Chapitre 2
Extensions de corps

Sommaire

Présentation du chapitre

On a vu dans le chapitre **1** que les propriétés d'une équation algébrique dépendent fortement du « corps de base ». Galois considérait des équations à coefficients dans un « domaine de rationalité », domaine auquel il « adjoignait des quantités ». La notion de corps est une formulation précise de l'idée de

domaine de rationalité. L'adjonction de quantités se traduit en termes modernes par le concept d'extension de corps.

Les premiers résultats sur les extensions sont des applications de l'algèbre linéaire. [1] L'idée principale est que *l'algébricité est une propriété de finitude*. En combinant la théorie des espaces vectoriels à la structure des idéaux de $\mathbb{K}[X]$, on obtient des preuves rapides et éclairantes des premiers théorèmes sur les nombres algébriques, ainsi qu'une description efficace du cadre de la théorie de Galois élémentaire : les *extensions finies*, étudiées dans la section **2**. Le point de vue des extensions éclaire l'étude des polynômes irréductibles. Les paragraphes **2.4** et **2.5** présentent des compléments, que le lecteur désireux d'aller vite à la théorie de Galois en caractéristique nulle pourra ignorer.

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 a longtemps été admis par les mathématiciens ; sa preuve n'est pas à proprement parler difficile, mais d'esprit assez différent de celui des sections précédentes. On établit également une version transfinie de cet énoncé, le théorème de Steinitz selon lequel tout corps admet une « clôture algébrique ». Il sera commode, lors de l'étude de la théorie de Galois de fixer une fois pour toutes une telle clôture ; en revanche, la démonstration de ce résultat n'est nullement fondamentale. [2]

Le lecteur qui souhaite un exposé rapide peut sans dommage se contenter de lire la section **1**, les paragraphes **2.1** à **2.4** et de survoler la section **3**. Les sections **4**, **5** et **6**, consacrées respectivement à la constructibilité à la règle et au compas et aux éléments entiers sur un anneau et à l'irrationalité et à la transcendance, sont entièrement optionnelles.

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.*

1. Ce point de vue remonte en substance à Dedekind.
2. Dans le cas « concret » des corps de nombres, le corps des nombres complexes algébriques est une clôture algébrique explicite.

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

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 $\displaystyle\sum_{i\in I}\alpha_{i,j}\lambda_i$ 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 μ_j comme combinaison $\mathbb{K}$-linéaire des λ_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 *On se donne V un $\mathbb{C}$-espace de dimension finie, u un endomorphisme de 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.*

La notion de degré a la conséquence suivante, qu'il ne semble pas aisé d'établir sans techniques linéaires.

Corollaire 2. *Soit $\mathbb{K}$ un corps fini. Alors il existe un nombre premier p tel que $|\mathbb{K}|$ soit une puissance exacte de p.* [3]

Remarque *Morphismes et extensions*

La définition des extensions de corps utilisée ici est adaptée à un premier cours. 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 φ est nécessairement injectif (lemme 1, **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 $\varphi(\mathbb{K})$. [4]

Cette définition des extensions par morphismes, plus souple que celle donnée plus haut, devient indispensable lorsqu'on remplace $\mathbb{K}$ par un anneau (**6.3**).

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 $E = \{x_1, \ldots, x_m\}$ est fini, on note $\mathbb{K}[E] = \mathbb{K}[x_1, \ldots, x_m]$. On a :

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

3. 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.

4. 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 ε 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 $\mathbb{R}[X]/(X^2 + 1)$ (cf **4.1**). 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

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

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

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

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

Exercice 4. ⑤ *Soient $\mathbb{A}_1, \ldots, \mathbb{A}_r$ 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 $E = \{x_1, \ldots, x_m\}$ est fini, on a :

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

et on note

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

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

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

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 $\mathbb{L}$. On suppose que l'extension $\mathbb{L}_1/(\mathbb{L}_1 \cap \mathbb{L}_2)$ est finie. Montrer que $\mathbb{L}_1\mathbb{L}_2/\mathbb{L}_2$ est finie 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 $\mathbb{L}_2$. [5]

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, $\mathbb{L}_1 \cap \mathbb{L}_2 = \mathbb{K}$.

5. 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.

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 :

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

L'image de δ_x est

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

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

Le noyau de δ_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, δ_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 $\mathbb{K}[X]$.

Le message de la proposition suivante est simple mais essentiel : *l'algébricité est une propriété de finitude.*

Proposition 1. *Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre, x un élément de $\mathbb{A}$.*

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 $\mathbb{K}$.

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 $\mathbb{K}$.

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 donc x algébrique de degré n sur $\mathbb{K}$. Par définition de $\Pi_{\mathbb{K},x}$, l'idéal annulateur de x dans $\mathbb{K}[X]$ ne contient aucun polynôme non nul de degré $\leq n-1$, d'où la liberté de $\left(1, x, \ldots, x^{n-1}\right)$. Observons ensuite que, si y est dans $\mathbb{K}[x]$, il s'écrit $P(x)$ 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 est de degré $\leq n-1$. Ceci montre que y est combinaison $\mathbb{K}$-linéaire de $1, x, \ldots, x^{n-1}$.

Corollaire 3. *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 $\lambda 1, \lambda \in \mathbb{K}$.
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 l'exemple précédent, 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 $\mathbb{K}$. On formalise ainsi la notion un peu vague du chapitre **1**.

1.4 Cas d'une algèbre intègre

Si x est un élément de la $\mathbb{K}$-algèbre $\mathbb{A}$ annulant le polynôme unitaire et irréductible P de $\mathbb{K}[X]$, on a 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 2. *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'était pas irréductible, on pourrait l'écrire comme produit de deux polynômes non constants. L'un au moins de ces deux polynômes annulerait x, contredisant la minimalité du degré de $\Pi_{\mathbb{K},x}$.

Nous avons utilisé dans le chapitre **1** l'existence d'une extension de $\mathbb{K}$ scindant un polynôme de $\mathbb{K}[X]$ donné. Ce fait sera établi un peu plus loin (**4.1**). En le combinant à la proposition 2, on voit que *l'étude des irréductibles de* $\mathbb{K}[X]$ *et celle des éléments algébriques d'une extension de* $\mathbb{K}$ *sont deux descriptions du même phénomène.*

Exemples

1. Le réel $2^{1/n}$ est de degré n sur $\mathbb{Q}$ et
$$\Pi_{\mathbb{Q},2^{1/n}} = X^n - 2.$$
2. Soit n un élément de $\mathbb{N}^*$. L'irréductibilité de Φ_n sur $\mathbb{Q}$ montre
$$\Pi_{\mathbb{Q},e^{2i\pi/n}} = \Phi_n.$$
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 π sont transcendants sur $\mathbb{Q}$. Ces résultats sont dûs respectivement à Hermite (1873) et Lindemann (1882).
5. Soient $\mathbb{K}$ un corps, F dans $\mathbb{K}(X)$ non constante. On écrit $F = A/B$ où A et B sont dans $\mathbb{K}[X]$ et $A \wedge B = 1$. On pose : $m = \max\{\deg A, \deg B\}$. Alors X est algébrique de degré m sur $\mathbb{K}(F)$. [6]

   En effet, l'indéterminée X est racine du polynôme $A(T) - FB(T)$ de $\mathbb{K}(F)[T]$. Reste à voir que $A(T) - FB(X)$ 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 2 du chapitre **1** (et donc, in fine, du lemme de Gauss) le fait suivant.

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

   Preuve. Il suffit de montrer que, si le polynôme unitaire P de $\mathbb{Z}[X]$ annule x, alors $\Pi_{\mathbb{Q},x}$ appartient à $\mathbb{Z}[X]$. Le théorème 2 du chapitre **1** montre qu'il existe Π dans $\mathbb{Z}[X]$ 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 $\mathbb{Z}[X]$.

6. 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.

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 *Soient* n *dans* $\mathbb{N}^*$, k *dans* $\mathbb{Z}$. *Montrer que* $\cos(2k\pi/n)$ *et* $\sin(2k\pi/n)$ *sont algébriques sur* $\mathbb{Q}$.

Exercice 10. ② *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 *un élément de degré* n *de* $\mathbb{K}[X]$. *Montrer que* P *est irréductible si et seulement si, pour toute extension finie* $\mathbb{L}$ *de* $\mathbb{K}$ *telle que* $[\mathbb{L}:\mathbb{K}] \leq n/2$, P *n'a pas de racine dans* $\mathbb{L}$.

Exercice 12. ③ *Soit* $x \in \overline{\mathbb{Q}}$. *Montrer qu'il existe un unique polynôme de* $\mathbb{Z}[X]$ *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.*[7]

1.5 Inversibles d'une algèbre monogène

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

Proposition 3. *Soient* $\mathbb{A}$ *une* $\mathbb{K}$*-algèbre,* x *un élément de* $\mathbb{A}$.

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 *est un élément de* $\mathbb{K}[X]$, *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 $\mathbb{K}$, δ_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 dans $\mathbb{K}[X]$ tel que

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

C'est donc dire 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 Π est un élément non constant de $\mathbb{K}[X]$, il y a équivalence entre :

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

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

Remarques

1. *Utilisation du quotient*
   Si x est algébrique sur $\mathbb{K}$, la considération du morphisme δ_x montre que la $\mathbb{K}$-algèbre $\mathbb{K}[x]$ est isomorphe à $\mathbb{K}[X]/(\Pi_{\mathbb{K},x})$. 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 2. *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 μ_x l'application de $\mathbb{A}$ dans $\mathbb{A}$ définie par
   $$\forall a \in \mathbb{A}, \qquad \mu_x(a) = ax.$$
   Alors μ_x est un endomorphisme du $\mathbb{K}$-espace vectoriel de dimension finie $\mathbb{A}$. L'hypothèse fait que μ_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 2 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 *Pour quels éléments x de la $\mathbb{K}$-algèbre $\mathbb{A}$ est-il vrai que $\mathbb{K}[x]$ ne possède pas d'élément nilpotent non nul ?*

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.*

Le corollaire ci-après résume l'essentiel des propriétés des éléments algébriques d'une extension de corps.

Corollaire 4. *Soient $\mathbb{L}/\mathbb{K}$ une extension de corps, x un élément de $\mathbb{L}$. 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.

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 θ une racine de P. Calculer le degré de θ sur $\mathbb{Q}$.

d) Montrer, si θ 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. *Pour tout n de $\mathbb{N}^*$, le polynôme Φ_n est irréductible sur $\mathbb{Q}$.*

Preuve. Étape 1. Nous allons montrer que, si ω est une racine primitive n-ième de l'unité et k un entier 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 Φ_n. L'irréductibilité de $\Pi_{\mathbb{Q},e^{2i\pi/n}}$ permettra de conclure.

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

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

Étape 2. Prouvons donc cette dernière assertion. Soient ω une racine primitive n-ième de 1, p un nombre premier ne divisant pas n. Les polynômes $\Pi_{Q,\omega}$ et $\Pi_{\mathbb{Q},\omega^p}$ appartiennent à $\mathbb{Z}[X]$ grâce à la remarque 6 de **2.3**. Comme $\Pi_{\mathbb{Q},\omega^p}(X^p)$ annule ω, le caractère unitaire de $\Pi_{\mathbb{Q},\omega}$ donne Q dans $\mathbb{Z}[X]$ tel que

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

Notons

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

la 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. 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 19. ④ *Soient m et n deux éléments de $\mathbb{N}^*$. Montrer*

$$\mathbb{Q}(e^{2i\pi/m}) \cap \mathbb{Q}(e^{2i\pi/n}) = \mathbb{Q}(e^{2i\pi/(m\wedge n)}), \quad \mathbb{Q}(e^{2i\pi/m}, e^{2i\pi/n}) = \mathbb{Q}(e^{2i\pi/(m\vee n)}).$$

Exercice 20. ④ *a) Soient $n \geq 3$ un entier et k un entier premier à n, calculer les degrés sur $\mathbb{Q}$ de $\cos(2k\pi/n)$ et $\sin(2k\pi/n)$.*

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

Exercice 21. ④ *Soit $n \geq 3$ un entier. Déterminer le groupe des racines de l'unité du corps $\mathbb{Q}\left(\exp\left(\frac{2i\pi}{n}\right)\right)$.*

Exercice 22. 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 T_n en produit de ψ_m. À quelle condition T_n est-il irréductible sur $\mathbb{Q}$?

2 Extensions finies, extensions algébriques

Dans toute cette section, $\mathbb{L}/\mathbb{K}$ est une extension de corps.

2.1 Sommes et produits d'éléments algébriques

On mesure dans la démonstration de la proposition ci-après l'efficacité des techniques linéaires.

Proposition 4. *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.

Remarques et applications

1. *Annulateur d'une somme ou d'un produit via le théorème des polynômes symétriques*[8].
   La preuve précédente ne fournit pas d'annulateur de $x+y$ ou de xy. Voici un moyen d'en calculer un et de redémontrer la proposition 4. 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 de $\mathbb{L}$. Alors

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

   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 V) entraîne que

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

8. Le résultant donne également une démonstration « effective » de la proposition 4 en utilisant le résultant, qui à l'avantage sur la suivante de mener les calculs en restant dans $\mathbb{K}$

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, toujours grâce au théorème des polynômes symétriques

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

Ces arguments, antérieurs à ceux fondés sur l'algèbre linéaire, établissent la version « effective » ci-après de la proposition 4.

Proposition 5. *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 $\mathbb{M}$.*

Appliquant cette méthode à $\mathbb{K} = \mathbb{Q}$, $x = \sqrt{2}, y = \sqrt{3}$, un petit calcul montre que $X^4 - 10X^2 + 1$ annule $\sqrt{2} + \sqrt{3}$.

2. *Sur le degré de $\mathbb{K}(x, y)$ sur $\mathbb{K}$*
   Avec les notations de la proposition 4, on a vu que $[\mathbb{K}(x, y) : \mathbb{K}]$ divise mn. Par ailleurs, ce degré est multiple de m et n (par multiplicativité des degrés et parce que $\mathbb{K}(x, y)$ contient $\mathbb{K}(x)$ et $\mathbb{K}(y)$. Ainsi :

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

3. *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

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

   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. [9]

9. Nous déterminerons dans le chapitre **3** les binômes $X^n - a$ irréductibles sur $\mathbb{K}$.

4. *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 $[\mathbb{L}(x) : \mathbb{L}]$ 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 télescopiques 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 23. ② *Soient $p_1, \ldots, p_r$ des nombres premiers deux à deux distincts, n leur produit, a un élément de $\mathbb{K}$ qui n'est pour aucun i de $\{1, \ldots, r\}$ une puissance p_i-ième exacte dans $\mathbb{K}$. Montrer que $X^n - a$ est un irréductible de $\mathbb{K}[X]$. Réciproque ?*

Exercice 24. ③ *Déterminer un annulateur de $\sqrt{2} + \sqrt[3]{2}$ sur $\mathbb{Q}$ en utilisant la méthode de la remarque 1, puis celle de la remarque 2.*

Exercice 25. ③ *Soient P un polynôme irréductible de degré n de $\mathbb{K}[X]$, Q un élément non constant de $\mathbb{K}[X]$, $U = P \circ Q$. Si Π est un diviseur irréductible de U dans $\mathbb{K}[X]$, montrer que le degré de Π est un multiple de n.*

Si l'élément x de $\mathbb{L}^*$ 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 4 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 26. 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 27. ③ *Soit $x \in \mathbb{L}$ algébrique sur $\mathbb{K}$ de degré impair. Montrer l'égalité : $\mathbb{K}(x) = \mathbb{K}(x^2)$.*

Exercice 28. ③ *Soient m et n deux éléments de $\mathbb{N}^*$. Montrer que Φ_n est irréductible sur $\mathbb{Q}(e^{2i\pi/m})$ si et seulement si $m \wedge n = 1$.*

Exercice 29. 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 déduit-on relativement à la question c) de l'exercice 6 du paragraphe* **2.1** *?*

2.2 Extensions finies, algébriques

Commençons par décrire les extensions finies de $\mathbb{K}$ contenues dans $\mathbb{L}$ au moyen des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$.

Proposition 6. *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.

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 $\mathbb{K}$.

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

   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

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

   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 $\mathbb{K}^*/(\mathbb{K}^*)^2$.

10. Notation cohérente car $\mathbb{K}(\sqrt{a})$ ne dépend pas de la racine choisie.

Exercice 30. ② *Expliciter la fin de l'argument pour la remarque 2.*

Exercice 31. 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 α réel.*

Exercice 32. 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 33. ⑤ *a) Soient $\mathbb{K}$ un corps de caractéristique différente de 2, $\mathbb{L}/\mathbb{K}$ une extension, $u_1, \ldots, u_m$ des éléments de $\mathbb{K}^*$ ayant des racines carrées notées respectivement $\sqrt{u_1}, \ldots, \sqrt{u_m}$ dans $\mathbb{L}$. On pose $\mathbb{K}^{*2} = \{x^2,\ x \in \mathbb{K}^*\}$. Montrer que $[\mathbb{K}(\sqrt{u_1}, \ldots, \sqrt{u_m}) : \mathbb{K}] = 2^m$ si et seulement si*

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

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

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

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 34. ⑤ *Soit $\mathbb{K}$ un corps.*

a) Montrer que les conditions suivantes sont équivalentes.

i) Pour tout r de $\mathbb{N}^*$, l'ensemble

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

est réduit à $\{(0, \ldots, 0)\}$.

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 35. 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 36. 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 37. 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 ce paragraphe par la transitivité de l'algébricité, héritée directement de celle de la finitude.

Proposition 7. *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.

Corollaire 5. *Soient $\mathbb{K}$ un corps, Ω un surcorps algébriquement clos de $\mathbb{K}$, $\mathbb{L}$ l'ensemble des éléments de Ω algébriques sur $\mathbb{K}$. Alors $\mathbb{L}$ est un sous-corps algébriquement clos de Ω.*

Preuve. On sait déjà que $\mathbb{L}$ est un sous-corps de Ω. 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 Ω : 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 $x \in \mathbb{L}$.

Le corps $\overline{\mathbb{Q}}$ est donc algébriquement clos.

Exercice 38. ③ *Soient α 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 39. ② *Montrer que $\overline{\mathbb{Q}} = (\overline{\mathbb{Q}} \cap \mathbb{R})(i)$.*

Le problème d'effectivité mentionné dans la remarque 1 après la proposition 4 de **3.1** se pose à nouveau : 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. On laisse le lecteur s'exercer avec l'exercice suivant.

Exercice 40. ③ *Avec les notations précédentes, exhiber un polynôme unitaire de $\mathbb{K}[X]$ annulant x.*

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 Ω 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 Ω, cette racine étant simple. Le pgcd Δ de ces deux polynômes vu dans $\Omega[X]$ est donc $X - y$. Par inertie du pgcd, il s'ensuit que Δ 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 du théorème montre que, pour tout t de $\mathbb{Q}$ 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 $Q\left(\sqrt[3]{2}, j\right)/\mathbb{Q}$. Tel est le cas en particulier pour $t = 1$.

Exercice 41. 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 42. 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 43. ① *Soient $\mathbb{K}$ un corps de caractéristique zéro, n un élément de $\mathbb{N}^*$. 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]

12. Emmy Noether et Artin ont montré que la théorie de Galois pouvait être développée sans recourir à cet énoncé. Leur motivation était 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.

Exercice 44. 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 45. ④ *Soient $\mathbb{K}$ un corps de caractéristique nulle, $P_1, \ldots, P_r$ des polynômes non constants de $\mathbb{K}[X]$. Montrer qu'il existe r polynômes $Q_1, \ldots, Q_r$ 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 $\mathbb{K}[X]$.*

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 46. 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 α 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 8. *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. *Soit $\mathbb{L}/\mathbb{K}$ une extension séparable finie. Si $\mathbb{K}$ est infini, l'extension $\mathbb{L}/\mathbb{K}$ est monogène.*

Preuve. 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 8.

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

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

2.5 Caractérisation des extensions monogènes

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

Lemme 3. *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.

Proposition 9. *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 4. *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 4, en dimension finie*

Reprenons les notations du lemme 4. 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]

16. Le résultat obtenu, dû à Steinitz, ne joue pas de rôle dans la suite. Ce paragraphe peut donc être vu comme un exercice.

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 $\cup_{i=1}^m H_i$.

Lemme 5. *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 $P(x_1, \ldots, x_{n-1}, X)$ est un élément de $\mathbb{K}[X]$ qui s'annule sur l'ensemble infini E_n. Ce polynôme est donc nul, 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 47. ① *Montrer que toute sous-extension d'une extension monogène finie est monogène.*

Exercice 48. 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

On a pu constater combien il est commode, pour l'étude de l'irréductibilité d'un polynôme P de $\mathbb{K}[X]$, de disposer d'un surcorps de $\mathbb{K}$ scindant P. La résolution des équations algébriques suppose par ailleurs qu'un polynôme non constant ait des racines « quelque part ». [19] Ce fait, justifié dans le paragraphe **4.1**, est suffisant 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 Ω de $\mathbb{K}$. La démonstration de l'existence d'un tel surcorps fait l'objet de **4.2** ; elle ne contient pas d'idée algébrique nouvelle, mais nécessite une certaine habitude de l'infini, à travers le lemme de Zorn. [20]

3.1 Corps de rupture, corps de décomposition

Le point de départ de ce paragraphe est le :

Lemme 6. *Soit P un élément irréductible de $\mathbb{K}[X]$. Il existe une extension $\mathbb{K}'$ de $\mathbb{K}$ telle que :*

i) P a une racine x dans $\mathbb{K}'$,

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

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. Laplace l'utilise dans la démonstration du théorème de d'Alembert-Gauss présenté dans le paragraphe **7.2** du chapitre **1**.

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

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 $\mathcal{M}_n(\mathbb{K})$.
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, ce qui donne une construction de $\mathbb{C}$ simple et géométriquement plaisante.

Exercice 49. ② *Montrer que, si P est un polynôme de $\mathbb{R}[X]$ de degré 2 sans racine réelle, la $\mathbb{R}$-algèbre $\mathbb{R}[X]/(P)$ est isomorphe à $\mathbb{C}$.*

Exercice 50. ③ *Soit n un élément de $\mathbb{N}^*$. Écrire la $\mathbb{K}$-algèbre $\mathbb{K}[X]/(\Phi_n)$ comme produit de corps pour $\mathbb{K} = \mathbb{C}$, $\mathbb{K} = \mathbb{R}$, $\mathbb{K} = \mathbb{Q}$.*

Proposition 10. *Soit P dans $\mathbb{K}[X]$ non constant. Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ telle que :*

i) 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 6 fournit une extension $\mathbb{K}(x)$ de $\mathbb{K}$ où x est racine de Q. Appliquant l'hypothèse de récurrence au polynôme $P/(X-x)$ de $\mathbb{K}(x)[X]$, on obtient une extension $\mathbb{L}$ de $\mathbb{K}(x)$ dans laquelle $P/(X-x)$ est scindé, et telle que : $\mathbb{L} = \mathbb{K}(x)(\mathcal{S})$, où S est l'ensemble des racines de $P/(X-x)$ 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. Par exemple le seul corps de rupture de X^2-2 sur $\mathbb{Q}$ contenu dans $\mathbb{C}$ est $\mathbb{Q}(\sqrt{2})$ alors que X^3-2 admet trois sous-corps de rupture dans $\mathbb{C}$: $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q}(j^2\sqrt[3]{2})$.
3. *Cas du corps de décomposition*
   Soit maintenant P un polynôme de $\mathbb{K}[X]$ 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 $\mathbb{K}=\mathbb{Q}$, $P=X^n-2$ où n est un entier supérieur ou égal à 2 et $P=X^n-2$. 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 51. ③ *Soient $\mathbb{K}$ un corps de caractéristique nulle, P dans $\mathbb{K}[X]$. Notons $x_1,\dots,x_m$ les racines distinctes de P dans un corps de décomposition de P sur $\mathbb{K}$. Montrer que $\prod_{i=1}^m (X-x_i)$ est dans $\mathbb{K}[X]$.*

Exercice 52. 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 53. 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 54. 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 55. ② *Soient P un polynôme de degré 3 irréductible sur $\mathbb{Q}$ ayant exactement une racine réelle α (par exemple X^3-2). Soient β 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 56. ④ *On suppose que $\mathbb{K}$ est de caractéristique 0. Soient $n\in\mathbb{N}^*$, P dans $\mathbb{K}[X]$ de degré n séparable, $x_1,\dots,x_n$ les racines de P dans une extension,*

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

$\mathbb{L} = \mathbb{K}(x_1, \ldots, x_n)$. *Si* I *est une partie de* $\{1, \ldots, n\}$, *soit* $S_I = \sum_{i \in I} x_i$. *On fixe* m *dans* $\{1, \ldots, n-1\}$ *et on note* $\mathbb{L}_m$ *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* $\mathbb{L}_m = \mathbb{L}$.

Si $P \in \mathbb{K}[X]$ est irréductible de degré n, tout 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 11. *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 $(n-d)!$. Par conséquent, $[\mathbb{L} : \mathbb{K}]$ divise $d!(n-d)!$, lequel divise $n!$ puisque $\binom{n}{d}$ 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 vient du fait que la suite $\left(\binom{n}{d}\right)_{1 \leq d \leq n/2}$ est croissante et de la relation de symétrie

$$\forall d \in \{0, \ldots, n\}, \qquad \binom{n}{d} = \binom{n}{n-d}.$$

Exercice 57. ④ *Soient* P *un polynôme irréductible de* $\mathbb{K}[X]$. *On suppose que* P *est de la forme* $X^6 + aX^3 + b$, *on note* $\mathbb{L}$ *un corps de décomposition de* P *sur* K. *Montrer que* $[\mathbb{L} : \mathbb{K}]$ *divise* 18.

Exercice 58. ④ *Montrer que le polynôme* $P = X^6 - 4X^3 + 2$ *est irréductible sur* $\mathbb{Q}$, *que* $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2+\sqrt{2}}, \sqrt[3]{2}, j)$ *est un corps de décomposition de* P *sur* $\mathbb{Q}$. *Calculer* $[\mathbb{L} : \mathbb{Q}] = 18$.

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, indispensable pour effectuer une version transfinie des constructions précédentes. On a en fait un résultat plus précis, le *théorème de Steinitz*.

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

Preuve (Artin). Soit $\mathbb{K}$ un corps.

Étape 1. Il existe une extension $\mathbb{K}_1$ de $\mathbb{K}$ dans laquelle tout polynôme 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 $\mathbb{A} = \mathbb{K}[\{X_P,\ P \in \mathcal{E}\}]$ des polynômes à une infinité d'indéterminées paramétrées 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 $P_1 \times \cdots \times P_m$ 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 θ de $\mathbb{A}$ dans $\mathbb{L}$ envoyant X_{P_i} sur x_i pour $1 \leq i \leq n$. Appliquant θ 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 de $\mathbb{N}^*$, $\mathbb{K}_{n+1}$ 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 [22] des $\mathbb{K}_n$. Si P est dans $\mathbb{K}_\infty[X]$, 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 $\mathbb{K}_\infty$; par suite, $\mathbb{K}_\infty$ est algébriquement clos. [23]

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 5, que nous reformulons ici.

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

23. 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.

Corollaire 6. *Soient $\mathbb{K}$ un corps, Ω une extension algébriquement close de $\mathbb{K}$, $\mathbb{L}$ l'ensemble des éléments de Ω 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 $\mathbb{Q}$.

3.3 Résolubilité des équations par radicaux : formulation

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

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

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

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 $D_{\mathbb{K}}(P)$. 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 que la situation est très différente si le degré est supérieur ou égal à 5.

4 Constructibilité à la règle et au compas (I)

Dans cette section, on applique la théorie des extensions de corps à un sujet géométrique classique : les constructions à la règle et au compas. Il s'agit d'un problème hérité de l'Antiquité, mais compris seulement au dix-neuvième siècle : la clé est la théorie des corps et non pas la géométrie élémentaire.

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 $3, 5, 6, 15$.

En fait, ces constructions sont impossibles. Le démontrer demandait de franchir un certain nombre d'étapes :

- 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, ce qui ne pouvait guère apparaître avant l'invention [24] 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 dernière étape, initiée par les travaux de Gauss sur les polygones réguliers, n'a été complètement clarifiée qu'avec la notion d'extension de corps et la théorie de Galois. Nous montrerons ici que les constructions à la règle et au compas sont un problème de nature algébrique, ce qui nous suffira pour résoudre par la négative plusieurs des « problèmes grecs ». Pour aller plus loin, il est préférable de disposer de la théorie de Galois ; nous reviendrons sur le sujet.

Dans le plan euclidien orienté $\mathbb{R}^2$, on cherche quels sont 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 $\mathbb{R}^2$:

- 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 Δ et le cercle Γ 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 Δ 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 Δ, on a terminé. Sinon, le cercle de centre A et de rayon AB coupe Δ 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 Δ passant par A.

24. La *Géométrie* de Descartes date de 1637.

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 Δ 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 Δ.

   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 Δ 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 Δ passant par A en C symétrique de A par rapport à Δ.

   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 Δ passant par A est dans $\widehat{\mathcal{C}}$.

   Preuve. On trace la perpendiculaire Δ' à Δ passant par A, puis la perpendiculaire à Δ' 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 Re(z) et 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 $1/a$.

   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 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 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 Δ et d'un cercle Γ de $\widehat{\mathcal{A}}$. L'équation de Δ est de la forme $\alpha x+\beta y+\gamma = 0$ où α, β et γ sont dans $\mathbb{K}$; celle de Γ est de la forme $x^2+y^2-\delta x-\varepsilon y = \lambda$ où δ, ε et λ sont dans $\mathbb{K}$. Si $\beta \neq 0$, on tire y en fonction de x de l'équation de Δ, 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 59. 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)* $\Rightarrow$ *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 est immédiate.

On déduit de la proposition et de la multiplicativité des degrés une condition suffisante simple de constructibilité.

Corollaire 7. *Si z appartient à $\mathcal{C}$, z est algébrique sur $\mathbb{Q}$ et le degré de z sur $\mathbb{Q}$ est une puissance de 2.*

Ce résultat, généralement 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 π est transcendant sur $\mathbb{Q}$), d'où l'impossibilité de la quadrature du cercle. [25] D'autre part, pour n dans $\mathbb{N}^*$, 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 $\mathbb{N}$. [26]

25. 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.

26. 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 2015, le plus grand nombre de Fermat connu reste 65537.

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

Exercice 60. ③ *On dit que l'angle θ est constructible à partir de l'angle α 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 : $\theta = \pi/3$.

Exercice 61. ⑤ *Soit x une racine de $X^4 + X + 1$ dans $\mathbb{C}$. Montrer que x n'est pas constructible.*

La condition nécessaire de constructibilité du corollaire 7 n'est pas suffisante. Le « bon » énoncé est le suivant : un nombre complexe z est constructible si et seulement si $[D_{\mathbb{Q}}\Pi_{\mathbb{Q},z} : \mathbb{Q}]$ est une puissance de 2. Le corollaire 7 exprime la propriété plus faible : $[\mathbb{Q}(z) : \mathbb{Q}]$ est une puissance de 2. La démonstration la plus naturelle de la condition nécessaire et suffisante repose sur la théorie de Galois.

Exercice 62. ③ *On rappelle la formule (cf « Équations, corps et polynômes », exercice 1) :*

$$\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{4}.$$

En déduire une construction du pentagone régulier de centre O et dont I est un des sommets.

Exercice 63. 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 Éléments entiers sur un anneau

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*, dont Dedekind a donné vers 1875 une présentation quasi-définitive. Cette notion, à la marge de notre étude de la théorie de Galois, a été évoquée dans la remarque 6 de **2.3**. On en dit un peu plus ici.

Le nombre complexe x est un entier algébrique s'il existe P dans $\mathbb{Z}[X]$ unitaire tel que $P(x) = 0$. Comme $\mathbb{Z}$ n'est pas un corps, le caractère unitaire est crucial dans la définition. On note $\overline{\mathbb{Z}}$ l'ensemble des entiers algébriques. Par exemple, les éléments de la forme $\sqrt[n]{a}$ avec n dans $\mathbb{N}^*$ et a dans $\mathbb{N}^*$, les racines de l'unité sont dans $\overline{\mathbb{Z}}$.

Le lemme 1 de **2.3** caractérise les entiers algébriques comme les $x \in \overline{\mathbb{Q}}$ tels que $\Pi_{\mathbb{Q},x} \in \mathbb{Z}[X]$. Par ailleurs, le « test des racines rationnelles » pour un élément de $\mathbb{Z}[X]$ fournit aussitôt l'énoncé suivant.

Lemme 7. *On a*

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

Comme attendu , $\overline{\mathbb{Q}}$ est le corps des fractions de $\overline{\mathbb{Z}}$. Plus précisément, on dispose du résultat suivant.

Lemme 8. *Soit $x \in \overline{\mathbb{Q}}$. Il existe $q \in \mathbb{N}^*$ tel que $qx \in \overline{\mathbb{Z}}$.*

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 $k \in \{0, \ldots, n-1\}$, 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 $a_0, \ldots, a_{n-1}$.

Exercice 64. 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 65. ③ *Soit n dans $\mathbb{N}^*$. Montrer qu'il existe un polynôme U_n unitaire de degré n tel que, pour tout réel x, on ait :*

$$U_n(2\cos(x)) = 2\cos(nx).$$

En déduire que, pour k dans $\mathbb{Z}$: $2\cos\left(\dfrac{2k\pi}{n}\right) \in \overline{\mathbb{Z}}$.

Exercice 66. ③ *Montrer que* $\dfrac{1}{3}\left(1 + 10^{1/3} + 10^{2/3}\right) \in \overline{\mathbb{Z}}$.

Exercice 67. ③ *Soit x dans $\overline{\mathbb{Z}} \setminus \{0\}$. Montrer que l'ensemble des q de $\mathbb{N}^*$ tels que x/q soit dans $\overline{\mathbb{Z}}$ est fini.*

On s'attend bien sûr à ce que $\overline{\mathbb{Z}}$ soit un sous-anneau de $\mathbb{C}$. Nous proposerons deux démonstrations de ce fait. La première est fondée sur une traduction linéaire de l'intégralité comme propriété de finitude, dans l'esprit de la proposition 1 de **2.2**, qui remonte à Dedekind. Pour formuler cette traduction, il nous faut introduire 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. 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, qui est le point *iv*) du théorème suivant.

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 immédiatement que le groupe additif du sous-anneau $\mathbb{Z}[x]$ de $\mathbb{C}$ est engendré par la famille finie $(x^k)_{0\leq k\leq n-1}$.

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 $\overline{\mathbb{Z}}$. On a démontré $i)$.

L'exercice suivant reformule plus géométriquement le théorème.

Exercice 68. ④ *Soient $x \in \mathbb{C}$, $n \in \mathbb{N}^*$. Montrer que x est un entier algébrique de degré inférieur ou égal à n sur $\mathbb{Q}$ si et seulement s'il existe un $\mathbb{Q}$-espace vectoriel V de dimension n, un sous-groupe R de $(V,+)$ de rang n et un endomorphisme f de V stabilisant R tel que $\chi_f(x) = 0$.*

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

Preuve. Il est immédiat de vérifier 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 $\left(x^i y^j\right)_{\substack{0\leq i\leq n-1\\ 0\leq j\leq p-1}}$ 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 $\overline{\mathbb{Z}}$.

Exemple

Soient n dans $\mathbb{N}^*$ et k dans $\mathbb{Z}$. Alors

$$2\cos\left(\frac{2k\pi}{n}\right) = \exp\left(\frac{2ik\pi}{n}\right) + \exp\left(-\frac{2ik\pi}{n}\right) \in \overline{\mathbb{Z}}.$$

On retrouve, bien plus directement, le résultat de l'exercice 63. De même,

$$2\sin\left(\frac{2k\pi}{n}\right) = i\left(\exp\left(-\frac{2ik\pi}{n}\right) - \exp\left(\frac{2ik\pi}{n}\right)\right) \in \overline{\mathbb{Z}}.$$

Remarques

1. *Autre démonstration 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 **3.1**. 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

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

2. *Irréductibilité sur $\mathbb{Q}[X]$ versus irréductibilité sur $\mathbb{Z}[X]$*

   Soient P_1 et P_2 deux polynômes unitaires de $\mathbb{Q}[X]$ tels que P_1P_2 appartienne à $\mathbb{Z}[X]$. Le corollaire 2 du chapitre **1** (**2.4**) assure que P_1 et P_2 appartiennent à $\mathbb{Z}[X]$. On peut établir ce résultat à l'aide du théorème 9. En effet, les racines de P_1P_2 dans $\mathbb{C}$ sont des entiers algébriques. Il en est donc de même des racines de P_1 et de P_2, puis, grâce aux formules de Viète et au théorème 9, des coefficients de P_1 et P_2. Le lemme 7 achève la démonstration.

L'exercice suivant propose une autre démonstration du théorème 8, qui est un déguisement d'une démonstration tensorielle.

Exercice 69. 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 70. ② *Soit x dans $\overline{\mathbb{Q}}$. Montrer que l'ensemble des q de $\mathbb{Z}$ tels que $q\,x \in \overline{\mathbb{Z}}$ est un idéal non nul de $\mathbb{Z}$.*

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

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

nommé *anneau des entiers de* $\mathbb{K}$. Ces anneaux sont des objets fondamentaux de l'arithmétique.

Exercice 71. ③ *Montrer que* $\overline{\mathbb{Z}}$ *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.

Exercice 72. ④ *Soit* d *un entier relatif sans facteur carré. Montrer que l'anneau des entiers du corps quadratique* $\mathbb{Q}\left(\sqrt{d}\right)$ *est :*

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

Exercice 73. 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 74. 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, $u_n/u_m \in \overline{\mathbb{Z}}$ *; en déduire que* u_m *divise* u_n.

5.2 Généralisation

Généraliser l'étude précédente est naturel et profitable. 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 restreint la généralité en se bornant à ce cas.

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

Généralisons le vocabulaire de l'adjonction. Si E est une partie de $\mathbb{B}$, on note $\mathbb{A}[E]$ la plus petit $\mathbb{A}$-sous-algèbre de $\mathbb{B}$ contenant $\mathbb{A}$. 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. [27] On a alors une généralisation très satisfaisante commune aux théorèmes 1 et 7.

Théorème 10. *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 un polynôme unitaire de degré n de $\mathbb{A}[X]$ 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 μ_x l'endomorphisme de multiplication par x dans le $\mathbb{A}$-module $\mathbb{M}$. En appliquant à μ_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 9. *Soient $\mathbb{M}$ un $\mathbb{A}$-module de type fini et φ 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 [28], 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 8 s'étend alors aussitôt pour donner le résultat suivant, que l'on peut également établir via le théorème des polynômes symétriques, en reprenant la remarque de **6.1**.

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

28. L'identité de Cayley-Hamilton vaut pour une matrice à coefficients dans un anneau commutatif quelconque.

Théorème 11. *L'ensemble des éléments de $\mathbb{B}$ entiers sur $\mathbb{A}$ est un sous-anneau de $\mathbb{B}$.*

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

Lemme 10. *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 6, **3.2**), on en déduit la conséquence suivante.

Corollaire 8. *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 ».

Proposition 12. *Soient $\mathbb{A}$ un anneau factoriel, x un élément du corps des fractions de $\mathbb{A}$ et*

$$P = \sum_{i=0}^{n} a_i X^i$$

un polynôme de degré $n \geq 1$ à coefficients dans $\mathbb{A}$. Écrivons $x = p/q$ où p et q sont deux éléments de A premiers entre eux. Si $P(x) = 0$, alors :

$$p \mid a_0 \quad et \quad q \mid a_n \ .$$

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 $\mathbb{A}$. On a ainsi le résultat suivant.

Proposition 13. *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 $\mathbb{A}$. C'est le contenu de la proposition suivante, dont la preuve est la même que pour $\mathbb{Z}$ (lemme de Gauss sur les contenus).

Proposition 14. *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 la proposition 13 aux anneaux intégralement clos [29], via une démonstration un peu différente.

Proposition 15. *Soient $\mathbb{A}$ un anneau intégralement clos de corps des fractions $\mathbb{K}$, $\mathbb{L}$ une extension de $\mathbb{K}$, 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 $\mathbb{A}[X]$.*

Preuve. Supposons x entier sur $\mathbb{A}$ et écrivons :

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

où les x_i appartiennent à une extension convenable de $\mathbb{L}$. Si P est un polynôme unitaire de $\mathbb{A}[X]$ annulant x, P est divisible dans $\mathbb{K}[X]$ par $\Pi_{\mathbb{K},x}$ donc annule les x_i. Les x_i sont ainsi entiers sur A ; il en est donc de même des coefficients de $\Pi_{\mathbb{K},x}$ d'où la conclusion puisque A est intégralement clos.

6 Irrationalité et transcendance (I)

Les notions d'algébricité et de transcendance affinent celle, beaucoup plus ancienne, d'irrationalité. On donne dans cette section une première approche du sujet, qui sera complétée dans le chapitre **3**.

Les démonstrations d'irrationalité et de transcendance sont souvent très délicates. Par ailleurs, certaines preuves peuvent être présentées rapidement, mais sans être véritablement éclairantes. Nous n'avons pas cherché la concision maximale, mais plutôt essayé de dégager quelques idées élémentaires sur le sujet, en particulier en soulignant les liens entre irrationalité, transcendance et approximation diophantienne.

6.1 Premiers exemples de nombres irrationnels

La découverte des nombres irrationnels remonte à l'Antiquité grecque : le théorème de Pythagore conduit en effet naturellement aux racines carrées des nombres entiers.

Il est facile de décider de l'irrationalité d'un nombre algébrique dont on connaît un annulateur : il suffit d'utiliser le test des racines rationnelles (chapitre **1**, **2.2**).

Exercice 75. ④ *Montrer que, si $r \in \mathbb{Q}$, $2\cos(\pi r)$ est un entier algébrique. En déduire les valeurs de r pour lesquelles $\cos(\pi r)$ est rationnel.*

Il existe d'autres exemples simples. Ainsi, pour $(p, q) \in \mathbb{N}^*$, on a

$$\log_2(3) = \frac{p}{q} \Longrightarrow 3^q = 2^p,$$

d'où l'irrationalité de $\log_2(3)$.

Exercice 76. ③ *Pour quels couples (a, b) d'entier ≥ 2 a-t-on $\log_a(b) \in \mathbb{Q}$?*

29. 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.

L'irrationalité des constantes fournies par l'analyse relève de techniques plus subtiles. Une première méthode, très élémentaire, est fournie par le critère suivant, dont nous n'utiliserons que l'implication facile *iii*) $\Rightarrow$ *iv*).

Théorème 12. *Soit x un nombre réel. S'équivalent.*

i) Pour tout $Q \in \mathbb{N}^*$, il existe q dans $\{1, \dots, q-1\}$ et p dans $\mathbb{Z}$ tels que

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{qQ}.$$

ii) Pour tout $\varepsilon > 0$, il existe q dans $\mathbb{N}^*$ et p dans $\mathbb{Z}$ tels que

$$0 < \left| x - \frac{p}{q} \right| < \frac{\varepsilon}{q}.$$

iii) Il existe une suite $(p_k)_{k\geq 0}$ d'éléments de $\mathbb{Z}$ et une suite $(q_k)_{k\geq 0}$ d'éléments de $\mathbb{N}^*$ tendant vers $+\infty$ et telles que

$$\forall k \in \mathbb{N}, \quad \frac{p_k}{q_k} \neq x \qquad et \qquad x - \frac{p_k}{q_k} \underset{k\to+\infty}{=} o\left(\frac{1}{q_k}\right).$$

iv) Le nombre x est irrationnel.

Preuve. L'implication *i*) $\Rightarrow$ *ii*) est immédiate : choisir Q tel que $Q\ \varepsilon \geq 1$. L'assertion *iii*) n'est qu'une reformulation séquentielle de *ii*).

Supposons *ii*) et, par l'absurde, x rationnel : $x = \dfrac{a}{b}$ avec a dans $\mathbb{Z}$ et b dans $\mathbb{N}^*$. Fixons $\varepsilon \in]0, \dfrac{1}{b}[$: on dispose de (p, q) dans $\mathbb{Z} \times \mathbb{N}^*$ tel que

$$\left| x - \frac{p}{q} \right| < \frac{\varepsilon}{q}, \quad \text{d'où} \quad 0 < |aq - bp| < 1.$$

La contradiction vient du fait que $aq - bp$ est entier.

L'implication *iv*) $\Rightarrow$ *i*) est plus profonde et ne sera pas utilisée. On la démontre à partir du principe des tiroirs. Notons $\{y\}$ la partie décimale du nombre réel y. Puisque x est irrationnel, les nombres $\{k\ x\},\ k \in \{0, \dots, Q\}$ sont des éléments deux à deux distincts de $[0, 1[$. On dispose donc de k et ℓ dans $\{0, \dots, Q\}$ tels que $k < \ell$ et

$$|\{\ell\ x\} - \{k\ x\}| < \frac{1}{Q}.$$

On en déduit aisément le résultat, en posant $q = \ell - k$.

On déduit du théorème 12 l'irrationalité de e, établie par Euler en 1737 ; la preuve présentée ici est due à Fourier (1815).

Théorème 13. *Le nombre e est irrationnel.*

Preuve. La formule $e = \displaystyle\sum_{i=0}^{+\infty} \frac{1}{i!}$ implique que, pour k dans $\mathbb{N}$

$$e = \frac{p_k}{k!} + \varepsilon_k \quad \text{où} \quad p_k \in \mathbb{N} \quad \text{et} \quad \varepsilon_k = \sum_{j=k+1}^{+\infty} \frac{1}{j!}.$$

Il est clair que les ε_k sont dans $\mathbb{R}^{+*}$. Il reste à vérifier que la suite $(k!\ \varepsilon_k)_{k\geq 0}$ tend vers 0. Or, le lemme ci-après implique que

$$\varepsilon_k \underset{k\to+\infty}{\sim} \frac{1}{(k+1)!}.$$

Lemme 11. *Soit $(u_k)_{k\geq 0}$ une suite d'éléments de $\mathbb{R}^{+*}$ telle que $u_{k+1} \underset{k\to+\infty}{=} o(u_k)$. Alors $\sum_{j=k+1}^{+\infty} u_j \underset{k\to+\infty}{\sim} u_{k+1}$.*

Preuve du lemme 11. La sommation des relations de comparaison entraîne l'asymptotique suivant, équivalent à la conclusion du lemme :

$$\sum_{j=k+2}^{+\infty} u_j \underset{k\to+\infty}{=} o\left(\sum_{j=k+1}^{+\infty} u_j\right).$$

On peut également montrer que $(k!\ \varepsilon_k)_{k\geq 0}$ tend vers 0 à partir de la forme intégrale du reste de Taylor :

$$\varepsilon_k = \int_0^1 \frac{(1-t)^k e^t}{k!}\,\mathrm{d}t, \quad \text{d'où} \quad 0 < \varepsilon_k < \frac{e}{(k+1)!}.$$

On peut encore simplifier l'argument en montrant que $\dfrac{1}{e}$ est irrationnel : dans ce cas, on utilise l'encadrement classique des restes d'une série « alternée » (i.e. justiciable de la règle de Leibniz).

Par ailleurs, la démonstration précédente ne se généralise pas directement à e^m pour $m \geq 2$ entier. Certains cas particuliers peuvent se traiter en considérant la 2-valuation de $n!$, notée $v_2(n!)$.

Exercice 77. ⑤ *a) Montrer que $v_2(n!) \underset{n\to+\infty}{=} n + O(\ln(n))$.*

b) Déduire de a) que e^2 et $\mathrm{ch}(\sqrt{2})$ sont irrationnels. Que dire de $\exp(\sqrt{2})$?

Exercice 78. ④ *Montrer par un argument analogue au précédent qu'il n'existe pas de triplet (a,b,c) dans $\mathbb{Z}^2 \setminus \{0\}$ tel que $ae + b + ce^{-1} = 0$. Ainsi, e n'annule aucun polynôme de degré 2 non trivial à coefficients dans $\mathbb{Z}$.*[30] *En particulier, e^2 est irrationnel.*

Exercice 79. ⑤ *En combinant les idées des deux exercices précédents, montrer que e^2 n'est pas algébrique de degré 2. En particulier, e^4 est irrationnel.*

Exercice 80. ⑤ *Soit $x \in]0,1]$.*

a) Montrer qu'il existe une unique suite croissante $(q_i)_{i\geq 1}$ d'entiers ≥ 2 tels que :

$$x = \sum_{i=1}^{+\infty} \frac{1}{q_1 \times \cdots \times q_i}.$$

30. Cette démonstration du fait que e n'est ni un rationnel, ni un irrationnel quadratique, est attribuée à Liouville.

b) Montrer que x est rationnel si et seulement si la suite $(q_i)_{i\geq 1}$ est stationnaire.

c) Retrouver l'irrationalité de e.

d) Soit $a \geq 2$ un entier. Montrer que $\displaystyle\sum_{k=0}^{+\infty} \frac{1}{a^{2^k}-1} \notin \mathbb{Q}$.

Dans le paragraphe **7.3**, qui est accessible dès maintenant, nous établirons simultanément l'irrationalité de e^r pour $r \in \mathbb{Q}^*$ et celle de π.

6.2 Approximation diophantienne

La proposition 16 appartient à la problématique de l'*approximation diophantienne*, c'est-à-dire à l'étude « quantitative » de l'approximation des nombres réels par les rationnels. Ce paragraphe expose les débuts de cette théorie. [31]

Un résultat préliminaire

Commençons par le résultat très simple et naturel ci-après.

Lemme 12. *Soient x un nombre irrationnel, $(p_k)_{k\geq 0}$ une suite d'entiers relatifs, une suite $(q_k)_{k\geq 0}$ d'éléments de $\mathbb{N}^*$, telles que $\dfrac{p_k}{q_k} \underset{k\to+\infty}{\longrightarrow} x$. Alors $q_k \underset{k\to+\infty}{\longrightarrow} +\infty$.*

Preuve. Supposons le résultat faux. Alors on dispose de q dans $\mathbb{N}^*$ et d'une extractrice φ telle que

$$\forall k \in \mathbb{N}, \qquad q_{\varphi(k)} = q.$$

Il s'ensuit que $(p_{\varphi(k)})_{k\geq 0}$ est convergente et à valeurs dans $\mathbb{Z}$, donc stationnaire ; on en déduit en passant à la limite que x est rationnel.

L'approximation en $\dfrac{1}{q^2}$

La théorie de l'approximation diophantienne part du problème suivant : étant donné un nombre irrationnel x, comment construire de bonnes approximations rationnelles de x ?

Le lemme 12 montre qu'une approximation précise d'un irrationnel par des rationnels nécessite des fractions de grand dénominateur. Il est donc raisonnable, si $(p,q) \in \mathbb{Z}\times\mathbb{N}^*$, de mesurer la qualité de l'approximation de x par $\dfrac{p}{q}$ s'obtient en comparant l'erreur $\left|x-\dfrac{p}{q}\right|$ au coût de l'approximation, mesuré par le dénominateur q. Grossièrement dit, l'approximation est de bonne qualité si $\left|x-\dfrac{p}{q}\right|$ est petit devant $\dfrac{1}{q}$.

L'implication non immédiate du théorème 12 entraîne le résultat d'approximation diophantienne suivant. Nous n'utiliserons pas vraiment cet énoncé, qui n'en demeure pas moins fondamental. [32]

31. L'approche reste superficielle. Notamment, on n'aborde pas la théorie des fractions continues, consubstantielle à ce sujet.

32. La théorie des fractions continues permet de remplacer l'inégalité par

$$\left|x-\frac{p_k}{q_k}\right| \leq \frac{1}{\sqrt{5}\,q_k^2}.$$

Théorème 14. *Soit x un nombre réel irrationnel. Il existe une suite $(p_k)_{k\geq 0}$ d'entiers relatifs, une suite $(q_k)_{k\geq 0}$ d'éléments de $\mathbb{N}^*$ tendant vers $+\infty$ telle que*

$$\forall k \in \mathbb{N}, \qquad \left| x - \frac{p_k}{q_k} \right| < \frac{1}{q_k^2}.$$

Preuve. On pose $q_0 = 1$, $p_0 = \lfloor x \rfloor$. Soit $k \in \mathbb{N}$. Supposons construits $p_0, \ldots, p_k$ et $q_0, \ldots, q_k$. Soit Q_k le plus petit élément de $\mathbb{N}^*$ tel que

$$\left| x - \frac{p_k}{q_k} \right| \geq \frac{1}{Q_k}.$$

On applique la condition *iii*) de la proposition 16 et on obtient p_{k+1} dans $\mathbb{Z}$, q_{k+1} dans $\{1, \ldots, Q_k - 1\}$ tels que

$$\left| x - \frac{p_{k+1}}{q_{k+1}} \right| < \frac{1}{q_{k+1}\, Q_k}.$$

On a

$$\left| x - \frac{p_{k+1}}{q_{k+1}} \right| < \frac{1}{Q_k} \quad \text{et} \quad \left| x - \frac{p_{k+1}}{q_{k+1}} \right| < \frac{1}{q_{k+1}^2}.$$

La suite $(Q_k)_{k\geq 0}$ est strictement croissante par construction, donc tend vers $+\infty$. La suite $\left(\frac{p_k}{q_k}\right)_{k\geq 0}$ tend donc vers x. Il découle du lemme 12 que $(q_k)_{k\geq 0}$ tend vers $+\infty$.

Mesures d'irrationalité

Le théorème 14 est un résultat positif. Les énoncés en sens inverse conduisent à la notion de *mesure d'irrationalité*. Soit x un nombre irrationnel. On appelle ainsi une collection d'inégalités du type

$$\forall (p, q) \in \mathbb{Z} \times \mathbb{N}^*, \qquad \left| x - \frac{p}{q} \right| \geq f(q),$$

où f est une fonction de $\mathbb{N}^*$ dans $\mathbb{R}^{+*}$, que l'on suppose décroissante et tendant vers 0 en $+\infty$. Ces inégalités quantifient l'irrationalité de x. On remarquera que, vu le caractère décroissant de f, il est inutile de se limiter aux couples (p, q) tels que $p \wedge q = 1$.

On peut obtenir une mesure d'irrationalité de x à partir d'une suite d'approximations rationnelles de x. Expliquons la méthode sur un exemple simple, qui conduit à un très mauvais résultat. On vérifie que la démonstration du théorème 13 produit une suite $(p_k)_{k\geq 0}$ d'entiers telle que

$$\forall k \in \mathbb{N}^*, \qquad \left| e - \frac{p_k}{k!} \right| \leq \frac{2}{(k+1)!}.$$

Soit maintenant (p, q) dans $\mathbb{Z} \times \mathbb{N}^*$. Pour $k \in \mathbb{N}^*$, on écrit

$$\left| \frac{p}{q} - \frac{p_k}{k!} \right| \leq \left| \frac{p}{q} - e \right| + \left| e - \frac{p_k}{q_k} \right| \leq \left| \frac{p}{q} - e \right| + \frac{2}{(k+1)!}.$$

Cette dernière formulation est optimale : si x est le nombre d'or, on ne peut pas remplacer $1/\sqrt{5}$ par une constante plus petite.

Supposons que $\frac{p}{q}$ n'est égal à aucun $\frac{p_k}{k!}$. Il vient alors que, pour $k \in \mathbb{N}^*$

$$\left|\frac{p}{q} - \frac{p_k}{k!}\right| \geq 1, \quad \text{d'où} \quad \left|\frac{p}{q} - e\right| \geq \frac{1}{q\,k!} - \frac{2}{(k+1)!}.$$

Choisissons $k = 2q - 1$. On obtient

$$\left|\frac{p}{q} - e\right| \geq \frac{1}{(2q)!}.$$

On vérifie que cette inégalité reste vraie s'il existe $k \in \mathbb{N}^*$ tel que $\frac{p}{q} = \frac{p_k}{k!}$. En effet, on a directement

$$\forall k \in \mathbb{N}^*, \qquad \left|e - \frac{p_k}{q_k}\right| \geq \frac{1}{(k+1)!}.$$

La mesure optimale d'irrationalité

Si $r \in [2, +\infty[$, on peut définir l'ensemble A_r des nombres irrationnels tels qu'il existe deux suites $(p_k)_{k\geq 0}$ et $(q_k)_{k\geq 0}$, respectivement à valeurs dans $\mathbb{Z}$ et $\mathbb{N}^*$, telles que

$$q_k \underset{k\to+\infty}{\longrightarrow} +\infty \qquad x - \frac{p_k}{q_k} \underset{k\to+\infty}{=} O\left(\frac{1}{{q_k}^r}\right).$$

Le théorème 13 assure que $A_2 = \mathbb{R} \setminus \mathbb{Q}$. Pour tout nombre irrationnel x, on note $\mu(x)$ la borne supérieure, dans $[2, +\infty]$ de l'ensemble des r tels que $x \in A_r$. L'élément $\mu(x)$ de $[2, +\infty[$ est la *mesure optimale d'irrationalité de* x.

Il est en général difficile de calculer, ou même de majorer $\mu(x)$. [33] Le théorème ci-après, qui remonte à Liouville, donne un premier renseignement.

Théorème 15. *Soit x un réel irrationnel algébrique de degré n sur $\mathbb{Q}$. Il existe un réel $C > 0$ tels que :*

$$\forall (p, q) \in \mathbb{Z} \times \mathbb{N}^*, \qquad \left|x - \frac{p}{q}\right| \geq \frac{C}{q^n}.$$

En particulier, $\mu(x) \leq n$.

Preuve. Soient $P \in \mathbb{Z}[X] \setminus \{0\}$ de degré n annulant x, $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$. Le nombre réel $q^n P\left(\frac{p}{q}\right)$ est entier, donc soit nul, soit de valeur absolue supérieure ou égale à 1.

D'autre part les zéros de P étant en nombre fini, on dispose de $\rho > 0$ tel que α soit la seule racine de P dans $[x - \rho, x + \rho]$.

Si $\left|\frac{p}{q} - x\right| \leq \rho$, on a $\frac{p}{q} \neq x$, $\left|q^n P\left(\frac{p}{q}\right)\right| \geq 1$ et $\left|P\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}$. Posant

$$A = \max_{t\in[x-\rho,x+\rho]} |P'(t)|,$$

33. On peut cependant accéder à $\mu(x)$ à partir du développement de x en fraction continue.

il vient :

$$\left|P\left(\frac{p}{q}\right)\right| \leq A\left|\frac{p}{q}-x\right| \quad \text{et} \quad \left|\frac{p}{q}-x\right| \geq \frac{1}{A\,q^n}.$$

On en déduit l'inégalité du théorème, avec $C = \max\left(\rho, \frac{1}{A}\right)$.

Remarques

1. *Les nombres de Liouville*

   Les nombres de Liouville sont les irrationnels x tels que $\mu(x) = +\infty$. On déduit du théorème 14 le résultat suivant.

   Corollaire 9. *Tout nombre de Liouville est transcendant.*

   Ce corollaire est à la base de la première construction de nombres transcendants, effectuée par Liouville en 1844.[34] À toute suite $(\varepsilon_n)_{n\geq 1}$ d'entiers de $\{1,\ldots,9\}$ associons en effet

   $$\alpha_\varepsilon = \sum_{n=1}^{+\infty} \frac{\varepsilon_n}{10^{n!}}.$$

   Le nombre α_ε, dont on établit l'irrationalité par une application immédiate de la proposition 16, est de Liouville. En effet, pour tout $m \in \mathbb{N}^*$, il existe $p_m \in \mathbb{N}$ (obtenu en tronquant à l'ordre m la série définissant α_ε) tel que :

   $$(1) \qquad \left|\alpha_\varepsilon - \frac{p_m}{10^{m!}}\right| \leq 9 \sum_{n=m+1}^{+\infty} 10^{-n!} \leq \frac{10}{\left(10^{m!}\right)^{m+1}}\ .$$

   L'algébricité de α_ε sur $\mathbb{Q}$ impliquerait l'existence de $C > 0$ et $n \geq 2$ tels que :

   $$(2) \qquad \forall m \in \mathbb{N}^*, \qquad \left|\alpha_\varepsilon - \frac{p_m}{10^{m!}}\right| \geq \frac{C}{\left(10^{m!}\right)^{n}}\ .$$

   Pour m assez grand, (1) et (2) sont contradictoires ; α_ε est transcendant.

2. *Le cas des nombres algébriques*

   Le théorème de Liouville n'est optimal que pour les irrationnels quadratiques. Une série de travaux, notamment de Thue et Siegel, culmine sur un théorème difficile de Roth assurant que, si x est un nombre irrationnel algébrique $\mu(x) = 2$. Par contraposition, on améliore ainsi la remarque 1 : tout nombre irrationnel x tel que $\mu(x) > 2$ est transcendant.

   On verra dans l'exercice l'intérêt qu'il peut y avoir à améliorer, fût-ce très légèrement, la majoration $\mu(x) \leq n$.

3. *Que se passe-t-il en général ?*

   La situation générique du point de vue de la mesure de Lebesgue est décrite par le résultat suivant.

   Proposition 16. *Pour presque tout nombre réel, on a $\mu(x) = 2$.*

34. C'est seulement en 1873 que Cantor a démontré la dénombrabilité de l'ensemble des nombres algébriques.

Preuve. Soit L la mesure de Lebesgue. Par continuité décroissante de L, il suffit d'établir que, pour tout $r > 2$, A_r est négligeable. On fixe désormais $r > 2$.

Puisque A_r est invariant par translation entière, on peut, grâce à l'additivité dénombrable et à l'invariance de L par translation, se borner à établir que $B_r = B \cap [0,1]$ est négligeable. Or, on peut écrire

$$B_r = \bigcup_{C\in\mathbb{N}^*} \bigcap_{Q\in\mathbb{N}^*} \bigcup_{\substack{q\in\mathbb{N}\\ q\geq Q}} \bigcup_{p\in\mathbb{Z}} \left(\left[\frac{p}{q} - \frac{C}{q^r}, \frac{p}{q} - \frac{C}{q^r} \right] \cap [0,1] \right).$$

Par additivité dénombrable de L, il suffit d'établir que, pour tout $C \in \mathbb{N}^*$,

$$L\left(\bigcap_{Q\in\mathbb{N}^*} \bigcup_{\substack{q\in\mathbb{N}\\ q\geq Q}} \bigcup_{p\in\mathbb{Z}} \left(\left[\frac{p}{q} - \frac{C}{q^r}, \frac{p}{q} - \frac{C}{q^r} \right] \cap [0,1] \right) \right) = 0.$$

Fixons désormais $C \in \mathbb{N}^*$. Si $Q \in \mathbb{N}^*$ et $q \geq Q$, il faut, pour que l'intervalle $\left[\frac{p}{q} - \frac{C}{q^r}, \frac{p}{q} + \frac{C}{q^r} \right]$ coupe $[0,1]$, que p appartienne à $[-C, q+C]$. Il s'ensuit que

$$L\left(\left[\frac{p}{q} - \frac{C}{q^r}, \frac{p}{q} - \frac{C}{q^r} \right] \cap [0,1] \right) \leq \frac{2C(q+2C+1)}{q^r}$$

Le majorant est $O\left(\frac{1}{q^{r-1}} \right)$ lorsque q tend vers $+\infty$. Comme $\sum \frac{1}{q^{r-1}}$ converge, l'inégalité

$$L\left(\bigcup_{\substack{q\in\mathbb{N}\\ q\geq Q}} \bigcup_{p\in\mathbb{Z}} \left(\left[\frac{p}{q} - \frac{C}{q^r}, \frac{p}{q} - \frac{C}{q^r} \right] \cap [0,1] \right) \right) \leq \sum_{q=Q}^{+\infty} \frac{2C(q+2C+1)}{q^r}$$

achève la démonstration, dans laquelle le lecteur aura reconnu un cas particulier du premier lemme de Borel-Cantelli. [35]

4. *Le cas de e et π*
   Il existe des nombres transcendants qui ne sont pas de Liouville. Tel est le cas de e et π. Précisément, $\mu(e) = 2$ et on sait en 2018 que $\mu(e) \leq 7,7$. Compte-tenu de la remarque précédente, on s'attend à $\mu(\pi) = 2$.

Exercice 81. ② *Déterminer $C \in \mathbb{R}^{+*}$ tel que*

$$\forall (p,q) \in \mathbb{Z} \times \mathbb{N}^*, \qquad \left| \sqrt{2} - \frac{p}{q} \right| \geq \frac{C}{q^2}.$$

Exercice 82. ② *Soient E un ensemble, D une partie dénombrable de E telle que $E \setminus D$ soit infini. Montrer que E et $E \setminus D$ sont équipotents. En déduire que l'ensemble des nombres réels transcendants est équipotent à $\mathbb{R}$.*

35. La proposition 17 peut être précisée. Ainsi, Jarnik a calculé la dimension de Hausdorff de A_r et Khintchine a déterminé la mesure d'ensembles généralisant les A_r, en établissant une « loi du tout ou rien » très précise.

Exercice 83. ④ *Soit φ une fonction décroissante de $\mathbb{N}^*$ dans $\mathbb{R}^{+*}$, tendant vers 0 en $+\infty$. Construire un nombre réel x, deux suites $(p_k)_{k\geq 0}$ et $(q_k)_{k\geq 0}$ d'éléments de $\mathbb{N}^*$ telles que*

$$\forall k \in \mathbb{N}, \qquad 0 < \left| x - \frac{p_k}{q_k} \right| \leq \varphi(q_k).$$

6.3 Irrationalité de π ; irrationalité de e^r pour r rationnel

Les équivalences du théorème 12 ne doivent pas induire en erreur : lorsqu'un nombre réel x est donné comme somme d'une série de nombres rationnels, les approximations rationnelles de x données par les sommes partielles vérifient rarement l'hypothèse de *iii)*. Donnons deux exemples.

– Comme on l'a signalé à la fin de **7.1**, le développement en série entière ne permet pas d'établir simplement l'irrationalité de e^m pour si m est un grand entier naturel. En fait, les seules preuves de ce type connues sont celles présentées dans les exercices 72 à 74, qui couvrent les cas $m = 2$ et $m = 4$.

– Si $s \geq 2$ est entier, soit

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}.$$

Par troncature de la série, on obtient $\zeta(s) = \dfrac{p_k}{q_k} + \varepsilon_k$, où $q_k = \mathrm{ppcm}(1, 2, 3, \ldots, k)^s$ et où, par comparaison somme-intégrale,

$$\varepsilon_k \underset{k\to+\infty}{\sim} \frac{1}{(s-1)\ k^{s-1}}.$$

Il est clair que la suite $(q_k\ \varepsilon_k)_{k\geq 1}$ tend vers $+\infty$. La méthode précédente est donc inopérante.

Il est cependant connu depuis Euler que, pour $s \geq 2$ pair, $\zeta(s)$ est de la forme $r_s\ \pi^s$ où r_s est rationnel ; dans ce cas, la transcendance de π entraîne celle de $\zeta(s)$. En revanche, ce n'est qu'en 1978 que Roger Apéry a démontré l'irrationalité de $\zeta(3)$; la démonstration d'Apéry repose sur le corollaire 9, mais une « accélération de convergence » très ingénieuse est nécessaire pour produire les suites requises. En 2019, on ignore si $\zeta(5)$ est irrationnel.

L'irrationalité de π a été démontrée en 1767 par Lambert, comme conséquence du développement en fraction continue de $\tan(x)$. Nous allons obtenir une forme plus générale de ce résultat, via une modification significative de la démonstration de l'irrationalité de e.

Théorème 16. *Si z est un élément non nul de $\mathbb{Q}(i)$, e^z n'est pas dans $\mathbb{Q}(i)$.*

En particulier[36] *:*

– si $r \in \mathbb{Q}^*$, e^r est irrationnel ;

– si $r \in \mathbb{Q}^{+*} \setminus \{1\}$, $\ln(r)$ est irrationnel ;

– le nombre π est irrationnel.

36. Ces cas particuliers étaient connus de Lambert.

Preuve. Étape 1. Réductions.

La déduction des cas particuliers à partir de la première phrase est immédiate, le dernier provenant de la relation $e^{i\pi} = -1$.

Par ailleurs, il suffit d'établir que, pour tout $z \in \mathbb{Z}[i] \setminus \{0\}$, $e^z \notin \mathbb{Q}(i)$. Admettons en effet ce point et considérons z dans $\mathbb{Q}[i] \setminus \{0\}$ et $q \in \mathbb{N}^*$ tel que $qz \in \mathbb{Z}[i]$, de sorte que $e^{qz} \notin \mathbb{Q}(i)$. Comme $e^{qz} = (e^z)^q$, e^z n'est pas dans $\mathbb{Q}(i)$.

Dans la suite, on fixe $z \in \mathbb{Z}[i] \setminus \{0\}$. Pour démontrer que $e^Z \notin \mathbb{Q}(i)$, nous allons accélérer la convergence de la série exponentielle, en la multipliant par un polynôme de $\mathbb{Z}[X]$ bien choisi ; il s'agit d'un exemple simple de la méthode dite « du polynôme auxiliaire », qui est un ingrédient essentiel de beaucoup de démonstrations d'irrationalité et de transcendance.

Étape 2. Principe de la preuve.

Pour z dans $\mathbb{C}$ et j dans $\mathbb{N}$, on a

$$z^j\ e^z = \sum_{k=0}^{+\infty} \frac{H_j(k)}{k!}\ z^k \quad \text{où} \quad H_j = \prod_{k=0}^{j-1} (X-k).$$

Pour tout $j \in \mathbb{N}$, H_j est un polynôme unitaire de degré j de $\mathbb{Z}[X]$. Il s'ensuit que tout polynôme de $\mathbb{Z}[X]$ s'écrit, de façon unique, comme combinaison $\mathbb{Z}$-linéaire des H_j, $j \in \mathbb{N}$. Par conséquent, pour tout P de $\mathbb{Z}[X]$, il existe un unique Q dans $\mathbb{Z}[X]$ tel que

$$\forall z \in \mathbb{C}, \qquad Q(z)\ e^z = \sum_{k=0}^{+\infty} \frac{P(k)}{k!}\ z^k.$$

Précisément, si $P = \displaystyle\sum_{j=0}^{+\infty} \alpha_j\ H_j$, alors $Q = \displaystyle\sum_{j=0}^{+\infty} \alpha_j\ X^j$. En particulier, P et Q ont même degré.

Posons alors, pour $n \in \mathbb{N}^*$:

$$P_n = \prod_{j=n+1}^{2n} (X-j).$$

Ce qui précède fournit Q_n dans $\mathbb{Z}[X]$, de degré n, tel que

$$(1) \qquad \forall z \in \mathbb{C}, \qquad Q_n(z)\ e^z = \sum_{k=0}^{+\infty} \frac{P_n(k)}{k!}\ z^k = \sum_{k=0}^{n} \frac{P_n(k)}{k!}\ z^k + \sum_{k=2n+1}^{+\infty} \frac{P_n(k)}{k!}\ z^k.$$

Pour k dans $\{0, \dots, n\}$,

$$\frac{P_n(k)}{k!} = (-1)^n\ \frac{(2n-k)!}{(n-k)!\ k!} = (-1)^n\ \frac{n!}{k!} \binom{2n-k}{n} \in \mathbb{Z}.$$

Par ailleurs, si $k \geq 2n+1$,

$$\frac{P_n(k)}{k!} = \frac{(k-n-1)!}{(k-2n-1)!\ k!}.$$

Prenons maintenant z dans $\mathbb{Z}[i] \setminus \{0\}$. On a

$$(2) \qquad \forall n \in \mathbb{N}^*, \qquad \sum_{k=0}^{n} \frac{P_n(k)}{k!}\, z^k \in \mathbb{Z}[i].$$

Posons, pour $n \in \mathbb{N}^*$:

$$u_n = \sum_{k=2n+1}^{+\infty} \frac{P_n(k)}{k!}\, z^k = z^{2n+1} \sum_{j=0}^{+\infty} \frac{(j+n)!}{j!\,(j+2n+1)!}\, z^j.$$

Au vu des relations (1) et (2), il reste à voir, pour obtenir une contradiction, que $(u_n)_{n\geq 1}$ tend vers 0 et que, pour une infinité d'entiers $n \geq 1$, $u_n \neq 0$. Les deux points se déduisent de l'équivalent

$$(3) \qquad u_n \underset{n\to+\infty}{\sim} e^{z/2}\, z^{2n+1}\, \frac{n!}{(2n+1)!}.$$

Étape 3. Preuve de l'équivalent (3).

On part de l'égalité

$$u_n = z^{2n+1}\, \frac{n!}{(2n+1)!} \sum_{j=0}^{+\infty} \alpha_{j,n} \quad \text{où} \quad \alpha_{j,n} = \frac{(j+n)!\,(2n+1)!}{n!\,(j+2n+1)!}\, \frac{z^j}{j!}.$$

Lorsque j est fixé, on a

$$\alpha_{j,n} \underset{n\to+\infty}{\longrightarrow} \frac{z^j}{2^j\, j!}.$$

Par ailleurs

$$\forall (j,n) \in \mathbb{N} \times \mathbb{N}^*, \qquad |\alpha_{j,n}| \leq \frac{|z|^j}{j!}.$$

Par convergence dominée,

$$\sum_{j=0}^{+\infty} \alpha_{j,n} \underset{n\to+\infty}{\longrightarrow} e^{z/2}, \quad \text{puis} \quad u_n \underset{n\to+\infty}{\sim} e^{z/2}\, z^{2n+1}\, \frac{n!}{(2n+1)!}.$$

Remarque *Simplification pour z rationnel ; non-annulation*

Si $x \in \mathbb{Q}^{+*}$, il est clair que les u_n sont > 0. La preuve de la convergence vers 0 se déduisant d'une majoration très simple, on en déduit sans recherche d'équivalent que $e^x \notin \mathbb{Q}$. En considérant $-x$, on étend aussitôt le résultat à $x \in \mathbb{Q}^{-*}$. Cette remarque met en évidence un phénomène fréquent dans les démonstrations d'irrationalité et de transcendance : établir que certains nombres sont non nuls peut être une partie difficile de la preuve !

Exercice 84. ③ *Donner une preuve d'une ligne de la convergence de $(u_n)_{n\geq 1}$ vers* 0.

On retrouve l'irrationalité de π dans l'exercice suivant, qui est une réécriture par Parks (1986) d'une démonstration de Niven (1947).

Exercice 85. ③ *Pour $c \in \mathbb{R}^{+*}$, soit R_c l'ensemble des fonctions de classe C^∞ de $[0,c]$ dans $\mathbb{R}$ telles que*

$$\forall j \in \mathbb{N}, \qquad (f^{(j)}(0), f^{(j)}(c)) \in \mathbb{Z}^2.$$

Il est clair que R_c est un sous-anneau de l'anneau des fonctions de classe C^∞ de $[0,c]$ dans $\mathbb{R}$. On note S_c l'ensemble des f de R_c telles que, pour tout $k \in \mathbb{N}$, il existe g dans R_c telle que $f = g^{(k)}$; autrement dit, si D est l'endomorphisme de dérivation de R_c,

$$S_c = \bigcap_{k\in\mathbb{N}} D^{(k)}(R_c).$$

a) Soient $c \in \mathbb{R}^{+*}$, f dans S_c, g une fonction polynomiale appartenant à R_c. Montrer que $\displaystyle\int_0^c f\, g \in \mathbb{Z}$.

b) Soient $c \in \mathbb{R}^{+*}$, g dans R_c telle que $g(0) = g(c) = 0$. Montrer que, pour tout $k \in \mathbb{N}$, $\dfrac{g^k}{k!} \in R_c$.

c) Soient a et b dans $\mathbb{N}^*$, $c = \dfrac{a}{b}$. Pour k dans $\mathbb{N}^*$, posons

$$\forall x \in [0,c], \qquad g_{a,b}(x) = x\,(bx - a).$$

Montrer que, pour $k \in \mathbb{N}$, $\dfrac{g_{a,b}^k}{k!} \in R_c$.

d) Soit $c \in \mathbb{R}^{+*}$. On suppose qu'il existe $f \in S_c$ non identiquement nulle qui prend des valeurs positives sur $[0,c]$. Montrer que c est irrationnel.

e) Retrouver l'irrationalité de π et celle de e^r pour $r \in \mathbb{Q}^*$.

Nous terminons ce paragraphe par un exercice très vivement conseillé au lecteur. Pour $q \in \mathbb{C}$ tel que $|q| > 1$ on définit la fonction de Tschakaloff T_q par

$$\forall z \in \mathbb{C}, \qquad T_q(z) = \sum_{n=0}^{+\infty} \frac{z^n}{q^{\frac{n(n+1)}{2}}}.$$

Cette fonction vérifie l'équation fonctionnelle

$$\forall z \in \mathbb{C}, \qquad T_q(z) = z + \frac{z}{q} T_q\left(\frac{z}{q}\right).$$

Cette équation fonctionnelle et la méthode du polynôme auxiliaire permettent de montrer que, comme exp, la fonction T_q envoie $\mathbb{Q}(i) \setminus \{0\}$ dans $\mathbb{C} \setminus \mathbb{Q}(i)$. Une différence avec la démonstration du théorème 16 est que le polynôme auxiliaire n'est pas explicité.

Exercice 86. ⑤ *On suppose que q est entier. On se propose d'établir que $T_q(\mathbb{Q}^*) \subset \mathbb{R} \setminus \mathbb{Q}$. On raisonne par l'absurde en supposant que $z \in \mathbb{Q}^*$ et que $T_q(z) \in \mathbb{Q}$. On écrit*

$$z = \frac{a}{b}, \quad T_q(z) = \frac{u}{v} \quad \text{où} \quad (a,u) \in \mathbb{Z}^2, \quad (b,v) \in \mathbb{N}^{*2}.$$

a) Montrer que, pour $n \in \mathbb{N}^*$, il existe $u_n \in \mathbb{Z}$ tel que

$$\forall n \in \mathbb{N}, \qquad T_q\left(\frac{z}{q^n}\right) = \frac{u_n}{v\ a^n}$$

b) Soient S une série entière formelle à coefficient dans un sous-corps $\mathbb{K}$ de $\mathbb{C}$, $e \in \mathbb{N}^*$. Montrer qu'il existe A et B dans $\mathbb{K}_e[X]$, non tous deux nuls, tels que la valuation de $AS - B$ soit supérieure ou égale à $2e$.

c) En appliquant la question b) à $S = T_q$ avec $\mathbb{K} = \mathbb{Q}$ et e bien choisi, obtenir une contradiction.

d) Montrer que, si z est dans $\mathbb{Q}(i)^*$, alors $T_q(z)$ n'est pas dans $\mathbb{Q}(i)$.

Nous reviendrons sur ces idées dans le chapitre **3**.

6.4 La transcendance de e

Considérations générales

Hormis le cas des nombres de Liouville, toutes les démonstrations de transcendance sont délicates.

Soit à établir que le nombre réel x est transcendant. On peut s'inspirer de la proposition 16, mais en observant qu'il nous faut maintenant approcher les puissances de x par des rationnels de même dénominateur. Supposons en effet l'existence d'une suite $(q_k)_{k\geq 1}$ d'éléments de $\mathbb{N}^*$ tendant vers $+\infty$ et de suites $(p_{k,j})_{k\geq 0}$, $j \in \mathbb{N}$ d'entiers relatifs telles que

$$\forall j \in \mathbb{N}, \qquad q_k\left(x^j - \frac{p_{k,j}}{q_k}\right) \underset{k\to+\infty}{\longrightarrow} 0.$$

Posons, pour $j \in \mathbb{N}$:

$$\forall k \in \mathbb{N}, \qquad x^j = \frac{p_{k,j}}{q_k} + \varepsilon_k^j.$$

Soit $P = \sum_{j=0}^{d} a_j\ X^j \in \mathbb{Z}[X]$ annulant x, avec $a_0 \neq 0$. Alors

$$\sum_{j=0}^{d} a_j\ p_{k,j} = -\sum_{j=0}^{d} a_j\ q_k\ \varepsilon_k^j.$$

Le premier membre de l'égalité est entier, le second tend vers 0 lorsque k tend vers $+\infty$. Nous obtiendrons une contradiction, et donc la transcendance de x, si nous pouvons imposer une condition assurant que le premier membre n'est pas nul. Ce point est souvent délicat.

La transcendance de e

En 1873, Hermite a démontré le théorème suivant.

Théorème 17. *Le nombre e est transcendant.*

Cette démonstration est le véritable point de départ de la théorie de la transcendance. Elle repose sur le schéma précédent et la construction de fractions rationnelles approchant en un certain sens la fonction exponentielle. Compte-tenu de l'importance du résultat, le travail d'Hermite a été repris et simplifié

par de nombreux auteurs. La partie « non annulation » a été substantiellement allégée par Hilbert, via un argument arithmétique : en reprenant les notations ci-dessus, Hilbert fait en sorte que les $p_{k,j}$ pour $1 \leq j \leq d$ soient divisibles par un même nombre premier ne divisant ni a_0 ni p_k^0.

Nous parachuter la construction des approximations des puissances de e, en utilisant le lemme ci-après.

Lemme 13. *Soient P dans $\mathbb{R}[X]$, k dans $\mathbb{N}$. Si $P = \sum_{i=0}^{+\infty} a_i\ (X-j)^i$, alors*

$$e^j \int_j^{+\infty} P(t)\ e^{-t}\,\mathrm{d}t = \sum_{i=0}^{+\infty} a_i\ i!.$$

Preuve. Pour $j = 0$, la démonstration résulte immédiatement de la formule

$$\forall i \in \mathbb{N}, \qquad \int_0^{+\infty} t^i\ e^{-t}\,\mathrm{d}t = i!.$$

Le cas général s'en déduit modulo le changement de variable $u = t - j$.

Écrivons alors, pour P dans $\mathbb{Q}[X]$,

$$e^j \int_0^{+\infty} P(t)\ e^{-t}\,\mathrm{d}t = e^j \int_j^{+\infty} P(t)\ e^{-t}\,\mathrm{d}t + e^j \int_0^j P(t)\ e^{-t}\,\mathrm{d}t.$$

Si p est un nombre premier et d un élément de $\mathbb{N}^*$, soit

$$P_{p,d}(X) = \frac{X^{p-1}}{(p-1)!} \prod_{k=1}^{d} (X-k)^p.$$

Pour k dans $\{1, \ldots, d\}$, on peut écrire

$$P_{p,d} = \frac{(X-k)^p}{(p-1)!} Q_{p,d,k} \qquad \text{avec} \quad Q_{p,d,k} \in \mathbb{Z}[X].$$

Le lemme 13 entraîne donc que, si $1 \leq j \leq d$, $e^j \int_0^{+\infty} P_{p,d}(t)\ e^{-t}\,\mathrm{d}t$ est un entier divisible par p, alors que

$$\int_0^{+\infty} P_{p,d}(t)\ e^{-t}\,\mathrm{d}t \equiv \prod_{k=1}^{d} (-k)^p\ [p].$$

Par ailleurs

$$\left| e^j \int_0^j P_{p,d}(t)\ e^{-t}\,\mathrm{d}t \right| \leq \frac{e^j\ j^{pd+p}}{(p-1)!}, \quad \text{d'où} \quad e^j \int_0^j P_{p,d}(t)\ e^{-t}\,\mathrm{d}t \underset{p\to+\infty}{\longrightarrow} 0.$$

Nous pouvons alors reprendre les considérations du début du paragraphe. Supposons

$$\sum_{j=0}^{d} a_j\ e^j = 0 \qquad (a_0, \ldots, a_d) \in \mathbb{Z}^{d+1},\ a_0 \neq 0.$$

Alors

$$0 = a_0 \int_0^j P_{p,d}(t)\, e^{-t}\, \mathrm{d}t + \sum_{j=1}^{d} a_j\, e^j \int_0^j P_{p,d}(t)\, e^{-t}\, \mathrm{d}t + \sum_{j=1}^{d} a_j \int_0^j P_{p,d}(t)\, e^{-t}\, \mathrm{d}t.$$

Le premier terme est un entier congru à $a_0 \prod_{k=1}^{d} (-k)^p$ modulo p ; le deuxième terme est un entier divisible par p ; le troisième terme tend vers 0 lorsque p tend vers $+\infty$. Pour conclure, il reste à choisir $p > |a_0|$ et tel que le troisième terme soit dans $]-1, 1[$.

Avec un certain travail supplémentaire, on peut généraliser cette démonstration et établir le *théorème de Hermite-Lindemann* : si z est un nombre complexe algébrique non nul, e^z est transcendant. Ce résultat implique la transcendance de π. Nous le démontrerons dans le chapitre **3**.