THÉORIE DE GALOIS

par

Vincent Sécherre

Introduction

La théorie de Galois naît, vers la fin des années 1820, de la résolution par Evariste Galois (1811-1832) du problème suivant : *étant donné un polynôme f à coefficients rationnels, de degré $d \geqslant 1$, qu'on écrit sous la forme :*

$$f = a_0 + a_1 \mathrm{X} + \cdots + a_d \mathrm{X}^d,$$

peut-on résoudre l'équation $f = 0$ par radicaux ? Ce qui signifie en gros : existe-t-il des formules exprimant les d racines complexes de f en fonction de ses coefficients $a_0, a_1, \ldots, a_d$ n'impliquant, outre les opérations élémentaires $+$ et $\times$, que des radicaux $z \mapsto z^{1/n}$ avec $n \geqslant 2$? Pour $d = 2$, on a l'expression célèbre :

$$\frac{-a_1 \pm (a_1^2 - 4a_0a_2)^{1/2}}{2a_2}$$

donnant les solutions d'une équation du second degré, et il existe des formules analogues, quoique sensiblement plus compliquées, pour $d = 3$ et $d = 4$. Lorsque $d \geqslant 5$, la réponse de Galois est : il n'existe pas de formule *générale*, c'est-à-dire de formule qui serait valable pour *tous* les polynômes de degré d.

L'argument – ou plutôt la théorie – de Galois est révolutionnaire : il s'agit du premier exemple de dictionnaire entre deux théories, en l'occurrence la théorie des corps et la théorie des groupes. Ce n'est pas un dictionnaire parfait, c'est-à-dire qu'il ne concerne pas n'importe quel corps ni n'importe quel groupe, et surtout c'est une théorie *relative* : elle ne concerne pas les corps en tant que tels mais les *extensions* d'un corps fixé. Le principe est d'associer au polynôme f un sous-groupe $\mathrm{G}(f)$ du groupe des permutations des d racines complexes de f : en langage moderne, il s'agit du groupe des automorphismes du corps $\mathbf{Q}(f) = \mathbf{Q}(f^{-1}(0))$ engendré par les racines complexes de f. Galois prouve que les sous-corps de $\mathbf{Q}(f)$ sont en correspondance bijective avec les sous-groupes de $\mathrm{G}(f)$. C'est ce qu'on appelle la *correspondance de Galois*.

Si l'équation *générale* du d-ième degré n'est pas résoluble par radicaux, certaines équations particulières, comme $X^d = 0$, sont évidemment résolubles, et ce quelque soit la valeur de d. On aimerait donc avoir un critère, portant sur f, permettant de décider dans quels cas l'équation $f = 0$ est résoluble par radicaux. La correspondance de Galois permet de traduire la question dans des termes de la théorie des groupes, ce qui donne le critère suivant : l'équation $f = 0$ est résoluble par radicaux si et seulement s'il existe une suite finie décroissante :

$$G(f) = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

de sous-groupes de $G(f)$ tels que, pour tout $i \geqslant 0$, d'une part G_{i+1} soit distingué dans G_i, d'autre part le groupe quotient G_i/G_{i+1} soit cyclique.

Depuis sa création il y a près de deux siècles, la théorie de Galois qui n'était, à l'origine, qu'un *moyen* de résoudre un problème donné est devenu une théorie jouant un rôle important dans plusieurs domaines des mathématiques. Mentionnons quelques théories qui y sont reliées :

(1) La théorie de Galois classique des extensions finies d'un corps quelconque — qui fait l'objet de ce cours — dont le but est la correspondance de Galois entre sous-extensions d'une extension finie galoisienne K/k et sous-groupes du groupe de Galois $\mathrm{Gal}(K/k)$.

(2) F. Klein (et d'autres) a montré que, si l'on affaiblit le sens que l'on donne à *résoluble* et que, outre $+, \times$ et les radicaux $z \mapsto z^{1/n}$, on autorise l'usage d'une certaine fonction σ dite *elliptique*, l'équation générale du cinquième degré devient résoluble.

(3) La théorie des revêtements galoisiens (due à H. Poincaré), dans laquelle l'extension finie galoisienne K/k est remplacée par un revêtement fini galoisien $X \to B$ d'espace topologique et le groupe de Galois $\mathrm{Gal}(K/k)$ par le groupe fondamental $\pi_1(B, b_0)$; on a une correspondance bijective entre sous-revêtements de $X \to B$ et sous-groupes du groupe fondamental $\pi_1(B, b_0)$.

(4) La théorie de Galois différentielle, dans laquelle les polynômes sont remplacés par des équations différentielles linéaires. Les motivations sont analogues à celles qui sont à l'origine de la théorie de Galois classique, notamment la question de la résolubilité d'une équation différentielle au moyen de "fonctions élémentaires".

(5) La reformulation récente (années 1960) par A. Grothendieck de la théorie de Galois dans le langage de la théorie des catégories, qui a permis l'unification des points de vue algébrique (extensions de corps) et géométrique (revêtements).

Références bibliographiques

1. Calais J., *Extensions de corps, théorie de Galois*, Ellipses, 2006.
2. Chambert-Loir A., *Algèbre corporelle*, disponible à l'adresse :
   `http://www.math.polytechnique.fr/~chambert/`
3. Escofier J.-P., *Théorie de Galois*, Dunod, 2000.
4. Gozard I., *Théorie de Galois*, Ellipses, 1997.
5. Morandi P., *Field and Galois theory*, GTM 167, Springer, 1996.
6. Tauvel P., *Corps commutatifs et théorie de Galois*, Calvage et Mounet, 2008.

Théories galoisiennes et équation du cinquième degré

7. Douady R. et A., *Algèbre et théories galoisiennes*, Cassini, 2005.
8. Pommaret J.-F., *Differential Galois theory*, Gordon and Breach, 1983.
9. Klein F., *Lectures on the icosahedron and the solution of equations of the fifth degree*, Dover, 1956.

Chapitre 1. Anneaux et algèbres

Avertissement : *Dans ce cours, tous les anneaux sont supposés commutatifs.*

1.1. Un *anneau* est un ensemble A muni de deux lois internes $+$ et $\times$ vérifiant les conditions suivantes :

(1) le couple $(\mathrm{A}, +)$ est un groupe commutatif, d'élément neutre noté 0_A ;
(2) la loi $\times$ est associative, commutative et distributive par rapport à la loi $+$, et possède un élément neutre noté 1_A.

Le plus souvent, le symbole $\times$ est omis, c'est-à-dire que, pour $a, a' \in \mathrm{A}$, on note aa' plutôt que $a \times a'$.

Exemple 1.1. — (i) Les anneaux $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ et $\mathbf{Z}/n\mathbf{Z}$ pour $n \geqslant 1$.
(ii) Un anneau A est dit *nul* lorsque $0_\mathrm{A} = 1_\mathrm{A}$, auquel cas on a $\mathrm{A} = \{0_\mathrm{A}\}$.

Un *sous-anneau* de A est un sous-ensemble de A contenant 1_A, stable par $+$ et par $\times$ et qui est un anneau pour ces deux lois.

1.2. Soient A, B des anneaux. Un *homomorphisme d'anneaux* de A vers B est une application $\varphi : \mathrm{A} \to \mathrm{B}$ vérifiant les conditions suivantes :

(1) pour tous $a, a' \in \mathrm{A}$, on a $\varphi(a + a') = \varphi(a) + \varphi(a')$ et $\varphi(aa') = \varphi(a)\varphi(a')$;
(2) on a $\varphi(1_\mathrm{A}) = 1_\mathrm{B}$.

Un *isomorphisme* d'anneaux est un homomorphisme d'anneaux bijectif. Sa bijection réciproque est un homomorphisme d'anneaux.

L'*image* d'un homomorphisme φ est l'ensemble $\{\varphi(a) \mid a \in \mathrm{A}\}$. C'est un sous-anneau de B, noté $\mathrm{Im}(\varphi)$.

Le *noyau* de φ est l'ensemble $\{a \in \mathrm{A} \mid \varphi(a) = 0_\mathrm{B}\}$. On le note $\mathrm{Ker}(\varphi)$. Si B n'est pas nul, ce n'est pas un sous-anneau de A (voir §1.4).

1.3. Une *unité* d'un anneau A est un élément $a \in \mathrm{A}$ inversible pour $\times$, c'est-à-dire tel qu'il y ait $b \in \mathrm{A}$ vérifiant $ab = 1_\mathrm{A}$. On note $\mathrm{A}^\times$ l'ensemble des unités de A. Lorsqu'on le munit de la loi $\times$, c'est un groupe, qu'on appelle le *groupe multiplicatif*, ou le groupe des unités, de A.

Exemple 1.2. — (i) $\mathbf{Z}^\times = \{-1, 1\}$ et $\mathbf{Q}^\times = \mathbf{Q} - \{0\}$.
(ii) Pour $n \geqslant 1$, le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ est formé des classes d'entiers premiers à n.

1.4. Soit A un anneau. Un *idéal* de A est un sous-groupe I de A tel que pour tous $a \in \mathrm{A}$ et $x \in \mathrm{I}$, on ait $ax \in \mathrm{I}$. Par exemple, A et $\{0_\mathrm{A}\}$ sont des idéaux de A. Si φ est un homomorphisme d'anneaux de A dans un anneau B, son noyau est un idéal de A. Si un idéal de A contient 1_A, ou plus généralement une unité de A, il est égal à A.

Si I est un idéal de A, deux éléments a, b de A sont dits *équivalents* mod. I si $a - b \in \mathrm{I}$. Il s'agit d'une relation d'équivalence sur A, et on note A/I le quotient de A par cette relation. Il existe sur A/I une unique structure d'anneau faisant de la projection canonique $\mathrm{A} \to \mathrm{A/I}$ un homomorphisme d'anneaux, structure que l'on appelle *anneau-quotient* de A par l'idéal I.

Exemple 1.3. — Pour $n \geqslant 1$, $\mathbf{Z}/n\mathbf{Z}$ est l'anneau-quotient de $\mathbf{Z}$ par l'idéal $n\mathbf{Z}$.

1.5. Soit A un anneau. Un idéal I de A est dit *maximal* si $\mathrm{I} \neq \mathrm{A}$ et si tout idéal $\mathrm{J} \neq \mathrm{A}$ contenant I est égal à I.

Un *corps* est un anneau non nul dont tous les éléments non nuls sont des unités.

Proposition 1.4. — *Un idéal* I *de* A *est maximal si et seulement si* A/I *est un corps.*

Démonstration. — Soit I un idéal maximal de A et soit $\mathrm{K} = \mathrm{A}/\mathrm{I}$. Alors $\mathrm{K} \neq \{0\}$ puisque $\mathrm{I} \neq \mathrm{A}$. Si $x \in \mathrm{K}$ est non nul, et si $b \in x$, l'idéal $\mathrm{I} + \mathrm{A}b$ est égal à A tout entier, de sorte qu'il existe $u \in \mathrm{I}$ et $a \in \mathrm{A}$ tels que $1 = u + ab$. Ainsi $ab \in 1 + \mathrm{I}$, c'est-à-dire que x est inversible dans K.

On suppose maintenant que $\mathrm{K} = \mathrm{A}/\mathrm{I}$ est un corps. Soit J un idéal de A vérifiant $\mathrm{I} \subset \mathrm{J} \subsetneq \mathrm{A}$. Alors J/I est un idéal strict de K ; s'il n'était pas nul, il contiendrait une unité de K, et serait donc égal à K tout entier. Il est donc nul, de sorte que $\mathrm{J} = \mathrm{I}$. □

Exemple 1.5. — Les idéaux maximaux de $\mathbf{Z}$ sont les $p\mathbf{Z}$, avec p premier.

1.6. Soit K un corps, qu'on fixe jusqu'à la fin du chapitre.

Définition 1.6. — Une K-*algèbre* est un ensemble B muni de deux lois internes $+, \times$ et d'une loi externe $\cdot$ vérifiant les conditions suivantes :

(1) le triplet $(\mathrm{B}, +, \times)$ est un anneau ;
(2) le triplet $(\mathrm{B}, +, \cdot)$ est un K-espace vectoriel ;
(3) pour tous $a \in \mathrm{K}$ et $b, b' \in \mathrm{B}$, on a $a \cdot (b \times b') = b \times (a \cdot b')$.

La condition (3) est une condition de compatibilité entre la structure d'anneau et celle d'espace vectoriel ; elle signifie que la loi $\times$ est une application K-bilinéaire. Comme pour les anneaux, le symbole $\times$ est le plus souvent omis. L'application :

$$\iota_{\mathrm{B}} : x \mapsto x \cdot 1_{\mathrm{B}} \tag{1}$$

est un homomorphisme injectif d'anneaux de K dans B, et on a $a \cdot b = \iota_{\mathrm{B}}(a)b$ pour tous $a \in \mathrm{K}$ et $b \in \mathrm{B}$. Il nous arrivera d'omettre $\cdot$ et ι_{B}, c'est-à-dire que $a \cdot b$ et $\iota_{\mathrm{B}}(a)b$ deviendront ab.

Proposition 1.7. — *Soit* B *une* K-*algèbre, et soient* $a, a' \in \mathrm{K}$ *et* $b, b' \in \mathrm{B}$. *On a les propriétés suivantes :*

(1) $a \cdot 0_{\mathrm{B}} = 0_{\mathrm{K}} \cdot b = 0_{\mathrm{B}}$ *et* $1_{\mathrm{K}} \cdot b = b$.
(2) $(a + a') \cdot b = a \cdot b + a' \cdot b$ *et* $(aa') \cdot b = a \cdot (a' \cdot b)$.
(3) $a \cdot (b + b') = a \cdot b + a \cdot b'$ *et* $a \cdot (bb') = b(a \cdot b')$.

Une *sous*-K-*algèbre* de B est un sous-ensemble de B qui en est à la fois un sous-anneau et un sous-espace vectoriel. Si $(\mathrm{C}_i)_{i \in \mathrm{I}}$ est une famille de sous-K-algèbres de B indexées par un ensemble I, l'intersection $\bigcap_{i \in \mathrm{I}} \mathrm{C}_i$ est une sous-K-algèbre de B. Si S est une partie de B, l'intersection de toutes les sous-K-algèbres de B contenant S est donc une sous-K-algèbre de B, dite *engendrée* par S, et on la note K[S]. C'est la plus petite sous-K-algèbre de B contenant S.

1.7. Soient B et B′ deux K-algèbres. Un *homomorphisme de* K-*algèbres* de B vers B′ est une application $\varphi : \mathrm{B} \to \mathrm{B}'$ qui est un homomorphisme à la fois d'anneaux et de K-espaces vectoriels. Par conséquent, un tel homomorphisme vérifie la relation $\varphi \circ \iota_{\mathrm{B}} = \iota_{\mathrm{B}'}$.

1.8. Si B est une K-algèbre et I un idéal de B, il existe sur B/I une unique structure d'anneau faisant de la projection canonique $\mathrm{B} \to \mathrm{B}/\mathrm{I}$ un homomorphisme de K-algèbres, structure que l'on appelle K-*algèbre-quotient* de B par l'idéal I.

Chapitre 2. Polynômes

Dans tout ce chapitre, on fixe un corps (commutatif) K.

2.1. Une suite $(a_n)_{n\in\mathbf{N}}$ d'éléments de K est dite *presque nulle* s'il existe un entier $n_0 \geqslant 1$ tel que $a_n = 0_{\mathrm{K}}$ pour tout $n \geqslant n_0$. On note $\mathrm{K}^{(\mathbf{N})}$ l'ensemble des suites presque nulles d'éléments de K, muni des deux lois $+$ et $*$ définies par :

$$\begin{aligned}(a+b)_n &= a_n + b_n,\\ (a*b)_n &= \sum_{k=0}^{n} a_k b_{n-k} = a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0.\end{aligned}$$

On définit une loi externe de $\mathrm{K}\times\mathrm{K}^{(\mathbf{N})}$ dans $\mathrm{K}^{(\mathbf{N})}$ par $(x\cdot a)_n = xa_n$ pour $x\in\mathrm{K}$ et $a\in\mathrm{K}^{(\mathbf{N})}$.

Théorème 2.1. — *L'ensemble* $\mathrm{K}^{(\mathbf{N})}$ *muni des deux lois internes* $+$ *et* $*$ *et de la loi externe* $\cdot$ *est une* K*-algèbre dont les éléments neutres sont* $0_{\mathrm{K}^{(\mathbf{N})}} = (0,0,\ldots)$ *et* $1_{\mathrm{K}^{(\mathbf{N})}} = (1,0,0,\ldots)$.

Cette K-algèbre est appelée l'*algèbre des polynômes à coefficients dans* K. Traditionnellement, la suite presque nulle $(0,1,0,0,\ldots)$ est notée X, auquel cas $\mathrm{K}^{(\mathbf{N})}$ est notée K[X]. (Cette notation est cohérente avec celle du §1.6 car K[X] est engendrée par X sur K.) Une suite presque nulle $(a_n)_{n\in\mathbf{N}}$ sera alors notée :

$$a_0 + a_1\mathrm{X} + a_2\mathrm{X}^2 + \ldots \tag{2}$$

2.2. Soit $f\in\mathrm{K}[\mathrm{X}]$ non nul écrit comme en (2). Le plus grand entier $n\geqslant 0$ tel qu'on ait $a_n\neq 0_{\mathrm{K}}$ est appelé le *degré* de f. On le note $\deg(f)$. Par convention, on décide que le degré du polynôme nul est $-\infty$.

Proposition 2.2. — *Soient* $f,g\in\mathrm{K}[\mathrm{X}]$. *On a :*

$$\begin{aligned}\deg(f+g) &\leqslant \max\{\deg(f),\deg(g)\},\\ \deg(fg) &= \deg(f)+\deg(g).\end{aligned}$$

Soit $f\in\mathrm{K}[\mathrm{X}]$ non nul, et soit n son degré. Le coefficient a_n est appelé le *coefficient dominant* de f. Par définition, il n'est jamais nul.

2.3. On a le résultat très important suivant, qui affirme que l'anneau K[X] est euclidien.

Théorème 2.3. — *Soient* $f,g\in\mathrm{K}[\mathrm{X}]$ *des polynômes avec* $g\neq 0$. *Il existe un unique couple* $(\mathrm{Q},\mathrm{R})\in\mathrm{K}[\mathrm{X}]\times\mathrm{K}[\mathrm{X}]$ *vérifiant* $f = \mathrm{Q}g + \mathrm{R}$ *et* $\deg(\mathrm{R}) < \deg(g)$.

Démonstration. — Pour l'unicité, si (Q,R) et $(\mathrm{Q}_1,\mathrm{R}_1)$ sont solutions, on écrit :

$$(\mathrm{Q}-\mathrm{Q}_1)g = \mathrm{R}_1 - \mathrm{R}.$$

Puisque le coefficient dominant de g n'est pas nul, on trouve, en prenant le degré de cette égalité :

$$\deg(\mathrm{Q}-\mathrm{Q}_1) + \deg(g) < \deg(g).$$

On en déduit que $\mathrm{Q}_1 = \mathrm{Q}$, puis que $\mathrm{R}_1 = \mathrm{R}$.

Pour l'existence, on procède par récurrence sur le degré de f. Si $\deg(f) < \deg(g)$, il suffit de prendre $\mathrm{Q} = 0$ et $\mathrm{R} = f$. Sinon, soient m le degré de f et n celui de g. On écrit :

$$f = a_0 + a_1\mathrm{X} + a_2\mathrm{X}^2 + \ldots + a_m\mathrm{X}^m,\quad g = b_0 + b_1\mathrm{X} + b_2\mathrm{X}^2 + \ldots + b_n\mathrm{X}^n.$$

Le polynôme $f_1 = f - a_m b_n^{-1} \mathrm{X}^{m-n} g$ est de degré strictement inférieur à m, de sorte qu'on peut lui appliquer l'hypothèse de récurrence. On trouve un couple $(\mathrm{Q}_1, \mathrm{R}_1)$ convenant à f_1 et g. Alors les polynômes $\mathrm{Q} = \mathrm{Q}_1 + a_m b_n^{-1} \mathrm{X}^{m-n} g$ et $\mathrm{R} = \mathrm{R}_1$ conviennent à f et g. □

2.4. Le résultat suivant est aussi très important pour la suite du cours.

Proposition 2.4. — *L'anneau* $\mathrm{K}[\mathrm{X}]$ *est principal.*

Démonstration. — Soient I un idéal non nul de K[X] et P un élément de degré minimal parmi les éléments non nuls de I. Si $f \in \mathrm{I}$, on lui applique la division euclidienne par P (corollaire 2.3). On obtient $f = \mathrm{QP} + \mathrm{R}$, avec $\deg(\mathrm{R}) < \deg(\mathrm{P})$. On a $\mathrm{R} = f - \mathrm{QP} \in \mathrm{I}$. Pour ne pas contredire la minimalité de P, la seule possibilité est que $\mathrm{R} = 0$, ce dont on déduit que I est l'idéal principal engendré par P. □

2.5. Un polynôme $f \in \mathrm{K}[\mathrm{X}]$ est dit *irréductible* s'il n'est pas une unité et si toute égalité de la forme $f = \mathrm{PQ}$ implique que ou bien P, ou bien Q, est une unité de K[X].

Proposition 2.5. — (1) *Un polynôme* $f \in \mathrm{K}[\mathrm{X}]$ *est une unité si et seulement* $\deg(f) = 0$.

(2) *Un polynôme* $f \in \mathrm{K}[\mathrm{X}]$ *est irréductible s'il est de degré* $\geqslant 1$*, et si toute égalité de la forme* $f = \mathrm{PQ}$ *implique que soit* P*, soit* Q*, est de degré* 0.

(3) *Un polynôme* $f \in \mathrm{K}[\mathrm{X}]$ *est irréductible si et seulement si l'idéal principal* (f) *est maximal.*

En d'autres termes, $f \in \mathrm{K}[\mathrm{X}]$ est irréductible s'il est de degré $\geqslant 1$, et s'il ne possède pas de diviseur de degré strictement compris entre 0 et $\deg(f)$.

Corollaire 2.6. — *Tout polynôme* $f \in \mathrm{K}[\mathrm{X}]$ *de degré* $\geqslant 1$ *a un facteur irréductible dans* $\mathrm{K}[\mathrm{X}]$.

Démonstration. — On procède par récurrence sur le degré de f. Si f est irréductible, il n'y a rien à faire. Sinon, l'idéal (f) n'est pas maximal, c'est-à-dire qu'il existe un idéal I de K[X] non trivial et contenant strictement (f). Puisque K[X] est principal, il existe $g \in \mathrm{K}[\mathrm{X}]$ tel que $\mathrm{I} = (g)$. Par hypothèse de récurrence, le polynôme g, qui est de degré strictement moindre que celui de f, a un facteur irréductible dans K[X], donc f aussi. □

Corollaire 2.7. — *Tout polynôme* $f \in \mathrm{K}[\mathrm{X}]$ *de degré* $\geqslant 1$ *se décompose sous la forme d'un produit de facteurs irréductibles dans* $\mathrm{K}[\mathrm{X}]$*, et une telle décomposition est unique à l'ordre des facteurs près.*

Démonstration. — L'existence s'obtient là encore par récurrence sur le degré de f. Pour l'unicité, soient $\mathrm{P}_1, \dots, \mathrm{P}_r$ et $\mathrm{Q}_1, \dots, \mathrm{Q}_s$ des polynômes irréductibles de K[X] tels que :

$$f = \mathrm{P}_1 \dots \mathrm{P}_r = \mathrm{Q}_1 \dots \mathrm{Q}_s. \tag{3}$$

Supposons, pour fixer les idées, que $r \geqslant s$. Puisque Q_1 divise le produit $\mathrm{P}_1 \dots \mathrm{P}_r$, et puisque l'idéal (Q_1) est maximal (voir la proposition 2.5), Q_1 divise l'un des P_i, donc lui est égal à une unité près. Puisque K[X] est intègre, on peut simplifier les deux membres par Q_1. De proche en proche, on obtient $r - s$ facteurs P_i dont le produit est égal à 1. On a donc $r = s$ et, à permutation près, on a $\mathrm{Q}_i = \mathrm{P}_i$. □

Exemple 2.8. — (i) Tout polynôme de degré 1 est irréductible.

(ii) Un polynôme $a\mathrm{X}^2 + b\mathrm{X} + c$ de degré 2 est irréductible si, et seulement si son discriminant $b^2 - 4ac$ n'est pas un carré dans K.

(iii) Un polynôme de degré $\leqslant 3$ est irréductible si et seulement s'il n'a pas de racine dans K.

Exemple 2.9. — (i) Un polynôme de $\mathbf{C}[X]$ est irréductible si et seulement s'il est de degré 1. (Cela équivaut à dire que le corps $\mathbf{C}$ est algébriquement clos : voir le §3.7.)

(ii) Un polynôme de $\mathbf{R}[X]$ est irréductible si et seulement s'il est ou bien de degré 1, ou bien de degré 2 avec un discriminant < 0.

(iii) Le polynôme $X^4 + 1$ est réductible sur $\mathbf{R}$, bien qu'il n'ait pas de racine réelle, comme le montre l'égalité :

$$X^4 + 1 = (X^4 + 2X^2 + 1) - 2X^2 = (X^2 + 1 + \sqrt{2}X)(X^2 + 1 - \sqrt{2}X).$$

(iv) Le polynôme $X^2 + X + 1$ est le seul polynôme irréductible de degré 2 sur $\mathbf{Z}/2\mathbf{Z}$.

2.6. Soit B une K-algèbre.

Proposition 2.10. — *L'application* $\mathrm{Hom}_K(K[X], B) \to B$ *définie par* $\varphi \mapsto \varphi(X)$ *est une bijection.*

Démonstration. — Ecrivons un polynôme $f \in K[X]$ sous la forme (2). L'injectivité provient de la formule :

$$\varphi(f) = a_0 + a_1\varphi(X) + a_2\varphi(X)^2 + \dots \tag{4}$$

et la surjectivité du fait qu'à $b \in K$ on fait correspondre l'application φ_b défini par :

$$\varphi_b(f) = a_0 + a_1 b + a_2 b^2 + \dots \tag{5}$$

dont on vérifie que c'est bien un homomorphisme de K-algèbres. □

Cette proposition peut être reformulée de la façon suivante. Soit B un anneau et soit φ un homomorphisme d'anneaux de K dans B. Pour tout $b \in B$, il existe un unique homomorphisme d'anneaux $\varphi_b : K[X] \to B$ prolongeant φ et tel que $\varphi_b(X) = b$.

2.7. Pour $f \in K[X]$ et $b \in B$, on note (f) l'idéal de $K[X]$ engendré par f et on introduit les notations suivantes :

$$\begin{aligned} K_f &= K[X]/(f) \\ f(b) &= \varphi_b(f) \\ \mathrm{Spec}_B(f) &= \{b \in B \mid f(b) = 0_B\}. \end{aligned}$$

L'élément $f(b) \in B$ est la *valeur* de f au point b, et $\mathrm{Spec}_B(f)$ est l'ensemble des *racines de* f *dans* B. Pour tout $\varphi \in \mathrm{Hom}_K(K[X], B)$, la formule (4) se traduit dans ces nouvelles notations sous la forme : $\varphi(f) = f(\varphi(X))$.

Proposition 2.11. — *Soient* $f \in K[X]$ *et* $b \in K$. *Alors* $f(b) = 0$ *si et seulement si* $X - b$ *divise* f.

Démonstration. — On effectue la division euclidienne de f par $X - b$, de sorte qu'on obtient $f = (X - b)Q + R$, où R est de degré $\leqslant 0$, c'est-à-dire un élément de K. En appliquant φ_b, on trouve $R = f(b)$, ce qui termine la démonstration. □

La proposition 2.11 peut se reformuler de la façon suivante : le noyau de φ_b est égal à l'idéal $(X - b)$ engendré par $X - b$.

Corollaire 2.12. — *Si* f *est non nul, alors* $\mathrm{Spec}_K(f)$ *est de cardinal* $\leqslant \deg(f)$.

Démonstration. — On procède par récurrence sur le degré de f. Si $\mathrm{Spec}_{\mathrm{K}}(f)$ est vide, il n'y a rien à prouver. Sinon, on choisit $b \in \mathrm{Spec}_{\mathrm{K}}(f)$ et on écrit $f = (\mathrm{X} - b)g$. Le polynôme $g \in \mathrm{K}[\mathrm{X}]$ est de degré strictement moindre que celui de f, de sorte que, par hypothèse de récurrence, l'ensemble $\mathrm{Spec}_{\mathrm{K}}(g)$ est de cardinal $\leqslant \deg(g)$. On a :

$$\mathrm{Spec}_{\mathrm{K}}(f) = \{b\} \cup \mathrm{Spec}_{\mathrm{K}}(g),$$

c'est-à-dire que le cardinal de $\mathrm{Spec}_{\mathrm{K}}(f)$ est majoré par $1 + \mathrm{card}(\mathrm{Spec}_{\mathrm{K}}(g))$, donc par $\deg(f)$. Ceci met fin à la démonstration. □

2.8. On note π_f la projection canonique de $\mathrm{K}[\mathrm{X}]$ sur K_f, et on pose $x = \pi_f(\mathrm{X})$.

Lemme 2.13. — *x est une racine de f dans K_f.*

Démonstration. — C'est une conséquence de l'égalité $f(\pi_f(\mathrm{X})) = \pi_f(f)$ ou, si l'on préfère, du fait que $\varphi_x \in \mathrm{Hom}_{\mathrm{K}}(\mathrm{K}[\mathrm{X}], \mathrm{K}_f)$ est égal à π_f. □

Le résultat suivant généralise la proposition 2.10.

Proposition 2.14. — *Soit $f \in \mathrm{K}[\mathrm{X}]$. Alors l'application $\mathrm{Hom}_{\mathrm{K}}(\mathrm{K}_f, \mathrm{B}) \to \mathrm{Spec}_{\mathrm{B}}(f)$ définie par $\varphi \mapsto \varphi(x)$ est une bijection.*

Démonstration. — Avant tout, on vérifie que cette application est bien définie. Tout homomorphisme $\varphi \in \mathrm{Hom}_{\mathrm{K}}(\mathrm{K}_f, \mathrm{B})$ définit un homomorphisme de K-algèbres $\varphi^* = \varphi \circ \pi_f$ de $\mathrm{K}[\mathrm{X}]$ dans B. On a :

$$f(\varphi(x)) = f(\varphi^*(\mathrm{X})) = \varphi^*(f) = 0_{\mathrm{B}},$$

ce qui signifie que $\varphi(x) \in \mathrm{Spec}_{\mathrm{B}}(f)$.

Pour l'injectivité, il suffit de vérifier que l'application $\varphi \mapsto \varphi^*$ est injective. Pour la surjectivité, soit $\varphi_b \in \mathrm{Hom}_{\mathrm{K}}(\mathrm{K}[\mathrm{X}], \mathrm{B})$ l'homomorphisme associé à la racine $b \in \mathrm{Spec}_{\mathrm{B}}(f)$. Comme (f) est inclus dans $\mathrm{Ker}(\varphi_b)$, il s'agit de voir que φ_b s'écrit $\varphi \circ \pi_f$, avec $\varphi \in \mathrm{Hom}_{\mathrm{K}}(\mathrm{K}_f, \mathrm{B})$, et que φ est un antécédent de b. □

Exemple 2.15. — En choisissant $f = \mathrm{X}$, on obtient $\mathrm{Spec}_{\mathrm{B}}(f) = \{0_{\mathrm{B}}\}$ et $\mathrm{K}_f = \mathrm{K}$ donc on a $\mathrm{Hom}_{\mathrm{K}}(\mathrm{K}, \mathrm{B}) = \{\iota_{\mathrm{B}}\}$.

Chapitre 3. Extensions de corps

Dans tout ce chapitre, on fixe un corps (commutatif) K.

3.1. Une *extension* de K, ou encore une K-extension, est une K-algèbre dont l'anneau sous-jacent est un corps.

Remarque 3.1. — Si L est une extension de K, les corps K et L ont même caractéristique.

Si L est un corps et si $\iota : \mathrm{K} \to \mathrm{L}$ est un homomorphisme d'anneaux, on note L_ι l'extension de K définie par :

(1) l'anneau sous-jacent à L_ι est L ;
(2) la structure de K-espace vectoriel sur L_ι est donnée par $(a, b) \mapsto \iota(a)b$.

Les applications $\iota \mapsto \mathrm{L}_\iota$ et $\mathrm{B} \mapsto \iota_\mathrm{B}$ sont des bijections réciproques entre $\mathrm{Hom}(\mathrm{K}, \mathrm{L})$ et l'ensemble des K-extensions d'anneau sous-jacent L.

Remarque 3.2. — (1) Si K est un sous-corps de L, la structure *naturelle* de K-extension sur L est celle qui correspond à l'homomorphisme $\iota(x) = x$ pour $x \in \mathrm{K}$.
(2) Le corps K n'est pas toujours contenu dans L : voir la proposition 3.4.

Exemple 3.3. — (i) Si L est de caractéristique nulle, il existe un unique homomorphisme d'anneaux de $\mathbf{Q}$ dans L, ce qui fait de L une extension de $\mathbf{Q}$.
(ii) Si L est de caractéristique p, il existe un unique homomorphisme d'anneaux de $\mathbf{Z}/p\mathbf{Z}$ dans L, ce qui fait de L une extension de $\mathbf{Z}/p\mathbf{Z}$.

Proposition 3.4. — *Soit $f \in \mathrm{K}[\mathrm{X}]$. Les assertions suivantes sont équivalentes :*
(1) $\mathrm{K}_f = \mathrm{K}[\mathrm{X}]/(f)$ *est une extension de* K *pour le morphisme* $\mathrm{K} \to \mathrm{K}[\mathrm{X}] \to \mathrm{K}_f$.
(2) K_f *est un corps.*
(3) f *est irréductible sur* K.

Démonstration. — C'est une conséquence de la proposition 2.5. □

3.2. Soit L une extension de K. Une *sous-extension* de L (sur K) est une sous-K-algèbre de L qui est un corps.

Si $(\mathrm{L}_i)_{i\in\mathrm{I}}$ est une famille de sous-extensions de L sur K indexées par I, l'intersection $\bigcap_{i\in\mathrm{I}} \mathrm{L}_i$ est une sous-extension de L sur K.

Si S est une partie de L, l'intersection de toutes les sous-extensions de L sur K contenant S est donc une sous-extension de L sur K, dite *engendrée* par S sur K, et on la note K(S). C'est la plus petite sous-extension de L sur K contenant S.

Proposition 3.5. — *Soient* S, S' *des partie de* L. *Alors on a :*

$$\mathrm{K}(\mathrm{S})(\mathrm{S}') = \mathrm{K}(\mathrm{S}')(\mathrm{S}) = \mathrm{K}(\mathrm{S} \cup \mathrm{S}').$$

Démonstration. — On pose $\mathrm{C} = \mathrm{K}(\mathrm{S})$. Comme $\mathrm{D} = \mathrm{K}(\mathrm{S} \cup \mathrm{S}')$ est une sous-extension de L sur K contenant S, elle contient C, donc c'est une sous-extension de L sur C. Comme elle contient également S', elle contient $\mathrm{C}(\mathrm{S}')$. Inversement, comme $\mathrm{K}(\mathrm{S})(\mathrm{S}')$ est une sous-extension contenant $\mathrm{S} \cup \mathrm{S}'$, elle contient $\mathrm{K}(\mathrm{S} \cup \mathrm{S}')$, ce qui termine la démonstration. □

Remarque 3.6. — Ne pas confondre K(S), la sous-extension de L engendrée par S, avec K[S], la sous-algèbre de L engendrée par S.

3.3. Soit L une extension de K. Lorsque L, considéré comme un espace vectoriel sur K, est de dimension finie (auquel cas l'extension est dite *finie*), cette dimension est notée $[\mathrm{L} : \mathrm{K}]$ et appelée le *degré* de L (sur K). Si M est une extension de L, alors c'est une extension de K obtenue en composant les morphismes $\mathrm{K} \to \mathrm{L}$ et $\mathrm{L} \to \mathrm{M}$.

Proposition 3.7. — *Si* M *est finie sur* K*, alors elle est finie sur* L *et* L *est finie sur* K*, et :*

$$[\mathrm{M} : \mathrm{K}] = [\mathrm{M} : \mathrm{L}] \cdot [\mathrm{L} : \mathrm{K}]. \tag{6}$$

Inversement, si M *est finie sur* L *et si* L *est finie sur* K*, alors* M *est finie sur* K *et on a* (6)*.*

Exemple 3.8. — Si $f \in \mathrm{K}[\mathrm{X}]$ est irréductible, K_f est finie sur K et de degré $\deg f$.

3.4. Soient L une extension de K et $\alpha \in \mathrm{L}$. Il existe un unique homomorphisme de K-algèbres de K[X] dans L envoyant X sur α (Proposition 2.10) et on le note φ_α. Son image, notée $\mathrm{K}[\alpha]$, est la sous-K-algèbre de L engendrée par α, qu'il ne faut pas confondre avec $\mathrm{K}(\alpha)$, la sous-extension de L sur K engendrée par α qui, en plus d'être une K-algèbre, est un corps. On a donc l'inclusion $\mathrm{K}[\alpha] \subseteq \mathrm{K}(\alpha)$.

Définition 3.9. — On dit que α est *algébrique* sur K si le noyau de φ_α est non nul, c'est-à-dire s'il existe un polynôme non nul $f \in \mathrm{K}[\mathrm{X}]$ tel que $f(\alpha) = 0$.

Proposition 3.10. — *Soit* $\alpha \in \mathrm{L}$ *algébrique sur* K*.*

(1) *La* K*-algèbre* $\mathrm{K}[\alpha]$ *est un corps, c'est-à-dire que* $\mathrm{K}[\alpha] = \mathrm{K}(\alpha)$*.*
(2) *Il existe un unique polynôme unitaire sur* K *engendrant* $\mathrm{Ker}(\varphi_\alpha)$*. On le note :*

$$\mathrm{Pmin}_{\mathrm{K}}(\alpha)$$

et on l'appelle le polynôme minimal de α sur K*.*

(3) *Le polynôme minimal* $\mathrm{P} = \mathrm{Pmin}_{\mathrm{K}}(\alpha)$ *est irréductible sur* K*, et on a un isomorphisme de* K*-algèbres entre* K_{P} *et* $\mathrm{K}(\alpha)$*.*

Corollaire 3.11. — *Soit* $\alpha \in \mathrm{L}$ *algébrique sur* K *et soit* $\mathrm{P} = \mathrm{Pmin}_{\mathrm{K}}(\alpha)$*.*

(1) *Pour tout* $f \in \mathrm{K}[\mathrm{X}]$*, on a* $f(\alpha) = 0$ *si et seulement si* P *divise* f*.*
(2) $\mathrm{K}(\alpha)$ *est une extension finie de* K *de degré* $\deg \mathrm{P}$*, qu'on appelle le* degré de α sur K*.*

Exemple 3.12. — $\sqrt{2}$ est racine de $\mathrm{X}^2 - 2$, et i est racine de $\mathrm{X}^2 + 1$, et $\sqrt[3]{7 + \sqrt{5}}$ est racine de $\mathrm{X}^6 - 14\mathrm{X}^3 + 44$.

Exemple 3.13. — Les éléments de L qui sont algébriques et de degré 1 sur K sont exactement les éléments de $\iota_{\mathrm{L}}(\mathrm{K})$.

Remarque 3.14. — Si E est une sous-extension de L sur K, alors tout élément de L algébrique sur K est algébrique sur E.

Remarque 3.15. — On dit que α est *transcendant* sur K s'il n'est pas algébrique sur K. Dans ce cas, les K-algèbres $\mathrm{K}[\alpha]$ et K[X] sont isomorphes, et $\mathrm{K}[\alpha]$ est strictement incluse dans $\mathrm{K}(\alpha)$. Sinon, on aurait $\alpha^{-1} = f(\alpha)$ pour un $f \in \mathrm{K}[\mathrm{X}]$, et le polynôme $\mathrm{X}f(\mathrm{X}) - 1$ appartiendrait au noyau de φ_α.

On peut prouver que l'ensemble des nombres complexes algébriques sur $\mathbf{Q}$ est dénombrable, tandis que celui des nombres complexes transcendants sur $\mathbf{Q}$ a la puissance du continu (c'est-à-dire qu'il est équipotent à $\mathbf{R}$). Pourtant, il est difficile en pratique de prouver qu'un nombre

donné est transcendant : voir Hermite pour la transcendance de e sur $\mathbf{Q}$, ainsi que Lindemann pour la transcendance de π sur $\mathbf{Q}$.

3.5. Une extension L de K est dite *algébrique* si tous les éléments de L sont algébriques sur K, et *transcendante* dans le cas contraire. Une extension finie est algébrique. La réciproque est fausse.

Proposition 3.16. — *Soit* $\alpha \in \mathrm{L}$. *L'extension* $\mathrm{K}(\alpha)$ *est finie sur* K *si, et seulement si* α *est algébrique sur* K.

Démonstration. — Si α est algébrique sur K, c'est une conséquence du corollaire 3.11. Inversement, si l'extension $\mathrm{K}(\alpha)$ est finie sur K, alors l'homomorphisme φ_α ne peut pas être injectif puisque K[X] est de dimension infinie sur K. □

Proposition 3.17. — *Soient* $\alpha_1, \ldots, \alpha_n \in \mathrm{L}$ *des éléments algébriques sur* K. *Alors l'extension* $\mathrm{K}(\alpha_1, \ldots, \alpha_n)$ *est finie sur* K, *de degré majoré par le produit des degrés des* α_i *sur* K.

Démonstration. — On procède par récurrence sur l'entier n, le cas $n = 1$ étant immédiat (Proposition 3.16). Si $n \geqslant 2$, on note E l'extension engendrée par les éléments $\alpha_1, \ldots, \alpha_{n-1}$, de sorte que l'élément α_n, algébrique sur K, est algébrique sur E (Remarque 3.14). On en déduit que $\mathrm{E}(\alpha_n)$ est finie sur E et, par hypothèse de récurrence, on sait que E est finie sur K et que son degré $[\mathrm{E} : \mathrm{K}]$ est majoré par le produit des $[\mathrm{K}(\alpha_i) : \mathrm{K}]$, avec $1 \leqslant i \leqslant n-1$. Pour conclure, il ne reste plus qu'à appliquer (6). □

Corollaire 3.18. — *Soient* L *une extension algébrique sur* K *et* M *une extension algébrique sur* L. *Alors* M *est algébrique sur* K.

Démonstration. — Soit $\alpha \in \mathrm{M}$, soit P son polynôme minimal sur L et soit E la sous-extension de L sur K engendrée par les coefficients de P. Ceux-ci étant algébriques sur K, l'extension E est finie sur K (Proposition 3.17) et, α étant algébrique sur E puisque annulé par le polynôme P vu dans E[X], l'extension $\mathrm{E}(\alpha)$ est également finie sur E. Donc $\mathrm{E}(\alpha)$, et *a fortiori* $\mathrm{K}(\alpha)$ qui en est une sous-extension, est finie sur K. □

Corollaire 3.19. — *Soit* L *une extension de* K. *L'ensemble* $\mathrm{A}_{\mathrm{L/K}}$ *des éléments de* L *algébriques sur* K *est une sous-extension algébrique de* L *sur* K, *appelée la* fermeture algébrique *de* K *dans* L.

Démonstration. — Soient $\alpha, \beta \in \mathrm{A}_{\mathrm{L/K}}$. Il suffit de voir que $\alpha\beta$ et $\alpha+\beta$, et α^{-1} lorsque α est non nul, appartiennent à $\mathrm{K}(\alpha, \beta)$, qui est finie donc algébrique sur K d'après la proposition 3.17. □

Exemple 3.20. — Donc $\sqrt[3]{7}+\sqrt[5]{19}$ est algébrique sur $\mathbf{Q}$. Pourriez-vous en trouver un polynôme annulateur non nul à coefficients rationnels ?

Une extension algébrique engendrée par un seul élément est finie. La réciproque n'est pas vraie en général, mais en pratique on peut se contenter du résultat suivant.

Proposition 3.21. — *Toute extension finie* L *de* K *est engendrée par un nombre fini d'éléments algébriques de* L, *c'est-à-dire est de la forme* $\mathrm{L} = \mathrm{K}(\alpha_1, \ldots, \alpha_n)$.

Démonstration. — Il suffit de choisir pour $(\alpha_1, \ldots, \alpha_n)$ une famille génératrice finie de L vu comme K-espace vectoriel de dimension finie. □

3.6. Soit $f \in \mathrm{K}[\mathrm{X}]$ de degré $\geqslant 1$, et soit L une extension de K. On dit que f est *scindé* sur L s'il se décompose dans L[X] sous la forme d'un produit de facteurs de degré 1.

Proposition 3.22. — *Soit $f \in \mathrm{K}[\mathrm{X}]$ de degré $\geqslant 1$. Il existe une extension de* K *sur laquelle f est scindé.*

Démonstration. — On procède par récurrence sur le degré de f. Soit P un facteur irréductible de f, soit $\mathrm{L} = \mathrm{K}_{\mathrm{P}}$ et soit α une racine de f dans L. Soit g l'unique polynôme de L[X] tel que $f = (\mathrm{X} - \alpha)g$. C'est un polynôme non constant à qui on applique l'hypothèse de récurrence : il existe une extension M de L sur laquelle g est scindé. Donc f est *a fortiori* scindé sur M. □

Définition 3.23. — On appelle *corps de décomposition* de f sur K une extension finie L de K sur laquelle f est scindé, et qui est engendrée sur K par $\mathrm{Spec}_{\mathrm{L}}(f)$.

3.7. Une extension L de K est dite *algébriquement close* si tout polynôme de K[X] de degré $\geqslant 1$ est scindé sur L. Une *clôture algébrique* de K est une extension algébrique de K qui est algébriquement close.

***Théorème 3.24* (Steinitz).** — *Tout corps admet une clôture algébrique.*

La démonstration nécessite le résultat suivant, qu'on admettra.

***Lemme 3.25* (Krull).** — *Tout anneau non nul possède un idéal maximal.*

Preuve du théorème. — On procède en deux temps. D'abord, on associe à tout corps K une extension algébrique K^+ dans laquelle tous les polynômes de degré $\geqslant 1$ de K[X] ont au moins une racine. (Une telle extension K^+ n'est pas unique.) Ensuite, on construit une extension Ω de K en prenant la "réunion" des corps $\mathrm{K}, \mathrm{K}^+, \mathrm{K}^{++} \ldots$ Il s'agit de donner un sens à cette "réunion", puis de prouver que Ω est une clôture algébrique de K.

– On note S l'ensemble des polynômes de degré $\geqslant 1$ de K[X]. Pour tout $f \in \mathrm{S}$, on introduit une indéterminée X_f et on note R la K-algèbre $\mathrm{K}[\mathrm{X}_f \mid f \in \mathrm{S}]$. On va voir que l'idéal I de R engendré par les $f(\mathrm{X}_f)$ pour $f \in \mathrm{S}$ est un idéal strict de R. Dans le cas contraire, on pourrait écrire 1 sous la forme :

$$1 = \sum_{f \in \mathrm{F}} f(\mathrm{X}_f)\mathrm{P}_f \tag{7}$$

où F est une partie finie de S et où les P_f sont dans R. Par conséquent, si l'on note R_{F} la K-algèbre $\mathrm{K}[\mathrm{X}_f \mid f \in \mathrm{F}]$ et I_{F} l'idéal de R_{F} engendré par les $f(\mathrm{X}_f)$ pour $f \in \mathrm{F}$, on obtient $\mathrm{I}_{\mathrm{F}} = \mathrm{R}_{\mathrm{F}}$. Pourtant, si l'on note Q le produit des $f \in \mathrm{F}$ et M une extension de K sur laquelle Q est scindé, on substitue à chaque X_f dans (7) une racine de f dans M et on trouve $1 = 0$, ce qui est contradictoire.

Puisque $\mathrm{I} \subsetneq \mathrm{R}$, on peut choisir un idéal maximal $\mathfrak{m}$ de R contenant I et poser $\mathrm{K}^+ = \mathrm{R}/\mathfrak{m}$. C'est une K-algèbre-quotient, et l'anneau sous-jacent est un corps puisque l'idéal $\mathfrak{m}$ est maximal. C'est donc une extension de K, et on va voir qu'elle est algébrique. En effet, pour chaque $f \in \mathrm{S}$, notons x_f une racine de f dans K^+, et soit $\alpha \in \mathrm{K}^+$. Il existe un ensemble fini $\mathrm{F} \subset \mathrm{S}$ tel que $\alpha \in \mathrm{K}(x_f \mid f \in \mathrm{F})$, donc α est algébrique sur K (Proposition 3.17).

– Par récurrence, on définit $\mathrm{K}_0 = \mathrm{K}$ et $\mathrm{K}_{n+1} = (\mathrm{K}_n)^+$. Pour chaque entier $n \geqslant 0$, on note $\varphi_n : \mathrm{K}_n \to \mathrm{K}_{n+1}$ le morphisme de K_{n+1} en tant qu'extension de K_n et, pour $0 \leqslant n \leqslant m$, on note φ_{nm} la composée des φ_k pour $n \leqslant k \leqslant m-1$, qui est un homomorphisme de K-algèbres

de K_n dans K_m. On note $\mathscr{E}$ la réunion *ensembliste* disjointe des K_n, $n \geqslant 0$, qui existe d'après la théorie des ensembles.

On définit maintenant une relation d'équivalence sur $\mathscr{E}$. Soient $x, y \in \mathscr{E}$, de sorte qu'il existe des entiers $n, m \geqslant 0$ tels que $x \in \mathrm{K}_n$ et $y \in \mathrm{K}_m$. On note $x \sim y$ s'il existe un entier k supérieur ou égal à n et m, tel que $\varphi_{nk}(x) = \varphi_{mk}(y)$. C'est une relation d'équivalence sur $\mathscr{E}$, et on note Ω le quotient de $\mathscr{E}$ par $\sim$.

Pour $n \geqslant 0$, on note $\mathscr{E}_n$ la réunion disjointe des K_k pour $k \leqslant n$, et on note Ω_n son image dans Ω. L'application naturelle de K_n dans Ω_n, qui à un élément associe sa classe d'équivalence, est bijective. Ceci permet de *transporter* la structure de corps de K_n sur Ω_n. Ce qu'on a gagné, au prix d'une construction un peu technique, c'est qu'on a maitenant une famille $(\Omega_n)_{n\geqslant 0}$ de corps telle que Ω_n est *inclus dans* Ω_{n+1} pour tout $n \geqslant 0$. En outre, Ω_{n+1} est une extension algébrique de Ω_n dans laquelle tout polynôme de degré $\geqslant 1$ de $\Omega_n[\mathrm{X}]$ a au moins une racine.

La réunion croissante Ω des Ω_n, $n \geqslant 0$, est naturellement munie d'une structure de corps, et plus précisément d'extension de Ω_0. On va voir que c'en est une clôture algébrique. D'abord, Ω_n est algébrique sur Ω_0 par transitivité, de sorte que Ω est algébrique sur Ω_0. Ensuite, soit $f \in \Omega[\mathrm{X}]$ de degré $\geqslant 1$. Il existe un $n \geqslant 0$ tel que les coefficients de f appartiennent tous à Ω_n, de sorte que f a une racine dans Ω_{n+1}, donc dans Ω.

Ainsi Ω est une clôture algébrique de Ω_0. Puisque K et Ω_0 sont des corps isomorphes, c'est aussi une clôture algébrique de K, ce qui termine la démonstration. □

Chapitre 4. Homomorphismes d'extensions de corps

4.1. Soit M une extension de K. Pour toute extension L de K, on note :

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

l'ensemble des homomorphismes de K-algèbres de L dans M. Un homomorphisme d'anneaux φ de L dans M est un homomorphisme de K-algèbres si, et seulement s'il prolonge le morphisme $\iota_{\mathrm{M}} : \mathrm{K} \to \mathrm{M}$.

Remarque 4.1. — Lorsque K est un sous-corps de L et de M et lorsque les morphismes définissant les extensions sont triviaux, la situation se simplifie. Un homomorphisme d'anneaux φ de L dans M est un homomorphisme de K-algèbres si, et seulement si on a $\varphi(x) = x$ pour tout $x \in \mathrm{K}$. Autrement dit, on a $\varphi(\lambda x) = \lambda\varphi(x)$ pour $\lambda \in \mathrm{K}$ et $x \in \mathrm{L}$.

Remarque 4.2. — Un homomorphisme de K-extensions est toujours injectif. En effet, le seul idéal strict d'un corps est l'idéal nul.

On remarque que, si S est une partie génératrice de L sur K en tant que K-extension, c'est-à-dire en tant que K-algèbre, tout homomorphisme de K-algèbres de L dans M est caractérisé par sa restriction à S. Plus précisément, on a le résultat suivant.

Proposition 4.3. — *Soit* S *une partie génératrice de* L *en tant que* K*-extension. L'application* $\varphi \mapsto \varphi_{|\mathrm{S}}$ *est injective de* $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L},\mathrm{M})$ *dans l'ensemble* M^{S} *des applications de* S *dans* M*.*

Démonstration. — Soient φ, φ' des homomorphismes de K-algèbres de L dans M coïncidant sur S. L'ensemble des éléments de L en lesquels ces homomorphismes coïncident est une sous-K-algèbre de L contenant S. C'est donc L. □

Mais, en général, elle *n'est pas* surjective. Voir par exemple le lemme 4.4.

4.2. On rappelle que, si $f \in \mathrm{K}[\mathrm{X}]$ est irréductible, on pose $\mathrm{K}_f = \mathrm{K}[\mathrm{X}]/(f)$, qui est une extension finie de K, et on note x l'image de X dans K_f, qui est une racine de f dans K_f. Le lemme suivant est un cas particulier de la proposition 2.14.

Lemme 4.4. — *Soit* $f \in \mathrm{K}[\mathrm{X}]$ *un polynôme irréductible. Alors l'application* $\varphi \mapsto \varphi(x)$ *de* $\mathrm{Hom}_{\mathrm{K}}(\mathrm{K}_f,\mathrm{M})$ *dans* $\mathrm{Spec}_{\mathrm{M}}(f)$ *est une bijection.*

On en déduit la proposition suivante :

Proposition 4.5. — *Soit* $\alpha \in \mathrm{L}$ *algébrique sur* K *et soit* P *son polynôme minimal sur* K*. Alors l'application* $\varphi \mapsto \varphi(\alpha)$ *de* $\mathrm{Hom}_{\mathrm{K}}(\mathrm{K}(\alpha),\mathrm{M})$ *dans* $\mathrm{Spec}_{\mathrm{M}}(\mathrm{P})$ *est une bijection. En particulier, le cardinal de* $\mathrm{Hom}_{\mathrm{K}}(\mathrm{K}(\alpha),\mathrm{M})$ *est fini et majoré par le degré de* α *sur* K*.*

Démonstration. — Le choix $\mathrm{X} \mapsto \alpha$ définit un homomorphisme $\varphi_\alpha : \mathrm{K}_{\mathrm{P}} \to \mathrm{K}(\alpha)$ de K-algèbres, et c'est un isomorphisme puisque les extensions ont même degré. Puis le choix $\mathrm{X} \mapsto s$ définit un homomorphisme de K-algèbres $\varphi_s : \mathrm{K}_{\mathrm{P}} \to \mathrm{M}$, et le composé $\varphi_s \circ \varphi_\alpha^{-1}$ répond à la question. □

Exemple 4.6. — Si on note $\sigma : z \mapsto \bar{z}$ l'homomorphisme de conjugaison complexe, alors on a $\mathrm{Hom}_{\mathbf{R}}(\mathbf{C},\mathbf{C}) = \{\mathrm{id}_{\mathbf{C}}, \sigma\}$. En posant $\mathbf{C} = \mathbf{R}(i)$, ces deux homomorphismes correspondent aux deux éléments de $\mathrm{Spec}_{\mathbf{C}}(\mathrm{X}^2 + 1) = \{i, -i\}$.

4.3. Soit K un corps, et soit $f \in \mathrm{K}[\mathrm{X}]$ de degré $\geqslant 1$.

Proposition 4.7. — *Soient* L *et* L′ *des corps de décomposition de* f *sur* K. *Il existe un isomorphisme de* K*-algèbres de* L *sur* L′.

Démonstration. — On procède par récurrence sur le degré de f. Si $\deg(f) = 1$, le résultat est immédiat, puisque dans ce cas, les extensions L et L′ sont K-isomorphes à K. Sinon, soit P un facteur irréductible de f dans K[X] et soit x (resp. x') une racine de P dans L (resp. dans L′). Il existe un unique homomorphisme de K-algèbres $\varphi : \mathrm{K}(x) \to \mathrm{L}'$ vérifiant $\varphi(x) = x'$, et il induit un isomorphisme entre $\mathrm{K}(x)$ et $\mathrm{K}(x')$ puisque les deux extensions $\mathrm{K}(x)$ et $\mathrm{K}(x')$ de K ont même degré, égal au degré de P. Soit g l'unique polynôme de L[X] tel que $f = (\mathrm{X} - x)g$. Alors L est naturellement une extension finie de $\mathrm{K}(x)$, et L′ est une extension finie de $\mathrm{K}(x)$ au moyen de φ. En outre, ce sont toutes les deux des corps de décomposition de g sur $\mathrm{K}(x)$. Par hypothèse de récurrence, L et L′ sont des $\mathrm{K}(x)$-algèbres isomorphes, donc *a fortiori* des K-algèbres isomorphes. □

4.4. Désormais, on fixe une fois pour toutes une extension algébriquement close Ω de K. Par exemple, pour $\mathrm{K} = \mathbf{Q}$, on pourra choisir $\Omega = \mathbf{C}$.

Soit L une sous-extension de Ω sur K.

Lemme 4.8 **(Prolongement des homomorphismes)**. — *Soit* E *une sous-extension de* L *sur* K *telle que* L *soit finie sur* E. *Alors l'application de restriction :*

$$\mathrm{Res}_{\mathrm{L/E}} : \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \Omega) \to \mathrm{Hom}_{\mathrm{K}}(\mathrm{E}, \Omega)$$

est surjective, et tout élément de $\mathrm{Hom}_{\mathrm{K}}(\mathrm{E}, \Omega)$ *admet au plus* $[\mathrm{L} : \mathrm{E}]$ *antécédents.*

Démonstration. — On écrit L sous la forme $\mathrm{L} = \mathrm{E}(\alpha_1, \ldots, \alpha_n)$ et on procède par récurrence sur l'entier n. Si $n = 1$, le résultat est une conséquence de la proposition 4.5 puisque $\mathrm{Pmin}_{\mathrm{E}}(\alpha)$ a une racine dans Ω. Si $n \geqslant 2$, on pose $\mathrm{F} = \mathrm{E}(\alpha_1, \ldots, \alpha_{n-1})$ et on écrit :

$$\mathrm{Res}_{\mathrm{L/E}} : \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \Omega) \to \mathrm{Hom}_{\mathrm{K}}(\mathrm{F}, \Omega) \to \mathrm{Hom}_{\mathrm{K}}(\mathrm{E}, \Omega).$$

Par hypothèse de récurrence, chacune des deux applications $\mathrm{Res}_{\mathrm{L/F}}$ et $\mathrm{Res}_{\mathrm{F/E}}$ est surjective ; leur composée $\mathrm{Res}_{\mathrm{L/E}}$ est donc surjective. Pour majorer le nombre d'antécédents, on utilise l'hypothèse de récurrence et (6). □

Corollaire 4.9. — *Si* L *est finie sur* K, *l'ensemble* $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \Omega)$ *n'est jamais vide.*

Démonstration. — C'est l'ensemble des antécédents de l'homomorphisme $x \mapsto x$ de K dans Ω par l'application surjective $\mathrm{Res}_{\mathrm{L/K}} : \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \Omega) \to \mathrm{Hom}_{\mathrm{K}}(\mathrm{K}, \Omega)$. □

Corollaire 4.10. — *Soient* L, M *des sous-extensions de* Ω *sur* K. *Si* L *est finie sur* K, *alors* $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{M})$ *est fini, et son cardinal est* $\leqslant [\mathrm{L} : \mathrm{K}]$.

Démonstration. — On remarque que $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{M})$ est inclus dans $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \Omega)$. □

Corollaire 4.11. — *Le groupe* $\mathrm{Aut}_{\mathrm{K}}(\mathrm{L})$ *est fini d'ordre* $\leqslant [\mathrm{L} : \mathrm{K}]$.

Démonstration. — On a $\mathrm{Aut}_{\mathrm{K}}(\mathrm{L}) = \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{L})$, puisque tout K-endomorphisme de L est injectif et que L est de dimension finie sur K. □

4.5. Le corollaire 4.11 peut également être prouvé sans recours au lemme 4.8, au moyen du lemme de Dedekind.

***Lemme 4.12* (Dedekind).** — *Soient* G *un groupe et* L *un corps. Les homomorphismes de groupes de* G *dans* $\mathrm{L}^\times$ *sont linéairement indépendants sur* L.

Démonstration. — Soient $\chi_1, \dots, \chi_r$ des homomorphismes de groupes de G dans $\mathrm{L}^\times$, que l'on suppose linéairement dépendants sur L, et écrivons :

$$c_1\chi_1 + \ldots + c_r\chi_r = 0, \tag{8}$$

où les c_i sont des éléments de L non tous nuls, choisis de telle sorte que le nombre de ceux qui ne sont pas nuls est minimal. Quitte à renuméroter les χ_i, on peut d'ailleurs supposer que $c_1 \neq 0$ et, quitte à diviser (8) par c_1, on peut supposer que $c_1 = 1$. On choisit des éléments $g, h \in \mathrm{G}$ et on évalue (8) en gh, de sorte que :

$$\chi_1(g)\chi_1(h) + \ldots + c_r\chi_r(g)\chi_r(h) = 0, \quad g, h \in \mathrm{G},$$

ce à quoi ou soustrait l'équation (8) évaluée en g puis multipliée par $\chi_1(h)$. Si l'on choisit $h \in \mathrm{G}$ de telle sorte que $\chi_i(h) \neq \chi_1(h)$ pour au moins un i tel que $c_i \neq 0$, on obtient une combinaison linéaire non triviale contenant strictement moins de coefficients non nuls que (8). □

Pour en déduire le corollaire 4.11, on fixe une base $\mathscr{B}$ de L sur K. Tout automorphisme $\sigma \in \mathrm{Aut_K(L)}$ peut être considéré comme une application de $\mathscr{B}$ dans L. Si le cardinal de $\mathscr{B}$ était strictement inférieur à l'ordre du groupe $\mathrm{Aut_K(L)}$, les automorphismes $\sigma \in \mathrm{Aut_K(L)}$ définiraient une famille d'applications L-liées de $\mathscr{B}$ dans L, donc une famille d'applications L-liées de $\mathrm{L}^\times$ dans L. Ceci contredirait l'indépendance linéaire donnée par le lemme de Dedekind avec $\mathrm{G} = \mathrm{L}^\times$.

4.6. Soit L un corps, et soit H un sous-groupe fini du groupe Aut(L) des automorphismes de corps de L.

Proposition 4.13. — *L'ensemble* $\mathrm{L^H} = \{x \in \mathrm{L} \mid \sigma(x) = x,\ \sigma \in \mathrm{H}\}$ *des éléments de* L *invariants par* H *est un sous-corps de* L.

On pose $\mathrm{K} = \mathrm{L^H}$, et on considère L comme une extension de K.

Théorème 4.14. — *L'extension* L *est finie sur* K*, son degré est l'ordre de* H*, et* $\mathrm{Aut_K(L)}$ *est égal à* H.

Démonstration. — Puisque les éléments de K sont invariants par H, le groupe H est un sous-groupe de $\mathrm{Aut_K(L)}$. On note n l'ordre de H, et on suppose que l'on peut choisir dans L un nombre $d \geqslant n+1$ d'éléments linéairement indépendants sur K, que l'on note $\alpha_1, \dots, \alpha_d$. On remarque qu'alors les d vecteurs $(\sigma(\alpha_i))_{\sigma \in \mathrm{H}}$ de L^n sont linéairement dépendants sur L, de sorte qu'on peut écrire :

$$c_1\sigma(\alpha_1) + \ldots + c_d\sigma(\alpha_d) = 0, \quad \sigma \in \mathrm{H}. \tag{9}$$

où les c_i sont des éléments de L non tous nuls, choisis de telle sorte que le nombre de ceux qui ne sont pas nuls est minimal. Quitte à renuméroter les α_i, on peut d'ailleurs supposer que $c_1 \neq 0$ et, quitte à diviser (9) par c_1, on peut supposer que $c_1 = 1$. En appliquant à (9) un élément $\tau \in \mathrm{H}$, et compte tenu du fait que $\sigma \mapsto \tau\sigma$ permute H, on obtient :

$$\tau(c_1)\sigma(\alpha_1) + \ldots + \tau(c_d)\sigma(\alpha_d) = 0, \quad \sigma, \tau \in \mathrm{H}. \tag{10}$$

Si tous les c_i appartiennent à K, alors on obtient l'égalité $c_1\alpha_1 + \ldots + c_d\alpha_d = 0$, ce qui contredit le fait que les α_i sont linéairement indépendants sur K. Il existe donc un $c_i \notin \mathrm{K}$, et donc un $\tau \in \mathrm{H}$ pour lequel la différence (9) − (10) est une combinaison linéaire non triviale contenant strictement moins de coefficients non nuls que (9).

De ceci on déduit que L est une extension finie de K, et que [L : K] est majoré par le cardinal de H. D'après le corollaire 4.10, le groupe $\mathrm{Aut}_{\mathrm{K}}(\mathrm{L})$ est fini d'ordre $\leqslant$ [L : K]. On en déduit l'égalité entre $\mathrm{Aut}_{\mathrm{K}}(\mathrm{L})$ et H. □

Chapitre 5. Correspondance de Galois en caractéristique nulle

Dans ce chapitre, on suppose que K est un corps de caractéristique nulle.

5.1. Soit Ω une extension algébriquement close de K. Pour $\mathrm{K} = \mathbf{Q}$, on pourra par exemple choisir $\Omega = \mathbf{C}$. Si L est une sous-extension de Ω finie sur K, on pose :

$$\mathrm{S} = \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \Omega), \quad \mathrm{G} = \mathrm{Aut}_{\mathrm{K}}(\mathrm{L}). \tag{11}$$

Puisque L est inclus dans Ω, le groupe G est inclus dans l'ensemble S, qui est fini et de cardinal majoré par le degré de L sur K.

Proposition 5.1. — *L'ordre de* G *divise le cardinal de* S.

Démonstration. — Le groupe G opère à droite sur l'ensemble S par $(\sigma, \varphi) \mapsto \varphi \circ \sigma$, pour $\sigma \in \mathrm{G}$ et $\varphi \in \mathrm{S}$. Puisque tout homomorphisme $\varphi \in \mathrm{S}$ est injectif, la condition $\varphi \circ \sigma = \varphi$ impose $\sigma = \mathrm{id}_{\mathrm{L}}$, c'est-à-dire que le stabilisateur dans G de n'importe quel élément de S est trivial. Chaque orbite de S sous G a donc pour cardinal l'ordre de G, et on a le résultat attendu. □

Proposition 5.2. — *L'ensemble* S *est de cardinal* $[\mathrm{L} : \mathrm{K}]$.

Démonstration. — On écrit L sous la forme $\mathrm{L} = \mathrm{K}(\alpha_1, \ldots, \alpha_n)$ et on procède par récurrence sur l'entier n. Si $n = 1$, on écrit simplement $\mathrm{L} = \mathrm{K}(\alpha)$ et on note P le polynôme minimal de α sur K. D'après la proposition 4.5, le cardinal de S est $\leqslant \deg(\mathrm{P})$, et il s'agit de prouver qu'il lui est égal. Si ce n'est pas le cas, cela signifie que P a une racine multiple dans Ω, et donc que P et son polynôme dérivé P' ont une racine en commun dans Ω. Puisque P est irréductible sur K, il est le polynôme minimal sur K de cette racine commune, et il divise donc P'. Mais comme K est de caractéristique nulle, on a l'égalité $\deg(\mathrm{P}') = \deg(\mathrm{P}) - 1$, ce qui contredit le fait que P divise P'.

Si $n \geqslant 2$, on pose $\mathrm{E} = \mathrm{K}(\alpha_1, \ldots, \alpha_{n-1})$, et on a $\mathrm{L} = \mathrm{E}(\alpha_n)$. Par hypothèse de récurrence, on a :

$$\mathrm{card}\ \mathrm{Hom}_{\mathrm{K}}(\mathrm{E}, \Omega) = [\mathrm{E} : \mathrm{K}], \quad \mathrm{card}\ \mathrm{Hom}_{\mathrm{E}}(\mathrm{L}, \Omega) = [\mathrm{L} : \mathrm{E}].$$

On conclut à l'aide de la formule (6). □

5.2. Soit L une sous-extension de Ω finie sur K.

Proposition 5.3. — *Les conditions suivantes sont équivalentes :*

(1) $\mathrm{G} = \mathrm{S}$.
(2) G *est d'ordre* $[\mathrm{L} : \mathrm{K}]$.
(3) *Pour tout* $\varphi \in \mathrm{S}$, *on a* $\varphi(\mathrm{L}) = \mathrm{L}$.
(4) *Pour tout* $\alpha \in \mathrm{L}$, *le polynôme* $\mathrm{Pmin}_{\mathrm{K}}(\alpha)$ *est scindé sur* L.
(5) *Il existe* $f \in \mathrm{K}[\mathrm{X}]$ *tel que* L *soit un corps de décomposition de* f *sur* K.

Démonstration. — L'équivalence entre (1) et (2) est immédiate. Pour un élément $\varphi \in \mathrm{S}$, la condition $\varphi(\mathrm{L}) = \mathrm{L}$ signifie que $\varphi \in \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{L})$. Mais on a $\mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{L}) = \mathrm{G}$, ce qui prouve que (2) et (3) sont équivalents.

Soit $\alpha \in \mathrm{L}$, soit P son polynôme minimal sur K et soit s une racine de P dans Ω. Il existe un homomorphisme $\varphi \in \mathrm{Hom}_{\mathrm{K}}(\mathrm{K}(\alpha), \Omega)$ prenant en α la valeur s. Il se prolonge en $\varphi \in \mathrm{S}$ d'après le lemme 4.8. Puisque $\varphi(\mathrm{L}) = \mathrm{L}$ on a $s \in \mathrm{L}$, donc P est scindé sur L. Ceci prouve que (3) implique (4).

Pour montrer que (4) ⇒ (5), on écrit $L = K(\alpha_1, \dots, \alpha_n)$, on note P_i le polynôme minimal de α_i sur K et on note $f = P_1 \dots P_n$. Alors L est un corps de décomposition de f sur K, car les P_i sont scindés sur L.

Pour montrer que (5) ⇒ (3), on choisit un $f \in K[X]$ dont L est un corps de décomposition sur K et on choisit $\varphi \in S$. Si $\alpha \in \mathrm{Spec}_\Omega(f)$, on aura $\varphi(\alpha) \in \mathrm{Spec}_\Omega(f) \subseteq L$, donc $\varphi(L) \subseteq L$. Puis on a $\varphi(L) = L$ puisque φ est injectif et L de dimension finie sur K. □

Définition 5.4. — Une extension finie L de K est dite *galoisienne* si elle vérifie les conditions équivalentes de la proposition 5.3. Dans ce cas, $\mathrm{Aut}_K(L)$ est noté Gal(L/K) et porte le nom de *groupe de Galois* de L sur K.

Remarque 5.5. — Si L est galoisienne sur K et si E est une sous-extension de L/K, alors L est galoisienne sur E. Par contre, E n'est pas galoisienne sur K en général (voir le théorème 5.7).

5.3. Soit L une sous-extension de Ω galoisienne sur K et soit G = Gal(L/K). Les trois théorèmes suivants sont les trois principaux résultats de la théorie de Galois.

Théorème 5.6. — *L'application* $E \mapsto \mathrm{Gal}(L/E)$ *est une bijection entre sous-extensions de* L/K *et sous-groupes de* G. *La bijection réciproque est donnée par* $H \mapsto L^H$.

Démonstration. — Le théorème 4.14 affirme que l'application $H \mapsto L^H$ est injective, que L est galoisienne sur L^H et que $\mathrm{Gal}(L/L^H) = H$. Soit maintenant E une sous-extension de L/K, et posons H = Gal(L/E). Alors L^H contient E, mais $[L : L^H] = |H|$ est égal à [L : E] puisque L est galoisienne sur E. Donc on a $L^H = E$. □

Théorème 5.7. — *Soit* E *une sous-extension de* L/K. *Alors* E *est galoisienne sur* K *si et seulement si* Gal(L/E) *est distingué dans* G, *auquel cas on a un isomorphisme entre le quotient* G/Gal(L/E) *et* Gal(E/K).

Démonstration. — Commençons par remarquer que, si $\sigma \in G$, alors :

$$\sigma \mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(L/\sigma(E)). \tag{12}$$

En effet, le groupe $H = \sigma\mathrm{Gal}(L/E)\sigma^{-1}$ fixe un élément $x \in L$ si et seulement si Gal(L/E) fixe $\sigma^{-1}(x)$, ce dont on déduit que $L^H = \sigma(E)$. Ainsi Gal(L/E) est distingué dans G si, et seulement si $\sigma(E) = E$ pour tout $\sigma \in G$.

Supposons que E soit galoisienne sur K. Alors tout automorphisme $\sigma \in G$ définit par restriction un élément de $\mathrm{Hom}_K(E, \Omega)$, de sorte que $\sigma(E) = E$. Inversement, supposons que Gal(L/E) soit distingué dans G, et soit $\varphi \in \mathrm{Hom}_K(E, \Omega)$. D'après le lemme 4.8, l'homomorphisme φ se prolonge à L en un homomorphisme $\sigma \in \mathrm{Hom}_K(L, \Omega)$. Mais L est galoisienne sur K, donc $\sigma(L) = L$, c'est-à-dire que $\sigma \in G$. On a donc $\sigma(E) = \varphi(E) = E$, c'est-à-dire que E est galoisienne sur K. □

Soit M une sous-extension de Ω sur K. On note LM le *composé* de L et M, c'est-à-dire l'extension L(M) engendrée par M sur L. C'est aussi M(L).

Théorème 5.8. — *Le corps* LM *est une extension galoisienne de* M, *et on a un isomorphisme entre* Gal(LM/M) *et* $\mathrm{Gal}(L/L \cap M)$. *Notamment, on a* $[LM : M] = [L : L \cap M]$.

Démonstration. — Considérons l'application de restriction de LM à L :

$$\mathrm{Res} : \mathrm{Aut}_{\mathrm{M}}(\mathrm{LM}) \to \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \mathrm{LM}). \tag{13}$$

Comme L est galoisienne sur K, tout $\sigma \in \mathrm{Aut}_{\mathrm{M}}(\mathrm{LM})$ vérifie $\sigma(\mathrm{L}) = \mathrm{L}$, donc le membre de droite de (13) est égal à $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$. Si σ est dans le noyau de la restriction, c'est un M-automorphisme de $\mathrm{LM} = \mathrm{M}(\mathrm{L})$ trivial sur L, il est donc trivial partout, ce qui prouve que (13) est une injection.

Ensuite, on remarque que l'image de (13) est incluse dans $\mathrm{Gal}(\mathrm{L}/\mathrm{L} \cap \mathrm{M})$. En outre, si $\varphi \in \mathrm{Gal}(\mathrm{L}/\mathrm{L} \cap \mathrm{M})$, il se prolonge en $\sigma \in \mathrm{Hom}_{\mathrm{M}}(\mathrm{LM}, \Omega)$ par M-linéarité (sachant qu'une base de L sur $\mathrm{L} \cap \mathrm{M}$ est une famille génératrice de LM sur M). Puis $\sigma(\mathrm{LM})$ est inclus dans $\mathrm{M}\varphi(\mathrm{L})$, qui est égal à LM. On a donc $\sigma \in \mathrm{Aut}_{\mathrm{M}}(\mathrm{LM})$ et on en déduit que (13) induit un isomorphisme de groupes entre $\mathrm{Aut}_{\mathrm{M}}(\mathrm{LM})$ et $\mathrm{Gal}(\mathrm{L}/\mathrm{L} \cap \mathrm{M})$.

Il ne reste plus qu'à prouver que LM est galoisienne sur M. Pour ça, il suffit d'écrire :

$$[\mathrm{LM} : \mathrm{M}] \leqslant [\mathrm{L} : \mathrm{L} \cap \mathrm{M}] = |\mathrm{Gal}(\mathrm{L}/\mathrm{L} \cap \mathrm{M})| = |\mathrm{Aut}_{\mathrm{M}}(\mathrm{LM})| \leqslant [\mathrm{LM} : \mathrm{M}].$$

On en déduit que toutes ces inégalités sont des égalités, ce qui prouve que LM est galoisienne sur M. □

5.4. Soit $n \geqslant 1$ un entier, et soit $\omega_n = \exp(2i\pi/n)$. Le corps $\mathbf{Q}(\omega_n)$, qui est une extension finie de $\mathbf{Q}$, s'appelle le *n-ième corps cyclotomique.*

Proposition 5.9. — *L'extension $\mathrm{K}_n/\mathbf{Q}$ est galoisienne.*

Démonstration. — C'est le corps de décomposition de $\mathrm{X}^n - 1$ sur $\mathbf{Q}$. □

On pose $\mathrm{G}_n = \mathrm{Gal}(\mathrm{K}_n/\mathbf{Q})$. Un automorphisme $\sigma \in \mathrm{G}_n$ est caractérisé par $\sigma(\omega_n)$, qui est une racine n-ième de l'unité. On a donc $\sigma(\omega_n) = \omega_n^{e(\sigma)}$ pour un unique $e(\sigma) \in \mathbf{Z}/n\mathbf{Z}$. L'application :

$$\mathrm{G}_n \to (\mathbf{Z}/n\mathbf{Z})^\times \tag{14}$$

définie par $\sigma \mapsto e(\sigma)$ est un homomorphisme injectif de groupes.

Théorème 5.10. — *L'homomorphisme (14) est un isomorphisme.*

Démonstration. — On pose $f = \mathrm{Pmin}_{\mathbf{Q}}(\omega_n)$ et on va montrer que tous les ω_n^k, $(k, n) = 1$, sont racines de f. Comme des telles racines sont en nombre égal à $\phi(n)$, qui est l'ordre du membre de droite de (14), on en déduira que (14) est un isomorphisme. Pour prouver ceci, il suffit de montrer que, si ζ est une racine complexe de f et si p est un nombre premier ne divisant pas n, alors ζ^p est encore une racine de f. On raisonne par l'absurde, en supposant qu'il existe une racine ζ de f telle que $f(\zeta^p)$ ne soit pas nulle. On remarque que f divise $\mathrm{X}^n - 1$, et on écrit :

$$\mathrm{X}^n - 1 = fh$$

avec $h \in \mathbf{Q}[\mathrm{X}]$. D'après le théorème du contenu de Gauss, les polynômes unitaires f et h sont à coefficients dans $\mathbf{Z}$. Ensuite ζ^p est une racine de $\mathrm{X}^n - 1$, donc de h. Le polynôme $h(\mathrm{X}^p)$ étant annulateur de ζ, il est divisible par f. On écrit $h(\mathrm{X}^p) = fg$ avec $g \in \mathbf{Q}[\mathrm{X}]$ qui, comme précédemment, est à coefficients dans $\mathbf{Z}$. En réduisant modulo p, on trouve que $\overline{h(\mathrm{X})}^p$ est égal à $\overline{f}\,\overline{g}$. On en déduit que f et h ne sont pas premiers entre eux. Mais :

$$\overline{\mathrm{X}^n - 1} = \overline{fh}$$

est à racines simples, ce qui conduit à une contradiction. □

Définition 5.11. — Le polynôme :

$$\Phi_n(\mathrm{X}) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n} (\mathrm{X} - \omega_n^k)$$

s'appelle le *n-ième polynôme cyclotomique*. C'est le polynôme minimal de ω_n sur $\mathbf{Q}$, et il est à coefficients dans $\mathbf{Z}$.

Chapitre 6. Corps finis

6.1. Par *corps fini* on entend corps commutatif de cardinal fini.

Si p est un nombre premier, l'anneau $\mathbf{Z}/p\mathbf{Z}$ est un corps fini de cardinal p, qu'on note $\mathbf{F}_p$. Il est unique à *unique* isomorphisme près, c'est-à-dire que si K est un corps de cardinal p, il existe un unique isomorphisme de corps de $\mathbf{F}_p$ dans K.

Exemple 6.1. — Le polynôme $f = \mathrm{X}^2 + \mathrm{X} + 1$ est irréductible sur $\mathbf{F}_2$. Ainsi le quotient $\mathbf{F}_2[\mathrm{X}]/(f)$ est une extension finie de degré 2 sur $\mathbf{F}_2$, donc de cardinal 4.

Proposition 6.2. — *Si* K *est un corps fini, sa caractéristique est un nombre premier.*

Démonstration. — Le morphisme canonique d'anneaux $\mathbf{Z} \to \mathrm{K}$ ne peut pas être injectif pour des raisons de cardinalité. Son noyau est donc un idéal maximal $p\mathbf{Z}$, où p est un nombre premier. □

Proposition 6.3. — *Soit* K *un corps fini de caractéristique p. Alors le cardinal de* K *est une puissance de p.*

Démonstration. — Il existe un unique homomorphisme d'anneaux $\mathbf{F}_p \to \mathrm{K}$, faisant de K une extension finie de $\mathbf{F}_p$. Si l'on note n le degré de K sur $\mathbf{F}_p$, on en déduit que K est un $\mathbf{F}_p$-espace vectoriel isomorphe à $\mathbf{F}_p^n$, donc de cardinal p^n. □

Proposition 6.4. — *Soit* K *un corps fini. Alors tout sous-anneau de* K *est un corps.*

Démonstration. — Soit A un sous-anneau de K et soit $a \in \mathrm{A}$ non nul. Alors l'application $x \mapsto ax$ est une injection de A dans lui-même : elle est donc bijective. En particulier, 1 admet un unique antécédent par cette application, qui est l'inverse de a dans A. □

6.2. Soit K un corps fini de caractéristique p.

Lemme 6.5. — *L'application $\sigma : x \mapsto x^p$ est un automorphisme de corps de* K.

Démonstration. — La multiplicativité de σ est une conséquence du fait que K est commutatif, et l'additivité provient du fait que, pour chaque $1 \leqslant r \leqslant p-1$, les coefficients binomiaux C_p^r sont des multiples de p, c'est-à-dire qu'ils sont nuls dans K. Puisque K est fini, alors σ, qui est injectif, est automatiquement bijectif. □

Proposition 6.6. — *Tout polynôme irréductible $f \in \mathrm{K}[\mathrm{X}]$ est à racines simples dans n'importe quelle extension de* K *qui scinde f.*

Démonstration. — Supposons qu'il existe un polynôme irréductible $f \in \mathrm{K}[\mathrm{X}]$ admettant une racine multiple a dans une extension L de K qui scinde f. Alors son polynôme dérivé vérifie $f'(a) = 0$, ce qui entraîne que f' est divisible par $\mathrm{Pmin}_{\mathrm{K}}(a)$. Mais $\mathrm{Pmin}_{\mathrm{K}}(a)$ divise aussi f, qui est irréductible sur K. On en déduit que f divise f', donc que $f' = 0$. Autrement dit, f appartient à $\mathrm{K}[\mathrm{X}^p]$, et on peut écrire :

$$f = a_0 + a_p\mathrm{X}^p + a_{2p}\mathrm{X}^{2p} + \cdots \in \mathrm{K}[\mathrm{X}^p].$$

Si l'on pose $\mathrm{Q} = \sigma^{-1}(a_0) + \sigma^{-1}(a_p)\mathrm{X} + \sigma^{-1}(a_{2p})\mathrm{X}^2 + \cdots \in \mathrm{K}[\mathrm{X}]$, on obtient $f = \mathrm{Q}^p$, ce qui contredit l'irréductibilité de f. □

6.3. Dans ce paragraphe, on prouve le théorème de classification des corps finis.

Théorème 6.7. — *Soit n un entier $\geqslant 1$, soit p un nombre premier et soit $q = p^n$. Alors il existe un corps de cardinal q, et tout corps de cardinal q est un corps de décomposition de $\mathrm{X}^q - \mathrm{X}$ sur $\mathbf{F}_p$.*

Démonstration. — On note K un corps de décomposition de $f = \mathrm{X}^q - \mathrm{X}$ sur $\mathbf{F}_p$, qui est fini puisque de dimension finie sur $\mathbf{F}_p$. On pose $\mathrm{E} = \mathrm{Spec}_{\mathrm{K}}(f)$ et on remarque que :

$$\mathrm{E} = \{x \in \mathrm{K} \mid \sigma^n(x) = x\}.$$

On en déduit que E est un sous-corps de K de cardinal inférieur ou égal à q. Mais f est à racines simples dans K d'après la proposition 6.6, de sorte que E est de cardinal exactement q.

Soit maintenant L un corps de cardinal q. Alors tout élément non nul $x \in \mathrm{L}^\times$ vérifie $x^{q-1} = 1$. Donc tout élément $x \in \mathrm{L}$ vérifie $x^q - x = 0$, ce qui montre que L est un corps de décomposition de f sur $\mathbf{F}_p$. □

Remarque 6.8. — Par conséquent, d'après la proposition 4.7, deux corps finis de même cardinal sont isomorphes.

6.4. Soit K un corps fini de cardinal q et soit L une extension finie de K de degré n. D'après le lemme 6.5, l'application $x \mapsto x^q$ est un automorphisme de corps de L, qu'on note σ_{K}. Puisqu'il laisse les éléments de K invariants, c'est un élément de $\mathrm{Aut}_{\mathrm{K}}(\mathrm{L})$.

Proposition 6.9. — *Le groupe $\mathrm{Aut}_{\mathrm{K}}(\mathrm{L})$ est cylique d'ordre n, engendré par σ_{K}. En outre, l'application :*

$$d \mapsto \{x \in \mathrm{L} \mid \sigma_{\mathrm{K}}^d(x) = x\} \tag{15}$$

est une bijection entre les diviseurs de n et les sous-extensions de L *sur* K.

Démonstration. — Si d est un diviseur de n, le polynôme $\mathrm{X}^{q^d} - \mathrm{X}$ est scindé sur L, et le sous-corps de L fixé par σ_{K}^d est l'ensemble :

$$\{x \in \mathrm{L} \mid x^{q^d} = x\},$$

qui est de cardinal q^d d'après ce qui a été vu au paragraphe précédent. Ceci prouve d'une part que l'application (15) est injective, et d'autre part que σ_{K}^d est égal à id_{L} si et seulement si $d = n$, c'est-à-dire que l'automorphisme σ_{K} est d'ordre n. Le groupe $\mathrm{Aut}_{\mathrm{K}}(\mathrm{L})$ est donc d'ordre $\geqslant n$, mais il est d'ordre $\leqslant n$ d'après le corollaire 4.10. Il est donc égal au sous-groupe cyclique d'ordre n engendré par σ_{K}. Il reste à voir que (15) est surjective. Soit E une sous-extension de L sur K, et soit d le degré de E sur K. On a :

$$[\mathrm{L} : \mathrm{K}] = [\mathrm{L} : \mathrm{E}] \cdot [\mathrm{E} : \mathrm{K}],$$

ce qui prouve que d est un diviseur de n. Donc E est égal à $\{x \in \mathrm{L} \mid \sigma_{\mathrm{K}}^d(x) = x\}$. □

6.5. On note φ la fonction indicatrice d'Euler, c'est-à-dire que, pour tout $n \geqslant 1$, l'entier $\varphi(n)$ est le nombre d'entiers compris entre 1 et n qui sont premiers à n. En écrivant :

$$n = \sum_{d|n} \sum_{(k,n)=d} 1 = \sum_{d|n} \varphi(n/d),$$

on voit que n est la somme des $\varphi(d)$, lorsque d décrit les diviseurs de n.

Lemme 6.10. — *Soit* K *un corps. Tout sous-groupe fini de* $\mathrm{K}^\times$ *est cyclique.*

Démonstration. — Soit G un sous-groupe fini de $\mathrm{K}^\times$, soit n son ordre et soit d un diviseur de n. Si G possède un élément x d'ordre d, alors les racines de $f = \mathrm{X}^d - 1$ dans K sont exactement les x^i, avec $1 \leqslant i \leqslant d$. En outre, si $y \in \mathrm{G}$ est d'ordre d, il est racine de f donc c'est une puissance de x, en conséquence de quoi les éléments d'ordre d de G sont les x^i, avec $1 \leqslant i \leqslant d$ premier à d. Finalement, pour un diviseur d de n, l'emsemble G_d des éléments d'ordre d de G est ou bien vide, ou bien de cardinal $\varphi(d)$. Compte tenu de la formule :

$$\sum_{d|n} \varphi(d) = n = \sum_{d|n} \mathrm{card}\ \mathrm{G}_d,$$

on en déduit qu'aucun des G_d, et en particulier G_n, ne peut être vide. □

Proposition 6.11. — *Soit* K *un corps fini, et soit* L *une extension finie de* K. *Il existe un élément* $\alpha \in \mathrm{L}$ *tel que* $\mathrm{L} = \mathrm{K}(\alpha)$.

Démonstration. — On choisit un générateur α du groupe cyclique $\mathrm{L}^\times$. Comme tout élément $x \in \mathrm{L}^\times$ est une puissance de α, on a bien $\mathrm{L} = \mathrm{K}(\alpha)$. □

Corollaire 6.12. — *Pour tout entier* $n \geqslant 1$, *il existe dans* $\mathrm{K}[\mathrm{X}]$ *des polynômes irréductibles de degré* n.

Démonstration. — Soit L l'unique extension de degré n de K, et soit $\alpha \in \mathrm{L}$ un élément tel que $\mathrm{L} = \mathrm{K}(\alpha)$. Alors le polynôme minimal de α sur K est irréductible sur K et de degré n. □

Chapitre 7. Extensions séparables

7.1. Soit $f \in \mathrm{K}[\mathrm{X}]$ de degré $\geqslant 1$, et soit M une extension de K sur laquelle f est scindé. Le polynôme f est dit *à racines simples* si le cardinal de $\mathrm{Spec}_{\mathrm{M}}(f)$ est égal au degré de f, c'est-à-dire si les facteurs irréductibles de f dans M[X] sont deux-à-deux distincts. Ceci ne dépend pas de M, comme le montre le résultat suivant.

Proposition 7.1. — *Un polynôme $f \in \mathrm{K}[\mathrm{X}]$ de degré $\geqslant 1$ est à racines simples si, et seulement s'il est premier à son polynôme dérivé f' dans* K[X].

Démonstration. — Soit f à racines simples de degré $\geqslant 1$, et soit R un facteur commun à f et f' dans K[X]. Si R est de degré $\geqslant 1$, il a une racine α dans un corps de décomposition M de f sur K. Donc f se factorise dans M[X] sous la forme $f = (\mathrm{X} - \alpha)\mathrm{Q}$, et la condition $f'(\alpha) = 0$ implique $\mathrm{Q}(\alpha) = 0$, ce qui contredit l'hypothèse.

Inversement, si f est un polynôme de degré $\geqslant 1$ premier à f' sur K et si sur un corps de décomposition on a $f = (\mathrm{X} - \alpha)^2\mathrm{Q}$, alors $f'(\alpha) = 0$, de sorte que f et f' ont en facteur commun le polynôme minimal de α sur K, ce qui contredit l'hypothèse. □

Définition 7.2. — Soit L une extension de K. Un élément $\alpha \in \mathrm{L}$ est dit *séparable* sur K s'il est algébrique sur K, et si son polynôme minimal sur K est à racines simples.

Proposition 7.3. — *Soit* L *une extension de* K, *soit $\alpha \in \mathrm{L}$ algébrique sur* K *et soit* P *le polynôme minimal de α sur* K. *Les conditions suivantes sont équivalentes :*

(1) *L'élément α n'est pas séparable sur* K.
(2) *On a* $\mathrm{P}' = 0$.
(3) *La caractéristique de* K *est non nulle, égale à p, et on a* $\mathrm{P} \in \mathrm{K}[\mathrm{X}^p]$.

Démonstration. — (1) ⇒ (2). Si α n'est pas séparable sur K, il existe un facteur unitaire non constant $g \in \mathrm{K}[\mathrm{X}]$ commun à P et P′. Mais P est irréductible, donc $g = \mathrm{P}$. Donc P divise P′ tout en étant de degré strictement supérieur, de sorte que $\mathrm{P}' = 0$.

(2) ⇒ (3). En caractéristique nulle, le degré de P′ serait exactement celui de P moins 1, donc P′ ne pourrait pas être nul. Le corps K est donc de caractéristique un nombre premier p. On écrit P sous la forme (2), de sorte que la condition $\mathrm{P}' = 0$ entraîne $ka_k = 0$ pour tout $k \geqslant 0$. Si k est premier à p, on en déduit que $a_k = 0$, et P s'écrit donc :

$$\mathrm{P} = a_0 + a_p\mathrm{X}^p + a_{2p}\mathrm{X}^{2p} + \ldots \in \mathrm{K}[\mathrm{X}^p].$$

(3) ⇒ (1). Si $\mathrm{P} \in \mathrm{K}[\mathrm{X}^p]$, c'est qu'il existe $g \in \mathrm{K}[\mathrm{X}]$ tel que $\mathrm{P} = g(\mathrm{X}^p)$. On a donc une égalité $\mathrm{P}' = p\mathrm{X}^{p-1}g'(\mathrm{X}^p) = 0$, donc P et P′ ne sont pas premiers entre eux. □

Exemple 7.4. — Soit $\mathrm{K} = \mathbf{F}_p(t)$ avec t transcendant sur K. Dans un corps de décomposition M de $f = \mathrm{X}^p - t$ sur K, aucune racine de f n'est séparable. Plus précisément, f a une seule racine dans M et elle est de multiplicité p.

7.2. Une extension algébrique L de K est *séparable* si chacun de ses éléments est séparable sur K.

Exemple 7.5. — Si K est de caractéristique nulle, toute extension algébrique de K est séparable.

Proposition 7.6. — *Soit* $\alpha \in \mathrm{L}$ *algébrique sur* K. *Alors* $\mathrm{K}(\alpha)$ *est séparable sur* K *si et seulement si* α *est séparable sur* K.

Démonstration. — Un sens étant évident, on traite l'autre. Soit Ω une extension algébriquement close de K. On choisit $x \in \mathrm{K}(\alpha)$ et on note P et Q les polynômes minimaux respectivement de α et x sur K. On a des bijections :

$$\mathrm{Hom}_{\mathrm{K}}(\mathrm{K}(\alpha), \Omega) \to \mathrm{Spec}_{\Omega}(\mathrm{P})$$

et :

$$\mathrm{Hom}_{\mathrm{K}}(\mathrm{K}(x), \Omega) \to \mathrm{Spec}_{\Omega}(\mathrm{Q})$$

définies respectivement par $\varphi \mapsto \varphi(\alpha)$ et $\varphi \mapsto \varphi(x)$, et l'application de restriction de $\mathrm{K}(\alpha)$ à $\mathrm{K}(x)$ est une surjection de $\mathrm{Hom}_{\mathrm{K}}(\mathrm{K}(\alpha), \Omega)$ vers $\mathrm{Hom}_{\mathrm{K}}(\mathrm{K}(x), \Omega)$ telle que chaque point de l'image admet au plus $[\mathrm{K}(\alpha) : \mathrm{K}(x)]$ antécédents. On obtient un encadrement :

$$\text{card } \mathrm{Spec}_{\Omega}(\mathrm{P}) \leqslant \text{card } \mathrm{Spec}_{\Omega}(\mathrm{Q}) \cdot [\mathrm{K}(\alpha) : \mathrm{K}(x)] \leqslant [\mathrm{K}(\alpha) : \mathrm{K}]. \tag{16}$$

Puisque α est séparable sur K, le polynôme P admet un nombre de racines égal à $\deg \mathrm{P} = [\mathrm{K}(\alpha) : \mathrm{K}]$, et (16) devient une égalité, ce qui prouve que Q est à racines simples. □

On peut reformuler ce résultat en disant qu'un élément algébrique α est séparable sur K si et seulement si l'ensemble $\mathrm{Hom}_{\mathrm{K}}(\mathrm{K}(\alpha), \Omega)$ est de cardinal $[\mathrm{K}(\alpha) : \mathrm{K}]$. Ce point de vue se généralise comme suit.

Théorème 7.7. — *Soit* L *une extension finie de* K. *Alors* L *est séparable sur* K *si et seulement si* $\text{card } \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \Omega) = [\mathrm{L} : \mathrm{K}]$.

Démonstration. — On procède par récurrence sur le degré de L sur K. Soit Ω une extension algébriquement close de K. Soit E une sous-extension stricte de L sur K telle que $\mathrm{L} = \mathrm{E}(\alpha)$ pour un $a \in \mathrm{L}$. Si L est séparable sur K, alors E aussi, de sorte qu'on a :

$$\text{card } \mathrm{Hom}_{\mathrm{K}}(\mathrm{E}, \Omega) = [\mathrm{E} : \mathrm{K}].$$

Mais par ailleurs $\text{card } \mathrm{Hom}_{\mathrm{E}}(\mathrm{L}, \Omega) = [\mathrm{L} : \mathrm{E}]$, de sorte que :

$$\text{card } \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \Omega) = [\mathrm{L} : \mathrm{E}] \cdot [\mathrm{E} : \mathrm{K}] = [\mathrm{L} : \mathrm{K}].$$

Inversement, on suppose qu'on a $\text{card } \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \Omega) = [\mathrm{L} : \mathrm{K}]$ et que L est non séparable sur K, c'est-à-dire qu'il existe un élément $\alpha \in \mathrm{L}$ non séparable sur K. La caractéristique de K est donc un nombre premier p et le polynôme minimal P de α sur K appartient à $\mathrm{K}[\mathrm{X}^p]$. Soit $e \geqslant 1$ le plus grand entier pour lequel on ait $\mathrm{P} \in \mathrm{K}[\mathrm{X}^{p^e}]$, et écrivons $\mathrm{P} = \mathrm{Q}(\mathrm{X}^{p^e})$. Le polynôme Q est irréductible et, par maximalité de e, il est à racines simples. On pose $x = \alpha^{p^e}$, qui est séparable sur K puisque de polynôme minimal Q. L'extension $\mathrm{K}(x)$ est donc strictement incluse dans $\mathrm{K}(\alpha)$.

On remarque que la restriction $\mathrm{Hom}_{\mathrm{K}}(\mathrm{K}(\alpha), \Omega) \to \mathrm{Hom}_{\mathrm{K}}(\mathrm{K}(x), \Omega)$ est bijective : en effet, le polynôme minimal de α sur $\mathrm{K}(x)$ divise $\mathrm{X}^{p^e} - x$ qui ne possède qu'une seule racine dans Ω. On a donc la majoration :

$$\begin{aligned}\text{card } \mathrm{Hom}_{\mathrm{K}}(\mathrm{L}, \Omega) = \text{card } \mathrm{Hom}_{\mathrm{K}(\alpha)}(\mathrm{L}, \Omega) \cdot \text{card } \mathrm{Hom}_{\mathrm{K}}(\mathrm{K}(x), \Omega) \\ \leqslant [\mathrm{L} : \mathrm{K}(\alpha)] \cdot [\mathrm{K}(x) : \mathrm{K}]\end{aligned}$$

qui est strictement inférieur à $[\mathrm{L} : \mathrm{K}]$. Ceci termine la démonstration. □

Corollaire 7.8. — *Si* L *est séparable sur* K *et si* M *est séparable sur* L*, alors* M *est séparable sur* K*.*

Vincent Sécherre, Université de Versailles Saint-Quentin, Bâtiment Fermat, 45 avenue des États-Unis, 78035 Versailles cedex • *E-mail :* vincent.secherre@math.uvsq.fr