Chapitre 3
Morphismes et conjugaison

Sommaire

1 Introduction

Dans tout ce chapitre, $\mathbb{K}$ est un corps et Ω une clôture algébrique de $\mathbb{K}$, c'est-à-dire un surcorps algébriquement clos de $\mathbb{K}$ tel que l'extension $\Omega/\mathbb{K}$ est algébrique. Les corps considérés seront souvent supposés contenus dans Ω, plus par commodité que par nécessité. Cette hypothèse ne nuit en rien à la généralité (section **4**, remarque finale).

Le chapitre **1** se cantonne aux objets « classiques » que sont les polynômes. Avec le chapitre **2**, consacré aux extensions, on entre dans une formulation plus « géométrique » de la théorie des équations. Le but du présent chapitre est d'étudier, dans une extension de corps $\mathbb{L}/\mathbb{K}$, les applications qui préservent les relations algébriques à coefficients dans $\mathbb{K}$, c'est-à-dire les endomorphismes de

la $\mathbb{K}$-algèbre $\mathbb{L}$. Cette « linéarisation de la notion de relation algébrique » est un point central de la théorie de Galois à la Dedekind-Artin-Noether.

Ce chapitre traite essentiellement de trois points : conjugaison sur un corps $\mathbb{K}$ (**2**), prolongement des morphismes (**3** et **5**), indépendance linéaire de morphismes (**6**). La section **4** est un approfondissement sur la séparabilité, qui conduit à une version définitive du théorème de l'élément primitif, dans laquelle on caractérise en termes de morphismes les éléments primitifs d'une extension monogène ; le lecteur souhaitant se limiter à la caractéristique nulle pourra lire **4.2** sous cette hypothèse, indépendamment de **4.1**. Enfin, la section **7**, optionnelle, introduit les notions de trace et de norme d'une extension finie, avec quelques applications.

Notations et rappels

Si $\mathbb{L}$ et $\mathbb{M}$ sont deux sous-corps de Ω, on note $\mathrm{Hom}(\mathbb{L},\mathbb{M})$ l'ensemble des morphismes de corps de $\mathbb{L}$ dans $\mathbb{M}$. Si $\mathbb{A}$ et $\mathbb{A}'$ sont deux $\mathbb{K}$-algèbres, on note $\mathrm{Hom}_{\mathbb{K}}(\mathbb{A},\mathbb{A}')$ l'ensemble des morphismes de $\mathbb{K}$-algèbres de $\mathbb{A}$ dans $\mathbb{A}'$. Si $\mathbb{L}$ et $\mathbb{M}$ sont deux extensions de $\mathbb{K}$, $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\mathbb{M})$ est donc l'ensemble des éléments de $\mathrm{Hom}(\mathbb{L},\mathbb{M})$ qui induisent l'identité sur $\mathbb{K}$.

- Tout morphisme d'anneaux dont la source est un corps est injectif (immédiat ; au besoin, cf. chapitre **1**, lemme 2, **2.3**).

- Si $\mathbb{K}$ est l'un des sous-corps premiers $\mathbb{Q}$ ou $\mathbb{F}_p$ avec p premier et $\mathbb{L}$ une extension de $\mathbb{K}$, il n'y a qu'un élément de $\mathrm{Hom}(\mathbb{K},\mathbb{L})$, à savoir l'inclusion de $\mathbb{K}$ dans $\mathbb{L}$, ceci parce qu'un morphisme d'anneau envoie 1 sur 1. Par conséquent, si $\mathbb{K}$ est l'un de ces corps et $\mathbb{L}$, $\mathbb{M}$ deux extensions de $\mathbb{K}$, on a

$$\mathrm{Hom}(\mathbb{L},\mathbb{M}) = \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\mathbb{M}).$$

- Soit $\mathbb{L}/\mathbb{K}$ une extension de corps. Un élément x de $\mathbb{L}$ est dit *séparable sur* $\mathbb{K}$ si x est algébrique sur $\mathbb{K}$ et si $\Pi_{\mathbb{K},x}$ est séparable, c'est-à-dire premier à son polynôme dérivé (ou, de manière équivalente, simplement scindé sur Ω). L'extension $\mathbb{L}/\mathbb{K}$ est dite séparable si tout élément de $\mathbb{L}$ est séparable sur $\mathbb{K}$. Si $\mathbb{K}$ est de caractéristique nulle, toute extension algébrique de $\mathbb{K}$ est séparable. Tel est plus généralement le cas si le corps $\mathbb{K}$ est parfait.

- Si $P = \sum_{i=0}^{n} a_i X^i$ est dans $\mathbb{K}[X]$, et si σ est un morphisme de corps de $\mathbb{K}$ dans $\mathbb{K}'$, on note $\sigma.P$ le polynôme :

$$\sum_{i=0}^{n} \sigma(a_i) X^i.$$

L'application

$$P \longmapsto \sigma.P$$

est l'unique prolongement de σ en un morphisme d'anneaux de $\mathbb{K}[X]$ dans $\mathbb{K}'[Y]$ envoyant X sur Y. Cette propriété entraîne que P est irréductible sur $\mathbb{K}$ si et seulement si $\sigma.P$ l'est sur $\sigma(\mathbb{K})$.

2 Éléments conjugués sur $\mathbb{K}$

Morphismes d'algèbres

Le lemme suivant, immédiat mais essentiel, est un point de départ naturel.

Lemme 1. *Soient $\mathbb{A}$ et $\mathbb{A}'$ deux $\mathbb{K}$-algèbres commutatives, σ une application de $\mathbb{A}$ dans $\mathbb{A}'$. Les deux notions suivantes sont équivalentes.*

i) L'application σ est un morphisme de $\mathbb{K}$-algèbres.

ii) Pour tout élément n de $\mathbb{N}^*$, tout P de $\mathbb{K}[X_1, \ldots, X_n]$ et tout $(x_1, \ldots, x_n)$ de $\mathbb{A}^n$:

$$\sigma\left(P(x_1, \ldots, x_n)\right) = P\left(\sigma(x_1), \ldots, \sigma(x_n)\right).$$

Si ces conditions sont réalisées, on a :

$$P(x_1, \ldots, x_n) = 0 \Longrightarrow P\left(\sigma(x_1), \ldots, \sigma(x_n)\right) = 0.$$

Conjugaison sur un corps

Deux éléments x et y d'une extension de $\mathbb{K}$ sont dits *conjugués sur* $\mathbb{K}$, ou $\mathbb{K}$-*conjugués* s'ils sont algébriques sur $\mathbb{K}$ et vérifient

$$\Pi_{\mathbb{K},x} = \Pi_{\mathbb{K},y}.$$ [1]

L'ensemble des $\mathbb{K}$-conjugués dans Ω d'un élément x de Ω est donc fini de cardinal majoré par $\deg(\Pi_{\mathbb{K},x}) = [\mathbb{K}(x) : K]$, avec égalité si et seulement si x est séparable sur $\mathbb{K}$.

Par définition, deux éléments de Ω sont $\mathbb{K}$-conjugués s'il est impossible de distinguer x et y à partir de relations algébriques à coefficients dans $\mathbb{K}$. C'est ce que confirme l'énoncé suivant, qui *linéarise* la notion a priori polynomiale de conjugaison sur $\mathbb{K}$.

Proposition 1. *Soient x et y deux éléments d'une extension $\mathbb{L}$ de $\mathbb{K}$, avec x algébrique sur $\mathbb{K}$. Les deux assertions suivantes sont équivalentes.*

i) Il existe σ dans $Hom_{\mathbb{K}}(\mathbb{K}(x), \mathbb{L})$ tel que $\sigma(x) = y$.

ii) Les éléments x et y sont $\mathbb{K}$-conjugués.

Dans ce cas, σ est unique et induit un isomorphisme de $\mathbb{K}(x)$ sur $\mathbb{K}(y)$.

Preuve. Analyse. S'il existe un morphisme de $\mathbb{K}$-algèbres σ de $\mathbb{K}(x) = \mathbb{K}[x]$ sur $\mathbb{K}(y)$ envoyant x sur y, ce morphisme vérifie, grâce au lemme 1 :

$$\forall P \in \mathbb{K}[X], \qquad \sigma(P(x)) = P(y),$$

ce qui en établit l'unicité. Cette même relation entraîne que $\Pi_{\mathbb{K},x}$ annule y, donc que y est un $\mathbb{K}$-conjugué de x.

Synthèse. Supposons $\Pi_{\mathbb{K},x} = \Pi_{\mathbb{K},y}$. Alors, pour P et Q dans $\mathbb{K}[X]$, on a :

$$P(x) = Q(x) \Rightarrow \Pi_{\mathbb{K},x} \mid P - Q \Rightarrow \Pi_{\mathbb{K},y} \mid P - Q \Rightarrow P(y) = Q(y).$$

1. Il est raisonnable de considérer que deux éléments transcendants sur $\mathbb{K}$ d'une même extension sont $\mathbb{K}$-conjugués, cf exercice 2. En vue de la théorie de Galois, le cas algébrique nous suffira.

Il s'ensuit qu'en posant

$$\forall P \in \mathbb{K}[X], \qquad \sigma(P(x)) = P(y),$$

on définit bien une application de $\mathbb{K}[x] = \mathbb{K}(x)$ dans $\mathbb{K}[y] = \mathbb{K}(y)$. Il est immédiat de vérifier que cette application appartient à $\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(x), \mathbb{K}(y))$ et est bijective.

Exercice 1. ① *Soient $\mathbb{M}$ un corps, $\mathbb{L}$ un sous-corps de $\mathbb{M}$, $\mathbb{K}$ un sous-corps de $\mathbb{L}$, x un élément de $\mathbb{M}$. Quelle relation d'inclusion y-a-t-il entre l'ensemble des $\mathbb{K}$-conjugués de x dans $\mathbb{M}$ et celui des $\mathbb{L}$-conjugués de x dans $\mathbb{M}$?*

Exercice 2. ③ *a) Soient x et y deux éléments d'une extension $\mathbb{L}$ de $\mathbb{K}$. On suppose x transcendant sur $\mathbb{K}$. Montrer qu'il existe un unique élément σ de $Hom_{\mathbb{K}}(\mathbb{K}[x], \mathbb{K}[y])$ tel que $\sigma(x) = y$.*

b) Montrer que le morphisme de a) se prolonge en un morphisme de corps de $\mathbb{K}(x)$ dans $\mathbb{K}(y)$ si et seulement si y est transcendant sur $\mathbb{K}$.

Exercice 3. ④ *Soient $\mathbb{L}$ et $\mathbb{L}'$ deux sous-corps distincts de Ω, chacun extension de degré 3 de $\mathbb{K}$. Montrer que $[\mathbb{L}\mathbb{L}' : \mathbb{K}]$ est égal à 9 ou 6, le second cas se produisant si et seulement s'il existe σ dans $Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{L}')$ tel que $\sigma(\mathbb{L}) = \mathbb{L}'$.*

Exemples et remarques

1. *La conjugaison complexe*
   En prenant $\mathbb{K} = \mathbb{R}$, $x = i$, on retrouve qu'il n'y a que deux endomorphismes de la $\mathbb{R}$-algèbre $\mathbb{C}$, l'identité et la conjugaison complexe, dont le nom se trouve ainsi justifié.
2. *Les $\mathbb{Q}$-conjugués de $\sqrt[n]{2}$*
   Soit n un entier ≥ 2. Comme $X^n - 2$ est irréductible sur $\mathbb{Q}$, les $\mathbb{Q}$-conjugués de $x = \sqrt[n]{2}$ sont les ωx pour ω dans U_n. Il y a n morphismes de corps de $\mathbb{Q}(\sqrt[n]{2})$ dans $\overline{\mathbb{Q}}$ (ou dans $\mathbb{C}$). Ce sont les σ_ω pour ω dans U_n, où σ_ω est défini par
   $$\forall P \in \mathbb{Q}[X], \qquad \sigma_\omega(P(x)) = P(\omega x).$$
3. *Les racines de l'unité*
   Soit n un élément de $\mathbb{N}^*$. Comme le polynôme cyclotomique Φ_n est irréductible sur $\mathbb{Q}$, les $\mathbb{Q}$-conjugués de $e^{2i\pi/n}$ sont les racines de Φ_n, c'est-à-dire les $e^{2ik\pi/n}$ avec k dans $\{1, \ldots, n\}$ premier à n. [2]
4. *Utilisation des quotients de $\mathbb{K}[X]$*
   En utilisant le quotient, on obtient une preuve plus conceptuelle du théorème 1. La propriété universelle de $\mathbb{K}[X]$ fournit un unique morphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[X]$ dans $\mathbb{K}[y]$ envoyant X sur y, disons ψ_y :
   $$\forall P \in \mathbb{K}[X], \qquad \psi_y(P) = P(y).$$
   On a de même un unique morphisme de $\mathbb{K}$-algèbres ψ_x de $K[X]$ tel que
   $$\forall P \in \mathbb{K}[X], \qquad \psi_x(P) = P(x).$$
   Les deux morphismes ψ_x et ψ_y ont même noyau $(\Pi_{\mathbb{K},x}) = (\Pi_{\mathbb{K},y})$, d'où un unique morphisme de $\mathbb{K}$-algèbres σ de $\mathbb{K}[x]$ dans $\mathbb{K}[y]$ tel que
   $$\sigma \circ \psi_x = \psi_y.$$

2. Paraphrase : les éléments d'ordre n de $(\mathbb{C}^*, \times)$ sont $\mathbb{Q}$-conjugués.

5. *Unicité du corps de rupture*

   La proposition 1 montre en particulier que deux corps de rupture d'un polynôme irréductible P de $\mathbb{K}[X]$ sont deux $\mathbb{K}$-algèbres isomorphes. Attention, il peut y avoir plusieurs isomorphismes entre deux tels corps (composer avec des automorphismes de la source et/ou du but).

Exercice 4. ② *Montrer que les seuls endomorphismes continus de l'anneau* $\mathbb{C}$ *sont l'identité et la conjugaison complexe.* [3]

Exercice 5. ③ *a) On pose* $\mathbb{L} = \mathbb{Q}(e^{i\pi/4})$. *Montrer que* $\mathbb{L}$ *contient* $\mathbb{K}_1 = \mathbb{Q}(i)$, $\mathbb{K}_2 = \mathbb{Q}(\sqrt{2})$, $\mathbb{K}_3 = \mathbb{Q}(i\sqrt{2})$ [4].

b) Déterminer les $\mathbb{Q}$*-conjugués de* $e^{i\pi/4}$.

c) Déterminer les conjugués de $e^{i\pi/4}$ *sur* $\mathbb{K}_1, \mathbb{K}_2$ *et* $\mathbb{K}_3$.

Exercice 6. ③ *Déterminer les* $\mathbb{Q}$*-conjugués de* $\sqrt{2} + \sqrt[4]{2}$.

Exercice 7. ③ *Soient* x *un élément de* Ω *de degré* n *sur* $\mathbb{K}$, $\mathbb{L}$ *un sous-corps de* Ω *tel que* $\mathbb{L}/\mathbb{K}$ *soit finie de degré premier à* n. *Montrer que les* $\mathbb{K}$*-conjugués de* x *sont aussi des* $\mathbb{L}$*-conjugués de* x.

Exercice 8. ③ *Soient* $\mathbb{L}/\mathbb{K}$ *une extension,* $\mathbb{K}'$ *et* $\mathbb{K}''$ *deux sous-corps de* $\mathbb{L}$ *contenant* $\mathbb{K}$, *de degré* 2 *sur* $\mathbb{K}$ *et isomorphes en tant que* $\mathbb{K}$*-algèbres. Montrer que* $\mathbb{K}' = \mathbb{K}''$.

Exercice 9. ③ *Soit* $\mathbb{A}$ *un sous-anneau de* $\overline{\mathbb{Q}}$ *possédant les deux propriétés suivantes :*

(i) si x *est dans* $\mathbb{A}$, *les* $\mathbb{Q}$*-conjugués de* x *sont dans* $\mathbb{A}$ *;*

(ii) $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.

Montrer que : $\mathbb{A} \subset \overline{\mathbb{Z}}$.

L'exercice ci-après, particulièrement recommandé, généralise simultanément le lemme 1 et la proposition 1.

Exercice 10. ③ *Soient* $x_1, \ldots, x_n, y_1, \ldots, y_n$ *des éléments de* Ω. *Montrer qu'il existe un élément de* $Hom(\mathbb{K}(x_1, \ldots, x_n), \Omega)$ *envoyant, pour tout* i *de* $\{1, \ldots, n\}$, x_i *sur* y_i *si et seulement si*

$$\forall P \in \mathbb{K}[X_1, \ldots, X_n], \quad P(x_1, \ldots, x_n) = 0 \Rightarrow P(y_1, \ldots, y_n) = 0.$$

Exercice 11. ④ *Soient* x *un élément de* Ω, $\mathbb{L} = \mathbb{K}[x] = K(x)$. *À quelle condition existe-t-il un morphisme de* $\mathbb{K}$*-algèbres de* $\mathbb{L}$ *dans* $\mathcal{M}_n(\mathbb{K})$ *?*

Exercice 12. ④ *a) Déterminer les endomorphismes, puis les automorphismes, de la* $\mathbb{K}$*-algèbre* $\mathbb{K}(X)$.

b) Vérifier que l'application :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \mapsto \quad \frac{aX+b}{cX+d}$$

3. L'axiome du choix permet de démontrer que l'ensemble des automorphismes de l'anneau $\mathbb{C}$ a la puissance du continu, cf exercice 36 de la section **5**. Mais les deux morphismes précédents sont les seuls « explicitables ».

4. La théorie de Galois nous apprendra que $\mathbb{Q}, \mathbb{K}_1, \mathbb{K}_2, \mathbb{K}_3, \mathbb{L}$ sont les seuls sous-corps de $\mathbb{L}$.

est un morphisme surjectif du $GL_2(\mathbb{K})$ dans le groupe (pour $\circ$) des homographies, dont le noyau est le centre de $GL_2(\mathbb{K})$.

c) Conclure que le groupe des automorphismes de la $\mathbb{K}$-algèbre $\mathbb{K}(X)$ est naturellement isomorphe à $PGL_2(\mathbb{K})$.

La suite de ce chapitre est une série de variations sur la proposition 1.

3 Morphismes de $\mathbb{K}$-algèbres

On étudie dans cette section les morphismes de $\mathbb{K}$-algèbres entre deux extensions finies de $\mathbb{K}$. Les résultats obtenus jouent un rôle central dans la suite. Ils sont fondés sur un théorème de prolongement des morphismes, auquel est dévolu le paragraphe **3.1**.

Dans les paragraphes **3.3** et **3.4**, on se limite à la caractéristique nulle, de manière à éviter les problèmes de séparabilité. La section **4**, facultative, reprend les mêmes questions dans le cas général.

3.1 Prolongement d'un morphisme à une extension monogène finie

Pour x dans Ω, les éléments de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(x), \Omega)$ peuvent être vus comme les prolongements de $\mathrm{Id}_{\mathbb{K}}$ en un morphisme de corps de $\mathbb{K}(x)$ dans Ω. Le résultat suivant est donc une généralisation naturelle de la proposition 1 : on part d'un morphisme de corps arbitraire plutôt que de l'identité. Il va jouer un rôle central.

Théorème 1. *Soient $\mathbb{K}, \mathbb{K}'$ deux corps, $\mathbb{L}/\mathbb{K}$ et $\mathbb{L}'/\mathbb{K}'$ deux extensions, σ un isomorphisme de $\mathbb{K}$ sur $\mathbb{K}'$, x un élément de $\mathbb{L}$ algébrique sur $\mathbb{K}$ et x' un élément de $\mathbb{L}'$. Les deux assertions suivantes sont équivalentes.*

i) Il existe σ' dans $Hom(\mathbb{K}(x), \mathbb{L}')$ prolongeant σ et envoyant x sur x'.

ii) L'élément x' est algébrique sur $\mathbb{K}'$, et $\Pi_{\mathbb{K}',x'} = \sigma.\Pi_{\mathbb{K},x}$.

Si ces conditions sont réalisées, le prolongement donné par i) est unique, et induit un isomorphisme du corps $\mathbb{K}(x)$ sur le corps $\mathbb{K}'(x')$.

Preuve. La démonstration copie celle de la proposition 1. Si *i)* est vérifiée, alors

$$\forall P \in \mathbb{K}[X], \qquad \sigma'\left(P(x)\right) = \sigma.P(x').$$

Ceci montre que x' est algébrique sur $\mathbb{K}'$ et que $\Pi_{\mathbb{K}',x'}$ divise $\sigma.\Pi_{\mathbb{K},x}$, d'où l'égalité de ces deux polynômes, tous deux irréductibles sur $\mathbb{K}'$ et unitaires. On a établi *ii)* et l'unicité d'un éventuel prolongement. Réciproquement, si *ii)* est réalisée, l'application :

$$\begin{array}{rccc} \Phi \ : & \mathbb{K}[X] & \to & \mathbb{L}' \\ & P & \mapsto & \sigma.P(x') \end{array}$$

définit un morphisme d'anneaux de noyau engendré par $\Pi_{\mathbb{K},x}$. Ceci permet de définir, par passage au quotient, un morphisme d'anneaux σ' de $\mathbb{K}[x]$ dans $\mathbb{L}$ en posant :

$$\forall P \in \mathbb{K}[X], \qquad \sigma'\left(P(x)\right) = \sigma.P(x').$$

Ce morphisme prolonge σ et induit clairement une bijection de $\mathbb{K}(x)$ sur $\mathbb{K}'(x')$.

Si $\mathbb{L}' = \Omega$, on dispose d'une racine x' de $\sigma.\Pi_{\mathbb{K},x}$ dans Ω et donc d'au moins un prolongement de σ en un élément de $\mathrm{Hom}(\mathbb{K}(x), \Omega)$. En notant qu'une extension finie de $\mathbb{K}$ est engendrée par un nombre fini d'éléments algébriques sur $\mathbb{K}$, une récurrence immédiate fournit l'énoncé ci-après.

Proposition 2. *Soit $\mathbb{L}/\mathbb{K}$ une extension finie. Tout élément de $Hom(\mathbb{K}, \Omega)$ admet au moins un prolongement en un élément de $Hom(\mathbb{L}, \Omega)$.*

La possibilité de prolonger un morphisme à une extension finie a la conséquence importante suivante.

Corollaire 1. *Soient x un élément de Ω, $\mathbb{L}$ une extension finie de $\mathbb{K}$ contenant x. Alors les $\mathbb{K}$-conjugués de x sont les $\sigma(x)$ pour σ dans $Hom_{\mathbb{K}}(\mathbb{L}, \Omega)$.*

Preuve. Soit x' un $\mathbb{K}$-conjugué de x. La proposition 1 donne un élément de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(x), \Omega)$ envoyant x sur x'. Comme l'extension $\mathbb{L}/\mathbb{K}(x)$ est finie, la proposition 2 permet d'étendre ce morphisme en un élément de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$.

Nous verrons dans la section **5** que la proposition 2 se généralise à une extension algébrique quelconque, non nécessairement finie.

Exercice 13. ③ *Soient P un polynôme de $\mathbb{K}[X]$, σ un morphisme de $\mathbb{K}$ dans le corps $\mathbb{K}'$, $\mathbb{L}$ (resp. $\mathbb{L}'$) un surcorps de $\mathbb{K}$ (resp. $\mathbb{K}'$) sur lequel P (resp. $\sigma.P$) est scindé. Montrer que le nombre de racines distinctes de P dans $\mathbb{L}$ est égal au nombre de racines distinctes de $\sigma.P$ dans $\mathbb{L}'$.*

Remarques

1. *Conjugués d'une somme, d'un produit*

   Soient x et y dans Ω, $x_1 = x, \ldots, x_m$ les $\mathbb{K}$-conjugués distincts de x dans Ω, $y_1 = y, \ldots, y_n$ ceux de y. Alors $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_m, y_1, \ldots, y_n)$, est une extension finie de $\mathbb{K}$. En appliquant le corollaire 1, on voit que les $\mathbb{K}$-conjugués de $x + y$ sont de la forme $x_i + y_j$, ceux de xy de la forme $x_i y_j$. Ce résultat peut également se déduire du théorème des polynômes symétriques, cf. chapitre **2**, paragraphe **3.1**, remarque 1.

2. *Conjugués d'un nombre complexe constructible*

   Rappelons (chapitre 2, section **5**) qu'un nombre complexe z est constructible s'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 $i \in \{0, \ldots, n-1\}$,
   - $z \in \mathbb{K}_n$.

   Il découle de cette caractérisation et de la proposition 2 que, si z est constructible, il en est de même de tout $\mathbb{Q}$-conjugué z' de z. Le critère de Wantzel montre alors que, pour tout $\mathbb{Q}$-conjugué de z, $[\mathbb{Q}(z) : \mathbb{Q}]$ est une puissance de 2. Par multiplicativité du degré, $[D_{\mathbb{Q}}P : \mathbb{Q}]$ est puissance de 2, comme annoncé dans le chapitre 2.

Exercice 14. ① *Avec les notations précédentes, donner un exemple très simple montrant que tous les $x_i + y_j$ ne sont pas des $\mathbb{K}$-conjugués de $x + y$.*

Exercice 15. ④ *Soient $\mathbb{K}$ un corps de caractéristique nulle, P un irréductible de $\mathbb{K}[X]$, x et y deux racines distinctes de P dans un surcorps de $\mathbb{K}$. Montrer que $x - y$ n'appartient pas à $\mathbb{K}$. Montrer que ce résultat tombe en défaut en caractéristique p.*

3.2 Unicité du corps de décomposition

La proposition 1 contient, comme on l'a signalé, l'énoncé d'« unicité du corps de rupture d'un polynôme irréductible ». Le théorème 1 permet d'établir le résultat correspondant concernant le corps de décomposition.

Proposition 3. *Soient $\mathbb{K}$ et $\mathbb{K}'$ deux corps, σ un isomorphisme de corps de $\mathbb{K}$ sur $\mathbb{K}'$, P un élément de $\mathbb{K}[X]$ non constant, $\mathbb{L}$ un corps de décomposition de P sur $\mathbb{K}$, $\mathbb{L}'$ une extension de $\mathbb{K}'$. Les assertions suivantes sont équivalentes.*

i) Il existe un morphisme $\tilde{\sigma}$ de corps de $\mathbb{L}$ dans $\mathbb{L}'$ prolongeant σ.

ii) Le polynôme $\sigma.P$ est scindé sur $\mathbb{L}'$.

Preuve. L'implication *i)* $\Rightarrow$ *ii)* doit être claire à ce stade. La réciproque se prouve par récurrence sur $[\mathbb{L} : \mathbb{K}]$. Si $\mathbb{L} = \mathbb{K}$, il n'y a rien à montrer. Admettons le résultat si $[\mathbb{L} : \mathbb{K}] \leq n - 1$ où $n \geq 2$, et supposons maintenant $[\mathbb{L} : \mathbb{K}] = n$ et $\sigma.P$ scindé sur L'. Soient $x \in \mathbb{L}$ une racine de P n'appartenant pas à $\mathbb{K}$ et $Q = \Pi_{\mathbb{K},x}$. Le polynôme Q est de degré ≥ 2, et divise P. Par hypothèse, on dispose d'une racine x' de $\sigma.P$ dans $\mathbb{L}'$. Le théorème 1 fournit un isomorphisme de corps σ' de $\mathbb{K}(x)$ sur $\mathbb{K}'(x')$ prolongeant σ et envoyant x sur x'. Mais $\mathbb{L}$ est un corps de décomposition de $U = \dfrac{P}{X - x}$ sur $\mathbb{K}(x)$, et $\sigma.U = \dfrac{\sigma.P}{X - x'}$ est scindé sur $\mathbb{L}'$. Puisque $[\mathbb{L} : \mathbb{K}(x)] < n$, l'hypothèse de récurrence donne un morphisme $\tilde{\sigma}$ de $\mathbb{L}$ dans $\mathbb{L}'$ prolongeant σ', donc σ.

On déduit de cette proposition l'unicité du corps de décomposition.

Corollaire 2. *Soient $\mathbb{K}$ un corps, $P \in \mathbb{K}[X]$, $\mathbb{L}$ et $\mathbb{L}'$ deux corps de décomposition de P sur $\mathbb{K}$. Les $\mathbb{K}$-algèbres $\mathbb{L}$ et $\mathbb{L}'$ sont isomorphes.*

Preuve. En prolongeant l'identité de $\mathbb{K}$, on obtient un morphisme de $\mathbb{K}$-algèbres σ de $\mathbb{L}$ dans $\mathbb{L}'$. Ce morphisme est injectif, d'où : $[\mathbb{L} : \mathbb{K}] \leq [\mathbb{L}' : \mathbb{K}]$. Comme $\mathbb{L}$ et $\mathbb{L}'$ jouent des rôles symétriques, on en déduit que $[\mathbb{L}' : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]$, d'où la bijectivité de σ.

En pratique, la question de l'unicité du corps de décomposition n'apparaît pas vraiment. Rappelons (chapitre **2**, **4.1**, remarque 3) que, si $P \in \mathbb{K}[X]$ est non constant, P admet un unique corps de décomposition contenu dans Ω, à savoir

$$D_{\mathbb{K}}P = \mathbb{K}(\mathcal{R})$$

où $\mathcal{R}$ désigne l'ensemble des racines de P dans Ω.

3.3 Nombre de prolongements (caractéristique nulle)

Si $\mathbb{K}$ est de caractéristique nulle, toute extension finie de $\mathbb{K}$ est monogène. D'autre part, les polynômes irréductibles sur un sous-corps de Ω sont simplement scindés sur Ω. Le théorème 1 admet donc la conséquence fondamentale ci-après.

Corollaire 3. *Supposons $\mathbb{K}$ de caractéristique nulle. Soit $\mathbb{L}/\mathbb{K}$ une extension finie. Tout élément de $Hom(\mathbb{K}, \Omega)$ admet exactement $[\mathbb{L} : \mathbb{K}]$ prolongements en un élément de $Hom(\mathbb{L}, \Omega)$.* [5]

5. Ce résultat et sa démonstration s'étendent aux corps parfaits. Il en est de même du corollaire 4.

Explicitons le cas où le morphisme est l'identité de $\mathbb{K}$ dans Ω.

Corollaire 4. *Supposons $\mathbb{K}$ de caractéristique nulle. Soit $\mathbb{L}/\mathbb{K}$ une extension finie. Alors*

$$|Hom_{\mathbb{K}}(\mathbb{L}, \Omega)| = [\mathbb{L} : \mathbb{K}].$$

3.4 Caractérisation du corps de base (caractéristique nulle)

On déduit du corollaire 1 un critère d'appartenance au corps de base. [6]

Corollaire 5. *Supposons $\mathbb{K}$ de caractéristique nulle. Soit $\mathbb{L}/\mathbb{K}$ une extension finie. Alors, pour x dans $\mathbb{L}$, on a* [7]

$$x \in \mathbb{K} \Longleftrightarrow \forall \sigma \in Hom_{\mathbb{K}}(\mathbb{L}, \Omega), \quad \sigma(x) = x.$$

Applications

1. *Annulateur d'une somme d'éléments algébriques*
   Supposons $\mathbb{K}$ de caractéristique 0. Soient x et y deux éléments de Ω algébriques sur $\mathbb{K}$. Factorisons sur Ω les polynômes minimaux de x et y :

   $$\Pi_{\mathbb{K},x} = \prod_{i=1}^{m}(X - x_i) \quad \Pi_{\mathbb{K},y} = \prod_{j=1}^{n}(X - y_j).$$

   Soient :

   $$P = \prod_{\substack{1 \le i \le m \\ 1 \le j \le n}} (X - (x_i + y_j)), \quad \mathbb{L} = \mathbb{K}(x_1, \ldots, x_m, y_1, \ldots, y_n).$$

   Si σ est un élément de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$, on a clairement

   $$\sigma.P = P.$$

   Il s'ensuit P est dans $\mathbb{K}[X]$, résultat démontré dans le chapitre **2** via le théorème des polynômes symétriques. On retrouve la « linéarité des $\mathbb{K}$-conjugués ». Un argument analogue vaut pour le produit.

2. *Décomposition $D + N$*
   Supposons $\mathbb{K}$ de caractéristique zéro. Soient $M \in \mathcal{M}_n(\mathbb{K})$ de polynôme caractéristique P et $\mathbb{L} = \mathrm{D}_{\mathbb{K}}P$ le corps de décomposition de P dans Ω. Il est classique que M s'écrit d'une unique façon sous la forme $D + N$ avec D et N dans $\mathcal{M}_n(\mathbb{L})$, D semi-simple, N nilpotente et $DN = ND$. Alors D et N sont dans $\mathcal{M}_n(\mathbb{K})$. En effet, si $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$ on a, avec des notations évidentes :

   $$M = \sigma.M = \sigma.D + \sigma.N.$$

   Les matrices $\sigma.D$ et $\sigma.N$ sont dans $\mathcal{M}_n(\mathbb{L})$, respectivement semi-simple et nilpotente, et commutent. L'unicité de la décomposition entraîne que $\sigma.D = D$ et $\sigma.N = N$, le corollaire 5 permet de conclure.

6. Généralisation de la caractérisation des nombres réels comme points fixes de la conjugaison complexe.

7. Ce résultat et sa démonstration s'étendent aux corps parfaits. Il en est de même de l'application à la réduction de Jordan ci-dessous, explicitée par Chevalley.

3. *Un résultat d'irrationalité*

   Soient $x_1, \ldots, x_r$ des éléments de $\mathbb{R}^{+*}$ algébriques sur $\mathbb{Q}$. On suppose que tous les $\mathbb{Q}$-conjugués de x_i sont de modules $\leq x_i$ si $1 \leq i \leq r$. Cherchons si $x = x_1 + \cdots + x_r$ peut être rationnel. Soit $\mathbb{K} = \mathbb{Q}(x_1, \ldots, x_r)$. Dire que $x \in \mathbb{Q}$ c'est dire que, pour tout morphisme σ de $\mathbb{K}$ dans $\overline{\mathbb{Q}}$, $\sigma(x) = x$. Grâce à l'hypothèse sur les modules, ceci n'est possible que si pour tout σ de $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{K}, \overline{\mathbb{Q}})$ et pour tout i de $\{1, \ldots, r\}$, $\sigma(x_i) = x_i$, autrement dit si $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{K}, \overline{\mathbb{Q}})$ est réduit à un élément, i.e. si et seulement si $\mathbb{K} = \mathbb{Q}$.

   Ainsi, x est dans $\mathbb{Q}$ si et seulement si tous les x_i sont dans $\mathbb{Q}$. Par exemple, si $a_1, \ldots, a_n \in \mathbb{Q}^{+*}$, $n_1, \ldots, n_r \in \mathbb{N}^*$, $\displaystyle\sum_{i=1}^{r} (a_i)^{1/n_i}$ n'est dans $\mathbb{Q}$ que s'il en est de même de tous les ${a_i}^{1/n_i}$.

Exercice 16. ③ *Soit P un élément irréductible de $\mathbb{Q}[X]$ admettant exactement une racine réelle r. Soient z une racine complexe de P autre que r, x sa partie réelle. Montrer qu'il existe σ dans $Hom_{\mathbb{Q}}(\mathbb{Q}(z, \overline{z}), \mathbb{C})$ tel que $\sigma(x) \notin \mathbb{R}$. En déduire que x n'est pas rationnel.*

4 Séparabilité (III)

Nous revenons sur les résultats de la section **3**, avec les objectifs suivants :

- examiner ce qui se passe en caractéristique p ;

- prouver les résultats sans recours au théorème de l'élément primitif (cf. chapitre **2**, paragraphe **3.3**, note 11) ;

- donner une nouvelle démonstration de ce dernier théorème. [8]

4.1 Séparabilité et morphismes

Soient $\mathbb{L}$ une extension de $\mathbb{K}$, x un élément de $\mathbb{L}$ algébrique sur $\mathbb{K}$. Le nombre de prolongements d'un élément σ de $\mathrm{Hom}(\mathbb{K}, \Omega)$ en un élément de $\mathrm{Hom}(\mathbb{K}(x), \Omega)$ est le nombre de racines de $\sigma.\Pi_{\mathbb{K},x}$ dans Ω. Puisque Ω est algébriquement clos, ce nombre est supérieur ou égal à 1, ce qui signifie que le prolongement est toujours possible et que le nombre de prolongements est majoré par le degré de $\sigma.\Pi_{\mathbb{K},x}$, c'est-à-dire par $[\mathbb{K}(x) : \mathbb{K}]$. Le cas d'égalité de cette majoration est atteint lorsque $\sigma.\Pi_{\mathbb{K},x}$ est séparable. Or, on a le lemme suivant.

Lemme 2. *Soient P un élément de $\mathbb{K}[X]$, σ un élément de $Hom(\mathbb{K}, \Omega)$. Alors P est séparable si et seulement si $\sigma.P$ est séparable.*

Preuve. Supposons P séparable. On dispose de U et V dans $\mathbb{K}[X]$ tels que

$$UP + VP' = 1.$$

On applique σ, en notant que

$$\sigma.P' = (\sigma.P)'$$

8. Comme d'habitude, le lecteur intéressé uniquement par la caractéristique nulle peut omettre cette section. Une option intermédiaire est de lire la preuve du théorème 2 et le paragraphe **4.2** en se plaçant en caractéristique nulle.

et on obtient une relation de Bézout entre $\sigma.P$ et $(\sigma.P)'$, ce qui entraîne que $\sigma.P$ est séparable. La réciproque se traite de même, en considérant le morphisme de corps σ^{-1}, dont la source est le corps $\sigma(\mathbb{K})$.

En utilisant ce lemme et la discussion qui le précède, on obtient le résultat suivant.

Proposition 4. *Soient $\mathbb{L}$ une extension de $\mathbb{K}$, x un élément de $\mathbb{L}$ algébrique sur $\mathbb{K}$, σ un élément de $Hom(\mathbb{K}, \Omega)$. L'ensemble des prolongements de σ en un élément de $Hom(\mathbb{K}(x), \Omega)$ est non vide de cardinal majoré par $[\mathbb{K}(x) : \mathbb{K}]$, avec égalité si et seulement si x est séparable sur $\mathbb{K}$.*

On peut maintenant établir une généralisation commune au théorème 1 et au corollaire 3, et ce sans utiliser le théorème de l'élément primitif.

Théorème 2. *Soient $\mathbb{L}/\mathbb{K}$ une extension finie, σ un élément de $Hom(\mathbb{K}, \Omega)$. L'ensemble des prolongements de σ en un élément de $Hom(\mathbb{L}, \Omega)$ est non vide de cardinal majoré par $[\mathbb{L} : \mathbb{K}]$. Il y a égalité si et seulement si $\mathbb{L}/\mathbb{K}$ est séparable.*

Preuve. Supposons $\mathbb{L}/\mathbb{K}$ séparable et écrivons $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_n)$ où les x_i sont algébriques et séparables sur $\mathbb{K}$. Pour tout i de $\{1, \ldots, n\}$, x_i est séparable sur $\mathbb{K}$, donc sur $\mathbb{K}(x_1, \ldots, x_{i-1})$. L'ensemble des prolongements d'un élément de $\mathrm{Hom}(\mathbb{K}(x_1, \ldots, x_{i-1}), \Omega)$ en un élément de $\mathrm{Hom}(\mathbb{K}(x_1, \ldots, x_i), \Omega)$ est donc fini de cardinal $[\mathbb{K}(x_1, \ldots, x_i) : \mathbb{K}(x_1, \ldots, x_{i-1})]$. On déduit de ce fait et de la multiplicativité des degrés, que pour tout i de $\{1, \ldots, n\}$, l'ensemble des prolongements de σ en un élément de $\mathrm{Hom}(\mathbb{K}(x_1, \ldots, x_i), \Omega)$ est fini de cardinal $[\mathbb{K}(x_1, \ldots, x_i) : \mathbb{K}]$.

Si $\mathbb{L}/\mathbb{K}$ n'est pas séparable, on reprend l'argument, mais en choisissant x_1 non séparable sur $\mathbb{K}$. Pour i dans $\{1, \ldots, n\}$, l'ensemble des prolongements d'un élément de $\mathrm{Hom}(\mathbb{K}(x_1, \ldots, x_{i-1}), \Omega)$ en un élément de $\mathrm{Hom}(\mathbb{K}(x_1, \ldots, x_i), \Omega)$ est donc fini de cardinal majoré par $[\mathbb{K}(x_1, \ldots, x_i) : \mathbb{K}(x_1, \ldots, x_{i-1})]$, avec inégalité stricte pour $i = 1$. On déduit de ce fait et de la multiplicativité des degrés que, pour tout i de $\{1, \ldots, n\}$, l'ensemble des prolongements du morphisme σ en un élément de $\mathrm{Hom}(\mathbb{K}(x_1, \ldots, x_i), \Omega)$ est fini de cardinal strictement inférieur à $[\mathbb{K}(x_1, \ldots, x_i) : \mathbb{K}]$.

Les corollaires 4 et 5 peuvent maintenant être raffiné et généralisés.

Corollaire 6. *Soit $\mathbb{L}/\mathbb{K}$ une extension finie. Alors*

$$|Hom_{\mathbb{K}}(\mathbb{L}, \Omega)| \leq [\mathbb{L} : \mathbb{K}],$$

avec égalité si et seulement si $\mathbb{L}/\mathbb{K}$ est séparable.

Preuve. C'est le cas particulier du théorème précédent pour lequel σ est l'identité de $\mathbb{K}$ dans Ω.

Corollaire 7. *Soit $\mathbb{L}/\mathbb{K}$ une extension séparable finie. Alors, pour x dans $\mathbb{L}$, on a*

$$x \in \mathbb{K} \Longleftrightarrow \forall \sigma \in Hom_{\mathbb{K}}(\mathbb{L}, \Omega), \quad \sigma(x) = x.$$

Exercice 17. ④ *a) Généraliser le résultat de* **3.4** *relatif à la décomposition* $D + N$.

b) Donner un exemple de matrice M *de* $\mathcal{M}_2(\mathbb{F}_2(T))$ *dont la partie semi-simple et la partie nilpotente n'appartiennent pas à* $\mathcal{M}_2(\mathbb{F}_2(T))$.

La démonstration du théorème 2 fournit également un résultat attendu.

Corollaire 8. *Soient* $x_1, \ldots, x_n$ *des éléments de* Ω *algébriques sur* $\mathbb{K}$. *L'extension* $\mathbb{K}(x_1, \ldots, x_n)/\mathbb{K}$ *est séparable si et seulement si tous les* x_i *sont séparables sur* $\mathbb{K}$.

Preuve. La séparabilité des x_i est ce qu'il faut pour faire fonctionner la preuve de la partie directe du théorème 2 et obtenir l'égalité

$$|\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(x_1, \ldots, x_n), \Omega)| = [\mathbb{K}(x_1, , \ldots, x_n) : \mathbb{K}].$$

La partie réciproque du corollaire 6 permet de conclure.

Du corollaire 8 on déduit immédiatement le fait suivant.

Corollaire 9. *Soit* $\mathbb{L}/\mathbb{K}$ *une extension. L'ensemble des éléments de* $\mathbb{L}$ *séparables sur* $\mathbb{K}$ *est un sous-corps de* $\mathbb{L}$.

L'exercice suivant donne une approche des résultats précédents fondée sur la réduction des endomorphismes. Ces arguments un peu ad-hoc se comprennent nettement mieux lorsque les notions sont reformulées en termes de produit tensoriel et d'algèbres étales [9].

Exercice 18. ④ *Soient* $\mathbb{L}/\mathbb{K}$ *une extension finie,* μ_x *l'endomorphisme de multiplication par* x *dans* $\mathbb{L}$.

a) Montrer que x *est séparable sur* $\mathbb{K}$ *si et seulement* μ_x *est semi-simple.*

b) Retrouver le corollaire 8 en utilisant a) et la codiagonalisabilité d'une famille commutative de matrices diagonalisables.

c) Retrouver le théorème de l'élément primitif à l'aide de a).

On peut également obtenir la transitivité de la séparabilité.

Corollaire 10. *Supposons* $\mathbb{L}/\mathbb{K}$ *et* $\mathbb{M}/\mathbb{L}$ *finies séparables. Alors* $\mathbb{M}/\mathbb{K}$ *est finie séparable.*

Preuve. On a

$$|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)| = [\mathbb{L} : \mathbb{K}]$$

et tout élément de $\mathrm{Hom}(\mathbb{L}, \Omega)$ admet exactement $[\mathbb{M} : \mathbb{L}]$ prolongements en un élément de $\mathrm{Hom}(\mathbb{M}, \Omega)$, ce qui prouve

$$|\mathrm{Hom}_{\mathbb{K}}(\mathbb{M}, \Omega)| = [\mathbb{M} : \mathbb{L}] \times [\mathbb{L} : \mathbb{K}] = [\mathbb{M} : \mathbb{K}].$$

Exercice 19. ③ *Montrer que si les extensions* $\mathbb{M}/\mathbb{L}$ *et* $\mathbb{L}/\mathbb{K}$ *sont séparables, il en est de même de* $\mathbb{M}/\mathbb{L}$.

9. Version Grothendieck de la théorie de Galois, fondamentale, mais sensiblement plus conceptuelle que le contenu de ces notes.

Exercice 20. ③ *Soit $\mathbb{L}$ une extension finie de $\mathbb{K}$. Montrer que $\mathbb{L}$ est parfait si et seulement si $\mathbb{K}$ est parfait.*

Exercice 21. ③ *Soient $\mathbb{L}/\mathbb{K}$ une extension séparable finie, x un élément de $\mathbb{L}$. Quel est le cardinal de l'ensemble des σ de $Hom_{\mathbb{K}}(\mathbb{L},\Omega)$ tels que $\sigma(x)=y$?*

Dans les exercices ci-après, $\mathbb{K}$ est un corps de caractéristique p. On étudie plus précisément le phénomène d'inséparabilité.

Exercice 22. ④ *Soient x un élément de Ω,*

$$r=\max\left\{i\in\mathbb{N},\ \Pi_{K,x}\in\mathbb{K}[X^{p^i}]\right\}.$$

a) Montrer que le nombre de $\mathbb{K}$-conjugués distincts de x dans Ω est

$$d=\frac{[\mathbb{K}(x):\mathbb{K}]}{p^r}.$$

De plus, x^{p^r} est séparable et de degré d sur $\mathbb{K}$.

Le nombre d est appelé degré séparable de x sur $\mathbb{K}$. Si $d=1$, on dit que x est radiciel (ou purement inséparable) sur $\mathbb{K}$.

b) Montrer qu'un élément x de Ω est radiciel sur $\mathbb{K}$ si et seulement s'il existe $s\in\mathbb{N}$ tel que x^{p^s} appartienne à $\mathbb{K}$.

c) Montrer que l'ensemble des éléments de Ω radiciels sur $\mathbb{K}$ est un sous-corps de Ω contenant $\mathbb{K}$.

d) Quels sont les éléments de Ω radiciels et séparables sur $\mathbb{K}$?

e) Soit x un élément de Ω radiciel sur $\mathbb{K}$. Décrire les sous-corps de $\mathbb{K}(x)$ contenant $\mathbb{K}$. Quel est leur nombre ?

Exercice 23. ④ *Une extension algébrique $\mathbb{L}$ de $\mathbb{K}$ est dite radicielle sur $\mathbb{K}$ si et seulement si tous ses éléments sont radiciels sur $\mathbb{K}$. Si $\mathbb{L}/\mathbb{K}$ est radicielle finie, montrer que son degré est une puissance de p.*

Exercice 24. ④ *Soient $\mathbb{L}$ une extension finie de $\mathbb{K}$ contenue dans Ω, $\mathbb{L}_s(\mathbb{K})$ le sous-corps des éléments de $\mathbb{L}$ séparables sur $\mathbb{K}$. Montrer que l'extension $\mathbb{L}/\mathbb{L}_s(\mathbb{K})$ est radicielle et que*

$$|Hom_{\mathbb{K}}(\mathbb{L},\Omega)|=[\mathbb{L}_s(\mathbb{K}):\mathbb{K}].$$

Exercice 25. ⑤ *Soit $\mathbb{F}$ un corps de caractéristique p. On note $\mathbb{K}=\mathbb{F}(X^p,Y^p)$, $\mathbb{L}=\mathbb{F}(X,Y)$, u une racine de T^p+YT+X dans Ω.*

a) Calculer $\Pi_{\mathbb{L},u}$ et $\Pi_{\mathbb{K},u}$.

b) Soit $\mathbb{M}$ un corps strictement intermédiaire entre $\mathbb{K}$ et $\mathbb{K}(u)$. Montrer que u n'est pas séparable sur $\mathbb{M}$. En déduire : $\mathbb{M}=\mathbb{K}(u^p)$.

c) Conclure que $\mathbb{K}(u)/\mathbb{K}$ n'est pas séparable mais que les éléments de $\mathbb{K}(u)$ radiciels sur $\mathbb{K}$ sont ceux de $\mathbb{K}$.

4.2 Le théorème de l'élément primitif (II)

Nous allons redémontrer et préciser le théorème suivant.

Théorème 3. *Soit $\mathbb{L}/\mathbb{K}$ une extension finie séparable, avec $\mathbb{K}$ infini. Alors $\mathbb{L}/\mathbb{K}$ est monogène.*

La preuve repose sur la caractérisation ci-après des éléments primitifs d'une extension séparable finie.

Lemme 3. *Soient $\mathbb{L}/\mathbb{K}$ une extension séparable finie. Si x est un élément de $\mathbb{L}$, on a $\mathbb{L} = \mathbb{K}(x)$ si et seulement si le seul élément σ de $Hom_{\mathbb{K}}(\mathbb{L}, \Omega)$ tel que $\sigma(x) = x$ est la restriction à $\mathbb{L}$ de l'identité de Ω.*

Preuve. L'extension $\mathbb{L}/\mathbb{K}(x)$ est séparable finie. Elle est donc de degré 1 si et seulement si $\left|\mathrm{Hom}_{\mathbb{K}(x)}(\mathbb{L}, \Omega)\right| = 1$, d'où le résultat.

Preuve du théorème 3. Notons $i_{\mathbb{L},\Omega}$ la restriction à $\mathbb{L}$ de l'identité de Ω, et fixons x dans $\mathbb{L}$. Le lemme 3 dit que $\mathbb{L} = \mathbb{K}(x)$ si et seulement si

$$x \notin \bigcup_{\substack{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega) \\ \sigma \neq i_{\mathbb{L},\Omega}}} \mathrm{Ker}\,(\sigma - i_{\mathbb{L},\Omega})$$

Comme un espace vectoriel sur un corps infini n'est pas réunion finie de sous-espaces stricts (lemme 3, chapitre 2), on a :

$$\mathbb{L} \neq \bigcup_{\substack{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega) \\ \sigma \neq i_{\mathbb{L},\Omega}}} \mathrm{Ker}\,(\sigma - i_{\mathbb{L},\Omega})\,.$$

Remarques

1. *Généricité des éléments primitifs*
   Si V est de dimension finie, la réunion d'un nombre fini de sous-espaces stricts est une sous-variété algébrique stricte de V ; un élément « générique » de $\mathbb{L}$ est donc primitif. La première démonstration du théorème de l'élément primitif (caractéristique nulle) établissait une forme faible de généricité : les éléments t de $\mathbb{K}$ tels que $x + ty$ soit élément primitif de $\mathbb{K}(x, y)/\mathbb{K}$ forment une partie cofinie de $\mathbb{K}$.
2. *Un exemple*
   Reprenons les notations de la seconde application de **3.2**. Le lemme 3 montre que :
   $$\sum_{i=1}^{r} x_i$$
   est élément primitif de $\mathbb{Q}(x_1, \ldots, x_r)$ sur $\mathbb{Q}$.

Exercice 26. ③ *On suppose $\mathbb{K}$ infini. Soient x et y dans Ω avec x séparable sur $\mathbb{K}$. Montrer que l'ensemble des t de $\mathbb{K}$ tels que : $\mathbb{K}(x, y) = \mathbb{K}(x + ty)$ est de complémentaire fini.*

Exercice 27. ③ *Soit $\mathbb{L}$ une extension séparable de degré infini de $\mathbb{K}$. Montrer que $\mathbb{L}$ contient des éléments de degré arbitrairement grand. Ce résultat subsiste-t-il pour une extension non séparable ?*

L'exercice ci-après montre que seule la première étape de la preuve du théorème de Steinitz est véritablement utile. On se borne à l'établir en caractéristique nulle, mais l'énoncé est vrai en toute généralité.

Exercice 28. ④ *On suppose $\mathbb{K}$ de caractéristique zéro. Soit $\mathbb{L}$ un sous-corps de Ω tel que tout polynôme non constant de $\mathbb{K}[X]$ admette au moins une racine dans $\mathbb{L}$. Montrer que $\mathbb{L} = \Omega$. Pour x dans Ω, on pourra considérer un élément primitif de $D_{\mathbb{K}}\Pi_{\mathbb{K},x}$ sur $\mathbb{K}$.*

Si P est un élément irréductible de degré n de $\mathbb{K}[X]$, tout corps de rupture de P est une extension de degré n de $\mathbb{K}$. Si $\mathbb{K}$ est de caractéristique nulle et admet une extension de degré n, le théorème de l'élément primitif permet d'écrire cette extension sous la forme $\mathbb{K}(x)$ et $\Pi_{\mathbb{K},x}$ est un irréductible de degré n de $\mathbb{K}[X]$. L'exercice ci-après établit un résultat analogue en caractéristique p.

Exercice 29. ⑤ *On suppose $\mathbb{K}$ de caractéristique $p > 0$. Soit $\mathbb{L}$ un sous-corps de Ω contenant $\mathbb{K}$ et de degré n sur $\mathbb{K}$.*

a) Justifier qu'il existe x dans $\mathbb{L}_s$ tel que $x \notin \mathbb{L}_s^p$ et $\mathbb{L}_s = \mathbb{K}(x)$, puis qu'il existe e dans $\mathbb{N}$ tel que $[\mathbb{L} : \mathbb{L}_s] = p^e$.

b) On pose $[\mathbb{L}_s : \mathbb{K}] = m$. Pour i dans $\mathbb{N}$, soit x_i une racine p^i-ième de x dans Ω. Montrer :

$$\forall i \in \mathbb{N}, \qquad [\mathbb{K}(x_i) : \mathbb{K}] = mp^i.$$

Conclure.

5 Prolongement d'un morphisme à une extension algébrique

Nous allons démontrer une généralisation, due à Steinitz, de la proposition 2 du paragraphe **3.1** aux extensions algébriques. La preuve ne comporte pas de nouvelle idée algébrique. L'essentiel est toujours d'arriver dans un corps algébriquement clos afin de pouvoir « résoudre » les équations qui apparaissent lors des prolongements successifs. L'ingrédient supplémentaire est un argument ensembliste standard permettant de « passer à l'infini ». [10]

Théorème 4. *Soient $\mathbb{L}/\mathbb{K}$ une extension algébrique, σ un morphisme de $\mathbb{K}$ dans Ω. Il existe alors un morphisme σ' de $\mathbb{L}$ dans Ω prolongeant σ.*

Preuve. Le cas des extensions finies est la proposition 2. Si $\mathbb{L} = \mathbb{K}(A)$ où A est dénombrable, on peut obtenir le résultat par une suite (dénombrable) de prolongements à des extensions finies.

Le cas général s'obtient à l'aide du lemme de Zorn. On considère l'ensemble $\mathcal{E}$ des couples $(\mathbb{M}, \theta)$, où $\mathbb{M}$ est un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et θ un morphisme de $\mathbb{L}$ dans Ω prolongeant σ. Cet ensemble est ordonné de façon naturelle par inclusion et prolongement :

$(\mathbb{M}, \theta) \leq (\mathbb{M}', \theta')$ si et seulement si $\mathbb{M} \subset \mathbb{M}'$ et θ' prolonge θ.

Le caractère inductif de l'ensemble ordonné $(\mathcal{E}, \leq)$ s'obtient facilement en considérant, si $(\mathbb{M}_i, \theta_i)_{i \in I}$ est une famille totalement ordonnée d'éléments de $\mathcal{E}$, le couple $(\mathbb{M}, \theta)$ formé de $\mathbb{M} = \cup_{i \in I} \mathbb{M}_i$ et du morphisme θ de $\mathbb{M}$ dans Ω

10. La situation est donc comparable à celle de la démonstration de l'existence d'un surcorps algébriquement clos. Ces résultats ont été démontrés dans le grand mémoire de Steinitz, *Algebraische Theorie des Körper*, datant de 1910, qui établit les résultats fondamentaux de la théorie des corps.

coïncidant, pour tout i de I, avec θ_i sur M_i. Ainsi, $(\mathcal{E}, \leq)$ admet un élément maximal $(\mathbb{M}', \sigma')$, et il reste à prouver que $\mathbb{M}' = \mathbb{L}$. Si tel n'est pas le cas, on choisit $x \in \mathbb{L} \setminus \mathbb{M}'$ et on étend σ' à $\mathbb{M}'(x)$, violant ainsi la maximalité de $(\mathbb{M}', \sigma')$.

Remarques

1. *Les extensions finies de $\mathbb{K}$ se plongent dans Ω*
   Le théorème 4 justifie l'assertion faite en début de chapitre : on ne perdrait rien à supposer d'emblée toutes les extensions finies (ou algébriques) de $\mathbb{K}$ considérées comme plongées dans Ω. Noter qu'une extension peut avoir plusieurs plongements : ainsi $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$ sont les trois corps de rupture de $X^3 - 2$ dans $\mathbb{C}$. La notion d'extension normale permettra de préciser ce point.
2. *Plongements et signature d'un corps de nombres*
   Rappelons qu'on appelle corps de nombres toute extension finie de $\mathbb{Q}$. On déduit du théorème 4 que tout corps de nombres se plonge dans $\overline{\mathbb{Q}}$, donc dans $\mathbb{C}$. Plus précisément, un corps de nombres $\mathbb{F}$ admet $[\mathbb{F} : \mathbb{Q}]$ plongements dans $\mathbb{C}$. Les plongements à image non contenue dans $\mathbb{R}$ se regroupent en paires conjuguées. Si r_1 (resp. $2r_2$) est le nombre de plongements réels (resp. irréels) de $\mathbb{F}$ alors $r_1 + 2r_2 = [\mathbb{F} : \mathbb{Q}]$. Le couple (r_1, r_2) est la *signature* de $\mathbb{F}$.

Exercice 30. ② *Retrouver à l'aide de la remarque 1 qu'une extension finie de $\mathbb{R}$ est isomorphe à $\mathbb{R}$ ou $\mathbb{C}$.*

Exercice 31. ① *Vérifier que deux corps de nombres isomorphes ont même signature.*

Exercice 32. ② *Déterminer la signature de $\mathbb{Q}(\sqrt[3]{2})$, celle de $\mathbb{Q}(\sqrt{3+\sqrt{3}})$, celle de $\mathbb{Q}(e^{2i\pi/n})$ pour n dans $\mathbb{N}^*$.*

Exercice 33. ③ *Soient $\mathbb{K}$ un corps de caractéristique $p > 0$, σ un morphisme de corps de $\mathbb{K}$ dans Ω, $\mathbb{L}$ une extension radicielle de $\mathbb{K}$. Montrer que σ admet un unique prolongement en un morphisme de $\mathbb{L}$ dans Ω.*

Exercice 34. ③ *Soit $\mathbb{F}$ un corps de nombres possédant au moins un plongement réel. Quelles sont les racines de l'unité contenues dans $\mathbb{F}$? Application au cas où $[\mathbb{F} : \mathbb{Q}]$ est impair.*

Exercice 35. ⑤ *Montrer que, pour tout couple (r_1, r_2) de $\mathbb{N}^2$, il existe un corps de nombres de signature (r_1, r_2).*

L'exercice ci-après demande un peu de pratique des questions de cardinalité.

Exercice 36. ④ *Soit $\mathbb{K}$ un corps infini. Montrer que toute extension algébrique de $\mathbb{K}$ est équipotente à $\mathbb{K}$.*

Le théorème 4 donne une description des $\mathbb{K}$-conjugués plus élégante que celles obtenues dans la proposition 1 et le corollaire 1.

Corollaire 11. *Soit x un élément de Ω. Alors les $\mathbb{K}$-conjugués de x sont les $\sigma(x)$ pour σ dans $Hom_{\mathbb{K}}(\Omega, \Omega)$.*

En particulier, le degré de $\Pi_{\mathbb{K},x}$ est le nombre d'éléments distincts de la forme $\sigma(x)$ avec σ dans $Hom_{\mathbb{K}}(\Omega, \Omega)$.

Nous allons établir l'unicité à isomorphisme près de « la » clôture algébrique. À cet effet, nous utiliserons le lemme élémentaire suivant.

Lemme 4. *Soient $\mathbb{L}/\mathbb{K}$ une extension algébrique, σ un endomorphisme de la $\mathbb{K}$-algèbre $\mathbb{L}$. Alors σ est bijectif.*

Preuve. Puisqu'un morphisme de corps est injectif, il suffit de prouver la surjectivité. Soient x dans $\mathbb{L}$ et $\mathcal{R}$ l'ensemble des racines de $\Pi_{\mathbb{K},x}$ dans $\mathbb{L}$. Si $y \in \mathcal{R}$ alors $\sigma(y) \in \mathcal{R}$. Puisque σ est injectif et $\mathcal{R}$ fini, σ induit une permutation de $\mathcal{R}$. En particulier, x admet un antécédent par σ.

Exercice 37. ② *Redémontrer le lemme 4 en utilisant le fait qu'un endomorphisme injectif d'un espace vectoriel de dimension finie est bijectif.*

Proposition 5. *Soient $\mathbb{K}_1$ et $\mathbb{K}_2$ deux clôtures algébriques de $\mathbb{K}$. Il existe un isomorphisme de $\mathbb{K}$-algèbres de $\mathbb{K}_1$ sur $\mathbb{K}_2$.*

Preuve. Le théorème 4 fournit deux morphismes de $\mathbb{K}$-algèbres $\sigma_1 : \mathbb{K}_1 \to \mathbb{K}_2$ et $\sigma_2 : \mathbb{K}_2 \to \mathbb{K}_1$. Le lemme 4 montre que $\sigma_1 \circ \sigma_2$ est bijectif, donc σ_1 aussi.

Remarque *Remord final*

La proposition 5 montre que les résultats relatifs aux morphismes à valeurs dans Ω ne dépendent pas de la clôture algébrique Ω de $\mathbb{K}$ que l'on s'est fixée.

Exercice 38. ③ *Montrer que le corollaire 7 s'étend aux extensions séparables infinies.*

Exercice 39. ③ *Soit $\mathbb{K}$ un sous-corps de $\mathbb{R}$ tel que*

$$(1) \qquad \forall x \in \mathbb{K} \cap \mathbb{R}^+, \qquad \sqrt{x} \in \mathbb{K}.$$

a) Montrer que l'extension $\mathbb{K}/\mathbb{Q}$ n'est pas finie.

b) Montrer que tout endomorphisme de $\mathbb{K}$ est croissant, puis que le seul endomorphisme de $\mathbb{K}$ est l'identité.

c) Montrer que $\mathbb{R} \cap \overline{\mathbb{Q}}$ vérifie (1).

Exercice 40. ④ *a) Soit $\mathbb{K} = \mathbb{Q}(i, \sqrt{2})$. Montrer qu'il existe un unique automorphisme σ de $\mathbb{K}$ envoyant i sur i, $\sqrt{2}$ sur $-\sqrt{2}$.*

b) Soit σ' un prolongement de σ en un automorphisme de $\overline{\mathbb{Q}}$. Montrer que $\sigma' \circ \sigma'$ n'est pas l'identité de $\overline{\mathbb{Q}}$.

c) En déduire un énoncé traduisant l'« absence d'un foncteur clôture algébrique »[11].

Exercice 41. ④ *Montrer que l'ensemble des automorphismes de $\overline{\mathbb{Q}}$ (c'est-à-dire le groupe de Galois de $\overline{\mathbb{Q}}/\mathbb{Q}$, comme nous le verrons dans le chapitre* **4***) est équipotent à $\mathbb{R}$.*

11. Question réservée au lecteur connaissant les rudiments de la théorie des catégories. Grossièrement dit, la première question montre qu'il n'existe pas de manière de prolonger un automorphisme de $\mathbb{K}$ en un automorphisme de « sa » clôture algébrique en respectant la composition.

6 L'indépendance linéaire des morphismes

L'énoncé suivant de Dedekind s'applique en particulier aux morphismes de corps ; Artin en a fait un des outils essentiels de la théorie de Galois. Il est largement indépendant du reste de ce chapitre.

Théorème 5. *Soient Γ un monoïde, $\mathbb{K}$ un corps, $\sigma_1, \dots, \sigma_n$ des morphismes distincts de Γ dans $(\mathbb{K}^*, \times)$. Alors $(\sigma_i)_{1 \leq i \leq n}$ est une famille libre du $\mathbb{K}$-espace vectoriel $\mathcal{F}(\Gamma, \mathbb{K})$.*

Preuve. Considérons par l'absurde une relation de dépendance de longueur minimale entre $\sigma_1, \dots, \sigma_n$. Quitte à réindexer, une telle relation s'écrit :

$$\sum_{i=1}^{p} \lambda_i \sigma_i = 0,$$

où les λ_i sont dans $\mathbb{K}^*$ et $2 \leq p \leq n$. Puisque $\sigma_1 \neq \sigma_2$, on choisit $y \in \Gamma$ tel que $\sigma_1(y) \neq \sigma_2(y)$. On a :

$$(1) \quad \forall x \in \Gamma, \quad \sum_{i=1}^{p} \lambda_i \sigma_i(x) = 0 \quad \text{et} \qquad (2) \quad \forall x \in \Gamma, \quad \sum_{i=1}^{p} \lambda_i \sigma_i(y) \sigma_i(x) = 0.$$

En combinant ces deux relations, on obtient :

$$(3) \qquad \forall x \in \Gamma, \qquad \sum_{i=2}^{p} \lambda_i \left(\sigma_i(y) - \sigma_1(y)\right) \sigma_i(x) = 0.$$

Comme $\lambda_2 \left(\sigma_2(y) - \sigma_1(y)\right)$ est non nul, (3) est une relation linéaire non triviale entre $\sigma_2, \dots, \sigma_p$, ce qui contredit la minimalité de (1).

Ce résultat permet de retrouver le corollaire 6. En effet, si $\mathbb{L}/\mathbb{K}$ une extension finie, les éléments de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$ forment une famille libre du Ω-espace vectoriel $\mathcal{L}_{\mathbb{K}}(\mathbb{L}, \Omega)$ des applications $\mathbb{K}$-linéaires de $\mathbb{L}$ dans Ω, d'où le corollaire 6 au vu de l'égalité :

$$\dim_{\Omega} \mathcal{L}_{\mathbb{K}}(\mathbb{L}, \Omega) = [\mathbb{L} : \mathbb{K}].$$

Exercice 42. ② *Déduire du théorème 5 l'indépendance linéaire sur $\mathbb{C}$:*

- *des fonctions $x \in \mathbb{R} \mapsto \exp(\alpha x)$, $\alpha \in \mathbb{C}$;*
- *des suites $(\theta^n)_{n \in \mathbb{N}}$, $\theta \in \mathbb{C}^*$.*

L'exercice suivant nécessite quelques connaissances en réduction des endomorphismes.

Exercice 43. ③ *Soient $\mathbb{L}/\mathbb{K}$ une extension finie de degré n, σ un élément de $Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{L})$. On voit σ comme un endomorphisme du $\mathbb{K}$-espace vectoriel $\mathbb{L}$. Montrer que le polynôme minimal de σ est de la forme $X^d - 1$. Que dire des invariants de similitude de σ ?*

L'exercice ci-après établit le *théorème d'Artin* sur l'indépendance algébrique des morphismes de corps en caractéristique nulle. [12]

12. Le résultat vaut en fait si $\mathbb{K}$ est un corps infini, mais quelques arguments supplémentaires sont nécessaires.

Exercice 44. ⑤ *On suppose $\mathbb{K}$ de caractéristique nulle. Soit n dans $\mathbb{N}^*$.*

a) Déterminer les P de $\mathbb{K}[X_1,\dots,X_n]$ tels que

$$P(X_1+Y_1,\dots,X_n+Y_n)=P(X_1,\dots,X_n)+P(Y_1,\dots,Y_n).$$

Soient $\lambda_1,\dots,\lambda_n$ des endomorphismes de $\mathbb{K}$, F un élément de $\mathbb{K}[X_1,\dots,X_n]$ tel que

$$\forall x\in\mathbb{K},\qquad F(\lambda_1(x),\dots,\lambda_n(x))=0.$$

b) Soit $G(X_1,\dots,X_n,Y_1,\dots,Y_n)$ le polynôme :

$$F(X_1+Y_1,\dots,X_n+Y_n)-F(X_1,\dots,X_n)-F(Y_1,\dots,Y_n).$$

Démontrer que G est nul.

c) Conclure que F est nul.

7 Trace et norme

Dans cette section optionnelle, on introduit deux applications importantes associés à une extension finie, la trace et la norme. Sans être indispensable, l'utilisation des morphismes clarifie le sujet.

Ces notions, à la marge de la théorie de Galois, jouent un rôle important en théorie algébrique des nombres ; on se contente ici d'élucider la structure additive de l'anneau des entiers d'un corps de nombres, en précisant le cas des corps cyclotomiques $\mathbb{Q}\left(\exp\left(\frac{2i\pi}{p}\right)\right)$ avec p premier. Par ailleurs, on démontre la caractérisation des binômes irréductibles de Vahlen-Capelli-Redei.

7.1 L'endomorphisme de multiplication par x

Si x est dans $\mathbb{L}$, l'application :

$$\begin{array}{rccc}\mu_x\ :& \mathbb{L} & \to & \mathbb{L}\\ & y & \mapsto & xy\end{array}$$

est $\mathbb{K}$-linéaire, de polynôme minimal :

$$\Pi_{\mathbb{K},x}=X^d+\sum_{i=0}^{d-1}a_iX^i.$$

On peut calculer son polynôme caractéristique de la manière suivante.

Lemme 5. *Le polynôme caractéristique de μ_x est $\Pi_{\mathbb{K},x}^{[\mathbb{L}:\mathbb{K}(x)]}$.*

Preuve. Soient $(u_1,\dots,u_{n/d})$ une base de $\mathbb{L}$ sur $\mathbb{K}(x)$, A la matrice compagnon de $\Pi_{\mathbb{K},x}$. D'après le théorème de la base téléscopique :

$$\left(u_1,xu_1,\dots,x^{d-1}u_1,u_2,\dots,x^{d-1}u_2,\dots,u_{n/d},\dots,x^{d-1}u_{n/d}\right)$$

est une base de $\mathbb{L}$ sur $\mathbb{K}$ dans laquelle la matrice de μ_x est :

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

On peut alors définir les applications *trace* et *norme* de l'extension $\mathbb{L}/\mathbb{K}$ notées respectivement $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ et $\mathrm{N}_{\mathbb{L}/\mathbb{K}}$ par :

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = \mathrm{Tr}\ \mu_x \qquad \text{et} \qquad \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) = \det \mu_x.$$

Ces deux applications sont définies sur $\mathbb{L}$, à valeurs dans $\mathbb{K}$; la première est $\mathbb{K}$-linéaire, la seconde multiplicative. Grâce au lemme précédent, on voit que

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = -\frac{n}{d} a_{d-1} \qquad \text{et} \qquad \mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) = (-1)^n {a_0}^{n/d}.$$

L'exercice ci-après établit la *transitivité* de la trace et de la norme.

Exercice 45. ④ *Soit $\mathbb{M}$ un corps, $\mathbb{K}$ et $\mathbb{L}$ deux sous-corps de $\mathbb{M}$ avec $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$. On suppose $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ finies séparables. Montrer, si $x \in \mathbb{M}$:*

$$N_{\mathbb{M}/\mathbb{K}}(x) = N_{\mathbb{L}/\mathbb{K}}\left(N_{\mathbb{M}/\mathbb{L}}(x)\right) \quad \text{et} \quad Tr_{\mathbb{M}/\mathbb{K}}(x) = Tr_{\mathbb{L}/\mathbb{K}}\left(Tr_{\mathbb{M}/\mathbb{L}}(x)\right).$$

Exercice 46. ④ *Soient q une puissance d'un nombre premier et n un élément de $\mathbb{N}^*$. Montrer que $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ induit un morphisme surjectif de $({\mathbb{F}_{q^n}}^*, \times)$ sur $({\mathbb{F}_q}^*, \times)$.*

7.2 Propriétés d'intégralité

La trace et la norme sont très utiles lors de l'étude des corps de nombres.

Proposition 6. *Si $\mathbb{K}$ est le corps des fractions de l'anneau intégralement clos $\mathbb{A}$, x un élément de entier sur $\mathbb{A}$, $Tr_{\mathbb{L}/\mathbb{K}}(x)$ et $N_{\mathbb{L}/\mathbb{K}}(x)$ appartiennent à $\mathbb{A}$.*

Preuve. Comme x est entier sur l'anneau intégralement clos $\mathbb{A}$, le polynôme $\Pi_{\mathbb{K},x}$ appartient à $\mathbb{A}[X]$. [13]

Proposition 7. *Sous les hypothèses de la proposition précédente, les assertions suivantes sont équivalentes :*

i) l'élément $1/x$ de $\mathbb{L}$ est entier sur $\mathbb{A}$,

ii) l'élément $N_{\mathbb{L}/\mathbb{K}}(x)$ est inversible dans $\mathbb{A}$,

iii) l'élement $1/x$ de $\mathbb{L}$ appartient à $\mathbb{A}[X]$.

En particulier, si $\mathcal{O}_{\mathbb{K}}$ est l'anneau des entiers du corps de nombres $\mathbb{K}$, un élément x de $\mathcal{O}_{\mathbb{K}}$ est un inversible de $\mathcal{O}_{\mathbb{K}}$ si et seulement si $N_{\mathbb{K}/\mathbb{Q}}(x) \in \{\pm 1\}$.

13. Si $\mathbb{A}$ est factoriel, le résultat se déduit aussitôt du « lemme de Gauss » sur les polynômes.

Preuve. La relation $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x^{-1}) = 1$ prouve *i) ⇒ ii).*

Pour *ii) ⇒ iii)*, on utilise encore l'appartenance de $\Pi_{\mathbb{K},x}$ à $\mathbb{A}[X]$ en notant que l'inversibilité dans $\mathbb{A}$ de $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)$implique celle du coefficient constant de $\Pi_{\mathbb{K},x}$. L'égalité $\Pi_{\mathbb{K},x}(x) = 0$ entraîne donc que x^{-1} est dans $\mathbb{A}[x]$.

Enfin *iii) ⇒ ii)* vient du fait que les éléments de $\mathbb{L}$ entiers sur $\mathbb{A}$ forment un sous-anneau de $\mathbb{L}$.

Exercice 47. ③ *Pour quels entiers $n \geq 2$ l'élément $(1 - e^{2i\pi/n})$ est-il un inversible de $\mathbb{Z}[e^{2i\pi/n}]$?*

7.3 Trace et norme dans une extension séparable

Si $\mathbb{L}/\mathbb{K}$ est séparable, trace et norme s'écrivent à l'aide des éléments de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$; précisément, on a le résultat suivant.

Proposition 8. *Si $\mathbb{L}/\mathbb{K}$ est séparable, on a :*

$$Tr_{\mathbb{L}/\mathbb{K}}(x) = \sum_{\sigma \in Hom_{\mathbb{K}}(\mathbb{L},\Omega)} \sigma(x) \qquad et \qquad N_{\mathbb{L}/\mathbb{K}}(x) = \prod_{\sigma \in Hom_{\mathbb{K}}(\mathbb{L},\Omega)} \sigma(x).$$

Preuve. Adoptons les notations du lemme 1 (paragraphe **1.1**). L'ensemble des $\mathbb{K}$-conjugués de x dans Ω a pour cardinal d. Si y est un de ces $\mathbb{K}$-conjugués, il y a exactement montre qu'il y a $\dfrac{n}{d}$ éléments de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$ envoyant x sur y. Comme la somme des $\mathbb{K}$-conjugués de x est $-a_{d-1}$, ceci prouve la première formule. La seconde s'établit de même.

À la trace est associée une forme bilinéaire symétrique sur le $\mathbb{K}$-espace $\mathbb{L}$:

$$(x, y) \in \mathbb{L}^2 \longmapsto \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(xy).$$

Elle jouera un rôle essentiel dans le paragraphe suivant.

Proposition 9. *Si $\mathbb{L}/\mathbb{K}$ est séparable, la forme trace n'est pas dégénérée.*

Preuve. Soit x dans le noyau de la forme trace. Alors, pour tout y de $\mathbb{L}$:

$$\sum_{\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\Omega)} \sigma(x)\sigma(y) = 0.$$

D'après le théorème d'indépendance des morphismes, ceci implique que les $\sigma(x)$ sont nuls, et $x = 0$.

Remarque *Noyau de la forme trace*

En fait, la forme trace est nulle ou non dégénérée. Soit en effet X son noyau. Si $x \in X \setminus \{0\}$ et $u \in \mathbb{L}$, la relation $uv = xx^{-1}uv$, valable pour $v \in L$, montre que u appartient à X. La proposition précédente équivaut donc à la non nullité de $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ pour une extension séparable $\mathbb{L}/\mathbb{K}$ - résultat par ailleurs immédiat si la caractéristique de $\mathbb{K}$ ne divise pas $[L : K]$ car $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(1) = [\mathbb{L} : \mathbb{K}]$.

Exercice 48. ③ *Soient $\mathbb{K}$ un corps de nombres de degré n sur $\mathbb{Q}$, $\sigma_1, \ldots, \sigma_n$ les éléments de $Hom_{\mathbb{Q}}(\mathbb{K}, \overline{\mathbb{Q}})$. Si x est dans $\mathcal{O}_{\mathbb{K}} \setminus \{0\}$, montrer :*

$$\sum_{i=1}^{n} |\sigma_i(x)|^2 \geq n.$$

Exercice 49. ③ *Un nombre algébrique x est dit totalement positif si tous ses $\mathbb{Q}$-conjugués sont dans $\mathbb{R}^+$. Montrer que, si x est un entier algébrique totalement positif de degré n sur $\mathbb{Q}$, alors $Tr_{\mathbb{Q}(x)/\mathbb{Q}}(x) \geq n$. Étudier le cas d'égalité.*

Exercice 50. ④ *Montrer que la forme trace d'une extension radicielle finie non triviale est nulle. En déduire les extensions finies dont la forme trace est non dégénérée.*

7.4 Caractérisation des binômes irréductibles

Nous allons utiliser la norme pour déterminer à quelle condition un binôme $X^n - a$ est irréductible ; le résultat ci-après, dû à Vahlen, Capelli et Redei. [14]

Théorème 6. *Si $n \in \mathbb{N}^*$, le polynôme $X^n - a$ est irréductible sur $\mathbb{K}$ si et seulement si :*

i) pour tout nombre premier p divisant n, a n'est pas puissance pième d'un élément de K,

ii) si 4 divise n, a n'est pas de la forme $-4b^4$ avec b dans K.

Rappelons d'abord le fait suivant, qui résulte de considérations simples sur la multiplicativité des degrés (chapitre **2**, paragraphe **3.1**, exemple 3).

Proposition 10. *Soient m et n deux éléments de $\mathbb{N}^*$ premiers entre eux, a dans $\mathbb{K}$. Alors $X^{mn} - a$ est irréductible sur $\mathbb{K}$ si et seulement si $X^m - a$ et $X^n - a$ sont irréductibles sur $\mathbb{K}$.*

Grâce à ce résultat, il suffit de démontrer le théorème 6 dans le cas où n est puissance d'un nombre premier. Ce travail est effectué dans les quatre lemmes ci-après, à partir de la proposition suivante, due à Abel et démontrée dans le chapitre 1 (proposition 1, **2.2**).

Proposition 11. *Soient p un nombre premier, a un élément de $\mathbb{K}$. Alors $X^p - a$ est irréductible sur $\mathbb{K}$ si et seulement s'il n'a pas de racine dans $\mathbb{K}$.*

Le lemme ci-après, qui utilise la norme, est le centre de la preuve.

Lemme 6. *Soient m et p dans $\mathbb{N}^*$ avec p premier, a dans $\mathbb{K}$. Supposons $X^m - a$ irréductible sur $\mathbb{K}$ et qu'il n'existe pas de b dans $\mathbb{K}$ tel que :*

$$a = (-1)^{m-1} b^p.$$

Alors $X^{mp} - a$ est irréductible sur $\mathbb{K}$.

14. Vahlen (1895) a établi le résultat pour $\mathbb{K} = \mathbb{Q}$; Capelli (1897) l'a étendu au cas où $\mathbb{K}$ est de caractéristique nulle et Redei (1957) a traité le cas général.

Preuve. Soient α une racine de $X^m - a$ dans Ω, β une racine p-ième de α dans Ω. Alors

$$[\mathbb{K}(\alpha) : \mathbb{K}] = m.$$

Comme β annule $X^{mp} - a$, il suffit pour conclure de montrer que

$$[\mathbb{K}(\beta) : \mathbb{K}(\alpha] = p,$$

ou encore que $X^p - \alpha$ est irréductible sur $\mathbb{K}(\alpha)$, ou encore, grâce à la proposition 11, que α n'a pas de racine p-ième dans $\mathbb{K}(\alpha)$ Dans le cas contraire, on disposerait de γ dans $\mathbb{K}(\alpha)$ tel que $\alpha = \gamma^p$. Mais alors, en notant N est la norme de l'extension $\mathbb{K}(\alpha)/\mathbb{K}$, on aurait :

$$N(\gamma)^p = N(\gamma^p) = N(\alpha) = (-1)^{m-1}a.$$

Lemme 7. *Soient p un nombre premier impair, r un élément de $\mathbb{N}^*$, a un élément de $\mathbb{K}$ qui n'est pas puissance p-ième d'un élément de $\mathbb{K}$. Alors $X^{p^r} - a$ est irréductible sur $\mathbb{K}$.*

Ce résultat subsiste si $p = 2$ et $\mathbb{K}$ est de caractéristique 2.

Preuve. Le résultat se démontre par une récurrence immédiate à partir du lemme précédent, l'initialisation venant de la proposition 11.

À ce stade, le théorème 6 est démontré pour n impair dans le cas général et sans restriction sur n si $\mathbb{K}$ est de caractéristique 2. Pour compléter la démonstration, deux nouveaux lemmes sont nécessaires.

Lemme 8. *Supposons $\mathbb{K}$ de caractéristique différente de 2. Soit a un élément de $\mathbb{K}$. Alors $X^4 - a$ est réductible sur $\mathbb{K}$ si et seulement si soit a est le carré d'un élément de $\mathbb{K}$, soit a est de la forme $-4b^4$ avec b dans $\mathbb{K}$.*

Preuve. Supposons $X^4 - a$ réductible sur $\mathbb{K}$ et a non carré dans $\mathbb{K}$. Alors il existe $(r, s, t, u) \in \mathbb{K}^4$ tel que :

$$X^4 - a = (X^2 + rX + s)(X^2 + tX + u),$$

d'où :

$$r + t = 0, \quad s + u + rt = 0, \quad ru + st = 0, \quad su = -a.$$

Si $r = 0$, alors $t = 0$ et $a = u^2$, contradiction. Sinon, $u = s = -\dfrac{r^2}{2}$ et $a = -\dfrac{r^4}{4}$. Ceci établit la nécessité de l'implication. La réciproque se fait en remontant les calculs.

Lemme 9. *Soit a un élément de $\mathbb{K}$. Supposons $X^4 - a$ est irréductible sur $\mathbb{K}$. A,lors pour tout $r \geq 2$, $X^{2^r} - a$ est irréductible sur $\mathbb{K}$.*

Preuve. On raisonne par récurrence en supposant la propriété démontrée à l'ordre $r \geq 2$ pour tout corps de caractéristique différente de 2.

Soient a un élément de $\mathbb{K}$ tel que $X^4 - a$ soit irréductible sur $\mathbb{K}$, α dans Ω tel que $\alpha^{2^{r+1}} = a$. Supposons par l'absurde $X^{2^{r+1}} - a$ réductible sur $\mathbb{K}$. Le lemme 6 donne b dans $\mathbb{K}$ tel que $-a = b^2$. Puisque a n'est pas un carré dans $\mathbb{K}$, -1 non

plus. Soit i dans Ω tel que $i^2 = -1$. Il suffit pour conclure de prouver que α est de degré 2^r sur $\mathbb{K}(i)$, ce qui amènera

$$[\mathbb{K}(i,\alpha) : \mathbb{K}] = [\mathbb{K}(i,\alpha) : \mathbb{K}(i)]\,[\mathbb{K}(i) : \mathbb{K}] = 2^r \times 2 = 2^{r+1},$$

d'où l'irréductibilité de $X^{2^{r+1}} - a$ sur $\mathbb{K}$ et la contradiction désirée.

Or, $\alpha^{2^r} = \varepsilon ib$ où $\varepsilon \in \{-1, 1\}$. Reste donc à voir que $X^{2^r} - \varepsilon ib$ est irréductible sur $\mathbb{K}(i)$. Dans le cas contraire, l'hypothèse de récurrence et le lemme 6 impliqueraient qu'il existe $c \in \mathbb{K}(i)$ tel que $\varepsilon ib = -c^2 = (ic)^2$. D'où la contradiction désirée en écrivant

$$\varepsilon ib = (x+iy)^2 \quad \text{avec} \quad (x,y) \in \mathbb{K}^2, \qquad b \in \left\{2x^2, -2x^2\right\}, \qquad a = -4x^4.$$

Exercice 51. ③ *Montrer que, si $n \in \mathbb{N}^*$ et $a \in \mathbb{K}$, alors $X^n - a$ admet au moins un diviseur irréductible ayant au plus trois coefficients non nuls.*

7.5 Structure additive d'un anneau d'entiers

Dans ce paragraphe, $\mathbb{K}$ est un corps de nombres. On note $\mathcal{O}_{\mathbb{K}}$ l'anneau des entiers de $\mathbb{K}$, c'est-à-dire l'ensemble des entiers algébriques qui appartiennent à $\mathbb{K}$, introduit à la fin du paragraphe **6.1** du chapitre **2**. Nous allons élucider la structure du groupe $(\mathcal{O}_{\mathbb{K}}, +)$.

Rappelons le résultat très simple suivant (chapitre **2**, **6.1**, lemme 8).

Lemme 10. *Soit $x \in \overline{\mathbb{Q}}$. Il existe $q \in \mathbb{N}^*$ tel que $qx \in \overline{\mathbb{Z}}$.*

Il découle de ce lemme que, si $\mathbb{K}$ est un corps de nombres, le $\mathbb{Q}$-espace $\mathbb{K}$ admet une base constituée d'éléments de $\mathcal{O}_{\mathbb{K}}$. Nous utilisons une telle base dans la démonstration du théorème suivant, explicité par Dedekind mais sans doute connu depuis Dirichlet.

Théorème 7. *Soient $\mathbb{K}$ un corps de nombres, $n = [\mathbb{K} : \mathbb{Q}]$, $x_1, \ldots, x_n$ une $\mathbb{Q}$-base de $\mathbb{K}$ formée d'éléments de $\mathcal{O}_K$. Notons Tr la forme trace de l'extension $\mathbb{K}/\mathbb{Q}$, D le déterminant de la matrice*

$$\left(Tr(x_i x_j)\right)_{1 \le i,j \le n}.$$

Alors :

$$\bigoplus_{i=1}^{n} \mathbb{Z}x_i \subset \mathcal{O}_K \subset \bigoplus_{i=1}^{n} \frac{\mathbb{Z}x_i}{D}.$$

Le groupe $(\mathcal{O}_K, +)$ est un g.a.l.t.f de rang n.

Preuve. Commençons par observer que, puisque la forme Tr est non dégénérée, D n'est pas nul. [15]

15. On dit que D est le discriminant de la forme Tr dans la base $(x_1, \ldots, x_n)$ de $\mathbb{K}$. Le discriminant (que l'on peut relier au discriminant d'un polynôme introduit dans le chapitre **1**) est un outil important en théorie algébrique des nombres.

Un résultat classique relatif aux g.a.l.t.f. montre qu'il suffit d'établir les deux inclusions pour obtenir que $(\mathcal{O}_{\mathbb{K}}, +)$ est un g.a.l.t.f de rang n. La première inclusion est immédiate. Prouvons la seconde. Soient $x \in \mathcal{O}_{\mathbb{K}}$, $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Q}^n$ tel que :

$$x = \sum_{i=1}^{n} \lambda_i x_i,$$

. Les n équations :

$$\mathrm{Tr}\,(x_j x) = \sum_{i=1}^{n} \lambda_i \mathrm{Tr}\,(x_j x_i)$$

forment un système d'inconnue $(\lambda_1, \ldots, \lambda_n)$. D'autre part, les $\mathrm{Tr}(x_j x)$ appartiennent à $\mathbb{Z}$ (proposition 6, **7.2**). Les formules de Cramer montrent que les λ_i sont dans $\mathbb{Z}/D$, d'où le résultat désiré.

Remarques

1. *Effectivité*
   L'ensemble des sous-groupes de $(\mathbb{K}, +)$ vérifiant la double inclusion du théorème est équipotent à l'ensemble des sous-groupes de $((\mathbb{Z}/D\mathbb{Z})^n, +)$, donc fini. De façon équivalente, il suffit pour déterminer $\mathcal{O}_{\mathbb{K}}$ de trouver ceux des D^n éléments :

   $$\sum_{i=1}^{n} \lambda_i x_i \quad \text{avec} \quad (\lambda_1, \ldots, \lambda_n) \in \{0, \ldots, D-1\}^n$$

   qui sont des entiers algébriques.

2. *Une variante*
   Voici une variante de la preuve précédente. En conservant les mêmes notations, on a, si $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{K}, \overline{\mathbb{Q}})$,

   $$\sigma(x) = \sum_{i=1}^{n} \lambda_i \sigma(x_i).$$

   Notant $\sigma_1, \ldots, \sigma_n$ les éléments de $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{K}, \overline{\mathbb{Q}})$ on obtient en écrivant l'égalité précédente pour $\sigma = \sigma_i$, $1 \leq i \leq n$ un système de n équations à n inconnues. Les formules de Cramer montrent que chaque λ_i est de la forme $\dfrac{u_i}{\delta}$ où u_i est un entier algébrique et δ un entier algébrique de carré D. En particulier λ_i s'écrit

   $$\frac{v_i}{D}, \quad v_i \in \overline{\mathbb{Z}}.$$

   Comme λ_i est rationnel, $v_i = D\lambda_i$ appartient à $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$.

7.6 Entiers d'un corps cyclotomique

Malgré la remarque 1 du paragraphe précédent, il peut être assez difficile de calculer un anneau d'entiers. Nous allons traiter l'exemple classique ci-après.

Théorème 8. *Soit p un nombre premier. Si $\mathbb{K} = \mathbb{Q}\left(\exp(\frac{2i\pi}{p})\right)$, alors*

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\exp\left(\frac{2i\pi}{p}\right)\right].$$

Preuve. Posons $\varepsilon = \exp\left(\frac{2i\pi}{p}\right)$. Puisque $\mathcal{O}_{\mathbb{K}}$ est un sous-anneau de $\mathbb{K}$, on a

$$\mathbb{Z}[\varepsilon] \subset \mathcal{O}_{\mathbb{K}}.$$

Il s'agit d'établir que cette inclusion est une égalité. Soit x dans $\mathcal{O}_{\mathbb{K}}$. On écrit

$$x = \sum_{j=0}^{p-2} \lambda_j \varepsilon^j \quad \text{où} \quad (\lambda_0, \ldots, \lambda_{p-2}) \in \mathbb{Q}^{p-1}.$$

On note Tr (resp. N) la forme trace (resp. norme) de l'extension $\mathbb{K}/\mathbb{Q}$. Les ε^j pour $1 \leq j \leq p-2$ sont $\mathbb{Q}$-conjugués, de polynôme minimal Φ_p. Il s'ensuit que

$$\forall j \in \{1, \ldots, p-2\}, \qquad \text{Tr } (\varepsilon^j) = -1.$$

La trace de 1 est le degré $p-1$ de l'extension $\mathbb{K}/\mathbb{Q}$.

Pour j dans $\mathbb{Z}$, chaque $\mathbb{Q}$-conjugué de $1-\varepsilon^j$ est divisible par $(1-\varepsilon)$ dans $\mathcal{O}_{\mathbb{K}}$, le lemme 11 ci-après assure, pour tout j de $\mathbb{Z}$:

$$\text{Tr } ((1-\varepsilon^j)x) \in p\mathbb{Z}.$$

Mais

$$\text{Tr } ((1-\varepsilon)x) = p\lambda_0,$$

d'où $\lambda_0 \in \mathbb{Z}$. De plus, si $1 \leq i \leq p-2$:

$$\text{Tr } ((1-\varepsilon^{-i})x) = \text{Tr } (x) - \text{Tr } (\varepsilon^{-i}x) = p(\lambda_0 - \lambda_i),$$

d'où la relation suivante, qui permet de conclure :

$$\lambda_i - \lambda_0 \in \mathbb{Z}.$$

Lemme 11. *On a*

$$((1-\varepsilon)\mathcal{O}_{\mathbb{K}}) \cap \mathbb{Z} = p\mathbb{Z}.$$

Preuve. On part de l'égalité :

$$N(1-\varepsilon) = \prod_{j=1}^{p-2}(1-\varepsilon^j) = \Phi_p(1) = p.$$

Cette formule entraîne d'abord que

$$p\mathbb{Z} \subset ((1-\varepsilon)\mathcal{O}_{\mathbb{K}}) \cap \mathbb{Z}.$$

Elle montre aussi que $1-\varepsilon$ n'est pas un inversible de $\mathcal{O}_{\mathbb{K}}$. Ainsi,

$$((1-\varepsilon)\mathcal{O}_{\mathbb{K}}) \cap \mathbb{Z}$$

est un idéal de $\mathbb{Z}$ distinct de $\mathbb{Z}$ et contenant $p\mathbb{Z}$, d'où le résultat.

Exercice 52. ③ *Identifier le quotient $\mathcal{O}_{\mathbb{K}}/(1-\varepsilon)$.*

Le théorème 8 subsiste si on remplace p par un entier $n \geq 2$ quelconque, au prix d'une démonstration un peu plus compliquée.