# Chapitre 7

# Extensions de corps et théorie de Galois

Version corrigée du 30 novembre 2004

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 même, de façon plus générale, les extensions d'anneaux $A \subset B$, mais ceci est en général trop compliqué et inabordable. On verra toutefois que l'étude des extensions de corps permet d'obtenir des informations importantes sur certaines extensions d'anneaux.

## 7.1 Sous-corps premier et caractéristique

### 7.1.1 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 $\geq 2$. Ils sont construits comme suit.

**Définition 7.1.1** *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.*

**Remarque 7.1.1** 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 $\alpha a + \beta b = 1$. Alors, les classes de $\alpha$ et $a$ modulo $p$ sont inverses l'une de l'autre.

En pratique, on peut trouver explicitement les "coefficients de Bezout" $\alpha$ et $\beta$ (et donc l'inverse $\alpha$ de $a$ modulo $p$), par la méthode des divisions successives.

**Exemple 7.1.1** 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.

### 7.1.2 Sous-corps premier et caractéristique

**Remarque 7.1.2** Soit $K$ un corps et $(K_i)_{i \in I}$ une famille quelconque de sous-corps de $K$, où $I$ est un ensemble non-vide. On voit facilement que l'intersection des $K_i$ est un sous-corps de $K$.

**Définition 7.1.2** *Soit $K$ un corps et 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 7.1.3** *Le sous-corps de $K$ engendré par l'élément unité $1_K$ s'appelle le sous-corps premier de $K$. Il est contenu dans tout sous-corps de $K$.*

**Remarque 7.1.3 (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, $\phi$ est injectif car $\ker \phi$, étant un idéal propre de $K$ (car $\phi(1) = 1$), est nécessairement égal à $(0)$.

**Proposition 7.1.1 (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 $\geq 0$ du noyau du morphisme $\mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$.*

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

1) Si $\ker \phi = (0)$, 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 $\phi$ 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 $\ker \phi \neq (0)$, alors $\ker \phi = (p)$, où $p$ est un nombre premier $\geq 2$. Dans ce cas, $\phi$ 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. □

**Notation** La caractéristique de $K$ est notée $\mathrm{car}(K)$.

## 7.2 Extensions, éléments algébriques ou transcendants, degré

### 7.2.1 Généralités sur les extensions

Soit $k \subset K$ une extension de corps. (On dira aussi que $K$ est un surcorps de $k$.) Alors $K$ est une $k$-algèbre et donc, en particulier, un $k$-espace vectoriel.

**Définition 7.2.1 (Sous-corps engendré sur $k$)** *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 $S = \{x_1, \ldots, x_n\}$.*

**Remarque 7.2.1** Dans la définition précédente, on peut bien entendu supposer que $S \subseteq K \setminus k$.

**Lemme 7.2.1** *Soit $K$ un surcorps de $k$ et $I, J$ deux parties de $K$. Alors $k(I)(J) = k(I \cup J)$.*

*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 7.2.2** *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 $K = k(x_1, \ldots, x_n)$.*

**Remarque 7.2.2** Il résulte du lemme précédent que

$$k(x_1, \ldots, x_n) = k(x_1)(x_2, \ldots, x_n) = k(x_1, \ldots, x_{n-1})(x_n).$$

Dans la suite, on aura besoin de la notion suivante.

**Définition 7.2.3** *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 $\phi$ est un isomorphisme de $k$-algèbres.*

### 7.2.2 Éléments algébriques ou bien transcendants

Soit $k \subset K$ une extension de corps.

**Notation** Pour $\alpha \in K$, on introduit les notations suivantes. Soit $k[\alpha]$ la sous-$k$-algèbre de $K$ engendrée par $\alpha$, soit $\phi_\alpha : k[X] \to K$ le morphisme de $k$-algèbres défini par $\phi_\alpha(X) = \alpha$, et soit $I_\alpha = \ker \phi_\alpha$. On a $\phi_\alpha(P) = P(\alpha) \in K$ pour tout $P \in k[X]$, et l'image de $\phi_\alpha$ est $k[\alpha]$.

**Définition 7.2.4 (Éléments algébriques ou transcendants)**

*1) On dit que $\alpha$ est algébrique sur $k$ s'il existe $Q \in k[X] \setminus \{0\}$ tel que $Q(\alpha) = 0$, c.-à-d., si $I_\alpha \neq (0)$. Dans ce cas, $I_\alpha = (P)$, où $P$ est l'unique polynôme unitaire de degré minimal dans $I_\alpha$ ; ce polynôme est appelé* **polynôme minimal de $\alpha$ sur $k$.** *On le notera parfois $\mathrm{Irr}_k(x)$. Son degré s'appelle* **degré de $x$ sur $k$** *et se note $\deg_k(x)$.*

*2) Dans le cas contraire, c.-à-d., si $I_\alpha = (0)$, on dit que $\alpha$ est transcendant sur $k$.*

**Remarque 7.2.3** Bien sûr, si $\alpha \in k$ il est algébrique sur $k$, de polynôme minimal $X - \alpha$. Dans la suite, on supposera toujours que les éléments de $K$ que l'on considère ne sont pas dans $k$.

**Théorème 7.2.2 (Le sous-corps $k(x)$, pour $x$ algébrique ou bien transcendant)**

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

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

*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 $\alpha$ est transcendant sur $k$, alors l'injection $\phi_\alpha : k[X] \to K$ 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, $I_x = (\mathrm{Irr}_k(x))$ est premier. D'après le lemme 5.3.4 et la proposition 5.3.5, $\mathrm{Irr}_k(x)$ est irréductible et engendre un idéal maximal de $k[X]$. Donc, $A := k[X]/(\mathrm{Irr}_k(x))$ est un corps. Par conséquent, son image par $\phi_x$, 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 $\alpha$ transcendant, c.-à-d., $\phi_\alpha : k[X] \to K$ injectif. Alors, tout élément de $\phi(k[X] \setminus \{0\})$ est inversible dans $K$, et donc $\phi$ se prolonge en un

morphisme d'anneaux $\psi : k(X) \to K$, nécessairement injectif puisque $k(X)$ est un corps. L'image de $\psi$ 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 7.2.4** 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 $k(x)$ est un cas particulier du lemme suivant.

**Lemme 7.2.3** *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. □

### 7.2.3 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 7.2.5** *Soit $k \subset K$ une extension de corps ; $\dim_k K$ s'appelle* **degré de $K$ sur $k$** *et se note $[K : k]$. C'est un élément de $\mathbb{N} \cup \{+\infty\}$.*

**Proposition 7.2.4 (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 tout élément de $\ell \in L$ s'écrit de façon unique

$$\ell = k_1 \ell_1 + \cdots + k_m \ell_m$$

avec les $k_i$ dans $K$, et chaque $k_i$ s'écrit de façon unique

$$k_i = a_{i,1}x_1 + \cdots + a_{i,n}x_n,$$

avec les $a_{i,j} \in k$. Il en résulte que $\ell$ s'écrit de façon unique

$$\ell = \sum_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} a_{i,j}x_j\ell_i.$$

Ceci montre que les produits $x_j\ell_i$ forment une base de $L$ sur $k$, d'où $\dim_k L = mn$. □

**Définition 7.2.6** *Soit $k \subset K$ une extension de corps. On dit que $k \subset K$ est une extension algébrique si tout élément de $K$ est algébrique sur $k$.*

**Proposition 7.2.5** *Soit $k \subset K$ une extension de corps.*

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

2) *Si $K$ est engendré sur $k$ par des éléments $x_1, \ldots, x_n$, chacun étant algébrique de degré $d_i$, alors $[K : k] \leq d_1 \cdots d_n$.*

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

2) Supposons $K$ engendré sur $k$ par des éléments $x_1, \ldots, x_n$, où chaque $x_i$ est de degré $d_i$. 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 $\phi$ 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 7.2.3, $A$ est un corps. Donc $A$ est le sous-corps $k(x_1, \ldots, x_n)$ de $K$ engendré par les $x_i$ ; par hypothèse, c'est $K$ lui-même. Donc $K = A$ est de dimension $\leq d_1 \cdots d_n$ sur $k$. La proposition est démontrée. □

**Corollaire 7.2.6** *Une extension de corps $k \subset K$ est de degré fini ssi elle est algébrique et de type fini.*

Dans toute la suite, on ne s'intéressera qu'aux extensions de degré fini.

## 7.3 Corps de rupture et corps de décomposition

### 7.3.1 Corps de rupture d'un polynôme

**Théorème 7.3.1 (Corps de rupture d'un polynôme irréductible)**
*Soient $k$ un corps et $P \in k[X]$ un polynôme unitaire irréductible de degré $\geq 2$. 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 $\alpha$, 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, $\psi$ 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 $\alpha$. 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 isomorphisme $\psi : K \to L$ 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 7.3.1** $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$. 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 7.3.1** L'exercice ci-dessus montre que des polynômes différents peuvent avoir des corps de rupture isomorphes.

**Définition 7.3.1** *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 7.3.2** *Soit $k \subset K$ une extension telle que $K = k(\alpha)$, où $\alpha$ est une racine de $P$. Alors $K$ est un corps de rupture de $P$ sur $k$.*

*Démonstration.* D'après le théorème, il existe un (unique) isomorphisme de $k[X]/(P)$ sur le sous-corps de $K$ engendré par $\alpha$, envoyant $x$ sur $\alpha$. La proposition en résulte. □

**Exemple 7.3.2** 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.

### 7.3.2 Corps de décomposition d'un polynôme

**Définition 7.3.2** *Soit $P \in k[X]$ un polynôme de degré $n \geq 1$. 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., si $P$ se décompose dans $K[X]$ comme un produit de facteurs linéaires :*

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

*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),*

*2) $K$ est engendré sur $k$ par $\alpha_1, \ldots, \alpha_n$, c.-à-d., $K = k(\alpha_1, \ldots, \alpha_n)$. En particulier, $K$ est de degré fini sur $k$, d'après la proposition 7.2.5.*

**Théorème 7.3.3 (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 $k$, est 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 termine la récurrence et montre l'existence d'un corps de décomposition. □

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

**Lemme 7.3.4** *Soit $\tau : K \xrightarrow{\sim} K'$ un isomorphisme de corps. Alors $\tau$ induit un isomorphisme d'anneaux*

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

*qu'on notera encore $\tau$. De plus, pour tout $P \in K[X]$, $\tau$ 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 $\phi_\tau(X) = X$. On vérifie facilement que $\phi_\tau$ est donné explicitement par la formule $(*)$ 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 $\phi_\tau$ et $\phi_{\tau^{-1}}$ sont inverses l'un de l'autre. Ceci prouve la 1ère assertion.

Enfin, pour tout $P \in K[X]$, il est clair que $\phi_\tau$ 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 7.3.5 (1er 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 7.3.6** *Soit $P \in k[X]$ de degré $\geq 1$. Le corps de décomposition de $P$ sur $k$ est unique, à $k$-isomorphisme près.*

*Démonstration.* Démontrons maintenant le théorème 7.3.5 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 $\lambda_i$ 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 $\geq 2$ 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 $\alpha$ l'une d'elles. D'après la proposition 7.3.2, 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 $\beta$ une racine de $\tau(P_1)$ dans $L'$. D'après la proposition 7.3.2, 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 $\tau$. On a donc le diagramme suivant :

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

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 7.3.3** *On dit que l'extension $k \subset K$ est 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 7.3.7** *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 $\beta$ une racine de $S$ dans $L$. D'après le théorème 7.3.1, 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 (7.3.5), $\tau$ se prolonge en un $k$-automorphisme $\sigma$ 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 $\sigma$ 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. □

## 7.4 L'arrivée des groupes

### 7.4.1 Le groupe des $k$-automorphismes d'une extension

**Définition 7.4.1** *1) Soit $k \subset K$ 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 $\alpha$ par les éléments de $G$ s'appelle* **l'orbite** *de $\alpha$ sous l'action de $G$, ou simplement la $G$-orbite de $\alpha$, 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 $\alpha$. Il est parfois aussi noté* $\mathrm{Stab}_G(\alpha)$.

**Proposition 7.4.1** *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 7.4.1** 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 $\xi$ l'une quelconque des racines de $P$ dans $\mathbb{C}$. On a vu

dans l'exemple 7.3.2 que $\xi$ 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 $\xi$, 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 introduire les définitions suivantes.

### 7.4.2 Polynômes et extensions séparables

**Définition 7.4.2** *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 7.3.5, 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 $\sigma$ 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.*

**Définition 7.4.3** *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 $k$.*

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 7.4.4** *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 7.4.2** *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. □

### 7.4.3 Extensions galoisiennes

**Définition 7.4.5** *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 7.4.1** L'exemple de $k = \mathbb{Q} \subset K = \mathbb{Q}[\sqrt[3]{2}]$ (*cf.* 7.4.1) montre que l'on peut avoir $k \neq K^G$.

**Définition 7.4.6** *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 $\alpha$ (dans $K$).*

**Proposition 7.4.3 (Propriétés des extensions galoisiennes)**
*Soient $k \subset K$ une extension galoisienne et $G = \mathrm{Aut}_k(K)$.*

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 7.4.1, $Q$ 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 7.4.2. La proposition est démontrée. □

**Théorème 7.4.4 (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 $\lambda_i$ 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 7.3.2 et le théorème 7.3.5, il existe, pour $i = 2, \ldots, d$, un $k$-automorphisme $\sigma_i$ 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 7.4.7 (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 7.3.5) 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 7.4.5** *Soit $K$ un corps de décomposition sur $k$ d'un polynôme séparable de degré $\geq 1$ 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 de la proposition 7.4.3. □

**Corollaire 7.4.6 (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) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 1) d'après le lemme 7.4.2, la proposition 7.4.3, et le théorème 7.4.4, respectivement. □

Le corollaire 7.4.5 apporte une réponse satisfaisante à la question 7.4.1 $(*)$, 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 $k \subset L \subset K$.

## 7.5 Sous-corps invariants et correspondance de Galois

### 7.5.1 Indépendance des caractères

Soit $K$ un corps.

**Définition 7.5.1** *Soit $X$ 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 7.5.2** *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 7.5.1 (Théorème d'indépendance des caractères)** *$X_K(G)$ est une partie libre de $\mathcal{F}(G, K)$, c.-à-d., si $\chi_1, \ldots, \chi_n$ sont des caractères distincts et si $a_1, \ldots, a_n \in K$ 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 $\chi_i$ 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 $\chi_2$ 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 7.5.2** *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 $\phi_i$ à $L^\times = L \setminus \{0\}$ est un caractère de $L$ à valeurs dans $K$. Donc, le théorème précédent entraîne que $a_i = 0$ pour tout $i$. Ceci prouve le corollaire. □

**Proposition 7.5.3** *Soit $K$ un corps et soient $\mathrm{id}_K = \phi_1, \ldots, \phi_n$ 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 $\dim_L K \geq n$.*

*Démonstration.* Il est immédiat que $L$ est un sous-corps de $K$. Observons que chaque $\phi_i$ 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 $x_1, \ldots, x_n$ :

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

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. □

### 7.5.2 Invariants d'un groupe fini : théorème d'Artin

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

**Théorème 7.5.4 (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 7.5.3, 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 $\varepsilon_i$, 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 :

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

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

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

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

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

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).

Le point 2) en découle facilement. D'une part, $G$ est contenu dans $H := \mathrm{Aut}_L(K)$. D'autre part, $K^H$ contient $L$ et donc

$$[K : K^H] \leq [K : L] = n.$$

Si l'on avait $G \neq H$, alors $H$ contiendrait un élément $\tau_{n+1} \notin G$ et, d'après la proposition 7.5.3, on aurait $[K : K^H] \geq n + 1$, ce qui n'est pas le cas. On a donc $G = H = \mathrm{Aut}_L(K)$. Comme $L = K^G$, il en résulte que l'extension $L \subset K$ est galoisienne, de groupe de Galois $G$. Le théorème est démontré. □

### 7.5.3 Un rappel sur les groupes

**Définition 7.5.3** *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 7.5.1** 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 7.5.5** *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 7.5.6 (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) *$\phi$ 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 $\pi$ désigne la projection $G \to G/K$.*

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

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

*Démonstration.* La démonstration est analogue à celle du théorème 2.2.2 et est laissée au lecteur. □

### 7.5.4 Le couronnement : correspondance de Galois

**Théorème 7.5.7 (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 la proposition 7.4.3, $K$ 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 (7.4.4), 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 7.5.4, $[K : L] = |H|$ et $[K : k] = |G|$. Comme $[K : k] = [K : L][L : k]$, d'après la proposition 7.2.4, 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 7.5.4, 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 $\pi$ 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 7.5.1** 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 7.4.6, 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 <u>normal</u> de $G$. Ceci explique la terminologie "extension normale".

## 7.6 Séparabilité

Avant de terminer ce chapitre, élucidons un peu la notion de polynôme séparable. On reviendra plus en détail sur cette notion dans le chapitre suivant, consacré aux corps de caractéristique $p > 0$.

### 7.6.1 L'opérateur de dérivation

**Définition 7.6.1** *Soit $k$ un corps arbitraire. 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 <u>polynôme dérivé</u> de $P$. On notera $D$ l'application $P \mapsto P'$ ; on voit facilement que c'est un endomorphisme $k$-linéaire de $k[X]$.*

**Lemme 7.6.1** *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. □

### 7.6.2 Racines multiples et séparabilité

**Proposition 7.6.2** *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 $\geq 1$.*

*Démonstration.* Soit $K$ un corps de décomposition de $P$ sur $k$. Supposons que $P$ ait dans $K$ une racine $\alpha$ 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 $\alpha$ 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 $\geq 1$, il admet une racine $\alpha$ dans une extension $L$ de $k$, et $\alpha$ est une racine de $P$ et $P'$, puisque $D$ divise $P$ et $P'$. Nécessairement, $\alpha$ 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, $\alpha$ est une racine de $P$ dans $L$ de multiplicité $\geq 2$. Soit $K$ un corps de décomposition de $P$ sur $L$. Alors, $K$ est un corps de décomposition de $P$ sur $k$, et $P$ a une racine multiple dans $K$. Ceci prouve 3) $\Rightarrow$ 1). Le proposition est démontrée. □

**Corollaire 7.6.3** *Soit $P \in k[X]$ irréductible ; $P$ est séparable $\Leftrightarrow P' \neq 0$.*

*Démonstration.* Soit $D = \text{pgcd}(P, P')$. 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 7.6.4** *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 $d = d \cdot 1 \neq 0$ (puisque $\mathrm{car}(k) = 0$). D'après le corollaire précédent, ceci montre que $P$ est séparable. □

**Remarque 7.6.1** 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 $k$.

## 7.7 Clôture normale, théorème de l'élément primitif

On a vu dans la Section 7.5 les bonnes propriétés des extensions galoisiennes finies et de leurs sous-extensions. On va voir plus bas que toute extension séparable finie est une sous-extension d'une extension galoisienne finie. En particulier, si $\mathrm{car}(k) = 0$, toute extension finie de $k$ est contenue dans une extension galoisienne finie de $k$. (Dans ce paragraphe, on a abrégé "de degré fini" en "finie").

### 7.7.1 Clôture normale ou galoisienne

Soit $k \subset K$ une extension de degré fini. Soit $\alpha_1, \ldots, \alpha_r$ un système de générateurs de $K$ sur $k$ et soit $S_i$ le polynôme minimal sur $k$ de $\alpha_i$. 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 7.3.7.

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 7.3.5, 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 7.4.4. On a donc obtenu le théorème ci-dessous.

**Théorème 7.7.1 (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 $L$ 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 $k$.*

**Corollaire 7.7.2** *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 7.5.7, 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. □

### 7.7.2 Extensions simples, éléments primitifs

**Définition 7.7.1** *On dit qu'une extension $k \subset K$ est simple 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 $\xi$ est un élément primitif de $K$ sur $k$.*

**Théorème 7.7.3 (Théorème de l'élément primitif)**
*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. (La démonstration lorsque $k$ est fini sera donnée 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 maximale parmi les sous-extensions simples contenues dans $K$. Ceci est possible puisque, par hypothèse, il n'y a qu'un nombre fini de corps intermédiaires. 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 $\xi_t$. 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 $\alpha$, et aussi $\xi$. 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 7.7.1** 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 simple $k[\alpha] \subset K$ est de degré $\leq p$ (et $= p$ si $\alpha \notin k$). Ceci montre que l'extension $k \subset K$ n'est pas simple, donc admet une infinité de corps intermédiaires.

# Table des matières