Chapitre 3

Morphismes et conjugaison

Sommaire

Présentation du chapitre

Dans tout ce chapitre, $\mathbb{K}$ est un corps et Ω une clôture algébrique de $\mathbb{K}$. Par commodité, les corps considérés seront souvent supposés contenus dans Ω. Cette hypothèse ne nuit en rien à la généralité (section **4**, remarque finale).

Le chapitre **1** est centré sur ces 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-Noether-Artin.

Ce court chapitre traite essentiellement de trois points : conjugaison sur un corps $\mathbb{K}$ (**1**), prolongement des morphismes (**2** et **4**), indépendance linéaire de morphismes (**5**). Un point important est la caractérisation de l'appartenance au corps de base (rationalité) en termes de morphismes, qui remplace souvent dans les exposés « modernes » les arguments à base de polynômes symétriques.

La section **3** 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. Elle n'est pas utile pour la théorie de Galois en caractéristique nulle. Il en est de même de la version générale du théorème de prolongement donnée en **4**. Les sections **6** et **7** sont, quant à elles, très éloignées de notre sujet principal ; on y développe les techniques linéaires du chapitre **2**, puis on les applique aux anneaux d'entiers des corps de nombres.

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, 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 $\mathbb{K}$, $\mathrm{Hom}(\mathbb{K},\mathbb{L})$ est réduit à un seul élément, l'inclusion de $\mathbb{K}$ dans $\mathbb{L}$. 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 en l'indéterminée Y :

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

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 $\sigma(\mathbb{K})$.

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

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

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 $\deg(\Pi_{\mathbb{K},x}) = [\mathbb{K}(x) : \mathbb{K}]$, 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 :

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

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 $\mathbb{M}$?*

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.

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 $n \in \mathbb{N}^*$. Comme le polynôme cyclotomique Φ_n est irréductible sur $\mathbb{Q}$, les $\mathbb{Q}$-conjugués de $\exp\left(\frac{2i\pi}{n}\right)$ sont les racines de Φ_n, i.e. les $\exp\left(\frac{2ik\pi}{n}\right)$ avec $k \in \{1, \ldots, n\}$ 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
   $$\sigma \circ \psi_x = \psi_y.$$
5. *Unicité du corps de rupture*
   La proposition 1 entraîne 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]

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

3. L'axiome du choix permet de démontrer que l'ensemble des automorphismes de l'anneau $\mathbb{C}$ a la puissance du continu (**4**, dernier exercice). Mais les deux morphismes précédents sont les seuls « explicitables ».

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* $x \in \Omega$ *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 $\mathbb{A} \subset \overline{\mathbb{Z}}$.

Exercice 10. ④ *a) Soit* $x \in \mathbb{R}$ *valeur propre d'une matrice symétrique à coefficients rationnels. Montrer que* x *est totalement réel, i.e. que* $x \in \overline{\mathbb{Q}}$ *et que tous les* $\mathbb{Q}$*-conjugués de* x *sont réels.*

b) Exhiber une matrice symétrique de $\mathcal{M}_2(\mathbb{Q})$ *admettant* $\sqrt{2}$ *comme valeur propre.*

c) Montrer qu'il n'existe pas de matrice symétrique de $\mathcal{M}_2(\mathbb{Q})$ *dont* $\sqrt{3}$ *soit valeur propre.*

d) Si $n \in \mathbb{N}^*$, *exhiber une matrice symétrique de* $\mathcal{M}_n(\mathbb{Q})$ *dont les valeurs propres soient les* $2\cos\left(\dfrac{2k\pi}{n}\right)$, *avec* $0 \leq k \leq n-1$. *En déduire une matrice de* $\mathcal{M}_3(\mathbb{Q})$ *dont* $\sqrt{3}$ *soit valeur propre.* [5]

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

Exercice 11. ③ *Soient* $n \in \mathbb{N}^*$, $(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \Omega^{2n}$. *Montrer qu'il existe un élément de* $Hom_{\mathbb{K}}(\mathbb{K}(x_1, \ldots, x_n), \Omega)$ *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 12. ④ *Soient* $x \in \Omega$, $\mathbb{L} = \mathbb{K}[x] = K(x)$. *À quelle condition existe-t-il un morphisme de* $\mathbb{K}$*-algèbres de* $\mathbb{L}$ *dans* $\mathcal{M}_n(\mathbb{K})$ *?*

Exercice 13. ④ *a) Déterminer les endomorphismes de la* $\mathbb{K}$*-algèbre* $\mathbb{K}(X)$. *Identifier parmi eux les automorphismes.*

b) Vérifier que l'application :

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

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

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 $\mathbb{L}$.

5. On peut démontrer que la réciproque de a) est vraie (Bender, 1968). On trouvera la démonstration dans l'exercice 61 de **6.3**.

Exercice 14. ③ *On appelle nombre de Pisot tout élément de* $\overline{\mathbb{Z}} \cap]1, +\infty[$ *dont les* $\mathbb{Q}$*-conjugués autre que lui-même sont de module strictement inférieur à* 1.

a) Montrer que $1 + \sqrt{3}$ *et le nombre d'or sont des nombres de Pisot.*

b) Soit $n \geq 2$ *un entier. Montrer que* $X^n - \sum_{k=0}^{n-1} X^k$ *admet une unique racine dans* $\mathbb{R}^+$*, qui est un nombre de Pisot.*

Exercice 15. ④ *On appelle nombre de Salem tout tout élément de* $\overline{\mathbb{Z}} \cap]1, +\infty[$ *irrationnel dont les* $\mathbb{Q}$*-conjugués autre que lui-même sont de module inférieur ou égal à* 1 *et qui admet au moins un* $\mathbb{Q}$*-conjugué de module* 1.

a) Soit x *est un nombre de Salem. Montrer que* $\Pi_{\mathbb{Q},x}$ *est un polynôme réciproque à coefficients entiers dont toutes les racines autres que* x *et* $1/x$ *sont de module* 1.

b) Soit x *un nombre de Salem. Montrer que le degré de* x *sur* $\mathbb{Q}$ *est un entier pair supérieur ou égal à* 4.

c) Déterminer un nombre de Salem de degré 4 *sur* $\mathbb{Q}$.

Exercice 16. ④ *Soit* $x \in \overline{\mathbb{Z}}$*. On suppose que les* $\mathbb{Q}$*-conjugués de* x *(dans* $\mathbb{C}$*) sont de module majoré par* 1*. On note* $x_1 = x, \ldots, x_n$ *ces conjugués. En observant que, pour tout* $k \in \mathbb{N}^*$*,* ${x_1}^k, \ldots, {x_n}^k$ *sont* $\mathbb{Q}$*-conjugués, montrer que* x *est nul ou racine de l'unité.* [6]

Exercice 17. ④ *Déterminer les éléments de* $\overline{\mathbb{Z}}$ *dont tous les* $\mathbb{Q}$*-conjugués appartiennent à* $[-2, 2]$.

Exercice 18. ④ *Indiquer un élément de* $\overline{\mathbb{Z}}$ *de module* 1 *qui n'est pas une racine de l'unité.*

Une grande partie de la suite de ce chapitre consiste en des variations sur la proposition 1.

2 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 **2.1**.

Dans les paragraphes **2.3** et **2.4**, on se limite à la caractéristique nulle, de manière à éviter les problèmes de séparabilité. La section **3** reprend les mêmes questions dans le cas général.

2.1 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* $\mathbb{K}'$*,* $x \in \mathbb{L}$ *algébrique sur* $\mathbb{K}$ *et* x' *un élément de* $\mathbb{L}'$*. Les deux assertions suivantes sont équivalentes.*

(i) Il existe $\sigma' \in Hom(\mathbb{K}(x), \mathbb{L}')$ *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* $\mathbb{K}'(x')$.

6. Théorème dû à Kronecker, 1857.

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 **4** que la proposition 2 se généralise à une extension algébrique quelconque, non nécessairement finie.

Exercice 19. ③ *Soient $P \in \mathbb{K}[X]$, 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 (chapitre **2**, paragraphe **2.1**, remarque 1 après la proposition 5).

2. *Conjugués d'un nombre complexe constructible*
   Rappelons (chapitre 2, section **4**) 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 20. 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 21. 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.*

2.2 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**, **3.1**, 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.

2.3 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 $Hom(\mathbb{L}, \Omega)$.* [7]

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*

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

2.4 Caractérisation du corps de base (caractéristique nulle)

On déduit du corollaire 1 un critère d'appartenance au corps de base. [8]

Corollaire 5. *Supposons $\mathbb{K}$ de caractéristique nulle. Soit $\mathbb{L}/\mathbb{K}$ une extension finie. Alors, pour x dans $\mathbb{L}$, on a* [9]

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

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 que 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 » (remarque 1, **2.1**). 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 $\mathcal{M}_n(\mathbb{L})$ et commutent ; elles sont respectivement semi-simple et nilpotente. L'unicité de la décomposition entraîne que $\sigma.D = D$ et $\sigma.N = N$, le corollaire 5 permet de conclure.

7. Ce résultat et sa démonstration s'étendent aux corps parfaits. Il en est de même du corollaire 4.
8. Généralisation de la caractérisation des nombres réels comme points fixes de la conjugaison complexe.
9. 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 $r \in \mathbb{N}^*$, $x_1, \ldots, x_r$ des éléments de $\mathbb{R}^{+*} \cap \overline{\mathbb{Q}}$. On suppose que, pour tout $i \in \{1, \ldots, r\}$, tous les $\mathbb{Q}$-conjugués de x_i sont de module majoré par x_i. 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 $(a_1, \ldots, a_r) \in \mathbb{Q}^{+*r}$, $(n_1, \ldots, n_r) \in \mathbb{N}^{*r}$, $\displaystyle\sum_{i=1}^{r} \sqrt[n_i]{a_i}$ n'est rationnel que s'il en est de même de tous les $\sqrt[n_i]{a_i}$.

Exercice 22. ③ *Soit P un 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 $\sigma \in Hom_{\mathbb{Q}}(\mathbb{Q}(z, \overline{z}), \mathbb{C})$ tel que $\sigma(x) \notin \mathbb{R}$. En déduire que x n'est pas rationnel.*

3 (*) Séparabilité (III)

Nous revenons sur les résultats de la section **2**, avec les objectifs suivants :

- examiner ce qui se passe en caractéristique p ;
- établir les résultats sans utiliser le théorème de l'élément primitif (chapitre **2**, **2.3**, note 11) ;
- donner une nouvelle démonstration de ce dernier théorème. [10]

3.1 Séparabilité et morphismes

Soient $\mathbb{L}$ une extension de $\mathbb{K}$, $x \in \mathbb{L}$ 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

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

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

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

10. Comme d'habitude, le lecteur intéressé uniquement par la caractéristique nulle peut omettre cette section. Option intermédiaire : lire la preuve du théorème 2 et le paragraphe **3.2** en se plaçant en caractéristique nulle.

Proposition 4. *Soient $\mathbb{L}$ une extension de $\mathbb{K}$, $x \in \mathbb{L}$ 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, $\sigma \in Hom(\mathbb{K}, \Omega)$. 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, a fortiori, 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 $x_1 \in \mathbb{L} \setminus \mathbb{K}$ non séparable sur $\mathbb{K}$. Si $i \in \{1, \ldots, n\}$, 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 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 $i \in \{1, \ldots, n\}$, l'ensemble des prolongements de σ en un élément de $\mathrm{Hom}(\mathbb{K}(x_1, \ldots, x_i), \Omega)$ est fini de cardinal 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. Cas particulier du théorème précédent, en prenant pour σ 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 23. ④ *a) Généraliser le résultat de* **2.4** *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 $n \in \mathbb{N}^*$, $(x_1, \ldots, x_n) \in \Omega^n$. 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 [11].

Exercice 24. 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 obtient également 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 l'égalité

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

Exercice 25. ③ *Montrer que, si les extensions $\mathbb{M}/\mathbb{L}$ et $\mathbb{L}/\mathbb{K}$ sont séparables, il en est de même de $\mathbb{M}/\mathbb{K}$.*

Exercice 26. 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 27. 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 28. ④ *Soient $x\in\Omega$, $r=\max\left\{i\in\mathbb{N},\ \Pi_{\mathbb{K},x}\in\mathbb{K}[X^{p^i}]\right\}$.*

a) Montrer que le nombre de $\mathbb{K}$-conjugués distincts de x dans Ω est $d=\dfrac{[\mathbb{K}(x):\mathbb{K}]}{p^r}$. 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) Déduire de b) 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 $x\in\Omega$ radiciel sur $\mathbb{K}$. Décrire les sous-corps de $\mathbb{K}(x)$ contenant $\mathbb{K}$. Quel est leur nombre ?

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

Exercice 29. 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 30. 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 31. ⑤ *Soient $p \in \mathcal{P}$, $\mathbb{F}$ un corps de caractéristique p, $\mathbb{K} = \mathbb{F}(X^p, Y^p)$, $\mathbb{L} = \mathbb{F}(X, Y)$, 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 que $\mathbb{M} = \mathbb{K}(u^p)$.

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

3.2 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 $x \in \mathbb{L}$, 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 **2.2**. 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 32. 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 une partie cofinie de $\mathbb{K}$.*

Exercice 33. 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, dans la démonstration du théorème de Steinitz donnée dans le chapitre **2** (**3.2**), seule la première partie est véritablement utile. On se borne à l'établir en caractéristique nulle, mais l'énoncé est vrai en toute généralité.

Exercice 34. 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 $x \in \Omega$, on pourra considérer un élément primitif de $D_{\mathbb{K}}\Pi_{\mathbb{K},x}$ sur $\mathbb{K}$.*

Si $P \in \mathbb{K}[X]$ est irréductible de degré n, 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 35. ⑤ *On suppose $\mathbb{K}$ de caractéristique p, avec $p \in \mathcal{P}$. Soit $\mathbb{L}$ un sous-corps de Ω contenant $\mathbb{K}$ et de degré n sur $\mathbb{K}$.*

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

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

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

Conclure.

4 (*) Prolongement d'un morphisme à une extension algébrique

Nous allons, en suivant Steinitz, généraliser la proposition 2 de **2.1** 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 ». [12]

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.*

12. 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.

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 :

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

Le caractère inductif de l'ensemble ordonné $(\mathcal{E}, \leq)$ s'obtient 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 $\mathbb{M} = \bigcup_{i \in I} \mathbb{M}_i$ et du morphisme θ de $\mathbb{M}$ dans Ω 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 36. ② *Retrouver à l'aide de la remarque 1 qu'une extension finie de $\mathbb{R}$ est isomorphe à $\mathbb{R}$ ou $\mathbb{C}$ (chapitre* **2**, **2**, *remarque 2).*

Exercice 37. ① *Vérifier que deux corps de nombres isomorphes ont même signature.*

Exercice 38. ③ *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 39. ② *Soient $\mathbb{K}$ et $\mathbb{K}'$ deux corps de nombres tels que $\mathbb{K} \subset \mathbb{K}'$, (r_1, r_2) et (r_1', r_2') leurs signatures respectives. Comparer r_2 et r_2'.*

Exercice 40. ③ *Soient $p \in \mathcal{P}$, $\mathbb{K}$ un corps de caractéristique p, $\sigma \in Hom(\mathbb{K}, \Omega)$, $\mathbb{L}$ une extension radicielle de $\mathbb{K}$. Montrer que σ admet un unique prolongement en un morphisme de $\mathbb{L}$ dans Ω.*

Exercice 41. 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 42. 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 43. 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. Dans le chapitre **4**, nous le reformulerons de façon définitive en termes de groupe de Galois.

Corollaire 11. *Soit $x \in \Omega$. 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 44. 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 45. ③ *Montrer que le corollaire 7 s'étend aux extensions séparables infinies.*

Exercice 46. 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 47. 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 » [13].

Exercice 48. 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 $\mathbb{R}$.*

13. 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.

5 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 indépendant des paragraphes précédents.

Théorème 5. *Soient Γ un monoïde, $\mathbb{K}$ un corps, $\sigma_1, \ldots, \sigma_n$ 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 $\sigma_1, \ldots, \sigma_n$. 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 $\sigma_2, \ldots, \sigma_p$, ce qui contredit la minimalité de (1).

Ce résultat permet de retrouver le corollaire 6 de **3.1**. 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 49. 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 50. 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. [14]

Exercice 51. ⑤ *On suppose $\mathbb{K}$ de caractéristique nulle. Soit n dans $\mathbb{N}^*$.*

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

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

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

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.

6 (*) Appendice : trace, norme, discriminant

On poursuit ici la linéarisation de la théorie des corps, en étudiant la trace et le déterminant de la multiplication par un élément donné d'une extension finie.

Dans cette section, $\mathbb{L}$ est une extension finie de $\mathbb{K}$ contenue dans Ω.

6.1 L'endomorphisme de multiplication par x

Si $x \in \mathbb{L}$, l'application

$$\begin{array}{rccc} \mu_x \ : & \mathbb{L} & \longrightarrow & \mathbb{L} \\ & y & \longmapsto & xy \end{array}$$

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

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

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

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

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

Exercice 52. ④ *Soit $\mathbb{M}$ un sous-corps de Ω extension finie de $\mathbb{L}$. On suppose que les extensions $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ sont séparables.*

a) Soit $\mathbb{M}'$ un sous-corps de Ω contenant les images de tous les éléments de $Hom_{\mathbb{K}}(\mathbb{M},\Omega)$. Pour $\sigma \in Hom_{\mathbb{K}}(\mathbb{M},\Omega)$, on choisit $\sigma' \in Hom_{\mathbb{K}}(\mathbb{M}',\Omega)$ prolongeant σ. Montrer que tout élément de $Hom_{\mathbb{K}}(\mathbb{M},\Omega)$ s'écrit de façon unique $\sigma' \circ \tau$ avec τ dans $Hom_{\mathbb{L}}(\mathbb{M},\Omega)$ et σ dans $Hom_{\mathbb{L}}(\mathbb{M},\Omega)$.

b) Montrer que, si $x \in \mathbb{M}$:

$$N_{\mathbb{M}/\mathbb{K}}(x) = N_{\mathbb{L}/\mathbb{K}}\left(N_{\mathbb{M}/\mathbb{L}}(x)\right) \quad et \quad \mathrm{tr}_{\mathbb{M}/\mathbb{K}}(x) = \mathrm{tr}_{\mathbb{L}/\mathbb{K}}\left(\mathrm{tr}_{\mathbb{M}/\mathbb{L}}(x)\right).$$

Exercice 53. ④ *Soient q une puissance d'un nombre premier et $n \in \mathbb{N}^*$. Montrer que $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ induit un morphisme surjectif de $({\mathbb{F}_{q^n}}^*, \times)$ sur $({\mathbb{F}_q}^*, \times)$.*

6.2 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 $\mathbb{A}$, si $x \in \mathbb{L}$ est entier sur $\mathbb{A}$, $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(x)$ 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 $\mathbb{A}[X]$ (lemme 18, **5.3**, chapitre **2**).

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

(i) l'élément x^{-1} 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 x^{-1} de $\mathbb{L}$ appartient à $\mathbb{A}[x]$.

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)* provient du fait que les éléments de $\mathbb{L}$ entiers sur $\mathbb{A}$ forment un sous-anneau de $\mathbb{L}$.

Exercice 54. ③ *Soient $d \in \mathbb{Z} \setminus \{0,1\}$ sans facteur carré, $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. Quels sont les inversibles de $\mathbb{Z}_{\mathbb{K}}$ (anneau déterminé dans le chapitre **2**, **5.1**, proposition 13) ?*

Exercice 55. ③ *Pour quels entiers $n \geq 2$ l'élément $(1 - e^{2i\pi/n})$ est-il un inversible de $\mathbb{Z}[e^{2i\pi/n}]$?*

Exercice 56. ③ *Soient $\mathbb{K}$ un corps de nombres de degré n sur $\mathbb{Q}$, $\sigma_1, \ldots, \sigma_n$ les éléments de $Hom_{\mathbb{Q}}(\mathbb{K}, \overline{\mathbb{Q}})$, $x \in \mathcal{O}_{\mathbb{K}} \setminus \{0\}$. Montrer que $\sum_{i=1}^{n} |\sigma_i(x)|^2 \geq n$.*

Exercice 57. ③ *Soit $x \in \overline{\mathbb{Z}}$. Montrer que x est inversible dans $\overline{\mathbb{Z}}$ si et seulement s'il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(0) \in \{-1, 1\}$ annulant x.*

Exercice 58. ③ *Si $x \in \overline{\mathbb{Q}}$, x est dit totalement positif si tous ses $\mathbb{Q}$-conjugués sont dans $\mathbb{R}^+$. Montrer que, si $x \in \overline{\mathbb{Z}}$ est totalement positif de degré d sur $\mathbb{Q}$, alors $\mathrm{tr}_{\mathbb{Q}(x)/\mathbb{Q}}(x) \geq d$. Étudier le cas d'égalité.*

Exercice 59. ③ *Soient $x \in \overline{\mathbb{Z}}$, d_x le degré de x sur $\mathbb{Q}$, $x_1 = x, \ldots, x_d$ les $\mathbb{Q}$-conjugués de x. On note* $\mathrm{tr} = \mathrm{tr}_{\mathbb{Q}(x)/\mathbb{Q}}$.

a) Soit $P \in \mathbb{Z}[X]$ n'annulant pas x. Montrer que $\displaystyle\prod_{i=1}^{n} |P(x_i)| \geq 1$.

b) On suppose que x est totalement dans $\mathbb{R}^+$, i.e. que les $\mathbb{Q}$-conjugués de x sont dans $\mathbb{R}^+$. Soient $m \in \mathbb{N}^*$, $P_1, \ldots, P_m$ des éléments de $\mathbb{Z}[X]$ n'annulant pas x, $(c_j)_{1 \leq j \leq m}$ une famille d'éléments de $\mathbb{R}^{+*}$, g la fonction $x \longmapsto x - \displaystyle\sum_{j=1}^{m} c_j \ln(|P_j(x)|)$. Montrer que $\mathrm{tr}(x) \geq d_x \ \min g$. [15]

Exercice 60. ③ *Si $n \in \mathbb{N}^*$, montrer, en considérant les $4\cos^2\left(\dfrac{\pi}{n}\right)$ pour $n \in \mathbb{N}^*$, que l'ensemble des entiers algébriques x totalement dans $\mathbb{R}^+$ et tels que $\mathrm{tr}(x) < 2\, d_x$ est infini.* [16]

6.3 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 :*

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

Preuve. 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 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 $u \in X$. La proposition précédente équivaut donc à la non nullité de $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}$ pour une extension séparable $\mathbb{L}/\mathbb{K}$. Ce dernier résultat est par ailleurs immédiat si la caractéristique de $\mathbb{K}$ ne divise pas $[\mathbb{L} : \mathbb{K}]$ car $\mathrm{tr}_{\mathbb{L}/\mathbb{K}}(1) = [\mathbb{L} : \mathbb{K}]$.

15. Par des choix judicieux des P_j et des c_j, on montre que, si on exclut un ensemble fini de x, $\mathrm{tr}(x) \geq 1,7719\ d_x$ (Smyth, 1984).

16. On comparera à l'exercice précédent. L'optimalité de 2 est un problème ouvert en 2022 (« problème de Schur-Siegel-Smyth »).

Exercice 61. 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.*

Exercice 62. ⑤ *Quelle est la signature de la forme quadratique déduite de* $\mathrm{tr}_{\mathbb{K}/\mathbb{Q}}$ *par extension des scalaires à* $\mathbb{R}$ *?*[17]

Exercice 63. ⑤ *Soit* $x \in \overline{\mathbb{Q}}$ *totalement réel. On se propose de montrer qu'il existe une matrice symétrique à coefficients rationnels dont* x *est valeur propre (exercice 10,* **1***).*

a) En utilisant la forme trace et l'endomorphisme de multiplication par x *de l'extension* $\mathbb{K}/\mathbb{Q}$*, établir qu'il existe un espace quadratique rationnel défini positif et un endomorphisme autoadajoint de cet espace admettant* x *comme valeur propre lorsqu'on étend les scalaires à* $\overline{\mathbb{Q}}$*.*

b) Soit $r \in \mathbb{Q}^{+*}$*. Montrer qu'il existe* $n \in \mathbb{N}^*$ *et une forme quadratique euclidienne sur* $\mathbb{Q}^n$ *prenant la valeur* r*.*

c) En utilisant b) et en raisonnant par récurrence, montrer que, si (E, q) *est un espace quadratique rationnel de dimension finie défini positif,* (E, q) *est facteur direct (au sens de la somme orthogonale) d'un espace quadratique rationnel euclidien.*

d) Montrer qu'il existe un espace quadratique rationnel euclidien et un endomorphisme autoadajoint de cet espace admettant x *comme valeur propre lorsqu'on étend les scalaires à* $\overline{\mathbb{Q}}$*. Conclure.*[18]

6.4 Discriminant

Supposons que $\mathbb{L}/\mathbb{K}$ une extension séparable de degré n, notons tr la forme trace de cette extension. La définition même de tr suggère l'étude des déterminants :

$$D_{\mathbb{L}/\mathbb{K}}(x_1, \ldots, x_n) = (\mathrm{tr}(x_i x_j))_{1 \leq i,j \leq n}$$

pour $(x_1, \ldots, x_n)$ dans $\mathbb{L}^n$. L'application $D_{\mathbb{L}/\mathbb{K}}$ de $\mathbb{L}^n$ ainsi définie est appelée *discriminant* de l'extension $\mathbb{L}/\mathbb{K}$. Le lemme ci-après en indique deux propriétés immédiates.

Lemme 6. *(i) On a* $D_{\mathbb{L}/\mathbb{K}}(x_1, \ldots, x_n) = 0$ *si et seulement si* $(x_1, \ldots, x_n)$ *est* $\mathbb{K}$*-liée.*

(ii) Soient $(y_1, \ldots, y_n)$ *et* $(x_1, \ldots, x_n)$ *deux* $\mathbb{K}$*-bases de* $\mathbb{L}$*,* P *la matrice de passage de* $(x_1, \ldots, x_n)$ *à* $(y_1, \ldots, y_n)$*, alors :*

$$D_{\mathbb{L}/\mathbb{K}}(y_1, \ldots, y_n) = (\det P)^2 D_{\mathbb{L}/\mathbb{K}}(x_1, \ldots, x_n).$$

Preuve. Le premier point résulte du caractère non dégénéré de la forme trace, le second de la formule de changement de base pour les formes quadratiques.

On peut écrire autrement le déterminant précédent. Numérotons $\sigma_1, \ldots, \sigma_n$ les éléments de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$. Si R est la matrice

$$(\sigma_i(x_j))_{1 \leq i,j \leq n}$$

et si on pose $Q = R^T R = (Q_{i,j})_{1 \leq i,j \leq n}$, on a alors :

$$\forall (i,j) \in \{1, \ldots, n\}^2, \qquad Q_{i,j} = \sum_{k=1}^{n} R_{k,i} R_{k,j} = \mathrm{tr}(x_i x_j).$$

Ceci prouve le :

17. Théorème dû à Taussky.

18. Se pose la question suivante : si $x \in \overline{\mathbb{Q}}$ est totalement réel de degré d sur $\mathbb{Q}$, quel est le plus petit n tel que x soi valeur propre d'une matrice symétrique rationnelle de taille n ? On peut montrer que $n \leq d + 3$. L'exemple de $\sqrt{3}$ donné dans l'exercice 10 montre qu'en général $n > d$.

Lemme 7. *Si* $(x_1, \ldots, x_n) \in \mathbb{L}^n$, $D_{\mathbb{L}/\mathbb{K}}(x_1, \ldots, x_n) = (\det(\sigma_i(x_j))_{1 \leq i,j \leq n})^2$.

L'énoncé suivant, souvent utile, fait relie $D_{\mathbb{L}/\mathbb{K}}$ et la notion de discriminant d'un polynôme.

Lemme 8. *Soit* α *dans* $\mathbb{L}$ *tel que* $\mathbb{L} = \mathbb{K}(\alpha)$. *Alors,*

$$D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \Delta(\Pi_{\mathbb{K},\alpha}).$$

Preuve. Notons $\alpha_1 = \alpha, \ldots, \alpha_n$ les racines de $\Pi_{\mathbb{K},\alpha}$ dans Ω. Alors :

$$\Delta(\Pi_{\mathbb{K},\alpha}) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Il suffit d'utiliser le calcul du déterminant de Vandermonde pour conclure.

7 (*) Appendice : anneau des entiers d'un corps de nombres

On montre dans cette section comment les outils de **6**, les rudiments d'algèbre linéaire sur $\mathbb{Z}$ (groupes abéliens libres de type fini) et la résolution des systèmes linéaires interagissent pour élucider la structure additive de l'anneau des entiers d'un corps de nombres. On obtient un énoncé général (le théorème 6), que l'on prolonge par quelques calculs effectifs, qui sont l'occasion de revisiter les notions de discriminant et de polynôme d'Eisenstein.

7.1 Structure additive d'un anneau d'entiers

Si $\mathbb{K}$ est un corps de nombres, on note $\mathbb{Z}_\mathbb{K}$ l'anneau des entiers de $\mathbb{K}$ (chapitre **2**, **5.1**). Nous allons utiliser la trace pour déterminer la structure additive de $\mathbb{Z}_\mathbb{K}$. .

Rappelons que, si $x \in \overline{\mathbb{Q}}$, il existe $q \in \mathbb{N}^*$ tel que $qx \in \overline{\mathbb{Z}}$ (chapitre **2**, **5.1**, lemme 10). Il en découle que, si $\mathbb{K}$ est un corps de nombres, le $\mathbb{Q}$-espace $\mathbb{K}$ admet une base constituée d'éléments de $\mathbb{Z}_\mathbb{K}$. Nous utilisons une telle base dans la démonstration du théorème suivant, dû à Dedekind.

Théorème 6. *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* $\mathbb{Z}_K$, $D = D_{\mathbb{K}/\mathbb{Q}}(x_1, \ldots, x_n)$. *Alors :*

$$\bigoplus_{i=1}^{n} \mathbb{Z}x_i \subset \mathbb{Z}_\mathbb{K} \subset \bigoplus_{i=1}^{n} \frac{\mathbb{Z}x_i}{D}.$$

Le groupe $(\mathbb{Z}_\mathbb{K}, +)$ *est un g.a.l.t.f de rang* n.

Preuve. Un résultat classique relatif aux groupes abéliens libres de type fini(g.a.l.t.f.) montre que les deux inclusions entraînent que $(\mathbb{Z}_\mathbb{K}, +)$ est un g.a.l.t.f de rang n. La première est immédiate. Prouvons la seconde. Soient $x \in \mathbb{Z}_\mathbb{K}$, $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Q}^n$ tel que :

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

tr la forme trace de l'extension $\mathbb{K}/\mathbb{Q}$. On a le système de n équations linéaires d'inconnue $(\lambda_1, \ldots, \lambda_n)$:

$$\forall j \in \{1, \ldots, n\}, \qquad \mathrm{tr}\,(x_j x) = \sum_{i=1}^{n} \lambda_i \,\mathrm{tr}\,(x_j x_i)\,.$$

L'appartenance de $(\mathrm{tr}(x_1x),\dots \mathrm{tr}(x_nx))$ à $\mathbb{Z}^n$, le fait que $D = D_{\mathbb{K}/\mathbb{Q}}(x_1,\dots x_n)$ soit non nul et les formules de Cramer montrent que les λ_i sont dans $\dfrac{\mathbb{Z}}{D}$.

Remarques

1. *Effectivité*
   L'ensemble des sous-groupes de $(\mathbb{K},+)$ vérifiant la double inclusion du théorème 6 est équipotent à l'ensemble des sous-groupes de $((\mathbb{Z}/D\mathbb{Z})^n,+)$, en particulier fini.

   Autre formulation : pour déterminer $\mathbb{Z}_\mathbb{K}$, il suffit de trouver ceux des éléments $\displaystyle\sum_{i=1}^{n}\lambda_i x_i$ où $(\lambda_1,\dots,\lambda_n)\in\{0,\dots,D-1\}^n$ qui sont des entiers algébriques.
2. *Une variante*
   Voici une variante de la preuve précédente. En conservant les mêmes notations, on a

   $$\forall\sigma\in\mathrm{Hom}_\mathbb{Q}(\mathbb{K},\overline{\mathbb{Q}}),\qquad \sigma(x)=\sum_{i=1}^{n}\lambda_i\sigma(x_i).$$

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

La détermination d'un anneau d'entiers est souvent délicate. Le cas des corps quadratiques a été traité dans le chapitre **2** (**5.1**, proposition 13). Les paragraphes suivants sont consacrés à des calculs explicites plus élaborés ; on y utilise la trace, la norme, le discriminant et les polynômes d'Eisenstein.

7.2 Discriminant d'un corps de nombres et anneaux d'entiers

Soient $\mathbb{K}$ un corps de nombres, $n=[\mathbb{K}:\mathbb{Q}]$.

Si Γ est un sous-groupe libre de rang n de $(\mathbb{K},+)$, on peut définir le discriminant D_Γ de Γ comme valeur commune des $D_\mathbb{K}(x_1,\dots,x_n)$ pour $(x_1,\dots,x_n)$ $\mathbb{Z}$-base de Γ.[19] Par exemple, si $\alpha\in\mathbb{Z}_\mathbb{K}$ est de degré n sur $\mathbb{K}$, $D_{\mathbb{Z}[\alpha]}$ est égal à $\Delta(\Pi_{\mathbb{Q},\alpha})$. Si $\Gamma\subset\mathbb{Z}_\mathbb{K}$ et si P est la matrice de présentation d'une $\mathbb{Z}$-base de Γ dans une $\mathbb{Z}$-base de $\mathbb{Z}_\mathbb{K}$, le déterminant de P a pour valeur absolue $|\mathbb{Z}_\mathbb{K}/\Gamma|$. Le lemme 6 de **6.4** entraîne le résultat ci-après.

Lemme 9. *Soit Γ un sous-groupe de rang n de $\mathbb{Z}_\mathbb{K}$. Alors :*

$$D_\Gamma = |\mathbb{Z}_\mathbb{K}/\Gamma|^2\ D_\mathbb{K}.$$

On en déduit une caractérisation des $\mathbb{Z}$-bases de $\mathbb{Z}_\mathbb{K}$.

19. Rappelons que, si G est un g.a.l.t.f. de rang $n\in\mathbb{N}^*$, la matrice de passage d'une $\mathbb{Z}$-base de G à une autre est dans $\mathrm{GL}_n(\mathbb{Z})$, donc de déterminant ±1. Le lemme 6 de **6.4** montre donc que la définition est indépendante de la $\mathbb{Z}$-base de Γ choisie.

Corollaire 12. *Soit $(x_1, \ldots, x_n)$ une famille $\mathbb{Q}$-libre d'éléments de $\mathbb{Z}_\mathbb{K}$. Alors*

$$|\Delta_{\mathbb{K}/\mathbb{Q}}(x_1, \ldots, x_n)| \geq |D_\mathbb{K}|,$$

avec égalité si et seulement si $(x_1, \ldots, x_n)$ est une $\mathbb{Z}$-base de $\mathbb{Z}_\mathbb{K}$.

Exercice 64. ③ *Montrer, sans utiliser le théorème 6, qu'une famille de $\mathcal{O}_\mathbb{K}$ dont le discriminant est non nul et de valeur absolue minimale est une $\mathbb{Z}$-base de $\mathcal{O}_\mathbb{K}$. En déduire une autre démonstration du théorème 6.*

Corollaire 13. *Si D_Γ s'écrit $q^2 r$ où q et r sont des entiers et r est sans facteur carré, alors $|\mathcal{O}_\mathbb{K}/\Gamma|$ divise q. En particulier, si D_Γ est sans facteur carré, $\Gamma = \mathcal{O}_\mathbb{K}$.*

Corollaire 14. *Soit $P \in \mathbb{Z}[X]$ unitaire, irréductible sur $\mathbb{Q}$, tel que $\Delta(P)$ ne soit divisible par aucun carré de nombre premier. Alors, pour toute racine α de P,*

$$\mathbb{Z}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha].$$

Exemples

1. *Discriminant d'un corps quadratique*
   Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteur carré. On déduit facilement de la proposition 13 du chapitre **2** (**5.1**) que $D_{\mathbb{Q}(\sqrt{d})}$ est égal à $4d$ si d est congru à 2 ou 3 modulo 4, à d si d est congru à 1 modulo 4.
2. Le discriminant de $P = X^3 - X - 1$ est -23. Si α est une racine de P, on a donc
   $$\mathbb{Z}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha].$$
3. Le discriminant de $P = X^3 - X - 4$ est -4×107. Soit α une racine de P. On vérifie que $\beta = \dfrac{\alpha + \alpha^2}{2}$ est entier algébrique. Si
   $$\Gamma = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta,$$
   on a immédiatement $D_\Gamma = -107$. Par suite,
   $$\mathbb{Z}_{\mathbb{Q}(\alpha)} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta.$$

Exercice 65. ③ *Soient $x \in \mathbb{C}$ une racine de $P = X^5 - X - 1$, $\mathbb{K} = \mathbb{Q}(x)$. Montrer que $\mathbb{Z}_\mathbb{K} = \mathbb{Z}[x]$.*

Exercice 66. ③ *Déterminer le signe de $D_\mathbb{K}$.* [20]

Exercice 67. ④ *a) Soient a et b deux nombres complexes tels que ab et $a + b$ soient dans $\mathbb{Z}$. Montrer que $(a - b)^2$ est un entier congru à 0 ou 1 modulo 4.*

b) Montrer que $D_\mathbb{K}$ est congru à 0 ou 1 modulo 4. [21]

Exercice 68. ③ *Soient $x \in \mathbb{C}$ une racine de $P = X^3 + X^2 + 2$, $\mathbb{K} = \mathbb{Q}(x)$. Calculer $\Delta(P)$ et en déduire, à l'aide de l'exercice précédent, que $\mathbb{Z}_\mathbb{K} = \mathbb{Z}[x]$.*

20. Théorème dû à Brill.
21. Théorème dû à Stickelberger.

Exercice 69. ④ *Soient $\mathbb{K}$ et $\mathbb{L}$ deux corps de nombres avec $\mathbb{K} \subset \mathbb{L}$.*

a) En utilisant le théorème de la base adaptée pour les g.a.l.t.f., montrer que $\mathbb{Z}_\mathbb{K}$ est facteur direct du groupe additif $\mathbb{Z}_\mathbb{L}$.

b) Montrer que $D_\mathbb{K}$ divise $D_\mathbb{L}$.

Indices ; anneaux d'entiers non monogènes

Soit $\alpha \in \mathbb{Z}_\mathbb{K}$ de degré n sur $\mathbb{Q}$. Alors $\mathbb{Z}[\alpha]$ est un sous-groupe de rang n de $(\mathbb{Z}_\mathbb{K}, +)$, donc d'indice fini. Cet indice est l'*indice de* α vis-à-vis de $\mathbb{K}$; on le note $\mathrm{ind}_\mathbb{K}(\alpha)$. Grâce au lemme 9 :

$$\mathrm{ind}_\mathbb{K}(\alpha) = \sqrt{\frac{|\Delta(\Pi_{\mathbb{Q},\alpha})|}{|D_\mathbb{K}|}}.$$

On définit également les notions suivantes.

- L'*indice de* $\mathbb{K}$, noté $\mathrm{ind}(\mathbb{K})$, est le p.g.c.d. des indices des entiers de $\mathbb{K}$ de degré n sur $\mathbb{Q}$. Dire que $\mathbb{Z}_\mathbb{K}$ est extension monogène de $\mathbb{Z}$, c'est dire qu'il existe $\alpha \in \mathcal{O}_\mathbb{K}$ d'indice 1 ; cette condition implique que $\mathrm{ind}(\mathbb{K}) = 1$, mais ne lui est pas équivalente.

- Si $\alpha \in \overline{\mathbb{Z}}$, l'indice de α, noté $\mathrm{ind}(\alpha)$, est l'indice de α relativement à $\mathbb{Q}(\alpha)$.

Si $\mathbb{K}$ est un corps de nombres quadratiques, $\mathbb{Z}_\mathbb{K}$ est extension monogène de $\mathbb{Z}$. Voici un exemple, dû à Dedekind, de corps de nombre d'indice différent de 1 : l'anneau $\mathbb{Z}_\mathbb{K}$ n'est donc pas extension monogène de $\mathbb{Z}$. Soient P le polynôme $X^3 + X^2 - 2X + 8$, α une de ses racines dans $\mathbb{C}$, $\mathbb{K}$ le corps $\mathbb{Q}(\alpha)$. Il est immédiat de vérifier que P n'a pas de racine rationnelle ; étant de degré 4, il est irréductible sur $\mathbb{Q}$. Le discriminant de P est -4×503. D'autre part, si $\beta = \dfrac{4}{\alpha}$, β est racine de $Q = X^3 - X^2 + 2X + 8$, donc est entier algébrique, donc appartient à $\mathbb{Z}_\mathbb{K}$. On a :

$$D_\mathbb{Q}(1, \alpha, \beta) = -503$$

donc, puisque 503 est sans facteur carré, le corps $\mathbb{K}$ a pour discriminant -503 et $(1, \alpha, \beta)$ est une $\mathbb{Z}$-base de $\mathbb{Z}_\mathbb{K}$.

Montrons que, si $\gamma \in \mathbb{Z}_\mathbb{K}$ est de degré 3 sur $\mathbb{Q}$, alors $\mathrm{ind}_\mathbb{K}(\gamma)$ est pair, ce qui entraînera que $\mathbb{Z}_\mathbb{K}$ n'est pas monogène sur $\mathbb{Z}$. Une méthode pédestre consiste à écrire

$$\gamma = x + y\alpha + z\beta \quad \text{avec} \quad (x, y, z) \in \mathbb{Z}^3$$

et à calculer en fonction de (x, y, z) le déterminant de la matrice de passage P de $(1, \alpha, \beta)$ à $(1, \gamma, \gamma^2)$. On décompose α^2 et β^2 sur la base $(1, \alpha, \beta)$:

$$\alpha^2 = 2 - \alpha - 2\beta, \quad \beta^2 = -2 - 2\alpha + \beta.$$

Il vient

$$P = \begin{pmatrix} 1 & x & x^2 + 2y^2 + 8yz - 2z^2 \\ 0 & y & 2xy - y^2 - 2z^2 \\ 0 & z & 2xz - 2y^2 + z^2 \end{pmatrix}.$$

Le déterminant de P est donc égal à

$$2(xy^2 - xyz - y^3 - z^3) + y^2z - yz^2,$$

qui est toujours pair.

Cette démonstration établit le résultat général de l'exercice ci-après.

Exercice 70. ③ *On se donne une $\mathbb{Z}$-base $(\alpha_1, \ldots, \alpha_n)$ de $\mathbb{Z}_\mathbb{K}$. Pour $\alpha \in \mathbb{Z}_\mathbb{K}$, on écrit $\alpha = \sum_{i=1}^{n} x_i \alpha_i$. Montrer qu'il existe $P \in \mathbb{Z}[X_1, \ldots, X_n]$ homogène de degré $\frac{n(n-1)}{2}$ tel que*

$$\forall \alpha \in \mathbb{Z}_\mathbb{K},\ \mathbb{K} = \mathbb{Q}(\alpha) \Longrightarrow ind_\mathbb{K}(\alpha) = P(x_1, \ldots, x_n).$$

Exercice 71. ③ *Montrer que l'anneau $\mathbb{Z}_\mathbb{K}/2\mathbb{Z}_\mathbb{K}$ est de cardinal 8 et ne contient que des éléments idempotents. En déduire que cet anneau n'est pas extension monogène de $\mathbb{F}_2$. Retrouver le fait que $\mathbb{Z}_\mathbb{K}$ n'est pas monogène sur $\mathbb{Z}$.*

On peut généraliser l'argument précédent. Si $\mathbb{K}$ est un corps de nombres, les diviseurs premiers de $\mathrm{ind}(\mathbb{K})$ sont appelés *facteurs premiers extraordinaires de $D_\mathbb{K}$*. S'il existe un tel nombre premier, $\mathbb{Z}_\mathbb{K}$ n'est pas extension monogène de $\mathbb{Z}$. Il existe cependant des corps de nombres dont le discriminant n'admet pas de facteur premier extraordinaire, mais dont l'anneau des entiers n'est pas monogène sur $\mathbb{Z}$ (**7.3**, exemple 3).

Exercice 72. *Soient $\mathbb{K} = \mathbb{Q}(\sqrt{7}, \sqrt{10})$, $\mathbb{A} = \mathbb{Z}_\mathbb{K}$, $\mathrm{tr} = \mathrm{tr}_{K/\mathbb{Q}}$ et*

$$\alpha_1 = (1 + \sqrt{7})(1 + \sqrt{10}).$$

a) Montrer que α_1 est dans $\mathbb{A}$, de degré 4 sur $\mathbb{Q}$; écrire ses $\mathbb{Q}$-conjugués $\alpha_2, \alpha_3, \alpha_4$. Vérifier en particulier, si $1 \leq i, j \leq 4$ et $i \neq j$, que $\alpha_i \alpha_j$ est dans $3\mathbb{A}$.

b) Si $n \in \mathbb{N}^*$, montrer que $\mathrm{tr}({\alpha_1}^n) \equiv 1\ [3\mathbb{A}]$, puis que que ${\alpha_1}^n \notin 3\mathbb{A}$.

On suppose désormais que $\mathbb{A} = \mathbb{Z}[\alpha]$. L'élément α de $\mathbb{Z}_\mathbb{K}$ est donc de degré 4 sur $\mathbb{Q}$. On note $\Pi = \Pi_{\mathbb{Q},\alpha}$. Si $1 \leq i \leq 4$, on peut écrire d'une unique façon $\alpha_i = P_i(\alpha)$ avec $P_i \in \mathbb{Z}[X]$ de degré ≤ 3. Enfin, on note $\overline{P}$ la réduction modulo 3 du polynôme P de $\mathbb{Z}[X]$.

c) Montrer que $\overline{\Pi}$ divise $\overline{P_i}.\overline{P_j}$ si $i \neq j$, mais ne divise pas $\overline{P_i}^n$ si $n \geq 1$.

d) Montrer, si $1 \leq i \leq 4$, l'existence de q_i dans $\mathbb{F}_3[X]$ irréductible, unitaire divisant : $\overline{\Pi}$ et $\overline{P_j}$ pour $j \neq i$ mais pas $\overline{P_i}$.

e) Aboutir à une contradiction.

Il est tentant d'identifier précisément l'anneau de l'exercice précédent.

Exercice 73. *Soient m et n deux entiers distincts différents de 1 sans facteur carré. On pose*

$$k\frac{mn}{(m \wedge n)^2} \quad ; \quad \mathbb{K} = \mathbb{Q}(\sqrt{m}, \sqrt{n}).$$

Supposons $m \equiv 3[4]$, $n \equiv 2[4]$, $k \equiv 2[4]$. On sait que $(1, \sqrt{m}, \sqrt{n}, \sqrt{k})$ est une $\mathbb{Q}$-base de $\mathbb{K}$. Notons $x = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{k}$ la décomposition de $x \in \mathbb{Z}_\mathbb{K}$ sur cette base.

a) En considérant $\mathrm{tr}_{\mathbb{K}/\mathbb{Q}(\sqrt{n})}(x)$ et les deux traces relatives analogues, montrer que $2a$, $2b$, $2c$ sont entiers.

a) En considérant $N_{\mathbb{K}/\mathbb{Q}(\sqrt{m})}(x)$, montrer que a et b sont pairs, que $c \equiv d[2]$. En déduire que $(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{k}}{2})$ est une $\mathbb{Z}$-base de $\mathbb{Z}_\mathbb{K}$.

7.3 Polynômes d'Eisenstein et anneaux d'entiers

Le théorème ci-après donne un renseignement intéressant sur l'anneau d'entiers d'un corps de nombres engendré sur $\mathbb{Q}$ par une racine d'un polynôme satisfaisant au critère d'Eisenstein (chapitre **1**, **2.4**, proposition 5). Afin d'en abréger l'énoncé, disons, si $p \in \mathcal{P}$, qu'un polynôme P unitaire de $\mathbb{Z}[X]$ est un *polynôme p-Eisenstein* s'il vérifie l'hypothèse du critère d'Eisenstein pour p.

Théorème 7. *Soient $p \in \mathcal{P}$, P un polynôme p-Eisenstein, α une racine de P dans $\mathbb{C}$, $\mathbb{K} = \mathbb{Q}(\alpha)$. Alors ind($\alpha$) n'est pas divisible par p.* [22]

Preuve. Pour établir la première, notons n le degré de P, N la norme de l'extension $\mathbb{K}/\mathbb{Q}$. Si le résultat était faux, le groupe additif $\mathbb{Z}_{\mathbb{K}}/\mathbb{Z}[\alpha]$ contiendrait un élément d'ordre p. Autrement dit, il existerait x dans $\mathbb{Z}_{\mathbb{K}} \setminus \mathbb{Z}[\alpha]$ tel que $px \in \mathbb{Z}[\alpha]$. Montrons que ceci est impossible. Écrivons : $x = \sum_{i=0}^{n-1} \frac{a_i}{p}\alpha^i$ où les a_i sont dans $\mathbb{Z}$, et montrons, par récurrence sur $i \in \{0, \ldots, n-1\}$, que a_i est dans $\mathbb{Z}$. On a

$$px = \sum_{i=0}^{n-1} a_i \alpha^i \in p\overline{\mathbb{Z}},$$

d'où on déduit que $\alpha^n \in p\overline{\mathbb{Z}}$. En multipliant par α^{n-1}, on a que $a_0\ \alpha^{n-1} \in p\overline{\mathbb{Z}}$. Si N la norme de l'extension $\mathbb{K}/\mathbb{Q}$, on a donc

$$a_0^n\ N(\alpha)^{n-1} \in p^n\mathbb{Z}.$$

La p-valuation de $N(\alpha)$ est 1, donc $a_0?^n$ est divisible par p, i.e. a_0 est divisible par p. Multipliant ensuite successivement par $\alpha^{n-2}, \ldots, \alpha, 1$ on obtient que $a_1, \ldots, a_{n-1}$ sont divisibles par p.

Exemples

1. *Corps cyclotomiques d'indices premiers*
   Gardons les hypothèses de la proposition précédente et supposons en outre $\Delta(P)$ de la forme $\pm p^m$, $m \in \mathbb{N}$. Alors, par définition de l'indice,

   $$\mathbb{Z}_{\mathbb{K}} = \mathbb{Z}[\alpha].$$

   Soit $p \in \mathcal{P}$. Alors

   $$\Delta(\Phi_p) = (-1)^{\frac{(p-1)(p-2)}{2}} \prod_{\omega \in \mathbb{U}_p \setminus \{1\}} \Phi_p'(\omega).$$

   Or, $\Phi_p = \dfrac{X^p - 1}{X - 1}$. Donc, si $\omega \in \mathbb{U}_p \setminus \{1\}$, $\Phi_p'(\omega) = \dfrac{p\omega^{p-1}}{\omega - 1} = \dfrac{p}{\omega\ (\omega - 1)}$. Mais

   $$\prod_{\omega \in \mathbb{U}_p \setminus \{1\}} (1 - \omega) = \Phi_p(1) = p,$$

   d'où il résulte que $\Delta(\Phi_p)$ est de a forme $\pm p^{p-2}$. [23] On en déduit le théorème suivant, que nous généraliserons en **7.4**.

   Théorème 8. *Si $p \in \mathcal{P}$ alors :*

   $$\mathbb{Z}_{\mathbb{Q}(e^{2i\pi/p})} = \mathbb{Z}[e^{2i\pi/p}].$$

2. *Corps cubiques purs*
   Appelons *corps cubique pur* tout corps de nombres de la forme $\mathbb{Q}(\sqrt[3]{q})$, où q est un entier qui n'est divisible par aucun cube de nombre premier. Les entiers des corps cubiques purs ont été déterminés par Dedekind. Nous allons traiter le cas particulier où l'entier q n'est divisible par aucun carré de nombre premier. Fixons un tel q, notons $\mathbb{K} = \mathbb{Q}(\sqrt[3]{q})$.

22. Autrement dit, les p-valuations de $D_{\mathbb{K}}$ et $D_{\mathbb{Q}}(\alpha)$ sont égales.
23. On trouvera une expression de $\Delta(\Phi_n)$ pour $n \in \mathbb{N}^*$ dans l'exercice 73 du chapitre **1** (**4.3**).

Le polynôme $X^3 - q$ a pour discriminant $-27q^2$, donc $|\mathcal{O}_K/\mathbb{Z}[\sqrt[3]{q}]|$ divise $3q$. D'autre part, $X^3 - q$ est p-Eisenstein pour tout nombre premier p divisant q. Il s'ensuit que $|\mathcal{O}_K/\mathbb{Z}[\sqrt[3]{q}]|$ est égal à 1 ou 3. Remarquons maintenant que, pour tout a dans $\mathbb{Z}$,

$$\mathbb{Z}[\sqrt[3]{q}] = \mathbb{Z}[a + \sqrt[3]{q}].$$

S'il existe a dans $\mathbb{Z}$ tel que $(X - a)^3 - q$ soit 3-Eisenstein, on a donc $\mathbb{Z}_\mathbb{K} = \mathbb{Z}[\sqrt[3]{q}]$. Cette condition revient à l'existence de $a \in \mathbb{Z}$ tel que $q + a^3$ soit divisible par 3 mais pas par 9, ou encore au fait que q ne soit congru ni à 1 ni à -1 modulo 9.

Ainsi, si q est sans facteur carré et n'est congru ni à 1 ni à -1 modulo 9,

$$\mathbb{Z}_\mathbb{K} = \mathbb{Z}[\sqrt[3]{q}], \quad D_K = -27q^2.$$

Si $q \equiv 1[9]$, l'élément

$$\beta = \frac{(\sqrt[3]{q} - 1)^2}{3}$$

de $\mathbb{K}$ appartient à $\mathbb{Z}_\mathbb{K}$. Pour le voir, on calcule le polynôme caractéristique de la multiplication par β dans $\mathbb{K}$ (en se plaçant dans la base $(1, \sqrt[3]{q}, \sqrt[3]{q^2})$). Ce polynôme est

$$X^3 - X^2 + \frac{(2q+1)}{3}X + \frac{(q-1)^2}{9}.$$

Il annule β. Comme β n'est pas dans $\mathbb{Z}[\sqrt[3]{q}]$, l'indice de $\mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta$ dans $\mathcal{O}_\mathbb{K}$ est 3, et, 3 étant premier et $\sqrt[3]{q}$ contenu dans $\mathbb{Z}[\beta]$, il vient :

$$\mathbb{Z}_\mathbb{K} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta, \quad D_\mathbb{K} = -9q^2.$$

Si $q \equiv -1[9]$, on pose

$$\gamma = \frac{(\sqrt[3]{q} + 1)^2}{3}.$$

Un raisonnement analogue au précédent donne :

$$\mathbb{Z}_\mathbb{K} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\gamma, \quad D_\mathbb{K} = -9q^2.$$

3. *Un exemple de corps de nombres dont l'anneau des entiers n'est pas monogène mais dont le discriminant n'admet pas de facteur premier extraordinaire (Hensel)*

Soient p et q deux nombres premiers distincts différents de 3, $\alpha = \sqrt[3]{p^2q}$, $\mathbb{K} = \mathbb{Q}(\alpha)$. Si $\beta = \sqrt[3]{pq^2}$, $\alpha\beta = pq$ de sorte que $\mathbb{K}$ contient β. Le discriminant de α (resp. β) sur $\mathbb{Q}$ est $-3^3p^2q^4$ (resp. $-3^3p^4q^2$), donc $D_\mathbb{K}$ divise $3^3p^2q^2$. Comme les polynômes $X^3 - p^2q$ et $X^3 - pq^2$ sont respectivement p-Eisenstein et q-Eisenstein, $D_\mathbb{K}$ est divisible par p^2q^2.

Supposons maintenant que p^2q n'est congru ni à 1 ni à -1 modulo 9. Alors, comme dans l'exemple précédent, le polynôme minimal de $\alpha + p^2q$ est 3-Eisenstein et $D_\mathbb{K}$ est divisible par 3^3. Vu que $D_\mathbb{Q}(1, \alpha, \beta) = -3^3p^2q^2$, il s'ensuit que $(1, \alpha, \beta)$ est une $\mathbb{Z}$-base de $\mathbb{Z}_\mathbb{K}$:

$$\mathbb{Z}_\mathbb{K} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta, \qquad D_\mathbb{K} = -3^3p^2q^2.$$

En considérant les discriminants de α et β on en déduit que $D_\mathbb{K}$ n'a pas de facteur premier extraordinaire.

Il reste à montrer que l'on peut choisir p et q de sorte que $\mathbb{Z}_\mathbb{K}$ ne soit pas monogène. Soit donc x dans $\mathbb{Z}_K$: $x = t + u\alpha + v\beta$ avec t, u, v dans $\mathbb{Z}$. Le discriminant de x sur $\mathbb{Q}$ est

celui de $x-t$. Vu que le polynôme minimal de α sur $\mathbb{Q}$ est X^3-p^2q, les $\mathbb{Q}$-conjugués de α sont $\alpha, j\alpha, j^2\alpha$. Enfin, vu que $\alpha\beta$ est rationnel, l'élément de $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{K},\mathbb{C})$ envoyant α sur $j\alpha$ (resp. $j^2\alpha$) envoie β sur $j^2\beta$ (resp. $j\beta$). Il s'ensuit que $D_{\mathbb{Q}}(x)$ vaut

$$\left(\left((j-1)u\alpha+(j^2-1)v\beta\right)\left((j^2-1)u\alpha+(j-1)v\beta\right)\left((j^2-j)(u\alpha-v\beta)\right)\right)^2,$$

c'est-à-dire, après calcul,

$$-3^3p^2q^2(pu^3-qv^3)^2.$$

L'égalité $\mathbb{Z}_K=\mathbb{Z}[x]$ équivaut à $pu^3-qv^3=\pm1$. Si on impose

$$p\equiv 1[3] \quad , \quad q^{(p-1)/3}\not\equiv 1[p],$$

q n'est pas un cube modulo p et $\mathbb{Z}_K$ n'est pas monogène.

Tel est le cas, par exemple, pour $(p,q)=(7,5)$. Ainsi, si $\mathbb{K}=\mathbb{Q}(\sqrt[3]{245})$,

$$\mathcal{O}_K=\mathbb{Z}\oplus\mathbb{Z}\sqrt[3]{245}\oplus\mathbb{Z}\sqrt[3]{175},\quad D_{\mathbb{K}}=-3^37^25^2,$$

$D_{\mathbb{K}}$ n'a pas de facteur premier extraordinaire et $\mathbb{Z}_{\mathbb{K}}$ n'est pas extension monogène de$\mathbb{Z}$.

Exercice 74. ③ *Généraliser la démonstration du théorème 8 aux corps cyclotomiques d'indices de la forme p^m avec $p\in\mathcal{P}$ et $m\in\mathbb{N}^*$.*

L'exercice ci-après montre en particulier que, si $p\in\mathcal{P}\setminus\{2\}$, l'anneau des entiers de $\mathbb{Q}(\sqrt[p]{2})$ est $\mathbb{Z}[\sqrt[p]{2}]$ si et seulement si p^2 ne divise pas $2^{p-1}-1$.

Exercice 75. ④ *Soient $p\in\mathcal{P}$, $a\in\mathbb{Z}\setminus\{0,1\}$ sans facteur carré et premier à p, $\alpha\in\mathbb{C}$ tel que $\alpha^p=a$, $\mathbb{K}=\mathbb{Q}(\alpha)$.*

a) On suppose que p^2 ne divise pas $a^{p-1}-1$. Montrer que $\mathbb{Z}_{\mathbb{K}}=\mathbb{Z}[\alpha]$.

b) Si p^2 divise $a^{p-1}-1$, montrer que $\dfrac{1+a\alpha^{p-2}+a^2\alpha^{p-3}+\cdots+a^{p-2}\alpha}{p}$ est dans $\mathcal{O}_{\mathbb{K}}$, ce qui entraîne que $\mathbb{Z}_{\mathbb{K}}\neq\mathbb{Z}[\alpha]$.

7.4 Entiers des corps cyclotomiques

Pour $n\in\mathbb{N}^*$, soit $\omega_n=e^{2i\pi/n}$. Le théorème 8 se généralise de la façon suivante.

Théorème 9. *Pour $n\in\mathbb{N}^*$,*

$$\mathbb{Z}_{\mathbb{Q}(\omega_n)}=\mathbb{Z}[\omega_n].$$

Preuve. Étape 1. Le point de départ de la preuve qui suit est une décomposition remarquable d'un élément x de $\mathbb{K}_n$ comme combinaison $\mathbb{K}$-linéaire des ${\omega_n}^j$ pour $0\leq j\leq n-1$.

Lemme 10. *Soient $\mathbb{K}$ un corps de nombres, $n\in\mathbb{N}^*$, tr la forme trace de $\mathbb{K}_n/\mathbb{K}$. Alors :*

$$\forall x\in\mathbb{K}_n,\qquad x=\frac{1}{n}\sum_{j=0}^{n-1}\mathrm{tr}({\omega_n}^{-j}x){\omega_n}^j.$$

Preuve du lemme 10. Abrégeons ω_n en ω, notons I l'ensemble des $i \in \{0,\dots,n-1\}$ tels que ω^i soit un $\mathbb{K}$-conjugué de ω. Pour i dans I soit σ_i le $\mathbb{K}$-automorphisme de $\mathbb{K}_n$ envoyant ω sur ω^i. Prenons $x \in \mathbb{K}_n$ et posons $x_i = \sigma_i(x)$ pour $i \in I$, $x_i = 0$ pour $i \in \{0,\dots,n-1\} \setminus I$. Considérons le système :

$$(S) \qquad \forall j \in \{0,\dots,n-1\}, \qquad \sum_{i=0}^{n-1} \omega^{ij} y_j = x_i$$

d'inconnue $(y_0,\dots,y_{n-1})$. Comme la matrice de Vandermonde $\left(\omega^{ij}\right)_{0\le i,j\le n-1}$ est inversible d'inverse[24] $\left(\dfrac{\omega^{-ij}}{n}\right)_{0\le i,j\le n-1}$, (S) a une unique solution donnée par :

$$y_j = \frac{1}{n}\sum_{i=0}^{n-1} \omega^{-ij} x_i = \frac{1}{n}\sum_{i\in I} \omega^{-ij} x_i = \frac{1}{n}\sum_{i\in I} \sigma_l(\omega^{-j}x) = \frac{1}{n}\mathrm{tr}(\omega^{-j}x)$$

pour tout $i \in \{0,\dots,n-1\}$. Puisque $x = x_1$, le résultat suit.

Étape 2. Il est clair que $\mathbb{Z}_{\mathbb{K}_n}$ contient $\mathbb{Z}_{\mathbb{K}}[\omega_n]$. Le lemme 10 entraîne l'inclusion

$$(1) \qquad n\mathbb{Z}_{\mathbb{K}_n} \subset \mathbb{Z}_{\mathbb{K}}[\omega_n].$$[25]

Tout va en découler. Observons déjà que le cas où $n = p^m$ avec $p \in \mathcal{P}$ et $m \in \mathbb{N}^*$ est immédiat au vu de (1) et du théorème 7.

Étape 3. Compte-tenu de la fin de l'étape 2, il suffit pour conclure d'établir le résultat de stabilité ci-après.

Lemme 11. *Soient $\mathbb{K}$ un corps de nombres, $\Lambda_{\mathbb{K}}$ l'ensemble des éléments n de $\mathbb{N}^*$ tels que : $\mathbb{Z}_{\mathbb{K}_n} = \mathbb{Z}_{\mathbb{K}}[\omega_n]$. Si m et n sont deux éléments premiers entre eux de $\Lambda_{\mathbb{K}}$, mn est dans $\Lambda_{\mathbb{K}}$.*

Preuve. En appliquant la relation (1) à $\mathbb{K}_m$, on a :

$$n\mathcal{O}_{\mathbb{K}_{mn}} \subset \mathcal{O}_{\mathbb{K}_m}[\omega_n] = \mathcal{O}_{\mathbb{K}}[\omega_m,\omega_n] = \mathcal{O}_{\mathbb{K}}[\omega_{mn}].$$

Symétriquement :

$$m\mathbb{Z}_{\mathbb{K}_{mn}} \subset \mathbb{Z}_{\mathbb{K}}[\omega_{mn}].$$

Une relation de Bézout permet de conclure que $\mathbb{Z}_{\mathbb{K}_{mn}}$ est contenu dans $\mathcal{O}_{\mathbb{K}}[\omega_{mn}]$.

Exercice 76. ③ *Soient $n \ge 3$ un entier, $\omega = \omega_n$, $c = 2\cos\left(\dfrac{2\pi}{n}\right)$, $m = \dfrac{\varphi(n)}{2}$, $\mathbb{K} = \mathbb{Q}(c)$.*

a) Montrer que $(\omega^{\pm k})_{1\le k\le m}$ est une $\mathbb{Z}$-base de $\mathbb{Z}[\omega]$.

b) Montrer que $(\omega^k)_{1\le k\le m}$ est une $\mathbb{Z}$-base de $\mathbb{Z}_{\mathbb{K}}$.

c) Montrer que $\mathbb{Z}_{\mathbb{K}} = \mathbb{Z}[c]$.

Exercice 77. ① *Pour $n \in \mathbb{N}^*$, calculer le discriminant de $\mathbb{Q}(\omega_n)$ (chapitre* **1***, 4.3, exercice 72).*

---

24. Ce résultat, vient de la relation suivante, valable pour $n \in \mathbb{N}^*$ et $m \in \mathbb{Z}$: $\displaystyle\sum_{\omega\in\mathbb{U}_n} \omega^m = n1_{n|m}$ (formule d'inversion de Fourier sur le groupe cyclique $\mathbb{U}_n$).

25. Renseignement plus précis que ce que donnerait le théorème 6 de **7.1**