# Chapitre 2

# Extensions de corps

## Sommaire



**Présentation du chapitre**

Galois considérait des équations à coefficients dans un « domaine de rationalité », domaine auquel il « adjoignait des quantités ». La notion de corps formalise l'idée de domaine de rationalité. L'adjonction de quantités se traduit en termes modernes par le concept d'extension de corps. L'adjonction de racines de polynômes à coefficients dans le corps de base s'exprime en termes d'extension finie et d'extension algébrique. Le point de vue des extensions apporte un regard un peu différent sur les équations algébriques, puisqu'il suggère de « positionner » simultanément des racines de plusieurs équations à coefficients dans le corps $\mathbb{K}$ dans des extensions de $\mathbb{K}$.

Le point de vue des extensions permet d'utiliser l'algèbre linéaire. De fait, la théorie élémentaire de la dimension des espaces vectoriels permet de linéariser la notion d'algébricité et la faire apparaître comme une propriété de finitude. Ces idées sont développées dans les sections **1** et **2**.

Dans la section **3**, on justifie qu'un polynôme non constant à coefficients dans le corps $\mathbb{K}$ admet des racines dans une extension adéquate du $\mathbb{K}$. Ce fait, énoncé et utilisé dans le chapitre **1**, a longtemps été admis par les mathématiciens ; sa preuve n'est pas difficile, mais d'esprit assez différent de celui des sections précédentes. On en établit également une version transfinie, le théorème de Steinitz selon lequel tout corps admet une « clôture algébrique ». Il sera commode, en théorie de Galois de fixer une fois pour toutes une telle clôture. [1]

Le contenu essentiel pour la suite est constitué de la section **1** (en omettant éventuellement la démonstration de l'irréductibilité de $\Phi_n$ en **1.6**), des paragraphes **2.1** à **2.3**, **3.1** et **3.3**. La section **4**, consacrée à la constructibilité à la règle et au compas, moins centrale, présente cependant un grand intérêt historique : on y résout très simplement, par la négative, trois problèmes de construction légués par les Grecs. La section **5**, plus optionnelle encore, est consacrée à la notion d'élément entier sur un anneau, qui généralise celle d'élément algébrique sur un corps.

Dans tout ce chapitre, $\mathbb{K}$ est un corps.

# 1 Extensions, algébricité et transcendance

## 1.1 La notion d'extension

Si $\mathbb{K}$ est un sous-corps de l'anneau $\mathbb{A}$, $\mathbb{A}$ est naturellement muni d'une structure de $\mathbb{K}$-algèbre. Pour définir cette structure, il suffit de préciser la multiplication « externe » d'un élément de $\mathbb{A}$ par un élément de $\mathbb{K}$ : cette multiplication est naturellement définie par restriction de la multiplication interne de $\mathbb{A}$.

Nous nous intéresserons principalement ici au cas où $\mathbb{A}$ est un corps $\mathbb{L}$. Si $\mathbb{L}$ est un surcorps de $\mathbb{K}$, on dit que que $\mathbb{L}$ muni de sa structure de $\mathbb{K}$-algèbre est une *extension* de $\mathbb{K}$ et on parle de l'extension (de corps) $\mathbb{L}/\mathbb{K}$.

L'extension $\mathbb{L}/\mathbb{K}$ est *finie* si $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie ; cette dimension, notée $[\mathbb{L} : \mathbb{K}]$, est le *degré de l'extension*. Ainsi, $\mathbb{C}/\mathbb{R}$ est une extension de degré 2, mais $\mathbb{R}/\mathbb{Q}$ n'est pas une extension finie (sans quoi $\mathbb{R}$ serait dénombrable). Les extensions finies de $\mathbb{Q}$ sont appelées *corps de nombres*.

**Exercice 1.** ② *Soit $\mathcal{P}$ l'ensemble des nombres premiers. Vérifier que la famille $(\ln(p))_{p\in\mathcal{P}}$ est $\mathbb{Q}$-libre. Retrouver que l'extension $\mathbb{R}/\mathbb{Q}$ n'est pas finie.*

À titre de première application de la notion de degré, mentionnons la conséquence suivante.

**Proposition 1.** *Soit $\mathbb{K}$ un corps fini. Alors il existe $p \in \mathcal{P}$ et $d \in \mathbb{N}^*$ tels que $|\mathbb{K}| = p^d$.* [2]

*Preuve.* Si $p$ est la caractéristique de $\mathbb{K}$, le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{F}_p$. Le corps $\mathbb{K}$ est donc une $\mathbb{F}_p$-algèbre, nécessairement de dimension finie. Si $d$ est cette dimension, $|\mathbb{K}| = p^d$.

Le théorème d'algèbre linéaire ci-après, souvent nommé *théorème de la base télescopique*, est central dans l'étude des extensions de corps.

1. Dans le cas « concret » des corps de nombres, le corps des nombres complexes algébriques est une clôture algébrique explicite.

2. Cet énoncé est le point de départ de la théorie des corps finis. On montre que, pour tout nombre premier $p$ et tout $n \in \mathbb{N}^*$, il existe un corps fini de cardinal $p^n$, unique à isomorphisme près.

**Théorème 1.** *Soient $\mathbb{L}/\mathbb{K}$ une extension de corps, $V$ un $\mathbb{L}$-espace vectoriel, $(\lambda_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(v_j)_{j\in J}$ une base de $V$ sur $\mathbb{L}$.*

*(i) La famille $(\lambda_i\, v_j)_{(i,j)\in I\times J}$ est une base de $V$ sur $\mathbb{K}$.*

*(ii) Supposons $V$ non nul. Alors le $\mathbb{K}$-espace $V$ est de dimension finie si et seulement si l'extension $\mathbb{L}/\mathbb{K}$ est finie et le $L$-espace $V$ est de dimension finie. On a alors :*

$$dim_{\mathbb{K}}(V) = [\mathbb{L} : \mathbb{K}] \times dim_{\mathbb{L}}(V).$$

*Preuve.* Le second point est conséquence directe du premier. Vérifions donc que la famille considérée est libre et génératrice.

a) Soit $(\alpha_{i,j})_{(i,j)\in I\times J}$ une famille presque nulle d'éléments de $\mathbb{K}$ telle que :

$$0 = \sum_{(i,j)\in I\times J} \alpha_{i,j}\lambda_i v_j = \sum_{j\in J}\left(\sum_{i\in I}\alpha_{i,j}\lambda_i\right) v_j.$$

Puisque chaque somme $\sum_{i\in I}\alpha_{i,j}\lambda_i$ est dans $\mathbb{L}$, la liberté sur $\mathbb{L}$ de $(v_j)_{j\in J}$ montre que chacun de ces coefficients est nul. La liberté sur $\mathbb{K}$ de $(\lambda_i)_{i\in I}$ implique alors la nullité des $\alpha_{i,j}$ : la famille $(\lambda_i v_j)_{(i,j)\in I\times J}$ est libre sur $\mathbb{K}$.

b) Si $x \in V$, on peut écrire

$$x = \sum_{j\in J}\mu_j v_j$$

où $(\mu_j)_{j\in J}$ est une famille presque nulle d'éléments de $\mathbb{L}$. Décomposant chaque $\mu_j$ comme combinaison $\mathbb{K}$-linéaire des $\lambda_i$, on voit que la famille $(\lambda_i v_j)_{(i,j)\in I\times J}$ engendre $V$ sur $\mathbb{K}$.

Nous utiliserons surtout le théorème 1 à travers le corollaire suivant.

**Corollaire 1.** *Soient $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ deux extensions de corps, $(e_i)_{i\in I}$ une base de $L$ sur $\mathbb{K}$, $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$.*

*(i) La famille $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.*

*(ii) L'extension $\mathbb{M}/\mathbb{K}$ est finie si et seulement s'il en est de même de $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$. Dans ce cas, on a :*

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}] \times [\mathbb{L} : \mathbb{K}].$$

Ce corollaire affirme la *transitivité des extensions finies*. La formule donnant $[\mathbb{M} : \mathbb{K}]$ est la propriété de *multiplicativité des degrés*.

**Exercice 2.** ① *Soit $\mathbb{L}/\mathbb{K}$ une extension finie avec $[\mathbb{L} : \mathbb{K}]$ premier. Quels sont les sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ ?*

**Exercice 3.** ④ *Soient $V$ un $\mathbb{C}$-espace de dimension finie, $u \in \mathcal{L}(V)$. On note $u_{\mathbb{R}}$ l'endomorphisme du $\mathbb{R}$-espace $V$. Calculer la trace et le déterminant de $u_{\mathbb{R}}$ en fonction de celui de $u$.*

**Remarque** *Extensions et morphismes*

La définition des extensions utilisée ici est adaptée à un cours élémentaire. Il serait cependant préférable de dire que le corps $\mathbb{L}$ est une extension de $\mathbb{K}$ s'il existe un morphisme d'anneaux de $\mathbb{K}$ dans $\mathbb{L}$. Un tel morphisme $\varphi$ est nécessairement injectif (lemme 2, **2.3**, chapitre **1**). Il s'ensuit que

$\varphi(\mathbb{K})$ est un sous-corps de $\mathbb{L}$ isomorphe à $\mathbb{K}$, que l'on identifie légitimement à $\mathbb{K}$ : une propriété « d'anneaux » est vraie dans $\mathbb{K}$ si et seulement si elle l'est dans $\varphi(\mathbb{K})$.[3] Cette définition des extensions, plus souple que la précédente, devient indispensable lorsqu'on remplace $\mathbb{K}$ par un anneau.

## 1.2 Adjonction

Si $E$ est une partie non vide de la $\mathbb{K}$-algèbre $\mathbb{A}$, on note $\mathbb{K}[E]$ la plus petite $\mathbb{K}$-sous-algèbre de $\mathbb{A}$ contenant $E$. On dit que $\mathbb{K}[E]$ est la sous-algèbre de $\mathbb{A}$ obtenue par *adjonction* à $\mathbb{K}$ des éléments de $E$. Si $E = \{x_1, \dots, x_m\}$ est fini, on note $\mathbb{K}[E] = \mathbb{K}[x_1, \dots, x_m]$. On a :

$$\mathbb{K}[x_1, \dots, x_m] = \{P(x_1, \dots, x_m)\ ;\ P \in \mathbb{K}[X_1, \dots, X_m]\}\,.$$

En particulier, pour $x \in \mathbb{A}$ :

$$\mathbb{K}[\{x\}] = \mathbb{K}[x] = \{P(x),\ P \in \mathbb{K}[X]\}\,.$$

Une $\mathbb{K}$-algèbre de la forme $\mathbb{A} = \mathbb{K}[x]$ est dite *monogène*.

**Exercice 4.** ⑤ *Soient $\mathbb{A}_1, \dots, \mathbb{A}_r$ des $\mathbb{K}$-algèbres monogènes de dimension finie. Si $\mathbb{K}$ est infini, montrer que $\mathbb{A}_1 \times \cdots \times \mathbb{A}_r$ est monogène.*

Si $\mathbb{L}$ est un surcorps de $\mathbb{K}$ et $E$ une partie de $\mathbb{L}$, on note $\mathbb{K}(E)$ le plus petit sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et $E$. Si $E = \{x_1, \dots, x_m\}$ est fini, on a :

$$\mathbb{K}(E) = \left\{ \frac{P(x_1, \dots, x_m)}{Q(x_1, \dots, x_m)}\ ;\ (P, Q) \in \mathbb{K}[X_1, \dots, X_m]^2,\ Q(x_1, \dots, x_m) \neq 0 \right\}$$

et on note

$$\mathbb{K}(E) = \mathbb{K}(x_1, \dots, x_m).$$

En particulier, pour $x$ dans $\mathbb{L}$ :

$$\mathbb{K}(\{x\}) = \mathbb{K}(x) = \left\{ \frac{P(x)}{Q(x)}\ ;\ (P, Q) \in \mathbb{K}[X]^2,\ Q(x) \neq 0 \right\}.$$

3. Ce type d'identification est très fréquent en mathématiques. Ainsi, on construit $\mathbb{Z}$ à partir de $\mathbb{N}$ par symétrisation, comme quotient de $\mathbb{N}^2$ par la relation

$$(a, b) \sim (a', b') \Longleftrightarrow a + b' = a' + b,$$

$\mathbb{Q}$ comme corps des fractions de $\mathbb{Z}$, c'est-à-dire comme quotient de $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ par la relation

$$(a, b) \sim (a', b') \Longleftrightarrow ab' = a'b,$$

$\mathbb{R}$ comme complétion de $\mathbb{Q}$, c'est-à-dire comme quotient de l'ensemble des suites de Cauchy de rationnels par la relation

$$(a_n)_{n\geq 0} \sim (b_n)_{n\geq 0} \Longleftrightarrow a_n - b_n \underset{n\to+\infty}{\longrightarrow} 0$$

(la convergence vers 0 dans l'ensemble des suites de rationnels peut bien sûr être définie sans connaître $\mathbb{R}$,« en prenant $\varepsilon$ dans $\mathbb{Q}^{+*}$ »), enfin $\mathbb{C}$ soit en munissant $\mathbb{R}^2$ de la loi idoine, soit en utilisant les matrices de similitudes

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \qquad (a, b) \in \mathbb{R}^2,$$

soit comme corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$ et donc comme quotient $\mathbb{R}[X]/(X^2 + 1)$ (**3.1**). On a ainsi une suite d'injections

$$\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$$

respectant les structures. En pratique, on effectue les identifications naturelles successives, ce qui permet d'écrire

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Bien sûr, on a $\mathbb{K}[E] \subset \mathbb{K}(E)$, avec égalité si et seulement si $\mathbb{K}[E]$ est un corps.

On définit enfin le *composé* $\mathbb{L}_1\mathbb{L}_2$ de deux sous-corps $\mathbb{L}_1$ et $\mathbb{L}_2$ du corps $\mathbb{L}$ comme le plus petit sous-corps de $\mathbb{L}$ contenant $\mathbb{L}_1$ et $\mathbb{L}_2$, c'est-à-dire

$$\mathbb{L}_1\mathbb{L}_2 = \mathbb{L}_2(\mathbb{L}_1) = \mathbb{L}_1(\mathbb{L}_2).$$

**Exercice 5.** ③ *Soient $\mathbb{L}_1$ et $\mathbb{L}_2$ deux sous-corps d'un corps $\mathbb{L}$.*

*a) Montrer que si $(e_i)_{i\in I}$ engendre le $\mathbb{L}_1 \cap \mathbb{L}_2$-espace vectoriel $\mathbb{L}_1$, elle engendre le $\mathbb{L}_2$-espace vectoriel $\mathbb{L}_1\mathbb{L}_2$.*

*b) En déduire que, si l'extension $\mathbb{L}_1/(\mathbb{L}_1 \cap \mathbb{L}_2)$ est finie, il en est de même de $\mathbb{L}_1\mathbb{L}_2/\mathbb{L}_2$, avec*

$$[\mathbb{L}_1\mathbb{L}_2 : \mathbb{L}_2] \leq [\mathbb{L}_1 : \mathbb{L}_1 \cap \mathbb{L}_2].$$

**Exercice 6.** ④ *Soient $\mathbb{L}$ un corps, $\mathbb{K}$ un sous-corps de $\mathbb{L}$, $\mathbb{L}_1$ et $\mathbb{L}_2$ deux sous-corps de $\mathbb{L}$ qui sont des extensions finies de $\mathbb{K}$, $(e_i)_{i\in I}$ une base de $\mathbb{L}_1$ sur $\mathbb{K}$.*

*a) Montrer que*

$$[\mathbb{L}_1\mathbb{L}_2 : \mathbb{K}] \leq [\mathbb{L}_1 : \mathbb{K}]\,[\mathbb{L}_2 : \mathbb{K}],$$

*avec égalité si et seulement si $(e_i)_{i\in I}$ est une base de $\mathbb{L}_1\mathbb{L}_2$ sur $\mathbb{L}_2$.*[4]

*b) Montrer que, si $[\mathbb{L}_1 : \mathbb{K}]$ et $[\mathbb{L}_2 : \mathbb{K}]$ sont premiers entre eux, l'égalité de a) est réalisée.*

*c) Montrer que, si l'égalité de a) est réalisée, $\mathbb{L}_1 \cap \mathbb{L}_2 = \mathbb{K}$.*

## 1.3 Sous-algèbres monogènes, algébricité et transcendance

Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre, $x$ un élément de $\mathbb{A}$. Considérons le morphisme de $\mathbb{K}$-algèbres :

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

L'image de $\delta_x$ est

$$\mathbb{K}[x] = \{P(x)\ ;\ P \in \mathbb{K}[X]\}\,.$$

C'est, au sens de l'inclusion, la plus petite $\mathbb{K}$-sous-algèbre de $\mathbb{A}$ contenant $x$.

Le noyau $I_{\mathbb{K},x}$ de $\delta_x$ est l'*idéal annulateur de $x$*. S'il est réduit à $\{0\}$, i.e. s'il n'existe pas de polynôme non nul $P$ de $\mathbb{K}[X]$ tel que $P(x) = 0$, $x$ est dit *transcendant* sur $\mathbb{K}$. Dans ce cas, $\delta_x$ est un isomorphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[X]$ sur $\mathbb{K}[x]$.

Sinon, $x$ est dit *algébrique* sur $\mathbb{K}$. L'idéal annulateur de $x$ est engendré par un unique polynôme unitaire de $\mathbb{K}[X]$, appelé *polynôme minimal* de $x$ sur $\mathbb{K}$ et noté $\Pi_{\mathbb{K},x}$. Le degré de ce polynôme est appelé *degré* de $x$ sur $\mathbb{K}$. Les annulateurs de $x$ dans $\mathbb{K}[X]$ sont donc les multiples de $P$ dans $\mathbb{K}[X]$.

La proposition suivante traduit une idée essentielle :

**algébricité = finitude**.

**Proposition 2.** *Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre, $x \in \mathbb{A}$.*

*(i) Si $x$ est transcendant sur $\mathbb{K}$, $(x^i)_{i\in\mathbb{N}}$ est une $\mathbb{K}$-base de $\mathbb{K}[x]$. En particulier, $\mathbb{K}[x]$ est de dimension infinie sur $\mathbb{K}$.*

*(ii) Si $x$ est algébrique de degré $n$ sur $\mathbb{K}$, alors $(x^i)_{0\leq i\leq n-1}$ est une $\mathbb{K}$-base de $\mathbb{K}[x]$. En particulier, $\mathbb{K}[x]$ est de dimension $n$ sur $\mathbb{K}$.*

4. On dit dans ce cas que les extensions $\mathbb{L}_1/\mathbb{K}$ et $\mathbb{L}_2/\mathbb{K}$ sont *linéairement disjointes*. Cette propriété se reformule mieux en termes de produit tensoriel.

*Preuve.* Dans tous les cas, la famille $(x^i)_{i\in\mathbb{N}}$ engendre le $\mathbb{K}$-espace vectoriel $\mathbb{K}[x]$. Si $x$ est transcendant, il n'existe pas de polynôme non nul de $\mathbb{K}[X]$ annulant $x$, ce qui signifie exactement que la famille $(x^i)_{i\in\mathbb{N}}$ est libre.

Supposons $x$ algébrique de degré $n$ sur $\mathbb{K}$. Par définition de $\Pi_{\mathbb{K},x}$, $I_{\mathbb{K},x} \cap \mathbb{K}_{n-1}[X] = \{0\}$, d'où la liberté de $\left(1, x, \ldots, x^{n-1}\right)$. Soit ensuite $y \in \mathbb{K}[x] : y = P(x)$, où $P \in \mathbb{K}[X]$. Notant $R$ le reste de la division euclidienne de $P$ par $\Pi_{\mathbb{K},x}$, on a $y = R(x)$, et $R \in \mathbb{K}_{n-1}[X]$. Ceci montre que $y$ est combinaison $\mathbb{K}$-linéaire de $1, x, \ldots, x^{n-1}$.

**Corollaire 2.** *Si $\mathbb{A}$ est une $\mathbb{K}$-algèbre de dimension finie, tout élément de $\mathbb{A}$ est algébrique sur $\mathbb{K}$.*

**Exemples**

1. Les éléments de $\mathbb{A}$ algébriques de degré 1 sur $\mathbb{K}$ sont les scalaires, c'est-à-dire les éléments de la forme $\lambda 1$ où $\lambda \in \mathbb{K}$.
2. Si $M \in \mathcal{M}_n(\mathbb{K})$ est une matrice de projecteur qui n'est ni $0_n$ ni $I_n$,
$$\Pi_{\mathbb{K},M} = X^2 - X = X(X-1).$$
3. Un nombre complexe irréel $z$ est de degré 2 sur $\mathbb{R}$, avec
$$\Pi_{\mathbb{R},z} = (X - z)\,(X - \overline{z}).$$

**Remarques**

1. *Indépendance algébrique*
   Soient $n \in \mathbb{N}^*$, $x_1, \ldots, x_n$ des éléments de la $\mathbb{K}$-algèbre $\mathbb{A}$. On dit que $x_1, \ldots, x_n$ sont *algébriquement indépendants sur* $\mathbb{K}$ si $x_1, \ldots, x_n$ ne vérifient aucune équation algébrique à coefficients dans $\mathbb{K}$, i.e. si le seul $P$ de $\mathbb{K}[X_1, \ldots, X_n]$ tel que $P(x_1, \ldots, x_n) = 0$ est $P = 0$, i.e. si l'application
   $$P \in \mathbb{K}[X_1, \ldots, X_n] \longmapsto P(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$$
   est un isomorphisme de $\mathbb{K}$-algèbres.

   Exemple. La partie « unicité » du théorème de structure des polynômes symétriques (chapitre **1**, **4.1**) assure que, si $X_1, \ldots, X_n$ sont des indéterminées indépendantes, les polynômes symétriques $\Sigma_1, \ldots, \Sigma_n$ sont algébriquement indépendants sur $\mathbb{K}$.
2. *L'équation générale de degré $n$*
   Soit $n \in \mathbb{N}^*$. On appelle *polynôme général de degré $n$ sur $\mathbb{K}$* tout polynôme $P$ de la forme
   $$\prod_{i=1}^{n}(T - x_i)$$
   où $x_1, \ldots, x_n$ sont des éléments d'un surcorps de $\mathbb{K}$ algébriquement indépendants sur $\mathbb{K}$ et $T$ une indéterminée. D'après la remarque 1, il revient au même de dire que $P$ est de la forme
   $$T^n + \sum_{k=0}^{n} a_k T^k$$
   où $a_0, \ldots, a_{n-1}$ sont des éléments d'un surcorps de $\mathbb{K}$ algébriquement indépendants sur $\mathbb{K}$. Autrement dit, un polynôme général de degré $n$ est un polynôme dont les coefficients (ou les racines) ne vérifient aucune équation algébriques non triviale à coefficients dans $\mathbb{K}$.

## 1.4 Cas d'une algèbre intègre

Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre, $P \in \mathbb{K}[X]$ irréductible unitaire, $x \in \mathbb{A}$ annulé par $x$. Nécessairement :

$$\Pi_{\mathbb{K},x} = P.$$

Dans le cas général, le polynôme minimal d'un élément algébrique n'est pas forcément irréductible : si $P$ est un polynôme unitaire de degré $n$, $P$ est le polynôme minimal de sa matrice compagnon, ou, plus conceptuellement, de la classe de $X$ dans la $\mathbb{K}$-algèbre $\mathbb{K}[X]/(P)$. Mais tel est cependant le cas si $\mathbb{A}$ est intègre, en particulier si $\mathbb{A}$ est un corps.

**Proposition 3.** *Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre intègre, $x$ un élément de $\mathbb{A}$, algébrique sur $\mathbb{K}$. Alors $\Pi_{\mathbb{K},x}$ est irréductible sur $\mathbb{K}$.*

*Preuve.* Si $\Pi_{\mathbb{K},x}$ n'est pas irréductible, il s'écrit produit de deux polynômes non constants. L'un au moins de ces deux polynômes annule $x$, contredisant la minimalité du degré de $\Pi_{\mathbb{K},x}$.

L'étude des irréductibles de $\mathbb{K}[X]$ et celle des éléments de surcorps de $\mathbb{K}$ algébriques sur $\mathbb{K}$ sont donc deux façons d'aborder un même sujet.

**Exemples**

1. Le réel $\sqrt[n]{2}$ est de degré $n$ sur $\mathbb{Q}$ et
$$\Pi_{\mathbb{Q},\sqrt[n]{2}} = X^n - 2.$$
2. Soit $n \in \mathbb{N}^*$. L'irréductibilité de $\Phi_n$ sur $\mathbb{Q}$, énoncée dans le chapitre **1** et démontrée un peu plus loin, se reformule en l'égalité
$$\Pi_{\mathbb{Q},e^{2i\pi/n}} = \Phi_n.$$
3. Puisque $\mathbb{Q}[X]$ est dénombrable et qu'un polynôme non nul admet un nombre fini de racines, l'ensemble des nombres complexes algébriques est au plus dénombrable. La « plupart » des nombres réels et complexes sont donc transcendants.
4. On démontre que $e$ et $\pi$ sont transcendants sur $\mathbb{Q}$. Ces résultats sont dûs respectivement à Hermite (1873) et Lindemann (1882).
5. (*) Soient $\mathbb{K}$ un corps, $F \in \mathbb{K}(X)$ non constante. On écrit $F = \dfrac{A}{B}$ où $A$ et $B$ sont dans $\mathbb{K}[X]$ et $A \wedge B = 1$. Alors $X$ est algébrique de degré $m = \max\{\deg A, \deg B\}$. sur $\mathbb{K}(F)$. [5]

   En effet, l'indéterminée $X$ est racine du polynôme $A(T) - FB(T)$ de $\mathbb{K}(F)[T]$. Reste à voir que $A(T) - FB(T)$ est irréductible sur $\mathbb{K}(F)$. Comme $\mathbb{K}[F]$ est principal (car $F$ est transcendant sur $\mathbb{K}$), donc factoriel, il suffit de voir que $A(T) - FB(T)$ est un irréductible de $\mathbb{K}[F][T]$. Or $\mathbb{K}[F][T] = \mathbb{K}[T][F]$. Comme polynôme en $F$, $A(T) - FB(T)$ est de degré 1 et de contenu $A(T) \wedge B(T) = 1$, ce qui achève la démonstration.
6. *Entiers algébriques*
   Supposons $\mathbb{K} = \mathbb{Q}$. On dit que $x$ est un *entier algébrique* s'il annule un polynôme $P$ de $\mathbb{Z}[X]$ unitaire. On déduit du théorème 4 du chapitre **1** (**2.4**) le fait suivant, dont nous donnerons une autre démonstration dans la remarque 2 de **5.1**.

   **Lemme 1.** *Soit $x$ un nombre complexe algébrique sur $\mathbb{Q}$. Alors $x$ est un entier algébrique si et seulement si $\Pi_{\mathbb{Q},x}$ appartient à $\mathbb{Z}[X]$.*

5. La démonstration qui suit utilise l'extension du lemme de Gauss sur les contenus à $\mathbb{K}[X]$ ; le résultat vaut en fait sur un anneau factoriel, en particulier sur un anneau principal.

*Preuve.* Il suffit de montrer que, si le polynôme unitaire $P \in \mathbb{Z}[X]$ annule $x$, alors $\Pi_{\mathbb{Q},x}$ appartient à $\mathbb{Z}[X]$. Le théorème 4 du chapitre **1** (**2.2**) montre qu'il existe $\Pi \in \mathbb{Z}[X]$ associé à $\Pi_{\mathbb{Q},x}$ et divisant $P$ dans $\mathbb{Z}[X]$. Comme $P$ est unitaire, l'un des deux polynômes $\pm\Pi$ l'est aussi. Il en résulte que $\Pi_{\mathbb{Q},x} = \pm\Pi$ est dans $\mathbb{Z}[X]$.

**Exercice 7.** ② *Soit $x = \sqrt{2+\sqrt{3}}$. Montrer que $x$ est algébrique sur $\mathbb{Q}$, déterminer $\Pi_{\mathbb{Q},x}$.*

**Exercice 8.** ② *Soit $x = \sqrt{2}+\sqrt{3}$. Montrer que $x$ est algébrique sur $\mathbb{Q}$, déterminer $\Pi_{\mathbb{Q},x}$.*

**Exercice 9.** ① *Soit $r \in \mathbb{Q}$. Montrer que $\cos(2\pi r)$ et $\sin(2\pi r)$ sont algébriques sur $\mathbb{Q}$.*

**Exercice 10.** ③ *Soit $x = \sqrt[3]{2+\sqrt{2}}$. Montrer que $x$ est algébrique sur $\mathbb{Q}$, déterminer $\Pi_{\mathbb{Q},x}$.*

**Exercice 11.** ③ *Soit $P \in \mathbb{K}[X]$ de degré $n$. Montrer que $P$ est irréductible sur $\mathbb{K}$ si et seulement si, pour toute extension finie $\mathbb{L}$ de $\mathbb{K}$ telle que $[\mathbb{L}:\mathbb{K}] \leq \dfrac{n}{2}$, $P$ n'a pas de racine dans $\mathbb{L}$.*

**Exercice 12.** ③ *Soit $x \in \overline{\mathbb{Q}}$. Montrer qu'il existe un unique $P \in \mathbb{Z}[X]$ de coefficient dominant strictement positif tel que*

$$\{Q \in \mathbb{Z}[X]\ ;\ Q(x) = 0\} = P\,\mathbb{Z}[X].$$

*Vérifier que $P$ est irréductible sur $\mathbb{Q}$ et primitif.* [6]

## 1.5 Inversibles d'une algèbre monogène

La proposition ci-après décrit les inversibles d'une algèbre monogène.

**Proposition 4.** *Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre, $x \in \mathbb{A}$.*

*(i) Si $x$ est transcendant sur $\mathbb{K}$, les inversibles de $\mathbb{K}[x]$ sont les scalaires non nuls.*

*(ii) Si $x$ est algébrique sur $\mathbb{K}$ et si $P \in \mathbb{K}[X]$, l'élément $P(x)$ de $\mathbb{K}[x]$ est inversible dans $\mathbb{K}[x]$ si et seulement si $P \wedge \Pi_{\mathbb{K},x} = 1$.*

*(iii) En particulier, $\mathbb{K}[x]$ est un corps si et seulement si $x$ est algébrique sur $\mathbb{K}$ et $\Pi_{\mathbb{K},x}$ irréductible sur $\mathbb{K}$.*

*Preuve.* Si $x$ est transcendant sur $\mathbb{K}$, $\delta_x$ est un isomorphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[X]$ sur $\mathbb{K}[x]$. Comme les inversibles de $\mathbb{K}[X]$ sont les scalaires non nuls, on en déduit le premier point.

Supposons maintenant $x$ algébrique sur $\mathbb{K}$. Posons $y = P(x)$. Dire que $y$ est inversible dans $\mathbb{K}[x]$, c'est dire qu'il existe $U \in \mathbb{K}[X]$ tel que

$$U(x)P(x) = 1, \qquad \text{i.e.} \qquad \Pi_{\mathbb{K},x} \mid UP - 1,$$

ou encore qu'il existe $U$ et $V$ dans $\mathbb{K}[X]$ tels que :

$$UP + V\Pi_{\mathbb{K},x} = 1, \text{ i.e.} \quad P \wedge \Pi_{\mathbb{K},x} = 1.$$

Le dernier point découle simplement du fait que, si $\Pi$ est un élément non constant de $\mathbb{K}[X]$, il y a équivalence entre les deux assertions :

- les éléments de $\mathbb{K}[X]$ non divisibles par $\Pi$ sont premiers à $\Pi$ ;
- le polynôme $\Pi$ est irréductible sur $\mathbb{K}$.

6. Le polynôme $P$ est unitaire si et seulement si $x$ est un entier algébrique.

**Remarques**

1. *Reformulation en termes d'anneau-quotient*
   En considérant le morphisme $\delta_x$, on obtient le

   **Lemme 2.** *Si $x$ est algébrique sur $\mathbb{K}$, la $\mathbb{K}$-algèbre $\mathbb{K}[x]$ est isomorphe à $\mathbb{K}[X]/(\Pi_{\mathbb{K},x})$.*

   On retrouve la proposition 4 : si $\Pi_{\mathbb{K},x}$ est irréductible dans l'anneau principal $\mathbb{K}[X]$, l'idéal qu'il engendre est maximal, et le quotient de $\mathbb{K}[X]$ par cet idéal est un corps.
2. *Une autre démonstration*
   Que $\mathbb{K}[x]$ soit un corps si $\mathbb{L}/\mathbb{K}$ est une extension de corps et $x$ un élément de $\mathbb{L}$ algébrique sur $\mathbb{K}$ est également une conséquence du lemme ci-après.

   **Lemme 3.** *Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre commutative de dimension finie, $x$ un élément de $\mathbb{A}$ non diviseur de zéro. Alors $x$ est inversible dans $\mathbb{A}$.*

   *En particulier, si $\mathbb{A}$ est intègre, $\mathbb{A}$ est un corps.*

   *Preuve.* Soit $\mu_x$ l'application de $\mathbb{A}$ dans $\mathbb{A}$ définie par

   $$\forall a \in \mathbb{A}, \qquad \mu_x(a) = ax.$$

   Alors $\mu_x$ est un endomorphisme du $\mathbb{K}$-espace vectoriel de dimension finie $\mathbb{A}$. L'hypothèse fait que $\mu_x$ est injectif : il est donc bijectif.
3. *Effectivité*
   La preuve de *(ii)* donne un moyen effectif de calculer l'inverse d'un élément inversible de $\mathbb{K}[x]$ : il suffit d'écrire une relation de Bézout. L'argument donné dans la démonstration du lemme 3 peut être rendu effectif (résolution d'un système linéaire).

**Exercice 13.** ② *Soit $x = 1 + \sqrt[3]{2} - (\sqrt[3]{2})^2$. Calculer l'inverse de $x$ dans $\mathbb{Q}(\sqrt[3]{2})$.*

**Exercice 14.** ③ *Soit $\mathbb{A}$ une $\mathbb{K}$-algèbre. Quels sont les $x \in \mathbb{A}$ tels que le seul élément nilpotent de $\mathbb{K}[x]$ soit 0 ?*

**Exercice 15.** ③ *On suppose que l'élément $x$ de la $\mathbb{K}$-algèbre $\mathbb{A}$ est algébrique sur $\mathbb{K}$. Décrire et dénombrer les idéaux de $\mathbb{K}[x]$.*

**Exercice 16.** ③ *Soit $z$ un nombre complexe algébrique sur $\mathbb{Q}$. Montrer qu'il existe un unique polynôme primitif de $\mathbb{Z}[X]$ de coefficient dominant positif, irréductible sur $\mathbb{Q}$ et tel que $P(z) = 0$. Montrer que les polynômes de $\mathbb{Z}[X]$ qui annulent $z$ sont les multiples de $P$.*

Des propositions 2 et 4, on tire deux caractérisations des éléments algébriques d'une extension.

**Corollaire 3.** *Soient $\mathbb{L}/\mathbb{K}$ une extension de corps, $x \in \mathbb{L}$. Il y a équivalence entre :*

*(i) l'élément $x$ est algébrique sur $\mathbb{K}$ ;*

*(ii) la $\mathbb{K}$-algèbre $\mathbb{K}[x]$ est un corps, i.e. $\mathbb{K}[x] = \mathbb{K}(x)$ ;*

*(iii) la $\mathbb{K}$-algèbre $\mathbb{K}[x]$ est de dimension finie ;*

*(iv) il existe une $\mathbb{K}$-sous-algèbre de $\mathbb{L}$ de dimension finie sur $\mathbb{K}$ et contenant $x$.*

**Exercice 17.** ③ *Soit $P = X^3 - X^2 - 2X + 1$.*

*a) Montrer que $P$ possède trois racines réelles distinctes $\theta_1, \theta_2, \theta_3$.*

*b) Montrer que les racines de $P$ sont irrationnelles.*

*c) Soit $\theta$ une racine de $P$. Calculer le degré de $\theta$ sur $\mathbb{Q}$.*

*d) Montrer, si $\theta$ est racine de $P$, que $2 - \theta^2$ est racine de $P$.*

*e) Comparer les corps $\mathbb{Q}(\theta_1)$, $\mathbb{Q}(\theta_2)$ et $\mathbb{Q}(\theta_3)$.*

## 1.6 (*) Polynômes cyclotomiques (II)

Nous allons utiliser la notion de polynôme minimal pour établir le résultat suivant, énoncé et démontré dans un cas particulier dans le chapitre **1**.

**Théorème 2.** *Soit $n \in \mathbb{N}^*$. Le polynôme $\Phi_n$ est irréductible sur $\mathbb{Q}$.*

*Preuve. Étape 1.* Nous allons montrer que, si $\omega$ est une racine primitive $n$-ième de l'unité et $k$ un entier naturel premier à $n$, alors

$$(1) \qquad \Pi_{\mathbb{Q},\omega}(\omega^k) = 0.$$

Il en résultera que $\Pi_{\mathbb{Q},e^{2i\pi/n}}$ annule toutes les racines primitives $n$-ièmes de 1, donc est divisible par $\Phi_n$. L'irréductibilité de $\Pi_{\mathbb{Q},e^{2i\pi/n}}$ permettra de conclure.

Pour établir (1), il suffit de montrer que, pour tout $\omega$ racine primitive $n$-ième de 1 et tout nombre premier $p$ ne divisant pas $n$, on a

$$(2) \qquad \Pi_{\mathbb{Q},\omega} = \Pi_{\mathbb{Q},\omega^p}.$$

Comme un entier naturel $k$ premier à $n$ est produit de nombres premiers ne divisant pas $n$, il suffit en effet d'appliquer (2) de manière répétée pour établir (1).

*Étape 2.* Prouvons donc cette dernière assertion. Soient $\omega$ une racine primitive $n$-ième de 1, $p$ un nombre premier ne divisant pas $n$. Comme $\omega$ et $\omega^p$ sont entiers algébriques, $\Pi_{\mathbb{Q},\omega}$ et $\Pi_{\mathbb{Q},\omega^p}$ sont dans $\mathbb{Z}[X]$ grâce au lemme 1 (**1.4**). Comme $\Pi_{\mathbb{Q},\omega^p}(X^p)$ annule $\omega$, le caractère unitaire de $\Pi_{\mathbb{Q},\omega}$ donne $Q \in \mathbb{Z}[X]$ tel que

$$(3) \qquad \Pi_{\mathbb{Q},\omega^p}(X^p) = \Pi_{\mathbb{Q},\omega}(X)\, Q(X).$$

Notons

$$U \in \mathbb{Z}[X] \longmapsto \overline{U} \in \mathbb{F}_p[X]$$

le morphisme de réduction modulo $p$. La réduction modulo $p$ de $U(X^p)$ est donc $\overline{U}^p$ (morphisme de Frobenius) et (3) entraîne

$$(4) \qquad \overline{\Pi_{\mathbb{Q},\omega^p}}^p = \overline{\Pi_{\mathbb{Q},\omega}}\ \overline{Q}.$$

Supposons donc, par l'absurde, que (2) soit fausse. Alors $\Pi_{\mathbb{Q},\omega}$ et $\Pi_{\mathbb{Q},\omega^p}$ sont deux diviseurs distincts de $X^n - 1$, donc leur produit divise $X^n - 1$ dans $\mathbb{Z}[X]$. Le produit de leurs réductions modulo $p$ divise donc $X^n - \overline{1}$. Grâce à (4), il s'ensuit que toute racine de $\overline{\Pi_{\mathbb{Q},\omega}}$ dans une extension de $\mathbb{F}_p$ est racine double de $X^n - \overline{1}$. Mais, comme $p \wedge n = 1$, $X^n - 1$ est séparable, contradiction.

**Exercice 18.** ② *Montrer, sans utiliser d'extension de $\mathbb{K}$, que, si $P \in \mathbb{K}[X]$ est premier à $P'$, $P$ n'est divisible par aucun carré non constant de $\mathbb{K}[X]$.*

**Exercice 19.** ④ *Montrer que $\varphi(n)$ tend vers $+\infty$ avec $n$. En déduire que, si $\mathbb{K}$ est un corps de nombres, le groupe de torsion de $\mathbb{K}^*$ est fini.*

**Exercice 20.** ④ *Pour $\ell \in \mathbb{N}^*$, notons $\mathbb{K}_\ell = \mathbb{Q}\left(\exp\left(\dfrac{2i\pi}{\ell}\right)\right)$. Soient $m$ et $n$ deux éléments de $\mathbb{N}^*$. Montrer que $\mathbb{K}_m \cap \mathbb{K}_n = \mathbb{K}_{m\wedge n}$ et que $\mathbb{K}_m\mathbb{K}_n = \mathbb{K}_{m\vee n}$.*

**Exercice 21.** ④ *Soit $n \geq 3$ un entier. Déterminer le groupe de torsion de $\mathbb{K}_n$ (notations de l'exemple précédent).*

**Exercice 22.** ④ *a) Soient $n \geq 3$ un entier et $k$ un entier premier à $n$, calculer les degrés sur $\mathbb{Q}$ de $\cos\left(\frac{2k\pi}{n}\right)$ et de $\sin\left(\frac{2k\pi}{n}\right)$.*

*b) Quel est le degré sur $\mathbb{Q}$ de $\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}$ ($n$ radicaux) ?*

**Exercice 23.** ⑤ *Si $n \in \mathbb{N}^*$, soit $T_n$ le $n$-ième polynôme de Tchébychev, défini par :*

$$\forall \theta \in \mathbb{R}, \qquad T_n(\cos\theta) = \cos(n\theta).$$

*On rappelle que $T_n$ est dans $\mathbb{Z}[X]$, de degré $n$, de coefficient dominant $2^{n-1}$. Posant, pour $m$ dans $\mathbb{N}^*$, $\psi_m = \Pi_{\mathbb{Q},\cos(2\pi/m)}$, décomposer $\dfrac{T_n}{2^{n-1}}$ en produit de polynômes de la forme $\psi_m$.*

# 2 Extensions finies, extensions algébriques

Dans toute cette section, $\mathbb{L}/\mathbb{K}$ est une extension de corps. Nous allons constater l'efficacité du point de vue linéaire.

## 2.1 Sommes et produits d'éléments algébriques

**Proposition 5.** *Soient $x$ et $y$ deux éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$, de degrés respectifs $m$ et $n$. Alors $\mathbb{K}(x,y)/\mathbb{K}$ est de degré fini majoré par $mn$.*

*En particulier, $x+y$ et $xy$ sont algébriques sur $\mathbb{K}$ de degré d'algébricité majoré par $mn$.*

*Preuve.* Puisque $\Pi_{\mathbb{K}(x),y}$ divise $\Pi_{\mathbb{K},y}$, $y$ est de degré au plus $n$ sur $\mathbb{K}(x)$, d'où le premier point par transitivité des extensions finies et multiplicativité des degrés. Le second point se déduit du premier, des inclusions

$$\mathbb{K}(x+y) \subset \mathbb{K}(x,y), \qquad \mathbb{K}(xy) \subset \mathbb{K}(x,y)$$

et de la traduction de l'algébricité comme propriété de finitude. La démonstration se résume en les diagrammes suivants

$$\begin{array}{ccc} \mathbb{K} & \underset{m}{\longrightarrow} & \mathbb{K}(x) \\ n\big\downarrow & \searrow & \big\downarrow n' \leq n \\ \mathbb{K}(y) & \underset{m' \leq m}{\longrightarrow} & \mathbb{K}(x,y) \end{array}$$

$$\mathbb{K} \longrightarrow \mathbb{K}(x+y) \longrightarrow \mathbb{K}(x,y) \quad \text{et} \quad \mathbb{K} \longrightarrow \mathbb{K}(xy) \longrightarrow \mathbb{K}(x,y).$$

**Remarques et applications**

1. *Annulateur d'une somme ou d'un produit via le théorème des polynômes symétriques*
   La preuve précédente ne fournit pas d'annulateur de $x+y$ ou de $xy$. Voici un moyen d'en calculer un. Soient $P$ et $Q$ dans $\mathbb{K}[X]$, unitaires, annulant respectivement $x$ et $y$. Écrivons :

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

où les $x_i$ et les $y_j$ appartiennent à une extension adéquate $\mathbb{L}$ de $\mathbb{K}$. Alors

$$S = \prod_{1\leq i\leq n,\ 1\leq j\leq m} (X - (x_i + y_j))$$

annule $x + y$. D'autre part, le théorème des polynômes symétriques (ou, plus précisément, le corollaire 3 du chapitre **1** (**4.1**, appliqué à chaque coefficient de $U$ ci-après) entraîne que

$$U = \prod_{j=1}^{m} P(X - y_j) \in \mathbb{K}[X].$$

On procède de même pour $xy$, en considérant

$$T = \prod_{1\leq i\leq n,\ 1\leq j\leq m} (X - x_i\ y_j)\,.$$

En effet, sous réserve que les $y_j$ soient non nuls, ce qui ne nuit pas à la généralité, on écrit

$$T = \left(\prod_{j=1}^{m} y_j\right)^n \prod_{j=1}^{m} P\left(\frac{X}{y_j}\right)$$

et on note que $\displaystyle\prod_{j=1}^{m} y_j$ est dans $\mathbb{K}$ (Viète) alors que, grâce au théorème des polynômes symétriques

$$V = \prod_{j=1}^{m} P\left(\frac{X}{y_j}\right) \in \mathbb{K}[X].$$

Ces arguments, historiquement antérieurs à ceux fondés sur l'algèbre linéaire, établissent la version « effective » ci-après de la proposition 5.

**Proposition 6.** *Si $x$ et $y$ sont des éléments d'une extension $\mathbb{L}$ de $\mathbb{K}$, si $\mathbb{M}$ est une extension de $\mathbb{L}$ scindant $\Pi_{\mathbb{K},x}\ \Pi_{\mathbb{K},y}$, alors $\Pi_{\mathbb{K},x+y}$ (resp. $\Pi_{\mathbb{K},xy}$) est scindé sur $\mathbb{M}$ et ses racines sont de la forme $x'+y'$ (resp. $x'y'$) où $x'$ (resp. $y'$) est une racine de $\Pi_{\mathbb{K},x}$ (resp. $\Pi_{\mathbb{K},y}$) dans $\mathbb{M}$.*

2. *(*) Avec le résultant*

   Reprenons les notation de la remarque 1. Soit $T$ une indéterminée indépendante de $X$, $\mathbb{A}$ l'anneau $\mathbb{K}[T]$, $R(T)$ le résultant de $(P(T - X), Q(X))$, qui est un élément de $\mathbb{A}$. Si $R(T) = \mathrm{Res}(P(T - X), Q(X))$, $R$ est dans $\mathbb{K}[T]$. D'autre part, si $t$ est un élément d'une extension $\mathbb{L}$ de $\mathbb{K}$, on a l'égalité dans $\mathbb{L}$ :

   $$R(t) = \mathrm{Res}(P(t - X), Q(X)).\ ^{7}$$

   Comme $P(x + y - X)$ et $Q(X)$ admettent $y$ comme racine commune, $R(x + y) = 0$. On obtient ainsi un annulateur de $x + y$ à coefficients dans $\mathbb{K}$.

7. Plus généralement, soient $\mathbb{A}_1$ et $\mathbb{A}_2$ deux anneaux intègres, $\varphi$ un morphisme de $\mathbb{A}_1$ dans $\mathbb{A}_2$, dont on note encore $\varphi$ l'extension en un morphisme de $\mathbb{A}_1[T]$ dans $\mathbb{A}_2[T]$. Il résulte immédiatement de l'expression du résultant que, si $P$ et $Q$ sont deux éléments unitaires de $\mathbb{A}_1[T]$,

$$\mathrm{Res}(\varphi(P), \varphi(Q)) = \varphi(\mathrm{Res}(P, Q)).$$

On applique cette remarque à $\mathbb{A}_1 = \mathbb{L}[T], \mathbb{A}_2 = \mathbb{L}, \varphi = \delta_t$.

Explicitons. Si $P = \sum_{k=0}^{m} p_k X^k, Q = \sum_{k=0}^{n} q_k X^k$,

$$P(T-X) = \sum_{k=0}^{m} p_k (T-X)^k = \sum_{k=0}^{m} \Pi_k(T) X^k,$$

où $\Pi_k \in \mathbb{K}_{m-k}[T]$ pour $0 \leq k \leq m$ et $\Pi_0 = P(-T)$, alors

$$R(T) = \det \begin{pmatrix} \Pi_m(T) & 0 & \cdots & \cdots & 0 & q_n & 0 & \cdots & 0 \\ \Pi_{m-1}(T) & \Pi_m(T) & \ddots & & \vdots & q_{n-1} & q_n & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & 0 \\ \Pi_1(T) & & \ddots & \ddots & 0 & \vdots & & \ddots & q_n \\ \Pi_0(T) & \ddots & & \ddots & \Pi_m(T) & q_1 & & & q_{n-1} \\ 0 & \ddots & \ddots & & \Pi_{m-1}(T) & q_0 & q_1 & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \Pi_1(T) & \vdots & \ddots & \ddots & q_1 \\ 0 & \cdots & \cdots & 0 & \Pi_0(T) & 0 & \cdots & 0 & q_0 \end{pmatrix}.$$

Il résulte de cette formule que $R$ est de degré $mn$, de coefficient dominant $(-1)^n {p_m}^n {q_n}^m$.

Par ailleurs, il découle de l'expression du résultant en fonction des racines (chapitre **1**, **4.4**, théorème 10) que

$$R(t) = (-1)^n {p_m}^n {q_n}^m \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (t - x_i - y_j).$$

On obtient donc *in fine* l'annulateur de $x+y$ explicité dans la remarque 1. Le discriminant a l'avantage d'être un déterminant à coefficients dans $\mathbb{K}[T]$. Bien sûr, une remarque analogue s'applique à $xy$.

3. *Encore une démonstration*

   On trouvera dans la section **5** deux démonstrations utilisant un peu plus d'algèbre linéaire (déterminants, Cayley-Hamilton) et donnant un résultat plus général, car applicable aux anneaux ; voir en particulier les théorèmes 11 et 12 de **5.3**.

4. *Sur le degré de $\mathbb{K}(x,y)$ sur $\mathbb{K}$*

   Avec les notations de la proposition 5, on a vu que $[\mathbb{K}(x,y) : \mathbb{K}]$ est majoré par $mn$. Par ailleurs, ce degré est multiple de $m$ et $n$ (car $\mathbb{K}(x,y)$ contient $\mathbb{K}(x)$ et $\mathbb{K}(y)$. Ainsi :

   $$m \wedge n = 1 \Longrightarrow [\mathbb{K}(x,y) : \mathbb{K}] = mn.$$

5. *(*) Une application des extensions à l'irréductibilité des binômes*

   Montrons par un exemple l'avantage qu'il peut y avoir à reformuler des questions d'irréductibilité en termes d'extensions. Soient $m$ et $n$ deux éléments de $\mathbb{N}^*$ premiers entre eux, $\mathbb{K}$ un corps, $a$ un élément de $\mathbb{K}$. Alors $X^m - a$ et $X^n - a$ sont irréductibles sur $\mathbb{K}$ si et seulement si $X^{mn} - a$ est irréductible sur $\mathbb{K}$.

Soit en effet $x$ une racine de $X^{mn}-a$ dans une extension de $\mathbb{K}$. Alors $x^m$ (resp. $x^n$) est une racine de $X^n-a$ (resp. $X^m-a$). Si $X^n-a$ et $X^m-a$ sont irréductibles sur $\mathbb{K}$, $x^m$ (resp. $x^n$) est de degré $n$ (resp. $m$) sur $\mathbb{K}$. On a donc

$$[\mathbb{K}(x^m):\mathbb{K}]=n \quad \text{et} \quad [\mathbb{K}(x^n):\mathbb{K}]=m.$$

Ainsi, $[\mathbb{K}(x):\mathbb{K}]$ est divisible par $m$ et $n$, donc par $mn$. Le degré de $\Pi_{\mathbb{K},x}$ est donc supérieur ou égal à $mn$. Puisque $x$ annule $X^{mn}-a$, on a $X^{mn}-a=\Pi_{\mathbb{K},x}$ et $X^{mn}-a$ est irréductible sur $\mathbb{K}$. La réciproque est évidente. [8]

6. *(*) Inertie de l'irréductibilité d'un polynôme de degré $d$ par passage à une extension de degré premier à $d$*

   Soient $\mathbb{L}/\mathbb{K}$ une extension finie, $P$ un irréductible de $\mathbb{K}[X]$ de degré $d$ premier à $[\mathbb{L}:\mathbb{K}]$. Alors $P$ est irréductible sur $\mathbb{L}$.

   L'argument est analogue à celui de l'exemple 2. Soit en effet $x$ une racine de $P$ dans une extension de $\mathbb{L}$. Alors $[\mathbb{L}(x):\mathbb{K}]$ est multiple de $[\mathbb{K}(x):\mathbb{K}]=d$ et de $[\mathbb{L}:\mathbb{K}]$, donc de $d\,[\mathbb{L}:\mathbb{K}]$. Par ailleurs, le théorème de la base télescopique assure que $[\mathbb{L}(x):\mathbb{K}]\leq d\,[\mathbb{L}:\mathbb{K}]$. Il s'ensuit que $[\mathbb{L}(x):\mathbb{K}]=d\,[\mathbb{L}:\mathbb{K}]$, puis que $[\mathbb{L}(x):\mathbb{L}]=d$. C'est dire que $P$ est irréductible sur $\mathbb{L}$.

**Exercice 24.** ② *Soient $p_1,\dots,p_r$ des nombres premiers deux à deux distincts, $n$ leur produit, $a$ un élément de $\mathbb{K}$ qui n'est pour aucun $i$ de $\{1,\dots,r\}$ une puissance $p_i$-ième exacte dans $\mathbb{K}$. Montrer que $X^n-a$ est un irréductible de $\mathbb{K}[X]$. Réciproque ?*

**Exercice 25.** ③ *Montrer, par exemple en utilisant le résultant, que, si $x=\sqrt{2}+\sqrt[3]{3}$, alors le polynôme $T^6-6T^4-6T^3+12T^2-36T+1$ annule $x$.*

**Exercice 26.** ③ *Soient $P\in\mathbb{K}[X]$ irréductible de degré $n$, $Q\in\mathbb{K}[X]$ non constant, $U=P\circ Q$. Si $\Pi$ est un diviseur irréductible de $U$ dans $\mathbb{K}[X]$, montrer que le degré de $\Pi$ est un multiple de $n$.*

Si l'élément $x$ de $\mathbb{L}\setminus\{0\}$ est algébrique de degré $n$ sur $\mathbb{K}$, $X^n\Pi_{\mathbb{K},x}(1/X)$ annule $1/x$. De cette remarque et de la proposition 5, on déduit aussitôt l'énoncé suivant.

**Théorème 3.** *L'ensemble des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$ est un sous-corps de $\mathbb{L}$.*

En particulier, l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est un corps appelé *corps des nombres algébriques* et noté $\overline{\mathbb{Q}}$.

**Exercice 27.** ③ *Soient $x$ et $y$ deux éléments de $\mathbb{L}$. Montrer que $\Pi_{\mathbb{K},y}$ est irréductible sur $\mathbb{K}(x)$ si et seulement si $\Pi_{\mathbb{K},x}$ est irréductible sur $\mathbb{K}(y)$.*

**Exercice 28.** ③ *Soit $x\in\mathbb{L}$ algébrique sur $\mathbb{K}$ de degré impair. Montrer l'égalité : $\mathbb{K}(x)=\mathbb{K}(x^2)$.*

**Exercice 29.** ③ *Soient $m$ et $n$ deux éléments de $\mathbb{N}^*$. Montrer que $\Phi_n$ est irréductible sur $\mathbb{Q}(e^{2i\pi/m})$ si et seulement si $m\wedge n=1$.*

**Exercice 30.** ③ *On prend $\mathbb{K}=\mathbb{Q}, \mathbb{L}_1=\mathbb{Q}(\sqrt[3]{2}), L_2=\mathbb{Q}(j\sqrt[3]{2})$ où on note $j=\exp\left(\frac{2i\pi}{3}\right)$. Déterminer $[\mathbb{L}_1\mathbb{L}_2:\mathbb{K}]$ et $\mathbb{L}_1\cap\mathbb{L}_2$. Qu'en déduire relativement à la question c) de l'exercice 6 de* **1.2** *?*

**Exercice 31.** ③ *Soient $a$ et $b$ deux nombres réels algébriques tels que $a<b$, $P$ un polynôme à coefficients réels algébriques. Montrer que $\max\{P(x)\ ;\ x\in[a,b]\}$ est algébrique.*

8. Vahlen et Capelli ont déterminé les binômes $X^n-a$ irréductibles sur $\mathbb{K}$.

## 2.2 Extensions finies, algébriques

Les extensions finies sont décrites par le résultat suivant.

**Proposition 7.** *Les deux assertions suivantes sont équivalentes.*

*i) L'extension $\mathbb{L}/\mathbb{K}$ est finie.*

*ii) Il existe $n$ dans $\mathbb{N}^*$ et des éléments $x_1, \ldots, x_n$ de $\mathbb{L}$ algébriques sur $\mathbb{K}$ tels que*

$$\mathbb{L} = \mathbb{K}(x_1, \ldots, x_n).$$

*Preuve.* Pour *i) ⇒ ii)*, il suffit de prendre pour $x_1, \ldots, x_n$ une base de $\mathbb{L}$ sur $\mathbb{K}$. Pour *ii) ⇒ i)*, on procède par récurrence sur $n$ en utilisant la transitivité des extensions finies. Le diagramme est

$$\mathbb{K} \longrightarrow \mathbb{K}(x_1) \longrightarrow \mathbb{K}(x_1, x_2) \longrightarrow \ldots \longrightarrow \mathbb{K}(x_1, x_2, \ldots, x_n).$$

**Remarques**

1. *Cas des corps algébriquement clos*

   Les corps algébriquement clos sont ceux qui n'ont aucune extension finie non triviale.

   En effet, si $\mathbb{K}$ est un corps algébriquement clos, $\mathbb{L}/\mathbb{K}$ une extension finie et $x$ un élément de $\mathbb{L}$, alors $\Pi_{\mathbb{K},x}$ est un irréductible de $\mathbb{K}[X]$, donc de degré 1 : $x$ appartient à $\mathbb{K}$. Réciproquement, si $\mathbb{K}$ n'est pas algébriquement clos, on dispose de $P \in \mathbb{K}[X]$ irréductible sur $\mathbb{K}$ de degré n$\geq 2$ ; si $x$ est une racine de $P$ dans un extension de $\mathbb{K}$, $\mathbb{K}(x)/\mathbb{K}$ est une extension finie de degré $n$.[9]

2. *Cas du corps des nombres réels*

   Le corps $\mathbb{R}$ n'a (à isomorphisme près) que deux extensions finies ($\mathbb{R}$ et $\mathbb{C}$). En effet, soient $\mathbb{K}$ un corps extension finie non triviale de $\mathbb{R}$, $x$ un élément de $\mathbb{K} \setminus \mathbb{R}$. Alors $\Pi_{\mathbb{R},x}$ est de degré 2 sans racine réelle. Il en résulte que $[\mathbb{K} : \mathbb{R}] = 2$. D'autre part, la résolution de l'équation de degré 2 montre que $\mathbb{K}$ contient une racine carrée de $-1$, ce qui implique facilement que $\mathbb{K}$ est isomorphe à $\mathbb{C}$.

3. *Corps finis, corps des rationnels*

   L'étude des extensions finies des corps finis est facile : pour $n$ dans $\mathbb{N}^*$, un corps fini $\mathbb{K}$ a, à isomorphisme près, exactement une extension de degré $n$. L'étude des extensions finies de $\mathbb{Q}$ (i.e. des corps de nombres) est en revanche très complexe.

4. *Extensions quadratiques*

   Soient $a$ un élément de $\mathbb{K}$ non carré, $x$ une racine carrée de $a$ dans une extension. Alors $\mathbb{K}(x)$ est une extension de degré 2 (ou quadratique) de $\mathbb{K}$ que l'on note $\mathbb{K}(\sqrt{a})$.[10] Inversement, si $\mathbb{K}$ n'est pas de caractéristique 2 et si $\mathbb{L}$ est une extension de degré 2 de $\mathbb{K}$, il existe $a$ dans $\mathbb{K}$ tel que $\mathbb{L} = \mathbb{K}(\sqrt{a})$. Soit en effet $x \in \mathbb{L} \setminus \mathbb{K}$. Il est clair que $\mathbb{L} = \mathbb{K}(x)$. Mais, si $a$ est le discriminant du trinôme $\Pi_{\mathbb{K},x}$, la résolution de l'équation du second degré en caractéristique différente de 2 montre que $\mathbb{K}(x) = \mathbb{K}(\sqrt{a})$.

5. *(*) Égalité de deux extensions quadratiques*

   Supposons toujours $\mathbb{K}$ de caractéristique différente de 2, soient $a$ et $b$ deux éléments de $\mathbb{K}$ non carrés, $\sqrt{a}$ et $\sqrt{b}$ des racines carrées respectivement de $a$ et $b$ dans une même extension. Si $b/a$ est le carré d'un élément de $\mathbb{K}$, on a

   $$\mathbb{K}(\sqrt{a}) = \mathbb{K}(\sqrt{b}).$$

9. Cette seconde partie de l'argument repose sur l'existence d'un corps de rupture de $P$ sur $\mathbb{K}$, établie en **3.1**.
10. Notation cohérente, car $\mathbb{K}(\sqrt{a})$ ne dépend pas de la racine choisie.

Montrons réciproquement que, si $\mathbb{K}(\sqrt{a})$ et $\mathbb{K}(\sqrt{b})$ sont égaux, alors $b/a$ est un carré. En effet, si $(x, y) \in \mathbb{K}^2$ est tel que $x + y\sqrt{a}$ est une racine carrée de $b$ dans $\mathbb{K}(\sqrt{a})$, alors : $b = x^2 + ay^2$ et $2xy = 0$. Il est exclu que $y$ soit nul, d'où $x = 0$ et $b = ay^2$.

Les extensions quadratiques de $\mathbb{K}$ sont ainsi en bijection avec les éléments non nuls du groupe $\mathbb{K}^*/(\mathbb{K}^*)^2$.

**Exercice 32.** ② *Expliciter la fin de l'argument pour la remarque 2.*

**Exercice 33.** ④ *Donner un exemple de nombre réel $x$, algébrique de degré 3 sur $\mathbb{Q}$ et tel que $\mathbb{Q}(x)$ ne soit pas de la forme $\mathbb{Q}(\sqrt[3]{\alpha})$ avec $\alpha$ réel.*

**Exercice 34.** ③ *Supposons $\mathbb{K}$ de caractéristique 2. Montrer que les extensions quadratiques de $\mathbb{K}$ sont les $K(x)$ où $x$ est un élément d'une extension de $\mathbb{K}$ tel que $x \notin \mathbb{K}$ mais $x^2 + x \in \mathbb{K}$.*

L'exercice suivant étudie les extensions *multiquadratiques*, c'est-à-dire engendrées par un ensemble fini de racines carrées d'éléments du corps de base.

**Exercice 35.** ⑤ *a) Soient $\mathbb{K}$ un corps de caractéristique différente de 2, $\mathbb{L}/\mathbb{K}$ une extension, $u_1, \dots, u_m$ des éléments de $\mathbb{K}^*$ ayant des racines carrées notées respectivement $\sqrt{u_1}, \dots, \sqrt{u_m}$ dans $\mathbb{L}$. On pose $\mathbb{K}^{*2} = \{x^2,\ x \in \mathbb{K}^*\}$. Montrer que $[\mathbb{K}(\sqrt{u_1}, \dots, \sqrt{u_m}) : \mathbb{K}] = 2^m$ si et seulement si*

$$\forall (\alpha_1, \dots, \alpha_m) \in \mathbb{Z}^m, \quad u_1^{\alpha_1} \times \cdots \times u_m^{\alpha_m} \in \mathbb{K}^{*2} \iff \forall i \in \{1, \dots, m\},\ 2 \mid \alpha_i.$$

*b) Soient $p_1, \dots, p_m$ des nombres premiers distincts. Calculer :*

$$[\mathbb{Q}\left(\sqrt{p_1}, \dots, \sqrt{p_m}\right) : \mathbb{Q}].$$

L'exercice ci-après est un théorème de Springer sur la conservation de l'isotropie d'une forme quadratique par passage à une extension de degré impair.

**Exercice 36.** ⑤ *Soit $\mathbb{K}$ un corps.*

*a) Montrer que les conditions suivantes sont équivalentes.*

*i) Pour tout $r \in \mathbb{N}^*$,*

$$\left\{(x_1, \dots, x_r) \in \mathbb{K}^r\ ;\ \sum_{i=1}^{r} {x_i}^2 = 0\right\} = \{(0, \dots, 0)\}.$$

*ii) On ne peut pas écrire $-1$ comme somme de carrés d'éléments de $\mathbb{K}$.*

*b) On suppose que $\mathbb{K}$ vérifie les propriétés de la question précédente, que $\mathbb{L}/\mathbb{K}$ est finie de degré impair. Montrer que $\mathbb{L}$ vérifie aussi les propriétés de la question précédente.*

L'extension $\mathbb{L}/\mathbb{K}$ est dite *algébrique* si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$. Toute extension finie est algébrique. La réciproque est fausse : $\overline{\mathbb{Q}}/\mathbb{Q}$ est algébrique infinie (parce qu'il existe des nombres algébriques dont le degré sur $\mathbb{Q}$ est arbitrairement grand).

**Exercice 37.** ③ *Soient $\mathbb{L}/\mathbb{K}$ une extension algébrique et $\mathbb{A}$ un sous-anneau de $\mathbb{L}$ contenant $\mathbb{K}$. Montrer que $\mathbb{A}$ est un corps. Montrer que cette propriété caractérise les extensions algébriques.*

**Exercice 38.** ③ *Soient $\mathbb{K} = \mathbb{Q}(X)$, $\mathbb{K}_1 = \mathbb{Q}(X^2), \mathbb{K}_2 = \mathbb{Q}(X^2 - X)$. Déterminer $\mathbb{K}_0 = \mathbb{K}_1 \cap \mathbb{K}_2$. En déduire que $\mathbb{K}/\mathbb{K}_1$ et $\mathbb{K}/\mathbb{K}_2$ sont algébriques, mais que $\mathbb{K}/\mathbb{K}_0$ ne l'est pas.*

**Exercice 39.** ④ *Soient $\mathbb{K}$ un corps infini et $\mathbb{L}/\mathbb{K}$ une extension algébrique. Prouver que les ensembles $\mathbb{K}$ et $\mathbb{L}$ sont équipotents*[11]*, ce qui généralise l'argument de Cantor prouvant l'existence de nombres transcendants sur $\mathbb{Q}$.*

Terminons avec la transitivité de l'algébricité, héritée directement de celle de la finitude.

**Proposition 8.** *Soient $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ deux extensions de corps. Alors $\mathbb{M}/\mathbb{K}$ est algébrique si et seulement si $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ sont algébriques.*

*Preuve.* Supposons $\mathbb{M}/\mathbb{L}$ et $\mathbb{L}/\mathbb{K}$ algébriques. Soient $x \in \mathbb{M}$ et $\mathbb{K}'$ le sous-corps de $\mathbb{L}$ engendré par $\mathbb{K}$ et les coefficients de $\Pi_{\mathbb{L},x}$. L'extension $\mathbb{K}'/\mathbb{K}$ est finie et $x$ est algébrique sur $\mathbb{K}'$. L'extension $\mathbb{K}'(x)/\mathbb{K}$ est donc également finie ; a fortiori, $\mathbb{K}(x)/\mathbb{K}$ est finie et $x$ est algébrique sur $\mathbb{K}$. La réciproque est évidente.

De cette proposition, on déduit la conséquence ci-après, qui implique notamment que le corps $\overline{\mathbb{Q}}$ est donc algébriquement clos.

**Corollaire 4.** *Soient $\mathbb{K}$ un corps, $\Omega$ un surcorps algébriquement clos de $\mathbb{K}$, $\mathbb{L}$ l'ensemble des éléments de $\Omega$ algébriques sur $\mathbb{K}$. Alors $\mathbb{L}$ est un sous-corps algébriquement clos de $\Omega$.*

*Preuve.* On sait déjà que $\mathbb{L}$ est un sous-corps de $\Omega$. Soit $P$ dans $\mathbb{L}[X]$ unitaire non constant : $P = X^n + \sum_{i=0}^{n-1} a_i X^i$. Soit $x$ une racine de $P$ dans $\Omega$ : $x$ est algébrique sur $\mathbb{K}(a_0, \ldots, a_{n-1})$, qui est une extension finie de $\mathbb{K}$. Par transitivité, $x$ est algébrique sur $\mathbb{K}$, d'où $x \in \mathbb{L}$. Voici le diagramme correspondant :

$$\mathbb{K} \longrightarrow \mathbb{K}(a_0) \longrightarrow \mathbb{K}(a_0, a_1) \cdots \longrightarrow \mathbb{K}(a_0, a_1 \ldots, a_{n-1}) \longrightarrow \mathbb{K}(a_0, a_1 \ldots, a_{n-1}, x)$$

**Exercice 40.** ③ *Soient $\alpha$ une racine de $X^3 + X + 1$, $x$ une racine complexe de*

$$P = X^{11} - (\sqrt{2} + \sqrt{5})X^8 + 3\sqrt[4]{12}X^5 + (1 + 3i)X^3 + \alpha X + i\sqrt{6}X^2 + \sqrt[5]{7}.$$

*Montrer que $x$ est algébrique sur $\mathbb{Q}$ et que son degré divise* 10560.

**Exercice 41.** ② *Montrer que $\overline{\mathbb{Q}} = (\overline{\mathbb{Q}} \cap \mathbb{R})(i)$.*

Le problème d'effectivité abordé dans la remarque 1 après la proposition 5 de **2.1** se pose à nouveau à propos du corollaire 4 : si $a_0, \ldots, a_{n-1}$ sont algébriques sur $\mathbb{K}$ et si $x$ est une racine de $P = X^n + \sum_{i=0}^{n-1} a_i X^i$, comment produire un annulateur de $x$ à coefficients dans $\mathbb{K}$ ? On peut encore y répondre à l'aide du théorème des polynômes symétriques : c'est l'exercice ci-après.

**Exercice 42.** ③ *Avec ces notations, exhiber un polynôme unitaire de $\mathbb{K}[X]$ annulant $x$.*

**Exercice 43.** ② *Soient $n \in \mathbb{N}^*$, $(x_1, \ldots, x_n) \in \mathbb{C}^n$ tel que, pour tout $k \in \{1, \ldots, n\}$, $\sum_{i=1}^{n} {x_i}^k$ appartienne à $\overline{\mathbb{Q}}$. Montrer que $(x_1, \ldots, x_n) \in \overline{\mathbb{Q}}^n$.*

11. Cet exercice nécessite une bonne pratique de la notion d'équipotence.

## 2.3 Le théorème de l'élément primitif (I)

Le résultat suivant, intéressant en lui même, simplifie certaines démonstrations de la théorie de Galois et joue un rôle central dans les exposés classiques. [12]

**Théorème 4.** *Supposons $\mathbb{K}$ de caractéristique bulle et $\mathbb{L}/\mathbb{K}$ finie. Alors $\mathbb{L}/\mathbb{K}$ est monogène.*

*Preuve (Galois).* Par récurrence, on ramène la preuve au cas où $\mathbb{L} = \mathbb{K}(x, y)$. On se place dans cette situation et on factorise les polynômes $\Pi_{\mathbb{K},x}$ et $\Pi_{\mathbb{K},y}$ dans une extension adéquate $\Omega$ de $\mathbb{L}$ :

$$\Pi_{\mathbb{K},x} = \prod_{i=1}^{m} (X - x_i), \qquad \Pi_{\mathbb{K},y} = \prod_{i=1}^{n} (X - y_i),$$

avec $x_1 = x$, $y_1 = y$. Les $x_i$ (resp. $y_i$) sont deux à deux distincts. Le corps $\mathbb{K}$ étant infini, on dispose donc de $t \in \mathbb{K}$ tel que :

$$\forall (i, j) \in \{1, \dots, m\} \times \{1, \dots, n\}, \quad x + ty = x_i + ty_j \;\Rightarrow\; i = j = 1.$$

Soit alors $z = x + ty$. Bien sûr : $\mathbb{K}(z) \subset \mathbb{L}$. Pour établir l'inclusion réciproque, il suffit de prouver : $y \in \mathbb{K}(z)$ ; la forme de $z$ permet en effet d'en déduire $x \in \mathbb{K}(z)$, puis $\mathbb{K}(z) = \mathbb{K}(x, y)$.

Or, le choix de $t$ montre que les polynômes $\Pi_{\mathbb{K},y}(X)$ et $\Pi_{\mathbb{K},x}(z - tX)$, qui sont tous deux à coefficients dans $\mathbb{K}(z)$, ont $y$ pour seule racine commune dans $\Omega$, cette racine étant simple. Le pgcd $\Delta$ de ces deux polynômes vu dans $\Omega[X]$ est donc $X - y$. Par inertie du pgcd, il s'ensuit que $\Delta$ appartient à $\mathbb{K}(z)[X]$, et donc que $y$ appartient à $\mathbb{K}(z)$.

La preuve est constructive. Cherchons par exemple un élément primitif de $\mathbb{Q}(j, \sqrt[3]{2})$ sur $\mathbb{Q}$. La preuve précédente montre que, pour tout $t \in \mathbb{Q}$ tel que :

$$tj + \sqrt[3]{2},\ tj^2 + \sqrt[3]{2},\ tj + j\sqrt[3]{2},\ tj^2 + j\sqrt[3]{2},\ tj + j^2\sqrt[3]{2},\ tj^2 + j^2\sqrt[3]{2},$$

soient distincts, $tj + \sqrt[3]{2}$ est élément primitif de $Q\left(\sqrt[3]{2}, j\right)/\mathbb{Q}$. Exemple : $t = 1$.

**Exercice 44.** ② *Si $n \geq 2$ est un entier, montrer*

$$\mathbb{Q}(e^{2i\pi/n}, \sqrt[n]{2}) = \mathbb{Q}(e^{2i\pi/n} + \sqrt[n]{2}).$$

**Exercice 45.** ② *Soient $p_1, \dots, p_k$ des nombres premiers deux à deux distincts. Montrer que $\sqrt{p_1} + \cdots + \sqrt{p_k}$ est un élément primitif de $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_k})/\mathbb{Q}$.*

**Exercice 46.** ① *Soient $\mathbb{K}$ un corps de caractéristique zéro, $n \in \mathbb{N}^*$. Montrer que $\mathbb{K}$ admet une extension finie de degré $n$ si et seulement s'il existe un irréductible de degré $n$ de $\mathbb{K}[X]$.* [13]

**Exercice 47.** ④ *Soient $p$ un nombre premier, $\mathbb{L} = \mathbb{F}_p(X, Y)$, $\mathbb{K} = \mathbb{F}_p(X^p, Y^p)$.*

*a) Montrer que $[\mathbb{L} : \mathbb{K}] = p^2$ mais que $\mathbb{L}/\mathbb{K}$ n'est pas monogène.*

*b) Indiquer une famille infinie de sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$.*

**Exercice 48.** ④ *Soient $\mathbb{K}$ un corps de caractéristique nulle, $P_1, \dots, P_r$ des polynômes non constants de $\mathbb{K}[X]$. Montrer qu'il existe $r$ polynômes $Q_1, \dots, Q_r$ de $\mathbb{K}[X]$ non constants tels que les $P_i \circ Q_i$ pour $1 \leq i \leq r$ aient un diviseur commun dans $\mathbb{K}[X]$.*

12. Emmy Noether et Emil Artin ont présenté la théorie de Galois sans recourir à cet énoncé. Leur motivation était sans doute le désir d'utiliser des concepts aussi intrinsèques que possible. Or, une extension monogène finie admet beaucoup d'éléments primitifs.

13. Ce résultat souligne le lien entre polynômes irréductibles et extensions finies. Il reste vrai en caractéristique $p$, mais la preuve est plus délicate.

## 2.4 (*) Séparabilité (II)

La démonstration du théorème de l'élément primitif suggère de revenir sur la notion de séparabilité, déjà abordée dans le cas des polynômes [14].

Soit $\mathbb{L}/\mathbb{K}$ une extension. Disons qu'un élément $x$ de $\mathbb{K}$ est *séparable sur* $\mathbb{K}$ s'il est algébrique sur $\mathbb{K}$ et si $\Pi_{\mathbb{K},x}$ est séparable, c'est-à-dire premier à sa dérivée. Disons que *l'extension* $\mathbb{L}/\mathbb{K}$ *est séparable* si tout élément $x$ de $\mathbb{L}$ est séparable sur $\mathbb{K}$, ce qui impose que $\mathbb{L}/\mathbb{K}$ est algébrique. Si $\mathbb{K}$ est de caractéristique nulle, toute extension algébrique $\mathbb{L}/\mathbb{K}$ est séparable. Il en est plus généralement de même si $\mathbb{K}$ est parfait. [15]

**Exercice 49.** ② *Montrer que* $\mathbb{K}$ *est parfait si et seulement si toute extension finie de* $\mathbb{K}$ *est séparable.*

Soient $\mathbb{K}$ un corps de caractéristique $p$ non parfait, $a$ un élément de $\mathbb{K}$ qui n'est pas une puissance $p$-ième et $\alpha$ est une racine de $X^p - a$ dans une extension de $\mathbb{K}$. Alors l'extension $\mathbb{K}(\alpha)/\mathbb{K}$ est finie de degré $p$ non séparable. Exemple traditionnel :

$$\mathbb{K} = \mathbb{F}_p(T), \qquad a = T.$$

On a l'énoncé suivant, dont la réciproque sera établie dans le chapitre **3**.

**Proposition 9.** *Soient* $\mathbb{L}/\mathbb{K}$ *et* $\mathbb{M}/\mathbb{L}$ *deux extensions finies. Si* $\mathbb{M}/\mathbb{K}$ *est séparable, alors* $\mathbb{L}/\mathbb{K}$ *et* $\mathbb{M}/\mathbb{L}$ *le sont.*

*Preuve.* Supposons $\mathbb{M}/\mathbb{K}$ séparable. Il est immédiat que $\mathbb{L}/\mathbb{K}$ est séparable. Pour montrer que $\mathbb{M}/\mathbb{L}$ l'est également, il suffit de noter que, pour tout $x$ de $\mathbb{M}$, $\Pi_{\mathbb{L},x}$ divise $\Pi_{\mathbb{K},x}$.

Voici la forme générale du théorème de l'élément primitif.

**Théorème 5.** *Une extension séparable finie est monogène.*

*Preuve.* Soit $\mathbb{L}/\mathbb{K}$ une extension séparable finie. Montrons que $\mathbb{L}/\mathbb{K}$ est monogène.

Si $\mathbb{K}$ est infini, on reprend la preuve du théorème 4. La récurrence permettant de passer de $\mathbb{K}(x_1, \ldots, x_n)$ à $\mathbb{K}(x_1, \ldots, x_{n+1})$ se fait via la proposition 9.

Si $\mathbb{K}$ est fini, le résultat se déduit de la cyclicité de $(\mathbb{L}^*, \times)$ (chapitre **1**, **3.1**, théorème 4).

## 2.5 (*) Caractérisation des extensions monogènes

On se propose ici de caractériser les extensions monogènes. [16]

**Lemme 4.** *Soient* $\mathbb{L}/\mathbb{K}$ *une extension monogène finie,* $x$ *dans* $\mathbb{L}$ *tel que :* $\mathbb{L} = \mathbb{K}(x)$. *Si* $\mathbb{M}$ *est un sous-corps de* $\mathbb{L}$ *contenant* $\mathbb{K}$, $\mathbb{M}$ *est engendré sur* $\mathbb{K}$ *par les coefficients de* $\Pi_{\mathbb{M},x}$.

*Preuve.* Soient $\mathbb{M}'$ le sous-corps de $\mathbb{M}$ engendré par $\mathbb{K}$ et les coefficients de $\Pi_{\mathbb{M},x}$, $d$ le degré de $\Pi_{\mathbb{M},x}$. Le degré de $x$ sur $\mathbb{M}$ (resp $\mathbb{M}'$) est $d$ (resp. majoré par $d$) puisque $\Pi_{\mathbb{M},x} \in \mathbb{M}'[X]$. Comme $\mathbb{M}$ contient $\mathbb{M}'$, on en déduit que $\mathbb{M}' = \mathbb{M}$.

Voici la caractérisation annoncée.

14. Ce paragraphe, qui prolonge le **2.3** du chapitre **1**, peut être omis si on se limite à la caractéristique nulle.

15. Rappelons que $\mathbb{K}$ est dit parfait si les irréductibles de $\mathbb{K}[X]$ sont séparables, que tout corps de caractéristique nulle est parfait, qu'un corps de caractéristique $p > 0$ est parfait si et seulement si son Frobenius est surjectif.

16. Le résultat obtenu, dû à Steinitz, ne joue aucun rôle dans la suite.

**Proposition 10.** *Soit $\mathbb{L}/\mathbb{K}$ une extension finie. Les deux assertions suivantes sont équivalentes.*

*(i) L'extension $\mathbb{L}/\mathbb{K}$ est monogène,*

*(ii) L'ensemble des sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ est fini.*

*Preuve.* Si $\mathbb{K}$ est fini, *(i)* et *(ii)* sont satisfaites. On suppose donc $\mathbb{K}$ infini.

Pour *(i)* $\Rightarrow$ *ii)*, on note que le lemme 3 donne une injection de l'ensemble des sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ dans l'ensemble fini des diviseurs unitaires de $\Pi_{\mathbb{K},x}$ dans $\mathbb{L}[X]$ de degrés supérieurs ou égaux à 1 et annulant $x$.

Pour *(ii)* $\Rightarrow$ *(i)*, on écrit :

$$\mathbb{L} = \bigcup_{x\in\mathbb{L}} \mathbb{K}(x).$$

Comme les $\mathbb{K}(x)$ distincts sont en nombre fini, on conclut avec le lemme ci-après.

**Lemme 5.** *Soient $\mathbb{F}$ un corps infini, $V$ un $\mathbb{F}$-espace vectoriel. Alors $V$ ne peut être réunion d'un nombre fini de sous-espaces stricts.*

*Preuve.* Soient $V_1, \ldots, V_m$ des sous espaces stricts de $V$ et $X = \bigcup_{i=1}^m V_i$. On va montrer que $X \neq V$. Quitte à éliminer les $V_i$ superflus on peut supposer :

$$\forall i \in \{1, \ldots, m\}, \qquad V_i \not\subset \bigcup_{1\leq j\leq m,\ j\neq i} V_j.$$

On choisit :

$$x_1 \in V_1 \setminus \bigcup_{j\neq 1} V_j, \qquad x_2 \in V_2 \setminus \bigcup_{j\neq 2} V_j,$$

et on note $D$ la droite affine passant par $x_1$ et $x_2$. Cette droite n'est contenue dans aucun des $V_j$, donc coupe chaque $V_j$ en au plus un point. Par suite $X \cap D$ est fini de cardinal majoré par $m$. Comme $\mathbb{F}$ est infini, $D$ aussi et $D \not\subset X$.

**Remarque** *Autre preuve du lemme 5, en dimension finie*

Reprenons les notations du lemme 5. Une réunion finie de sous-espaces stricts de $V$ est contenue dans une réunion finie d'hyperplans. Supposons maintenant $V$ de dimension finie. Une réunion finie d'hyperplans est l'ensemble des zéros d'une fonction polynomiale non nulle de $V$ dans $\mathbb{F}$. Puisque $\mathbb{F}$ est infini, le lemme ci-après assure que le complémentaire de cette réunion est donc non vide. [17]

**Lemme 6.** *Soient $\mathbb{K}$ un corps, $n \in \mathbb{N}^*$, $P$ un élément de $\mathbb{K}[X_1, \ldots, X_n]$. Pour $i$ dans $\{1, \ldots, n\}$, soit $E_i$ une partie infinie de $\mathbb{K}$. Si $P$ s'annule sur $\prod_{i=1}^n E_i$, alors $P = 0$.*

*En particulier, si $\mathbb{K}$ est infini, $P$ s'annule sur $\mathbb{K}^n$ si et seulement si $P = 0$.*

*Preuve.* Le résultat est évident pour $n = 1$. Supposons $n \geq 2$ et le résultat vrai à l'ordre $n-1$. Adoptons les notations de l'énoncé et écrivons $P = \sum_{j=0}^{d} Q_j(X_1, \ldots, X_{n-1})\, X_n^j$, où les $Q_j$ sont dans $\mathbb{K}[X_1, \ldots, X_{n-1}]$. Soit $(x_1, \ldots, x_{n-1})$ dans $\prod_{i=1}^{n-1} E_i$. Alors $Q(X) = P(x_1, \ldots, x_{n-1}, X)$ est un

17. Cet argument montre que, si $H_1, \ldots, H_m$ sont des hyperplans de $V$, un élément « générique » de $V$ n'appartient pas à $\bigcup_{i=1}^m H_i$.

élément de $\mathbb{K}[X]$ qui s'annule sur l'ensemble infini $E_n$. Ainsi $Q = 0$, ce qui implique que, pour $j \in \{0, \ldots, d\}$, $G_j$ s'annule sur $\prod_{i=1}^{n-1} E_i$. En appliquant l'hypothèse de récurrence, on obtient que les $G_j$ sont nuls, donc que $P = 0$.

**Exercice 50.** ① *Montrer que toute sous-extension d'une extension monogène finie est monogène.*

**Exercice 51.** ③ *Supposons $\mathbb{L} = \mathbb{K}(x)$ où $x$ est algébrique sur $\mathbb{K}$ de degré $n$. Montrer que le nombre de sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ est majoré par $2^n$.* [18]

# 3 Extensions de décomposition

La résolution des équations algébriques suppose qu'un polynôme non constant ait des racines « quelque part ». [19] Nous avons déjà formulé des résultats dans cette direction (chapitre **1**, **2.2**, théorème 1 et 2). Nous les démontrons ici. L'existence d'un « corps de décomposition » d'un polynôme (proposition 11) est suffisante pour développer la théorie de Galois des extensions finies. Le parti pris dans ce cours est de fixer, plus radicalement, un corps $\mathbb{K}$ et un surcorps algébriquement clos $\Omega$ de $\mathbb{K}$. La démonstration de l'existence d'un tel surcorps fait l'objet de **3.2** ; elle ne contient pas d'idée algébrique nouvelle, mais nécessite un argument transfini (ici le lemme de Zorn). [20]

## 3.1 Corps de rupture, corps de décomposition

Le point de départ de ce paragraphe est le :

**Lemme 7.** *Soit $P$ un élément irréductible de $\mathbb{K}[X]$. Il existe une extension $\mathbb{K}'$ de $\mathbb{K}$ telle que :*

*(i) le polynôme $P$ a une racine $x$ dans $\mathbb{K}'$ ;*

*(ii) on a $\mathbb{K}' = \mathbb{K}(x)$.*

*Preuve.* Soit $\mathbb{K}'$ l'anneau quotient $\mathbb{K}[X]/(P)$. Puisque $P$ est irréductible et $\mathbb{K}[X]$ principal, l'anneau $\mathbb{K}'$ est un corps. La surjection canonique de $\mathbb{K}[X]$ sur $\mathbb{K}'$ induit, lorsqu'on la restreint à $\mathbb{K}$, un morphisme injectif de $\mathbb{K}$ dans $\mathbb{K}'$. On peut donc identifier $\mathbb{K}$ à un sous-corps de $\mathbb{K}'$. La classe $x$ de $X$ modulo $P$ est, par définition, une racine de $P$ dans $\mathbb{K}'$, et il est clair que $\mathbb{K}' = \mathbb{K}(x)$.

Un corps $\mathbb{K}'$ vérifiant les propriétés *i)* et *ii)* est un *corps de rupture* de $P$ sur $\mathbb{K}$. On renvoie à la remarque « Extensions et morphismes » du paragraphe **1** pour une discussion de l'identification de $\mathbb{K}$ à un sous-corps de $\mathbb{K}[X]/(P)$.

**Remarques**

1. *Construction de $\mathbb{C}$ à partir de $\mathbb{R}$*
   En appliquant le lemme précédent à $\mathbb{K} = \mathbb{R}$ et $P = X^2 + 1$, on obtient ce qui est sans doute la meilleure construction de $\mathbb{C}$, due à Cauchy.
2. *Réalisation matricielle*
   Soit $P$ dans $\mathbb{K}[X]$, unitaire de degré $n$ et irréductible sur $\mathbb{K}$. Soit $M$ la matrice compagnon de $P$ : $M$ est dans $\mathcal{M}_n(\mathbb{K})$, de polynôme minimal égal à $P$. Il s'ensuit que $\mathbb{K}[X]/(P)$ est isomorphe à la sous-algèbre $\mathbb{K}[M]$ de $\mathcal{M}_n(\mathbb{K})$.

18. On voit en considérant une extension multiquadratique qu'on ne peut pas trouver de majoration polynomiale en $n$.

19. Ce fait a longtemps été admis. Ainsi, Laplace l'utilise dans la démonstration du théorème de d'Alembert-Gauss présenté dans le paragraphe **6.2** du chapitre **1**.

20. Il est raisonnable d'admettre le résultat en première lecture.

3. *Réalisation matricielle de $\mathbb{C}$ (cas particulier de la remarque 2)*

   Prenons $\mathbb{K} = \mathbb{R}$, $P = X^2 + 1$ et pour $M$ la « rotation d'angle $\pi/2$ » : $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

   Alors :

$$\mathbb{R}[M] = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ ; \ (a,b) \in \mathbb{R}^2 \right\}$$

   est l'algèbre des similitudes, réalisation classique de $\mathbb{C}$ comme sous-algèbre de $\mathcal{M}_2(\mathbb{R})$.

**Exercice 52.** ② *Montrer que, si $P \in \mathbb{R}[X]$ est de degré 2 sans racine réelle, la $\mathbb{R}$-algèbre $\mathbb{R}[X]/(P)$ est isomorphe à $\mathbb{C}$.*

**Exercice 53.** ③ *Montrer que, si $P \in \mathbb{R}[X]$ n'est pas constant et $\mathbb{A} = \mathbb{K}[X]/(P)$, on a équivalence entre :*

*- le polynôme $P$ n'est divisible par aucun carré non constant de $\mathbb{K}[X]$ ;*

*- la $\mathbb{K}$-algèbre $\mathbb{A}$ est un produit fini de corps ;*

*- la $\mathbb{K}$-algèbre $\mathbb{A}$ est réduite, i.e. ne contient aucun nilpotent non nul.*

**Exercice 54.** ③ *Soit $n \in \mathbb{N}^*$. Écrire la $\mathbb{K}$-algèbre $\mathbb{K}[X]/(\Phi_n)$ comme produit de corps dans chacun des cas $\mathbb{K} = \mathbb{C}$, $\mathbb{K} = \mathbb{R}$, $\mathbb{K} = \mathbb{Q}$.*

L'énoncé suivant contient le théorème 1 du chapitre **1** (**2.2**).

**Proposition 11.** *Soit $P \in \mathbb{K}[X]$ non constant. Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ telle que :*

*(i) le polynôme $P$ est scindé sur $\mathbb{L}$,*

*(ii) si $\mathcal{R}$ est l'ensemble des racines de $P$ dans $\mathbb{L}$, alors $\mathbb{L} = \mathbb{K}(\mathcal{R})$.*

*Preuve.* On raisonne par récurrence sur le degré $d$ de $P$. Si ce degré est 1, le résultat est évident. Supposons le prouvé si $d = n \in \mathbb{N}^*$, soit $P$ dans $\mathbb{K}[X]$ de degré $n+1$. Soit $Q$ un facteur irréductible de $P$ dans $\mathbb{K}[X]$. Le lemme 7 fournit une extension $\mathbb{K}(x)$ de $\mathbb{K}$ où $x$ est racine de $Q$. Appliquant l'hypothèse de récurrence au polynôme $Q := \dfrac{P}{X - x}$ de $\mathbb{K}(x)[X]$, on obtient une extension $\mathbb{L}$ de $\mathbb{K}(x)$ dans laquelle $Q$ est scindé, et telle que : $\mathbb{L} = \mathbb{K}(x)\,(\mathcal{S})$, où $S$ est l'ensemble des racines de $Q$ dans $\mathbb{L}$. Bien évidemment, $P$ est scindé sur $\mathbb{L}$ et avec pour ensemble de racines $\mathcal{R} = \mathcal{S} \cup \{x\}$. Enfin : $\mathbb{L} = \mathbb{K}(\mathcal{R})$.

Un corps vérifiant *i*) et *ii*) est un *corps de décomposition* de $P$ sur $\mathbb{K}$. [21]

**Remarques** *Questions d'unicité*

1. *Unicité à isomorphisme près du corps de rupture*

   Si $P$ est un irréductible de $\mathbb{K}[X]$, nous verrons dans le chapitre **3** que deux corps de rupture de $P$ sur $\mathbb{K}$ sont isomorphes comme $\mathbb{K}$-algèbres.

2. *Coexistence de plusieurs corps de rupture dans une extension donnée*

   Soient $P$ un irréductible de $\mathbb{K}[X]$, $\mathbb{K}'$ un corps de rupture de $P$. Il se peut que $\mathbb{K}'$ contienne une racine de $P$ ou plusieurs racines de $P$. Par exemple, $\mathbb{Q}(\sqrt[3]{2})$ contient une seule racine de $X^3 - 2$ (les autres racines ne sont pas réelles) alors que $\mathbb{Q}(\sqrt{2})$ contient les deux racines de $X^2 - 2$.

   Autre formulation : si $\mathbb{L}$ est un surcorps de $\mathbb{K}$ scindant $P$, $\mathbb{L}$ peut contenir un ou plusieurs corps de rupture de $P$. Ainsi, le seul corps de rupture de $X^2 - 2$ sur $\mathbb{Q}$ contenu dans $\mathbb{C}$ est $\mathbb{Q}(\sqrt{2})$, mais $X^3 - 2$ admet trois sous-corps de rupture dans $\mathbb{C}$ : $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q}(j^2\sqrt[3]{2})$.

21. En substance, l'existence d'un corps de décomposition est due à Kronecker, vers 1880.

3. *Cas du corps de décomposition*

   Soit maintenant $P \in \mathbb{K}[X]$ non constant. Nous verrons dans le chapitre **3** que deux corps de décomposition de $P$ sont isomorphes comme $\mathbb{K}$-algèbres. De plus, si $\mathbb{L}$ un corps sur lequel $P$ est scindé, $P$ n'a qu'un corps de décomposition contenu dans $\mathbb{L}$, à savoir $\mathbb{K}(\mathcal{R})$ où $\mathcal{R}$ est l'ensemble des racines de $P$ dans $\mathbb{L}$.

   Exemple. Prenons $\mathbb{K} = \mathbb{Q}$ et $P = X^n - 2$ où $n$ est un entier supérieur ou égal à 2. Le corps de décomposition de $X^n - 2$ sur $\mathbb{Q}$ contenu dans $\mathbb{C}$ est $\mathbb{Q}(2^{1/n}, e^{2i\pi/n})$.

**Exercice 55.** ③ *Soient $\mathbb{K}$ un corps de caractéristique nulle, $P \in \mathbb{K}[X]$, $x_1, \ldots, x_m$ les racines distinctes de $P$ dans un corps de décomposition de $P$ sur $\mathbb{K}$. Montrer que $\prod_{i=1}^{m}(X - x_i) \in \mathbb{K}[X]$.*

**Exercice 56.** ② *Montrer que le polynôme $P = X^4 - 6X^2 + 6$ est irréductible sur $\mathbb{Q}$ et que $\mathbb{Q}(\sqrt{3+\sqrt{3}}, \sqrt{2})$ est un corps de décomposition de $P$ sur $\mathbb{Q}$.*

**Exercice 57.** ③ *Soit $p$ un nombre premier. Expliciter le corps de décomposition de $X^p - 2$ sur $\mathbb{Q}$ contenu dans $\mathbb{C}$. Quel est son degré sur $\mathbb{Q}$ ?*

**Exercice 58.** ② *Soient $\mathbb{K}$ un corps de caractéristique nulle, $n$ un élément de $\mathbb{N}^*$, $a$ un élément de $\mathbb{K}^*$. Montrer que, si $\mathbb{L}$ est un corps de décomposition de $X^n - a$ sur $\mathbb{K}$, $[\mathbb{L} : \mathbb{K}] \leq n\,\varphi(n)$.*

**Exercice 59.** ② *Soient $P$ un polynôme de degré 3 irréductible sur $\mathbb{Q}$ ayant exactement une racine réelle $\alpha$ (par exemple $X^3 - 2$). Soient $\beta$ et $\bar{\beta}$ les racines de $P$ dans $\mathbb{C} \setminus \mathbb{R}$. Montrer que le corps de décomposition de $P$ sur $\mathbb{Q}$ est de degré 6 sur $\mathbb{Q}$ et que $\mathbb{Q}(\beta)$ est un sous-corps de $\mathbb{C}$ instable par conjugaison.*

**Exercice 60.** ② *Soient $p \in \mathcal{P}$, $n \in \mathbb{N}^*$, $M \in \mathcal{M}_n(\mathbb{Z})$. On note $\overline{M}$ la réduction de $M$ modulo $p$. En considérant un surcorps de $\mathbb{F}_p$ scindant $\chi_{\overline{M}}$, montrer que $tr(M^p) \equiv tr(M)\ [p]$.*

**Exercice 61.** ④ *On suppose que $\mathbb{K}$ est de caractéristique 0. Soient $n \in \mathbb{N}^*$, $P$ dans $\mathbb{K}[X]$ de degré $n$ séparable, $x_1, \ldots, x_n$ les racines de $P$ dans une extension, $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_n)$. Si $I$ est une partie de $\{1, \ldots, n\}$, soit $S_I = \sum_{i \in I} x_i$. Soient $m \in \{1, \ldots, n-1\}$, $\mathbb{L}_m$ le sous-corps de $\mathbb{L}$ engendré par les $S_I$ pour $I$ décrivant l'ensemble des parties de cardinal $m$ de $\{1, \ldots, n\}$. Montrer que $\mathbb{L}_m = \mathbb{L}$.*

**(*) Remarque** *Degré d'un corps de décomposition*

Si $P \in \mathbb{K}[X]$ est irréductible de degré $n$, un corps de rupture de $P$ sur $\mathbb{K}$ est de degré $n$ sur $\mathbb{K}$. Qu'en est-il d'un corps de décomposition ?

**Proposition 12.** *Soient $P$ dans $\mathbb{K}[X]$ non constant, $\mathbb{L}$ un corps de décomposition de $P$ sur $\mathbb{K}$.*

*(i) Si $P$ est de degré $n$, $[\mathbb{L} : \mathbb{K}]$ divise $n!$.*

*(ii) Supposons $P$ réductible sur $\mathbb{K}$ : $P = UV$ avec $U$ et $V$ dans $\mathbb{K}[X]$ de degrés respectifs $d$ et $n - d$, où $1 \leq d \leq n - 1$. Alors $[\mathbb{L} : \mathbb{K}]$ divise $d!\,(n-d)!$ et est donc majoré par $(n-1)!$.*

*Preuve de (i).* On raisonne par récurrence sur $n$. Le cas $n = 1$ est immédiat. Supposons $n \geq 2$ et le résultat vrai pour $P$ de degré au plus $n - 1$. Soient $P$ dans $\mathbb{K}[X]$ de degré $n$, $\mathbb{L}$ un corps de décomposition de $P$ sur $\mathbb{K}$. On distingue deux cas.

– Supposons $P$ réductible sur $\mathbb{K}$ : $P$ s'écrit $UV$ avec $U$ et $V$ dans $\mathbb{K}[X]$ non constants. Notons $d$ le degré de $U$, $\mathcal{R}$ (resp. $\mathcal{R}'$) l'ensemble des racines de $U$ (resp. $V$) dans $\mathbb{L}$. On a

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{K}(\mathcal{R}) : \mathbb{K}] \times [\mathbb{L} : \mathbb{K}(\mathcal{R})].$$

Mais $\mathbb{K}(\mathcal{R})$ est un corps de décomposition de $U$ sur $\mathbb{K}$, tandis que $L = \mathbb{K}(\mathcal{R} \cup \mathcal{R}')$ est un corps de décomposition de $V$ sur $\mathbb{K}(\mathcal{R})$. L'hypothèse de récurrence montre que $[\mathbb{K}(\mathcal{R}) : \mathbb{K}]$ divise $d!$ et que $[\mathbb{L} : \mathbb{K}(\mathcal{R})]$ divise $(n-d)!$. Ainsi, $[\mathbb{L} : \mathbb{K}]$ divise $d!(n-d)!$, lequel divise $n!$ ($\binom{n}{d}$ est entier).

– Supposons $P$ irréductible sur $\mathbb{K}$, notons $x_1, \ldots, x_n$ les racines de $P$ dans $\mathbb{L}$ comptées avec multiplicité. Formons le polynôme $Q = \dfrac{P}{X - x_n}$. Alors $Q$ appartient à $\mathbb{K}(x_n)[X]$ et est de degré $n-1$ ; de plus, $\mathbb{L}$ est un corps de décomposition de $Q$ sur $\mathbb{K}(x_n)$. L'hypothèse de récurrence entraîne que $[\mathbb{L} : K(x_n)]$ divise $(n-1)!$. Comme $[\mathbb{K}(x_n) : \mathbb{K}] = n$ (irréductibilité de $P$), on conclut par multiplicativité des degrés.

*Preuve de (ii).* L'argument justifiant la première assertion a été donné dans la preuve de *i)*. La seconde s'en déduit via des propriétés classiques des coefficients binomiaux. [22]

**Exercice 62.** ④ *Soient $P \in \mathbb{K}[X]$ irréductible sur $\mathbb{K}$, de la forme $X^6 + aX^3 + b$, $\mathbb{L}$ un corps de décomposition de $P$ sur $K$. Montrer que $[\mathbb{L} : \mathbb{K}]$ divise 18.*

**Exercice 63.** ④ *Soit $P = X^6 - 4X^3 + 2$.*

*a) Montrer que $P$ est irréductible sur $\mathbb{Q}$.*

*b) Montrer que $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2+\sqrt{2}}, \sqrt[3]{2}, j)$ est un corps de décomposition de $P$ sur $\mathbb{Q}$.*

*c) Montrer que $[\mathbb{L} : \mathbb{Q}] = 18$.*

## 3.2 (*) Corps algébriquement clos, clôture algébrique

Il est naturel de se demander s'il existe une extension de $\mathbb{K}$ dans laquelle tout polynôme de $\mathbb{K}[X]$ est scindé. La réponse est oui, sous réserve d'accepter l'axiome du choix, de manière à effectuer une version transfinie des constructions précédentes. [23] On a en fait un résultat plus précis, le *théorème de Steinitz*, énoncé dans le chapitre **1** (**2.2**, théorème 2).

**Théorème 6.** *Tout corps admet un surcorps algébriquement clos.*

L'axiome du choix intervient par le biais du *théorème de Krull* ci-après.

**Lemme 8.** *Soit $\mathbb{A}$ un anneau commutatif, $\mathcal{I}$ un idéal de $\mathbb{A}$ distinct de $\mathbb{A}$. Il existe alors un idéal maximal $\mathcal{J}$ de $\mathbb{A}$ contenant $\mathcal{I}$.*

*Preuve.* L'ensemble $\mathcal{E}$ des idéaux stricts de $\mathbb{A}$ contenant $\mathcal{I}$ est naturellement ordonné par inclusion. Il suffit d'établir le caractère inductif de cet ordre pour conclure via le lemme de Zorn. Si on se donne une partie $\mathcal{E}'$ totalement ordonnée de $\mathcal{E}$, la réunion des éléments de $\mathcal{E}'$ est un idéal contenant $\mathcal{I}$. Il reste à voir que cet idéal est différent de $\mathbb{A}$. Si tel n'était pas le cas, 1 appartiendrait à un des éléments de $\mathcal{E}'$, contradiction.

*Preuve du théorème 6 (Artin).* Soit $\mathbb{K}$ un corps.

*Étape 1. Il existe une extension $\mathbb{K}_1$ de $\mathbb{K}$ dans laquelle tout polynôme non constant de $\mathbb{K}[X]$ admet une racine.*

Notons $\mathcal{E}$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{K}[X]$ et $\mathbb{A}$ l'anneau

$$\mathbb{A} = \mathbb{K}\left[\{X_P \ ; \ P \in \mathcal{E}\}\right]$$

22. Croissance de la suite $\left(\binom{n}{d}\right)_{1 \leq d \leq n/2}$ et relation de symétrie $\binom{n}{d} = \binom{n}{n-d}$.

23. On peut en fait se contenter d'un énoncé ensembliste plus faible que l'axiome du choix, le théorème de l'idéal premier dans une algèbre de Boole, mais suffisant pour impliquer le théorème de Krull (Banaschewski, 1992).

des polynômes à une infinité d'indéterminées indexées par $\mathcal{E}$. On considère l'idéal $\mathcal{I}$ de $\mathbb{A}$ engendré par les polynômes $P(X_P)$ pour $P \in \mathcal{E}$. Admettant que $\mathcal{I} \neq \mathbb{A}$, le théorème de Krull fournit un idéal maximal $\mathcal{J}$ de $\mathbb{A}$ contenant $\mathcal{I}$. L'anneau $\mathbb{K}_1 = \mathbb{A}/\mathcal{J}$ est un corps dans lequel $\mathbb{K}$ s'injecte canoniquement. Si $P \in \mathcal{E}$, $P$ admet l'image de $X_P$ par la surjection canonique de $A$ sur $\mathbb{K}_1$ comme racine dans $\mathbb{K}_1$ ; le résultat suit.

Reste à vérifier que $\mathcal{I} \neq \mathbb{A}$. Si tel n'était pas le cas, il existerait $m \in \mathbb{N}^*$, des éléments $P_1, \ldots, P_m$ de $\mathcal{E}$ et des éléments $F_1, \ldots, F_m$ de $\mathbb{A}$ tels que :

$$1 = \sum_{i=1}^{m} P_i\left(X_{P_i}\right) F_i.$$

Soit $\mathbb{L}$ un corps de décomposition de $\prod_{i=1}^{m} P_i$ sur $\mathbb{K}$. Si $1 \leq i \leq m$, soit $x_i$ une racine de $P_i$ dans $\mathbb{L}$. La « propriété universelle des algèbres de polynômes » fournit un morphisme de $\mathbb{K}$-algèbres $\theta$ de $\mathbb{A}$ dans $\mathbb{L}$ envoyant $X_{P_i}$ sur $x_i$ pour $1 \leq i \leq n$. Appliquant $\theta$ à la relation précédente, on arrive à l'absurdité $1 = 0$.

*Étape 2.* On répète la construction précédente, et on obtient les corps :

$$\mathbb{K} \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_n \subset \cdots$$

où, pour tout $n \in \mathbb{N}^*$, $\mathbb{K}_{n+1}$ est une extension de $\mathbb{K}_n$ dans laquelle tout polynôme irréductible de $\mathbb{K}_n$ admet une racine. Soit $\mathbb{K}_\infty$ la réunion [24] des $\mathbb{K}_n$. Si $P \in \mathbb{K}_\infty[X]$, $P$ appartient à $\mathbb{K}_n[X]$ pour un $n$ de $\mathbb{N}^*$ et a donc une racine dans $\mathbb{K}_{n+1}$, donc dans $\mathbb{K}_\infty$. Il s'ensuit que $\mathbb{K}_\infty$ est algébriquement clos. [25]

On appelle *clôture algébrique* de $\mathbb{K}$ tout surcorps algébriquement clos $\mathbb{L}$ de $\mathbb{K}$ algébrique sur $\mathbb{K}$. L'existence d'une clôture algébrique de $\mathbb{K}$ vient du théorème de Steinitz et du corollaire 4 de **2.2**, que nous reformulons ici.

**Corollaire 5.** *Soient $\mathbb{K}$ un corps, $\Omega$ une extension algébriquement close de $\mathbb{K}$, $\mathbb{L}$ l'ensemble des éléments de $\Omega$ algébriques sur $\mathbb{K}$. Alors $\mathbb{L}$ est une clôture algébrique de $\mathbb{K}$.*

Le corps $\overline{\mathbb{Q}}$ est donc une clôture algébrique de $\mathbb{Q}$.

L'exercice ci-après, sans lien avec la théorie des corps, met en garde contre une application trop rapide du lemme de Zorn.

**Exercice 64.** ④ *Montrer que le groupe $(\mathbb{Q}, +)$ ne contient aucun sous-groupe strict maximal pour l'inclusion.*

24. Il serait plus correct de parler de considérer $\mathbb{K}_i$ comme plongé dans $\mathbb{K}_{i+1}$ et de définir $\mathbb{K}_\infty$ comme limite inductive.

25. La première étape de la preuve précédente est une adaptation, avec suffisamment de variables, de la démonstration de l'existence d'un corps de rupture. Les difficultés supplémentaires ne viennent pas de l'algèbre mais de la « théorie » (naïve) des ensembles, un argument transfini étant indispensable pour prouver le théorème dans toute sa généralité. Bien sûr, si $\mathbb{K}$ est dénombrable, la forme dénombrable de l'axiome du choix est suffisante. D'autre part, on dispose souvent en pratique d'une extension algébriquement close explicite ($\mathbb{C}$, séries de Puiseux...). Enfin, dans de nombreuses questions, on peut substituer un corps de décomposition idoine à un corps algébriquement clos ; par exemple, pour trigonaliser une matrice, il suffit de se placer dans une extension scindant le polynôme caractéristique.

### 3.3 Résolubilité des équations par radicaux : formulation

**En théorie de Galois, nous fixerons un corps $\mathbb{K}$, un surcorps algébriquement clos $\Omega$ de $\mathbb{K}$ et travaillerons dans $\Omega$. Si $P$ est un élément de $\mathbb{K}[X]$, nous noterons $D_{\mathbb{K}}(P)$ le corps de décomposition de $P$ contenu dans $\Omega$.**

Formulons, dans ce cadre, le problème de la résolubilité des équations par radicaux. Si $P \in \mathbb{K}[X]$, nous dirons que *$P$ est résoluble par radicaux* (sous-entendu : sur $\mathbb{K}$) s'il existe des entiers $n_1, \dots, n_r$ de $\mathbb{N}^*$ et des éléments $a_1, \dots, a_r$ de $\Omega$ tels que :

$$\forall i \in \{0, \dots, r-1\}, \quad {a_{i+1}}^{n_{i+1}} \in \mathbb{K}(a_1, \dots, a_i) \quad \text{et :} \quad D_{\mathbb{K}}P \subset \mathbb{K}(a_1, \dots, a_r).$$

Cette définition capture bien l'idée que l'on peut obtenir les racines de $P$ (et donc le corps de décomposition de $P$) par des opérations de corps et des extractions de radicaux. L'objet important dans cette formulation n'est pas l'ensemble des racines de $P$, mais le corps de décomposition $D_{\mathbb{K}}(P)$.[26] Notons aussi que l'on peut, quitte à insérer des radicaux intermédiaires, supposer que les $n_i$ sont des nombres premiers.

Certains polynômes sont trivialement résolubles par radicaux. Tel est par exemple le cas des binômes :

$$X^n - a \qquad (n, a) \in \mathbb{N}^* \times \mathbb{K}.$$

Il en est de même des polynômes de degré $2, 3, 4$. Le cas du degré 2 est évident, les degrés 3 et 4 relèvent des formules de Cardan et Ferrari. Nous verrons, dans le chapitre **5**, que la situation est très différente si le degré est supérieur ou égal à 5.

## 4 (*) Constructibilité à la règle et au compas (I)

La géométrie grecque accordait une grande place aux constructions à la règle et au compas. Elle a à son actif de nombreux succès, dont l'un des plus connus est la construction du pentagone régulier. Elle a cependant échoué devant plusieurs problèmes : quadrature du cercle, duplication du cube, trisection de l'angle, construction de l'heptagone régulier ou plus généralement de polygones réguliers à $n$ côtés pour $n$ autre que $3, 5, 6, 15$.

Ces constructions sont impossibles. Le démontrer demandait de lever plusieurs barrières :

- envisager l'impossibilité ;

- se libérer d'une conception des nombres fondée de manière très contraignante sur la géométrie, qui a sévèrement limité les mathématiciens grecs ;

- disposer d'une méthode efficace reliant nombres et constructions, qui ne pouvait guère apparaître avant l'invention[27] par Descartes de la « méthode des coordonnées » ;

- s'intéresser à la structure algébrique de l'ensemble des nombres réels qui sont des coordonnées de points « constructibles ».

La clé est donc à chercher dans l'algèbre plus que dans la géométrie. Nous montrerons ici les impossibilités. Nous reviendrons sur le sujet au chapitre **5**, une fois la théorie de Galois établie, afin notamment d'expliquer le théorème de Gauss sur la constructibilité du polygone régulier à 17 côtés.

Dans le plan euclidien orienté $\mathbb{R}^2$, on cherche les points que l'on peut construire à la règle et au compas à partir des deux points de base $O = (0, 0)$ et $I = (1, 0)$. Formalisons. Étant donnée une partie $\mathcal{A}$ de $\mathbb{R}^2$, soit $\widehat{\mathcal{A}}$ l'ensemble formé des parties suivantes de $\mathbb{R}^2$ :

26. Il existe beaucoup d'éléments de $\mathbb{K}[X]$ ayant même corps de décomposition sur $\mathbb{K}$.
27. La *Géométrie* de Descartes date de 1637.

- les droites passant par deux points distincts de $\mathcal{A}$,

- les cercles centrés sur un point de $\mathcal{A}$, et de rayon égal à la longueur d'un segment joignant deux points de $\mathcal{A}$.

On dit alors que le point $M$ de $\mathbb{R}^2$ est *constructible en un pas à partir de* $\mathcal{A}$ s'il existe deux éléments distincts de $\widehat{\mathcal{A}}$ dont $M$ soit un point d'intersection. On dit que $M$ est *constructible* si et seulement s'il existe une suite $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \cdots \subset \mathcal{A}_n$ de parties de $\mathbb{R}^2$ telles que :

*(i)* $\mathcal{A}_0 = \{0, I\}$ ;

*(ii)* pour $1 \leq i \leq n$, $\mathcal{A}_i = \mathcal{A}_{i-1} \cup \{M_i\}$, où $M_i$ est constructible en un pas à partir de $\mathcal{A}_i$ ;

*(iii)* $M \in \mathcal{A}_n$.

Le nombre complexe $z$ est dit *constructible* si le point d'affixe $z$ est constructible. Nous noterons $\mathcal{C}$ des nombres complexes constructibles. La droite $\Delta$ et le cercle $\Gamma$ sont dits constructibles s'ils sont dans $\widehat{\mathcal{C}}$.

Nous allons caractériser l'ensemble $\mathcal{C}$ à l'aide de la notion d'extension. Cette caractérisation repose sur quelques constructions géométriques élémentaires mais fastidieuses. Il est recommandé au lecteur de faire des dessins.

1. Si $\Delta \in \widehat{\mathcal{C}}$ et $A \in \mathcal{C}$, la perpendiculaire à $\Delta$ passant par $A$ est dans $\widehat{\mathcal{C}}$.

   *Preuve.* Il existe un point $B$ de $\Delta \cap \mathcal{C}$ distinct de $A$. Si $B$ est le projeté orthogonal de $A$ sur $\Delta$, on a terminé. Sinon, le cercle de centre $A$ et de rayon $AB$ coupe $\Delta$ en $B$ et en un autre point $C$. Les deux cercles de rayon $BC$ et de centres respectifs $B$ et $C$ ont pour intersection deux points distincts de la perpendiculaire à $\Delta$ passant par $A$.

2. Si $A$ et $B$ sont constructibles, l'image de $B$ par la rotation de centre $A$ et d'angle $\pi/2$ est constructible.

   *Preuve.* La droite $\Delta$ perpendiculaire à $(AB)$ et passant par $A$ est constructible grâce à **1**. Le point recherché est situé à l'intersection du cercle de centre $A$ et de rayon $AB$, et de $\Delta$.

   Ainsi, si $z \in \mathcal{C}$, $iz \in \mathcal{C}$.

3. Si $\Delta \in \widehat{\mathcal{C}}$ et $A \in \mathcal{C}$, le projeté orthogonal de $A$ sur $\Delta$ et le symétrique de $A$ par rapport à $D$ sont constructibles.

   *Preuve.* Pour le projeté orthogonal, il suffit d'appliquer **1**. Si $B$ est ce projeté, le cercle de centre $B$ et de rayon $AB$ recoupe la perpendiculaire à $\Delta$ passant par $A$ en $C$ symétrique de $A$ par rapport à $\Delta$.

   Ainsi, si $z \in \mathcal{C}$, les points Re $z$, Im $z$ et $\bar{z}$ sont dans $\mathcal{C}$.

4. Si $\Delta \in \widehat{\mathcal{C}}$ et $A \in \mathcal{C}$, la parallèle à $\Delta$ passant par $A$ est dans $\widehat{\mathcal{C}}$.

   *Preuve.* On trace la perpendiculaire $\Delta'$ à $\Delta$ passant par $A$, puis la perpendiculaire à $\Delta'$ passant par $A$ qui est la droite cherchée.

5. Si $a \in \mathbb{C}$ et $b \in \mathbb{C}$ sont dans $\mathcal{C}$, le point $a + b$ est dans $\mathcal{C}$.

   *Preuve.* Soient $A$ et $B$ les points de $\mathbb{R}^2$ d'affixes $a$ et $b$. Si $O, A$ et $B$ sont alignés, on trace le cercle de centre $B$ et rayon $OA$ ; le point d'affixe $a + b$ est l'un des points d'intersection de ce cercle et de la droite $(OA)$. Sinon, on trace la parallèle à $(OA)$ passant par $B$ et la parallèle à $(OB)$ passant par $A$ ; ces deux parallèles se coupent au point d'affixe $a + b$.

6. Si $A$ et $B$ sont constructibles, le symétrique de $B$ par rapport à $A$ est constructible.

   *Preuve.* Le point recherché est le symétrique de $B$ par rapport à la perpendiculaire à $(AB)$ passant par $A$.

7. Si $a \in \mathbb{C}$ et $b \in \mathbb{C}$ sont dans $\mathcal{C}$, le point d'affixe $ab$ est dans $\mathcal{C}$.

   *Preuve.* On sait que $z \in \mathcal{C}$ si et seulement si $\mathrm{Re}(z)$ et $\mathrm{Im}(z)$ sont dans $\mathcal{C}$. Grâce à ce qui précède et aux formules exprimant parties réelle et imaginaire d'un produit, on peut se contenter de traiter le cas où $a$ et $b$ sont réels non nuls. Soient $A$ le point d'affixe $a$ et $B$ le point d'affixe $ib$. On trace la parallèle à $(IB)$ passant par $A$, et cette parallèle coupe l'axe imaginaire au point d'affixe $iab$.

8. Si $a \in \mathbb{C} \setminus \{0\}$ est dans $\mathcal{C}$, il en est de même du point d'affixe $\dfrac{1}{a}$.

   *Preuve.* La stabilité de $\mathcal{C}$ par somme, produit, partie réelle et imaginaire permet encore de se borner au cas où $a$ est réel. Soient $A$ le point d'affixe $a$, $J$ le point d'affixe $i$, et $B$ le point d'intersection de l'axe imaginaire et de la parallèle à $(AJ)$ passant par $I$. Alors l'affixe de $B$ est $\dfrac{i}{a}$.

   Il résulte de ce qui précède que $\mathcal{C}$ est un corps. En particulier, le milieu de deux points de $\mathcal{C}$ est dans $\mathcal{C}$ (ce que l'on peut obtenir plus directement). Cette observation nous sera utile pour la prochaine construction.

9. Si $a \in \mathbb{C}$ est dans $\mathcal{C}$, les racines carrées de $a$ sont dans $\mathcal{C}$.

   *Preuve.* La méthode « algébrique » de résolution des équations de degré 2 dans $\mathbb{C}$ montre que l'on peut se borner au cas où $a \in \mathbb{R}^{+*}$. Soient $A$ le point d'affixe $a+1$ et $M$ le milieu du segment $OA$. La perpendiculaire en $I$ à l'axe réel coupe le cercle de centre $M$ et de rayon $OM$ en un point $B$ d'ordonnée positive. On vérifie que $B = (1, \sqrt{a})$.

10. Soient $\mathcal{A}$ une partie de $\mathbb{C}$, et $\mathbb{K}$ le sous-corps de $\mathbb{C}$ engendré par les parties réelles et imaginaires de $\mathcal{A}$, i.e. $\mathbb{K} = \mathbb{Q}(\mathcal{A}, \overline{\mathcal{A}})$. Si $M = (a, b)$ est constructible en un pas à partir de $\mathcal{A}$, alors $a$ et $b$ appartiennent à une extension de $\mathbb{K}$ de degré 1 ou 2.

    *Preuve.* Si $M$ s'obtient comme intersection de deux droites de $\widehat{\mathcal{A}}$, $a$ et $b$ sont dans $\mathbb{K}$. Supposons que $M$ se trouve à l'intersection d'une droite $\Delta$ et d'un cercle $\Gamma$ de $\widehat{\mathcal{A}}$. L'équation de $\Delta$ est de la forme $\alpha x + \beta y + \gamma = 0$ avec $(\alpha, \beta, \gamma) \in \mathbb{K}^3$ ; celle de $\Gamma$ est de la forme $x^2 + y^2 - \delta x - \varepsilon y = \lambda$ où $\delta$, $(\varepsilon, \lambda) \in \mathbb{K}^2$. Si $\beta \neq 0$, on tire $y$ en fonction de $x$ de l'équation de $\Delta$, et on voit, en reportant, que $x$ vérifie une équation de degré 2 à coefficients dans $\mathbb{K}$, ce qui permet de conclure. Le cas où $M$ est intersection de deux cercles se ramène au précédent en faisant la différence des équations.

**Exercice 65.** ② *On se donne deux droites sécantes de $\mathbb{C}$. Expliquer comment construire leurs bissectrices à la règle et au compas.*

Ces considérations établissent le résultat suivant.

**Théorème 7.** *Soit $z \in \mathbb{C}$. les assertions suivantes sont équivalentes.*

*(i) Le nombre complexe $z$ appartient à $\mathcal{C}$.*

*(ii) Il existe une chaîne $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n$ de sous-corps de $\mathbb{C}$ telle que :*
- $\mathbb{K}_0 = \mathbb{Q}$,
- $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$ *pour tout* $i \in \{0, \ldots, n-1\}$,
- $z \in \mathbb{K}_n$.

*Autrement dit, $\mathcal{C}$ est le plus petit sous-corps de $\mathbb{C}$ stable par racine carrée.*

*Preuve.* L'implication *i) ⇒ ii)* découle du point 10 et de la définition de la constructibilité, la réciproque du fait que $\mathcal{C}$ est un sous-corps de $\mathbb{C}$ stable par racine carrée. La reformulation se déduit de la remarque 4 de **2.2**.

On déduit de ce théorème et de la multiplicativité des degrés une condition nécessaire de constructibilité.

**Corollaire 6.** *Si $z \in \mathcal{C}$, $z$ est algébrique sur $\mathbb{Q}$ et le degré de $z$ sur $\mathbb{Q}$ est une puissance de 2.*

Ce résultat, attribué à Wantzel (1837), est postérieur aux travaux de Galois. Il a plusieurs conséquences : $\sqrt[3]{2}$ n'est pas constructible, ce qui montre l'impossibilité de la duplication du cube ; $\sqrt{\pi}$ non plus (car $\pi$ est transcendant sur $\mathbb{Q}$), d'où l'impossibilité de la quadrature du cercle. [28] D'autre part, pour $n \in \mathbb{N}^*$, la constructibilité de $e^{2i\pi/n}$ implique que $\varphi(n)$ est une puissance de 2, c'est-à-dire que $n$ est produit de nombres premiers de la forme $2^q + 1$ avec $q$ dans $\mathbb{N}$. [29]

L'exercice ci-après étudie un autre problème d'origine géométrique, la *trisection de l'angle*.

**Exercice 66.** ③ *On dit que l'angle $\theta$ est constructible à partir de l'angle $\alpha$ si le point $e^{i\theta}$ est constructible à partir de $e^{i\alpha}$.*

*a) Montrer que $e^{i\theta/3}$ est constructible à partir de $e^{i\theta}$ si et seulement si $\cos(\theta/3)$ est constructible à partir de $\cos(\theta)$.*

*b) Montrer que la condition de a) est satisfaite si et seulement si le polynôme $X^3 - 3X^2 - 2\cos(\theta)$ a une racine dans $\mathbb{Q}(\cos(\theta))$. Application : $\theta = \dfrac{\pi}{3}$.*

**Exercice 67.** ⑤ *Soit $x$ une racine de $X^4 + X + 1$ dans $\mathbb{C}$. Montrer que $x$ n'est pas constructible.*

La condition du corollaire 6 n'est pas suffisante. Voici le « bon » énoncé : le nombre complexe $z$ est constructible si et seulement si $[D_{\mathbb{Q}}\Pi_{\mathbb{Q},z} : \mathbb{Q}]$ est une puissance de 2. La démonstration la plus naturelle repose sur la théorie de Galois (chapitre **5**).

**Exercice 68.** ③ *On rappelle la formule (chapitre* **1**, **1.1**, *exercice 1) :* $\cos\left(\dfrac{2\pi}{5}\right) = \dfrac{\sqrt{5}-1}{4}$. *En déduire une construction du pentagone régulier de centre $O$ et dont $I$ est un des sommets.*

**Exercice 69.** ③ *Dans le plan complexe, on note $\mathcal{D}$ la bissectrice intérieure de l'angle $\widehat{OJ'I}$, où $J'$ est le milieu de $[OJ]$. Calculer l'intersection de $\mathcal{D}$ et de l'axe réel. En déduire une construction du pentagone régulier de centre $O$ et dont $I$ est un des sommets.*

# 5 (*) Appendice : éléments entiers sur un anneau

On étend ici les considérations « linéaires » de la section **1** des corps aux anneaux. Assumant une certaine redondance, on traite en premier lieu le cas essentiel des entiers algébriques.

## 5.1 L'anneau des entiers algébriques

L'étude de l'arithmétique des corps de nombres a conduit les mathématiciens du dix-neuvième siècle à dégager la notion d'*entier algébrique*, définitivement fixée par Dedekind un peu après 1870. Rappelons la définition (**1.4**, exemple 6) : le nombre complexe $x$ s'il existe $P \in \mathbb{Z}[X]$ unitaire annulant $x$. Rappelons également le lemme 1 (**1.4**) : les entiers algébriques sont les éléments de $\overline{\mathbb{Q}}$ tels que $\Pi_{\mathbb{Q},x}$ appartienne à $\mathbb{Z}[X]$.

On note désormais $\overline{\mathbb{Z}}$ l'ensemble des entiers algébriques. Par exemple, les éléments de la forme $\sqrt[n]{a}$ avec $n \in \mathbb{N}^*$ et $a \in \mathbb{N}^*$ sont dans $\overline{\mathbb{Z}}$, les racines de l'unité également. Le « test des racines rationnelles » (chapitre **1**, **2.2**, lemme 1) entraîne par ailleurs le résultat suivant.

28. Avec les notations précédentes, la duplication du cube est la construction à la règle et au compas de l'arête d'un cube de volume double de celui d'un cube dont $OI$ et $OJ$ sont des arêtes. La quadrature du cercle est la construction à la règle et au compas d'un carré dont l'aire est celle du cercle de rayon $OI$.

29. Les nombres premiers de la forme $2^q + 1$ sont dits *de Fermat*. Il est facile de voir que l'exposant $q$ est nécessairement une puissance de 2. En 2022, le plus grand nombre de Fermat connu reste 65537.

**Lemme 9.** *On a*

$$\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}.$$

**Exercice 70.** ② *Les nombres complexes suivants sont-ils des entiers algébriques :*

$$\sqrt{3+\sqrt{5}}, \quad \frac{1+\sqrt{5}}{2}, \quad \frac{\sqrt{2}}{2} \ ?$$

**Exercice 71.** ③ *a) Soit $n \in \mathbb{N}^*$. Montrer qu'il existe $U_n \in \mathbb{Z}[X]$ unitaire de degré $n$ tel que :*

$$\forall \theta \in \mathbb{R}, \qquad U_n(2\cos(\theta)) = 2\cos(n\theta).$$

*b) En déduire que, pour $k \in \mathbb{Z}$, $2\cos\left(\dfrac{2k\pi}{n}\right) \in \overline{\mathbb{Z}}$. Déterminer les $r \in \mathbb{Q}$ tels que $\cos(\pi r) \in \mathbb{Q}$.*

**Exercice 72.** ③ *Montrer que $\dfrac{1}{3}\left(1 + 10^{1/3} + 10^{2/3}\right) \in \overline{\mathbb{Z}}$.*

**Exercice 73.** ③ *Soit $x \in \overline{\mathbb{Z}} \setminus \{0\}$. Montrer que l'ensemble $\left\{q \in \mathbb{N}^* \ ; \ \dfrac{x}{q} \in \overline{\mathbb{Z}}\right\}$ est fini.*

On attend que $\overline{\mathbb{Z}}$ soit un sous-anneau de $\mathbb{C}$. Nous allons établir ce fait, en passant par une linéarisation de la notion d'intégralité, dans l'esprit de la proposition 2 de **1.3**. Dans ce but, introduisons le vocabulaire de l'adjonction pour l'anneau $\mathbb{Z}$.

Si $E$ est une partie de $\mathbb{C}$, on note $\mathbb{Z}[E]$ le plus petit sous-anneau de $\mathbb{C}$ contenant $E$. Cas particulier : si $E = \{x_1, \ldots, x_m\}$ est fini, on note $\mathbb{Z}[E] = \mathbb{Z}[x_1, \ldots, x_m]$. On a :

$$\mathbb{Z}[x_1, \ldots, x_m] = \{P(x_1, \ldots, x_m) \ ; \ P \in \mathbb{Z}[X_1, \ldots, X_m]\}.$$

En particulier, pour $x$ dans $\mathbb{C}$ :

$$\mathbb{Z}[x] = \{P(x) \ ; \ P \in \mathbb{Z}[X]\}.$$

Nous pouvons alors obtenir la caractérisation attendue, due en substance à Dedekind, qui est le point *iv*) du théorème suivant. Comme en **1.3** :

**intégralité = finitude**.

La démonstration utilise les déterminants, et non pas la théorie élémentaire de la dimension.

**Théorème 8.** *Soit $x$ un nombre complexe. Les conditions suivantes sont équivalentes.*

*(i) Le nombre $x$ appartient à $\overline{\mathbb{Z}}$.*

*(ii) Le groupe additif du sous-anneau $\mathbb{Z}[x]$ de $\mathbb{C}$ est de type fini.*

*(iii) Le nombre $x$ appartient à un sous-anneau de $\mathbb{C}$ dont le groupe additif est de type fini.*

*(iv) Il existe un sous-groupe de type fini $G$ de $(\mathbb{C}, +)$ tel que*

$$xG \subset G.$$

*Preuve.* Supposons $(i)$. Soit $P$ un polynôme unitaire de degré $n$ de $\mathbb{Z}[X]$ annulant $x$. On voit facilement que le sous-groupe de $\mathbb{C}$ engendré par la famille $(x^k)_{0 \leq k \leq n-1}$ contient $x^\ell$ pour tout $\ell \geq n$, donc est égal à $\mathbb{Z}[x]$.

Les implications $(ii) \Longrightarrow (iii)$ et $(iii) \Longrightarrow (iv)$ sont immédiates.

Supposons enfin $(iv)$. Soient $G$ un sous-groupe additif de type fini de $\mathbb{C}$ stable par multiplication par $x$, $(a_1, \ldots, a_m)$ une famille génératrice de $G$. Pour $1 \leq i \leq m$, $xa_i$ s'écrit

$$\sum_{j=1}^{m} \lambda_{i,j}\, a_j \quad \text{avec} \quad (\lambda_{i,1}, \ldots, \lambda_{i,m}) \in \mathbb{Z}^m.$$

C'est dire que $x$ est valeur propre de la matrice $(\lambda_{i,j})_{1\leq i,j\leq m}$. Comme cette matrice est dans $\mathcal{M}_m(\mathbb{Z})$, son polynôme caractéristique est unitaire à coefficients entiers : $x$ appartient à $\overline{\mathbb{Z}}$.

**Théorème 9.** *L'ensemble $\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$.*

*Preuve.* En considérant, pour $a \in \mathbb{Z}$, le polynôme $X - a$, on voit que $\overline{\mathbb{Z}}$ contient $\mathbb{Z}$. Soient $x$ et $y$ dans $\overline{\mathbb{Z}}$. Soient $P$ et $Q$ deux polynômes unitaires de $\mathbb{Z}[X]$, annulant respectivement $x$ et $y$, de degrés respectifs $n$ et $p$. On vérifie immédiatement que la famille finie $\left(x^i y^j\right)_{\substack{0\leq i\leq n-1\\ 0\leq j\leq p-1}}$ engendre le sous-anneau $\mathbb{Z}[x, y]$ de $\mathbb{C}$. Ce sous-anneau est donc contenu dans $\overline{\mathbb{Z}}$, ce qui montre en particulier que $x - y$ et $xy$ appartiennent à $\overline{\mathbb{Z}}$.

**Exemples**

1. Si $z \in \overline{\mathbb{Z}}$, alors $2\,\mathrm{Re}(z) = z + \overline{z} \in \overline{\mathbb{Z}}$ et $2\,\mathrm{Im}(z) = i\,(\overline{z} - z) \in \overline{\mathbb{Z}}$.

   En particulier, si $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$, on retrouve très simplement le résultat de l'exercice 70 :

   $$2\cos\left(\frac{2k\pi}{n}\right) \in \overline{\mathbb{Z}} \quad \text{et} \quad 2\sin\left(\frac{2k\pi}{n}\right) \in \overline{\mathbb{Z}}.$$

2. Si $x \in \mathbb{C}$ est valeur propre d'une matrice de $\mathcal{M}_n(\mathbb{Z})$, $x \in \overline{\mathbb{Z}}$. Réciproquement, si $x \in \overline{\mathbb{Z}}$ est de degré $n$ sur $\mathbb{Q}$, $x$ est valeur propre de la matrice compagnon de $\Pi_{\mathbb{Q},x}$, laquelle appartient à $\mathcal{M}_n(\mathbb{Z})$.

**Remarques**

1. *Autres démonstrations du théorème 9*

   On peut démontrer le théorème 9 sans recours au théorème 8, en utilisant le théorème des polynômes symétriques. Il suffit à cet effet de reprendre la remarque 1 de **2.1**. Soient $P$ et $Q$ dans $\mathbb{Z}[X]$, unitaires, annulant respectivement $x$ et $y$. Factorisons $P$ et $Q$ sur $\mathbb{C}$ :

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

   Alors

   $$S = \prod_{1\leq i\leq n,\ 1\leq j\leq m} (X - (x_i + y_j))$$

   annule $x + y$. D'autre part

   $$S = \prod_{j=1}^{m} P(X - y_j)$$

   est à coefficients dans $\mathbb{Z}$ grâce au théorème des polynômes symétriques. On procède de même pour $xy$, en considérant

   $$T = \prod_{1\leq i\leq n,\ 1\leq j\leq m} (X - x_i\, y_j)\,.$$

   On peut aussi démontrer le théorème 9 à l'aide du résultant (adapter la remarque 2 de **2.1**).

2. *Retour sur la caractérisation en termes de polynôme minimal*
   Le théorème 9 permet de retrouver le lemme 1 de **1.4**, i.e. le fait que, si $x \in \overline{\mathbb{Z}}$, $\Pi_{\mathbb{Q},x}$ est dans $\mathbb{Z}[X]$. Soit en effet $P \in \mathbb{Z}[X]$ unitaire annulant $x$. Les racines de $P$ sont dans $\overline{\mathbb{Z}}$. Puisque $\Pi_{\mathbb{Q},x}$ divise $P$ dans $\mathbb{Q}[X]$, les formules de Viète montrent que les coefficients de $\Pi_{\mathbb{Q},x}$ sont dans $\overline{\mathbb{Z}}$. Mais ces coefficients sont rationnels, d'où la conclusion via le lemme 9.
3. *Lien entre $\overline{\mathbb{Q}}$ et $\overline{\mathbb{Z}}$*
   **Lemme 10.** *Soit $x \in \overline{\mathbb{Q}}$. Il existe $q \in \mathbb{N}^*$ tel que $qx \in \overline{\mathbb{Z}}$.*
   *En particulier, $\overline{\mathbb{Q}}$ est le corps des fractions de $\overline{\mathbb{Z}}$.*
   *Preuve.* Soient $\Pi_{\mathbb{Q},x} = X^n + \sum_{k=0}^{n-1} a_k\, X^k$ et $q \in \mathbb{N}^*$. Si $y = qx$, $y$ annule $X^n + \sum_{k=0}^{n-1} a_k\, q^{n-k}\, X^k$.
   Si, pour tout $k \in \{0, \dots, n-1\}$, le nombre rationnel $qa_k$ est entier, le polynôme précédent est unitaire et dans $\mathbb{Z}[X]$ et $y$ appartient à $\overline{\mathbb{Z}}$. Il suffit ainsi de choisir pour $q$ le ppcm des dénominateurs des rationnels $a_0, \dots, a_{n-1}$.

L'exercice suivant propose une autre démonstration du théorème 9, qui déguise un argument tensoriel.

**Exercice 74.** ④ *Soient $x$ et $y$ deux éléments de $\overline{\mathbb{Z}}$ de degrés respectifs $m$ et $n$, $A$ (resp. $B$) la matrice compagnon du polynôme minimal de $x$ (resp. $y$) sur $\mathbb{Q}$. En considérant l'endomorphisme de $\mathcal{M}_{m,n}(\mathbb{C})$ :*

$$M \longmapsto AMB,$$

*montrer que $xy$ est un entier algébrique. Donner un argument analogue pour $x + y$.*

**Exercice 75.** ② *Soit $x \in \overline{\mathbb{Q}}$. Montrer que $\{q \in \mathbb{Z}\ ;\ q\, x \in \overline{\mathbb{Z}}\}$ est un idéal non nul de $\mathbb{Z}$.*

**Exercice 76.** ⑤ *Quels sont les $r \in \mathbb{Q}$ tels que $\cos(\pi r) \in \overline{\mathbb{Z}}$ ?*

*L'anneau des entiers d'un corps de nombres*

L'anneau des entiers algébriques est « trop gros » pour jouir d'une arithmétique satisfaisante. En revanche, on peut associer à tout corps de nombre $\mathbb{K}$ le sous-anneau

$$\mathbb{Z}_{\mathbb{K}} = \mathbb{K} \cap \overline{\mathbb{Z}},$$

nommé *anneau des entiers de* $\mathbb{K}$. Ces anneaux ont une arithmétique particulière, qui généralise de faaçon subtile celle de $\mathbb{Z}$ : ils ne sont généralement pas factoriels, mais tout idéal non nul est, d'une façon unique, produit d'idéaux premiers (Dedekind). [30]

**Exercice 77.** ③ *Montrer que l'anneau $\overline{\mathbb{Z}}$ n'est pas noetherien.*

La détermination de l'anneau des entiers d'un corps de nombres est en général délicate. Voici un exemple classique relativement simple. Dans le chapitre **3** (sections **6** et **7**), nous introduirons de nouveaux outils et donnerons d'autres exemples.

**Proposition 13.** *Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré. L'anneau des entiers du corps quadratique $\mathbb{Q}\left(\sqrt{d}\right)$ est :*

- $\mathbb{Z}\left[\sqrt{d}\right] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$ *si* $d \equiv 2\ [4]$ *ou* $d \equiv 3\ [4]$,
- $\mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] = \mathbb{Z} \oplus \mathbb{Z}\dfrac{1+\sqrt{d}}{2}$ *si* $d \equiv 1\ [4]$.

30. Par ailleurs, on sait décrire leur groupe d'inversibles (Dirichlet).

*Preuve.* Soient $(a,b) \in \mathbb{Q}^2$ et $x = a + b\sqrt{d}$. Si $b = 0$, $x$ est rationnel et est donc un entier algébrique si et seulement s'il est entier. Sinon $x$ est irrationnel, donc de degré 2 sur $\mathbb{Q}$.

Supposons donc $b \neq 0$. Le polynôme $X^2 - 2aX + a^2 - b^2d$ annule $x$, c'est donc le polynôme minimal de $x$, et $x$ est entier algébrique si et seulement si $2a \in \mathbb{Z}$ et $a^2 - b^2d \in \mathbb{Z}$.

Posons donc $a = \dfrac{a'}{2}$ avec $a' \in \mathbb{Z}$. La seconde condition s'écrit :

$$a'^2 - 4b^2d \in 4\mathbb{Z} \quad \text{d'où} \quad 4b^2d \in \mathbb{Z}.$$

Puisque $d$ est sans facteur carré, la considération des facteurs premiers montre alors que $2b \in \mathbb{Z}$. Ainsi, $b = \dfrac{b'}{2}$ avec $b' \in \mathbb{Z}$. Avec ces notations, $x$ est entier algébrique si et seulement si

$$(1) \qquad a'^2 - b'^2 d \in 4\mathbb{Z}.$$

*Premier cas : $d \equiv 1$ [4].* Alors

$$(1) \iff a'^2 - b'^2 \in 4\mathbb{Z} \iff (a' - b')(a' + b') \in 4\mathbb{Z}.$$

Autrement dit (1) a lieu si et seulement si $a' - b'$ est pair.

*Second cas : $d \equiv 2$ [4].* Alors

$$(1) \Leftrightarrow a'^2 - 2b'^2 \in 4\mathbb{Z}.$$

L'étude des congruences modulo 4 montre que ceci est vrai si et seulement si $a'$ et $b'$ sont pairs.

*Troisième cas $d \equiv 3$ [4].* On arrive au même résultat qu'en b).

**Exercice 78.** ① *Vérifier que, pour tout $d$ de $\mathbb{Z}^*$ sans facteur carré, l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ est de la forme $\mathbb{Z}[\alpha]$.*

**Exercice 79.** ③ *Soient $a$ et $b$ dans $\mathbb{Z}$, $(u_n)_{n\in\mathbb{N}}$ une suite d'entiers telle que $u_0 = 0$ et*

$$\forall n \in \mathbb{N}, \qquad u_{n+2} = au_{n+1} + bu_n.$$

*Montrer que, si $m$ divise $n$, $\dfrac{u_n}{u_m} \in \overline{\mathbb{Z}}$ ; en déduire que $u_m$ divise $u_n$.*

**Exercice 80.** ③ *Soient $n \geq 3$ un entier, $x \in \mathbb{R}$ tels que $x^2 - x := a$ et $x^n - x := b$ soient dans $\mathbb{Z}$. On suppose dans les questions a) et b) que $x \notin \mathbb{Z}$.*

*a) Déterminer $\Pi_{\mathbb{Q},x}$.*

*b) En déduire que* $\left(\dfrac{1+\sqrt{1+4a}}{2}\right)^n - \left(\dfrac{1-\sqrt{1+4a}}{2}\right)^n = \left(\dfrac{1-\sqrt{1+4a}}{2}\right) - \left(\dfrac{1+\sqrt{1+4a}}{2}\right)$.

*c) Obtenir une contradiction : le nombre réel $x$ est donc entier.*

## 5.2 Application : congruences dans $\overline{\mathbb{Z}}$ et loi de réciprocité quadratique

Ce paragraphe est un intermède destiné à montrer l'intérêt de l'anneau $\overline{\mathbb{Z}}$. Des congruences dans cet anneau vont nous aider à établir la loi de réciprocité quadratique de Gauss.

*Critère d'Euler et symbole de Legendre*

Soit $p$ un nombre premier impair. Nous allons étudier les carrés de $\mathbb{F}_p$.

**Proposition 14.** *(i) Il y a exactement* $\frac{p-1}{2}$ *carrés et* $\frac{p-1}{2}$ *non carrés dans* $\mathbb{F}_p^*$.

*(ii) Si* $x \in {\mathbb{F}_p}^*$, $x^{\frac{p-1}{2}} = 1$ *si* $x$ *est un carré et* $x^{\frac{p-1}{2}} = -1$ *sinon.*

*Preuve.* Les éléments de ${\mathbb{F}_p}^*$ sont racines de $X^{p-1} - 1$ ; les carrés de $\mathbb{F}_p^*$ sont donc racines de $X^{\frac{p-1}{2}} - 1$ D'autre part, $x \mapsto x^2$ est un endomorphisme de $({\mathbb{F}_p}^*, \times)$ de noyau $\{\pm 1\}$, et il y a donc $\frac{p-1}{2}$ carrés dans $({\mathbb{F}_p}^*, \times)$. Puisque $X^{\frac{p-1}{2}} - 1$ ne peut avoir plus de $\frac{p-1}{2}$ racines dans $\mathbb{F}_p$, ses racines sont exactement les carrés de ${\mathbb{F}_p}^*$. On conclut avec l'identité :

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

Le point *(ii)* est connu comme *critère d'Euler.*

Pour $x \in \mathbb{Z}$, définissons maintenant le symbole de Legendre $\left(\frac{x}{p}\right)$ par :

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{si } x = 0 \\ 1 & \text{si } x \text{ est un carré non nul modulo } p, \text{ i.e. si la classe de } x \text{ dans } \mathbb{F}_p \text{ est un carré non nul} \\ -1 & \text{sinon} \end{cases}$$

On déduit de la proposition 14 le premier point de la proposition suivante, qui lui-même entraîne immédiatement les deux autres

**Proposition 15.** *(i) Si* $x \in \mathbb{Z}$,

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \ [p].$$

*(ii) Le symbole de Legendre est multiplicatif, i.e.*

$$\forall (x, y) \in \mathbb{Z}^2, \qquad \left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\ \left(\frac{y}{p}\right).$$

*(iii) Le nombre* $-1$ *est un carré modulo* $p$ *si et seulement si* $p \equiv 1\ [4]$.

**Exercice 81.** ② *Utiliser la cyclicité de* $(\mathbb{F}_p^*, \times)$ *pour donner une preuve plus rapide du critère d'Euler.*

**Exercice 82.** ③ *Supposons* $p \equiv 1[4]$. *Montrer que l'ensemble* $\left\{1, \ldots, \frac{p-1}{2}\right\}$ *contient autant de résidus quadratiques modulo* $p$ *que de non-résidus quadratiques*[31].

**Exercice 83.** ④ *Soient* $(a, b) \in {\mathbb{F}_p^*}^2$ *et* $c \in \mathbb{F}_p$. *On pose :*

$$C = \left\{(x, y) \in {\mathbb{F}_p}^2 \ ;\ ax^2 + by^2 = c\right\}.$$

*a) Montrer que* $C \neq \emptyset$.

*b) Dénombrer* $C$. *En particulier, pour* $c \neq 0$, *montrer que* $|C| = p - \left(\frac{-abc}{p}\right)$. *On pourra paramétrer la conique* $C$ *par la méthode de la corde*[32].

31. Si $p \equiv 3\ [4]$, on peut démontrer, en utilisant des méthodes analytiques (fonctions $L$ de Dirichlet) qu'il y a davantage de résidus quadratiques que de non résidus quadratiques dans $\left\{1, \ldots, \frac{p-1}{2}\right\}$.

32. Cette méthode, qui montre qu'une conique est unicursale (c'est-à-dire peut qu'elle admet une paramétrisation rationnelle) consiste à partir d'un point $(x_0, y_0)$ de $C$, à mener par ce point une droite affine et en examinant si cette droite recoupe $C$.

Le résultat de l'exercice suivant est souvent connu comme « théorème de Frobenius-Zolotarev ».

**Exercice 84.** ⑤ *Soient $p \in \mathcal{P} \setminus \{2\}$, $E$ un $\mathbb{F}_p$-espace vectoriel de dimension finie, $u \in GL(E)$. Montrer la signature de $u$ vu comme permutation de $E$ est $\left(\dfrac{\det(u)}{p}\right)$.*

**Exercice 85.** ③ *On suppose $p \equiv 1\ [4]$. Déduire du théorème de Wilson un entier $x$ tel que $x^2 \equiv -1\ [p]$.*

**Exercice 86.** ④ *Si $(a,b) \in {\mathbb{F}_p}^2$, montrer que le polynôme $X^4 + aX^2 + b^2$ est réductible sur $\mathbb{F}_p$.*

**Exercice 87.** ③ *Montrer que $X^8 - 16$ admet une racine dans $\mathbb{F}_p$.*

*La loi de réciprocité quadratique*

La proposition 15 ramène le calcul de $\left(\dfrac{x}{p}\right)$ au cas où $x$ est premier. Ce cas est l'objet du célèbre énoncé suivant, établi par Gauss, et dont le second volet porte le nom de *loi de réciprocité quadratique*.

**Théorème 10.** *(i) Si $p$ est un nombre premier impair,*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

*(ii) Si $p$ et $p'$ sont deux nombres premiers impairs distincts,*

$$\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right) = (-1)^{\frac{(p-1)(p'-1)}{4}}.$$

Ainsi les assertions « $p'$ est un carré modulo $p$ » et « $p$ est un carré modulo $p'$ » sont simultanément vraies si $p \equiv 1\ [4]$ ou $p' \equiv 1\ [4]$, incompatibles sinon.

Avant de prouver le théorème, observons qu'on obtient en y spécifiant $p'$ des énoncés concrets. Ainsi, si $p \neq 5$ :

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} 1 & \text{si} \quad p \equiv \pm 1\ [5] \\ -1 & \text{si} \quad p \equiv \pm 2\ [5] \end{cases}$$

D'autre part, si on fixe $p'$, on voit que $\left(\frac{p'}{p}\right)$ ne dépend que de la classe modulo $4p'$ du nombre premier $p$, fait nullement évident a priori.

**Exercice 88.** ③ *Soit $p \in \mathcal{P} \setminus \{2,3\}$. Montrer que $-3$ est un carré modulo $p$ si et seulement si $p \equiv 1\ [3]$. On donnera une démonstration fondée sur les résultats précédents et une autre, plus directe, en observant que, si $x$ est dans $\mathbb{F}_p$, $x$ est un élément d'ordre 3 de $\mathbb{F}_p^*$ si et seulement si $x^2 + x + 1 = 0$ et en notant que le discriminant de ce trinôme est $-3$.*

*Principe de la démonstration*

On connaît de nombreuses démonstrations du théorème 10. Certaines sont complètement élémentaires : « tout se passe dans $\mathbb{Z}$ ». D'autres font intervenir des racines de l'unité dans des anneaux adéquats. Nous travaillerons dans $\overline{\mathbb{Z}}$. [33]

33. On peut écrire une démonstration très proche de celle qui suit en se plaçant dans des corps finis.

Si $p' \in \mathcal{P} \setminus \{p\}$, nous allons expliciter un élément $g$ de $\overline{\mathbb{Z}}$, combinaison linéaire à éléments $\pm 1$ des racines $p'$-ièmes de 1, et deux éléments $s$ et $s'$ de $\{-1, 1\}$ tels que

$$(1) \qquad g^2 = sp' \quad \text{et} \quad g^p \equiv s'g \ [p\overline{\mathbb{Z}}].$$

On en déduira que

$$p'^{\frac{p-1}{2}} = s^{\frac{p-1}{2}} g^{p-1}, \quad \text{d'où} \quad gp'^{\frac{p-1}{2}} = s^{\frac{p-1}{2}} g^p, \quad \text{puis} \quad gp'^{\frac{p-1}{2}} \equiv s^{\frac{p-1}{2}} s'g \ [p\overline{\mathbb{Z}}].$$

Multipliant cette congruence par $g$, on obtiendra finalement que

$$g^2 p'^{\frac{p-1}{2}} \equiv s^{\frac{p-1}{2}} s' g^2 \ [p\overline{\mathbb{Z}}].$$

Comme les deux membres de cette dernière congruence sont dans $\mathbb{Z}$, le lemme 9 amènera que la congruence est vraie modulo $p\mathbb{Z}$. Enfin, comme $g^2 = \pm p'$, on en déduira que

$$p'^{\frac{p-1}{2}} \equiv s' s^{\frac{p-1}{2}} \ [p\mathbb{Z}],$$

c'est-à-dire que

$$(2) \qquad \left(\frac{p'}{p}\right) = s' s^{\frac{p-1}{2}}.$$

L'expression explicite de $s$ et $s'$ permettra de conclure.

La seconde relation de (1) se déduira du lemme suivant.

**Lemme 11.** *Soient $p \in \mathcal{P}$, $\mathbb{A}$ un anneau commutatif, $(x, y) \in \mathbb{A}^2$. Alors :*

$$(x + y)^p \equiv x^p + y^p \ [pA].$$

*Preuve.* Il suffit d'utiliser la formule du binôme et le fait que, si $k \in \{1, \ldots, p-1\}$, $\binom{p}{k}$ est divisible par $p$.

**Exercice 89.** ③ *Soient $p \in \mathcal{P}$, $n \in \mathbb{N}^*$, $M \in \mathcal{M}_n(\mathbb{Z})$. Montrer que $tr(M^p) \equiv tr(M) \ [p]$.* [34]

*Calcul de $\left(\frac{2}{p}\right)$*

Pour $p' = 2$, on part de

$$2 = \left(2\cos\left(\frac{\pi}{4}\right)\right)^2 = \varepsilon_8 + {\varepsilon_8}^{-1}, \text{ où } \varepsilon_8 = \exp\left(\frac{2i\pi}{8}\right).$$

On pose donc $g = \varepsilon_8 + {\varepsilon_8}^{-1}$. Grâce au lemme 11,

$$g^p \equiv {\varepsilon_8}^p + {\varepsilon_8}^{-p} \ [p\,\overline{\mathbb{Z}}].$$

Mais on vérifie immédiatement, en discutant selon la classe de $p$ modulo 8, que

$${\varepsilon_8}^p + {\varepsilon_8}^{-p} = (-1)^{\frac{p^2-1}{8}} g.$$

On termine en appliquant la formule (2) avec $s = 1$ et $s' = (-1)^{\frac{p^2-1}{8}}$.

34. Comparer à l'exercice 59 de **3.1**.

**Exercice 90.** ② *Pour quels nombres premiers impairs $-2$ est-il résidu quadratique modulo $p$ ?*

*Sommes de Gauss et démonstration de la loi de réciprocité quadratique*

**Lemme 12.** *Soient $p'$ un nombre premier impair, $\mathbb{A}$ un anneau et $\xi$ un élément de $\mathbb{A}\setminus\{1\}$ tel que $\xi^{p'}=1$. Pour $x\in\mathbb{F}_{p'}$, on définit $\xi^x$ et $\left(\frac{x}{p'}\right)$ de la façon naturelle, et on pose :*

$$g=\sum_{x\in{\mathbb{F}_{p'}}^*}\left(\frac{x}{p'}\right)\xi^x.$$

*On a alors les deux propriétés ci-après :*

*(i)* $g^2=\left(\frac{-1}{p'}\right)p'$,

*(ii)* $g^p\equiv\left(\frac{p}{p'}\right)g\ [p\mathbb{A}]$.

La somme définissant $g$ est une *somme de Gauss*. Prenons $\mathbb{A}=\overline{\mathbb{Z}}$ et $\xi=\exp\left(\frac{2i\pi}{p'}\right)$. Les relations (1) sont satisfaites, avec

$$s=(-1)^{\frac{p'-1}{2}}\quad\text{et}\quad s'=\left(\frac{p}{p'}\right).$$

L'application de la relation (2) donne la loi de réciprocité quadratique.

*Preuve du lemme 12.* Nous utiliserons les deux relations :

$$\sum_{a\in{\mathbb{F}_p'}^*}\left(\frac{a}{p'}\right)=0\qquad\text{et}\qquad\sum_{x\in\mathbb{F}_{p'}}\xi^{\mu x}=\begin{cases}p' & \text{si}\quad \mu=0\\ 0 & \text{si}\quad \mu\in{\mathbb{F}_{p'}}^*\end{cases}.$$

La première vient du fait qu'il y a autant de carrés que de non carrés dans ${\mathbb{F}_{p'}}^*$ ; l'autre est un simple calcul de somme de progression géométrique.

*Preuve de (i).* On part de :

$$g^2=\sum_{(x,y)\in({\mathbb{F}_{p'}}^*)^2}\left(\frac{xy}{p'}\right)\xi^{x+y},$$

et on effectue le changement de variable $y=\lambda x$. Il vient :

$$g^2=\sum_{(x,\lambda)\in({\mathbb{F}_{p'}}^*)^2}\left(\frac{\lambda x^2}{p'}\right)\xi^{x(1+\lambda)}=\sum_{\lambda\in{\mathbb{F}_{p'}}^*}\left(\frac{\lambda}{p'}\right)S_\lambda\qquad\text{où}\quad S_\lambda=\sum_{x\in{\mathbb{F}_{p'}}^*}\xi^{x(1+\lambda)}.$$

Or :

$$S_\lambda=\begin{cases}-1 & \text{si}\quad \lambda\in{\mathbb{F}_{p'}}^*\setminus\{-1\}\\ p'-1 & \text{si}\quad \lambda=-1\end{cases},$$

d'où :

$$g^2=(p'-1)\left(\frac{-1}{p'}\right)-\sum_{\lambda\in{\mathbb{F}_{p'}}^*\setminus\{-1\}}\left(\frac{\lambda}{p'}\right)=p'\ \left(\frac{-1}{p'}\right).$$

*Preuve de (ii).* Le lemme 11 entraîne que

$$g^p \equiv \sum_{x\in\mathbb{F}_{p'}{}^*} \left(\frac{x}{p'}\right)^p \xi^{px}\ [p\mathbb{A}] \quad \text{i.e. que} \quad g^p \equiv \sum_{x\in\mathbb{F}_{p'}{}^*} \left(\frac{x}{p'}\right) \xi^{px}\ [p\mathbb{A}].$$

Le changement de variable $y = px$ donne alors la formule désirée.

**Exercice 91.** ④ *Soit $(F_n)_{n\geq 0}$ la suite de Fibonacci définie par :*

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

*Si $p \in \mathcal{P} \setminus \{2\}$, montrer que $F_p \equiv \left(\frac{p}{5}\right)\ [p]$.*

L'exercice ci-après est le *test de primalité de Pépin* pour les nombres premiers de Fermat.

**Exercice 92.** ③ *Pour $n \in \mathbb{N}^*$, soit $F_n = 2^{2^n} + 1$. Montrer que $F_n$ est premier si et seulement si*

$$3^{\frac{F_n-1}{2}} \equiv -1\ [F_n].$$

*Si tel est le cas, montrer que la classe de 3 modulo $F_n$ engendre $\mathbb{F}_{F_n}^*$.*

**Exercice 93.** ④ *Soient $n$ un entier $\geq 2$, $F_n = 2^{2^n} + 1$, $p$ un diviseur premier de $F_n$. Montrer que $p \equiv 1\ [2^{n+2}]$. On déterminera l'ordre de la classe de 2 modulo $p$ et on remarquera que 2 est un carré modulo $p$.*

## 5.3 Extensions d'anneaux et intégralité : cas général

Dans ce paragraphe, $\mathbb{A}$ est un anneau commutatif et $\mathbb{B}$ une $\mathbb{A}$-algèbre, c'est-à-dire la donnée d'un morphisme de $\mathbb{A}$ dans $\mathbb{B}$. La situation la plus évidente est celle où $\mathbb{A}$ est un sous-anneau de $\mathbb{B}$. Cependant, contrairement à ce qui se passe dans le cas des corps, on restreindrait la généralité en se bornant à ce cas (remarque, **1.1**).

Sous les hypothèses précédentes, on parle encore de *l'extension d'anneaux* $\mathbb{B}/\mathbb{A}$. L'élément $x$ de $\mathbb{B}$ est dit *entier sur* $\mathbb{A}$ s'il existe un polynôme unitaire $P$ à coefficients dans $\mathbb{A}$ tel que $P(x) = 0$. Si $\mathbb{A}$ est un corps, « $x$ entier sur $\mathbb{A}$ » revient à « $x$ algébrique sur $\mathbb{A}$ ».

*Adjonction*

Si $E$ est une partie de $\mathbb{B}$, on note $\mathbb{A}[E]$ la plus petite $\mathbb{A}$-sous-algèbre de $\mathbb{B}$ contenant $\mathbb{A}$ (en cohérence avec **2.1** et **5.1**). Si $E = \{x_1, \ldots, x_m\}$ est fini, on note $\mathbb{A}[E] = \mathbb{A}[x_1, \ldots, x_m]$. On a :

$$\mathbb{A}[x_1, \ldots, x_m] = \{P(x_1, \ldots, x_m),\ P \in \mathbb{A}[X_1, \ldots, X_m]\}\,.$$

En particulier, pour $x$ dans $\mathbb{B}$ :

$$\mathbb{A}[x] = \{P(x)\ ;\ P \in \mathbb{A}[X]\}\,.$$

*Extensions finies et linéarisation de l'intégralité*

Comme dans le cas des corps, on dit que l'extension d'anneaux $\mathbb{B}/\mathbb{A}$ est *finie* si $\mathbb{B}$ est un $\mathbb{A}$-module de type fini. Ceci signifie que $\mathbb{B}$ admet une famille génératrice finie comme $\mathbb{A}$-module i.e., une famille $\{x_1, \ldots, x_n\}$ d'éléments de $\mathbb{B}$ telle que tout élément de $\mathbb{B}$ soit combinaison $\mathbb{A}$-linéaire des $x_i$.[35] On généralise alors simultanément la proposition 2 et le théorème 8.

35. On notera que l'on généralise la notion de « dimension finie » sans pour autant définir un invariant numérique appelé dimension.

**Théorème 11.** *Soit $x \in \mathbb{B}$. Les trois assertions suivantes sont équivalentes.*

*i) L'élément $x$ est entier sur $\mathbb{A}$.*

*ii) L'anneau $\mathbb{A}[x]$ est un $\mathbb{A}$-module de type fini.*

*iii) Il existe un sous-anneau $\mathbb{A}'$ de $\mathbb{B}$ contenant $\mathbb{A}[x]$ qui est un $\mathbb{A}$-module de type fini ;*

*iv) Il existe un $\mathbb{A}$-sous-module $\mathbb{M}$ de type fini de $\mathbb{B}$ tel que*

$$x\mathbb{M} \subset \mathbb{M}.$$

*Preuve.* Supposons *i)* . Soit $P \in \mathbb{A}[X]$ unitaire de degré $n$ annulant $x$. On voit immédiatement que le groupe additif du sous-anneau $\mathbb{A}[x]$ de $\mathbb{B}$ est engendré comme $\mathbb{A}$-module par la famille finie $(x^k)_{0\leq k\leq n-1}$.

Les implications *ii)* $\Longrightarrow$ *iii)* et *iii)* $\Longrightarrow$ *iv)* sont immédiates.

Pour l'implication *iv)* $\Rightarrow$ *i)*, on peut, si $\mathbb{A}$ est intègre, reprendre la démonstration de l'implication correspondante du théorème 8. Dans le cas général, on l'adapte comme suit. Soit $\mu_x$ l'endomorphisme de multiplication par $x$ dans le $\mathbb{A}$-module $\mathbb{M}$. En appliquant à $\mu_x$ le lemme ci-après, on obtient $\lambda_0, \ldots, \lambda_{n-1}$ dans $A$ tels que :

$$x^n + \sum_{i=0}^{n-1} \lambda_i x^i = 0.$$

**Lemme 13.** *Soient $\mathbb{M}$ un $\mathbb{A}$-module de type fini et $\varphi$ dans $End_{\mathbb{A}}(\mathbb{M})$. Il existe alors $\lambda_0, \ldots, \lambda_{n-1}$ dans $\mathbb{A}$ tels que :*

$$\varphi^n + \sum_{i=0}^{n-1} \lambda_i \varphi^i = 0.$$

*Preuve.* Soient $\{v_1, \ldots, v_n\}$ une famille génératrice de $\mathbb{M}$ comme $\mathbb{A}$-module. Si $1 \leq j \leq n$, on écrit : $\varphi(v_j) = \sum_{i=1}^{n} M_{i,j} v_i$ où les $M_{i,j}$ sont dans $\mathbb{A}$. La matrice $M = (M_{i,j})_{1\leq i,\, j\leq n}$ de $\mathcal{M}_n(\mathbb{A})$ vérifie l'identité de Cayley-Hamilton [36], d'où une relation :

$$M^n + \sum_{i=0}^{n-1} \lambda_i M^i = 0 \quad \text{où les } \lambda_i \text{ sont dans } \mathbb{A}.$$

La démonstration du théorème 9 s'étend alors pour donner le résultat suivant, que l'on peut également établir via le théorème des polynômes symétriques, en reprenant la remarque 1 de **6.1**.

**Théorème 12.** *L'ensemble des éléments de $\mathbb{B}$ entiers sur $\mathbb{A}$ est un sous-anneau de $\mathbb{B}$.*

36. L'identité de Cayley-Hamilton vaut pour une matrice à coefficients dans un anneau commutatif $\mathbb{A}$ quelconque. On peut le voir de plusieurs façons.

- Il en existe des démonstrations ne faisant appel qu'aux propriétés des déterminants vraies sur un anneau commutatif.

- On peut se ramener au cas des corps de la manière suivante. Notons $\mathbb{Z}[T_{i,j} \ ; \ 1 \leq i,j \leq n]$ l'anneau des polynômes à une indéterminée à coefficients dans $\mathbb{Z}$. Comme un sous-anneau du corps $\mathbb{Q}(T_{i,j} \ ; \ 1 \leq i,j \leq n)$, il vérifie l'identité de Cayley-Hamilton. Si maintenant $\mathbb{A}$ est un anneau commutatif quelconque et si $M = (M_{i,j})_{1\leq i,j\leq n}$ est dans $\mathcal{M}_n(\mathbb{A})$, on considère l'unique morphisme de $\mathbb{Z}[T_{i,j} \ ; \ 1 \leq i,j \leq n]$ dans $A$ envoyant, si $1 \leq i,j \leq n$, $T_{i,j}$ sur $M_{i,j}$. L'identité de Cayley-Hamilton pour la matrice générique de $\mathcal{M}_n(\mathbb{Z}[T_{i,j} \ ; \ 1 \leq i,j \leq n])$ entraîne l'identité de Cayley-Hamilton pour $M$.

Poursuivons l'analogie avec la théorie des extensions de corps. La propriété de transitivité de la finitude se généralise immédiatement.

**Lemme 14.** *Soient $\mathbb{B}/\mathbb{A}$ et $\mathbb{C}/\mathbb{B}$ deux extensions d'anneaux finies. Alors $\mathbb{C}/\mathbb{A}$ est finie.*

*Preuve.* Si $(e_i)_{1\leq i\leq m}$ (resp. $(f_j)_{1\leq j\leq n}$) engendre $\mathbb{B}$ comme $\mathbb{A}$-module (resp. $\mathbb{C}$ comme $\mathbb{B}$-module), alors $(e_i f_j)_{\substack{1\leq i\leq m\\ 1\leq j\leq n}}$ engendre $\mathbb{C}$ comme $\mathbb{A}$-module.

En recopiant la preuve de la caractérisation des extensions finies (proposition 7, **2.2**), on en déduit la conséquence suivante.

**Proposition 16.** *L'extension $\mathbb{B}/\mathbb{A}$ est finie si et seulement s'il existe $n \in \mathbb{N}^*$ et des éléments $x_1, \ldots, x_n$ de $\mathbb{B}$ entiers sur $\mathbb{A}$ tels que $B = \mathbb{A}[x_1, \ldots, x_n]$.*

Enfin, la notion d'extension algébrique se généralise : l'extension $\mathbb{B}/\mathbb{A}$ est dite *entière* si et seulement si tout élément de $\mathbb{B}$ est entier sur $\mathbb{A}$. Une extension finie est entière, mais la réciproque est fausse : $\overline{\mathbb{Z}}$ n'est pas extension finie de $\mathbb{Z}$.

*Le cas où $\mathbb{A}$ est factoriel ; anneaux intégralement clos*

Si $\mathbb{A}$ est factoriel, on peut généraliser plusieurs faits établis pour $\mathbb{A} = \mathbb{Z}$. D'abord, les éléments du corps de fractions de $\mathbb{A}$ entiers sur $\mathbb{A}$ sont les éléments de $\mathbb{A}$. La preuve est fondée sur une généralisation immédiate du « test des racines rationnelles ».

**Lemme 15.** *Soient $\mathbb{A}$ un anneau factoriel de corps des fractions $\mathbb{K}$, $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{A}[X]$ de degré $n \geq 1$, $x \in \mathbb{K}$ une racine de $P$ : $x = \frac{p}{q}$, où $p$ et $q$ sont deux éléments de $\mathbb{A}$ premiers entre eux. Alors :*

$$p \mid a_0 \quad \textit{et} \quad q \mid a_n \ .$$

Il s'ensuit bien que, si $P$ est unitaire, les racines de $P$ dans le corps des fractions de $\mathbb{A}$ appartiennent à $\mathbb{A}$. Ceci suggère la définition suivante. Un anneau commutatif intègre $\mathbb{A}$ est dit *intégralement clos* si les seuls éléments du corps des fractions de $\mathbb{A}$ entiers sur $\mathbb{A}$ sont les éléments de $\mathbb{A}$. Le lemme 15 se spécialise en l'énoncé ci-après.

**Lemme 16.** *Un anneau factoriel est intégralement clos.*

On peut également décrire les éléments entiers sur $\mathbb{A}$ à l'aide de leur polynôme minimal sur le corps des fractions de $\mathbb{A}$. La preuve est la même que pour $\mathbb{Z}$ (lemme 1, **1.4**, reposant sur le lemme de Gauss sur les contenus).

**Lemme 17.** *Soient $\mathbb{A}$ un sous-anneau factoriel du corps $\mathbb{K}$, $\mathbb{L}$ une extension de $\mathbb{K}$ et $x$ un élément de $\mathbb{L}$ algébrique sur $\mathbb{K}$. Alors $x$ est entier sur $\mathbb{A}$ si et seulement si $\Pi_{\mathbb{K},x}$ appartient à $\mathbb{A}[X]$.*

Terminons en étendant le lemme 17 aux anneaux intégralement clos. [37]

**Lemme 18.** *Soient $\mathbb{A}$ un anneau intégralement clos de corps des fractions $\mathbb{K}$, $\mathbb{L}$ une extension de $\mathbb{K}$, $x \in \mathbb{L}$ algébrique sur $\mathbb{K}$. Alors $x$ est entier sur $\mathbb{A}$ si et seulement si $\Pi_{\mathbb{K},x}$ appartient à $\mathbb{A}[X]$.*

*Preuve.* Il suffit de reprendre la démonstration indiquée dans la remarque 2 de **5.1**.

37. Les anneaux intégralement clos apparaissent plus fréquemment que les anneaux factoriels. Par exemple, l'anneau des entiers d'un corps de nombres est intégralement clos, mais le plus souvent non factoriel.