# Théorie de Galois

Grégory Berhuy

# Table des matières


Chapitre I. Dans les épisodes précédents... 5
- I.1. Extensions de corps 5
- I.2. Extensions algébriques, transcendantes 8
- I.3. Polynômes et racines 12

Chapitre II. Constructions à la règle et au compas et théorie des corps 19
- II.1. Préliminaires 19
- II.2. Nombres constructibles et extensions de corps 23
- II.3. Disjonction linéaire 30
- II.4. Quelques problèmes de construction à la règle et au compas 34
- II.5. Et après 44

Chapitre III. Plongements et extensions séparables 47
- III.1. Plongements 47
- III.2. Propriétés des extensions séparables 55
- III.3. Polynômes séparables 61
- III.4. Traces et normes 65

Chapitre IV. Extensions galoisiennes 71
- IV.1. Extensions normales 71
- IV.2. Extensions galoisiennes 74
- IV.3. Le groupe de Galois d'un polynôme 81
- IV.4. Corps finis 86
- IV.5. Extensions cyclotomiques 87
- IV.6. Théorie de Kummer 96

Chapitre V. Nul n'est censé ignorer Galois 101
- V.1. Théorie de Galois 101
- V.2. Résolubilité des équations par radicaux 110
- V.3. Constructions à la règle et au compas : le retour 122

Index 127

Chapitre I

# Dans les épisodes précédents...

Dans ce chapitre, on fait un survol des notions et résultats qui nous seront utiles pour étudier la théorie de Galois.

Nous allons maintenant faire quelques rappels sur les extensions de corps afin de poursuivre notre investigation.

## I.1. Extensions de corps

Définition I.1.1. Soit $K$ un corps. Une *extension* de $K$ est un corps $L$ contenant $K$ comme sous-corps. On le note $L/K$.

On vérifie aisément que $L$, muni de son produit et de la loi externe

$$\begin{aligned} K \times L &\longrightarrow L \\ (\lambda, x) &\longmapsto \lambda x, \end{aligned}$$

est une $K$-algèbre associative unitaire.

On appelle *degré* de $L/K$ la dimension de $L$ comme $K$-espace vectoriel. On le note $[L : K]$.

Un *morphisme* d'extensions de $K$ est un morphisme de $K$-algèbres.

Une *sous-extension* de $L/K$ est une extension $L'/K$ telle que $L'$ soit un sous-corps de $L$.

Le lemme suivant sera abondamment utilisé dans la suite sans référence ultérieure.

Lemme I.1.2. *Soient $L$, $L'$ deux corps. Alors, tout morphisme $\varphi : L \longrightarrow L'$ est injectif.*

*En particulier, tout morphisme d'extensions d'un même corps $K$ est injectif.*

Remarque I.1.3. Soit $K$ un corps, et soit

$$\begin{aligned} \Theta_K \colon \mathbb{Z} &\longrightarrow K \\ n &\longmapsto n{\cdot}1_K \end{aligned}$$

le morphisme d'anneaux canonique.

Si $\mathrm{car}(K) = 0$, ce morphisme est injectif, et identifie le sous-anneau engendré par $1_K$ à $\mathbb{Z}$. Dans ce cas, puisque tout élément non nul de $K$ est inversible, on montre aisément que l'application

$$\begin{aligned} \mathbb{Q} &\longrightarrow K \\ \frac{a}{b} &\longmapsto (a{\cdot}1_K)(b{\cdot}1_K)^{-1} \end{aligned}$$

est un morphisme d'anneaux injectif bien défini. Ainsi, $K$ contient un sous-corps isomorphe à $\mathbb{Q}$. Si $\mathrm{car}(K) = p$ ($p$ nombre premier), le morphisme $\Theta_K$ se factorise en un morphisme d'anneaux injectif

$$\begin{aligned} \mathbb{F}_p &\longrightarrow K \\ \overline{n} &\longmapsto n{\cdot}1_K. \end{aligned}$$

Ainsi, $K$ contient un sous-corps isomorphe à $\mathbb{F}_p$.

Autrement dit, tout corps $K$ peut se voir comme une extension de $\mathbb{Q}$ ou de $\mathbb{F}_p$, à une identification canonique près.

On continue en étudiant les propriétés du degré.

Proposition I.1.4 (Formule de multiplicativité des degrés). *Soient $M/K$ et $L/M$ des extensions de corps. Alors, $L/K$ est de degré fini si, et seulement si, $M/K$ et $L/M$ sont de degrés finis. Dans ce cas, on a l'égalité*

$$[L : K] = [L : M][M : K].$$

*En particulier, si $L/K$ est de degré fini, toute sous-extension $M/K$ est de degré fini, et l'on a*

$$[M : K] \mid [L : K].$$

On continue ce paragraphe en introduisant la notion de sous-extension engendrée par une partie. On vérifie facilement que l'intersection de sous-corps d'un même corps $L$ est encore un sous-corps de $L$. Cela justifie la définition suivante.

Définition I.1.5. Soit $L/K$ une extension, et soit $\mathscr{S}$ une partie de $L$. On note $K(\mathscr{S})$ l'intersection des sous-corps de $L$ contenant $K$ et $\mathscr{S}$. C'est donc la plus petite sous-extension de $L/K$ contenant $\mathscr{S}$.

L'extension $K(\mathscr{S})/K$ s'appelle la *sous-extension de $L/K$ engendrée par $\mathscr{S}$*. Si $\mathscr{S} = \{s_1, \ldots, s_n\}$, on la note $K(s_1, \ldots, s_n)/K$.

On dit que $L/K$ est *monogène* s'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

Remarque I.1.6. Il existe des extensions $L/K$ de degré fini non monogènes.

PROPOSITION I.1.7. *Soit $L/K$ une extension de corps, et soient $\mathscr{S}$, $\mathscr{S}_1$, $\mathscr{S}_2$ des parties de $L$. Alors :*

(1) *pour $i = 1, 2$, on a $K(\mathscr{S}_i) \subset K(\mathscr{S}_1 \cup \mathscr{S}_2)$. De plus, on a les égalités entre extensions de $K(\mathscr{S}_1)$*

$$K(\mathscr{S}_1 \cup \mathscr{S}_2) = K(\mathscr{S}_1)(\mathscr{S}_2)$$

*et les égalités entre extensions de $K(\mathscr{S}_2)$*

$$K(\mathscr{S}_1 \cup \mathscr{S}_2) = K(\mathscr{S}_2)(\mathscr{S}_1).$$

*En particulier, pour tous éléments $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \in L$, on a*

$$\begin{aligned} K(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) &= K(\alpha_1, \ldots, \alpha_n)(\beta_1, \ldots, \beta_m) \\ &= K(\beta_1, \ldots, \beta_m)(\alpha_1, \ldots, \alpha_n)\,; \end{aligned}$$

(2) *on a :*

$$\begin{aligned} K(\mathscr{S}) \;=\; \big\{ & P(s_1, \ldots, s_n)Q(s_1, \ldots, s_n)^{-1} \mid \\ & n \geq 0,\ s_1, \ldots, s_n \in \mathscr{S},\ P, Q \in K[X_1, \ldots, X_n] \\ & \text{tels que } Q(s_1, \ldots, s_n) \neq 0 \big\}. \end{aligned}$$

*En particulier, si $\mathscr{S} = \{s_1, \ldots, s_k\}$, alors on a :*

$$\begin{aligned} K(s_1, \ldots, s_k) \;=\; \big\{ & P(s_1, \ldots, s_k)Q(s_1, \ldots, s_k)^{-1} \mid P, Q \in K[X_1, \ldots, X_k] \\ & \text{tels que } Q(s_1, \ldots, s_k) \neq 0 \big\}. \end{aligned}$$

EXEMPLES I.1.8.

(1) Soit $L/K$ une extension. Si $\mathscr{S} \subset K$, on a $K(\mathscr{S}) = K$, puisque $K$ est un sous-corps de $L$ contenant $\mathscr{S}$.

(2) Soit $L/K$ une extension. Pour tout $\alpha \in L$, et tous $a$, $b \in K$, $b \neq 0$, on a

$$K(a + b\alpha) = K(\alpha).$$

En effet, puisque $a + b\alpha \in K(\alpha)$, on a $K(a + b\alpha) \subset K(\alpha)$. Puisque $b$ est non nul, on a aussi

$$\alpha = -b^{-1}a + b^{-1}(a + b\alpha) \in K(a + b\alpha),$$

d'où l'inclusion $K(\alpha) \subset K(a + b\alpha)$.

(3) On a l'égalité

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8),$$

où $\zeta_8 = e^{\frac{2i\pi}{8}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$.

En effet, il est clair que $\zeta_8 \in \mathbb{Q}(i, \sqrt{2})$, d'où l'inclusion $\mathbb{Q}(\zeta_8) \subset \mathbb{Q}(i, \sqrt{2})$. D'autre part, on a $\zeta_8^2 = e^{i\frac{\pi}{2}} = i$, d'où $i \in \mathbb{Q}(\zeta_8)$. Mais alors, on a

$$\sqrt{2} = \frac{2\zeta_8}{1+i} \in \mathbb{Q}(\zeta_8).$$

Il s'avère ainsi que $i$ et $\sqrt{2} \in \mathbb{Q}(\zeta_8)$, d'où l'inclusion manquante.

(4) Soit $K$ un sous-corps de $\mathbb{C}$, et soit $d \in K$. Deux racines carrées de $d$ dans $\mathbb{C}$ différant seulement par un signe, elles engendrent la même sous-extension. Aussi, par commodité, on note $\sqrt{d} \in \mathbb{C}$ un nombre complexe de carré $d$.

Alors, on a l'égalité

$$K(\sqrt{d}) = \{a + b\sqrt{d} \mid a,\, b \in K\}.$$

En particulier, $[K(\sqrt{d}) : K] \leq 2$.

Si $\sqrt{d} \in K$, alors $K(\sqrt{d}) = K$, et il n'y a rien à faire. On peut donc supposer que $\sqrt{d} \notin K$. L'inclusion « $\supset$ » étant triviale, montrons l'autre inclusion. Il suffit pour cela de démontrer que l'ensemble

$$\{a + b\sqrt{d} \mid a,\, b \in K\}$$

est un sous-corps de $\mathbb{C}$ contenant $K$ et $\sqrt{d}$. Tous les points à vérifier sont immédiats, sauf la stabilité par passage à l'inverse.

Supposons que $z = a + b\sqrt{d} \neq 0$. Alors, $a^2 - db^2 \neq 0$. En effet, si on avait $a^2 - db^2 = 0$, alors $b \neq 0$ (sinon $a = 0$ et $z = 0$), et par conséquent $d$ serait le carré d'un élément de $K$, ce qui entraînerait alors que $\sqrt{d} \in K$. Mais alors, on vérifie que l'on a

$$z^{-1} = \frac{a - b\sqrt{d}}{a^2 - db^2} \in \{a + b\sqrt{d} \mid a,\, b \in K\},$$

d'où le résultat.

## I.2. Extensions algébriques, transcendantes

Si $L/K$ est une extension de corps, et si $\alpha \in L$, il existe un unique morphisme de $K$-algèbres $ev_\alpha : K[X] \longrightarrow L$ tel que $ev_\alpha(X) = \alpha$. Si $P \in K[X]$, l'image de $P$ est notée $P(\alpha)$. Si $P = a_nX^n + \cdots + a_1X + a_0$, on a donc

$$P(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0.$$

On note $K[\alpha]$ l'image de $ev_\alpha$.

On a alors la définition suivante.

Définition I.2.1. Soit $L/K$ une extension de corps, et soit $\alpha \in L$. On dit que $\alpha$ est *algébrique sur* $K$ s'il existe un polynôme $P \in K[X]$ non nul tel que $P(\alpha) = 0$. On dit que $\alpha$ est *transcendant sur* $K$ sinon.

On dit que $L/K$ est *algébrique* si tout élément de $L$ est algébrique sur $K$. On dit que $L/K$ est *transcendante* sinon.

Remarque I.2.2. Soit $L/K$ une extension, et soit $M/K$ une sous-extension. Si $L/K$ est algébrique, alors $M/K$ et $L/M$ sont algébriques.

En effet, si tout élément de $L$ est algébrique sur $K$, c'est a fortiori vrai pour tout élément de $M$, et $M/K$ est donc une extension algébrique. De plus, tout polynôme à coefficients dans $K$ peut être vu comme un polynôme à coefficients dans $M$. Ainsi, tout élément algébrique sur $K$ l'est aussi sur $M$. En particulier, si $L/K$ est algébrique, $L/M$ est algébrique.

Exemples I.2.3.

(1) Charles Hermite et Carl Louis Ferdinand von Lindemann ont respectivement démontré que $e$ et $\pi$ sont transcendants sur $\mathbb{Q}$.
(2) En revanche, le réel $\pi$ est algébrique sur $\mathbb{R}$, puisqu'il est racine du polynôme $X - \pi \in \mathbb{R}[X]$.
(3) Le nombre complexe $i \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$, puisque $i^2+1 = 0$.
(4) Si $T$ est une indéterminée sur $K$, alors $T$ est transcendant sur $K$.
(5) Si $L/K$ est une extension de degré fini, alors tout élément $\alpha \in L$ est algébrique sur $K$.

    En effet, si $d = [L : K] = \dim_K(L)$, alors la famille $(1, \alpha, \ldots, \alpha^d)$ est liée, puisqu'elle possède $d+1$ éléments. Ainsi, il existe $a_0, \ldots, a_d \in K$ non tous nuls, tels que $a_d\alpha^d + \cdots + a_1\alpha + a_0 = 0$. Par conséquent, le polynôme $P = a_dX^d + \cdots + a_1X + a_0 \in K[X]$ est non nul et vérifie $P(\alpha) = 0$.

Remarque I.2.4. On montre facilement que l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est dénombrable. En particulier, si l'on prend un nombre complexe « au hasard », il y a de fortes chances qu'il soit transcendant. Néanmoins, il est extrêmement difficile en pratique de déterminer si un nombre complexe donné est algébrique ou transcendant.

Proposition I.2.5. *Soit $L/K$ une extension, et soit $\alpha \in L$. Alors, l'ensemble*

$$I_\alpha = \{P \in K[X] \mid P(\alpha) = 0\}$$

*est un idéal de $K[X]$. Il est non nul si, et seulement si, $\alpha$ est algébrique sur $K$. Dans ce cas, il existe un unique polynôme unitaire irréductible*

*$\mu_{\alpha,K}$ de $K[X]$ tel que*

$$\mu_{\alpha,K}(\alpha) = 0.$$

*Ce polynôme est l'unique générateur unitaire de $I_\alpha$.*

Définition I.2.6. Le polynôme $\mu_{\alpha,K}$ est appelé le *polynôme minimal de $\alpha$ sur $K$.*

Exemples I.2.7.

(1) Soit $K = \mathbb{R}$, et soit $\alpha = i$. Alors, $f = X^2 + 1 \in \mathbb{R}[X]$ annule $\alpha$. Il est unitaire, et irréductible, car il est de degré 2 et n'a pas de racines réelles. Ainsi, $\mu_{\alpha,\mathbb{R}} = X^2 + 1$.

(2) Soit $K = \mathbb{Q}$ et soit $\alpha = \sqrt[4]{3}$. Alors, $f = X^4 - 3 \in \mathbb{Q}[X]$ annule $\alpha$. Il est unitaire, à coefficients dans $\mathbb{Z}$, donc primitif, et irréductible dans $\mathbb{Z}[X]$, et donc dans $\mathbb{Q}[X]$, par le critère d'Eisenstein. Ainsi, $\mu_{\alpha,\mathbb{Q}} = X^4 - 3$.

(3) Soit $K = \mathbb{Q}$, et soit $\alpha = \sqrt{2}+\sqrt{3}$. On vérifie que $f = X^4-10X^2+1$ annule $\alpha$. On peut démontrer qu'il est irréductible (exercice).

Ainsi, $\mu_{\alpha,\mathbb{Q}} = X^4 - 10X^2 + 1$.

Théorème I.2.8. *Soit $L/K$ une extension. Alors, $\alpha \in L$ est algébrique sur $K$ si, et seulement si, $K(\alpha)/K$ est une extension de degré fini. Dans ce cas, une $K$-base de $K(\alpha)$ est $(1, \alpha, \ldots, \alpha^{d-1})$, où $d = \deg(\mu_{\alpha,K})$. En particulier, on a $K(\alpha) = K[\alpha]$, ainsi que*

$$[K(\alpha) : K] = \deg(\mu_{\alpha,K}).$$

Remarque I.2.9. Si $\alpha \in L$ est algébrique sur $K$, la démonstration du théorème nous fournit un isomorphisme de $K$-algèbres

$$K[X]/(\mu_{\alpha,K}) \xrightarrow{\sim} K(\alpha),$$

qui envoie $\overline{X}$ sur $\alpha$.

Exemples I.2.10.

(1) D'après les exemples I.2.7, on a

$$[\mathbb{R}(i) : \mathbb{R}] = 2, \quad [\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4, \quad \text{et} \quad [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4.$$

(2) Soit $d \in \mathbb{Z}$ non nul et sans facteurs carrés. Alors, $X^2-d \in \mathbb{Q}[X]$ est irréductible puisqu'il est de degré 2 et n'a pas de racines. Comme il est unitaire et annule $\sqrt{d}$, on a $\mu_{\sqrt{d},\mathbb{Q}} = X^2 - d$. Le théorème précédent nous donne alors

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a,\, b \in \mathbb{Q}\},$$

ainsi que $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$.

Corollaire I.2.11. *Soit $L/K$ une extension. Si $\alpha_1, \ldots, \alpha_n \in L$ sont algébriques sur $K$, alors $K(\alpha_1, \ldots, \alpha_n)/K$ est de degré fini. En particulier, l'extension $K(\alpha_1, \ldots, \alpha_n)/K$ est algébrique, et l'on a*

$$K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n],$$

*où* $K[\alpha_1, \ldots, \alpha_n] = \{P(\alpha_1, \ldots, \alpha_n) \mid P \in K[X_1, \ldots, X_n]\}$.

La définition suivante sera bien commode pour raccourcir les énoncés.

Définition I.2.12. Soit $L/K$ une extension, et soit $\alpha \in L$ un élément algébrique sur $K$. Le *degré* de $\alpha$ sur $K$ est le degré de l'extension $K(\alpha)/K$. C'est donc aussi le degré de $\mu_{\alpha,K}$.

Corollaire I.2.13. *Soit $L/K$ une extension. Alors, l'ensemble des éléments de $L$ qui sont algébriques sur $K$ est une sous-extension de $L/K$.*

Corollaire I.2.14. *Soit $L/K$ une extension, et soit $\mathscr{S}$ une partie de $L$. Alors, $K(\mathscr{S})/K$ est algébrique si, et seulement si, tout élément de $\mathscr{S}$ est algébrique sur $K$.*

*Démonstration.* Soit $M$ l'ensemble des éléments de $L$ qui sont algébriques sur $K$. Supposons que tout élément de $\mathscr{S}$ soit algébrique sur $K$. Alors, $\mathscr{S}$ est contenue dans $M$. Comme $M$ est un sous-corps de $L$ contenant $K$ d'après le corollaire précédent, on a $K(\mathscr{S}) \subset M$. Autrement dit, $K(\mathscr{S})/K$ est algébrique. L'autre implication est immédiate. □

Avant de continuer, nous avons besoin d'une nouvelle définition.

Définition I.2.15. Soit $L/K$ une extension. Si $E/K$ et $E'/K$ sont deux sous-extensions de $L/K$, le *compositum* de $E/K$ et $E'/K$ dans $L/K$ est la sous-extension de $L/K$ engendrée par $E \cup E'$. Autrement dit, c'est la plus petite sous-extension de $L/K$ contenant $E$ et $E'$. On la note $EE'/K$.

Exemple I.2.16. Si $E = K(\mathscr{S})$, on vérifie aisément que l'on a

$$EE' = E'(\mathscr{S}).$$

En particulier, on a

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

Corollaire I.2.17. *Soit $L/K$ une extension, et soient $E/K$ et $E'/K$ deux sous-extensions de $L/K$. Si $E/K$ est algébrique, alors $EE'/E'$ est algébrique.*

*Démonstration.* Puisque tout élément de $E$ est algébrique sur $K$, tout élément de $E$ est aussi algébrique sur $E'$ par la remarque I.2.2. D'après le corollaire précédent, tout élément de la sous-extension $M/E'$ de $L/E'$ engendrée par $E$ est algébrique. Mais cette extension n'est rien d'autre que $EE'$. En effet, $M$ est un sous-corps de $L$ contenant $E$ et $E'$. Il contient aussi $K$, et par suite, il contient $EE'$. Inversement, $EE'$ est une extension de $E'$ contenant $E$ par définition, et contient donc $M$, d'où finalement l'égalité $M = EE'$. Cela achève la démonstration. □

Corollaire I.2.18. *Soit $L/K$ une extension, et soient $E/K$ et $E'/K$ deux sous-extensions de $L/K$. Si $E/K$ et $E'/K$ sont algébriques, $EE'/K$ est algébrique.*

*Démonstration.* Pour obtenir le résultat voulu, il suffit d'appliquer le corollaire I.2.14 à $\mathscr{S} = E \cup E'$. □

On a également la proposition suivante.

Proposition I.2.19. *Soit $K \subset M \subset L$ une tour d'extensions. Alors, $L/K$ est algébrique si, et seulement si, $M/K$ et $L/M$ sont algébriques.*

*Démonstration.* Le sens direct est donné par la remarque I.2.2. Supposons que $M/K$ et $L/M$ soient algébriques, et soit $\alpha \in L$. Comme $\alpha$ est algébrique sur $M$ par hypothèse, il existe $a_0, \ldots, a_n \in M$ non tous nuls tels que

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0.$$

Soit $K' = K(a_0, \ldots, a_n)$. L'égalité précédente montre en fait que $\alpha$ est algébrique sur $K'$. En particulier, $K'(\alpha)/K'$ est une extension de degré fini par le théorème I.2.8. De plus, par hypothèse, $a_0, \ldots, a_n$ sont algébriques sur $K$. Par le corollaire I.2.11, le degré $[K' : K]$ est fini. La formule de multiplicativité des degrés montre alors que $[K'(\alpha) : K]$ est fini. Comme on a $K \subset K(\alpha) \subset K'(\alpha)$, ce même résultat implique que $[K(\alpha) : K]$ est également fini. Le théorème I.2.8 montre alors que $\alpha$ est algébrique sur $K$. Cela achève la démonstration. □

## I.3. Polynômes et racines

Il est temps de rappeler un théorème fondamental, qui nous servira constamment par la suite. Commençons par introduire une notation commode.

Si $K$ et $M$ sont des corps, et si $\iota : K \longrightarrow M$ est un morphisme d'anneaux, pour tout $P = a_nX^n + \cdots + a_1X + a_0 \in K[X]$, on pose

$$\iota(P) = \iota(a_n)X^n + \cdots + \iota(a_1)X + \iota(a_0) \in M[X].$$

On a alors le résultat suivant.

THÉORÈME I.3.1 (de prolongement des isomorphismes). *Soit $L/K$ une extension, et soit $\alpha \in L$ un élément algébrique sur $K$. Soit $M$ un corps quelconque, et soit $\iota : K \longrightarrow M$ un morphisme d'anneaux. Alors, l'ensemble des morphismes d'anneaux $\sigma : K(\alpha) \longrightarrow M$ prolongeant $\iota$ est en bijection avec l'ensemble des racines*[1] *de $\iota(\mu_{\alpha,K})$ dans $M$.*

*Plus précisément :*

(1) *pour tout morphisme d'anneaux $\sigma : K(\alpha) \longrightarrow M$ prolongeant $\iota$, $\sigma(\alpha)$ est une racine de $\iota(\mu_{\alpha,K})$ dans $M$ ;*

(2) *pour toute racine $\beta \in M$ de $\iota(\mu_{\alpha,K})$, il existe un unique morphisme d'anneaux $\sigma_\beta : K(\alpha) \longrightarrow M$ tel que*

$$\sigma_\beta(\alpha) = \beta \quad \text{et} \quad \sigma_{\beta|_K} = \iota.$$

*Il est défini par*

$$\sigma_\beta\big(P(\alpha)\big) = \iota(P)(\beta), \qquad \text{pour tout } P \in K[X];$$

(3) *les deux applications*

$$\begin{array}{ccc} \sigma & \longmapsto & \sigma(\alpha) \\ \sigma_\beta & \longleftarrow\!\shortmid & \beta \end{array}$$

*sont bijectives, et inverses l'une de l'autre.*

*Démonstration.* Soit $\sigma : K(\alpha) \longrightarrow M$ un morphisme d'anneaux prolongeant le morphisme $\iota : K \longrightarrow M$. Pour tout $P \in K[X]$, on a

$$\sigma\big(P(\alpha)\big) = \sigma(P)\big(\sigma(\alpha)\big), \qquad \text{pour tout } P \in K[X],$$

où $\sigma(P)$ est l'image de $P$ par le morphisme $K[X] \longrightarrow M[X]$ induit par $\sigma$. Comme $P \in K[X]$ et que $\sigma$ prolonge $\iota$, cette égalité se récrit

$$\sigma\big(P(\alpha)\big) = \iota(P)\big(\sigma(\alpha)\big), \qquad \text{pour tout } P \in K[X]. \qquad (*)$$

En appliquant cela à $P = \mu_{\alpha,K}$, on obtient que $\sigma(\alpha) \in M$ est une racine de $\iota(\mu_{\alpha,K}) \in M[X]$, d'où (1).

Montrons (2). Soit $\beta \in M$ une racine de $\iota(\mu_{\alpha,K})$. Supposons qu'il existe un morphisme d'anneaux $\sigma_\beta : K(\alpha) \longrightarrow M$ prolongeant $\iota$ tel que $\sigma_\beta(\alpha) = \beta$. L'égalité $(*)$ montre alors que

$$\sigma_\beta\big(P(\alpha)\big) = \iota(P)(\beta), \qquad \text{pour tout } P \in K[X].$$

Comme $\alpha$ est algébrique sur $K$, tout élément de $K(\alpha)$ est de la forme $P(\alpha)$, avec $P \in K[X]$, d'après le théorème I.2.8. Ainsi, si $\sigma_\beta$ existe,

1. S'il en existe !

il est unique, et défini par la formule précédente. Il reste à démontrer qu'un tel morphisme existe bel et bien.

Puisque $\beta \in M$ est une racine de $\iota(\mu_{\alpha,K})$, le morphisme

$$\begin{aligned} K[X] &\longrightarrow M \\ P &\longmapsto \iota(P)(\beta) \end{aligned}$$

se factorise en un morphisme d'anneaux

$$\begin{aligned} \varphi\colon K[X]/(\mu_{\alpha,K}) &\longrightarrow M \\ \overline{P} \qquad &\longmapsto \iota(P)(\beta). \end{aligned}$$

D'après la remarque I.2.9, on a un isomorphisme de $K$-algèbres

$$K[X]/(\mu_{\alpha,K}) \xrightarrow{\sim} K(\alpha),$$

qui envoie $\overline{X}$ sur $\alpha$. En composant $\varphi$ et l'inverse de cet isomorphisme, on obtient un morphisme $\sigma_\beta : K(\alpha) \longrightarrow M$ vérifiant les propriétés voulues.

Le point (3) est alors une conséquence immédiate des deux premiers points. Cela achève la démonstration. □

On continue en faisant des rappels sur les notions de corps de décomposition et de clôture algébrique d'un corps.

Définition I.3.2. Soit $K$ un corps, et soit $f \in K[X]$ non constant. Un *corps des racines* de $f$ (ou *corps de décomposition*) est une extension $L/K$ vérifiant les deux conditions suivantes :

(1) le polynôme $f$ se décompose en facteurs de degré 1 dans $L[X]$ ;
(2) $L = K(\alpha_1, \ldots, \alpha_n)$, où $\alpha_1, \ldots, \alpha_n \in L$ sont les racines de $f$ dans $L$.

Remarque I.3.3. Comme $\alpha_1, \ldots, \alpha_n \in L$ sont algébriques sur $K$, un corps des racines $L/K$ de $f$ est algébrique de degré fini (cf. corollaire I.2.11).

On rappelle alors la proposition suivante.

Proposition I.3.4. *Soit $f \in K[X]$ un polynôme non constant. Alors, $f$ admet un corps des racines, unique à isomorphisme de $K$-algèbres près.*

En fait, on peut faire beaucoup mieux, et construire une extension dans laquelle tout polynôme non constant est scindé (et donc qui contient un corps des racines de chaque polynôme non constant).

On commence par quelques définitions.

Définition I.3.5. On dit qu'un corps $L$ est *algébriquement clos* si tout polynôme $f \in L[X]$ non constant possède une racine dans $L$. Une récurrence facile montre que cela revient à dire que tout polynôme $f \in L[X]$ est scindé dans $L$.

On dit que $L$ est une *clôture algébrique* de $K$ si $L/K$ est une extension algébrique et $L$ est algébriquement clos.

Exemple I.3.6. Le corps $\mathbb{C}$ est algébriquement clos d'après le théorème de d'Alembert, mais $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$, car il contient au moins un élément transcendant sur $\mathbb{Q}$. En revanche, $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Remarque I.3.7. Si $L$ est un corps algébriquement clos, alors l'extension triviale $L/L$ est la seule extension algébrique de $L$.

En effet, si $L'/L$ est algébrique, et si $\alpha \in L'$, le polynôme minimal de $\alpha$ sur $L$ admet une racine dans $L$. Comme il est irréductible, il est nécessairement de degré 1. Autrement dit, $\alpha \in L$ et $L' = L$.

Les corps algébriquement clos ont de bonnes propriétés vis-à-vis du prolongement de morphismes.

Proposition I.3.8. *Soit $L/K$ une extension algébrique (non nécessairement de degré fini), et soit $L'$ un corps algébriquement clos. Alors, tout morphisme d'anneaux $\iota : K \longrightarrow L'$ se prolonge en un morphisme d'anneaux $\varphi : L \longrightarrow L'$.*

Démonstration. La démonstration repose sur le lemme de Zorn (et donc l'axiome du choix). Soit $\mathcal{F}$ l'ensemble

$$\mathcal{F} = \{(F, \tau) \mid K \subset F \subset L, \tau : F \hookrightarrow L', \tau_{|_K} = \iota\}.$$

Remarquons que $\mathcal{F}$ est non vide puisqu'il contient $(K, \iota)$. On vérifie aisément que la relation $\preceq$ définie sur $\mathcal{F}$ par

$$(F, \tau) \preceq (F', \tau') \iff F \subset F' \text{ et } \tau'_{|_F} = \tau,$$

est une relation d'ordre (partiel) sur $\mathcal{F}$. Montrer que $\mathcal{F}$ est inductif. Soit $(I, \leq)$ un ensemble non vide totalement ordonné, et soit $((F_i, \tau_i))_{i \in I}$ une chaîne d'éléments de $\mathcal{F}$ indexée par $I$. On a donc $(F_i, \tau_i) \preceq (F_j, \tau_j)$ pour tout $i \leq j$.

Posons $F = \bigcup_{i \in I} F_i$ et soit $\tau : F \longrightarrow L'$ l'application définie par

$$\tau(x) = \tau_i(x),$$

dès que $x \in F_i$. On vérifie que $F$ est un sous-corps de $L$ contenant $K$ (cela provient du fait que les sous-corps $F_i$ sont emboîtés). De plus,

$\tau(x)$ ne dépend pas de l'indice $i \in I$ choisi, puisque, si $x \in F_i \cap F_j$, avec par exemple $i \leq j$, alors on a $F_i \subset F_j$ et donc

$$\tau_j(x) = (\tau_j)_{|F_i}(x) = \tau_i(x).$$

On vérifie alors que $\tau$ est un morphisme d'anneaux prolongeant $\iota$. Ainsi, $(F, \tau) \in \mathcal{F}$. Mais par définition, $F_i \subset F$ pour tout $i \in I$ et $\tau_{|f} = \tau_i$. Ainsi, on a

$$(F_i, \tau_i) \preceq (F, \tau) \text{ pour tout } i \in I.$$

Autrement dit, $(F, \tau)$ est un majorant de $((F_i, \tau_i))_{i \in I}$, et $\mathcal{F}$ est inductif. Comme il est non vide, il possède un élément maximal $(F_0, \varphi)$. Pour conclure, il reste donc à montrer que $F_0 = L$.

Supposons a contrario que $F_0 \subsetneq L$, et soit $\alpha \in L \setminus F_0$. Puisque $L/K$ est algébrique, $\alpha$ est algébrique sur $K$, donc sur $F_0$. Soit $f = \mu_{\alpha, F_0}$. Puisque $L'$ est algébriquement clos, $\varphi(f) \in L'[X]$ possède une racine dans $L'$. Le théorème de prolongement des isomorphismes montre alors que $\varphi$ se prolonge en un morphisme d'anneaux $\psi : F_0(\alpha) \longrightarrow L'$. En particulier, $\psi$ prolonge $\iota$. De plus, on a $F_0 \subsetneq F_0(\alpha)$ puisque $\alpha \notin F_0$. Ainsi, $(F_0, \varphi) \prec (F_0(\alpha), \psi)$, ce qui contredit la maximalité de $(F_0, \varphi)$. On a donc $F_0 = L$, et ceci achève la démonstration. □

On peut maintenant démontrer l'existence et l'unicité d'une clôture algébrique.

Théorème I.3.9 (Steinitz). *Tout corps $K$ admet une clôture algébrique, unique à isomorphisme de $K$-algèbres près.*

Démonstration. Commençons par l'unicité. Soient $L_1$ et $L_2$ deux clôtures algébriques de $K$. Puisque par définition, l'extension $L_1/K$ est algébrique et que le corps $L_2$ est algébriquement clos, la proposition précédente montre que l'inclusion $K \subset L_2$ se prolonge en un morphisme d'anneaux $\sigma : L_1 \longrightarrow L_2$, qui est alors $K$-linéaire, et donc un morphisme de $K$-algèbres. De plus, $\sigma$ étant injectif, il reste à démontrer sa surjectivité. Remarquons tout d'abord que $\sigma(L_1)$ est algébriquement clos. En effet, soit $g \in \sigma(L_1)[X]$ non constant. Alors, on peut écrire

$$g = \sigma(a_n)X^n + \cdots + \sigma(a_1)X + a_0, a_i \in L_1, a_n \neq 0, n \geq 1.$$

Mais alors $g = \sigma(f)$, où $f = a_n X^n + \cdots + a_1 X + a_0 \in L[X]$. Comme $f$ est aussi non constant, il possède une racine $\alpha \in L_1$, et ainsi $\sigma(\alpha)$ est une racine de $g$ dans $\sigma(L_1)$.

Soit maintenant $\beta \in L_2$. Comme $\beta$ est algébrique sur $K$, il existe $f \in K[X]$ non nul tel que $f(\beta) = 0$. Comme $f \in K[X] \subset \sigma(L_1)[X]$ est non constant (puisqu'il a une racine et qu'il est non nul) et que $\sigma(L_1)$

est algébriquement clos, $f$ possède toutes ses racines dans $\sigma(L_1)$. En particulier, $\beta \in \sigma(L_1)$ et on a donc $\sigma(L_1) = L_2$, d'où la surjectivité de $\sigma$.

Passons maintenant à l'existence d'une clôture algébrique. Remarquons tout d'abord que si $L/K$ est une extension telle que $L$ est algébriquement clos, alors l'ensemble $L_{alg}$ des éléments de $L$ algébriques sur $K$ est une clôture algébrique de $K$.

En effet, c'est un sous-corps de $L$ contenant $K$ d'après le corollaire I.2.13. Soit $f = a_nX^n + \cdots + a_1X + a_0 \in L_{alg}[X]$ non constant. On doit vérifier que $f$ possède une racine dans $L_{alg}$. Puisque $L$ est algébriquement clos, $f$ possède une racine $\alpha \in L$. Vérifions que $\alpha$ est algébrique sur $K$. Puisque $f(\alpha) = 0$, $\alpha$ est algébrique sur $K(a_0, \ldots, a_n)$. Le corollaire I.2.14 montre que $K(a_0, \ldots, a_n, \alpha)/K(a_0, \ldots, a_n)$ est algébrique. Or, $a_i$ est algébrique sur $K$, donc $K(a_0, \ldots, a_n)/K$ est algébrique par ce même corollaire. La proposition I.2.19 montre alors que $K(a_0, \ldots, a_n, \alpha)/K$ est algébrique. En particulier, $\alpha$ est algébrique sur $K$.

Il reste donc à démontrer l'existence d'un corps algébriquement clos contenant $K$.

Pour tout polynôme $f \in K[T] \setminus K$, on considère une indéterminée $X_f$, et on considère l'anneau des polynômes

$$A = K[(X_f)_{f \in K[T]\setminus K}] = \{P(X_{f_1}, \ldots, X_{f_n}) \in K[X_{f_1}, \ldots, X_{f_n}] \mid n \geq 0, f_1, \ldots, f_n \in K[T]\setminus K\}.$$

Autrement dit, c'est la réunion des anneaux de polynômes $K[X_{f_1}, \ldots, X_{f_n}]$, lorsque $f_1, \ldots, f_n$ parcourent les parties finies de $K[T]$.

On considère $\mathfrak{a}$ l'idéal de $A$ engendré par les éléments

$$f(X_f), f \in K[T] \setminus K.$$

Montrons que $\mathfrak{a} \neq A$. Dans le cas contraire, on aurait $1 \in \mathfrak{a}$. Il existerait alors des polynômes $f_1, \ldots, f_n \in K[T]$ et des éléments $h_1, \ldots, h_n \in A$ tels que

$$1 = h_1 f_1(X_{f_1}) + \cdots + h_n f(X_{f_n}).$$

Remarquons que chaque $f_i$ possède une racine $\alpha_i$ dans un corps des racines de $f_1 \cdots f_n \in K[X]$. En spécialisant $X_{f_i}$ en $\alpha_i$, on obtient alors la contradiction $0 = 1$.

Ainsi, $\mathfrak{a} \neq A$, et il existe un idéal maximal $\mathfrak{m}$ de $A$ contenant $\mathfrak{a}$. L'anneau quotient $L_1' = A/\mathfrak{m}$ est alors un corps. Considérons le morphisme de $K$-algèbres $\iota : K \longrightarrow L_1'$. Pour tout $f \in K[X]$ non constant, le polynôme $\iota(f)$ a une racine dans $L_1'$. En effet, on a

$$\iota(f)(\overline{X}_f) = \overline{f(X_f)} = \overline{0},$$

car $f(X_f) \in \mathfrak{a} \subset \mathfrak{m}$. Par transport de structure, on construit une extension $L_1/K$ dans laquelle tout polynôme non constant de $K[X]$ possède une racine.

Par récurrence, on construit une suite $(L_i)_{i\geq 1}$ d'extensions de $L$ vérifiant $L_i \subset L_{i+1}$ pour tout $i \geq 1$, et telles que tout polynôme non constant de $L_i[X]$ possède une racine dans $L_{i+1}$. Posons alors $L = \bigcup_{i\geq 1} L_i$, et montrons que $L$ est algébriquement clos. Soit $f \in L[X]$ non constant. Alors, puisque la suite $(L_i)_{i\geq 1}$ est croissante, il existe un indice $j \geq 1$ tel que $f \in L_j[X]$. Mais alors par construction, $f$ possède une racine dans $L_{j+1}$, donc dans $L$. Ceci achève la démonstration. □

Remarque I.3.10. On peut démontrer (mais c'est plus délicat) que la sous-extension des éléments algébriques de $L_1$ est déjà une clôture algébrique de $K$.

On finit par un critère d'irréductibilité, qui sera fort utile lorsque le corps de base est fini.

Proposition I.3.11. *Soit $K$ un corps, et soit $f \in K[X]$ de degré $n \geq 1$. Alors $f$ est irréductible si et seulement si pour tout extension $L/K$ de degré $\leq n/2$, $f$ n'a pas de racines dans $L$.*

*Démonstration.* Si $f$ n'est pas irréductible, alors $f = gh, g, h \in K[X]$ non constants. Au moins, un des deux facteurs est de degré $\leq n/2$ (sinon on aurait $\deg(gh) \geq n+1 = \deg(f)$), disons $g$. Soit $\pi$ un facteur irréductible de $g$, qui est donc aussi de degré $\leq n/2$. Alors un corps de rupture $L/K$ de $\pi$ est une extension de degré $\leq n/2$ dans lequel $\pi$ a une racine, et par suite $f$ a une racine dans $L$ (car $\pi \mid g \mid f$).

Inversement, si $f$ a une racine $\alpha \in L$, avec $[L : K] \leq n/2$, soit $g = \mathrm{Irr}(\alpha, K)$ le polynôme minimal de $\alpha$ sur $K$. Alors, puisque $f(\alpha) = 0$, on a $g \mid f$, donc $f$ n'est pas irréductible puisque $1 \leq \deg(g) < n$. □

Chapitre II

# Constructions à la règle et au compas et théorie des corps

*Si un algébriste est malade, est-ce faute d'anticorps ?*

Dans ce chapitre, nous allons motiver l'étude approfondie de la théorie des corps en expliquant comment celle-ci apparaît naturellement dans les problèmes de construction à la règle et au compas, et en montrant comment elle permet de résoudre des problèmes datant de l'Antiquité, tels que la trisection de l'angle, la duplication du cube ou la quadrature du cercle.

## II.1. Préliminaires

Commençons par mettre en place le contexte géométrique qui nous servira tout au long de ce chapitre.

Le problème qui va nous intéresser est le suivant : étant donné un segment unité $OI$ et éventuellement un nombre fini de points du plan, peut-on construire une figure donnée à partir de ces points à l'aide de la règle et du compas seulement ?

Définition II.1.1. Soit $\mathscr{A}_0$ un ensemble fini de points du plan contenant les points $O$ et $I$.

On dit qu'un point $P$ du plan est *élémentairement constructible à la règle et au compas à partir de* $\mathscr{A}_0$, ou *élémentairement* $\mathscr{A}_0$*-constructible* si $P$ est obtenu par intersection de deux objets géométriques appartenant aux ensembles suivants :

(1) l'ensemble des droites passant par deux points distincts de $\mathscr{A}_0$ ;
(2) l'ensemble des cercles centrés en un point de $\mathscr{A}_0$ et dont le rayon est la distance entre deux points de $\mathscr{A}_0$.

On dit qu'un point $P$ du plan est *constructible à la règle et au compas à partir de* $\mathscr{A}_0$ s'il existe un nombre fini de points $P_1, \ldots, P_r = P$ tels que, pour tout $i \in [\![1, r]\!]$, le point $P_i$ est élémentairement constructible à partir de $\mathscr{A}_0 \cup \{P_1, \ldots, P_{i-1}\}$.

Une longueur $\ell$ est dite *constructible à la règle et au compas à partir de* $\mathscr{A}_0$ s'il existe deux points $P, Q$ constructibles à la règle et au compas à partir de $\mathscr{A}_0$ tels que $PQ = \ell$.

Remarquons que, puisqu'un compas permet de reporter les longueurs, cela équivaut à demander l'existence d'un point $P$ constructible à la règle et au compas à partir de $\mathscr{A}_0$ tel que $OP = \ell$.

Enfin, une droite du plan est dite *constructible à la règle et au compas à partir de* $\mathscr{A}_0$ si elle passe par deux points constructibles à la règle et au compas à partir de $\mathscr{A}_0$.

Dans ce qui suit, on abrégera souvent l'expression « constructible à la règle et au compas à partir de $\mathscr{A}_0$ » par l'expression « $\mathscr{A}_0$-constructible ». De plus, si $\mathscr{A}_0 = \{O, I\}$, on dira simplement « constructible », plutôt que « $\mathscr{A}_0$-constructible ».

Parmi les divers problèmes de construction à la règle et au compas les plus célèbres, on peut citer :

(i) la quadrature du cercle : étant donné un segment-unité, est-il possible de construire à la règle et au compas un carré dont l'aire est la même que celle du cercle-unité ? Autrement dit, la longueur $\sqrt{\pi}$ est-elle constructible ?

(ii) la duplication du cube : étant donné un segment-unité, peut-on construire l'arête d'un cube dont le volume est le double du cube-unité, à la règle et au compas ? Autrement dit, peut-on construire la longueur $\sqrt[3]{2}$ ?

(iv) la trisection de l'angle : étant donné un angle $\theta$, peut-on construire l'angle $\dfrac{\theta}{3}$ à la règle et au compas ?

(v) la construction du $n$-gone régulier : étant donné un entier $n \geq 2$, peut-on construire les sommets d'un $n$-gone régulier à la règle et au compas ?

Nous reviendrons sur ces considérations plus loin. Pour l'instant, commençons par des résultats plus modestes.

Lemme II.1.2. *Soit $\mathscr{A}_0$ un ensemble fini de points du plan contenant $O$ et $I$. Soient $A$, $B$ et $C$ des points $\mathscr{A}_0$-constructibles. On suppose que $A$ et $B$ sont distincts. Alors :*

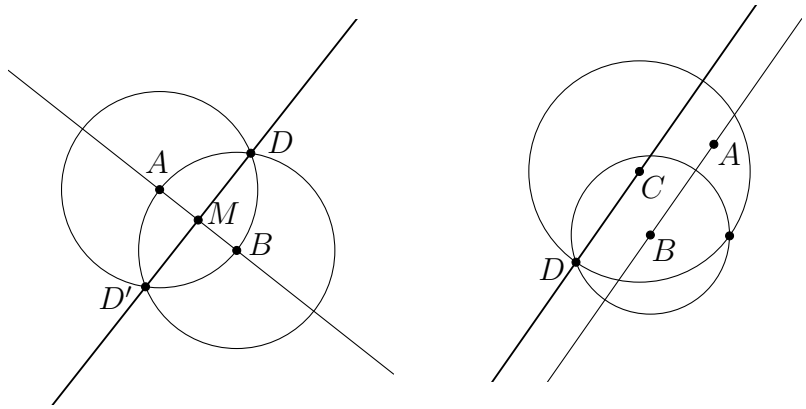
(1) *le milieu du segment $AB$ et sa médiatrice sont $\mathscr{A}_0$-constructibles ;*

(2) *la parallèle à $(AB)$ passant $C$ est $\mathscr{A}_0$-constructible ;*

(3) *la perpendiculaire à $(AB)$ passant $C$ est $\mathscr{A}_0$-constructible.*

*Démonstration.*

(1) Soient $D$ et $D'$ les points d'intersection des cercles de rayon $AB$ centrés en $A$ et $B$ respectivement. Alors, $(DD')$ est la médiatrice de $AB$, et son intersection $M$ avec $(AB)$ est le milieu de $AB$ (figure de gauche).

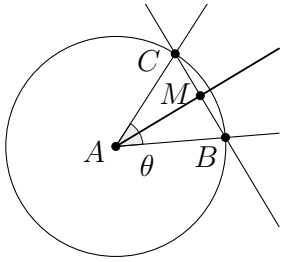



(2) Il n'y a rien à faire si $C = A$ ou $C = B$. On peut donc supposer que les points $A$, $B$, $C$ sont deux à deux distincts. Le cercle de centre $B$ et de rayon $AC$ et le cercle de centre $C$ et de rayon $AB$ s'intersectent en deux points. Un des deux points d'intersection, que l'on note $D$, est tel que la droite $(CD)$ soit parallèle à $(AB)$ (figure de droite).

(3) En considérant l'intersection de $(AB)$ et du cercle de centre $A$ et de rayon $AB$, on obtient un point $B' \in (AB)$ tel que $A$ soit le milieu de $BB'$. La perpendiculaire $\Delta$ à $(AB)$ passant par $A$ est alors la médiatrice de $BB'$, qui est constructible par (1). La perpendiculaire voulue est alors l'unique parallèle à $\Delta$ passant par $C$, qui est constructible par (2) (puisque par définition $\Delta$ est obtenue à l'aide de deux points $\mathscr{A}_0$-constructibles). □

Corollaire II.1.3. *Soit $\theta$ un angle formé par deux demi-droites du plan. Alors, la bissectrice de $\theta$ est constructible. Autrement dit, la bissection de l'angle est possible à la règle et au compas.*

*Démonstration.* Soit $A$ le point d'intersection des deux demi-droites. En traçant le cercle de centre $A$ et de rayon $OI$, on obtient deux points d'intersection $B$ et $C$. Or, la médiatrice de $BC$ est constructible d'après le lemme II.1.2 (1) et elle passe par $A$. La bissectrice est alors la portion convenable de cette médiatrice. □



D'après le lemme II.1.2, à partir de $O$ et $I$, on peut construire la perpendiculaire à $(OI)$ passant par $O$. En choisissant un point d'intersection $J$ du cercle de centre $O$ et de rayon $OI$ avec cette perpendiculaire, on peut construire un repère orthonormé. Quitte à changer la numérotation et le point d'intersection, on peut supposer que l'on a

$$O = (0,0), \quad I = (1,0) \quad \text{et} \quad J = (0,1).$$

On peut donc se placer sans perte de généralité dans $\mathbb{R}^2$, muni de son repère orthonormé canonique. On peut alors définir un point $P$ du plan par ses coordonnées dans ce repère.

**Convention.** Dans toute la suite, on suppose que $\mathscr{A}_0$ est un sous-ensemble fini de points de $\mathbb{R}^2$, contenant $O = (0,0)$ et $I = (1,0)$.

Lemme II.1.4. *Un point $P = (x,y)$ du plan est $\mathscr{A}_0$-constructible si, et seulement si, les points $(x,0)$ et $(0,y)$ le sont.*

*Démonstration.* Si $P = (x,y)$ est constructible, le lemme II.1.2 montre que la perpendiculaire et la parallèle à l'axe des abscisses passant par $P$ sont constructibles. Leurs intersections avec l'axe des abscisses et l'axe des ordonnées sont respectivement $(x,0)$ et $(0,y)$. Inversement, si $Q = (x,0)$ et $R = (0,y)$ sont constructibles, ce même lemme montre que l'on peut construire la parallèle à l'axe des ordonnées passant par $Q$ et la parallèle à l'axe des abscisses passant par $R$. L'intersection de ces deux droites est le point $P$. □

Remarque II.1.5. Une utilisation élémentaire du compas montre que $(0,y)$ est $\mathscr{A}_0$-constructible si, et seulement si, $(y,0)$ l'est. Autrement dit, par le lemme précédent, $P = (x,y)$ est $\mathscr{A}_0$-constructible si, et seulement si, $(x,0)$ et $(y,0)$ le sont. Cela motive la définition suivante.

Définition II.1.6. Un nombre réel $x \in \mathbb{R}$ est *constructible à la règle et au compas à partir de $\mathscr{A}_0$* si le point $(x,0)$ est constructible à la règle et au compas à partir de $\mathscr{A}_0$.

Un nombre complexe $z = x + iy \in \mathbb{C}$ est *constructible à la règle et au compas à partir de $\mathscr{A}_0$* si le point $(x,y)$ est constructible à la règle et au compas à partir de $\mathscr{A}_0$.

D'après la remarque précédente, cela équivaut au fait que les réels $x$, $y$ sont constructibles à la règle et au compas à partir de $\mathscr{A}_0$.

Nous allons maintenant faire le lien entre le problème de la construction à la règle et au compas et la théorie des extensions de corps.

## II.2. Nombres constructibles et extensions de corps

Rappelons que si $L$ est un corps, un sous-corps de $L$ est un sous-anneau $K$ de $L$ tel que pour tout $x \in K^\times$, on ait $x^{-1} \in K^\times$.

On commence par un premier résultat qui relie notre problème géométrique à la théorie des extensions de corps.

THÉORÈME II.2.1. *L'ensemble des nombres complexes $\mathscr{A}_0$-constructibles est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$.*

*De plus, si $z \in \mathbb{C}$ est $\mathscr{A}_0$-constructible, toute racine carrée de $z$ (i.e. tout nombre complexe de carré $z$) est aussi $\mathscr{A}_0$-constructible.*

*Démonstration.* On va tout d'abord montrer que l'ensemble des nombres réels $\mathscr{A}_0$-constructibles est un sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$, et que de plus, si $r > 0$ est $\mathscr{A}_0$-constructible, alors $\sqrt{r}$ l'est également.

Bien entendu, 0 et 1 sont $\mathscr{A}_0$-constructibles, puisque $\mathscr{A}_0$ contient $O = (0,0)$ et $I = (1,0)$.

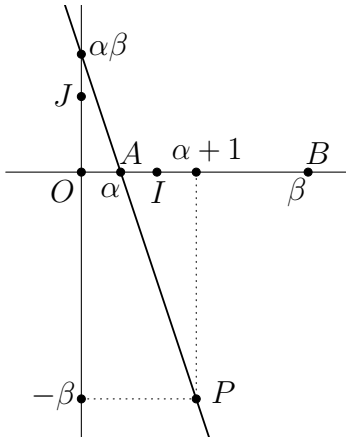
Soient maintenant $\alpha, \beta \in \mathbb{R}$ deux réels $\mathscr{A}_0$-constructibles. Les points $A = (\alpha, 0)$ et $B = (\beta, 0)$ sont donc $\mathscr{A}_0$-constructibles.

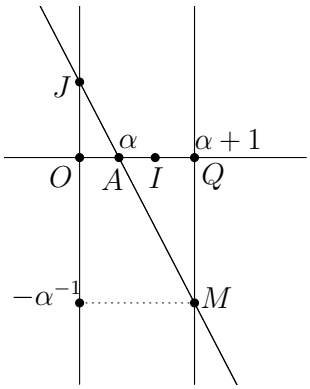
En reportant les longueurs grâce au compas, on construit l'unique point $D$ de l'axe des abscisses tel que $\overrightarrow{BD} = \overrightarrow{AO}$. Autrement dit, on a $\overrightarrow{OD} = \overrightarrow{AB}$, et donc $D = (\beta - \alpha, 0)$. Ainsi, $\beta - \alpha$ est $\mathscr{A}_0$-constructible.

Passons au cas du produit. Comme $1, \alpha$ et $\beta$ sont $\mathscr{A}_0$-constructibles, $\alpha+1$ et $-\beta$ le sont aussi d'après ce qui précède, et le point $P = (\alpha + 1, -\beta)$ est donc $\mathscr{A}_0$-constructible.
On vérifie alors aisément que l'équation de la droite $(AP)$ est donnée par

$$y = -\beta(x - \alpha).$$

Son intersection avec l'axe des ordonnées est le point $(0, \alpha\beta)$, on en déduit que le réel $\alpha\beta$ est $\mathscr{A}_0$-constructible conformément à la remarque II.1.5.






Enfin, supposons que $\alpha \neq 0$. Comme le réel $\alpha + 1$ est $\mathscr{A}_0$-constructible, le point $Q = (\alpha + 1, 0)$ est $\mathscr{A}_0$-constructible. De plus, le point $J = (0, 1)$ l'est aussi. L'équation de la droite $(JA)$ est alors

$$y = -\alpha^{-1}(x - \alpha).$$

Son intersection avec la parallèle à l'axe des ordonnées passant par $Q$ est donc le point $M = (\alpha + 1, -\alpha^{-1})$. En particulier, le réel $-\alpha^{-1}$ est $\mathscr{A}_0$-constructible, et par conséquent $\alpha^{-1}$ l'est également.

Ainsi, l'ensemble des réels $\mathscr{A}_0$-constructibles est un sous-corps de $\mathbb{R}$.

Soient maintenant $a$, $b \in \mathbb{Z}$, avec $b \neq 0$. Puisque 1 est $\mathscr{A}_0$-constructible, $-1$ aussi, et une récurrence immédiate montre que $a$, $b \in \mathbb{Z}$ le sont également. Mais alors, $\dfrac{1}{b}$ l'est aussi. On en déduit alors que $\dfrac{a}{b}$ est $\mathscr{A}_0$-constructible.

Enfin, supposons que $r > 0$ soit $\mathscr{A}_0$-constructible.

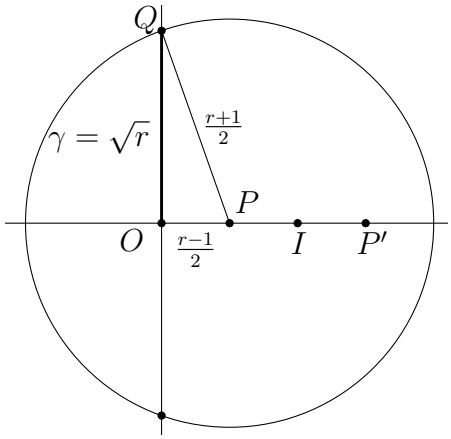
Supposons tout d'abord que $r > 1$. Puisque $1, 2$ et $r$ sont $\mathscr{A}_0$-constructibles, les réels $\dfrac{r-1}{2}$ et $\dfrac{r+1}{2}$ le sont aussi.

Soient $P = \left(\dfrac{r-1}{2}, 0\right)$ et $P' = \left(\dfrac{r+1}{2}, 0\right)$. Soit $Q = (0, \gamma)$ le point d'intersection du cercle de centre $P$ et de rayon $OP'$ avec l'axe des ordonnées, tel que $\gamma > 0$. Un tel point existe, car $r > 1$. Le triangle $OPQ$ étant rectangle en $O$, on a

$$\gamma^2 + \left(\frac{r-1}{2}\right)^2 = \left(\frac{r+1}{2}\right)^2.$$

On en déduit que $\gamma = \sqrt{r}$. Ainsi, $\sqrt{r}$ est $\mathscr{A}_0$-constructible dans ce cas.

Si maintenant $0 < r < 1$, alors $\dfrac{1}{r} > 1$ est aussi $\mathscr{A}_0$-constructible. Par le cas précédent $\sqrt{\dfrac{1}{r}} = \dfrac{1}{\sqrt{r}}$ l'est aussi, et son inverse $\sqrt{r}$ est $\mathscr{A}_0$-constructible.



Passons maintenant au cas général. Supposons que $z = x + iy$ et $z' = x' + iy'$ soient $\mathscr{A}_0$-constructibles. Les réels $x$, $x'$, $y$ , $y'$ sont donc $\mathscr{A}_0$-constructibles. Mais alors, les réels $x - x'$, $y - y'$, $xx' - yy'$ et $xy' + x'y$ le sont aussi.
Par conséquent, les nombres complexes

$$z - z' = (x - x') + i(y - y') \quad \text{et} \quad zz' = (xx' - yy') + i(xy' + x'y)$$

sont $\mathscr{A}_0$-constructibles.

De plus, si $z \neq 0$, $\dfrac{1}{x^2 + y^2}$ est $\mathscr{A}_0$-constructible, et par conséquent

$$z^{-1} = \frac{x - iy}{x^2 + y^2}$$

est encore $\mathscr{A}_0$-constructible.

Ainsi, l'ensemble des nombres complexes $\mathscr{A}_0$-constructibles est bien un sous-corps de $\mathbb{C}$, contenant $\mathbb{Q}$, d'après ce qui précède.

Montrons maintenant que si $z \in \mathbb{C}$ est $\mathscr{A}_0$-constructible, toute racine carrée de $z$ l'est aussi. On peut toujours supposer $z \neq 0$. Écrivons alors $z = re^{i\theta}$, avec $r > 0$ et $\theta \in [0, 2\pi[$. Les racines carrées de $z$ sont alors $\pm\sqrt{r}e^{i\frac{\theta}{2}}$. Soit $P$ le point du plan d'affixe $z$. Alors, l'intersection du cercle de centre $O$ et de rayon $OP$ et de l'axe des abscisses est le point $(r, 0)$. Ainsi, le réel $r > 0$ est $\mathscr{A}_0$-constructible. D'après le cas précédent, $\sqrt{r}$ est $\mathscr{A}_0$-constructible. Autrement dit, $A = (\sqrt{r}, 0)$ est $\mathscr{A}_0$-constructible. En intersectant le cercle $\mathscr{C}$ de centre 0 et de rayon $OA$, et la droite $(OP)$, on construit le point $P'$ d'affixe $z' = \sqrt{r}e^{i\theta}$.

Les intersections de la médiatrice de $AP'$ et du cercle $\mathscr{C}$ sont les points d'affixes $\pm\sqrt{r}e^{i\frac{\theta}{2}}$. Cela achève la démonstration. □

Nous allons maintenant pouvoir résoudre (tout du moins en théorie) le problème de la construction à la règle et au compas. Commençons par introduire une nouvelle notation.

**Notation.** Si $\mathscr{A}$ est un ensemble fini de points du plan, on note $\mathbb{Q}(\mathscr{A})/\mathbb{Q}$ la sous-extension de $\mathbb{C}$ engendré par les coordonnées des éléments de $\mathscr{A}$.

Exemple II.2.2. Si $\mathscr{A} = \{(0, 0), (1, 0)\}$, alors $\mathbb{Q}(\mathscr{A}) = \mathbb{Q}$.

On a alors le résultat suivant.

Lemme II.2.3. *Le sous-corps des nombres complexes $\mathscr{A}_0$-constructibles est une extension de $\mathbb{Q}(\mathscr{A}_0)$.*

*En particulier, tout élément de $\mathbb{Q}(\mathscr{A}_0)$ est $\mathscr{A}_0$-constructible.*

*Démonstration.* Soit $E$ l'ensemble des nombres complexes $\mathscr{A}_0$-constructibles. D'après le théorème II.2.1, $E$ est une extension de $\mathbb{Q}$. Par hypothèse, $E$ contient les coordonnées des points de $\mathscr{A}_0$. Il contient donc également la sous-extension engendrée par celles-ci, à savoir $\mathbb{Q}(\mathscr{A}_0)$. □

Nous allons maintenant nous intéresser de plus près à la structure des extensions de $\mathbb{Q}(\mathscr{A}_0)$ obtenues à partir de points $\mathscr{A}_0$-constructibles. On commence par le cas des constructions élémentaires.

Proposition II.2.4. *Soit $P$ un point élémentairement $\mathscr{A}_0$-constructible. Alors, $\mathbb{Q}(\mathscr{A}_0 \cup \{P\})$ est une extension de $\mathbb{Q}(\mathscr{A}_0)$, et l'on a*

$$[\mathbb{Q}(\mathscr{A}_0 \cup \{P\}) : \mathbb{Q}(\mathscr{A}_0)] \leq 2.$$

*Démonstration.* Le premier point est clair, puisque $\mathscr{A}_0 \subset \mathscr{A}_0 \cup \{P\}$. Montrons le second point.

Soient $P_0 = (x_0, y_0)$, $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ trois points de $\mathscr{A}_0$. Supposons que $P_0$ et $P_1$ soient distincts.

Alors :

(i) l'équation de la droite $(P_0P_1)$ est donnée par

$$(x_1 - x_0)(y - y_0) - (y_1 - y_0)(x - x_0) = 0,$$

et est donc de la forme

$$ax + by + c = 0, \qquad \text{avec } a,\ b,\ c \in \mathbb{Q}(\mathscr{A}_0)$$

(ii) l'équation du cercle de centre $P_2$ et de rayon $P_0P_1$ est donnée par

$$(x - x_2)^2 + (y - y_2)^2 = (x_1 - x_0)^2 + (y_1 - y_0)^2,$$

et est donc de la forme

$$x^2 + y^2 + ax + by + c = 0, \qquad \text{avec } a,\ b,\ c \in \mathbb{Q}(\mathscr{A}_0).$$

Supposons tout d'abord que $P = (x, y)$ soit l'intersection de deux droites passant par des points de $\mathscr{A}_0$. D'après ce qui précède, $(x, y)$ est l'unique solution d'un système linéaire de la forme

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0, \end{cases}$$

avec $a,\ b,\ c,\ a', b,', c' \in \mathbb{Q}(\mathscr{A}_0)$. En utilisant les formules de Cramer (ou en résolvant le système directement), on constate que $x$, $y$ sont des fractions rationnelles en $a,\ a', b,\ b', c,\ c'$ à coefficients dans $\mathbb{Q}$, donc des éléments du corps $\mathbb{Q}(\mathscr{A}_0)$. Dans ce cas, on a

$$\mathbb{Q}(\mathscr{A}_0)(x, y) = \mathbb{Q}(\mathscr{A}_0),$$

puisque le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}(\mathscr{A}_0)$, $x$ et $y$ est $\mathbb{Q}(\mathscr{A}_0)$ lui-même.

En particulier, $[\mathbb{Q}(\mathscr{A}_0 \cup \{P\}) : \mathbb{Q}(\mathscr{A}_0)] = 1$.

Supposons maintenant que $P = (x, y)$ soit l'intersection d'une droite et d'un cercle du type précédent. On a ainsi

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0, \end{cases}$$

avec $a$, $b$, $c$, $a', b', c' \in \mathbb{Q}(\mathscr{A}_0)$.

Remarquons que $(a, b) \neq (0, 0)$. Supposons par exemple que $b \neq 0$, et donc que $y = -\dfrac{ax + c}{b}$. Il s'ensuit que $y \in \mathbb{Q}(\mathscr{A}_0)(x)$. Par conséquent,

$$\mathbb{Q}(\mathscr{A}_0)(x, y) = \mathbb{Q}(\mathscr{A}_0)(x)(y) = \mathbb{Q}(\mathscr{A}_0)(x).$$

En remplaçant $y$ par son expression dans la seconde équation, on obtient

$$ux^2 + vx + w = 0, \qquad \text{avec } u,\ v,\ w \in \mathbb{Q}(\mathscr{A}_0).$$

On a nécessairement $(u, v) \neq (0, 0)$. Sinon, cela signifierait que l'intersection du cercle et de la droite est soit vide, ce qui n'est pas le cas par hypothèse, soit infinie, ce qui est impossible. Supposons que $u = 0$. On a donc $v \neq 0$, et par conséquent $x = -wv^{-1} \in \mathbb{Q}(\mathscr{A}_0)$. On conclut alors comme précédemment. Si $u \neq 0$, on a

$$x = \frac{-v \pm \omega}{2u},$$

où $\omega^2$ vérifie $\omega^2 = v^2 - 4uw$. D'après l'exemple I.1.8 (2), on a

$$\mathbb{Q}(\mathscr{A}_0)(x) = \mathbb{Q}(\mathscr{A}_0)(\omega).$$

On utilise alors l'exemple I.1.8 (4) pour conclure. Le cas $a \neq 0$ se traite de la même manière.

Finalement, supposons que $P = (x, y)$ soit l'intersection de deux cercles distincts du type précédent. Ainsi, $(x, y)$ est solution d'un système de la forme

$$\begin{cases} x^2 + y^2 + ax + by + c = 0 \\ x^2 + y^2 + a'x + b'y + c' = 0, \end{cases}$$

avec $a$, $b$, $c$, $a', b', c' \in \mathbb{Q}(\mathscr{A}_0)$.

Remarquons que $(a, b) \neq (a', b')$, car sinon les deux cercles seraient égaux ou d'intersection vide. Ainsi, $(a - a', b - b') \neq (0, 0)$. En soustrayant la seconde équation à la première, on se ramène alors au cas précédent. Cela achève la démonstration. $\square$

On peut alors facilement en déduire le résultat suivant.

Corollaire II.2.5. *Soit $P = (x, y) \in \mathbb{R}^2$ un point $\mathscr{A}_0$-constructible. Alors, il existe une tour d'extensions*

$$E_0 = \mathbb{Q}(\mathscr{A}_0) \subset E_1 \subset \cdots \subset E_r$$

*telle que :*

(1) *pour tout $i \in [\![1, r]\!]$, on a $[E_i : E_{i-1}] \leq 2$,*
(2) *on a $x$, $y \in E_r$.*

*Démonstration.* Soient $P_1, \ldots, P_r = P$ des points de $\mathbb{R}^2$ tels que, pour tout entier $i \in [\![1, r]\!]$, le point $P_i$ soit élémentairement constructible à partir de l'ensemble $\mathscr{A}_0 \cup \{P_1, \ldots, P_{i-1}\}$.

Pour tout $i \in [\![0, r]\!]$, posons $E_i = \mathbb{Q}(\mathscr{A}_0 \cup \{P_1, \ldots, P_i\})$. Alors, on a bien entendu

$$E_0 = \mathbb{Q}(\mathscr{A}_0) \subset E_1 \subset \cdots \subset E_r,$$

et la proposition II.2.4 montre que l'on a $[E_i : E_{i-1}] \leq 2$ pour tout $i \in [\![1, r]\!]$. Enfin, par définition, le corps $E_r$ contient les coordonnées du point $P$, d'où le résultat. □

Ce corollaire conduit naturellement à poser la définition suivante.

Définition II.2.6. On dit qu'une extension $L/K$ est 2-*décomposable* s'il existe une tour d'extensions

$$E_0 = K \subset E_1 \subset \cdots \subset E_r = L$$

vérifiant $[E_i : E_{i-1}] \in \{1, 2\}$, pour tout $i \in [\![1, r]\!]$.

Remarque II.2.7. Le degré d'une extension 2-décomposable est fini et est une puissance de 2. En effet, la formule de multiplicativité des degrés montre que $[L : K]$ est le produit des degrés des extensions $E_i/E_{i-1}$.

Attention néanmoins, une extension dont le degré est une puissance de 2 n'est pas nécessairement 2-décomposable.

Corollaire II.2.8. *Tout nombre complexe $\mathscr{A}_0$-constructible est contenu dans une extension 2-décomposable de $\mathbb{Q}(\mathscr{A}_0)$.*

*Démonstration.* Soit $z = x + iy$ un nombre complexe $\mathscr{A}_0$-constructible. Alors, par définition, le point $P = (x, y)$ est $\mathscr{A}_0$-constructible. Par le corollaire II.2.5, il existe une extension $L/\mathbb{Q}(\mathscr{A}_0)$ 2-décomposable contenant $x$ et $y$. D'après l'exemple I.1.8 (4), on a $[L(i) : L] \leq 2$. L'extension $L(i)/\mathbb{Q}(\mathscr{A}_0)$ est alors aussi 2-décomposable. De plus, $L(i)$ contient $x$, $y$ et $i$, et contient donc $z$. □

Remarque II.2.9. La démonstration du corollaire II.2.5 montre en fait que l'extension 2-décomposable de $\mathbb{Q}(\mathscr{A}_0)$ contenant les coordonnées d'un point élémentairement constructible est un sous-corps de $\mathbb{R}$ (puisqu'elle est construite en rajoutant les coordonnées de points intermédiaires). On a donc en fait le résultat suivant.

Si $z \in \mathbb{C}$ est $\mathscr{A}_0$-constructible, il existe un sous-corps $L$ de $\mathbb{R}$ tel que l'extension $L/\mathbb{Q}(\mathscr{A}_0)$ soit 2-décomposable, et tel que :

(1) $z \in L$ si $z \in \mathbb{R}$ ;
(2) $z \in L(i)$ si $z \in \mathbb{C} \setminus \mathbb{R}$.

Nous en arrivons au théorème fondamental de la construction à la règle et au compas, qui donne une réciproque au corollaire II.2.8.

Théorème II.2.10. *Un nombre complexe est $\mathscr{A}_0$-constructible si, et seulement si, il est contenu dans une extension 2-décomposable de $\mathbb{Q}(\mathscr{A}_0)$.*

*Démonstration.* Le sens direct étant donné par le corollaire II.2.8, il reste donc à voir que tout élément d'une extension 2-décomposable de $\mathbb{Q}(\mathscr{A}_0)$ est $\mathscr{A}_0$-constructible.

On commence par démontrer le résultat suivant : soit $L/K$ une extension de degré 1 ou 2, où $L$ et $K$ sont des sous-corps de $\mathbb{C}$. Alors, si tout élément de $K$ est $\mathscr{A}_0$-constructible, il en est de même de tout élément de $L$.

Soit $z \in L$. Puisque $L$ est de dimension au plus 2 comme $K$-espace vectoriel, la famille $(1, z, z^2)$ est $K$-liée. Il existe donc $u$, $v$, $w \in K$ non tous nuls tels que

$$uz^2 + vz + w = 0.$$

De plus, on a $(u, v) \neq (0, 0)$, car sinon, on aurait $w = 0$.

Supposons tout d'abord que $u = 0$. On a donc $v \neq 0$, et ainsi $z = -wv^{-1}$ est $\mathscr{A}_0$-constructible par le théorème II.2.1. Si $u \neq 0$, on a

$$z = \frac{-v \pm \omega}{2u},$$

où $\omega^2$ vérifie $\omega^2 = v^2 - 4uw$. D'après ce même théorème, le nombre complexe $\omega$ est $\mathscr{A}_0$-constructible et par conséquent, $z$ l'est aussi puisque $u$, $v$ et $\omega$ le sont, d'où le résultat voulu.

Soit maintenant $L/\mathbb{Q}(\mathscr{A}_0)$ une extension 2-décomposable. Il existe donc une tour d'extensions

$$E_0 = \mathbb{Q}(\mathscr{A}_0) \subset E_1 \subset \cdots \subset E_r = L$$

vérifiant $[E_i : E_{i-1}] \leq 2$, pour tout entier $i \in [\![1, r]\!]$. Puisque tout élément de $\mathbb{Q}(\mathscr{A}_0)$ est $\mathscr{A}_0$-constructible par le lemme II.2.3, le point précédent et une récurrence immédiate permettent de conclure. □

Corollaire II.2.11 (Critère de Wantzel). *Si $z \in \mathbb{C}$ est $\mathscr{A}_0$-constructible, alors l'extension $\mathbb{Q}(\mathscr{A}_0)(z)/\mathbb{Q}(\mathscr{A}_0)$ est de degré fini et $[\mathbb{Q}(\mathscr{A}_0)(z) : \mathbb{Q}(\mathscr{A}_0)]$ est une puissance de 2.*

*Autrement dit, si $z \in \mathbb{C}$ est $\mathscr{A}_0$-constructible, alors $z$ est algébrique sur $\mathbb{Q}(\mathscr{A}_0)$, et son degré est une puissance de 2.*

*Démonstration.* D'après le théorème précédent, $z$ est contenu dans un extension $L/\mathbb{Q}(\mathscr{A}_0)$ 2-décomposable. On a donc

$$\mathbb{Q}(\mathscr{A}_0) \subset \mathbb{Q}(\mathscr{A}_0)(z) \subset L.$$

La formule de multiplicativité des degrés montre alors que le degré de l'extension $\mathbb{Q}(\mathscr{A}_0)(z)/\mathbb{Q}(\mathscr{A}_0)$ divise le degré de $L/\mathbb{Q}(\mathscr{A}_0)$, qui est une puissance de 2, par la remarque II.2.7. Le résultat en découle aisément. □

**Attention !** La réciproque de ce résultat est fausse. On peut construire une infinité de nombres complexes non constructibles, mais engendrant une extension de degré 4 sur $\mathbb{Q}$.

Le théorème I.2.8 nous permet donc de calculer le degré d'une extension algébrique $K(\alpha)/K$, sous réserve que l'on sache calculer $\mu_{\alpha,K}$. En utilisant ce théorème de façon répétée, on peut aussi calculer le degré d'une extension de la forme $K(\alpha_1, \ldots, \alpha_n)/K$, où $\alpha_1, \ldots, \alpha_n$ sont algébriques sur $K$, mais les calculs peuvent devenir assez délicats, car le calcul d'un polynôme minimal sur un corps quelconque n'est pas toujours aisé.

Nous allons pour cela introduire la notion d'extensions linéairement disjointes.

## II.3. Disjonction linéaire

Nous allons maintenant nous intéresser au problème suivant. On se fixe une fois pour toutes une extension $L/K$, et deux sous-extensions $E/K$ et $E'/K$ de $L/K$. Peut-on comparer les degrés de $EE'/E'$ et de $E/K$ ?

Un premier pas dans cette direction est donné par le lemme suivant.

Lemme II.3.1. *Si $E/K$ est algébrique, toute famille $K$-génératrice de $E$ est une famille $E'$-génératrice de $EE'$. En particulier, on a*

$$EE' = \Big\{ \sum_{i=1}^{n} x_i x_i' \mid n \geq 0,\ x_i \in E,\ x_i' \in E' \Big\},$$

*et l'on a*

$$[EE' : E'] \leq [E : K].$$

*Démonstration.* Soit $\mathscr{S}$ une famille $K$-génératrice de $E$. En particulier, on a l'égalité $E = K(\mathscr{S})$, et ainsi $EE' = E'(\mathscr{S})$, par l'exemple I.2.16.

Soit $y \in EE'$. D'après la proposition I.1.7, $y$ est une fraction rationnelle à coefficients dans $E'$ en un nombre fini d'éléments $s_1, \ldots, s_n \in \mathscr{S}$. En particulier, $y \in E'(s_1, \ldots, s_n)$. Comme $s_1, \ldots, s_n$ sont algébriques sur $K$ par hypothèse, donc algébriques aussi sur $E'$, on a

$$E'(s_1, \ldots, s_n) = E'[s_1, \ldots, s_n],$$

d'après le corollaire I.2.11. Or, un monôme en $s_1, \ldots, s_n$ est un élément de $E$. Il est donc combinaison $K$-linéaire d'éléments de $\mathscr{S}$. On en déduit que tout élément de $E'[s_1, \ldots, s_n]$ est une combinaison $E'$-linéaire d'éléments de $\mathscr{S}$. En particulier, c'est le cas de $y$. Ainsi, $\mathscr{S}$ est bien une famille $E'$-génératrice de $EE'$. L'égalité décrivant $EE'$ est alors claire.

L'inégalité $[EE' : E'] \leq [E : K]$ s'obtient alors en appliquant ce qui précède à une $K$-base de $E$ (même si $E/K$ est de degré infini, car l'inégalité est alors triviale). Cela achève la démonstration. □

Remarque II.3.2. Ce résultat est faux si l'extension $E/K$ n'est pas algébrique. En effet, soient $X, Y$ deux indéterminées sur $\mathbb{C}$, et soit $L = \mathbb{C}(X, Y)$. Posons $E = \mathbb{C}(X)$ et $E' = \mathbb{C}(Y)$. Alors, le théorème de décomposition en éléments simples montre que les éléments

$$X^n, \quad \frac{1}{(X-a)^m}, \quad n \geq 0,\ m \geq 1$$

engendrent $E$. En revanche, ces éléments n'engendrent pas $EE' = \mathbb{C}(X, Y)$ sur $E'$, comme on peut le constater en considérant $\dfrac{1}{X+Y}$.

Nous allons maintenant nous intéresser à la conservation de la liberté d'une famille. On commence par un lemme.

Lemme II.3.3. *Soient $E/K$ et $E'/K$ deux sous-extensions de $L/K$. Alors, les propriétés suivantes sont équivalentes :*

(1) *toute famille $K$- libre de $E$ est encore une famille $E'$-libre de $EE'$ ;*
(2) *toute famille $K$- libre de $E'$ est encore une famille $E$-libre de $EE'$.*

*Dans ce cas, on a nécessairement $E \cap E' = K$.*

*Démonstration.* Il suffit de démontrer l'implication « (1) $\Longrightarrow$ (2) », l'autre implication s'en déduisant en échangeant les rôles de $E$ et $E'$.

Il suffit bien entendu de considérer les familles libres de cardinal fini, vu la définition d'une famille libre. Soit $(x'_1, \dots, x'_n)$ une famille $K$-libre d'éléments de $E'$. Supposons qu'elle soit $E$-liée. En particulier, $n \geq 1$. Il existe donc $x_1, \dots, x_n \in E$ non tous nuls tels que

$$x_1 x'_1 + \cdots + x_n x'_n = 0.$$

Si $(x_1, \dots, x_n)$ était $K$-libre, elle serait aussi $E'$-libre par hypothèse, et l'on aurait donc $x'_1 = \cdots = x'_n = 0$, ce qui contredirait la liberté de $(x'_1, \dots, x'_n)$.

Ainsi, $(x_1, \dots, x_n)$ est $K$-liée. Quitte à renuméroter, on peut supposer que la famille $(x_1, \dots, x_r)$ est une base du sous-espace engendré par $(x_1, \dots, x_n)$, pour un certain entier $r \in [\![1, n-1]\!]$.

Pour tout $j \in [\![r+1, n]\!]$, on peut alors écrire

$$x_j = \sum_{i=1}^{r} \lambda_{ij} x_i, \quad \lambda_{ij} \in K.$$

Mais alors, on a

$$x_1 x'_1 + \cdots + x_r x'_r + \sum_{j=r+1}^{n} x'_j \Big( \sum_{i=1}^{r} \lambda_{ij} x_i \Big) = 0,$$

soit encore

$$\sum_{i=1}^{r} \Big( x'_i + \sum_{j=r+1}^{n} \lambda_{ij} x'_j \Big) x_i = 0.$$

Puisque $(x_1, \dots, x_r)$ est $K$-libre, elle est $E'$-libre par hypothèse, d'où

$$x'_i = - \sum_{j=r+1}^{n} \lambda_{ij} x'_j, \quad \text{pour tout } i \in [\![1, r]\!].$$

Mais alors, $(x'_1, \dots, x'_n)$ est $K$-liée, d'où une contradiction. Cela démontre le résultat voulu.

Montrons la dernière partie. Supposons que la propriété (1) soit vérifiée, par exemple, mais que $E \cap E' \neq K$. En particulier, $[E \cap E' : K] \geq 2$. Il existe donc deux éléments $x$, $y \in E \cap E'$ tels que la famille $(x, y)$ soit libre. En particulier, ces éléments sont tous deux non nuls. Or, deux tels éléments sont $E'$-liés, puisque $-yx + xy = 0$, d'où une contradiction. On a donc bien $E \cap E' = K$. □

Définition II.3.4. Soit $L/K$ une extension de corps.

Deux sous-extensions $E/K$ et $E'/K$ de $L/K$ sont dites *linéairement disjointes* si elles vérifient une des conditions équivalentes du lemme précédent.

Dans ce cas, on a nécessairement $E \cap E' = K$.

Exemple II.3.5. La condition $E \cap E' = K$ est nécessaire pour avoir la disjonction linéaire, mais elle n'est pas suffisante.

Posons en effet $E = \mathbb{Q}(\sqrt[3]{2})$ et $E' = \mathbb{Q}(j\sqrt[3]{2})$. Le polynôme unitaire $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$ d'après le critère d'Eisenstein. On a donc

$$\mu_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2,$$

et ainsi $[E : \mathbb{Q}] = 3$. Puisque $E \cap E'/\mathbb{Q}$ est une sous-extension de $E/\mathbb{Q}$, on a $[E \cap E' : \mathbb{Q}] \mid [E : \mathbb{Q}]$. Ainsi, $[E \cap E' : \mathbb{Q}] = 1$ ou 3.

Si l'on avait $[E \cap E' : \mathbb{Q}] = 3$, on aurait $E \cap E' = E$ et donc $E' = E \subset \mathbb{R}$, ce qui n'est pas le cas. Par conséquent, $[E \cap E' : \mathbb{Q}] = 1$, ou encore $E \cap E' = \mathbb{Q}$.

D'autre part, $(1, \sqrt[3]{2}, (\sqrt[3]{2})^2)$ est une $\mathbb{Q}$-base de $E$. Elle est donc $\mathbb{Q}$-libre. En revanche, elle est $E'$-liée, puisque

$$2 \cdot 1 + (j\sqrt[3]{2})^2 \cdot \sqrt[3]{2} + j\sqrt[3]{2} \cdot (\sqrt[3]{2})^2 = 2(1 + j + j^2) = 0.$$

L'intérêt de cette notion est donnée par la proposition suivante.

Proposition II.3.6. *Soient $E/K$ et $E'/K$ deux sous-extensions de $L/K$. On suppose que $E/K$ est de degré fini. Alors, on a*

$$[EE' : E'] \leq [E : K],$$

*et l'on a égalité si, et seulement si, $E/K$ et $E'/K$ sont linéairement disjointes.*

*Démonstration.* Puisqu'une extension de corps de degré fini est algébrique, l'inégalité $[EE' : E'] \leq [E : K]$ découle du lemme II.3.1. Si les extensions $E/K$ et $E'/K$ sont linéairement disjointes, toute $K$-base de $E$ reste une $E'$-base de $EE'$, d'après la définition et ce même lemme. On a donc égalité dans ce cas. Inversement, supposons que l'on ait

$$[EE' : E'] = [E : K] = d.$$

Soit $(x_1, \ldots, x_r)$ une famille $K$-libre de $E$ (donc $r \leq d$), que l'on complète en une $K$-base $(x_1, \ldots, x_d)$ de $E$. C'est donc une famille $E'$-génératrice de $EE'$ par le lemme II.3.1. Puisque $EE'$ est de dimension $d$ sur $E'$ par hypothèse, c'est une $E'$-base de $EE'$. En particulier, la famille $(x_1, \ldots, x_r)$ est $E'$-libre. Par conséquent, $E/K$ et $E'/K$ sont linéairement disjointes. □

Corollaire II.3.7. *Soient $E/K$ et $E'/K$ deux sous-extensions de $L/K$ de degré fini. Alors, on a*

$$[EE' : E'] \leq [E : K], \ [EE' : E] \leq [E' : K], \ [EE' : K] \leq [E : K][E' : K],$$

*et l'on a* $[EE' : K] = [E : K][E' : K]$ *si, et seulement si,* $E/K$ *et* $E'/K$ *sont linéairement disjointes.*

*En particulier, c'est le cas si* $[E : K]$ *et* $[E' : K]$ *sont premiers entre eux.*

*Démonstration.* Les deux premières inégalités découlent de la proposition précédente. On a alors

$$[EE' : K] = [EE' : E'][E' : K] \leq [E : K][E' : K].$$

On a égalité si, et seulement si, $[EE' : E'] = [E : K]$, c'est-à-dire si, et seulement si, $E/K$ et $E'/K$ sont linéairement disjointes, toujours d'après cette même proposition.

Supposons que les entiers $[E : K]$ et $[E' : K]$ soient premiers entre eux. Puisque $[E : K]$ et $[E' : K]$ divisent $[EE' : K]$, $[E : K][E' : K]$ divise aussi $[EE' : K]$. En particulier, on a $[EE' : K] \geq [E : K][E' : K]$. Le premier point implique alors que $[EE' : K] = [E : K][E' : K]$. Cela achève la démonstration. □

Exemple II.3.8. Puisque $\alpha = \sqrt[4]{2}$ et $\beta = \sqrt[5]{2}$ sont algébriques sur $\mathbb{Q}$, l'extension $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ est algébrique. D'après le critère d'Eisenstein, les polynômes $X^4 - 2$ et $X^5 - 2$ sont irréductibles dans $\mathbb{Q}[X]$. On a donc

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 \quad \text{et} \quad [\mathbb{Q}(\beta) : \mathbb{Q}] = 5.$$

D'après le corollaire précédent, les extensions $\mathbb{Q}(\alpha)/\mathbb{Q}$ et $\mathbb{Q}(\beta)/\mathbb{Q}$ sont linéairement disjointes. On a alors

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}] = 20.$$

Nous allons maintenant pouvoir résoudre les problèmes de construction cités en début de chapitre.

## II.4. Quelques problèmes de construction à la règle et au compas

Intéressons nous maintenant à quelques problèmes de construction à la règle et au compas. On commence par le plus célèbre d'entre eux.

*La quadrature du cercle.* Comme expliqué au début de ce chapitre, il s'agit de savoir si $\sqrt{\pi}$ est constructible à la règle au compas à partir du segment-unité. Si c'était le cas, $\pi = (\sqrt{\pi})^2$ serait aussi constructible. En particulier, le critère de Wantzel entraînerait que $\mathbb{Q}(\pi)/\mathbb{Q}$ serait de degré fini, et donc que $\pi$ serait algébrique sur $\mathbb{Q}$. Or, un célèbre

théorème de Lindemann affirme que $\pi$ est transcendant sur $\mathbb{Q}$. La quadrature du cercle est donc impossible.

*La duplication du cube-unité.* Cela revient à savoir si $\sqrt[3]{2}$ est constructible à partir du segment-unité. Comme on l'a déjà constaté, $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$, de degré 3. D'après le critère de Wantzel, $\sqrt[3]{2}$ n'est pas constructible, et la duplication du cube-unité s'avère impossible.

*La trisection de l'angle.* On se donne un segment-unité $OI$, ainsi que trois points $A$, $B$, $C$ du plan, tels que les deux demi-droites issues de $A$ et passant respectivement par $B$ et $C$ forment un angle de mesure $\theta \in [0, \pi[$, non orienté.

En utilisant pour origine d'un repère orthonormé le point $A$, et une des deux droites $(AB)$ ou $(AC)$ comme un des axes, et en traçant le cercle de centre $A$ et de rayon $OI = 1$, on peut toujours se ramener à la question suivante : peut-on construire le point $Q = \Big(\cos\big(\frac{\theta}{3}\big), \sin\big(\frac{\theta}{3}\big)\Big)$ à partir des points $O, I$ et du point $P = \big(\cos(\theta), \sin(\theta)\big)$ ?

Remarquons qu'un point $\big(\cos(\varphi), \sin(\varphi)\big)$, avec $\varphi \in [0, \pi[$, est constructible à partir d'un ensemble $\mathscr{A}_0$ si, et seulement si, $\big(\cos(\varphi), 0\big)$ l'est, puisque l'on peut retrouver $\big(\cos(\varphi), \sin(\varphi)\big)$ en intersectant la droite $x = \cos(\varphi)$ avec la moitié supérieure du cercle-unité. Le problème de la trisection de l'angle se reformule donc de la façon suivante : soit $\mathscr{A}_0 = \{(0,0), (1,0), \big(\cos(\theta), 0\big)\}$. Le réel $\cos\big(\frac{\theta}{3}\big)$ est-il $\mathscr{A}_0$-constructible ?

Remarquons que dans ce cas, on a $\mathbb{Q}(\mathscr{A}_0) = \mathbb{Q}\big(\cos(\theta)\big)$. Pour tout $\varphi \in \mathbb{R}$, on a

$$e^{3i\varphi} = (e^{i\varphi})^3 = \big(\cos(\varphi) + i\sin(\varphi)\big)^3.$$

En développant et en identifiant les parties réelles, on obtient

$$\cos(3\varphi) = \cos(\varphi)^3 - 3\cos(\varphi)\sin(\varphi)^2 = 4\cos(\varphi)^3 - 3\cos(\varphi).$$

En particulier, le polynôme $P = 4X^3 - 3X - \cos(\theta) \in \mathbb{Q}\big(\cos(\theta)\big)[X]$ annule le réel $\alpha = \cos\left(\frac{\theta}{3}\right)$. Ainsi, $\mu_{\alpha,\mathbb{Q}(\cos(\theta))} \mid P$.

Si $P$ possède une racine dans $\mathbb{Q}\big(\cos(\theta)\big)$, il n'est pas irréductible et par conséquent $\mu_{\alpha,\mathbb{Q}(\cos(\theta))}$ est de degré 1 ou 2. Ainsi, $\mathbb{Q}\big(\cos(\theta)\big)(\alpha)/\mathbb{Q}\big(\cos(\theta)\big)$ est 2-décomposable et $\alpha$ est $\mathscr{A}_0$-constructible par le théorème II.2.10.

Si $P$ n'a pas de racine dans $\mathbb{Q}\big(\cos(\theta)\big)$, alors $P$ est irréductible puisque $P$ est de degré 3. On a alors $\mu_{\alpha,\mathbb{Q}(\cos(\theta))} = \dfrac{1}{4}P$, et $\alpha$ est alors alors de degré 3 sur $\mathbb{Q}\big(\cos(\theta)\big)$. Dans ce cas, $\alpha$ n'est pas $\mathscr{A}_0$-constructible.

En résumé, nous avons démontré le résultat suivant.

THÉORÈME II.4.1. *Soit $\theta \in [0, \pi[$. Alors, l'angle de mesure $\theta$ est trisectable à la règle et au compas si, et seulement si, le polynôme*

$$4X^3 - 3X - \cos(\theta)$$

*admet une racine dans* $\mathbb{Q}\big(\cos(\theta)\big)$.

EXEMPLES II.4.2. (1) Soit $\theta = \dfrac{2\pi}{3}$. Alors, $\cos(\theta) = -\dfrac{1}{2}$, et ainsi $\mathbb{Q}\big(\cos(\theta)\big) = \mathbb{Q}$. On doit vérifier si le polynôme $4X^3 - 3X + \dfrac{1}{2}$ a une racine rationnelle ou non. Cela revient à savoir si $8X^3 - 6X + 1$ a une racine rationnelle ou non. Les racines rationnelles possibles sont ici

$$\pm 1, \quad \pm\frac{1}{2}, \quad \pm\frac{1}{4}, \quad \pm\frac{1}{8},$$

et l'on vérifie qu'aucune de ces possibilités ne convient. Ainsi, $\dfrac{2\pi}{3}$ n'est pas trisectable à la règle et au compas.

(2) Soit $\theta = \dfrac{\pi}{4}$. Ici, $\cos(\theta) = \dfrac{\sqrt{2}}{2}$, d'où $\mathbb{Q}\big(\cos(\theta)\big) = \mathbb{Q}(\sqrt{2})$. Il faut donc voir si le polynôme $4X^3 - 3X + \sqrt{2}/2$ possède une racine dans $\mathbb{Q}(\sqrt{2})$. On vérifie effectivement que $-\sqrt{2}/2$ est une telle racine. Par conséquent, l'angle de mesure $\dfrac{\pi}{4}$ est trisectable à la règle et au compas.

Il y a en fait une manière plus simple de le constater. Comme on a l'égalité $\cos\left(\frac{\pi}{6}\right) = \sqrt{3}/2$, on peut construire l'angle de mesure $\dfrac{\pi}{6}$ à la règle et au compas à partir du segment-unité, puis obtenir celui de mesure $\dfrac{\pi}{12}$ par bissection.

*La construction du $n$-gone régulier.* Le problème est ici de construire les sommets d'un $n$-gone régulier à la règle et au compas. On se convainc facilement qu'il suffit de savoir construire un $n$-gone régulier centré en $O$, et dont un des sommets est le point $I = (1, 0)$. Dans ce cas, il faut et il suffit de savoir construire le point $P = \left(\cos\left(\frac{2\pi}{n}\right), \sin\left(\frac{2\pi}{n}\right)\right)$. Une fois ce point construit, il suffit d'utiliser le compas pour obtenir les autres sommets en reportant la longueur $IP$.

Par conséquent, la question devient : étant donné un entier $n \geq 3$, le nombre complexe $\zeta_n = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ est-il constructible ?

On commence par se réduire au cas des puissances de nombres premiers.

LEMME II.4.3. *Soient $m, n \geq 1$ deux entiers premiers entre eux.*

*Alors, le mn-gone régulier est constructible si, et seulement si, le n-gone régulier et le m-gone régulier sont constructibles.*

*Démonstration.* Il suffit de voir que $\zeta_{mn}$ est constructible si, et seulement si, $\zeta_m$ et $\zeta_n$ le sont. Si $\zeta_{mn}$ est constructible, alors $\zeta_n = \zeta_{mn}^m$ et $\zeta_m = \zeta_{mn}^n$ sont aussi constructibles.

Inversement, supposons que $\zeta_m$ et $\zeta_n$ soient constructibles. Puisque $m$ et $n$ sont premiers entre eux, il existe $u$, $v \in \mathbb{Z}$ tels que $um + vn = 1$.

Mais alors, on a

$$\zeta_{mn} = (\zeta_{mn}^m)^u (\zeta_{mn}^n)^v = \zeta_n^u \zeta_m^v.$$

Ainsi, $\zeta_{mn}$ est aussi constructible. □

Ce lemme implique immédiatement que $\zeta_n$ est constructible si, et seulement si, $\zeta_{p^{v_p(n)}}$ est constructible pour tout diviseur premier $p$ de $n$. Il reste à examiner le cas d'une puissance de nombre premier.

Lemme II.4.4. *Soit $p$ un nombre premier et $m \geq 1$. Alors, $\mu_{\zeta_{p^m},\mathbb{Q}} = X^{p^{m-1}(p-1)} + X^{p^{m-1}(p-2)} + \cdots + X^{p^{m-1}} + 1$.*

*En particulier, $[\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}] = p^{m-1}(p-1)$.*

*Démonstration.* Soit $f = X^{p^{m-1}(p-1)} + X^{p^{m-1}(p-2)} + \cdots + X^{p^{m-1}} + 1$. Pour démontrer le lemme, il suffit de démontrer que $f(\zeta_{p^m}) = 0$ et que $f$ est irréductible sur $\mathbb{Q}$.

On commence par remarquer que

$$(X^{p^{m-1}} - 1)f = (X^{p^{m-1}})^p - 1 = X^{p^m} - 1.$$

En particulier, en évaluant en $\zeta_{p^m}$, on obtient $(\zeta_p^m - 1)f(\zeta_{p^m}) = 0$, d'où $f(\zeta_{p^m}) = 0$. Montrons que $f$ est irréductible sur $\mathbb{Q}$. Ceci est équivalent à montrer que $f(X+1)$ est irréductible sur $\mathbb{Q}$. Dans l'anneau $\mathbb{F}_p[X]$, on a

$$((X+1)^{p^{m-1}} - 1)f(X+1) = X^{p^{m-1}} f(X+1) = (X+1)^{p^m} - 1 = X^{p^m}.$$

Ainsi, $f(X+1) = X^{p^m - p^{m-1}}$ dans $\mathbb{F}_p[X]$. Par conséquent, $p$ ne divise pas le coefficient dominant de $f(X+1)$, et $p$ divise tous les autres coefficients de $f(X+1)$. Un simple calcul montre également que le terme constant de $f(X+1)$ est $p$, qui est non divisible par $p^2$. Par conséquent, $f(X+1)$ est $p$-Eisenstein, donc irréductible sur $\mathbb{Q}$. □

Revenons à notre problème de constructibilité.

Remarquons que par bissections successives de l'angle plat, qui est évidemment constructible, on peut obtenir l'angle de mesure $\dfrac{2\pi}{2^m}$ pour

tout entier $m \geq 0$. Ainsi, le polygone régulier à $2^m$ côtés est constructible pour tout entier $m \geq 0$.

Supposons maintenant que $\zeta_{p^m}$ soit constructible, où $p$ est impair et $m \geq 1$. Le critère de Wantzel et le lemme précédent impliquent que $m = 1$ et $p - 1$ est une puissance de 2.

Écrivons $p = 1 + 2^k$. Alors, $k$ une puissance de 2. En effet, supposons que $k$ soit divisible par un nombre premier impair $\ell$, et écrivons $k = \ell r$, avec $r \geq 1$. Alors, on a $1 + (2^r)^\ell = 1 - (-2^r)^\ell$ car $\ell$ est impair, d'où

$$p = (1 + 2^r)(2^{r(\ell-1)} - 2^{r(\ell-2)} + \cdots + 2^{2r} - 2^r + 1).$$

Ainsi, $1+2^r \mid p$. Puisque $\ell > 1$, $1+2^r < p$ et est donc un diviseur strict de $p$, ce qui contredit la primalité de $p$.

Définition II.4.5. Soit $m \geq 0$. L'entier $F_m = 1 + 2^{2^m}$ est appelé le *$m$-ième nombre de Fermat.*

On vient donc de démontrer le résultat partiel suivant.

Proposition II.4.6. *Si le $n$-gone régulier est constructible, alors $n$ est produit d'une puissance de 2 et de nombres de Fermat premiers deux à deux distincts.*

Remarque II.4.7. Fermat conjecturait que les entiers $F_m$ étaient tous premiers. C'est vrai pour $m = 0$, 1, 2, 3 et 4, puisque

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257 \quad \text{et} \quad F_4 = 65537,$$

mais faux pour $m = 5$, puisque

$$F_5 = 641 \cdot 6700417.$$

Les seuls nombres de Fermat premiers connus à ce jour sont $F_0, \ldots, F_4$. On ne sait pas à l'heure actuelle s'il existe une infinité de nombres de Fermat premiers.

La question qui se pose maintenant est de savoir si la réciproque de la proposition précédente est vraie. Commençons par réduire le problème au cas d'un nombre de côtés premier impair. Il résulte de ce qui précède que la réciproque à la proposition II.4.6 est vraie si, et seulement si, pour tout nombre premier de Fermat $p$, le $p$-gone régulier est constructible.

Nous allons maintenant démontrer que c'est effectivement le cas. **ZE** bonne idée [1] est de considérer le groupe des automorphismes de $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Avant d'expliquer pourquoi, introduisons une définition.

1. Due à Évariste Galois.

Définition II.4.8. Soit $L/K$ une extension. Le *groupe de Galois* de $L/K$ est le groupe des automorphismes de l'extension $L/K$, c'est-à-dire le groupe des automorphismes de $K$-algèbres de $L$. On le note $\mathrm{Gal}(L/K)$.

Si $\sigma, \tau \in \mathrm{Gal}(L/K)$, on écrira $\sigma\tau$ au lieu de $\sigma \circ \tau$.

On a alors le lemme suivant.

Lemme II.4.9. *Soit $L$ un corps, et soit $\mathscr{S}$ un ensemble de morphismes d'anneaux $L \longrightarrow L$. Alors :*

(1) *l'ensemble*

$$L^{\mathscr{S}} = \{x \in L \mid \sigma(x) = x, \quad \textit{pour tout } \sigma \in \mathscr{S}\}$$

*est un sous-corps de $L$ ;*

(2) *si tous les éléments de $\mathscr{S}$ sont des automorphismes, on a*

$$L^{\mathscr{S}} = L^{\langle \mathscr{S} \rangle},$$

*où $\langle \mathscr{S} \rangle$ est le sous-groupe de $\mathrm{Aut}(L)$ engendré par $\mathscr{S}$ ;*

(3) *si $L$ est une extension de $K$, et si $\mathscr{S} \subset \mathrm{Gal}(L/K)$, alors $L^{\mathscr{S}}$ est une extension de $K$.*

*Démonstration.* Montrons le premier point. Puisque les éléments de $\mathscr{S}$ sont des morphismes d'anneaux, on a $\sigma(0) = 0$ et $\sigma(1) = 1$, pour tout $\sigma \in \mathscr{S}$. Ainsi, $0, 1 \in L^{\mathscr{S}}$. Si de plus $x$, $y \in L^{\mathscr{S}}$, pour tout $\sigma \in \mathscr{S}$, on a

$$\sigma(x - y) = \sigma(x) - \sigma(y) = x - y \quad \text{et} \quad \sigma(xy) = \sigma(x)\sigma(y) = xy.$$

Ainsi, $x - y$, $xy \in L^{\mathscr{S}}$. Enfin, si $x \in L^{\times}$, on a aussi

$$\sigma(x^{-1}) = \sigma(x)^{-1} = x^{-1}, \quad \text{pour tout } \sigma \in L^{\mathscr{S}},$$

et ainsi $x^{-1} \in L^{\mathscr{S}}$, d'où le premier point.

Supposons que $\mathscr{S} \subset \mathrm{Aut}(L)$. Comme $\mathscr{S} \subset \langle \mathscr{S} \rangle$, on a $L^{\mathscr{S}} \supset L^{\langle \mathscr{S} \rangle}$. Si maintenant $x \in L$ est fixé par tous les éléments de $\mathscr{S}$, il est fixé par les produits des éléments de $\mathscr{S}$ et de leurs inverses. On a donc l'inclusion manquante.

Le dernier point découle directement de (1) et du fait qu'un élément du groupe $\mathrm{Gal}(L/K)$ fixe $K$ point par point. Cela achève la démonstration. $\square$

Le groupe de Galois permet donc de construire des sous-extensions de $L/K$. Nous allons maintenant regarder le cas de l'extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

Lemme II.4.10. *Soit $p$ un nombre premier. Alors,*

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\big) \simeq (\mathbb{Z}/p\mathbb{Z})^\times.$$

*Plus précisément, pour tout $m \in \mathbb{Z}$ premier à $p$, il existe un unique $\sigma_m \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ tel que $\sigma_m(\zeta_p) = \zeta_p^m$.*

*Réciproquement, tout élément de $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ est de la forme $\sigma_m$, où $m$ est un entier premier à $p$, unique modulo $p$.*

*Enfin, l'application*

$$\begin{aligned}(\mathbb{Z}/p\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\\ \overline{m} &\longmapsto \sigma_m\end{aligned}$$

*est un isomorphisme de groupes.*

*Démonstration.* Soit $\sigma \in \mathrm{Gal}\big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\big)$. Alors, $\sigma(\zeta_p)^p = \sigma(\zeta_p^p) = \sigma(1) = 1$. Comme $\sigma$ induit un automorphisme de groupes de $\mathbb{Q}(\zeta_p)^\times$, $\sigma(\zeta_p)$ est une racine l'unité d'ordre $p$, i.e. une racine primitive $p$-ième de l'unité. Il existe donc un entier $m_\sigma \in \mathbb{Z}$ premier à $p$ tel que $\sigma(\zeta_p) = \zeta_p^{m_\sigma}$. Cet entier $m_\sigma$ est unique modulo $p$, et la classe $\overline{m}_\sigma$ est donc un élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ bien défini, que l'on note $\rho(\sigma)$. Montrons que l'application

$$\begin{aligned}\rho\colon \mathrm{Gal}\big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\big) &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times\\ \sigma &\longmapsto \overline{m}_\sigma\end{aligned}$$

est un morphisme de groupes injectif.

Soient $\sigma_1$, $\sigma_2 \in \mathrm{Gal}\big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\big)$, et soient $m_1$, $m_2 \in \mathbb{Z}$ premiers à $p$ tels que

$$\sigma_i(\zeta_p) = \zeta_p^{m_i}, \quad i = 1, 2.$$

On a alors

$$(\sigma_1\sigma_2)(\zeta_p) = \sigma_1(\zeta_p^{m_2}) = \sigma_1(\zeta_p)^{m_2} = \zeta_p^{m_1 m_2}.$$

On en déduit donc

$$\rho(\sigma\tau) = \overline{m_1 m_2} = \overline{m}_1\overline{m}_2 = \rho(\sigma)\rho(\tau).$$

Ainsi, $\rho$ est bien un morphisme de groupes. Soit alors $\sigma \in \mathrm{Gal}\big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\big)$ tel que $\rho(\sigma) = \overline{1}$. Cela signifie donc que $\sigma(\zeta_p) = \zeta_p$.

Le théorème de prolongement des isomorphismes montre alors que $\sigma = \mathrm{Id}_{\mathbb{Q}(\zeta_p)}$. Le lemme II.4.4 montre que le polynôme minimal de $\zeta_p$ sur $\mathbb{Q}$ est $X^{p-1} + \cdots + X + 1$, dont les racines sont exactement les racines primitives $p$-ièmes de l'unité, qui sont toutes dans $\mathbb{Q}(\zeta_p)$ (ce sont des puissances de $\zeta_p$). Le théorème de prolongements des isomorphismes implique alors que $|\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = p - 1$, et $\rho$ est un isomorphisme.

Le reste du lemme en découle, en observant que $\rho^{-1}(m) = \sigma_m$. $\square$

Revenons à notre problème de construction du $p$-gone régulier, où $p = 1 + 2^n$ est un nombre de Fermat premier. Posons $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Puisque $p$ est un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique d'ordre $p-1$. D'après le lemme II.4.10, il est donc de même du groupe $G$. Soit $\rho$ un générateur de $G$.

Pour tout $i \in [\![0, n]\!]$, on pose $G_i = \langle \rho^{2^i} \rangle$ et $L_i = \mathbb{Q}(\zeta_p)^{G_i}$. Comme on a

$$G_n = \{\mathrm{Id}\} \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G,$$

on a

$$L_0 \subset L_1 \subset \cdots \subset L_{n-1} \subset L_n = \mathbb{Q}(\zeta_p).$$

Nous allons montrer la proposition suivante.

Proposition II.4.11. *Avec les notations précédentes, on a :*

(1) $L_0 = \mathbb{Q}$ ;

(2) *pour tout* $i \in [\![1, n]\!]$, *on a* $[L_i : L_{i-1}] = 2$. *De plus, on a* $L_i = L_{i-1}(\alpha_i)$, *avec* $\alpha_i = \sum_{k=0}^{2^{n-i}-1} \rho^{2^i k}(\zeta_p)$.

*En particulier,* $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ *est* 2*-décomposable, et* $\zeta_p$ *est constructible.*

*Démonstration.* Avant tout, rappelons que chaque élément de $G$ est déterminé de façon unique par l'image de $\zeta_p$, qui est une racine primitive $p$-ième de l'unité. Ainsi, les éléments

$$\zeta_p,\ \rho(\zeta_p), \ldots,\ \rho^{p-2}(\zeta_p)$$

sont les $p-1$ puissances non triviales de $\zeta_p$. Ils forment une famille $\mathbb{Q}$-libre, donc une $\mathbb{Q}$-base de $\mathbb{Q}(\zeta_p)$.

Soit maintenant $z \in L_0 = \mathbb{Q}(\zeta_p)^G$. Écrivons $z = a_0\zeta_p + \cdots + a_{p-2}\rho^{p-2}(\zeta_p)$, avec $a_i \in \mathbb{Q}$. Puisque $z \in L_0$, en tenant compte de l'égalité $\rho^{p-1} = \mathrm{Id}$, on a

$$z = \rho(z) = a_0\rho(\zeta_p) + \cdots + a_{p-3}\rho^{p-2}(\zeta_p) + a_{p-2}\zeta_p.$$

On en déduit les égalités $a_0 = \cdots = a_{p-2}$, d'où $z = a_0\big(\zeta_p + \cdots + \rho^{p-2}(\zeta_p)\big)$, ou encore

$$z = a_0(\zeta_p + \cdots + \zeta_p^{p-1}) = -a_0 \in \mathbb{Q}.$$

On a donc $L_0 = \mathbb{Q}$, d'où (1).

Passons au point (2). Montrons que $\alpha_i \in L_i \setminus L_{i-1}$.

On a :

$$\begin{aligned}\rho^{2^i}(\alpha_i) &= \sum_{k=0}^{2^{n-i}-1} \rho^{2^i(k+1)}(\zeta_p)\\ &= \sum_{k=1}^{2^{n-i}} \rho^{2^i k}(\zeta_p)\\ &= \sum_{k=1}^{2^{n-i}-1} \rho^{2^i k}(\zeta_p) + \rho^{2^n}(\zeta_p).\end{aligned}$$

Puisque $\rho^{2^n} = \rho^{p-1} = \mathrm{Id}$, on en déduit que $\rho^{2^i}(\alpha_i) = \alpha_i$. Comme $G_i$ est engendré par $\rho^{2^i}$, on en conclut que $\alpha_i$ est fixé par tout élément de $G_i$, c'est-à-dire $\alpha_i \in L_i$. Par ailleurs, on a

$$\rho^{2^{i-1}}(\alpha_i) = \sum_{k=0}^{2^{n-i}-1} \rho^{2^i k + 2^{i-1}}(\zeta_p).$$

Or, pour tout $i \in [\![1, n]\!]$, on a

$$1 \leq 2^i(2^{n-i} - 1) + 2^{i-1} = 2^n - 2^{i-1} = p - 1 - 2^{i-1} \leq p - 2.$$

Par unicité de l'écriture dans la base $\big(\zeta_p, \rho(\zeta_p), \ldots, \rho^{p-2}(\zeta_p)\big)$, on en déduit que $\rho^{2^{i-1}}(\alpha_i) \neq \alpha_i$, d'où $\alpha_i \notin L_{i-1}$.

On a ainsi $[L_i : L_{i-1}] \geq 2$ pour tout $i \in [\![1, n]\!]$. D'autre part, on a

$$[L_1 : L_0] \cdots [L_n : L_{n-1}] = [L_n : L_0] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \varphi(p) = p - 1 = 2^n,$$

Si un des degrés $[L_i : L_{i-1}]$ était $> 2$, leur produit serait $> 2^n$. On a donc

$$[L_i : L_{i-1}] = 2, \qquad \text{pour tout } \ i \in [\![1, n]\!].$$

Comme $\alpha_i \in L_i \setminus L_{i-1}$, $(1, \alpha_i)$ est une famille $L_{i-1}$-libre de $L_i$, donc a fortiori une $L_{i-1}$-base de $L_i$. En particulier, $L_i = L_{i-1}(\alpha_i)$. Cela achève la démonstration. □

En mettant bout à bout tous les résultats précédents, on a donc obtenu le résultat suivant.

Théorème II.4.12 (Gauss). *Soit $n \geq 2$ un entier. Alors, le $n$-gone régulier est constructible si, et seulement si, $n$ est produit d'une puissance de 2 et de nombres de Fermat premiers deux à deux distincts.*

Les constructions du triangle équilatéral et du pentagone régulier sont classiques, et laissées au lecteur à titre d'exercice. Nous épargnerons au lecteur la construction du 257-gone régulier et du 65537-gone régulier, faute de place dans la marge.

En ce qui concerne l'heptadécagone régulier, on peut démontrer que la valeur exacte de $\cos(\frac{2\pi}{17})$ est

$$\frac{1}{16}\Bigg(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}} \\ +\sqrt{68+12\sqrt{17}-2(1-\sqrt{17})\sqrt{34-2\sqrt{17}}-16\sqrt{34+2\sqrt{17}}}\Bigg).$$

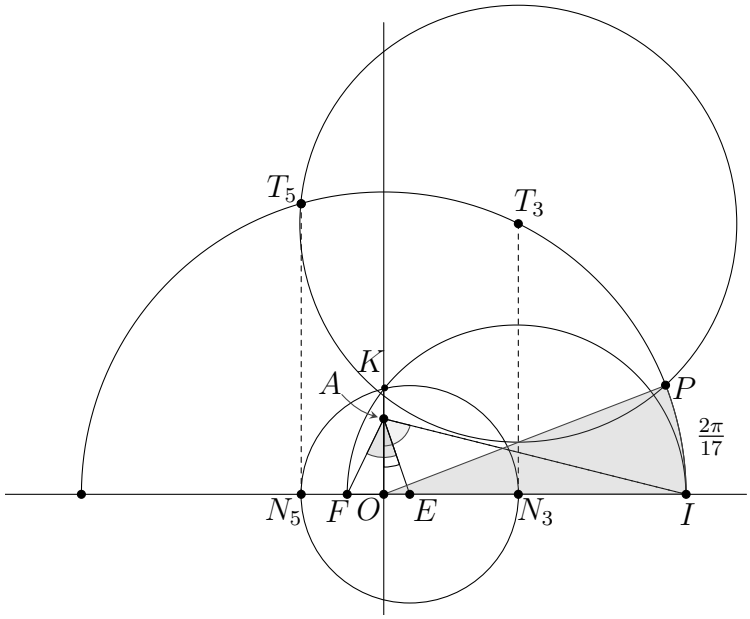
La construction suivante (que nous ne justifierons pas) permet de construire le point $P=(\cos(\frac{2\pi}{17}),\sin(\frac{2\pi}{17}))$ à la règle et au compas.

On construit le point $A=\left(0,\frac{1}{4}\right)$, puis, en utilisant deux bissections successives, on construit le point $E$ sur l'axe des abscisses tel que l'angle $\widehat{OAE}=\frac{1}{4}\widehat{OAI}$.

En construisant la perpendiculaire à $(AE)$ passant par $A$, puis à l'aide d'une bissection, on obtient l'unique point $F$ sur l'axe des abscisses tel que l'angle $\widehat{FAE}$ soit de mesure $\dfrac{\pi}{4}$.

Le demi-cercle supérieur de diamètre $IF$ coupe l'axe des ordonnées en un point $K$. On construit enfin le cercle de centre $E$ et de rayon $EK$. Celui-ci coupe la droite $(OI)$ en deux points $N_3$ et $N_5$, projections orthogonales respectives des points $T_3$ et $T_5$ du demi-cercle-unité supérieur, $N_3$ étant celui appartenant au segment $OI$.

Soit $C$ le milieu de $IF$. Le demi-cercle-unité supérieur et le cercle de centre $T_3$ et de rayon $T_3T_5$ se coupent en un point $P\neq T_5$ du cercle-unité, qui est le point recherché.




## II.5. Et après...

La démonstration du théorème de Gauss peut sembler un peu miraculeuse. En fait, elle ne l'est pas tant que ça.

Si $L$ est un corps et $G$ est un sous-groupe fini du groupe des automorphismes d'anneaux de $L$, nous démontrerons dans un chapitre ultérieur que l'extension $L/L^G$ est de degré fini et que

$$[L : L^G] = |G|.$$

En particulier, si $H$ est un sous-groupe de $G$, on a $L^G \subset L^H$, et

$$[L^H : L^G] = \frac{[L : L^G]}{[L : L^H]} = \frac{|G|}{|H|} = [G : H].$$

Supposons maintenant que $L/K$ soit une extension de degré fini. On vérifie alors que $\mathrm{Gal}(L/K)$ est fini. Si $\mathrm{Gal}(L/K)$ est un 2-groupe, il existe une suite de sous-groupes

$$G_r = \{\mathrm{Id}_L\} \triangleleft G_{r-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = \mathrm{Gal}(L/K),$$

où $[G_i : G_{i+1}] = 2$ pour tout $i \in [\![0, r-1]\!]$ (on reviendra sur ce point dans un chapitre ultérieur) En posant $L_i = L^{G_i}$, on obtient une tour d'extensions

$$K \subset L_0 \subset \cdots \subset L_{r-1} \subset L_r = L,$$

où $[L_{i+1} : L_i] = [G_i : G_{i+1}] = 2$.

Cela explique de manière un peu plus conceptuelle le point (2) de la proposition II.4.11, puisque si $p$ est un nombre de Fermat premier, le groupe de Galois $\mathrm{Gal}\big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\big)$ est cyclique d'ordre $p-1$, donc un 2-groupe fini.

L'autre point crucial faisant fonctionner la démonstration est le point (1) de cette même proposition, à savoir

$$\mathbb{Q}(\zeta_p)^{\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})} = \mathbb{Q}.$$

On peut donc se poser légitimement la question suivante : soit $L/K$ une extension de degré fini. A-t-on $L^{\mathrm{Gal}(L/K)} = K$?

La réponse est négative, comme le montrent les exemples suivants.

Exemples II.5.1. (1) Soit $K = \mathbb{Q}$, soit $\alpha = \sqrt[3]{2}$, et soit $L = \mathbb{Q}(\alpha)$.

Si $\sigma \in \mathrm{Gal}(L/K)$, on a

$$\sigma(\alpha)^3 = \sigma(\alpha^3) = \sigma(2) = 2.$$

Comme $L \subset \mathbb{R}$, $\sigma(\alpha)$ est une racine réelle du polynôme $\mu_{\alpha,K} = X^3 - 2$. On a donc $\sigma(\alpha) = \alpha$. Comme $(1, \alpha, \alpha^2)$ est une $K$-base de $L$, on en déduit que $\sigma = \mathrm{Id}_L$. Par conséquent, $\mathrm{Gal}(L/K) = \{\mathrm{Id}_L\}$, et ainsi

$$L^{\mathrm{Gal}(L/K)} = L \neq K.$$

(2) Soit $K = \mathbb{F}_2(T^2)$. Le polynôme $f = X^2 - T^2 \in K[X]$ est irréductible, puisque $T \notin \mathbb{F}_2(T^2)$, comme le lecteur le vérifiera à titre d'exercice. Soit $\alpha = T$, et $L = K(\alpha)$. On a alors

$$\mu_{\alpha,K} = X^2 - T^2 = (X - T)^2,$$

puisque $K$ est de caractéristique 2. Un raisonnement similaire au précédent montre alors que $\mathrm{Gal}(L/K) = \{\mathrm{Id}_L\}$, et donc que

$$L^{\mathrm{Gal}(L/K)} = L \neq K.$$

Remarque II.5.2. On peut aussi construire un exemple d'extension $L/\mathbb{Q}$ de degré 4 telle que $L^{\mathrm{Gal}(L/\mathbb{Q})} \neq \mathbb{Q}$.

Analysons un peu les deux contre-exemples précédents. Dans chacun des cas, le polynôme minimal de $\alpha$ sur $K$ n'a pas assez de racines dans $L$, et cela pour deux raisons distinctes. Dans le premier cas, $\mu_{\alpha,K}$ a toutes ses racines distinctes (dans $\mathbb{C}$), mais une seule appartient à $L$. Dans le second cas, c'est parce que le polynôme minimal de $\alpha$ sur $K$ possède une racine multiple.

Les extensions $L/K$ de degré fini vérifiant $L^{\mathrm{Gal}(L/K)} = K$ jouissent en fait de propriétés particulières : ce sont les extensions dites *galoisiennes*.

Elles seront définies et étudiées dans un chapitre ultérieur. Pour l'instant, disons simplement que ce sont exactement les extensions pour lesquelles les deux phénomènes précédents ne peuvent se produire.

Ces exemples montrent également que tous les sous-corps d'une extension de corps $L/K$ ne sont pas forcément de la forme $L^H$, où $H$ est un sous-groupe de $\mathrm{Gal}(L/K)$. Nous verrons néanmoins que c'est le cas lorsque $L/K$ est galoisienne.

Chapitre III

# Plongements et extensions séparables

Dans tout ce qui suit, on se fixe un corps de base $K$, et une clôture algébrique $\overline{K}/K$ de $K$. Toutes les extensions algébriques considérées (en particulier les extensions de degré fini) seront alors des sous-extensions de $\overline{K}/K$.

## III.1. Plongements

Un des buts principaux de ce chapitre est de comprendre un peu mieux le groupe $\mathrm{Gal}(L/K)$ lorsque $L/K$ est une extension de degré fini. En particulier, on aimerait étudier son ordre. Lorsque $L = K(\alpha)$, la réponse est donnée par le théorème I.3.1 (appliqué à $\iota = \mathrm{Id}_K$) : l'ordre de $\mathrm{Gal}(L/K)$ est le nombre de racines de $\mu_{\alpha,K}$ dans $L$.

Lorsque $L$ est engendrée par plus d'un générateur, la réponse paraît moins immédiate. Par exemple, supposons que $L = K(\alpha_1, \alpha_2)$. Comme on a la tour d'extensions

$$K \subset K(\alpha_1) \subset K(\alpha_1)(\alpha_2) = L,$$

il est tentant d'essayer de se ramener au cas précédent. Hélas, ce n'est pas si simple : si $\sigma \in \mathrm{Gal}(L/K)$, on obtient par restriction un morphisme de $K$-algèbres $\sigma' : K(\alpha_1) \longrightarrow L$, mais qui n'est a priori pas un automorphisme, car il n'y aucune raison pour que son image soit incluse dans $K(\alpha_1)$. En revanche, $\sigma'$ peut être vu comme un morphisme d'extensions $K(\alpha_1) \longrightarrow \overline{K}$.

Inversement, un tel morphisme s'étend en un morphisme $L \longrightarrow \overline{K}$ par le théorème I.3.1. Ainsi, les bons objets à étudier, à la fois d'un point de vue théorique et d'un point de vue calculatoire, sont les morphismes d'extensions $L \longrightarrow \overline{K}$. Remarquons qu'en particulier l'ensemble de ces morphismes contient $\mathrm{Gal}(L/K)$ (puisque $L$ est un sous-corps de $\overline{K}$).

Dans ce chapitre, nous allons nous intéresser à l'ensemble des morphismes de $K$-algèbres $L \longrightarrow \overline{K}$.

Commençons par définir une des notions principales de ce paragraphe.

Définition III.1.1. Soit $L/K$ une extension de corps algébrique. Un *plongement* de $L/K$ est un morphisme d'extensions $\sigma : L \longrightarrow \overline{K}$. L'ensemble des plongements de $L/K$ est noté $\mathscr{X}(L/K)$.

Le lemme suivant, bien que de démonstration fort simple, est très important pour la suite. Comme nous en aurons besoin en toute généralité, commençons par introduire la notion de monoïde et de morphismes de monoïdes.

Définition III.1.2. Un *monoïde* est un ensemble $M$ non vide muni d'une loi interne $*$ associative et possédant un élément neutre $1_M$ (nécessairement unique).

Un *morphisme de monoïdes* est une application $f : (M, *) \longrightarrow (M', \perp)$ entre deux monoïdes vérifiant :

(i) pour tous $x$, $y \in M$, $f(x * y) = f(x) \perp f(y)$ ;
(ii) $f(1_M) = 1_{M'}$.

Exemples III.1.3.

(1) Tout groupe est en particulier un monoïde, et tout morphisme de groupes $f : G \longrightarrow G'$ est un morphisme de monoïdes [1].
(2) Si $A$ est un anneau, $(A, \cdot)$ est un monoïde qui n'est pas un groupe (sauf si $A$ est trivial), et tout morphisme d'anneaux $f : A \longrightarrow B$ est un morphisme de monoïdes $(A, \cdot) \longrightarrow (B, \cdot)$.
(3) Les couples $(\mathbb{N}, +)$ et $(\mathbb{N}, \cdot)$ sont des monoïdes.

On peut maintenant énoncer le lemme d'indépendance de Dedekind.

Lemme III.1.4 (d'indépendance de Dedekind). *Soit $(M, *)$ un monoïde et soit $E$ un corps.*

*Alors, toute famille de morphismes de monoïdes $(M, *) \longrightarrow (E, \cdot)$ deux à deux distincts est $E$-libre dans le $E$-espace vectoriel $\mathscr{F}(M, E)$.*

*Démonstration.* Il suffit bien entendu de se réduire aux familles finies.

Montrons par récurrence que pour tout entier $n \geq 1$, $n$ morphismes de monoïdes $(M, *) \longrightarrow (E, \cdot)$ deux à deux distincts sont linéairement indépendants sur $E$.

Si $n = 1$, c'est clair puisqu'un morphisme $(M, *) \longrightarrow (E, \cdot)$ est non nul (il envoie $1_M$ sur $1_E \neq 0_E$).

1. Puisque $f(1_G) = 1_{G'}$.

Soit $n \geq 1$, et supposons la propriété soit vraie pour $n$ morphismes de monoïdes. Soient $\varphi_1, \ldots, \varphi_{n+1} : (M, *) \longrightarrow (E, \cdot)$, $n+1$ morphismes de monoïdes, deux à deux distincts, et soient $\lambda_1, \ldots, \lambda_{n+1} \in E$ tels que

$$\lambda_1\varphi_1 + \cdots + \lambda_{n+1}\varphi_{n+1} = 0.$$

Fixons $x \in M$. On a alors

$$\lambda_1\varphi_1(x * y) + \cdots + \lambda_{n+1}\varphi_{n+1}(x * y) = 0, \quad \text{pour tout } y \in M,$$

soit encore

$$\lambda_1\varphi_1(x)\varphi_1(y) + \cdots + \lambda_{n+1}\varphi_{n+1}(x)\varphi_{n+1}(y) = 0, \quad \text{pour tout } y \in M.$$

Mais on a aussi

$$\lambda_1\varphi_1(y) + \cdots + \lambda_{n+1}\varphi_{n+1}(y) = 0, \quad \text{pour tout } y \in M.$$

En multipliant cette dernière équation par $\varphi_{n+1}(x)$ et en soustrayant à la précédente, on obtient

$$\lambda_1\big(\varphi_1(x) - \varphi_{n+1}(x)\big)\varphi_1(y) + \cdots + \lambda_n\big(\varphi_n(x) - \varphi_{n+1}(x)\big)\varphi_n(y) = 0,$$

pour tout $y \in M$. Autrement dit,

$$\lambda_1\big(\varphi_1(x) - \varphi_{n+1}(x)\big)\varphi_1 + \cdots + \lambda_n\big(\varphi_n(x) - \varphi_{n+1}(x)\big)\varphi_n = 0.$$

Par hypothèse de récurrence, on a alors

$$\lambda_i\big(\varphi_i(x) - \varphi_{n+1}(x)\big) = 0, \quad \text{pour tout } i \in [\![1, n]\!].$$

Cela étant vrai pour tout $x \in M$, cela se récrit

$$\lambda_i(\varphi_i - \varphi_{n+1}) = 0, \quad \text{pour tout } i \in [\![1, n]\!].$$

Les morphismes $\varphi_1, \ldots, \varphi_{n+1}$ étant deux à deux distincts, on obtient

$$\lambda_i = 0, \quad \text{pour tout } i \in [\![1, n]\!].$$

Par conséquent, $\lambda_{n+1}\varphi_{n+1} = 0$, d'où également $\lambda_{n+1} = 0$ comme on l'a déjà vu précédemment.

Cela achève la récurrence, ainsi que la démonstration. □

Corollaire III.1.5. *Soient $L$ et $M$ deux corps.*

*Alors, toute famille de morphismes d'anneaux $L \longrightarrow M$ deux à deux distincts est $M$-libre dans le $M$-espace vectoriel $\mathscr{F}(L, M)$.*

*En particulier, pour toute extension $L/K$, les éléments de $\mathscr{X}(L/K)$ (resp. les éléments de $\mathrm{Gal}(L/K)$) forment une famille $\overline{K}$-libre de $\mathscr{F}(L, \overline{K})$ (resp. une famille $L$-libre de $\mathscr{F}(L, L)$).*

*Démonstration.* Il suffit de remarquer qu'une famille de morphismes d'anneaux $L \longrightarrow M$ deux à deux distincts induit une famille de morphismes de monoïdes $(L, \cdot) \longrightarrow (M, \cdot)$ deux à deux distincts, et d'appliquer le lemme précédent. □

On va maintenant étudier de plus près les plongements d'une extension monogène.

Lemme III.1.6. *Soit $\alpha \in \overline{K}$, et soit $L = K(\alpha)$.*

*Alors, tout morphisme d'anneaux $\iota : K \longrightarrow \overline{K}$ possède au plus $[L : K]$ prolongements $\sigma : L \longrightarrow \overline{K}$ à $L$. En particulier, on a*

$$|\mathscr{X}(L/K)| \leq [L : K].$$

*De plus, les propriétés suivantes sont équivalentes :*

(1) *tout morphisme d'anneaux $\iota : K \longrightarrow \overline{K}$ admet exactement $[L : K]$ prolongements à $L$ ;*
(2) *on a l'égalité $|\mathscr{X}(L/K)| = [L : K]$ ;*
(3) *le polynôme $\mu_{\alpha,K}$ ne possède que des racines simples dans $\overline{K}$.*

*Démonstration.* Gardons les notations de l'énoncé.

Par le théorème I.3.1, $\iota$ possède autant de prolongements à $L$ que le polynôme $\iota(\mu_{\alpha,K})$ possède de racines distinctes dans $\overline{K}$. En particulier, il y a au plus $\deg\big(\iota(\mu_{\alpha,K})\big)$ prolongements. Or, on a

$$\deg\big(\iota(\mu_{\alpha,K})\big) = \deg(\mu_{\alpha,K}) = [L : K],$$

d'où la première partie.

Un plongement de $L/K$ n'étant rien d'autre qu'un prolongement de l'inclusion $K \subset \overline{K}$, on en déduit que $|\mathscr{X}(L/K)|$ est le nombre de racines distinctes de $\mu_{\alpha,K}$ dans $\overline{K}$. On obtient alors l'inégalité

$$|\mathscr{X}(L/K)| \leq [L : K],$$

ainsi que la chaîne d'implications « $(1) \Longrightarrow (2) \Longrightarrow (3)$ ».

Il reste à démontrer « $(3) \Longrightarrow (1)$ ». Soit $\iota : K \longrightarrow \overline{K}$, et soit $E/K$ la sous-extension de $\overline{K}$ engendrée par les racines de $f = \mu_{\alpha,K}$ dans $\overline{K}$. Cette extension étant algébrique (puisqu'elle est engendrée par des éléments algébriques), $\iota$ se prolonge en un morphisme $\tau : E \longrightarrow \overline{K}$ d'après la proposition I.3.8 (on peut aussi appliquer plusieurs fois le théorème des prolongements des isomorphismes). On a alors $\iota(f) = \tau(f)$. Ainsi, si $f = \prod_{i=1}^{n}(X - \alpha_i) \in E[X] \subset \overline{K}[X]$, on a $\iota(f) = \prod_{i=1}^{n}(X -$

$\tau(\alpha_i)) \in \overline{K}[X]$. Comme $\tau$ est injectif, on en déduit que $f \in K[X]$ n'a que des racines simples dans $\overline{K}$ si, et seulement si, $\iota(f) \in \overline{K}[X]$ ne possède que des racines simples dans $\overline{K}$.

Supposons maintenant que $\mu_{\alpha,K} \in K[X]$ ne possède que des racines simples dans $\overline{K}$, et soit $\iota : K \longrightarrow \overline{K}$ un morphisme d'anneaux. D'après ce qui précède, $\iota(\mu_{\alpha,K})$ ne possède que des racines simples dans $\overline{K}$. Les considérations faites en début de démonstration montrent alors que $\iota$ possède $[L : K]$ prolongements à $L$, ce qui achève la démonstration. $\square$

Ce résultat nous conduit naturellement à la définition suivante.

Définition III.1.7. On dit qu'un polynôme $P \in K[X]$ non constant est *séparable sur* $K$ si $P$ n'a que des racines simples dans $\overline{K}$. On dit que $\alpha \in \overline{K}$ est *séparable sur* $K$ si $\mu_{\alpha,K}$ est séparable sur $K$. On dit qu'une extension $L/K$ est *séparable* si $L/K$ est algébrique, et si tout élément de $L$ est séparable sur $K$.

Remarque III.1.8. Soit $P \in K[X]$ un polynôme non constant. Alors, les propriétés suivantes sont équivalentes :

(1) le polynôme $P$ est séparable ;
(2) il existe une extension $L/K$ dans laquelle $P$ est scindé à racines simples ;
(3) pour toute extension $L/K$ dans laquelle $P$ est scindé, $P$ est à racines simples.

Les implications « (1) $\Longrightarrow$ (2) » et « (3) $\Longrightarrow$ (1) » sont évidentes. Supposons maintenant qu'il existe une extension $L/K$ dans laquelle $P$ est scindé à racines simples, et soit $L'/K$ une extension dans laquelle $P$ est scindé. Alors, $L/K$ et $L'/K$ contiennent des corps des racines $E/K$ et $E'/K$ de $P$. De plus, $P$ est scindé à racines simples dans $E$. Ces corps des racines sont isomorphes par la proposition I.3.4. Soit $\varphi : E \xrightarrow{\sim} E'$ un tel isomorphisme. On a alors

$$\varphi\big(P(\alpha)\big) = P\big(\varphi(\alpha)\big).$$

Comme $\varphi$ est bijective, on en déduit aisément que $\varphi$ induit une bijection entre l'ensemble des racines de $P$ dans $E$ et l'ensemble des racines de $P$ dans $E'$. En particulier, $P$ n'a que des racines simples dans $E'$, donc dans $L'$, d'où le résultat.

En particulier, la définition de séparabilité ne dépend pas de la clôture algébrique choisie.

Cela démontre également qu'un élément $\alpha \in L/K$ est séparable sur $K$ si, et seulement si, il existe une extension de $K$ (non nécessairement

algébrique) dans laquelle $\mu_{\alpha,K}$ est scindé à racines simples. Ce fait sera utilisé dans la suite sans référence ultérieure.

Exemples III.1.9. (1) Tout élément de $\alpha \in K$ est séparable sur $K$ puisque $\mu_{\alpha,K} = X - \alpha$.

(2) Le nombre complexe $i$ est séparable sur $\mathbb{Q}$, puisque
$$\mu_{i,\mathbb{Q}} = X^2 + 1 = (X - i)(X + i).$$

(3) Soit $K = \mathbb{F}_2(T^2)$ et $L = \mathbb{F}_2(T)$. Alors, $T$ n'est pas séparable sur $K$, puisque
$$\mu_{T,K} = X^2 - T^2 = (X - T)^2.$$

Remarque III.1.10. Soit $L/K$ une extension, et soit $M/K$ une sous-extension. Si $\alpha \in L$ est séparable sur $K$, il est séparable sur $M$.

En effet, si $\alpha \in L$ est algébrique, alors $\mu_{\alpha,K}$ est un polynôme unitaire annulant $\alpha$, que l'on peut voir à coefficients dans $M$. Ainsi, $\mu_{\alpha,M} \mid \mu_{\alpha,K}$. Par conséquent, si $\mu_{\alpha,K}$ n'a que des racines simples dans $\overline{K}$, il en est de même de $\mu_{\alpha,M}$. Ainsi, si $L/K$ est séparable, $L/M$ et $M/K$ sont séparables (le fait que $M/K$ soit séparable est clair).

On a alors le théorème suivant.

Théorème III.1.11. *Soit $L/K$ une extension de degré fini.*

*Alors, tout morphisme d'anneaux $\iota : K \longrightarrow \overline{K}$ admet au plus $[L : K]$ prolongements $\sigma : L \longrightarrow \overline{K}$ à $L$. En particulier, on a*
$$|\mathscr{X}(L/K)| \leq [L : K].$$
*De plus, les propriétés suivantes sont équivalentes :*

(1) *tout morphisme d'anneaux $\iota : K \longrightarrow \overline{K}$ admet exactement $[L : K]$ prolongements à $L$ ;*
(2) *on a l'égalité $|\mathscr{X}(L/K)| = [L : K]$ ;*
(3) *l'extension $L/K$ est séparable.*

*Démonstration.* Montrons le résultat par récurrence sur $[L : K]$. Plus précisément, pour tout $n \geq 1$, soit $(H_n)$ la propriété suivante :

$(H_n)$ Pour tout corps $K$, et toute extension $L/K$ de degré $\leq n$, l'énoncé du théorème est vrai.

Si $n = 1$, alors $L = K$ et toutes les propriétés de l'énoncé sont trivialement vraies. Soit $n \geq 1$ un entier, et supposons que la propriété $(H_n)$ soit vraie. Montrons que $(H_{n+1})$ est vraie. Soit $K$ un corps, et soit $L/K$ une extension de degré $\leq n + 1$. On peut toujours supposer que $[L : K] = n+1 \geq 2$, car sinon il suffit d'appliquer $(H_n)$. En particulier,

$L \neq K$. Soit $\alpha \in L \setminus K$. On a donc $K(\alpha) \neq K$, et par conséquent $[L : K(\alpha)] \leq n$.

Remarquons maintenant que tout prolongement de $\iota$ à $L$ s'obtient par extension d'un prolongement de $\iota$ à $K(\alpha)$. En effet, si $\sigma : L \longrightarrow \overline{K}$ est un prolongement de $\iota$ à $L$, alors $\sigma_{|_{K(\alpha)}}$ est un prolongement de $\iota$ à $K(\alpha)$. Inversement, tout prolongement de $\iota$ à $K(\alpha)$ possède au plus $[L : K(\alpha)]$ extensions à $L$ par hypothèse de récurrence, donc au moins une. De plus, il y a exactement $n_\alpha$ prolongements de $\iota$ à $K(\alpha)$ par le lemme III.1.6, où $n_\alpha$ est le nombre de racines de $\iota(\mu_{\alpha,K})$ dans $\overline{K}$. On en déduit que $\iota$ admet au plus $n_\alpha[L : K(\alpha)]$ extensions à $L$. Comme $n_\alpha \leq [K(\alpha) : K]$ et que $[K(\alpha) : K][L : K(\alpha)] = [L : K]$, cela démontre le premier point.

Notons que tout cela est valable pour un élément $\alpha \in L \setminus K$ arbitraire.

Montrons maintenant l'équivalence des trois propriétés $\big($toujours sous l'hypothèse $(H_n)\big)$.

(1) $\Longrightarrow$ (2). Il suffit d'appliquer la propriété (1) à l'inclusion $K \subset \overline{K}$.

(2) $\Longrightarrow$ (3). On procède par contraposition. Supposons que $L/K$ ne soit pas séparable. Il existe donc $\alpha \in L \setminus K$ non séparable[2]. Les considérations précédentes appliquées à l'inclusion $K \subset \overline{K}$ montrent alors que le nombre de plongements est $< [L : K(\alpha)][K(\alpha) : K] = [L : K]$, d'où l'implication voulue.

(3) $\Longrightarrow$ (1). Supposons que $L/K$ soit séparable, et soit $\iota : K \longrightarrow \overline{K}$ un morphisme d'anneaux. Comme $L \neq K$, on peut choisir un élément $\alpha \in L \setminus K$. Un tel élément est séparable par hypothèse. Ainsi, $\iota$ admet $[K(\alpha) : K]$ prolongements à $K(\alpha)$. De plus, l'extension $L/K(\alpha)$ est séparable d'après la remarque III.1.10. Par hypothèse de récurrence, n'importe quel prolongement de $\iota$ à $K(\alpha)$ admet lui-même $[L : K(\alpha)]$ prolongements. Mais alors, $\iota$ possède $[K(\alpha) : K][L : K(\alpha)] = [L : K]$ prolongements à $L$.

Cela achève la récurrence, ainsi que la démonstration. □

Corollaire III.1.12. *Soit $L/K$ une extension de degré fini. Alors, on a*

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

Remarque III.1.13. Soit $L/K$ une extension de degré fini. Alors, il existe des éléments $\alpha_1, \ldots, \alpha_n \in L$ tels que $L = K(\alpha_1, \ldots, \alpha_n)$. En effet, on peut par exemple prendre les éléments d'une $K$-base $L$. On

2. Les éléments de $K$ sont séparables sur $K$.

peut alors déterminer les éléments de $\mathscr{X}(L/K)$ de la manière suivante. Pour tout $i \in [\![0, n]\!]$, posons

$$L_i = K(\alpha_1, \ldots, \alpha_i),$$

si bien que $L_i = L_{i-1}(\alpha_i)$ pour tout $i \in [\![1, n]\!]$.

On trouve tous les prolongements de $K \subset \overline{K}$ à $L_1 = K(\alpha_1)$ en utilisant le théorème I.3.1, puis on étend chaque prolongement $L_1 \longrightarrow \overline{K}$ au corps $L_2 = L_1(\alpha_2)$ en utilisant ce même lemme, et ainsi de suite.

**Notation.** Soit $L/K$ une extension de degré fini. Écrivons

$$L = K(\alpha_1, \ldots, \alpha_n).$$

Comme on a l'égalité $L = K[\alpha_1, \ldots, \alpha_n]$ (cf. corollaire I.2.11), un plongement $\sigma : L \longrightarrow \overline{K}$ est déterminé de manière unique par les images de $\alpha_1, \ldots, \alpha_n$. Si $\beta_i \in \overline{K}$ est l'image de $\alpha_i$ par $\sigma$, on notera simplement le morphisme par

$$\sigma : \left| \begin{array}{ccc} \alpha_1 & \rightsquigarrow & \beta_1 \\ & \vdots & \\ \alpha_n & \rightsquigarrow & \beta_n \end{array} \right.$$

Exemple III.1.14. Soit $K = \mathbb{Q}$ et soit $L = \mathbb{Q}(\alpha, \beta)$, avec $\alpha = \sqrt[4]{2}$ et $\beta = \sqrt[5]{2}$. D'après le critère d'Eisenstein, on a

$$\mu_{\alpha,K} = X^4 - 2 = (X - \alpha)(X + \alpha)(X - i\alpha)(X + i\alpha).$$

D'après le théorème I.3.1, l'inclusion $K \subset \overline{K}$ possède quatre prolongements

$$\tau_k : \alpha \rightsquigarrow i^k \alpha, \quad k \in [\![0, 3]\!].$$

Passons à l'étape suivante. Pour cela, il faut calculer le polynôme minimal de $\beta$ sur $K(\alpha)$. D'après l'exemple II.3.8, $K(\alpha)/K$ et $K(\beta)/K$ sont linéairement disjointes, et l'on a $[L : K] = 20$. En particulier, on a

$$[L : K(\alpha)] = \frac{[L : K]}{[K(\alpha) : K]} = \frac{20}{4} = 5.$$

Or, $X^5 - 2$ est un polynôme de $K(\alpha)[X]$ unitaire annulant $\beta$ de degré 5. Comme $\mu_{\beta,K(\alpha)}$ est de degré 5 et divise $X^5 - 2$, on a nécessairement

$$\mu_{\beta,K(\alpha)} = X^5 - 2 = \prod_{m=0}^{m=4} (X - \beta\zeta_5^m).$$

Puisque $\tau_k(\mu_{\beta,K(\alpha)}) = X^5 - 2$, le théorème I.3.1 montre que $\tau_k$ admet cinq prolongements à $L$, à savoir

$$\sigma_{k,m} : \left| \begin{array}{ccc} \alpha & \rightsquigarrow & i^k\alpha \\ \beta & \rightsquigarrow & \zeta_5^m\beta \end{array} \right. , \quad k \in [\![0,3]\!] \,,\ m \in [\![0,4]\!] \,.$$

On a donc exactement vingt plongements de $L$ dans $\overline{K}$. En particulier, $L/K$ est séparable par le théorème III.1.11. Notons également que $L \subset \mathbb{R}$. On en déduit alors l'égalité

$$\mathrm{Gal}(L/K) = \{\sigma_{0,0}, \sigma_{2,0}\}.$$

Nous allons maintenant étudier de plus près les extensions séparables.

## III.2. Propriétés des extensions séparables

Proposition III.2.1. *Soit $L/K$ une extension. Alors, l'ensemble des éléments de $L$ séparables sur $K$ est une sous-extension de $L/K$.*

*Démonstration.* Soit $M$ l'ensemble des éléments de $L$ séparables sur $K$. Alors, $M$ contient $K$, donc contient a fortiori 0 et 1. Soient $\alpha$, $\beta \in M$, et soit $E = K(\alpha, \beta)$. L'extension de corps $E/K$ est de degré fini d'après le corollaire I.2.11. Nous allons montrer que $E/K$ est séparable. Cela démontrera en particulier que $-\alpha$, $\alpha + \beta$, $\alpha\beta$ et $\alpha^{-1}$ (lorsque $\alpha \neq 0$) sont séparables, puisque ce sont des éléments de $E$.

Pour cela, comptons le nombre de plongements de $E/K$. Puisque $\alpha$ est séparable sur $K$, l'inclusion $K \subset \overline{K}$ admet $[K(\alpha) : K]$ prolongements au corps $K(\alpha)$ d'après le lemme III.1.6. Puisque $\beta$ est séparable sur $K$, il est aussi séparable sur $K(\alpha)$ par la remarque III.1.10. Chaque plongement de $K(\alpha)$ admet alors $[E : K(\alpha)]$ prolongements à $E$, toujours d'après le lemme III.1.6. Ainsi, $E/K$ admet exactement

$$[K(\alpha) : K][E : K(\alpha)] = [E : K]$$

plongements. Par le théorème III.1.11, $E/K$ est séparable, d'où le résultat. □

On en déduit alors le résultat suivant.

Corollaire III.2.2. *Soit $L/K$ une extension, et soit $\mathscr{S}$ une partie de $L$. Alors, l'extension $K(\mathscr{S})/K$ est séparable si, et seulement si, tout élément de $\mathscr{S}$ est séparable sur $K$.*

*Démonstration.* Soit $M$ l'ensemble des éléments de $L$ qui sont séparables sur $K$. Supposons que tout élément de $\mathscr{S}$ soit séparable sur $K$. Alors, $\mathscr{S}$ est contenue dans $M$. Comme $M$ est un sous-corps de $L$ contenant

$K$ d'après la proposition précédente, on a $K(\mathscr{S}) \subset M$. Autrement dit, $K(\mathscr{S})/K$ est séparable. L'autre implication est immédiate. □

Corollaire III.2.3. *Soit $L/K$ une extension, et soient $E/K, E'/K$ deux sous-extensions de $L/K$. Si $E/K$ est séparable, alors $EE'/E'$ est séparable.*

*Démonstration.* Puisque tout élément de $E$ est séparable sur $K$, tout élément de $E$ est aussi séparable sur $E'$ par la remarque III.1.10. Ainsi, tout élément de $E$ est séparable sur $E'$. Par le corollaire précédent, tout élément de la sous-extension $M/E'$ de $L/E'$ engendrée par $E$ est séparable. Or, cette extension n'est rien d'autre que $EE'$, comme on l'a déjà constaté. Cela achève la démonstration. □

Corollaire III.2.4. *Soit $L/K$ une extension, et soient $E/K, E'/K$ deux sous-extensions de $L/K$. Si $E/K$ et $E'/K$ sont séparables, alors $EE'/K$ est séparable.*

*Démonstration.* Il suffit d'appliquer le corollaire III.2.2 à $\mathscr{S} = E \cup E'$. □

On a enfin le résultat suivant.

Proposition III.2.5. *Soit $K \subset M \subset L$ une tour d'extensions. Alors, $L/K$ est séparable si, et seulement si, $M/K$ et $L/M$ sont séparables.*

*Démonstration.* Le sens direct est donné par la remarque III.1.10. Supposons maintenant que $M/K$ et $L/M$ soient séparables. En particulier, les extensions $M/K$ et $L/K$ sont algébriques par la proposition I.2.19. Soit $\alpha \in L$. Par hypothèse, $\alpha$ est séparable sur $M$. Écrivons

$$\mu_{\alpha,M} = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in M[X],$$

et posons $E = K(a_0, \ldots, a_{n-1})$. Cette extension est de degré fini par le corollaire I.2.11. De même, $E(\alpha)/K$ est de degré fini. Nous allons montrer que cette extension est séparable.

Puisque $\mu_{\alpha,M} \in E[X]$ est irréductible dans $M[X]$, il est aussi irréductible dans $E[X]$, et l'on a donc $\mu_{\alpha,E} = \mu_{\alpha,M}$. Ainsi, $\alpha$ est séparable sur $E$. Puisque les éléments $a_0, \ldots, a_{n-1} \in M$ sont séparables sur $K$, $E/K$ est séparable sur $K$ d'après le corollaire III.2.2, et de degré fini. Le nombre de plongements de $E/K$ est donc égal à $[E : K]$ d'après le théorème III.1.11. Comme $\alpha$ est séparable sur $E$, chaque plongement de $E$ admet $[E(\alpha) : E]$ extensions à $E(\alpha)$ par le lemme III.1.6. Ainsi, $E(\alpha)/K$ admet $[E(\alpha) : K]$ plongements, et $E(\alpha)/K$ est donc séparable. En particulier, $\alpha$ est séparable sur $K$, ce qui achève la démonstration. □

Nous continuons maintenant en démontrant qu'une extension séparable de degré fini est monogène. On commence par un lemme.

LEMME III.2.6. *Soit $L/K$ une extension de corps séparable de degré $n \geq 1$, et soient $\sigma_1, \ldots, \sigma_n$ les $n$ plongements de $L/K$. Alors, pour tout $\alpha \in L$, on a $L = K(\alpha)$ si, et seulement si, les $n$ éléments $\sigma_1(\alpha), \ldots, \sigma_n(\alpha) \in \overline{K}$ sont distincts.*

*Démonstration.* Remarquons d'abord que la restriction de chaque plongement de $L/K$ à $K(\alpha)$ fournit un plongement de $K(\alpha)/K$. Ainsi, si les éléments $\sigma_1(\alpha), \ldots, \sigma_n(\alpha) \in \overline{K}$ sont tous distincts, $K(\alpha)/K$ possède au moins $n$ plongements distincts. D'après le lemme III.1.6 par exemple, on a donc $n \leq [K(\alpha) : K]$.

Puisque l'on a aussi $[K(\alpha) : K] \leq [L : K] = n$, on en déduit

$$[K(\alpha) : K] = n = [L : K].$$

Ainsi, $L = K(\alpha)$. Si maintenant $L = K(\alpha)$, puisque chaque plongement est uniquement déterminé par l'image de $\alpha$ (cf. théorème I.3.1) et que les plongements $\sigma_1, \ldots, \sigma_n$ sont deux à deux distincts par hypothèse, on en déduit que les $n$ éléments $\sigma_1(\alpha), \ldots, \sigma_n(\alpha) \in \overline{K}$ sont distincts, d'où le résultat souhaité. □

Énonçons à présent le théorème de l'élément primitif.

THÉORÈME III.2.7 (de l'élément primitif). *Soit $L/K$ une extension séparable de degré fini. Alors, il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

*Démonstration.* Si $K$ est fini, alors $L$ aussi, et $L^\times$ est cyclique. En particulier, $L = \mathbb{F}_p(\alpha)$, où $\alpha$ est un générateur de $K^\times$ et $p$ est la caractéristique de $L$ (donc aussi celle de $K$). Comme $\mathbb{F}_p \subset K \subset L$ et $\alpha \in L$, on a $\mathbb{F}_p(\alpha) \subset K(\alpha) \subset L = \mathbb{F}_p(\alpha)$, d'où $L = K(\alpha)$.

Supposons maintenant que $K$ soit infini. L'extension $L/K$ admet donc $n$ plongements $\sigma_1, \ldots, \sigma_n$ deux à deux distincts, où $n = [L : K]$. Puisque $L$ est un $K$-espace vectoriel de dimension finie $n$, il est engendré par un nombre fini d'éléments. On peut donc écrire

$$L = K(\alpha_1, \ldots, \alpha_m),$$

pour certains $\alpha_1, \ldots, \alpha_m \in L$. Si $m = 1$, il n'y a rien à faire. Si $m \geq 2$, une récurrence facile montre qu'il suffit de considérer le cas $m = 2$. Supposons donc que $L = K(\alpha_1, \alpha_2)$, et posons

$$P = \prod_{1 \leq i < j \leq n} \Big( \sigma_i(\alpha_1) - \sigma_j(\alpha_1) + \big(\sigma_i(\alpha_2) - \sigma_j(\alpha_2)\big) X \Big) \in \overline{K}[X].$$

Montrons que l'on a $P \neq 0$. Si $P = 0$, cela signifie qu'un des facteurs de degré 1 est nul, et donc qu'il existe $1 \leq i < j \leq n$ tels que

$$\sigma_i(\alpha_1) = \sigma_j(\alpha_1) \quad \text{et} \quad \sigma_i(\alpha_2) = \sigma_j(\alpha_2).$$

Mais, comme $\alpha_1$ et $\alpha_2$ engendrent $L$ comme anneau, on en déduit $\sigma_i = \sigma_j$, d'où une contradiction.

Ainsi, $P \neq 0$, et puisque $K$ est infini, il existe $\lambda \in K$ tel que $P(\lambda) \neq 0$. Pour tout $1 \leq i < j \leq n$, on a donc $\sigma_i(\alpha_1) - \sigma_j(\alpha_1) + \big(\sigma_i(\alpha_2) - \sigma_j(\alpha_2)\big)\lambda \neq 0$, c'est-à-dire $\sigma_i(\alpha_1 + \lambda\alpha_2) \neq \sigma_j(\alpha_1 + \lambda\alpha_2)$.

Posons $\alpha = \alpha_1 + \lambda\alpha_2$. Les $n$ éléments $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ sont distincts par construction, et donc $L = K(\alpha)$, d'après le lemme III.2.6. □

Définition III.2.8. Soit $L/K$ une extension de corps. Un élément $\alpha \in L$ est dit *primitif* si $L = K(\alpha)$.

Remarques III.2.9.

(1) La réciproque de ce théorème est bien entendu fausse, comme le montre déjà l'exemple III.1.9 (3).

(2) Un examen attentif de la démonstration montre que l'on a le résultat plus précis suivant : soit $L/K$ une extension séparable de degré fini, et soient $\alpha_1, \ldots, \alpha_m \in L$ tels que $L = K(\alpha_1, \ldots, \alpha_m)$. Si $K$ est infini, il existe un élément primitif $\alpha \in L$ de la forme

$$\alpha = \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n, \quad \lambda_i \in K.$$

Exemple III.2.10. Soit $K = \mathbb{Q}$ et soit $L = \mathbb{Q}(\alpha, \beta)$, avec $\alpha = \sqrt[4]{2}$ et $\beta = \sqrt[5]{2}$. D'après l'exemple III.1.14, on sait que $L/K$ est séparable, et que les plongements sont donnés par

$$\sigma_{k,m} : \left| \begin{array}{ccc} \alpha & \rightsquigarrow & i^k\alpha \\ \beta & \rightsquigarrow & \zeta_5^m\beta \end{array} \right. , \quad k \in [\![0,3]\!]\,,\ m \in [\![0,4]\!]\,.$$

On vérifie alors, en utilisant le lemme III.2.6, que $L = K(\alpha + \beta)$.

On finit ce paragraphe en faisant le lien entre plongements et polynômes minimaux.

Lemme III.2.11. *Soit $L/K$ une extension séparable de degré fini. Alors, pour tout $\alpha \in L$, on a*

$$\prod_{\sigma \in \mathscr{X}(L/K)} \big(X - \sigma(\alpha)\big) = \mu_{\alpha,K}^{[L:K(\alpha)]}.$$

*En particulier, si $\alpha \in L$ est un élément primitif, on a*

$$\prod_{\sigma \in \mathscr{X}(L/K)} \big(X - \sigma(\alpha)\big) = \mu_{\alpha,K}.$$

*Démonstration.* Posons $M = K(\alpha)$, et soit $n = [M : K]$. Par hypothèse, $\alpha$ est séparable sur $K$. Soient $\alpha_1, \ldots, \alpha_n \in \overline{K}$ les racines de $\mu_{\alpha,K}$ dans $\overline{K}$.

On peut donc écrire

$$\mu_{\alpha,K} = \prod_{i=1}^{n} (X - \alpha_i) \in \overline{K}[X].$$

Le théorème I.3.1 montre alors que les plongements sont les morphismes

$$\sigma_i : \alpha \rightsquigarrow \alpha_i, \quad i \in [\![1, n]\!].$$

Comme $L/K$ est séparable, $L/M$ est séparable (cf. remarque III.1.10) et chaque $\sigma_i$ admet exactement $[L : M]$ prolongements à $L$.

Autrement dit, pour un $i \in [\![1, n]\!]$ fixé, il y a exactement $[L : M]$ plongements dont la restriction à $M$ est $\sigma_i$. Pour un tel plongement $\sigma$, on a alors

$$\sigma(\alpha) = \sigma_i(\alpha) = \alpha_i,$$

puisque $\alpha \in M$. Ainsi, on obtient

$$\prod_{\sigma \in \mathscr{X}(L/K)} \big(X - \sigma(\alpha)\big) = \Big(\prod_{i=1}^{n} (X - \alpha_i)\Big)^{[L:K(\alpha)]} = \mu_{\alpha,K}^{[L:K(\alpha)]},$$

d'où le résultat. □

Corollaire III.2.12. *Soit $L/K$ une extension séparable de degré fini. Alors, pour tout $\alpha \in L$, on a*

$$\sigma(\alpha) = \alpha, \quad \textit{pour tout } \sigma \in \mathscr{X}(L/K) \qquad \Longleftrightarrow \qquad \alpha \in K.$$

*Démonstration.* Si $\alpha \in L$ est fixé par tout élément de $\mathscr{X}(L/K)$, le lemme précédent montre que

$$\mu_{\alpha,K}^{[L:K(\alpha)]} = (X - \alpha)^{[L:K]}.$$

En particulier, $\mu_{\alpha,K}$ admet une unique racine dans $\overline{K}$, à savoir $\alpha$. Comme le polynôme $\mu_{\alpha,K}$ est séparable, on en déduit que

$$\mu_{\alpha,K} = X - \alpha \in \overline{K}[X],$$

et puisque $\mu_{\alpha,K}$ est à coefficients dans $K$, on obtient $\alpha \in K$. Le sens indirect est clair, puisqu'un plongement est $K$-linéaire et envoie 1 sur 1. Cela achève la démonstration. □

Remarque III.2.13. Soit $L/K$ une extension de degré fini (pas nécessairement séparable), et soit $\alpha \in L$ un élément séparable. Le lemme III.2.11 montre en particulier que l'on a

$$\prod_{\tau \in \mathscr{X}(K(\alpha)/K)} \big(X - \tau(\alpha)\big) = \mu_{\alpha,K}.$$

On peut alors en déduire une méthode pour calculer le polynôme minimal de $\alpha$, dès lors que l'on connaît tous les plongements de $L$ dans $\overline{K}$.

On calcule les éléments $\sigma(\alpha), \sigma \in \mathscr{X}(L/K)$, et l'on choisit une famille

$$\sigma_1(\alpha), \ldots, \sigma_r(\alpha)$$

d'éléments deux à deux distincts de cardinal maximal. Alors, on a

$$\mu_{\alpha,K} = \prod_{i=1}^{r} \big(X - \sigma_i(\alpha)\big).$$

En effet, les éléments $\tau(\alpha), \tau \in \mathscr{X}(K(\alpha)/K)$, sont tous de la forme $\sigma(\alpha)$, avec $\sigma \in \mathscr{X}(L/K)$, puisque chaque plongement de $K(\alpha)$ se prolonge[3] à $L$. La maximalité de $r$ assure alors l'égalité

$$\{\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\} = \{\tau(\alpha) \mid \tau \in \mathscr{X}\big(K(\alpha)/K\big)\},$$

d'où le résultat.

Exemple III.2.14. Soit $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. On a

$$\mu_{\sqrt{2},\mathbb{Q}} = X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2}),$$

et l'inclusion $\mathbb{Q} \subset \overline{\mathbb{Q}}$ se prolonge en deux plongements, à savoir

$$\tau_m : \sqrt{2} \rightsquigarrow (-1)^k \sqrt{2}, \quad k = 0, 1.$$

Montrons que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Supposons que $\sqrt{3} = a + b\sqrt{2},\ a,\, b \in \mathbb{Q}$. En élevant au carré, on obtient

$$3 = a^2 + 2b^2 + 2ab\sqrt{2}.$$

On en déduit $b = 0$, puis $3 = a^2$, i.e. $\sqrt{3} \in \mathbb{Q}$, d'où une contradiction. Mais alors, $X^2 - 3 \in \mathbb{Q}[X] \subset \mathbb{Q}(\sqrt{2})[X]$ est unitaire, irréductible, et annule $\sqrt{3}$. On a donc $\mu_{\sqrt{3},\mathbb{Q}(\sqrt{2})} = X^2 - 3$. Comme $\tau_k(X^2 - 3) = X^2 - 3$ pour $k = 0, 1$, les plongements de $M$ dans $\overline{\mathbb{Q}}$ sont

$$\sigma_{k,m} : \left| \begin{array}{ccc} \sqrt{2} & \rightsquigarrow & (-1)^k\sqrt{2} \\ \sqrt{3} & \rightsquigarrow & (-1)^m\sqrt{3} \end{array} \right. , \qquad \text{pour tous } k,\, m \in \{0, 1\}.$$

3. On peut remarquer que $L/K(\alpha)$ est de degré fini, et procéder comme dans la remarque III.1.13 pour prolonger $\tau$, ou utiliser la proposition I.3.8.

Soit $\alpha = \sqrt{2} + \sqrt{3}$. Les images de $\alpha$ par les divers plongements sont distinctes, et valent

$$\sqrt{2} + \sqrt{3}, \quad \sqrt{2} - \sqrt{3}, \quad -\sqrt{2} + \sqrt{3}, \quad -\sqrt{2} - \sqrt{3}.$$

On a alors

$$\mu_{\alpha,\mathbb{Q}} = (X - \sqrt{2} - \sqrt{3})(X + \sqrt{2} - \sqrt{3})(X - \sqrt{2} + \sqrt{3})(X + \sqrt{2} + \sqrt{3}),$$

soit $\mu_{\alpha,\mathbb{Q}} = X^4 - 10X^2 + 1$. On en déduit a posteriori que ce polynôme est irréductible, ce que l'on peut montrer directement (mais ce n'est pas si immédiat).

## III.3. Polynômes séparables

Nous allons maintenant étudier à quelques conditions un polynôme de $K[X]$ est séparable, en mettant l'accent sur les polynômes irréductibles.

Commençons par un lemme.

Lemme III.3.1. *Soient $f$, $g \in K[X]$, et soit $\iota : K \longrightarrow L$ un morphisme d'anneaux. Alors, on a*

$$\operatorname{pgcd}\big(\iota(f), \iota(g)\big) = \iota\big(\operatorname{pgcd}(f, g)\big).$$

*Démonstration.* Si $P_1$, $P_2 \in K[X]$, avec $P_2 \neq 0$, soit $P_1 = P_2Q + R$ la division euclidienne de $P_1$ par $P_2$. On a donc $\deg(R) < \deg(P_2)$. Le morphisme d'anneaux $\iota$ étant injectif, pour tout $S \in K[X]$, les polynômes $S$ et $\iota(S)$ ont même degré. Comme on a

$$\iota(P_1) = \iota(P_2Q + R) = \iota(P_2)\iota(Q) + \iota(R),$$

cela montre que le polynôme $\iota(R) \in L[X]$ est le reste de la division euclidienne de $\iota(P)$ par $\iota(Q)$. De plus, $\iota(R)$ est nul si, et seulement si, $R$ l'est. En particulier, si $R_0$, $R_1, \ldots, R_n$ sont les restes non nuls obtenus dans l'algorithme d'Euclide associé à $f$ et $g$, $\iota(R_0)$, $\iota(R_1), \ldots, \iota(R_n)$ sont les restes non nuls obtenus dans l'algorithme d'Euclide associé à $\iota(f)$ et $\iota(g)$. Par conséquent, $\iota(R_n)$ est un pgcd de $\iota(f)$ et $\iota(g)$, ce qui démontre le résultat voulu en normalisant les pgcd. $\square$

On continue par une caractérisation de la séparabilité en termes de polynôme dérivé, bien connue dans le cas des polynômes à coefficients réels.

Lemme III.3.2. *Soit $K$ un corps, et soit $P \in K[X]$ un polynôme non constant. Alors, $P$ est séparable si, et seulement si, $P$ et $P'$ sont premiers entre eux.*

*Démonstration.* On peut supposer $P$ unitaire sans perte de généralité. Le lemme précédent, appliqué à l'inclusion $K \subset \overline{K}$, montre que les pgcd unitaires de $P$ et $P'$ calculés dans $K[X]$ et $\overline{K}[X]$, sont égaux. Quitte à remplacer $K$ par $\overline{K}$, on peut donc aussi supposer que $P$ est scindé sur $K$. Écrivons

$$P = \prod_{i=1}^{r} (X - \alpha_i)^{m_i}, \quad \alpha_i \in K,\ m_i \geq 1,\ r \geq 1.$$

On a alors

$$P' = \sum_{i=1}^{r} m_i (X - \alpha_i)^{m_i - 1} \prod_{j \neq i} (X - \alpha_j)^{m_j}.$$

Un diviseur irréductible unitaire éventuel de $\operatorname{pgcd}(P, P')$ est un diviseur irréductible unitaire de $P$. C'est donc un des polynômes $X - \alpha_k,\ k \in [\![1, r]\!]$.

Soit $k \in [\![1, r]\!]$. Remarquons que pour tout $i \neq k$, on a

$$X - \alpha_k \mid \prod_{j \neq i} (X - \alpha_j)^{m_j}.$$

Ainsi, on a

$$\begin{aligned} X - \alpha_k \mid P' \quad &\Longleftrightarrow \quad X - \alpha_k \mid m_k (X - \alpha_k)^{m_k - 1} \prod_{j \neq k} (X - \alpha_j)^{m_j} \\ &\Longleftrightarrow \quad X - \alpha_k \mid m_k (X - \alpha_k)^{m_k - 1}, \end{aligned}$$

la dernière équivalence provenant du lemme de Gauss.

Si $P$ est séparable, on a $m_k = 1$ pour tout $k \in [\![1, r]\!]$, et cette dernière condition de divisibilité n'a jamais lieu. Ainsi, $P$ et $P'$ sont premiers entre eux dans ce cas.

Si $P$ n'est pas séparable, il existe $k \in [\![1, r]\!]$ tel que $m_k > 1$. La condition précédente montre alors que $X - \alpha_k \mid P'$. Dans ce cas, $P$ et $P'$ ne sont pas premiers entre eux, d'où le résultat. □

Remarque III.3.3. Soit $\iota : K \longrightarrow L$ un morphisme d'anneaux. Les deux résultats précédents permettent de démontrer que $P \in K[X]$ est séparable si, et seulement si, $\iota(P) \in L[X]$ est séparable, de manière directe.

En effet, en remarquant que $\iota(P') = \iota(P)'$, on obtient alors

$$\begin{aligned} \operatorname{pgcd}(P, P') = 1 \quad &\Longleftrightarrow \quad \iota\big(\operatorname{pgcd}(P, P')\big) = \iota(1) \\ &\Longleftrightarrow \quad \iota\big(\operatorname{pgcd}(P, P')\big) = 1 \\ &\Longleftrightarrow \quad \operatorname{pgcd}\big(\iota(P), \iota(P')\big) = 1 \\ &\Longleftrightarrow \quad \operatorname{pgcd}\big(\iota(P), \iota(P)'\big) = 1, \end{aligned}$$

d'où le résultat.

Corollaire III.3.4. *Soit $K$ un corps, et soit $P \in K[X]$ un polynôme irréductible. Alors, $P$ n'est pas séparable si, et seulement si, $P' = 0$.*

*Démonstration.* On peut toujours supposer $P$ unitaire. Puisque $P$ est irréductible, les diviseurs unitaires de $P$ sont 1 ou $P$. On a donc

$$\operatorname{pgcd}(P, P') = 1 \quad \text{ou} \quad P.$$

D'après le lemme précédent, on a

$$P \text{ n'est pas séparable} \iff \operatorname{pgcd}(P, P') = P \iff P \mid P'.$$

Mais, $\deg(P') < \deg(P)$. La condition $P \mid P'$ est alors réalisée si, et seulement si, $P' = 0$. Cela achève la démonstration. □

On peut maintenant décortiquer la structure des polynômes irréductibles séparables.

Lemme III.3.5. *Soit $K$ un corps.*

(1) *Si $\operatorname{car}(K) = 0$, tout polynôme irréductible de $K[X]$ est séparable.*
(2) *Si $\operatorname{car}(K) = p > 0$, et si $P \in K[X]$ est irréductible, alors $P$ n'est pas séparable si, et seulement si, il existe $Q \in K[X]$ tel que $P = Q(X^p)$.*

*Démonstration.* Soit $P \in K[X]$ un polynôme irréductible de degré $n \geq 1$. Si $P = a_n X^n + \cdots + a_1 X + a_0$, avec $a_n \in K^\times$, on a

$$P' = n a_n X^{n-1} + \cdots + 2a_2 X + a_1.$$

Ainsi, on a

$$P' = 0 \iff k a_k = 0, \quad \text{pour tout } k \in [\![1, n]\!].$$

Si $\operatorname{car}(K) = 0$, on a $n a_n \neq 0$ et $P' \neq 0$. Par conséquent, $P$ est séparable par le corollaire III.3.4.

Supposons que $\operatorname{car}(K) = p > 0$. Si $p \mid k$, alors $k = pm, m \in \mathbb{Z}$ et l'on a

$$k a_k = p(m a_k) = 0,$$

car $K$ est de caractéristique $p$. Si $p \nmid k$, alors $k{\cdot}1$ est inversible dans $K$ (puisque le sous-anneau engendré par 1 est isomorphe à $\mathbb{Z}/p\mathbb{Z}$), et dans ce cas, on a[4]

$$k a_k = 0 \iff a_k = 0.$$

Ainsi, $P' = 0$ si, et seulement si, il existe $Q \in K[X]$ tel que $P = Q(X^p)$, ce qui démontre le résultat voulu. □

4. On peut aussi remarquer que $k$ et $p$ sont premiers entre eux. Si $u, v \in \mathbb{Z}$ sont deux entiers tels que $uk + vp = 1$, on a alors $a_k = u(k a_k) + v(p a_k) = u{\cdot}0 + v{\cdot}0 = 0$.

En guise d'application, nous allons maintenant caractériser les corps pour lesquels toute extension algébrique est séparable. De tels corps méritent un nom bien à eux.

Définition III.3.6. Un corps $K$ est dit *parfait* si toute extension algébrique de $K$ est séparable.

On a alors le théorème suivant.

Théorème III.3.7. *Soit $K$ un corps. Alors, $K$ est parfait si, et seulement si, une des deux conditions suivantes est réalisée :*

(1) $\mathrm{car}(K) = 0$ ;

(2) $\mathrm{car}(K) = p > 0$ *et* $K = K^p$, *où* $K^p = \{x^p \mid x \in K\}$.

*En particulier, tout corps fini est parfait.*

*Démonstration.* Remarquons qu'un corps $K$ est parfait si, et seulement si, tout élément algébrique sur $K$ est séparable, ou encore si, et seulement si, tout polynôme irréductible unitaire de $K[X]$ est séparable.

Si $\mathrm{car}(K) = 0$, tout polynôme irréductible unitaire de $K[X]$ est séparable par le lemme III.3.5 (1).

On se place maintenant dans le cas où $\mathrm{car}(K) = p > 0$. Supposons tout d'abord que $K = K^p$, et soit $P$ un polynôme irréductible unitaire de $K[X]$. Si $P$ n'est pas séparable, il existe $Q \in K[X]$ tel que $P = Q(X^p)$, par le lemme III.3.5 (2). On peut donc écrire

$$P = a_n X^{pn} + \cdots + a_1 X^p + a_0, \quad a_k \in K,\ a_n \in K^\times.$$

Par hypothèse, pour tout $k \in [\![0, n]\!]$, il existe $b_k \in K$ tel que $a_k = b_k^p$. On a donc

$$P = (b_n X^n + \cdots + b_1 X + b_0)^p.$$

En particulier, $P$ n'est pas irréductible, d'où une contradiction. Ainsi, $P$ est séparable.

Supposons maintenant que $K \neq K^p$. Il existe donc $a \in K \setminus K^p$. Montrons que $P = X^p - a$ est irréductible, non séparable. Soit $\alpha \in \overline{K}$ une racine de $P$. On a alors $\alpha^p = a$, et ainsi

$$P = X^p - \alpha^p = (X - \alpha)^p.$$

En particulier, $P$ n'est pas séparable. Supposons que $P$ ne soit pas irréductible, et soit $Q \in K[X]$ un diviseur unitaire de degré $d \in [\![1, p-1]\!]$. Alors, on a $Q = (X - \alpha)^d \in \overline{K}[X]$. Comme $Q$ est à coefficients dans $K$, le coefficient de $X^{d-1}$ est dans $K$. Autrement dit, $-d\alpha \in K$. Comme $d \in [\![1, p-1]\!]$, l'élément $d \cdot 1_K$ est inversible dans $K$, on en déduit que $-\alpha \in K$. Par conséquent, $\alpha \in K$. Mais alors,

$a = \alpha^p \in K^p$, d'où une contradiction. Ainsi, $P$ est irréductible et non séparable.

Cela démontre la première partie du théorème.

Supposons maintenant que $K$ soit un corps à $p^d$ éléments, où $p$ est premier et $d \geq 1$. Pour tout $x \in K$, on a

$$x = x^{p^d} = \left(x^{p^{d-1}}\right)^p \in K^p.$$

Ainsi, $K = K^p$. Comme $p = \mathrm{car}(K)$, on en déduit que $K$ est parfait d'après la première partie. Cela achève la démonstration. □

Remarque III.3.8. Ce théorème montre deux choses :

(i) la séparabilité d'une extension $L/K$ est automatique lorsque $K$ est de caractéristique nulle ou un corps fini ;

(ii) il faut vraiment se fatiguer pour construire des éléments algébriques sur $K$ non séparables. En fait, si $\overline{K}$ contient un élément non séparable, alors $K$ est une extension transcendante de $\mathbb{F}_p$, où $p$ est un nombre premier. En effet, si le corps $K$ n'est pas parfait, on a $\mathrm{car}(K) = p > 0$. Dans ce cas, $K$ est une extension de $\mathbb{F}_p$. Supposons que $K/\mathbb{F}_p$ soit algébrique. Si $L/K$ est une extension algébrique, alors $L/\mathbb{F}_p$ est une extension algébrique par la proposition I.2.19, donc séparable puisque $\mathbb{F}_p$ est parfait. Mais alors, $L/K$ est aussi séparable par la remarque III.1.10. Ainsi, si l'extension $K/\mathbb{F}_p$ est algébrique, $K$ est parfait. Cela montre le fait annoncé.

## III.4. Traces et normes

Pour finir ce chapitre, nous allons introduire la trace et la norme d'une extension, qui généralisent respectivement la partie réelle et le module d'un nombre complexe[5], et qui s'avèrent extrêmement utiles pour les calculs.

Comme ce n'est pas plus compliqué, nous allons les définir pour une algèbre associative unitaire de dimension finie.

Définition III.4.1. Soit $E$ une $K$-algèbre associative unitaire de dimension finie. Pour tout $x \in E$, on appelle *trace* et *norme* de $x \in E$, la trace et le déterminant de l'application $K$-linéaire

$$\begin{aligned} \ell_x \colon E &\longrightarrow E \\ y &\longmapsto xy. \end{aligned}$$

5. Ou presque...

On les note respectivement $\mathrm{Tr}_{E/K}(x)$ et $N_{E/K}(x)$.

Exemples III.4.2.

(1) Soit $E = K^n$. Si $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, la matrice représentative de la multiplication à gauche par $x \in E$ dans la base canonique est la matrice diagonale
$$\begin{pmatrix} x_1 & & \\ & \ddots & \\ & & x_n \end{pmatrix}.$$
On a alors
$$\mathrm{Tr}_{E/K}(x) = x_1 + \cdots + x_n \quad \text{et} \quad N_{E/K}(x) = x_1 \dots x_n.$$

(2) Soit $E = K(\sqrt{d})$, où $d \in K$ n'est pas un carré dans $K$. Dans ce cas, la famille $(1, \sqrt{d})$ est une $K$-base de $E$. Si $x = a + b\sqrt{d},\ a,\ b \in K$, la matrice représentative de la multiplication à gauche par $x \in E$ dans cette base est
$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}.$$
Ainsi, on a
$$\mathrm{Tr}_{K(\sqrt{d})/K}(a + b\sqrt{d}) = 2a \quad \text{et} \quad N_{K(\sqrt{d})/K}(a + b\sqrt{d}) = a^2 - db^2.$$
En particulier, si $K = \mathbb{R}$ et $d = -1$, on a $E = \mathbb{C}$, et l'on obtient
$$\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(z) = 2\Re(z) \quad \text{et} \quad N_{\mathbb{C}/\mathbb{R}}(z) = |z|^2.$$

Le lemme suivant donne quelques propriétés de la trace et de la norme.

Lemme III.4.3. *Soit $E$ une $K$-algèbre associative unitaire, de dimension finie. Alors :*

(1) *l'application $\mathrm{Tr}_{E/K} : E \longrightarrow K$ est une forme linéaire ;*
(2) *pour tous $x$, $y \in E$, on a*
$$\mathrm{Tr}_{E/K}(xy) = \mathrm{Tr}_{E/K}(yx) \quad \textit{et} \quad N_{E/K}(xy) = N_{E/K}(x)N_{E/K}(y)$$
(3) *pour tout $\lambda \in K$, on a $\mathrm{Tr}_{E/K}(\lambda) = n{\cdot}\lambda$ et $N_{E/K}(\lambda) = \lambda^n$, où $n$ est la dimension de $E$ sur $K$;*
(4) *pour tout $x \in E$, on a $N_{E/K}(x) \neq 0$ si, et seulement si, $x \in E^\times$.*

*Démonstration.* Une application des définitions montre que
$$\begin{aligned} \mu_{E/K} \colon E &\longrightarrow \mathscr{L}(E) \\ x &\longmapsto \ell_x \end{aligned}$$

est $K$-linéaire. Or, la trace $\mathrm{tr} : \mathscr{L}(E) \longrightarrow K$ est également $K$-linéaire. Ainsi, $\mathrm{Tr}_{E/K} = \mathrm{tr} \circ \mu_{E/K}$ est aussi $K$-linéaire, d'où (1).

De plus, pour tous $x$, $y \in E$, on a $\ell_{xy} = \ell_x \circ \ell_y$. Les propriétés usuelles de la trace et du déterminant d'un endomorphisme donnent alors (2). Si maintenant $\lambda \in K$, on a $\ell_\lambda = \lambda \mathrm{Id}_E$, et (3) s'en déduit immédiatement.

Montrons (4). Si $x \in E^\times$, alors $\ell_x$ est inversible, d'inverse $\ell_{x^{-1}}$. En particulier,

$$N_{E/K}(x) = \det(\ell_x) \neq 0.$$

Supposons maintenant que $N_{E/K}(x) \neq 0$. Alors, $\ell_x$ est inversible, donc surjective. Il existe alors $y \in E$ tel que $\ell_x(y) = xy = 1_E$. Mais alors, on a

$$x(yx) = (xy)x = x = x{\cdot}1_E.$$

Comme $\ell_x$ est bijective, on en déduit $yx = 1_E$. Ainsi, $xy = yx = 1_E$, ce qui démontre que $x \in E^\times$. Cela achève la démonstration. □

Nous allons maintenant nous intéresser de plus près aux propriétés de la trace et de la norme des extensions de degré fini. On commence par un lemme qui permet de calculer la trace et la norme d'un élément pourvu que l'on connaisse son polynôme minimal.

Lemme III.4.4. *Soit $L/K$ une extension de degré fini. Alors, pour tout $x \in L$, on a*

$$\chi_{\ell_x} = \mu_{x,K}^{[L:K(x)]}.$$

*En particulier :*

(1) *si $\mu_{x,K} = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, alors $\mathrm{Tr}_{K(x)/K}(x) = -a_{n-1}$ et $N_{K(x)/K}(x) = (-1)^n a_0$ ;*

(2) *$\mathrm{Tr}_{L/K}(x) = [L : K(x)]{\cdot}\mathrm{Tr}_{K(x)/K}(x)$ et $N_{L/K}(x) = \big(N_{K(x)/K}(x)\big)^{[L:K(x)]}$.*

*Démonstration.* Soit $n = [K(x) : K]$, et soit $m = [L : K(x)]$.

Soit $\mathbf{f} = (f_1, \ldots, f_m)$ une $K(x)$-base de $L$. Comme $\mathbf{e} = (1, x, \ldots, x^{n-1})$ est une $K$-base de $K(x)$, la famille

$$\mathbf{g} = (f_1, xf_1, \ldots, x^{n-1}f_1, \ldots, f_m, xf_m, \ldots, x^{n-1}f_m)$$

est une $K$-base[6] de $L$.

On vérifie alors aisément l'égalité

$$\mathrm{Mat}(\ell_x; \mathbf{g}) = \begin{pmatrix} \mathrm{Mat}(\ell_x; \mathbf{e}) & & \\ & \ddots & \\ & & \mathrm{Mat}(\ell_x; \mathbf{e}) \end{pmatrix},$$

6. C'est un cas particulier d'un fait général établi dans la démonstration de la formule de multiplicativité des degrés.

où $\ell_x$ est vu dans le membre de droite comme un endomorphisme de $K(x)$. Or, on vérifie aisément que $\mathrm{Mat}(\ell_x\,;\mathbf{e})$ n'est rien d'autre que la matrice compagnon du polynôme $\mu_{x,K}$. Le polynôme caractéristique de $\ell_x \in \mathscr{L}\big(K(x)\big)$ est donc $\mu_{x,K}$. On en déduit alors l'égalité voulue.

Remarquons au passage que l'on a obtenu que le polynôme caractéristique de $\ell_x \in \mathscr{L}\big(K(x)\big)$ est $\mu_{x,K}$, ce qui donne alors le point (1). L'égalité $\chi_{\ell_x} = \mu_{x,K}^{[L:K(x)]}$ et le point (1) nous donne alors

$$\mathrm{Tr}_{L/K}(x) = -[L:K(x)]\cdot a_{n-1} = [L:K(x)]\cdot \mathrm{Tr}_{K(x)/K}(x),$$

ainsi que

$$N_{L/K}(x) = (-1)^{n[L:K(x)]} a_0^{[L:K(x)]} = \big(N_{K(x)/K}(x)\big)^{[L:K(x)]}.$$

Cela achève la démonstration. □

La proposition suivante donne un autre moyen de calculer la trace et la norme dans une extension séparable.

Proposition III.4.5. *Soit $L/K$ une extension séparable de degré fini. Alors, pour tout $x \in L$, on a*

$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma\in\mathscr{X}(L/K)} \sigma(x) \quad \textit{et} \quad N_{L/K}(x) = \prod_{\sigma\in\mathscr{X}(L/K)} \sigma(x)$$

*Démonstration.* Le lemme précédent donne $\chi_{\ell_x} = \mu_{x,K}^{[L:K(x)]}$ pour tout $x \in L$. Le lemme III.2.11 nous fournit alors l'égalité

$$\chi_{\ell_x} = \prod_{\sigma\in\mathscr{X}(L/K)} \big(X - \sigma(x)\big).$$

On obtient alors

$$\mathrm{Tr}_{L/K}(x) = \mathrm{tr}(\ell_x) = \sum_{\sigma\in\mathscr{X}(L/K)} \sigma(x),$$

ainsi que

$$N_{L/K}(x) = \det(\ell_x) = \prod_{\sigma\in\mathscr{X}(L/K)} \sigma(x),$$

d'où le résultat. □

On continue par une caractérisation des extensions séparables en termes de trace.

On peut maintenant montrer le résultat suivant.

Théorème III.4.6. *Soit $L/K$ une extension de degré fini. Alors, $L/K$ est séparable si, et seulement si, $\mathrm{Tr}_{L/K}$ est non identiquement nulle.*

*Démonstration.*

Supposons que $L/K$ soit séparable. Alors, les éléments de $\mathscr{X}(L/K)$ sont deux à deux distincts. Par le corollaire III.1.5, $\displaystyle\sum_{\sigma\in\mathscr{X}(L/K)} \sigma$ est non nulle. Ceci revient à dire que $\iota \circ \mathrm{Tr}_{L/K}$ est non nulle, où $\iota : K \longrightarrow \overline{K}$ est l'inclusion. En particulier, $\mathrm{Tr}_{L/K}$ est non nulle.

Supposons que $L/K$ ne soit pas séparable. Par le lemme III.3.5 (2), $K$ est de caractéristique $p > 0$. Soit $M/K$ la sous-extension de $L/K$ formée des éléments de $L$ séparables sur $K$. Si $L/M$ était séparable, $L/K$ serait séparable par la proposition III.2.5. Ainsi, il existe $y \in L$ non séparable sur $M$. On a donc $\mu_{y,M} = Q(X^p)$, où $Q \in M[X]$ est non constant, toujours d'après le lemme III.3.5 (2). En particulier, on a $p \mid [M(y) : M]$, et par conséquent $p \mid [L : M]$.

Cela étant dit, soit $x \in L$. Rappelons que l'on a

$$\mathrm{Tr}_{L/K}(x) = [L : K(x)]\cdot\mathrm{Tr}_{K(x)/K}(x)$$

par le lemme III.4.4.

Si $x$ est séparable sur $K$, alors $x \in M$. On a donc $K(x) \subset M$, et en particulier, on a $[L : K(x)] = [L : M][M : K(x)]$. Ainsi, $p \mid [L : K(x)]$. Puisque $K$ est de caractéristique $p$, on a alors $\mathrm{Tr}_{L/K}(x) = 0$.

Si $x$ n'est pas séparable sur $K$, on a $\mu_{x,K} = P(X^p)$, où $P \in K[X]$ est de degré $d \geq 1$. Ainsi, $\mu_{x,K}$ est de degré $dp$, mais ne possède pas de terme en $X^{dp-1}$. Le lemme III.4.4 montre alors que $\mathrm{Tr}_{K(x)/K}(x) = 0$, et l'on a encore $\mathrm{Tr}_{L/K}(x) = 0$. Autrement dit, $\mathrm{Tr}_{L/K}$ est identiquement nulle. Cela achève la démonstration. $\square$

Chapitre IV

# Extensions galoisiennes

Nous nous intéressons plus spécifiquement dans ce chapitre au groupe des automorphismes d'une extension de degré fini. Dans la suite, nous identifierons $\mathrm{Gal}(L/K)$ avec l'image de l'application

$$\mathrm{Gal}(L/K) \longrightarrow \mathscr{X}(L/K),$$

obtenue en composant à droite par l'inclusion $L \subset \overline{K}$. Comme nous l'avons déjà remarqué, on a alors une inclusion

$$\mathrm{Gal}(L/K) \subset \mathscr{X}(L/K),$$

mais l'inclusion est stricte en général.

Nous allons en premier lieu nous intéresser aux conditions sous lesquelles cette inclusion est une égalité.

## IV.1. Extensions normales

Entrons immédiatement dans le vif du sujet.

Lemme IV.1.1. *Soit $L/K$ une extension de degré fini. Les propriétés suivantes sont équivalentes :*

(1) *tout plongement de $L/K$ est un automorphisme de $L/K$ ;*
(2) *tout polynôme irréductible unitaire de $K[X]$ ayant au moins une racine dans $L$ est scindé dans $L$ ;*
(3) *l'extension $L/K$ est le corps des racines d'un polynôme de $K[X]$.*

*Démonstration.*

(1) $\Longrightarrow$ (2). Soit $P \in K[X]$ un polynôme irréductible unitaire possédant une racine $\alpha \in L$. Soient $\alpha_1 = \alpha$, $\alpha_2, \ldots, \alpha_n \in \overline{K}$ les racines distinctes de $P$ dans $\overline{K}$. On a donc $\mu_{\alpha,K} = P$.

Pour tout $i \in [\![1, n]\!]$, soit $\tau_i : K(\alpha) \longrightarrow \overline{K}$ l'unique plongement de $K(\alpha)/K$ tel que $\tau_i(\alpha) = \alpha_i$. Soit alors $\sigma_i : L \longrightarrow \overline{K}$ une extension de $\tau_i$

à $L$. Par hypothèse, $\sigma$ est un automorphisme de $L/K$. En particulier, $\sigma(L) = L$. Mais alors, on a

$$\sigma_i(\alpha) = \tau_i(\alpha) = \alpha_i \in L,$$

et $P$ est scindé dans $L$.

(2) $\Longrightarrow$ (3). Soient $\alpha_1, \ldots, \alpha_m \in L$ tels que $L = K(\alpha_1, \ldots, \alpha_m)$. Par hypothèse, $\mu_{\alpha_i,K}$ est scindé dans $L$ pour tout $i \in [\![1, m]\!]$. En particulier, $L$ contient toutes les racines du polynôme

$$P = \prod_{i=1}^{m} \mu_{\alpha_i,K}.$$

Comme l'ensemble des racines $P$ contient $\alpha_1, \ldots, \alpha_m$, on en déduit que l'extension $L/K$ est engendrée par les racines de $P$. Autrement dit, $L/K$ est le corps des racines de $P$.

(3) $\Longrightarrow$ (1). Supposons que l'extension $L/K$ soit le corps des racines d'un polynôme $P \in K[X]$, que l'on peut supposer unitaire. Il existe donc des éléments $\alpha_1, \ldots, \alpha_m \in L$ tels que

$$P = (X - \alpha_1) \cdots (X - \alpha_m) \quad \text{et} \quad L = K(\alpha_1, \ldots, \alpha_m).$$

Soit $\sigma \in \mathscr{X}(L/K)$. Puisque $\sigma$ est $K$-linéaire, on a

$$P\big(\sigma(\alpha_i)\big) = \sigma\big(P(\alpha_i)\big) = 0,$$

et $\sigma(\alpha_i)$ est donc une racine de $P$. Ainsi, on a

$$\sigma(\alpha_i) \in \{\alpha_1, \ldots, \alpha_m\} \subset L.$$

Or, puisque $L = K[\alpha_1, \ldots, \alpha_m]$, on en déduit que $\sigma(L) \subset L$. Ainsi, $\sigma$ est donc un morphisme de $K$-algèbres injectif de $L$ dans lui-même. Comme $L/K$ est de degré fini, on en déduit que $\sigma$ est bijectif. Par conséquent, $\sigma$ est un automorphisme de $L/K$.

Cela achève la démonstration. □

Définition IV.1.2. Une extension $L/K$ de degré fini est dite *normale* si elle vérifie une des conditions équivalentes du lemme précédent.

Exemples IV.1.3. (1) Soit $K = \mathbb{Q}$, et soit $L = \mathbb{Q}(\sqrt[3]{2})$. Alors, l'extension $L/K$ n'est pas normale. En effet,

$$P = X^3 - 2 = (X - \sqrt[3]{2})(X - j\sqrt[3]{2})(X - j^2\sqrt[3]{2})$$

est irréductible dans $\mathbb{Q}[X]$ et a une racine dans $L$, à savoir $\sqrt[3]{2}$, mais n'a pas toutes ses racines dans $L$, puisque $L \subset \mathbb{R}$ et $P$ a des racines complexes non réelles.

(2) Soit $K = \mathbb{Q}$, et soit $L = \mathbb{Q}(\sqrt[3]{2}, j)$. Alors, $L/K$ est normale. En effet, on a les égalités
$$L = \mathbb{Q}(\sqrt[3]{2}, j,\ j^2) = \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}).$$
En particulier, $L/K$ est le corps des racines de $X^3 - 2 \in K[X]$.

(3) Soit $K = \mathbb{F}_2(T^2)$ et $L = \mathbb{F}_2(T)$. Alors, $L/K$ est le corps des racines du polynôme $X^2 - T^2 \in K[X]$. En effet, on a
$$X^2 - T^2 = (X - T)^2.$$
Ainsi, $L/K$ est normale.

(4) Soit $K = \mathbb{Q}$, et soit $L = \mathbb{Q}(\zeta_n)$, avec $n \geq 1$. Les racines complexes de $X^n - 1$ étant les puissances de $\zeta_n$, on en déduit que $L/K$ est le corps des racines de $X^n - 1$. Par conséquent, l'extension $L/K$ est normale.

(5) Puisque $\mathbb{F}_q$ est le corps des racines de $X^q - X$ sur $\mathbb{F}_p$, l'extension $\mathbb{F}_q/\mathbb{F}_p$ est normale.

**Attention !** Une extension normale n'est pas nécessairement le corps des racines d'un polynôme **irréductible**.

Par exemple, soit $K = \mathbb{F}_2(X, Y)$ et $L = K(\sqrt{X}, \sqrt{Y})$. Alors, $L/K$ est normale, puisque c'est le corps des racines de $(T^2 - X)(T^2 - Y) \in \mathbb{F}_2[T]$. On montre (exercice) que $L/K$ est de degré 4 (cela revient à démontrer que $XY$ n'est pas un carré dans $K$). Ainsi, $(1, \sqrt{X}, \sqrt{Y}, \sqrt{XY})$ est une $K$-base de $L$. On en déduit ensuite que, pour tout $x \in L$, on a $x^2 \in K$. En particulier, le polynôme minimal d'un élément de $L$ est soit de la forme $X - a$, soit de la forme $X^2 - a$. Dans les deux cas, ce polynôme minimal possède une unique racine dans $\overline{K}$. Supposons maintenant que $L = \mathrm{Dec}_K(P)$, avec $P$ irréductible. Comme une racine $\alpha \in \overline{K}$ de $P$ est de degré $\leq 2$, $P = \mu_{\alpha,K}$ est de degré 1 ou 2, avec une unique racine $\alpha$, qui est dans $L$. Mais alors, $L/K$ serait de degré $\leq 2$, d'où une contradiction.

Lemme IV.1.4. *Soient $L/K$ et $L'/K$ deux extensions normales. Alors, $LL'/K$ est normale.*

*Démonstration.* Si $L/K$ et $L'/K$ sont respectivement les corps de racines de $P$ et $Q$ respectivement, on vérifie facilement que $LL'/K$ est le corps des racines de $PQ$, d'où le résultat. □

Lemme IV.1.5. *Soit $L/K$ une extension, et soient $E/K$ et $E'/K$ deux sous-extensions. Si $E/K$ est normale, alors $EE'/E'$ est normale.*

*En particulier, si $L/K$ est normale, et si $M/K$ est une sous-extension, alors $L/M$ est normale.*

*Démonstration.* Si $E/K$ est le corps des racines de $P \in K[X]$, alors $EE'/E'$ est le corps des racines de $P$, vu comme polynôme de $E'[X]$. La seconde partie s'obtient en appliquant ce qui précède à $E = L$ et $E' = M$. □

Remarque IV.1.6. Les exemples IV.1.3 (1) et (2) montrent qu'une sous-extension d'une extension normale n'est pas nécessairement normale.

Lemme IV.1.7. *L'intersection d'une famille non vide d'extensions normales de $K$ est une extension normale de $K$.*

*Démonstration.* Soit $(L_i/K)_{i\in I}$ une famille non vide d'extensions normales, et soit

$$L = \bigcap_{i\in I} L_i.$$

Alors, $L/K$ est de degré fini. Soit $P \in K[X]$ un polynôme irréductible unitaire ayant une racine dans $L$. Comme $L \subset L_i$ pour tout $i \in I$, l'hypothèse sur $L_i/K$ montre que toutes les racines de $P$ dans $\overline{K}$ sont en fait dans $L_i$, et cela pour tout $i \in I$. Autrement dit, les racines de $P$ dans $\overline{K}$ sont dans $L$, d'où le résultat. □

Pour finir ce paragraphe, remarquons qu'une extension $L/K$ de degré fini est contenue dans une extension normale. En effet, si $(\alpha_1, \dots, \alpha_m)$ est une $K$-base de $L$, alors $L = K(\alpha_1, \dots, \alpha_m)$, et $L$ est contenue dans le corps des racines de $\mu_{\alpha_1,K} \cdots \mu_{\alpha_m,K}$. Cela justifie la définition suivante.

Définition IV.1.8. Soit $L/K$ une extension de degré fini. La *clôture normale* de $L/K$ est l'intersection de tous les extensions normales contenant $L$. Autrement dit, c'est la plus petite sous-extension normale contenant $L/K$.

## IV.2. Extensions galoisiennes

Soit $L/K$ une extension de degré fini. Rappelons que l'on a l'inclusion

$$\mathrm{Gal}(L/K) \subset \mathscr{X}(L/K),$$

et donc

$$|\mathrm{Gal}(L/K)| \leq |\mathscr{X}(L/K)| \leq [L : K],$$

par le lemme III.1.6. Nous allons maintenant déterminer sous quelles conditions on a $|\mathrm{Gal}(L/K)| = [L : K]$.

Lemme IV.2.1. *Soit $L/K$ une extension de corps de degré fini. Alors, on a l'égalité $|\mathrm{Gal}(L/K)| = [L : K]$ si, et seulement si, $L/K$ est normale et séparable.*

*Démonstration.* Si $|\mathrm{Gal}(L : K)| = [L : K]$, on a donc $|\mathscr{X}(L/K)| = [L : K]$, ce qui prouve que $L/K$ est séparable d'après le lemme III.1.6, ainsi que l'égalité $\mathrm{Gal}(L/K) = \mathscr{X}(L/K)$, ce qui montre que $L/K$ est normale par définition.

Inversement, supposons que $L/K$ soit normale et séparable. La normalité de $L/K$ implique alors que $|\mathrm{Gal}(L/K)| = |\mathscr{X}(L/K)|$, et la séparabilité montre alors que $|\mathscr{X}(L/K)| = [L : K]$, d'où l'égalité requise. Cela achève la démonstration. □

Cela motive la définition suivante.

Définition IV.2.2. Une extension $L/K$ de degré fini est dite *galoisienne* si elle est normale et séparable. Dans ce cas, on a

$$\mathrm{Gal}(L/K) = [L : K].$$

C'est même équivalent par le lemme précédent.

Exemples IV.2.3.

(1) Soit $n \geq 1$. Alors, l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne. En effet, elle est normale par l'exemple IV.1.3 (4) et séparable, car $\mathbb{Q}$ est de caractéristique nulle (cf. théorème III.3.7).

(2) Soit $q$ une puissance d'un nombre premier $p$ et soit $d \geq 1$. Alors, l'extension $\mathbb{F}_{q^d}/\mathbb{F}_q$ est galoisienne (Rappelons que l'on a bien $\mathbb{F}_q \subset \mathbb{F}_{q^d}$, puisqu'un élément $x \in \mathbb{F}_q$ vérifie $x^q = x$, et donc a fortiori $x^{q^d} = x$).

En effet, l'extension $\mathbb{F}_{q^d}/\mathbb{F}_p$ est normale par l'exemple IV.1.3 (5). On en déduit que $\mathbb{F}_{q^d}/\mathbb{F}_q$ est normale par le lemme IV.1.5. De plus, cette extension est séparable par le théorème III.3.7.

Elle est donc galoisienne de degré $d$ (si $q = p^m$, on a $[\mathbb{F}_{q^d} : \mathbb{F}_q] = \dfrac{[\mathbb{F}_{q^d} : \mathbb{F}_p]}{[\mathbb{F}_q : \mathbb{F}_p]} = \dfrac{dm}{m} = d$).

On calculera son groupe de Galois un peu plus loin.

(3) Si $K = \mathbb{F}_2(T^2)$ et $L = \mathbb{F}_2(T)$, l'extension est normale, non séparable d'après les exemples IV.1.3 (3) et III.1.9 (3).

(4) Soit $K = \mathbb{F}_2(T)$, et soit $L = K(\sqrt[3]{T}, \sqrt{T})$. Alors, $L/K$ n'est ni normale, ni séparable (exercice).

(5) L'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ est séparable, car $\mathbb{Q}$ est de caractéristique nulle, mais n'est pas normale d'après l'exemple IV.1.3 (1).

(6) L'extension $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est galoisienne. En effet, elle est normale par l'exemple IV.1.3 (2), et séparable, car $\mathbb{Q}$ est de caractéristique

nulle. Calculons son groupe de Galois. Il revient au même de calculer les plongements de cette extension.

Puisque $\mu_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2$, les plongements de $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ sont les morphismes

$$\tau_k : \sqrt[3]{2} \rightsquigarrow j^k \sqrt[3]{2}, \quad k \in [\![0,2]\!] .$$

On remarque que $j, j^2 \notin \mathbb{Q}(\sqrt[3]{2})$, puisque $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$. On a donc

$$\mu_{j,\mathbb{Q}(\sqrt[3]{2})} = X^2 + X + 1,$$

puisque que ce polynôme annule $j$ et n'a pas de racines dans $\mathbb{Q}(\sqrt[3]{2})$. Ainsi, on a $\tau_k(\mu_{j,\mathbb{Q}(\sqrt[3]{2})}) = \mu_{j,\mathbb{Q}(\sqrt[3]{2})}$ pour tout $k \in [\![0,2]\!]$.

On en déduit alors que les éléments de $\mathrm{Gal}\big(\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}\big)$ sont les morphismes

$$\sigma_{k,m} : \left| \begin{array}{ccc} \sqrt[3]{2} & \rightsquigarrow & j^k \sqrt[3]{2} \\ j & \rightsquigarrow & j^m \end{array} \right. , \quad k \in [\![0,2]\!] , \ m \in [\![1,2]\!] .$$

Soient $\sigma = \sigma_{1,1}$ et $\tau = \sigma_{0,2}$. On vérifie aisément que $\sigma$ et $\tau$ ne commutent pas. Ainsi, $\mathrm{Gal}\big(\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}\big)$ est un groupe d'ordre 6 non abélien, d'où un isomorphisme

$$\mathrm{Gal}\big(\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}\big) \simeq D_3.$$

De simples calculs montrent d'ailleurs que $\sigma$ est d'ordre 3, que $\tau$ est d'ordre 2, et que $\tau\sigma\tau^{-1} = \sigma^{-1}$.

Lemme IV.2.4. *Toute extension séparable de degré fini est contenue dans une extension galoisienne.*

*Démonstration.* Soit $F/K$ une extension séparable de degré fini. D'après le théorème de l'élément primitif, il existe $\alpha \in L$ tel que $F = K(\alpha)$. Soit $L/K$ le corps des racines de $\mu_{\alpha,K}$. Par hypothèse, $\alpha$ est séparable sur $K$ et le polynôme $\mu_{\alpha,K} \in K[X]$ est donc séparable. En particulier, toutes les racines de $\mu_{\alpha,K}$ sont aussi séparables sur $K$. Comme $L/K$ est engendrée par ces racines, $L/K$ est séparable sur $K$. De plus, $L/K$ est normale par définition. Ainsi, $L/K$ est une extension galoisienne. De plus, $\alpha \in L$, donc $K(\alpha) \subset L$, d'où le résultat. □

Passons aux propriétés élémentaires des extensions galoisiennes.

Proposition IV.2.5. *Soit $L/K$ une extension, et soient $E/K$ et $E'/K$ deux sous-extensions. Si $E/K$ est galoisienne, alors $EE'/E'$ est galoisienne.*

*De plus, pour tout* $\sigma \in \mathrm{Gal}(EE'/E')$*, on a* $\sigma_{|_E} \in \mathrm{Gal}(E/K)$*, et l'application*

$$\begin{aligned} \mathrm{Gal}(EE'/E') &\longrightarrow \mathrm{Gal}(E/K) \\ \sigma &\longmapsto \sigma_{|_E} \end{aligned}$$

*est un morphisme de groupes injectif, identifiant ainsi* $\mathrm{Gal}(EE'/E')$ *à un sous-groupe de* $\mathrm{Gal}(E/K)$*.*

*En particulier, si* $L/K$ *est galoisienne, et si* $M/K$ *est une sous-extension, alors* $L/M$ *est galoisienne et* $\mathrm{Gal}(L/M)$ *est un sous-groupe de* $\mathrm{Gal}(L/K)$*.*

*Démonstration.* D'après le corollaire III.2.3, $EE'/E'$ est séparable, et d'après le lemme IV.1.5, $EE'/E'$ est normale. Ainsi, $EE'/E'$ est galoisienne. Soit maintenant $\sigma \in \mathrm{Gal}(EE'/E')$. Comme $\sigma$ est un morphisme de $E'$-algèbres, c'est aussi un morphisme de $K$-algèbres. Ainsi, $\sigma_{|_E}$ est un plongement de $E/K$, donc un automorphisme de $E/K$ par hypothèse. Il est alors clair que l'application

$$\begin{aligned} \mathrm{Gal}(EE'/E') &\longrightarrow \mathrm{Gal}(E/K) \\ \sigma &\longmapsto \sigma_{|_E} \end{aligned}$$

est un morphisme de groupes. Supposons maintenant que $\sigma \in \mathrm{Gal}(EE'/E')$ vérifie $\sigma_{|_E} = \mathrm{Id}_E$. Le lemme II.3.1 et la $E'$-linéarité de $\sigma$ impliquent alors que $\sigma = \mathrm{Id}_{EE'}$, d'où l'injectivité annoncée.

Le dernier point s'obtient en appliquant ce qui précède à $E = L$ et $E' = M$, auquel cas le morphisme précédent est en fait une inclusion (on peut aussi raisonner directement). Cela achève la démonstration. □

Lemme IV.2.6. *L'intersection d'une famille non vide d'extensions galoisiennes est galoisienne.*

*Démonstration.* Soit $(L_i/K)_{i\in I}$ une famille non vide d'extensions galoisiennes, et soit

$$L = \bigcap_{i\in I} L_i.$$

Alors, $L/K$ est normale par le lemme IV.1.7. D'autre part, comme $L/K$ est une sous-extension d'une extension séparable (par exemple, c'est une sous-extension de $L_i/K$, où $i \in I$ est fixé arbitrairement), $L/K$ est aussi séparable par la remarque III.1.10, d'où le résultat. □

Le lemme IV.2.4 et ce dernier lemme nous permet de donner la définition suivante.

Définition IV.2.7. Soit $F/K$ une extension séparable de degré fini. L'intersection de toutes les extensions galoisiennes de degré fini contenant $F$ est appelée la *clôture galoisienne* de $F/K$.

Exemple IV.2.8. Soit $F/K$ une extension séparable de degré fini. Si $\alpha \in F$ est un élément primitif, la démonstration du lemme IV.2.4 montre que le corps des racines $L/K$ de $\mu_{\alpha,K}$ est une extension galoisienne contenant $F$. C'est en fait la clôture galoisienne de $F/K$.

En effet, soit $L'/K$ une extension galoisienne contenant $F$. Alors, le corps $L'$ contient $\alpha$, et $\mu_{\alpha,K}$ a donc une racine dans $L'$. Comme $L'/K$ est normale, $L'$ contient toutes les racines de $\mu_{\alpha,K}$, et contient par conséquent la sous-extension engendrée par ces racines, c'est-à-dire $L$.

Lemme IV.2.9. *Soient $L_1/K$ et $L_2/K$ deux extensions galoisiennes. Alors, l'extension $L_1L_2/K$ est galoisienne. De plus, l'application*

$$\begin{aligned} \mathrm{Gal}(L_1L_2/K) &\longrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \\ \sigma &\longmapsto (\sigma_{|L_1}, \sigma_{|L_2}) \end{aligned}$$

*est un morphisme de groupes injectif, et identifie donc* $\mathrm{Gal}(L_1L_2/K)$ *à un sous-groupe de* $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

*Démonstration.* Le premier point découle du corollaire III.2.4 ainsi que du lemme IV.1.4.

Soit $\sigma \in \mathrm{Gal}(L_1L_2/K)$. Pour $i \in \{1,2\}$, $\sigma_{|L_i}$ est un plongement de $L_i/K$, donc un élément de $\mathrm{Gal}(L_i/K)$ puisque $L_i/K$ est galoisienne. On vérifie alors aisément que l'application de l'énoncé est un morphisme de groupes. Supposons maintenant que $\sigma \in \mathrm{Gal}(L_1L_2/K)$ vérifie

$$\sigma_{|L_i} = \mathrm{Id}_{L_i}, \qquad \text{pour tout } i \in \{1,2\},$$

le lemme II.3.1 montre alors que $\sigma = \mathrm{Id}_{L_1L_2}$, d'où le résultat. □

Profitons-en également pour énoncer un résultat annoncé sans démonstration dans le paragraphe II.5, et qui explique de manière plus conceptuelle le point (1) de la proposition II.4.11.

Lemme IV.2.10. *Soit $L/K$ une extension galoisienne. Alors, $L^{\mathrm{Gal}(L/K)} = K$.*

*Démonstration.* Puisque $L/K$ est galoisienne, on a $\mathscr{X}(L/K) = \mathrm{Gal}(L/K)$. Il suffit alors d'appliquer le corollaire III.2.12 pour conclure. □

On continue ce paragraphe par une proposition qui facilite grandement les calculs.

Proposition IV.2.11. *Soient $E/K$ et $E'/K$ deux sous-extensions d'une extension $L/K$. Si $E/K$ est galoisienne, alors $E/K$ et $E'/K$ sont linéairement disjointes si, et seulement si, $E \cap E' = K$.*

*En particulier, si $E/K$ est galoisienne, alors $E/E \cap E'$ et $E'/E \cap E'$ sont linéairement disjointes.*

*Démonstration.* On sait déjà que la condition $E \cap E' = K$ est nécessaire. Supposons maintenant que $E \cap E' = K$. Supposons que $E/K$ et $E'/K$ ne soient pas linéairement disjointes. Soit $(x'_1, \ldots, x'_n)$ une famille $K$-libre de $E'$ qui est $E$-liée. On suppose $n \geq 1$ minimal. Remarquons que $n \geq 2$. Quitte à renuméroter, on peut supposer qu'il existe $x_1, \ldots, x_{n-1} \in E$ tels que

$$x'_n = \sum_{i=1}^{n-1} x_i x'_i.$$

Pour tout $\sigma \in \mathrm{Gal}(EE'/E')$, on a donc $x'_n = \sum_{i=1}^{n-1} \sigma(x_i) x'_i$, et par conséquent

$$\sum_{i=1}^{n-1} (\sigma(x_i) - x_i) x'_i = 0, \qquad \text{pour tout } \sigma \in \mathrm{Gal}(EE'/E').$$

Par la proposition IV.2.5, on a $\sigma(x_i) \in E$, et par suite $\sigma(x_i) - x_i \in E$ pour tout $i \in [\![1, n-1]\!]$. Par minimalité de $n$, on en déduit

$$\sigma(x_i) = x_i, \qquad \text{pour tout } i \in [\![1, n-1]\!].$$

Puisque l'extension $EE'/E'$ est galoisienne, le lemme IV.2.10 implique alors que $x_i \in E'$ pour tout $i \in [\![1, n-1]\!]$. Comme on a aussi $x_i \in E$, on obtient que $x_i \in K$ pour tout $i \in [\![1, n-1]\!]$. Mais alors, on en déduit que la famille $(x'_1, \ldots, x'_n)$ est $K$-liée, d'où une contradiction. Ainsi, $E/K$ et $E'/K$ sont bien linéairement disjointes.

Le dernière point provient du fait que $E/E \cap E'$ est aussi galoisienne d'après la proposition IV.2.5, et du point précédent. Cela achève la démonstration. □

Signalons maintenant deux applications de cette proposition. La première précise les résultats de la proposition IV.2.5.

Théorème IV.2.12. *Soit $L/K$ une extension, et soient $E/K$ et $E'/K$ deux sous-extensions. Si $E/K$ est galoisienne, alors pour tout $\sigma \in \mathrm{Gal}(EE'/E')$, on a $\sigma_{|E} \in \mathrm{Gal}(E/E \cap E')$, et l'application*

$$\begin{array}{rccc} \rho\colon & \mathrm{Gal}(EE'/E') & \longrightarrow & \mathrm{Gal}(E/E \cap E') \\ & \sigma & \longmapsto & \sigma_{|E} \end{array}$$

*est un isomorphisme de groupes.*

*En particulier, on a* $\mathrm{Gal}(EE'/E') \simeq \mathrm{Gal}(E/K)$ *si, et seulement si,* $E/K$ *et* $E'/K$ *sont linéairement disjointes.*

*Démonstration.* Puisque $E/K$ est galoisienne, $E/E \cap E'$ est aussi galoisienne par la dernière partie de la proposition IV.2.5. En appliquant la première partie de cette proposition aux extensions $E/E \cap E'$ et $E'/E \cap E'$, on obtient que pour tout $\sigma \in \mathrm{Gal}(EE'/E')$, on a $\sigma_{|_E} \in \mathrm{Gal}(E/E \cap E')$, et que l'application

$$\begin{array}{rccc} \rho\colon & \mathrm{Gal}(EE'/E') & \longrightarrow & \mathrm{Gal}(E/E \cap E') \\ & \sigma & \longmapsto & \sigma_{|_E} \end{array}$$

est un morphisme de groupes injectif. Comme $E/E \cap E'$ et $E'/E \cap E'$ sont linéairement disjointes d'après la proposition précédente, on a

$$[EE' : E'] = [E : E \cap E'].$$

Mais alors, $|\mathrm{Gal}(EE'/E')| = |\mathrm{Gal}(E/E \cap E')|$, et $\rho$ est donc bijective.

Montrons la dernière partie. Si $E/K$ et $E'/K$ sont linéairement disjointes, alors $E \cap E' = K$, et le premier point fournit un isomorphisme de groupes

$$\mathrm{Gal}(EE'/E') \simeq \mathrm{Gal}(E/K).$$

Supposons enfin que les groupes $\mathrm{Gal}(EE'/E')$ et $\mathrm{Gal}(E/K)$ soient isomorphes. En particulier, ils ont même ordre, et donc $[EE' : E'] = [E : K]$. Mais alors, $E/K$ et $E'/K$ sont linéairement disjointes, et cela d'après la proposition II.3.6. Cela achève la démonstration. □

Théorème IV.2.13. *Soient* $L_1/K$ *et* $L_2/K$ *deux extensions galoisiennes. Alors, les extensions* $L_1/L_1 \cap L_2, L_2/L_1 \cap L_2$ *et* $L_1L_2/L_1 \cap L_2$ *sont galoisiennes, et l'application*

$$\begin{array}{rccc} \theta\colon & \mathrm{Gal}(L_1L_2/L_1 \cap L_2) & \longrightarrow & \mathrm{Gal}(L_1/L_1 \cap L_2) \times \mathrm{Gal}(L_2/L_1 \cap L_2) \\ & \sigma & \longmapsto & (\sigma_{|_{L_1}}, \sigma_{|_{L_2}}) \end{array}$$

*est un isomorphisme de groupes.*

*En particulier, on a* $\mathrm{Gal}(L_1L_2/K) \simeq \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ *si, et seulement si,* $L_1/K$ *et* $L_2/K$ *sont linéairement disjointes.*

*Démonstration.* Soit $i \in \{1, 2\}$. Puisque $L_i/K$ est galoisienne, $L_i/L_1 \cap L_2$ est galoisienne par la proposition IV.2.5. Le lemme IV.2.9 montre alors que l'extension $L_1L_2/L_1 \cap L_2$ est galoisienne.

Pour tout $\sigma \in \mathrm{Gal}(L_1L_2/L_1 \cap L_2)$, $\sigma_{|_{L_i}}$ est un plongement de $L_i/L_1 \cap L_2$, donc un élément de $\mathrm{Gal}(L_i/L_1 \cap L_2)$ puisque $L_i/L_1 \cap L_2$ est galoisienne. On vérifie aisément que $\theta$ est un morphisme de groupes. De plus, les

deux extensions $L_1/L_1 \cap L_2$ et $L_2/L_1 \cap L_2$ sont linéairement disjointes par la proposition IV.2.11. On a donc

$$[L_1L_2 : L_1 \cap L_2] = [L_1 : L_1 \cap L_2][L_2 : L_1 \cap L_2]$$

par le corollaire II.3.7. Comme les extensions $L_1/L_1 \cap L_2$, $L_2/L_1 \cap L_2$ et $L_1L_2/L_1 \cap L_2$ sont galoisiennes, cela revient à dire que les deux groupes finis $\mathrm{Gal}(L_1L_2/L_1 \cap L_2)$ et $\mathrm{Gal}(L_1/L_1 \cap L_2) \times \mathrm{Gal}(L_2/L_1 \cap L_2)$ ont même ordre.

Il suffit donc de montrer que $\theta$ est injectif pour en conclure que c'est un isomorphisme. Or, si $\sigma \in \mathrm{Gal}(L_1L_2/L_1 \cap L_2)$ vérifie

$$\sigma_{|L_i} = \mathrm{Id}_{L_i}, \qquad \text{pour tout } i \in \{1, 2\},$$

le lemme II.3.1 montre alors que $\sigma = \mathrm{Id}_{L_1L_2}$, d'où le premier point.

Notons que $L_1L_2/K$ est galoisienne par le lemme IV.2.9. Si les extensions $L_1/K$ et $L_2/K$ sont linéairement disjointes, on a $L_1 \cap L_2 = K$, et le point précédent donne un isomorphisme de groupes

$$\mathrm{Gal}(L_1L_2/K) \simeq \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K).$$

Inversement, si $\mathrm{Gal}(L_1L_2/K)$ et $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ sont isomorphes, ils ont même ordre, et par conséquent

$$[L_1L_2 : K] = [L_1 : K][L_2 : K],$$

puisque les extensions $L_1/K, L_2/K$ et $L_1L_2/K$ sont galoisiennes. Par le corollaire II.3.7, $L_1/K$ et $L_2/K$ sont linéairement disjointes. Cela achève la démonstration. □

## IV.3. Le groupe de Galois d'un polynôme

Dans la présente section, nous allons nous intéresser au groupe de Galois du corps des racines d'un polynôme. Introduisons tout d'abord quelques notations.

**Notation.** Si $P \in K[X]$ est un polynôme, on note $\mathrm{Dec}_K(P)$ le corps des racines de $P$ dans $\overline{K}$. On note $\mathrm{Gal}_K(P)$ le groupe de Galois de $\mathrm{Dec}_K(P)$.

Définition IV.3.1. Soit $P \in K[X]$ un polynôme. Le *groupe de Galois* de $P$ est le groupe de Galois de son corps des racines. On le note $\mathrm{Gal}_K(P)$.

Remarque IV.3.2. Si $P \in K[X]$ est un polynôme séparable, $\mathrm{Dec}_K(P)/K$ est une extension galoisienne. En effet, c'est une extension normale par définition. De plus, si $\alpha \in L$ est une racine de $P$, on a $\mu_{\alpha,K} \mid P$. Comme $P$ n'a que des racines simples dans $L$, il en est de même de

$\mu_{\alpha,K}$. Or, $L/K$ est engendré par les racines de $P$, qui sont des éléments séparables, et $L/K$ est donc séparable par le corollaire III.2.2.

On peut maintenant donner une autre caractérisation des extensions galoisiennes.

Lemme IV.3.3. *Une extension $L/K$ de degré fini est galoisienne si, et seulement si, $L/K$ est le corps de décomposition d'un polynôme $P \in K[X]$ irréductible séparable.*

*Dans ce cas, on peut choisir $P$ de degré $[L : K]$.*

*Démonstration.* Si $L = \mathrm{Dec}_K(P)$, avec $P \in K[X]$ irréductible séparable, alors $L/K$ est galoisienne de degré fini d'après la remarque précédente. Inversement, soit $L/K$ une extension galoisienne de degré fini. Comme $L/K$ est séparable, le théorème de l'élément primitif assure l'existence de $\alpha \in L$ tel que $L = K(\alpha)$. Posons $P = \mu_{\alpha,K}$. Puisque, $L/K$ est séparable, $\alpha$ est séparable, et ainsi $P$ est un polynôme irréductible séparable. De plus, on a

$$[L : K] = [K(\alpha) : K] = \deg(P).$$

Montrons que $L = \mathrm{Dec}_K(P)$. Par construction, le polynôme $P$ possède une racine dans $L$, à savoir $\alpha$. Puisque $L/K$ est normale, $P$ possède toutes ses racines dans $L$. Ainsi, $L$ contient toutes les racines de $P$, et par conséquent

$$\mathrm{Dec}_K(P) \subset L.$$

D'autre part, on a

$$L = K(\alpha) \subset \mathrm{Dec}_K(P),$$

puisque $\alpha$ est une racine de $P$. Finalement, on obtient $L = \mathrm{Dec}_K(P)$. Cela achève la démonstration. □

Remarque IV.3.4. Si $P \in K[X]$ est un polynôme irréductible séparable de degré $n \geq 1$, il se peut très bien que l'on ait $[\mathrm{Dec}_K(P) : K] > n$.

Par exemple, si $P = X^3 - 2 \in \mathbb{Q}[X]$, l'exemple IV.1.3 (2) montre que l'on a

$$\mathrm{Dec}_{\mathbb{Q}}(P) = \mathbb{Q}(\sqrt[3]{2}, j),$$

qui est de degré 6 sur $\mathbb{Q}$ d'après l'exemple IV.2.3 (6).

Cela démontre également qu'une extension galoisienne de degré $n$ peut être égale au corps de décomposition d'un polynôme irréductible séparable de degré strictement inférieur à $n$.

Nous allons maintenant étudier de plus près le groupe de Galois d'un polynôme séparable.

LEMME IV.3.5. *Soit $P \in K[X]$ un polynôme de degré $n \geq 1$. Alors :*

(1) *le groupe $\mathrm{Gal}_K(P)$ stabilise l'ensemble des racines dans $\overline{K}$ de tout facteur irréductible de $P$ ;*

(2) *si $X_P$ est l'ensemble des racines de $P$ dans $\overline{K}$, l'application*

$$\begin{aligned} \mathrm{Gal}_K(P) \times X_P &\longrightarrow X_P \\ (\sigma, \alpha) &\longmapsto \sigma(\alpha) \end{aligned}$$

*définit une action fidèle de $\mathrm{Gal}_K(P)$ sur $X_P$.*

*Autrement dit, l'application*

$$\begin{aligned} \mathrm{Gal}_K(P) &\longrightarrow \mathfrak{S}(X_P) \\ \sigma &\longmapsto \sigma_{|X_P} \end{aligned}$$

*est un morphisme de groupes injectif. En particulier, si $P$ est séparable, on a $[\mathrm{Dec}_K(P) : K] \mid n!$ ;*

(3) *si $P$ est irréductible, $\mathrm{Gal}_K(P)$ agit transitivement sur l'ensemble des racines de $P$. Si de plus $P$ est séparable, la réciproque est vraie.*

*Démonstration.*

(1) Soit $Q \in K[X]$ un facteur irréductible unitaire de $P$. Alors, pour toute racine $\alpha \in \mathrm{Dec}_K(P)$ de $Q$, et tout $\sigma \in \mathrm{Gal}_K(P)$, on a

$$Q\big(\sigma(\alpha)\big) = \sigma\big(Q(\alpha)\big) = 0.$$

Ainsi, $\sigma(\alpha)$ est encore une racine de $Q$.

(2) Le point précédent montre en particulier que tout élément de $\mathrm{Gal}_K(P)$ stabilise $X_P$ (fait déjà établi et utilisé maintes fois). Le fait que l'application

$$\begin{aligned} \mathrm{Gal}_K(P) \times X_P &\longrightarrow X_P \\ (\sigma, \alpha) &\longmapsto \sigma(\alpha) \end{aligned}$$

définisse une action de $\mathrm{Gal}_K(P)$ sur $X_P$ est clair. Montrons que cette action est fidèle. Si $\sigma \in \mathrm{Gal}_K(P)$ fixe chaque racine $\alpha_1, \ldots, \alpha_n \in \overline{K}$ de $P$, alors $\sigma$ fixe chaque élément de $\mathrm{Dec}_K(P)$, puisque

$$\mathrm{Dec}_K(P) = K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n].$$

Ainsi, $\sigma$ est le morphisme identité, et l'action est bien fidèle. Comme le morphisme correspondant à cette action n'est rien d'autre que le morphisme

$$\begin{aligned} \mathrm{Gal}_K(P) &\longrightarrow \mathfrak{S}(X_P) \\ \sigma &\longmapsto \sigma_{|X_P}, \end{aligned}$$

celui-ci est injectif. En particulier, le groupe $\mathrm{Gal}_K(P)$ s'identifie à un sous-groupe de $\mathfrak{S}(X_P)$. Si $P$ est séparable, alors $|X_P| = n$, et de plus $\mathrm{Dec}_K(P)/K$ est galoisienne. On a alors

$$[\mathrm{Dec}_K(P) : K] = |\mathrm{Gal}_K(P)| \mid |\mathfrak{S}(X_P)|,$$

ce qui est exactement le résultat souhaité.

(3) Supposons que $P$ soit irréductible. On peut toujours supposer $P$ unitaire. Soient $\alpha, \beta \in \mathrm{Dec}_K(P)$ deux racines de $P$. Puisque $P$ est irréductible unitaire, on a $\mu_{\alpha,K} = P$. D'après le théorème I.3.1, il existe un plongement $\sigma_\beta : K(\alpha) \longrightarrow \overline{K}$ tel que $\sigma_\beta(\alpha) = \beta$. Ce plongement se prolonge alors en un plongement $\sigma : \mathrm{Dec}_K(P) \longrightarrow \overline{K}$. Comme $\mathrm{Dec}_K(P)/K$ est une extension normale, $\sigma \in \mathrm{Gal}_K(P)$. Par construction, $\sigma(\alpha) = \beta$, et l'action de $\mathrm{Gal}_K(P)$ est bien transitive.

Supposons maintenant que $P$ soit séparable. Si $P$ n'est pas irréductible, il possède au moins deux facteurs irréductibles unitaires distincts $Q_1$ et $Q_2$. Pour $i = 1, 2$, soit $X_i$ l'ensemble des racines de $Q_i$ dans $\mathrm{Dec}_K(P)$. Par hypothèse sur $P$, ces deux sous-ensembles sont disjoints. Par (1), tout élément de $\mathrm{Gal}_K(P)$ stabilise $X_i$. On en déduit que l'orbite de toute racine de $Q_i$ est contenue dans $X_i$. En particulier, les orbites d'une racine de $Q_1$ et d'une racine de $Q_2$ sont distinctes, et l'action de $\mathrm{Gal}_K(P)$ n'est pas transitive.

Cela achève la démonstration. □

Remarque IV.3.6. Le point (2) montre en particulier que, pour tout polynôme séparable $P \in K[X]$ de degré $n$, on a $[\mathrm{Dec}_K(P) : K] \leq n!$. La remarque IV.3.4 entraîne que cette borne ne peut être améliorée en général.

Le lemme précédent montre que l'on a un morphisme injectif

$$\begin{aligned} \mathrm{Gal}_K(P) &\longrightarrow \mathfrak{S}(X_P) \\ \sigma &\longmapsto \sigma_{|X_P}. \end{aligned}$$

On continue maintenant par un résultat qui détermine sous quelles conditions l'image de ce morphisme est incluse dans $\mathfrak{A}(X_P)$.

Théorème IV.3.7. *Soit $P \in K[X]$ un polynôme séparable de degré $n \geq 1$. Alors, l'extension $K\big(\sqrt{\mathrm{disc}(P)}\big)/K$ est une sous-extension de $\mathrm{Dec}_K(P)/K$. De plus, si $X_P$ est l'ensemble des racines de $P$ dans $\overline{K}$, l'image du morphisme injectif*

$$\begin{aligned} \mathrm{Gal}_K(P) &\longrightarrow \mathfrak{S}(X_P) \\ \sigma &\longmapsto \sigma_{|X_P} \end{aligned}$$

*est incluse dans* $\mathfrak{A}(X_P)$ *si, et seulement si,* $\operatorname{disc}(P) \in K^{\times 2}$.

*Démonstration.* Soit $a_n \in K^\times$ le coefficient dominant de $P$, et soient

$$\alpha_1, \dots, \alpha_n \in \operatorname{Dec}_K(P)$$

les racines de $P$. Par définition, l'élément

$$\gamma = a_n^{n-1} \prod_{i<j} (\alpha_j - \alpha_i) \in \operatorname{Dec}_K(P)$$

vérifie $\gamma^2 = \operatorname{disc}(P)$. On a donc bien $K\big(\sqrt{\operatorname{disc}(P)}\big) \subset \operatorname{Dec}_K(P)$.

Pour tout $\sigma \in \operatorname{Gal}_K(P)$, posons $M_\sigma = \big(\sigma(\alpha_j)^{i-1}\big)_{i,j}$. Cette matrice étant une matrice de Vandermonde, on a

$$\sigma(\gamma) = a_n^{n-1} \prod_{i<j} \big(\sigma(\alpha_j) - \sigma(\alpha_i)\big) = a_n^{n-1} \det(M_\sigma)$$

pour tout $\sigma \in \operatorname{Gal}_K(P)$. Remarquons que pour tout $\sigma \in \operatorname{Gal}_K(P)$, la permutation $\sigma_{|X_P}$ induit une permutation des colonnes de $M_{\mathrm{Id}}$. La matrice obtenue n'étant rien d'autre que $M_\sigma$, on en déduit l'égalité

$$\det(M_\sigma) = \varepsilon(\sigma_{|X_P}) \det(M_{\mathrm{Id}}), \quad \text{pour tout } \sigma \in \operatorname{Gal}_K(P).$$

Autrement dit, on a

$$\sigma(\gamma) = \varepsilon(\sigma_{|X_P})\gamma, \quad \text{pour tout } \sigma \in \operatorname{Gal}_K(P).$$

Comme $\gamma \neq 0$ (puisque $P$ est séparable), l'image du morphisme injectif

$$\begin{aligned} \operatorname{Gal}_K(P) &\longrightarrow \mathfrak{S}(X_P) \\ \sigma &\longmapsto \sigma_{|X_P} \end{aligned}$$

est donc incluse dans $\mathfrak{A}(X_P)$ si, et seulement si, $\gamma$ est fixe par tout élément de $\operatorname{Gal}_K(P)$. D'après le lemme IV.2.10, cela est équivalent à $\gamma \in K^\times$ Cela revient à dire que $\operatorname{disc}(P) \in K^{\times 2}$. Cela achève la démonstration. □

Remarque IV.3.8. Soit $P \in K[X]$ un polynôme **irréductible** séparable de degré $n$. Après le choix d'une numérotation des racines de $P$, les résultats précédents montrent que le groupe $\operatorname{Gal}_K(P)$ s'identifie à un sous-groupe transitif de $\mathfrak{S}_n$ (i.e. un sous-groupe agissant transitivement sur $[\![1, n]\!]$), voire même à un sous-groupe transitif de $\mathfrak{A}_n$ si $\operatorname{disc}(P) \in K^{\times 2}$.

Ce simple fait limite donc les possibilités pour $\operatorname{Gal}_K(P)$ (même si le nombre de sous-groupes transitifs de $\mathfrak{S}_n$ peut être très grand). Par exemple, si $P$ est un polynôme irréductible séparable de degré 5, il n'y a que cinq possibilités à isomorphisme près.

Nous allons maintenant expliquer comment la réduction modulo $p$ peut permettre d'obtenir des renseignements sur le groupe de Galois d'un polynôme unitaire $P \in \mathbb{Z}[X]$.

THÉORÈME IV.3.9. *(admis) Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire, soit $p$ un nombre premier, et soit $\overline{P} \in \mathbb{F}_p[X]$ sa réduction modulo $p$. On suppose que $\overline{P}$ est séparable. Alors, il existe un morphisme de groupes injectif*

$$\mathrm{Gal}_{\mathbb{F}_p}(\overline{P}) \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(P).$$

*De plus, si $d_1, \ldots, d_r$ sont les degrés des facteurs irréductibles unitaires de $\overline{P}$, alors $\mathrm{Gal}_{\mathbb{Q}}(P)$ contient une permutation de type $(d_1, \ldots, d_r)$.*

EXEMPLE IV.3.10. Soit $P = X^5 - X - 1 \in \mathbb{Q}[X]$.

En listant les polynômes irréductibles unitaires de degré 2 et 3 de $\mathbb{F}_5[X]$, et en vérifiant qu'aucun d'entre eux ne divise $P$, on constate que $P$ est irréductible modulo 5. De plus, $\overline{P}$ est séparable modulo 5. Ainsi, $\mathrm{Gal}_{\mathbb{Q}}(P)$ (identifié à un sous-groupe de $\mathfrak{S}_5$ après le choix d'une numérotation de ses racines) contient un 5-cycle.

De plus, on a

$$X^5 - X - \overline{1} = (X^2 + X + \overline{1})(X^3 + X^2 + \overline{1}) \in \mathbb{F}_2[X].$$

Le groupe $\mathrm{Gal}_{\mathbb{Q}}(P)$ contient donc une permutation de type $(2, 3)$. Le cube de cette permutation est donc une transposition. Finalement, $\mathrm{Gal}_{\mathbb{Q}}(P)$ s'identifie à un sous-groupe de $\mathfrak{S}_5$ contenant un 5-cycle et une transposition. Or, il est bien connu que $\mathfrak{S}_p$ est engendré par un $p$-cycle et une transposition arbitraires lorsque $p$ est premier.

Par conséquent, $\mathrm{Gal}_{\mathbb{Q}}(P) \simeq \mathfrak{S}_5$.

Le reste de ce chapitre est consacré à l'étude de quelques familles d'extensions galoisiennes.

## IV.4. Corps finis

Comme on l'a déjà vu dans l'exemple IV.2.3 (2), si $q$ est une puissance d'un nombre premier $p$ et $d \geq 1$, l'extension $\mathbb{F}_{q^d}/\mathbb{F}_q$ est galoisienne.

La proposition suivante donne son groupe de Galois.

PROPOSITION IV.4.1. *Soit $q \geq 2$ une puissance d'un nombre premier $p$. Alors, pour tout $d \geq 1$, le groupe $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ est cyclique d'ordre $d \geq 1$, engendré par l'automorphisme de Frobenius*

$$\begin{aligned} \sigma \colon \mathbb{F}_{q^d} &\longrightarrow \mathbb{F}_{q^d} \\ x &\longmapsto x^q. \end{aligned}$$

*Démonstration.* Commençons par montrer que $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$. Comme $q$ est une puissance d'un nombre premier $p$, qui est la caractéristique de $\mathbb{F}_q$ et de $\mathbb{F}_{q^d}$, $\sigma$ est un morphisme d'anneaux. C'est donc un isomorphisme, puisque $\sigma$ est une application injective et $\mathbb{F}_{q^d}$ est fini. Enfin, on a $\sigma(x) = x$ pour tout $x \in \mathbb{F}_q$. Cela implique facilement que $\sigma$ est $\mathbb{F}_q$-linéaire.

Soit $m \geq 1$ l'ordre de $\sigma$. On a alors

$$\sigma^m = \mathrm{Id}_{\mathbb{F}_{q^d}} \quad \Longleftrightarrow \quad x^{q^m} = x, \quad \text{pour tout } x \in \mathbb{F}_{q^d}.$$

En particulier, le polynôme $X^{q^m} - X \in \mathbb{F}_q[X]$ de degré $q^m$ possède au moins $q^d$ racines, et ainsi $m \geq d$. D'autre part, on a aussi $\sigma^d = \mathrm{Id}_{\mathbb{F}_q}$ car $x^{q^d} = x$ pour tout $x \in \mathbb{F}_{q^d}$. Ainsi, $\sigma$ est d'ordre $d$.

Comme $\mathbb{F}_{q^d}/\mathbb{F}_q$ est galoisienne de degré $d$, son groupe de Galois est d'ordre $d$ (cf. lemme IV.2.1), ce qui permet de conclure. □

## IV.5. Extensions cyclotomiques

Soit $n \geq 1$ un entier, et soit $K$ un corps. On suppose que $\mathrm{car}(K) \nmid n$. Le polynôme $P = X^n - 1 \in K[X]$ est alors séparable.

En effet, on a $P' = nX^{n-1}$. L'hypothèse sur $K$ montre que $P' \neq 0$, et donc que $X$ est le seul facteur irréductible unitaire de $P'$. Or, $X \nmid P$. Ainsi, $P$ et $P'$ sont premiers entre eux et $P$ est séparable par le lemme III.3.2. L'ensemble

$$\mu_n(\overline{K}) = \{x \in \overline{K} \mid x^n = 1\}$$

est donc un sous-groupe de $\overline{K}^\times$ d'ordre $n$. Il est donc cyclique.

Définition IV.5.1. Soit $n \geq 1$ un entier, et soit $K$ un corps. On suppose que l'on a $\mathrm{car}(K) \nmid n$.

Un élément de $\mu_n(\overline{K})$ est appelé une *racine $n$-ième de l'unité*.

On dit que $\zeta \in \overline{K}$ est une *racine primitive $n$-ième de l'unité* si c'est un générateur de $\mu_n(\overline{K})$, i.e. si c'est un élément de $\overline{K}^\times$ d'ordre $n$.

Dans ce cas, si $\zeta \in \overline{K}$ est une racine primitive $n$-ième de l'unité, alors les racines primitives $n$-ièmes de l'unité sont les éléments [1]

$$\zeta^m, \quad m \in \mathbb{Z}, \ \mathrm{pgcd}(m, n) = 1.$$

Exemple IV.5.2. Si $K = \mathbb{Q}$, alors $\zeta_n = e^{\frac{2i\pi}{n}}$ est une racine primitive $n$-ième de l'unité.

1. Bien entendu, on peut se restreindre à $m \in [\![0, n-1]\!]$.

Remarque IV.5.3. Si $\zeta \in \overline{K}$ est une racine primitive $n$-ième de l'unité, on a

$$X^n - 1 = \prod_{k=0}^{n-1} (X - \zeta^k),$$

puisque $\zeta$ engendre $\mu_n(\overline{K})$, qui est exactement l'ensemble des racines du polynôme $X^n - 1$ dans $\overline{K}$.

On va maintenant étudier les extensions engendrées par une racine primitive $n$-ième de l'unité, notée $\zeta_n$ dans la suite.

D'après ce qui précède, $K(\zeta_n)/K$ est le corps des racines de $X^n - 1$, qui est un polynôme séparable. L'extension $K(\zeta_n)/K$ est donc galoisienne par la remarque IV.3.2. En particulier, elle ne dépend pas de la racine primitive choisie (puisqu'en fait elle les contient toutes).

Théorème IV.5.4. *Soit $n \geq 1$ un entier. Soit $K$ un corps tel que $\mathrm{car}(K) \nmid n$, et soit $\zeta_n \in \overline{K}$ une racine primitive $n$-ième de l'unité. Alors, $K(\zeta_n)/K$ est galoisienne, et $\mathrm{Gal}\big(K(\zeta_n)/K\big)$ s'identifie à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$.*

*En particulier, $\mathrm{Gal}\big(K(\zeta_n)/K\big)$ est abélien, d'ordre divisant $\varphi(n)$.*

*Démonstration.* On vient de constater que $K(\zeta_n)/K$ est galoisienne. Pour le reste, il suffit de recopier le début de la démonstration du lemme II.4.10 en remplaçant $\mathbb{Q}$ par $K$ et $\zeta_p$ par $\zeta_n$ pour obtenir un morphisme de groupes injectif $\rho : \mathrm{Gal}\big(K(\zeta_n)/K\big) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.

Le dernier point est alors clair. □

Profitons-en pour introduire une nouvelle définition.

Définition IV.5.5. Soit $K$ un corps. Une extension $L/K$ est dite *abélienne* (resp. *cyclique*), si $L/K$ est galoisienne, et si $\mathrm{Gal}(L/K)$ est un groupe abélien (resp. cyclique).

On dit que $L/K$ est une extension *cyclotomique* s'il existe un entier $n \geq 1$ tel que $\mathrm{car}(K) \nmid n$ et $L = K(\zeta_n)$.

Exemple IV.5.6. D'après le théorème précédent, toute extension cyclotomique est abélienne.

Il peut être assez délicat de déterminer $[K(\zeta_n) : K]$ et $\mathrm{Gal}\big(K(\zeta_n)/K\big)$ en général (le cas $K = \mathbb{Q}$ est déjà non trivial, comme on va le voir). En revanche, lorsque $K$ est un corps fini, on a une réponse complète, donnée par la proposition suivante.

Proposition IV.5.7. *Soit $q \geq 2$ une puissance d'un nombre premier. On suppose que $q$ est premier à $n$. Soit $d$ l'ordre de $\overline{q} \in (\mathbb{Z}/n\mathbb{Z})^\times$.*

*Alors, $\mathbb{F}_q(\zeta_n) \simeq \mathbb{F}_{q^d}$, et le groupe $\mathrm{Gal}\big(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q\big)$ est isomorphe au sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$ engendré par $\overline{q}$.*

*Démonstration.* Puisque $\mathbb{F}_q(\zeta_n)$ est un corps fini, la proposition IV.4.1 montre que $\mathrm{Gal}\big(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q\big)$ est cyclique, engendré par

$$\begin{aligned} \sigma_q \colon \mathbb{F}_q(\zeta_n) &\longrightarrow \mathbb{F}_q(\zeta_n) \\ x &\longmapsto x^q. \end{aligned}$$

Si $\rho : \mathrm{Gal}\big(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q\big) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ est le morphisme injectif défini dans la démonstration du théorème précédent, on a donc $\rho(\sigma_q) = \overline{q}$. Ainsi, on obtient un isomorphisme

$$\mathrm{Gal}\big(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q\big) \simeq \langle \overline{q} \rangle.$$

En particulier, on a

$$[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = |\mathrm{Gal}\big(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q\big)| = d.$$

Mais alors, $\mathbb{F}_q(\zeta_n)$ est un corps à $q^d$ éléments, donc isomorphe à $\mathbb{F}_{q^d}$. □

On s'occupe maintenant du cas $K = \mathbb{Q}$. Pour cela, on a besoin d'introduire les polynômes cyclotomiques.

**Notation.** Si $n \geq 1$ est un entier, on note $\mathbb{U}_n$ le sous-groupe de $\mathbb{C}^\times$ constitué des racines $n$-ièmes de l'unité, à savoir

$$\mathbb{U}_n = \{\zeta \in \mathbb{C}^\times \mid \zeta^n = 1\}.$$

On note aussi $\mathbb{U}_n^*$ l'ensemble des éléments de $\mathbb{U}_n$ d'ordre $n$.

Autrement dit, on a

$$\mathbb{U}_n = \left\{ e^{\frac{2ik\pi}{n}} \mid k \in [\![0, n-1]\!] \right\} = \left\langle e^{\frac{2i\pi}{n}} \right\rangle.$$

Puisque $\mathbb{U}_n$ est cyclique d'ordre $n$, engendré par $e^{\frac{2i\pi}{n}}$, on a

$$\mathbb{U}_n^* = \left\{ e^{\frac{2ik\pi}{n}} \mid k \in [\![0, n-1]\!],\ \mathrm{pgcd}(k, n) = 1 \right\}.$$

Remarquons que, par définition de la fonction indicatrice d'Euler, on a

$$|\mathbb{U}_n^*| = \varphi(n), \qquad \text{pour tout } n \geq 1.$$

Définition IV.5.8. Soit $n \geq 1$ un entier. Le *$n$-ième polynôme cyclotomique* est le polynôme de $\mathbb{C}[X]$ défini par

$$\Phi_n = \prod_{\zeta \in \mathbb{U}_n^*} (X - \zeta) \in \mathbb{C}[X].$$

C'est un polynôme unitaire de degré $\varphi(n)$.

Exemples IV.5.9. (1) On a clairement $\Phi_1 = X - 1$ et $\Phi_2 = X + 1$.

(2) Soit $p$ un nombre premier. Alors, on a $\mathbb{U}_p^* = \mathbb{U}_p \setminus \{1\}$, puisque tout entier $k \in [\![1, p-1]\!]$ est premier à $p$. On a donc $X^p - 1 = (X-1)\Phi_p$, d'où
$$\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Nous allons maintenant démontrer quelques propriétés des polynômes cyclotomiques. On commence par démontrer que ce sont en fait des polynômes à coefficients entiers.

Lemme IV.5.10. *Pour tout $n \geq 1$, on a*
$$X^n - 1 = \prod_{d|n} \Phi_d.$$

*Démonstration.* Montrons que $\mathbb{U}_n$ est l'union disjointe des ensembles $\mathbb{U}_d^*$ lorsque $d \mid n$. Clairement, tout élément de $\mathbb{U}_d^*$ est aussi une racine $n$-ième de l'unité, et l'on a
$$\bigcup_{d|n} \mathbb{U}_d^* \subset \mathbb{U}_n.$$

Inversement, si $\zeta \in \mathbb{U}_n$, et si $d$ est l'ordre de $\zeta$ dans $\mathbb{C}^\times$, on a $d \mid n$. En particulier, $\zeta^d = 1$ et $\zeta \in \mathbb{U}_d$. Mais, $\zeta$ étant d'ordre $d$, on a $\zeta \in \mathbb{U}_d^*$.

On a donc bien
$$\mathbb{U}_n = \bigcup_{d|n} \mathbb{U}_d^*.$$

Remarquons maintenant que les éléments de $\mathbb{U}_d^*$ sont d'ordre $d$ dans $\mathbb{C}^\times$, donc les ensembles $\mathbb{U}_d^*$, $d \mid n$ sont deux à deux disjoints. On a alors
$$X^n - 1 = \prod_{\zeta \in \mathbb{U}_n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mathbb{U}_d^*} (X - \zeta) = \prod_{d|n} \Phi_d.$$

Cela achève la démonstration. □

Corollaire IV.5.11. *Pour tout $n \geq 1$, $\Phi_n \in \mathbb{Z}[X]$.*

*Démonstration.* Pour tout $n \geq 1$, on note $(H_n)$ la propriété suivante :

$(H_n)$ Pour tout $m \in [\![1, n]\!]$, $\Phi_m$ est un polynôme unitaire de $\mathbb{Z}[X]$.

Clairement, $(H_1)$ est vraie puisque $\Phi_1 = X - 1 \in \mathbb{Z}[X]$ et est unitaire. Supposons maintenant que $(H_n)$ soit vraie pour un entier $n \geq 1$, et

montrons $(H_{n+1})$. Il reste à démontrer que $\Phi_{n+1} \in \mathbb{Z}[X]$ et est unitaire. Par le lemme IV.5.10, on a

$$X^{n+1} - 1 = \Phi_{n+1} \prod_{d|n+1, d<n+1} \Phi_d.$$

Comme les diviseurs stricts de $n+1$ sont inférieurs ou égaux à $n$, l'hypothèse de récurrence montre que le polynôme $Q = \prod_{d|n+1, d<n+1} \Phi_d$ est un polynôme unitaire de $\mathbb{Z}[X]$. On peut alors effectuer la division de $X^{n+1} - 1$ par $Q$ dans $\mathbb{Z}[X]$. Mais le quotient et le reste de cette division, qui sont des polynômes de $\mathbb{Z}[X]$, sont aussi le quotient et le reste de la division dans $\mathbb{C}[X]$. Par unicité, ce quotient est $\Phi_{n+1}$, on a donc que $\Phi_{n+1} \in \mathbb{Z}[X]$ et est unitaire car $Q$ et $X^{n+1} - 1$ le sont. Cela achève la récurrence, ainsi que la démonstration. □

Théorème IV.5.12. *Pour tout $n \geq 1$, le polynôme $\Phi_n$ est irréductible dans les anneaux $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.*

*Démonstration.* La démonstration qui suit est due à Landau.

Il suffit de démontrer l'irréductibilité de $\Phi_n$ dans l'anneau $\mathbb{Z}[X]$, puisque $\mathbb{Z}$ est factoriel et $\Phi_n$ est unitaire, donc primitif.

Puisque $\Phi_n$ est unitaire, le coefficient dominant d'un facteur irréductible $P$ de $\Phi_n$ dans $\mathbb{Z}[X]$ est inversible dans $\mathbb{Z}$, donc égal à $\pm 1$. Quitte à remplacer $P$ par $-P$, on peut supposer $P$ unitaire. Il est en particulier non constant.

Pour tout $k \geq 0$, on note $R_k$ le reste de la division de $P(X^k)$ par $P$. En particulier, $\deg(R_k) < \deg(P)$ pour tout $k \geq 0$. Remarquons que $R_k$ est aussi le reste de la division de $P(X^k) - P(X)^k$ par $P$. Enfin, si $\zeta \in \mathbb{U}_n^*$ est une racine de $P$, on a $P(\zeta^k) = R_k(\zeta)$, puisque $P(X^k) - R_k$ est un multiple de $P$.

On commence par montrer que si l'on écrit $k = qn + s$, avec $s \in [\![0, n-1]\!]$, alors $R_k = R_s$.

Comme $\zeta^n = 1$, on a $\zeta^k = \zeta^s$, et par suite

$$R_k(\zeta) = P(\zeta^k) = P(\zeta^s) = R_s(\zeta).$$

Ainsi, $R_k - R_s$ s'annule en toute racine de $P$. Or, $\Phi_n$ étant à racines simples, il en est de même de $P$, et on en conclut que $P \mid R_k - R_s$. Or, on a

$$\deg(R_k - R_s) < \deg(P),$$

et donc nécessairement $R_k - R_s = 0$, soit $R_k = R_s$.

Avant de continuer, remarquons que pour tout nombre premier $p$, et tout polynôme $Q \in \mathbb{F}_p[X]$, on a $Q(X^p) = Q(X)^p \in \mathbb{F}_p[X]$.

En effet, puisque $\mathbb{F}_p[X]$ est de caractéristique $p$, si $Q = \overline{a}_d X^d + \cdots + \overline{a}_1 X + \overline{a}_0$, on a

$$Q(X)^p = \overline{a}_d^p X^{dp} + \cdots + \overline{a}_1^p X^p + \overline{a}_0^p,$$

et le petit théorème de Fermat donne alors

$$Q(X)^p = \overline{a}_d X^{dp} + \cdots + \overline{a}_1 X^p + \overline{a}_0 = Q(X^p).$$

Dans $\mathbb{Z}[X]$, cette identité se retraduit de la manière suivante : pour tout polynôme $S \in \mathbb{Z}[X]$, on a $S(X^p) - S(X)^p \in p\mathbb{Z}[X]$.

Cela étant dit, soit $\ell \geq 1$ un entier majorant les valeurs absolues de tous les coefficients des polynômes $R_0, \ldots, R_{n-1}$. Fixons un nombre premier $p > \ell$. Alors, $P(X^p) - P(X)^p \in p\mathbb{Z}[X]$ d'après ce qui précède. Mais alors, le reste de la division de $P(X^p) - P(X)^p$ par $P$ est aussi dans $p\mathbb{Z}[X]$. Autrement dit, $R_p \in p\mathbb{Z}[X]$. En effet, si l'on écrit $P(X^p) - P(X)^p = pS,\ S \in \mathbb{Z}[X]$, le reste de la division de $P(X^p) - P(X)^p$ par $P$ est égal à $p$ fois le reste de la division de $S$ par $P$, par unicité du reste.

Or, d'après le premier point, $R_p = R_s$ pour un certain entier $s \in [\![0, n-1]\!]$. Si $R_p$ était non nul, il aurait un coefficient de valeur absolue $\geq p$, ce qui contredit le choix de $p$. Par conséquent, $R_p = 0$, d'où $P \mid (P(X^p) - P(X)^p)$, ou encore $P \mid P(X^p)$ pour tout $p > \ell$. Il en découle que, pour tout nombre premier $p > \ell$, et pour toute racine $\zeta \in \mathbb{U}_n^*$ de $P$, $\zeta^p$ est aussi une racine de $P$.

Une récurrence facile montre que pour tout entier $m \geq 1$ dont tous les facteurs premiers sont $> \ell$, et pour toute racine $\zeta \in \mathbb{U}_n^*$ de $P$, $\zeta^m$ est une racine de $P$. Notons qu'a priori, rien ne garantit que $\zeta^m$ soit d'ordre $n$.

Fixons maintenant $\zeta_0 \in \mathbb{U}_n^*$ une racine de $P$. Soit $k \in [\![1, n]\!]$ un entier premier à $n$. Soit $q$ le produit de tous les nombres premiers $p \leq \ell$ ne divisant pas $k$, et soit $m = nq + k$. Soit $p$ un nombre premier $\leq \ell$. Si $p \mid k$, alors $p \nmid q$ par définition, et $p \nmid n$, car $k$ et $n$ sont premiers entre eux. Ainsi, on a $p \nmid nq$, car $p$ est premier, et donc $p \nmid m$. Si $p \nmid k$, alors on a $p \mid q$, et donc $p \mid nq$. Par conséquent, $p \nmid m$ dans ce cas également. Autrement dit, tous les diviseurs premiers de $m$ sont $> \ell$.

D'après le premier point, $\zeta_0^m$ est une racine de $P$. Comme $m = nq+k$, on en déduit que $\zeta_0^k$ est une racine de $P$, et cela pour tout entier $k \in [\![1, n]\!]$ premier à $n$. Or, comme $\zeta_0$ est d'ordre $n$, les divers éléments

$$\zeta_0^k, \quad k \in [\![1, n]\!]\,,\ \operatorname{pgcd}(k, n) = 1$$

sont $\varphi(n)$ éléments de $\mathbb{U}_n^*$ deux à deux distincts, et décrivent donc $\mathbb{U}_n^*$ tout entier. Il s'ensuit que $\Phi_n \mid P$, d'où $P = \Phi_n$, car $P$ et $\Phi_n$ sont tous deux unitaires. On en conclut que $\Phi_n$ est irréductible dans $\mathbb{Z}[X]$, ce qui achève la démonstration. □

Puisque $\Phi_n \in \mathbb{Q}[X]$ est irréductible, unitaire et annule $\zeta_n$, on a le résultat suivant.

Corollaire IV.5.13. *Pour tout $n \geq 1$, on a $\mu_{\zeta_n,\mathbb{Q}} = \Phi_n$.*

On a alors le théorème suivant.

Théorème IV.5.14. *Soit $n \geq 1$. L'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne de degré $\varphi(n)$. De plus,*

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big) \simeq (\mathbb{Z}/n\mathbb{Z})^\times.$$

*Plus précisément, pour tout $m \in \mathbb{Z}$ premier à $n$, il existe un unique $\sigma_m \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ tel que $\sigma_m(\zeta_n) = \zeta_n^m$.*

*Réciproquement, tout élément de $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ est de la forme $\sigma_m$, où $m$ est un entier premier à $n$, unique modulo $n$.*

*Enfin, l'application*

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})\\ \overline{m} &\longmapsto \sigma_m\end{aligned}$$

*est un isomorphisme de groupes.*

*Démonstration.* La première partie découle immédiatement du corollaire précédent. Pour le reste, il suffit de recopier la démonstration du lemme II.4.10, par exemple, ou de constater que le morphisme de groupes injectif introduit dans la démonstration du théorème IV.5.4 est bijectif, en comparant les ordres des deux groupes en jeu. □

La définition des polynômes cyclotomiques n'est pas très efficace pour pouvoir les calculer. À titre d'exercice, le lecteur pourra démontrer successivement les propriétés suivantes.

(1) Pour tous entiers $n$, $m \geq 1$ distincts, les polynômes $\Phi_n$ et $\Phi_m$ sont premiers entre eux dans $\mathbb{Q}[X]$ et $\mathbb{C}[X]$.
(2) Si $p \nmid n$, on a $\Phi_n(X)\Phi_{np}(X) = \Phi_n(X^p)$.
(3) Si $p \mid n$, on a $\Phi_{np}(X) = \Phi_n(X^p)$.
(4) Si $n \geq 3$ est impair, on a $\Phi_{2n}(X) = \Phi_n(-X)$.

(5) Pour tout $p$ premier, tout $n$ premier à $p$, et tout $r \geq 1$, on a

$$\Phi_{np^r} = \frac{\Phi_n(X^{p^r})}{\Phi_n(X^{p^{r-1}})}.$$

En particulier, on a

$$\Phi_{p^r} = \Phi_p(X^{p^{r-1}}) = X^{(p-1)p^{r-1}} + X^{(p-2)p^{r-1}} + \cdots + X^{p^{r-1}} + 1.$$

(6) Pour tout $n \geq 3$ impair, et tout $r \geq 1$, on a

$$\Phi_{2^r n} = \Phi_n(-X^{2^{r-1}}).$$

Ces deux dernières formules permettent de calculer $\Phi_n$ de proche en proche en connaissant la décomposition en facteurs premiers de $n$.

Pour achever cette section, nous allons étudier le comportement des extensions $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ par composition et par intersection. Puisque l'extension cyclotomique $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ne dépend pas du choix de la racine $n$-ième de l'unité, on peut supposer que $\zeta_n = e^{\frac{2i\pi}{n}}$, ce que l'on fera implicitement dans la suite.

Théorème IV.5.15. *Soient $m, n \geq 1$ deux entiers. Alors, on a*

$$\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_D) \quad \text{et} \quad \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d),$$

*où $d = \mathrm{pgcd}(m, n)$ et $D = \mathrm{ppcm}(m, n)$.*

*Démonstration.* Écrivons $D = rm = sn$, avec $r$ et $s$ premiers entre eux.

D'une part, on a $\zeta_m = \zeta_D^r$ et $\zeta_n = \zeta_D^s$. Ainsi, on a $\zeta_m, \zeta_n \in \mathbb{Q}(\zeta_D)$. Par conséquent, on obtient

$$\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\zeta_D).$$

D'autre part, il existe $u, v \in \mathbb{Z}$ tels que $ur + vs = 1$. On a alors

$$\zeta_D = (\zeta_D^r)^u (\zeta_D^s)^v = \zeta_m^u \zeta_n^v \in \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n).$$

Ainsi, on a $\mathbb{Q}(\zeta_D) \subset \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$, d'où la première égalité.

Posons $K = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. Écrivons $m = kd$ et $n = \ell d$, avec $k$ et $\ell$ premiers entre eux.

On a alors

$$\zeta_d = \zeta_m^k \in \mathbb{Q}(\zeta_m),$$

ainsi que

$$\zeta_d = \zeta_n^\ell \in \mathbb{Q}(\zeta_n).$$

On en déduit que $\mathbb{Q}(\zeta_d) \subset \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. Comme les extensions $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ et $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ sont galoisiennes, $\mathbb{Q}(\zeta_m)/K$ et $\mathbb{Q}(\zeta_n)/K$ sont linéairement disjointes par la proposition IV.2.11. On a alors

$$[\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) : K] = [\mathbb{Q}(\zeta_D) : K] = [\mathbb{Q}(\zeta_m) : K][\mathbb{Q}(\zeta_n) : K].$$

En multipliant par $[K : \mathbb{Q}]^2$, et en utilisant la formule de multiplicativité des degrés, on obtient

$$\varphi(D)[K : \mathbb{Q}] = \varphi(m)\varphi(n).$$

Comme $[K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta_d)][\mathbb{Q}(\zeta_d) : \mathbb{Q}]$, on obtient finalement

$$[K : \mathbb{Q}(\zeta_d)] = \frac{\varphi(m)\varphi(n)}{\varphi(d)\varphi(D)}.$$

Il nous faut donc démontrer que cette dernière quantité est égale 1.

Soit $T_1$ l'ensemble des diviseurs premiers de $m$, et $T_2$ l'ensemble des diviseurs premiers de $n$. On a donc

$$\varphi(m) = m \prod_{p \in T_1} \Big(1 - \frac{1}{p}\Big) \quad \text{et} \quad \varphi(n) = n \prod_{p \in T_2} \Big(1 - \frac{1}{p}\Big),$$

ainsi que

$$\varphi(d) = d \prod_{p \in T_1 \cap T_2} \Big(1 - \frac{1}{p}\Big) \quad \text{et} \quad \varphi(D) = D \prod_{p \in T_1 \cup T_2} \Big(1 - \frac{1}{p}\Big).$$

On a ainsi

$$\varphi(d)\varphi(D) = dD\Big(\prod_{p \in T_1 \cap T_2} \Big(1-\frac{1}{p}\Big)\Big)^2\Big(\prod_{p \in T_1 \setminus T_2} \Big(1-\frac{1}{p}\Big)\Big)\Big(\prod_{p \in T_2 \setminus T_1} \Big(1-\frac{1}{p}\Big)\Big).$$

Mais, on a aussi

$$\varphi(m) = m\Big(\prod_{p \in T_1 \cap T_2} \Big(1 - \frac{1}{p}\Big)\Big)\Big(\prod_{p \in T_1 \setminus T_2} \Big(1 - \frac{1}{p}\Big)\Big),$$

ainsi que

$$\varphi(n) = n\Big(\prod_{p \in T_1 \cap T_2} \Big(1 - \frac{1}{p}\Big)\Big)\Big(\prod_{p \in T_2 \setminus T_1} \Big(1 - \frac{1}{p}\Big)\Big).$$

Par conséquent, on a

$$\varphi(m)\varphi(n) = mn\Big(\prod_{p \in T_1 \cap T_2} \Big(1-\frac{1}{p}\Big)\Big)^2\Big(\prod_{p \in T_1 \setminus T_2} \Big(1-\frac{1}{p}\Big)\Big)\Big(\prod_{p \in T_2 \setminus T_1} \Big(1-\frac{1}{p}\Big)\Big).$$

Comme $mn = dD$, on a l'égalité désirée, ce qui achève la démonstration. $\square$

## IV.6. Théorie de Kummer

Nous allons nous intéresser dans cette section aux extensions cycliques.

Exemples IV.6.1.

(1) Si $q \geq 2$ est une puissance d'un nombre premier, l'extension $\mathbb{F}_{q^d}/\mathbb{F}_q$ est cyclique pour tout $d \geq 1$ $\big($cf. proposition IV.4.1$\big)$.

(2) Pour tout nombre premier $p$ impair, et tout $r \geq 1$, $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$ est cyclique, puisqu'elle est galoisienne, de groupe de Galois isomorphe au groupe $(\mathbb{Z}/p^r\mathbb{Z})^\times$, qui est cyclique.

(3) Soit $K$ un corps, et soit $n \geq 1$ un entier. On suppose que $\mathrm{car}(K) \nmid n$, et que $\mu_n(\overline{K}) \subset K$ (ou ce qui revient au même, que $K$ contient une racine primitive $n$-ième de l'unité).

Soit $a \in K^\times$. Alors, le polynôme $P = X^n - a \in K[X]$ est séparable. En effet, si $\alpha \in \overline{K}$ est une racine de $P$, on a

$$P = \prod_{\zeta \in \mu_n(\overline{K})} (X - \zeta\alpha).$$

Puisque $\mu_n(\overline{K}) \subset K$, on remarque alors que l'extension de $K$ engendrée par une racine de $P$ ne dépend pas de la racine choisie. On note cette extension $K(\sqrt[n]{a})/K$.

Autrement dit, c'est l'extension engendrée par un élément $\alpha \in \overline{K}$ vérifiant $\alpha^n = a$. On écrira d'ailleurs souvent $\alpha = \sqrt[n]{a}$ par abus dans la suite.

Tout ce qui précède montre que $K(\sqrt[n]{a}) = \mathrm{Dec}_K(P)$. Comme $P$ est séparable, $K(\sqrt[n]{a})/K$ est galoisienne par la remarque IV.3.2. De plus, si $\sigma \in \mathrm{Gal}\big(K(\sqrt[n]{a})/K\big)$, on a

$$\sigma(\sqrt[n]{a})^n = \sigma(\sqrt[n]{a}^n) = \sigma(a) = a.$$

Ainsi, $\sigma(\sqrt[n]{a})$ est une racine $P$, et il existe une unique racine $n$-ième de l'unité $\zeta$ telle que $\sigma(\sqrt[n]{a}) = \zeta\sqrt[n]{a}$. On a donc une application

$$\begin{aligned} \varphi\colon \mathrm{Gal}\big(K(\sqrt[n]{a})/K\big) &\longrightarrow \mu_n(\overline{K}) \\ \sigma \qquad\qquad &\longmapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}. \end{aligned}$$

De plus, pour tous $\sigma, \tau \in \mathrm{Gal}\big(K(\sqrt[n]{a})/K\big)$, on a

$$\begin{aligned}\varphi(\sigma\tau) &= \frac{(\sigma\tau)(\sqrt[n]{a})}{\sqrt[n]{a}}\\ &= \frac{\sigma(\varphi(\tau)\sqrt[n]{a})}{\sqrt[n]{a}}\\ &= \varphi(\tau)\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\\ &= \varphi(\sigma)\varphi(\tau),\end{aligned}$$

l'avant-dernière égalité provenant du fait que $\varphi(\tau) \in \mu_n(\overline{K}) \subset K$. Ainsi, $\varphi$ est un morphisme de groupes. De plus, $\varphi$ est injectif. En effet, si $\sigma \in \mathrm{Gal}\big(K(\sqrt[n]{a})/K\big)$ vérifie $\varphi(\sigma) = 1$, on a $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}$, et par suite $\sigma = \mathrm{Id}$.

Ainsi, $\mathrm{Gal}\big(K(\sqrt[n]{a})/K\big)$ est isomorphe à un sous-groupe du groupe cyclique $\mu_n(\overline{K})$. Par conséquent, $\mathrm{Gal}\big(K(\sqrt[n]{a})/K\big)$ est cyclique d'ordre divisant $n$. En particulier, $[K(\sqrt[n]{a}) : K] \mid n$.

Définition IV.6.2. Une *extension de Kummer* est une extension de corps de la forme $K(\sqrt[n]{a})/K$, où $\mathrm{car}(K) \nmid n$ et $\mu_n(\overline{K}) \subset K$.

Exemple IV.6.3. Soit $K$ un corps de caractéristique différente de 2. Alors, toute extension $L/K$ de degré $\leq 2$ est une extension de Kummer. Autrement dit, si $[L : K] \leq 2$, on a $L = K(\sqrt{d})$, avec $d \in K^\times$.

Ce fait a été déjà établi plus ou moins explicitement lorsque $K = \mathbb{Q}$, mais il est suffisamment essentiel dans les applications pour qu'il soit bon de le souligner encore une fois.

Si $[L : K] = 1$, on a $L = K$ et on peut prendre $d = 1$.

Supposons que $[L : K] = 2$. Alors, $L \neq K$, et l'on peut choisir $\alpha \in L \backslash K$. Comme $\alpha \notin K$, $\mu_{\alpha,K}$ est de degré $\geq 2$. On a alors

$$K \subset K(\alpha) \subset L,$$

et puisque $L$ et $K(\alpha)$ ont même degré sur $K$, on a $L = K(\alpha)$.

Écrivons $\mu_{\alpha,K} = X^2 + aX + b,\ a, b \in K$, et posons $d = a^2 - 4b$. Alors, on a

$$0 = \alpha^2 + a\alpha + b = \left(\alpha + \frac{a}{2}\right)^2 - \frac{d}{4}.$$

Ainsi, $\omega = 2\alpha + a \in L$ et vérifie $\omega^2 = d$. On a alors $K(\omega) \subset K(\alpha)$. Comme on a $\alpha = \dfrac{-a + \omega}{2}$, on obtient aussi $K(\alpha) \subset K(\omega)$, et par conséquent

$$L = K(\alpha) = K(\omega) = K(\sqrt{d}).$$

D'après l'exemple IV.6.1 (3), une extension de Kummer est cyclique. Nous allons démontrer que la réciproque est vraie. Nous aurons besoin d'un théorème dû à Hilbert.

THÉORÈME IV.6.4 (Théorème 90 de Hilbert). *Soit $L/K$ une extension cyclique, et soit $\sigma$ un générateur de* $\mathrm{Gal}(L/K)$.

*Alors, pour tout $x \in L$, on a $N_{L/K}(x) = 1$ si, et seulement si, il existe un élément $y \in L^\times$ tel que $x = \dfrac{y}{\sigma(y)}$.*

*Démonstration.* Soit $n = [L : K]$. Supposons tout d'abord qu'il existe un élément $y \in L^\times$ tel que $x = \dfrac{y}{\sigma(y)}$. Comme $\mathscr{X}(L/K) = \mathrm{Gal}(L/K) = \langle\sigma\rangle$, d'après la proposition III.4.5, on a

$$N_{L/K}(x) = \prod_{k=0}^{n-1} \sigma(x) = \prod_{k=0}^{n-1} \frac{\sigma^k(y)}{\sigma^{k+1}(y)} = \frac{y}{\sigma^n(y)}.$$

Puisque $\sigma^n = \mathrm{Id}_L$, on obtient $N_{L/K}(x) = 1$.

Inversement, si $N_{L/K}(x) = 1$, on a $x$, $\sigma(x), \dots, \sigma^{n-1}(x) \in L^\times$. D'après le corollaire III.1.5, la famille $(\mathrm{Id}_L, \sigma, \dots, \sigma^{n-1})$ est $L$-libre. En particulier, on a

$$\mathrm{Id}_L + x\sigma + \big(x\sigma(x)\big)\sigma^2 + \cdots + \big(x\sigma(x)\cdots\sigma^{n-2}(x)\big)\sigma^{n-1} \neq 0.$$

Il existe donc $z \in L$ tel que

$$y = z + x\sigma(z) + \big(x\sigma(x)\big)\sigma^2(z) + \cdots + \big(x\sigma(x)\dots\sigma^{n-2}(x)\big)\sigma^{n-1}(z) \neq 0.$$

Mais alors, en tenant compte du fait que $\sigma^n = \mathrm{Id}_L$, on obtient

$$\sigma(y) = \sigma(z) + \cdots + \big(\sigma(x)\cdots\sigma^{n-2}(x)\big)\sigma^{n-1}(z) + \big(\sigma(x)\cdots\sigma^{n-1}(x)\big)z.$$

Puisque $x\sigma(x)\cdots\sigma^{n-1}(x) = N_{L/K}(x) = 1$, on a finalement $x\sigma(y) = y$, soit encore $x = \dfrac{y}{\sigma(y)}$. Cela achève la démonstration. □

Nous pouvons maintenant démontrer le résultat principal de cette section.

THÉORÈME IV.6.5 (Kummer). *Soit $n \geq 1$ un entier. Soit $K$ un corps tel que* $\mathrm{car}(K) \nmid n$ *et $\mu_n(\overline{K}) \subset K$. Alors, une extension $L/K$ est cyclique de degré divisant $n$ si, et seulement si, il existe $a \in K^\times$ tel que $L = K(\sqrt[n]{a})$.*

*De plus, pour tous $a$, $b \in K^\times$, on a $K(\sqrt[n]{a}) = K(\sqrt[n]{b})$ si, et seulement si, il existe $m \in \mathbb{Z}$ premier à $n$ et $u \in K^\times$ tels que $b = a^m u^n$.*

*Démonstration.* L'exemple IV.6.1 (3) montre que $K(\sqrt[n]{a})/K$ est cyclique de degré divisant $n$. Réciproquement, soit $L/K$ une extension cyclique de degré $d \mid n$. Par hypothèse, $K$ contient les racines $n$-ièmes de l'unité. Soit $\zeta_d \in \mu_n(\overline{K}) \subset K$ un élément d'ordre $d$. On a alors

$$N_{L/K}(\zeta_d) = \zeta_d^d = 1.$$

Par le théorème 90 de Hilbert, il existe $y \in L^\times$ tel que $\zeta_d = \dfrac{y}{\sigma(y)}$, où $\sigma$ est un générateur de $\mathrm{Gal}(L/K)$. Posons $\alpha = y^{-1}$, si bien que $\zeta_d = \dfrac{\sigma(\alpha)}{\alpha}$. Comme $\zeta_d \in \mu_n(\overline{K})$, on a

$$\zeta_d^n = 1 = \frac{\sigma(\alpha^n)}{\alpha^n},$$

soit $\sigma(\alpha^n) = \alpha^n$. Puisque $\sigma$ engendre $\mathrm{Gal}(L/K)$, on en déduit que $\alpha^n$ est fixe par tout élément du groupe $\mathrm{Gal}(L/K)$. Par le lemme IV.2.10, on a donc $\alpha^n \in K^\times$.

Posons $a = \alpha^n$, et vérifions que $L = K(\alpha) = K(\sqrt[n]{a})$. Bien entendu, on a l'inclusion $K(\sqrt[n]{a}) \subset L$. Par construction, on a $\sigma(\sqrt[n]{a}) = \zeta_d \sqrt[n]{a}$, et par récurrence

$$\sigma^i(\sqrt[n]{a}) = \zeta_d^i \sqrt[n]{a}, \qquad \text{pour tout } i \in [\![0, d-1]\!].$$

Comme $\zeta_d$ est d'ordre $d$, ces éléments dont deux à deux distincts. Comme $L/K$ est cyclique, de groupe de Galois engendré par $\sigma$, les $d$ puissances successives de $\sigma$ sont exactement les plongements de $L/K$. Par le lemme III.2.6, $\sqrt[n]{a}$ est un élément primitif de $L/K$.

Supposons maintenant que $L = K(\sqrt[n]{a}) = K(\sqrt[n]{b})$. Soit $\sigma$ un générateur du groupe $\mathrm{Gal}(L/K)$. D'après l'exemple IV.6.1 (3), il existe $\zeta \in \mu_n(\overline{K})$ tel que

$$\sigma(\sqrt[n]{a}) = \zeta \sqrt[n]{a}.$$

Comme $\sigma$ est d'ordre $d$, des calculs similaires aux précédents montrent que $\zeta$ est d'ordre $d$. De même, il existe $\zeta' \in \mu_n(\overline{K})$ d'ordre $d$ tel que

$$\sigma(\sqrt[n]{b}) = \zeta' \sqrt[n]{b}.$$

Puisque $\mu_d(\overline{K})$ est cyclique[2] d'ordre $d$, il existe donc $r \in \mathbb{Z}$ premier à $d$ tel que $\zeta' = \zeta^r$.

Soit $t$ le produit des nombres premiers $p$ tels que $p \nmid d$ et $p \mid n$. Les entiers $t$ et $d$ étant premiers entre eux, le théorème chinois montre l'existence d'un entier $m \in \mathbb{Z}$ tel que $m \equiv r\ [d]$ et $m \equiv 1\ [t]$.

2. En effet, puisque $\mathrm{car}(K) \nmid n$, on a aussi $\mathrm{car}(K) \nmid d$.

Par construction, l'entier $m$ est premier à $n$ et $m = r + ds,\ s \in \mathbb{Z}$. Mais alors, on a

$$\zeta' = \zeta^{m-ds} = \zeta^m.$$

Par conséquent, on obtient

$$\sigma\Big(\frac{\sqrt[n]{b}}{(\sqrt[n]{a})^m}\Big) = \frac{\zeta^m \sqrt[n]{b}}{\zeta^m(\sqrt[n]{a})^m} = \frac{\sqrt[n]{b}}{(\sqrt[n]{a})^m}.$$

Ainsi, $u = \frac{\sqrt[n]{b}}{(\sqrt[n]{a})^m}$ est fixé par $\sigma$, donc par tout élément de $\mathrm{Gal}(L/K)$. Par conséquent, $u \in K^\times$, et $b = a^m u^n$.

Inversement, si $b = a^m u^n$, avec $m \in \mathbb{Z}$ premier à $n$ et $u \in K^\times$, on a

$$K(\sqrt[n]{b}) = K\big(u(\sqrt[n]{a})^m\big) = K\big((\sqrt[n]{a})^m\big) \subset K(\sqrt[n]{a}).$$

Puisque $m$ est premier à $n$, il existe $k,\ \ell \in \mathbb{Z}$ tels que $km + \ell n = 1$. On a alors $a = (a^m)^k (a^\ell)^n$, et donc

$$u^{nk} a = b^k a^{\ell n},$$

d'où $a = b^k (a^\ell u^{-k})^n$. Comme précédemment, on obtient

$$K(\sqrt[n]{a}) \subset K(\sqrt[n]{b}),$$

d'où l'égalité désirée. Cela achève la démonstration. □

Remarque IV.6.6. Lorsque $n = 2$, la condition $\mu_2(\overline{K}) \subset K$ est automatiquement vérifiée. En tenant compte du fait qu'un entier premier à 2 est de la forme $2k + 1,\ k \in \mathbb{Z}$, on obtient le fait suivant. Pour tout corps $K$ de caractéristique différente de 2, et tous $a,\ b \in K^\times$, on a

$$K(\sqrt{a}) = K(\sqrt{b}) \quad \Longleftrightarrow \quad \text{il existe } u \in K^\times, \text{ tel que } b = au^2,$$

ce que l'on peut démontrer directement.

Chapitre V

# Nul n'est censé ignorer Galois

Ce chapitre au titre empreint d'humour glacé et sophistiqué[1] vise à établir une correspondance bijective entre les sous-groupes de $\mathrm{Gal}(L/K)$ et les sous-extensions de $L/K$ lorsque $L/K$ est galoisienne (correspondance annoncée dans la section II.5), et d'en donner quelques applications classiques.

## V.1. Théorie de Galois

Soit $L/K$ une extension de corps de degré fini. On note $\mathscr{SE}(L/K)$ l'ensemble des sous-extensions de $K$, et $\mathscr{SG}\big(\mathrm{Gal}(L/K)\big)$ l'ensemble des sous-groupes de $\mathrm{Gal}(L/K)$. Le lemme II.4.9 (2) implique que l'on a une application

$$\begin{array}{rcl} \Phi_{L/K}\colon \mathscr{SG}\big(\mathrm{Gal}(L/K)\big) & \longrightarrow & \mathscr{SE}(L/K) \\ H & \longmapsto & L^H/K. \end{array}$$

Notons que l'on peut également définir une application en sens inverse. Si $F/K$ est une sous-extension de $L/K$, le groupe $\mathrm{Gal}(L/F)$ est un sous-groupe de $\mathrm{Gal}(L/K)$, puisque si un automorphisme de $L$ est $F$-linéaire, il est aussi $K$-linéaire. On a donc une application

$$\begin{array}{rcl} \Psi_{L/K}\colon \mathscr{SE}(L/K) & \longrightarrow & \mathscr{SG}\big(\mathrm{Gal}(L/K)\big) \\ F/K & \longmapsto & \mathrm{Gal}(L/F). \end{array}$$

Il est naturel de se demander si ces applications sont bijectives, et inverses l'une de l'autre. Comme on l'a déjà constaté dans l'exemple II.5.1, l'application $\Phi_{L/K}$ n'est pas nécessairement surjective. Néanmoins, nous allons démontrer qu'elle est toujours injective.

Commençons sans plus attendre par le résultat-clef de cette section.

1. Le fabuleux jeu de mots présent dans le titre m'a obligeamment été prêté par mon ex-étudiant Louis-Thibault Gauthier. Dépêchez-vous de rire, il faut que je le lui rende.

Théorème V.1.1 (Lemme d'Artin). *Soit $L$ un corps, et soit $H$ un sous-groupe fini du groupe* $\mathrm{Aut}(L)$ *des automorphismes de l'anneau $L$. Alors, l'extension $L/L^H$ est galoisienne, et l'on a*

$$\mathrm{Gal}(L/L^H) = H.$$

*Démonstration.* Nous allons d'abord établir le fait suivant.

**Fait.** Soit $\alpha \in L$, et soit $S = \{\sigma_1, \ldots, \sigma_r\}$ un sous-ensemble maximal de $H$ tels que $\sigma_1(\alpha), \ldots, \sigma_r(\alpha) \in L$ soient deux à deux distincts [2]. Quitte à remplacer $S$ par $S' = \{\sigma_1^{-1}\sigma_j, j \in [\![1, r]\!]\}$, on peut supposer sans perte de généralité que $\mathrm{Id}_L \in S$ (les $\sigma_1^{-1}\sigma_j(\alpha)$ sont bien deux à deux distincts par injectivité de $\sigma_1^{-1}$).

Alors, $Q_\alpha = \prod_{i=1}^{r} \big(X - \sigma_i(\alpha)\big) \in L^H[X]$, $Q_\alpha$ est séparable sur $L^H$, et l'on a de plus $\mu_{\alpha,L^H} \mid Q_\alpha$.

Gardons les notations précédentes. Pour tout $\sigma \in H$, on a alors

$$\sigma(Q_\alpha) = \prod_{i=1}^{r} \big(X - \sigma\big(\sigma_i(\alpha)\big)\big).$$

Soit $i \in [\![1, r]\!]$. Puisque $H$ est un groupe, on a encore $\sigma\sigma_i \in H$. Par maximalité de $S$, il existe $k \in [\![1, r]\!]$ tel que $\sigma\big(\sigma_i(\alpha)\big) = \sigma_k(\alpha)$.

De plus, par injectivité de $\sigma$, pour tous $i$, $j \in [\![1, r]\!]$, on a

$$\sigma\big(\sigma_i(\alpha)\big) = \sigma\big(\sigma_j(\alpha)\big) \quad \Longrightarrow \quad i = j,$$

puisque les éléments $\sigma_1(\alpha), \ldots, \sigma_r(\alpha)$ sont deux à deux distincts. Autrement dit, $\sigma$ induit une permutation de l'ensemble $\{\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\}$. On en déduit alors que $\sigma(Q_\alpha) = Q_\alpha$ pour tout $\sigma \in H$, ce qui revient à dire que l'on a $Q_\alpha \in L^H[X]$.

Le fait que $Q_\alpha$ soit séparable sur $L^H$ découle alors de sa définition. Enfin, puisque $\mathrm{Id}_L \in S$, on a $Q_\alpha(\alpha) = 0$. Comme $Q_\alpha \in L^H[X]$, on obtient alors $\mu_{\alpha,L^H} \mid Q_\alpha$.

Montrons maintenant le théorème. D'après le fait précédent, dont on garde les notations, pour tout $\alpha \in L$, $\mu_{\alpha,L^H} \mid Q_\alpha$. Comme $Q_\alpha$ est séparable sur $L^H$, il en est de même de $\mu_{\alpha,L^H}$, et $\alpha$ est donc séparable sur $L^H$. Ainsi, l'extension $L/L^H$ est séparable. De plus, puisque $\mu_{\alpha,L^H} \mid Q_\alpha$, on a $[L^H(\alpha) : L^H] \leq \deg(Q_\alpha) \leq |H|$ pour tout $\alpha \in L$.

Montrons que $L/L^H$ est de degré fini $\leq |H|$. Supposons au contraire que $[L : L^H] \geq |H| + 1$ (où $[L : L^H]$ est possiblement infini). Alors, il existe

2. Les éléments $\sigma_1(\alpha), \ldots, \sigma_r(\alpha)$ sont bien dans $L$, puisque $\sigma_i$ est un automorphisme de $L$.

une famille $(\alpha_1, \ldots, \alpha_{|H|+1})$ d'éléments de $L$ qui est $L^H$-libre. Mais alors, l'extension $L^H(\alpha_1, \ldots, \alpha_{|H|+1})/L^H$ est séparable, de degré fini $\geq |H|+1$ (puisque les $\alpha_i$ sont $K$-linéairement indépendants). Par le théorème de l'élément primitif, elle est engendré par un unique élément de $L$. Elle est donc de degré $\leq |H|$ par ce qui précède, d'où une contradiction.

Or, tout élément de $H$ fixe évidemment les éléments de $L^H$, et donc $H \subset \mathrm{Gal}(L/L^H)$. On a ainsi

$$|\mathrm{Gal}(L/L^H)| \geq |H|.$$

Mais on a aussi $|\mathrm{Gal}(L/L^H)| \leq [L : L^H] \leq |H|$ d'après le corollaire III.1.12. On déduit de tout cela que $|\mathrm{Gal}(L/L^H)| = |H|$, ce qui démontre que $L/L^H$ est galoisienne par le lemme IV.2.1, puis que $H = \mathrm{Gal}(L/L^H)$. Cela achève la démonstration. □

Comme corollaire immédiat du lemme d'Artin, on obtient une nouvelle caractérisation des extensions galoisiennes.

Corollaire V.1.2. *Soit $L/K$ une extension de degré fini. Alors, $L/K$ est galoisienne si, et seulement si, $L^{\mathrm{Gal}(L/K)} = K$.*

*Démonstration.* Le sens direct est donné par le lemme IV.2.10. Supposons maintenant que $L^{\mathrm{Gal}(L/K)} = K$. Par le lemme d'Artin, $L/K = L/L^{\mathrm{Gal}(L/K)}$ est galoisienne. □

Le lemme d'Artin nous donne également le résultat suivant.

Proposition V.1.3. *Soit $L/K$ une extension de degré fini. Alors, on a*

$$\Psi_{L/K} \circ \Phi_{L/K} = \mathrm{Id}_{\mathscr{SG}(\mathrm{Gal}(L/K))}.$$

*En particulier, l'application*

$$\begin{array}{rcl} \Phi_{L/K} \colon \mathscr{SG}\big(\mathrm{Gal}(L/K)\big) & \longrightarrow & \mathscr{SE}(L/K) \\ H & \longmapsto & L^H/K \end{array}$$

*est injective.*

*De plus, si $\Phi_{L/K}$ est bijective, alors son inverse est l'application*

$$\begin{array}{rcl} \Psi_{L/K} \colon \mathscr{SE}(L/K) & \longrightarrow & \mathscr{SG}\big(\mathrm{Gal}(L/K)\big) \\ F/K & \longmapsto & \mathrm{Gal}(L/F). \end{array}$$

*Dans ce cas, $L/K$ est nécessairement galoisienne.*

*Démonstration.* L'égalité $\Psi_{L/K} \circ \Phi_{L/K} = \mathrm{Id}_{\mathscr{SG}(\mathrm{Gal}(L/K))}$ découle du lemme d'Artin. Tout le reste de la proposition est alors clair, sauf le dernier point. Supposons que $\Phi_{L/K}$ soit bijective. En particulier, il existe

un sous-groupe $H$ de $\mathrm{Gal}(L/K)$ tel que $L^H = K$. Mais alors, on a

$$K \subset L^{\mathrm{Gal}(L/K)} \subset L^H = K,$$

d'où $L^{\mathrm{Gal}(L/K)} = K$. Le corollaire V.1.2 montre alors que $L/K$ est galoisienne, d'où le résultat. □

Continuons par établir quelques propriétés des applications $\Phi_{L/K}$ et $\Psi_{L/K}$, valables pour toute extension $L/K$ de degré fini.

Lemme V.1.4. *Soit $L/K$ une extension de degré fini. Pour toutes sous-extensions $F_1/K$, $F_2/K$ et $F/K$ de $L/K$, et pour tous sous-groupes $H_1$, $H_2$ et $H$ de $\mathrm{Gal}(L/K)$, on a :*

(1) $\mathrm{Gal}(L/F) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma_{|_F} = \mathrm{Id}_F\}$ ;
(2) $\mathrm{Gal}(L/F_1F_2) = \mathrm{Gal}(L/F_1) \cap \mathrm{Gal}(L/F_2)$ ;
(3) $L^{H_1} \cap L^{H_2} = L^{\langle H_1, H_2\rangle}$ ;
(4) *pour tout $\sigma \in \mathrm{Gal}(L/K)$, on a $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$.*

*Démonstration.* Gardons les notations du lemme.

Si $\sigma \in \mathrm{Gal}(L/F)$ est $F$-linéaire, elle est $K$-linéaire et donc $\sigma \in \mathrm{Gal}(L/K)$. De plus, $\sigma$ fixe les éléments de $F$, puisque pour tout $x \in F$, on a

$$\sigma(x) = \sigma(x1) = x\sigma(1) = x1 = x.$$

Inversement, si $\sigma \in \mathrm{Gal}(L/K)$ et fixe les éléments de $F$, $\sigma$ est $F$-linéaire. En effet, c'est un morphisme de groupes additifs, et de plus, pour tout $x \in F$ et tout $x' \in L$, on a

$$\sigma(xx') = \sigma(x)\sigma(x') = x\sigma(x').$$

Cela démontre (1).

Montrons le point (2). Par (1), il suffit de montrer que $\sigma \in \mathrm{Gal}(L/K)$ fixe les éléments de $F_1F_2$ si, et seulement si, $\sigma$ fixe les éléments de $F_1$ et de $F_2$. Si $\sigma \in \mathrm{Gal}(L/K)$ fixe les éléments de $F_1F_2$, il fixe aussi les éléments de $F_1$ et de $F_2$. Inversement, si $\sigma \in \mathrm{Gal}(L/K)$ fixe les éléments de $F_1$ et de $F_2$, alors $\sigma$ fixe les éléments de $L$ de la forme

$$\sum_{i=1}^{n} x_i y_i, \quad n \geq 0,\ x_i \in F_1,\ y_i \in F_2.$$

Comme $F_1/K$ est de degré fini, elle est algébrique. Le lemme II.3.1 montre alors que les éléments de $F_1F_2$ sont exactement de la forme précédente, d'où (2).

Le point (3) provient du fait qu'un élément $x \in L$ est fixé par tous les éléments de $\langle H_1, H_2\rangle$ si, et seulement si, il est fixé par les éléments de $H_1$ et par les éléments de $H_2$.

Il reste à démontrer (4). Pour tout $x \in L$, et tout $\tau \in H$, on a

$$\sigma\big(\tau(x)\big) = \sigma\tau\sigma^{-1}\big(\sigma(x)\big).$$

En particulier, pour tout $x \in L^H$, on a $\sigma(x) = \sigma\tau\sigma^{-1}\big(\sigma(x)\big)$. Ainsi, on obtient

$$\sigma(L^H) \subset L^{\sigma H \sigma^{-1}}.$$

Si maintenant $y \in L^{\sigma H \sigma^{-1}}$, soit $x \in L$ tel que $y = \sigma(x)$. Pour tout $\tau \in H$, on a alors

$$\sigma\big(\tau(x)\big) = \sigma\tau\sigma^{-1}(y) = y = \sigma(x),$$

et par injectivité de $\sigma$, on obtient $\tau(x) = x$. Par conséquent, on a $x \in L^H$, et ainsi $y \in \sigma(L^H)$. Cela achève la démonstration. $\square$

Nous allons maintenant démontrer que si $L/K$ est galoisienne, les applications $\Phi_{L/K}$ et $\Psi_{L/K}$ sont inverses l'une de l'autre.

Théorème V.1.5 (Correspondance de Galois). *Soit $L/K$ une extension galoisienne de degré fini. Alors, on a une correspondance bijective décroissante entre l'ensemble des sous-groupes de* $\mathrm{Gal}(L/K)$ *et l'ensemble des sous-extensions de $L/K$. Cette correspondance est donnée par*

$$\begin{array}{ccc} \mathscr{SG}\big(\mathrm{Gal}(L/K)\big) & & \mathscr{SE}(L/K) \\ H & \overset{\Phi_{L/K}}{\longmapsto} & L^H/K \\ \mathrm{Gal}(L/F) & \overset{\Psi_{L/K}}{\longleftarrow} & F/K. \end{array}$$

*De plus, pour tout sous-groupe $H$ de* $\mathrm{Gal}(L/K)$, *et toute sous-extension $F/K$ de $L/K$, on a*

$$[F : K] = [\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F)] \quad \textit{et} \quad [L^H : K] = [\mathrm{Gal}(L/K) : H].$$

*Enfin, pour toutes sous-extensions $F_1/K$, $F_2/K$ et $F/K$ de $L/K$ correspondant respectivement aux sous-groupes $H_1$, $H_2$ et $H$ de* $\mathrm{Gal}(L/K)$, *on a les propriétés suivantes :*

(1) *la sous-extension $F_1F_2/K$ correspond au sous-groupe $H_1 \cap H_2$ ;*
(2) *la sous-extension $F_1 \cap F_2/K$ correspond au sous-groupe $\langle H_1, H_2\rangle$ ;*
(3) *pour tout $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(F)/K$ correspond au sous-groupe $\sigma H \sigma^{-1}$ ;*
(4) *l'extension $F/K$ est galoisienne si, et seulement si, $H$ est un sous-groupe distingué de* $\mathrm{Gal}(L/K)$. *Dans ce cas, on a un isomorphisme de groupes*

$$\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(L/K)/H.$$

*Démonstration.* Montrons que $\Phi_{L/K}$ est bijective, d'inverse $\Psi_{L/K}$. D'après la proposition V.1.3, on sait déjà que

$$\Psi_{L/K} \circ \Phi_{L/K} = \mathrm{Id}_{\mathscr{SG}(\mathrm{Gal}(L/K))}.$$

Si maintenant $F/K$ est une sous-extension de $L/K$, l'extension $L/F$ est galoisienne d'après la proposition IV.2.5. Mais alors, on a

$$(\Phi_{L/K} \circ \Psi_{L/K})(F/K) = L^{\mathrm{Gal}(L/F)}/K = F/K,$$

la dernière égalité étant donnée par le corollaire V.1.2. Autrement dit, on a bien $\Phi_{L/K} \circ \Psi_{L/K} = \mathrm{Id}_{\mathscr{SE}(L/K)}$, d'où la bijectivité de la correspondance.

De plus, si $H_1 \subset H_2$, on a clairement $L^{H_2} \subset L^{H_1}$. De même, si $F_1 \subset F_2$, on a $\mathrm{Gal}(L/F_2) \subset \mathrm{Gal}(L/F_1)$, puisqu'un automorphisme $F_2$-linéaire de $L$ est aussi $F_1$-linéaire. Ainsi, la correspondance est décroissante.

Si $F/K$ est une sous-extension de $L/K$, comme $L/F$ est galoisienne, on a

$$[L : F] = |\mathrm{Gal}(L/F)|.$$

Pour la même raison, on a $[L : K] = |\mathrm{Gal}(L/K)|$. Par conséquent, on a

$$[F : K] = \frac{[L : K]}{[L : F]} = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/F)|} = [\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F)].$$

L'autre égalité en découle par bijectivité de la correspondance [3].

Montrons maintenant les propriétés $(1) - (4)$. Les propriétés $(1) - (3)$ découlent directement du lemme V.1.4. Il reste à démontrer le point(4). Soit $F/K$ une sous-extension de $L/K$, et soit $H = \mathrm{Gal}(L/F)$ le sous-groupe correspondant. On a donc $F = L^H$.

Supposons que $H$ soit distingué dans $\mathrm{Gal}(L/K)$, et soit $\tau \in \mathscr{X}(F/K)$. Alors, $\tau$ se prolonge en un plongement $\sigma$ de $L/K$, qui est en fait un élément de $\mathrm{Gal}(L/K)$, puisque l'extension $L/K$ est normale. Par hypothèse sur $H$, on a l'égalité $\sigma H \sigma^{-1} = H$. La bijectivité de la correspondance et le point (3) donnent alors

$$\tau(F) = \sigma(F) = F.$$

Cela implique que $\tau$ est un automorphisme de $F/K$. Ainsi, $F/K$ est normale. Elle est aussi séparable, comme sous-extension d'une extension séparable. Par conséquent, $F/K$ est galoisienne.

Supposons maintenant que $F/K$ soit galoisienne. Pour tout $\sigma \in \mathrm{Gal}(L/K)$, sa restriction $\sigma_{|_F}$ à $F$ est un plongement de $F/K$, donc un élément du groupe $\mathrm{Gal}(F/K)$ puisque $F/K$ est normale.

3. On peut aussi la démontrer de la même manière, grâce au lemme d'Artin.

On a donc un morphisme de groupes

$$\begin{array}{rcl} \rho_F \colon \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(F/K) \\ \sigma & \longmapsto & \sigma_{|_F}. \end{array}$$

Montrons que $\rho_F$ est surjectif. Un élément de $\mathrm{Gal}(F/K)$ est en particulier un plongement de $F/K$, qui se prolonge alors en un plongement de $L/K$, qui est lui-même un élément de $\mathrm{Gal}(L/K)$, car $L/K$ est normale. Cela établit la surjectivité désirée. De plus, par le lemme V.1.4 (1), on a

$$\mathrm{Ker}(\rho_F) = \mathrm{Gal}(L/F).$$

En particulier, $H = \mathrm{Gal}(L/F)$ est distingué dans $\mathrm{Gal}(L/K)$, et le premier théorème d'isomorphisme appliqué à $\rho_F$ fournit un isomorphisme

$$\mathrm{Gal}(L/K)/H \simeq \mathrm{Gal}(F/K),$$

d'où le résultat. □

Remarques V.1.6. Soit $L/K$ une extension de degré fini.

(1) On a en fait démontré que les applications $\Phi_{L/K}$ et $\Psi_{L/K}$ sont des bijections inverses l'une de l'autre si, et seulement si, $L/K$ est galoisienne.

(2) Si $L/K$ est galoisienne, la correspondance de Galois implique que $L/K$ admet un nombre fini de sous-extensions, puisqu'un groupe fini n'admet qu'un nombre fini de sous-groupes. C'est vrai plus généralement si l'extension $L/K$ est monogène. En fait, une extension algébrique n'a qu'un nombre fini de sous-extensions si, et seulement si, cette extension est monogène (exercice).

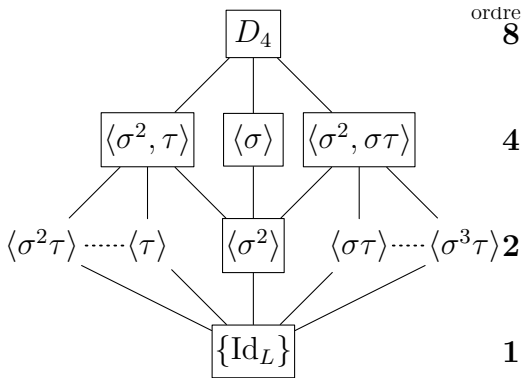
Exemple V.1.7. Soit $L = \mathbb{Q}(\alpha, i)$, avec $\alpha = \sqrt[4]{2}$.

On peut démontrer (exercice) que $L/\mathbb{Q}$ est une extension galoisienne, de groupe de Galois isomorphe à $D_4$, engendré par les deux automorphismes

$$\sigma : \left| \begin{array}{lcl} \alpha & \rightsquigarrow & i\alpha \\ i & \rightsquigarrow & i \end{array} \right.$$

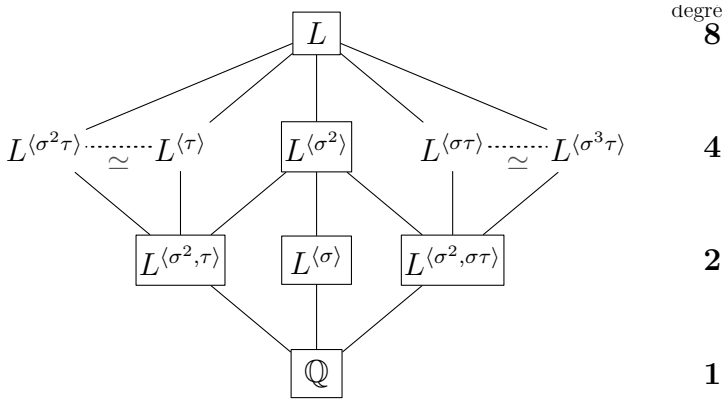
et

$$\tau : \left| \begin{array}{lcl} \alpha & \rightsquigarrow & \alpha \\ i & \rightsquigarrow & -i \end{array} \right.$$




Le treillis des sous-groupes de $D_4$ est donné ci-dessus, les sous-groupes distingués sont encadrés ; les pointillés relient les sous-groupes conjugués.

On a donc dix sous-groupes, les trois sous-groupes au deuxième étage sont d'indice 2, et les cinq sous-groupes au premier étage sont d'indice 4. Par la correspondance de Galois $L/\mathbb{Q}$ possède trois sous-extensions de degré 2, et cinq sous-extensions de degré 4. Cette correspondance étant décroissante, le treillis des sous-extensions de $L/\mathbb{Q}$ est de la forme




Nous allons maintenant déterminer tous ces sous-corps, et marquer ceux d'entre eux qui sont isomorphes. Remarquons que $L$ contient $\alpha^2 = \sqrt{2}$. On a donc trois sous-extensions quadratiques « évidentes », à savoir

$$\mathbb{Q}(\sqrt{2})/\mathbb{Q}, \quad \mathbb{Q}(i)/\mathbb{Q} \quad \text{et} \quad \mathbb{Q}(i\sqrt{2})/\mathbb{Q}.$$

Pour savoir à quels sous-corps fixes elles correspondent, remarquons par exemple que l'on a

$$\sigma^2(\sqrt{2}) = \sigma^2(\alpha^2) = \sigma^2(\alpha)^2 = \big(\sigma(i\alpha)\big)^2 = (-\alpha)^2 = \sqrt{2},$$

ainsi que

$$\tau(\sqrt{2}) = \tau(\alpha^2) = \tau(\alpha)^2 = \alpha^2 = \sqrt{2}.$$

Ainsi, on a $\sqrt{2} \in L^{\langle \sigma^2, \tau \rangle}$, et par conséquent $\mathbb{Q}(\sqrt{2}) \subset L^{\langle \sigma^2, \tau \rangle}$. Comme ces deux extensions ont même degré sur $\mathbb{Q}$, on obtient

$$\mathbb{Q}(\sqrt{2}) = L^{\langle \sigma^2, \tau \rangle}.$$

On a aussi $\sigma(i) = i$, et en raisonnant comme précédemment, on obtient

$$\mathbb{Q}(i) = L^{\langle \sigma \rangle}.$$

Par élimination (ou par un raisonnement similaire), on a alors

$$\mathbb{Q}(i\sqrt{2}) = L^{\langle \sigma^2, \sigma\tau \rangle}.$$

Passons aux sous-extensions de degré 4. Il y a trois extensions auxquelles on pense immédiatement :

$$\mathbb{Q}(i\alpha)/\mathbb{Q}, \quad \mathbb{Q}(\alpha)/\mathbb{Q} \quad \text{et} \quad \mathbb{Q}(i, \sqrt{2})/\mathbb{Q}.$$

En raisonnant comme ci-dessus, on montre qu'elles correspondent respectivement aux sous-extensions

$$L^{\langle \sigma^2\tau \rangle}, \ \ L^{\langle \tau \rangle} \quad \text{et} \quad L^{\langle \sigma^2 \rangle}.$$

Pour déterminer les deux sous-corps manquants, rappelons que

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8).$$

Un simple calcul montre alors que l'on a

$$\sigma(\zeta_8) = -\zeta_8 \quad \text{et} \quad \tau(\zeta_8) = \overline{\zeta}_8 = \zeta_8^{-1}.$$

On a alors

$$\sigma\tau(\zeta_8^{-1}\alpha) = \sigma(\zeta_8\alpha) = -i\zeta_8\alpha = \zeta_8^{-1}\alpha.$$

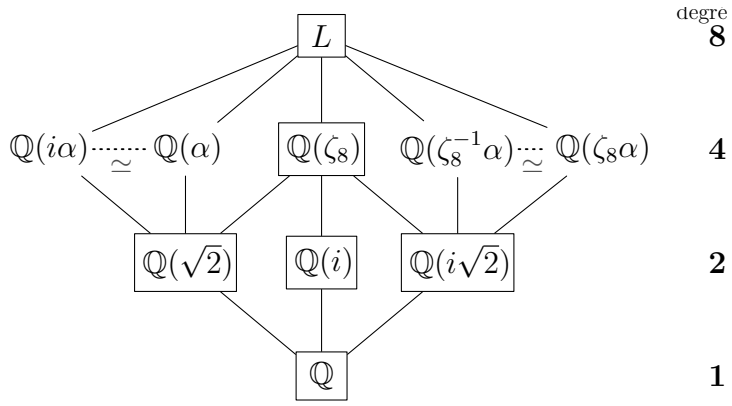
Comme précédemment, on en déduit

$$\mathbb{Q}(\zeta_8^{-1}\alpha) = L^{\langle \sigma\tau \rangle}.$$

On montre de même l'égalité $\mathbb{Q}(\zeta_8\alpha) = L^{\langle \sigma^3\tau \rangle}$.

De manière alternative, on peut remarquer que $[L : \mathbb{Q}(i, \sqrt{2})] = 2$. En particulier, $(1, \alpha)$ est une $\mathbb{Q}(i, \sqrt{2})$-base de $L$, et l'on peut expliciter les éléments de $L^{\langle \sigma\tau \rangle}$ et de $L^{\langle \sigma^3\tau \rangle}$.

Au final, on obtient le treillis des sous-extensions de $L/\mathbb{Q}$ :




Notons que les sous-groupes distingués (encadrés) de $\mathrm{Gal}(L/\mathbb{Q})$ sont

$$\mathrm{Gal}(L/\mathbb{Q}),\ \ \langle\sigma^2\rangle,\ \ \langle\sigma\rangle,\ \ \langle\sigma^2,\tau\rangle,\ \ \langle\sigma^2,\sigma\tau\rangle,\ \ \{\mathrm{Id}_L\},$$

et donc que seules les sous-extensions encadrées

$$L/\mathbb{Q},\ \ \mathbb{Q}(\zeta_8)/\mathbb{Q},\ \ \mathbb{Q}(i)/\mathbb{Q},\ \ \mathbb{Q}(\sqrt{2})/\mathbb{Q},\ \ \mathbb{Q}(i\sqrt{2})/\mathbb{Q},\ \ \mathbb{Q}/\mathbb{Q}$$

sont les sous-extensions galoisiennes de $L/\mathbb{Q}$.

## V.2. Résolubilité des équations par radicaux

L'application que nous allons donner maintenant est l'origine historique de la théorie de Galois et de la théorie des groupes.

Avant tout, nous avons besoin de quelques définitions.

Définition V.2.1. Soit $K$ un corps de caractéristique 0. Une extension $F/K$ est dite *radicale* s'il existe une tour d'extensions

$$K = F_0 \subset F_1 \subset \cdots \subset F_r = F$$

telle que, pour tout entier $i \in [\![1, r]\!]$, il existe $\alpha_i \in F_i$ et un entier $n_i \geq 1$ vérifiant $F_i = F_{i-1}(\alpha_i)$ et $\alpha_i^{n_i} \in F_{i-1}$.

En particulier, si $F/K$ et $E/F$ sont radicales, $E/K$ est radicale.

Remarques V.2.2.

(1) Cette définition mérite quelques commentaires. Soit $F/K$ une extension de corps. Supposons qu'il existe $\alpha \in F$ et $n \geq 1$ tels que $F = K(\alpha)$ et $\alpha^n \in K$. On a donc $\alpha^n = a$, pour un certain $a \in K$. On serait ainsi tenté de faire l'abus de notation $\alpha = \sqrt[n]{a}$ et $F = K(\sqrt[n]{a})$, comme dans le cas des extensions de Kummer.

La difficulté cachée est que l'on n'a pas supposé que $K$ contient $\mu_n(\overline{K})$, si bien que chaque racine du polynôme $X^n - a$ peut engendrer une extension différente.

Par exemple, si $K = \mathbb{Q}$, $\sqrt[3]{2}$ et $j\sqrt[3]{2}$ sont deux racines de $X^3-2$, mais $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ et $\mathbb{Q}(j\sqrt[3]{2})/\mathbb{Q}$ sont deux extensions de degré 3 bien distinctes, puisque la première est incluse dans $\mathbb{R}$, ce qui n'est pas le cas de la seconde.

La situation devient encore pire lorsque $X^n-a$ n'est pas irréductible dans $K[X]$. Par exemple, si $K = \mathbb{Q}$, 1 et $i$ sont deux racines du polynôme $X^8-1 \in \mathbb{Q}[X]$, mais la première engendre une extension de degré 1, tandis que la seconde engendre une extension de degré 2.

(2) Si $F/K$ est radicale et $E/K$ est quelconque, alors $EF/E$ est radicale. En effet, si l'on a

$$K = F_0 \subset F_1 \subset \cdots \subset F_r = F$$

telle que, pour tout $i \in [\![1, r]\!]$, il existe $\alpha_i \in F_i$ et un entier $n_i \geq 1$ vérifiant $F_i = F_{i-1}(\alpha_i)$ et $\alpha_i^{n_i} \in F_{i-1}$, alors on a aussi

$$E = EF_0 \subset EF_1 \subset \cdots \subset EF_r = EF,$$

et $EF_i = EF_{i-1}(\alpha_i)$ pour tout $i \in [\![1, r]\!]$. Ainsi, $EF/E$ est radicale.

En particulier, le compositum d'un nombre fini d'extensions radicales est radicale. En effet, supposons que $E/K$ et $F/K$ soient radicales. Alors, $EF/E$ est radicale. Mais alors, comme $E/K$ est radicale, il est clair que $EF/K$ est aussi radicale, puisqu'il suffit de recoller les deux tours d'extensions associées à $E/K$ et à $EF/E$.

Exemples V.2.3. Soit $K$ un corps de caractéristique 0.

(1) Toute extension cyclotomique de $K$ est radicale.

(2) Une extension de degré 2 d'un corps de caractéristique nulle est radicale d'après l'exemple IV.6.3.

Par conséquent, toute extension 2-décomposable de $K$ est radicale.

Définition V.2.4. Soit $K$ un corps de caractéristique 0. On dit que $\alpha \in \overline{K}$ est *exprimable par radicaux* s'il est contenu dans une extension $E/K$ radicale.

Exemple V.2.5. Malgré la remarque précédente, nous allons faire ici l'abus de notation usuel, à savoir que si $K$ est un corps quelconque et $a \in K$, on désigne par $\sqrt[n]{a}$ **une** racine du polynôme $X^n - a \in K[X]$ dans $\overline{K}$.

Avec cette notation, le nombre complexe $\alpha = 2 + \sqrt[3]{7 - i\sqrt[4]{2-\sqrt{6}}} \in \mathbb{C}$ est exprimable par radicaux.

Définition V.2.6. Soit $K$ un corps de caractéristique 0. On dit qu'un polynôme $P \in K[X]$ non constant est *résoluble par radicaux* si toutes les racines de $P$ dans $\overline{K}$ sont exprimables par radicaux.

Remarques V.2.7. (1) Puisque le compositum d'un nombre fini d'extensions radicales est radicale par la remarque V.2.2 (2), un polynôme $P \in K[X]$ est résoluble par radicaux si, et seulement si, $\mathrm{Dec}_K(P)$ est contenu dans une extension radicale $E/K$.

(2) Clairement, un polynôme $P \in K[X]$ est résoluble par radicaux si, et seulement si, chacun de ses facteurs irréductibles est résoluble par radicaux.

Nous allons maintenant introduire une autres notion importante de ce paragraphe.

Définition V.2.8. Soit $G$ un groupe. Une *suite de composition* de $G$ est une suite de sous-groupes $(G_0, \ldots, G_r)$ telle que

$$G_r = \{1\} \subset G_{r-1} \subset \cdots \subset G_1 \subset G_0 = G,$$

et pour tout $i \in [\![0, r-1]\!]$, on a $G_{i+1} \triangleleft G_i$.

Un groupe $G$ est dit *résoluble* s'il existe une suite de composition $(G_0, \ldots, G_r)$ telle que pour tout $i \in [\![0, r-1]\!]$, le groupe quotient $G_i/G_{i+1}$ est abélien.

Exemple V.2.9. Tout groupe abélien est évidemment résoluble.

Le théorème suivant donne l'exemple d'une famille de groupes résolubles.

Théorème V.2.10. *Soit $p$ un nombre premier, et soit $G$ un $p$-groupe d'ordre $p^n$. Alors, il existe des sous-groupes*

$$G_n = \{1\} \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$$

*tels que pour tout $i \in [\![0, n]\!]$, on a $G_i \triangleleft G$ et $|G_i| = p^{n-i}$.*

*En particulier, tout $p$-groupe est résoluble.*

*Démonstration.* Soit $G$ un groupe d'ordre $p^n$, avec $p$ premier, et $n \geq 0$. Le cas $n = 0$ étant évident, on peut supposer que $n \geq 1$.
On procède par récurrence sur $n$. Soit $(H_n)$ la propriété :

$(H_n)$ Le théorème est vrai pour tout groupe d'ordre $p^n$.

Si $n = 1$, le groupe $G$ est cyclique d'ordre $p$, et la propriété $(H_1)$ est vraie. Supposons maintenant que $(H_n)$ soit vraie pour un entier $n \geq 1$, et montrons $(H_{n+1})$. Soit $G$ un groupe d'ordre $p^{n+1}$. Son centre $Z(G)$ est donc non trivial. En particulier, son ordre est divisible par $p$, et le

théorème de Cauchy assure l'existence d'un élément $x \in Z(G)$ d'ordre $p$.

Alors, $\langle x \rangle$ est cyclique d'ordre $p$, et distingué dans $G$, car $x \in Z(G)$. Mais, alors, le groupe $G/\langle x \rangle$ est d'ordre $p^n$. Par hypothèse de récurrence, il existe une suite de composition $(G_0/\langle x \rangle, \ldots, G_n/\langle x \rangle)$ de $G/\langle x \rangle$ telle que $G_i/\langle x \rangle$ soit un sous-groupe distingué de $G/\langle x \rangle$ d'indice $p^i$ (où $G_i$ est un sous-groupe de $G$ contenant $\langle x \rangle$), et cela pour tout $i \in [\![0, n]\!]$. Puisque le sous-groupe $G_i/\langle x \rangle$ est distingué dans $G/\langle x \rangle$, $G_i$ est distingué dans $G$. De plus, on a les égalités

$$[G : G_i] = \frac{|G|}{|G_i|} = \frac{|G|\,|\langle x \rangle|}{|\langle x \rangle|\,|G_i|} = [G/\langle x \rangle : G_i/\langle x \rangle] = p^i.$$

Puisque $G_n/\langle x \rangle$ est trivial, on a $G_n = \langle x \rangle$, qui est cyclique d'ordre $p$. Si l'on pose $G_{n+1} = \{1_G\}$, la suite de composition $(G_0, \ldots, G_{n+1})$ est une suite de composition de $G$ qui vérifie les conditions demandées. Cela achève la récurrence.

Le dernier point découle du fait que, pour tout $i \in [\![0, n]\!]$, $G_i/G_{i+1}$ est d'ordre $p$ premier, donc cyclique, et en particulier abélien. □

On s'intéresse maintenant à la notion duale en théorie des corps.

Définition V.2.11. Soit $K$ un corps quelconque. On dit qu'une extension de corps $L/K$ de degré fini est *résoluble* si elle est galoisienne, et $\mathrm{Gal}(L/K)$ est un groupe résoluble.

Exemples V.2.12. (1) Une extension abélienne est résoluble, puisqu'un groupe abélien est résoluble.

(2) Si $L/K$ est galoisienne, de degré $p^n$, où $p$ est premier, alors $L/K$ est résoluble, car un $p$-groupe fini est résoluble par le théorème V.2.10.

Afin de démontrer des résultats intéressants sur les extensions résolubles, il nous faut étudier plus avant les groupes résolubles.

Lemme V.2.13. *Soit $G$ un groupe, et soit $H$ un sous-groupe de $G$. Alors :*

(1) *Si $(G_0, \ldots, G_r)$ est une suite de composition de $G$, alors $(G_0 \cap H, \ldots, G_r \cap H)$ est une suite de composition de $H$. De plus, pour tout $i \in [\![0, r-1]\!]$, $G_i \cap H/G_{i+1} \cap H$ est isomorphe à un sous-groupe de $G_i/G_{i+1}$ ;*

(2) *on suppose que $H$ est distingué dans $G$. Si $(G_0, \ldots, G_r)$ est une suite de composition de $G$, alors $(\langle G_0, H \rangle/H, \ldots, \langle G_r, H \rangle/H)$ est une suite de composition de $G/H$. De plus, pour tout $i \in [\![0, r-1]\!]$,*

*le groupe quotient* $(\langle G_i, H\rangle/H)/(\langle G_{i+1}, H\rangle/H)$ *est isomorphe à un quotient de* $G_i/G_{i+1}$.

(3) *on suppose que* $H$ *est distingué dans* $G$. *Si* $(H_0, \ldots, H_r)$ *est une suite de composition de* $H$, *et si* $(G'_0/H, \ldots, G'_s/H)$ *est une suite de composition du quotient* $G/H$ *(où* $G'_i$ *est un sous-groupe de* $G$ *contenant* $H$*), alors la suite*

$$(G'_0,\ \ldots,\ G'_s,\ H_1,\ \ldots,\ H_r)$$

*est une suite de composition de* $G$, *dont la liste des quotients successifs s'obtient en concaténant les listes des quotients successifs des deux suites ci-dessus.*

*Démonstration.*

(1) Soit $(G_0, \ldots, G_r)$ une suite de composition de $G$, et soit $H$ un sous-groupe de $G$. Il est facile de voir que $(G_0 \cap H, \ldots, G_r \cap H)$ est une suite de composition de $H$, i.e. que $G_{i+1} \cap H$ est un sous-groupe distingué de $G_i \cap H$ pour tout $i \in [\![0, r-1]\!]$. De plus, pour tout $i \in [\![0, r-1]\!]$, $G_i \cap H/G_{i+1} \cap H$ est isomorphe à un sous-groupe de $G_i/G_{i+1}$. En effet, le noyau du morphisme de groupes

$$\begin{aligned} G_i \cap H &\longrightarrow G_i/G_{i+1} \\ x &\longmapsto \overline{x} \end{aligned}$$

est $G_{i+1} \cap H$, et induit donc un morphisme injectif $G_i \cap /G_{i+1} \cap H \longrightarrow G_i/G_{i+1}$.

(2) pour tous $h$, $h' \in H$, tout $g_i \in G_i$, et tout $g_{i+1} \in G_{i+1}$, on a

$$g_i h' g_i^{-1} \in \langle G_i, H\rangle$$

par définition d'un sous-groupe engendré (ou bien parce que $H$ est distingué dans $G$), et $hh'h^{-1} \in H$. Ainsi, $H$ est distingué dans $\langle G_i, H\rangle$. De plus, on a

$$hg_{i+1}h^{-1} \in \langle G_{i+1}, H\rangle \subset \langle G_i, H\rangle,$$

et aussi

$$g_i g_{i+1} g_i^{-1} \in G_{i+1} \subset \langle G_i, H\rangle.$$

Cela montre que $G_{i+1}$ est aussi distingué dans $\langle G_i, H\rangle$. Par conséquent, le sous-groupe $\langle G_{i+1}, H\rangle$ est bien distingué dans $\langle G_i, H\rangle$.

Considérons le morphisme de groupes

$$\begin{aligned} f_i \colon G_i &\longrightarrow \langle G_i, H\rangle/\langle G_{i+1}, H\rangle \\ g_i &\longmapsto \overline{g}_i. \end{aligned}$$

Alors, $f_i$ est surjectif.

En effet, pour tout $i \in [\![0, r-1]\!]$, on a

$$\langle G_i, H\rangle = \langle H, G_i\rangle = HG_i,$$

car $H$ est distingué dans $G$. Pour tout $hg_i \in HG_i = \langle H, G_i\rangle$, on a alors

$$\overline{hg_i} = \overline{h}\ \overline{g}_i = \overline{g}_i = f_i(g_i),$$

d'où la surjectivité[4].

De plus, $\mathrm{Ker}(f_i)$ contient $G_{i+1}$, et induit donc par passage au quotient un morphisme de groupes

$$\overline{f}_i : G_i/G_{i+1} \longrightarrow \langle G_i, H\rangle/\langle G_{i+1}, H\rangle.$$

Ce morphisme est surjectif, puisque $f_i$ l'est. Le premier théorème d'isomorphisme permet alors de conclure que $\langle G_i, H\rangle/\langle G_{i+1}, H\rangle$ est isomorphe au quotient de $G_i/G_{i+1}$ par $\mathrm{Ker}(f_i)$.

Enfin, par le troisième théorème d'isomorphisme, puisque $H$ est distingué dans $G$, donc dans $\langle G_i, H\rangle$ et dans $\langle G_{i+1}, H\rangle$, on obtient l'isomorphisme

$$\langle G_i, H\rangle/\langle G_{i+1}, H\rangle \simeq \big(\langle G_i, H\rangle/H\big)/\big(\langle G_{i+1}, H\rangle/H\big).$$

Ce dernier groupe est donc bien isomorphe à un quotient de $G_i/G_{i+1}$.

(3) Par définition, on a $H_r = \{1_H\} = \{1_G\}$, et $G'_0/H = G/H$. On a donc $G'_0 = G$. Remarquons également que le sous-groupe $G'_{j+1}$ est distingué dans $G'_j$ pour tout $j \in [\![0, s-1]\!]$. Enfin, puisque $G'_s/H = \{\overline{1}_G\}$, on a $G'_s = H$. Mais alors, $H_1$ est bien distingué dans $G'_s = H = H_0$, d'où le résultat.

En ce qui concerne l'affirmation sur les quotients successifs, il suffit d'utiliser l'isomorphisme

$$G'_j/G'_{j+1} \simeq (G_j/H)/(G_{j+1}/H),$$

et le fait que $G'_s = H = H_0$.

□

Proposition V.2.14. *Soit $G$ un groupe. Alors :*

(1) *si $G$ est résoluble, il en est de même de tout sous-groupe de $G$ ;*
(2) *si $G$ est résoluble, il en est de même de tout quotient de $G$ ;*
(3) *pour tout sous-groupe $H$ distingué dans $G$, le groupe $G$ est résoluble si, et seulement si, les groupes $H$ et $G/H$ sont résolubles.*

*Démonstration.*

4. On aurait aussi pu effectuer un raisonnement direct.

(1) Il suffit d'appliquer le lemme V.2.13 (1), et de remarquer que si $G_i/G_{i+1}$ est abélien, il en est de même de tout sous-groupe, et donc du groupe $G_i \cap H/G_{i+1} \cap H$.
(2) On applique cette fois le lemme V.2.13 (2), et de remarquer que si$G_i/G_{i+1}$ est abélien, il en est de même de tout quotient, et donc de $(\langle G_i, H\rangle/H)/(\langle G_{i+1}, H\rangle/H)$.
(3) Il reste à démontrer le sens indirect. On applique alors le lemme V.2.13 (2), et le fait que $G/H$ et $H$ sont résolubles, pour voir que tous les quotients successifs sont abéliens.

□

On a besoin d'une dernière proposition.

Proposition V.2.15. *Soit $G$ un groupe fini. Alors, $G$ est résoluble si, et seulement si, il existe une suite de composition $(G'_0, \dots, G'_s)$ tel que $G'_j/G'_{j+1}$ est cyclique pour tout $j \in [\![0, s-1]\!]$.*

*Démonstration.* Seul le sens direct mérite une démonstration, l'autre étant clair puisqu'un groupe cyclique est abélien.

Nous allons nous appuyer sur le fait suivant.

**Fait 1.** Soit $A$ un groupe abélien fini. Alors, il existe une suite de composition $(A_0, \dots, A_t)$ telle que $A_k/A_{k+1}$ est cyclique pour tout $k \in [\![0, t-1]\!]$.

Supposons ce fait démontré. On peut alors démontrer le

**Fait 2.** Soit $G$ un groupe, et soit $H$ un sous-groupe distingué. Si $G/H$ est abélien fini, il existe une suite de sous-groupes

$$G_t = H \subset G_{t-1} \subset \cdots \subset G_0 = G$$

tels que pour tout $k \in [\![0, t-1]\!]$, $G_{k+1}$ est distingué dans $G_k$ et $G_k/G_{k+1}$ est cyclique.

En effet, d'après le fait 1, on a une suite de composition $(G'_0/H, \dots, G'_t/H)$ de $G/H$ telle que $G'_k/H/G'_{k+1}/H$ est cyclique pour tout $k \in [\![0, t-1]\!]$. En particulier, $G'_t/H$ est trivial et $G'_t = H$. De même, $G'_0/H = G/H$ et $G'_0 = G$. Comme $G'_k/G'_{k+1} \simeq (G'_k/H)/(G'_{k+1}/H)$, ce quotient est cyclique, et la suite de sous-groupe $G'_t \subset \cdots \subset G'_0$ convient.

Soit maintenant $(G_0, \dots, G_r)$ une suite de composition, où chaque quotient est abélien. Pour obtenir une suite de composition ayant les propriétés requises, il suffit d'appliquer le fait 2 à chaque quotient $G_i/G_{i+1}$ et d'insérer les sous-groupes correspondants.

Il reste donc à établir le fait 1. On va procéder par récurrence sur $n = |A|$.[5]

Plus précisément, pour tout $n \geq 1$, soit $(H_n)$ la propriété suivante :

$(H_n)$ pour tout groupe abélien $A$ d'ordre $\leq n$, il existe une suite de composition $(A_0, \ldots, A_t)$ telle que $A_k/A_{k+1}$ est cyclique pour tout $k \in [\![0, t-1]\!]$.

La propriété $(H_1)$ est trivialement vraie, puisque $A$ est alors trivial. Supposons que $(H_n)$ soit vraie pour un entier $n \geq 1$, et montrons $(H_{n+1})$. Soit $A$ un groupe abélien d'ordre $\leq n+1$. Si $A$ est d'ordre $\leq n$, on applique $(H_n)$. On peut donc supposer que $|A| = n+1 \geq 2$. En particulier, $|A|$ est divisible par un nombre premier $p$, et le théorème de Cauchy assure l'existence d'un élément $a \in A$ d'ordre $p$.

Alors, $A/\langle a \rangle$ est abélien d'ordre $\dfrac{n+1}{p} \leq n$ (car $p \geq 2$), et il existe une suite de composition de $A/\langle a \rangle$ possédant les propriétés voulues. Comme $(\langle a \rangle)$ est bien entendu également une suite de composition de $\langle a \rangle$ vérifiant les propriétés souhaitées, il en est de même de la suite de composition de $A$ obtenue à l'aide du lemme V.2.13. Ceci achève la récurrence, et la démonstration. □

On peut maintenant démontrer quelques propriétés des extensions résolubles.

Lemme V.2.16. *Soit $K$ un corps. Soit $L/K$ une extension galoisienne, et soit $F/K$ une sous-extension de $L/K$. Alors :*

(1) *si $L/K$ est résoluble, alors $L/F$ est résoluble ;*
(2) *si $L/K$ est résoluble et $F/K$ est galoisienne, alors $F/K$ est résoluble ;*
(3) *si $F/K$ est galoisienne, alors $L/K$ est résoluble si, et seulement si, les extensions $F/K$ et $L/F$ sont résolubles ;*
(4) *si $L/K$ est une extension résoluble, et si $E/K$ est une extension quelconque, alors $EL/E$ est résoluble ;*
(5) *le compositum d'un nombre fini d'extensions résolubles de $K$ est une extension résoluble de $K$.*

*Démonstration.* Soit $L/K$ une extension galoisienne, et soit $G = \mathrm{Gal}(L/K)$. Alors, $H = \mathrm{Gal}(L/F)$ est un sous-groupe de $G$. Si de plus, $F/K$ est galoisienne, alors $H$ est distingué dans $G$ par la correspondance de Galois, et l'on a dans ce cas $\mathrm{Gal}(F/K) \simeq G/H$. Les propriétés $(1) - (3)$ découlent alors directement de la proposition V.2.14.

5. On peut aussi le démontrer aisément en utilisant le théorème de structure des groupes abéliens finis.

Montrons (4). Si $L/K$ est résoluble et $E/K$ est une extension quelconque, la proposition IV.2.5 montre que $LE/E$ est galoisienne, et que $\mathrm{Gal}(LE/E)$ est isomorphe à un sous-groupe de $\mathrm{Gal}(L/K)$. Comme $\mathrm{Gal}(L/K)$ est résoluble, $\mathrm{Gal}(LE/E)$ l'est également.

Il reste à vérifier (5). Il suffit de montrer que le compositum de deux extensions résolubles est encore résoluble. Soient $L/K$ et $L'/K$ deux telles extensions. D'après le point (4), l'extension $LL'/L'$ est résoluble. Comme $L'/K$ est résoluble, le point (3) montre que $LL'/K$ est résoluble. Cela achève la démonstration. □

Le lemme suivant relie les notions d'élément exprimable par radicaux et d'extension résoluble.

Lemme V.2.17. *Soit $K$ un corps de caractéristique* 0. *Alors, tout élément d'une extension résoluble est exprimable par radicaux.*

*Démonstration.* Soit $L/K$ une extension résoluble de degré $n \geq 1$.

Soit $E = K(\zeta_n)$. L'extension $E/K$ étant résoluble, $EL/E$ est résoluble par le lemme précédent. D'après la proposition IV.2.5, $\mathrm{Gal}(EL/E)$ est isomorphe à un sous-groupe de $\mathrm{Gal}(L/K)$, qui est d'ordre $n$ puisque $L/K$ est galoisienne. On a donc

$$|\mathrm{Gal}(EL/E)| \mid n.$$

Puisque $E/K$ est radicale et que $EL$ contient les éléments de $L$, il suffit de montrer que $EL/E$ est radicale.

On peut donc supposer sans perte de généralité que $\mu_n(\overline{K}) \subset K$ et que l'extension $L/K$ est résoluble, de degré divisant $n$.

Posons $G = \mathrm{Gal}(L/K)$. Puisque $G$ est résoluble, d'après la proposition V.2.15, il existe une suite de composition

$$G_r = \{\mathrm{Id}_L\} \lhd G_{r-1} \lhd \cdots \lhd G_1 \lhd G_0 = G,$$

avec $G_i/G_{i+1}$ cyclique pour tout $i \in [\![0, r-1]\!]$.

Posons $F_i = L^{G_i}$ pour tout $i \in [\![0, r]\!]$. Ainsi, on a

$$K = F_0 \subset F_1 \subset \cdots \subset F_r = L.$$

Soit $i \in [\![0, r-1]\!]$. Le lemme d'Artin montre que

$$\mathrm{Gal}(L/F_{i+1}) = G_{i+1} \lhd G_i = \mathrm{Gal}(L/F_i).$$

D'après la correspondance de Galois, l'extension $F_{i+1}/F_i$ est galoisienne, et $\mathrm{Gal}(F_{i+1}/F_i) \simeq G_i/G_{i+1}$ est un groupe cyclique. Remarquons enfin que l'entier $[F_{i+1} : F_i]$ divise $[L : K]$, et donc divise $n$.

Il suffit donc de démontrer que chaque extension $F_{i+1}/F_i$ est radicale, ce qui est donné par la théorie de Kummer. Cela achève la démonstration. $\square$

Nous allons maintenant nous intéresser à la démonstration de la réciproque de ce résultat, à savoir qu'un élément exprimable par radicaux est contenu dans une extension résoluble. On commence par un lemme technique.

Lemme V.2.18. *Soit $K$ un corps de caractéristique $0$, et soit $E/K$ une extension galoisienne. Soit $F/E$ une extension telle qu'il existe $\alpha \in F$ et un entier $n \geq 1$ vérifiant $F = E(\alpha)$ et $\alpha^n \in E$. Alors, $F$ est contenue dans une extension galoisienne $L/K$ telle que $L/E$ soit résoluble. Si de plus $n = 2$, on peut choisir $L/K$ telle que $[L : E]$ soit une puissance de $2$.*

*Démonstration.* Soit $a \in E$ tel que $\alpha^n = a$, et posons

$$P = \prod_{\tau \in \mathrm{Gal}(E/K)} \big(X^n - \tau(a)\big) \in E[X].$$

Pour tout $\sigma \in \mathrm{Gal}(E/K)$, on a

$$\sigma(P) = \prod_{\tau \in \mathrm{Gal}(E/K)} \big(X^n - \sigma\tau(a)\big) = \prod_{\tau \in \mathrm{Gal}(E/K)} \big(X^n - \tau(a)\big).$$

Ainsi, les coefficients de $P$ sont fixés par tous les éléments de $\mathrm{Gal}(E/K)$, donc ce sont des éléments de $K$. Autrement dit, $P \in K[X]$.

Soient $\alpha = \alpha_1, \ldots, \alpha_m \in \overline{K}$ les racines de $P$. Posons

$$M = \mathrm{Dec}_K(P) = K(\alpha_1, \ldots, \alpha_m).$$

Alors, $M/K$ est normale par construction, et séparable puisque $K$ est de caractéristique nulle. Ainsi, $M/K$ est galoisienne. Posons $L = K(\zeta_n)EM$. Comme $E/K, M/K$ et $K(\zeta_n)/K$ sont galoisiennes, $L/K$ est aussi galoisienne par le lemme IV.2.9. Par construction, $F = E(\alpha) \subset L$.

Montrons que $L/E$ est résoluble. Remarquons que $L/E(\zeta_n)$ est le compositum des extensions $E(\zeta_n, \alpha_i)/E(\zeta_n),\ i \in [\![1, m]\!]$. Or, par définition, pour tout $i \in [\![1, m]\!]$, il existe un élément $a_i \in E$ tel que $\alpha_i^n = a_i$. Ainsi, l'extension $E(\zeta_n, \alpha_i)/E(\zeta_n)$ est une extension de Kummer, donc cyclique, et en particulier résoluble. Le dernier point du lemme V.2.16 assure alors que $L/E(\zeta_n)$ est résoluble. Comme $E(\zeta_n)/E$ est une extension abélienne, donc résoluble, le point (3) de ce même lemme entraîne que $L/E$ est résoluble.

Supposons maintenant que $n = 2$, et vérifions que $[L : E]$ est une puissance de 2.

Remarquons que dans ce cas, on a $L = E(\alpha_1, \ldots, \alpha_n)$. Remarquons aussi que chaque $\alpha_i$ est une racine d'un polynôme de $E[X]$ de degré 2, et est donc de degré au plus 2 sur $E$. Or, on a le fait suivant.

**Fait.** Soit $E'/E$ une extension de degré fini, et soit $\alpha \in \overline{E}$ de degré au plus 2 sur $E$. Alors, $[E'(\alpha) : E] = [E' : E]$ ou $2[E' : E]$.

En effet, on a $[E'(\alpha) : E'] \leq [E(\alpha) : E] \leq 2$ par le lemme II.3.1. On a donc $[E'(\alpha) : E'] = 1$ ou 2, d'où le résultat par la formule de multiplicativité des degrés.

En utilisant ce fait, on démontre par récurrence que $[E(\alpha_1, \ldots, \alpha_n) : E]$ est une puissance de 2. Cela achève la démonstration. □

On en déduit le résultat suivant.

Lemme V.2.19. *Soit $K$ un corps de caractéristique 0. Alors, toute extension radicale $F/K$ est contenue dans une extension résoluble $L/K$.*

*Si de plus $F/K$ est 2-décomposable, on peut choisir $L/K$ telle que $[L : K]$ soit une puissance de 2.*

*Démonstration.* Rappelons qu'une extension 2-décomposable est radicale, d'après l'exemple V.2.3 (2). Nous allons démontrer la propriété suivante pour tout $r \geq 0$ par récurrence :

$(H_r)$ pour toute extension $F/K$ radicale (resp. 2-décomposable) telle que

$$K = F_0 \subset F_1 \subset \cdots \subset F_{r-1} \subset F_r = F,$$

avec $F_i = F_{i-1}(\alpha_i)$ , où $\alpha_i \in F_i$ vérifie $\alpha_i^{n_i} \in F_{i-1}$ pour un certain $n_i \geq 1$ (resp. $n_i \leq 2$) pour tout $i \in [\![1, r]\!]$, l'extension $F$ est contenue dans une extension résoluble de $K$ (resp. une extension galoisienne dont le degré est une puissance de 2).

La propriété $(H_0)$ étant trivialement vraie, supposons que $(H_r)$ soit vraie pour un certain entier $r \geq 0$, et considérons une extension radicale (resp.2-décomposable) $F/K$ de la forme

$$K = F_0 \subset F_1 \subset \cdots \subset F_{r-1} \subset F_r \subset F_{r+1} = F$$

vérifiant les propriétés adéquates.

Par hypothèse de récurrence, $F_r/K$ est une sous-extension d'une extension résoluble $E/K$. De plus, on peut supposer que $[E : K]$ est une puissance de 2 dans le cas 2-décomposable.

Puisque $E$ contient $F_r$, on a $E = EF_r$. On a alors $EF_{r+1} = E(\alpha_{r+1})$. D'après le lemme précédent, $EF_{r+1}$ est contenue dans une extension galoisienne $L/K$ telle que $L/E$ soit résoluble. Dans le cas 2-décomposable,

on peut supposer de plus que $[L : E]$ est une puissance de 2. Comme $E/K$ et $L/E$ sont résolubles, $L/K$ est résoluble par le lemme V.2.16. Dans le cas 2-décomposable, $[E : K]$ et $[L : E]$ sont des puissances de 2, et il en est donc de même de $[L : K]$. Cela achève la récurrence, ainsi que la démonstration. □

On peut maintenant énoncer le théorème suivant.

THÉORÈME V.2.20. *Soit $K$ un corps de caractéristique 0, et soit $\alpha \in \overline{K}$. Les propriétés suivantes sont équivalentes :*

(1) *$\alpha$ est exprimable par radicaux ;*
(2) *$\alpha$ est contenu dans une extension résoluble de $K$ ;*
(3) *le groupe $\mathrm{Gal}_K(\mu_{\alpha,K})$ est résoluble.*

*Démonstration.*

(1) $\Longrightarrow$ (2). Si $\alpha$ est exprimable par radicaux, il est contenu dans une extension $F/K$ radicale. Le lemme V.2.19 montre alors que $F/K$ est une sous-extension d'une extension $L/K$ résoluble. Comme $\alpha \in L$, on obtient le résultat voulu.

(2) $\Longrightarrow$ (3). Soit $L/K$ une extensions résoluble contenant $\alpha$. Puisque $\alpha \in F$, l'extension normale $L/K$ contient une racine de $\mu_{\alpha,K}$, et donc les contient toutes. Ainsi, on a

$$\mathrm{Dec}_K(\mu_{\alpha,K}) \subset L.$$

Comme $L/K$ est résoluble et $\mathrm{Dec}_K(\mu_{\alpha,K})/K$ est galoisienne, cette dernière extension est aussi résoluble par le lemme V.2.16 (2).

(3) $\Longrightarrow$ (1). Par hypothèse, $\mathrm{Dec}_K(\mu_{\alpha,K})/K$ est résoluble et contient $\alpha$. D'après le lemme V.2.17, $\alpha$ est exprimable par radicaux.

Cela achève la démonstration. □

COROLLAIRE V.2.21. *Soit $K$ un corps de caractéristique 0, et soit $P \in K[X]$ un polynôme non constant. Les propriétés suivantes sont équivalentes :*

(1) *le polynôme $P$ est résoluble par radicaux ;*
(2) *$\mathrm{Dec}_K(P)$ est contenu dans une extension résoluble de $K$ ;*
(3) *le groupe $\mathrm{Gal}_K(P)$ est résoluble.*

*Démonstration.*

(1) $\Longrightarrow$ (2). Soient $\alpha_1, \ldots, \alpha_n \in \overline{K}$ les racines de $P$. D'après le théorème précédent, chaque $\alpha_i$ est contenu dans une extension résoluble $L_i/K$. Posons $L = L_1 \ldots L_n$. Alors, $L/K$ est résoluble par le lemme V.2.16 (5). Comme $L/K$ contient toutes les racines de $P$, elle contient $\mathrm{Dec}_K(P)$.

(2) $\Longrightarrow$ (3). Soit $L/K$ une extension résoluble contenant $\mathrm{Dec}_K(P)$. Comme l'extension $\mathrm{Dec}_K(P)/K$ est galoisienne, cette dernière extension est aussi résoluble par le lemme V.2.16 (2).

(3) $\Longrightarrow$ (1). Comme $\mathrm{Dec}_K(P)/K$ est résoluble et contient toutes les racines de $P$, il suffit d'appliquer le théorème précédent pour conclure que $P$ est résoluble par radicaux. $\square$

Exemple V.2.22. Un polynôme de degré $\geq 5$ à coefficients dans $\mathbb{Q}$ n'est pas en général résoluble par radicaux. Ce résultat, dû au mathématicien norvégien Abel [6], est antérieur aux résultats précédents, qui eux ont été démontrés par Galois.

Pour le voir, il suffit d'exhiber un exemple de polynôme irréductible à coefficients rationnels de degré $n$ dont le groupe de Galois n'est pas résoluble. Or, pour tout $n \geq 5$, on peut construire un polynôme de $\mathbb{Q}[X]$ dont le groupe de Galois est isomorphe à $\mathfrak{S}_n$.

Par exemple, le polynôme $X^5 - X - 1 \in \mathbb{Q}[X]$ n'est pas résoluble par radicaux, puisque son groupe de Galois est isomorphe à $\mathfrak{S}_5$, qui n'est pas résoluble (cf. exemple IV.3.10).

Il est en revanche bien connu qu'un polynôme de degré $\leq 4$ est résoluble par radicaux. C'est évident pour les degrés 1 et 2. Pour le degré 3, la méthode de Cardan permet de se ramener à la résolution d'une équation de degré 2. Pour le degré 4, la méthode de Ferrari permet quant à elle de se ramener au cas d'une équation de degré 3.

Cela peut se retrouver aisément grâce aux résultats de cette section. En effet, soit $K$ un corps de caractéristique 0, et soit $P \in K[X]$ un polynôme de degré $n \leq 4$. Comme $\mathrm{Gal}_K(P)$ est isomorphe à un sous-groupe de $\mathfrak{S}_n$, qui est résoluble, $\mathrm{Gal}_K(P)$ est résoluble. On conclut en utilisant le corollaire précédent.

## V.3. Constructions à la règle et au compas : le retour

Dans cette courte section, nous donnons une condition nécessaire et suffisante sur la constructibilité d'un nombre complexe algébrique à la règle et au compas en termes de groupe de Galois.

Théorème V.3.1. *Soit $\mathscr{A}_0$ un ensemble de points de $\mathbb{R}^2$ contenant $O = (0,0)$ et $I = (1,0)$, et soit $\alpha \in \mathbb{C}$. Les propriétés suivantes sont équivalentes :*

(1) *$\alpha$ est $\mathscr{A}_0$-constructible ;*

6. À ne pas confondre avec l'Abel de Cadix, qui lui a des yeux de velours.

(2) *$\alpha$ est contenu dans une extension galoisienne $L/\mathbb{Q}(\mathscr{A}_0)$ dont le degré est une puissance de 2 ;*
(3) *$\alpha$ est algébrique sur $\mathbb{Q}(\mathscr{A}_0)$ et $\mathrm{Gal}_{\mathbb{Q}(\mathscr{A}_0)}(\mu_{\alpha,\mathbb{Q}(\mathscr{A}_0)})$ est un 2-groupe.*

*Démonstration.* Pour alléger les notations, posons $K = \mathbb{Q}(\mathscr{A}_0)$.

(1) $\Longrightarrow$ (2). Si $\alpha$ est un nombre complexe $\mathscr{A}_0$-constructible, il est contenu dans une extension $F/K$ 2-décomposable. Le lemme V.2.19 montre alors que $F/K$ est une sous-extension d'une extension galoisienne $L/K$ dont le degré est une puissance de 2. Comme $\alpha \in F$, on obtient le résultat voulu.

(2) $\Longrightarrow$ (3). Puisque $\alpha$ est contenu dans une extension de $K$ de degré fini, il est algébrique sur $K$. De plus, puisque $\alpha \in L$, l'extension normale $L/K$ contient une racine de $\mu_{\alpha,K}$, et donc les contient toutes.

Ainsi, on a
$$\mathrm{Dec}_K(\mu_{\alpha,K}) \subset L.$$
Comme $[\mathrm{Dec}_K(\mu_{\alpha,K}) : K]$ divise $[L : K]$, $[\mathrm{Dec}_K(\mu_{\alpha,K}) : K]$ est aussi une puissance de 2. Comme l'extension $\mathrm{Dec}_K(\mu_{\alpha,K})/K$ est galoisienne, on en déduit que $\mathrm{Gal}_K(\mu_{\alpha,K})$ est un 2-groupe.

(3) $\Longrightarrow$ (1). Soit $G = \mathrm{Gal}_K(\mu_{\alpha,K})$. Comme $G$ est un 2-groupe, d'après le théorème V.2.10, il existe une suite de composition
$$G_r = \{\mathrm{Id}\} \lhd G_{r-1} \lhd \cdots \lhd G_1 \lhd G_0 = G,$$
où $[G_i : G_{i+1}] = 2$ pour tout $i \in [\![0, r-1]\!]$. En posant $F_i = \mathrm{Dec}_K(\mu_{\alpha,K})^{G_i}$, on obtient une tour d'extensions
$$K \subset F_0 \subset \cdots \subset F_{r-1} \subset F_r = \mathrm{Dec}_K(\mu_{\alpha,K}).$$
De plus, par le lemme d'Artin, on a $[F_{i+1} : F_i] = [G_i : G_{i+1}] = 2$ pour tout entier $i \in [\![0, r-1]\!]$. Ainsi, l'extension $\mathrm{Dec}_K(\mu_{\alpha,K})/K$ est 2-décomposable et contient $\alpha$. Cela achève la démonstration. □

Remarque V.3.2. Ce théorème permet de retrouver de façon plus directe que $\zeta_n$ est constructible si, et seulement si, $\varphi(n)$ est une puissance de 2. En effet, on a $\mu_{\zeta_n,\mathbb{Q}} = \Phi_n$, et $\mathrm{Dec}_{\mathbb{Q}}(\Phi_n) = \mathbb{Q}(\zeta_n)$, qui est de degré $\varphi(n)$. On a donc
$$|\mathrm{Gal}(\mu_{\zeta_n,\mathbb{Q}})| = \varphi(n),$$
et l'on applique alors le théorème V.3.1.

Exemple V.3.3. Soit $P = X^4 - X - 1 \in \mathbb{Q}[X]$, et soit $X_P$ l'ensemble des racines complexes de $P$.

On vérifie que $P$ est irréductible modulo 2. En effet, $\overline{P}$ n'a pas de racines dans $\mathbb{F}_2$, et n'est pas divisible par l'unique polynôme unitaire de degré

2 irréductible de $\mathbb{F}_2[X]$, à savoir $X^2 + X + \overline{1}$. De manière alternative, on peut utiliser la proposition I.3.11, et remarquer que $P$ n'a pas de racines dans $\mathbb{F}_2$ et dans $\mathbb{F}_4$, puisque si $x \in \mathbb{F}_4$, on a $x^4 - x - 1 = -1 \neq 0$.

Soit $\alpha \in X_P$. On a donc $\mu_{\alpha,\mathbb{Q}} = P$. Remarquons maintenant que

$$\overline{P} = (X + \overline{4})(X^3 + \overline{3}X^2 + \overline{2}X + \overline{5}) \in \mathbb{F}_7[X].$$

Le deuxième facteur est irréductible, car il n'a pas de racines dans $\mathbb{F}_7$. D'après le théorème IV.3.9, le groupe $\mathrm{Gal}_{\mathbb{Q}}(P)$ $\big($identifié à un sous-groupe de $\mathfrak{S}(X_P)\big)$ contient un 3-cycle. En particulier, $3 \mid |\mathrm{Gal}_{\mathbb{Q}}(P)|$. On en déduit que $\alpha$ n'est pas constructible à la règle et au compas.

On peut même préciser ici le groupe de Galois. L'irréductibilité de $P$ modulo 2 montre que $\mathrm{Gal}_{\mathbb{Q}}(P)$ contient un 4-cycle. Ainsi, $4 \mid |\mathrm{Gal}_{\mathbb{Q}}(P)|$, et par conséquent $12 \mid |\mathrm{Gal}_{\mathbb{Q}}(P)|$. Comme $\mathrm{Gal}_{\mathbb{Q}}(P)$ s'identifie à un sous-groupe de $\mathfrak{S}(X_P)$, qui est d'ordre 24, $\mathrm{Gal}_{\mathbb{Q}}(P)$ est donc d'ordre 12 ou 24. Il est donc isomorphe à $\mathfrak{A}(X_P)$ ou $\mathfrak{S}(X_P)$ (car le groupe alterné est l'unique sous-groupe d'indice 2 du groupe symétrique). Or, on vérifie que $P$ a exactement deux racines réelles, et par conséquent deux racines complexes conjuguées. La conjugaison complexe induit alors une transposition de $\mathfrak{S}(X_P)$. Cela exclut la première possibilité. Finalement, on a

$$\mathrm{Gal}_{\mathbb{Q}}(P) \simeq \mathfrak{S}(X_P) \simeq \mathfrak{S}_4.$$

Corollaire V.3.4. *Soit $\mathscr{A}_0$ un ensemble de points de $\mathbb{R}^2$ contenant les deux points $O = (0,0)$ et $I = (1,0)$, et soit $P \in \mathbb{Q}(\mathscr{A}_0)[X]$. Les propriétés suivantes sont équivalentes :*

(1) *toute racine de $P$ est $\mathscr{A}_0$-constructible ;*
(2) $\mathrm{Dec}_{\mathbb{Q}(\mathscr{A}_0)}(P)$ *est contenu dans une extension galoisienne de $\mathbb{Q}(\mathscr{A}_0)$ dont le degré est une puissance de 2 ;*
(3) *le groupe $\mathrm{Gal}_{\mathbb{Q}(\mathscr{A}_0)}(P)$ est un 2-groupe.*

*Démonstration.* Posons $K = \mathbb{Q}(\mathscr{A}_0)$.

(1) $\Longrightarrow$ (2). Soient $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ les racines complexes de $P$. Par hypothèse, chaque $\alpha_i$ est $\mathscr{A}_0$-constructible, donc contenu dans une extension galoisienne $L_i/K$ dont le degré est une puissance de 2. Posons

$$L = L_1 \cdots L_n.$$

Alors, l'extension $L/K$ est galoisienne. De plus, le lemme IV.2.9 et une récurrence facile montrent que le groupe $\mathrm{Gal}(L/K)$ s'identifie à un sous-groupe de $\mathrm{Gal}(L_1/K) \times \cdots \times \mathrm{Gal}(L_n/K)$, qui est un 2-groupe. En particulier, $\mathrm{Gal}(L/K)$ est un 2-groupe et $[L : K]$ est une puissance

de 2. Comme $L/K$ contient toutes les racines de $P$, elle contient aussi $\mathrm{Dec}_K(P)$.

(2) $\Longrightarrow$ (3). Soit $L/K$ une extension galoisienne dont le degré est une puissance de 2, et contenant $\mathrm{Dec}_K(P)$. Comme $\mathrm{Dec}_K(P)/K$ est galoisienne, son groupe de Galois est isomorphe à un quotient de $\mathrm{Gal}(L/K)$ par la correspondance de Galois, donc est aussi un 2-groupe.

(3) $\Longrightarrow$ (1). Comme $\mathrm{Dec}_K(P)/K$ est galoisienne de degré une puissance de 2 et contient toutes les racines de $P$, il suffit d'appliquer le théorème précédent pour conclure. $\square$

# Index


clôture
  algébrique, 43
  galoisienne, 77
  normale, 74
compositum, 23
corps
  algébriquement clos, 43
  de décomposition, 43
  des racines, 43
  parfait, 64
critère de Wantzel, 19, 28

degré
  d'un élément, 22
  d'une extension, 12

élément
  exprimable par radicaux, 111
  primitif, 58
  séparable, 51
extension de corps
  2-décomposable, 18
  abélienne, 88
  algébrique, transcendante, 20
  cyclique, 88
  définition, 11
  de Kummer, 96
  galoisienne, 75
  monogène, 13
  normale, 72
  résoluble, 112
  radicale, 110
  séparable, 51
extensions de corps linéairement
    disjointes, 26

groupe de Galois
  d'un polynôme, 81
  d'une extension, 33

lemme
  d'Artin, 102
  d'indépendance de Dedekind, 49

monoïde, 48
morphisme
  d'extensions, 12
  de monoïdes, 48

nombre de Fermat, 32
norme, 66

plongement, 48
polynôme
  cyclotomique, 89
  minimal
    d'un élément algébrique, 21
  résoluble par radicaux, 111
  séparable, 51

sous-extension
  définition, 12
  engendrée par une partie, 13

théorème
  90 de Hilbert, 97
  de Gauss (polygones
    constructibles), 38
  de Kummer, 98
  de l'élément primitif, 57
  de la correspondance de Galois,
    105
  de prolongement des
    isomorphismes, 34
trace, 66