6 Extensions de corps et théorie de Galois

Version du 28 novembre 2005

Dans les chapitres précédents, les corps sont apparus comme des anneaux très simples (pas d'idéaux propres non nuls, modules se réduisant aux espaces vectoriels, qui sont classifiés par leur dimension, etc.) et on ne s'est pas intéressé à eux. Dans ce chapitre et les suivants, on va étudier les extensions de corps, c.-à-d., la donnée d'une paire de corps $k \subset K$. Essentiellement, ceci revient à étudier K non seulement comme corps, mais aussi comme k-algèbre. Ceci donne lieu à une théorie très riche.

Bien sûr, on pourrait étudier, de façon plus générale, les extensions d'anneaux $A \subset B$, mais ceci est en général trop compliqué et inabordable.

23 Caractéristique et extensions de corps

23.1 Les corps fondamentaux $\mathbb{Q}$ et $\mathbb{F}_p$

Il y a deux exemples fondamentaux de corps. D'une part, le corps des rationnels $\mathbb{Q}$, qui est le corps des fractions de $\mathbb{Z}$. D'autre part, les corps finis $\mathbb{F}_p$, où $p \in \mathbb{Z}$ est un nombre premier ≥ 2. Ils sont construits comme suit.

Définition 23.1.1 *Soit $p \geq 2$ un nombre premier. On note $\mathbb{F}_p$ l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$. C'est un corps car l'idéal $p\mathbb{Z}$ est maximal, puisque $\mathbb{Z}$ est principal et p irréductible.*

De façon équivalente, mais plus concrète, le fait que $\mathbb{Z}/(p)$ soit un corps résulte du théorème de Bezout. En effet, soit $a \in \mathbb{Z}$ non divisible par p. Comme l'idéal engendré par a et p est $\mathbb{Z}$, il existe $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha a + \beta p = 1$. Alors, les classes de α et a modulo p sont inverses l'une de l'autre.

En pratique, on peut trouver explicitement les « coefficients de Bezout » α et β (et donc l'inverse α de a modulo p), par la méthode des divisions successives.

Exemples 23.1.2 1) Prenons $p = 37$ et $a = 7$. Alors

$$\begin{cases} 37 &= 5 \times 7 + 2 \\ 3 \times 2 + 1 &= 7, \end{cases} \quad \text{d'où} \quad \begin{cases} 3 \cdot 37 &= 15 \times 7 + 3 \times 2 \\ 3 \times 2 + 1 &= 7, \end{cases}$$

et $16 \cdot 7 - 3 \cdot 37 = 1$. Donc l'inverse de 7 mod. 37 est 16.

2) Prenons $p = 167$ et $a = 17$. Alors

$$\begin{cases} 167 &= 9 \times 17 + 14 \\ 14 + 3 &= 17 \\ 14 &= 4 \times 3 + 2 \\ 1 + 2 &= 3, \end{cases} \quad \text{d'où} \quad \begin{cases} 14 + 1 &= 5 \times 3, \\ 6 \times 14 + 1 &= 5 \times 17, \\ 6 \times 167 + 1 &= (6 \cdot 9 + 5) \times 17. \end{cases}$$

Donc $1 = 59 \cdot 17 - 6 \cdot 167$ et 59 est l'inverse de 17 modulo 167.

Définition 23.1.3 (Sous-corps engendré) *Soit K un corps.*

1) *Si $(K_i)_{i \in I}$ est une famille de sous-corps de K, où I est un ensemble non-vide, l'intersection des K_i est un sous-corps de K.*

2) *Soit S une partie non-vide de K. L'ensemble des sous-corps de K contenant S est non-vide (car il contient K) et donc l'intersection de tous ces sous-corps est un sous-corps de K, qui est le plus petit sous-corps contenant S. On l'appelle le sous-corps* **engendré par** *S.*

Définition 23.1.4 *Le sous-corps de K engendré par l'élément 1_K s'appelle le* **sous-corps premier** *de K. Il est contenu dans tout sous-corps de K.*

Remarque 23.1.5 (Facile mais importante) Soient K et K' deux corps. Tout morphisme d'anneaux $\phi : K \to K'$ est un morphisme de corps, car l'égalité

$$1 = \phi(1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$$

entraîne que $\phi(x^{-1}) = \phi(x)^{-1}$ pour tout $x \in K \setminus \{0\}$. De plus, ϕ est injectif car $\operatorname{Ker} \phi$, étant un idéal propre de K (car $\phi(1) = 1$), est nécessairement nul.

Proposition 23.1.6 (Sous-corps premier et caractéristique)

Soit K un corps arbitraire. Le sous-corps de K engendré par 1 est isomorphe soit à $\mathbb{Q}$, soit à $\mathbb{F}_p$, pour un nombre premier $p \geq 2$ uniquement

déterminé. On dit que la **caractéristique** *de K est 0 dans le premier cas, et p dans le second cas. De façon plus précise, la caractéristique de K est le générateur ≥ 0 du noyau du morphisme $\mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$. On la note* $\mathrm{car}(K)$.

Démonstration. Comme K est un groupe abélien, c'est un $\mathbb{Z}$-module, pour l'action définie, pour tout $n \geq 0$ et $x \in K$, par $n \cdot x = x + \cdots + x$ (n fois), et $(-n) \cdot x = n \cdot (-x)$. De plus, le morphisme de $\mathbb{Z}$-modules $\phi : \mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$ est un morphisme d'anneaux, puisque la distributivité de la multiplication dans K entraîne :

$$(m \cdot 1_K)(n \cdot 1_K) = (1 + \cdots + 1)(1 + \cdots + 1) = (mn) \cdot 1_K.$$

Observons aussi que $\mathrm{Ker}\,\phi$ est un idéal premier de $\mathbb{Z}$, puisque $\mathbb{Z}/\mathrm{Ker}\,\phi$ est isomorphe à un sous-anneau de K, donc intègre. Par conséquent, de deux choses l'une.

1) Si $\mathrm{Ker}\,\phi = (0)$, on peut identifier $\mathbb{Z}$ à son image $\mathbb{Z}1_K$. Comme tout élément de $\phi(\mathbb{Z} \setminus \{0\})$ est inversible dans K, alors ϕ se prolonge en un morphisme d'anneaux $\psi : \mathbb{Q} \to K$, nécessairement injectif puisque $\mathbb{Q}$ est un corps. De plus, tout sous-corps de K contient 1_K, les éléments $n \cdot 1_K$ et leurs inverses. Ceci montre que le sous-corps premier de K est $\psi(\mathbb{Q})$, isomorphe à $\mathbb{Q}$. Dans ce cas, on identifiera $\mathbb{Q}$ à son image dans K :

$$\mathbb{Q} = \{x \in K \mid \exists n, m \in \mathbb{Z}, n \neq 0, \text{ tels que } nx = m1_K\}.$$

2) Si $\mathrm{Ker}\,\phi \neq (0)$, alors $\mathrm{Ker}\,\phi = (p)$, où p est un nombre premier ≥ 2. Dans ce cas, ϕ induit un isomorphisme de $\mathbb{F}_p$ sur son image, qui est formée des éléments $n1_K$ pour $0 \leq n < p$. Ceci montre que, dans ce cas, le sous-corps premier de K est formé des éléments $n1_K$ pour $0 \leq n < p$; on l'identifiera à $\mathbb{F}_p$. La proposition est démontrée. □

23.2 Généralités sur les extensions

Définition 23.2.1 (Sous-corps engendré sur k) *Soit $k \subset K$ une extension de corps. (On dira aussi que K est un surcorps de k.) Soit S une partie de K. L'ensemble des sous-corps de K contenant k et S est non-vide (car il contient K) et donc l'intersection de tous ces sous-corps est un sous-corps de K, qui est le plus petit sous-corps contenant k et S. On l'appelle le sous-corps* **engendré par** *S* **sur** *k et on le note $k(S)$, ou $k(x_1, \ldots, x_n)$ si $S = \{x_1, \ldots, x_n\}$.*

Définition 23.2.2 (Extensions de type fini) *On dit que $k \subset K$ est une* **extension de type fini** *si K est engendré comme surcorps de k par un nombre fini d'éléments, c.-à-d., s'il existe $x_1, \ldots, x_n \in K$ tels que $K = k(x_1, \ldots, x_n)$. Si de plus il existe $x \in K$ tel que $K = k(x)$, on dira que l'extension $k \subset K$ est* **monogène**.

Lemme 23.2.3 *Soit K un surcorps de k et soient I, J deux parties de K. Alors $k(I)(J) = k(I \cup J)$. Par conséquent, toute extension de type fini $k \subset k(x_1, \ldots, x_n)$ est obtenue comme composée d'extensions monogènes :*

$$k(x_1, \ldots, x_n) = k(x_1)(x_2, \ldots, x_n) = k(x_1)(x_2) \cdots (x_n).$$

Démonstration. $k(I)(J)$ contient $I \cup J$ et donc $k(I \cup J)$. Réciproquement, $k(I \cup J)$ contient $k(I)$ et J, donc $k(I)(J)$. Ceci prouve le lemme. □

Définition 23.2.4 *Soient K et K' deux extensions de k. On dira que K et K' sont k-***isomorphes** *s'il existe un isomorphisme $\phi : K \xrightarrow{\sim} K'$ (de corps ou d'anneaux ; on a vu que c'était la même chose) tel que $\phi(\lambda) = \lambda$ pour tout $\lambda \in k$. Ceci équivaut à dire que ϕ est un isomorphisme de k-algèbres.*

*Plus généralement, si, plutôt qu'une inclusion de k dans K et K', on s'est donné des morphismes de corps $\tau : k \hookrightarrow K$ et $\tau' : k \hookrightarrow K'$, alors un k-***morphisme** *de K vers K' est un morphisme de corps $\phi : K \to K'$ tel que $\phi \circ \tau = \tau'$.*

23.3 Extensions entières d'anneaux

Dans cette section, on va étudier les extensions entières d'anneaux, déjà abordées dans la section 14.1 du chapitre 3. Le but de cette section est double : d'une part, ajouter certains résultats omis dans la section 14.1 (et utilisés dans la preuve du théorème des zéros) et, d'autre part, traiter les extensions algébriques de corps, qui sont des cas particuliers d'extensions entières. Soient $A \subset B$ deux anneaux.

Définition 23.3.1 *Un élément $b \in B$ est dit* **entier sur** *A s'il existe $P \in A[X]$* **unitaire** *tel que $P(b) = 0$, c.-à-d., s'il existe $a_1, \ldots, a_n \in A$ tels que*

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0.$$

Une telle équation s'appelle une équation de **dépendance intégrale** *(de b sur A).*

On dit que B est **entier sur** *A si tout $b \in B$ est entier sur A.*

Pour tout $b \in B$, on note $A[b]$ la sous-A-algèbre de B engendrée par b.

Proposition 23.3.2 (Caractérisation des éléments entiers) *Les conditions suivantes sont équivalentes :* (i) *b est entier sur A.*

(ii) *$A[b]$ est un A-module de type fini.*

(iii) *$A[b]$ est contenu dans un sous-anneau C de B qui est un A-module de type fini.*

Démonstration. Si l'on a une équation de dépendance intégrale $P(b) = 0$ de degré n, on obtient (par une récurrence sur le degré, ou bien en utilisant la division euclidienne dans $A[X]$ par le polynôme unitaire P), que les éléments $1, b, \ldots, b^{n-1}$ engendrent $A[b]$ comme A-module. Ceci montre que (i) $\Rightarrow$ (ii). Il est clair que (ii) $\Rightarrow$ (iii).

Supposons (iii) vérifié et soient $x_1, \ldots, x_n$ des générateurs de C comme A-module. Pour tout j, bx_j appartient à C donc il existe des éléments $a_{ij} \in A$ tels que

$$(\dagger) \qquad bx_j = \sum_{i=1}^{n} a_{ij} x_i, \qquad \forall j = 1, \ldots, n.$$

Désignons par $P \in M_n(C)$ la matrice dont le coefficient d'indice (i, j) est $a_{ij} - \delta_{ij} b$, où δ_{ij} désigne le symbole de Kronecker ($\delta_{ij} = 1$ si $i = j$ et $= 0$ sinon). Alors, les équations (†) se récrivent de façon matricielle :

$$(1) \qquad P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

(Égalité de matrices à coefficients dans l'anneau C). Notons $\widetilde{P}$ la transposée de la matrice des cofacteurs de P (c.-à-d., $(-1)^{i+j} \widetilde{P}_{ij}$ égale le déterminant de la matrice obtenue en supprimant dans P la ligne j et la colonne i). Alors, d'après la formule de développement d'un déterminant suivant une ligne ou une colonne, on a l'égalité matricielle :

$$(2) \qquad (\det P) I_n = \widetilde{P} P,$$

où I_n désigne la matrice unité. Combiné avec l'égalité (1), ceci donne que l'élément $d := \det P$ de C vérifie $dx_i = 0$ pour $i = 1, \ldots, n$. Donc d annule le A-module C, et comme C contient l'élément neutre $1 \in B$, ceci donne

dét $P = 0$. Or, $P = M - bI_n$, où M désigne la matrice dont les coefficients sont les $a_{ij} \in A$. Donc, en développant dét P, on obtient une égalité

$$(-1)^n b^n + \alpha_1 b^{n-1} + \cdots + \alpha_n = 0,$$

où les α_ℓ sont des polynômes en les a_{ij}, donc appartiennent à A. Ceci montre que b est entier sur A. La proposition est démontrée. □

Lemme 23.3.3 *Soient $A \subset B$ des anneaux et N un B-module de type fini. On suppose que B est un A-module de type fini. Alors N est un A-module de type fini.*

Démonstration. Par hypothèse, il existe des éléments $x_1, \ldots, x_r$ dans N (resp. $b_1, \ldots, b_n$ dans B) qui engendrent N comme B-module (resp. B comme A-module). Alors

$$N = Bx_1 + \cdots + Bx_r$$

et chaque Bx_j est engendré, comme A-module, par les éléments $b_i x_j$. Il en résulte que N est engendré comme A-module par les éléments $b_i x_j$. Ceci prouve le lemme. □

Définition 23.3.4 *Soient $A \subset B$ deux anneaux.*

1) On dit que l'extension $A \subset B$ est **de type fini** *si B est une A-***algèbre** *de type fini, c.-à-d., s'il existe $x_1, \ldots, x_n \in B$ engendrant B comme A-algèbre, c.-à-d., tels que $B = A[x_1, \ldots, x_n]$.*

2) On dit que l'extension $A \subset B$ est **finie** *si B est un A-***module** *de type fini, c.-à-d., s'il existe $m_1, \ldots, m_r \in B$ engendrant B comme A-module, c.-à-d., tels que $B = Am_1 + \cdots + Am_r$.*

Bien sûr, toute extension finie est de type fini, mais la réciproque est fausse. Par exemple, l'extension $k \subset k[X]$ est de type fini, mais n'est pas finie car $k[X]$ n'est pas un k-espace vectoriel de dimension finie.

Proposition 23.3.5 (type fini + entier ⇒ fini) *Si $C = A[x_1, \ldots, x_n]$ et si chaque x_i est entier sur A, alors C est un A-module de type fini.*

Démonstration. Par récurrence sur n. Le cas $n = 1$ a été vu dans la proposition 23.3.2. On peut donc supposer $n \geq 2$ et le résultat établi pour $n - 1$. Posons $B = A[x_1, \ldots, x_{n-1}]$. Par hypothèse de récurrence, B est fini sur A. D'autre part, x_n étant entier sur A ; il l'est aussi sur B, et donc $C = B[x_n]$ est fini sur B. Donc, d'après le lemme 23.3.3, appliqué à $N = C$, on obtient que C est un A-module de type fini. La proposition est démontrée. □

Remarque 23.3.6 Écrivant que chaque x_i vérifie une équation intégrale sur A de degré d_i, on peut aussi montrer par un argument direct que le sous-A-module de C engendré par les monômes

$$x_1^{s_1} \cdots x_n^{s_n}, \quad \text{avec} \quad 0 \leq s_i \leq d_i$$

est stable par multiplication par chaque x_j, donc coïncide avec C (*cf.* preuve du théorème 2.4.3).

Remarque 23.3.7 1) La proposition précédente a été utilisée implicitement dans la preuve du théorème de Zariski 15.2.1, page 98, ligne 2, dans la phrase : « chaque x_i, et donc aussi L, est entier sur le sous-anneau $K[X_1][1/f]$ ».

2) Deux autres corrections à la page 98 : dans la 2ème ligne de la preuve de 15.2.2, remplacer $k[X_1, \ldots, X_n]$ par $k[X_1, \ldots, X_n]/\mathfrak{m}$. Et ligne 3 du bas : remplacer « en particulier pour $g = f$ » par : « donc le point $(x_1, \ldots, x_n)$ appartient à $V(I) \subseteq k^n$, et donc $f(x_1, \ldots, x_n) = 0$ puisque $f \in \mathcal{I}(V(I))$ ».

Proposition 23.3.8 (Clôture intégrale de A dans B) *Soient $A \subset B$ des anneaux, et $\widetilde{A}$ l'ensemble des $b \in B$ qui sont entiers sur A. Alors $\widetilde{A}$ est un sous-anneau de B, appelé la clôture intégrale de A dans B.*

Démonstration. D'abord, $\widetilde{A}$ contient A et donc 1. Soient $x, y \in \widetilde{A}$. Alors, d'après la proposition 23.3.5, le sous-anneau $A[x, y]$ est un A-module de type fini. Il contient $x-y$ et xy et donc, d'après le point 3) de la proposition 23.3.2, $x - y$ et xy sont entiers sur A. Ceci montre que $\widetilde{A}$ est un sous-anneau de B. □

Proposition 23.3.9 (Transitivité des extensions entières) *Soient $A \subset B \subset C$, avec B entier sur A. Si $x \in C$ est entier sur B, alors x est entier sur A. En particulier, si C est entier sur B, il est entier sur A.*

Démonstration. Par hypothèse, il existe $b_1, \ldots, b_n \in B$ tels que

$$x^n + b_1 x^{n-1} + \cdots + b_n = 0.$$

Posons $B_0 := A[b_1, \ldots, b_n]$. Alors $B_0[x]$ est fini sur B_0 et, d'après la proposition 23.3.5, celui-ci est un A-module de type fini. Donc, d'après le lemme 23.3.3, le sous-anneau $B_0[x]$ est un A-module de type fini. D'après la proposition 23.3.2, ceci entraîne que x est entier sur A. La proposition est démontrée. □

Définition 23.3.10 *1) Soient $A \subset B$ deux anneaux. On dit que A est* **intégralement fermé dans** *B si tout élément de b entier sur A appartient à A, c.-à-d., si A est égal à sa clôture intégrale dans B.*

2) On dit qu'un anneau A est **intégralement clos** *s'il est* **intègre** *et s'il est intégralement fermé dans son corps des fractions K, c.-à-d., si tout $\alpha \in K$ entier sur A appartient à A.*

Corollaire 23.3.11 *Soient $A \subset B$ deux anneaux et $\widetilde{A}$ la clôture intégrale de A dans B. Alors $\widetilde{A}$ est intégralement fermé dans B. En particulier, si A est intègre et B son corps des fractions, alors $\widetilde{A}$ est intégralement clos.*

Démonstration. Soit $x \in B$ entier sur $\widetilde{A}$. D'après la proposition 23.3.9, x est entier sur A, donc appartient à $\widetilde{A}$. □

Les anneaux intégralement clos jouent un rôle important en géométrie algébrique et en théorie des nombres ; voir par exemple [AM, Chap.9], [Die, §5], [Sa].

Proposition 23.3.12 *Soit A factoriel. Alors A est intégralement clos.*

Démonstration. Soient K le corps des fractions de A et $\alpha \in K \setminus \{0\}$. On peut écrire $\alpha = b/c$, avec b et c sans facteur commun. Supposons α entier sur A. Alors il existe $a_1, \ldots, a_n \in A$ tels que

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0.$$

Multipliant cette égalité par c^n, on obtient que

$$(*) \qquad -b^n = ca_1b^{n-1} + \cdots + c^n a_n$$

est divisible par c. Ceci entraîne que c est inversible dans A. En effet, sinon soit p un élément irréductible divisant c. D'après $(*)$ il divise b^n et donc, d'après le Lemme d'Euclide (puisque A est factoriel), p divise b, une contradiction. Donc c est un élément inversible de A et $\alpha \in A$. La proposition est démontrée. □

Proposition 23.3.13 *Soit $A \subset B$ une extension entière.*

1) *Soient J un idéal propre de B et $I = A \cap J$. Alors l'extension $A/I \subseteq B/J$ est entière.*

2) *Si S est une partie multiplicative de A, l'extension $S^{-1}A \subseteq S^{-1}B$ est entière.*

Démonstration. Facile, et laissée au lecteur. □

23.4 Éléments algébriques ou bien transcendants

Soit $k \subset K$ une extension de corps et soit $\alpha \in K$. On note $k[\alpha]$ la **sous-k-algèbre** de K engendrée par α.

Soit $\phi_\alpha : k[X] \to K$ le morphisme de k-algèbres défini par $\phi_\alpha(X) = \alpha$. On a $\phi_\alpha(P) = P(\alpha) \in K$ pour tout $P \in k[X]$, et l'image de ϕ_α est $k[\alpha]$. Posons $I_\alpha = \operatorname{Ker} \phi_\alpha$. Puisque $k[X]/I_\alpha \cong k[\alpha]$ est intègre, alors I_α est un idéal premier de $k[X]$. Donc, de deux choses l'une : ou bien $I_\alpha = (0)$ ou bien $I_\alpha = (P)$ pour un polynôme irréductible unitaire uniquement déterminé.

Définition 23.4.1 (Éléments transcendants ou algébriques)

1) Si $I_\alpha = (0)$, on dit que α est **transcendant** *sur k.*

2) Si $I_\alpha \neq (0)$, on dit que α est **algébrique** *sur k. Dans ce cas, $I_\alpha = (P)$, où P est l'unique polynôme unitaire de degré minimal dans I_α ; par conséquent, α est* **entier** *sur k.*

Le polynôme P est appelé **polynôme minimal de α sur k** *; on le notera* $\operatorname{Irr}_k(\alpha)$. *Son degré s'appelle* **degré de α sur k** *et se note* $\deg_k(\alpha)$.

Remarque 23.4.2 Soit L un corps intermédiaire entre k et K, c.-à-d., $k \subseteq L \subseteq K$. Si $\alpha \in k$ est algébrique sur k, il l'est aussi sur L et $\operatorname{Irr}_k(\alpha)$ est divisible, dans $L[X]$, par $\operatorname{Irr}_L(\alpha)$.

Théorème 23.4.3 (Le sous-corps $k(x)$, pour x algébrique ou bien transcendant)

1) *Supposons x algébrique sur k. Alors* $\operatorname{Irr}_k(x)$ *est irréductible et l'on a*

$$(*) \qquad k[X]/(\operatorname{Irr}_k(x)) \xrightarrow{\sim} k[x] = k(x).$$

Par conséquent, les éléments $1, x, \ldots, x^{d-1}$, où $d = \deg_k(x)$, forment une base de $k(x)$ sur k. En particulier, $\dim_k k(x) = d$.

2) *Si α est transcendant sur k, alors l'injection $\phi_\alpha : k[X] \hookrightarrow K$ induit un k-isomorphisme $k(X) \xrightarrow{\sim} k(\alpha)$. En particulier,* $\dim_k k(\alpha) = +\infty$.

Démonstration. 1) $k[X]/I_x$ est intègre car isomorphe à $k[x]$, la sous-k-algèbre de K engendrée par x. Ainsi, $I_x = (\operatorname{Irr}_k(x))$ est premier. D'après le lemme 14.3.1, $\operatorname{Irr}_k(x)$ est irréductible et engendre un idéal maximal de $k[X]$. Donc, $A := k[X]/(\operatorname{Irr}_k(x))$ est un corps. Par conséquent, son image par ϕ_x, qui est $k[x]$, égale le corps $k(x)$ engendré par x. Ceci prouve $(*)$. Comme les images de $1, \ldots, X^{d-1}$ forment une base de A sur k, la dernière assertion de 1) en découle.

2) Supposons α transcendant, c.-à-d., $\phi_\alpha : k[X] \hookrightarrow K$ injectif. Alors, tout élément de $\phi(k[X] \setminus \{0\})$ est inversible dans K, et donc ϕ se prolonge en un morphisme d'anneaux $\psi : k(X) \to K$, nécessairement injectif puisque $k(X)$ est un corps. L'image de ψ est formée des fractions

$$\left\{ \frac{P(\alpha)}{Q(\alpha)} \mid P, Q \in k[X], Q \neq 0 \right\};$$

c'est le sous-corps $k(\alpha)$, qui est donc isomorphe à $k(X)$. □

Remarque 23.4.4 Écrivons $\mathrm{Irr}_k(x) = x^d + a_1 x^{d-1} + \cdots + a_d$ et observons que $a_d \neq 0$ puisque $\mathrm{Irr}_k(x)$ est irréductible. Alors l'inverse de x est égal à

$$(x^d + a_1 x^{d-2} + \cdots + a_{d-1}) a_d^{-1}.$$

D'autre part, le fait que, dans ce cas, $k[x]$ coïncide avec $k(x)$ résulte aussi du lemme suivant.

Lemme 23.4.5 *Soit A une k-algèbre commutative intègre de dimension finie sur k. Alors A est un corps.*

Démonstration. Soit $x \in A \setminus \{0\}$. La multiplication par x est un endomorphisme k-linéaire injectif de A, donc surjectif (puisque $\dim_k A < \infty$). Donc il existe $x' \in A$ tel que $xx' = 1$, et x' est l'inverse de x. Ceci montre que A est un corps. □

23.5 Extensions algébriques de corps et degré d'une extension

On a vu plus haut que si $K = k(x)$, où x est un élément algébrique sur k, alors $\dim_k K = \deg_k(x)$. Ceci explique la terminologie introduite dans la définition suivante.

Définition 23.5.1 *Soit $k \subset K$ une extension de corps ; la dimension de K comme k-espace vectoriel est appelée* **degré de K sur k** *et notée $[K : k]$. C'est un élément de $\mathbb{N}^* \cup \{+\infty\}$.*

Proposition 23.5.2 (Multiplicativité des degrés) *Soient $k \subset K \subset L$ des extensions de corps. On a $[L : k] = [L : K][K : k]$.*

Démonstration. Si l'un de $[L : K]$ ou $[K : k]$ égale $+\infty$, il en est de même de $[L : k]$. On peut donc supposer $[L : K] = m$ et $[K : k] = n$. Soient $(\ell_1, \ldots, \ell_m)$ une base de L sur K et $(x_1, \ldots, x_n)$ une base de K sur k. Alors,

d'après la preuve du lemme 23.3.3, les éléments $x_i \ell_j$ engendrent L comme k-espace vectoriel. Montrons qu'ils sont linéairement indépendants. Supposons qu'on ait une égalité

$$0 = \sum_{i,j} a_{i,j} x_i \ell_j,$$

avec les $a_{i,j} \in k$. Alors on a

$$0 = \sum_{1 \leq i \leq m} \left(\sum_{1 \leq j \leq n} a_{i,j} x_j \right) \ell_i.$$

Comme les ℓ_i sont linéairement indépendants sur K, on obtient que, pour tout $i = 1, \ldots, m$,

$$\sum_{1 \leq j \leq n} a_{i,j} x_j = 0.$$

Puis, comme les x_j sont linéairement indépendants sur k, on obtient que $a_{i,j} = 0$ pour tout i, j. Ceci montre que les produits $x_j \ell_i$ forment une base de L sur k, d'où $\dim_k L = mn$. □

Remarque 23.5.3 La même démonstration montre que si $A \subset B$ sont deux anneaux, et si $B \cong A^n$ comme A-module, alors, pour tout $r \geq 1$, B^r est libre comme A-module, de rang rn.

Définition 23.5.4 *Soit $k \subset K$ une extension de corps. On dit que K/k est une extension* **algébrique** *si tout élément de K est algébrique sur k. Dans ce cas, K/k est en fait une extension* **entière**.

Proposition 23.5.5 *Soient $k \subset K$ et $K \subset L$ des extensions algébriques de corps. Alors l'extension $k \subset L$ est algébrique.*

Démonstration. Ceci résulte de la proposition 23.3.9. □

Proposition 23.5.6 *Soit $k \subset K$ une extension de corps.*

1) *Si $[K : k] < \infty$, alors K/k est une extension algébrique de type fini.*

2) *Si $K = k(x_1, \ldots, x_n)$ et si chaque x_i est algébrique sur k de degré d_i, alors $K = k[x_1, \ldots, x_n]$, c.-à-d., K est engendré comme k-***algèbre** *par les x_i, et l'on a $[K : k] \leq d_1 \cdots d_n$.*

Démonstration. 1) est facile. En effet, supposons $[K : k] < \infty$. Alors, tout élément de K est algébrique sur k, d'après le point 2) du théorème 23.4.3.

De plus, toute base de K sur k est un système fini de générateurs de K sur k. Ceci prouve 1).

2) Montrons que $K = k[x_1, \ldots, x_n]$ et $[K : k] \leq d_1 \cdots d_n$ par récurrence sur n. Si $n = 1$, c'est le théorème 23.4.3. On peut donc supposer $n \geq 2$ et l'assertion établie pour $n - 1$. Posons $K' = k(x_1, \ldots, x_{n-1})$. Alors x_n est algébrique sur K' de degré $\leq d_n$ et donc, par l'hypothèse de récurrence plus le cas $n = 1$ appliqué à K', on obtient :

$$(*) \qquad K = K'(x_n) = K'[x_n] = k[x_1, \ldots x_n],$$

et $[K : k] = [K : K'][K' : k] \leq d_n d_{n-1} \cdots d_1$. Ceci prouve 2).

Une autre démonstration est la suivante. Soit $\phi : k[X_1, \ldots, X_n] \to K$ le morphisme de k-algèbres défini par $\phi(X_i) = x_i$, pour $i = 1, \ldots, n$; on a $\phi(P) = P(x_1, \ldots, x_n) \in K$ pour tout $P \in k[X_1, \ldots, X_n]$. L'image de ϕ est $A := k[x_1, \ldots, x_n]$, la sous-k-algèbre de K engendré par les x_i. Comme chaque monôme x_i^n est combinaison k-linéaire des monômes x_i^r, avec $0 \leq r < d_i$, on en déduit que A est engendrée sur k par les monômes

$$x_1^{r_1} \cdots x_n^{r_n},$$

où $r_i < d_i$ pour tout i. Par conséquent, A est une k-algèbre de dimension finie $\leq d_1 \cdots d_n$. De plus, A est intègre, puisque contenue dans K. D'après le lemme 23.4.5, A est un corps, et l'égalité $(*)$ en résulte. Donc $K = A$ est de dimension $\leq d_1 \cdots d_n$ sur k. □

Corollaire 23.5.7 *Une extension de corps $k \subset K$ est de degré fini si et seulement si elle est algébrique et de type fini.*

Remarque 23.5.8 Le point 2) de la proposition admet une réciproque. C'est le théorème de Zariski démontré dans le chapitre 3 et utilisé pour démontrer le théorème des zéros. Pour mémoire, rappelons-le ici.

Théorème 23.5.9 (Zariski) *Soient $k \subseteq K$ des corps. On suppose que K est une k-algèbre de type fini. Alors K est algébrique sur k et donc de degré fini sur k.*

23.6 Bases de transcendances et extensions de type fini

Soit $k \subset K$ une extension de corps, et soient $x_1, \ldots, x_n \in K$.

Définition 23.6.1 *On dit que $x_1, \ldots, x_n$ sont* **algébriquement indépendants sur** *k si le morphisme*

$$\phi : k[X_1, \ldots, X_n] \to K, \qquad P \mapsto P(x_1, \ldots, x_n)$$

est injectif. Dans ce cas, ϕ se prolonge en un isomorphisme de $k(X_1, \ldots, X_n)$ sur le sous-corps de K engendré par les x_i. En particulier, chaque x_i est transcendant sur k.

Remarque 23.6.2 Soit K le corps des fractions de l'anneau $k[x, y]$, où $x^2 = y^3$. Alors x et y sont transcendants sur k, mais ne sont pas algébriquement indépendants sur k, puisqu'on a la relation $x^2 = y^3$.

Définition 23.6.3 *On dit qu'une partie B de K est une* **base de transcendance sur** *k si elle vérifie les deux conditions suivantes :*

(i) les éléments de B sont algébriquement indépendants sur k ;

(ii) le corps K est extension algébrique du sous-corps $k(B)$.

Ceci équivaut à dire que B est une partie **algébriquement indépendante maximale**.

Lemme 23.6.4 *Soit K/k une extension et soit S une partie* **finie** *de K telle que K soit algébrique sur $k(S)$. Alors S contient une base de transcendance B de K sur k. De plus, $[k(S) : k(B)] < \infty$; en particulier, si $K = k(S)$, alors K est de degré fini sur $k(B)$.*

Démonstration. Posons $S = \{x_1, \ldots, x_n\}$. Quitte à renuméroter les x_i, on peut supposer que $x_1, \ldots, x_r$ sont algébriquement indépendants sur k et que, pour tout $i > r$, x_i est algébrique sur $k(B)$, où $B = \{x_1, \ldots, x_r\}$. Alors, par transitivité des extensions algébriques (23.5.5), K est algébrique sur $k(B)$, et donc B est une base de transcendance de K sur k.

De plus, d'après la proposition 23.5.6, $k(S)$ est de degré fini sur $k(B)$. □

Proposition 23.6.5 *Soit K/k une extension de corps telle que K possède une base de transcendance sur k* **finie**.

1) *Soit B une base de transcendance de K sur k de cardinal* **minimum** *n. Alors, toute partie B' algébriquement indépendante sur k est de cardinal $\leq n$.*

2) *Par conséquent,* **toute** *base de transcendance de K sur k est de cardinal n.*

Démonstration. On procède par récurrence sur l'entier $s(B, B') := \#B - \#(B \cap B')$. Si $s = 0$, alors $B \subseteq B'$ donc $B' = B$ par maximalité de B. On peut donc supposer $s \geq 1$ et l'assertion établie pour $s - 1$.

Écrivons $B = \{b_1, \ldots, b_n\}$. Sans perte de généralité, on peut supposer que

$$B \cap B' = \{b_{s+1}, \ldots, b_n\}.$$

Si $B' \subseteq B$, l'assertion est vérifiée, donc on peut supposer qu'il existe $b' \in B'$ tel que $b' \notin B$. Alors $B \cup \{b'\}$ n'est pas algébriquement indépendante, par maximalité de B. Donc, il existe $P \in k[X_1, \ldots, X_n, X_{n+1}]$ non nul tel que

$$P(b_1, \ldots, b_n, b') = 0.$$

De plus, $P \notin k[X_{s+1}, \ldots, X_{n+1}]$, puisque les éléments de B' sont algébriquement indépendants. Donc, sans perte de généralité, on peut supposer que P contient la variable X_1.

Posons alors $B_1 = \{b_2, \ldots, b_n, b'\}$. Alors b_1 est algébrique sur $k(B_1)$, et comme K est algébrique sur $k(B_1)[b_1]$, il est aussi algébrique sur $k(B_1)$.

Comme $\#B_1 = n$, la minimalité de n, jointe au lemme 23.6.4, entraîne que B_1 est une base de transcendance de K sur k (car sinon, B_1 contiendrait une base de transcendance de K sur k de cardinal $< n$, contredisant la minimalité de n). De plus,

$$\#B_1 - \#(B_1 \cap B') = s - 1, \quad \text{car} \quad B_1 \cap B' = \{b_{s+1}, \ldots, b_n, b'\}.$$

Donc, par l'hypothèse de récurrence, appliquée à B_1 et B', on obtient que $\#B' \leq \#B_1 = n$. Ceci prouve 1).

En particulier, si B' est une autre base de transcendance de K/k, alors $\#B' \leq n$, et donc $\#B' = n$ par minimalité de n. La proposition est démontrée. □

Théorème 23.6.6 *Soit $k \subset K$ une extension de corps de type fini. Alors :*

1) *Toutes les bases de transcendance de K ont le même cardinal, appelé* **degré de transcendance de K sur k** *et noté* $\deg.\ \mathrm{tr}_k K$. *De plus, tout ensemble d'éléments algébriquement indépendants est contenu dans une base de transcendance.*

2) *Soit L/k une sous-extension de K/k (c.-à-d., L est un sous-corps de K contenant k). Alors L/k est de type fini et l'on a*

$$\deg.\ \mathrm{tr}_k L \leq \deg.\ \mathrm{tr}_k K.$$

Démonstration. D'après le lemme 23.6.4, il existe une base de transcendance B_0 de K sur k ayant r éléments. Alors, d'après la proposition précédente, toute base de transcendance de K sur k a r éléments, et toute partie algébriquement libre est de cardinal $\leq r$. Par conséquent, toute suite croissante de parties algébriquement indépendantes est stationnaire (après au plus r étapes), et donc toute partie algébriquement indépendante est contenue dans une partie algébriquement indépendante maximale, c.-à-d., dans une base de transcendance de K sur k. Ceci prouve 1).

Démontrons 2). Comme toute partie de L algébriquement indépendante sur k est aussi une partie de K algébriquement indépendante sur k, on obtient que L possède une base de transcendance finie $B = \{b_1, \ldots, b_t\}$, qu'on peut compléter en une base de transcendance

$$\widetilde{B} = B \sqcup C = \{b_1, \ldots, b_t\} \sqcup \{c_1, \ldots, c_s\}$$

de K sur k (où $t + s = r = \text{deg. tr}_k K$). Montrons que L est de degré fini sur $k(B)$. Ceci va résulter du lemme suivant.

Lemme 23.6.7 *C est algébriquement indépendante sur L.*

Démonstration. Sinon, il existe un polynôme $P \in L[X_1, \ldots, X_s]$ non nul tel que $P(c_1, \ldots, c_s) = 0$. Sans perte de généralité, on peut supposer que X_s apparaît dans P, et donc que c_s est algébrique sur $L(C')$, où $C' = \{c_1, \ldots, c_{s-1}\}$. Or,

$$L(c_1, \ldots, c_{s-1}) = k(B \cup C')(L)$$

est algébrique sur $k(B \cup C')$, puisque L est algébrique sur $k(B)$. Donc, d'après la transitivité des extensions entières (23.3.9), c_s est algébrique sur $k(B \cup C')$, une contradiction. Ceci prouve le lemme. □

On peut maintenant achever la preuve du théorème. Soient $\ell_1, \ldots, \ell_n$ des éléments de L linéairement indépendants sur $k(B)$. Montrons qu'ils sont encore linéairement indépendants sur $k(\widetilde{B})$. Supposons que

$$(*) \qquad 0 = F_1\ell_1 + \cdots + F_n\ell_n,$$

avec $F_i \in k(\widetilde{B})$. En chassant les dénominateurs, on se ramène au cas où $F_i \in k[\widetilde{B}]$. On peut alors écrire chaque F_i comme une somme finie :

$$F_i = \sum_{\nu \in \mathbb{N}^s} P_{i,\nu}(b_1, \ldots, b_t) c_1^{\nu_1} \cdots c_s^{\nu_s}.$$

Alors, $(*)$ entraîne, avec des notations évidentes,

$$0 = \sum_{\nu \in \mathbb{N}^s} \left(\sum_{i=1}^{n} P_{i,\nu}(b)\ell_i \right) c^\nu.$$

D'après le lemme, on en déduit $\sum_{i=1}^{n} P_{i,\nu}(b)\ell_i = 0$, pour tout ν, et comme les ℓ_i sont linéairement indépendants sur $k(B)$, il vient $P_{i,\nu} = 0$ pour tout i, ν, et donc $F_i = 0$ pour $i = 1, \ldots, n$. Ceci montre que $\ell_1, \ldots, \ell_n$ sont linéairement indépendants sur $k(\widetilde{B})$. On en déduit que

$$[L : k(B)] \leq [K : k(\widetilde{B})].$$

Or, $[K : k(\widetilde{B})] < \infty$, d'après le lemme 23.6.4. Donc L est une extension de degré fini, et a fortiori de type fini, de $k(B)$, et donc L est une extension de type fini de k. Ceci achève la preuve du théorème. □

24 Corps de rupture et corps de décomposition

24.1 Corps de rupture d'un polynôme

Théorème 24.1.1 (Corps de rupture d'un polynôme irréductible)
Soient k un corps et $P \in k[X]$ un polynôme unitaire irréductible de degré ≥ 2. Alors $K := k[X]/(P)$ est un surcorps de k dans lequel P a au moins une racine, à savoir l'image x de X. On l'appelle le **corps de rupture de P sur k.**

Le couple (K, x) vérifie la propriété universelle suivante : pour toute extension $k \subset L$ telle que P admette dans L une racine α, il existe un **unique** *k-morphisme $\psi : K \to L$ tel que $\psi(x) = \alpha$; son image est le sous-corps $k[\alpha]$ de L. En particulier, ψ est un isomorphisme si $L = k[\alpha]$.*

Démonstration. On a déjà vu que (P) est un idéal maximal, donc K est un corps. Notant x l'image de X dans K, on a $P(x) = 0$ et donc $x \in K$ est bien une racine de P.

Soit $k \subset L$ une extension telle que P admette dans L une racine α. Alors $\mathrm{Irr}_k(\alpha)$ divise P, donc lui est égal puisque P est irréductible et unitaire. Par conséquent, le morphisme de k-algèbres $\phi : k[X] \to L$ défini par $\phi(X) = \alpha$ induit un morphisme $\psi : K \to L$ tel que $\psi(x) = \alpha$. De plus, ce morphisme est unique, puisque $K = k[x]$ est engendré comme k-algèbre par x. Ceci prouve le théorème. □

Exemple 24.1.2 $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$. Plus généralement, montrer que pour tout binôme $P = X^2+bX+c$ tel que $\Delta := b^2-4c$ soit < 0, le corps $\mathbb{R}[X]/(P)$ est isomorphe à $\mathbb{C}$.

Remarque 24.1.3 L'exercice ci-dessus montre que des polynômes différents peuvent avoir des corps de rupture isomorphes.

Définition 24.1.4 *Soit $P \in k[X]$ irréductible. Il est commode de dire qu'une extension K de k est un corps de rupture de P sur k si $K \cong k[X]/(P)$.*

Proposition 24.1.5 *Soit $K = k(\alpha)$ une extension algébrique monogène et soient $P = \mathrm{Irr}_k(\alpha)$ et $d = \deg P = \deg_k(\alpha)$. Alors :*

1) *K est un corps de rupture de P sur k.*

2) *Pour toute extension L/k, le nombre de k-morphismes $K \to L$ est égal au nombre de racines de P dans L. Par conséquent, on a*

$$\#\mathrm{Hom}_{k\text{-}alg.}(K, L) \leq \deg P,$$

avec égalité si et seulement si P a d racines distinctes dans L.

Démonstration. D'après le théorème, il existe un (unique) isomorphisme de $k[X]/(P)$ sur le sous-corps de K engendré par α, envoyant X sur α. Ceci prouve 1).

Pour tout k-morphisme $\phi : K \to L$, $\phi(\alpha)$ est une racine de P dans L. Réciproquement, comme $K \cong k[X]/(P)$, alors toute racine β de P dans L définit un morphisme de k-algèbres $\phi_\beta : K \to L$ tel que $\phi_\beta(\alpha) = \beta$, et évidemment ces morphismes sont deux à deux distincts. Ceci prouve 2). □

Exemple 24.1.6 Soient $k = \mathbb{Q}$ et $P = X^3 - 2$. Alors P est irréductible sur $\mathbb{Q}$, car il n'a pas de racine dans $\mathbb{Q}$. Notons $\sqrt[3]{2}$ la racine cubique réelle de 2 et $j = \exp(2i\pi/3)$, $j^2 = \exp(4i\pi/3)$ les racines primitives de l'unité d'ordre 3 dans $\mathbb{C}$. Les racines de P dans $\mathbb{C}$ sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ et chacun des sous-corps suivants de $\mathbb{C}$:

$$\mathbb{Q}[\sqrt[3]{2}], \quad \mathbb{Q}[j\sqrt[3]{2}], \quad \mathbb{Q}[j^2\sqrt[3]{2}]$$

est un corps de rupture de P. Bien que $\mathbb{Q}$-isomorphes, ces trois sous-corps de $\mathbb{C}$ sont deux à deux distincts. En effet, $\mathbb{Q}[\sqrt[3]{2}]$ est contenu dans $\mathbb{R}$, donc distinct des deux autres. Si l'on avait $\mathbb{Q}[j\sqrt[3]{2}] = \mathbb{Q}[j^2\sqrt[3]{2}]$, alors ce corps, disons K, contiendrait j et donc $\sqrt[3]{2}$, donc contiendrait $\mathbb{Q}[\sqrt[3]{2}]$. Comme ces deux corps sont de même dimension $\deg P = 3$ sur $\mathbb{Q}$, on aurait $\mathbb{Q}[\sqrt[3]{2}] = K$, ce qui n'est pas le cas.

24.2 Corps de décomposition d'un polynôme

Définition 24.2.1 *Soient $k \subseteq K$ une extension de corps et $P \in k[X]$ un polynôme de degré $n \geq 1$. On dit que P est* **scindé** *dans $K[X]$ (on dit aussi : sur K) si P se décompose dans $K[X]$ comme un produit de facteurs linéaires :*

$$P = a\prod_{i=1}^{d}(X - \alpha_i),$$

où a est le coefficient dominant de P, et $\alpha_1, \ldots, \alpha_n \in K$ sont les racines de P, comptées avec leur multiplicité (c.-à-d., non nécessairement distinctes). Dans ce cas, on dit aussi que P **a toutes ses racines dans** *K.*

Définition 24.2.2 *Soit $P \in k[X]$ un polynôme non constant. On dit qu'une extension K de k est un* **corps de décomposition de** *P* **sur** *k si elle vérifie les deux conditions suivantes :*

1) P a toutes ses racines dans K, c.-à-d., est scindé dans $K[X]$.

2) K est engendré sur k par les racines de P. En particulier, K est de degré fini sur k, d'après la proposition 23.5.6.

Théorème 24.2.3 (Corps de décomposition d'un polynôme)
Pour chaque corps k, tout $P \in k[X]$ de degré $n \geq 1$ admet un corps de décomposition sur k, unique à k-isomorphisme près.

Démonstration. On va démontrer l'existence par récurrence sur $n = \deg P$. Si $n = 1$, alors $P = aX + b = a(X - b/a)$ et k est un corps de décomposition de P. Supposons $n \geq 2$ et le théorème établi pour tout corps et tout polynôme de degré $< n$, et soit $P \in k[X]$ de degré n.

Soit S un facteur irréductible de P et soit $k_1 = k(\alpha)$ un corps de rupture de P. Alors, dans $k_1[X]$, on a $P = (X-\alpha)Q$, avec $Q \in k_1[X]$ de degré $n-1$. Par hypothèse de récurrence, il existe une extension $k_1 \subset K$ dans laquelle Q a des racines $\alpha_2, \ldots, \alpha_n$ et telle que $K = k_1(\alpha_2, \ldots, \alpha_n)$. Alors, $\alpha, \alpha_2, \ldots, \alpha_n$ sont les racines de P dans K, et K est engendré sur k par ces élements. Ceci montre l'**existence** d'un corps de décomposition. □

Pour démontrer l'**unicité**, on aura besoin d'établir le théorème plus général, et très important, qui va suivre. Commençons par le lemme ci-dessous.

Lemme 24.2.4 *Soit $\tau : K \xrightarrow{\sim} K'$ un isomorphisme de corps. Il induit un isomorphisme d'anneaux $\phi_\tau : K[X] \xrightarrow{\sim} K'[X]$, $\sum_i a_i X^i \mapsto \sum_i \tau(a_i)X^i$, qu'on notera encore τ. De plus, pour tout $P \in K[X]$, τ induit un isomorphisme d'anneaux $K[X]/(P) \xrightarrow{\sim} K'[X]/(\tau(P))$.*

Démonstration. L'isomorphisme $\tau : K \xrightarrow{\sim} K'$ munit K', et donc aussi $K'[X]$, d'une structure de K-algèbre. D'après la propriété universelle de $K[X]$, il existe un unique morphisme de K-algèbres $\phi_\tau : K[X] \to K'[X]$ tel que $\phi_\tau(X) = X$, et ϕ_τ vérifie la formule donnée ci-dessus. On obtient de même que l'isomorphisme $\tau^{-1} : K' \xrightarrow{\sim} K$ induit un morphisme

$$\phi_{\tau^{-1}} : K'[X] \xrightarrow{\sim} K[X], \quad \sum_i a_i X^i \mapsto \sum_i \tau^{-1}(a_i) X^i,$$

et il est alors clair que ϕ_τ et $\phi_{\tau^{-1}}$ sont inverses l'un de l'autre. Ceci prouve la première assertion.

Enfin, pour tout $P \in K[X]$, il est clair que ϕ_τ et $\phi_{\tau^{-1}}$ induisent des bijections réciproques entre les idéaux (P) et $(\tau(P))$, et donc entre les anneaux quotients $K[X]/(P)$ et $K'[X]/(\tau(P))$. Ceci prouve le lemme. □

Théorème 24.2.5 (Premier théorème fondamental)
Soient $\tau : K \xrightarrow{\sim} K'$ un isomorphisme de corps, $P \in K[X]$ de degré $n \geq 1$ et L, resp. L', un corps de décomposition de P, resp. de $\tau(P)$. Il existe un isomorphisme $\sigma : L \xrightarrow{\sim} L'$ tel que $\sigma|_K = \tau$.

Avant de démontrer ce théorème, observons que le cas particulier $K = K' = k$ et $\tau = \mathrm{id}_K$, fournit l'unicité du corps de décomposition :

Corollaire 24.2.6 *Soit $P \in k[X]$ de degré ≥ 1. Le corps de décomposition de P sur k est unique, à k-isomorphisme près.*

Démonstration. Démontrons maintenant le théorème 24.2.5 par récurrence sur le **nombre m de racines de P qui sont dans L mais pas dans K**. Sans perte de généralité, on peut supposer P unitaire. Si $m = 0$, alors

$$P = (X - \lambda_1) \cdots (X - \lambda_n),$$

avec les λ_i dans K. Dans ce cas, $L = K$ et

$$\tau(P) = (X - \tau(\lambda_1)) \cdots (X - \tau(\lambda_n)),$$

avec $\tau(\lambda_i) \in K'$, donc $L' = K'$ et l'on peut prendre $\sigma = \tau$.

Supposons $m > 0$ et le théorème établi pour tout $m' < m$. Soit $P \in K[X]$ ayant exactement m racines dans $L \setminus K$, et soit

$$P = P_1 \cdots P_r \tag{1}$$

sa décomposition en facteurs irréductibles dans $K[X]$. Comme $m > 0$, l'un au moins de ces facteurs, disons P_1, est de degré ≥ 2 et n'a pas de racines dans K.

Par hypothèse, P se scinde dans $L[X]$ comme produit de facteurs (irréductibles !) de degré 1. Comme $L[X]$ est factoriel, l'unicité d'une telle décomposition entraîne que chaque P_i est un produit de certains de ces facteurs linéaires. En particulier, P_1 a toutes ses racines dans L. Soit α l'une d'elles. D'après la proposition 24.1.5, on a un K-isomorphisme

$$\psi : K[X]/(P_1) \xrightarrow{\sim} K[\alpha]. \tag{2}$$

D'autre part,

$$\tau(P) = \tau(P_1) \cdots \tau(P_r), \tag{1'}$$

et, par le même argument que précédemment, chaque $\tau(P_i)$ a toutes ses racines dans L'. Soit β une racine de $\tau(P_1)$ dans L'. D'après la proposition 24.1.5, à nouveau, on a un K'-isomorphisme

$$\psi' : K'[X]/(\tau(P_1)) \xrightarrow{\sim} K'[\beta]. \tag{2'}$$

De plus, d'après le lemme précédent, on a un isomorphisme

$$\phi_\tau : K[X]/(P_1) \xrightarrow{\sim} K'[X]/(\tau(P_1))$$

qui prolonge $\tau : K \xrightarrow{\sim} K'$. Posons $K_1 = K[\alpha]$ et $K_1' = K'[\beta]$. Alors, $\tau_1 := \psi' \circ \phi_\tau \circ \psi^{-1}$ est un isomorphisme $K_1 \xrightarrow{\sim} K_1'$ qui prolonge τ. On a donc le diagramme suivant :

$$\begin{array}{ccccc} K & \subset & K_1 & \subset & L \\ {\scriptstyle\tau}\downarrow \cong & & {\scriptstyle\tau_1}\downarrow \cong & & \\ K' & \subset & K_1' & \subset & L'. \end{array}$$

Maintenant, L (resp. L') est un corps de décomposition sur K_1 (resp. sur K_1') de notre polynôme P (resp. de $\tau(P)$), et le nombre de racines de P dans $L \setminus K_1$ est $< m$. Donc, par hypothèse de récurrence, il existe un isomorphisme $\sigma : L \xrightarrow{\sim} L'$ tel que $\sigma|_{K_1} = \tau_1$. Par conséquent, $\sigma|_K = \tau_1|_K = \tau$. Ceci achève la preuve du théorème. □

Définition 24.2.7 (Extensions quasi-galoisiennes) *On dit que K/k est une extension* **quasi-galoisienne**, *ou* **normale**, *si elle est algébrique et vérifie la propriété suivante : pour tout $\alpha \in K$, le polynôme minimal* $\mathrm{Irr}_k(\alpha)$ *a toutes ses racines dans K.*

Proposition 24.2.8 *Soit $P \in k[X]$ de degré $n \geq 1$ et K un corps de décomposition de P sur k. L'extension $k \subset K$ est quasi-galoisienne.*

Démonstration. Soit $\alpha \in K$ et soit $S = \mathrm{Irr}_k(\alpha)$ son polynôme minimal sur k. Soit L un corps de décomposition sur K de S. Alors PS a toutes ses racines dans L et celles-ci engendrent L sur k. Par conséquent, L est un corps de décomposition de PS sur k.

Soit β une racine de S dans L. D'après le théorème 24.1.1, il existe un (unique) k-isomorphisme $\tau : k[\alpha] \xrightarrow{\sim} k[\beta]$ tel que $\tau(\alpha) = \beta$. De plus, d'après le premier théorème fondamental (24.2.5), τ se prolonge en un k-automorphisme σ de L.

Soient $x_1, \ldots, x_m$ les racines distinctes de P dans K ; alors K, resp. $\sigma(K)$, est le sous-corps de L engendré par les x_i, resp. les $\sigma(x_i)$. Or, pour chaque i, $\sigma(x_i)$ est une racine de $\sigma(P) = P$. On en déduit que σ induit une bijection f de $\{1, \ldots, m\}$ telle que $\sigma(x_i) = x_{f(i)}$, pour $i = 1, \ldots, m$. Il en résulte que $\sigma(K) = K$. Comme $\sigma(\alpha) = \tau(\alpha) = \beta$, on obtient ainsi que $\beta \in K$. Ceci montre que S a toutes ses racines dans K (et donc $L = K$). La proposition est démontrée. □

24.3 Le groupe des k-automorphismes d'une extension

Définition 24.3.1 *1) Soit K/k une extension algébrique. On note* $\mathrm{Aut}(K/k)$ *le groupe des k-automorphismes de K.*

2) Posons $G = \mathrm{Aut}(K/k)$ et soit $\alpha \in K$. L'ensemble $\{g(\alpha) \mid g \in G\}$ des transformés de α par les éléments de G s'appelle **l'orbite** *de α sous l'action de G, ou simplement la G-orbite de α, et se note $G\alpha$. D'autre part, l'ensemble*

$$G_\alpha := \{g \in G \mid g(\alpha) = \alpha\}$$

est un **sous-groupe** *de G, on l'appelle le stabilisateur de α. Il est parfois aussi noté* $\mathrm{Stab}_G(\alpha)$.

Proposition 24.3.2 *Soit $k \subset K$ une extension algébrique et soit $\alpha \in K$.*

1) *Pour tout $\sigma \in \mathrm{Aut}(K/k)$, $\sigma(\alpha)$ est racine de* $\mathrm{Irr}_k(\alpha)$.

2) *Posons $G = \mathrm{Aut}(K/k)$. L'orbite $G\alpha$ est un ensemble fini de cardinal $\leq \deg_k(\alpha)$, et* $\mathrm{Irr}_k(\alpha)$ *est divisible par le polynôme*

$$\prod_{\beta \in G\alpha} (X - \beta).$$

Démonstration. 1) Posons $P = \mathrm{Irr}_k(\alpha)$ et écrivons $P = X^d + a_1 X^{d-1} + \cdots + a_d$, où $d = \deg_k(\alpha)$. Soit $\sigma \in \mathrm{Aut}(K/k)$. Alors

$$0 = \sigma(P(\alpha)) = \sigma(\alpha)^d + a_1(\sigma(\alpha))^{d-1} + \cdots + a_d = P(\sigma(\alpha)).$$

Ceci montre que $\sigma(\alpha)$ est racine de P.

Par conséquent, $X - g(\alpha)$ divise P, pour tout $g \in G = \mathrm{Aut}(K/k)$. Or, d'après l'unicité de la décomposition en facteurs irréductibles, P a au plus d diviseurs irréductibles distincts. Il en résulte que l'orbite $G\alpha$ est finie, de cardinal $\leq d$, et que P est divisible par le produit des $X - \beta$, pour $\beta \in G\alpha$. La proposition est démontrée. □

Une question Au vu de la proposition précédente, on est conduit à se demander si, pour tout $\alpha \in K$, on a l'égalité

$$(*) \qquad \mathrm{Irr}_k(\alpha) = \prod_{\beta \in G\alpha} (X - \beta) \quad ?$$

En cas de réponse positive, on obtiendrait que la connaissance du groupe G (et de son action sur K) permet de déterminer, pour tout $\alpha \in K$, le polynôme minimal $\mathrm{Irr}_k(\alpha)$ et donc la structure du sous-corps $k[\alpha] \subset K$.

On va voir dans un instant qu'il faut imposer certaines hypothèses, assez naturelles, sur l'extension $k \subset K$ pour que $(*)$ soit vraie. On verra ensuite que, sous ces hypothèses, la structure du groupe G et des ses sous-groupes détermine complètement la structure de l'extension $k \subset K$ et des sous-corps L tels que $k \subset L \subset K$ (on dira qu'un tel L est une **extension intermédiaire**).

Exemples 24.3.3 1) Une première obstruction, évidente, à $(*)$ est que K peut ne pas contenir suffisamment de racines de $\mathrm{Irr}_k(\alpha)$. Par exemple, soient $k = \mathbb{Q}$, $P = X^3 - 2$ et ξ l'une quelconque des racines de P dans $\mathbb{C}$. On a vu dans l'exemple 24.1.6 que ξ est la seule racine de P dans $\mathbb{Q}[\xi]$. Donc $g(\xi) = \xi$, pour tout $g \in G := \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\xi])$, et comme $\mathbb{Q}[\xi]$ est engendré sur $\mathbb{Q}$ par ξ, on obtient en fait que $G = \{1\}$.

En fait, si $(*)$ est vérifiée, alors $\mathrm{Irr}_k(\alpha)$ a toutes ses racines dans K. Donc, pour que $(*)$ soit vérifiée pour tout $\alpha \in K$, il est **nécessaire** de supposer que l'extension $k \subset K$ soit **quasi-galoisienne**.

2) Une autre obstruction, plus subtile, est la suivante. Le terme de droite dans $(*)$ est un polynôme dont les racines sont deux à deux distinctes, c.-à-d., où chacune est de multiplicité 1. Or, pour certains corps k de caractéristique $p > 0$, il existe des extensions $k \subset K$ et $\alpha \in K$ tels que $\mathrm{Irr}_k(\alpha)$ ait des racines

multiples. (Une telle situation ne peut se produire si $\mathrm{car}(k) = 0$ ou si k est un corps fini.) Ceci conduit à étudier la notion de séparabilité.

25 Extensions séparables et théorème de l'élément primitif

25.1 Polynômes et extensions séparables

Définition 25.1.1 *Soit $P \in k[X]$ un polynôme* **irréductible**. *On dit que P est* **séparable sur** *k s'il vérifie la propriété suivante : ses racines $\alpha_1, \ldots, \alpha_n$ dans un corps de décomposition K de P sur k sont deux à deux distinctes, c.-à-d., chacune de multiplicité* 1.

Ceci ne dépend pas du corps de décomposition K. En effet, si K' est un autre corps de décomposition, il existe, d'après le théorème 24.2.5, un k-isomorphisme $\sigma : K \xrightarrow{\sim} K'$. On a $\sigma(P) = P$, puisque P est à coefficients dans k. D'autre part, on a dans $K[X]$, $P = a(X - \alpha_1) \cdots (X - \alpha_n)$, où $a \in k$ est le coefficient dominant de P, et appliquant σ à cette égalité on obtient la décomposition $P = \sigma(P) = a(X - \sigma(\alpha_1)) \cdots (X - \sigma(\alpha_n))$. Par conséquent, les racines de P dans K' sont les $\sigma(\alpha_i)$, qui sont deux à deux distinctes.

Lemme 25.1.2 *Soient $P \in k[X]$ séparable, L une extension de k, et Q un diviseur de P dans $L[X]$. Alors Q est séparable sur L.*

Démonstration. Soit K un corps de décomposition de P sur L. Alors Q est scindé dans L et ses racines sont parmi celles de P donc sont deux à deux distinctes. □

Définition 25.1.3 *Soit $k \subset K$ une extension algébrique.*

1) On dit que $\alpha \in K$ est **séparable sur** *k si son polynôme minimal $\mathrm{Irr}_k(\alpha)$ est séparable sur k.*

2) On dit que l'extension $k \subset K$ **est séparable** *si tout $\alpha \in K$ est séparable sur k.*

Proposition 25.1.4 *Soient $k \subset L \subset K$ des extensions de corps. Si K/k est séparable, L/k et K/L le sont aussi.*

Démonstration. Il est clair que L/k est séparable ; montrons que K/L l'est aussi. Soit $x \in K$. Par hypothèse, $\mathrm{Irr}_k(x)$ est séparable. Or, il est multiple, dans $L[X]$, de $\mathrm{Irr}_L(x)$. Donc ce dernier est séparable, d'après le lemme précédent. □

On a introduit plus haut la notion de séparabilité pour un polynôme $P \in k[X]$ **irréductible**. Pour la suite, il est commode d'étendre cette notion à un polynôme non constant quelconque, de la façon suivante.

Définition 25.1.5 *Soit $P \in k[X]$, non constant, et soit $P = P_1 \cdots P_r$ sa décomposition en facteurs irréductibles dans $k[X]$. On dit que P est* **séparable** *sur k si chaque P_i l'est.*

Lemme 25.1.6 *Soit $k \subset K$ une extension séparable et quasi-galoisienne, de degré fini. Alors K est le corps de décomposition sur k d'un polynôme séparable.*

Démonstration. Soient $\alpha_1, \ldots, \alpha_n$ des générateurs de K sur k. Posons $P_i = \mathrm{Irr}_k(\alpha_i)$. Par hypothèse, chaque P_i a toutes ses racines dans K et est séparable. Alors le polynôme $P = P_1 \cdots P_r$ est séparable, et K est un corps de décomposition de P sur k. Ceci prouve le lemme. □

25.2 Racines multiples et séparabilité

Élucidons maintenant la notion de polynôme séparable.

Définition 25.2.1 (L'opérateur de dérivation) *Soit k un corps. Pour tout élément $P = a_0 + a_1X + \cdots + a_nX^n$ de $k[X]$, on pose*

$$P' = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

On l'appelle le **polynôme dérivé** *de P. On notera D l'application $P \mapsto P'$; on voit facilement que c'est un endomorphisme k-linéaire de $k[X]$.*

Lemme 25.2.2 *Pour tout $P, Q \in k[X]$, on a $D(PQ) = PD(Q) + D(P)Q$, c.-à-d., $(PQ)' = PQ' + P'Q$.*

Démonstration. Les deux termes de l'égalité à démontrer étant bilinéaires en (P, Q), il suffit de vérifier cette égalité lorsque $P = X^m$ et $Q = X^n$. Dans ce cas, les deux termes valent $(m+n)X^{m+n-1}$. Ceci prouve le lemme. □

Proposition 25.2.3 *Soit $P \in k[X]$ non constant. Les assertions suivantes sont équivalentes :*

1) *P a une racine multiple dans un (et donc dans tout) corps de décomposition de P sur k ;*

2) *P et P' ont une racine commune dans une extension de k ;*

3) *Le* pgcd *de P et P' est de degré ≥ 1.*

Démonstration. Soit K un corps de décomposition de P sur k. Supposons que P ait dans K une racine α de multiplicité $n \geq 2$. Alors, $P = (X-\alpha)^n Q$, avec $Q \in K[X]$. D'après le lemme précédent, appliqué dans $K[X]$, on obtient

$$(*) \qquad P' = n(X-\alpha)^{n-1}Q + (X-\alpha)^n Q',$$

d'où $P'(\alpha) = 0$. Ceci montre que 1) $\Rightarrow$ 2).

Soit D un pgcd de P et P'. D'après le théorème de Bezout, il existe $A, B \in k[X]$ tels que $AP + BP' = D$. Si α est une racine commune de P et P' dans une extension L de k, c'est aussi une racine de D, d'où $\deg D \geq 1$. Ceci montre que 2) $\Rightarrow$ 3).

Réciproquement, si D est de degré ≥ 1, il admet une racine α dans une extension L de k, et α est une racine de P et P', puisque D divise P et P'. Nécessairement, α est une racine multiple de P. En effet, on aurait sinon, dans $L[X]$,

$$P = (X-\alpha)Q \quad \text{avec} \quad Q(\alpha) \neq 0,$$

d'où, d'après $(*)$ ci-dessus, $P'(\alpha) = Q(\alpha) \neq 0$. Donc, α est une racine de P dans L de multiplicité ≥ 2. Soit K un corps de décomposition de P sur $k(\alpha)$. Alors, K est un corps de décomposition de P sur k, et P a une racine multiple dans K. Ceci prouve 3) $\Rightarrow$ 1). La proposition est démontrée. □

Corollaire 25.2.4 *Soit $P \in k[X]$ irréductible ; P est séparable $\Leftrightarrow$ $P' \neq 0$.*

Démonstration. Soit $D = \mathrm{pgcd}(P, P')$. D'après la proposition précédente, il suffit de montrer que $\deg D \geq 1 \Leftrightarrow P' = 0$. L'implication $\Leftarrow$ est évidente. Supposons $\deg D \geq 1$. Comme P est irréductible, D est associé à P donc de degré $\deg P$. D'autre part, P' est nul ou bien de degré $< \deg P$. Comme D divise P', on a nécessairement $P' = 0$. Ceci prouve le corollaire. □

Corollaire 25.2.5 *Si $\mathrm{car}(k) = 0$, tout polynôme est séparable.*

Démonstration. D'après la définition, il suffit de montrer que tout polynôme irréductible P est séparable. On peut supposer P unitaire, disons de degré d. Alors le terme dominant de P' est dX^{d-1}, qui est non nul car puisque $\mathrm{car}(k) = 0$. Donc P est séparable, d'après le corollaire précédent. □

Remarque 25.2.6 Soit $k = \mathbb{F}_p(T)$ le corps des fractions rationnelles sur $\mathbb{F}_p$. On peut montrer que le polynôme $P = X^p - T \in k[X]$ est irréductible. D'autre part, il vérifie $P' = pX^{p-1} = 0$. Il n'est donc pas séparable sur k.

25.3 Caractérisation de la séparabilité en termes de morphismes

Remarque 25.3.1 Pour arriver au « théorème principal de la théorie de Galois » 26.6.1, il y a essentiellement deux approches. On peut démontrer directement le théorème d'Artin 26.3.1 en étudiant deux systèmes linéaires homogènes (26.2.5 et 26.3.1), et ensuite déduire le théorème de l'élément primitif 26.7.3 du théorème principal 26.6.1, combiné avec la proposition 25.4.5. C'est l'approche originelle d'Emil Artin ([Art]). Elle est plus simple et, peut-être, plus pédagogique.

On peut, d'autre part, caractériser les extensions séparables en termes de morphismes (théorème 25.3.3 ci-dessous), puis démontrer le théorème de l'élément primitif 25.4.2 et son corollaire 25.4.4, et en déduire le théorème d'Artin (26.4.1). C'est l'approche suivie dans [Ne04], [Esc], et [La]. Elle est plus courte, mais peut-être moins pédagogique, car l'intérêt du théorème 25.3.3 ci-dessous n'apparaît que plus tard.

Définition 25.3.2 *Soit K/K_1 une extension de corps et soit $\tau : K_1 \to L$ un morphisme de corps (nécessairement injectif!). On note* $\mathrm{Hom}_\tau(K, L)$ *l'ensemble des morphismes de corps $\phi : K \to L$ tels que $\phi|_{K_1} = \tau$. Si l'on identifie K_1 à son image $\tau(K_1)$, ce n'est autre que l'ensemble des K_1-morphismes de K vers L.*

Théorème 25.3.3 (Séparabilité sur k et k-morphismes) *Soit K/k une extension de degré fini.*

1) *Pour toute extension L/k, on a*

$$(*) \qquad \#\mathrm{Hom}_{k\text{-}alg.}(K, L) \leq [K : k],$$

et si l'égalité a lieu pour un certain L alors l'extension K/k est séparable.

2) *Réciproquement, si K/k est séparable alors l'égalité a lieu pour tout L contenant un corps de décomposition sur K du produit des polynômes minimaux sur k d'un système de générateurs de K sur k.*

3) *Pour toute extension K'/k, il existe une extension M de K' telle que* $\mathrm{Hom}_{k\text{-}alg.}(K, M) \neq \emptyset$.

Démonstration. Par hypothèse, $K = k[x_1, \ldots, x_r]$. On va montrer 1) et 2) par récurrence sur r. Si $r = 1$, c.-à-d., si $K = k[x]$, l'assertion 1) et l'implication $\Leftarrow$ de 2) résultent de la proposition 24.1.5. D'autre part, si $k[x]$ est séparable sur k, l'égalité est obtenue dans $(*)$ si L est un corps de décomposition sur k de $\mathrm{Irr}_k(x)$. Ceci prouve 1) et 2) pour $r = 1$. De plus, on

obtient 3) en prenant pour M un corps de décomposition sur K' de $\mathrm{Irr}_k(x)$. On peut donc supposer $r \geq 2$ et le résultat établi pour $r-1$.

Posons $K_1 = k[x_1]$. Alors, d'une part,

$$\#\mathrm{Hom}_{k\text{-alg.}}(K_1, L) \leq [K_1 : k]. \tag{1}$$

D'autre part, soit $\tau : K_1 \to L$ un k-morphisme. Par hypothèse de récurrence, appliquée à l'extension $K_1 \subseteq K$, on a

$$\#\mathrm{Hom}_{\tau}(K, L) \leq [K : K_1]. \tag{2}$$

Or, si $\phi : K \to L$ est un k-morphisme, alors sa restriction ϕ_1 à K_1 est un k-morphisme, et $\phi \in \mathrm{Hom}_{\phi_1}(K, L)$. Combiné avec (1), (2) et la multiplicativité des degrés, ceci donne :

$$\#\mathrm{Hom}_{k\text{-alg.}}(K, L) \leq [K : K_1][K_1 : k] = [K : k], \tag{3}$$

et de plus, pour un L fixé, l'égalité a lieu dans (3) si et seulement si elle a lieu dans (1) et (2). Ceci prouve 1), ainsi que l'implication $\Leftarrow$ dans 2). En effet, supposons que pour un certain L on ait égalité dans (3), alors on a aussi égalité dans (1), et donc x_1 est séparable sur k. Mais comme on peut choisir x_1 arbitrairement dans K, ceci montre que K est séparable sur k.

Réciproquement, supposons K/k séparable. Alors, d'après la proposition 25.1.4, les extensions K_1/k et K/K_1 sont séparables. Posons $P_i = \mathrm{Irr}_k(x_i)$, pour $i = 1, \ldots, n$, et soit L un corps de décomposition sur K de $P_1 \cdots P_n$. Alors, par hypothèse de récurrence, on a égalité dans (1) et (2), et donc aussi dans (3). Ceci achève la preuve des assertions 1) et 2).

De même, on montre par récurrence sur r que $\mathrm{Hom}_{k\text{-alg.}}(K, M) \neq \emptyset$, pour tout corps M contenant un corps de décomposition sur K' de $P_1 \cdots P_r$. Ceci achève la preuve du théorème. □

Corollaire 25.3.4 1) *Soit K/k une extension algébrique et $x \in K$. Si x est séparable sur k, alors l'extension $k[x]/k$ est séparable.*

2) *Si K/E et E/k sont des extensions de degré fini séparables, alors K/k l'est aussi.*

Démonstration. 1) Soit L un corps de décomposition sur K de $\mathrm{Irr}_k(x)$. D'après la proposition 24.1.5, on a

$$\#\mathrm{Hom}_{k\text{-alg.}}(k[x], L) = \deg_k(x) = [k[x] : k].$$

Par conséquent, d'après le théorème précédent, l'extension $k \subseteq k[x]$ est séparable. Ceci prouve 1).

Écrivons $K = E[x_1, \ldots, x_s]$ et $E = k[x_{s+1}, \ldots, x_r]$ et notons P_i le polynôme minimal de x_i sur k. Soit L un corps de décomposition de $P_1 \cdots P_r$ sur K. D'après le théorème, on a

$$\#\mathrm{Hom}_{k\text{-alg.}}(E, L) = [E : k],$$

et tout k-morphisme $\tau : E \to L$ se prolonge en exactement $[K : E]$ morphismes $K \to L$. Par conséquent, on a

$$\#\mathrm{Hom}_{k\text{-alg.}}(K, L) = [K : E][E : k] = [K : k],$$

et donc, d'après le théorème, l'extension K/k est séparable. □

25.4 Le théorème de l'élément primitif

Définition 25.4.1 *On rappelle qu'une extension $k \subset K$ est dite* **monogène** *si K est engendré sur k par un seul élément, c.-à-d., s'il existe $\xi \in K$ tel que $K = k(\xi)$. Dans ce cas, on dit que ξ est un* **élément primitif** *de K sur k.*

Théorème 25.4.2 (Théorème de l'élément primitif) *Soit K/k une extension* **séparable de degré fini**. *Alors K admet un élément primitif sur k.*

Démonstration. On verra dans le chapitre suivant que si k est un corps fini et K/k une extension de degré fini, alors le groupe multiplicatif $K^\times$ est cyclique, et donc $K = k[\xi]$ pour tout générateur ξ de $K^\times$.

On peut donc supposer k infini. Posons $n = [K : k]$. Comme K/k est séparable, il existe une extension L de k et des k-morphismes $K \to L$ deux à deux distincts $\tau_1, \ldots, \tau_n$. Alors $\mathrm{Ker}(\tau_i - \tau_j)$ est un sous-espace propre de K, pour tout $i \neq j$.

Lemme 25.4.3 *Un espace vectoriel V sur un corps infini k n'est pas réunion finie de sous-espaces propres $V_1, \ldots, V_t$.*

Démonstration. C'est clair si $t = 1$. Donc on peut supposer $t \geq 2$ et le résultat établi pour $t - 1$. Alors, il existe $u, v \in V$ tels que $u \notin V_t$ et $v \notin V_1 \cup \cdots \cup V_{t-1}$. Supposons

$$V = V_1 \cup \cdots \cup V_t.$$

Alors $v \in V_t$. Comme l'ensemble des $x_\mu := u + \mu v$, pour $\mu \in k$, est infini, il existe $\mu \neq \nu$ dans k tels que x_μ et x_ν appartiennent au même V_j. On ne peut

avoir $j = t$, car sinon on aurait $u \in V_t$, une contradiction. Donc $j < t$, et V_j contient $x_\mu - x_\nu = (\mu - \nu)v$ donc aussi v, une contradiction. Ceci prouve le lemme. □

On peut maintenant achever la preuve du théorème de l'élément primitif. D'après le lemme, il existe $x \in K$ n'appartenant à aucun des $\mathrm{Ker}(\tau_i - \tau_j)$. Alors, les $\tau_i(x)$ sont deux à deux distincts. Comme ce sont des racines, dans L, de $\mathrm{Irr}_k(x)$, ceci entraîne $\deg_k(x) \geq n$, et donc

$$n \leq \deg_k(x) = [k(x) : k] \leq [K : k] = n.$$

Il en résulte que $k(x) = K$. Le théorème est démontré. □

Corollaire 25.4.4 *Soit K/k une extension algébrique séparable. On suppose qu'il existe $n \in \mathbb{N}^*$ tel que $\deg_k(x) \leq n$ pour tout $x \in K$. Alors $[K : k] \leq n$.*

Démonstration. Quitte à diminuer n, on peut supposer qu'il existe $x \in K$ tel que $\deg_k(x) = n$. Soit $y \in K$ arbitraire. Comme l'extension $k \subseteq k[x, y]$ est séparable de degré fini, elle admet un élément primitif z. On a donc $k[x] \subseteq k[z]$, et cette inclusion est une égalité par maximalité de $\deg_k(x)$. Donc $k[x] = k[z] = k[x, y]$, d'où $y \in k[x]$. Ceci montre que $K = k[x]$. □

Pour terminer cette section, signalons aussi la proposition suivante.

Proposition 25.4.5 *Soit $k \subset K$ une extension de degré fini. Alors K admet un élément primitif sur $k \Leftrightarrow$ le nombre d'extensions intermédiaires est fini.*

Démonstration. $\Rightarrow$ Supposons $K = k[\xi]$ et soit $P = \mathrm{Irr}_k(\xi)$. Soit $k \subseteq L \subseteq K$ une extension intermédiaire et soit $Q = \mathrm{Irr}_L(\xi)$. Alors $[K : L] = \deg Q$. Observons que Q divise P dans $L[X]$, donc a fortiori dans $K[X]$. Par conséquent, il n'y a qu'un nombre fini de possibilités pour Q.

Soit $L' \subseteq L$ le sous-corps de L engendré sur k par les coefficients de Q. Comme Q est irréductible dans $L[X]$, il l'est aussi dans $L'[X]$. Par conséquent, $K = L'[\xi]$ est de degré $\deg Q$ sur L'. On a donc

$$[K : L] = \deg Q = [K : L'],$$

d'où $[L : L'] = 1$, c.-à-d., $L = L'$. Ceci montre que L est entièrement déterminé par la donnée de Q. Comme il n'y a qu'un nombre fini de tels Q, ceci prouve la finitude du nombre des extensions intermédiaires.

Démontrons maintenant l'implication $\Leftarrow$ sous l'hypothèse que k est **infini**. (On verra le cas des corps finis dans le prochain chapitre).

Choisissons un élément $\xi \in K$ tel que $\deg_k(\xi)$ soit maximal, c.-à-d., tel que $k[\xi]$ soit de degré maximal parmi les sous-extensions simples contenues dans K. Ceci est possible puisque K est de degré fini sur k. On va montrer que $k[\xi] = K$.

Soit $\alpha \in K$. Pour t variant dans k, posons $\xi_t = \xi + t\alpha$ et notons L_t le sous-corps de K engendré par ξ_t. Ces corps sont en nombre fini et donc, k étant supposé infini, il existe des éléments $s \neq t$ dans k tels que $L_s = L_t$. Ce corps contient alors $(s-t)\alpha$, donc α, et aussi ξ. Donc,

$$k[\xi] \subseteq k[\xi, \alpha] \subseteq k[\xi_s].$$

La maximalité de $\deg_k(\xi)$ entraîne alors que les inclusions ci-dessus sont des égalités, d'où $\alpha \in k[\xi]$. Comme $\alpha \in K$ était arbitraire, ceci montre que $k[\xi] = K$. Le théorème est démontré. □

Remarque 25.4.6 Soit $K = \mathbb{F}_p(X, Y)$ le corps des fractions rationnelles à deux variables sur $\mathbb{F}_p$, et soit k le sous-corps engendré par X^p et Y^p. On verra dans le chapitre suivant que $[K : k] = p^2$, et que tout élément $\alpha \in K$ vérifie $\alpha^p \in k$. Par conséquent, toute extension monogène $k[\alpha] \subset K$ est de degré $\leq p$ (et $= p$ si $\alpha \notin k$). Ceci montre que l'extension $k \subset K$ n'est pas monogène, donc admet une infinité de corps intermédiaires.

26 Extensions galoisiennes et correspondance de Galois

26.1 Extensions galoisiennes

Définition 26.1.1 *Soient $k \subset K$ une extension algébrique et H un sous-groupe de $G = \mathrm{Aut}(K/k)$. On pose*

$$K^H = \{x \in K \mid \forall h \in H,\ h(x) = x\}.$$

C'est un sous-corps de K contenant k, appelé **corps des invariants de** *H dans K.*

Remarque 26.1.2 L'exemple de $k = \mathbb{Q} \subset K = \mathbb{Q}[\sqrt[3]{2}]$ (*cf.* 24.3.3) montre que l'on peut avoir $k \neq K^G$.

Définition 26.1.3 (Extensions galoisiennes) *Une extension algébrique $k \subset K$ est dite* **galoisienne** *si, posant $G = \mathrm{Aut}(K/k)$, l'on a $K^G = k$. Dans ce cas, on dit que G est le* **groupe de Galois** *de l'extension, et on le note*

$\mathrm{Gal}(K/k)$. *De plus, pour tout* $\alpha \in K$, *les éléments* $g(\alpha)$, *pour* $g \in \mathrm{Gal}(K/k)$, *s'appellent les* **conjugués** *sur* k *de* α *(dans* K*).*

Théorème 26.1.4 (Propriétés des extensions galoisiennes)
Soit $k \subset K$ *une extension* **galoisienne** *et soit* $G = \mathrm{Aut}(K/k)$.

1) *Pour tout* $\alpha \in K$, *on a*

$$(*) \qquad \mathrm{Irr}_k(\alpha) = \prod_{\beta \in G\alpha} (X - \beta);$$

en particulier, l'orbite $G\alpha$ *est formée d'exactement* $\deg_k(\alpha)$ *éléments.*

2) *L'extension* $k \subset K$ *est* **quasi-galoisienne** *et* **séparable**. *En particulier, si* $[K : k] < \infty$, K *est le corps de décomposition sur* k *d'un polynôme séparable.*

Démonstration. 1) Posons $Q = \prod_{\beta \in G\alpha}(X - \beta)$; a priori, c'est un élément de $K[X]$. On va montrer que $Q \in k[X]$. Écrivons $Q = X^n + b_1 X^{n-1} + \cdots + b_n$, où $n = |G\alpha|$. Pour montrer que $Q \in k[X]$, il suffit de montrer que $Q = g(Q)$ pour tout $g \in G$, car alors chaque b_i appartiendra à K^G, qui égale k par hypothèse.

Soit $g \in G$. On a

$$g(Q) = \prod_{\beta \in G\alpha} (X - g(\beta)),$$

et donc l'égalité $g(Q) = Q$ est claire, puisque l'application $\beta \mapsto g(\beta)$ est une bijection de l'orbite $G\alpha$, dont la bijjection inverse est $\gamma \mapsto g^{-1}(\gamma)$.

On a donc $Q \in k[X]$. Par conséquent, $\mathrm{Irr}_k(\alpha)$ divise Q, puisque $Q(\alpha) = 0$. D'autre part, d'après la proposition 24.3.2, Q divise $\mathrm{Irr}_k(\alpha)$. On a donc $\mathrm{Irr}_k(\alpha) = Q$, puisque tous deux sont unitaires. Ceci prouve le point 1).

2) De plus, l'égalité $(*)$ montre que les racines de $\mathrm{Irr}_k(\alpha)$ sont toutes dans K, et deux à deux distinctes. Puisque $\alpha \in K$ est arbitraire, ceci montre que l'extension $k \subset K$ est quasi-galoisienne et séparable. Enfin, la dernière assertion résulte du lemme 25.1.6. La proposition est démontrée. □

Théorème 26.1.5 (Second théorème fondamental)
Soient k *un corps et* $P \in k[X]$ *un polynôme séparable de degré* $n \geq 1$. *Soit* K *un corps de décomposition de* P *sur* k *et soit* $G = \mathrm{Aut}(K/k)$. *Alors,* $K^G = k$, *c.-à-d., l'extension* $k \subset K$ *est* **galoisienne**.

Démonstration. On va démontrer le théorème pour toute paire (k, P), en procédant par récurrence sur le **nombre** m **de racines de** P **qui sont**

dans K mais pas dans k. Sans perte de généralité, on peut supposer P unitaire. Si $m = 0$, alors

$$P = (X - \lambda_1) \cdots (X - \lambda_n),$$

avec les λ_i dans k. Dans ce cas, $K = k$, $G = \{1\}$ et il n'y a rien à montrer.

Supposons $m > 0$ et le théorème établi pour tout $m' < m$. Soit $P \in k[X]$ ayant exactement $n - m$ racines dans k, où $n = \deg P$, et soit K un corps de décomposition de P sur k. Alors P a exactement m racines dans $K \setminus k$. Soit

$$P = P_1 \cdots P_r$$

sa décomposition en facteurs irréductibles dans $k[X]$. On peut supposer les P_i unitaires. Comme $m > 0$, l'un au moins de ces facteurs, disons P_1, est de degré $d \geq 2$ et n'a pas de racines dans k. Par hypothèse, P se scinde dans $K[X]$ comme produit de facteurs (irréductibles !) de degré 1. Comme $K[X]$ est factoriel, on en déduit que la même propriété est vérifiée par chacun des P_i ; en particulier par P_1. Donc, dans $K[X]$, P_1 se factorise :

$$P_1 = (X - \alpha_1) \cdots (X - \alpha_d),$$

avec $\alpha_1 = \alpha$ et les $\alpha_i \in K$ deux à deux distincts, puisque P_1 est séparable par hypothèse.

Or, K est un corps de décomposition de P sur $k(\alpha)$, et P est séparable et a moins de m racines dans $K \setminus k(\alpha)$. Donc, par hypothèse de récurrence, le sous-groupe

$$H = \mathrm{Aut}_{k(\alpha)}(K) = \{g \in \mathrm{Aut}(K/k) \mid g(x) = x, \forall x \in k(\alpha)\}$$

vérifie $K^H = k(\alpha)$. D'autre part, d'après la proposition 24.1.5 et le théorème 24.2.5, il existe, pour $i = 2, \ldots, d$, un k-automorphisme σ_i de K tel que $\sigma_i(\alpha) = \alpha_i$.

Soit maintenant $z \in K^G$. Alors $z \in K^H = k(\alpha)$ et donc (puisque $P_1 = \mathrm{Irr}_k(\alpha)$ et $d = \deg P_1$) il existe $a_0, \ldots, a_{d-1} \in k$ tels que

$$z = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}.$$

Soit $i \in \{2, \ldots, d\}$. Appliquant $\sigma_i \in G$ à cette égalité, on obtient :

$$z = a_0 + a_1\alpha_i + \cdots + a_{d-1}\alpha_i^{d-1}.$$

Il en résulte que les d éléments distincts $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ sont tous racines du polynôme

$$Q(X) = (a_0 - z) + a_1X + \cdots + a_{d-1}X^{d-1}.$$

Celui-ci étant de degré $\leq d-1$, il est donc nul. Par conséquent, $z = a_0$ appartient à k. Ceci achève la preuve du théorème. □

Définition 26.1.6 (Groupe de Galois d'un polynôme séparable)
Soient $P \in k[X]$ un polynôme séparable et K un corps de décomposition de P sur k. Le groupe $\mathrm{Gal}(K/k)$ *est noté* $\mathrm{Gal}(P/k)$ *et appelé* **groupe de Galois de P sur k**. *Ceci est licite, car ce groupe ne dépend, à isomorphisme près, que de P. En effet, si K' est un autre corps de décomposition de P sur k, on a vu (théorème 24.2.5) qu'il existe un k-isomorphisme $\tau : K \xrightarrow{\sim} K'$. Alors, l'application $g \mapsto \tau \circ g \circ \tau^{-1}$ est un isomorphisme de* $\mathrm{Gal}(K/k)$ *sur* $\mathrm{Gal}(K'/k)$.

Corollaire 26.1.7 *Soit K un corps de décomposition sur k d'un polynôme séparable de degré ≥ 1 et soit $G = \mathrm{Aut}(K/k)$. Pour tout $\alpha \in K$, on a*

$$\mathrm{Irr}_k(\alpha) = \prod_{\beta \in G\alpha} (X - \beta).$$

Démonstration. Ceci découle du théorème précédent et du théorème 26.1.4. □

Corollaire 26.1.8 (Caractérisation des extensions galoisiennes finies)
Soit $k \subset K$ une extension de degré fini. Les conditions suivantes sont équivalentes :

1) *$k \subset K$ est quasi-galoisienne et séparable ;*
2) *K est le corps de décomposition sur k d'un polynôme séparable ;*
3) *$k \subset K$ est galoisienne.*

Démonstration. On a 1) ⇒ 2) ⇒ 3) ⇒ 1) d'après le lemme 25.1.6, le théorème 26.1.4, et le théorème 26.1.5, respectivement. □

Corollaire 26.1.9 1) *Soit $k \subset K = k[x_1, \ldots, x_n]$ une extension de degré fini. Si chaque x_i est séparable sur k, alors K/k est séparable.*

2) *Si K/k et E/K sont des extensions de degré fini séparables, alors E/k l'est aussi.*

Démonstration. 1) Posons $P_i = \mathrm{Irr}_k(x_i)$ et soit L un corps de décomposition sur K de $P := P_1 \cdots P_n$. D'après les théorèmes 26.1.5 et 26.1.4, L/k est galoisienne donc séparable, et donc K/k est séparable. Ceci prouve 1).

Prouvons 2). Soit $x \in E$. Alors $Q := \mathrm{Irr}_K(x)$ est séparable, et il s'agit de montrer que $\mathrm{Irr}_k(x)$ l'est aussi. On se ramène au cas où l'extension K/k est

galoisienne, de la façon suivante. Avec les notations de 1), soit E' un corps de décomposition sur $K[x]$ de P. Alors, le sous-corps K' de E' engendré par K et les racines de P est galoisien. D'autre part, le polynôme minimal de x sur K' divise Q, donc est séparable. Par conséquent, remplaçant E/K par E'/K', on se ramène au cas où E/K est galoisienne. Soit G son groupe de Galois et soient $Q_1 = Q$, et $Q_2, \dots Q_r$ les conjugués de Q sous l'action de G. Alors, chaque Q_i est séparable, et il en est de même du produit $Q = Q_1 \cdots Q_r \in K[X]$. Mais Q est invariant par G, donc appartient à $k[X]$.

Par conséquent, x est annulé par le polynôme séparable $Q \in k[X]$, et il en résulte que $\mathrm{Irr}_k(x)$ est séparable. Le corollaire est démontré. □

Remarque 26.1.10 Le corollaire 26.1.7 apporte une réponse satisfaisante à la question 24.3 $(*)$, qui nous avait servi de point de départ et motivation pour l'étude du groupe $G = \mathrm{Aut}(K/k)$.

Dans la section suivante, on développera certains résultats sur les groupes, qui permettront d'établir que si $k \subset K$ est une extension galoisienne finie, alors $G = \mathrm{Aut}(K/k)$ est un groupe fini de cardinal $[K : k]$ et la correspondance $H \mapsto K^H$ établit une bijection entre l'ensemble des sous-groupes de G et les extensions intermédiaires $k \subset L \subset K$.

26.2 Indépendance des caractères

Définition 26.2.1 (L'espace des fonctions $X \to K$) *Soient K un corps et X un ensemble arbitraire. On note $\mathcal{F}(X, K)$ l'ensemble de toutes les applications $X \to K$. Il est muni d'une structure d'espace vectoriel : pour $\phi, \psi \in \mathcal{F}(X, K)$ et $a \in K$, on définit $a\phi + \psi$ par $(a\phi + \psi)(g) = a\phi(x) + \psi(x)$, pour tout $x \in X$.*

Soit maintenant G un groupe arbitraire. Parmi toutes les fonctions $\psi : G \to K$, on distingue les suivantes.

Définition 26.2.2 (Caractères) *On dit qu'une fonction $\chi : G \to K$ est un* **caractère** *de G à valeurs dans K si c'est un morphisme de G dans le groupe multiplicatif de K, c.-à-d., si elle vérifie $\chi(1_G) = 1$ et $\chi(gg') = \chi(g)\chi(g')$ pour tout $g, g' \in G$. On note $X_K(G)$ l'ensemble de ces caractères.*

Théorème 26.2.3 (Théorème d'indépendance des caractères)

$X_K(G)$ est une **partie libre** *de $\mathcal{F}(G, K)$, c.-à-d., si $\chi_1, \dots, \chi_n$ sont des caractères distincts et si $a_1, \dots, a_n \in K$ sont tels que $a_1\chi_1 + \cdots + a_n\chi_n = 0$, alors $a_i = 0$ pour tout i.*

Démonstration. Supposons le théorème en défaut et soit n minimal tel qu'il existe une relation

$$a_1\chi_1 + \cdots + a_n\chi_n = 0, \tag{1}$$

avec les χ_i deux à deux distincts et chaque $a_i \neq 0$. Nécessairement, $n \geq 2$. Comme $\chi_1 \neq \chi_2$, il existe $h \in G$ tel que $\chi_1(h) \neq \chi_2(h)$. Soit $g \in G$ arbitraire. Appliquant (1) à hg, on obtient

$$a_1\chi_1(h)\chi_1(g) + \cdots + a_n\chi_n(h)\chi_n(g) = 0. \tag{2}$$

D'autre part, en appliquant (1) à g puis en multipliant par $\chi_1(h)$, on obtient :

$$a_1\chi_1(h)\chi_1(g) + \cdots + a_n\chi_1(h)\chi_n(g) = 0. \tag{3}$$

Soustrayant (3) de (2), on obtient que la fonction

$$a_2(\chi_2(h) - \chi_1(h))\chi_2 + \cdots + a_n(\chi_n(h) - \chi_1(h))\chi_n$$

est identiquement nulle. Comme le coefficient de χ_2 est $\neq 0$, ceci est une relation linéaire non-triviale entre $\chi_2, \ldots, \chi_n$, et ceci contredit la minimalité de n. Ceci démontre le théorème. □

Corollaire 26.2.4 *Soient L et K deux corps. L'ensemble des morphismes de corps $L \to K$ est une partie libre de $\mathcal{F}(L, K)$.*

Démonstration. Soient $\phi_1, \ldots, \phi_n$ des morphismes de corps $L \to K$, deux à deux distincts, et soient $a_1, \ldots, a_n \in K$. Supposons qu'on ait dans $\mathcal{F}(L, K)$ l'égalité

$$a_1\phi_1 + \cdots + a_n\phi_n = 0.$$

Or, la restriction de chaque ϕ_i à $L^\times = L \setminus \{0\}$ est un caractère de $L^\times$ à valeurs dans K. Donc, le théorème précédent entraîne que $a_i = 0$ pour tout i. Ceci prouve le corollaire. □

Proposition 26.2.5 *Soit K un corps et soient $\phi_1, \ldots, \phi_n$ des automorphismes de K, deux à deux distincts. Soit*

$$L = \{x \in K \mid \forall i = 1, \ldots, n,\ \phi_i(x) = x\}.$$

Alors L est un sous-corps de K et $[K : L] \geq n$. En particulier, si G est un groupe fini d'automorphismes de K, alors $[K : K^G] \geq |G|$.

Démonstration. Il est immédiat que L est un sous-corps de K. Observons que chaque ϕ_i est un automorphisme L-linéaire de K, puisque $\phi_i(ab) = \phi_i(a)\phi_i(b) = a\phi_i(b)$, pour tout $a \in L$, $b \in K$.

Posons $r = \dim_L K$ et supposons que $r < n$. Soit $(\varepsilon_1, \ldots, \varepsilon_r)$ une base de K sur L. Considérons le système linéaire suivant, d'inconnues $x_1, \ldots, x_n$:

$$\begin{cases} \phi_1(\varepsilon_1)x_1 + \phi_2(\varepsilon_1)x_2 + \cdots + \phi_n(\varepsilon_1)x_n &= 0 \\ \phi_1(\varepsilon_2)x_1 + \phi_2(\varepsilon_2)x_2 + \cdots + \phi_n(\varepsilon_2)x_n &= 0 \\ \vdots & \\ \phi_1(\varepsilon_r)x_1 + \phi_2(\varepsilon_r)x_2 + \cdots + \phi_n(\varepsilon_r)x_n &= 0. \end{cases}$$

C'est un système à coefficients dans K, homogène, avec $r < n$ équations. Il admet donc au moins une solution non triviale $(a_1, \ldots, a_n) \in K^n \setminus \{0\}$. Alors le système ci-dessus montre que la fonction L-linéaire

$$\phi := a_1\phi_1 + a_2\phi_2 + \cdots + a_n\phi_n$$

s'annule sur la L-base $(\varepsilon_1, \ldots, \varepsilon_r)$ de K, donc est identiquement nulle. Comme $(a_1, \ldots, a_n) \neq 0$, ceci contredit l'indépendance de $\phi_1, \ldots, \phi_n$. Cette contradiction montre que $r \geq n$. La proposition est démontrée. □

26.3 Invariants d'un groupe fini : théorème d'Artin

On peut maintenant démontrer le 3ème théorème fondamental, dû à Emil Artin.

Théorème 26.3.1 (Artin)
Soient K un corps, G un groupe fini d'automorphismes de K, et $L = K^G$ son corps des invariants.

1) *On a $[K : L] = |G|$.*

2) *Par conséquent, $G = \mathrm{Aut}_L(K)$ et $L \subset K$ est une extension galoisienne, de groupe de Galois $\mathrm{Gal}(K/L) = G$.*

Démonstration. 1) Posons $n = |G|$. D'après la proposition 26.2.5, on a $\dim_L K \geq n$. Supposons que $\dim_L K > n$. Alors, posant $r = n + 1$, il existe des éléments $\varepsilon_1, \ldots, \varepsilon_r \in L$ linéairement indépendants sur K. Choisissons une numérotation $\tau_1, \ldots, \tau_n$ des éléments de G telle que $\tau_1 = \mathrm{id}_K$. Considérons, cette fois, le système :

$$(*) \qquad \begin{cases} \varepsilon_1 x_1 + \cdots + \varepsilon_r x_r &= 0 \\ \tau_2(\varepsilon_1)x_1 + \cdots + \tau_2(\varepsilon_r)x_r &= 0 \\ \vdots & \\ \tau_n(\varepsilon_1)x_1 + \cdots + \tau_n(\varepsilon_r)x_r &= 0. \end{cases}$$

C'est un système homogène, à coefficients dans K, de n équations à $r = n+1$ inconnues. Alors $(*)$ admet des solutions non nulles.

Soit $a = (a_1, \ldots, a_r) \in K^r$ une solution non nulle, ayant un nombre minimum s de coordonnées a_i non-nulles. Quitte à changer la numérotation des ε_i, on peut supposer que

$$a = (a_1, \ldots, a_s, 0, \ldots, 0),$$

avec $a_i \neq 0$ pour $i = 1, \ldots, s$. Divisant a par a_s, on se ramène au cas où $a_s = 1$. On a alors les égalités :

$$\tau(\varepsilon_1)a_1 + \cdots + \tau(\varepsilon_s) = 0, \qquad \forall \tau \in G. \tag{1}$$

Comme $\varepsilon_1, \ldots, \varepsilon_s$ sont indépendants sur L, cette égalité pour $\tau = \mathrm{id}_K$ entraîne que $a_1, \ldots, a_{s-1}$ ne sont pas tous dans L. On peut donc supposer $a_1 \notin L$. Alors, il existe $\sigma \in G$ tel que $\sigma(a_1) \neq a_1$.

Appliquons σ aux égalités (1). Comme l'application $\tau \mapsto \tau\sigma$ est une bijection de G, on obtient les égalités

$$\tau(\varepsilon_1)\sigma(a_1) + \cdots + \tau(\varepsilon_s) = 0, \qquad \forall \tau \in G. \tag{2}$$

Soustrayant (2) de (1), on obtient les égalités :

$$\tau(\varepsilon_1)(a_1 - \sigma(a_1)) + \cdots + \tau(\varepsilon_{s-1})(a_{s-1} - \sigma(a_{s-1})) = 0, \qquad \forall \tau \in G. \tag{3}$$

Ceci montre que le r-uplet

$$(a_1 - \sigma(a_1), \ldots, a_{s-1} - \sigma(a_{s-1}), 0, \ldots, 0)$$

est solution du système $(*)$. Il est non nul, car $a_1 \neq \sigma(a_1)$, et a au plus $s-1$ coordonnées non nulles. Ceci contredit la minimalité de s. Cette contradiction montre que l'hypothèse $\dim_K L > n$ est impossible. On a donc $\dim_K L = n$, ce qui prouve le point 1).

Montrons le point 2). Posons $H = \mathrm{Aut}(K/L)$. Alors, par définition, $L \subseteq K^H$. D'autre part, il est clair que $G \subseteq H$, et donc K^H est contenu dans $K^G = L$. Par conséquent, on a $K^H = L$, ce qui montre que K/L est galoisienne.

Enfin, si l'on avait $G \neq H$, alors H contiendrait un élément $\tau_{n+1} \notin G$ et, d'après la proposition 26.2.5, on aurait $[K : K^H] \geq n+1$, ce qui n'est pas le cas. On a donc $G = H = \mathrm{Aut}(K/L)$. Ceci achève la preuve du théorème. □

Remarque 26.3.2 À la fin de la preuve, on ne peut pas immédiatement appliquer le point 1) à G et H pour obtenir que $|G| = [K : L] = |H|$, car on ne sait pas a priori que H est fini. C'est pour cette raison que l'on fait appel à la proposition 26.2.5 : si l'inclusion $G \subset H$ était stricte, on aurait $[K : K^H] > n$.

26.4 Autre démonstration du théorème d'Artin

Théorème 26.4.1 (Artin) *Soient K un corps, G un groupe fini d'automorphismes de K, et $L = K^G$ son corps des invariants.*

1) *On a $[K : L] = |G|$.*

2) *Par conséquent, $G = \mathrm{Aut}_L(K)$ et $L \subset K$ est une extension galoisienne, de groupe de Galois $\mathrm{Gal}(K/L) = G$.*

Démonstration. Soit $x \in K$ arbitraire. D'après la proposition 24.3.2, on a

$$\mathrm{Irr}_L(x) = \prod_{\beta \in Gx} (X - \beta).$$

Donc x est séparable sur L et de degré $\leq |G|$. Par conséquent, d'après le corollaire 25.4.4, on a

$$[K : L] \leq |G|.$$

D'autre part, G est un sous-groupe de $\mathrm{Aut}(K/L)$ et, d'après le théorème 25.3.3 (ou la proposition 26.2.5) on a

$$|\mathrm{Aut}(K/L)| \leq [K : L].$$

Il en résulte que $G = \mathrm{Aut}(K/L)$ et que l'extension K/L est galoisienne. □

26.5 Un rappel sur les groupes

Définition 26.5.1 *Soit G un groupe. Un sous-groupe H est dit* **normal**, *ou* **distingué**, *s'il vérifie $gHg^{-1} = H$, pour tout $g \in G$.*

Exemple 26.5.2 Soit $\phi : G \to G'$ un morphisme de groupes. Son noyau $\ker \phi = \{h \in G \mid \phi(h) = 1\}$ est un sous-groupe normal. En effet, pour tout $h \in \ker \phi$ et $g \in G$, on a

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = 1.$$

De plus, si H est un sous-groupe normal de G, on peut construire le groupe quotient G/H et H est le noyau du morphisme $\pi : G \to G/H$. Rappelons la construction de G/H. Pour tout $g \in G$, on pose

$$gH := \{gh \mid h \in H\}.$$

On l'appelle la **classe à gauche** de g modulo H (la classe à droite étant l'ensemble Hg défini de façon analogue). On note G/H l'ensemble de ces classes à gauche, et $\pi : G \to G/H$ l'application $g \mapsto gH$. On voit que $\pi(g) = \pi(g')$ ssi $g^{-1}g' \in H$.

Proposition 26.5.3 *Soit H un sous-groupe normal de G. Il existe sur G/H une unique structure de groupe telle que $\pi : G \to G/H$ soit un morphisme de groupes. Elle est définie par*

$$(*) \qquad (g_1H)(g_2H) = g_1g_2H.$$

Le noyau du morphisme $G \to G/H$ égale H.

Démonstration. Montrons que la formule $(*)$ fait sens, c.-à-d., que l'élément $(g_1H)(g_2H)$ est bien défini. Pour $i = 1, 2$, soit g_i' un autre élément de g_iH. Alors, $g_i' = g_ih_i$ avec $h_i \in H$ et l'on a

$$g_1'g_2' = g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2.$$

Or, par hypothèse, $g_2^{-1}h_1g_2 \in H$ et il en résulte que $g_1'g_2'H = g_1g_2H$. On vérifie alors facilement que la multiplication définie par $(*)$ est associative, admet pour élément neutre la classe $1H = H$, et que l'inverse de gH est $g^{-1}H$. Donc, G/H est un groupe, et $(*)$ montre que $\pi : G \to G/H$ est un morphisme de groupes surjectif. Enfin, $\ker \pi = \{g \in G \mid gH = H\}$ égale H. La proposition est démontrée. □

Théorème 26.5.4 (Propriété universelle du noyau et théorème fondamental d'isomorphisme)
Soit $\phi : G \to G'$ un morphisme de groupes et soit K un sous-groupe normal de G contenu dans $\ker \phi$.

1) *ϕ se factorise de façon unique à travers G/K, c.-à-d., il existe un unique morphisme de groupes $\overline{\phi} : G/K \to G'$ tel que $\overline{\phi} \circ \pi = \phi$, où π désigne la projection $G \to G/K$.*

2) $\mathrm{Im}(\phi)$ *est un sous-groupe de G' et ϕ induit un isomorphisme de groupes*

$$\overline{\phi} : G/\ker \phi \xrightarrow{\cong} \mathrm{Im}(\phi).$$

Démonstration. La démonstration est analogue à celle du théorème 9.2.5 et est laissée au lecteur. □

26.6 Le couronnement : correspondance de Galois

Théorème 26.6.1 (Théorème principal de la théorie de Galois)
Soit $k \subset K$ une extension galoisienne finie, de groupe G. Pour toute extension intermédiaire $k \subset L \subset K$, on pose

$$\mathrm{Fix}(L) = \{g \in G \mid \forall x \in L,\, g(x) = x\} = \mathrm{Aut}_L(K).$$

1) *Pour tout L, l'extension $L \subset K$ est galoisienne, c.-à-d.,*

$$L = K^{\mathrm{Fix}(L)},$$

et l'on a $[K : L] = |\mathrm{Fix}(L)|$ et $[L : k] = |G|/|\mathrm{Fix}(L)|$.

2) *L'application $H \mapsto K^H$ induit une bijection de l'ensemble des sous-groupes de G sur l'ensemble des extensions intermédiaires $k \subseteq L \subseteq K$. La bijection inverse est donnée par $L \mapsto \mathrm{Fix}(L)$. Ces deux bijections sont* **décroissantes**, *c.-à-d., $H \subseteq H' \Leftrightarrow K^H \supseteq K^{H'}$ et $L \subseteq L' \Leftrightarrow \mathrm{Fix}(L) \supseteq \mathrm{Fix}(L')$.*

3) *Soit L un corps intermédiaire. Pour tout $g \in G$, on a*

$$(*) \qquad \mathrm{Fix}(g(L)) = g\mathrm{Fix}(L)g^{-1}.$$

Par conséquent, l'extension $k \subset L$ est galoisienne ssi $\mathrm{Fix}(L)$ est un sous-groupe distingué de G. Dans ce cas, $\mathrm{Aut}_k(L) \cong G/\mathrm{Fix}(L)$.

4) *Soit L un corps intermédiaire et soit $H = \mathrm{Fix}(L)$. Alors les bijections de* 2) *induisent une bijection entre l'ensemble des sous-extensions $k \subseteq L' \subseteq L$ et l'ensemble des sous-groupes H' de G contenant H. En particulier, il n'y a qu'un nombre fini de tels L'.*

Démonstration. 1) D'après le théorème 26.1.4, K est un corps de décomposition sur k d'un polynôme séparable P. Alors, K est aussi un corps de décomposition de P sur L, pour tout corps intermédiaire L. Par conséquent, d'après le second théorème fondamental (26.1.5), l'extension $L \subset K$ est galoisienne.

Posant $H = \mathrm{Fix}(L) = \mathrm{Aut}_L(K)$, on a donc $K^H = L$ et, d'après le théorème d'Artin 26.3.1, $[K : L] = |H|$ et $[K : k] = |G|$. Comme $[K : k] = [K : L][L : k]$, d'après la proposition 23.5.2, on obtient $[L : k] = |G|/|H|$. Ceci prouve le point 1).

2) Réciproquement, soit H un sous-groupe de G. D'après le théorème d'Artin 26.3.1, l'on a $\mathrm{Fix}(K^H) = H$. Combiné avec le point 1), ceci prouve que les applications $H \mapsto K^H$ et $L \mapsto \mathrm{Fix}(L)$ sont des bijections réciproques. De plus, il est clair que

$$H \subseteq H' \Rightarrow L^{H'} \subseteq L^H \quad \text{et} \quad L \subseteq L' \Rightarrow \mathrm{Fix}(L') \subseteq \mathrm{Fix}(L).$$

La dernière assertion de 2) en découle.

3) Il est clair que $g\mathrm{Fix}(L)g^{-1}$ laisse fixe tout élément de $g(L)$. On a donc $g\mathrm{Fix}(L)g^{-1} \subseteq \mathrm{Fix}(g(L))$, et, de même, $g^{-1}\mathrm{Fix}(g(L))g \subseteq \mathrm{Fix}(L)$. Ceci prouve $(*)$. Posons $H = \mathrm{Fix}(L)$.

Supposons $k \subset L$ galoisienne. Alors L est le corps de décomposition sur k d'un polynôme $P \in k[X]$, c.-à-d., il existe $\alpha_1, \ldots, \alpha_n \in L$ tels que $L = k[\alpha_1, \ldots, \alpha_n]$ et $P = \prod_{i=1}^n (X - \alpha_i)$. Soit $g \in G$. Comme $g(P) = P$, il existe une bijection f de $\{1, \ldots, n\}$ telle que $g(\alpha_i) = \alpha_{f(i)}$ pour $i = 1, \ldots, n$. Comme $g(L)$ est le sous-corps de K engendré par les $g(\alpha_i)$, il en résulte que $g(L) = L$. Alors, $(*)$ entraîne que $gHg^{-1} = H$. Ceci montre que H est un sous-groupe normal de G.

Réciproquement, supposons H normal. Alors, pour tout $g \in G$, on a

$$g(L) = K^{gHg^{-1}} = K^H = L.$$

Par conséquent, l'application de restriction $\pi : g \mapsto g|_L$ induit un morphisme de groupes $G \to \mathrm{Aut}_k(L)$, dont le noyau égale $\mathrm{Fix}(L)$. Son image $\pi(G)$ est un sous-groupe de $\mathrm{Aut}_k(L)$. Il est clair que

$$k \subseteq L^{\mathrm{Aut}_k(L)} \subseteq L^{\pi(G)}.$$

Or, un élément x de L est fixé par $\pi(G)$ ssi il est fixé par G, et ceci est le cas ssi $x \in K^G = k$. Par conséquent, les deux inclusions ci-dessus sont des égalités. Donc $k \subset L$ est galoisienne et de plus, d'après le théorème d'Artin, l'on a $\pi(G) = \mathrm{Aut}_k(L)$. Ceci montre que l'application de restriction π induit un isomorphisme

$$G/\mathrm{Fix}(L) \xrightarrow{\sim} \mathrm{Gal}(L/k).$$

Ceci prouve le point 3).

Enfin, le point 4) est une conséquence immédiate du point 2). Le théorème est démontré. □

Remarque 26.6.2 Sous les hypothèses du théorème, soit $k \subset L \subset K$ une extension intermédiaire. Puisque K est séparable sur k, alors L l'est aussi. Donc, d'après le corollaire 26.1.8, l'extension $k \subset L$ est galoisienne ssi elle est normale. D'après le point 3) du théorème précédent, on peut donc dire que l'extension $k \subset L$ est normale ssi $\mathrm{Fix}(L)$ est un sous-groupe **normal** de G. Ceci explique la terminologie « extension normale ».

26.7 Clôture normale ou galoisienne

On a vu les bonnes propriétés des extensions galoisiennes finies et de leurs sous-extensions. Pour cette raison, étant donné une extension finie arbitraire K/k, il est parfois utile de la plonger, dans une extension finie plus grande

L/k qui soit galoisienne, si cela est possible. Comme une extension galoisienne est séparable, ainsi que toute sous-extension (*cf.* 25.1.4), une condition nécessaire est que K/k soit séparable. On va voir que cette condition est également suffisante.

En particulier, si $\mathrm{car}(k) = 0$, toute extension finie de k est contenue dans une extension galoisienne finie de k.

Théorème 26.7.1 (Clôture normale ou galoisienne)
Soit $k \subset K$ une extension de corps, de degré fini. Alors K est contenu dans une extension L, de degré fini et normale sur k, minimale pour cette propriété, et unique à K-isomorphisme près. Un tel L s'appelle une **clôture normale** *de K sur k.*

De plus, si $k \subset K$ est **séparable***, alors L est galoisienne sur k et l'on dit que c'est une* **clôture galoisienne** *de K sur k.*

Démonstration. Soit $\alpha_1, \ldots, \alpha_r$ un système de générateurs de K sur k et soit P_i le polynôme minimal sur k de α_i. Posons $P = P_1 \cdots P_r$ et soit L un corps de décomposition de P sur K. C'est aussi un corps de décomposition de P sur k et donc l'extension $k \subset L$ (de degré fini) est normale, d'après la proposition 24.2.8.

Elle est de plus minimale, au sens suivant. Soit L' une extension intermédiaire entre K et L, qui soit normale sur k. Alors L' contient $\alpha_1, \ldots, \alpha_r$, et donc toutes les racines de chaque $P_i = \mathrm{Irr}_k(\alpha_i)$. Par conséquent, $L' = L$. Ceci montre que L est une extension de K normale sur k et minimale pour cette propriété.

De plus, L est unique à K-isomorphisme près. En effet, soit E une extension de K, normale sur k. Alors, E contient un corps de décomposition L' de P sur K. D'après le théorème 24.2.5, il existe un K-isomorphisme $\tau : L \xrightarrow{\sim} L'$. Si de plus, E est supposée minimale, alors $E = L'$ et donc E est K-isomorphe à L.

Enfin, si $k \subset K$ est séparable, alors $P_1, \ldots, P_r$ et P sont séparables. Comme L est un corps de décomposition de P sur k, l'extension $k \subset L$ est galoisienne, d'après le second théorème fondamental 26.1.5. Ceci prouve le théorème. □

Corollaire 26.7.2 *Soit $k \subset K$ une extension séparable de degré fini. Le nombre d'extensions intermédiaires $k \subseteq L \subseteq K$ est fini.*

Démonstration. Soit $\widetilde{K}$ une clôture galoisienne de K, et G son groupe de Galois sur k. C'est un groupe fini, de cardinal $[\widetilde{K} : k]$. D'après le théorème principal 26.6.1, les extensions intermédiaires $k \subseteq L \subseteq K$ sont en bijection

avec l'ensemble des sous-groupes de G contenant $H = \mathrm{Fix}(K)$, qui est fini. □

On déduit de ce qui précède une autre démonstration du théorème de l'élément primitif, qui n'utilise pas les résultats de 25.3.

Théorème 26.7.3 (Théorème de l'élément primitif) *Soit K/k une extension séparable de degré fini. Alors K admet un élément primitif sur k.*

Démonstration. Ceci résulte du corollaire précédent et de la proposition 25.4.5. □

Table des matières

Bibliographie

[Art] E. Artin, Galois Theory, nouvelle édition, Dover, 1998.

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

[BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877 ; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press 1996.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedic Fernand Nathan, 1977.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Kru] W. Krull, Idealtheorie, Springer Verlag, 1937 (2e édition 1968).

[La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : *Algèbre*, Dunod, 2004.

[Ne04] J. Nekovàř, Théorie de Galois, cours UPMC 2003/4, disponible à l'adresse : www.math.jussieu.fr/˜nekovar/co/ln

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[St] J. Stillwell, Chapitre d'introduction dans [De].

[vdW] B. L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.