute extension $K \hookrightarrow \Omega$, où Ω est un corps algébriquement clos, se prolonge en $L \hookrightarrow \Omega$.*

Démonstration. — Lorsque l'extension $K \hookrightarrow L$ est *finie,* cela résulte immédiatement du lemme précédent : il suffit de l'écrire comme une suite d'extensions emboîtées

$$K \hookrightarrow K(x_1) \hookrightarrow K(x_1, x_2) \hookrightarrow \cdots \hookrightarrow K(x_1, \ldots, x_n) = L$$

et d'appliquer le lemme à chaque extension.

Dans le cas général, il faut appliquer le lemme de Zorn : on considère l'ensemble non vide $\mathscr{E}$ des paires (M, σ), où M est un sous-corps de L contenant K et $\sigma : M \hookrightarrow \Omega$ une extension de $\iota : K \hookrightarrow \Omega$ à M. Il est partiellement ordonné par la relation

$$(M, \sigma) \leq (M', \sigma') \;\Leftrightarrow\; (M \subseteq M' \text{ et } \sigma'|_M = \sigma).$$

Si $(M_i, \sigma_i)_{i \in I}$ est un sous-ensemble totalement ordonné de $\mathscr{E}$, la réunion $M := \bigcup_{i \in I} M_i$ est un sous-corps de L et on définit uniquement $\sigma : M \to \Omega$ par $\sigma|_{M_i} = \sigma_i$. La paire (M, σ) est alors dans $\mathscr{E}$ et c'est un majorant de la famille $(M_i, \sigma_i)_{i \in I}$. Il existe donc un élément maximal (M_0, σ_0).

Puisque L est une extension algébrique de K, tout élément x de L est algébrique sur K, donc *a fortiori* sur M_0. Le lemme précédent dit que l'on peut alors étendre σ_0 en $M_0(x) \hookrightarrow \Omega$. Par maximalité de (M_0, σ_0), cela entraîne $M_0(x) = M_0$, c'est-à-dire $x \in M_0$. On a donc $L = M_0$, ce qui prouve le lemme. □

Terminons maintenant la preuve du th. 3.15. Si $\iota : K \hookrightarrow \Omega$ et $\iota' : K \hookrightarrow \Omega'$ sont des clôtures algébriques, ι' se prolonge par le lemme 3.17 en $\sigma : \Omega \hookrightarrow \Omega'$. Comme Ω est algébriquement clos, il en est de même pour $\sigma(\Omega)$. Mais Ω' est une extension algébrique de $\sigma(\Omega)$, donc $\sigma(\Omega) = \Omega'$. Les extensions $K \hookrightarrow \Omega$ et $K \hookrightarrow \Omega'$ sont donc isomorphes. □

Exercice 3.18. — Écrire la preuve de la partie existence du th. 3.15 dans le cas général.

4. Extensions normales

Rappelons que le polynôme irréductible $X^3 - 2 \in \mathbf{Q}[X]$ a une racine dans l'extension $\mathbf{Q}(\sqrt[3]{2})$, mais n'y est pas scindé.

Définition 4.1. — *On dit qu'une extension algébrique $K \hookrightarrow L$ est* normale *si tout polynôme irréductible dans $K[X]$ qui a une racine dans L est scindé dans L.*

5. Cela siginifie que si $\iota : K \hookrightarrow \Omega$ et $\alpha : K \hookrightarrow L$ sont les extensions données, il existe $\sigma : L \hookrightarrow \Omega$ tel que $\sigma \circ \alpha = \iota$.

Les extensions $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[n]{2})$ ne sont donc pas normales pour $n \geq 3$, mais $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2}, j)$ l'est (à cause du théorème ci-dessous). L'extension d'un corps dans une clôture algébrique est toujours normale, puisque tout polynôme y est scindé.

Théorème 4.2. — *Soit $K \hookrightarrow L$ une extension de corps. Les propriétés suivantes sont équivalentes :*

(i) *l'extension $K \hookrightarrow L$ est finie et normale ;*

(ii) *L est le corps de décomposition d'un polynôme à coefficients dans K.*

Démonstration. — Soit $K \hookrightarrow L$ une extension finie et normale, soit $(x_1, \ldots, x_d)$ une base du K-espace vectoriel L, et soit $P_i \in K[X]$ le polynôme minimal de x_i. Comme $K \hookrightarrow L$ est normale, chaque P_i est scindé dans L, donc aussi $Q := P_1 \cdots P_d$. Comme L est engendré sur K par les x_i, qui sont des racines de Q, le corps L est un corps de décomposition de $Q \in K[X]$.

Soit maintenant L le corps de décomposition d'un polynôme $Q \in K[X]$. C'est une extension finie de K. Soit $P \in K[X]$ un polynôme irréductible qui a une racine x_1 dans L, soit $L \hookrightarrow M$ un corps de décomposition de P, et soit x_2 une racine de P dans M. Il suffit de montrer $x_2 \in L$, puisque cela entraînera que toutes les racines de P dans M sont en fait dans L, donc que P est déjà scindé dans L.

Or, pour chaque $i \in \{1, 2\}$, $L(x_i)$ est un corps de décomposition de Q sur $K(x_i)$. D'autre part, chaque $K(x_i)$ est un corps de rupture de P sur K, donc (cor. 3.5) il existe un K-isomorphisme $\sigma : K(x_1) \xrightarrow{\sim} K(x_2)$. Les extensions $K(x_1) \hookrightarrow L(x_1) = L$ et $K(x_1) \xrightarrow{\sigma} K(x_2) \hookrightarrow L(x_2)$ sont alors des corps de décomposition de Q sur $K(x_1)$. Elles sont donc $K(x_1)$-isomorphes (th. 3.6), de sorte que $[L : K(x_1)] = [L(x_2) : K(x_1)]$, puis $[L : K] = [L(x_2) : K]$ (th. 2.4). On en déduit $L = L(x_2)$, donc $x_2 \in L$. □

Remarque 4.3. — Si $K \hookrightarrow M$ est une extension finie et normale de corps et que L est un corps intermédiaire entre K et M, le théorème entraîne que l'extension de corps $L \hookrightarrow M$ est encore normale. En revanche, ce n'est pas nécessairement le cas pour l'extension $K \hookrightarrow L$, comme le montre l'exemple $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2}) \subseteq \mathbf{Q}(\sqrt[3]{2}, j)$.

De plus, la composée de deux extensions normales $K \hookrightarrow L$ et $L \hookrightarrow M$ n'est pas nécessairement normale, comme le montre l'exemple $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\sqrt[4]{2})$.

Corollaire 4.4. — *Soit $K \hookrightarrow L$ une extension finie de corps et soit Ω un corps algébriquement clos contenant K. L'extension $K \hookrightarrow L$ est normale si et seulement si tous les K-morphismes de L dans Ω la même image.*

En particulier, si Ω est un corps algébriquement clos contenant L, l'extension finie $K \hookrightarrow L$ est normale si et seulement si tous les K-morphismes de L dans Ω sont d'image L.

Démonstration. — Si l'extension $K \hookrightarrow L$ est normale, L est le corps de décomposition d'un polynôme $Q \in K[X]$ par le th. 4.2. Pour tout K-morphisme $\sigma : L \to \Omega$, l'image de σ est l'extension de K engendrée par les racines de Q dans Ω, donc ne dépend pas de σ.

Inversement, supposons que tous les K-morphismes de L dans Ω ont la même image, que l'on note $L' \subseteq \Omega$. Soit $Q \in K[X]$ un polynôme irréductible avec une racine $x \in L$ et soit y une racine de Q dans Ω. Les corps $K(x) \subseteq L$ et $K(y) \subseteq \Omega$ sont des corps de rupture de Q, donc sont K-isomorphes (cor. 3.5). On en déduit un K-morphisme $K(x) \to K(y) \subseteq \Omega$ que l'on peut étendre en un K-morphisme $L \to \Omega$ (lemme 3.17) dont l'image est L'. On en déduit que y est dans L'. Le polynôme Q est donc scindé dans L', donc l'extension $K \hookrightarrow L'$ est normale, ainsi que l'extension $K \hookrightarrow L$ puisqu'elle lui est isomorphe. □

Corollaire 4.5. — *Soit $K \hookrightarrow L$ une extension finie et normale de corps. Tout automorphisme du corps K se prolonge en un automorphisme du corps L.*

Démonstration. — Soit $\sigma : K \xrightarrow{\sim} K$ un automorphisme du corps K et soit Ω un corps algébriquement clos contenant L (th. 3.15). Par le lemme 3.17, l'extension $K \xrightarrow{\sigma} K \hookrightarrow L \subseteq \Omega$ se prolonge à $K \hookrightarrow L$, et par le corollaire précédent, l'image de cette extension $L \hookrightarrow \Omega$ est L. On obtient ainsi un automorphisme du corps L qui prolonge σ. □

Proposition 4.6. — *Soit $K \hookrightarrow L$ une extension finie de corps et soit Ω un corps algébriquement clos contenant L. Il existe une plus petite extension M de L dans Ω telle que l'extension $K \hookrightarrow M$ soit normale.*

On appelle cette extension la *clôture normale* de L dans Ω ; elle est finie sur K.

Démonstration. — Comme dans la preuve précédente, soit $(x_1, \dots, x_d)$ une base du K-espace vectoriel L, et soit $P_i \in K[X]$ le polynôme minimal de x_i. Soit $M \subseteq \Omega$ le sous-corps engendré par les racines de $Q := P_1 \cdots P_d$ dans Ω. C'est un corps de décomposition du polynôme Q, donc l'extension $K \hookrightarrow M$ est finie et normale.

De plus, pour tout corps $L \subseteq M' \subseteq \Omega$ tel que l'extension $K \hookrightarrow M'$ est normale, le polynôme irréductible P_i a une racine dans M' (à savoir x_i), donc y est scindé (déf. 4.1), donc aussi Q. On en déduit que M, qui est engendré par les racines de Q, est contenu dans M'. □

Exercice 4.7. — Soient K et K' des sous-corps d'un corps L tels que l'extension $K \cap K' \subseteq L$ soit algébrique. On suppose que les extensions $K \subseteq L$ et $K' \subseteq L$ sont normales. Montrer que l'extension $K \cap K' \subseteq L$ est aussi normale.

5. Séparabilité

5.1. Polynômes séparables. —

Définition 5.1. — *On dit qu'un polynôme $P \in K[X]$ est* séparable *s'il n'a aucune racine multiple dans son corps de décomposition. Dans le cas contraire, on dit que P est* inséparable.

Lemme 5.2. — *Un polynôme P est séparable si et seulement si P et P' sont premiers entre eux.*

Démonstration. — Remarquons que le pgcd de P et P' est le même dans K ou dans toute extension de K (utiliser l'algorithme d'Euclide), en particulier dans un corps de décomposition L de P. Dans L, ce pgcd vaut 1 si et seulement si aucune racine de P n'est multiple. □

Lemme 5.3. — *Un polynôme* irréductible $P \in K[X]$ *est séparable si et seulement si $P' \neq 0$. Il est inséparable si et seulement si la caractéristique p de K est non nulle et $P \in K[X^p]$.*

Démonstration. — La premier énoncé résulte du lemme précédent : P est inséparable si et seulement si $P \wedge P'$ est un polynôme non constant, qui divise P, ce qui entraîne que c'est P (puisque P est irréductible) puis que P divise P', puis que P' est nul car il est sinon de degré $< \deg(P)$.

Écrivons

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

Le polynôme

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

est nul si et seulement si $a_i = 0$ pour chaque i non divisible par p. □

Lemme 5.4. — *Supposons K de caractéristique $p > 0$. Si $a \in K - K^p$, le polynôme $X^p - a$ est irréductible dans $K[X]$ et inséparable.*

Démonstration. — Soit P un facteur irréductible unitaire de $Q(X) = X^p - a$ dans $K[X]$ et soit x une racine de P dans un corps de rupture L. On a $a = x^p$ donc $Q(X) = X^p - x^p = (X - x)^p$ dans $L[X]$, de sorte que $P(X) = (X - x)^i$ dans $L[X]$, avec $1 \leq i \leq p$. Comme $x \notin K$, on a $i \geq 2$, donc P n'est pas séparable. Par le lemme 5.3, le degré de P est un multiple de p, donc $i = p$ et $P = Q$ est irréductible. De plus, P est clairement inséparable puisque $P' = 0$. □

Lemme 5.5. — *Si un polynôme irréductible unitaire $P \in K[X]$ de degré ≥ 2 n'a qu'une seule racine dans un corps de décomposition, alors la caractéristique de K est $p > 0$, et il existe $n \geq 1$ et $a \in K - K^p$ tels que $P(X) = X^{p^n} - a$.*

La réciproque est vraie (exerc. 5.8).

Démonstration. — Dans un corps de décomposition de P, on peut écrire $P(X) = (X - x)^m$, avec $m \geq 2$, de sorte que P est inséparable. Par le lemme 5.3, la caractéristique de K est un nombre premier p qui divise m. Écrivons $m = rp^n$, avec $r \wedge p = 1$, de sorte que $P(X) = (X^{p^n} - x^{p^n})^r$, et posons $Q(X) = (X - x^{p^n})^r$, de sorte que $P(X) = Q(X^{p^n})$. Le polynôme Q est alors irréductible (car P l'est) et n'a qu'une seule racine, x^{p^n}, dans un corps de décomposition. Si $r \geq 2$, il est inséparable, donc $p \mid r$ (lemme 5.3), ce qui est absurde. Donc $r = 1$, et $a := x^{p^n} \notin K^p$ (puisque P est irréductible), ce qui montre le lemme. □

5.2. Corps parfaits. —

Définition 5.6. — *Le corps K est* parfait *si tout polynôme irréductible de $K[X]$ est séparable.*

Théorème 5.7. — *Le corps K est parfait s'il est soit de caractéristique nulle, soit de caractéristique $p > 0$ et $K = K^p$.*

Démonstration. — Si K est de caractéristique nulle, il est parfait par le lemme 5.3. S'il est de caractéristique p et $K^p \neq K$, il n'est pas parfait par le lemme 5.4.

Si au contraire $K = K^p$, tout polynôme P inséparable s'écrit par le lemme 5.3

$$P(X) = a_{mp}X^{mp} + \cdots + a_pX^p + a_0.$$

Comme $K = K^p$, on peut écrire $a_{ip} = b_i^p$ et

$$\begin{aligned} P(X) &= a_{mp}X^{mp} + \cdots + a_pX^p + a_0 \\ &= b_m^pX^{mp} + \cdots + b_1^pX^p + b_0^p \\ &= (b_mX^m + \cdots + b_1X + b_0)^p, \end{aligned}$$

ce qui entraîne que P ne peut être irréductible. Donc tout polynôme irréductible de $K[X]$ est séparable : K est parfait. □

En particulier, tout corps fini est parfait, puisque le morphisme de Frobenius $x \mapsto x^p$ étant injectif est automatiquement surjectif. Tout corps algébriquement clos est aussi parfait. En revanche, le corps $\mathbf{F}_p(T)$ n'est pas parfait (le polynôme $X^p - T \in \mathbf{F}_p(T)[X]$ est irréductible par le lemme 5.4 mais non séparable).

Dans un corps parfait K, le morphisme de Frobenius Fr_K est bijectif. Pour tout $x \in K$, on notera $x^{1/p}$ son image inverse par Fr_K.

Exercice 5.8. — Soit K un corps de caractéristique $p > 0$. Si $a \in K - K^p$, montrer que pour tout $n \geq 1$, le polynôme $X^{p^n} - a$ est irréductible dans $K[X]$. En déduire que si $K \hookrightarrow L$ est une extension finie de corps et que L est un corps parfait, alors K est un corps parfait. Montrer qu'un sous-corps d'un corps parfait n'est pas nécessairement parfait.

Exercice 5.9. — Soit K un sous-corps d'un corps parfait L de caractéristique non nulle. Le morphisme de Frobenius $\mathrm{Fr}_L : L \to L$ est alors bijectif (th. 5.7). Montrer que

$$\bigcup_{n=1}^{\infty} \mathrm{Fr}_L^{-n}(K)$$

est le plus petit sous-corps parfait de L contenant K.

Exercice 5.10. — Soit K une extension de type fini d'un corps parfait de caractéristique $p > 0$. Montrer que K est une extension finie de K^p. Donner un exemple de corps K de caractéristique $p > 0$ qui n'est pas une extension finie de K^p.

5.3. Extensions séparables. —

Définition 5.11. — *Soit $K \hookrightarrow L$ une extension de corps. On dit qu'un élément de L est* séparable *sur K s'il est algébrique sur K et que son polynôme minimal sur K est séparable.*

On dit qu'une extension $K \hookrightarrow L$ est séparable *si tout élément de L est séparable sur K.*

Avec cette définition, une extension séparable est en particulier algébrique. Un corps K est parfait si et seulement si toute extension algébrique de K est séparable (pourquoi ?). En particulier, toute extension algébrique de corps de caractéristique nulle est séparable.

Soit $K \hookrightarrow L$ une extension algébrique de corps et soit $K \hookrightarrow \Omega$ un morphisme dans un corps algébriquement clos Ω. On a vu dans le lemme 3.16 qu'il existe une extension de ce morphisme en $\sigma : L \hookrightarrow \Omega$. L'extension $K \hookrightarrow \sigma(L)$ est alors algébrique, donc contenue dans la clôture algébrique de K dans Ω, qui est un corps algébriquement clos (prop. 3.13), donc une clôture algébrique de K. Comme deux clôtures algébriques de K sont K-isomorphes (th. 3.15), le cardinal de l'ensemble des extensions de $K \hookrightarrow \Omega$ à L est indépendant de l'extension algébriquement close Ω ; on le note $[L : K]_s$ et on l'appelle le *degré séparable* de l'extension $K \hookrightarrow L$. Il est toujours ≥ 1 par le lemme 3.16.

Exemple 5.12. — On a $[\mathbf{C} : \mathbf{R}]_s = 2$, les deux $\mathbf{R}$-morphismes de $\mathbf{C}$ dans $\mathbf{C}$ étant l'identité et la conjugaison complexe.

Exemple 5.13. — Si K est le corps de rupture sur $\mathbf{Q}$ du polynôme irréductible $X^3 - 2$, c'est-à-dire $K = \mathbf{Q}(a)$ avec $a^3 = 2$, on a $[K : \mathbf{Q}]_s = 3$, les trois $\mathbf{Q}$-morphismes de K dans $\mathbf{C}$ étant définis par $a \mapsto e^{2ik\pi/3}\sqrt[3]{2}$, pour $k \in \{0, 1, 2\}$.

Exemple 5.14. — Soit p un nombre premier. Posons $L = \mathbf{F}_p(T)$ et $K := L^p = \mathbf{F}_p(T^p)$. L'extension $K \subseteq L$ est finie de degré p. Si $\iota : K \hookrightarrow \Omega$ est un morphisme dans un corps algébriquement clos Ω et $\sigma : L \hookrightarrow \Omega$ un prolongement de f, on a nécessairement $\sigma(T) = (\iota(T^p))^{1/p}$, de sorte que $[L : K]_s = 1$.

Théorème 5.15. — *Soit $K \hookrightarrow L$ une extension finie de corps. On a*

$$1 \leq [L : K]_s \leq [L : K]$$

et il y a égalité à droite si et seulement si l'extension $K \hookrightarrow L$ est séparable.

Démonstration. — On commence par montrer la multiplicativité des degrés séparables.

Lemme 5.16. — *Soient $K \hookrightarrow L$ et $L \hookrightarrow M$ des extensions algébriques de corps. On a*

$$[M : K]_s = [M : L]_s [L : K]_s.$$

Démonstration. — Soit Ω une extension algébriquement close de M et soit $(\sigma_i)_{i \in I}$ la famille des K-morphismes de L dans Ω, avec $\mathrm{Card}(I) = [L : K]_s$. Considérons l'extension $\sigma_i : L \hookrightarrow \Omega$; comme on l'a déjà noté, le cardinal de l'ensemble des extensions à M est indépendant de i et vaut $[M : L]_s$. On peut donc

noter $(\tau_{ij})_{j\in J}$ cet ensemble, avec $\mathrm{Card}(J) = [M : L]_s$. On obtient ainsi une famille de K-morphismes distincts de M dans Ω indexée par $I \times J$.

Inversement, étant donné un tel morphisme $M \hookrightarrow \Omega$, il se restreint à L en un des σ_i ; c'est donc l'un des τ_{ij}. Le lemme est ainsi démontré. □

Lorsque l'extension $K \hookrightarrow L$ est engendrée par un élément x, de polynôme minimal P, on a vu dans le lemme 3.16 que $[L : K]_s$ est égal au nombre de racines distinctes de P dans son corps de décomposition. On a donc bien $[L : K]_s \leq [L : K]$ dans ce cas (avec égalité si et seulement si x est séparable).

Dans le cas général, on écrit l'extension finie $K \hookrightarrow L$ comme une suite d'extensions emboîtées

$$K \hookrightarrow K(x_1) \hookrightarrow K(x_1, x_2) \hookrightarrow \cdots \hookrightarrow K(x_1, \ldots, x_n) = L$$

et l'on applique le lemme 5.16 à chaque extension pour obtenir l'inégalité $[L : K]_s \leq [L : K]$.

Si $K \hookrightarrow L$ est séparable, ou même plus généralement si L est engendré par des éléments $x_1, \ldots, x_n$ séparables sur K, alors chaque x_i est *a fortiori* séparable sur $K(x_1, \ldots, x_{i-1})$ (son polynôme minimal sur ce corps divise son polynôme minimal sur K, donc est aussi séparable) et on a $[K(x_1, \ldots, x_{i-1})(x_i) : K(x_1, \ldots, x_{i-1})]_s = [K(x_1, \ldots, x_{i-1})(x_i) : K(x_1, \ldots, x_{i-1})]$, d'où l'égalité $[L : K]_s = [L : K]$ par le lemme 5.16.

Inversement, supposons $[L : K]_s = [L : K]$. Pour tout $x \in L$, comme $[L : K(x)]_s \leq [L : K(x)]$ et $[K(x) : K]_s \leq [K(x) : K]$, le lemme 5.16 entraîne qu'il y a égalité dans ces deux inégalités. La discussion précédente dit alors que x est séparable sur K. Donc l'extension $K \hookrightarrow L$ est bien séparable. □

La preuve montre aussi que *si L est engendré par des éléments séparables, l'extension $K \hookrightarrow L$ est séparable.*

Théorème 5.17. — *Soient $K \hookrightarrow L$ et $L \hookrightarrow M$ des extensions de corps. Si un élément x de M est séparable sur L et que L est une extension séparable de K, alors x est séparable sur K.*

En particulier, $K \hookrightarrow M$ est une extension séparable si et seulement si les extensions $K \hookrightarrow L$ et $L \hookrightarrow M$ le sont.

Démonstration. — Si un élément x de M est séparable sur L, il est algébrique sur L, donc racine d'un polynôme $P \in L[X]$. Si l'extension $K \hookrightarrow L$ est séparable, l'extension (finie) $L' \subseteq L$ de K engendrée par les coefficients de P est alors finie séparable, donc $[L' : K]_s = [L' : K]$ (th. 5.15). Comme x est séparable sur L', l'extension $L' \hookrightarrow L'(x)$ est séparable, donc $[L'(x) : L']_s = [L'(x) : L']$. Le lemme 5.16 entraîne alors $[L'(x) : K]_s = [L'(x) : K]$. L'extension finie $K \hookrightarrow L'(x)$ est alors séparable (th. 5.15), donc x est séparable sur K.

Si l'extension $K \hookrightarrow M$ est séparable, il est clair que l'extension $K \hookrightarrow L$ l'est aussi, ainsi que l'extension $L \hookrightarrow M$, puisque le polynôme minimal de x sur L divise le polynôme minimal de x sur K. L'implication réciproque résulte de la première partie du théorème. □

Corollaire 5.18. — *Soit $K \hookrightarrow L$ une extension de corps. L'ensemble des éléments de L séparables sur K est un sous-corps de L, extension séparable de K appelée* clôture séparable de K dans L.

Si $L' \subseteq L$ est la clôture séparable de K dans L, il résulte du corollaire précédent que tout élément de $L - L'$ est inséparable sur L'.

Démonstration. — Soient x et y des éléments non nuls de L séparables sur K. Comme on vient de le remarquer, cela entraîne que l'extension finie $K \hookrightarrow K(x, y)$ est séparable. Les éléments $x - y$ et x/y de L sont donc séparables sur K. □

En particulier, si $\overline{K}$ est une clôture algébrique de K, l'ensemble des éléments de $\overline{K}$ séparables sur K est une extension séparable $\overline{K}^s$ de K appelée *clôture séparable* de K. On peut montrer que les clôtures séparables de K sont toutes K-isomorphes.

Le corps K est parfait si et seulement si $\overline{K}^s = \overline{K}$. Toute extension séparable de $\overline{K}^s$ est triviale (th. 5.17). Tout élément de $\overline{K}$ – $\overline{K}^s$ est inséparable sur $\overline{K}^s$ donc sur K.

Exercice 5.19. — Soit $K \hookrightarrow L$ une extension finie de corps et soit $L^s \subseteq L$ la clôture séparable de K dans L (*cf.* cor. 5.18). Montrer $[L : K]_s = [L^s : K]$. En déduire que $[L : K]_s$ divise $[L : K]$ et que soit le quotient est 1, soit la caractéristique de K est $p > 0$ et le quotient est une puissance de p (il vous faudra sans doute aller explorer un peu la littérature sur les extensions dites *purement inséparables* (ou *radicielles)*...).

Exercice 5.20. — Montrer que toute extension algébrique d'un corps parfait est encore un corps parfait. En particulier, un corps imparfait (de caractéristique $p > 0$) ne peut être algébrique sur $\mathbf{F}_p$ (on rappelle que le corps $\mathbf{F}_p(T)$ est imparfait ; *cf.* § 5.2).

5.4. Théorème de l'élément primitif. — On a rencontré à plusieurs reprises l'extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2}, j)$. Peut-on engendrer cette extension par un seul élément (on dit que l'extension est *simple*) ? La réponse est oui : on a $\mathbf{Q}(\sqrt[3]{2}, j) = \mathbf{Q}(\sqrt[3]{2} + j)$ (*cf.* exerc. 6.16). En revanche, en caractéristique non nulle, il existe des extensions finies non simples. Il se trouve que cette propriété d'une extension finie (d'être engendrée par un élément) est liée à sa séparabilité.

Exemple 5.21. — Soit p un nombre premier. Posons $L = \mathbf{F}_p(X, Y)$ (corps des fractions rationnelles en deux indéterminées à coefficients dans $\mathbf{F}_p$) et $K := L^p = \mathbf{F}_p(X^p, Y^p)$. L'extension $K \subseteq L$ est finie de degré p^2. Pour tout $F \in L$, on a $F^p \in K$, donc $[K(F) : K]$ vaut 1 ou p, et L n'est pas de la forme $K(F)$: l'extension $K \hookrightarrow L$ n'est pas simple.

***Théorème 5.22* (de l'élément primitif)**. — *Soit $K \hookrightarrow L$ une extension finie de corps, que l'on peut écrire $L = K(x, y_1, \ldots, y_n)$, où $y_1, \ldots, y_n$ sont séparables sur K. Il existe $z \in L$ tel que $L = K(z)$.*

Démonstration. — Si K est fini, L l'est aussi, le groupe $(L^*, \times)$ est cyclique (prop. 2.2). Si $z \in L^*$ est un générateur de ce groupe, $L = K(z)$.

On suppose donc K infini. En raisonnant par récurrence sur n, on voit qu'il suffit de traiter le cas $n = 1$. On cherche z sous la forme $z = x + ty_1$, avec $t \in K$. Soit P le polynôme minimal de x sur K et soit Q celui de y_1. Ces polynômes se décomposent dans leur corps de décomposition en

$$P(X) = \prod_{i=1}^{r}(X - \alpha_i) \qquad , \qquad Q(X) = \prod_{j=1}^{s}(X - \beta_j),$$

avec $\alpha_1 = x$ et $\beta_1 = y_1$. Comme y_1 est séparable sur K, les β_j sont distincts deux à deux. Comme K est infini, on peut trouver $t \in K$ distinct de tous les $(x - \alpha_i)/(\beta_j - y_1)$, pour tout i et tout $j \neq 1$. Posant $z = x + ty_1 \in L$, on a

$$P(z - t\beta_1) = P(x) = 0 \qquad , \qquad P(z - t\beta_j) \neq 0 \quad \text{pour } j \neq 1.$$

Les polynômes $Q(X) \in K[X]$ et $P(z - tX) \in K(z)[X]$ ont donc une unique racine commune, à savoir $\beta_1 = y_1$, et leur pgcd est ainsi $X - y_1$. Les coefficients de ce pgcd sont dans $K(z)$, donc $y_1 \in K(z)$. Mais alors $x = z - ty_1 \in K(z)$, donc $L = K(x, y_1) = K(z)$. □

Théorème 5.23. — *Soit $K \hookrightarrow L$ une extension finie de corps. Les conditions suivantes sont équivalentes :*

(i) *il n'existe qu'un nombre fini de corps intermédiaires entre K et L ;*

(ii) *il existe $x \in L$ tel que $L = K(x)$.*

Si l'extension $K \hookrightarrow L$ est finie et séparable, elle vérifie (th. 5.22) les conditions de ce théorème. La réciproque est fausse (*cf.* ex. 5.14).

Démonstration. — Si K est fini, L l'est aussi, et le groupe $(L^*, \times)$ est cyclique (prop. 2.2). Si $x \in L^*$ est un générateur de ce groupe, $L = K(x)$. Donc (ii) est toujours vérifié dans ce cas, et il en est bien sûr de même pour (i).

On suppose donc K infini. Si (i) est vérifié, on écrit $L = K(x_1, \ldots, x_n)$ et, procédant par récurrence sur n, on voit qu'il suffit de traiter le cas $n = 2$. Vue l'hypothèse (i), et comme K est infini, il existe deux éléments distincts t et u de K tels que $K(x_1 + tx_2) = K(x_1 + ux_2)$. On en déduit que $x_2 = ((x_1 + tx_2) - (x_1 + ux_2))/(t - u)$ est dans ce corps, ainsi que $x_1 = (x_1 + tx_2) - tx_2$, donc qu'il est égal à L. Cela prouve (ii).

Inversement, si (ii) est vérifié, c'est-à-dire $L = K(x)$, on note $P \in K[X]$ le polynôme minimal de x sur K. Soit M un corps intermédiaire entre K et L. Le polynôme minimal $P_M \in M[X]$ de x sur M divise alors P dans $M[X]$, donc aussi dans $L[X]$. C'est donc un produit de facteurs irréductibles unitaires de P dans $L[X]$ et il n'y a qu'un nombre fini de tels polynômes (*cf.* th. 1.16). Soit $M' \subseteq M$ le sous-corps engendré par les coefficients de P_M. Le polynôme P_M est *a fortiori* irréductible dans $M'[X]$, donc c'est le polynôme minimal de x sur M'. On en déduit

$$[L : M'] = \deg P_M = [L : M],$$

de sorte que $M = M'$. L'application $M \mapsto P_M$, de l'ensemble des extensions intermédiaires entre K et L dans l'ensemble des facteurs irréductibles de P dans $L[X]$, est donc injective, ce qui montre (i). □

Exercice 5.24. — Trouver une infinité d'extensions intermédiaires entre les corps $\mathbf{F}_p(X^p, Y^p)$ et $\mathbf{F}_p(X, Y)$ (*cf.* ex. 5.21).

Exercice 5.25. — Soit $K \hookrightarrow L$ une extension séparable telle que les degrés des éléments de L sur K soient majorés. Montrer que l'extension $K \hookrightarrow L$ est finie. Montrer que la conclusion ne subsiste pas nécessairement si l'extension $K \hookrightarrow L$ n'est pas séparable.

Exercice 5.26. — Soit $K \hookrightarrow L$ une extension algébrique de corps. On suppose que tout polynôme de $K[X]$ a une racine dans L. On veut montrer que L est une clôture algébrique de K (il suffit pour cela (prop. 3.12) de montrer que tout polynôme de $K[X]$ est scindé dans L).

a) Montrer la conclusion sous l'hypothèse que le corps K est *parfait* (*Indication :* si $P \in K[X]$, on pourra appliquer le théorème de l'élément primitif à un corps de décomposition de P et considérer le polynôme minimal d'un générateur).

b) On suppose à partir de maintenant que la caractéristique de K est $p > 0$. Montrer que $M := \{x \in L \mid \exists n \in \mathbf{N}^* \quad x^{p^n} \in K\}$ est un sous-corps parfait de L.

c) En déduire que L est un corps parfait.

d) Montrer que tout polynôme de $M[X]$ a une racine dans L. Conclure.

5.5. 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 $\mathbf{F}_p$. L'extension $\mathbf{F}_p \hookrightarrow K$ est de degré fini n, de sorte que K est de cardinal p^n.

Théorème 5.27. — *a) Pour tout entier premier p et tout entier $n \geq 1$, il existe un corps fini à p^n éléments.*

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

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

Démonstration. — Soit $\mathbf{F}_p \hookrightarrow K$ un corps de décomposition du polynôme $P(X) := X^{p^n} - X$ sur $\mathbf{F}_p$ et soit $K' := \{x_1, \ldots, x_{p^n}\} \subseteq K$ l'ensemble des racines de P dans K. C'est un sous-corps de K (par (1)) qui lui est donc égal. Ces racines sont toutes distinctes car sa dérivée étant -1, le polynôme P est séparable (lemme 5.2). En particulier, $\mathrm{Card}(K) = p^n$. Ceci montre a).

Soit K un corps fini à p^n éléments. Le groupe $(K^*, \times)$ est d'ordre $p^n - 1$, donc tout élément non nul x de K vérifie $x^{p^n-1} = 1$. 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. 3.6, ceci montre b). □

Exercice 5.28. — Écrire les tables d'addition et de multiplication du corps $\mathbf{F}_4$.

Exercice 5.29. — Quel est le groupe additif $(\mathbf{F}_{p^n}, +)$?

5.6. Trace. — À toute extension finie $K \hookrightarrow L$, nous allons associer une forme K-linéaire $\mathrm{Tr}_{L/K}$ sur L dont la non nullité caractérise les extensions (finies) séparables.

Définition 5.30. — *Soit $K \hookrightarrow L$ une extension finie de corps. Pour $x \in L$, on note m_x le K-endomorphisme de L défini par $m_x(z) = xz$ pour tout z dans L. On définit l'application* trace $\mathrm{Tr}_{L/K} : L \to K$ *par*

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(m_x).$$

Si $a, b \in K$ et $x, y \in L$, on a $m_{ax+by} = am_x + bm_y$; l'application trace est donc une forme K-linéaire sur L. Si x est dans K, on a $\mathrm{Tr}_{L/K}(x) = [L : K]x$.

Exemple 5.31. — Considérons l'extension $\mathbf{Q} \subseteq \mathbf{Q}(i)$. Dans la base $(1, i)$ du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}(i)$, la matrice de l'endomorphisme m_{a+ib} est $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. On a donc

$$\mathrm{Tr}_{\mathbf{Q}(i)/\mathbf{Q}}(a + ib) = 2a.$$

Théorème 5.32. — *Soient $K \hookrightarrow L$ et $L \hookrightarrow M$ des extensions de corps. On a*

$$\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}\,.$$

Démonstration. — On garde les notations de la preuve du th. 2.4 : $(l_1, \ldots, l_r)$ est une base du K-espace vectoriel L et soit $(m_1, \ldots, m_s)$ une base du L-espace vectoriel M, de sorte que $(l_i m_j)_{1 \leq i \leq r,\ 1 \leq j \leq s}$ est une base du K-espace vectoriel M. Soit $x \in M$. On écrit

$$xm_j = \sum_{k=1}^{s} b_{jk} m_k,$$

avec $b_{jk} \in L$, de sorte que $xl_i m_j = \sum_{k=1}^{s} b_{jk} l_i m_k$. On écrit ensuite

$$b_{jk} l_i = \sum_{n=1}^{r} a_{jkin} l_n,$$

avec $a_{jkin} \in L$, de sorte que $xl_i m_j = \sum_{k=1}^{s} \sum_{n=1}^{r} a_{jkin} l_n m_k$. On en déduit

$$\mathrm{Tr}_{M/K}(x) = \sum_{j=1}^{s} \sum_{i=1}^{r} a_{jjii}.$$

On a d'autre part $\mathrm{Tr}_{M/L}(x) = \sum_{j=1}^{s} b_{jj}$ et $\mathrm{Tr}_{L/K}(b_{jj}) = \sum_{n=1}^{r} a_{jjnn}$, ce qui montre le théorème. □

Corollaire 5.33. — *Soit $K \hookrightarrow L$ une extension finie de corps et soit x un élément de L* inséparable *sur K. On a $\mathrm{Tr}_{L/K}(x) = 0$.*

Démonstration. — Considérons les extensions $K \hookrightarrow K(x) \hookrightarrow L$. D'après le th. 5.32, on a

$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{K(x)/K}\big(\mathrm{Tr}_{L/K(x)}(x)\big) = \mathrm{Tr}_{K(x)/K}([L : K(x)]x).$$

Il suffit donc de montrer $\mathrm{Tr}_{K(x)/K}(x) = 0$. Le polynôme minimal P de x sur K est, par le lemme 5.3, dans $K[X^p]$, où p est la caractéristique (non nulle) du corps K. Dans la base $(1, x, \ldots, x^{pn-1})$ de $K(x)$ sur K (où $pn = \deg(P)$), la matrice de m_x est la matrice *compagnon* de P (*cf.* § II.4.2), dont la trace est l'opposé du coefficient de X^{pn-1} dans P, c'est-à-dire 0. □

Corollaire 5.34. — *Soit $K \hookrightarrow L$ une extension finie de corps qui n'est pas séparable. La forme linéaire $\mathrm{Tr}_{L/K}$ est identiquement nulle.*

Démonstration. — Soit $L' \subsetneq L$ la clôture séparable de K dans L (cor. 5.18). Tout élément x de $L - L'$ est alors inséparable sur L', donc $\mathrm{Tr}_{L/L'}(x) = 0$ par le corollaire précédent. D'autre part, le lemme 5.3 entraîne que $[L'(x) : L']$ est un multiple de p, donc aussi $[L : L']$ (th. 2.4). Pour tout $x' \in L'$, on a alors $\mathrm{Tr}_{L/L'}(x') = [L : L']x' = 0$, ce qui montre que la forme linéaire $\mathrm{Tr}_{L/L'}$ est identiquement nulle. Le corollaire résulte alors du th. 5.32. □

Théorème 5.35. — *Soit $K \hookrightarrow L$ une extension finie et séparable de corps. La forme linéaire $\mathrm{Tr}_{L/K}$ n'est pas identiquement nulle et la forme bilinéaire symétrique*

$$\begin{array}{ccc} L \times L & \longrightarrow & K \\ (x, y) & \longmapsto & \mathrm{Tr}_{L/K}(xy) \end{array}$$

est non dégénérée.

Le théorème est évident en caractéristique nulle, puisque l'on a alors $\mathrm{Tr}_{L/K}(1_K) = [L : K]1_K \neq 0$ et $\mathrm{Tr}_{L/K}(xx^{-1}) = \mathrm{Tr}_{L/K}(1_K) \neq 0$ si $x \in L - \{0\}$.

Démonstration. — Comme on l'a vu dans le § 5.4, l'extension $K \hookrightarrow L$ est engendrée par un élément $x \in L$, de polynôme minimal $P \in K[X]$. Si $n = [L : K]$, une base du K-espace vectoriel L est alors formée de $1, x, \ldots, x^{n-1}$. La matrice de m_x dans cette base est la matrice compagnon C_P de P (*cf.* § II.4.2) dont la trace est l'opposé du coefficient de X^{n-1} dans P, c'est-à-dire la somme des racines $x_1, \ldots, x_n$ de P dans un corps de décomposition de P (ces racines sont distinctes deux à deux puisque P est séparable). Pour tout entier $r \geq 0$, la matrice de $m_x^r = m_{x^r}$ est C_P^r, dont la trace est la somme $\sum_{i=1}^n x_i^r$. Ces sommes ne peuvent pas être toutes nulles lorsque r décrit $\{0, \ldots, n-1\}$, puisque le déterminant $\det(x_i^r)_{1 \leq i \leq n,\ 0 \leq r \leq n-1}$ est non nul (déterminant de Vandermonde). Donc l'une au moins des traces $\mathrm{Tr}_{L/K}(x^r)$ est non nulle, et la forme linéaire $\mathrm{Tr}_{L/K}$ n'est pas identiquement nulle.

Soit $x_0 \in L$ tel que $\mathrm{Tr}_{L/K}(x_0) \neq 0$. Si $y \in L$ est non nul, on a alors $\mathrm{Tr}_{L/K}(y \cdot x_0/y) \neq 0$, donc la forme bilinéaire considérée est bien non dégénérée. □

Exercice 5.36. — Soit $K \hookrightarrow L$ une extension finie et séparable de corps. Soit Ω une extension algébriquement close de K et soient $\sigma_1, \ldots, \sigma_n$ les différents K-morphismes de L dans Ω. Montrer que pour tout x dans L, on a $\mathrm{Tr}_{L/K}(x) = \sigma_1(x) + \cdots + \sigma_n(x)$.

6. Théorie de Galois

6.1. Groupe de Galois d'une extension de corps. — La définition suivante s'inspire de la déf. 3.3.

Définition 6.1. — *Soit $K \hookrightarrow L$ une extension de corps. Un* K-automorphisme de L *est un automorphisme de corps $L \xrightarrow{\sim} L$ qui est l'identité sur K. Le* groupe de Galois $\mathrm{Gal}(L/K)$ *est le groupe des K-automorphismes de L.*

Exemple 6.2. — Soit σ un élément de $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$. On a

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1,$$

de sorte que $\sigma(i) = \pm i$. On en déduit que le groupe $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ a deux éléments : l'identité et la conjugaison complexe.

Soit σ un élément de $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q})$. On a

$$\sigma(\sqrt[3]{2})^3 = \sigma((\sqrt[3]{2})^3) = \sigma(2) = 2,$$

de sorte que $\sigma(\sqrt[3]{2})$ est une racine cubique de 2 dans le sous-corps $\mathbf{Q}(\sqrt[3]{2})$ de $\mathbf{R}$. On a donc nécessairement $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ et le groupe $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q})$ n'a qu'un seul élément, l'identité.

Exercice 6.3. — Déterminer les groupes de Galois $\mathrm{Gal}(\mathbf{Q}(\sqrt{2},\sqrt{3})/\mathbf{Q})$ et $\mathrm{Gal}(\mathbf{R}/\mathbf{Q})$.

Théorème 6.4. — *Soit $K \hookrightarrow L$ une extension finie de corps. On a*

$$\mathrm{Card}(\mathrm{Gal}(L/K)) \leq [L:K]_s \leq [L:K].$$

La première inégalité est une égalité si et seulement si l'extension $K \hookrightarrow L$ est normale ; la seconde est une égalité si et seulement si l'extension $K \hookrightarrow L$ est séparable.

Démonstration. — Soit Ω une extension algébriquement close de K. Le groupe $\mathrm{Gal}(L/K)$ agit à droite sur l'ensemble des K-morphismes $\sigma : L \hookrightarrow \Omega$ (dont le cardinal est par définition $[L:K]_s$) par la formule

$$\forall g \in \mathrm{Gal}(L/K) \qquad \sigma \cdot g = \sigma \circ g.$$

Cette action est libre (si $\sigma \circ g = \sigma$, on a $g = \mathrm{Id}$ puisque σ est injectif), d'où la première inégalité. Il y a égalité si et seulement si l'action est transitive.

Lemme 6.5. — *L'action de $\mathrm{Gal}(L/K)$ sur l'ensemble des K-morphismes de L dans Ω est transitive si et seulement si tous ces morphismes ont la même image dans Ω.*

Démonstration. — Il est clair que $\sigma \circ g$ et σ ont la même image. Inversement, si $\sigma(L) = \sigma'(L)$, l'application $g : L \to L$ définie par $g = (\sigma_{L \to \sigma(L)})^{-1} \circ \sigma'$ est un K-automorphisme tel que $\sigma' = \sigma \circ g$. □

On invoque alors le cor. 4.4 pour en déduire qu'il y a égalité dan l'inégalité de gauche si et seulement si l'extension $K \hookrightarrow L$ est normale.

L'égalité de droite du théorème, et le cas d'égalité, sont juste une retranscription du th. 5.15. □

Exercice 6.6. — Soit $K \hookrightarrow L$ une extension finie de corps. Montrer que $\mathrm{Card}(\mathrm{Gal}(L/K))$ divise $[L:K]_s$ (*cf.* exerc. 5.19).

6.2. Groupe de Galois de $K \hookrightarrow K(X)$ et théorème de Lüroth. — Le but de cette section (indépendante du reste du cours) est de comprendre le groupe de Galois de l'extension transcendante $K \hookrightarrow K(X)$ et la nature des extensions intermédiaires entre K et $K(X)$.

Lemme 6.7. — *Soit $F \in K(X) - K$, que l'on écrit $F = P/Q$, avec P et Q dans $K[X]$, premiers entre eux. Alors :*

a) *F est transcendant sur K ;*

b) *l'extension $K(F) \hookrightarrow K(X)$ est finie, de degré $\delta(F) := \max(\deg P, \deg Q)$;*

c) *le polynôme minimal de X sur $K(F)$ est $P(T) - Q(T)F \in K(F)[T]$.*

Démonstration. — Posons $R(T) := P(T) - Q(T)F \in K(F)[T]$. On a $R(X) = 0$, donc X est algébrique sur $K(F)$. Comme X est transcendant sur K, il en est de même pour F par le th. 2.16, ce qui montre a). 1

Cela entraîne que $K[F]$ est isomorphe à un anneau de polynômes en une variable à coefficients dans K. On peut donc considérer R comme un élément de l'anneau de polynômes en deux variables $K[F][T]$ et il faut montrer que R est irréductible dans $K(F)[T]$. Dans $K[T][F]$, R est irréductible car de degré 1 (en F) à coefficients premiers entre eux. Il est donc aussi irréductible dans $K[F][T]$. Ses coefficients sont du type $p_i - q_i F$, donc leur pgcd dans $K[F]$ est 1 (sinon, P et Q seraient proportionnels). Cela entraîne (th. III.1.10) que R est encore irréductible dans $K(F)[T]$. Cela montre c), et comme le degré de R est $\delta(F)$, cela montre aussi b). □

Pour tout corps K et tout entier $n > 0$, on note $\mathrm{GL}(n, K)$ le groupe des matrices inversibles d'ordre n à coefficients dans K, et $\mathrm{PGL}(n, K)$ le groupe quotient de $\mathrm{GL}(n, K)$ par le sous-groupe distingué des matrices de la forme tI_n, pour $t \in K^*$.

Théorème 6.8. — *On a un isomorphisme*

$$\begin{array}{ccc} \mathrm{PGL}(2,K) & \longrightarrow & \mathrm{Gal}(K(X)/K) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \Big(X \mapsto \dfrac{aX+b}{cX+d}\Big). \end{array}$$

Démonstration. — Soit $\varphi : K(X) \to K(X)$ un K-automorphisme. Il est déterminé par $F = \varphi(X)$. Comme φ est surjectif, on a par le lemme 6.7 $\delta(F) = 1$, donc $F(X) = \frac{aX+b}{cX+d}$ avec $(c, d) \neq (0, 0)$ et (a, b) non proportionnel à (c, d). L'application de l'énoncé du théorème est donc surjective. On vérifie que c'est un morphisme dont le noyau est formé des homothéties tI_2, pour $t \in K^*$. □

Théorème 6.9 **(Lüroth, 1874)**. — *Les extensions intermédiaires entre K et $K(X)$ sont de la forme $K(F)$, avec $F \in K(X)$. Autrement dit, ce sont K ou des corps de fractions rationnelles en une variable.*

Démonstration. — Soit $K \subsetneq L \subseteq K(X)$ et soit $F \in L - K$. Par le lemme 6.7, X est algébrique sur $K(F)$, donc aussi sur L. Soit

$$\Phi(T) = T^n + F_{n-1}T^{n-1} + \cdots + F_0 \in L[T]$$

le polynôme minimal de X sur L. Comme X n'est pas algébrique sur K, il existe i tel que $F_i \in L - K$. On va montrer $L = K(F_i)$. Écrivons $F_j = P_j/P_n$, avec $P_j \in K[X]$ et où P_n est le ppcm des dénominateurs des F_j. On a ainsi

$$\Phi(T) = \frac{1}{P_n(X)}(P_n(X)T^n + P_{n-1}(X)T^{n-1} + \cdots + P_0(X)) \in L[T].$$

Notons

$$P(X, T) := P_n(X)T^n + P_{n-1}(X)T^{n-1} + \cdots + P_0(X)$$

et posons $m := \deg_X P(X, T) = \max(\deg P_j)$. On a $[K(X) : L] = \deg(\Phi) = n$ et

$$[K(X) : L] \leq [K(X) : K(F_i)] = \delta(F_i) \leq \max(\deg P_i, \deg P_n) \leq m.$$

On va montrer $m = n$, ce qui entraînera $L = K(F_i)$ et le théorème.

Le polynôme $P_i(T) - F_i P_n(T) \in L[T]$ admet X comme racine. Il est donc multiple de Φ : il existe $\Psi \in L[T]$ tel que

$$P_i(T) - F_i P_n(T) = \Phi(T)\Psi(T).$$

En multipliant par $P_n(T)$, on obtient

$$D(X, T) := P_i(T)P_n(X) - P_i(X)P_n(T) = P(X, T)\Psi(T) \in L[T] \cap K[X][T].$$

Comme $P(X,T)$ est primitif vu comme polynôme en T, on a $\Psi \in K[X][T]$ (lemme III.1.9). Dans cette dernière égalité, le degré en X est $\leq m$ à gauche et $m + \deg_X \Psi$ à droite. Donc il vaut m des deux côtés et $\Psi \in K[T]$. On a donc

$$P(X,T)\Psi(T) = D(X,T) = -D(T,X) = -P(T,X)\Psi(X).$$

Comme $P(X,T)$ et $\Psi(T)$ sont primitifs vus comme polynôme en T à coefficients dans $K[X]$, il en est de même pour leur produit (lemme III.1.8), donc le polynôme $\Psi(X)$, constant vu comme polynôme en T, est une constante inversible dans $K[X]$. Les polynômes D et P sont donc proportionnels. Les degrés de D en X et en T étant égaux, cela vaut aussi pour P, donc $m = n$. □

Remarque 6.10. — L'analogue du théorème de Lüroth reste vrai en caractéristique 0 pour $K(X,Y)$ (toutes les sous-extensions non triviales sont des corps de fractions rationnelles en une ou deux variables sur K) ; c'est un théorème de Castelnuovo. Cela est faux en caractéristique non nulle d'après des exemples de Zariski et de Shioda. Avec au moins trois indéterminées, c'est faux même sur $\mathbf{C}$. L'étude de ces problèmes se fait par des outils de géométrie algébrique (il s'agit de savoir si une variété algébrique « unirationnelle » est « rationnelle »).

Exercice 6.11. — Soit K un corps. Quelles sont les fractions rationnelles $F \in K(X)$ vérifiant $F \circ F(X) = X$? Plus généralement, quelles sont les fractions rationnelles vérifiant $F \circ \cdots \circ F(X) = X$?

Exercice 6.12. — Soit K un corps. Déterminer le corps

$$L = \{F \in K(X) \mid F(X) = F(1/X)\}.$$

6.3. Extensions galoisiennes. —

Définition 6.13. — *Une extension de corps $K \hookrightarrow L$ est dite* galoisienne *si elle est séparable et normale.*

Le th. 6.4 entraîne qu'une extension finie $K \hookrightarrow L$ est galoisienne si et seulement si

$$\mathrm{Card}(\mathrm{Gal}(L/K)) = [L : K].$$

Remarque 6.14. — Si $K \hookrightarrow L$ est une extension de corps galoisienne et que M est un corps intermédiaire entre K et L, l'extension $M \hookrightarrow L$ est encore galoisienne (rem. 4.3 et th. 5.17) et $\mathrm{Gal}(L/M)$ est un sous-groupe de $\mathrm{Gal}(L/K)$:

$$\mathrm{Gal}(L/M) = \{g \in \mathrm{Gal}(L/K) \mid g|_M = \mathrm{Id}_M\}.$$

En revanche, l'extension $K \hookrightarrow M$ n'est pas nécessairement galoisienne (*cf.* th. 6.20.b)).

Proposition 6.15. — *Une extension finie $K \hookrightarrow L$ est galoisienne si et seulement si c'est le corps de décomposition sur K d'un polynôme séparable.*

Démonstration. — Si L est le corps de décomposition d'un polynôme séparable $Q \in K[X]$, l'extension L est engendrée par des éléments séparables (les racines de Q) donc est séparable. Elle est aussi normale par le th. 4.2.

Pour la réciproque, on reprend la démonstration du th. 4.2 : si $K \hookrightarrow L$ est une extension galoisienne, on écrit $L = K(x_1, \ldots, x_n)$ et l'on note $P_i \in K[X]$ le polynôme minimal de x_i. Comme $K \hookrightarrow L$ est normale (resp. séparable), chaque P_i est scindé (resp. à racines simples) dans L, donc aussi le ppcm $Q := P_1 \vee \cdots \vee P_n$. Comme L est engendré sur K par les x_i, qui sont des racines de Q, le corps L est un corps de décomposition du polynôme séparable $Q \in K[X]$. □

En utilisant le th. 5.22, on peut aussi dire qu'il existe $x \in L$ tel que le polynôme minimal de x sur K est scindé à racines simples dans L et que $L = K(x)$.

Soit $K \hookrightarrow L$ une extension finie galoisienne. C'est donc le corps de décomposition d'un polynôme séparable $P \in K[X]$. Si $n = \deg(P)$, le groupe $\mathrm{Gal}(L/K)$ permute les n racines distinctes de P et $\mathrm{Gal}(L/K)$ s'identifie à un sous-groupe du groupe symétrique $\mathfrak{S}_n$.

Exercice 6.16. — Montrer que l'extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2}, j)$ est galoisienne et que son groupe de Galois est $\mathfrak{S}_3$. En déduire $\mathbf{Q}(\sqrt[3]{2}, j) = \mathbf{Q}(\sqrt[3]{2} + j)$ et calculer le polynôme minimal de $\sqrt[3]{2} + j$ sur $\mathbf{Q}$.

Proposition 6.17. — *Soit $K \hookrightarrow L$ une extension finie et normale de corps et soit $P \in K[X]$ un polynôme séparable scindé dans L. L'action de $\mathrm{Gal}(L/K)$ sur l'ensemble des racines de P dans L est transitive si et seulement si P est irréductible dans $K[X]$.*

Démonstration. — Si P n'est pas irréductible, on l'écrit $P = QR$ avec Q et R dans $K[X]$, non constants. Comme P est séparable, Q et R n'ont pas de racine commune. Tout élément de $\mathrm{Gal}(L/K)$ envoie chaque racine de Q (dans L) sur une racine de Q, donc l'action sur les racines de P n'est pas transitive.

Supposons P irréductible. Soit $Q \in K[X]$ un polynôme dont L est un corps de décomposition (th. 4.2). Soient x et y des racines de P dans L. Les sous-corps $K(x)$ et $K(y)$ de L sont des corps de rupture de P, donc sont K-isomorphes. Plus précisément, il existe un K-isomorphisme $\sigma : K(x) \xrightarrow{\sim} K(y)$ tel que $\sigma(x) = y$. Les extensions $\iota : K(x) \hookrightarrow L$ et $\iota' : K(x) \xrightarrow{\sigma} K(y) \hookrightarrow L$ sont alors des corps de décomposition de Q vu comme polynôme à coefficients dans $K(x)$, donc sont $K(x)$-isomorphes (th. 3.6) : il existe un automorphisme $g : L \xrightarrow{\sim} L$ tel que $g \circ \iota = \iota'$. D'une part g est un K-automorphisme, donc $g \in \mathrm{Gal}(L/K)$, d'autre part $g(x) = g \circ \iota(x) = \iota'(x) = y$. □

Exemple 6.18. — L'extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}, \sqrt{3})$ est galoisienne car c'est le corps de décomposition du polynôme $(X^2 - 2)(X^2 - 3)$. Son groupe de Galois agit de façon non transitive sur l'ensemble $\{\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}\}$ de ses racines ; il est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$.

Exercice 6.19. — Soit $K \hookrightarrow L$ une extension finie galoisienne de corps. Montrer que pour tout x dans L, on a $\mathrm{Tr}_{L/K}(x) = \sum_{g \in \mathrm{Gal}(L/K)} g(x)$.

6.4. Correspondance de Galois, lemme d'Artin. — Nous montrons maintenant le résultat principal de cette section : le fait que pour une extension finie galoisienne, les extensions intermédiaires correspondent bijectivement aux sous-groupes du groupe de Galois. On retrouve ainsi le fait qu'il n'y a qu'un nombre fini d'extensions intermédiaires (*cf.* th. 5.23) mais surtout, on dispose d'un moyen « concret » de les trouver toutes.

Théorème 6.20. — *Soit $K \subseteq L$ une extension finie galoisienne de corps, de groupe de Galois $G := \mathrm{Gal}(L/K)$.*

a) *Il existe des bijections inverses l'une de l'autre, qui renversent les inclusions,*

$$\begin{array}{ccc} \{\text{sous-groupes de } G\} & \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} & \{\text{extensions intermédiaires entre } K \text{ et } L\} \\ H & \longmapsto & L^H := \{x \in L \mid \forall g \in H\ g(x) = x\} \\ \mathrm{Gal}(L/M) & \longmapsfrom & M. \end{array}$$

b) *Si H est un sous-groupe de G, l'extension $K \subseteq L^H$ est galoisienne si et seulement si H est distingué dans G. Son groupe de Galois est alors le groupe quotient G/H.*

Pour clarifier les choses, l'égalité $\Phi \circ \Psi = \mathrm{Id}$ signifie

$$L^{\mathrm{Gal}(L/M)} = M$$

pour tout corps intermédiaire M, tandis que, par la rem. 6.14, l'égalité $\Psi \circ \Phi = \mathrm{Id}$ signifie

$$\{g \in G \mid g|_{L^H} = \mathrm{Id}\} = H$$

pour tout sous-groupe H de G.

Démonstration. — Il est clair que l'on a, pour toute extension intermédiaire M et tout sous-groupe H de G :

$$M \subseteq \Phi(\Psi(M)) = L^{\mathrm{Gal}(L/M)} \quad \text{et} \quad H \subseteq \Psi(\Phi(H)) = \mathrm{Gal}(L/L^H)$$

et il s'agit de montrer que ces deux inclusions sont des égalités. L'extension $M \subseteq L$ est finie galoisienne (rem. 6.14). Nous lui appliquerons le lemme suivant.

Lemme 6.21. — *Soit $K \subseteq L$ une extension finie galoisienne de corps, de groupe G. On a $K = L^G$.*

Démonstration. — Il est clair que K est contenu dans L^G. Soit $x \in L^G$ et soit $P \in K[X]$ son polynôme minimal, qui est scindé dans L. Soit y une racine de P dans L ; comme l'extension $K \hookrightarrow L$ est normale et que P est irréductible dans $K[X]$, il existe $g \in G$ tel que $y = g(x)$ (prop. 6.17). Comme $x \in L^G$, on a $y = x$. Donc P n'a qu'une seule racine. Comme il est séparable, il est de degré 1 et x est dans K. □

En appliquant ce lemme à l'extension finie galoisienne $M \subseteq L$, on obtient $M = L^{\mathrm{Gal}(L/M)}$, c'est-à-dire $M = \Phi(\Psi(M))$). L'autre égalité $H = \mathrm{Gal}(L/L^H)$ résulte du th. 6.22 ci-dessous. Ceci montre le point a) du théorème.

Montrons maintenant b). Soit H un sous-groupe de G et soit $g \in G$. On vérifie que l'extension intermédiaire $g(L^H)$ correspond au sous-groupe gHg^{-1} de G.

Si H est un sous-groupe distingué dans G, on a donc, par a), $g(L^H) = L^H$, d'où un morphisme de groupes

$$\rho : G \to \mathrm{Gal}(L^H/K)$$

dont le noyau est $\{g \in G \mid g|_{L^H} = \mathrm{Id}\}$, c'est-à-dire, par a), H. On en déduit

$$\mathrm{Card}(\mathrm{Gal}(L^H/K)) \geq \mathrm{Card}(G)/\mathrm{Card}(H) = [L : K]/[L : L^H] = [L^H : K].$$

Cela entraîne (th. 6.4) que l'extension finie $K \subseteq L^H$ est galoisienne, que ρ est surjectif, et que $\mathrm{Gal}(L^H/K)$ est isomorphe à G/H.

Inversement, supposons l'extension $K \hookrightarrow L^H$ galoisienne et considérons le sous-groupe $N := \{g \in G \mid gHg^{-1} = H\}$ de G (le *normalisateur* de H dans G) ainsi que le morphisme $\pi : N \to \mathrm{Gal}(L^H/K)$. Son noyau est $\{g \in N \mid g|_{L^H} = \mathrm{Id}\}$, c'est-à-dire de nouveau H.

Comme l'extension $K \subseteq L$ est normale, tout K-automorphisme $L^H \xrightarrow{\sim} L^H$ se prolonge en un K-automorphisme $L \xrightarrow{\sim} L$ (cor. 4.5), c'est-à-dire en un élément g de G qui doit satisfaire $g(L^H) = L^H$. Par la correspondance a), cela signifie $gHg^{-1} = H$, c'est-à-dire $g \in N$. Le morphisme π est donc surjectif et on en déduit :

$$\begin{aligned} \mathrm{Card}(N)/\mathrm{Card}(H) &= \mathrm{Card}(\mathrm{Gal}(L^H/K)) \\ &= [L^H : K] \\ &= [L : K]/[L : L^H] \\ &= \mathrm{Card}(G)/\mathrm{Card}(H), \end{aligned}$$

de sorte que $N = G$: le sous-groupe H est distingué dans G. Ceci prouve b). □

***Théorème 6.22* (Lemme d'Artin)**. — *Soit L un corps et soit G un groupe fini d'automorphismes de L. L'extension $L^G \subseteq L$ est finie galoisienne de groupe de Galois G.*

Démonstration. — Posons $K = L^G$. Soit $x \in L$; posons $P(X) = \prod_{y \in Gx}(X - y)$. Pour tout $g \in G$, on a alors $gP = P$, donc P est à coefficients dans K. Comme P est séparable, il en résulte que x est séparable algébrique sur K de degré $\leq \mathrm{Card}(G)$.

Choisissons x de degré maximal sur K. Nous allons montrer $L = K(x)$. Soit $y \in L$. Comme l'extension $K(x, y)$ est séparable, elle est engendrée par un élément z (th. 5.22). Comme $K(z)$ contient $K(x)$, ces deux corps sont égaux par maximalité du degré de x. On a donc $y \in K(x)$ et $L = K(x)$, extension finie et séparable de K de degré $\leq \mathrm{Card}(G)$. De plus, G est un sous-groupe de $\mathrm{Gal}(L/K)$.

On en déduit (th. 6.4)

$$\mathrm{Card}(G) \leq \mathrm{Card}(\mathrm{Gal}(L/K)) \leq [L : K] \leq \mathrm{Card}(G),$$

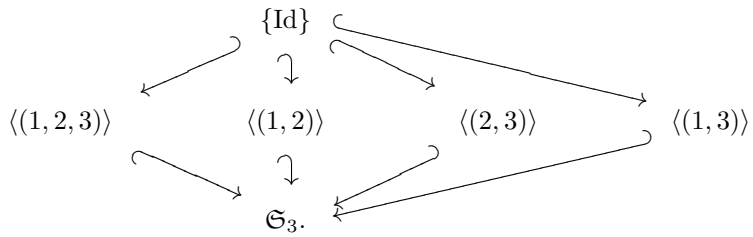
de sorte qu'il y a égalité partout. On en déduit que l'extension $K \subseteq L$ est galoisienne (th. 6.4), et $\mathrm{Gal}(L/K) = G$. □

Exercice 6.23. — Soit L un corps et soit G un groupe *infini* d'automorphismes de L. Montrer que l'extension $L^G \subseteq L$ est *infinie.*

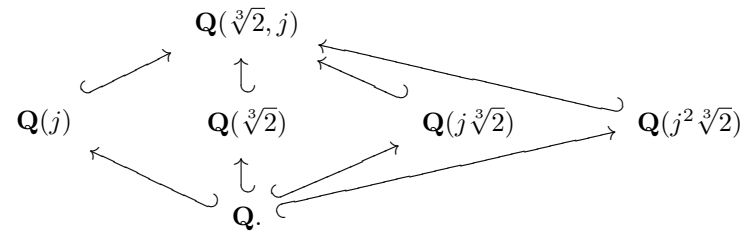
Exercice 6.24. — Soit $K \subseteq L$ une extension de corps finie et normale et soit G le groupe $\mathrm{Gal}(L/K)$ des K-automorphismes de L. On a des extensions $K \subseteq L^G \subseteq L$. Si la caractéristique de K est nulle, le lemme 6.21 entraîne $K = L^G$. Supposons donc que la caractéristique de K est $p > 0$.

a) Soit $x \in L^G$. Montrer que le polynôme minimal de x sur K a une seule racine dans L.
b) En déduire qu'il existe un entier $n \geq 0$ tel que $x^{p^n} \in K$ (*Indication :* on pourra utiliser le lemme 5.5).
c) Montrer qu'il existe un entier $n \geq 0$ tel que $(L^G)^{p^n} \subseteq K$.

Exemple 6.25. — Revenons à l'exerc. 6.16, où l'on a montré que l'extension $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2}, j)$ est galoisienne de groupe de Galois isomorphe à $\mathfrak{S}_3$ (après numérotation des racines du polynôme $X^3 - 2$ par $x_k = e^{2ik\pi/3}\sqrt[3]{2}$, $k \in \{1, 2, 3\}$). Les sous-groupes de $\mathfrak{S}_3$ sont



Le seul sous-groupe distingué non trivial est $\langle(1, 2, 3)\rangle$ (cyclique d'ordre 3). La transposition $(1, 2)$ correspond à la conjugaison complexe et le cycle $(1, 2, 3)$ à la permutation cyclique des racines. Les sous-extensions correspondantes de $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2}, j)$ sont



Les quatre extensions de la ligne supérieures sont galoisiennes, tandis que sur la ligne inférieure, seule l'extension (quadratique) $\mathbf{Q} \subseteq \mathbf{Q}(j)$ l'est.

Exemple 6.26. — On vérifie (par exemple en utilisant le critère d'Eisenstein ; th. III.1.12) que le polynôme $P(X) = X^5 - 6X + 3$ est irréductible dans $\mathbf{Q}[X]$. Une étude de fonction montre qu'il a exactement trois racines réelles $x_1 < x_2 < x_3$, donc deux racines complexes conjuguées x_4 et $x_5 = \bar{x}_4$. Soit $\mathbf{Q} \hookrightarrow L$

un corps de décomposition de P et soit $G < \mathfrak{S}_5$ son groupe de Galois. Le groupe G contient la conjugaison complexe, qui agit comme la transposition $(4,5)$. Le corps L contient la sous-extension $\mathbf{Q}(x_1)$, qui est de degré 5, donc le cardinal de G est divisible par 5 ; il divise d'autre part $\mathrm{Card}(\mathfrak{S}_5) = 5! = 120 = 2^3 \cdot 3 \cdot 5$. Le théorème de Sylow entraîne que G contient un élément d'ordre 5, c'est-à-dire un 5-cycle dont on peut supposer, quitte à le remplacer par une puissance, qu'il envoie 4 sur 5. En renumérotant les racines réelles, on peut supposer que c'est le cycle $(1,2,3,4,5)$, qui avec $(4,5)$ engendre $\mathfrak{S}_5$. On a donc $G = \mathfrak{S}_5$.

Le seul sous-groupe distingué non trivial de $\mathfrak{S}_5$ est le groupe alterné $\mathfrak{A}_5$. L'extension $\mathbf{Q} \hookrightarrow L$ contient donc une unique sous-extension galoisienne de $\mathbf{Q}$ et elle est quadratique.

Exercice 6.27. — Dans l'exemple ci-dessus, montrer que le *discriminant*

$$\Delta(P) = \prod_{1 \leq i < j \leq 5} (x_i - x_j)^2$$

du polynôme P est égal à $5^5 \cdot 3^4 - 4^4 \cdot 6^5$. En déduire que la seule sous-extension quadratique de L est $\mathbf{Q}(\sqrt{-21451})$ (vous aurez sans doute besoin d'aller consulter la littérature sur le discriminant d'un polynôme ; *cf.* par exemple [**CL**], § 1.5 et § 3.4).

Exercice 6.28. — Soit K un corps, soit $P \in K[X]$ un polynôme irréductible séparable de degré $n \geq 3$ et soit $K \hookrightarrow L$ un corps de décomposition de P, où il est scindé à racines simples $a_1, \ldots, a_n$. Si le groupe $\mathrm{Gal}(L/K)$ est isomorphe à $\mathfrak{S}_n$, montrer que les corps de rupture $K(a_i)$ de P (tous K-isomorphes) vérifient $K(a_i) \cap K(a_j) = K$ pour $1 \leq i < j \leq n$.

6.5. Clôture galoisienne. — On montre qu'une extension séparable finie est toujours contenue dans une extension galoisienne finie, qui n'est autre que sa clôture normale (*cf.* prop. 4.6).

Proposition 6.29. — *Soit $K \hookrightarrow L$ une extension finie séparable de corps et soit Ω un corps algébriquement clos contenant L. La clôture normale de L dans Ω est une extension finie galoisienne de K. On l'appelle la* clôture galoisienne *de L dans Ω.*

Cette proposition permet de retrouver le fait qu'il n'existe qu'un nombre fini d'extensions intermédiaires entre K et L (*cf.* th. 5.23).

Démonstration. — Dans la preuve de la prop. 4.6, et en gardant les mêmes notations, le polynôme P_i est séparable, donc aussi le ppcm $P_1 \vee \cdots \vee P_n$, donc l'extension normale $K \hookrightarrow M$ est séparable. □

Exercice 6.30. — On admettra que si M est une matrice carrée à coefficients dans un corps algébriquement clos $\overline{K}$, il existe un *unique* couple (D_M, N_M) de matrices à coefficients dans $\overline{K}$ telles que $M = D_M + N_M$, $D_M N_M = N_M D_M$, D_M est diagonalisable et N_M est nilpotente.

a) Si M est à coefficients réels, montrer qu'il en est de même pour D_M et N_M.

b) Si M est à coefficients rationnels, montrer qu'il en est de même pour D_M et N_M (*Indication :* on pourra utiliser la théorie de Galois).

c) Si M est à coefficients dans un corps parfait K, montrer qu'il en est de même pour D_M et N_M.

d) On considère la matrice $M = \begin{pmatrix} 0 & T \\ 1 & 0 \end{pmatrix}$ à coefficients dans $K := \mathbf{F}_2[T]$. Montrer que les matrices D_M et D_N ne sont pas à coefficients dans K.

7. Théorie de Galois générale

Que devient la théorie de Galois pour une extension $K \hookrightarrow L$ galoisienne (c'est-à-dire séparable et normale) pas nécessairement finie ? Nous allons présenter quelques résultats sans preuve (voir [**B1**], Chap. V, § 10, pour plus de détails). Soit $G := \mathrm{Gal}(L/K)$ le groupe de Galois. On a encore $K = L^G$ (*cf.* lemme 6.21) ; en particulier, le groupe G est fini si et seulement si l'extension $K \hookrightarrow L$ est finie (exerc. 6.23).

On peut encore définir, comme dans le th. 6.20, des applications

$$\begin{array}{ccc} \{\text{sous-groupes de } G\} & \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} & \{\text{extensions intermédiaires entre } K \text{ et } L\} \\ H & \longmapsto & L^H := \{x \in L \mid \forall g \in H\ g(x) = x\} \\ \mathrm{Gal}(L/M) & \longmapsfrom & M \end{array}$$

et on a toujours $\Phi \circ \Psi = \mathrm{Id}$. En particulier, Ψ est injective ; cependant, son image ne consiste qu'en certains sous-groupes de G : ceux qui sont *fermés* pour une certaine topologie dont on munit G.

Si K est un corps et $\overline{K}^s$ une clôture séparable de K (*cf.* § 5.3), on peut alors considérer le groupe (topologique) $\mathrm{Gal}(\overline{K}^s/K)$, appelé *groupe de Galois absolu de* K, qui gouverne toutes les extensions algébriques séparables de K ! Pour tout entier premier p, on a par exemple $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p) \simeq \widehat{\mathbf{Z}}$ (le *complété profini* de $\mathbf{Z}$) ; mais nous sommes encore bien loin de comprendre l'énorme groupe $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$... (*cf.* exerc. 8.10 et 8.19).

8. Applications de la théorie de Galois

8.1. Correspondance de Galois pour les corps finis. — Soit p un nombre premier. Comme $\mathbf{F}_{p^n}$ est le corps de décomposition du polynôme $X^{p^n} - X \in \mathbf{F}_p[X]$ (th. 5.27) et que toute extension de corps finis est séparable (tout corps fini est parfait par le th. 5.7), l'extension $\mathbf{F}_p \hookrightarrow \mathbf{F}_{p^n}$ est galoisienne et son groupe de Galois est de cardinal n

Proposition 8.1. — *Le groupe de Galois de l'extension $\mathbf{F}_p \hookrightarrow \mathbf{F}_{p^n}$ est cyclique d'ordre n, engendré par l'automorphisme de Frobenius* $\mathrm{Fr} : x \mapsto x^p$.

Démonstration. — Il est clair que Fr est dans $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ et que $\mathrm{Fr}^n = \mathrm{Id}_{\mathbf{F}_{p^n}}$. Soit m son ordre, un diviseur de n. On a alors $\mathrm{Fr}^m = \mathrm{Id}_{\mathbf{F}_{p^n}}$, d'où $x^{p^m} = x$ pour tout x dans $\mathbf{F}_{p^n}$. Tous les éléments de $\mathbf{F}_{p^n}$ sont ainsi racines du polynôme $X^{p^m} - X$, donc $\mathrm{Card}(\mathbf{F}_{p^n}) \leq p^m$ et $m = n$. Comme le groupe $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ est de cardinal n, il est cyclique engendré par Fr. □

Comme les sous-groupes du groupe cyclique $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p) \simeq \mathbf{Z}/n\mathbf{Z}$ sont les sous-groupes cycliques engendrés par les classes de chacun des diviseurs de n, le théorème principal de la théorie de Galois (th. 6.20) nous dit que les seuls sous-corps de $\mathbf{F}_{p^n}$ sont les

$$\mathbf{F}_{p^m} = \{x \in \mathbf{F}_{p^n} \mid x^{p^m} = x\}.$$

En particulier, le corps $\mathbf{F}_{p^n}$ est une extension de $\mathbf{F}_{p^m}$ si et seulement si m divise n et $\mathbf{F}_{p^n}$ a un unique sous-corps à p^m éléments. Le groupe de Galois de l'extension $\mathbf{F}_{p^m} \hookrightarrow \mathbf{F}_{p^n}$ est cyclique d'ordre n/m, engendré par Fr^m.

Exercice 8.2. — Soient m et n des entiers positifs non nuls. Quel est le nombre de racines du polynôme $X^{p^m} - X$ dans $\mathbf{F}_{p^n}$?

Corollaire 8.3. — *Pour tout entier premier p et tout entier $n > 0$, on a*

$$X^{p^n} - X = \prod_{m|n} \text{(polynômes irréductibles unitaires de degré } m \text{ dans } \mathbf{F}_p[X]).$$

Démonstration. — Le groupe $G = \mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ agit sur $\mathbf{F}_{p^n}$; soit $\mathbf{F}_{p^n} = O_1 \cup \cdots \cup O_N$ la décomposition en orbites. Pour chaque $i \in \{1, \ldots, N\}$, on pose $P_i = \prod_{x \in O_i}(X - x)$, de sorte que

$$X^{p^n} - X = \prod_{x \in \mathbf{F}_{p^n}} (X - x) = \prod_{i=1}^{N} \prod_{x \in O_i} (X - x) = \prod_{i=1}^{N} P_i.$$

Comme $\mathrm{Fr}(P_i) = P_i$, le polynôme P_i est à coefficients dans $\mathbf{F}_p$. Comme Fr agit transitivement sur l'ensemble de ses racines, il est irréductible sur $\mathbf{F}_p$ (prop. 6.17). Son degré est $\mathrm{Card}(O_i)$, qui est un diviseur de $\mathrm{Card}(G) = n$. On a donc écrit la décomposition en facteurs irréductibles dans $\mathbf{F}_p[X]$ du polynôme $X^{p^n} - X$. Il n'y a pas de facteur multiple car ce polynôme est séparable.

Inversement, soit P un polynôme irréductible dans $\mathbf{F}_p[X]$ de degré m, soit $\mathbf{F}_p \hookrightarrow K$ un corps de rupture de P et soit x une racine de P dans K. Cette extension est de degré m, de sorte que K est isomorphe à $\mathbf{F}_{p^m}$ et $x^{p^m} = x$. Si m divise n, on a $x^{p^n} = x$, et P, qui est le polynôme minimal de x, divise donc $X^{p^n} - X$. □

8.2. Constructibilité à la règle et au compas, polynômes cyclotomiques. — Revenons sur les constructions à la règle et au compas telles qu'elles sont expliquées dans le § 2.5. Plus précisément, on s'intéresse ici au nombres complexes z constructibles à partir de $\{0, 1\}$ (cela signifie par définition que ses parties réelle et complexe sont toutes deux constructibles). On peut déduire du théorème de Wantzel (th. 2.23, qui traite le cas $z \in \mathbf{R}$) que z est alors algébrique de degré une puissance de 2 sur $\mathbf{Q}$. On a déjà remarqué que cette condition n'est pas suffisante (exerc. 2.28).

Théorème 8.4. — *Un nombre algébrique $z \in \mathbf{C}$ est constructible si et seulement si le degré de l'extension de $\mathbf{Q}$ engendrée par tous les conjugués* [6] *de z est une puissance de 2.*

Démonstration. — Soit $z \in \mathbf{C}$. On note L le sous-corps de $\mathbf{C}$ engendré par tous les conjugués de z (c'est-à-dire le corps de décomposition du polynôme minimal de z sur $\mathbf{Q}$).

Supposons z constructible. Montrons que tous ses conjugués sont constructibles. Soit

$$\mathbf{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

une suite d'extensions telle que $[K_i : K_{i-1}] = 2$ et $z \in K_n$, et soit M la clôture normale de K_n dans $\mathbf{C}$. C'est une extension galoisienne de $\mathbf{Q}$ et pour tout conjugué z' de z, il existe $g \in \mathrm{Gal}(M/\mathbf{Q})$ tel que $z' = g(z)$ (*cf.* prop. 6.17). Les corps $g(K_i)$ forment une suite d'extensions de degré 2, donc z', qui est dans $g(K_n)$, est constructible par le théorème de Wantzel. En particulier, (*cf.* th. 2.22, qui s'étend facilement aux nombres complexes constructibles), tous les éléments de L sont constructibles. Le corps L est une extension séparable de $\mathbf{Q}$, donc elle est engendrée par un élément $x \in L$ tel que $L = \mathbf{Q}[x]$ (th. 5.22), dont on vient de montrer qu'il est constructible. Son degré $[L : \mathbf{Q}]$ est donc une puissance de 2.

Inversement, supposons que $[L : \mathbf{Q}] = 2^m$. Le groupe $\mathrm{Gal}(L/\mathbf{Q})$ est alors d'ordre 2^m donc il existe une suite de sous-groupes

$$\mathrm{Gal}(L/\mathbf{Q}) = G_0 > \cdots > G_{m-1} > G_m = \{\mathrm{Id}\}$$

tels que G_i est d'indice 2 dans G_{i-1}. La correspondence de Galois (th. 6.20) lui associe une suite

$$\mathbf{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = L$$

d'extensions de degré 2. Par le théorème de Wantzel, tout élément de L est constructible (donc en particulier z !). □

Exercice 8.5. — Montrer qu'aucune racine du polynôme $X^4 - X - 1$ n'est constructible (*cf.* ex. 2.28). Quel est le groupe de Galois (sur $\mathbf{Q}$) de ce polynôme ?

6. C'est-à-dire les racines dans $\mathbf{C}$ du polynôme minimal de z sur $\mathbf{Q}$.

Dans le but d'étudier la constructibilité des polygones réguliers, nous nous intéressons maintenant au groupe de Galois des polynômes $X^n - 1$.

Proposition 8.6. — *Soit K un corps et soit n un entier strictement positif non divisible par la caractéristique de K. Le groupe de Galois du polynôme séparable $X^n - 1 \in K[X]$ est isomorphe à un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$. Il est en particulier abélien.*

En particulier, toute sous-extension de l'extension $\mathbf{Q}(e^{2i\pi/n})$ de $\mathbf{Q}$ est galoisienne de groupe de Galois abélien. Un théorème difficile, dit de Kronecker-Weber (mais dont la première démonstration complète est due à Hilbert), assure que la réciproque est vraie ! On démontre aujourd'hui ce résultat comme conséquence de la théorie du corps de classes, qui débouche naturellement sur la théorie de Langlands...

Démonstration. — Soit $K \hookrightarrow L$ un corps de décomposition de $X^n - 1$. Le groupe multiplicatif $\mu_n(L)$ des racines n-ièmes de l'unité dans L est d'ordre n et est cyclique (prop. 2.2), donc isomorphe à $(\mathbf{Z}/n\mathbf{Z}, +)$. Tout élément g de $\mathrm{Gal}(L/K)$ induit un automorphisme de $\mu_n(L)$, donc de $(\mathbf{Z}/n\mathbf{Z}, +)$ et cet automorphisme détermine uniquement g. Un tel automorphisme est déterminé par l'image de 1, qui doit être un générateur de ce groupe, donc une unité de l'anneau $(\mathbf{Z}/n\mathbf{Z}, +, \times)$. On a donc une injection de $\mathrm{Gal}(L/K)$ dans $(\mathbf{Z}/n\mathbf{Z})^*$. □

Exemple 8.7. — On a déjà rencontré (en § 5.5) une situation dans laquelle le lemme s'applique : si p est un nombre premier, $q = p^n$ et $K = \mathbf{F}_p$, le corps de décomposition du polynôme séparable $X^{q-1} - 1$ est $\mathbf{F}_q$. On a vu que le groupe de Galois de l'extension galoisienne $\mathbf{F}_p \hookrightarrow \mathbf{F}_q$ est cyclique d'ordre n. La proposition dit que c'est un sous-groupe de $(\mathbf{Z}/(q-1)\mathbf{Z})^*$, qui en est en général distinct.

Soit K un corps, soit n un entier non divisible par la caractéristique de K et soit $K \hookrightarrow L$ un corps de décomposition de $X^n - 1$. La démonstration de la proposition montre que le polynôme séparable

$$\Phi_n^K(X) = \prod_{\substack{\zeta \text{ racine primitive} \\ n\text{-ième de 1 dans } L}} (X - \zeta)$$

est de degré $\varphi(n)$ et invariant sous l'action de $\mathrm{Gal}(L/K)$, donc à coefficients dans K par le lemme d'Artin (th. 6.22). On l'appelle le n-ième *polynôme cyclotomique ;* son corps de décomposition, qui est aussi le corps de décomposition de $X^n - 1$, s'appelle un *corps cyclotomique.*

On peut montrer que $\Phi_n^{\mathbf{Q}}$ est irréductible, de sorte que le groupe de Galois de $X^n - 1$ sur $\mathbf{Q}$ est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$. En revanche, $\Phi_n^{\mathbf{F}_p}$ n'est pas toujours irréductible (on a par exemple $\Phi_{mp}^{\mathbf{F}_p} = (\Phi_m^{\mathbf{F}_p})^{p-1}$ si $m \wedge p = 1$).

Exercice 8.8. — Calculer Φ_n^K pour $1 \leq n \leq 6$ et pour tout n premier. Pour tout entier $n \geq 1$, montrer l'égalité

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

(En particulier, $\Phi_n^K(X)$ ne dépend en fait pas du corps K (toujours lorsque n est premier à la caractéristique de K).)

Exercice 8.9. — Soient m et n des entiers ≥ 1. Déterminer un générateur pour les corps

$$\mathbf{Q}[e^{2i\pi/m}, e^{2i\pi/n}] \quad \text{et} \quad \mathbf{Q}[e^{2i\pi/m}] \cap \mathbf{Q}[e^{2i\pi/n}].$$

Exercice 8.10. — **(Problème de Galois inverse sur Q pour les groupes abéliens finis)** En utilisant à bon escient les faits suivants :

- structure des groupes abéliens finis (th. II.4.10) ;
- théorème de la progression arithmétique de Dirichlet : pour tout entier $n > 1$, il existe une infinité de nombres premiers congrus à 1 modulo n,

montrer que tout groupe abélien fini est groupe de Galois d'une extension galoisienne de $\mathbf{Q}$, donc quotient de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ (*Indication :* on pourra utiliser les corps cyclotomiques).

On termine cette section par un théorème qui identifie les polygones réguliers constructibles à la règle et au compas. Rappelons qu'un *nombre premier de Fermat* est un nombre premier de la forme $F_m := 2^{2^m}+1$. 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 $F_6, \ldots, F_{32}$ et $F_{2543548}$ ne sont pas premiers [7].

Théorème 8.11. — *Un polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n est le produit d'une puissance de 2 et de nombres premiers de Fermat distincts.*

Démonstration. — Soit $\mathscr{N}$ l'ensemble des nombres entiers $n \geq 1$ tels que le polygone régulier à n côtés soit constructible à la règle et au compas. Si $n \in \mathscr{N}$, alors $2n \in \mathscr{N}$ (on peut bissecter n'importe quel angle constructible), et tout diviseur de n est dans $\mathscr{N}$. De plus, si m et n sont dans $\mathscr{N}$ et sont premiers entre eux, alors $mn \in \mathscr{N}$: en effet, $\exp(2i\pi/m)$ et $\exp(2i\pi/n)$ sont alors constructibles, et si u et v sont des entiers tels que $um + vn = 1$, on a

$$\exp(2i\pi/mn) = \exp(2i\pi/m)^u \exp(2i\pi/n)^v,$$

de sorte que $\exp(2i\pi/mn)$ est aussi constructible.

Il suffit donc de montrer que les seuls nombres premiers impairs p qui appartiennent à $\mathscr{N}$ sont des nombres premiers de Fermat, et que le carré d'un nombre premier impair n'est pas dans $\mathscr{N}$.

Soit p un nombre premier impair. Les deux assertions découlent du th. 8.4 et du fait que le degré de $\exp(2i\pi/p^2)$ sur $\mathbf{Q}$ est $\varphi(p^2) = p(p-1)$ tandis que le degré de $\exp(2i\pi/p)$ sur $\mathbf{Q}$ est $\varphi(p) = p-1$ (on a besoin ici de l'irréductibilité des polynômes cyclotomiques $\Phi_{p^2}^{\mathbf{Q}}$ et $\Phi_p^{\mathbf{Q}}$; celle du second se démontre facilement à l'aide du critère d'Eisenstein ; *cf.* exerc. III.1.13). Ensuite, $p(p-1)$, impair, n'est donc jamais une puissance de 2, tandis que si $p-1$ s'écrit 2^r, alors r doit lui-même être une puissance de 2 (pourquoi ?). □

On retrouve le fait que le polygone régulier à 9 côtés n'est pas constructible à la règle et au compas (cor. 2.29).

Corollaire 8.12 **(Gauss, 1801)**. — *Le polygone régulier à 17 côtés est constructible à la règle et au compas.*

Exercice 8.13. — On pose $\zeta = \exp(2i\pi/17)$. Le groupe de Galois G du polynôme $X^{17}-1$, c'est-à-dire celui de l'extension $\mathbf{Q} \subseteq \mathbf{Q}(\zeta)$, est isomorphe au groupe multiplicatif $((\mathbf{Z}/17\mathbf{Z})^*, \times)$ (prop. 8.6).

a) Montrer que ce groupe est engendré par la classe de 3 ; on note $g \in G$ le générateur correspondant.
b) On pose $a_0 = \sum_{k=0}^{7} g^{2k}(\zeta)$ et $a_1 = \sum_{k=0}^{7} g^{2k+1}(\zeta)$. Calculer $a_0 + a_1$ et $a_0 a_1$, puis a_0 et a_1 (un signe est difficile à déterminer).
c) Pour $0 \leq j \leq 3$, on pose $b_j = \sum_{k=0}^{3} g^{4k+j}(\zeta)$. Calculer $b_0 + b_2$ et $b_0 b_2$, puis b_0, b_2, b_1, b_3 (là encore, les signes sont difficiles à déterminer).
d) Pour $0 \leq j \leq 7$, on pose $c_j = g^j(\zeta) + g^{8+j}(\zeta)$. Calculer $c_0 + c_4$, $c_0 c_4$, puis $\cos 2\pi/17$.

8.3. Extensions cycliques. — Soit K un corps et soit n un entier ≥ 2. On fait l'hypothèse que le groupe $\mu_n(K)$ des racines n-ièmes de l'unité est d'ordre n. Cela entraîne que la caractéristique de K ne divise pas n et que le polynôme $X^n - 1$ est séparable (il n'a pas de racine commune avec son polynôme dérivé). Rappelons enfin que le groupe $\mu_n(K)$ est toujours cyclique (*cf.* prop. 2.2 ; dans notre cas, il est donc isomorphe à $\mathbf{Z}/n\mathbf{Z}$). Les générateurs de ce groupe sont les racines primitives.

7. Cela ne veut pas dire que l'on sait tous les factoriser : si on sait par exemple factoriser explicitement $F_6 = 274177 \cdot 67280421310721$, F_7, F_8, F_9, F_{10} et F_{11} (un nombre de 617 chiffres), et que l'on connaît explicitement un facteur non trivial pour F_{14}, F_{22}, F_{31} et $F_{2543548}$ (à savoir $9 \times 2^{22543551} + 1$; en fait, Euler a montré que tout diviseur de F_n, pour > 2, est du type $k2^{n+2} + 1$), on ne connaît aucun facteur non trivial pour les nombres F_{20} et F_{24}.

Sous cette hypothèse, nous allons déterminer toutes les *extensions cycliques* de degré n de K, c'est-à-dire les extensions galoisiennes de groupe de Galois $\mathbf{Z}/n\mathbf{Z}$.

Lemme 8.14. — *Soit K un corps tel que $\mathrm{Card}(\mu_n(K)) = n$ et soit $a \in K$. Si une extension de corps $K \hookrightarrow L$ est engendrée par une racine du polynôme $X^n - a$, cette extension est galoisienne et $\mathrm{Gal}(L/K)$ est un sous-groupe de $\mu_n(K)$. En particulier, c'est un groupe cyclique.*

Démonstration. — Soit x une racine de $X^n - a$ engendrant L. Les racines de ce polynôme sont les ζx, pour $\zeta \in \mu_n(K)$, et elles sont toutes dans L par hypothèse. L'extension $K \hookrightarrow L$ est donc un corps de décomposition du polynôme séparable $X^n - a$, donc est galoisienne.

Tout élément g de $\mathrm{Gal}(L/K)$ permute les racines de $X^n - a$ et est déterminé par l'image $\zeta_g x$ de x (puisque les éléments ζ de $\mu_n(K) \subseteq K$ sont fixes), d'où un morphisme de groupes injectif $\mathrm{Gal}(L/K) \hookrightarrow \mu_n(K)$ envoyant g sur ζ_g. □

Exemple 8.15. — On a déjà vu, dans l'ex. 6.25, un cas où le lemme s'applique : c'est celui de l'extension $\mathbf{Q}(j) \subseteq \mathbf{Q}(\sqrt[3]{2}, j)$, qui est galoisienne de groupe de Galois isomorphe à $\mathbf{Z}/3\mathbf{Z}$. En revanche, il ne s'applique pas à l'extension (non galoisienne) $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2})$, car $\mathbf{Q}$ ne contient pas toutes les racines cubiques de 1.

Théorème 8.16 **(Kummer)**. — *Soit K un corps tel que $\mathrm{Card}(\mu_n(K)) = n$. Une extension $K \hookrightarrow L$ est cyclique d'ordre n si et seulement s'il existe $a \in K$ avec $a \notin K^d$ pour tout diviseur $d > 1$ de n, tel que L est le corps de décomposition de $X^n - a$; ce polynôme est alors irréductible, et L est aussi son corps de rupture.*

Cet énoncé généralise le lemme 2.24, qui traitait le cas des extensions de degré 2.

Démonstration. — Supposons que L est un corps de décomposition de $P(X) = X^n - a$, avec $a \notin K^d$ pour tout diviseur $d > 1$ de n. Soit $x \in L$ une racine de P. On a

$$P(X) = \prod_{\zeta \in \mu_n(K)} (X - \zeta x)$$

dans $L[X]$. Comme L est engendré par les racines de P, et que tous les ζ sont dans K, il l'est aussi par x. Par le lemme 8.14, $K \hookrightarrow L$ est galoisienne cyclique (d'ordre $[L : K]$). Il suffit donc de montrer que P est irréductible (ce sera ainsi le polynôme minimal de x).

Soit $Q \in K[X]$ un facteur unitaire de P, de degré $e > 0$. Son coefficient constant est produit de e facteurs ζx, avec $\zeta \in K$, donc $x^e \in K$. Comme $x^n = a \in K$, par le théorème de Bézout, on a $x^d \in K$, où $d = n \wedge e$, de sorte que $a = x^n = (x^d)^{n/d}$. L'hypothèse faite entraîne $n = d$, donc $P = Q$ et P est irréductible.

Montrons la réciproque : on suppose $\mathrm{Gal}(L/K)$ cyclique d'ordre n et on en prend un générateur g, que l'on considère comme un endomorphisme du K-espace vectoriel L. Comme $g^n = \mathrm{Id}_L$ et que $X^n - 1$ est scindé à racines simples dans K, l'endomorphisme g est diagonalisable. Les valeurs propres de g forment un sous-groupe de $\mu_n(K)$: si λ et μ sont des valeurs propres, et que $g(x) = \lambda x$ et $g(y) = \mu y$, avec x et y non nuls, on a $g(xy^{-1}) = g(x)g(y)^{-1} = \lambda\mu^{-1}(xy^{-1})$, de sorte que $\lambda\mu^{-1}$ est aussi une valeur propre.

Par la prop. 2.2, ce sous-groupe (fini) est cyclique d'ordre un diviseur d de n. On a alors $g^d = \mathrm{Id}_L$, d'où $d = n$ puisque g est d'ordre n. Donc il existe $x \in L - \{0\}$ tel que $g(x) = \zeta x$ où ζ est une racine primitive n-ième de l'unité. Considérons le polynôme

$$\prod_{i=1}^{n} (X - \zeta^i x) = X^n - a,$$

avec $a = x^n$. C'est un polynôme séparable scindé dans L, qui est invariant sous l'action de g, donc de $\mathrm{Gal}(L/K)$. Il est donc à coefficients dans K par le lemme d'Artin (th. 6.22). Comme le groupe $\mathrm{Gal}(L/K)$ agit transitivement sur ses racines, il est irréductible dans $K[X]$ (prop. 6.17). Son corps de décomposition est de degré n sur K et contenu dans L, donc c'est L. Enfin, si $d > 1$ divise n, et $a = b^d$, le polynôme irréductible $X^n - a = (X^{n/d})^d - b^d$ est divisible par $X^{n/d} - b$, donc $b \notin K$. □

Sans l'hypothèse faite sur K, la conclusion du théorème n'est en général plus valide. Par exemple, si $\mathbf{Q} \hookrightarrow L$ est une extension galoisienne de degré 3 (par exemple l'extension $L = \mathbf{Q}(\cos 2\pi/9)$, où $\cos 2\pi/9$ est une racine de $X^3 - X + 1$; *cf.* la preuve du cor. 2.29), elle ne peut pas être engendrée par des éléments x tels que $x^3 \in \mathbf{Q}$: comme elle est galoisienne, elle devrait contenir une racine cubique non triviale de 1, ce qui n'est pas le cas !

Dans une direction différente, si K est de caractéristique $p > 0$ (la seule racine p-ième de l'unité est alors 1, donc $\mathrm{Card}(\mu_p(K)) = 1$), on peut décrire les extensions galoisiennes $K \hookrightarrow L$ de groupe de Galois $\mathbf{Z}/p\mathbf{Z}$: c'est la théorie d'Artin-Schreier, qui montre qu'il existe $a \in K$ tel que L soit le corps de décomposition de $X^p - X - a$ (*cf.* exerc. 8.17 et 8.18 ci-dessous).

Exercice 8.17. — Soit K un corps de caractéristique $p > 0$ et soit $a \in K$. On pose $P(X) = X^p - X - a$ et on note $K \hookrightarrow L$ un corps de décomposition de P.

a) Si x est une racine de P dans L, montrer que les racines de P sont $x, x+1, \ldots, x+p-1$.
b) Montrer que P est soit scindé, soit irréductible dans $K[X]$.
c) Si P n'a pas de racine dans K, montrer $\mathrm{Gal}(L/K) \simeq \mathbf{Z}/p\mathbf{Z}$.

Exercice 8.18. — Soit K un corps de caractéristique $p > 0$ et soit $K \hookrightarrow L$ une extension galoisienne de groupe de Galois isomorphe à $\mathbf{Z}/p\mathbf{Z}$. Soit g un générateur de ce groupe.

a) Montrer qu'il existe $y \in L$ tel que $\sum_{j=0}^{p-1} g^j(y) = 1$ (*Indication :* on pourra utiliser le th. 5.35 et l'exerc. 6.19). On pose $x = \sum_{j=0}^{p-1} j g^j(y)$.
b) Calculer $g(x)$ et montrer que $a = x^p - x$ est dans K.
c) En déduire que L est un corps de décomposition du polynôme $X^p - X - a$.

Exercice 8.19 **(Éléments d'ordre fini de** $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$**)**. — Soit K un corps de caractéristique nulle.

a) Soit $a \in K$, soit p un nombre premier et soit $r \in \mathbf{N}^*$. Montrer que le polynôme $X^{p^r} - a$ est irréductible dans $K[X]$ si et seulement si soit $p \geq 3$ et $a \notin K^p$, soit $p = 2$ et $a \notin -4K^4$ (*Indication :* lorsque $p = 2$, on pourra discuter une éventuelle factorisation dans $K(\sqrt{-1})[X]$).
b) Soit $K \hookrightarrow L$ une extension finie. Si le corps L est algébriquement clos, montrer $L = K(\sqrt{-1})$ (*Indication :* on pourra commencer par supposer $-1 \in K^2$ et considérer une extension intermédiaire d'indice premier dans L).
c) Montrer que tous les éléments d'ordre fini de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sont d'ordre 2.

Exercice 8.20. — Soit p un nombre premier et soit m un entier qui n'est pas la puissance p-ième d'un nombre entier. On note $\zeta := \exp(2i\pi/p)$ et $P(X) := X^p - m \in \mathbf{Q}[X]$.

a) Montrer que m n'est pas la puissance p-ième d'un élément de $\mathbf{Q}(\zeta)$ (*Indication :* on pourra calculer de deux façon le déterminant de l'endomorphisme $\mathbf{Q}$-linéaire $x \mapsto mx$ du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}(\zeta)$).
b) Montre que le polynôme P est irréductible sur $\mathbf{Q}(\zeta)$. Quel est son groupe de Galois sur ce corps ?
c) Soit G le groupe de Galois du polynôme P sur $\mathbf{Q}$. Montrer qu'on a une suite exacte

$$0 \to \mathbf{Z}/p\mathbf{Z} \to G \to (\mathbf{Z}/p\mathbf{Z})^* \to 1.$$

8.4. Extensions radicales, équations résolubles par radicaux. — Étant donné un polynôme P, disons à coefficients rationnels, on aimerait savoir si chaque racine de P peut être exprimée au moyen d'une formule ne faisant intervenir que des nombres rationnels, les opérations arithmétiques usuelles (addition, soustraction, multiplication et division) et l'extraction de racines. Pour formuler ce problème de façon précise, nous sommes amenés à poser les définitions suivantes. On suppose (pour simplifier) dans cette section que l'on est en caractéristique 0.

Définition 8.21. — *Une extension $K \hookrightarrow L$ (de corps de caractéristique 0) est dite* radicale *s'il existe une suite d'extensions*

$$K = K_0 \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_n = L$$

telle qu'il existe pour chaque i un élément x_i de K_i et un entier $d_i > 0$ tels que $K_i = K_{i-1}(x_i)$ et $x_i^{d_i} \in K_{i-1}$.

On dit que L s'obtient à partir de K par adjonctions successives de racines. Il est clair que si $K \hookrightarrow L$ et $L \hookrightarrow M$ sont des extensions radicales (de corps de caractéristique 0), il en est de même de l'extension composée $K \hookrightarrow M$.

Définition 8.22. — *Soit K un corps de caractéristique 0. Un polynôme à coefficients dans K est dit* résoluble par radicaux *(sur K) s'il est scindé dans une extension radicale de K.*

Lemme 8.23. — *Soit $K \hookrightarrow L$ une extension radicale de corps de caractéristique 0. La clôture normale de L (dans n'importe quelle clôture algébrique) est encore une extension radicale de K.*

Démonstration. — Soit

$$K = K_0 \hookrightarrow \cdots \hookrightarrow K_{n-1} \hookrightarrow K_n = L$$

une suite d'extensions comme dans la déf. 8.21, avec $L = K_{n-1}(x)$ et $x^d \in K_{n-1}$. Soit $K \hookrightarrow M$ la clôture normale de $K \hookrightarrow K_{n-1}$ dans une extension algébriquement close Ω de L. La clôture normale de $K \hookrightarrow L$ dans Ω contient M et x, donc c'est la clôture normale M' de $M(x)$ dans Ω. En raisonnant par récurrence sur n, on voit qu'il suffit de montrer que l'extension $M \hookrightarrow M'$ est radicale.

Celle-ci est engendrée par tous les conjugués de x dans Ω, c'est-à-dire les racines dans Ω du polynôme minimal de x sur K, ou encore les images de x par tous les K-morphismes $\sigma : M \to \Omega$. Comme $x^d \in M$, on a $\sigma(x)^d \in \sigma(M)$, et $\sigma(M) = M$ puisque $K \hookrightarrow M$ est une extension normale. L'extension $M \hookrightarrow M'$ est donc obtenue en ajoutant successivement les éléments $\sigma(x)$ de Ω, dont la puissance d-ième est dans M. C'est bien une extension radicale. □

Théorème 8.24 **(Galois)**. — *Une extension galoisienne finie de corps de caractéristique 0 est contenue dans une extension radicale si et seulement si son groupe de Galois est résoluble* [8].

Démonstration. — Soit K un corps de caractéristique 0 et soit $K \hookrightarrow L$ une extension galoisienne contenue dans une extension radicale $K \hookrightarrow M$, que l'on peut par le lemme 8.23 supposer galoisienne. Comme tout quotient d'un groupe résoluble est résoluble, il suffit de montrer que le groupe $\mathrm{Gal}(M/K)$ est résoluble. Il existe une suite d'extensions

$$K = K_0 \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_n = M$$

avec $K_i = K_{i-1}(x_i)$ et $x_i^{d_i} \in K_{i-1}$. On aimerait pouvoir appliquer le lemme 8.14 aux extensions $K_{i-1} \hookrightarrow K_i$ pour dire qu'elle est cyclique, mais il faut auparavant pour cela ajouter des racines de l'unité à K. Considérons donc l'extension $K \hookrightarrow K'$ obtenue en adjoignant à K toutes les racines $d_1 \cdots d_n$-ièmes de l'unité, c'est-à-dire le corps de décomposition du polynôme $X^{d_1 \cdots d_n} - 1$ sur K. Par la prop. 8.6, c'est une extension galoisienne abélienne. Si on note $K_i \hookrightarrow K_i'$ l'extension analogue pour chaque i, on obtient une suite d'extensions

$$K \hookrightarrow K' = K_0' \subseteq K_1' \hookrightarrow \cdots \hookrightarrow K_n' =: M'$$

avec $K_i' = K_{i-1}'(x_i)$ et $x_i^{d_i} \in K_{i-1}'$. L'extension $K \hookrightarrow M$ est galoisienne donc c'est le corps de décomposition d'un polynôme $P \in K[X]$ (th. 4.2). L'extension $K \hookrightarrow M'$ est alors le corps de décomposition de

8. On rappelle qu'un groupe G est *résoluble* s'il existe une suite de sous-groupes $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{n-1} \triangleright G_n = \{\mathrm{Id}\}$ où les groupes G_{i-1}/G_i sont tous abéliens. Si G est fini, on peut même supposer ces quotients cycliques. Tout sous-groupe et tout groupe quotient d'un groupe résoluble est résoluble. Inversement, si H est un sous-groupe distingué de G et que H et G/H sont résolubles, alors G est résoluble.

$(X^{d_1\cdots d_n}-1)P(X)\in K[X]$: elle est galoisienne. La suite d'extensions ci-dessus correspond à une suite de sous-groupes

$$G:=\mathrm{Gal}(M'/K)>G_0>G_1>\cdots>G_n=\{\mathrm{Id}\},$$

avec $G_i=\mathrm{Gal}(M'/K'_i)$.

Considérons la suite d'extensions

$$K'_{i-1}\hookrightarrow K'_i\hookrightarrow M'.$$

Comme l'extension $K'_{i-1}\hookrightarrow K'_i$ est galoisienne cyclique (lemme 8.14), la correspondance de Galois nous dit que $G_i=\mathrm{Gal}(M'/K'_i)$ est distingué dans $G_{i-1}=\mathrm{Gal}(M'/K'_{i-1})$, avec G_{i-1}/G_i cyclique. De même, en considérant la suite d'extensions

$$K\hookrightarrow K'\hookrightarrow M',$$

on voit que $G_0=\mathrm{Gal}(M'/K')$ est distingué dans $G=\mathrm{Gal}(M'/K)$, avec $G/G_0\simeq\mathrm{Gal}(K'/K)$ abélien (prop. 8.6). Cela montre que G est résoluble, donc aussi son quotient $\mathrm{Gal}(M/K)$.

Inversement, supposons le groupe $\mathrm{Gal}(L/K)$ résoluble et montrons que L est contenu dans une extension radicale de K. Comme tout-à-l'heure, considérons l'extension galoisienne radicale $K\hookrightarrow K'$ obtenue en adjoignant à K toutes les racines d'ordre $[L:K]!$ de l'unité et l'extension analogue $L\hookrightarrow L'$, galoisienne abélienne (prop. 8.6). L'extension $K\hookrightarrow L'$ est galoisienne (comme plus haut, c'est le corps de décomposition d'un polynôme), le sous-groupe $\mathrm{Gal}(L'/L)$ de $\mathrm{Gal}(L'/K)$ est distingué, et le quotient est $\mathrm{Gal}(L/K)$.

Comme $\mathrm{Gal}(L/K)$ est résoluble et $\mathrm{Gal}(L'/L)$ abélien, $\mathrm{Gal}(L'/K)$ est résoluble (voir note 8), donc aussi son sous-groupe $G:=\mathrm{Gal}(L'/K')$, et il suffit de montrer que l'extension $K'\hookrightarrow L'$ est radicale (puisque l'extension $K\hookrightarrow K'$ l'est). Remarquons que son degré est $\leq[L:K]$ (si $L=K(a)$ (th. 5.22) et que le polynôme minimal de a sur K est P, de degré $[L:K]$, alors $L'=K'(a)$, et le polynôme minimal de a sur K divise P), donc que K' contient toutes les racines d'ordre $[L':K']!$ de l'unité.

Comme G est résoluble, il existe une suite de sous-groupes $G=G_0\triangleright G_1\triangleright\cdots\triangleright G_n=\{\mathrm{Id}\}$ où les quotients G_{i-1}/G_i sont tous cycliques. Par la théorie de Galois, elle correspond à une suite d'extensions $K'=K'_0\hookrightarrow K'_1\hookrightarrow\cdots\hookrightarrow K'_n=L'$, où chaque extension $K'_{i-1}\hookrightarrow K'_i$ est galoisienne cyclique, d'ordre $n_i:=[K'_i:K'_{i-1}]$: cela se voit en considérant comme plus haut la suite d'extensions $K'_{i-1}\hookrightarrow K'_i\hookrightarrow L'$. Comme $n_i\mid[L':K']!$, le corps K'_{i-1} contient les racines n_i-ièmes de l'unité, donc le théorème de Kummer (th. 8.16) s'applique et montre que l'extension $K'_{i-1}\hookrightarrow K'_i$ est radicale. L'extension $K'\hookrightarrow L'$ est donc bien radicale et ceci termine la démonstration du théorème. □

En particulier, le polynôme irréductible $P(X)=X^5-6X+3\in\mathbf{Q}[X]$, dont on a vu dans l'ex. 6.26 que le groupe de Galois est isomorphe à $\mathfrak{S}_5$, non résoluble, n'est pas résoluble par radicaux sur $\mathbf{Q}$.

Une autre façon de formuler la question posée au début de cette section est de demander s'il existe une « formule » ne faisant intervenir que des nombres rationnels, les opérations arithmétiques usuelles et l'extraction de racines, permettant d'exprimer les racines de l'équation « générale »

$$X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n,$$

en fonction de ses coefficients. On regarde cette équation comme étant à coefficients dans $\mathbf{Q}(a_0,\ldots,a_{n-1})$. On démontre alors assez facilement que le groupe de Galois de ce polynôme est isomorphe à $\mathfrak{S}_n$ [9], qui n'est pas résoluble pour $n\geq5$. Ce polynôme n'est donc pas résoluble par radicaux sur $\mathbf{Q}(a_0,\ldots,a_{n-1})$ (Abel, 1826).

9. Soient $x_1,\ldots,x_n$ les racines de ce polynôme dans un corps de décomposition. Les coefficients sont alors, au signe près, les polynômes symétriques élémentaires $\sigma_1,\sigma_2,\ldots,\sigma_n$ en les x_i. Il s'agit simplement de remarquer que le groupe de Galois de l'extension finie $\mathbf{Q}(\sigma_1,\sigma_2,\ldots,\sigma_n)\hookrightarrow\mathbf{Q}(x_1,\ldots,x_n)$ est isomorphe à $\mathfrak{S}_n$ (utiliser le lemme d'Artin, th. 6.22).

Exercice 8.25. — Soit K un sous-corps de $\mathbf{R}$. Une extension $K \subseteq L$ est dite *radicale réelle* si $L \subseteq \mathbf{R}$ et qu'il existe une suite d'extensions

$$K = K_0 \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_n = L$$

et, pour chaque i, un élément x_i de K_i et un entier $d_i > 0$ tels que $K_i = K_{i-1}(x_i)$ et $x_i^{d_i} \in K_{i-1}$. Soit $K \subseteq L$ une extension contenue dans une extension radicale réelle.

a) Montrer que $[L : K]$ est une puissance de 2.

b) Montrer que l'extension $\mathbf{Q} \subseteq \mathbf{Q}(\cos 2\pi/17)$ est contenue dans une extension radicale mais pas dans une extension radicale réelle.

c) Soit $P \in K[X]$ un polynôme irréductible de degré 3.

- Si P a trois racines réelles x, y et z, montrer qu'aucune des extensions $K \subseteq K(x)$, $K \subseteq K(x)$ ou $K \subseteq K(x)$, n'est contenue dans une extension radicale réelle.
- Si P n'a qu'une racine réelle x, montrer que l'extension $K \subseteq K(x)$ est contenue dans une extension radicale réelle.

Exercice 8.26. — Les polynômes $X^5 - 5X^2 + 1$ et $X^7 - 7X^2 + 1$ de $\mathbf{Q}[X]$ sont-il résolubles par radicaux ? (*Indication :* pour le second, on pourra utiliser le fait qu'un sous-groupe de $\mathfrak{S}_7$ engendré par un 7-cycle et une double transposition est soit $\mathfrak{A}_7$, soit un groupe simple à 168 éléments).

CHAPITRE II

MODULES

Soit A un anneau (commutatif unitaire). Un A-module est un groupe commutatif M muni d'une opération

$$\begin{array}{ccc} A \times M & \longrightarrow & M \\ (a, m) & \longmapsto & am \end{array}$$

qui vérifie les relations habituelles (les mêmes que pour un espace vectoriel [1]). On définit comme d'habitude sous-modules (par exemple, les sous-A-modules de A sont ses idéaux), sous-module engendré par une partie d'un module, modules quotients, sommes et produits directs de A-modules, système générateur, système libre, morphismes (de A-modules), noyau, image, dual... Il n'y a pas de piège ici. En revanche, contrairement à ce qui se passe dans la théorie des espaces vectoriels sur un corps, certains A-modules n'ont pas de base. Ceux qui en ont une sont isomorphes à une somme directe $A^{(\Lambda)}$ (ensemble des familles presque nulles d'éléments de A indexées par Λ), où Λ est un ensemble (pas nécessairement fini) ; on dit qu'ils sont *libres.*

Enfin, si M est un A-module et I un idéal de A, on note IM le sous-module de M formé des sommes finies $\sum_i a_i m_i$, avec $a_i \in I$ et $m_i \in M$.

Exemple 0.27. — Si A n'est pas un corps, il existe des tas de A-modules non libres, par exemple tous les A/I, où I est un idéal de A distinct de $\{0\}$ et de A.

Exercice 0.28. — Soit I un idéal non nul de A. Montrer que I est un A-module libre si et seulement si I est un idéal principal engendré par un non diviseur de zéro.

Exercice 0.29. — Déterminer, pour chaque $m, n \in \mathbf{N}$, le $\mathbf{Z}$-module $\mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}/m\mathbf{Z}, \mathbf{Z}/n\mathbf{Z})$.

1. Modules libres

Proposition 1.1. — *Soit A un anneau non nul et soit M un A-module libre. Toutes les bases de M ont le même cardinal. On l'appelle le* rang *de M.*

Démonstration. — On se ramène au résultat analogue pour les espaces vectoriels en procédant ainsi. Soit $(e_\lambda)_{\lambda\in\Lambda}$ une base de M. Soit $\mathfrak{m}$ un idéal maximal de A. Le quotient $k = A/\mathfrak{m}$ est un corps et $M/\mathfrak{m}M$ est un k-espace vectoriel dans lequel la famille des classes $(\bar{e}_\lambda)_{\lambda\in\Lambda}$ est génératrice. Montrons qu'elle est libre. Si on a une relation

$$\sum_{\lambda\in\Lambda} \bar{a}_\lambda \bar{e}_\lambda = 0$$

1. En particulier, $1_A \cdot m = m$ pour tout m dans M et le seul module sur l'anneau nul est le module nul !

dans $M/\mathfrak{m}M$, avec $a_\lambda \in A$, cela signifie

$$\sum_{\lambda\in\Lambda} a_\lambda e_\lambda \in \mathfrak{m}M.$$

Cette somme s'écrit donc $\sum_{j=1}^n b_j m_j$, avec $b_j \in \mathfrak{m}$ et $m_j \in M$. En décomposant chaque m_j sur la base $(e_\lambda)_{\lambda\in\Lambda}$, on voit que l'on peut aussi écrire cette somme $\sum_{\lambda\in\Lambda} c_\lambda e_\lambda$, avec $c_\lambda \in \mathfrak{m}$. La famille $(e_\lambda)_{\lambda\in\Lambda}$ étant libre, on en déduit pour pour tout $\lambda \in \Lambda$, on a $a_\lambda = c_\lambda \in \mathfrak{m}$, donc $\bar{a}_\lambda = 0$.

La famille $(\bar{e}_\lambda)_{\lambda\in\Lambda}$ est donc une base du k-espace vectoriel $M/\mathfrak{m}M$. Le cardinal de Λ est donc la dimension de cet espace vectoriel : il est indépendant de la base $(e_\lambda)_{\lambda\in\Lambda}$. □

Exercice 1.2. — Soit A un anneau non nul, soit M un A-module libre et soit N un sous-module *libre* de M. Montrer $\mathrm{rang}(N) \leq \mathrm{rang}(M)$.

Attention aux habitudes issues de la théorie des espaces vectoriels ! Par exemple, une famille libre à n éléments dans un module libre de rang n n'est pas nécessaire une base (par exemple, 2 n'est pas une base du $\mathbf{Z}$-module libre $\mathbf{Z}$, de rang 1). En revanche, toute famille génératrice à n éléments d'un A-module libre de rang n en est bien une base (cor. 3.4).

Exercice 1.3. — Montrer que le $\mathbf{Z}$-module $\mathbf{Q}$ n'est pas libre.

Exercice 1.4. — Tout espace vectoriel est libre. En particulier le $\mathbf{Q}$-espace vectoriel $\mathbf{Q}^{\mathbf{N}}$ des suites de nombres rationnels a une base (mais il faut l'axiome du choix pour montrer son existence). Nous allons montrer cependant que le $\mathbf{Z}$-module $M := \mathbf{Z}^{\mathbf{N}}$ n'est pas libre. Supposons par l'absurde qu'il admet une base $\mathscr{B}$.

a) Montrer que $\mathscr{B}$ n'est pas dénombrable.

b) Soit $e_n \in M$ la suite dont tous les termes sont nuls, sauf le n-ième qui vaut 1. On écrit e_n comme combinaison linéaire d'une partie finie $\mathscr{B}_n$ de $\mathscr{B}$ et on considère le sous-module (libre) $N \subseteq M$ engendré par la partie dénombrable $\bigcup_{n\in\mathbf{N}} \mathscr{B}_n$ de $\mathscr{B}$. Montrer que si $x \in M/N$ est non nul, il existe au plus un nombre fini d'entiers $k \in \mathbf{Z}$ tels que l'on puisse écrire $x = ky$, avec $y \in M/N$.

c) Montrer que la partie $S = \{(\varepsilon_n n!)_{n\in\mathbf{N}} \mid \varepsilon_n \in \{-1, 1\}\}$ de M n'est pas dénombrable. En déduire qu'il existe $s \in S$ tel que $s \notin N$.

d) Montrer que pour chaque $k \in \mathbf{Z}$, il existe $y \in M/N$ tel que $\bar{s} = ky$. Conclure.

2. Modules de torsion

Étant donné un élément m (même non nul) d'un A-module M, il peut très bien exister un élément non nul a de A tel que $am = 0$ (penser par exemple à 1 dans le $\mathbf{Z}$-module $\mathbf{Z}/n\mathbf{Z}$). On dit alors que m est un élément *de torsion* de M. *Si A est intègre* [2], l'ensemble

$$T(M) := \{m \in M \mid \exists a \in A - \{0\} \;\; am = 0\}$$

des éléments de torsion de M est un sous-module de M appelé *sous-module de torsion* de M. On dit que M est *sans torsion* si $T(M) = 0$ (c'est une condition nécessaire, mais pas suffisante (*cf.* exerc. 1.3), pour pouvoir être libre !). Le module quotient $M/T(M)$ est alors sans torsion.

3. Modules de type fini

On dit qu'un A-module est *de type fini* s'il admet une famille génératrice finie. Tout quotient d'un module de type fini est encore de type fini, mais un sous-module d'un module de type fini n'est pas nécessairement de type fini (c'est le cas, dans un anneau non noethérien, pour les idéaux qui ne sont pas de type fini ; *cf.* prop. III.2.1).

2. Dans le $\mathbf{Z}/6\mathbf{Z}$-module libre $\mathbf{Z}/6\mathbf{Z}$, les éléments de torsion sont 0, 2, 3 et 4 : ils ne forment pas un sous-module.

Exercice 3.1. — Soit M un A-module et soit N un sous-A-module de M. Si N et M/N sont de type fini, montrer que M est de type fini.

On rappelle que si R est une matrice carrée d'ordre n à coefficients dans un anneau A, on a la formule

$$R \cdot {}^t\mathrm{Com}(R) = \det(R) \cdot I_n$$

En particulier, R est inversible dans $\mathscr{M}_n(A)$ si et seulement si $\det(R)$ est une unité dans A.

Théorème 3.2 **(Cayley-Hamilton)**. — *Soit M un A-module de type fini et soit $u : M \to M$ un endomorphisme.*

Si $m_1, \ldots, m_n$ sont des générateurs de M, on peut écrire $u(m_i) = \sum_{j=1}^n a_{ij} m_j$, où la matrice $R = (a_{ij})_{1 \leq i,j \leq n}$ est dans $\mathscr{M}_n(A)$. Posons $P(X) = \det(XI_n - R) \in A[X]$. Alors $P(u) = 0$.

Il est important de remarquer que si I est un idéal de A tel que $u(M) \subseteq IM$, on peut prendre les a_{ij} dans I (le choix des a_{ij} n'est en général pas unique et on verra dans les applications qu'il est parfois crucial de le faire de façon astucieuse !). Si on écrit $P(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n$, on a alors $a_j \in I^j$.

Démonstration. — Munissons M d'une structure de $A[X]$-module en posant

$$\forall Q \in A[X] \ \ \forall m \in M \qquad Q \cdot m := Q(u)(m).$$

On a alors

$$(XI_n - R) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

où $XI_n - R$ est une matrice carrée d'ordre n à coefficients dans $A[X]$. En multipliant cette égalité à gauche par la transposée de la comatrice de $XI_n - R$, on obtient

$$\det(XI_n - R) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0,$$

ce qui signifie que $P(X) = \det(XI_n - R)$ annule le $A[X]$-module M, ou encore que $P(u)$ est nul sur M. □

Corollaire 3.3. — *Soit M un A-module de type fini. Tout endomorphisme surjectif de M est bijectif*[3].

Démonstration. — Soit $f : M \to M$ un endomorphisme surjectif. Comme dans la preuve du théorème, on munit M d'une structure de $A[X]$-module en posant $X \cdot m = f(m)$. Comme f est surjectif, on a $M = IM$, où $I = (X)$. Appliquons le th. 3.2 à $u = \mathrm{Id}_M$. On en déduit l'égalité suivante dans $\mathrm{End}_A(M)$:

$$u^n + P_1 u^{n-1} + \cdots + P_{n-1}u + P_n \,\mathrm{Id}_M = 0,$$

avec $P_j \in I^j = (X^j)$. En écrivant $P_j = XQ_j$, on obtient

$$\begin{aligned} \forall m \in M \qquad 0 &= (u^n + P_1 u^{n-1} + \cdots + P_{n-1}u + P_n \,\mathrm{Id}_M)(m) \\ &= m + P_1 \cdot m + \cdots + P_{n-1} \cdot m + P_n \cdot m \\ &= m + P_1(f)(m) + \cdots + P_{n-1}(f)(m) + P_n(f)(m) \\ &= m + f(Q_1(f) + \cdots + Q_{n-1}(f) + Q_n(f))(m), \end{aligned}$$

3. Attention ! Ce résultat ne généralise pas celui de l'exerc. III.2.14 : un endomorphisme d'anneaux (unitaires) $u : A \to A$ qui serait aussi un endomorphisme de A-modules devrait vérifier $u(a) = u(a1_A) = au(1_A) = a1_A = a$ pour tout a, donc seule l'identité convient !

c'est-à-dire $\mathrm{Id}_M + f \circ Q(f) = 0$ pour un polynôme $Q \in A[X]$. L'endomorphisme $-Q(f)$ de M est l'inverse de f. □

Corollaire 3.4. — *Soit M un A-module libre de rang n. Toute famille génératrice de M à n éléments est une base de M.*

Démonstration. — On peut supposer $M = A^n$. Une famille génératrice $\mathscr{B}$ à n éléments définit un endomorphisme surjectif $A^n \to A^n$. Le cor. 3.3 dit qu'il est bijectif, donc $\mathscr{B}$ est une base de M. □

Corollaire 3.5. — *Soit M un A-module de type fini et soit I un idéal tel que $IM = M$. Il existe $a \in I$ tel que $(1 + a)M = 0$.*

Démonstration. — Appliquons le th. 3.2 à $u = \mathrm{Id}_M$. On en déduit qu'il existe des $a_j \in I^j$ tels que $u^n + a_1 u^{n-1} + \cdots + a_{n-1}u + a_n \mathrm{Id}_M = 0$, d'où le corollaire avec $a = a_1 + \cdots + a_n$. □

Soit A un anneau non nul. On définit son *radical de Jacobson* comme l'intersection de ses idéaux maximaux :

$$\mathrm{rad}(A) := \bigcap_{\mathfrak{m} \subseteq A} \mathfrak{m}.$$

C'est un idéal de A.

Exemple 3.6. — On a $\mathrm{rad}(\mathbf{Z}) = \{0\}$. Si $\mathscr{C}$ est l'anneau des fonctions continues de $[0, 1]$ dans $\mathbf{R}$, on a aussi $\mathrm{rad}(\mathscr{C}) = \{0\}$ (exerc. I.1.6). Soit K un corps. Il y a une infinité de polynômes irréductibles dans $K[X]$ donc $\mathrm{rad}(K[X]) = \{0\}$. En revanche, dans l'anneau des séries formelles $K[[X]]$, il y a un seul idéal maximal (on dit que c'est un *anneau local)*, à savoir (X) (exerc. I.1.10). On a donc $\mathrm{rad}(K[[X]]) = (X)$.

Lemme 3.7. — *Pour tout anneau non nul A, on a*

$$\mathrm{rad}(A) = \{a \in A \mid 1 + xa \text{ est inversible pour tout } x \in A\}.$$

Démonstration. — Supposons $a \notin \mathrm{rad}(A)$. Il existe un idéal maximal $\mathfrak{m} \subseteq A$ tel que $a \notin \mathfrak{m}$. On a alors $\mathfrak{m} + (a) = A$, de sorte qu'il existe $m \in \mathfrak{m}$ et $x \in A$ tels que $1 = m + xa$. Comme $\mathfrak{m} \cap A^* = \varnothing$, cela entraîne $1 - xa \notin A^*$.

Inversement, si $1 + xa$ n'est pas inversible pour un $x \in A$, on a $(1 + xa) \subsetneq A$ et cet idéal est contenu dans un idéal maximal $\mathfrak{m}$ de A. Comme $1 \notin \mathfrak{m}$, cela entraîne $a \notin \mathfrak{m}$. □

Théorème 3.8 **(Lemme de Nakayama, 1951)**. — *Soit A un anneau non nul, soit I un idéal contenu dans $\mathrm{rad}(A)$ et soit M un A-module de type fini.*

a) *Si $IM = M$, on a $M = 0$.*
b) *Soient $m_1, \ldots, m_n$ des éléments de M ; si les images de $m_1, \ldots, m_n$ dans M/IM engendrent ce A-module, $m_1, \ldots, m_n$ engendrent M.*

Il semble que ce lemme soit en fait dû à Krull dans le cas où M est un idéal de A, puis à Azumaya dans le cas général.

Démonstration. — Le point a) résulte du cor. 3.5, puisque si $a \in \mathrm{rad}(A)$, l'élément $1 + a$ est inversible (lemme 3.7).

Supposons que les images de $m_1, \ldots, m_n$ dans M/IM engendrent ce A-module et considérons le A-module $N := M/(Am_1 + \cdots + Am_n)$. Soit $m \in M$. On peut écrire $m = \sum_{j=1}^n a_j m_j \pmod{IM}$ avec $a_1, \ldots, a_n \in A$, c'est-à-dire $m \in IM \pmod{Am_1 + \cdots + Am_n}$. On a ainsi $IN = N$, donc, puisque N est de type fini, $N = 0$ par a). Ceci se réécrit $M = Am_1 + \cdots + Am_n$, d'où b). □

Cet énoncé est particulièrement utile lorsque A est un anneau local, d'unique idéal maximal $\mathfrak{m}$. L'hypothèse de a) se réduit alors à $\mathfrak{m}M = M$, tandis que dans b), l'hypothèse est que les images de $m_1, \dots, m_n$ dans $M/\mathfrak{m}M$ engendrent ce $A/\mathfrak{m}$-espace vectoriel (dire que $m_1, \dots, m_n$ engendrent M/IM comme A-module est la même chose que de dire qu'ils l'engendrent comme A/I-module). Le corps $A/\mathfrak{m}$ s'appelle le *corps résiduel* de l'anneau local $(A, \mathfrak{m})$.

***Exemple 3.9* (Un exemple d'anneau local).** — Notons $\mathscr{C}$ l'anneau des fonctions continues de $[0, 2]$ dans $\mathbf{R}$. Soit $I \subseteq \mathscr{C}$ l'idéal des fonctions continues nulles dans un voisinage de 1. L'anneau quotient $A := \mathscr{C}/I$ est l'anneau des *germes de fonctions continues* en 1 (deux fonctions y sont identifiées si et seulement si elles coïncident au voisinage de 1). Les idéaux maximaux de A correspondent aux idéaux maximaux de $\mathscr{C}$ contenant I ; d'après l'exerc. I.1.6, il n'y en a qu'un : l'idéal $\mathfrak{m}_1$ des fonctions nulles en 1. L'anneau A est donc local, d'idéal maximal $\mathfrak{m}_1/I$ constitué des germes de fonctions nulles en 1 ; son corps résiduel est $\mathbf{R}$.

Cet exemple (qui est la version topologique de constructions analogues en géométrie algébrique) explique l'emploi de l'adjectif « local ».

4. Modules de type fini sur les anneaux principaux

Dans toute cette section, A est un anneau principal. Nous allons décrire tous les A-modules de type fini. J'ai choisi de présenter une approche matricielle de ce problème. Le point central de l'argument consiste à trouver, étant donnée une matrice M à coefficients dans A, une matrice équivalente à M la plus simple possible. On sait qu'une matrice M de rang r à coefficients dans un corps est équivalente à la matrice par blocs

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Nous allons montrer une version analogue de ce résultat pour les matrices à coefficients dans A. On a vu qu'une matrice carrée à coefficients dans un anneau A est inversible si et seulement si son déterminant est dans A^*. Le groupe (multiplicatif) des matrices inversibles d'ordre n à coefficients dans A est noté $\mathrm{GL}(n, A)$. Le sous-groupe distingué formé des matrices de déterminant 1 est noté $\mathrm{SL}(n, A)$.

Théorème 4.1. — *Soit M une matrice (non nécessairement carrée) à coefficients dans un anneau principal A. Il existe des matrices inversibles P et Q à coefficients dans A et des éléments non nuls $d_1, \dots, d_r$ de A tels que avec $d_1 \mid \cdots \mid d_r$ telles que*

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

L'entier r est uniquement déterminé. Les éléments $d_1, \dots, d_r$ de A sont aussi uniquement déterminés, à multiplication par une unité de A près ; on les appelle les facteurs invariants *de la matrice M.*

Bien sûr, l'entier r est le rang de la matrice M vue comme matrice à coefficients dans le corps des fractions de A.

On peut voir ce théorème comme la description des *classes d'équivalence* des matrices à coefficients dans un anneau principal. Il est beaucoup plus difficile de déterminer les *classes de similitude* (on sait le faire lorsque A est un corps ; *cf.* § 4.2).

Avant de commencer la preuve de ce théorème, faisons quelques rappels sur les *opérations élémentaires.* Par « opération élémentaire » sur les lignes (resp. sur les colonnes), nous entendrons uniquement ici « ajouter un multiple d'une ligne (resp. d'une colonne) à une autre ». Cela correspond à multiplier à gauche (resp. à droite) la matrice d'origine par une *matrice élémentaire,* c'est-à-dire une matrice qui ne diffère de la matrice identité que par un seul coefficient, situé hors de la diagonale. Une matrice élémentaire est inversible (son déterminant est 1) donc on obtient après des opérations élémentaires une matrice équivalente à la matrice d'origine (et de même déterminant). Nous noterons

$$E(n, A) < \mathrm{SL}(n, A)$$

le sous-groupe engendré par les matrices élémentaires.

Avec des opérations élémentaires, on peut aussi échanger deux lignes, l'une d'elles étant changée en son opposé :

$$\begin{pmatrix} L_i \\ L_j \end{pmatrix} \longrightarrow \begin{pmatrix} L_i \\ L_i + L_j \end{pmatrix} \longrightarrow \begin{pmatrix} -L_j \\ L_i + L_j \end{pmatrix} \longrightarrow \begin{pmatrix} -L_j \\ L_i \end{pmatrix}$$

(on ne peut pas juste échanger deux lignes, puisque le déterminant est inchangé par nos opérations élémentaires).

Lemme 4.2. — *Soit A un anneau principal et soient $a_1, \dots, a_s$ des éléments de A. Il existe un matrice carrée d'ordre s à coefficients dans A dont la première ligne est $\begin{pmatrix} a_1 & \cdots & a_s \end{pmatrix}$ et dont le déterminant est un pgcd de $a_1, \dots, a_s$.*

Démonstration. — On raisonne par récurrence sur s, le cas $s = 1$ étant évident. Supposons $s \geq 2$. Par hypothèse de récurrence, il existe donc une matrice carrée N d'ordre $s-1$ de première ligne $\begin{pmatrix} a_2 & \cdots & a_s \end{pmatrix}$ et de déterminant $d = a_2 \wedge \cdots \wedge a_s$. Soient x et y des éléments de A tels que

$$a_1 \wedge a_2 \wedge \cdots \wedge a_s = a_1 \wedge d = a_1 x + dy.$$

La matrice

$$\begin{pmatrix} a_1 & & \\ 0 & & \\ \vdots & & N \\ 0 & & \\ (-1)^{s-1} y & (-1)^s a_2 x/d & \cdots & (-1)^s a_s x/d \end{pmatrix}$$

convient alors. □

On remarquera que la construction d'une matrice obéissant aux conditions du lemme est le seul endroit où la preuve du th. 4.1 n'est pas « algorithmique » (sauf dans le cas où A est un anneau euclidien ; *cf.* exerc. 4.4).

Démonstration du théorème. — Le lemme entraîne facilement le théorème dans le cas où M est une matrice ligne (ou colonne), que l'on peut supposer non nulle : si $M = \begin{pmatrix} m_1 & \cdots & m_s \end{pmatrix}$ et $d = m_1 \wedge \cdots \wedge m_s$ (non nul), il existe $a_1, \dots, a_s$ dans A tels que $d = a_1 m_1 + \cdots + a_s m_s$ et $a_1, \dots, a_s$ sont premiers entre eux dans leur ensemble. Il existe donc d'après le lemme une matrice inversible Q dont la première colonne est $\begin{pmatrix} a_1 \\ \vdots \\ a_s \end{pmatrix}$. Le produit MQ s'écrit alors

$$MQ = \begin{pmatrix} d & b_2 & \cdots & b_s \end{pmatrix},$$

où d divise chacun des b_i. En effectant des opérations élémentaires sur les colonnes de MQ, on arrive à la matrice

$$\begin{pmatrix} d & 0 & \cdots & 0 \end{pmatrix},$$

ce qui montre l'existence d'une réduction dans ce cas.

Traitons le cas général, en raisonnant par récurrence sur la taille de la matrice. Par le processus décrit ci-dessus, on se ramène à une matrice dont la première ligne est du type $\begin{pmatrix} d^{(1)} & 0 & \cdots & 0 \end{pmatrix}$ puis, en procédant de façon analogue, on peut aussi supposer que la première colonne est de ce type. Cela détruit la forme de la première ligne, donc on recommence le processus. On obtient ainsi alternativement des matrices de première ligne ou de première colonne de ce type, avec des premiers coefficients $d^{(i)}$ qui vérifient $d^{(i+1)} \mid d^{(i)}$. Comme l'anneau A est principal, cette suite se stabilise (*cf.* prop. III.2.1), ce qui veut dire que l'on arrive après un nombre fini d'opérations à une matrice disons de première ligne $\begin{pmatrix} d^{(m)} & 0 & \cdots & 0 \end{pmatrix}$ telle que le pgcd des coefficients de la première colonne soit associé à $d^{(m)}$. Cela signifie que $d^{(m)}$ divise chacun de ces coefficients. On peut alors, par opérations élémentaires sur les lignes, se ramener à une matrice du type :

$$\begin{pmatrix} d & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & N & \\ 0 & & & \end{pmatrix}.$$

Appliquant l'hypothèse de récurrence à N, nous sommes ramenés à une matrice du type

$$\begin{pmatrix} d & & & \\ & d_2 & 0 & \\ & 0 & \ddots & \\ & & & d_r \end{pmatrix}$$

(où nous n'avons écrit que les r premières lignes et colonnes de la matrice, tous les autres coefficients étant nuls) avec $d_2 \mid \cdots \mid d_r$, mais on n'a pas encore la condition que d divise d_2 ! Par une opération élémentaire sur les lignes, on arrive à la matrice

$$\begin{pmatrix} d & d_2 & 0 & 0 \\ 0 & d_2 & & 0 \\ & & \ddots & \\ 0 & 0 & & d_r \end{pmatrix}.$$

En appliquant le lemme 4.2 encore une fois, on peut remplacer d par $d_1 := d \wedge d_2$. La coefficient d_1 divise maintenant $d_2, d_3, \ldots, d_r$, mais le nouveau d_2 peut ne plus diviser d_3. Le même procédé nous permet de le remplacer par $d_2 \wedge d_3$. On conclut facilement en procédant de proche en proche.

Pour montrer l'unicité, le plus rapide est de considérer

$$\delta_k(M) = \operatorname{pgcd}(k \times k \text{ mineurs de } M)$$

et de montrer que $\delta_k(M)$ *divise* $\delta_k(PM)$ *pour toute matrice carrée* P *de taille convenable.* Lorsque P est inversible, on a alors $\delta_k(PM) \mid \delta_k(P^{-1}PM) = \delta_k(M)$, de sorte que $\delta_k(M)$ et $\delta_k(PM)$ sont associés. On en déduit en considérant les matrices transposées que si Q est aussi inversible, $\delta_k(M)$ et $\delta_k(MQ)$ sont associés, donc finalement que $\delta_k(M)$ et $\delta_k(PMQ)$ sont associés. Si PMQ a la forme donnée dans le théorème, on a de plus

$$\delta_k(PMQ) = d_1 \cdots d_k,$$

ce qui exprime les d_k en fonction d'éléments de A qui ne dépendent que de M (à multiplication par une unité de A près).

Il reste à démontrer cette propriété. Elle résulte du fait que les lignes de PM sont combinaisons linéaires des lignes de M. Plus précisément, si l'on appelle L_i^k le k-vecteur formé des k premiers coefficients de la $i$ème ligne de M et que l'on note $P = (b_{i,j})_{1 \leq i,j \leq p}$, le premier $k \times k$ mineur de PM est

$$\det(b_{1,1}L_1^k + \cdots + b_{1,p}L_p^k, \ldots, b_{k,1}L_1^k + \cdots + b_{k,p}L_p^k)$$

qui est une combinaison linéaire des $k \times k$ mineurs extraits des k premières colonnes de M. Il est donc divisible par $\delta_k(M)$. □

Exercice 4.3. — Soit A un anneau principal et soient a et b des éléments non nuls de A. Quelle est la forme réduite que l'on obtient en appliquant le théorème à la matrice $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$?

Exercice 4.4. — Soit A un anneau *euclidien.*

a) Montrer que dans la conclusion du théorème, on peut choisir les matrices P et Q (qui ne sont pas uniquement déterminées !) produits de matrices élémentaires.

b) Si $M \in \mathrm{GL}(n, A)$, montrer qu'il existe $P \in E(n, A)$ telle que

$$PM = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \det M \end{pmatrix}.$$

En déduire $\mathrm{SL}(n, A) = E(n, A)$.

Exercice 4.5. — Soit A un anneau.

a) Soit M un élément de $\mathrm{GL}(n, A)$. Utiliser l'identité

$$\begin{pmatrix} M & 0 \\ 0 & M^{-1} \end{pmatrix} = \begin{pmatrix} I_n & M \\ 0 & I_n \end{pmatrix} \begin{pmatrix} I_n & 0 \\ -M^{-1} & I_n \end{pmatrix} \begin{pmatrix} I_n & M \\ 0 & I_n \end{pmatrix} \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}$$

pour montrer que la matrice $\begin{pmatrix} M & 0 \\ 0 & M^{-1} \end{pmatrix}$ est dans $E(2n, A)$.

b) Soient M et N des éléments de $\mathrm{GL}(n, A)$. Utiliser l'identité

$$\begin{pmatrix} MNM^{-1}N^{-1} & 0 \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} MN & 0 \\ 0 & N^{-1}M^{-1} \end{pmatrix} \begin{pmatrix} M^{-1} & 0 \\ 0 & M \end{pmatrix} \begin{pmatrix} N^{-1} & 0 \\ 0 & N \end{pmatrix}$$

pour montrer que la matrice $MNM^{-1}N^{-1}$ est dans $E(2n, A)$.

Un peu de K-théorie. Les groupes $E(n, A)$ et $\mathrm{GL}(n, A)$ ont été très étudiés car ils interviennent en *K-théorie.* Considérons l'injection de groupes

$$\mathrm{GL}(n, A) \to \mathrm{GL}(n+1, A)$$

obtenue en envoyant une matrice $M \in \mathrm{GL}(n, A)$ sur $\begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$ et posons

$$\mathrm{GL}(A) := \bigcup_{n \geq 1} \mathrm{GL}(n, A).$$

C'est un groupe, constitué de matrices infinies avec un bloc fini inversible et un bloc infini qui est l'identité, et dont

$$E(A) := \bigcup_{n \geq 1} E(n, A)$$

est un sous-groupe. On montre (cela résulte des deux derniers exercices ci-dessus) que $E(A)$ est le *sous-groupe dérivé* de $\mathrm{GL}(A)$ (c'est-à-dire le sous-groupe engendré par les commutateurs d'éléments de $\mathrm{GL}(A)$). Il est donc distingué et le groupe quotient

$$K_1(A) := \mathrm{GL}(A)/E(A)$$

est abélien (on l'appelle *l'abélianisé* de $\mathrm{GL}(A)$) [4]. Le déterminant induit une surjection

$$\text{dét} : K_1(A) \to A^*$$

dont on note $SK_1(A)$ le noyau. D'après l'exerc. 4.4, $SK_1(A)$ est trivial lorsque A est euclidien. Il existe en revanche des anneaux principaux A pour lesquels $SK_1(A)$ n'est pas trivial, mais ils sont compliqués [5]. Pour l'exemple standard d'anneau principal non euclidien $A = \mathbf{Z}[(1 + i\sqrt{19})/2]$, le groupe $SK_1(A)$ est trivial [6].

***Corollaire 4.6* (Théorème de la base adaptée).** — *Soit A un anneau principal, soit M un A-module libre de type fini et soit N un sous-module de M. Alors N est libre et il existe une base $(e_1, \dots, e_n)$ de M et des éléments non nuls $d_1, \dots, d_r$ de A, avec $0 \leq r \leq n$, tels que $d_1 \mid \cdots \mid d_r$ et que $(d_1e_1, \dots, d_re_r)$ soit une base de N.*

Il est facile de montrer que N est de type fini (voir la preuve ci-dessous). Si on savait déjà que N était libre, le fait que son rang soit $\leq \mathrm{rang}(M)$ résulterait de l'exerc. 1.2, mais c'est bien la liberté de N qui est le point difficile, et qui ne marche pas dès que A n'est pas principal.

Attention aux erreurs habituelles : le théorème de la base adaptée ne dit pas que N admet un supplémentaire, ni que l'on peut compléter une base de N en une base de M.

Enfin, il est clair qu'un sous-module, même de type fini, d'un module libre de type fini n'est pas nécessairement libre (c'est le cas, par l'exerc. 0.28, pour les idéaux non principaux d'un anneau non principal), et qu'un sous-module d'un module libre de type fini n'est pas nécessairement de type fini (c'est le cas, dans un anneau non noethérien, pour les idéaux qui ne sont pas de type fini (*cf.* prop. III.2.1)).

Démonstration. — On peut supposer $M = A^n$. Montrerons par récurrence sur n que N est un A-module de type fini. Pour $n = 0$, il n'y a rien à démontrer. Si $n > 0$, on considère la projection $p : A^n \to A$ sur un facteur. Le noyau $Q = N \cap A^{n-1}$ du morphisme $N \to p(N)$ est un sous-module de A^{n-1} donc est de type fini par hypothèse de récurrence. L'image $p(N) \simeq N/Q$ est un idéal de A donc est engendrée (en tant qu'idéal, donc aussi en tant que A-module) par un élément. Il en résulte que N est de type fini (exerc. 3.1).

Choisissons une base de M et un système fini de générateurs de N, dont on écrit la matrice des coordonnées dans la base de M. Multiplier à gauche cette matrice par une matrice inversible revient à changer de base pour M. Multiplier à droite cette matrice par une matrice inversible revient à changer de système de générateurs pour N. Le th. 4.1 donne immédiatement le résultat. □

***Corollaire 4.7*.** — *Soit M un module de type fini sur un anneau principal A. Il existe des éléments non nuls et non inversibles $d_1, \dots, d_s$ de A, avec $s \geq 0$, tels que $d_1 \mid \cdots \mid d_s$, et un entier $r \geq 0$, tels que*

$$M \simeq A^r \oplus A/(d_1) \oplus \cdots \oplus A/(d_s).$$

Les entiers r et s, et les d_i à association près, ne dépendent que de M. On appelle ces derniers les facteurs invariants *de M.*

---

4. Ce groupe a été défini et étudié par Whitehead dès 1950 ; on l'appelle parfois le *groupe de Whitehead* de l'anneau A. Le groupe $K_2(A)$ a ensuite été défini par Milnor (médaillé Fields 1962), puis Quillen a donné en 1973 une définition pour toute une suite de groupes $(K_n(A))_{n\in\mathbf{N}}$. Il a obtenu pour cela la médaille Fields en 1978.

5. Voir Ischebeck, F., Hauptidealringe mit nichttrivialer SK_1-Gruppe, *Arch. Math. (Basel)* **35** (1980), 138–139. Pour un exemple où l'on a simplement $E(2, A) \neq \mathrm{SL}(2, A)$, voir le chap. 6 de Cohn, P. M., On the structure of the GL_2 of a ring, *Publ. Math. IHÉS* **30** (1966), 5–53.

6. C'est un théorème difficile de Milnor (1971) que SK_1 est trivial pour tous les anneaux d'entiers de corps de nombres (*cf.* exerc. III.8.20).

Démonstration. — Comme M est de type fini, il est engendré par n éléments, qui définissent un morphisme surjectif $A^n \to M$ de A-modules. Il suffit d'appliquer le cor. 4.6 à son noyau N, en ne gardant que les d_i non inversibles.

Pour l'unicité, il ne semble pas que l'on puisse facilement appliquer l'énoncé analogue qui apparaît dans le th. 4.1. Nous allons donc procéder directement. Tout d'abord, dans une telle décomposition, on a

$$T(M) \simeq A/(d_1) \oplus \cdots \oplus A/(d_s)$$

donc ce A-module ne dépend que de M et pas de la décomposition. De plus, l'entier r ne dépend aussi que de M : c'est le rang du A-module libre $M/T(M)$. Supposons que l'on ait un isomorphisme

$$A/(d_1) \oplus \cdots \oplus A/(d_s) \simeq A/(e_1) \oplus \cdots \oplus A/(e_t). \tag{3}$$

où les d_i et les e_j ne sont ni nuls ni inversibles, $d_1 \mid \cdots \mid d_s$ et $e_1 \mid \cdots \mid e_t$. Nous allons montrer $s = t$ puis, par récurrence sur s, que e_i est associé à d_i pour tout i. Si T est le A-module apparaissant dans (3), l'astuce est de regarder ce que deviennent les deux membres lorsqu'on considère dT et T/dT, pour $d \in A$ bien choisi.

On commence donc par la remarque suivante : soient d et e des éléments de A ; on a

$$d\big(A/(e)\big) \simeq A/(e/d \wedge e); \tag{4}$$

$$\big(A/(e)\big)\Big/d\big(A/(e)\big) \simeq A/(d \wedge e). \tag{5}$$

Le A-module de gauche dans (4) est l'image de la multiplication $A \xrightarrow{\times d} A/(e)$. Un élément x de A est dans le noyau si et seulement si e divise dx, c'est-à-dire $e/d \wedge e$ divise x (utiliser le lemme de Gauss I.1.14). On a bien l'isomorphisme cherché par factorisation canonique.

Pour (5), regardons la surjection canonique $A \to \big(A/(e)\big)/d\big(A/(e)\big)$. Un élément x de A est dans le noyau si et seulement s'il existe $y \in A$ avec $\bar{x} = d\bar{y}$ dans $A/(e)$, c'est-à-dire si et seulement s'il existe $y, z \in A$ avec $x = dy + ez$. Cela signifie $x \in (d, e) = (d \wedge e)$.

En particulier, si p est un élément irréductible de A, de sorte que $A/(p)$ est un corps (prop. I.1.15), on a par (5) :

$$A/(e)/p(A/(e)) \simeq \begin{cases} 0 & \text{si } p \wedge e = 1; \\ A/(p) & \text{si } p \mid e. \end{cases}$$

Si on choisit $p \mid d_1$, on voit que la dimension du $A/(p)$-espace vectoriel T/pT est s, tandis que c'est aussi le nombre ($\leq t$) de e_j divisibles par p. On a donc $s \leq t$, puis égalité par symétrie.

Considérons maintenant le A-module d_1T. On a par (4)

$$d_1T \simeq A/(d_2/d_1) \oplus \cdots \oplus A/(d_s/d_1) \simeq A/(e_1/d_1 \wedge e_1) \oplus \cdots \oplus A/(e_s/d_1 \wedge e_s).$$

Le nombre de facteurs non nuls de chaque côté devant être le même (comme on vient de le démontrer), on en déduit que $e_1/d_1 \wedge e_1$ est inversible, donc que e_1 divise d_1. Par symétrie, ils sont associés, et on obtient des isomorphismes

$$d_1T \simeq A/(d_2/d_1) \oplus \cdots \oplus A/(d_s/d_1) \simeq A/(e_2/d_1) \oplus \cdots \oplus A/(e_s/d_1).$$

On conclut par l'hypothèse de récurrence que soit d_i/d_1 et e_i/d_1 sont inversibles, soit ils sont associés, donc que d_i et e_i sont toujours associés. Ceci termine la démonstration. □

Corollaire 4.8. — *Soit A un anneau principal. Un A-module de type fini est libre si et seulement s'il est sans torsion.*

Attention : $\mathbf{Q}$ est un $\mathbf{Z}$-module sans torsion, mais pas libre (pourquoi ?).

Exercice 4.9. — a) Soit A un anneau principal et soient M, P et Q des A-modules de type fini. On suppose que les A-modules $M \oplus P$ et $M \oplus Q$ sont isomorphes. Montrer que les A-modules P et Q sont isomorphes (on dit que M est *simplifiable*).

b) Soit A un anneau et soient P et Q des A-modules non isomorphes. Soit M le A-module $(P \oplus Q)^{(\mathbf{N})}$. Montrer que les A-modules $M \oplus P$ et $M \oplus Q$ sont isomorphes (M n'est donc pas simplifiable).

c) Soit A l'anneau $\mathbf{R}[X, Y, Z]/(X^2+Y^2+Z^2-1)$. Soit P le noyau du morphisme de A-modules $A^3 \to A$ défini en envoyant les vecteurs de la base canonique de A^3 sur $\bar{X}$, $\bar{Y}$ et $\bar{Z}$ respectivement. Montrer que l'on a $A \oplus P \simeq A^3 \simeq A \oplus A^2$, mais que P n'est pas isomorphe à A^2 (A n'est donc pas simplifiable) (*Indication :* on pourra utiliser des résultats sur la topologie de la sphère $\mathbf{S}^2$).

.

4.1. Application aux groupes abéliens de type fini. — Un groupe abélien de type fini (c'est-à-dire engendré par un nombre fini d'éléments) n'est autre qu'un $\mathbf{Z}$-module de type fini. On déduit donc du cor. 4.7 le théorème de structure suivant.

Théorème 4.10. — *Soit M un groupe abélien de type fini. On a*

$$M \simeq \mathbf{Z}^r \oplus \mathbf{Z}/d_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_s\mathbf{Z},$$

où $r \in \mathbf{N}$ et les d_i sont des entiers strictement positifs vérifiant $d_1 \mid \cdots \mid d_s$. De plus, les entiers r, s et $d_1, \ldots, d_s$ sont uniquement déterminés par M.

Bien entendu, M est fini si et seulement si $r = 0$.

4.2. Application à la réduction des endomorphismes. — Soit K un corps, soit E un K-espace vectoriel de dimension finie et soit u un endomorphisme de E. On définit sur E une structure de $K[X]$-module en posant

$$\forall P \in K[X] \ \ \forall x \in E \qquad P \cdot x := P(u)(x).$$

Remarquons que les sous-$K[X]$-modules de E correspondent aux sous-K-espaces vectoriels stables par u. Comme E est de dimension finie, c'est un $K[X]$-module de torsion et, puisque $K[X]$ est un anneau principal, on peut appliquer les résultats du § 4. On obtient en particulier un isomorphisme de $K[X]$-modules :

$$E \simeq K[X]/(P_1) \oplus \cdots \oplus K[X]/(P_s)$$

où les P_i sont des polynômes unitaires non constants vérifiant $P_1 \mid \cdots \mid P_s$, uniquement déterminés par E et u. C'est en particulier un isomorphisme de K-espaces vectoriels qui correspond à une décomposition

$$E \simeq E_1 \oplus \cdots \oplus E_s$$

en somme directe de sous-espaces vectoriels stables par u qui sont dits *cycliques,* c'est-à-dire qu'il existe $x_i \in E_i$ (l'image de la classe de 1 par l'isomorphisme $K[X]/(P_i) \simeq E_i$) tel que la famille $(u^m(x_i))_{m \in \mathbf{N}}$ engendre le K-espace vectoriel E_i.

Regardons d'un peu plus près la structure des espaces cycliques. Soit (F, v) un tel espace et soit x un élément de F tel que la famille $(v^m(x))_{m \in \mathbf{N}}$ engendre F. Soit r le plus grand entier tel que la famille $\mathscr{B} := (x, v(x), \ldots, v^{r-1}(x))$ soit libre. Par définition de r, le vecteur $v^r(x)$ est combinaison linéaire des vecteurs de cette famille : on peut écrire

$$v^r(x) + a_{r-1}v^{r-1}(x) + \cdots + a_1 v(x) + a_0 x = 0.$$

Le polynôme $P(X) := X^r + a_{r-1}X^{r-1} + \cdots + a_0$ est d'ailleurs celui qui apparaît dans l'isomorphisme de $K[X]$-modules $K[X]/(P) \simeq F$. On a $P(v)(x) = 0$, donc $P(v)(v^m(x)) = v^m(P(v)(x)) = 0$ pour tout $m \in \mathbf{N}$, donc $P(v) = 0$. Comme la famille $\mathscr{B}$ est libre, aucun polynôme de degré $< r$ ne peut annuler v, de sorte que P est le polynôme minimal de v.

Dans la base $\mathscr{B}$, la matrice de v est la *matrice compagnon* de P

$$C(P) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{r-1} \end{pmatrix}$$

(la matrice compagnon du polynôme constant 1 est vide). Le polynôme minimal de $C(P)$ est donc P et on calcule facilement que c'est aussi son polynôme caractéristique.

Théorème 4.11. — *Pour tout endomorphisme u d'un K-espace vectoriel E de dimension finie, il existe une base de E dans laquelle la matrice de u est diagonale par blocs, de la forme*

$$\begin{pmatrix} C(P_1) & & & \\ & C(P_2) & & \\ & & \ddots & \\ & & & C(P_s) \end{pmatrix}$$

où les P_i sont des polynômes unitaires non constants de $K[X]$ vérifiant $P_1 \mid \cdots \mid P_s$.

Les P_i sont entièrement déterminés par u ; on les appelle les invariants de similitude *de u.*

Deux matrices de $\mathscr{M}_n(K)$ sont semblables si et seulement si elles ont les mêmes invariants de similitude [7].

Démonstration. — Il résulte de ce qui précède que la matrice de u dans une base convenable est du type cherché si et seulement si le $K[X]$-module E est isomorphe à $K[X]/(P_1) \oplus \cdots \oplus K[X]/(P_s)$. Le théorème résulte donc du cor. 4.7. □

Le polynôme minimal de u est P_s (c'est « le plus grand ») et le polynôme caractéristique est $P_1 \cdots P_s$ (puisque celui de $C(P_i)$ est P_i). Le théorème permet par exemple de voir immédiatement que si deux matrices de $\mathscr{M}_n(K)$ sont semblables sur une extension de K, elles sont déjà semblables sur K, résultat qui n'est pas du tout évident *a priori* (en particulier si K est fini).

Proposition 4.12. — *Soit $M \in \mathscr{M}_n(K)$ et soient $P_1 \mid \cdots \mid P_s$ ses invariants de similitude. La suite des n facteurs invariants* [8] *de la matrice $XI_n - M \in \mathscr{M}_n(K[X])$ est $(1, \ldots, 1, P_1, \ldots, P_s)$.*

Démonstration. — La matrice M est semblable à une matrice diagonale par blocs comme dans le th. 4.11, donc la matrice $XI_n - M$ est semblable (donc aussi équivalente) à la matrice diagonale par blocs du type $XI_{\deg(P_i)} - C(P_i)$. Il suffit donc de montrer que la suite $(d_1, \ldots, d_r)$ des facteurs invariants d'une matrice $XI_r - C(P)$ d'ordre r est $(1, \ldots, 1, P)$. Or on a vu lors de la preuve du th. 4.1 que $d_1 \cdots d_i$ est le pgcd des $i \times i$ mineurs de $XI_r - C(P)$. Le mineur d'ordre $r-1$ obtenu en effaçant la première ligne et la dernière colonne est 1. On a donc (à association près) $d_1 = \cdots = d_{r-1} = 1$ et $d_r = \det(XI_r - C(P)) = P$. □

En particulier, la proposition entraîne qu'étant données des matrices M et N dans $\mathscr{M}_n(K)$, les matrices M et N sont semblables si et seulement si les matrices $XI_n - M$ et $XI_n - N$ sont équivalentes, une propriété qui peut se vérifier directement « à la main » (mais ce n'est pas facile !).

7. Bien entendu, les invariants de similitude d'une matrice sont par définition les invariants de l'endomorphisme de K^n qu'elle représente dans la base canonique.

8. Voir th. 4.1 pour la définition.

Nous nous arrêterons ici pour ce qui est de la réduction des endomorphismes, mais on peut poursuive dans cette voie pour arriver d'une part, lorsque le polynôme caractéristique de l'endomorphisme u est scindé, à la réduction de Jordan, d'autre part, lorsque K est parfait, à la décomposition de Dunford $u = d + n$, avec d semi-simple (diagonalisable dans une extension finie de K), n nilpotent et $dn = nd$ (*cf.* exerc. I.6.30).

Exercice 4.13. — Soient P et Q des polynômes. Calculer les invariants de similitude de la matrice par blocs

$$\begin{pmatrix} C(P) & 0 \\ 0 & C(Q) \end{pmatrix}.$$

Exercice 4.14. — Soit u un endomorphisme d'un K-espace vectoriel E de dimension finie. On pose

$$\begin{aligned} \mathrm{Com}(u) &= \{v \in \mathrm{End}(E) \mid uv = vu\}, \\ \mathscr{P}(u) &= \{P(u) \mid P \in K[X]\} \subseteq \mathrm{Com}(u) \subseteq \mathrm{End}(E). \end{aligned}$$

La dimension du K-espace vectoriel $\mathscr{P}(u)$ est le degré du polynôme minimal de u.

a) Montrer $\mathscr{P}(u) = \bigcap_{v \in \mathrm{Com}(u)} \mathrm{Com}(v)$.

b) Si K est infini [9], montrer que les propriétés suivantes sont équivalentes :

(i) u est cyclique ;

(ii) le polynôme minimal de u est égal à son polynôme caractéristique ;

(iii) $\mathrm{Com}(u) = \mathscr{P}(u)$;

(iv) E n'a qu'un nombre fini de sous-espaces vectoriels stables par u.

9. Cette hypothèse n'est pas nécessaire pour toutes les implications.

CHAPITRE III

ANNEAUX

Commençons par un peu d'histoire. On peut dire en première approximation que les débuts de l'algèbre commutative sont dus à diverses tentatives de résoudre la conjecture de Fermat :

$$x^n + y^n + z^n = 0 \implies xyz = 0,$$

pour x, y, z entiers et $n \geq 3$. Il suffit de traiter les cas $n = 4$ (une démonstration a été laissée par Fermat) et $n = p$, nombre premier impair. Des démonstrations *ad hoc* ont été apportées par Euler en 1770 pour $p = 3$ (avec une erreur), par Legendre en 1823 pour $p = 5$, par Lamé en 1839 pour $p = 7$, etc. Lamé annonce le 1er mars 1847 qu'il a une preuve complète, mais Liouville trouve une faute majeure, que nous allons expliquer.

Une des idées pour attaquer le problème de Fermat (que l'on trouve déjà dans la « preuve » d'Euler) est de transformer cette équation en

$$-z^p = \prod_{j=0}^{p-1} (x + \zeta_p^j y),$$

où l'on a posé $\zeta_p = \exp(2i\pi/p)$. On obtient ainsi une équation à coefficients dans le sous-anneau $\mathbf{Z}[\zeta_p] = \mathbf{Z} + \mathbf{Z}\zeta_p + \cdots + \mathbf{Z}\zeta_p^{p-1}$ de $\mathbf{C}$ engendré par ζ_p. Si par hasard les facteurs du produit sont premiers entre eux deux à deux dans l'anneau $\mathbf{Z}[\zeta_p]$ (et c'est vrai lorsque p ne divise pas xyz) et *que l'on a unicité de la décomposition de z^p en facteurs irréductibles dans l'anneau* $\mathbf{Z}[\zeta_p]$, on en déduit que chaque facteur $x + \zeta_p^j y$ est une puissance p-ième dans cet anneau. La suite n'est pas facile, mais on peut ensuite arriver à une contradiction avec un peu de travail (essentiellement par la méthode de « descente infinie » de Fermat : on produit, à partir d'une solution donnée, une autre solution plus petite).

Le problème majeur (à l'origine des erreurs d'Euler et de Lamé) est que l'anneau $\mathbf{Z}[\zeta_p]$ n'est en général pas *factoriel* (il n'y a pas unicité de la décomposition en irréductibles) : il ne l'est pour aucun $p \geq 23$.

C'est en essayant d'élargir le concept de facteur irréductible que Kummer crée celui de *nombre idéal,* qui donnera plus tard lieu à la théorie actuelle des idéaux et des modules (Dedekind). Les travaux de Kummer lui permettront de montrer le théorème de Fermat pour tous les nombres premiers p *réguliers,* c'est-à-dire tels que p ne divise le dénominateur d'aucun des nombres de Bernoulli [1] $B_2, B_4, B_6, \ldots, B_{p-3}$ (on estime que la probabilité pour un nombre premier d'être régulier est $e^{-1/2}$, soit environ 61%, même si on ne sait pas montrer qu'il y en a une infinité !).

1. Ces nombres sont définis par la série génératrice $\frac{t}{e^t - 1} = \sum_{m=0}^{+\infty} B_m \frac{t^m}{m!}$.

1. Anneaux factoriels

On formalise ici une propriété dont on a déjà montré (th. I.1.16) qu'elle est satisfaite par l'anneau des polynômes à une indéterminée à coefficients dans un corps. On montrera plus loin (cor. 2.6) qu'elle est en fait satisfaite par tout anneau principal.

Définition 1.1. — *Un anneau A est* factoriel [2] *s'il est intègre et que tout élément non nul a de A peut s'écrire*

$$a = up_1 \cdots p_r$$

avec $u \in A^*$ et $p_1, \ldots, p_r$ irréductibles [3]*, et que cette décomposition est unique au sens suivant : si $a = vq_1 \cdots q_s$ est une autre telle décomposition, on a $r = s$ et il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que q_i soit associé à $p_{\sigma(i)}$ pour tout i.*

La plupart des anneaux intègres que l'on rencontre en algèbre ont la propriété d'existence de la décomposition (*cf.* prop. 2.4) ; la propriété forte est l'unicité. On peut la reformuler ainsi : fixons un système de représentants irréductibles $\mathscr{P}$ de A, c'est-à-dire un ensemble d'éléments irréductibles tels que tout irréductible de A soit associé à un et un seul élément de $\mathscr{P}$. Alors tout élément non nul a de A s'écrit d'une manière unique

$$a = u \prod_{p \in \mathscr{P}} p^{n_p},$$

avec $u \in A^*$, et où $(n_p)_{p \in \mathscr{P}}$ est une famille presque nulle d'entiers naturels. On note alors $v_p(a) := n_p$.

Nous avons défini en § I.1.3 le pgcd de deux éléments d'un anneau principal. On peut donner une définition analogue pour deux éléments a et b d'un anneau factoriel : si $a = 0$, le pgcd $a \wedge b$ est par définition b ; de même $a \wedge 0 = a$. Si $ab \neq 0$, on pose

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

Cette définition dépend du choix de $\mathscr{P}$; on peut aussi déclarer que $a \wedge b$ est bien défini à association près. Dans tous les cas, le pgcd $a \wedge b$ est alors un diviseur commun de a et b, et tout diviseur commun à a et b divise $a \wedge b$.

On a une discussion analogue pour le ppcm, qui est laissée en exercice. On peut aussi parler du pgcd et du ppcm d'une famille finie quelconque d'éléments d'un anneau factoriel.

Rappelons (*cf.* § I.1.2) que des éléments d'un anneau A sont premiers entre eux si leurs seuls diviseurs communs sont les unités de A (par exemple, si p est irréductible, tout élément de A est ou bien premier avec p, ou bien divisible par p). Si A est un anneau factoriel, des éléments de A sont donc premiers entre eux si et seulement si leur pgcd est une unité.

Exemple 1.2. — L'anneau $\mathbf{Z}$ est factoriel et on peut prendre pour $\mathscr{P}$ l'ensemble des nombres premiers positifs. Comme on l'a montré dans le th. I.1.16, si K est un corps, l'anneau $K[X]$ est factoriel, et on peut prendre pour $\mathscr{P}$ l'ensemble des polynômes irréductibles unitaires.

La proposition suivante donne un critère pour qu'un anneau soit factoriel quand on connaît déjà l'existence de la décomposition en irréductibles.

Proposition 1.3. — *Soit A un anneau intègre tel que tout élément non nul de A soit produit d'irréductibles. Les propriétés suivantes sont équivalentes :*

2. En anglais, on écrit souvent « UFD », pour « unique factorization domain ».

3. On rappelle (*cf.* § I.1.2) qu'un élément a d'un anneau A est *irréductible* si a n'est pas inversible et que si $a = xy$, alors soit x, soit y est inversible. La seconde condition signifie que les seuls diviseurs de a sont ses associés et les unités de A.

(i) *A est factoriel ;*

(ii) *pour tout élément irréductible p de A, l'idéal (p) est premier* [4] *;*

(iii) *pour tous éléments non nuls a, b et c de A tels que a divise bc mais est premier avec b, a divise c.*

Démonstration. — Montrons que (iii) implique (ii). Si p irréductible divise ab et ne divise pas a, alors p est premier avec a puisque p est irréductible, de sorte que p divise b d'après (iii). Ainsi l'idéal (p) est premier.

Montrons que (ii) implique (i). Soit $\mathscr{P}$ un système de représentants irréductibles. Si

$$u \prod_{p\in\mathscr{P}} p^{m_p} = v \prod_{p\in\mathscr{P}} p^{n_p}$$

sont des décompositions d'un élément non nul de A, la condition $m_q > n_q$ pour un certain $q \in \mathscr{P}$ implique, par intégrité de A, que q divise $v \prod_{p\in\mathscr{P},\ p\neq q} p^{n_p}$, donc l'un des facteurs d'après (ii). Mais q ne peut diviser un élément p de $\mathscr{P}$ distinct de q car $\mathscr{P}$ est un système de représentants irréductibles. Ainsi $m_p = n_p$ pour tout $p \in \mathscr{P}$, puis $u = v$ par intégrité de A.

Montrons que (i) implique (iii). On écrit $ad = bc$ et on décompose les éléments non nuls a, b, c et d comme ci-dessus. Alors pour tout $p \in \mathscr{P}$, on a (par unicité de la décomposition) $v_p(b) + v_p(c) = v_p(a) + v_p(d) \geq v_p(a)$. Si $v_p(b) = 0$, on a donc $v_p(a) \leq v_p(c)$. Si $v_p(b) > 0$, on a $v_p(a) = 0$ (car a est premier avec b) donc $v_p(a) \leq v_p(c)$. Ainsi a divise c. □

Exemple 1.4. — L'anneau $\mathbf{Z}[\sqrt{-5}] = \mathbf{Z}[X]/(X^2+5)$ est intègre mais n'est pas factoriel : 3 est irréductible mais l'idéal (3) n'est pas premier (*cf.* ex. I.1.9).

Exercice 1.5. — Soit K un corps. Montrer que le sous-anneau $K[X^2, X^3]$ de $K[X]$ engendré par X^2 et X^3 n'est pas factoriel.

Exercice 1.6. — Soit A un anneau factoriel tel que tout idéal premier non nul est maximal (on dit que la dimension de Krull de A est 1 ; *cf.* § 5.4). On se propose de montrer que A est principal.

a) Montrer que pour tout x et tout y non nuls dans A, il existe u et v dans A tels que $ux + vy = x \wedge y$.

b) Soit I un idéal non nul de A. Montrer qu'il existe $d \in A$ non nul qui est un pgcd de tous les éléments de $I \cap (A - \{0\})$. Conclure.

Définition 1.7. — *Soit A un anneau factoriel. Le* contenu, *noté $c(P)$, d'un polynôme $P \in A[X]$ est le pgcd de ses coefficients. Le polynôme P est dit* primitif *si $c(P) = 1$.*

On notera que le contenu est défini à multiplication par une unité de A près. Le contenu d'un polynôme est nul si et seulement si le polynôme est nul.

***Lemme 1.8* (Gauss)**. — *Soit A un anneau factoriel. Pour tous polynômes P et Q dans $A[X]$, on a*

$$c(PQ) = c(P)c(Q) \pmod{A^*}.$$

Démonstration. — Supposons d'abord P et Q primitifs et montrons que PQ est primitif. Soit p un irréductible de A. Comme P et Q sont primitifs, chacun a au moins un coefficient non divisible par p. Soit a_i (resp. b_j) le coefficient de P (resp. de Q) d'indice minimal non divisible par p. Alors le coefficient d'indice $i + j$ de PQ est somme de termes divisibles par p et de $a_i b_j$ donc il n'est pas divisible par p car (p) est premier vu que A est factoriel. Ceci montre qu'aucun élément irréductible de A ne divise tous les coefficients de PQ, qui est donc primitif.

Le cas général s'en déduit : si P ou Q est nul, il est évident ; sinon, on applique le résultat précédent à $P/c(P)$ et $Q/c(Q)$. □

4. Autrement dit, si a et b sont des éléments de A et que p divise ab, alors p divise a ou p divise b.

On en déduit le résultat suivant, utilisé lors de la démonstration du théorème de Lüroth (th. I.6.9).

Lemme 1.9. — *Soit A un anneau factoriel de corps des fractions K. Soient P et Q des éléments de $A[X]$, avec P primitif, et soit $R \in K[X]$ tel que $Q = PR$. Alors $R \in A[X]$.*

Démonstration. — On peut écrire $R = R_1/r$, avec $r \in A$ et $R_1 \in A[X]$. On a alors $rQ = PR_1$, puis $rc(Q) = c(P)c(R_1) = c(R_1) \pmod{A^*}$ par le lemme de Gauss, de sorte que r divise $c(R_1)$, donc aussi R_1, ce qui termine la démonstration. □

On a aussi l'important résultat suivant.

Théorème 1.10. — *Soit A un anneau factoriel de corps des fractions K. Les éléments irréductibles de $A[X]$ sont :*

a) *les polynômes constants p avec p irréductible dans A ;*

b) *les polynômes primitifs de degré ≥ 1 qui sont irréductibles dans $K[X]$.*

En particulier, pour un polynôme primitif de $A[X]$, il revient au même d'être irréductible dans $A[X]$ et dans l'anneau principal $K[X]$ (ce qui n'est pas du tout évident vu qu'il y a *a priori* plus de décompositions possibles dans $K[X]$).

Démonstration. — Comme $(A[X])^* = A^*$ il est clair qu'un polynôme constant p est irréductible si et seulement si p est irréductible dans A.

Soit maintenant P un polynôme primitif de degré ≥ 1 de $A[X]$ qui est irréductible dans $K[X]$. Montrons qu'il est irréductible dans $A[X]$. Supposons donc qu'il sécrive $P = QR$ avec Q et R dans $A[X]$. Le lemme de Gauss 1.7 entraîne que $c(Q)$ et $c(R)$ sont inversibles. D'autre part, l'un des polynômes Q ou R est constant (parce que P est irréductible dans $K[X]$), et c'est donc une constante inversible dans A, donc une unité de $A[X]$. Donc P, qui n'est pas inversible dans $A[X]$ car de degré au moins 1, est bien irréductible dans $A[X]$.

Montrons inversement qu'un polynôme P de degré ≥ 1 et irréductible dans $A[X]$ est primitif et irréductible dans K[X]. Comme $c(P)$ divise P dans $A[X]$ et ne lui est pas associé pour raison de degré, c'est une unité de $A[X]$, donc de A, et P est bien primitif. Il reste à montrer que P (qui n'est pas inversible dans $K[X]$) est irréductible dans $K[X]$. Or si $P = QR$ dans $K[X]$, on peut écrire $Q = Q_1/q$ et $R = R_1/r$ avec q et r dans A et Q_1 et R_1 dans $A[X]$. On obtient $qrP = Q_1R_1$ et, en passant aux contenus (lemme de Gauss), $qr = c(Q_1)c(R_1)$. Ainsi $P = Q_1R_1/qr = (Q_1/c(Q_1))(R_1/c(R_1)) \pmod{A^*}$. Comme P est irréductible dans $A[X]$, l'un des polynômes Q_1 ou R_1 de $A[X]$ est constant, et l'un des polynômes Q ou R est constant, ce qui achève la preuve. □

On a enfin le théorème fondamental suivant.

Théorème 1.11. — *Soit A un anneau factoriel. Les anneaux $A[X_1, \ldots, X_n]$ sont factoriels pour tout $n \in \mathbf{N}$.*

La conclusion reste vraie avec un nombre infini d'indéterminées (cela découle du cas fini).

Démonstration. — Il suffit de montrer que $A[X]$ est factoriel. Montrerons d'abord l'existence de la décomposition en produit d'irréductibles d'un polynôme P non nul. Après avoir écrit $P = c(P)(P/c(P))$ et décomposé $c(P)$ en produit d'irréductibles dans A, on se ramène à P primitif non constant.

On décompose alors P en produit d'irréductibles dans l'anneau factoriel $K[X]$ (th. I.1.16) soit, en chassant les dénominateurs, $aP = P_1 \cdots P_r$ avec $a \in A$ et $P_i \in A[X]$ irréductible dans $K[X]$. Écrivons

$P_i = c(P_i)Q_i$, avec Q_i primitif, donc irréductible dans $A[X]$ d'après le théorème précédent. En passant aux contenus, on obtient qu'il existe $u \in A^*$ tel que $ua = c(P_1)\cdots c(P_r)$, et $P = u\prod_{i=1}^r Q_i$ est une décomposition de P en produits d'irréductibles de $A[X]$.

Il suffit donc d'après la prop. 1.3 de montrer que si $P \in A[X]$ est irréductible, l'idéal (P) est premier. Si P est une constante irréductible p de $A[X]$, c'est clair (par vérification directe, ou encore en remarquant que $A[X]/(p)$ est isomorphe à $(A/(p))[X]$, qui est intègre vu que (p) est premier dans A, et que l'anneau des polynômes à coefficients dans un anneau intègre est aussi intègre). Supposons maintenant P primitif de degré au moins 1, donc irréductible dans $K[X]$ d'après le théorème précédent. Si P divise le produit QR de polynômes dans $A[X]$, il divise alors Q ou R dans l'anneau principal $K[X]$ (prop. I.1.15), disons par exemple Q. Comme P est primitif, par le lemme 1.9, le quotient Q/P est dans $A[X]$, de sorte que P divise Q dans $A[X]$. C'est ce que l'on voulait montrer. □

Théorème 1.12 **(Critère d'Eisenstein)**. — *Soit A un anneau factoriel, soit K_A son corps de fractions, soit $P(X) = \sum_{k=0}^n a_k X^k$ un polynôme non constant à coefficients dans A et soit p un élément irréductible de A. On suppose :*

- *p ne divise pas a_n ;*
- *p divise a_k pour chaque $k \in \{0, \dots, n-1\}$;*
- *p^2 ne divise pas a_0.*

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

Démonstration. — Vu que $c(P)$ n'est pas divisible par p par le premier point, $P/c(P)$ vérifie les mêmes hypothèses que P. On peut donc supposer P primitif. Si P n'est pas irréductible, il s'écrit (d'après le th. 1.10) $P = QR$ avec Q et R dans $A[X]$, non constants. Posons $Q(X) = b_r X^r + \cdots + b_0$ et $R(X) = c_s X^s + \cdots + c_0$, avec $r + s = n$, $r, s > 0$ et $a_n = b_r c_s$. L'anneau $B = A/(p)$ est intègre, et, comme on l'a remarqué dans la démonstration plus haut, $A[X]/(p)$ est isomorphe à $B[X]$. Dans cet anneau, on a $\bar{a}_n X^n = \bar{Q}\bar{R}$. D'autre part, $\bar{a}_n \neq 0$ dans B, donc $\bar{b}_r$ et $\bar{c}_s$ sont aussi non nuls. Ainsi $\bar{Q}$ et $\bar{R}$ ne sont pas constants et l'égalité $\bar{a}_n X^n = \bar{Q}\bar{R}$ dans l'anneau factoriel $B[X]$ implique alors, comme X y est irréductible, que $\bar{Q}$ et $\bar{R}$ sont divisibles par X dans $B[X]$. Cela signifie que p divise b_0 et c_0, ce qui contredit le fait que a_0 n'est pas divisible par p^2. □

Par exemple $X^{18} - 4X^7 - 2$ est irréductible dans $\mathbf{Q}[X]$, et $X^5 - XY^3 - Y$ est irréductible dans $\mathbf{C}[X, Y]$ (prendre $A = \mathbf{C}[Y]$ et $p = Y$).

Exercice 1.13. — Montrer que si p est un nombre premier, le polynôme cyclotomique $\Phi_p(X) = X^{p-1} + \cdots + X + 1 = \frac{X^p - 1}{X - 1}$ est irréductible dans $\mathbf{Q}[X]$ (on pourra poser $X = Y + 1$).

2. Anneaux noethériens

Les anneaux principaux sont agréables, mais ils sont très rares en algèbre. En affaiblissant un peu les hypothèses (propriété (i) ci-dessous), on tombe sur une classe d'anneaux absolument fondamentale.

Proposition 2.1. — *Soit A un anneau commutatif. Les trois propriétés suivantes sont équivalentes :*

(i) *tout idéal de A est engendré par un nombre fini d'éléments ;*

(ii) *toute suite croissante (pour l'inclusion) d'idéaux de A est stationnaire ;*

(iii) *toute famille non vide d'idéaux de A a un élément maximal pour l'inclusion.*

On dira que l'anneau A est noethérien *s'il vérifie ces propriétés* [5].

5. Ces anneaux sont nommés ainsi en l'honneur d'Emmy Noether (1882–1935).

Démonstration. — Montrons que (i) implique (ii). Soit (I_n) une telle suite ; la réunion I des I_n est encore un idéal car la famille (I_n) est totalement ordonnée pour l'inclusion. Par (i), il existe des éléments $x_1, \dots, x_r$ de I qui l'engendrent. Chaque x_i est dans l'un des I_n, donc il existe n_0 (le plus grand des indices correspondants) tel que I_{n_0} les contienne tous. Alors $I = I_{n_0}$ et la suite (I_n) stationne à I_{n_0}.

Montrons que (ii) implique (iii). Si une famille non vide d'idéaux de A n'a pas d'élément maximal, on construit par récurrence une suite infinie strictement croissante d'idéaux de A, ce qui contredit (ii).

Montrons que (iii) implique (i). Soit I un idéal de A. La famille $\mathscr{E}$ des idéaux $J \subseteq I$ qui sont engendrés par un nombre fini d'éléments est non vide (elle contient l'idéal (0)). Soit J_0 un élément maximal de $\mathscr{E}$. Pour tout $x \in I$, l'idéal $J_0 + xA$ est aussi dans $\mathscr{E}$, donc $J_0 + xA = J_0$ par maximalité. Ceci signifie $x \in J_0$. Finalement $I = J_0$ et I est engendré par un nombre fini d'éléments. □

Tout anneau principal est noethérien ((i) est trivialement vérifié). Si A est noethérien, tout quotient de A l'est encore (c'est immédiat à partir de la caractérisation (ii), vu que les idéaux de A/I sont les idéaux de A contenant I)). En revanche, un sous-anneau d'un anneau noethérien n'est pas nécessairement noethérien (*cf.* exerc. 2.9).

Si K est un corps, l'anneau $K[(X_n)_{n\in\mathbf{N}}]$ n'est pas noethérien car

$$(X_0) \subseteq (X_0, X_1) \subseteq \cdots \subseteq (X_0, \dots, X_n) \subseteq \cdots$$

forme une suite infinie strictement croissante d'idéaux.

Exercice 2.2. — Soit A un anneau tel que tout idéal *premier* de A est engendré par un nombre fini d'éléments. Montrer que A est noethérien (*Indication :* on pourra considérer un élément maximal I dans la famille des idéaux qui ne sont pas engendrés par un nombre fini d'éléments, des éléments x et y de $A - I$ tels que $xy \in I$, des générateurs $x_1, \dots, x_r, y$ de l'idéal $I + (y)$, avec $x_1, \dots, x_r \in I$, des générateurs $y_1, \dots, y_s$ de l'idéal $\{a \in A \mid ay \in I\}$, et montrer que $x_1, \dots, x_r, ay_1, \dots, ay_s$ engendrent I).

Exercice 2.3. — Soit A un anneau noethérien et soit M un A-module de type fini.

a) Montrer que tout sous-A-module de M est encore de type fini (*Indication :* on pourra se ramener à $M = A^n$, puis procéder par récurrence sur n en utilisant l'exerc. II.3.1).

b) Montrer que toute suite croissante de sous-A-modules de M est stationnaire (*Indication :* on pourra se ramener à $M = A^n$, puis procéder par récurrence sur n).

Proposition 2.4. — *Soit A un anneau intègre noethérien. Tout élément non nul de A peut s'écrire $up_1 \cdots p_r$ avec $u \in A^*$ et $p_1, \dots, p_r$ irréductibles.*

Démonstration. — Soit $\mathscr{E}$ l'ensemble des idéaux de A de la forme (x), avec x non inversible ne s'écrivant pas comme demandé. Si $\mathscr{E}$ n'est pas vide, il admet un élément maximal (a) (prop. 2.1). En particulier a n'est alors pas irréductible. Comme il n'est pas inversible, il s'écrit $a = bc$ avec b et c non associés à a. Comme A est intègre, les idéaux (b) et (c) contiennent alors strictement (a), donc par maximalité, ils ne sont pas dans $\mathscr{E}$, de sorte que b et c se décomposent en produit d'irréductibles, ce qui contredit le fait que a ne s'écrit pas comme produit d'irréductibles. □

On déduit alors de la prop. 1.3 les deux corollaires suivants.

Corollaire 2.5. — *Un anneau intègre noethérien est factoriel si et seulement si tout élément irréductible engendre un idéal premier.*

Il existe des anneaux factoriels non noethériens (comme par exemple $K[(X_n)_{n\in\mathbf{N}}]$).

Corollaire 2.6. — *Tout anneau principal est factoriel.*

La plupart des anneaux avec lesquels on travaille en algèbre commutative sont noethériens, via le théorème et le corollaire suivants.

***Théorème 2.7* (Hilbert).** — *Soit A un anneau noethérien. Les anneaux $A[X_1, \dots, X_n]$ sont noethériens pour tout $n \in \mathbf{N}$.*

Démonstration. — Il suffit de montrer que $A[X]$ est noethérien. Soit I un idéal de $A[X]$. Pour chaque $k \in \mathbf{N}$, on note $D_k(I)$ le sous-ensemble de A constitué de 0 et des coefficients dominants des polynômes de degré k de I. Il est immédiat que $D_k(I)$ est un idéal de A, et qu'une inclusion $I \subseteq J$ entraîne $D_k(I) \subseteq D_k(J)$. On a d'autre part les deux propriétés suivantes :

a) pour tout $k \in \mathbf{N}$, on a $D_k(I) \subseteq D_{k+1}(I)$: il suffit de remarquer que si $P \in I$, alors $XP \in I$;

b) si $I \subseteq J$, le fait que $D_k(I) = D_k(J)$ pour tout $k \in \mathbf{N}$ entraîne $I = J$: si $I \neq J$, on choisit un polynôme $P \in J - I$ de degré r minimal ; comme $D_r(I) = D_r(J)$, l'idéal I contient un polynôme Q de degré r qui a même coefficient dominant que P, mais alors $P - Q$ est dans $J - I$ et est de degré $< r$, contradiction.

Ceci étant établi, soit $(I_n)_{n\in\mathbf{N}}$ une suite croissante d'idéaux de $A[X]$. Comme A est noethérien, la famille des $D_k(I_n)$ pour $k \in \mathbf{N}$ et $n \in \mathbf{N}$ admet un élément maximal $D_l(I_m)$. D'autre part, pour chaque $k \leq l$, la suite d'idéaux $(D_k(I_n))_{n\in\mathbf{N}}$ est croissante, donc elle est stationnaire, c'est-à-dire qu'il existe n_k tel que pour

$$\forall n \geq n_k \qquad D_k(I_n) = D_k(I_{n_k}).$$

Soit alors N le plus grand des entiers $m, n_0, n_1, \dots, n_l$. Nous allons montrer que pour tout $n \geq N$ et tout k, on a $D_k(I_n) = D_k(I_N)$, ce qui suffira à conclure $I_n = I_N$ via la propriété b) ci-dessus. On distingue deux cas :

1) si $k \leq l$, on a $D_k(I_N) = D_k(I_{n_k}) = D_k(I_n)$ par définition de n_k puisque n et N sont tous deux $\geq n_k$;

2) si $k > l$, on a $D_k(I_N) \supseteq D_l(I_N) \supseteq D_l(I_m)$ (d'après la propriété a) ci-dessus, et puisque $N \geq m$) et $D_k(I_n) \supseteq D_l(I_n) \supseteq D_l(I_m)$ pour les mêmes raisons, donc par maximalité de $D_l(I_m)$, on a $D_k(I_N) = D_l(I_m) = D_k(I_n)$. □

***Corollaire 2.8*.** — *Soit A un anneau noethérien. Toute A-algèbre de type fini est noethérienne.*

Démonstration. — Par définition, une A-algèbre engendrée par des éléments $x_1, \dots, x_n$ est un quotient de l'anneau $A[X_1, \dots, X_n]$, qui est noethérien par le th. 2.7. C'est donc un anneau noethérien. □

L'anneau de séries formelles $A[[X]]$ est noethérien, mais n'est jamais une A-algèbre de type fini (lorsque A est non nul ! *Cf.* cor. 10.8).

***Exercice 2.9*.** — Soit K un corps. Montrer que le sous-anneau de $K[X, Y]$ engendré par les X^nY, pour $n \in \mathbf{N}^*$, n'est pas noethérien.

***Corollaire 2.10*.** — *Soit A un anneau noethérien et soit I un idéal de A. Pour tout $x \in \bigcap_{n=1}^{\infty} I^n$, on a $x \in xI$.*

Démonstration. — Soient $a_1, \dots, a_r$ des éléments de A qui engendrent l'idéal I. Pour chaque $n \geq 1$, on a $x \in I^n$ donc il existe un polynôme $P_n \in A[X_1, \dots, X_r]$ *homogène de degré* n tel que $x = P_n(a_1, \dots, a_r)$. Soit J_n l'idéal de $A[X_1, \dots, X_r]$ engendré par $P_1, \dots, P_n$. On a bien sûr $J_n \subseteq J_{n+1}$. Comme l'anneau $A[X_1, \dots, X_r]$ est noethérien (th. 2.7), il existe un entier $N > 0$ tel que $J_N = J_{N+1}$. On peut donc écrire

$$P_{N+1} = Q_1 P_N + \cdots + Q_N P_1,$$

où $Q_i \in A[X_1, \ldots, X_r]$ est homogène de degré i. En substituant a_j à X_j, on obtient

$$x = Q_1(a_1, \ldots, a_r)x + \cdots + Q_N(a_1, \ldots, a_r)x,$$

ce qui, puisque chaque Q_i est homogène de degré strictement positif, prouve le théorème. □

***Corollaire 2.11* (Krull).** — *Soit A un anneau noethérien et soit I un idéal de A. On suppose qu'au moins* l'une des deux *conditions suivantes est vérifiée :*

- *l'anneau A est intègre et $I \neq A$;*
- $I \subseteq \mathrm{rad}(A)$.

Alors $\bigcap_{n=1}^{\infty} I^n = 0$.

On rappelle (§ II.3) que le radical de Jacobson $\mathrm{rad}(A)$ de A est défini comme l'intersection de ses idéaux maximaux. En particulier, le corollaire entraîne que si A a un unique idéal maximal $\mathfrak{m}$ (c'est-à-dire que A est un anneau local) et est noethérien, $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0$.

Démonstration. — Soit x un élément de $\bigcap_{n=1}^{\infty} I^n$. Le cor. 2.10 entraîne l'existence d'un élément a de I tel que $x = xa$. Sous la première hypothèse, on a $a \neq 1$ (puisque $I \neq A$), donc $x = 0$. Sous la seconde hypothèse, on a $a \in \mathrm{rad}(A)$, donc $1 - a$ inversible (lemme II.3.7), et de nouveau $x = 0$. □

Exercice 2.12. — Dans l'anneau local A des germes en 0 de fonctions de classe $\mathscr{C}^\infty$ de $\mathbf{R}$ dans $\mathbf{R}$ (*cf.* exerc. II.3.9), on note $\mathfrak{m}$ l'idéal maximal des fonctions nulles en 0. Produire un élément non nul de $\bigcap_{n=1}^{\infty} \mathfrak{m}^n$ (cela entraîne que l'anneau A n'est pas noethérien !).

***Remarque 2.13* (Topologie I-adique).** — Soit I un idéal d'un anneau A. On peut munir A de la topologie pour laquelle les $a + I^n$, $n \in \mathbf{N}^*$, forment une base de voisinages ouverts d'un point quelconque a de A. On l'appelle la *topologie I-adique* (cette construction généralise la topologie p-adique sur $\mathbf{Z}$, qui est la topologie associée à l'idéal (p)). Si $I = A$ (resp. $I = 0$), la topologie I-adique est la topologie grossière (resp. discrète).

Les opérations d'anneau sont continues pour cette topologie. Elle est séparée si et seulement si on a $\bigcap_{n=1}^{\infty} I^n = 0$. Le résultat de Krull donne donc des conditions suffisantes pour que cette propriété soit satisfaite. Dans ce cas, la topologie I-adique est métrisable (par une distance ultramétrique) et l'on construit le complété I-adique $\widehat{A}$ de A de la façon habituelle via les suites de Cauchy. C'est un anneau topologique que l'on peut aussi voir comme la limite projective $\varprojlim_n (A/I^n)$; il est muni d'un morphisme d'anneaux $A \to \widehat{A}$ qui est injectif et continu et dont l'image est dense. Par exemple, si $A = \mathbf{Z}$ et $I = (p)$ (p nombre premier), le complété I-adique de $\mathbf{Z}$ est l'anneau des entiers p-adiques $\mathbf{Z}_p$. Si $A = B[X]$ (B anneau) et $I = (X)$, le complété I-adique de A est l'anneau des séries formelles $B[[X]]$.

Toutes ces constructions s'étendent au cas d'un A-module (voir [**M**], § 8).

Exercice 2.14. — Montrer que tout endomorphisme surjectif d'un anneau noethérien est bijectif. Donner un exemple d'un tel endomorphisme injectif mais non surjectif. Montrer que le résultat ne subsiste pas en général pour des anneaux non noethériens.

Exercice 2.15. — Soit $\bar{\mathbf{Z}}$ l'anneau des entiers algébriques (c'est-à-dire l'ensemble des nombres complexes qui sont racines d'un polynôme *unitaire* à coefficients dans $\mathbf{Z}$; *cf.* § 8, en particulier le cor. 8.7, où l'on montre que c'est bien un anneau). Montrer que $\bar{\mathbf{Z}}$ est un anneau intègre qui n'est pas noethérien (*Indication :* on pourra considérer l'idéal de $\bar{\mathbf{Z}}$ engendré par les $2^{1/n}$, pour $n \in \mathbf{N}^*$). On peut montrer que tout idéal de $\bar{\mathbf{Z}}$ engendré par un nombre *fini* d'éléments est principal (on dit que c'est un « anneau de Bézout »), mais je ne connais pas de preuve « élémentaire ».

Exercice 2.16. — Soit $X \subseteq \mathbf{R}$ un compact. On définit comme dans l'exerc. I.1.6 l'anneau $\mathscr{C}_X$ des fonctions continues de X dans $\mathbf{R}$ et ses idéaux maximaux

$$I_x = \{f \in \mathscr{C}_X \mid f(x) = 0\},$$

pour chaque $x \in X$.

a) Montrer que les conditions suivantes sont équivalentes :

(i) l'idéal I_x est engendré par un nombre fini d'éléments ;

(ii) l'idéal I_x est principal ;

(iii) le point x est isolé dans X.

b) Montrer que les conditions suivantes sont équivalentes :

(i) l'anneau $\mathscr{C}_X$ est noethérien ;

(ii) le $\mathbf{R}$-espace vectoriel $\mathscr{C}_X$ est de dimension finie ;

(iii) X est fini.

Exercice 2.17. — On dit qu'un anneau A est *artinien* si toute suite décroissante (pour l'inclusion) d'idéaux de A est stationnaire.

a) Si A est artinien et que I est un idéal de A, montrer que l'anneau A/I est artinien.

b) Montrer qu'un anneau artinien intègre est un corps (*Indication :* si $x \in A - \{0\}$, considérer la suite d'idéaux $((x^n))_{n\geq 1}$).

c) Dans un anneau artinien, montrer que les idéaux premiers sont maximaux (*Indication :* utiliser a) et b)).

d) Montrer qu'un anneau artinien n'a qu'un nombre fini d'idéaux premiers (*Indication :* si $(\mathfrak{m}_n)_{n\geq 1}$ est une suite d'idéaux maximaux distincts, on pourra considérer la suite d'idéaux $(\mathfrak{m}_1 \cdots \mathfrak{m}_n)_{n\geq 1}$).

On peut montrer qu'un anneau est artinien si et seulement s'il est noethérien et que tous ses idéaux premiers sont maximaux ([**P**], th. 4.9).

3. Radical d'un idéal

Définition 3.1. — *Soit I un idéal de A. On pose*

$$\sqrt{I} := \{a \in A \mid \exists m \in \mathbf{N}^* \ \ a^m \in I\}.$$

C'est un idéal de A contenant I, que l'on appelle radical de I. *On dit que I est* radical *si $I = \sqrt{I}$.*

Tout idéal premier est bien sûr radical. Le fait que $\sqrt{I}$ est bien un idéal de A est démontré dans le lemme suivant. Les éléments de $\sqrt{(0)}$ sont dits *nilpotents.* On dit que l'anneau A est réduit si 0 est le seul élément nilpotent. L'idéal I est radical si et seulement si l'anneau A/I est réduit.

Lemme 3.2. — *Pour tous idéaux I et J de A, on a :*

a) *$\sqrt{I}$ est le plus petit idéal radical de A contenant I ;*

b) *$\sqrt{I}$ est l'intersection des idéaux premiers contenant I ;*

c) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$;

d) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

En particulier, pour tout entier $n \geq 1$, on a $\sqrt{I^n} = \sqrt{I}$.

Démonstration. — Si $a \in \sqrt{I}$, avec $a^m \in I$, et $x \in A$, on a $(xa)^m = x^m a^m \in I$ donc $xa \in \sqrt{I}$. Si $b \in \sqrt{I}$, avec $b^n \in I$, on a

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

par la formule du binôme, donc $a + b \in I$, puisque soit $i \geq m$, soit $m + n - i \geq n$. Cela montre que $\sqrt{I}$ est un idéal (contenant I). Montrons qu'il est radical. Si $a \in \sqrt{\sqrt{I}}$, il existe $m \geq 1$ tel que $a^m \in \sqrt{I}$, puis $n \geq 1$ tel que $a^{mn} = (a^m)^n \in I$, de sorte que $a \in \sqrt{I}$. Enfin, si J est un idéal radical contenant I, l'idéal $J = \sqrt{J}$ contient $\sqrt{I}$. Ceci montre a).

Montrons b). Si $\mathfrak{p}$ est un idéal premier contenant I, on a $\mathfrak{p} = \sqrt{\mathfrak{p}} \supseteq \sqrt{I}$. On a donc $\sqrt{I} \subseteq \bigcap_{I \subseteq \mathfrak{p} \subseteq A} \mathfrak{p}$.

Inversement, supposons $a \notin \sqrt{I}$ et considérons l'ensemble $\mathscr{F}$, ordonné par l'inclusion, des idéaux de A contenant I mais ne contenant aucun des a^m pour $m \geq 1$. Il est non vide car il contient I, et toute famille non vide totalement ordonnée d'éléments de $\mathscr{F}$ admet une borne supérieure (leur réunion). Le lemme de Zorn entraîne qu'il existe un élément maximal $J \in \mathscr{F}$. Montrons que J est un idéal premier. Si x et y ne sont pas dans J, on a $J + Ax \notin \mathscr{F}$, donc il existe $m \geq 1$ avec $a^m \in J + Ax$. De même, il existe $n \geq 1$ avec $a^n \in J + Ay$. On a alors $a^{m+n} \in J + Axy$, donc $J + Axy \notin \mathscr{F}$ et $xy \notin J$. Comme $a \notin J$, on a donc montré $a \notin \bigcap_{I \subseteq \mathfrak{p} \subseteq A} \mathfrak{p}$, d'où b).

Pour le point c), les inclusions $\sqrt{IJ} \subseteq \sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$ sont évidentes. Soit a un élément de $\sqrt{I} \cap \sqrt{J}$, et soient m et n des entiers strictement positifs tels que $a^m \in I$ et $a^n \in J$. On a $a^{m+n} = a^m a^n$, qui est dans IJ, donc $a \in \sqrt{IJ}$.

En ce qui concerne le point d), l'inclusion $\sqrt{I+J} \subseteq \sqrt{\sqrt{I} + \sqrt{J}}$ est claire. Soit donc a un élément de $\sqrt{\sqrt{I} + \sqrt{J}}$ et soit n un entier strictement positif tels que $a^n = b + c$, avec $b^r \in I$ et $c^s \in J$. On écrit

$$a^{n(r+s)} = \sum_{i=0}^{r+s} \binom{r+s}{i} b^i c^{r+s-i}$$

qui est dans $J + I$, puisque soit $i \geq r$, soit $r + s - i \geq s$. On a donc bien $a \in \sqrt{I+J}$, ce qui prouve d). □

Exercice 3.3. — Soit I un idéal d'un anneau noethérien A. Montrer qu'il existe $n \in \mathbf{N}^*$ tel que $(\sqrt{I})^n \subseteq I$. Montrer par un exemple qu'il ne suffit pas que I soit engendré par un nombre fini d'éléments.

Exercice 3.4. — Soit $\mathscr{C}$ l'anneau des fonctions continues de $[0,1]$ dans $\mathbf{R}$ (*cf.* exerc. I.1.6). On pose

$$I = \{f \in \mathscr{C} \mid \forall m \in \mathbf{N} \ \lim_{x \to 0} f(x)/x^m = 0\}.$$

Montrer que I est un idéal radical de $\mathscr{C}$. En déduire qu'il existe dans $\mathscr{C}$ des idéaux premiers non maximaux.

4. Décomposition primaire

Une fois qu'il est apparu que l'unicité de la décomposition en irréductibles n'était plus vraie dans des anneaux pourtant très simples (comme $\mathbf{Z}[\sqrt{-5}]$; *cf.* ex. 1.4), il a fallu chercher un substitut valable dans un cadre suffisamment général. C'est cette recherche qui a mené à la « décomposition primaire » des idéaux (en fait, plus généralement, des modules) dans les anneaux noethériens. La première formulation en revient à Lasker (1905, champion du monde d'échecs et joueur de go), qui ne prouve cependant son existence que dans certains anneaux, avec des méthodes très compliquées. C'est à Emmy Noether (1921) que l'on doit la théorie actuelle qui déduit tout de la seule propriété que l'on appelle maintenant « noethérianité » en son honneur.

La première piste (explorée par Dedekind) est de convertir la décomposition d'un élément a non nul d'un anneau factoriel A en produits d'irréductibles en la décomposition d'un idéal non nul en produit d'idéaux premiers. Plus précisément, si on a

$$a = u p_1^{v_1} \cdots p_n^{v_n},$$

avec $u \in A^*$ et $p_1, \ldots, p_n$ irréductibles distincts, on a aussi

$$(a) = (p_1^{v_1} \cdots p_n^{v_n}) = (p_1^{v_1}) \cdots (p_n^{v_n}) = (p_1)^{v_1} \cdots (p_n)^{v_n} = (p_1) \cdots (p_r), \tag{6}$$

où l'on a autorisé des répétitions dans la dernière écriture. De plus, on vérifie immédiatement que cette dernière décomposition est unique dans le sens où si

$$(a) = (q_1) \cdots (q_s),$$

où les idéaux (q_i) sont premiers, alors $r = s$ et il existe une permutation σ de $\{1, \dots, r\}$ telle que $(q_i) = (p_{\sigma(i)})$ pour tout i.

Cette « généralisation » paraît toute bête, mais il existe déjà beaucoup plus d'anneaux qui ont cette propriété de factorisation unique des idéaux (pas nécessairement principaux ; *cf.* § 16). Ceux qui ne sont pas des corps sont appelés *anneaux de Dedekind* et peuvent être aussi caractérisés (c'est comme cela que nous les définirons dans le § 16) comme les anneaux noethériens intègres de dimension 1 (c'est-à-dire pour lesquels tout idéal premier non nul est maximal) intégralement clos (*cf.* § 5.4). Tous les anneaux d'entiers de corps de nombres (*cf.* § 8), dont la plupart ne sont pas factoriels, sont des anneaux de Dedekind (§ 8.2). Mais il reste encore des tas d'anneaux très simples qui n'ont pas cette propriété.

Exercice 4.1. — On a remarqué dans l'ex. 1.4 que les factorisations

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

dans l'anneau $\mathbf{Z}[\sqrt{-5}]$ prouvent que celui-ci n'est pas factoriel (mais c'est un anneau de Dedekind, car c'est l'anneau des entiers de $\mathbf{Q}[\sqrt{-5}]$; *cf.* exerc. 8.20). Montrer que l'on a les décompositions suivantes en produits d'idéaux premiers :

$$\begin{aligned} (2) &= (2, 1 + \sqrt{-5})^2, \\ (3) &= (3, 1 + \sqrt{-5}) \cdot (3, 1 - \sqrt{-5}), \\ (1 \pm \sqrt{-5}) &= (2, 1 \pm \sqrt{-5}) \cdot (3, 1 \pm \sqrt{-5}). \end{aligned}$$

Exercice 4.2. — Nous montrons dans cet exercice que l'anneau intègre $\mathbf{Z}[\sqrt{5}]$ n'a pas la propriété de factorisation unique des idéaux : ce n'est pas un anneau de Dedekind (en revanche, $\mathbf{Z}[(1 + \sqrt{5})/2]$ en est un : c'est l'anneau des entiers de $\mathbf{Q}[\sqrt{5}]$; *cf.* exerc. 8.20).

a) Montrer que l'idéal $\mathfrak{m} := (2, 1 - \sqrt{5})$ de $\mathbf{Z}[\sqrt{5}]$ est maximal (on pourra montrer que l'anneau quotient $\mathbf{Z}[\sqrt{5}]/\mathfrak{m}$ a deux éléments) et que c'est le seul idéal premier de $\mathbf{Z}[\sqrt{5}]$ qui contient l'idéal $I = (2)$ de $\mathbf{Z}[\sqrt{5}]$.

b) Montrer $\mathfrak{m}^2 \subsetneq I \subsetneq \mathfrak{m}$. En déduire que I ne peut s'écrire comme produit (ni intersection) d'un nombre fini d'idéaux premiers de $\mathbf{Z}[\sqrt{5}]$.

Exercice 4.3. — Soit A un anneau noethérien.

a) Soit I un idéal de A. Montrer qu'il existe un entier $n \geq 0$, des idéaux premiers $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ de A et des entiers strictement positifs $r_1, \dots, r_n$ tels que

$$\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} \subseteq I \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n.$$

(*Indication :* on pourra raisonner par l'absurde et considérer un élément maximal dans l'ensemble des idéaux de A qui ne satisfont pas cette propriété.)

b) En déduire qu'il n'existe qu'un nombre fini d'idéaux premiers minimaux dans A.

Pour aller plus loin, réécrivons la décomposition (6) encore d'une autre façon, en utilisant le lemme suivant.

Lemme 4.4. — *Soient $I_1, \dots, I_n$ des idéaux d'un anneau A tels que $I_i + I_j = A$ pour tout $1 \leq i < j \leq n$. Alors*

$$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n.$$

Démonstration. — On a toujours $I_1 \cdots I_n \subseteq I_1 \cap \cdots \cap I_n$. Pour montrer l'autre inclusion, on procède par récurrence sur n, en commençant par le cas $n = 2$. On peut écrire $1 = a_1 + a_2$, avec $a_j \in I_j$. Si $a \in I_1 \cap I_2$, on écrit $a = a(a_1 + a_2) = aa_1 + aa_2$, égalité dans laquelle $aa_1 \in I_1 I_2$ (puisque $a \in I_2$) et $aa_2 \in I_1 I_2$ (puisque $a \in I_1$). On a donc montré $a \in I_1 I_2$.

Pour faire le pas de récurrence, il suffit de montrer que l'on peut appliquer l'hypothèse de récurrence aux idéaux $I_1 I_2, I_3, \dots, I_r$, donc que l'on a $I_1 I_2 + I_j = A$ pour $3 \leq j \leq n$. Écrivons de nouveau $1 = a_1 + a_j =$

a_2+b_j avec a_i dans I_i et b_j dans I_j. On en déduit $1=(a_1+a_j)(a_2+b_j)=a_1a_2+a_1b_j+a_ja_2+a_jb_j$, où $a_1a_2\in I_1I_2$ et les trois autres termes sont dans I_j. On a donc bien montré $I_1I_2+I_j=A$, et le lemme. □

Soit A un anneau qui a la propriété de factorisation unique des idéaux non nuls (c'est-à-dire un anneau de Dedekind ; *cf.* § 16) et soit I un idéal non nul A. On peut l'écrire

$$I=\mathfrak{p}_1^{v_1}\cdots\mathfrak{p}_n^{v_n},$$

où les idéaux $\mathfrak{p}_1,\dots,\mathfrak{p}_n$ sont premiers non nuls (donc maximaux) distincts. Posons $\mathfrak{q}_i=\mathfrak{p}_i^{v_i}$, de sorte que $\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$ (lemme 3.2.c)). Pour $1\leq i<j\leq n$, on a en particulier $\mathfrak{p}_i+\mathfrak{p}_j=A$, ce qui entraîne (lemme 3.2.d))

$$\sqrt{\mathfrak{q}_i+\mathfrak{q}_j}=\sqrt{\mathfrak{p}_i+\mathfrak{p}_j}=A,$$

soit encore $\mathfrak{q}_i+\mathfrak{q}_j=A$. Le lemme 4.4 entraîne alors

$$I=\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_n.$$

C'est un exemple de *décomposition primaire* de l'idéal I, et c'est ce genre de décomposition que l'on va étendre à tous les anneaux noethériens. Les puissances d'idéaux premiers y seront remplacées par les idéaux *primaires,* que nous allons maintenant définir.

***Exercice 4.5* (Lemme d'évitement).** — Soit A un anneau. Montrer que tout idéal de A contenu dans une réunion finie d'idéaux premiers de A est contenu dans l'un d'eux (*Indication :* on pourra procéder par récurrence sur le nombre d'idéaux premiers).

***Exercice 4.6* (Théorème des restes chinois).** — Soient $I_1,\dots,I_n$ des idéaux d'un anneau A tels que $I_i+I_j=A$ pour tout $1\leq i<j\leq n$. Montrer que le morphisme injectif naturel

$$A/(I_1\cap\cdots\cap I_n)\to(A/I_1)\times\cdots\times(A/I_n)$$

est bijectif.

4.1. Idéaux primaires, idéaux irréductibles. —

Définition 4.7. — *Soit I un idéal d'un anneau A.*

a) L'idéal I est primaire *si*

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

b) L'idéal I est irréductible *si, pour tous idéaux I_1 et I_2 de A tels que $I=I_1\cap I_2$, on a $I=I_1$ ou $I=I_2$.*

On dit qu'un élément a d'un anneau A est un *diviseur de zéro* s'il existe $b\in A-\{0\}$ tel que $ab=0$. Un anneau est donc intègre si et seulement si 0 est le seul diviseur de zéro, et un idéal I de A est premier si et seulement si 0 est le seul diviseur de zéro dans A/I. L'idéal I est primaire si et seulement si tout diviseur de zéro est nilpotent.

Un idéal premier est bien sûr primaire ! Mais une puissance d'un idéal premier n'est pas nécessairement primaire (exerc. 4.8) et un idéal primaire n'est pas non plus en général une puissance d'un idéal premier (exerc. 4.9 et 4.10). Dans les anneaux principaux, la situation est plus simple (*cf.* exerc. 4.11).

La terminologie de b) n'est pas excellente : si $I=(a)$ est un idéal principal, « I est irréductible » n'est pas la même chose que « a est irréductible » (même dans un anneau principal ; *cf.* exerc. 4.11). Mais elle sera justifiée plus tard lorsque l'on introduira la topologie de Zariski (§ 5).

Exercice 4.8. — Soit K un corps et soit A l'anneau $K[X,Y,Z]/(XY-Z^2)$. Montrer que l'idéal $\mathfrak{p}$ de A engendré par les classes $\bar{X}$ et $\bar{Z}$ est premier, mais que $\mathfrak{p}^2$ n'est pas primaire.

Exercice 4.9. — Dans l'anneau $\mathbf{Z}[X]$, montrer que l'idéal $(4, X)$ est primaire, de radical $(2, X)$, mais n'est pas une puissance d'un idéal premier.

Exercice 4.10. — Dans l'anneau $\mathbf{Z}[\sqrt{5}]$, montrer que l'idéal (2) est primaire, de radical $(2, 1-\sqrt{5})$, mais n'est pas une puissance d'un idéal premier (*cf.* exerc. 4.2).

Exercice 4.11. — Soit A un anneau principal et soit I un idéal de A. Montrer les équivalences :

$$I \text{ primaire} \iff I \text{ irréductible} \iff I \text{ puissance d'un idéal premier.}$$

Voici quelques implications vraies en général.

Proposition 4.12. — *Soit A un anneau et soit I un idéal de A.*

a) *I premier $\Leftrightarrow$ I irréductible et radical ;*

b) *si A est noethérien, I irréductible $\Rightarrow$ I primaire ;*

c) *$\sqrt{I}$ maximal $\Rightarrow$ I primaire $\Rightarrow$ $\sqrt{I}$ premier.*

Aucune des implications dans b) et c) n'est en général une équivalence (*cf.* exerc. 4.17 et ex. 4.15).

Soit $\mathfrak{p}$ un idéal premier. On dit qu'un idéal primaire I est $\mathfrak{p}$-*primaire* si $\sqrt{I} = \mathfrak{p}$. La terminologie peut sembler étrange, mais elle est pratique.

Enfin, si I et J sont des idéaux d'un anneau A, il est pratique (et classique) de poser

$$(I : J) := \{x \in A \mid xJ \subseteq I\}.$$

C'est un idéal de A contenant I (y penser comme à « I divisé par J »). Si $a \in A$, on pose aussi $(I : a) := (I : (a)) = \{x \in A \mid xa \in I\}$.

Démonstration de la proposition. — Prouvons a). Supposons I premier. Il est alors radical et il s'agit de montrer qu'il est irréductible. Supposons donc $I = I_1 \cap I_2$. Si $I \subsetneq I_1$ et $I \subsetneq I_2$, il existe $a_j \in I_j - I$. Mais $a_1 a_2 \in I_1 I_2 \subseteq I$, ce qui contredit le fait que I est premier.

Pour la réciproque, supposons $ab \in I$. On a alors $((a) + I) \cdot ((b) + I) \subseteq I$, donc

$$I^2 \subseteq \big(((a) + I) \cap ((b) + I)\big)^2 \subseteq ((a) + I) \cdot ((b) + I) \subseteq I.$$

En prenant les radicaux, on obtient, en utilisant le lemme 3.2.c),

$$\sqrt{I} \subseteq \sqrt{((a) + I) \cap ((b) + I)} = \sqrt{(a) + I} \cap \sqrt{(b) + I} \subseteq \sqrt{I}.$$

On a donc égalité et, si I est radical, $I = \sqrt{(a) + I} \cap \sqrt{(b) + I}$. Si I est de plus irréductible, il est égal à $(a) + I$ ou à $(b) + I$, donc soit $a \in I$, soit $b \in I$. Cela montre que I est premier.

Prouvons b). On suppose A noethérien et I irréductible, avec $ab \in I$ mais $a \notin I$. Pour chaque entier $m > 0$, considérons l'idéal

$$I_m := (I : b^m) = \{c \in A \mid cb^m \in I\}.$$

On a des inclusions $I \subseteq I_1 \subseteq I_2 \subseteq \cdots$, donc, A étant noethérien, cette suite croissante se stabilise : il existe $n > 0$ tel que $I_n = I_{n+1}$.

Montrons $((b^n) + I) \cap ((a) + I) = I$. Une inclusion est claire. Pour l'autre, prenons $x \in ((b^n) + I) \cap ((a) + I)$. On peut écrire $x = cb^n + u = da + v$, avec c et d dans A et u et v dans I. On a $cb^{n+1} = dab + b(v - u) \in I$, donc $c \in I_{n+1}$. Ainsi, c est dans I_n, et x est dans I.

Comme $a \notin I$ et que I est irréductible, on en déduit $(b^n) + I = I$, soit $b^n \in I$.

Prouvons c). Supposons $\sqrt{I}$ maximal et prenons $ab \in I$. Si $b \notin \sqrt{I}$, on a $(b) + \sqrt{I} = A$, de sorte que l'on peut écrire $1 = xb + c$, avec $x \in A$ et $c^n \in I$. Mais $c^n = (1 - xb)^n$ peut s'écrire $c^n = 1 + yb$, avec

$y \in A$, et $a = a(c^n - yb) = ac^n - yab$ est dans I puisque c^n et ab y sont. Cela prouve que I est un idéal primaire.

Si I est un idéal primaire, et que $ab \in \sqrt{I}$, on a $a^m b^m \in I$ pour un $m > 0$. Si $a \notin \sqrt{I}$, on a $a^m \notin I$. Puisque I est primaire, on a $(b^m)^n \in I$ pour un $n > 0$, donc $b \in \sqrt{I}$. □

Exercice 4.13. — Soit A un anneau noethérien avec un seul idéal premier. Celui-ci est alors maximal ; on le note $\mathfrak{m}$. Soit M un A-module de type fini. Pour tout $m \in M$, on pose $(0 : m) := \{a \in A \mid am = 0_M\}$. C'est un idéal de A.

a) Si M est non nul, montrer qu'il existe $m \in M$ tel que $(0 : m) = \mathfrak{m}$ (*Indication :* choisir $m \in M - \{0\}$ tel que l'idéal $(0 : m)$ soit maximal parmi tous les idéaux de A de ce type, et montrer qu'il est premier). Montrer que le sous-A-module Am de M est isomorphe à $A/\mathfrak{m}$.

b) Montrer qu'il existe une suite finie $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ de sous-A-modules de M telle que les A-modules M_{i+1}/M_i soient tous isomorphes à $A/\mathfrak{m}$ (*Indication :* on pourra utiliser l'exerc. 2.3). On note $\ell(M)$ le plus petit entier n pour lequel il existe une telle suite.

c) Soit N un sous-A-module de M (il est encore de type fini par l'exerc. 2.3). Montrer que l'on a $\ell(N) \leq \ell(M)$ et qu'il y a égalité si et seulement si $N = M$ (*Indication :* on pourra utiliser la suite de A-modules $(M_i \cap N)_{0 \leq i \leq n}$).

d) Montrer que pour toute suite de sous-A-modules de M comme dans b), on a $n = \ell(M)$.

e) Soit N un sous-A-module de M. Montrer que l'on a $\ell(M) = \ell(N) + \ell(M/N)$.

4.2. Décomposition primaire dans un anneau noethérien. —

Théorème 4.14. — *Dans un anneau noethérien, tout idéal peut s'écrire comme intersection finie d'idéaux irréductibles, donc primaires.*

Une telle décomposition est dite *décomposition primaire* de l'idéal I.

Démonstration. — Supposons au contraire que l'ensemble $\mathscr{E}$ des idéaux d'un anneau noethérien A qui n'ont pas cette propriété soit non vide. Comme A est noethérien, $\mathscr{E}$ admet un élément maximal I, qui ne peut être irréductible. Il existe donc des idéaux I_1 et I_2 de A tels que $I = I_1 \cap I_2$, mais $I \subsetneq I_1$ et $I \subsetneq I_2$. Mais ni I_1, ni I_2 ne sont alors dans $\mathscr{E}$. Ils s'écrivent ainsi tous les deux comme intersection finie d'idéaux irréductibles, et I aussi, ce qui contredit $I \notin \mathscr{E}$. Donc $\mathscr{E}$ est vide, ce qui montre le théorème. □

Si on revient un peu sur les démonstrations précédentes, on réalise qu'elles fournissent une méthode pour trouver pratiquement une telle décomposition.

Soit I un idéal d'un anneau noethérien A. Si I est primaire, c'est terminé. Sinon, il existe $ab \in I$ avec $a \notin I$ et $b \notin \sqrt{I}$. La suite croissante d'idéaux

$$(I : b) \subseteq (I : b^2) \subseteq \cdots$$

se stabilise : il existe $n > 0$ avec $(I : b^n) = (I : b^{n+1})$. La preuve du point b) de la prop. 4.12 montre que l'on a alors $I = ((b^n) + I) \cap ((a) + I)$. On a ainsi écrit I comme intersection de deux idéaux contenant strictement I. Il « suffit » alors de recommencer le processus. Notons tout de suite que cette méthode n'est pas un algorithme : elle n'explique ni comment tester si un idéal est primaire ou non, ni, s'il ne l'est pas, comment trouver les éléments a et b comme ci-dessus. Montrons quand même comment cela peut fonctionner sur un exemple.

Exemple 4.15. — Soit K un corps. L'idéal $I = (X^2, XY)$ de $K[X,Y]$ n'est pas primaire (bien que $\sqrt{I} = (X)$ soit premier) : on a $XY \in I$ mais $X \notin I$ et $Y \notin \sqrt{I}$. On a

$$\begin{aligned}(I : Y) &= \{P \in K[X,Y] \mid YP \in I\} = (X),\\ (I : Y^2) &= \{P \in K[X,Y] \mid Y^2P \in I\} = (X) = (I : Y),\end{aligned}$$

donc $I = ((Y)+I) \cap ((X)+I) = (X^2, Y) \cap (X)$. L'idéal X est premier, donc primaire. L'idéal (X^2, Y) est primaire par prop. 4.12.c) puisque son radical (X, Y) est maximal. L'écriture

$$I = (X) \cap (X^2, Y)$$

est donc une décomposition primaire de I.

Mais on peut aussi partir des éléments $X \notin I$ et $Y^n \notin \sqrt{I}$ (pour chaque $n \in \mathbf{N}^*$). On obtient alors

$$(I : Y^n) = \{P \in K[X,Y] \mid Y^nP \in I\} = (X) = (I : Y^{2n})$$

et une autre décomposition primaire

$$I = (X) \cap (X^2, XY, Y^n)$$

pour tout $n \geq 1$, où l'idéal (X^2, XY, Y^n) est encore (X, Y)-primaire. Il n'y a donc pas unicité.

Maintenant que nous savons qu'une décomposition primaire existe, nous allons la simplifier pour supprimer les redondances possibles et arriver autant que faire se peut à des énoncés d'unicité (cor. 4.20 et th. 4.23).

Lemme 4.16. — *Toute intersection finie d'idéaux* $\mathfrak{p}$*-primaires est encore* $\mathfrak{p}$*-primaire.*

Démonstration. — Il suffit de montrer que l'intersection de deux idéaux $\mathfrak{p}$-primaires I et J a la même propriété. Tout d'abord, on a bien $\sqrt{I \cap J} = \mathfrak{p}$ par le lemme 3.2.c). Supposons $ab \in I \cap J$, avec $a \notin I \cap J$, disons $a \notin I$. Comme I est $\mathfrak{p}$-primaire et $ab \in I$, on a $b \in \mathfrak{p}$. □

Étant donnée une décomposition primaire d'un idéal I, on peut donc toujours la réécrire, grâce au lemme ci-dessus,

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

de façon que $I \neq \bigcap_{i \neq j} \mathfrak{q}_i$ pour tout j et que $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$ pour tout $i \neq j$. On dit alors qu'elle est *minimale.*

Exercice 4.17. — Soit A un anneau noethérien. Comme le montre le th. 4.14, tout idéal I de A peut s'écrire comme intersection $I_1 \cap \cdots \cap I_m$ d'idéaux irréductibles. Une telle décomposition est *minimale* si, pour tout $i \in \{1, \ldots, m\}$, on a $I \neq \bigcap_{k \neq i} I_k$.

a) Montrer que si on a deux décompositions irréductibles minimales $I = I_1 \cap \cdots \cap I_m = J_1 \cap \cdots \cap J_n$, il existe $\sigma \in \mathfrak{S}_n$ tel que $\sqrt{J_k} = \sqrt{I_{\sigma(k)}}$ pour tout k (*Indication :* on pourra montrer que pour tout $j \in \{1, \ldots, m\}$, il existe $k \in \{1, \ldots, n\}$ tel que $I = I_1 \cap \cdots \cap I_{j-1} \cap J_k \cap I_{j+1} \cap \cdots \cap I_m$).

b) Soit K un corps. Dans l'anneau $K[X,Y]$, on considère l'idéal $I = (X^2, XY, Y^2)$. Montrer que

$$I = (X^2, Y) \cap (X, Y^2) = (X^2, X+Y) \cap (X, (X+Y)^2)$$

sont deux décompositions irréductibles minimales, qui ne sont pas minimales comme décompositions primaires.

4.3. Idéaux premiers associés, idéaux premiers immergés. —

Définition 4.18. — *Soit I un idéal d'un anneau A. On dit qu'un idéal premier $\mathfrak{p}$ de A est* associé *à I s'il existe $x \in A$ tel que $\mathfrak{p} = (I : x)$.*

On a toujours $(I : x) \supseteq I$, et $(I : x) = A$ si $x \in I$. Attention, l'idéal $(I : x)$ n'est pas toujours premier. Par exemple, dans $\mathbf{Z}$, on a $((m) : (n)) = (m/m \wedge n)$ si m et n sont non nuls.

Théorème 4.19. — *Soit A un anneau noethérien, soit I un idéal de A et soit*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

une décomposition primaire minimale. Les $\sqrt{\mathfrak{q}_i}$ sont exactement les idéaux premiers associés à I.

En particulier, les $\sqrt{\mathfrak{q}_i}$, qui sont des idéaux premiers deux à deux distincts, sont indépendants de la décomposition primaire minimale de I.

Démonstration. — Posons $\mathfrak{p}_1 := \sqrt{\mathfrak{q}_1}$. Comme la décomposition est minimale, il existe $y \in \bigcap_{i=2}^n \mathfrak{q}_i - \mathfrak{q}_1$. Il existe $m > 0$ tel que $\mathfrak{p}_1^m \subseteq \mathfrak{q}_1$ (exerc. 3.3), de sorte que $y\mathfrak{p}_1^m \subseteq y\mathfrak{q}_1 \subseteq I$. Soit r le plus petit entier vérifiant $y\mathfrak{p}_1^r \subseteq I$. Comme $y \notin I$, on a $r \geq 1$. Choisissons $x \in y\mathfrak{p}_1^{r-1} - I$. On a alors $x \in \bigcap_{i=2}^n \mathfrak{q}_i$, donc $x \notin \mathfrak{q}_1$. Tout comme y, l'élément x est donc dans $\bigcap_{i=2}^n \mathfrak{q}_i - \mathfrak{q}_1$, mais on a de plus $x\mathfrak{p}_1 \subseteq I$, c'est-à-dire $\mathfrak{p}_1 \subseteq (I : x)$.

Montrons $\mathfrak{p}_1 = (I : x)$. On a déjà l'inclusion $\mathfrak{p}_1 \subseteq (I : x)$. Inversement, si $z \in (I : x)$, on a $zx \in I \subseteq \mathfrak{q}_1$, et, comme $\mathfrak{q}_1$ est primaire et $x \notin \mathfrak{q}_1$, on en déduit $z \in \mathfrak{p}_1$. On a donc montré que $\mathfrak{p}_1$ est un idéal premier associé à I.

Soit maintenant $\mathfrak{p} = (I : x)$ un idéal premier associé à I. On a $\mathfrak{p} = (\bigcap_i \mathfrak{q}_i : x) = \bigcap_i (\mathfrak{q}_i : x)$, et comme $\mathfrak{p}$ est irréductible (prop. 4.12.a)), il existe $i \in \{1, \ldots, n\}$ tel que $\mathfrak{p} = (\mathfrak{q}_i : x)$. En particulier, $\mathfrak{p}$ contient $\mathfrak{q}_i$, donc son radical $\sqrt{\mathfrak{q}_i}$ (lemme 3.2.a)). Inversement, si $y \in \mathfrak{p}$, comme $\mathfrak{p} = (I : x)$, on a $yx \in I \subseteq \mathfrak{q}_i$. Si $x \in \mathfrak{q}_i$, on a $(\mathfrak{q}_i : x) = A$, ce qui est absurde, puisque cet idéal est $\mathfrak{p}$. Donc $x \notin \mathfrak{q}_i$, de sorte que $y \in \sqrt{\mathfrak{q}_i}$. On a donc montré $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$. □

Corollaire 4.20. — *Soit A un anneau noethérien, soit I un idéal de A et soient*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m = \mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_n$$

des décompositions primaires minimales. Alors $m = n$ et il existe une permutation σ de $\{1, \ldots, n\}$ telle que $\sqrt{\mathfrak{q}'_i} = \sqrt{\mathfrak{q}_{\sigma(i)}}$ pour tout i.

> ***Exercice 4.21***. — Soit A un anneau noethérien. Montrer que l'ensemble des éléments nilpotents de A est l'intersection des idéaux premiers associés à l'idéal (0), tandis que l'ensemble des diviseurs de 0 est la réunion de ces mêmes idéaux.

Si les idéaux premiers $\sqrt{\mathfrak{q}_i}$ qui apparaissent dans une décomposition minimale de I sont ainsi uniquement déterminés par I, il n'est pas vrai en général que les $\mathfrak{q}_i$ eux-mêmes sont uniquement déterminés, comme le montre l'ex. 4.15. Cependant, on va voir dans le prochain théorème que *certains des* $\mathfrak{q}_i$ sont uniquement déterminés : il s'agit de ceux pour lesquels l'idéal $\sqrt{\mathfrak{q}_i}$ est un *idéal premier minimal contenant* I, c'est-à-dire tel qu'il n'existe aucun autre idéal premier contenu dedans et contenant I.

Exemple 4.22. — Soit K un corps. On a mis en évidence dans l'ex. 4.15 des décompositions primaires de l'idéal $I = (X^2, XY) \subseteq K[X, Y]$: on a

$$I = (X) \cap (X^2, XY, Y^n)$$

pour chaque $n \geq 1$. Celles-ci sont toutes minimales. L'idéal premier associé $(X) = (I : Y)$ est minimal. L'idéal (X^2, XY, Y^n) est (X, Y)-primaire, et $(X, Y) = (I : X)$ est associé mais pas minimal (il contient (X)).

Théorème 4.23. — *Soit A un anneau noethérien, soit I un idéal de A et soit $\mathfrak{p}$ un idéal premier* minimal *contenant I. Alors $\mathfrak{p}$ est associé à I, et dans toute décomposition primaire minimale de I, l'idéal $\mathfrak{p}$-primaire est*

$$\bigcup_{x \notin \mathfrak{p}} (I : x).$$

Il est en particulier indépendant de la décomposition.

En particulier, dans un anneau noethérien, il n'y a qu'un nombre fini d'idéaux premiers minimaux (*cf.* exerc. 4.3). Évidemment, si l'anneau est intègre, le seul idéal premier minimal est (0) !

Démonstration. — Soit $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ une décomposition primaire minimale de I. Si $\mathfrak{p}$ est un idéal premier minimal contenant I, on a $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \subseteq \mathfrak{p}$. Cela entraîne qu'il existe $i \in \{1, \ldots, n\}$ tel que $\mathfrak{q}_i \subseteq \mathfrak{p}$: sinon, on choisit $x_i \in \mathfrak{q}_i - \mathfrak{p}$ pour chaque i ; le produit $x_1 \cdots x_n$ est dans $\mathfrak{q}_1 \cdots \mathfrak{q}_n$, donc dans $\mathfrak{p}$, mais c'est absurde car $\mathfrak{p}$ est premier et aucun des facteurs n'est dans $\mathfrak{p}$. Cela entraîne $I \subseteq \sqrt{\mathfrak{q}_i} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$ et comme $\mathfrak{p}$ est minimal et $\sqrt{\mathfrak{q}_i}$ premier, on a $\sqrt{\mathfrak{q}_i} = \mathfrak{p}$ et $\mathfrak{p}$ est bien associé à I (th. 4.19).

Si $j \neq i$, on a $\mathfrak{p} \neq \sqrt{\mathfrak{q}_j}$, et l'argument qui précède montre que $\bigcap_{j \neq i} \mathfrak{q}_j$ n'est pas contenu dans $\mathfrak{p}$. Prenons $x \in \left(\bigcap_{j \neq i} \mathfrak{q}_j\right) - \mathfrak{p}$. Pour tout élément a de $\mathfrak{q}_i$, on a $ax \in \bigcap_j \mathfrak{q}_j = I$, donc $a \in (I : x)$. On a ainsi montré $\mathfrak{q}_i \subseteq (I : x)$.

Inversement, si $x \notin \mathfrak{p}$ et $a \in (I : x)$, on a $xa \in I$ donc $xa \in \mathfrak{q}_i$. Comme $\mathfrak{q}_i$ est $\mathfrak{p}$-primaire, cela entraîne $a \in \mathfrak{q}_i$. On a ainsi montré $\mathfrak{q}_i = \bigcup_{x \notin \mathfrak{p}} (I : x)$, ce qui termine la démonstration du théorème. □

Soit A un anneau noethérien et soit I un idéal de A. Les idéaux premiers associés à I qui ne sont pas minimaux sont appelés *idéaux premiers immergés.* Si

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

est une décomposition primaire minimale de I, les idéaux premiers associés sont les $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ et

$$\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n,$$

décomposition dans laquelle donc les idéaux premiers immergés ont disparu (cela justifie partiellement la terminologie !).

On a indiqué plus haut une méthode qui peut aider à trouver à la main une décomposition primaire d'un idéal (*cf.* ex. 4.15). Il existe par ailleurs de nombreux algorithmes et plusieurs logiciels informatiques (Singular, Macaulay 2, CoCoA, Magma, etc.) qui font cela très bien dans les anneaux de polynômes. Voici un autre exemple dans $K[X, Y, Z]$:

$$(X^2Y^3 - X^3YZ, Y^2Z - XZ^2) = (Y^2 - XZ) \cap (X^2, Z) \cap (Y, Z^2).$$

L'idéal $(Y^2 - XZ)$ est un idéal premier minimal ; l'idéal (X^2, Z) est (X, Z)-primaire, et (X, Z) est un idéal premier minimal ; l'idéal (Y, Z^2) est (Y, Z)-primaire, et (Y, Z) est un idéal premier immergé (il contient l'idéal premier minimal $(Y^2 - XZ)$).

Exercice 4.24. — Montrer que l'idéal (0) dans l'anneau des fonctions continues de $[0, 1]$ dans $\mathbf{R}$ n'est pas intersection finie d'idéaux primaires.

Exercice 4.25. — Soit I un idéal d'un anneau noethérien. Montrer que I est radical si et seulement si tous les idéaux primaires qui apparaissent dans une décomposition minimale sont premiers. En particulier, si I est radical, I n'a pas d'idéal premier immergé.

Exercice 4.26. — Soient I et J des idéaux d'un anneau noethérien A, avec $I \neq A$. Montrer que $I = (I : J)$ si et seulement si J n'est contenu dans aucun idéal premier associé à I.

Exercice 4.27. — Soit K un corps. Dans l'anneau $K[X, Y, Z]$, on définit $\mathfrak{p}_1 = (X, Y)$, $\mathfrak{p}_2 = (X, Z)$, $I = \mathfrak{p}_1\mathfrak{p}_2$ et $\mathfrak{m} = (X, Y, Z)$. Montrer que $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont des idéaux premiers, tandis que $\mathfrak{m}$ est un idéal maximal. Montrer que

$$I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$$

est une décomposition primaire minimale de I. Quels sont les idéaux premiers associés ? Lesquels sont immergés ?

Exercice 4.28. — Soit K un corps. Dans l'anneau $K[X, Y, Z]$, trouver une décomposition primaire de l'idéal (XY, YZ, ZX).

Exercice 4.29. — a) Donner une décomposition primaire minimale de l'idéal $(X^2 - 2, Y^2 - 2)$ dans $\mathbf{C}[X, Y]$. Y a-t-il des idéaux premiers immergés ?

b) Donner une décomposition primaire minimale de l'idéal $(X^2 - 2, Y^2 - 2)$ dans $\mathbf{Q}[X, Y]$.

5. Topologie de Zariski

Pour comprendre la décomposition primaire d'un point de vue géométrique, il est utile d'introduire la *topologie de Zariski.*

5.1. Spectre d'un anneau. — Soit A un anneau. On appelle *spectre de A,* et l'on note $\mathrm{Spec}(A)$, l'ensemble des idéaux premiers de A. Il est vide si et seulement si $A = 0$. Grâce au lemme suivant, on peut munir cet ensemble d'une topologie en décrétant que les fermés sont les

$$V(I) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \supseteq I\},$$

où I décrit l'ensemble des idéaux de A.

Lemme 5.1. — *Soit A un anneau.*

a) *On a $V((0)) = \mathrm{Spec}(A)$, et $V(I) = \varnothing$ si et seulement si $I = A$.*

b) *Si (I_α) est une famille d'idéaux de A, on a*

$$\bigcap_\alpha V(I_\alpha) = V(\sum_\alpha I_\alpha).$$

c) *Si $I_1, \ldots, I_n$ sont des idéaux de A,*

$$V(I_1) \cup \cdots \cup V(I_n) = V(I_1 \cap \cdots \cap I_n) = V(I_1 \cdots I_n).$$

Démonstration. — Le premier point est évident (avec le lemme de Zorn !). Pour le deuxième point, on a

$$\mathfrak{p} \in \bigcap_\alpha V(I_\alpha) \iff \forall \alpha \quad \mathfrak{p} \supseteq I_\alpha \iff \mathfrak{p} \supseteq \sum_\alpha I_\alpha.$$

Pour le dernier point, il suffit de traiter le cas $n = 2$. Remarquons d'abord que si $I \subseteq J$, alors $V(I) \supseteq V(J)$. Comme $I_1I_2 \subseteq I_1 \cap I_2 \subseteq I_j$, on obtient

$$V(I_1I_2) \supseteq V(I_1 \cap I_2) \supseteq V(I_1) \cup V(I_2).$$

Soit maintenant $\mathfrak{p} \in V(I_1I_2) - V(I_1)$. Il existe alors $x_1 \in I_1 - \mathfrak{p}$, et pour tout $x_2 \in I_2$, on a $x_1x_2 \in I_1I_2 \subseteq \mathfrak{p}$, donc $x_2 \in \mathfrak{p}$ puisque $\mathfrak{p}$ est un idéal premier. On a donc $I_2 \subseteq \mathfrak{p}$, de sorte que $V(I_1I_2) - V(I_1) \subseteq V(I_2)$. □

Une base d'ouverts pour cette topologie est formée des

$$D(f) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid f \notin \mathfrak{p}\} = \mathrm{Spec}(A) - V((f)) \tag{7}$$

pour $f \in A$. En effet, on a, pour tout idéal I, par lemme 5.1.b), $V(I) = \bigcap_{f\in I} V((f))$, donc

$$\mathrm{Spec}(A) - V(I) = \bigcup_{f\in I} D(f).$$

Lemme 5.2. — *On a $V(I) \subseteq V(J)$ si et seulement si $\sqrt{J} \subseteq \sqrt{I}$. En particulier, $V(I) = V(J)$ si et seulement si $\sqrt{I} = \sqrt{J}$.*

Démonstration. — Le lemme 3.2.b) peut aussi s'énoncer

$$\sqrt{I} = \bigcap_{\mathfrak{p}\in V(I)} \mathfrak{p}.$$

On en déduit que si $V(I) \subseteq V(J)$, alors $\sqrt{J} \subseteq \sqrt{I}$. Pour la réciproque, on remarque que $V(I) = V(\sqrt{I})$. Si $\sqrt{J} \subseteq \sqrt{I}$, on en déduit

$$V(J) = V(\sqrt{J}) \supseteq V(\sqrt{I}) = V(I),$$

ce qui termine la démonstration du lemme. □

Pour toute partie S de $\mathrm{Spec}(A)$, on notera

$$I(S) := \bigcap_{\mathfrak{p}\in S} \mathfrak{p}.$$

C'est un idéal de A qui est radical car intersection d'idéaux premiers (donc radicaux). On a :

$$\begin{aligned} V(I(S)) &= \overline{S} \quad \text{pour toute partie } S \text{ de } \mathrm{Spec}(A)\,; \\ I(V(J)) &= \sqrt{J} \quad \text{pour tout idéal } J \text{ de } A. \end{aligned}$$

En effet, il est d'abord clair que le fermé $V(I(S))$ contient S, donc $\overline{S}$. En particulier, pour tout idéal J, on a $V(I(V(J))) \supseteq V(J)$. D'autre part, l'idéal $I(V(J))$ contient J. On en déduit aussi $V(I(V(J))) \subseteq V(J)$ (puisque V renverse les inclusions) ; il y a donc égalité. En particulier, comme $\overline{S}$ peut s'écrire $V(J)$, on en déduit $V(I(\overline{S})) = \overline{S}$. Mais V et I renversent les inclusions, donc $V(I(S)) \subseteq V(I(\overline{S})) = \overline{S}$, et on a la première relation. Enfin, de l'égalité $V(I(V(J))) = V(J)$, on déduit (avec le lemme 5.2, et puisque $I(V(J))$ est radical) la seconde relation.

Une façon agréable de résumer tout cela est de dire que les correspondances

$$\{\text{idéaux radicaux de } A\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{parties fermées de } \mathrm{Spec}(A)\} \tag{8}$$

sont des bijections réciproques qui renversent les inclusions.

L'adhérence d'un point $\mathfrak{p}$ de $\mathrm{Spec}(A)$ est l'intersection de tous les fermés de $\mathrm{Spec}(A)$ contenant $\mathfrak{p}$, c'est-à-dire de tous les $V(I)$ pour lesquels $\mathfrak{p} \in V(I)$, c'est-à-dire $I \subseteq \mathfrak{p}$. Mais on a alors $V(I) \supseteq V(\mathfrak{p})$, donc

$$\overline{\{\mathfrak{p}\}} = \bigcap_{I\subseteq\mathfrak{p}} V(I) = V(\mathfrak{p}) = \{\mathfrak{q} \in \mathrm{Spec}(A) \mid \mathfrak{q} \supseteq \mathfrak{p}\}. \tag{9}$$

En particulier, *le point $\mathfrak{p}$ est fermé si et seulement si $\mathfrak{p}$ est un idéal maximal.* Si l'anneau A est intègre, l'idéal $\{0\}$ correspond à un point dense dans $\mathrm{Spec}(A)$. On dit que c'est le *point générique,* souvent noté η.

Exemple 5.3. — Si K est un corps, $\mathrm{Spec}(K)$ a un seul élément, (0).

Exemple 5.4. — L'ensemble $\mathrm{Spec}(\mathbf{Z})$ est

$$\{\eta\} \cup \{\text{nombres premiers}\}.$$

Tous les points sont fermés, sauf η qui est dense. Les fermés sont les $V((m))$, pour $m \in \mathbf{Z}$, et cet ensemble est $\mathrm{Spec}(\mathbf{Z})$ si $m = 0$, composé des facteurs premiers de m sinon ; ce sont donc les sous-ensembles finis de $\mathrm{Spec}(\mathbf{Z})$ formés de points fermés, ainsi que $\mathrm{Spec}(\mathbf{Z})$ tout entier.

Si f est un entier non nul, l'ouvert $D(f)$ est le complémentaire de l'ensemble (fini) $V((f))$ des diviseurs premiers de f.

Exemple 5.5. — Si K est un corps, $\mathrm{Spec}(K[X])$ est

$$\{\eta\} \cup \{\text{polynômes irréductibles unitaires}\}.$$

Tous les points sont fermés, sauf η qui est dense. Si K est algébriquement clos, les polynômes irréductibles unitaires sont les $X - a$, pour $a \in K$. On a alors

$$\mathrm{Spec}(K[X]) = \{\eta\} \cup K.$$

Les sous-ensembles fermés sont les sous-ensembles finis formés de points fermés, ainsi que $\mathrm{Spec}(K[X])$.

Lorsque $K = \mathbf{R}$, on a

$$\mathrm{Spec}(\mathbf{R}[X]) = \{\eta\} \cup \mathbf{R} \cup \{\text{paires de nombres complexes conjugués non réels}\}.$$

Exemple 5.6. — Si K est un corps, on a (*cf.* exerc. I.1.10)

$$\mathrm{Spec}(K[[X]]) = \{(0)\} \cup \{(X)\}.$$

Il y a donc deux points : un point dense (le point générique) et un point fermé.

Si A est un anneau, on note $A^{\text{réd}}$ le quotient de A par l'idéal des éléments nilpotents de A. On dit que A est *réduit* si le seul élément nilpotent de A est 0. L'anneau $A^{\text{réd}}$ est toujours réduit.

Exercice 5.7. — a) Soit $u : A \to B$ un morphisme d'anneaux. Montrer que l'image inverse par u induit une application continue $u^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$.

b) Soit I un idéal d'un anneau A et soit $p : A \to A/I$ la surjection canonique. Alors $p^\sharp : \mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$ induit un homéomorphisme de $\mathrm{Spec}(A/I)$ sur le fermé $V(I)$ de $\mathrm{Spec}(A)$.

En particulier, la surjection canonique $A \to A^{\text{réd}}$ induit un *homéomorphisme* de $\mathrm{Spec}(A^{\text{réd}})$ sur $\mathrm{Spec}(A)$.

Exemple 5.8. — Soit $\mathscr{P}$ un ensemble de nombres premiers positifs et soit $\mathbf{Z}_{\mathscr{P}}$ l'anneau des nombres rationnels dont le dénominateur n'est divisible par aucun élément de $\mathscr{P}$ [6]. Les éléments de son spectre sont (0) et tous les (p), pour $p \in \mathscr{P}$. L'inclusion $\mathbf{Z} \hookrightarrow \mathbf{Z}_{\mathscr{P}}$ induit une inclusion $\mathrm{Spec}(\mathbf{Z}_{\mathscr{P}}) \hookrightarrow \mathrm{Spec}(\mathbf{Z})$ dont l'image est $\{(0)\} \cup \mathscr{P}$. Elle n'est donc (en général) ni ouverte, ni fermée.

Exemple 5.9. — Si K est un corps, l'inclusion canonique de l'anneau des séries formelles $K[[X]]$ dans son corps des fractions $K((X))$ des séries de Laurent induit une application continue

$$\mathrm{Spec}(K((X))) \to \mathrm{Spec}(K[[X]])$$

qui envoie le seul point (fermé) de $\mathrm{Spec}(K((X)))$ sur le point générique de $\mathrm{Spec}(K[[X]])$.

Nous allons maintenant examiner diverses propriétés topologiques de l'espace $\mathrm{Spec}(A)$. Commençons par deux remarques sur les anneaux produit.

Supposons $A = A_1 \times A_2$. Soit I un idéal de A. Posons $I_1 = \{x_1 \in A_1 \mid (x_1, 0) \in I\}$ et $I_2 = \{x_2 \in A_2 \mid (0, x_2) \in I\}$. Ce sont des idéaux de A_1 et A_2 respectivement, et on a $I_1 \times I_2 \subseteq I$. Inversement, si

6. Avec la terminologie du § 6, l'anneau $\mathbf{Z}_{\mathscr{P}}$ est le localisé de $\mathbf{Z}$ en la partie multiplicative engendrée par les nombres premiers positifs qui ne sont pas dans $\mathscr{P}$.

$x = (x_1, x_2) \in I$, on a $(x_1, 0) = x \cdot (1, 0) \in I$, donc $x_1 \in I_1$, et de la même façon, $x_2 \in I_2$. On a donc $I = I_1 \times I_2$: *tout idéal de A se décompose donc en produit.*

Posons $e = (1, 0)$; on a $e^2 = e$. On dit que e est un *idempotent* de A, et qu'il est non trivial ($e \neq 0$ et $e \neq 1$).

Inversement, si e est un idempotent non trivial d'un anneau A, il en est de même pour $1 - e$, et l'application canonique $p : A \to A/(e) \times A/(1 - e)$ est un isomorphisme d'anneaux (elle est injective parce que si $ae = b(1 - e)$, on obtient $ae = 0$ en multipliant par e ; elle est surjective car l'image contient $(1, 0) = p(1 - e)$ et $(0, 1) = p(e)$). *Un anneau A est* donc *produit d'anneaux non nuls si et seulement s'il contient un idempotent non trivial.*

Proposition 5.10. — *Soit A un anneau. L'espace topologique $\mathrm{Spec}(A)$ est connexe si et seulement si A ne peut pas s'écrire comme produit d'anneaux non nuls.*

Démonstration. — Supposons $A = A_1 \times A_2$. L'exerc. 5.7.b) montre que les deux projections $A \to A_i$ induisent une injection continue de $\mathrm{Spec}(A_1) \sqcup \mathrm{Spec}(A_2)$ dans $\mathrm{Spec}(A)$ qui est un homéomorphisme sur son image. Si $\mathfrak{p} \in \mathrm{Spec}(A)$, il s'écrit comme on l'a vu plus haut $\mathfrak{p} = I_1 \times I_2$. On a $(1, 0) \cdot (0, 1) = (0, 0) \in \mathfrak{p}$, donc soit $(1, 0) \in \mathfrak{p}$, c'est-à-dire $I_1 = A_1$, soit $(0, 1) \in \mathfrak{p}$, c'est-à-dire $I_2 = A_2$. Cela prouve que l'on a une décomposition

$$\mathrm{Spec}(A) = \mathrm{Spec}(A_1) \sqcup \mathrm{Spec}(A_2)$$

en union de deux fermés disjoints.

Supposons maintenant $\mathrm{Spec}(A)$ réunion de deux fermés disjoints non vides $V(I_1)$ et $V(I_2)$. On a alors $I_1 \neq A$, $I_2 \neq A$, $I_1 + I_2 = A$ et $\sqrt{I_1 I_2} = \sqrt{(0)}$ (lemme 5.2). Écrivons $1 = x_1 + x_2$, avec $x_1 \in I_1$ et $x_2 \in I_2$. L'élément $x_1 x_2$ de $I_1 I_2$ est alors nilpotent, donc il existe $m \in \mathbf{N}^*$ tel que $x_1^m x_2^m = 0$. On a alors

$$1 = (x_1 + x_2)^{2m} = x_1^m \sum_{i=m+1}^{2m} \binom{2m}{i} x_1^{i-m} x_2^{2m-i} + x_2^m \sum_{i=0}^{m} \binom{2m}{i} x_1^i x_2^{m-i} := y_1 + y_2.$$

On a alors $y_1 \in I_1$, $y_2 \in I_2$, $1 = y_1 + y_2$ et $y_1 y_2 = 0$. Comme $I_1 \neq A$ et $I_2 \neq A$, ni y_1, ni y_2 n'est nul, donc y_1 est un idempotent non trivial de A, qui est ainsi produit de deux anneaux non nuls. □

On rappelle qu'un espace topologique est *quasi-compact* si de tout recouvrement ouvert on peut extraire un recouvrement fini (de sorte que « compact » est équivalent à « quasi-compact et séparé »).

Proposition 5.11. — *Soit A un anneau. L'espace topologique $\mathrm{Spec}(A)$ est quasi-compact. Il est séparé si et seulement si tout idéal premier est maximal.*

Démonstration. — Soit (U_α) un recouvrement ouvert de $\mathrm{Spec}(A)$. Soit $I_\alpha \subseteq A$ un idéal tel que $\mathrm{Spec}(A) - U_\alpha = V(I_\alpha)$. On a alors $\bigcap_\alpha V(I_\alpha) = \varnothing$, de sorte que $\sum_\alpha I_\alpha = A$ par lemme 5.1.b) et a). On peut donc écrire $1 = \sum_{\alpha \in \Lambda} x_\alpha$, où Λ est un ensemble *fini* et $x_\alpha \in I_\alpha$. En d'autres termes, on a $\sum_{\alpha \in \Lambda} I_\alpha = A$, donc $\mathrm{Spec}(A) = \bigcup_{\alpha \in \Lambda} U_\alpha$. Cela montre que $\mathrm{Spec}(A)$ est quasi-compact.

Un espace topologique est séparé si et seulement si deux points distincts ont des voisinages disjoints. Cela entraîne que tout point est fermé donc, comme on l'a vu plus haut, que tout idéal premier est maximal.

Inversement, si tout idéal premier de A est maximal, tout point est fermé donc, étant donné deux points distincts $\mathfrak{p}$ et $\mathfrak{q}$, le complémentaire de $\{\mathfrak{q}\}$ est un voisinage de $\mathfrak{p}$ qui ne contient pas $\mathfrak{q}$. Mais montrer qu'il existe des voisinages disjoints est plus délicat et ne sera pas fait ici. □

Exercice 5.12. — Terminer la démonstration ci-dessus, en montrant que si A est anneau dans lequel tout idéal premier est maximal, $\mathrm{Spec}(A)$ est séparé (lorsque A est noethérien, cela sera fait dans le § 5.3 ; c'est alors équivalent au fait que $\mathrm{Spec}(A)$ est un ensemble fini muni de la topologie discrète. Dans le cas général, je ne connais pas de preuve simple...).

5.2. Espaces topologiques irréductibles, composantes irréductibles. — Venons-en maintenant à une propriété moins courante.

Définition 5.13. — *Un espace topologique est* irréductible *s'il est non vide et s'il n'est pas réunion de deux fermés stricts.*

Un espace topologique séparé X est irréductible si et seulement s'il est réduit à un point : si X contient deux points distincts, ils ont des voisinages ouverts disjoints U et V, et $X = (X - U) \cup (X - V)$ est une décomposition en réunion de deux fermés stricts. Cette notion n'a donc d'intérêt que pour les espaces topologiques non séparés.

Proposition 5.14. — *Pour un espace topologique X non vide, les propriétés suivantes sont équivalentes :*

(i) *X est irréductible ;*

(ii) *toute intersection finie d'ouverts non vides de X est non vide ;*

(iii) *tout ouvert non vide de X est dense.*

Démonstration. — Supposons X irréductible et soient $U_1, \ldots, U_n$ des ouverts non vides de X. Pour montrer que $U_1 \cap \cdots \cap U_n$ n'est pas vide, on voit qu'il suffit de le faire pour $n = 2$. Si $U_1 \cap U_2 = \varnothing$, on a $X = (X - U_1) \cup (X - U_2)$, ce qui contredit l'irréductibilité de X. Ceci montre que (i) entraîne (ii).

Supposons (ii). Si U est un ouvert non vide de X, les ouverts U et $X - \overline{U}$ sont disjoints, donc $X - \overline{U}$ est vide, de sorte que U est dense dans X. Ceci montre que (ii) entraîne (iii).

Enfin, si tout ouvert non vide de X est dense, et si F_1 et F_2 sont des fermés stricts de X, les ouverts non vides $X - F_1$ et $X - F_2$ sont denses donc se rencontrent, et $F_1 \cup F_2 \neq X$. Ceci montre que (iii) entraîne (i). □

Proposition 5.15. — *Soit X un espace topologique et soit Y une partie de X. Alors Y (muni de la topologie induite) est irréductible si et seulement si $\overline{Y}$ l'est.*

Démonstration. — Supposons Y irréductible. Si $\overline{Y}$ est réunion de fermés F_1 et F_2, alors Y est réunion des fermés $Y \cap F_1$ et $Y \cap F_2$, donc (par exemple) $Y \subseteq F_1$. En passant aux adhérences, on obtient $\overline{Y} = F_1$. Ceci prouve que $\overline{Y}$ est irréductible.

Inversement, si $\overline{Y}$ est irréductible et si Y est réunion de fermés F_1 et F_2, il existe, par définition de la topologie induite, des fermés G_1 et G_2 de X tels que $F_j = Y \cap G_j$. On a alors $Y \subseteq G_1 \cup G_2$, donc $\overline{Y} \subseteq G_1 \cup G_2$. Comme $\overline{Y}$ est irréductible, on a (par exemple) $\overline{Y} \subseteq G_1$, donc $Y \subseteq Y \cap G_1 = F_1$. Ceci montre que Y est irréductible. □

Un espace irréductible est connexe, mais la réciproque est fausse. Comme pour les espaces connexes, on a le résultat utile suivant.

Proposition 5.16. — *L'image d'un espace irréductible par une application continue est encore irréductible.*

Démonstration. — Soit X un espace irréductible et soit $f : X \to Y$ une application continue et supposons $f(X) = F_1 \cup F_2$. On a alors $X = f^{-1}(F_1) \cup f^{-1}(F_2)$, donc, par irréductibilité de X, on a (par exemple) $X = f^{-1}(F_1)$, d'où $f(X) = F_1$. Donc $f(X)$ est bien irréductible. □

Soit X un espace topologique. Un sous-espace de X irréductible maximal (pour l'inclusion) est appelé *composante irréductible* de X ; c'est une partie fermée de X par prop. 5.15. Le lemme de Zorn entraîne que tout point de X est contenu dans une composante irréductible de X, de sorte que X est réunion de ses composantes irréductibles.

Voyons un peu ce que donnent ces concepts dans le cas $X = \mathrm{Spec}(A)$. Tout d'abord, un espace topologique admettant un point dense est irréductible (prop. 5.14). En particulier, le spectre d'un anneau *intègre* est irréductible, et donc, si $\mathfrak{p}$ est un idéal premier d'un anneau A, le fermé $V(\mathfrak{p})$ de $\mathrm{Spec}(A)$, qui s'identifie au spectre de l'anneau intègre $A/\mathfrak{p}$, est irréductible.

Proposition 5.17. — *Soit A un anneau. Les applications de (8) induisent des bijections décroissantes réciproques*

$$\{\text{idéaux premiers de } A\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{parties fermées irréductibles de } \mathrm{Spec}(A)\}.$$

En particulier, les composantes irréductibles de $\mathrm{Spec}(A)$ *correspondent aux idéaux premiers minimaux de A, et* $\mathrm{Spec}(A)$ *est irréductible si et seulement si l'idéal $\sqrt{(0)}$ des éléments nilpotents de A est premier, c'est-à-dire si et seulement si l'anneau $A^{\text{réd}}$ est intègre.*

Cela justifie *a posteriori* la terminologie introduite dans la déf. 4.7 : parmi les idéaux radicaux, les idéaux irréductibles au sens de cette définition (qui, par la prop. 4.12, sont exactement les idéaux premiers) correspondent aux fermés irréductibles au sens topologique.

Démonstration. — On vient de voir que $V(\mathfrak{p})$ est un fermé irréductible. Inversement, une partie fermée de $\mathrm{Spec}(A)$ s'écrit $V(I)$, avec I idéal radical. L'anneau $B = A/I$ est alors réduit, et il s'agit de montrer que si $\mathrm{Spec}(B)$ est irréductible, B est intègre. Si $bc = 0$ dans B, on a $V((b)) \cup V((c)) = V((bc)) = \mathrm{Spec}(B)$ (lemme 5.1.c)). On a donc par exemple $V((b)) = \mathrm{Spec}(B)$ par irréductibilité, donc $\sqrt{(b)} = \sqrt{(0)} = (0)$ (puisque B est réduit). Cela entraîne $b = 0$ et prouve que B est intègre. □

5.3. Espaces topologiques noethériens. —

Définition 5.18. — *Un espace topologique est* noethérien *si toute suite décroissante de parties fermées est stationnaire.*

On peut formuler cette définition de différentes façons : toute suite croissante de parties ouvertes est stationnaire, toute famille non vide de parties fermées a un élément minimal, toute famille non vide de parties ouvertes a un élément maximal, tout ouvert est quasi-compact (on laisse les démonstrations en exercice).

Toute partie d'un espace topologique noethérien, munie de la topologie induite, est encore un espace topologique noethérien.

De nouveau, cette notion n'a donc d'intérêt que pour les espaces topologiques non séparés : un espace topologique noethérien séparé est fini.

Proposition 5.19. — *Un espace topologique noethérien n'a qu'un nombre fini de composantes irréductibles (dont il est la réunion).*

Démonstration. — Soit X un espace topologique noethérien. Soit $\mathscr{E}$ l'ensemble des parties fermées de X qui ne peuvent s'écrire comme réunion finie de parties irréductibles fermées. Si $\mathscr{E}$ n'est pas vide, il admet un élément minimal Y, qui n'est pas irréductible. On peut donc l'écrire comme rénion de deux fermés stricts Y_1 et Y_2. Par minimalité de Y, Y_1 et Y_2 ne sont pas dans $\mathscr{E}$, donc s'écrivent comme union finie de parties irréductibles fermées. Il en est de même pour Y, ce qui est une contradiction. Donc $\mathscr{E}$ est vide : toute partie fermée de X (donc aussi X) peut s'écrire comme réunion finie de parties irréductibles fermées.

Écrivons donc $X = X_1 \cup \cdots \cup X_n$. Si l'un des X_i est contenu dans un autre X_j, on le retire. On arrive ainsi à une décomposition où aucun des X_i n'est contenu dans un autre X_j.

Montrons que X_i est une composante irréductible de X. Supposons $X_i \subseteq Y$, où $Y \subseteq X$ est irréductible. On a $Y = \bigcup_j (Y \cap X_j)$, donc il existe j tel que $Y \cap X_j = X_j$. On a alors $X_i \subseteq Y \subseteq X_j$, ce qui entraîne $i = j$ et $X_i = Y$. Chaque X_i est donc une composante irréductible de X.

Inversement, si Y est une composante irréductible de X, on a de nouveau $Y = \bigcup_j (Y \cap X_j)$, et il existe i tel que $Y \subseteq X_i$. Par maximalité de Y, on a égalité. Ceci termine la démonstration de la proposition. □

La preuve ci-dessus montre que pour trouver les composantes irréductibles d'un espace noethérien, il suffit de le décomposer en réunion finie de parties fermées irréductibles et de supprimer les redondances.

Exemple 5.20. — Soit K un corps. Posons $A := K[X,Y]/(XY)$. L'espace topologique $\mathrm{Spec}(A)$ a deux composantes irréductibles : $V((X))$ et $V((Y))$. En effet $V((X))$ est homéomorphe à $\mathrm{Spec}(A/(X)) = \mathrm{Spec}(K[Y])$, qui est irréductible puisque $K[Y]$ est intègre, et $V((Y))$ est irréductible pour la même raison. Comme aucune de ces deux parties n'est contenue dans l'autre, et que

$$V((X)) \cup V((Y)) = V((XY)) = V((0)) = \mathrm{Spec}(A),$$

ce sont les composantes irréductibles de $\mathrm{Spec}(A)$.

Proposition 5.21. — *Soit A un anneau. L'espace topologique $\mathrm{Spec}(A)$ est noethérien si et seulement si toute suite croissante d'idéaux radicaux de A est stationnaire. En particulier, si l'anneau A est noethérien, $\mathrm{Spec}(A)$ est noethérien.*

Démonstration. — Cela résulte du fait que l'application $I \mapsto V(I)$ induit une bijection décroissante entre idéaux radicaux de A et parties fermées de $\mathrm{Spec}(A)$ (lemme 5.2). □

Corollaire 5.22. — *Soit A un anneau noethérien. Tout idéal radical de A peut s'écrire comme intersection finie non redondante d'idéaux premiers, et ceux-ci sont alors uniquement déterminés.*

On peut en déduire une forme faible de la décomposition primaire des idéaux dans un anneau noethérien. Notons quand même que la formulation du corollaire fait disparaître toute les subtilités liées aux idéaux premiers immergés.

Démonstration. — Cela résulte des prop. 5.17 et 5.19. □

On peut aussi terminer la démonstration de la prop. 5.11 dans le cas où A est noethérien : si tout idéal premier de A est maximal, les composantes irréductibles de $\mathrm{Spec}(A)$ sont des points fermés (prop. 5.17), donc $\mathrm{Spec}(A)$ est un ensemble fini de points fermés (prop. 5.19), et il est séparé.

5.4. Dimension d'un espace topologique, dimension de Krull d'un anneau. —

Définition 5.23. — *Soit X un espace topologique. On appelle* dimension (combinatoire) *de X le supremum des longueurs n des chaînes $F_n \subsetneq \cdots \subsetneq F_1 \subsetneq F_0$ de fermés irréductibles de X.*

Soit A un anneau. On appelle dimension (de Krull) *de A le supremum des longueurs n des chaînes $\mathfrak{p}_n \supsetneq \cdots \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_0$ d'idéaux premiers de A.*

Ces dimensions sont des éléments de $\mathbf{N} \cup \{\pm\infty\}$ et on a bien sûr $\dim(\mathrm{Spec}(A)) = \dim(A)$. La dimension d'un espace topologique est $-\infty$ si et seulement s'il est vide et la dimension de Krull d'un anneau est $-\infty$ si et seulement s'il est nul.

Si A est noethérien, il n'y a pas de chaîne infinie d'idéaux, mais il se peut quand même que la dimension de A soit infinie (exerc. 6.7). En revanche, nous verrons plus tard (cor. 11.12) que toute algèbre de type fini sur un corps est de dimension de Krull finie. Il existe aussi des anneaux A noethériens (dits « non caténaires ») dans lesquels il existe des chaînes d'idéaux premiers maximales (c'est-à-dire, que l'on ne

peut pas agrandir) de longueur $< \dim(A)$ [7] ; heureusement, de nouveau, ce genre de pathologie n'arrive pas pour les algèbres de type fini sur un corps.

Si B est un anneau quotient de A, on a $\dim(A) \geq \dim(B)$, puisque toute chaîne d'idéaux premiers de B se remonte dans A en une chaîne d'idéaux premiers de A.

De façon plus générale, si Y est un sous-espace d'un espace topologique X, on a $\dim(Y) \leq \dim(X)$ (exerc. 5.30).

Exemple 5.24. — Soit $\mathfrak{p}$ un idéal premier d'un anneau A. Les idéaux premiers de l'anneau intègre $A/\mathfrak{p}$ sont en correspondance bijective (et croissante) avec les idéaux premiers de A contenant $\mathfrak{p}$. La dimension de Krull de l'anneau $A/\mathfrak{p}$ est donc le supremum des longueurs n des chaînes d'idéaux premiers de A commençant en $\mathfrak{p}$, c'est-à-dire du type $\mathfrak{p}_n \supsetneq \cdots \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_0 = \mathfrak{p}$.

Exemple 5.25. — Un anneau non nul est de dimension 0 si et seulement si tout idéal premier est maximal (c'est le cas si et seulement si $\mathrm{Spec}(A)$ est séparé ; *cf.* prop. 5.11). Un corps est de dimension 0, puisque le seul idéal premier est (0) ; plus précisément, les corps sont les anneaux intègres de dimension 0.

En fait, les anneaux noethériens de dimension 0 sont les anneaux dits « artiniens », c'est-à-dire ceux pour lesquels toute suite décroissante d'idéaux est stationnaire (exerc. 2.17).

Exemple 5.26. — Un anneau intègre est de dimension 1 si et seulement si tout idéal premier non nul est maximal. C'est le cas pour tous les anneaux principaux qui ne sont pas des corps (prop. I.1.15), comme $\mathbf{Z}$ ou $K[X]$, où K est un corps. Plus généralement, les anneaux de Dedekind (introduits rapidement dans le § 4) sont les anneaux noethériens de dimension 1 intégralement clos (*cf.* déf. 8.15). Ceci inclut tous les anneaux d'entiers de corps de nombres (*cf.* § 8).

Exemple 5.27. — On a vu dans l'exerc. 1.6 qu'un anneau factoriel de dimension 1 est principal.

Exemple 5.28. — Soit K un corps. La chaîne

$$(X_1, \ldots, X_n) \supsetneq \cdots \supsetneq (X_1) \supsetneq (0)$$

d'idéaux premiers de $K[X_1, \ldots, X_n]$ entraîne que la dimension de cet anneau est $\geq n$. Nous montrerons (th. 11.10) qu'elle est exactement n. Plus généralement, si A est un anneau, on a $\dim(A[X]) \geq \dim(A)+1$ (si $\mathfrak{p}_n \supsetneq \cdots \supsetneq \mathfrak{p}_0$ est une chaîne d'idéaux premiers de A, alors $(X, \mathfrak{p}_n) \supsetneq (\mathfrak{p}_n) \supsetneq \cdots \supsetneq (\mathfrak{p}_0)$ est une chaîne d'idéaux premiers de $A[X]$). Il y a égalité si A est noethérien [8], mais pas en général (on a toujours $\dim(A[X]) \leq 2\dim(A) + 1$, et il peut y avoir égalité).

Exercice 5.29. — Soit A un anneau. Montrer $\dim(A[[X]]) \geq \dim(A) + 1$ (mais il existe des anneaux A de dimension de Krull finie pour lesquels $A[[X]]$ est de dimension infinie !). De nouveau, on peut montrer que l'on a égalité lorsque A est un anneau noethérien ([**B3**], Chap. VIII, § 3, n°4, cor. 3 de la prop. 8).

Exercice 5.30. — Soit X un espace topologique et soit Y une partie de X. Montrer $\dim(Y) = \dim(\overline{Y}) \leq \dim(X)$.

Exercice 5.31. — Soit X un espace topologique réunion de parties fermées $X_1, \ldots, X_n$ (par exemple ses composantes irréductibles s'il est noethérien ; *cf.* prop. 5.19). Montrer

$$\dim(X) = \sup_{1 \leq i \leq n} \dim(X_i).$$

Si X est réunion d'une famille (quelconque) $(U_i)_{i \in I}$ de parties ouvertes, montrer

$$\dim(X) = \sup_{i \in I} \dim(U_i).$$

7. Le premier exemple d'un tel anneau est dû à Nagata (On the chain problem of prime ideals, *Nagoya Math. J.* **10** (1956), 51–64).
8. *Cf.* [**B3**], Chap. VIII, § 3, n°4, cor. 3 de la prop. 7 ; voir aussi exerc. 11.13 lorsque A est une algèbre de type fini sur un corps.

6. Localisation

Nous allons avoir maintenant besoin de parler de localisation, une opération fondamentale en algèbre commutative (que nous avons réussi à éviter jusqu'alors !).

Soit A un anneau et S une *partie multiplicative* de A, c'est-à-dire telle que $1 \in S$ et $S \cdot S \subseteq S$. Le but est d'inverser les éléments de S dans un anneau A_S. La procédure est analogue à celle de la construction du corps des fractions d'un anneau intègre (où l'on prend pour S l'ensemble de tous les éléments non nuls). Plus précisément, on définit sur $S \times A$ une relation d'équivalence en posant

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

On note a/s la classe d'équivalence de (s, a) et $S^{-1}A$ l'ensemble des classes d'équivalence. On munit ce dernier d'une structure d'anneau en posant

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

(Il faut bien sûr vérifier que ces définitions sont compatibles avec la relation d'équivalence.) Les éléments de S deviennent ainsi inversibles dans $S^{-1}A$.

Le noyau de l'application canonique $A \to S^{-1}A$ qui envoie a sur $a/1$ est l'idéal $\{a \mid \exists s \in S \ \ as = 0\}$; elle est donc injective si A est intègre et que S ne contient pas 0. L'anneau $S^{-1}A$ est nul si et seulement si S contient 0.

Soit $J \subseteq S^{-1}A$ un idéal ; il est courant (même si c'est un abus de notation) de noter $J \cap A$ l'idéal image inverse de J par l'application canonique $A \to S^{-1}A$ (on fait comme si c'était une inclusion !). On vérifie que l'on a

$$(J \cap A)S^{-1}A = J.$$

(De nouveau, on a fait un abus de notation : $(J \cap A)S^{-1}A$ désigne l'idéal de $S^{-1}A$ engendré par $J \cap A$.)

L'application $\mathrm{Spec}(S^{-1}A) \to \mathrm{Spec}(A)$ définie par $\mathfrak{p} \mapsto \mathfrak{p} \cap A$ est donc injective ; son image est l'ensemble des idéaux premiers de A qui ne rencontrent pas S : si $\mathfrak{p}$ est un tel idéal, c'est l'image de $\mathfrak{p}S^{-1}A$. On a donc en particulier $\dim(S^{-1}A) \leq \dim(A)$ (l'inégalité peut bien sûr être stricte !).

Exemple 6.1. — Soit A un anneau, soit f un élément de A et soit $S \subseteq A$ la partie multiplicative $\{f^n \mid n \in \mathbf{N}\}$. L'anneau $S^{-1}A$ est souvent noté A_f, ou même $A[f^{-1}]$; on peut aussi le voir comme $A[X]/(fX - 1)$, et il est nul si et seulement si f est nilpotent. L'image de l'application $\mathrm{Spec}(A_f) \to \mathrm{Spec}(A)$ est l'ouvert

$$D(f) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid f \notin \mathfrak{p}\} = \mathrm{Spec}(A) - V((f))$$

introduit dans (7).

Par exemple, l'anneau $A[X]_X$ (noté aussi $A[X, X^{-1}]$) est l'anneau des *polynômes de Laurent*

$$\sum_{k \in \mathbf{Z}} a_k X^k,$$

où les coefficients $a_k \in A$ sont presque tous nuls.

Si $\mathfrak{p} \subseteq A$ est un idéal premier, la partie $A - \mathfrak{p}$ est multiplicative et on note

$$A_{\mathfrak{p}} := (A - \mathfrak{p})^{-1}A.$$

C'est un anneau local appelé *localisé de A en $\mathfrak{p}$* : son unique idéal maximal est $\mathfrak{p}A_{\mathfrak{p}}$ et son corps résiduel $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ est le corps des fractions de l'anneau intègre $A/\mathfrak{p}$ (en particulier, si $\mathfrak{m}$ est un idéal maximal de A, le corps résiduel de l'anneau local $A_{\mathfrak{m}}$ est simplement $A/\mathfrak{m}$).

Exercice 6.2. — Notons $\mathscr{C}$ l'anneau (non intègre !) des fonctions continues de $[0,2]$ dans $\mathbf{R}$ et soit $\mathfrak{m}_1 \subseteq \mathscr{C}$ l'idéal maximal des fonctions nulles en 1 (exerc. I.1.6). Montrer que le localisé $\mathscr{C}_{\mathfrak{m}_1}$ s'identifie à l'anneau local des germes de fonctions continues en 1 (*cf.* exerc. II.3.9). En particulier, l'application $\mathscr{C} \to \mathscr{C}_{\mathfrak{m}_1}$ est loin d'être injective.

L'application $\mathrm{Spec}(A_\mathfrak{p}) \to \mathrm{Spec}(A)$ envoie l'idéal maximal $\mathfrak{p}A_\mathfrak{p}$ sur $\mathfrak{p}$ et son image est l'ensemble des idéaux premiers de A contenus dans $\mathfrak{p}$. C'est aussi l'ensemble des points de $\mathrm{Spec}(A)$ auquel $\mathfrak{p}$ est adhérent (*cf.* (9)), ou encore l'intersection de tous les voisinages de $\mathfrak{p}$; il n'est en général ni fermé, ni ouvert.

Les idéaux premiers de l'anneau $A_\mathfrak{p}$ sont ainsi en correspondance bijective (et croissante) avec les idéaux premiers de A contenus dans $\mathfrak{p}$, et la dimension de Krull de l'anneau $A_\mathfrak{p}$ est donc le supremum des longueurs n des chaînes d'idéaux premiers de A terminant en $\mathfrak{p}$, c'est-à-dire du type $\mathfrak{p} = \mathfrak{p}_n \supsetneq \cdots \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_0$. On l'appelle aussi la *hauteur* de $\mathfrak{p}$, notée $\mathrm{ht}(\mathfrak{p})$. Nous montrerons plus loin (th. 7.2) que si A est noethérien, la hauteur de tout idéal premier $\mathfrak{p}$ est finie, majorée par le cardinal d'un ensemble quelconque de générateurs de $\mathfrak{p}$.

On a (*cf.* ex. 5.24)

$$\dim(A_\mathfrak{p}) + \dim(A/\mathfrak{p}) \leq \dim(A)$$

(le membre de gauche est la longueur maximale des chaînes d'idéaux premiers de A dont l'un des maillons est $\mathfrak{p}$). On n'a pas toujours égalité, même si A est noethérien (des contre-exemples très compliqués ont été construits par Nagata en 1956). En revanche, pour la plupart des anneaux intervenant dans les applications (en particulier en géométrie algébrique et en théorie des nombres), on a bien égalité pour tout $\mathfrak{p}$ (c'est vrai en particulier pour toute algèbre A de type fini sur un corps ; *cf.* cor. 14.2). Il faut alors penser à la hauteur de $\mathfrak{p}$ comme à la *codimension* de $\mathfrak{p}$ dans A (elle est égale à $\dim(A) - \dim(A/\mathfrak{p})$ c'est-à-dire, en termes topologiques, à $\dim(\mathrm{Spec}(A)) - \dim(\{\mathfrak{p}\})$).

Exercice 6.3. — Soit A un anneau et soient $\mathfrak{p} \subseteq \mathfrak{q}$ des idéaux premiers de A. Exhiber un anneau dont la dimension de Krull est le supremum des longueurs n des chaînes d'idéaux premiers de A commençant en $\mathfrak{p}$ et terminant en $\mathfrak{q}$, c'est-à-dire du type $\mathfrak{q} = \mathfrak{p}_n \supsetneq \cdots \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_0 = \mathfrak{p}$.

Lorsque A est intègre, l'idéal (0) est premier et le localisé de A en cet idéal est le corps des fractions K_A de A. Tous les localisés $S^{-1}A$, où $S \subseteq A$ est une partie multiplicative ne contenant pas 0, sont alors des sous-anneaux de K_A ; ce sont en particulier des anneaux intègres.

Remarque 6.4. — Si A est un anneau et B une A-algèbre de type fini, les localisations $S^{-1}B$ sont des A-algèbres qui ne sont pas en général de type fini (penser à $K[X]_{(0)} = K(X)$). Cette famille d'algèbres est cependant suffisamment importante pour avoir reçu un nom : on dit que ce sont les A-algèbres *essentiellement de type fini.*

Exercice 6.5. — Soit A un anneau intègre. Montrer

$$A = \bigcap_{\mathfrak{p} \subseteq A \text{ premier}} A_\mathfrak{p} = \bigcap_{\mathfrak{m} \subseteq A \text{ maximal}} A_\mathfrak{m},$$

où les intersections sont prises dans le corps des fractions de A.

Exercice 6.6. — Soit A un anneau et soit $S \subseteq A$ une partie multiplicative.

a) Si A est principal et que S ne contient pas 0, montrer que l'anneau $S^{-1}A$ est principal.
b) Si A est factoriel et que S ne contient pas 0, montrer que l'anneau $S^{-1}A$ est factoriel.
c) Si A est noethérien, montrer que l'anneau $S^{-1}A$ est noethérien.

***Exercice 6.7* (Un anneau noethérien de dimension infinie (Nagata))**. — Soit K un corps et soit A l'anneau de polynômes $K[(X_n)_{n\in\mathbf{N}}]$ en une infinité de variables. Soit $(u_n)_{n\in\mathbf{N}}$ une suite tendant vers l'infini, avec $u_1 = 0$. On note $\mathfrak{p}_n$ l'idéal premier $(X_{u_n}+1, \ldots, X_{u_{n+1}})$, puis S le complémentaire de la réunion des $\mathfrak{p}_n$, et $B = S^{-1}A$.

a) Quels sont les idéaux maximaux de B ?

b) Calculer la dimension de Krull de B et montrer qu'elle peut être infinie si la suite (u_n) est bien choisie.
c) Soit R un anneau dont les localisés en tout idéal maximal sont noethériens et tel que pour tout $x \in R$, il existe un nombre fini d'idéaux maximaux contenant x. Montrer que R est noethérien.
d) Montrer que l'anneau B construit ci-dessus est noethérien.

Nous aurons aussi besoin plus tard du petit lemme suivant.

Lemme 6.8. — *Soit $A \hookrightarrow B$ une extension d'anneaux, soit S une partie multiplicative de A (donc de B) et soit J un idéal de B. On a*

$$(J \cap A)S^{-1}A = JS^{-1}B \cap S^{-1}A.$$

Nous avons fait dans cet énoncé les abus de notation habituels signalés plus haut.

Démonstration. — Il est clair que $(J \cap A)S^{-1}A$ est contenu dans $JS^{-1}B \cap S^{-1}A$. Les éléments de $JS^{-1}B$ sont les x/s, avec $x \in J$ et $s \in S$. Si cet élément est dans $S^{-1}A$, il existe $s', t \in S$ et $a \in A$ tels que $(xs' - as)t = 0$. On a alors $ast = xs't \in J \cap A$ et $x/s = (xs't)/(ss't) \in (J \cap A)S^{-1}A$, ce qui montre le lemme. □

7. Hauptidealsatz

Le nom de ce paragraphe signifie en allemand « théorème de l'idéal principal ». Il majore la hauteur d'un idéal principal dans un anneau noethérien.

Rappelons que la hauteur d'un idéal premier $\mathfrak{p}$ dans un anneau A est le supremum des longueurs n des chaînes d'idéaux premiers de A terminant en $\mathfrak{p}$, c'est-à-dire du type $\mathfrak{p} = \mathfrak{p}_n \supsetneq \cdots \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_0$. C'est aussi la dimension de Krull de l'anneau local $A_\mathfrak{p}$. Si $I \subsetneq A$ est un idéal propre, on notera encore $\mathrm{ht}(I)$ l'infimum des hauteurs $\mathrm{ht}(\mathfrak{p})$, où $\mathfrak{p}$ est un idéal premier de A contenant I. On a toujours l'inégalité

$$\mathrm{ht}(I) + \dim(A/I) \leq \dim(A).$$

De nouveau, dans les « bons » anneaux (où l'on a égalité), il faut penser à la hauteur de I comme à sa « codimension » : elle est égale à $\dim(\mathrm{Spec}(A)) - \dim(V(I))$.

Théorème 7.1 **(Krulls Hauptidealsatz)**. — *Soit A un anneau noethérien et soit a un élément de A. Pour tout idéal premier minimal $\mathfrak{p}$ contenant (a), on a $\mathrm{ht}(\mathfrak{p}) \leq 1$. En particulier, si a n'est pas inversible, $\mathrm{ht}((a)) \leq 1$.*

Démonstration. — Soit $\mathfrak{p}$ un idéal premier minimal contenant (a). Raisonnons par l'absurde et supposons qu'il existe une chaîne $\mathfrak{p} = \mathfrak{p}_2 \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_0$ d'idéaux premiers de A. Si on remplace A par $A/\mathfrak{p}_0$, on se ramène au cas $\mathfrak{p}_0 = 0$ (l'anneau est en particulier intègre) ; si on remplace ensuite A par $A_\mathfrak{p}$, on se ramène finalement au cas où A est un anneau intègre local noethérien d'idéal maximal $\mathfrak{m}$ avec un élément a tel que $\mathfrak{m}$ est le seul idéal premier de A contenant a. Autrement dit, l'anneau $B := A/(a)$ a un seul idéal premier. Nous utiliserons les notations et résultats de l'exerc. 4.13.

Prenons $b \in \mathfrak{p}_1$ non nul. Soit $n \in \mathbf{N}^*$; nous allons considérer $M := A/(a^n)$ comme un B-module. Notons M_1 le noyau de son endomorphisme « multiplication par b », M_3 son image et $M_2 := M/M_3$ son conoyau. On a

$$\begin{aligned} M_1 &= \{\overline{x} \in M \mid xb \in (a^n)\} \simeq ((a^n) : b)/(a^n), \\ M_2 &= \big(A/(a^n)\big)\big/\big(bA/(a^n)\big) \simeq A/(a^n, b). \end{aligned}$$

Comme $M_3 \simeq M/M_1$ et $M_2 = M/M_3$, nous avons d'autre part (exerc. 4.13.e))

$$\ell(M_1) = \ell(M) - \ell(M_3) = \big(\ell(M_2) + \ell(M_3)\big) - \ell(M_3) = \ell(M_2),$$

de sorte que $\ell(M_1) = \ell(M_2)$.

D'autre part, pour tout $\overline{x} \in M_1$, il existe $y \in A$ tel que $xb = ya^n$. On a en particulier $y \in ((b) : a^n)$. Comme x est bien défini à addition d'un multiple de a^n près et que A est intègre, x est bien défini à addition d'un multiple de b près et l'association $x \mapsto y$ définit un isomorphisme $((a^n) : b)/(a^n) \simeq ((b) : a^n)/(b)$ de A-modules.

Comme A est noethérien, la suite croissante d'idéaux $((b) : a^n)$ de A est stationnaire, donc $((b) : a^n) = ((b) : a^{n+1})$ pour un entier $n > 0$ assez grand. On en déduit un isomorphisme

$$((a^n) : b)/(a^n) \simeq ((a^{n+1}) : b)/(a^{n+1})$$

de A-modules, donc aussi de B-modules. Ils ont donc la même longueur. Il s'ensuit que les B-modules $A/(a^n, b)$ et $A/(a^{n+1}, b)$ ont aussi la même longueur. Cela entraîne (exerc. 4.13.e)) que la surjection canonique $A/(a^{n+1}, b) \to A/(a^n, b)$ est un isomorphisme, donc que l'on a $(a^n, b) = (a^{n+1}, b)$. Il existe donc des éléments x et y de A tels que $a^n = xa^{n+1} + yb$, c'est-à-dire $a^n(1 - xa) = by$.

Mais $1 - xa$ est une unité de A (lemme 3.7), donc $a^n \in (b) \subseteq \mathfrak{p}_1$ et $a \in \mathfrak{p}_1$. Mais c'est absurde car $\mathfrak{p}$ est un idéal premier minimal contenant a. Ceci termine donc la démonstration. □

On généralise le théorème précédent ainsi.

Théorème 7.2. — *Soit A un anneau noethérien et soit I un idéal propre de A engendré par n éléments. Pour tout idéal premier minimal $\mathfrak{p}$ contenant I, on a $\mathrm{ht}(\mathfrak{p}) \leq n$. En particulier, $\mathrm{ht}(I) \leq n$.*

Dans un « bon » anneau A, ce théorème dit que la partie fermée de $\mathrm{Spec}(A)$ correspondant à un idéal engendré par n éléments est de codimension au plus n (cor. 14.7).

On n'a bien sûr pas toujours égalité (on peut toujours ajouter des générateurs « inutiles ») ; plus sérieusement, si $\mathrm{ht}(I) = n$, il n'est pas toujours possible d'engendrer I avec seulement n éléments [9].

Démonstration. — On procède par récurrence sur n, le cas $n = 1$ étant le théorème précédent. Comme dans la preuve précédente, on se ramène au cas où A est un anneau intègre local noethérien d'idéal maximal $\mathfrak{m}$; si $a_1, \ldots, a_n$ engendrent un idéal $I \subseteq \mathfrak{m}$ tel que $\mathfrak{m}$ est le seul idéal premier de A contenant I, il s'agit de montrer $\mathrm{ht}(\mathfrak{m}) = \dim(A) \leq n$.

Supposons au contraire qu'il existe une chaîne $\mathfrak{m} = \mathfrak{p}_m \supsetneq \cdots \supsetneq \mathfrak{p}_1 \supsetneq (0)$ d'idéaux premiers de A avec $m > n$. Comme A est noethérien, on peut supposer que $\mathfrak{p}_{m-1}$ est maximal parmi tous les idéaux premiers strictement contenus dans $\mathfrak{m}$. L'idéal $\mathfrak{p}_{m-1}$ ne contient pas tous les a_i ; supposons $a_n \notin \mathfrak{p}_{m-1}$. L'idéal $\mathfrak{p}_{m-1} + (a_n)$ n'est alors contenu dans aucun autre idéal premier de A autre que $\mathfrak{m}$, qui est donc son radical (lemme 3.2.b)).

Pour chaque $i \in \{1, \ldots, n-1\}$, on a $a_i \in \mathfrak{m}$; il existe donc un entier $r > 0$ tel que $a_i^r \in \mathfrak{p}_{m-1} + (a_n)$ pour tout i. On écrit $a_i^r \in x_i + y_i a_n$, avec $x_i \in \mathfrak{p}_{m-1}$ et $y_i \in A$. On a $(a_1^r, \ldots, a_{n-1}^r, a_n) = (x_1, \ldots, x_{n-1}, a_n)$, donc le seul idéal premier de A contenant $(x_1, \ldots, x_{n-1}, a_n)$ est $\mathfrak{m}$.

Posons $J := (x_1, \ldots, x_{n-1})$. Dans l'anneau quotient $\overline{A} := A/J$, cela signifie que le seul idéal premier de A contenant l'idéal principal $(\overline{a}_n)$ est $\overline{\mathfrak{m}} := \mathfrak{m}/J$. Le th. 7.1 entraîne $\mathrm{ht}(\overline{\mathfrak{m}}) \leq 1$. Comme on a $\overline{\mathfrak{m}} \supsetneq \mathfrak{p}_{m-1}/J$, cela signifie que $\mathfrak{p}_{m-1}$ est un idéal premier minimal contenant J. L'hypothèse de récurrence entraîne alors $m - 1 \leq n - 1$, d'où le théorème. □

Corollaire 7.3. — *La hauteur de tout idéal propre d'un anneau noethérien est finie.*

Corollaire 7.4. — *La dimension d'un anneau local noethérien est finie.*

9. Si K un corps, l'idéal (XY, YZ, ZX) de l'anneau $K[X, Y, Z]$ est de hauteur 2 (*cf.* exerc. 4.28 et cor. 14.2), mais ne peut être engendré par 2 éléments (c'est difficile à montrer !).

Exercice 7.5. — Soit A un anneau local noethérien d'idéal maximal $\mathfrak{m}$. On pose $B = A[X]$. Soit I un idéal de A de radical $\mathfrak{m}$ et soit J un idéal de B contenu dans $\mathfrak{m}B$ tel que $J + XB = IB + XB$.

a) Montrer que $\mathfrak{m}B + XB$ est un idéal maximal de B qui est le radical de $IB + XB$.

b) Dans l'anneau $\overline{B} := B/J$, montrer que l'idéal $(\mathfrak{m}B + XB)/J$ est un idéal premier minimal contenant l'idéal principal $(\overline{X})$.

c) En déduire que $\mathfrak{m}B$ est un idéal premier minimal contenant J (*Indication :* on pourra utiliser le th. 7.1).

Exercice 7.6 **(Eagon-Northcott)**. — Soit A un anneau noethérien et soit $M \in \mathscr{M}_{m\times n}(A)$ une matrice à coefficients dans A. Soit I l'idéal de A engendré par les $r \times r$ mineurs de M. Le but de cet exercice est de montrer que pour tout idéal premier minimal $\mathfrak{p}$ contenant I, on a [10]

$$\mathrm{ht}(\mathfrak{p}) \leq (m - r + 1)(n - r + 1).$$

a) Montrer que cette inégalité est vraie lorsque $m = 1$. On procède par récurrence sur m.

b) Montrer que l'inégalité est vraie lorsque $r = 1$.

c) Montrer qu'on peut supposer A local d'idéal maximal $\mathfrak{m} = \mathfrak{p}$, égal au radical de I.

d) Montrer que si un des coefficients de M est une unité de A, l'inégalité est vraie (*Indication :* on pourra utiliser des opérations élémentaires pour se ramener à une matrice de taille $(m - 1) \times (n - 1)$).

e) On suppose $r > 1$ et que tous les coefficients de M sont dans $\mathfrak{m}$, et on pose $B = A[X]$. Soit $N \in \mathscr{M}_{m\times n}(B)$ la matrice obtenue à partir de M en changeant le coefficient a_{11} en $a_{11} + X$, et soit J l'idéal de B engendré par les $r \times r$ mineurs de N. Montrer $J \subseteq \mathfrak{m}B$ et $J + XB = IB + XB$. En déduire $\mathrm{ht}(\mathfrak{m}B) \leq (m-r+1)(n-r+1)$ (*Indication :* on pourra utiliser l'exerc. précédent, puis travailler dans l'anneau local $B_{\mathfrak{m}B}$ et utiliser d)).

f) Montrer $\mathrm{ht}(\mathfrak{m}) \leq \mathrm{ht}(\mathfrak{m}B)$ et conclure.

Exercice 7.7 **(Anneaux locaux réguliers)**. — Soit A un anneau local noethérien d'idéal maximal $\mathfrak{m}$. On note κ le corps $A/\mathfrak{m}$ (on l'appelle le *corps résiduel* de l'anneau local A).

a) Montrer que $\mathfrak{m}/\mathfrak{m}^2$ est naturellement muni d'une structure de κ-espace vectoriel de dimension finie.

b) Montrer que $\dim_\kappa \mathfrak{m}/\mathfrak{m}^2$ est égal au nombre minimum de générateurs de l'idéal $\mathfrak{m}$ de A (*Indication :* on pourra utiliser le lemme de Nakayama (th. II.3.8)).

c) Montrer $\dim(A) \leq \dim_\kappa \mathfrak{m}/\mathfrak{m}^2$. On dit que l'anneau local A est *régulier* s'il y a égalité.

d) Soient m et n des entiers strictement positifs et soit A le localisé de l'anneau quotient $\mathbf{C}[X, Y]/(X^m - Y^n)$ en l'idéal maximal $(\overline{X}, \overline{Y})$. Avec les notations précédentes, calculer $\dim_\kappa \mathfrak{m}/\mathfrak{m}^2$ en fonction de m et n. Déterminer les paires (m, n) pour lesquelles l'anneau A est régulier (*Indication :* on pourra utiliser le fait que l'anneau A est de dimension 1 (cor. 11.14)).

8. Extensions finies et entières d'anneaux

Soit A un anneau. Une A-algèbre est un anneau B muni d'un morphisme d'anneaux $A \to B$.

Définition 8.1. — *Soit A un anneau et soit B une A-algèbre.*

a) *On dit que B est une* A-algèbre de type fini *si elle peut être engendrée, en tant que A-algèbre, par un nombre fini d'éléments.*

b) *On dit que B est une* A-algèbre finie *si elle peut être engendrée, en tant que A-module, par un nombre fini d'éléments.*

Pour être tout-à-fait explicite, B est une A-algèbre de type fini s'il existe des éléments $x_1, \ldots, x_n$ de B tels que tout élément de B puisse s'écrire $P(x_1, \ldots, x_n)$, où P est un polynôme en n variables à coefficients dans A. De façon équivalente, la A-algèbre B est quotient d'un algèbre de polynômes $A[X_1, \ldots, X_n]$.

10. Si l'on utilise le th. 10.2, la prop. 10.9 et le cor. 14.2, ce résultat entraîne que lorsque K est un corps algébriquement clos, le fermé de $\mathscr{M}_{m\times n}(K) \simeq K^{mn}$ constitué des matrices de rang $\leq s$ est de codimension au plus (en fait exactement) $(m - s)(n - s)$ (il est défini par l'annulation des $(s + 1) \times (s + 1)$ mineurs).

L'anneau de séries formelles $A[[X]]$ n'est pas une A-algèbre de type fini lorsque A est non nul (*cf.* cor. 10.8).

De même, B est une A-algèbre finie s'il existe des éléments $x_1, \dots, x_n$ de B tels que tout élément de B puisse sécrire $a_1x_1 + \cdots + a_nx_n$, avec $a_1, \dots, a_n \in A$. De façon équivalente, le A-module B est quotient d'un A-module libre de type fini A^n. Une telle algèbre est bien sûr de type fini, mais la réciproque est fausse en général : la A-algèbre $A[X]$ est de type fini, mais n'est pas finie.

Définition 8.2. — *Soit A un anneau et soit B une A-algèbre.*

a) *On dit qu'un élément x de B est* entier sur A *s'il existe un polynôme* unitaire $P \in A[X]$ *tel que* $P(x) = 0$.

b) *On dit que B est* entier sur A *si tout élément de B est entier sur A.*

On dira qu'une A-algèbre B est une *extension* de A si l'application canonique $A \to B$ est injective. On notera alors $A \hookrightarrow B$.

Si $A \hookrightarrow B$ est une extension de corps, elle est entière si et seulement si elle est algébrique, tandis que les deux définitions de « finie » coïncident.

Proposition 8.3. — *Soit $A \hookrightarrow B$ une extension d'anneaux et soit $x \in B$. Les propriétés suivantes sont équivalentes :*

(i) *x est entier sur A ;*

(ii) *$A[x]$ est une A-algèbre finie ;*

(iii) *il existe une A-algèbre finie C telle que $A[x] \subseteq C \subseteq B$.*

Démonstration. — Supposons x entier sur A. Il est alors annulé par un polynôme unitaire de degré n et on vérifie que le A-module $A[x]$ est engendré par $\{1, x, \dots, x^{n-1}\}$. Comme (ii) entraîne trivialement (iii), il reste à montrer que (iii) entraîne (i).

Appliquons le théorème de Cayley-Hamilton (th. II.3.2) à l'endomorphisme u du A-module C donné par la multiplication par x. Il fournit un polynôme unitaire $P \in A[X]$ tel que $P(u) = 0$. Mais alors $P(x) = P(u)(1)$ s'annule. □

Corollaire 8.4. — *Une extension d'anneaux finie est entière.*

Proposition 8.5. — *Soient $A \hookrightarrow B \hookrightarrow C$ des extensions d'anneaux.*

a) *Si les extensions $A \hookrightarrow B$ et $B \hookrightarrow C$ sont finies, il en est de même pour l'extension $A \hookrightarrow C$.*

b) *Si les extensions $A \hookrightarrow B$ et $B \hookrightarrow C$ sont entières, il en est de même pour l'extension $A \hookrightarrow C$.*

c) *Si $x_1, \dots, x_n$ sont des éléments de B entiers sur A, la A-algèbre $A[x_1, \dots, x_n]$ est finie.*

Démonstration. — La démonstration de a) est la même que dans le cas des corps (*cf.* preuve du th. I.2.4) : si $(b_i)_{i\in I}$ engendre le A-module B et que $(c_j)_{j\in J}$ engendre le B-module C, alors $(b_ic_j)_{(i,j)\in I\times J}$ engendre le A-module C.

Le point c) résulte de a) et de la prop. 8.3, par récurrence sur n.

Enfin, supposons les extensions $A \hookrightarrow B$ et $B \hookrightarrow C$ entières et soit $x \in C$. Comme il est entier sur B, il existe une relation

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 = 0.$$

Comme les b_i sont entiers sur A, la A-algèbre $A[b_0, \dots, b_{n-1}]$ est finie. Comme x est entier sur cette algèbre, $A[b_0, \dots, b_{n-1}, x]$ est finie sur $A[b_0, \dots, b_{n-1}]$. Par a), il en résulte que $A[b_0, \dots, b_{n-1}, x]$ est finie sur A, donc x est entier sur A par cor. 8.4. Ceci montre b) et termine la démonstration de la proposition. □

La réciproque du point b) est vraie : si l'extension $A \hookrightarrow C$ est entière, tout élément de C est entier sur A, donc sur B, de sorte que l'extension $B \hookrightarrow C$ est entière ; de même, tout élément de B est entier sur A, de sorte que l'extension $A \hookrightarrow B$ est entière.

Si l'extension $A \hookrightarrow C$ est finie, C est un A-module de type fini, donc aussi un B-module de type fini, de sorte que l'extension $B \hookrightarrow C$ est entière. L'extension $A \hookrightarrow B$ est entière si A est noethérien (parce qu'un sous-module d'un A-module de type fini est alors encore de type fini ; *cf.* exerc. 2.3), mais pas en général [11].

On a aussi l'analogue du cor. I.2.11.

Corollaire 8.6. — *Toute extension d'anneaux $A \hookrightarrow B$ engendrée par un nombre fini d'éléments entiers sur A est finie, donc entière. En particulier, toute extension d'anneaux entière et de type fini est finie.*

Démonstration. — Ce n'est qu'une réécriture de la prop. 8.5.c). □

Corollaire 8.7. — *Soit $A \hookrightarrow B$ une extension d'anneaux. L'ensemble des éléments de B entiers sur A est un sous-anneau de B, extension entière de A appelée* clôture intégrale *de A dans B.*

On dit que A est *intégralement clos* dans B si sa clôture intégrale dans B est A, c'est-à-dire que tout élément de B entier sur A est dans A. La clôture intégrale de A dans B est intégralement close dans B (pourquoi ?).

Démonstration. — Si x et y sont des éléments de B entiers sur A, la A-algèbre $A[x, y]$ est finie par prop. 8.5.c), donc ses éléments $x - y$ et xy sont entiers sur A (cor. 8.4). □

Nous aurons besoin plus loin du résultat suivant.

Lemme 8.8. — *Soit $A \hookrightarrow B$ une extension d'anneaux entière et soit S une partie multiplicative de A (donc de B). L'extension d'anneaux $S^{-1}A \hookrightarrow S^{-1}B$ est entière.*

Démonstration. — Soit x/s un élément de $S^{-1}B$. L'élément x de B est entier sur A donc il existe une relation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

avec $a_0, \ldots, a_{n-1} \in A$. On a alors

$$(x/s)^n + (a_{n-1}/s)(x/s)^{n-1} + \cdots + (a_1/s^{n-1})(x/s) + (a_0/s^n) = 0$$

dans $S^{-1}A$, de sorte que x/s est entier sur cet anneau. □

Exercice 8.9. — Soit $A \hookrightarrow B$ une extension d'anneaux entière et soit S une partie multiplicative de A.

a) Si l'extension $A \hookrightarrow B$ est finie, l'extension $S^{-1}A \hookrightarrow S^{-1}B$ est finie.

b) Si A est intégralement clos dans B, l'anneau $S^{-1}A$ est intégralement clos dans $S^{-1}B$.

Exercice 8.10. — Soit $A \hookrightarrow B$ une extension finie d'anneaux intègres. Montrer que l'extension associée $K_A \hookrightarrow K_B$ des corps de fractions est finie, mais que la réciproque est fausse.

11. Voici un exemple. Soit J un idéal d'un anneau A qui n'est pas engendré par un nombre fini d'éléments. Soit C la A-algèbre finie $A[X]/(X^2)$ et soit B la sous-A-algèbre de C engendrée par 1 et JX, c'est-à-dire $\{a + rX \mid a \in A,\ r \in J\}$. Le A-module quotient B/A est isomorphe à J, donc n'est pas de type fini ; il s'ensuit que le A-module B n'est pas non plus de type fini (merci à Jin Lie pour cet exemple !).

***Exercice 8.11* (Lemme d'Artin-Tate).** — Soit A un anneau noethérien et soient $A \hookrightarrow B \hookrightarrow C$ des extensions d'anneaux. On suppose que C est une A-algèbre de type fini et une B-algèbre finie. Le but de cet exercice est de montrer que B est une A-algèbre de type fini.

Soient $c_1, \dots, c_m$ des générateurs de la A-algèbre C et soient $c'_1, \dots, c'_n$ des générateurs du B-module C. On écrit $c_i = \sum_j b_{ij} c'_j$, avec $b_{ij} \in B$ et $c'_i c'_j = \sum_k b'_{ijk} c'_k$, avec $b'_{ijk} \in B$. Soit $B' \subseteq B$ la sous-A-algèbre engendrée par les b_{ij} et les b'_{ijk}.

a) Montrer que l'anneau B' est noethérien.
b) Montrer que C est une extension finie de B'.
c) Montrer que B est une extension finie de B'.
d) Conclure.

Exercice 8.12. — Soit K un corps et soit A une K-algèbre de type fini. Soit G un groupe fini agissant sur A de façon que l'action soit triviale sur K.

a) Montrer que $A^G := \{a \in A \mid \forall g \in G \ \ g \cdot a = a\}$ est une sous-K-algèbre de A.
b) Montrer que A est une extension finie de A^G (*Indication :* si $a \in A$, on pourra considérer le polynôme $\prod_{g \in G}(X - g \cdot a)$).
c) Montrer que A^G est une K-algèbre de type fini (*Indication :* on pourra utiliser l'exerc. 8.11).

Exercice 8.13. — Soit K un corps de caractéristique différente de 2. Le groupe $G := \mathbf{Z}/2\mathbf{Z}$ agit sur $A := K[X, Y]$ par la multiplication par -1. Identifier la sous-K-algèbre $A^G := \{a \in A \mid \forall g \in G \ \ g \cdot a = a\}$ de A et montrer qu'elle est isomorphe à $K[U, V, W]/(UV - W^2)$.

8.1. Traces d'entiers. — Soit $K \hookrightarrow L$ une extension finie de corps. On a défini dans le § I.5.6 la forme K-linéaire $\mathrm{Tr}_{L/K} : L \to K$ comme l'application qui à $x \in L$ associe la trace de l'endomorphisme K-linéaire m_x de L « multiplication par x ».

Proposition 8.14. — *Soit A un anneau intègre de corps de fractions K et soit $K \hookrightarrow L$ une extension finie de corps. Si $x \in L$ est entier sur A, l'élément $\mathrm{Tr}_{L/K}(x)$ de K est entier sur A.*

La preuve ci-dessous montre aussi que tous les coefficients du polynôme minimal de x sur K sont entiers sur A.

Démonstration. — Il ressort du th. I.5.32 que l'on a

$$\mathrm{Tr}_{L/K}(x) = [L : K(x)] \, \mathrm{Tr}_{K(x)/K}(x).$$

On peut donc supposer $L = K(x)$. On a vu au cours de la preuve du th. I.5.35 que $\mathrm{Tr}_{L/K}(x)$ est alors la somme des racines (dans un corps de décomposition de P) du polynôme minimal P de x sur K. Comme x est aussi racine d'un polynôme unitaire $Q \in A[X]$, le polynôme P divise Q, donc toutes les racines de P sont aussi racines de Q et sont ainsi entières sur A. Il en est donc de même pour leur somme $\mathrm{Tr}_{L/K}(x)$ (cor. 8.7). □

8.2. Anneaux intégralement clos. —

Définition 8.15. — *Un anneau est dit* intégralement clos *s'il est intègre et intégralement clos dans son corps des fractions.*

Exemple 8.16. — L'anneau intègre $A = \mathbf{Z}[\sqrt{5}]$ n'est pas intégralement clos : son corps des fractions est $K = \mathbf{Q}[\sqrt{5}]$, l'élément $(1 + \sqrt{5})/2$ de K est entier sur A (il est annulé par le polynôme $X^2 - X - 1 \in A[X]$), mais il n'est pas dans A. Sa clôture intégrale dans K est $\mathbf{Z}[(1 + \sqrt{5})/2]$ (exerc. 8.20).

Exercice 8.17. — Soit A un anneau intègre. Montrer que les propriétés suivantes sont équivalentes (*cf.* exerc. 6.5) :

(i) l'anneau A est intégralement clos ;

(ii) pour tout idéal premier $\mathfrak{p}$ de A, l'anneau $A_\mathfrak{p}$ est intégralement clos ;

(iii) pour tout idéal maximal $\mathfrak{m}$ de A, l'anneau $A_\mathfrak{m}$ est intégralement clos.

Exercice 8.18. — Soit A un anneau intégralement clos de corps des fractions K et soit $K \hookrightarrow L$ une extension algébrique de corps. Montrer qu'un élément de L est entier sur A si et seulement si son polynôme minimal sur K est à coefficients dans A.

Un *corps de nombres* L est une extension finie de $\mathbf{Q}$. L'*anneau des entiers* de L est la clôture intégrale B de $\mathbf{Z}$ dans L. C'est un anneau intégralement clos. Comme $\mathbf{Z}$, l'anneau B est de dimension 1 (th. 11.8 ; mais il existe une preuve plus simple dans ce cas particulier que l'on peut trouver dans [**L**], prop. I.5.6). Enfin, il est noethérien grâce au théorème suivant. C'est donc un *anneau de Dedekind,* comme défini brièvement dans le § 4. Remarquons que le groupe abélien $(B, +)$ est sans torsion, de type fini par le théorème, donc isomorphe à un $\mathbf{Z}^n$ (th. II.4.10).

Théorème 8.19. — *Soit A un anneau* noethérien intégralement clos, *de corps de fractions K et soit $K \hookrightarrow L$ une extension finie* séparable *de K. La clôture intégrale de A dans L est un anneau noethérien, extension finie de A.*

Démonstration. — Soit B la clôture intégrale de A dans L. Soit x un élément de L. Il satisfait alors à une équation

$$x^n + \lambda_{n-1}x^{n-1} + \cdots + \lambda_1 x + \lambda_0 = 0,$$

avec $\lambda_{n-1}, \ldots, \lambda_0 \in K$. Soit $a \in A - 0$ tel que $a\lambda_i$ soit dans A pour tout i. On a alors

$$(ax)^n + a\lambda_{n-1}(ax)^{n-1} + \cdots + a^{n-1}\lambda_1(ax) + a^n\lambda_0 = 0,$$

de sorte que ax est entier sur A, donc dans B. En particulier, il existe une base $(b_1, \ldots, b_m)$ du K-espace vectoriel L constituée d'éléments de B.

Posons

$$N := \{x \in L \mid \forall j \in \{1, \ldots, m\} \quad \mathrm{Tr}_{L/K}(xb_j) \in A\}.$$

C'est un sous-A-module de L contenant B (prop. 8.14). L'extension $K \hookrightarrow L$ étant séparable, l'application $\mathrm{Tr}_{L/K}$ définit une forme K-bilinéaire symétrique non dégénérée sur L (th. I.5.35) et il existe une base $(x_1, \ldots, x_m)$ du K-espace vectoriel L telle que $\mathrm{Tr}_{L/K}(x_i b_j) = \delta_{i,j}$ (symbole de Kronecker). On a alors $N = Ax_1 + \cdots + Ax_m$, de sorte que N est un A-module de type fini. Comme A est noethérien, B est aussi un A-module de type fini (exerc. 2.3) ; c'est ainsi une extension finie de A. C'est un anneau noethérien par cor. 2.8. □

Exercice 8.20. — Soit d un entier sans facteur carré, différent de 1. Montrer que l'anneau des entiers du corps $\mathbf{Q}(\sqrt{d})$ est $\mathbf{Z}[\sqrt{d}]$ si $d \equiv 2$ ou $3 \pmod 4$, et $\mathbf{Z}[(1+\sqrt{d})/2]$ si $d \equiv 1 \pmod 4$.

Lorsque $d < 0$, l'anneau des entiers de $\mathbf{Q}(\sqrt{d})$ est principal si et seulement si d est l'un des entiers -1, -2, -3, -7, -11, -19, -43, -67, -163. Pour $d > 0$, les anneaux principaux sont beaucoup plus nombreux. En 2008, il est conjecturé qu'il en existe une infinité [12].

Proposition 8.21. — *Un anneau factoriel est intégralement clos.*

La réciproque est fausse : on a vu (ex. 1.4) que l'anneau intègre $\mathbf{Z}[\sqrt{-5}]$ n'est pas factoriel ; mais il est intégralement clos (exerc. 8.20).

12. Pour tous les anneaux d'entiers de corps de nombres, et plus généralement pour tous les anneaux de dimension 1, le fait d'être principal ou factoriel est la même chose (exerc. 1.6).

Démonstration. — Soit A un anneau factoriel. Supposons qu'un élément x/y de son corps des fractions (avec $x \wedge y = 1$) soit racine d'un polynôme unitaire

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1 x + a_0 \in A[X].$$

On a alors

$$x^n + a_{n-1}x^{n-1}y + \cdots + a_1 x y^{n-1} + a_0 y^n = 0,$$

de sorte que y divise x^n. La prop. 1.3 entraîne que y divise x, donc est une unité de A, de sorte que $x/y \in A$. □

Exemple 8.22. — Si K est un corps, on a vu dans l'exerc. 1.5 que le sous-anneau $A = K[X^2, X^3]$ de $K[X]$ n'est pas factoriel. Il n'est en fait pas intégralement clos, puisque son corps des fractions est $K(X)$, que X est entier sur A (il est annulé par le polynôme $T^2 - X^2 \in A[T]$), mais qu'il n'est pas dans A.

Théorème 8.23. — *Soit A un anneau intégralement clos. L'anneau $A[X]$ est intégralement clos.*

Démonstration. — Commençons par deux lemmes.

Lemme 8.24. — *Soit $A \hookrightarrow B$ une extension d'anneaux et soit P un élément de $A[X]$ tel que $P = QR$, où Q et R sont des polynômes* unitaires *de $B[X]$. Les coefficients de Q et de R sont entiers sur A.*

Démonstration. — Notons B_1 l'anneau $B[T]/(Q)$. Comme Q est unitaire, c'est un B-module libre de rang $\deg(Q)$ et l'application canonique $B \to B_1$ est en particulier injective. Si α_1 est la classe de T dans B_1, on a $Q(X) = (X - \alpha_1)Q_1(X)$ dans $B_1[X]$. En répétant cette construction, on obtient une extension finie d'anneaux $B \hookrightarrow C$ dans laquelle $Q(X) = \prod_j (X - \alpha_j)$ et $R(X) = \prod_k (X - \beta_k)$ sont scindés. Les α_j et β_k sont entiers sur A car annulés par P, donc aussi les coefficients de Q et de R, puisque ce sont des polynômes en les α_j et β_k (cor. 8.7). □

On en déduit immédiatement le lemme suivant, qui est une version du « lemme de Gauss » (lemme 1.9) pour les anneaux intégralement clos.

Lemme 8.25. — *Soit A un anneau intégralement clos de corps des fractions K et soit $P \in A[X]$ tel que $P = QR$, où Q et R sont des polynômes unitaires de $K[X]$. Alors Q et R sont dans $A[X]$.*

Revenons à la démonstration du théorème. Si K est le corps des fractions de A, celui de $A[X]$ est $K(X)$. On prend donc un élément P de $K(X)$ entier sur $A[X]$ et il s'agit de montrer qu'il est dans $A[X]$. Comme $K[X]$ est principal, donc intégralement clos (cor. 2.6 et prop. 8.21), $P \in K[X]$ et on a une relation

$$P^n + A_{n-1}P^{n-1} + \cdots + A_1 P + A_0 = 0,$$

où $A_0, \ldots, A_{n-1} \in A[X]$. On peut donc écrire A_0 comme le produit de P et d'un autre polynôme. Malheureusement, on ne peut pas appliquer le lemme 8.25, puisque ces polynômes n'ont aucune raison d'être unitaires. L'astuce consiste à poser $Q = P - X^m$, où m est un entier $> \max(\deg(P), \deg(A_0), \ldots, \deg(A_{n-1}))$. On a alors

$$0 = (X^m + Q)^n + A_{n-1}(X^m + Q)^{n-1} + \cdots + A_1(X^m + Q) + A_0,$$

qui peut se réécrire

$$Q^n + B_{n-1}Q^{n-1} + \cdots + B_1 Q + B_0 = 0,$$

avec

$$B_0 = A_0 + A_1 X^m + \cdots + A_{n-1}X^{m(n-1)} + X^{mn} \in A[X].$$

Le choix de m entraîne que $-Q$ et B_0 sont unitaires, puis le lemme 8.25 que Q est dans $A[X]$, c'est-à-dire $P \in A[X]$. □

Exercice 8.26. — Soit A un anneau factoriel dans lequel 2 est inversible et soit $a \in A$ un élément divisible par le carré d'aucun élément irréductible de A. Montrer que l'anneau $A[\sqrt{a}] := A[X]/(X^2 - a)$ est intégralement clos (*Indication :* utiliser l'exerc. 8.18).

Exercice 8.27. — Soit A un anneau intègre sur lequel agit un groupe fini G. On note A^G l'anneau des invariants, c'est-à-dire $A^G := \{a \in A \mid \forall g \in G \ \ g \cdot a = a\}$.

a) Montrer que l'action de G sur A se prolonge de façon unique en une action sur son corps des fractions K_A.
b) Montrer que le corps des fractions K_{A^G} de A^G est un sous-corps du corps des invariants K_A^G.
c) Montrer que l'on a en fait $K_{A^G} = K_A^G$.
d) Si A est intégralement clos, montrer que A^G est intégralement clos.

9. Lemme de normalisation de Noether

Soit K un corps et soit A une K-algèbre. Des éléments $a_1, \ldots, a_n$ de A sont dits *algébriquement indépendants* si

$$\forall P \in K[X_1, \ldots, X_n] \quad \big(P(a_1, \ldots, a_n) = 0\big) \Rightarrow \big(P = 0\big).$$

En d'autres termes, la sous-extension $K[a_1, \ldots, a_n] \subseteq A$ est isomorphe à $K[X_1, \ldots, X_n]$. Dans le cas contraire, on dit que $a_1, \ldots, a_n$ sont *algébriquement liés.*

Théorème 9.1 **(Lemme de normalisation d'E. Noether)**. — *Soit K un corps et soit A une K-algèbre de type fini. Il existe des éléments algébriquement indépendants $a_1, \ldots, a_n$ de A tels que A soit une extension finie de $K[a_1, \ldots, a_n]$.*

En d'autres termes, l'extension $K \hookrightarrow A$ se décompose en $K \hookrightarrow K[a_1, \ldots, a_n] \hookrightarrow A$ où la première extension est dite *transcendante pure* et la seconde est finie. L'extension intermédiaire $K[a_1, \ldots, a_n]$ n'est pas unique, mais l'entier n l'est : nous montrerons plus tard (cor. 11.12) que c'est la dimension de Krull de A.

La démonstration ci-dessous est due à Nagata (1962). La démonstration originale d'E. Noether (1926) supposait K infini.

Démonstration. — Elle repose sur le lemme suivant.

Lemme 9.2. — *Soit A une K-algèbre de type fini engendrée par des éléments $x_1, \ldots, x_m$ algébriquement liés. Il existe des éléments $y_1, \ldots, y_{m-1}$ de A tels que x_m est entier sur $A' := K[y_1, \ldots, y_{m-1}]$ et $A = A'[x_m]$.*

Montrons comment ce lemme entraîne le théorème. Supposons A engendrée par des éléments $x_1, \ldots, x_m$ et procédons par récurrence sur m. Si les x_i sont algébriquement indépendants, on les prend pour les a_i et A est une extension transcendante pure de K. S'ils sont algébriquement liés, on applique le lemme : il existe $y_1, \ldots, y_{m-1} \in A$ tels que A est fini sur $A' := K[y_1, \ldots, y_{m-1}]$. L'hypothèse de récurrence s'applique à A' : il existe des éléments algébriquement indépendants $a_1, \ldots, a_n \in A'$ tels que A' soit une extension finie de $K[a_1, \ldots, a_n]$. La prop. 8.5.a), appliquée aux extensions finies

$$K[a_1, \ldots, a_n] \hookrightarrow A' \hookrightarrow A,$$

permet alors de terminer la démonstration du théorème. □

Démonstration du lemme. — Soit $P \in K[X_1, \ldots, X_m]$ non nul tel que $P(x_1, \ldots, x_m) = 0$. On cherche les y_i sous la forme $y_i = x_i - x_m^{e^i}$, pour $1 \leq i \leq m-1$, où e est un entier suffisamment grand. Pour tout choix de e, on a $A = K[y_1, \ldots, y_{m-1}, x_m]$. En outre,

$$0 = P(y_1 + x_m^e, \ldots, y_{m-1} + x_m^{e^{m-1}}, x_m) =: Q(y_1, \ldots, y_{m-1}, x_m).$$

Posons $A' := K[y_1, \ldots, y_{m-1}]$. On aimerait que le coefficient dominant du polynôme $Q(y_1, \ldots, y_{m-1}, X)$, vu comme élément de $A'[X]$, soit inversible dans A' (car cela impliquerait que x_m est entier sur A'). On a pour tout monôme

$$\begin{aligned} X_1^{r_1} \cdots X_m^{r_m} &= \Big(\prod_{i=1}^{m-1} (Y_i + X_m^{e^i})^{r_i} \Big) X_m^{r_m} \\ &= Y_1^{r_1} \cdots Y_{m-1}^{r_{m-1}} X_m^{r_m} + \cdots + X_m^{r_1 e + r_2 e^2 + \cdots + r_{m-1} e^{m-1} + r_m}. \end{aligned}$$

Le dernier terme est l'unique terme de plus haut degré en X_m. Si e est strictement plus grand que tous les exposants r_i qui apparaissent dans les monômes de P, le degré $r_1 e + r_2 e^2 + \cdots + r_{m-1} e^{m-1} + r_m$ détermine les r_i uniquement : ce sont les chiffres de son écriture en base e. Dans ce cas, des monômes distincts de P donnent des puissances distinctes de X_m dans Q. Une seule de ces puissances est maximale et elle apparaît avec un coefficient dans K^*. □

La clôture intégrale d'un anneau noethérien intègre n'est pas toujours un anneau noethérien (encore un contre-exemple dû à Nagata !). Nous allons déduire du lemme de Noether que dans le cas « géométrique », ce genre de pathologie n'arrive heureusement pas.

Corollaire 9.3. — *Soit K un corps, soit A une K-algèbre intègre de type fini, de corps des fractions K_A, et soit $K_A \hookrightarrow L$ une extension finie. La clôture intégrale de A dans L est une K-algèbre intègre de type fini, extension finie de A.*

Démonstration. — D'après le th. 9.1, il existe des éléments algébriquement indépendants $a_1, \ldots, a_n$ de A tels que A soit une extension finie de l'anneau $K[a_1, \ldots, a_n]$; ce dernier est isomorphe à un anneau de polynômes $K[X_1, \ldots, X_n]$, donc est *noethérien intégralement clos.* Le corps K_A est alors une extension finie de $K(a_1, \ldots, a_n)$ (exerc. 8.10), de sorte que L est aussi une extension finie de $K(a_1, \ldots, a_n)$. La clôture intégrale B de A dans L est aussi la clôture intégrale de $K[a_1, \ldots, a_n]$ dans L (les éléments de L entiers sur A sont les mêmes que les éléments de L entiers sur $K[a_1, \ldots, a_n]$ par la prop. 8.5.b)).

Si la caractéristique de K est nulle, l'extension finie $K(a_1, \ldots, a_n) \hookrightarrow L$ est séparable, et B est, par le th. 8.19, un anneau noethérien, extension finie de $K[a_1, \ldots, a_n]$, donc de A.

Reste à traiter le cas plus compliqué où la caractéristique de K est un nombre premier $p > 0$. Comme expliqué dans le cas de caractéristique nulle, on peut supposer $A = K[a_1, \ldots, a_n]$, isomorphe à un anneau de polynômes $K[X_1, \ldots, X_n]$. Comme A est noethérien, un sous-A-module d'un A-module de type fini est encore de type fini (exerc. 2.3), donc on peut aussi remplacer pour la preuve L par une extension finie, par exemple par sa clôture normale dans une clôture algébrique. L'extension finie $K_A \hookrightarrow L$ est alors normale. Soit $G := \mathrm{Gal}(L/K_A)$ le groupe de ses K_A-automorphismes ; l'extension $L' := L^G \hookrightarrow L$ est galoisienne (lemme d'Artin ; th. 6.22) donc séparable.

Montrons tout d'abord le résultat pour la clôture intégrale B' de A dans L'. Considérons des générateurs $y_1, \ldots, y_m$ de l'extension $K_A \hookrightarrow L'$. Par l'exerc. I.6.24, il existe un entier $r > 0$ tel que tous les $y_i^{p^r}$ sont dans K_A. On peut écrire $y_i^{p^r} = P_i/Q_i$, où P_i et Q_i sont dans $A = K[a_1, \ldots, a_n]$. Soient $t_1, \ldots, t_s \in K$ tous les coefficients non nuls qui interviennent dans ces polynômes. Notons $K' := K(t_1^{p^{-r}}, \ldots, t_s^{p^{-r}})$ (où

les racines p^r-ièmes sont prises dans une clôture algébrique de L') ; c'est une extension finie de K, et

$$\begin{aligned} L' &= K_A(y_1, \dots, y_m) \\ &\subseteq K_A(P_1^{p^{-r}}, Q_1^{p^{-r}}, \dots, P_m^{p^{-r}}, Q_m^{p^{-r}}) \\ &\subseteq K_A(t_1^{p^{-r}}, \dots, t_s^{p^{-r}}, a_1^{p^{-r}}, \dots, a_n^{p^{-r}}) \\ &= K'(a_1^{p^{-r}}, \dots, a_n^{p^{-r}}) =: L''. \end{aligned}$$

La clôture intégrale B' de A dans L' est contenue dans la clôture intégrale de A dans L''. Comme l'extension de corps $K \hookrightarrow K'$ est finie, l'extension d'anneaux $A = K[a_1, \dots, a_n] \hookrightarrow K'[a_1, \dots, a_n]$ est aussi finie. L'extension d'anneaux $K'[a_1, \dots, a_n] \hookrightarrow K'[a_1^{p^{-r}}, \dots, a_n^{p^{-r}}]$ est aussi finie, donc l'extension composée $A \hookrightarrow K'[a_1^{p^{-r}}, \dots, a_n^{p^{-r}}]$ est finie (prop. 8.5.a)), donc entière. Comme l'anneau $K'[a_1^{p^{-r}}, \dots, a_n^{p^{-r}}]$ est intégralement clos (dans son corps des fractions L''), c'est la clôture intégrale de A dans L'', qui est ainsi un A-module de type fini. Comme A est noethérien, cela entraîne que son sous-A-module B' est aussi de type fini.

Comme B est la clôture intégrale de B' dans L, l'argument employé en caractéristique nulle entraîne que l'extension $B' \hookrightarrow B$ est finie, donc aussi l'extension composée $A \hookrightarrow B' \hookrightarrow B$. L'anneau B est en particulier une A-algèbre de type fini, donc aussi une K-algèbre de type fini. □

Exercice 9.4. — Soit K un corps et soit A une K-algèbre intègre essentiellement de type fini (rem. 6.4). Montrer que la clôture intégrale de A dans son corps de fractions est une extension finie de A.

Remarque 9.5 **(Anneaux excellents)**. — La finitude de la clôture intégrale est une propriété essentielle pour pouvoir construire ce que l'on appelle la « normalisation » d'une variété en géométrie algébrique. Elle est heureusement partagée par de nombreux anneaux noethériens, en particulier les anneaux appelés « excellents » par Grothendieck (Éléments de géométrie algébrique IV 2, *Publ. Math. IHÉS* **24** (1965), § 7.8). Cette classe d'anneau est stable par localisation et passage à une algèbre de type fini ; elle comprend aussi les anneaux de Dedekind de caractéristique nulle (donc par exemple $\mathbf{Z}$) et les anneaux de séries formelles sur un corps.

10. Théorème des zéros de Hilbert

Ce théorème fondamental (« Nullstellensatz » en allemand) prend plusieurs formes. Sa plus frappante est celle du cor. 10.4.

Lemme 10.1. — *Soit $A \hookrightarrow B$ une extension entière d'anneaux intègres. Alors A est un corps si et seulement si B est un corps.*

Démonstration. — Supposons que A est un corps. Soit x un élément non nul de B. Comme x est entier sur A, le A-espace vectoriel $A[x]$ est de dimension finie et comme la multiplication par x est une application linéaire injective (puisque B est intègre), elle est surjective. Donc 1 est atteint, et un inverse de x existe dans $A[x]$. Cela signifie que x est inversible dans B, qui est donc un corps.

Inversement, supposons que B est un corps. Soit x un élément non nul de A et soit y l'inverse de x dans B. Il est entier sur A, donc on a une relation $y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0$. En multipliant par x^{n-1}, on obtient

$$y + a_{n-1} + \cdots + a_0 x^{n-1} = 0,$$

ce qui prouve que y est dans A. □

Théorème 10.2 **(Nullstellensatz)**. — *Soit $K \hookrightarrow L$ une extension de corps telle que L est une K-algèbre de type fini. L'extension $K \hookrightarrow L$ est finie.*

Démonstration. — Par le lemme de normalisation, il existe des éléments algébriquement indépendants $a_1, \ldots, a_n$ de L tels que L soit une extension finie, donc entière (cor. 8.4), de $K[a_1, \ldots, a_n]$. Par le lemme 10.1, $K[a_1, \ldots, a_n]$ est un corps, donc $n = 0$. □

Le Nullstellensatz entraîne que si K est un corps, pour tout idéal maximal $\mathfrak{m}$ de l'anneau $K[X_1, \ldots, X_n]$, le corps $K[X_1, \ldots, X_n]/\mathfrak{m}$, qui est une K-algèbre de type fini, est une extension finie de K.

Corollaire 10.3. — *Soit K un corps algébriquement clos. Les idéaux maximaux de l'anneau de polynômes $K[X_1, \ldots, X_n]$ sont les idéaux*

$$\mathfrak{m}_x := (X_1 - x_1, \ldots, X_n - x_n),$$

pour $x = (x_1, \ldots, x_n)$ décrivant K^n.

Démonstration. — Soit $x \in K^n$. L'idéal $\mathfrak{m}_x$ est le noyau du morphisme (surjectif) d'évaluation $e_x : K[X_1, \ldots, X_n] \to K$ défini par $e_x(P) = P(x)$. On a donc $K[X_1, \ldots, X_n]/\mathfrak{m}_x \simeq K$ et $\mathfrak{m}_x$ est donc bien un idéal maximal (quel que soit le corps K).

Inversement, si $\mathfrak{m}$ est un idéal maximal, on a vu ci-dessus que $K[X_1, \ldots, X_n]/\mathfrak{m}$ est une extension finie de K, qui est donc, K étant algébriquement clos, isomorphe à K. Soit x_i l'image de X_i par cet isomorphisme. Chaque polynôme $X_i - x_i$ s'annule dans ce quotient, donc est dans $\mathfrak{m}$. L'idéal maximal $\mathfrak{m}_{(x_1,\ldots,x_n)}$ est contenu dans $\mathfrak{m}$, donc lui est égal. □

Corollaire 10.4. — *Soit K un corps algébriquement clos. Considérons un système d'équations polynomiales*

$$\begin{cases} F_1(x_1, \ldots, x_n) = 0 \\ \qquad\vdots \\ F_r(x_1, \ldots, x_n) = 0 \end{cases}$$

à coefficients dans K. Pour que ce système n'admette aucune solution dans K^n, il faut et il suffit qu'il existe $G_1, \ldots, G_r \in K[X_1, \ldots, X_n]$ tels que $\sum_{i=1}^r F_i G_i = 1$.

Démonstration. — Soit I l'idéal de $K[X_1, \ldots, X_n]$ engendré par $F_1, \ldots, F_r$. Pour que $x \in K^n$ soit solution du système, il faut et il suffit que $e_x(F_i)$ soit nul pour tout i, c'est-à-dire que I soit contenu dans $\mathrm{Ker}(e_x) = \mathfrak{m}_x$.

Pour que le système n'ait pas de solution, il faut et il suffit donc que I ne soit contenu dans aucun $\mathfrak{m}_x$, donc dans aucun idéal maximal de $K[X_1, \ldots, X_n]$ (cor. 10.3). Cela n'est possible que lorsque $I = K[X_1, \ldots, X_n]$, c'est-à-dire lorsque $1 \in I$. □

Il existe des versions « effectives » de ce résultat qui bornent *a priori* les degrés des polynômes G_i en fonction de ceux des F_i ; c'est important du point de vue du calcul pratique des G_i et de la preuve de leur existence (ou pas) [13].

Exercice 10.5. — Soit K un corps quelconque et soient $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$ des polynômes qui n'ont pas de zéro commun dans une clôture algébrique $\overline{K}$ de K (c'est-à-dire que le système d'équations du cor. 10.4 n'a aucune solution dans $\overline{K}^n$). Montrer qu'il existe des polynômes $G_1, \ldots, G_r \in K[X_1, \ldots, X_n]$ tels que $\sum_{i=1}^r F_i G_i = 1$.

13. Kollár a démontré (Sharp effective Nullstellensatz, *J. Amer. Math. Soc.* **1** (1988), 963–975) que si $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$, avec $n \geq 2$, n'ont pas de zéro commun (dans une clôture algébrique de K) et que $d_1 \geq \cdots \geq d_r \geq 3$, où $d_i := \deg(F_i)$, il existe des polynômes $G_1, \ldots, G_r \in K[X_1, \ldots, X_n]$ comme dans l'énoncé du corollaire avec $\deg(F_i G_i) \leq d_1 \cdots d_r$ pour tout i.

Corollaire 10.6. — *Soit K un corps et soit I un idéal de $K[X_1, \ldots, X_n]$. On a*

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{m} \text{ maximal}} \mathfrak{m}.$$

Rappelons que dans tout anneau, $\sqrt{I}$ est l'intersection des idéaux *premiers* contenant I (lemme 3.2.b)).

Démonstration. — Une inclusion est claire. Soit donc $P \notin \sqrt{I}$. Nous allons construire un idéal maximal de $K[X_1, \ldots, X_n]$ contenant I mais pas P. Considérons l'idéal J de $K[X_1, \ldots, X_n, X_{n+1}]$ engendré par $X_{n+1}P - 1$ et I. Si $J = K[X_1, \ldots, X_{n+1}]$, on peut écrire

$$1 = A(X_1, \ldots, X_{n+1})(X_{n+1}P - 1) + \sum_{j=0}^{m} X_{n+1}^j F_j(X_1, \ldots, X_n), \tag{10}$$

où les F_j sont tous dans I. Considérons le morphisme de K-algèbres

$$K[X_1, \ldots, X_n, X_{n+1}] \to K(X_1, \ldots, X_n)$$

qui envoie X_i sur X_i pour $1 \leq i \leq n$ et X_{n+1} sur $1/P$. L'image de (10) par ce morphisme se réécrit, dans $K[X_1, \ldots, X_n]$,

$$P^m = \sum_{j=0}^{m} P^{m-j} F_j(X_1, \ldots, X_n),$$

ce qui contredit le fait que P n'est pas dans $\sqrt{I}$. On a donc $J \neq K[X_1, \ldots, X_{n+1}]$ et il existe un idéal maximal $\mathfrak{n}$ de $K[X_1, \ldots, X_{n+1}]$ contenant J.

Comme on l'a vu plus haut, le Nullstellensatz entraîne que l'extension de corps $K \hookrightarrow K[X_1, \ldots, X_{n+1}]/\mathfrak{n}$ est finie. Posons

$$\mathfrak{m} := \mathfrak{n} \cap K[X_1, \ldots, X_n].$$

C'est un idéal premier de $K[X_1, \ldots, X_n]$ contenant I, mais pas P (puisque $1 = X_{n+1}P - (X_{n+1}P - 1) \notin \mathfrak{n}$) et on a des inclusions

$$K \subseteq K[X_1, \ldots, X_n]/\mathfrak{m} \subseteq K[X_1, \ldots, X_{n+1}]/\mathfrak{n}.$$

Le K-espace vectoriel $K[X_1, \ldots, X_n]/\mathfrak{m}$ est donc de dimension finie, de sorte que l'anneau intègre $K[X_1, \ldots, X_n]/\mathfrak{m}$ est une extension d'anneaux finie de K. C'est donc un corps (lemme 10.1), ce qui montre que $\mathfrak{m}$ est un idéal maximal de $K[X_1, \ldots, X_n]$ contenant I mais pas P. □

Corollaire 10.7. — *Soit K un corps et soit A une K-algèbre de type fini. Les points fermés sont denses dans toute partie fermée de* $\mathrm{Spec}(A)$.

Un anneau A qui vérifie la conclusion du corollaire est dit « anneau de Jacobson ».

Démonstration. — On peut écrire A comme quotient d'une algèbre de polynômes $B := K[X_1, \ldots, X_n]$, de sorte que $\mathrm{Spec}(A)$ s'identifie à une partie fermée de $\mathrm{Spec}(B)$. Il suffit donc de traiter le cas où A est une algèbre de polynômes.

Toute partie fermée de $\mathrm{Spec}(A)$ est du type $V(I)$, où I est un idéal radical de A. L'adhérence de l'ensemble des points fermés de $V(I)$ s'écrit $V(J) \subseteq V(I)$, où J est un idéal radical de A contenant I.

Tous les idéaux maximaux de A qui sont dans $V(I)$, c'est-à-dire qui contiennent I, sont alors dans $V(J)$, donc contiennent J. Le cor. 10.6 entraîne alors

$$I = \bigcap_{I \subseteq \mathfrak{m} \text{ maximal}} \mathfrak{m} \supseteq \bigcap_{J \subseteq \mathfrak{m} \text{ maximal}} \mathfrak{m} = J,$$

d'où $V(I) \subseteq V(J)$. Cela montre que les points fermés sont denses dans toute partie fermée de $\mathrm{Spec}(A)$. □

Rappelons que les points fermés ne sont en général pas denses dans le spectre d'un anneau, même noethérien (*cf.* ex. 5.6). Cela nous permet d'ailleurs de démontrer un résultat déjà évoqué pp. 61 et 85.

Corollaire 10.8. — *Soit A un anneau non nul. L'anneau $A[[X]]$ n'est pas une A-algèbre de type fini.*

Démonstration. — Quitte à quotienter par un idéal maximal de A (qui existe puisque A est non nul), on peut supposer que A est un corps K. L'unique point fermé de $\mathrm{Spec}(K[[X]])$ n'est alors pas dense, donc $K[[X]]$ n'est pas une K-algèbre de type fini par le cor. 10.7. □

Lorqu'il y a beaucoup de points fermés dans le spectre d'un anneau A, on peut se limiter à considérer le sous-ensemble

$$\mathrm{Specmax}(A) := \{\text{idéaux maximaux de } A\}$$

de $\mathrm{Spec}(A)$, muni de la topologie induite par la topologie de Zariski. Il a l'« avantage » psychologique que tous ses points sont fermés [14].

Soit A une algèbre de type fini sur un corps (on dit souvent que A est une algèbre « géométrique »). Notons $\iota : \mathrm{Specmax}(A) \hookrightarrow \mathrm{Spec}(A)$ l'injection naturelle. Pour tout fermé F de $\mathrm{Spec}(A)$, on a $F = \overline{\iota^{-1}(F)}$ (cor. 10.7) et F est irréductible si et seulement si $\iota^{-1}(F)$ l'est (prop. 5.15).

Proposition 10.9. — *Soit K un corps algébriquement clos. L'application*

$$\varphi : K^n \to \mathrm{Specmax}(K[X_1, \dots, X_n])$$

qui associe à $(x_1, \dots, x_n)$ l'idéal maximal $(X_1 - x_1, \dots, X_n - x_n)$ est une bijection. Pour tout idéal I de $K[X_1, \dots, X_n]$, on a

$$\varphi^{-1}(V_{\max}(I)) = \{x \in K^n \mid \forall P \in I \quad P(x) = 0\}.$$

Démonstration. — Le fait que φ soit une bijection est juste le cor. 10.3. Pour le second point, on a

$$\varphi^{-1}(V_{\max}(I)) = \{x \in K^n \mid \mathfrak{m}_x \supseteq I\} = \{x \in K^n \mid e_x(I) = 0\}$$

et $e_x(I) = 0$ est équivalent au fait que tous les éléments de I s'annulent en x. □

Toujours si K est algébriquement clos, la bijection φ permet de munir aussi K^n d'une topologie, encore dite de Zariski, pour laquelle les fermés sont les sous-ensembles décrits ci-dessus, c'est-à-dire les

$$V_{\max}(I) := \{x \in K^n \mid \forall P \in I \quad P(x) = 0\}.$$

Pour tout anneau A, on a défini en général dans § 5.1 (8) des bijections réciproques

$$\{\text{idéaux radicaux de } A\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{parties fermées de } \mathrm{Spec}(A)\}.$$

Lorsque $A = K[X_1, \dots, X_n]$, comme alors $V(I) = \overline{V_{\max}(I)}$ (cor. 10.7), celles-ci induisent, par la prop. 10.9, des bijections réciproques

$$\{\text{idéaux radicaux de } K[X_1, \dots, X_n]\} \underset{I_{\max}}{\overset{V_{\max}}{\rightleftarrows}} \{\text{parties fermées de } K^n\},$$

où

$$I_{\max}(S) := \{P \in K[X_1, \dots, X_n] \mid \forall x \in S \quad P(x) = 0\}.$$

14. Rappelons cependant que même s'il peut sembler désagréable d'avoir à considérer l'espace topologique $\mathrm{Spec}(A)$ et ses points non fermés, c'est celui qui se comporte le mieux en général : l'avantage primordial des idéaux premiers sur les idéaux maximaux est que l'image inverse d'un idéal premier par un morphisme d'anneaux est encore un idéal premier, alors que ce n'est pas vrai en général pour les idéaux maximaux ; c'est cet avantage essentiel qui permet d'avoir la propriété fonctorielle de l'exerc. 5.7.a).

Plus généralement, si A est une K-algèbre de type fini, on peut l'écrire sous la forme (non unique) $A = K[X_1, \ldots, X_n]/I$, et $\mathrm{Specmax}(A)$ est homéomorphe à $V_{\max}(I) \subseteq K^n$. On a alors des bijections réciproques

$$\{\text{idéaux radicaux de } A\} \underset{I_{\max}}{\overset{V_{\max}}{\rightleftarrows}} \{\text{parties fermées de } V_{\max}(I) \subseteq K^n\},$$

Exemple 10.10. — Soit K un corps algébriquement clos, soit P un élément non nul de$K[X_1, \ldots, X_n]$ et soit $V_{\max}(P) \subseteq K^n$ l'*hypersurface* qu'il définit. Si

$$P = uP_1^{v_1} \cdots P_n^{v_n}$$

est sa décomposition en produits d'irréductibles, on a (lemme 5.1)

$$V_{\max}(P) = V_{\max}((P_1)^{v_1} \cdots (P_n)^{v_n}) = V_{\max}(P_1) \cup \cdots \cup V_{\max}(P_n).$$

Comme chaque P_i est irréductible, chaque idéal (P_i) est premier (prop. 1.3), donc chaque $V_{\max}(P_i)$ est irréductible et ils sont distincts deux à deux (prop. 5.17) : ce sont les composantes irréductibles de $V_{\max}(P)$ (§ 5.2). Nous montrerons dans le cor. 11.14 (*cf.* aussi cor. 12.5) qu'elles sont toutes de dimension $n-1$.

Exemple 10.11. — Soit K un corps algébriquement clos, soit $I = (X^2, XY) \subseteq K[X, Y]$ l'idéal considéré dans l'ex. 4.15, et soit A la K-algèbre $K[X, Y]/I$. On a $\sqrt{I} = (X)$ et

$$\mathrm{Specmax}(A) \simeq V_{\max}(I) = V_{\max}(\sqrt{I}) = \{(x, y) \in K^2 \mid x = 0\}.$$

C'est une droite dans le plan affine. Elle est irréductible (donc aussi $\mathrm{Spec}(A)$).

Exemple 10.12. — Soit K un corps algébriquement clos, soit

$$I = (X^2Y^3 - X^3YZ, Y^2Z - XZ^2) \subseteq K[X, Y, Z]$$

l'idéal considéré p. 71, et soit A la K-algèbre $K[X, Y, Z]/I$. On a

$$\sqrt{I} = (Y^2 - XZ) \cap (X, Z)$$

et

$$\begin{aligned} \mathrm{Specmax}(A) &\simeq V_{\max}(I) = V_{\max}(\sqrt{I}) \\ &= \{(x, y, z) \in K^3 \mid y^2 = xz\} \cup \{(x, y, z) \in K^3 \mid x = z = 0\}. \end{aligned}$$

C'est la réunion d'une surface quadrique et d'une droite dans l'espace affine, qui sont ses composantes irréductibles (pourquoi ?).

Exemple 10.13. — Soit K un corps algébriquement clos et soit A la K-algèbre$K[X, Y]/(XY)$ considérée dans l'ex. 5.20. On a

$$\mathrm{Specmax}(A) \simeq (K \times \{0\}) \cup (\{0\} \times K).$$

C'est la réunion des deux axes de coordonnées dans le plan affine, qui sont ses composantes irréductibles.

Exemple 10.14. — Soit K un corps algébriquement clos, soit

$$I = (XY, YZ, ZX) \subseteq K[X, Y, Z]$$

l'idéal considéré dans l'exerc. 4.28, et soit A la K-algèbre $K[X, Y, Z]/I$. On a

$$\mathrm{Specmax}(A) \simeq V_{\max}(I) = (K \times \{0\} \times \{0\}) \cup (\{0\} \times K \times \{0\}) \cup (\{0\} \times \{0\} \times K).$$

C'est la réunion des trois axes de coordonnées dans l'espace affine, qui sont ses composantes irréductibles.

Exemple 10.15. — Soit K un corps algébriquement clos et soit A la sous-K-algèbre$K[X^2, X^3]$ de $K[X]$ considérée dans l'ex. 8.22. Elle est de type fini, engendrée par X^2 et X^3, avec la relation $(X^2)^3 = (X^3)^2$, ce qui permet de l'écrire

$$A \simeq K[Y, Z]/(Y^3 - Z^2).$$

On a donc

$$\mathrm{Specmax}(A) \simeq \{(y, z) \in K^2 \mid y^3 = z^2\}.$$

C'est une courbe irréductible (pourquoi ?) plane. Le fait que l'anneau A ne soit pas intégralement clos est relié au fait que cette courbe présente une singularité en $(0, 0)$ (*cf.* exerc. 16.2).

Exercice 10.16. — Soit A un anneau qui est une extension de type fini de $\mathbf{Z}$.

a) Montrer que pour tout idéal maximal $\mathfrak{m}$ de A, le corps $A/\mathfrak{m}$ est fini (*Indication :* on pourra appliquer le th. 10.2 à la $(\mathbf{Z}/\mathbf{Z} \cap \mathfrak{m})$-algèbre $A/\mathfrak{m}$, puis montrer $\mathbf{Z} \cap \mathfrak{m} \neq 0$).

b) Montrer que A est un anneau de Jacobson, c'est-à-dire que les points fermés sont denses dans toute partie fermée de $\mathrm{Spec}(A)$ (*cf.* cor. 10.7) (*Indication :* soit $f \in A$ non nilpotent et soit $\mathfrak{n} \subseteq A_f$ un idéal maximal ; on pourra montrer que $A_f/\mathfrak{n}$, puis $A/A \cap \mathfrak{n}$, sont des corps finis).

Exercice 10.17. — Cet exercice présente une preuve élémentaire du Nullstellensatz (sous la forme du cor. 10.4) due à E. Arrondo. Elle ne nécessite que l'utilisation du résultant $R(P, Q)$ de deux polynômes P et Q à coefficients dans un anneau A. Si on écrit $P(X) = \sum_{i=0}^{m} a_i X^i$ et $Q(X) = \sum_{j=0}^{n} b_j X^j$, alors

$$R(P,Q) := \begin{vmatrix} a_0 & a_1 & \cdots & a_m & 0 & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_{m-1} & a_m & 0 & \cdots & 0 \\ & & \ddots & & & & & \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{m-1} & a_m \\ b_0 & b_1 & \cdots & b_n & 0 & 0 & \cdots & 0 \\ 0 & b_0 & \cdots & b_{n-1} & b_n & 0 & \cdots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_{n-1} & b_n \end{vmatrix} \in A.$$

Soit K un corps algébriquement clos et soit I un idéal propre de $K[X_1, \ldots, X_n]$. Nous allons montrer par récurrence sur n que les éléments de I ont un zéro commun dans K^n.

a) Montrer que c'est le cas pour $n = 1$.

b) Montrer que quitte à faire un changement linéaire des indéterminées $X_1, \ldots, X_n$, on peut supposer (ce que l'on fera) que I contient un polynôme Q unitaire en l'indéterminée X_n.

c) On suppose $n > 1$. Montrer que $I' := I \cap K[X_1, \ldots, X_{n-1}]$ est un idéal propre de $K[X_1, \ldots, X_{n-1}]$. Par hypothèse de récurrence, ses éléments ont donc un zéro commun $(a_1, \ldots, a_{n-1}) \in K^{n-1}$.

d) Montrer que $J := \{P(a_1, \ldots, a_{n-1}, X_n) \mid P \in I\}$ est un idéal propre de $K[X_n]$ (*Indication :* on pourra raisonner par l'absurde et supposer qu'il existe $P \in I$ tel que $P(a_1, \ldots, a_{n-1}, X_n) = 1$, considérer P et Q comme des polynômes en l'indéterminée X_n à coefficients dans $K[X_1, \ldots, X_{n-1}]$, montrer que leur résultant $R(P, Q) \in K[X_1, \ldots, X_{n-1}]$ est dans I' mais que $R(P, Q)(a_1, \ldots, a_{n-1}) = 1$).

e) Conclure.

11. « Going-up » et théorème de Cohen-Seidenberg

Soit $\iota : A \hookrightarrow B$ une extension d'anneaux entière. On va étudier l'application induite

$$\begin{array}{ccc} \mathrm{Spec}(B) & & \mathfrak{q} \\ {\scriptstyle \iota^\sharp}\downarrow & & \downarrow \\ \mathrm{Spec}(A) & & \mathfrak{q} \cap A \end{array}$$

Dans ce contexte, on dit souvent que l'idéal $\mathfrak{q}$ est « au-dessus » de l'idéal $\mathfrak{p} := \mathfrak{q} \cap A$ (il est traditionnel de représenter une application comme $\iota^\sharp$ « verticalement », comme ci-dessus, avec sa source au-dessus de son

but). La *fibre* d'un élément $\mathfrak{p}$ de $\mathrm{Spec}(A)$ est $(\iota^\sharp)^{-1}(\mathfrak{p})$, c'est-à-dire l'ensemble (fermé, peut-être vide) des idéaux de B au-dessus de $\mathfrak{p}$.

Lemme 11.1. — *Soit $\mathfrak{q}$ un idéal premier de B. Si $\iota^\sharp(\mathfrak{q}) = \mathfrak{p}$, l'idéal $\mathfrak{p}$ est maximal si et seulement si $\mathfrak{q}$ est maximal.*

Démonstration. — Le noyau de la composée $A \hookrightarrow B \to B/\mathfrak{q}$ est $\mathfrak{p}$. On a donc une extension d'anneaux intègres $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$ qui est entière (le vérifier !) et le lemme résulte du lemme 10.1. □

Lemme 11.2. — *Soient $\mathfrak{q}_1$ et $\mathfrak{q}_2$ des idéaux premiers de B. Si $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ et $\iota^\sharp(\mathfrak{q}_1) = \iota^\sharp(\mathfrak{q}_2)$, on a $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Démonstration. — Posons $\mathfrak{p} := \iota^\sharp(\mathfrak{q}_1) = \iota^\sharp(\mathfrak{q}_2)$, idéal premier de A. Considérons la partie multiplicative $S = A - \mathfrak{p}$ de A (et de B). On a (lemme 6.8)

$$\mathfrak{p}S^{-1}A = \mathfrak{q}_1 S^{-1}B \cap S^{-1}A = \mathfrak{q}_2 S^{-1}B \cap S^{-1}A.$$

Comme l'idéal $\mathfrak{p}S^{-1}A$ est maximal et que l'extension $S^{-1}A \hookrightarrow S^{-1}B$ est entière (lemme 8.8), l'idéal $\mathfrak{q}_1 S^{-1}B$ est maximal (lemme 11.1). Il en est de même pour l'idéal $\mathfrak{q}_2 S^{-1}B$, et comme il contient le précédent, ils sont égaux. On en déduit

$$\mathfrak{q}_1 = (\mathfrak{q}_1 S^{-1}B) \cap B = (\mathfrak{q}_2 S^{-1}B) \cap B = \mathfrak{q}_2,$$

d'où le lemme. □

Lemme 11.3. — *L'application $\iota^\sharp$ est surjective.*

Démonstration. — On peut supposer l'anneau A non nul (puisque sinon, son spectre est vide !). Il s'agit de montrer que pour tout idéal premier $\mathfrak{p}$ de A, il existe un idéal premier $\mathfrak{q}$ de B tel que $\mathfrak{q} \cap A = \mathfrak{p}$.

Considérons la partie multiplicative $S = A - \mathfrak{p}$. L'extension $S^{-1}A \hookrightarrow S^{-1}B$ est entière (lemme 8.8). Si $\mathfrak{m}$ est un idéal maximal de l'anneau (non nul !) $S^{-1}B$, l'idéal $\mathfrak{m} \cap S^{-1}A$ est un idéal maximal de $S^{-1}A$ (lemme 11.1). Cet anneau étant local, c'est $\mathfrak{p}S^{-1}A$. Posons $\mathfrak{q} := \mathfrak{m} \cap B$ (c'est l'abus de notation usuel : on écrit $\cap B$ pour désigner l'image inverse par $B \to S^{-1}B$). On a alors (avec les mêmes abus de notation)

$$\mathfrak{q} \cap A = \mathfrak{m} \cap B \cap A = \mathfrak{m} \cap S^{-1}A \cap A = \mathfrak{p}S^{-1}A \cap A = \mathfrak{p},$$

ce qui termine la preuve. □

Exercice 11.4. — Soit $\iota : A \hookrightarrow B$ une extension d'anneaux.

a) Montrer que l'application $\iota^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ est *dominante,* c'est-à-dire que son image est dense dans $\mathrm{Spec}(A)$.

b) Si ι est une extension entière, montrer que l'application $\iota^\sharp$ est *fermée,* c'est-à-dire que pour toute partie fermée F de $\mathrm{Spec}(B)$, la partie $\iota^\sharp(F)$ de $\mathrm{Spec}(A)$ est fermée.

Le théorème suivant est appelé dans la littérature « going-up ». Ce nom provient de sa représentation suivante : on se demande si on peut trouver $\mathfrak{q}_2$ qui complète le diagramme ci-dessous

$$\begin{array}{ccccc} \mathrm{Spec}(B) & & \mathfrak{q}_1 & \subseteq & \mathfrak{q}_2 ? \\ {\scriptstyle \iota^\sharp}\downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}(A) & & \mathfrak{p}_1 & \subseteq & \mathfrak{p}_2 \end{array}$$

(voir th. 13.4 pour le « going-down », un énoncé analogue mais de démonstration plus délicate !).

***Théorème 11.5* (« Going-up »)**. — *Soit $A \hookrightarrow B$ une extension d'anneaux entière. Soient $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq A$ des idéaux premiers et soit $\mathfrak{q}_1$ un idéal premier de B au-dessus de $\mathfrak{p}_1$. Il existe un idéal premier $\mathfrak{q}_2$ de B, contenant $\mathfrak{q}_1$, au-dessus de $\mathfrak{p}_2$.*

Démonstration. — L'extension d'anneaux $A/\mathfrak{p}_1 \hookrightarrow B/\mathfrak{q}_1$ est entière. Par le lemme 11.3, il existe un idéal premier de $B/\mathfrak{q}_1$ au-dessus de l'idéal premier $\mathfrak{p}_2/\mathfrak{p}_1$ de $A/\mathfrak{p}_1$. Cet idéal correspond à un idéal premier de B contenant $\mathfrak{q}_1$ au-dessus de $\mathfrak{p}_2$. □

Exercice 11.6. — Soit $\iota : A \hookrightarrow B$ une extension d'anneaux. Si l'application $\iota^\sharp$ est fermée (*cf.* exerc. 11.4), montrer que ι satisfait la propriété de « going-up ».

Remarque 11.7. — En termes « géométriques », la propriété de « going-up » pour une extension d'anneaux $\iota : A \hookrightarrow B$ signifie la chose suivante : pour tous fermés irréductibles $F_2 \subseteq F_1$ de $\mathrm{Spec}(A)$, et tout fermé irréductible $G_1 \subseteq \mathrm{Spec}(B)$ tel que $\iota^\sharp(G_1) = F_1$, il existe un fermé irréductible $G_2 \subseteq G_1$ tel que $\iota^\sharp(G_2) = F_2$.

Théorème 11.8 **(Cohen-Seidenberg, 1946)**. — *Soit $A \hookrightarrow B$ une extension d'anneaux entière. On a alors* $\dim(A) = \dim(B)$.

Démonstration. — Comme A est nul si et seulement si B est nul, et que dans ce cas, ces anneaux sont de même dimension $-\infty$, on va supposer A et B non nuls, donc de dimension ≥ 0.

Soit $\mathfrak{q}_n \supsetneq \cdots \supsetneq \mathfrak{q}_0$ une chaîne d'idéaux premiers de B. Alors

$$(\mathfrak{q}_n \cap A) \supsetneq \cdots \supsetneq (\mathfrak{q}_0 \cap A)$$

est une chaîne d'idéaux premiers de A (lemme 11.2). On en déduit $\dim(A) \geq \dim(B)$.

Inversement, si on se donne une chaîne d'idéaux premiers $\mathfrak{p}_m \supsetneq \cdots \supsetneq \mathfrak{p}_0$ de A, et $\mathfrak{q}_0$ un idéal premier de B tel que $\mathfrak{q}_0 \cap A = \mathfrak{p}_0$ (lemme 11.3), on va montrer par récurrence sur m qu'on peut trouver une chaîne d'idéaux premiers $\mathfrak{q}_m \supsetneq \cdots \supsetneq \mathfrak{q}_0$ de B telle que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ pour tout i. Le cas $m = 0$ est trivial. Si $\mathfrak{p}_{m-1} \supsetneq \cdots \supsetneq \mathfrak{p}_0$ est relevée en $\mathfrak{q}_{m-1} \supsetneq \cdots \supsetneq \mathfrak{q}_0$, le th. 11.5 montre qu'il existe un idéal premier $\mathfrak{q}_m \supsetneq \mathfrak{q}_{m-1}$ au-dessus de $\mathfrak{p}_m$. On a donc $\dim(A) \leq \dim(B)$. □

Exemple 11.9. — Soit K un corps. L'extension

$$\iota : K[X] \hookrightarrow K[X,Y]/(X^2 + Y^2 - 1)$$

est finie (donc entière) puisque les classes de 1 et de Y engendrent le $K[X]$-module$K[X,Y]/(X^2+Y^2-1)$. On en déduit que la dimension de Krull de l'anneau $K[X,Y]/(X^2 + Y^2 - 1)$ est 1 (ex. 5.26 et th. 11.8).

Si K est algébriquement clos, l'application $\iota^\sharp_{\max}$ s'identifie à la projection

$$\begin{aligned} \{(x,y) \in K^2 \mid x^2 + y^2 = 1\} &\longrightarrow K \\ (x,y) &\longmapsto x. \end{aligned}$$

Elle est bien surjective. Tout point a deux préimages, sauf -1 et 1, qui n'en ont qu'une.

Théorème 11.10. — *Soit K un corps. Pour tout $n \in \mathbf{N}$, la dimension de Krull de l'anneau $K[X_1, \ldots, X_n]$ est n.*

Démonstration. — On a déjà remarqué (ex. 5.28) que cette dimension est $\geq n$. Nous allons procéder par récurrence sur n pour montrer l'égalité (qui a bien lieu pour $n = 0$). Supposons donc $n \geq 1$ et soit $\mathfrak{p}_m \supsetneq \cdots \supsetneq \mathfrak{p}_1 \supsetneq (0)$, avec $m \geq 1$, une chaîne d'idéaux premiers de $A := K[X_1, \ldots, X_n]$ et soit P un élément non nul de $\mathfrak{p}_1$. Alors

$$\mathfrak{p}_m/(P) \supsetneq \cdots \supsetneq \mathfrak{p}_1/(P)$$

est une chaîne d'idéaux premiers de l'anneau $B := A/(P)$, donc $\dim(B) \geq m - 1$. Soit x_i l'image de X_i dans B. Les éléments $x_1, \ldots, x_n$ de B sont algébriquement liés (par P), donc il existe (lemme 9.2) des éléments $y_1, \ldots, y_{n-1}$ de B tels que x_n est entier sur $B' := K[y_1, \ldots, y_{n-1}]$ et $B = B'[x_n]$. Le th. 11.8 donne $\dim(B') = \dim(B)$.

D'autre part, B' est un quotient de l'algèbre de polynômes $K[Y_1, \ldots, Y_{n-1}]$, donc, par l'hypothèse de récurrence,

$$\dim(B') \leq \dim(K[Y_1, \ldots, Y_{n-1}]) = n - 1.$$

On en déduit $m - 1 \leq \dim(B) = \dim(B') \leq n - 1$, ce qui donne l'inégalité cherchée. □

Remarque 11.11. — On peut montrer que l'anneau de séries formelles $K[[X_1, \ldots, X_n]]$ est aussi de dimension n ([**ZS2**], th. 33 ; *cf.* exerc. 5.29).

Corollaire 11.12. — *Toute algèbre de type fini sur un corps est de dimension de Krull finie.*

Démonstration. — Soit A une telle algèbre sur un corps K. Le lemme de normalisation (th. 9.1) dit que c'est une extension finie d'un anneau de polynômes $K[X_1, \ldots, X_n]$. Par le th. 11.8 et le th. 11.10, on en déduit $\dim(A) = n$. □

Exercice 11.13. — Soit K un corps et soit A une K-algèbre de type fini. Pour tout $n \in \mathbf{N}$, montrer l'égalité $\dim(A[X_1, \ldots, X_n]) = \dim(A) + n$ (*Indication :* on pourra utiliser le th. 9.1 et le th. 11.10).

Corollaire 11.14. — *Soit K un corps et soit P un élément non constant de $K[X_1, \ldots, X_n]$. La dimension de $K[X_1, \ldots, X_n]/(P)$ est $n - 1$.*

Nous donnerons dans le cor. 12.5 une autre démonstration de ce résultat.

Démonstration. — La démonstration du lemme 9.2 nous dit que la K-algèbre$A := K[X_1, \ldots, X_n]/(P)$ est finie sur la sous-K-algèbre engendrée par les classes y_i de $Y_i := X_i - X_n^{e^i}$, pour $1 \leq i \leq n - 1$ et $e \gg 0$.

Montrons que ces classes sont algébriquement indépendantes dans A. Si ce n'est pas le cas, il existe un polynôme non nul $R \in K[Y_1, \ldots, Y_{n-1}]$ tel que

$$P(X_1, \ldots, X_n) \mid R(X_1 - X_n^e, \ldots, X_{n-1} - X_n^{e^{n-1}})$$

dans $K[X_1, \ldots, X_n]$, ou encore

$$Q(Y_1, \ldots, Y_{n-1}, X_n) := P(Y_1 + X_n^e, \ldots, Y_{n-1} + X_n^{e^{n-1}}, X_n) \mid R(Y_1, \ldots, Y_{n-1})$$

dans $K[Y_1, \ldots, Y_{n-1}, X_n]$. Mais on a vu au cours de la preuve du lemme 9.2 que comme P est non constant, le degré de Q, vu comme polynôme en X_n, est, pour $e \gg 0$, strictement positif. Comme R est de degré nul en X_n, on a une contradiction.

Le th. 11.8 donne $\dim(A) = \dim(K[y_1, \ldots, y_{n-1}])$. Comme les y_i sont algébriquement indépendants, le th. 11.10 nous donne $\dim(K[y_1, \ldots, y_{n-1}]) = n - 1$, ce qui termine la preuve du corollaire. □

Soit $\iota : A \hookrightarrow B$ une extension de type fini d'anneaux intègres et soit $\jmath : K_A \hookrightarrow K_B$ l'extension des corps de fractions associée. La condition que ι est une extension d'anneaux finie est très forte. Elle entraîne que $\jmath$ est une extension de corps finie (exerc. 8.10) ; la réciproque est fausse, comme le montre l'exemple ci-dessous, mais on peut quand même dire quelque chose. Supposons donc l'extension $\jmath$ finie, et soient $b_1, \ldots, b_n$ des générateurs de la A-algèbre B. Chaque b_i est algébrique sur K_A ; soit f un dénominateur commun à tous les coefficients des polynôme minimaux correspondants. Chaque b_i est alors algébrique sur le localisé A_f, donc l'extension $A_f \hookrightarrow B_f$ est finie (prop. 8.5.c)). En particulier, l'application

$$\iota^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$$

se restreint sur l'ouvert dense $\mathrm{Spec}(B_f) \subseteq \mathrm{Spec}(B)$ en une application

$$\mathrm{Spec}(B_f) \to \mathrm{Spec}(A_f)$$

à laquelle on peut appliquer les résultats vus plus haut : elle est surjective (lemme 11.3), fermée (exerc. 11.4) et à fibres finies (rem. 13.3).

Exemple 11.15. — Soit K un corps algébriquement clos. Posons $A = K[X,Y]$ et $B = K[X,Y,Z]/(XZ-Y)$. L'inclusion $\iota : A \hookrightarrow B$ n'est pas entière car l'application

$$\begin{array}{rcl} \iota^\sharp_{\max} : \mathrm{Specmax}(B) = \{(x,y,z) \in K^3 \mid xz = y\} & \longrightarrow & K^2 = \mathrm{Specmax}(A) \\ (x,y,z) & \longmapsto & (x,y) \end{array}$$

n'est pas surjective (lemme 11.3) : son image est $\{(x,y) \in K^2 \mid x \neq 0 \text{ ou } x = y = 0\}$. L'inclusion $\jmath : K_A \hookrightarrow K_B$ est un isomorphisme puisque $Z = Y/X$ dans K_A. L'inclusion $A_X \hookrightarrow B_X$ est aussi un isomorphisme. Cela correspond au fait que l'application

$$\{(x,y,z) \in K^3 \mid xz = y,\ x \neq 0\} \longrightarrow \{(x,y) \in K^2 \mid x \neq 0\}$$

induite par $\iota^\sharp_{\max}$ est un isomorphisme.

Exercice 11.16. — Soit K un corps. Soit A le sous-anneau de $K[X,Y]$ engendré par les X^nY, pour $n \in \mathbf{N}^*$ (il n'est pas noethérien par l'exerc. 2.9). Montrer que l'extension d'anneaux intègres $A \hookrightarrow K[X,Y]$ n'est pas de type fini, mais qu'elle induit un isomorphisme entre les corps de fractions.

12. Bases et degré de transcendance

On s'intéresse ici aux extensions de corps qui ne sont pas algébriques, en définissant leur *degré de transcendance.* Nous faisons ensuite le lien entre ce degré et la dimension des algèbres intègres de type fini sur un corps.

Définition 12.1. — *Soit $K \subseteq L$ une extension de corps. Une partie B de L est une* base de transcendance *de L sur K si*

- *les éléments de B sont algébriquement indépendants sur K* [15] *;*
- *le corps L est une extension algébrique du corps $K(B)$.*

Par exemple, $\{X_1, \ldots, X_n\}$ est une base de transcendance de $K(X_1, \ldots, X_n)$ sur K, tandis que $\varnothing$ est une base de transcendance de n'importe quelle extension algébrique.

Si $K \hookrightarrow L$ une extension de corps de type fini et que $S \subseteq L$ est une partie finie telle que $L = K(S)$, un sous-ensemble maximal algébriquement indépendant de S est une base de transcendance finie de L sur K. Il existe donc toujours (pour une extension de type fini), une base de transcendance (finie). Nous allons maintenant montrer que ces bases ont toutes le même cardinal [16].

Proposition 12.2. — *Soit $K \hookrightarrow L$ une extension de corps de type fini.*

a) *Soit $A \subseteq L$ une partie finie formée d'éléments algébriquement indépendants et soit $S \subseteq L$ une partie telle que L est algébrique sur $K(S)$. Alors* $\mathrm{Card}(S) \geq \mathrm{Card}(A)$.

b) *Toutes les bases de transcendance de L sur K ont le même cardinal (fini).*

Dans la situation de la proposition, le cardinal commun (fini) des bases de transcendance de L sur K s'appelle le *degré de transcendance de L sur K* ; on le note $\deg.\mathrm{tr}_K\, L$.

Démonstration. — Notons $A = \{a_1, \ldots, a_n\}$. On peut supposer $n > 0$. Si tous les éléments de S sont algébriques sur $K(a_2, \ldots, a_n)$, l'extension $K(a_2, \ldots, a_n) \subseteq K(\{a_2, \ldots, a_n\} \cup S)$ est algébrique (cor. 2.13), donc aussi l'extension $K(a_2, \ldots, a_n) \subseteq L$ par le th. 2.16 (puisque L est algébrique sur $K(S)$), ce qui est absurde (puisque a_1 n'est pas algébrique sur $K(a_2, \ldots, a_n)$).

15. Cela siginife que tout sous-ensemble fini de B a cette propriété.

16. Nous nous limitons ici aux extensions de type fini, mais on peut développer cette théorie (qui est d'ailleurs analogue à celle des bases dans les espaces vectoriels, et qui est traitée parallèlement dans [**ZS1**]) pour toute extension ([**ZS1**], Ch. 2, §12, th. 24).

Il existe donc un élément s_1 de S qui n'est pas algébrique sur $K(a_2, \ldots, a_n)$, de sorte que $s_1, a_2, \ldots, a_n$ sont algébriquement indépendants. En continuant ainsi, on peut remplacer un par un les éléments $a_1, \ldots, a_n$ de A par des éléments $s_1, \ldots, s_n$ de S (qui restent algébriquement indépendants, donc distincts), ce qui montre a).

Soient B et B' des bases de transcendance de L sur K, avec B finie. Tout sous-ensemble fini A de B' est formé d'éléments algébriquement indépendants, donc est de cardinal $\leq \mathrm{Card}(B)$ par a). On en déduit que B' est (fini) de cardinal $\leq \mathrm{Card}(B)$. Par symétrie, on a égalité. □

Exercice 12.3. — Soient $K \hookrightarrow L$ et $L \hookrightarrow M$ des extensions de corps. On suppose que l'extension $K \hookrightarrow M$ est de type fini. Montrer les extensions $K \hookrightarrow L$ et $L \hookrightarrow M$ sont de type fini et que

$$\deg.\mathrm{tr}_K M = \deg.\mathrm{tr}_K L + \deg.\mathrm{tr}_L M.$$

Théorème 12.4. — *Soit K un corps et soit A une K-algèbre de type fini* intègre *de corps des fractions K_A. On a*

$$\dim(A) = \deg.\mathrm{tr}_K K_A.$$

Démonstration. — D'après le lemme de Noether (th. 9.1), il existe des éléments algébriquement indépendants $a_1, \ldots, a_n$ de A tels que A soit une extension finie de $K[a_1, \ldots, a_n]$. Alors $\{a_1, \ldots, a_n\}$ est une base de transcendance de K_A sur K et

$$\deg.\mathrm{tr}_K K_A = n = \dim(K[a_1, \ldots, a_n]) = \dim(A),$$

ce qui prouve la proposition. □

On peut donner une autre preuve du corollaire 11.14.

Corollaire 12.5. — *Soit K un corps et soit P un élément non constant de $K[X_1, \ldots, X_n]$. La dimension de $K[X_1, \ldots, X_n]/(P)$ est $n-1$.*

Démonstration. — Grâce à l'ex. 10.10, on peut supposer P irréductible puis, quitte à réordonner les variables, $P \notin K[X_1, \ldots, X_{n-1}]$. Le morphisme canonique entre anneaux intègres

$$K[X_1, \ldots, X_{n-1}] \to A := K[X_1, \ldots, X_n]/(P)$$

est alors injectif, d'où une extension de corps

$$K(X_1, \ldots, X_{n-1}) \to K_A$$

qui est finie (puisque K_A est engendré sur $K(X_1, \ldots, X_{n-1})$ par l'élément algébrique $\bar{X}_n$). On en déduit

$$\dim(A) = \deg.\mathrm{tr}_K K_A = \deg.\mathrm{tr}_K K(X_1, \ldots, X_{n-1}) = n-1,$$

ce qui prouve le corollaire. □

Exercice 12.6. — Soit K un corps algébriquement clos. On considère des polynômes *homogènes* $P_1, \ldots, P_m \in K[X_1, \ldots, X_n]$ de degré > 0. Le but de l'exercice est de montrer que si $n > m$, il existe dans K^n un zéro *différent de* $(0, \ldots, 0)$ commun à $P_1, \ldots, P_m$. On suppose donc que le seul zéro commun à $P_1, \ldots, P_m$ est $(0, \ldots, 0)$ et on va montrer $n \leq m$.

a) Montrer qu'il existe $r \in \mathbf{N}$ tel que tout monôme de degré (total) $\geq r$ en $X_1, \ldots, X_n$ appartienne à l'idéal engendré par $P_1, \ldots, P_m$ dans $K[X_1, \ldots, X_n]$.

b) En déduire que tout monôme de degré total $\geq r$ en $X_1, \ldots, X_n$ peut s'écrire sous la forme $Q(X_1, \ldots, X_n)$, où Q est un polynôme de degré total $< r$ en $X_1, \ldots, X_n$ à coefficients dans l'anneau $A := K[P_1, \ldots, P_m]$, sous-anneau de $K[X_1, \ldots, X_n]$.

c) En notant $K_A = K(P_1, \ldots, P_m) \subseteq K(X_1, \ldots, X_n)$ le corps des fractions de l'anneau intègre A, en déduire que le K_A-espace vectoriel $K_A[X_1, \ldots, X_n]$ est de dimension finie. Conclure que $K(X_1, \ldots, X_n)$ est un K_A-espace vectoriel de dimension finie.

d) En raisonnant sur le degré de transcendance, conclure $n \leq m$.

13. « Going-down »

Soit $\iota : A \hookrightarrow B$ une extension d'anneaux. Nous avons vu dans le § 11 que des propriétés *algébriques* de ι se traduisent par des propriétés *topologiques* de l'application continue $\iota^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$. Par exemple, si ι est entière, $\iota^\sharp$ est surjective (lemme 11.3) et fermée (exerc. 11.4). Nous continuons ici à explorer ces relations.

Théorème 13.1. — *Soit A un anneau intégralement clos, soit K son corps des fractions, soit $K \hookrightarrow L$ une extension finie et normale et soit $B \subseteq L$ la clôture intégrale de A dans L.*

Soit $\mathfrak{p}$ un idéal premier de A. Tous les idéaux premiers de B au-dessus de $\mathfrak{p}$ sont conjugués sous l'action du groupe des automorphismes de L sur K.

Démonstration. — Commençons par remarquer que l'image d'un élément de B par n'importe quel élément σ de $G := \mathrm{Gal}(L/K)$ est encore entière sur A (elle est racine du même polynôme unitaire à coefficients dans A), donc est dans B. En d'autres termes, on a $\sigma(B) = B$ et l'image par σ d'un idéal premier de B est encore un idéal premier de B. Le groupe G agit alors bien sur l'ensemble des idéaux premiers $\mathfrak{q}$ de B au-dessus de $\mathfrak{p}$, puisque ceux-ci sont caractérisés par la propriété $\mathfrak{q} \cap A = \mathfrak{p}$.

Soient $\mathfrak{q}_1$ et $\mathfrak{q}_2$ des idéaux premiers de B au-dessus de $\mathfrak{p}$. On raisonne par l'absurde, en supposant

$$\forall \sigma \in G \qquad \mathfrak{q}_2 \neq \sigma(\mathfrak{q}_1). \tag{11}$$

On a alors

$$\forall \sigma \in G \qquad \mathfrak{q}_2 \not\subseteq \sigma(\mathfrak{q}_1).$$

En effet, $\sigma(\mathfrak{q}_1)$ et $\mathfrak{q}_2$ sont des idéaux premiers distincts de B au-dessus de $\mathfrak{p}$. Par le lemme 11.2, il ne peut y avoir d'inclusion entre les deux.

Par l'exerc. 4.5, $\mathfrak{q}_2$ n'est pas contenu dans la réunion $\bigcup_{\sigma\in G} \sigma(\mathfrak{q}_1)$. Il existe donc $x \in \mathfrak{q}_2$ qui n'est dans aucun $\sigma(\mathfrak{q}_1)$. Posons $y_0 = \prod_{\sigma\in G} \sigma(x)$. On a $y_0 \in L^G$, de sorte que soit la caractéristique de K est nulle et $y := y_0 \in K$ (l'extension $K \hookrightarrow L$ est alors galoisienne et on peut appliquer le lemme I.6.21), soit la caractéristique de K est $p > 0$ et il existe $n \geq 0$ tel que $y := y_0^{p^n} \in K$ (exerc. I.6.24).

Chaque $\sigma(x)$, donc aussi y, est dans B, donc entier sur A. Comme $y \in K$ et que A est intégralement clos, on a $y \in A$. Parmi les éléments de G se trouve l'identité. Tout comme x, l'élément y de B est donc dans $\mathfrak{q}_2$, de sorte que $y \in \mathfrak{q}_2 \cap A = \mathfrak{p} \subseteq \mathfrak{q}_1$. Comme $\mathfrak{q}_1$ est un idéal premier, cela contredit le fait qu'aucun des $\sigma(x)$ n'est dans $\mathfrak{q}_1$ (car $\sigma(x) \in \mathfrak{q}_1$ est la même chose que $x \in \sigma^{-1}(\mathfrak{q}_1)$).

L'hypothèse (11) faite plus haut est donc absurde, et le théorème est démontré. □

Corollaire 13.2. — *Soit $A \hookrightarrow B$ une extension finie d'anneaux intègres, avec A intégralement clos. Les fibres de l'application canonique $\iota^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ sont finies.*

Démonstration. — Soit K_A le corps de fractions de A et soit K_B celui de B. L'extension $K_A \hookrightarrow K_B$ induite par ι est alors finie (exerc. 8.10). Soit $K_A \hookrightarrow L$ la clôture normale de $K_A \hookrightarrow K_B$ dans une clôture algébrique de K_B (prop. I.4.6). C'est une extension normale finie de K_A contenant K_B. On note enfin $C \subseteq L$ la clôture intégrale de A dans L ; c'est une extension entière [17] de A contenant B. On a des applications

$$\mathrm{Spec}(C) \xrightarrow{\jmath^\sharp} \mathrm{Spec}(B) \xrightarrow{\iota^\sharp} \mathrm{Spec}(A).$$

Le th. 13.1 entraîne que la composée $\iota^\sharp \circ \jmath^\sharp$ est à fibres finies (puisque le groupe $\mathrm{Gal}(L/K)$ est fini), tandis que l'application $\jmath^\sharp$ est surjective (lemme 11.3). Cela entraîne que $\iota^\sharp$ est à fibres finies. □

17. Pas nécessairement finie !

Remarque 13.3. — On peut montrer que les fibres de $\iota^\sharp$ sont finies pour toute extension finie d'anneaux ι (c'est-à-dire que les hypothèses « A intégralement clos et B intègre » dans le corollaire sont inutiles). On trouvera une démonstration dans [**B2**], Chap. V, § 2, n°1, prop. 3 ; sans être très difficile, elle fait appel à quelques notions que nous n'avons pas vues dans ce cours.

Le théorème suivant est appelé dans la littérature « going-down » : on se demande si on peut trouver $\mathfrak{q}_1$ qui complète le diagramme ci-dessous

$$\begin{array}{ccccc} \mathrm{Spec}(B) & & \mathfrak{q}_1 ? & \subseteq & \mathfrak{q}_2 \\ {\scriptstyle \iota^\sharp}\downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}(A) & & \mathfrak{p}_1 & \subseteq & \mathfrak{p}_2 \end{array}$$

***Théorème 13.4* (« Going-down »)**. — *Soit $A \hookrightarrow B$ une extension finie d'anneaux intègres, avec A intégralement clos. Soient $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ des idéaux premiers de A et soit $\mathfrak{q}_2$ un idéal premier de B au-dessus de $\mathfrak{p}_2$. Il existe un idéal premier $\mathfrak{q}_1$ de B tel que $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ au-dessus de $\mathfrak{p}_1$.*

Démonstration. — On garde les mêmes notations que dans la preuve du cor. 13.2. Grâce au lemme 11.3, il existe des idéaux premiers $\mathfrak{r}_2 \subseteq C$ au-dessus de $\mathfrak{q}_2$ et $\mathfrak{r}'_1 \subseteq C$ au-dessus de $\mathfrak{p}_1$. Par le going-up (th. 11.5), on peut trouver $\mathfrak{r}'_2 \subseteq C$ contenant $\mathfrak{r}'_1$ au-dessus de $\mathfrak{p}_2$. Mais alors $\mathfrak{r}_2$ et $\mathfrak{r}'_2$ sont au-dessus de $\mathfrak{p}_2$, donc il existe (th. 13.1) $\sigma \in \mathrm{Gal}(L/K_A)$ tel que $\sigma(\mathfrak{r}'_2) = \mathfrak{r}_2$. Posant $\mathfrak{r}_1 := \sigma(\mathfrak{r}'_1)$, on a $\mathfrak{r}_1 \subseteq \mathfrak{r}_2$ et $\mathfrak{r}_1 \cap A = \mathfrak{r}'_1 \cap A = \mathfrak{p}_1$. Posant $\mathfrak{q}_1 := \mathfrak{r}_1 \cap B$, on a $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$ et $\mathfrak{q}_1 \subseteq \mathfrak{r}_2 \cap B = \mathfrak{q}_2$. Ceci termine la preuve du théorème. □

Remarque 13.5. — En termes « géométriques », la propriété de « going-down » pour une extension d'anneaux $\iota : A \hookrightarrow B$ signifie la chose suivante : pour tous fermés irréductibles $F_2 \subseteq F_1$ de $\mathrm{Spec}(A)$, et tout fermé irréductible $G_2 \subseteq \mathrm{Spec}(B)$ tel que $\iota^\sharp(G_2) = F_2$, il existe un fermé irréductible $G_1 \supseteq G_2$ tel que $\iota^\sharp(G_1) = F_1$.

Exemple 13.6. — La propriété de « going-down » n'est pas vraie pour toutes les extensions entières. Voici un contre-exemple dû à Cohen et Seidenberg [18].

Considérons l'anneau $B := \mathbf{Z}[X]/(X^2 - X, 2X)$ et notons $x \in B$ la classe de X. On a $B = \mathbf{Z} + \mathbf{Z}x$, donc l'extension d'anneaux $\mathbf{Z} \hookrightarrow B$ est finie. Considérons les idéaux premiers $(0) \subsetneq (2)$ de $\mathbf{Z}$ et l'idéal maximal $\mathfrak{q}_2 := (2, x-1)$ de B au-dessus de (2). Il n'existe aucun idéal premier $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ de B au-dessus de (0). En effet, on aurait alors $2x = 0 \in \mathfrak{q}_1$ et $2 \notin \mathfrak{q}_1$, donc $x \in \mathfrak{q}_1$; mais c'est impossible puisqu'alors $1 = (1-x) + x \in \mathfrak{q}_2$.

Théorème 13.7. — *Soit $A \hookrightarrow B$ une extension finie d'anneaux intègres, avec A intégralement clos. L'application canonique $\iota^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ est ouverte.*

Démonstration. — Soit K_A le corps de fractions de A et soit K_B celui de B. Soit $b \in B$ non nul et soit

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in K_A[X]$$

le polynôme minimal de b sur K_A. Comme b est entier sur A, il existe un polynôme unitaire $Q \in A[X]$ tel que $Q(b) = 0$. Par définition du polynôme minimal, P divise Q. Comme A est intégralement clos, le lemme 8.25 entraîne que P est à coefficients dans A (*cf.* aussi exerc. 8.18).

18. Il est tiré de l'article : Prime ideals and integral dependance, *Bull. Amer. Math. Soc.* **52** (1946), 252–261. Je conseille la lecture de cet article, très accessible, qui démontre de façon très moderne beaucoup des théorèmes de cette section. Les contre-exemples se trouvent au § 3.

Nous allons montrer (avec les notations de (7))

$$\iota^\sharp(D(b)) = \bigcup_{i=0}^{n-1} D(a_i).$$

C'est donc un ouvert de $\mathrm{Spec}(A)$. Comme tout ouvert de $\mathrm{Spec}(B)$ est réunion d'ouverts du type $D(b)$, cela montrera le théorème.

Soit $\mathfrak{q} \in D(b)$. Posons $\mathfrak{p} := \iota^\sharp(\mathfrak{q}) = \mathfrak{q} \cap A$. Si tous les a_i sont dans $\mathfrak{p}$, on a $b^n \in \mathfrak{q}$, donc $b \in \mathfrak{q}$ puisque $\mathfrak{q}$ est un idéal premier, ce qui contredit $\mathfrak{q} \in D(b)$. On a donc bien $\iota^\sharp(\mathfrak{q}) \in \bigcup_{i=0}^{n-1} D(a_i)$, ce qui montre une inclusion.

Supposons inversement $\mathfrak{p} \in \bigcup_{i=0}^{n-1} D(a_i)$.

Notons R le sous-anneau $A[b]$ de B. Supposons $b \in \sqrt{\mathfrak{p}R}$. C'est un A-module libre dont une base est $(1, b, \dots, b^{n-1})$. Comme $b^m \in \mathfrak{p}R$ pour un $m \geq 1$, il existe $a'_0, \dots, a'_{n-1} \in \mathfrak{p}$ tels que $b^m = \sum_{i=0}^{n-1} a'_i b^i$. Par définition du polynôme minimal, P divise le polynôme $X^m - \sum_{i=0}^{n-1} a'_i X^i \in A[X]$ dans $K_A[X]$, donc aussi dans $A[X]$ par le même lemme 8.25 que ci-dessus. En passant modulo $\mathfrak{p}$, on obtient, puisque chaque a'_i est dans $\mathfrak{p}$, que X^m est divisible par

$$\bar{P}(X) = X^n + \bar{a}_{n-1}X^{n-1} + \cdots + \bar{a}_1 X + \bar{a}_0$$

dans $(A/\mathfrak{p})[X]$. Comme $(A/\mathfrak{p})[X]$ est un anneau intègre, cela entraîne que tous les $\bar{a}_i$ sont nuls, ce qui contredit l'hypothèse $\mathfrak{p} \in \bigcup_{i=0}^{n-1} D(a_i)$.

On a donc $b \notin \sqrt{\mathfrak{p}R}$. Comme $\sqrt{\mathfrak{p}R}$ est l'intersection des idéaux premiers de R contenant $\mathfrak{p}R$, il existe un tel idéal $\mathfrak{q}_2$ ne contenant pas b. On pose $\mathfrak{p}_2 := \mathfrak{q}_2 \cap A$. Par le going-down (th. 13.4) appliqué à l'extension entière $A \hookrightarrow R$, il existe $\mathfrak{q} \in \mathrm{Spec}(R)$ avec $\mathfrak{q} \subseteq \mathfrak{q}_2$ et $\mathfrak{q} \cap A = \mathfrak{p}$.

Comme B est entier sur R, il existe $\mathfrak{r} \in \mathrm{Spec}(B)$ au-dessus de $\mathfrak{q}$ (lemme 11.3). On a $\mathfrak{r} \in D(b)$, puisque sinon $b \in \mathfrak{r} \cap R = \mathfrak{q} \subseteq \mathfrak{q}_2$. On a ainsi montré $\mathfrak{p} = \iota^\sharp(\mathfrak{r}) \in \iota^\sharp(D(b))$. □

14. Dimension des algèbres de type fini sur un corps

Dans ce paragraphe, nous allons utiliser le « going-down » pour montrer des résultats sur la hauteur des idéaux premiers dans les algèbres de type fini sur un corps.

Soit A un anneau. On dira qu'une chaîne d'idéaux premiers de A est *saturée* si elle n'est contenue dans aucune chaîne d'idéaux premiers de longueur strictement supérieure. *A priori,* on peut seulement dire que la longueur d'une chaîne saturée est au plus la dimension de A.

Lorsque A n'est pas intègre, il est facile d'exhiber des chaînes saturées de longueur $< \dim(A)$: si $\mathrm{Spec}(A)$ a deux composantes irréductibles de dimensions différentes, celles-ci correspondent à des idéaux premiers $\mathfrak{p}_1$ et $\mathfrak{p}_2$ minimaux (prop. 5.17) tels que $\dim(A/\mathfrak{p}_1) \neq \dim(A/\mathfrak{p}_2)$. Des chaînes d'idéaux premiers de $A/\mathfrak{p}_i$ de longueur maximale donnent lieu à des chaînes saturées d'idéaux premiers de A de longueurs différentes.

Il est plus surprenant d'apprendre qu'il existe un anneau noethérien intègre A avec une chaîne saturée d'idéaux premiers de longueur $< \dim(A) < +\infty$. Ces anneaux restent très exotiques. Un tel phénomène n'arrive pas dans le cadre « géométrique », comme le montre le théorème suivant.

Théorème 14.1. — *Soit K un corps et soit A une K-algèbre de type fini* intègre. *Toute chaîne saturée d'idéaux premiers de A est de longueur* $\dim(A)$.

Démonstration. — On raisonne par récurrence sur la dimension de A. Si cette dimension vaut 0, il n'y a rien à démontrer.

Soit $\mathfrak{p}_m \supsetneq \cdots \supsetneq \mathfrak{p}_1 \supsetneq (0)$ une telle chaîne. D'après le lemme de Noether (th. 9.1), il existe des éléments algébriquement indépendants $a_1, \ldots, a_n$ de A tels que A soit une extension finie de l'anneau $B := K[a_1, \ldots, a_n]$ (attention, les notations sont inversées par rapport aux notations habituelles !). On a $\dim(A) = n$ par les th. 11.8 et 11.10.

Pour tout $i \in \{0, \ldots, m\}$, posons $\mathfrak{q}_i := \mathfrak{p}_i \cap B$. Soit $b \in \mathfrak{q}_1$ un élément irréductible dans l'anneau factoriel B. L'idéal premier (b) est contenu dans $\mathfrak{q}_1$ et B est intégralement clos, donc il existe, par le th. 13.4 (« going-down »), un idéal premier $\mathfrak{p}'_1 \subseteq \mathfrak{p}_1$ tel que $\mathfrak{p}'_1 \cap B = (b)$. Comme la chaîne $(\mathfrak{p}_i)$ est saturée, on a $\mathfrak{p}'_1 = \mathfrak{p}_1$, d'où $\mathfrak{p}_1 \cap B = (b)$. En particulier, $B/(b)$ est un sous-anneau de $A/\mathfrak{p}_1$, et l'extension correspondante est entière. Par le cor. 12.5 et le th. 11.8, on a $\dim(A/\mathfrak{p}_1) = n-1$. Or $\mathfrak{p}_m/\mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_1/\mathfrak{p}_1 = (0)$ est une chaîne saturée d'idéaux premiers de la K-algèbre de type fini intègre $A/\mathfrak{p}_1$. L'hypothèse de récurrence entraîne $\dim(A/\mathfrak{p}_1) = m - 1$. On en déduit $m = n$, ce qui termine la preuve. □

Corollaire 14.2. — *Soit K un corps et soit A une K-algèbre de type fini* intègre. *Pour tout idéal premier $\mathfrak{p}$ de A, on a* $\mathrm{ht}(\mathfrak{p}) = \dim(A) - \dim(A/\mathfrak{p})$.

Démonstration. — On rappelle que $\mathrm{ht}(\mathfrak{p}) + \dim(A/\mathfrak{p})$ est la longueur maximale des chaînes d'idéaux premiers de A contenant $\mathfrak{p}$. Cette longueur maximale (qui est $\leq \dim(A)$, donc finie) est atteinte pour une chaîne qui est nécessairement saturée. Il suffit donc d'appliquer le th. 14.1. □

Corollaire 14.3. — *Soit K un corps et soit A une K-algèbre de type fini* intègre. *Pour tous idéaux premiers $\mathfrak{q} \subseteq \mathfrak{p}$ de A, la longueur maximale des chaînes d'idéaux premiers de A entre $\mathfrak{p}$ et $\mathfrak{q}$ est*

$$\dim(A/\mathfrak{q}) - \dim(A/\mathfrak{p}).$$

Démonstration. — Il suffit d'appliquer le corollaire précédent à l'idéal premier $\mathfrak{p}/\mathfrak{q}$ de la K-algèbre de type fini intègre $A/\mathfrak{q}$. □

On a vu (cor. 12.5) que si K est un corps et P un élément non constant de $K[X_1, \ldots, X_n]$, la dimension de $V(P)$ est $n-1$. On va montrer que la réciproque est vraie : toute partie fermée de $\mathrm{Spec}(K[X_1, \ldots, X_n])$ qui est de dimension $n-1$ « peut être définie par une équation » (c'est-à-dire, est du type $V(P)$). Cela résulte du corollaire plus général suivant, dont la conclusion est remarquable : une partie de $\mathrm{Spec}(K[X_1, \ldots, X_n])$ de dimension $n - c$ ne peut pas en général être définie par c équations lorsque $c \geq 2$ (*cf.* note 9).

Corollaire 14.4. — *Soit K un corps et soit A une K-algèbre de type fini* factorielle. *Toute partie fermée irréductible de* $\mathrm{Spec}(A)$ *de dimension* $\dim(A) - 1$ *est du type $V(a)$, où a est un élément irréductible de A.*

Démonstration. — Une telle partie s'écrit $V(\mathfrak{p})$, où $\mathfrak{p}$ est un idéal premier de A qui, grâce au cor. 14.2, est de hauteur 1. Le corollaire résulte alors du lemme ci-dessous. □

Lemme 14.5. — *Soit A un anneau factoriel noethérien. Tout idéal premier de A de hauteur 1 est principal, engendré par un élément irréductible.*

Démonstration. — Soit $\mathfrak{p}$ un tel idéal et soit a un élément non nul de $\mathfrak{p}$. Décomposons a en produits d'irréductibles. L'un au moins des facteurs est dans $\mathfrak{p}$; prenons-en un, p. L'idéal (p) est premier (prop. 1.3) et $\mathfrak{p} \supseteq (p) \supsetneq (0)$. Comme $\mathfrak{p}$ est de hauteur 1, on a $\mathfrak{p} = (p)$. □

Exercice 14.6. — Prouver la réciproque du lemme : un anneau noethérien intègre dans lequel tout idéal premier de hauteur 1 est principal est factoriel (*Indication :* on pourra utiliser le cor. I.2.5 et le th. 7.1).

Le corollaire suivant généralise le cor. 12.5.

Corollaire 14.7. — *Soit K un corps, soit A une K-algèbre de type fini* intègre *et soit I un idéal de A engendré par n éléments. Toutes les composantes irréductibles de $V(I)$ sont de dimension $\geq \dim(A) - n$.*

Démonstration. — Les composantes irréductibles de $V(I)$ s'identifient aux $\mathrm{Spec}(A/\mathfrak{p})$, où $\mathfrak{p}$ décrit l'ensemble des idéaux premiers de A minimaux contenant I (prop. 5.17). Par le th. 7.2, on a $\mathrm{ht}(\mathfrak{p}) \leq n$. Il suffit donc d'appliquer le cor. 14.2 pour conclure. □

Exercice 14.8. — Redémontrer l'exerc. 12.6 comme conséquence immédiate du cor. 14.7.

15. Anneaux de valuation discrète

Ces anneaux jouent un rôle important en géométrie algébrique et il serait dommage de les passer sous silence.

Définition 15.1. — *Un* anneau de valuation discrète *est un anneau local principal qui n'est pas un corps.*

En anglais, on dit « discrete valuation ring », souvent abbrévié en « DVR ».

Exemple 15.2. — Soit K un corps. L'anneau des séries formelles $K[[X]]$ est un anneau de valuation discrète : il est local d'idéal maximal (X), et il est euclidien (exerc. I.1.10) donc principal.

Exemple 15.3. — Le localisé d'un anneau principal en un idéal premier est encore principal (exerc. 6.6). Si ce n'est pas un corps, c'est un anneau de valuation discrète. Si K est un corps, c'est le cas par exemple de $K[X]_{(X)}$, anneau des fractions rationnelles du type P/Q, avec $Q(0) \neq 0$. Si $p \in \mathbf{N}$ est un nombre premier, c'est aussi le cas de l'anneau $\mathbf{Z}_{(p)}$ formé des rationnels a/b, où p ne divise pas b.

Pourquoi le mot *valuation* ? Tout d'abord, si A est un anneau de valuation discrète, d'idéal maximal $\mathfrak{m}$, on appelle *uniformisante* de A tout générateur de $\mathfrak{m}$. Toute uniformisante est un élément irréductible de A (prop. I.1.15). Inversement, tout élément irréductible de A engendre $\mathfrak{m}$ (prop. I.1.15) donc est une uniformisante. Comme A est factoriel (cor. 2.6), si π est une uniformisante de A, tout élément non nul de A s'écrit de façon unique sous la forme $u\pi^n$, où u est une unité de A et $n \in \mathbf{N}$; remarquons que l'entier n ne dépend pas du choix de π : c'est le plus petit $n \in \mathbf{N}$ tel que $x \in \mathfrak{m}^n$. Les seuls idéaux de A sont (0) et les $\mathfrak{m}^n$, pour $n \in \mathbf{N}$, et les seuls idéaux premiers sont (0) et $\mathfrak{m}$.

Soit $v : A - \{0\} \to \mathbf{N}$ l'application définie par $v(x) = n$. Elle vérifie les propriétés suivantes :

1. $v(xy) = v(x) + v(y)$;
2. $v(x + y) \geq \min(v(x), v(y))$.

Soit K_A le corps des fractions de A. On étend v en une application surjective $v : K_A - \{0\} \to \mathbf{Z}$ vérifiant les mêmes propriétés en posant $v(x/y) = v(x) - v(y)$ (on doit bien sûr vérifier que cela ne dépend pas de l'écriture x/y).

Inversement, si K est un corps, une application *surjective* $v : K - \{0\} \to \mathbf{Z}$ vérifiant ces propriétés s'appelle une *valuation discrète* de K [19]. Le sous-ensemble

$$A := \{0\} \cup \{x \in K^* \mid v(x) \geq 0\}$$

de K en est un sous-anneau qui est un anneau de valuation discrète d'idéal maximal

$$\mathfrak{m} := \{0\} \cup \{x \in K^* \mid v(x) > 0\}.$$

En effet, la vérification du fait que A est un sous-anneau étant laissée au lecteur, soit I un idéal non nul de A et soit a un élément non nul de I tel que $v(a)$ soit minimal. Si $b \in I$ est non nul, on a $v(b/a) = v(b) - v(a) \geq 0$, donc $b/a \in A$ et $b = (b/a)a \in (a)$. On en déduit $I = (a)$, de sorte que tout idéal de A

19. Le terme *discret* renvoie au fait que l'image de v est contenue dans le groupe discret $\mathbf{Z}$. On peut définir une valuation générale en remplaçant $\mathbf{Z}$ par un groupe abélien ordonné quelconque.

est principal. Enfin, si $x \in A - \{0\}$ n'est pas inversible, on a $v(1/x) < 0$, donc $v(x) > 0$; si $\pi \in A$ est tel que $v(\pi) = 1$, le même raisonnement montre que x est dans (π). C'est donc l'unique idéal maximal de A.

Exemple 15.4. — Le corps des fractions de l'anneau de valuation discrète $K[[X]]$ est l'anneau $K((X))$ des séries de Laurent. La valuation associée $v : K((X)) - \{0\} \to \mathbf{Z}$ envoie une telle série non nulle $\sum_{m \in \mathbf{Z}} a_m X^m$ (avec $a_m = 0$ pour tout $m \ll 0$) sur le plus petit entier m tel que $a_m \neq 0$.

Exemple 15.5. — Pour tout élément irréductible p d'un anneau factoriel A, on a défini dans le § 1 une valuation discrète v_p sur A (si $a \in A$, l'entier $v_p(a)$ est le plus grand entier n tel que p^n divise A) qui se prolonge comme ci-dessus à son corps des fractions K_A. L'anneau de valuation discrète associé est $A_{(p)}$.

On peut montrer (c'est une conséquence du théorème d'Ostrowski qui détermine toutes les valeurs absolues sur le corps $\mathbf{Q}$) que les seules valuations discrètes de $\mathbf{Q}$ sont les *valuations p-adiques* v_p, pour $p \in \mathbf{N}$ nombre premier.

Théorème 15.6. — *Soit A un anneau. Les propriétés suivantes sont équivalentes :*

(i) *A est un anneau de valuation discrète ;*

(ii) *A est un anneau local noethérien, $\dim(A) > 0$ et son idéal maximal est principal ;*

(iii) *A est un anneau local noethérien intégralement clos de dimension 1.*

Démonstration. — Il est clair que (i) entraîne (iii) (prop. 8.21 et ex. 5.26).

Supposons (iii). Par hypothèse, A est intègre. Soit K_A son corps de fractions. L'idéal maximal $\mathfrak{m}$ de A n'est pas nul par hypothèse, donc $\mathfrak{m}^2 \subsetneq \mathfrak{m}$ (théorème de Krull ; cor. 2.11). Soit $\pi \in \mathfrak{m} - \mathfrak{m}^2$. Comme $\dim(A) = 1$ et que A est local, les seuls idéaux premiers de A sont (0) et $\mathfrak{m}$. L'idéal premier $\mathfrak{m}$ est donc minimal contenant (π) ; il lui est donc associé (th. 4.23) : il existe (déf. 4.18) $a \in A$ tel que $\mathfrak{m} = ((\pi) : a) = \{b \in A \mid \pi \mid ab\}$. Posons $x := a\pi^{-1} \in K_A$; comme $1 \notin \mathfrak{m}$, on a $x \notin A$, mais $x\mathfrak{m} \subseteq A$.

Si $x\mathfrak{m} \subseteq \mathfrak{m}$, appliquons le théorème de Cayley-Hamilton (th. II.3.2) à l'endomorphisme u du A-module de type fini $\mathfrak{m}$ donné par la multiplication par x. Il fournit un polynôme unitaire $P \in A[X]$ tel que $P(u) = 0$. Alors $P(x) = P(u)(1) = 0$, de sorte que x est entier sur A. Comme A est intégralement clos, $x \in A$, ce qui est absurde.

On a donc $x\mathfrak{m} = A$, c'est-à-dire $x^{-1} \in \mathfrak{m}$. On en déduit

$$\mathfrak{m} = ((\pi) : a) = ((ax^{-1}) : a) = (x^{-1}),$$

ce qui montre que $\mathfrak{m}$ est principal, d'où (ii).

Supposons (ii). Soit π un générateur de l'idéal maximal $\mathfrak{m}$ de A. Le théorème de Krull (cor. 2.11) entraîne $\bigcap_{n=1}^{\infty} (\pi^n) = 0$.

Pour tout $x \in A - \{0\}$, il existe donc un plus grand entier $m \geq 0$ tel que $x \in (\pi^m)$. On peut écrire $x = u\pi^m$, avec $u \notin (\pi) = \mathfrak{m}$, donc u inversible. Montrons que l'entier m est uniquement déterminé : si $x = u\pi^m = w\pi^n$, avec disons $m \geq n$, on a $(uw^{-1}\pi^{m-n} - 1)\pi^n = 0$. Si $m > n$, on a $uw^{-1}\pi^{m-n} - 1 \notin \mathfrak{m}$, donc il est inversible et $\pi^n = 0$. Comme $\dim(A) > 0$, il existe un idéal premier $\mathfrak{p} \subsetneq \mathfrak{m}$. On a alors $\pi^n \in \mathfrak{p}$, donc $\pi \in \mathfrak{p}$, ce qui est absurde. On a donc $m = n$. On pose $v(x) = m$, définissant ainsi une application $v : A - \{0\} \to \mathbf{N}$.

Si x et y sont non nuls, on les écrit $x = u\pi^m$ et $y = w\pi^n$. On a alors $xy = uw\pi^{m+n}$ et on montre de la même façon que ce n'est pas nul. Donc A est intègre. L'application v se prolonge alors en une valuation discrète sur le corps des fractions de A, et A est l'anneau de valuation discrète associé à cette valuation, d'où (i). □

Remarque 15.7. — *Les anneaux de valuation discrète sont les anneaux locaux noethériens réguliers de dimension 1* (*cf.* exerc. 7.7 ; si A est un tel anneau, d'idéal maximal $\mathfrak{m}$ et de corps résiduel $\kappa := A/\mathfrak{m}$, cela signifie que le κ-espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$ est de dimension 1).

En effet, si A est un anneau de valuation discrète d'uniformisante π, tout élément de $\mathfrak{m}$ est multiple de π, qui engendre donc le κ-espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$. Inversement, si cet espace vectoriel est de dimension 1, $\mathfrak{m}$ est principal (exerc. 7.7), et A est un anneau de valuation discrète (th. 15.6).

Exercice 15.8 **(Vecteurs de Witt)**. — Soit K un corps parfait de caractéristique $p > 0$. Montrer qu'il existe un anneau de valuation discrète $W(K)$ de caractéristique 0 et de corps résiduel K (*Indication :* on pourra consulter la littérature ([**S**], chap. II, § 6 ou [**B3**], chap. IX, § 1)). L'anneau $W(K)$ s'appelle *anneau des vecteurs de Witt à coefficients dans* K. Lorsque $K = \mathbf{F}_p$, l'anneau $W(\mathbf{F}_p)$ est l'anneau des entiers p-adiques $\mathbf{Z}_p$ (*cf.* rem. 2.13).

16. Anneaux de Dedekind

Rappelons que nous avons défini (rapidement dans le § 4) les anneaux de Dedekind comme les anneaux noethériens de dimension 1 (c'est-à-dire pour lesquels tout idéal premier non nul est maximal) intégralement clos (*cf.* § 5.4). Les anneaux de Dedekind locaux sont donc les anneaux de valuation discrète (th. 15.6).

D'autres exemples sont donnés par les anneaux principaux qui ne sont pas des corps, ainsi que par les anneaux d'entiers de corps de nombres (*cf.* § 8), c'est-à-dire les clôtures intégrales de $\mathbf{Z}$ dans des extensions finies de $\mathbf{Q}$. Notre but est de montrer la décomposition des idéaux non nuls en produit d'idéaux maximaux (th. 16.3).

Proposition 16.1. — *Soit A un anneau intègre noethérien. Les deux propriétés suivantes sont équivalentes :*

(i) *A est un anneau de Dedekind ;*

(ii) *pour tout idéal maximal $\mathfrak{m}$ de A, l'anneau local $A_\mathfrak{m}$ est un anneau de valuation discrète.*

Démonstration. — Soit A un anneau de Dedekind et soit $\mathfrak{m}$ un idéal maximal de A. L'anneau local $A_\mathfrak{m}$ est noethérien et intégralement clos (exerc. 8.17) et il est de dimension 1 puisque tout chaîne d'idéaux premiers de $A_\mathfrak{m}$ est une chaîne d'idéaux premiers de A et que $\mathfrak{m} \supsetneq (0)$ est une telle chaîne. C'est donc un anneau de valuation discrète (th. 15.6).

Inversement, supposons (ii). Comme l'anneau A est intègre et que chaque $A_\mathfrak{m}$ est intégralement clos, il en est de même pour A (exerc. 8.17). Enfin, toute chaîne saturée d'idéaux premiers de A commence par un idéal maximal $\mathfrak{m}$ donc est de longueur $\dim(A_\mathfrak{m}) = 1$. On a donc montré que A est un anneau de Dedekind. □

Exercice 16.2. — Soit P un élément non constant de $\mathbf{C}[X, Y]$. Si on note A l'anneau quotient $\mathbf{C}[X, Y]/(P)$, l'ensemble $\mathrm{Specmax}(A)$ est en bijection avec la *courbe plane*

$$C := \{(x, y) \in \mathbf{C}^2 \mid P(x, y) = 0\}$$

(prop. 10.9, ex. 10.10, ex. 10.15). Nous allons montrer que l'anneau A est un anneau de Dedekind si et seulement si la courbe C est non singulière au sens de la géométrie différentielle, c'est-à-dire qu'en chaque point (x, y) de C, une des dérivées partielles $\frac{\partial P}{\partial X}(x, y)$ ou $\frac{\partial P}{\partial Y}(x, y)$ n'est pas nulle. Remarquons que cette condition est équivalente, par le cor. 10.4, à l'égalité

$$\Big(P, \frac{\partial P}{\partial X}, \frac{\partial P}{\partial Y}\Big) = \mathbf{C}[X, Y].$$

a) Soit (x, y) un point de C et soit $\mathfrak{m}$ l'idéal maximal $(X - x, Y - y)$ de $\mathbf{C}[X, Y]$. Montrer que l'anneau $A_\mathfrak{m}$ est un anneau de valuation discrète si et seulement si l'une des dérivées partielles $\frac{\partial P}{\partial X}(x, y)$ ou $\frac{\partial P}{\partial Y}(x, y)$ n'est pas nulle (*Indication :* on pourra utiliser la rem. 15.7).

b) En déduire l'énoncé annoncé.

Théorème 16.3. — *Tout idéal non nul d'un anneau de Dedekind s'écrit de façon unique comme produit d'idéaux maximaux.*

Démonstration. — Soit A un anneau de Dedekind et soit $\mathfrak{q}$ un idéal primaire non nul de A, de radical $\mathfrak{m}$ (maximal comme tout idéal premier non nul de A). Le localisé $A_\mathfrak{m}$ est un anneau de valuation discrète, donc l'idéal $\mathfrak{q}A_\mathfrak{m}$ est une puissance $(\mathfrak{m}A_\mathfrak{m})^n = \mathfrak{m}^n A_\mathfrak{m}$ de son idéal maximal, avec $n \geq 1$. Mais $\mathfrak{m}^n$ est, comme $\mathfrak{q}$, un idéal $\mathfrak{m}$-primaire : $\mathfrak{m}$ est l'unique idéal premier de A contenant $\mathfrak{m}^n$, donc il est sa propre décomposition primaire minimale (th. 4.19). Pour ces idéaux, on vérifie facilement que l'on a (*cf.* § 6 pour les idéaux premiers)

$$\mathfrak{m}^n = \mathfrak{m}^n A_\mathfrak{m} \cap A \quad \text{et} \quad \mathfrak{q} = \mathfrak{q}A_\mathfrak{m} \cap A.$$

On en déduit $\mathfrak{q} = \mathfrak{m}^n$.

Soit I un idéal non nul de A. Une décomposition primaire minimale de I (th. 4.19) s'écrit donc $I = \bigcap_{i=1}^s \mathfrak{m}_i^{n_i}$. Les idéaux premiers $\mathfrak{m}_i$ sont aussi minimaux contenant I, donc cette décomposition est unique (th. 4.23). Enfin, on déduit du lemme 4.4 que l'on a aussi $I = \prod_{i=1}^s \mathfrak{m}_i^{n_i}$. □

Remarque 16.4. — On peut montrer qu'un anneau intègre pour lequel tout idéal non nul est produit d'idéaux premiers est un anneau de Dedekind.

Corollaire 16.5. — *Soit I un idéal non nul d'un anneau de Dedekind A. Tout idéal de l'anneau A/I est engendré par un élément.*

Attention, l'anneau A/I n'est en général pas intègre, donc ce n'est pas un anneau principal.

Démonstration. — Le th. 16.3 fournit une décomposition $I = \bigcap_{i=1}^s \mathfrak{m}_i^{n_i}$ et le théorème des restes chinois (exerc. 4.6) un isomorphisme

$$A/I \simeq \prod_{i=1}^s (A/\mathfrak{m}_i^{n_i}).$$

Chaque facteur $A/\mathfrak{m}_i^{n_i}$ est isomorphe à $A_{\mathfrak{m}_i}/\mathfrak{m}_i^{n_i} A_{\mathfrak{m}_i}$ donc est un anneau principal comme quotient de l'anneau de valuation discrète (donc principal) $A_{\mathfrak{m}_i}$. Comme on l'a vu dans le § 5, tout idéal de A/I est produit d'idéaux des anneaux $A/\mathfrak{m}_i^{n_i}$, qui sont engendrés par un élément. Il a donc la même propriété. □

Nous montrons maintenant que tout idéal d'un anneau de Dedekind est engendré par deux éléments, sous la forme plus précise suivante.

Proposition 16.6. — *Soit A un anneau intègre qui n'est pas un corps. Alors A est un anneau de Dedekind si et seulement si, pour tout idéal non nul I de A et tout $a \in I - \{0\}$, il existe $b \in I$ tel que $I = (a, b)$.*

Démonstration. — Soit A un anneau de Dedekind, soit I un idéal non nul de A et soit $a \in I - \{0\}$. Le cor. 16.5 entraîne que dans $A/(a)$, l'idéal $I/(a)$ est engendré par un élément $\overline{b}$. On a alors $I = (a, b)$.

Montrons la réciproque. L'anneau A est alors noethérien, et il suffit donc, par la prop. 16.1, de montrer que pour tout idéal maximal $\mathfrak{m}$ de A, l'anneau local intègre $A_\mathfrak{m}$ (qui n'est pas un corps) est un anneau principal. Soit I un idéal non nul de cet anneau. Comme $\mathfrak{m} \neq (0)$, il existe $a \in \mathfrak{m}(I \cap A) - \{0\}$, puis $b \in I$ tel que $I \cap A = (a, b)$. On a alors

$$I = (I \cap A)A_\mathfrak{m} = (a, b)A_\mathfrak{m} = \mathfrak{m}I + bA_\mathfrak{m}.$$

Le lemme de Nakayama (th. II.3.8) entraîne alors $I = bA_\mathfrak{m}$, de sorte que I est principal. □

Proposition 16.7. — *Un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux premiers non principaux est principal.*

En particulier, un anneau de Dedekind qui n'a qu'un nombre fini d'idéaux maximaux est principal.

La proposition dit qu'un anneau de Dedekind non principal a une infinité d'idéaux premiers non principaux. Noter que dans l'anneau (non intégralement clos) $\mathbf{Z}[\sqrt{-3}]$, il y a exactement un idéal premier non principal : $(1+\sqrt{-3}, 1-\sqrt{-3})$.

Démonstration. — Soit A un anneau de Dedekind et soient $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ les différents idéaux maximaux non principaux de A. Supposons $n \geq 1$. Par le lemme d'évitement (exerc. 4.5), il existe $a \in \mathfrak{m}_1$ tel que $a \notin \mathfrak{m}_1^2 \cup \mathfrak{m}_2 \cup \cdots \cup \mathfrak{m}_n$. L'idéal (a) n'est contenu dans aucun des idéaux $\mathfrak{m}_2, \ldots, \mathfrak{m}_n$, donc sa décomposition primaire s'écrit

$$(a) = \mathfrak{m}_1 \prod_{i=2}^{s} \mathfrak{n}_i,$$

où les idéaux maximaux $\mathfrak{n}_2, \ldots, \mathfrak{n}_s$ sont distincts des idéaux $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$, donc principaux. On en déduit $(a) = \mathfrak{m}_1(b)$ pour un $b \in A$. On peut donc écrire $a = xb$, avec $x \in \mathfrak{m}_1$. Comme A est intègre, on obtient $\mathfrak{m}_1 = (x)$, ce qui est absurde. On a donc $n = 0$ et A est principal. □

Exercice 16.8. — Soit A un anneau de Dedekind. Le contenu, noté $c(P)$, d'un polynôme $P \in A[X]$ est l'idéal de A engendré par les coefficients de P (comparer avec la déf. 1.7). Montrer le lemme de Gauss (*cf.* lemme 1.8) : pour tous polynômes P et Q dans $A[X]$, on a $c(PQ) = c(P)c(Q)$ (*Indication :* on pourra localiser en les idéaux maximaux de A).

Exercice 16.9. — Soit A un anneau de Dedekind. Pour tous idéaux I_1, I_2 et I_3 de A, montrer les égalités

$$\begin{aligned} I_1 \cap (I_2 + I_3) &= (I_1 \cap I_2) + (I_1 \cap I_3), \\ I_1 + (I_2 \cap I_3) &= (I_1 + I_2) \cap (I_1 + I_3). \end{aligned}$$

(*Indication :* localiser !)

Remarque 16.10 **(Ramification)**. — Soit A un anneau de Dedekind et soit K_A son corps de fractions. Soit $K_A \hookrightarrow L$ une extension séparable et soit $B \subseteq L$ la clôture intégrale de A dans L. C'est un anneau noethérien, extension finie de A (th. 8.19), donc c'est un anneau de Dedekind (th. 11.8). Soit $\mathfrak{m}$ un idéal maximal de A ; par le lemme 11.3, il est contenu dans un idéal maximal de B, donc on peut écrire

$$\mathfrak{m}B = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_s^{e_s}.$$

où $e_1, \ldots, e_e$ sont des entiers strictement positifs et $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ des idéaux maximaux de B (ce sont les idéaux premiers de B « au-dessus » de $\mathfrak{m}$; *cf.* § 11). L'entier e_i est appelé l'*indice de ramification* de $\mathfrak{m}_i$ au-dessus de $\mathfrak{m}$. On a la belle formule ([**ZS1**], cor. du th. V.21 ; [**S**], chap. I, § 4, prop. 10)

$$[L : K_A] = \sum_{i=1}^{s} e_i [B/\mathfrak{m}_i : A/\mathfrak{m}].$$

Voici un exemple géométrique. Reprenons l'exemple 11.9 (avec $K = \mathbf{C}$) avec ses notations. Posons $A = \mathbf{C}[X]$ et $B = \mathbf{C}[X,Y]/(X^2 + Y^2 - 1)$. L'anneau B est intégralement clos (exerc. 16.2), donc c'est la clôture intégrale de A dans K_B. Rappelons que l'application $\iota_{\max}^\sharp$ s'identifie à la projection (surjective)

$$\begin{aligned} \{(x,y) \in \mathbf{C}^2 \mid x^2 + y^2 = 1\} &\longrightarrow \mathbf{C} \\ (x,y) &\longmapsto x. \end{aligned}$$

Tout point $t \in \mathbf{C}$ a deux préimages, sauf -1 et 1, qui n'en ont qu'une. Soit $\mathfrak{m}_t \subseteq A$ l'idéal maximal $(X - t)$. On a

$$\mathfrak{m}_t B = (X - t, Y - \sqrt{t^2 - 1})(X - t, Y + \sqrt{t^2 - 1}).$$

Les indices de ramification sont donc 1, sauf lorsque $t \in \{-1, 1\}$, où l'on a $\mathfrak{m}_t B = (X - t, Y)^2$. Le terme « ramifié » correspond au fait géométrique que l'unique préimage de 1 se « sépare » en deux au voisinage de 1.

Voici maintenant un exemple arithmétique. Soit d un entier sans facteur carré, différent de 1, soit B l'anneau des entiers du corps $\mathbf{Q}(\sqrt{d})$, c'est-à-dire la clôture intégrale de $A = \mathbf{Z}$ dans ce corps (*cf.* exerc. 8.20), et soit $p \in \mathbf{N}$ un nombre premier, supposé impair pour simplifier. On est alors dans exactement un des trois cas suivants :

- $p \mid d$ et $(p) = (p, \sqrt{d})^2$ (où l'idéal $(p, \sqrt{d})$ de B est maximal ; on dit que p est *ramifié* dans B) ;
- $p \nmid d$, d n'est pas un carré modulo p et (p) est un idéal maximal de B (on dit que p est *inerte* dans B) ;
- $p \nmid d$, $d = n^2 \pmod{p}$ et $(p) = (p, \sqrt{d} + n)(p, \sqrt{d} - n)$ (où les idéaux $(p, \sqrt{d} \pm n)$ de B sont maximaux distincts ; on dit que p est *décomposé* dans B).

Pour plus de détails, on pourra consulter [**L**], Chap. III.

Remarque 16.11 **(Modules de type fini sur un anneau de Dedekind)**. — On peut étendre aux anneaux de Dedekind la description des modules de type fini sur un anneau principal donnée au cor. II.4.7. On montre ainsi que tout module de type fini sur un anneau de Dedekind A est isomorphe à une somme directe

$$A^r \oplus I \oplus A/I_1 \oplus \cdots \oplus A/I_s,$$

où $I, I_1, \ldots, I_s$ sont des idéaux de A vérifiant $A \supsetneq I_1 \supseteq \cdots \supseteq I_s \supsetneq (0)$. Le fait qu'il n'y ait qu'un seul idéal dans la décomposition provient du résultat suivant : si I et J sont des idéaux de A, on a un isomorphisme de A-modules $I \oplus J \simeq A \oplus IJ$ (exercice !). Si A n'est pas principal, il existe donc des modules sans torsion, de type fini, non libres (n'importe quel idéal non principal ! Comparer avec le cor. II.4.8).

BIBLIOGRAPHIE

[AM] Atiyah, M. F., Macdonald, I. G., *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[B1] Bourbaki, N., *Éléments de mathématique. Algèbre.* Chapitres 4 à 7. Masson, Paris.

[B2] Bourbaki, N., *Éléments de mathématique. Algèbre commutative.* Chapitres 5 à 7. Masson, Paris.

[B3] Bourbaki, N., *Éléments de mathématique. Algèbre commutative.* Chapitres 8 et 9. Masson, Paris.

[CL] Chambert-Loir, A., *A field guide to algebra.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2005, ou en version française : *Algèbre corporelle.* École Polytechnique, 2005.

[L] Lorenzini, D., *An invitation to arithmetic geometry.* Graduate Studies in Mathematics **9**. American Mathematical Society, Providence, RI, 1996.

[M] Matsumura, H., *Commutative algebra.* Second edition. Mathematics Lecture Note Series **56**. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.

[P] Peskine, Ch., *An algebraic introduction to complex projective geometry. 1. Commutative algebra.* Cambridge Studies in Advanced Mathematics **47**. Cambridge University Press, Cambridge, 1996.

[S] Serre, J.-P., *Corps locaux.* Hermann, Paris, 1997.

[ZS1] Zariski, O., Samuel, P., *Commutative algebra. Vol. I.* With the cooperation of I. S. Cohen. Corrected reprinting of the 1958 edition. Graduate Texts in Mathematics **28**. Springer-Verlag, New York-Heidelberg-Berlin, 1975.

[ZS2] Zariski, O., Samuel, P., *Commutative algebra. Vol. II.* Reprint of the 1960 edition. Graduate Texts in Mathematics **29**. Springer-Verlag, New York-Heidelberg, 1975.