Théorie de Galois

D'après le cours du prof. J. Thévenaz
TEXé par C. Ho Thanh

Printemps 2014

Table des matières

Introduction

Définition. Ce polycopié est la retranscription non officielle des notes du cours de théorie de Galois, donné par le professeur J. Thévenaz durant le semestre de printemps 2014.

Corollaire. *Malgré de nombreuses relectures, des erreurs peuvent subsister... ce polycopié est donc fourni sans garantie !*

Chapitre 1

Notions de base

1.1 Anneaux de polynomes

Soit K un corps, et $K[X]$ l'anneau des polynomes à coefficients dans K.

Théorème 1.1.1. *$K[X]$ est principal.*

Théorème 1.1.2. *Soit $f \in K[X]$, $f \neq 0$. Les conditions suivantes sont équivalentes :*

1. *(f) est un idéal premier,*
2. *$K[X]/(f)$ est intègre,*
3. *(f) est maximal,*
4. *$K[X]/(f)$ est un corps,*
5. *f est irréductible.*

On utilise le point 4. pour construire des corps. Par exemple
— $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$, $i = \bar{X}$,
— $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$.

1.2 Critères d'irréductibilité

Définition 1.2.1 (Element irréductible)**.** Soit A une anneau commutatif, et $a \in A$. Alors a est *irréductible* si a est non nul, non inversible, et si pour toute décomposition $a = bc$, b ou c est inversible.

Exemple 1.2.2.
1. Si $A = \mathbb{Z}$, alors un nombre est irréductible si et seulement s'il est premier.
2. Si $A = K[X]$, alors les deux définitions de polynome irréductible coincident.

Définition 1.2.3 (Anneau factoriel)**.** Un anneau A est *factoriel* si A est commutatif, intègre, et si tout élément non nul non inversible $a \in A$ peut s'écrire comme $a = up_1 \cdots p_n$, avec $u \in A^*$, $p_1, \ldots, p_n$ irréductibles, de manière essentiellement unique, i.e. si $a = vq_1 \cdots q_m$ avec des conditions similaires, alors $n = m$, et $\exists \sigma \in \mathfrak{S}_n$ tel que p_i et $q_{\sigma(i)}$ sont associés.

Théorème 1.2.4. *Tout anneau principal est factoriel.*

Théorème 1.2.5. *Soit A un anneau factoriel et soit $K = \operatorname{Frac} A$. Soit $f = a_0 + a_1X + \cdots \in A[X]$, tel que $\deg f \geq 1$, et $\operatorname{pgcd}(a_1, \ldots) = 1$. Alors f est irréductible dans $A[X]$ si et seulement si il l'est dans $K[X]$.*

Théorème 1.2.6 (Critère de réduction modulo q)**.** *Sous les mêmes hypothèses que précédemment, soit $q \in A$ irréductible. Si $\bar{f} \in (A/(q))[X]$ est irréductible, alors f l'est aussi dans $A[X]$, et donc dans $K[X]$.*

Exemple 1.2.7. Si $A = \mathbb{Z}$, $q = 2$, $f = X^3 + 16X + 7X - 2015$, alors $\bar{f} = X^3 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ est irréductible car $\deg \bar{f} = 3$ et $\bar{f}$ n'admet pas de racine dans $\mathbb{Z}/2\mathbb{Z}$. Donc f est irréductible dans $\mathbb{Q}[X]$, et $\mathbb{Q}[X]/(X^3 + 16X + 7X - 2015)$ est un corps.

Théorème 1.2.8 (Critère d'Eisenstein)**.** *Sous les mêmes hypothèses que le théorème précédent, soit $f = a_nX_n + \cdots + a_1X + a_0 \in A[X]$. Soit $q \in A$ irréductible tel que $q \not| a_n$, $q|a_i$, $0 \leq i \leq n-1$, $q^2|a_0$. Alors f est irréductible dans $A[X]$.*

Exemple 1.2.9. Si $A = F[t]$, avec F un corps, $K = F(t) = \operatorname{Frac} A$ le corps des fractions rationelles, $f = X^{2014} - t \in A[X]$, alors on prend $q = t$, qui est irréductible dans A. On a $t \not| 1$, $t|t$, $t^2 \not| t$. Donc f est irréductible dans $A[X]$, et donc dans $K[X]$.

1.3 Dérivation

Soit K un corps, et posons

$$\begin{aligned} D : K[X] &\longrightarrow K[X] \\ X^s &\longmapsto sX^{s-1}. \end{aligned}$$

Remarquer que D est K-linéaire, $D(fg) = D(f)g + fD(g)$, $D((X-a)^m) = m(X-a)^{m-1}$. On note $f' = D(f)$, $\forall f \in A[X]$.

Proposition 1.3.1. *Soit $f \in A[X]$, $a \in A$ une racine de f. Alors a est une racine multiple de f si et seulement si c'est aussi une racine de f'.*

1.4 Caractéristique d'un corps

Soit K un corps, et considérons

$$\begin{aligned} \eta : \mathbb{Z} &\longrightarrow K \\ n &\longmapsto \operatorname{sgn}(n)(\underbrace{1 + \cdots + 1}_{n \text{ fois}}). \end{aligned}$$

C'est un homomorphisme d'anneaux, donc $\mathbb{Z}/\ker\eta$ est un anneau intègre, et donc $\ker\eta$ est un idéal premier. On a deux possibilités :

1. $\ker\eta = 0$, et on dit que K est de *caractéristique* 0. On a que η est injective, et on a une injection induite $\mathbb{Q} \hookrightarrow K$.

2. $\ker \eta = (p)$, avec p premier, et on dit que K est de caractéristique p. On a alors une injection induite par le 1er théorème d'isomorphisme $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow K$.

On note $\operatorname{car} K$ la caractéristique de K.

Proposition 1.4.1. *Soit $f \in K[X]$, $\deg f \geq 1$.*

1. *Si $\operatorname{car} K = 0$, alors $f' \neq 0$.*
2. *Si $\operatorname{car} K = p \neq 0$, alors $f' = 0$ si et seulement si f est un polynome en X^p, i.e. $f = g(X^p)$, pour un certain $g \in K[X]$.*

Chapitre 2

Extensions de corps

2.1 Généralités

Rappel 2.1.1. Tout homomorphisme de coprs est injectif ou nul.

Définition 2.1.2 (Extension de corps)**.** Soit K un corps. Une *extension* de K est un corps E contenant K comme sous coprs. On note

$$\begin{array}{c} E \\ | \\ K. \end{array}$$

On a une structure naturelle de K-espace vectoriel sur E, et on note $[E : K] = \dim_K E$ de *degré de l'extension*.

Théorème 2.1.3. *Si*

$$\begin{array}{c} F \\ | \\ E \\ | \\ K, \end{array}$$

alors $[F : K] = [F : E][E : K]$.

Démonstration. Soit $\{x_i \mid i \in I\}$ une K-base de E, et $\{y_j \mid j \in J\}$ une E-base de F. On montre que $B = \{x_i y_j \mid (i, j) \in I \times J\}$ est une K-base de F.

— Soit $f \in F$. Alors :

$$\begin{aligned} f &\overset{\exists}{=} \sum_{j\in J} e_j y_j \\ &\overset{\exists}{=} \sum_{j\in J} y_j \sum_{i\in I} k_{i,j} x_i \\ &= \sum_{(i,j)\in I\times J} k_{i,j} x_i y_j. \end{aligned}$$

Donc B est une partie génératrice.

— On a

$$\begin{aligned} &\sum_{(i,j)\in I\times J} k_{i,j}x_iy_j = \sum_{j\in J} y_j \sum_{i\in I} k_{i,j}x_i = 0 \\ \implies &\sum_{i\in I} k_{i,j}x_i = 0 && \forall j \in J \\ \implies &k_{i,j} = 0 && \forall (i,j) \in I \times J. \end{aligned}$$

□

Notation 2.1.4. Si E est une extension de K, et $\alpha \in E$, on note

— $K[\alpha] = \{f(\alpha) \mid f \in K[X]\}$, l'anneau des expressions polynomiales en α, c'est le plus petit sous anneau de E contenant à la fois K et α,

— $K(\alpha) = \operatorname{Frac} K[\alpha]$, le corps des expressions rationelles en α, le plus petit sous corps de E contenant à la fois K et α.

Plus généralement, si $\alpha_1, \ldots, \alpha_n \in E$, on définit

— $K[\alpha_1, \ldots, \alpha_n] = K[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n]$,

— $K(\alpha_1, \ldots, \alpha_n) = \operatorname{Frac} K[\alpha_1, \ldots, \alpha_n]$ dans E. On dit que $K(\alpha_1, \ldots, \alpha_n)$ est de *type fini* sur K.

Exemple 2.1.5. En considérent $\mathbb{C}$ comme une extension de $\mathbb{R}$, on a $\mathbb{R}[i] = \mathbb{C} = \mathbb{R}(i)$.

2.2 Extensions simples

Une extension E de K est *simple* s'il existe $\alpha \in E$ tel que $E = K(\alpha)$. Il y a deux types d'extensions simples. Considérons $\mathrm{ev}_\alpha : K[X] \longrightarrow K(\alpha)$, l'évaluation en α.

— Si ev_α est injective, alors $K[X] \cong K[\alpha]$, $K \leq K[\alpha] < K(\alpha) = E$, et on dit que α est *transcendant* sur K. Dans ce cas, $K[\alpha]$ est un K-espace vectoriel de dimension infinie, et de base $(1, \alpha, \alpha^2, \ldots)$. Donc $[K[\alpha] : K] = \infty$. Par exemple, e et π sont transcendants sur $\mathbb{Q}$.

— Si ev_α n'est pas injective, donc si $\ker \mathrm{ev}_\alpha \neq 0$, on dit que α est *algébrique* sur K. On a $\ker \mathrm{ev}_\alpha = (f)$, pour un certain f unitaire, car $K[X]$ est principal. On appelle f le *polyome minimal* de α, et on note $f = \min(\alpha, K)$. On a que $K[X]/(f) \cong \operatorname{im} \mathrm{ev}_\alpha \leq K[\alpha]$ qui est un anneau intègre. Donc f est premier, et donc irréductible. Ainsi, $K[\alpha]$ est un corps, et $K(\alpha) = K[\alpha]$. De plus, $K[\alpha]$ possède une K-base finie : $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$, où $n = \deg f$, et donc $[K[\alpha] : K] = n$. Par exemple, i, $\sqrt{2}$, $\sqrt[7]{181}$ sont algébriques sur $\mathbb{Q}$.

Les considérations du 2eme point nous disent comment construire des extensions algébriques : on part d'un polynome irréductible $f \in K[X]$, et on pose $E = K[X]/(f)$. C'est un corps contenant K comme sous corps, et c'est une extension simple, engendrée par $\alpha = \bar{X}$.

Exemple 2.2.1. $\mathbb{F}_5 < \mathbb{F}_5[X]/(X^2 - 2) = \mathbb{F}_{25}$.

Remarquer qu'une extension finie est algébrique.

2.3 Transitivité des extensions algébriques

Théorème 2.3.1. *Si*

$$\begin{array}{c} F \\ \big| \text{ alg.} \\ E \\ \big| \text{ alg.} \\ K, \end{array}$$

alors F est une extension algébrique de K.

Démonstration. Soit $\beta \in F$, alors β est algébrique sur E, i.e. β est racine d'un certain $f \in E[X]$, où $f = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_1 X + \alpha_0$. Alors $\alpha_0, \ldots, \alpha_{n-1} \in E$ sont algébriques sur K, et $K[\alpha_0, \ldots, \alpha_{n-1}]$ est une extension algébrique de degré fini sur K (ex. 5, série 2). Donc $K[\alpha_0, \ldots, \alpha_{n-1}, \beta]$ est une extension finie de K, et donc algébrique.

$$\begin{array}{c} K[\alpha_0, \ldots, \alpha_{n-1}][\beta] \\ \big| \text{ fin.} \\ K[\alpha_0, \ldots, \alpha_{n-1}] \\ \big| \text{ fin.} \\ K. \end{array}$$

□

Corollaire 2.3.2. *Soit E une extension de K, $\alpha, \beta \in E$. Si α et β sont algébrique sur K, alors $\alpha+\beta$, $\alpha - \beta$, $\alpha\beta$, et α/β le sont aussi.*

Démonstration.

$$\begin{array}{c} K[\alpha, \beta] \\ \big| \text{ alg.} \\ K[\alpha] \\ \big| \text{ alg.} \\ K. \end{array}$$

□

Définition 2.3.3. Soit K un corps, $f \in K[X]$. Un *corps de décomposition* de f est une extension E de K telle que

— f est scindé sur E,
— E est engendré par les racines de f.

Proposition 2.3.4. *Un tel corps existe.*

Démonstration. Par récurrence sur le degré n de $\deg f$. On choisi un facteur irrédictible g de f, et on construit l'extension $K[\alpha_1] = K[X]/(g)$. On a que α_1 est une racine de g dans ce nouveau corps, et donc de f. On considère ensuite f dans $K[\alpha_1][X]$, et on a une factorisation $f = (X - \alpha_1)h$, et h est de degré $n - 1$. On conclu par récurrence. □

Proposition 2.3.5. *Soit K un corps. Les conditions suivantes sont équivalentes :*

1. *tout polynome dans $K[X]$ est scindé,*
2. *tout polynome de degré au moins 1 possède une racine dans K,*
3. *tout polynome irréductible est de degré 1,*
4. *tout extension algébrique de K est égale à K.*

Définition 2.3.6. Un tel corps est dit *algébriquement clos*.

Théorème 2.3.7. *Soit K un corps. Alors il existe une extension algébriquement close E de K.*

Démonstration (Artin). — On va construire une extension F_1 de K dans laquelle tout polynome $f \in K[X]$ possède une racine. Soit $K[X]_{\geq 1}$ l'ensemble des polynomes de $K[X]$ de degré au moins 1. Prenons une indéterminée X_f, pour chaque $f \in K[X]_{\geq 1}$, et posons $A = K[X_f \mid f \in K[X]_{\geq 1}]$. Soit I l'idéal de A généré par les éléments $f(X_f)$. Assertion : $I \neq A$. Dans ce cas, il existe un idéal maximal $\mathfrak{m} \supseteq I$, par le théorème de Krull, et dans le corps $F_1 = A/\mathfrak{m}$, tout polynome $f \in K[X]_{\geq 1}$ admet $\overline{X_f}$ comme racine. On prouve maintenant l'assertion. Supposons que $I = A$. Alors $1 \in I$, et donc

$$1 = \sum_{j=1}^{n} h_j f_j(X_{f_j}),$$

où $h_j \in A$. Soit L une estension de K dans laquelle $f_j(X_{f_j})$ possède une racine α_j, pour $1 \leq j \leq n$. On considère l'évaluation

$$\begin{aligned} \phi : A &\longrightarrow L \\ X_{f_j} &\longmapsto \alpha_j \\ X_f &\longmapsto 0 \qquad\qquad f \neq f_j. \end{aligned}$$

C'est bien sur un homomorphisme d'anneaux. On a alors

$$\begin{aligned} 1 &= \phi(1) \\ &= \sum_{j=1}^{n} \phi(h_j)\phi(f_j(X_{f_j})) \\ &= \sum_{j=1}^{n} \phi(h_j) f_j(\alpha_j) \\ &= 0. \end{aligned}$$

On a donc prouve l'assertion.

— On construit une extension F de K avec F algébriquement clos. On considère F_2, une extension de F_1 dans laquelle tout polynome de $F_1[X]$ possède une racine (construction du point précédent). Par récurrence, on consuit F_{i+1} à partir de F_i. On a

$$K \leq F_1 \leq F_2 \leq \cdots \leq F_i \leq F_{i+1} \leq \cdots .$$

Posons $F = \bigcup_{i=1}^{\infty} F_i$. C'est clairement algébriquement clos.

□

Corollaire 2.3.8. *Pour tout corps K, il existe une extension C de K telle que*
— *C est une extension algébrique de K,*
— *C est algébriquement clos.*
Un tel corps s'appelle une cloture algébrique *de K.*

Démonstration. Par le théorème précédent, il existe une extension algébriquement close F de K. Posons $C = \{\alpha \in F \mid \alpha \text{ alg. sur } K\}$. C'est un sous corps de F contenant K, qui est algébrique sur K. Soit $\beta \in F$, avec β algébrique sur C. Alors

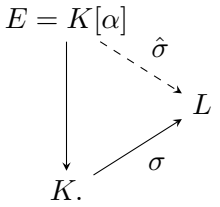
$$\begin{array}{c} C[\beta] \\ \big| \text{alg.} \\ C \\ \big| \text{alg.} \\ K, \end{array}$$

et donc β est algébrique sur K, et $\beta \in C$. Donc C est algébriquement clos. □

Remarque 2.3.9. Soit $\sigma : K \longrightarrow L$ un homomorphisme de corps. Alors σ est injectif, et se prolonge en un homomorphisme injectif d'anneaux $\sigma : K[X] \longrightarrow L[X]$.

Théorème 2.3.10 (Prolongement des homomorphismes dans le cas des extensions simples)**.** *Soit $\sigma : K \longrightarrow L$ un homomorphisme de corps, avec L algébriquement clos. Soit $E = K[\alpha]$ une extension algébrique simple de K. Alors si $f = \min(\alpha, K)$*

1. *Il existe un prolongement $\hat{\sigma} : E \longrightarrow L$. Plus précisément, pour tout racine β de $\sigma(f)$ dans L, il existe $\hat{\sigma} : E \longrightarrow L$ telle que $\hat{\sigma}(\alpha) = \beta$.*



2. *Si $\tilde{\sigma} : E \longrightarrow L$ est un prolongement de σ, alors $\tilde{\sigma}(\alpha)$ est une racine de $\sigma(f)$.*
3. *Le nombre de prolongement de σ sur E est égale au nombre de racine de $\sigma(f)$ dans L.*
4. *Le nombre de prolongement de σ sur E est au plus $[E : K]$.*

Démonstration. 1. Soit $\beta \in L$ une racine de $\sigma(f)$. On a que σ induit un isomorphisme $\sigma : K \xrightarrow{\cong} K' = \sigma(K) \leq L$, et donc un isomorphisme d'anneaux $\sigma : K[X] \xrightarrow{\cong} K'[X]$. Ainsi, $\sigma(f)$ est irréductible dans $K'[X]$, car f l'est dans $K[X]$. On obtient

$$\begin{array}{ccccc} K[X] & \xrightarrow{\sigma} & K'[X] & \xrightarrow{\pi} & K'[X]/(\sigma(f)) \cong K'[\beta] \\ \downarrow & & & \nearrow_{\hat{\sigma}} & \\ K[X]/(f) \cong K[\alpha] & & & & \end{array}$$

car $\ker \pi \circ \sigma = (f)$. On a bien un prolongement de σ tel que $\hat{\sigma}(\alpha) = \beta$.

2. Soit $\tilde{\sigma} : E \longrightarrow L$ un prolongement de $\sigma : K \longrightarrow L$. Si $f = \sum_i a_i X^i$, alors $\sigma(f) = \sum_i \sigma(a_i) X^i$, et

$$\begin{aligned} \sigma(f)(\tilde{\sigma}(\alpha)) &= \sum_i \underbrace{\sigma(a_i)}_{=\tilde{\sigma}(a_i)} \tilde{\sigma}(\alpha)^i \\ &= \tilde{\sigma}(f(\alpha)) \\ &= 0. \end{aligned}$$

3. Clair à partir des points précédents.
4. Clair à partir des points précédents.

□

Théorème 2.3.11 (Prolongement des homomorphismes, cas général)**.** *Soit $\sigma : K \longrightarrow L$ un homomorphisme de corps, avec L algébriquement clos.*

1. *Soit E une extension finie de K. Alors σ se prolonge en $\hat{\sigma} : E \longrightarrow L$. Le nombre de tels prolongements est au plus $[E : K]$.*

2. Soit E une extension algébrique de K. Alors σ se prolonge en $\hat{\sigma} : E \longrightarrow L$.

Démonstration. 1. Si E est une extension finie, alors $E = K[\alpha_1, \ldots, \alpha_n]$, avec α_i algébrique sur $K[\alpha_1, \ldots, \alpha_{i-1}]$, et donc sur K. On applique le théorème précédent.

2. On utilise le lemme de Zorn. Soit $\mathcal{E}$ l'ensemble de toutes les paires (F, τ), où $K \leq F \leq E$, et $\tau : F \longrightarrow L$ est un prolongement de σ. Alors $\mathcal{E}$ est inductivement ordonné par l'ordre suivant :

$$(F_1, \tau_1) \preceq (F_2, \tau_2) \iff \begin{cases} F_1 \leq F_2, \\ \tau_2|_{F_1} = \tau_1. \end{cases}$$

Donc il existe un élément maximal $(G, \eta) \in \mathcal{E}$. On montre que $G = E$. Soit $\alpha \in E$. Alors α est algébrique sur K, et donc aussi sur G. Ainsi, $(G, \eta) \prec (G[\alpha], \hat{\eta})$, ce qui montre que $G = G[\alpha]$, et donc que $\alpha \in G$. Ainsi, $G = E$, et $\eta : E \longrightarrow L$ prolonge σ.

□

Définition 2.3.12 (Corps de décomposition)**.** Soit $\mathcal{F} \subseteq K[X]$. Un *corps de décomposition* de $\mathcal{F}$ est une extension algébrique E de K telle que

1. tout polynome $f \in \mathcal{F}$ est scindé dans E,
2. E est engendré par les racines de $\mathcal{F}$, i.e. $\bigcup_{f \in \mathcal{F}} R_f$, où R_f est l'ensemble des racindes de f.

Proposition 2.3.13. *Un tel corps existe toujours. Si E_1 et E_2 sont deux tels corps, alors il existe un K-isomorphisme $\sigma : E_1 \longrightarrow E_2$, i.e. un isomorphisme tel que $\sigma|_K = \mathrm{id}_K$.*

Démonstration. Existence : Soit $\bar{K}$ une cloture algébrique de K. Posons E le sous corps de $\bar{K}$ engendré par K et $\bigcup_{f \in \mathcal{F}} R_f$.

Unicité : Soient $\bar{E}_1$ et $\bar{E}_2$ des clotures algébriques de E_1 et E_2 respectivement. On a un prolongement $\sigma : E_1 \longrightarrow \bar{E}_2$ de l'identité $\mathrm{id}_K : K \longrightarrow K$.

$$\begin{array}{ccc} \bar{E}_1 & & \bar{E}_2 \\ | & \overset{\sigma}{\nearrow} & | \\ E_1 & & E_2 \\ | & & | \\ K & \xrightarrow{\mathrm{id}_K} & K. \end{array}$$

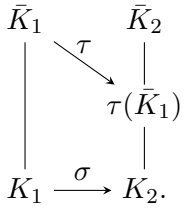
De plus, si $f \in \mathcal{F}$, et $\alpha \in R_f$ une racine de f dans E_1, alors $\sigma(\alpha) \in R_f$ dans $\bar{E}_2$. Donc $\sigma(\alpha) \in E_2$. Ainsi, on a une injection $\sigma : R_f \subseteq E_1 \longrightarrow R_f \subseteq E_2$ entre deux ensembles finis, qui est donc une bijection. Donc $\sigma : E_1 \longrightarrow E_2$ est une injection contenant tous les générateurs de E_2, et c'est donc un K-isomorphisme $\sigma : E_1 \longrightarrow E_2$.

□

Théorème 2.3.14 (Unicité de la cloture algébrique)**.** *1. Soient $\sigma : K_1 \xrightarrow{\cong} K_2$ un isomorphisme de corps. Soit $\bar{K}_i$ une cloture algébrique de K_i. Alors il existe un isomorphisme $\tau : \bar{K}_1 \xrightarrow{\cong} \bar{K}_2$ qui prolonge σ.*

2. Soit K un corps, et soient E_1 et E_2 deux clotures algébriques de K. Alors elles sont K-isomorphes, i.e. il existe un K-isomorphisme $\tau : E_1 \xrightarrow{\cong} E_2$.

Démonstration. 1. Par le théorème de prolongement, on a :



Comme $\bar{K}_1$ est algébriquement clos, $\tau(\bar{K}_1)$ l'est aussi. De plus, $\bar{K}_2$ est une extension algébrique de K_2, et donc de $\tau(\bar{K}_1)$. Ainsi, $\tau(\bar{K}_1) = \bar{K}_2$.

2. Clair.

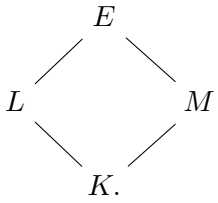
□

On note $\bar{K}$ la clotude algébrique de K. On considère maintenant les corps de décomposition dans les clotures algébriques, et ils deviennent alors uniques.

Exemple 2.3.15. $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algébrique sur } \mathbb{Q}\}$ est l'ensemble des nombres algébriques.

2.4 Composée de deux corps

Soit



Le *composé* de L et M est le plus petit sous corps de E contenant L et M, et est noté $L \vee M$.

Lemme 2.4.1 (Cas particuliers)**.** *1. Si $L = K[\alpha_1, \ldots, \alpha_r]$, alors $L \vee M = M[\alpha_1, \ldots, \alpha_r]$.*

2. Si de plus $M = K[\beta_1, \ldots, \beta_s]$, alors $L \vee M = K[\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s]$.

Démonstration. Clair. □

Chapitre 3

Extensions normales

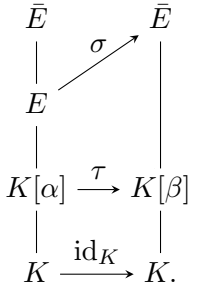
Théorème 3.0.2. *Soit E une extension algébrique de K. Les conditions suivantes sont équivalentes :*

1. *E est le corps de décomposition d'une certaine famille $\mathcal{F} \subseteq K[X]$,*
2. *tout K-homomorphisme $\sigma : E \longrightarrow \bar{E}$ est tel que $\sigma(E) = E$,*
3. *tout K-homomorphisme $\sigma : E \longrightarrow \bar{E}$ est tel que $\sigma(E) \leq E$,*
4. *pour tout polynome irréductible $f \in K[X]$, si f a une racine dans E, alors il a toutes ses racines dans E, i.e. il est scindé dans E.*

Démonstration. 1. $\implies$ 2. On suppose que E est le corps de décomposition de $\mathcal{F} \subseteq K[X]$. Soit $\sigma : E \longrightarrow \bar{E}$ un K-homomorphisme. Alors $\forall f \in \mathcal{F}$, f possède toute ses racines dans E, et $\forall \alpha \in R_f$, $\sigma(\alpha) \in R_f$ dans $\bar{E}$. Donc $\sigma(\alpha) \in E$. Ainsi, $\sigma : R_f \subseteq E \longrightarrow R_f \subseteq \bar{E}$ est une injection entre deux ensembles finis, et donc une bijection. Ainsi, $\sigma(E) = E$.

2. $\implies$ 3. Sérieusement ?

3. $\implies$ 4. Soit $f \in K[X]$ un polynome irréductible avec une racine $\alpha \in E$. Soit β une autre racine de f dans $\bar{E}$. Par le théorème de prolongement, il existe $\tau : K[\alpha] \longrightarrow \bar{E}$ un prolongement de σ tel que $\tau(\alpha) = \beta$, et ainsi, τ corestreint en $\tau : K[\alpha] \longrightarrow K[\beta]$. Il se prolonge à son tour en $\sigma : E \longrightarrow \bar{E}$, qui est forcément tel que $\sigma(E) \leq E$.



Donc $\sigma(\alpha) = \beta \in \sigma(E) \leq E$.

4. $\implies$ 1 On a que $E = K[\alpha_i \mid i \in I]$, avec α_i des générateurs. Soit $\mathcal{F} = \{\min(\alpha_i, K) \mid i \in I\}$. Par hypothèse, si $f = \min(\alpha_i, K)$, alors toutes les racines de f sont dans E. Donc E est engendré

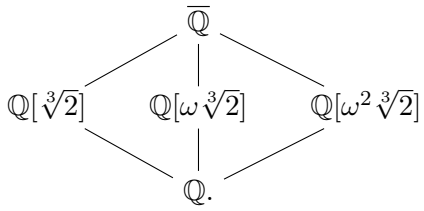
par K et les racines de $\mathcal{F}$. De plus, chaque $f \in \mathcal{F}$ est scindé dans E. Donc E est un corps de décomposition de $\mathcal{F}$.

□

Une telle extension est dite *normale*.

Exemples 3.0.3. 1. Toute extension E de K de degré 2 est normale. En effet, $E = K[\alpha]$, avec $\min(\alpha, K) = f = X^2 + bX + c$. Si α' est l'autre racine de f, alors $b = \alpha + \alpha'$. Ainsi, $\alpha' = -b - \alpha \in K[\alpha]$, et il s'agit bien d'une extension normale.

2. $\mathbb{Q}[\sqrt[3]{2}] \leq \mathbb{R}$ est une extension de $\mathbb{Q}$ de polynome minimal $X^3 - 2$. Les racines sont $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, et $\omega^2\sqrt[3]{2}$, où $\omega = \frac{-1+i\sqrt{3}}{2}$ est une racine cubique de 1. Clairement $\omega\sqrt[3]{2} \notin \mathbb{R}$, donc $\omega\sqrt[3]{2} \notin \mathbb{Q}[\sqrt[3]{2}]$, et cette extension n'est pas normale.



3. Soit ξ une racine primitive p-ième de l'unité, avec p premier, et considérons $\mathbb{Q}[\xi]$ comme extension de $\mathbb{Q}$. On sait que ξ est une racine de $X^p - 1$, et donc $\min(\xi, \mathbb{Q})|(X^p - 1)$. Les autres racines sont des puissances de ξ, donc des éléments de $\mathbb{Q}[\xi]$. Ainsi, $\mathbb{Q}[\xi]$ est une extension normale de $\mathbb{Q}$.

4. Considérons le corps $\mathbb{K}_p(t)$, et $f = X^p - t$, qui est irréductible par le critère d'Eisenstein. Si α est une racine de f, alors $f = X^p - \alpha^p = (X - \alpha)^p$, ce qui montre que α est l'unique racine de f. Donc $\mathbb{F}_p(t)[\alpha]$ est une extension normale de $\mathbb{F}_p(t)$.

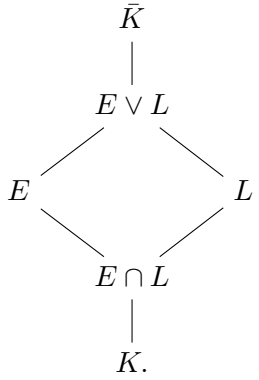
5. On a une tour d'extensions normales :

$$\begin{array}{c} \mathbb{Q}[\sqrt[4]{2}] \\ 2 \,| \\ \mathbb{Q}[\sqrt{2}] \\ 2 \,| \\ \mathbb{Q}. \end{array}$$

Pourtant, $\mathbb{Q}[\sqrt[4]{2}]$ n'est pas une extension normale de $\mathbb{Q}$...

Proposition 3.0.4. *1. Soient $K \leq F \leq E$ des extensions de K. Alors si E est normal sur K, il l'est aussi sur F.*

2. *Soit*



   Si E est normal sur K, alors $E \vee L$ l'est sur L.

3. *Si E et L sont normal sir K, aors $E \cap L$ et $E \vee L$ aussi.*

Démonstration. 1. On a que $E = K[R]$, où R est l'ensemble des racines d'une famille de polynomes de $K[X]$. On a que $E = F[R]$, et par conséquent, E est normale sur F.

2. Avec les mêmes notations que le point précédents, on a que $E \wedge L = K[R] \wedge K = L[R]$. Donc $E \wedge L$ est normale sur L.

3. Soit $\sigma : E \wedge L \longrightarrow \bar{K}$ un K-homomorphisme. Alors $\sigma|_L : L \longrightarrow \bar{K}$ est aussi un K-homomorphisme, et comme L est normale sur K, on a que $\sigma(L) \leq L$. De même pour E. Par conséquent, $\sigma(E \wedge L) \leq E \wedge L$, et $E \wedge L$ est normale sur K. Soit $\tau : E \cap L \longrightarrow \bar{K}$ un K-homomorphisme. Alors τ se prolonge en $\tilde{\tau} : E \longrightarrow \bar{K}$ et $\bar{\tau} : L \longrightarrow \bar{K}$. Comme E est normale sur K, on a que $\tilde{\tau}(E) \leq E$. De même, $\bar{\tau}(L) \leq L$. Donc $\tau(E \cap L) \leq \tilde{\tau}(E) \cap \bar{\tau}(L) \leq E \cap L$, et $E \cap L$ est normale sur K.

□

Définition 3.0.5 (Cloture normale)**.** Soit E une extension de K dans une cloture algébrique $\bar{K}$ de K. La *cloture normale* de E dans K est

$$E^{\mathrm{nc}} = \bigcap_{\substack{E \leq F \leq \bar{K} \\ F \text{ norm. sur } K}} F.$$

Chapitre 4

Extensions séparables

4.1 Polynomes séparables

Définition 4.1.1 (Polynome séparable)**.** Soit K un corps. Un polynome irréductibe $f \in K[X]$ est dit *séparable* s'il n'a pas de racine multilpes dans $\bar{K}$. Il est dit *inséparable* sinon.

Proposition 4.1.2. *Soit $f \in K[X]$ irréductible. Alors f est séparable si et seulement si $f' \neq 0$.*

Démonstration. Soit α une racine de f dans $\bar{K}$. Alors $f = \lambda \min(\alpha, K)$, pour un certain $\lambda \in K^*$. Si α est une racine multiple, alors $f'(\alpha) = 0$, et f' est un multiple de f. Or, $\deg f' < \deg f$, et donc $f' = 0$. Réciproquement, si $f' = 0$, alors toute racine α de f dans $\bar{K}$ est une racine de f', et donc une racine multiple. □

Corollaire 4.1.3. *Si K est un corps de caractéristique 0. Alors tout polynome irréductible $f \in K[X]$ est séparable.*

Démonstration. Si $\deg f \geq 1$, alors $f' \neq 0$. □

Corollaire 4.1.4. *Soit K un corps de caractéristique p, où p est un nombre premier. Soit $f \in K[X]$ un polynome inséparable. Alors il existe $d \in \mathbb{N}^*$ et un polynome séparable $g \in K[X]$ tels que $f(X) = g(X^{p^d})$.*

Démonstration. Si f est inséparable, alors $f' = 0$. Donc f est un polynome en X^p. Soit $d \geq 1$ le plus grand entier tel que f est un polynome en X^{p^d}, i.e. tel qu'il existe $g \in K[X]$ tel que $f(X) = g(X^{p^d})$. Alors g est irréductible, car f l'est. De plus, g n'est pas un polynome en X^p par maximalité de d. Donc $g' \neq 0$, et il est séparable. □

Exemple 4.1.5. Posons $K = \mathbb{F}_p(t)$. Alors le polynome $f = X^{p^d} - t$ est irréductible par le critère d'Eisenstein. Si α est une racine de f dans $\bar{K}$, alors $\alpha^{p^d} - t = 0$, et donc $f(X) = X^{p^d} - \alpha^{p^d} = (X - \alpha)^{p^d}$, ce qui montre que α est une racine de multiplicité p^d. De plus, $f(X) = g(X^{p^d})$, où $g(X) = X - t$ est séparable.

Théorème 4.1.6. *Soit K un corps fini, de caractéristique p. Alors tout polynome irréductible $f \in K[X]$ est séparable.*

Démonstration. Soit $h \in K[X]$ un polynome en X^p. On va montrer qu'il ne peut pas être irréductible. Ecrivons $h(X) = a_0 + a_1X^p + \cdots + a_mX^{mp}$. L'application $K \longrightarrow K$, $c \longmapsto c^p$ est un homomorphisme de groupes additifs injectif, donc bijectif. Par surjectivité, $a_i = b_i^p$, pour un certain b_i, et donc

$$\begin{aligned} h(X) &= a_0 + a_1X^p + \cdots + a_mX^{mp} \\ &= b_0^p + b_1^pX^p + \cdots + b_m^pX^{mp} \\ &= (b_0 + b_1X + \cdots + b_mX^m)^p. \end{aligned}$$

Ainsi, h n'est pas irréductible. □

Définition 4.1.7 (Element séparable, extension séparable)**.** Soit E une extension algébrique de K, et soit $\alpha \in E$. On dit que α est *séparable* sur K si $\min(\alpha, K)$ est séparable. On dit que α est *inséparable* sinon. On dit que E est une *extension séparable* de K si tout élément $\alpha \in E$ est séparable sur K.

Remarque 4.1.8. Si $\operatorname{car} K = 0$, ou si K est fini, toute extension algébrique de K est séparable.

4.2 Degré de séparabilité

Définition 4.2.1 (Degré de séparabilité)**.** Soit E une extension finie de K (donc algébrique). Alors le *degré de séparabilité* de E sur K, noté $[E : K]_s$ est le nombre de K-homomorphisme $\sigma : E \longrightarrow \bar{K}$.

Lemme 4.2.2. *Soit $\hat{K}$ une cloture algébrique de K contenant E, et soit $j : K \longrightarrow \hat{K}$ un homomorphisme de corps. Alors $[E : K]_s$ est égal au nombre de prolongements de j en un homomorphisme $\tau : E \longrightarrow \hat{K}$.*

Démonstration. Il existe un prolongement de j en $\phi : \bar{K} \longrightarrow \hat{K}$.

$$\begin{array}{ccc} \bar{K} & \overset{\phi}{\dashrightarrow} & \hat{K} \\ \text{fin.}\,\big| & \nearrow_{j} & \\ K. & & \end{array}$$

On a que ϕ est nécessairement un isomorphisme, car $\phi(\bar{K})$ est algébriquement clos. Les compositions par ϕ et ϕ^{-1} induisent des bijections

$$\{\sigma : E \longrightarrow \bar{K} \mid \sigma \text{ un } K\text{-hom.}\} \longleftrightarrow \{\tau : E \longrightarrow \hat{K} \mid \tau|_K = j\}.$$

□

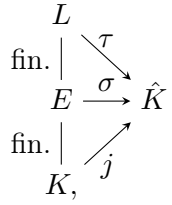
Remarque 4.2.3. Par le théorème des prolongements, $[E : K]_s \leq [E : K]$.

Lemme 4.2.4. *Si*

$$\begin{array}{l} L \\ \big|\,\text{fin.} \\ E \\ \big|\,\text{fin.} \\ K, \end{array}$$

alors $[L : K]_s = [F : E]_s[E : K]_s$.

Démonstration. Considérer



et appliquer le lemme précédent. □

Proposition 4.2.5 (Degré séparable d'une extension simple)**.** *Soit* $E = K[\alpha]$ *une extension algébrique simple. Alors*

1. $[E : K]_s$ *est égal au nombre de racines distinctes de* $\min(\alpha, K)$.
2. $[E : K]_s | [E : K]$.
3. α *est séparable sur* K *si et seulement si* $[E : K]_s = [E : K]$.

Démonstration.

1. Clair par la définition du degré de séparabilité et par le théorème des prolongements.
2. On distingue deux cas.
   — Si $\operatorname{car} K = 0$, alors $\min(\alpha, K)$ possède n racines distinctes, où $n = [E : K]$. Donc $[E : K]_s = [E : K]$.
   — Si $\operatorname{car} K = p$, alors $\min(\alpha, K)$ est de la forme $g(X^{p^d})$, avec d maximal pour cette propriété. Alors g est irréductible et séparable. Il s'ensuit que β est une racine de $\min(\alpha, K)$ si et seulement si β^{p^d} est une racine de g. Donc $[E : K]_s$ est égal au nombre tels β, qui est égal au nombre de tel β^{p^d}, qui est $\deg g$ car g est séparable. Or $p^d \times \deg g = \deg f$. Donc $p^d \times [E : K]_s = [E : K]$.
3. On a que $\min(\alpha, K)$ n'est pas un polynome en X^p. Donc $d = 1$, et $[E : K]_s = [E : K]$.

□

Corollaire 4.2.6. *Si* E *est une extension finie de* K*, alors* $[E : K]_s | [E : K]$.

Démonstration. On a que $E = K[\alpha_1, \ldots, \alpha_n]$, et on procède par récurrence sur n. □

Théorème 4.2.7. *Soit* E *une extension finie de* K*. Les conditions suivantes sont équivalentes :*

1. E *est séparable sur* K*,*
2. E *est engendré par des éléments séparables,*
3. $[E : K]_s = [E : K]$.

Démonstration. 1. $\implies$ 2. Clair.

2. $\implies$ 3. On a $K \leq K[\alpha_1] \leq K[\alpha_1, \alpha_2] \leq \cdots \leq K[\alpha_1, \ldots, \alpha_n] = E$, avec α_i séparable. On a une tour d'extensions simples séparables, et donc

$$\begin{aligned}[E : K] &= \prod_i [K[\alpha_1, \ldots, \alpha_i] : K[\alpha_1, \ldots, \alpha_{i-1}]] \\ &= \prod_i [K[\alpha_1, \ldots, \alpha_i] : K[\alpha_1, \ldots, \alpha_{i-1}]]_s \\ &= [E : K]_s.\end{aligned}$$

3. $\implies$ 1. On suppose $[E : K]_s = [E : K]$, et soit $\beta \in E$. On a

$$\underbrace{[E : K]}_{=[E:K]_s} = \underbrace{E : K[\beta]]}_{\geq [E:K[\beta]]} \underbrace{[K[\beta] : K]}_{\geq [K[\beta]:K]_s}.$$

Donc $[K[\beta] : K] = [K[\beta] : K]_s$, et β est séparable.

□

4.3 Elements primitifs

Définition 4.3.1 (Element primitif)**.** Soit E une extension finie de K. Un élément $\alpha \in E$ est dit *primitif* si $E = K[\alpha]$.

Lemme 4.3.2. *Soit K un corps infini, et V un K-espace vectoriel de dimension finie. Soient $H_1, \ldots, H_r$ des sous espaces propres. Alors $\bigcup_i H_i \neq V$.*

Démonstration. Par récurrence sur r. Si $r = 1$ c'est clair. Supposons $\bigcup_{i=1}^{r-1} H_i \neq V$, et doit $w \in V \setminus \bigcup_{i=1}^{r-1} H_i$. Si $w \notin H_r$, on a gagné. Supposons donc $w \in H_r$, et choisissons $v \notin H_r$. Considérons $v + \lambda w$, avec $\lambda \in K$. Alors $v + \lambda w \notin H_r$. Supposons que $v + \lambda w, v + \mu w \in H_i$, avec $\mu \neq \lambda$, et $i < r$. Alors $(\lambda - \mu)w \in H_i$, et $w \in H_i$ ce qui est impossible. Donc il existe au plus un scalaire λ_i tel que $v + \lambda_i w \in H_i$. Posons $\eta \neq \lambda_i$, $\forall i < r$, ce qui est possible car K est infini. Alors $v + \eta w \notin H_i$, $\forall i < r$.

□

Lemme 4.3.3. *Soit E un corps fini. Alors le groupe multiplicatif E^* est cyclique.*

Démonstration. Exercice. □

Théorème 4.3.4 (Steinitz)**.** *Soit E une extension finie de K. Alors il existe un élément primitif si et seulement si le nombre d'extensions intermédiaires (entre K et E) est fini.*

Démonstration.
— Si K est fini, alors E l'est aussi. En particulier, le nombre d'extensions intermédiaires est fini. Par le lemme précédent, il existe un générateur α de E^*, et clairement, $E = K[\alpha]$.
— Supposons que K soit infini, et qu'il existe un élément primitif $\alpha \in E$. On a que $E = K[\alpha]$, et $E = F[\alpha]$, pour toute extension intermédiaire $K \leq F \leq E$. Posons

$$\begin{aligned}\phi : \{\text{Ext. inter.}\} &\longrightarrow \{\text{Div. unitaire de } \min(\alpha, K)\} \\ F &\longmapsto \min(\alpha, F)\end{aligned}$$

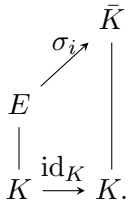
Remarquer que l'ensemble de droite est fini. On montre que ϕ est injective. Prenons F une extension intermédiaire, et $g = \phi(F)$. Soit F_0 le corps engendré par K est les coefficients de g. Alors $F_0 \leq F$, et g est irréductible dans $F[X]$, donc dans $F_0[X]$, et $g = \min(\alpha, F_0)$. Puis,

$$\begin{aligned}[E : F_0] &= [F_0[\alpha] : F_0] \\ &= \deg g \\ &= [E : F].\end{aligned}$$

Or $[E : F_0] = [E : F][F : F_0]$, et donc $[F : F_0] = 1$, ce qui montre que $F = F_0$. Ainsi, ϕ est inversible à gauche, et donc injective. Ainsi, il n'y a qu'un nombre fini d'extension intermédiaires entre K et E.
Réciproquement, supposons qu'il n'y a qu'un nombre fini d'extensions intermédiaires. Alors $\bigcup_{K\leq F\leq E} F$ est une réunion finie de sous K-espaces vectoriels de E, donc différent de E. Soit $\alpha \in E \setminus \bigcup_{K\leq F\leq E} F$. Alors $K[\alpha]$ est une extension intermédiaire, donc forcément $K[\alpha] = E$. □

Théorème 4.3.5 (de l'élément primitif)**.** *Soit E une extension finie de K. Si E est une extension séparable, alors il existe un élément primitif.*

Démonstration. Si K est fini on a déja vu qu'il existe un élément primitif. Supposons K infini. Soit $n = [E : K]$. Alors par séparabilité, $[E : K]_s = n$, donc il existe n prolongements distincts $\sigma_1, \ldots, \sigma_n : E \longrightarrow \bar{K}$ de id_K.



On considère $\sigma_i - \sigma_j : E \longrightarrow \bar{K}$. C'est une application K-linéaire, et posons $H_{i,j} = \ker(\sigma_i - \sigma_j) \leq E$. Si $i \neq j$, alors $H_{i,j} \neq E$. On a un nombre fini d'espaces $H_{i,j}$ qui sont propres ($i \neq j$). Soit $\alpha \in E \setminus \bigcup_{i\neq j} H_{i,j}$. On montre que α est primitif. Par choix de α, on a $\sigma_i(\alpha) \neq \sigma_j(\alpha)$, $\forall i \neq j$. On a donc n prolongements distincts $\sigma_1, \ldots, \sigma_n : K[\alpha] \longrightarrow \bar{K}$ de id_K, et $[K[\alpha] : K]_s = n$. Donc $K[\alpha] = E$. □

Cette preuve donne une méthode pour trouver des éléments primitifs.

Corollaire 4.3.6. *Si $\operatorname{car} K = 0$, ou si K est fini, alors il existe toujours un élément primitif dans une extension finie.*

Exemples 4.3.7.
1. $\mathbb{Q}[\sqrt{2}, i, \sqrt[7]{21}]$ admet un élément primitif sur $\mathbb{Q}$.
2. $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

Chapitre 5

Extensions galoisiennes

5.1 Définition

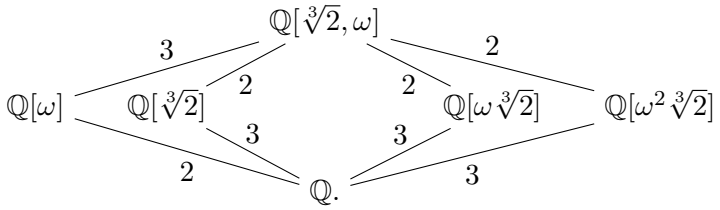
Définition 5.1.1 (Extension galoisienne)**.** Une extension algébrique E d'un corps K est dite *galoisienne* si elle est normale et séparable.

Remarque 5.1.2. Si $\operatorname{car} K = 0$ ou K fini, alors galoisienne est équivalente à normale.

Définition 5.1.3 (Groupe de Galois)**.** Soit E une extension algébrique de K. Posons $\mathrm{Gal}(E, K)$, le *groupe de Galois* de l'extension, comme étant le groupe des K-automorphismes de E. Comme le suggère finement le nom, on s'intéressera à ce groupe quand E est galoisienne sur K.

Remarque 5.1.4. Supposons que $[E : K] = n$, avec E galoisienne. Alors il existe exactement n prolongements distincts $\sigma : E \longrightarrow \bar{K}$ de id_K (par séparabilité), et $\sigma(E) = E$ (par normalité). Donc σ est un K-automorphisme de E, et un élément de $\mathrm{Gal}(E, K)$. En particulier, $|\mathrm{Gal}(E, K)| = n$.

Exemple 5.1.5. L'extension $\mathbb{Q}[\sqrt[3]{2}]$ n'est pas normale sur $\mathbb{Q}$. Sa clôture normale est $E = \mathbb{Q}[\sqrt[3]{2}, \omega]$, avec $\omega = \frac{-1+i\sqrt{3}}{2}$ une racine cubique de 1. Alors E est galoisienne sur $\mathbb{Q}$.



On a

$$\begin{aligned} \sigma : E &\longrightarrow E \\ \sqrt[3]{2} &\longmapsto \omega\sqrt[3]{2} \\ \omega &\longmapsto \omega, \end{aligned} \qquad \begin{aligned} \tau : E &\longrightarrow E \\ \sqrt[3]{2} &\longmapsto \sqrt[3]{2} \\ \omega &\longmapsto \omega^2, \end{aligned}$$

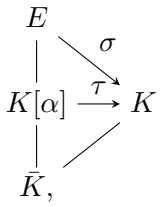
et $\sigma^3 = \mathrm{id}$, $\tau^2 = \mathrm{id}$. Donc $\mathrm{Gal}(E, K) \cong \mathfrak{S}_3$. Remarquer que $\mathrm{Gal}(\mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}) = \{\mathrm{id}\}$, mais que $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$...

Notation 5.1.6. Si H est un groupe de K-automorphismes de E (où E une extension algébrique de K), on note $E^H = \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall \sigma \in H\}$.

Théorème 5.1.7. *Soit E une extension galoisienne de K. Alors les points fixes sous l'action du groupe de galois $E^{\mathrm{Gal}(E,K)} = K$.*

Démonstration. $\supseteq$ Evident, car $\forall \sigma \in \mathrm{Gal}(E,K)$, $\sigma|_K = \mathrm{id}_K$, si bien que $K \subseteq E^{\mathrm{Gal}(E,K)}$.

$\subseteq$ Soit $\alpha \in E^{\mathrm{Gal}(E,K)}$.



On prolonge l'inclusion $K \hookrightarrow \bar{K}$ en $\tau : K[\alpha] \longrightarrow \bar{K}$, puis en $\sigma : E \longrightarrow \bar{K}$. Comme E est une extension normale de K, $\sigma(E) = E$. Donc $\sigma \in \mathrm{Gal}(E,K)$. Comme $\alpha \in E^{\mathrm{Gal}(E,K)}$, on a $\sigma(\alpha) = \alpha$, donc $\tau(\alpha) = \alpha$. Ainsi, tout prolongement τ de $K \hookrightarrow \bar{K}$ à $K[\alpha]$ est de nouveau l'inclusion $K[\alpha] \longrightarrow \bar{K}$. Donc $[K[\alpha] : K]_s = 1$. De plus, comme E est séparable sur K, α l'est aussi, et $[K[\alpha] : K] = [K[\alpha] : K] = 1$, ce qui montre que $K[\alpha] = K$, et $\alpha \in K$. On obtient l'autre inclusion.

□

Théorème 5.1.8 (Artin)**.** *Soit E un corps, et soit $H \leq \mathrm{Aut}\, E$ un groupe fini d'automorphismes de E. Alors*

1. *E^H est un sous corps de E,*
2. *E est une extension galoisienne finie de E^H,*
3. *$\mathrm{Gal}(E, E^H) = H$,*
4. *$[E, E^H] = |H|$.*

Démonstration. 1. Evident.

2. Soit $\alpha \in E$. On considère l'orbite (finie) Y de α sous l'action de H. On pose $f = \prod_{y \in Y}(X - y) \in E[X]$. Alors $f(\alpha) = 0$. De plus, $\sigma(f) = f$, $\forall \sigma \in H$, et $f \in E^H[X]$. Par conséquent, f un multiple de $\min(\alpha, E^H)$. Les autres racines de $\min(\alpha, E^H)$ sont nécessairement des racines de f, donc des éléments de $Y \subseteq E$. Ceci prouve que E est une extension normale de E^H.
   L'extension E est séparable car $\min(\alpha, E^H)$ l'est (car f l'est), pour tout $\alpha \in E$. Ainsi, E est galoisienne.
   On montre maintenant que E est une extension finie de E^H. On prend $\alpha \in E$, et on considère $n = [E^H[\alpha], E^H]$. Alors

$$\begin{aligned} n &= \deg \min(\alpha, E^H) \\ &\leq \deg f \\ &\leq |Y| \\ &\leq |H|. \end{aligned}$$

On choisi $\beta \in E$ tel que $[E^H[\beta], E^H]$ est le plus grand possible (au plus $|H|$ car $E^H \leq E^H[\beta] \leq E$). Soit $\alpha \in E$ arbitraire, et considérons l'extension $E^H[\beta, \alpha]$ de E^H. Elle est séparable car E l'est. Il existe donc un élément primitif $\gamma \in E^H[\beta, \alpha]$. Alors $E^H \leq E^H[\beta] \leq E^H[\gamma]$. Par maximalité de $[E^H[\beta], E^H]$, on a que $E^H[\beta] = E^H[\gamma]$, et donc $\alpha \in E^H[\beta]$, ce qui montre que $E^H[\beta] = E$, donc en particulier que E est une extension finie de E^H.

3. On a $E = E^H[\beta]$ pour un certain élément primitif $\beta \in E$. Soit Z l'orbite (finie) de β sous l'action de H, et $g = \prod_{z \in Z}(X - z)$. Comme avant, $g \in E^H[X]$ est un multiple de $\min(\beta, E^H)$. Alors

$$\begin{aligned}
[E : E^H] &= [E^H[\beta] : E^H] \\
&= \deg \min(\beta, E^H) \\
&\leq \deg g \\
&= |Z| \\
&\leq |H| \\
&\leq |\operatorname{Gal}(E : E^H)| && H \leq \operatorname{Gal}(E, E^H) \\
&= [E, E^H] && E \text{ gal.}
\end{aligned}$$

Donc $|H| = |\operatorname{Gal}(E, E^H)|$, et donc $H = \operatorname{Gal}(E, E^H)$.

4. Fait au point précédent.

□

5.2 Correspondance de Galois

Soit E une extension galoisienne de K, et posons

$$\begin{aligned}
\Phi : \{\text{ext. inter}\} &\longrightarrow \{\text{sous grps. de } \operatorname{Gal}(E, K)\} \\
F &\longmapsto \operatorname{Gal}(E, F), \\
\Psi : \{\text{sous grps. de } \operatorname{Gal}(E, K)\} &\longrightarrow \{\text{ext. inter}\} \\
H &\longmapsto E^H.
\end{aligned}$$

Théorème 5.2.1. *On a $\Psi \circ \Phi = \mathrm{id}$, i.e. $F = E^{\mathrm{Gal}(E,F)}$, pour toute extension intermédiaire $K \leq F \leq E$. En particulier, Φ est injective et Ψ est surjective.*

Démonstration. Soit F un corps intermédiaire. On a que E est une extension normale de K, donc sur F. De même pour la séparabilité, et ainsi, E est galoisienne sur F. En particulier, $E^{\mathrm{Gal}(E,F)} = F$. □

Remarque 5.2.2. Si E n'est pas finie sur K, alors $\Phi \circ \Psi \neq \mathrm{id}$. On doit restreindre le type de sous groupes de $\operatorname{Gal}(E, K)$ en ne prenant que des sous groupes fermés pour une certaine topologie.

Théorème 5.2.3 (Correspondence de Galois)**.** *Soit E une extension galoisienne finie de K. Alors*

1. *Φ et Ψ sont mutuellement inverses ;*

2. *ces bijections sont décroissantes pour les ordres évidents, i.e.* $F \leq F' \implies \mathrm{Gal}(E,F) \geq \mathrm{Gal}(E,F')$*, et réciproquement ;*
3. *si* F *correspond à* H*, i.e.* $H = \mathrm{Gal}(E,F)$ *alors* $[E:F] = |H|$*, et* $[F:K] = [\mathrm{Gal}(E,K) : H]$ *;*
4. *soit* $H \leq \mathrm{Gal}(E,K)$*, et* $\sigma \in \mathrm{Gal}(E,K)$*, soit* $F = E^H$ *l'extension intermédiaire correspondante, alors* $\sigma H \sigma^{-1}$ *correspond à l'extension intermédiaire* $\sigma(F)$*, appelée corps conjugué ;*
5. *soit* H *correspondant à* F*, alors* $H \trianglelefteq \mathrm{Gal}(E,K)$ *si et seulement si* F *est une extension normale de* K *(donc galoisienne) ;*
6. *si* $H \trianglelefteq \mathrm{Gal}(E,K)$ *correspond à* F*, alors la restriction* $\mathrm{Gal}(E,K) \longrightarrow \mathrm{Gal}(F,K)$ *induit un isomorphisme* $\mathrm{Gal}(E,K)/H \cong \mathrm{Gal}(F,K)$ *:*

$$\begin{array}{l} \\ \mathrm{Gal}(E,K) \left(\begin{array}{l} E \\ \big| \ \big) \, \mathrm{Gal}(E,F) \\ F \\ \big| \ \big) \, \mathrm{Gal}(E,K)/\mathrm{Gal}(E,F) \\ K. \end{array} \right. \end{array}$$

Démonstration. 1. On sait déja que $\Psi \circ \Phi = \mathrm{id}$, et $\Phi \circ \Psi(H) = \mathrm{Gal}(E, E^H)$. Par le théorème d'Artin, et comme H est fini, $\mathrm{Gal}(E, E^H) = H$.

2. Trivial.

3. On sait déja que $[E:F] = |H|$ par le théorème d'Artin. L'autre égalité découle par multiplicité des degrés.

4. Clairement, $\sigma(F)$ est un sous corps de $\sigma(E) = E$, car σ est un automorphisme. Soit $\tau \in \mathrm{Gal}(E, \sigma(F))$, alors $\tau|_{\sigma(F)} = \mathrm{id}_{\sigma(F)}$. Donc $\tau(\sigma(f)) = \sigma(f)$, $\forall f \in F$, et en appliquant σ^{-1}, on a $\sigma^{-1}\tau\sigma(f) = f$, et ainsi $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(E,F)$. Récipriquement, si $\eta \in \mathrm{Gal}(E,F) = H$, $\sigma\eta\sigma^{-1} \in \mathrm{Gal}(E, \sigma(F))$. Ainsi, $\mathrm{Gal}(E, \sigma(F)) = \sigma H \sigma^{-1}$.

5. Par le point précédent, si $H \trianglelefteq \mathrm{Gal}(E,F)$, alors F est fixé par tout élément de $\mathrm{Gal}(E,K)$. Ainsi, F est normale sur K.

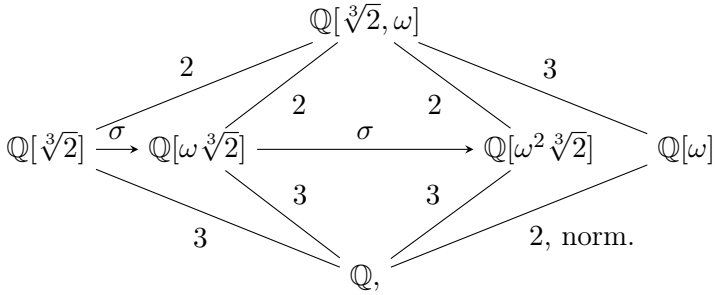
6. Par le 1er théorème d'isomorphisme.

□

Remarque 5.2.4. Si E est une extension galoisienne infinie de K, alors le précédent théorème ne s'applique pas. Plus précisément, $\Psi \circ \Phi = \mathrm{id}$, mais pas $\Phi \circ \Psi$. On peut se restreindre aux sous groupes de $\mathrm{Gal}(E,K)$ qui sont fermés pour la topologie de Krull. Alors $\Phi \circ \Psi|_{\mathrm{ferm.}} = \mathrm{id}$, et on a de nouveau des bijections.

Exemple 5.2.5. Soit $E = \mathbb{Q}[\sqrt[3]{2}, \omega]$, qui est une extension galoisienne de $\mathbb{Q}$, où, comme toujours,

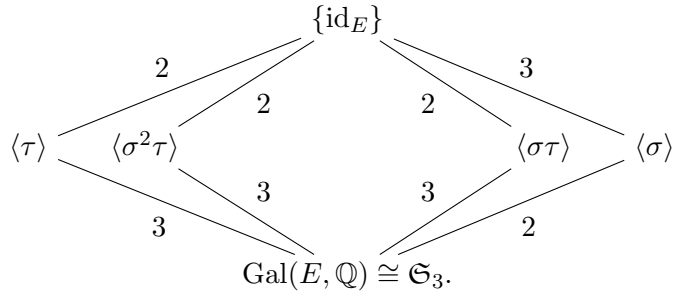
$\omega = \frac{1+i\sqrt{3}}{2}$ est une racine cubique de 1.



où

$$\begin{aligned} \sigma : E &\longrightarrow E \\ \sqrt[3]{2} &\longmapsto \omega\sqrt[3]{2} \\ \omega &\longmapsto \omega \end{aligned} \qquad \begin{aligned} \tau : E &\longrightarrow E \\ \sqrt[3]{2} &\longmapsto \sqrt[3]{2} \\ \omega &\longmapsto \omega^2 \end{aligned}$$

sont les générateurs de $\mathrm{Gal}(E, \mathbb{Q})$. Les sous corps $\mathbb{Q}[\sqrt[3]{2}]$, $\mathbb{Q}[\omega\sqrt[3]{2}]$ et $\mathbb{Q}[\omega^2\sqrt[3]{2}]$ sont conjugués, et $\mathbb{Q}[\omega]$ est normal. On a $\mathrm{Gal}(E, \mathbb{Q}) \cong \mathfrak{S}_3$, et l'isomorphisme est donné par $\sigma \longmapsto (1\,2\,3)$ et $\tau \longmapsto (2\,3)$.



Les sous groupes $\langle\tau\rangle$, $\langle\sigma^2\tau\rangle$ et $\langle\sigma\tau\rangle$ sont conjugués, et $\langle\sigma\rangle$ est normal.

Chapitre 6

Extensions abéliennes et cycliques

Définition 6.0.6 (Extensions abéliennes et cycliques)**.** Une extension galoisienne E d'un corps K est dite *abélienne* (resp. *cyclique*) si $\mathrm{Gal}(E, K)$ est abélien (resp. cyclique).

6.1 Extensions cyclotomiques

Définition 6.1.1 (Racine de l'unité, racine primitive de l'unité)**.** Soit K un corps, et $n \geq 1$ un entier tel que $\mathrm{car}\, K \not| n$. Une racine du polynome $X^n - 1$ dans $\bar{K}$ s'appelle une *racine n-ième de l'unité*. Une telle racine ζ est dite *primitive* si ζ n'est pas racine de $X^d - 1$, pour $d|n$.

Lemme 6.1.2. *Soit ζ une racine primitive n-ième de l'unité.*

1. *Les racines n-ièmes de 1 sont $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$.*
2. *Soit ζ^i une autre racine primitive de 1 si et seulement si i et n sont premiers entre eux.*

Démonstration. 1. Remarquer que $X^n - 1$ n'a pas de racine double, car sa dérivée est non nulle.

2. Si $\mathrm{pgcd}(i, n) \neq 1$, alors il existe un diviseur commun $p > 1$. Alors $(\zeta^p)^{n/p} = 1$. Comme $i = pj$ pour un certain j, on a $((\zeta^i)^{n/p}) = 1^j = 1$, donc ζ^i n'est pas primitive. Réciproquement, si $\mathrm{pgcd}(i, n) = 1$, alors par le théorème de Bézout, $\exists a, b \in \mathbb{Z}$ tels que $ai + bn = 1$. Donc $\zeta = \zeta^1 = (\zeta^i)^a(\zeta^n)^b = (\zeta^i)^a$. Donc si $(\zeta^i)^d = 1$ avec $d < n$, alors $(\zeta^{ia})^d = 1$, donc $\zeta^d = 1$. Comme ζ est primitive, on doit avoir $d = n$. Ceci montre que ζ^i est primitive.

□

Définition 6.1.3 (Extension cyclotomique)**.** Soit K un corps, et ζ une racine primitive n-ième de 1 dans $\bar{K}$. Alors l'extension $K[\zeta]$ s'appelle une extension *cyclotomique* de K.

Lemme 6.1.4. *On a que $K[\zeta]$ est une extension abélienne de K, et $\mathrm{Gal}(K[\zeta], K)$ est isomorphe à un sous groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$, les entiers inversibles modulo n.*

Démonstration. Les racines de $X^n - 1$ sont toutes distinctes, et toutes présentes dans $K[\zeta]$. Ainsi, $K[\zeta]$ est séparable et normale, donc galoisienne. Si $\sigma \in \mathrm{Gal}(K[\zeta], K)$, alors $\sigma(\zeta)$ est une racine de $\min(\zeta, K)$, donc de $X^n - 1$, donc de la forme ζ^i, pour un certain i. De plus, ζ^i est également une

racine primitive, car σ est inversible. Ainsi, $\text{pgcd}(i,n)=1$, et i est inversible dans $(\mathbb{Z}/n\mathbb{Z})^*$. On définit l'homomorphisme suivant :

$$\begin{aligned}\psi : \text{Gal}(K[\zeta],K) &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma &\longmapsto [i] \qquad\qquad \text{où } \sigma(\zeta)=\zeta^i.\end{aligned}$$

C'est un homomorphisme injectif car $\psi(\sigma)=[1]$ si et seulement si $\sigma(\zeta)=\zeta$, et donc $\sigma = 1_{K[\zeta]}$. Il est alors clair que $\text{Gal}(K[\zeta],K)$ est abélien, et donc que l'extension est abélienne. □

Théorème 6.1.5 (Petit théorème de Fermat)**.** *Soit p premier. $\forall \bar{b} \in \mathbb{F}_p$ on a $\bar{b}^p = \bar{b}$.*

Démonstration. Si $\bar{b}=0$, alors c'est bon. Sinon, $\bar{b} \in \mathbb{F}_p^*$ qui est un groupe d'ordre $p-1$. Donc $\bar{b}^{p-1}=1$, et $\bar{b}^p = \bar{b}$. □

Théorème 6.1.6 (Extensions cyclotomiques de $\mathbb{Q}$)**.** *Soit $n \geq 1$, soit $\zeta = \zeta_n$ une racine primitive n-ième de l'unité dans $\mathbb{C}$. Alors*

1. $\min(\zeta,\mathbb{Q})$ *est le polynome cyclotomique*

$$\Phi_n(X) = \prod_{\substack{1\leq i\leq n \\ \text{pgcd}(i,n)=1}} (X-\zeta^i),$$

de degré $\phi(n)$, l'indicatrice d'Euler en n. De plus, $\Phi_n \in \mathbb{Z}[X]$.

2. $\mathbb{Q}[\zeta]$ *est un extension de degré $\phi(n)$.*
3. $\mathbb{Q}[\zeta]$ *est une extension galoisienne de groupe de galois $(\mathbb{Z}/n\mathbb{Z})^*$. En particulier, c'est une extension abélienne.*

Démonstration. 1. On décomose X^n-1 dans $\mathbb{Z}[X]$:

$$X^n - 1 = f(X)g(X),$$

avec $f(X)$ irréductible et unitaire, et $f(\zeta)=0$. Rappelons que $f(X)$ reste irréductible dans $\mathbb{Q}[X]$, et est donc le polynome minimal de ζ sur $\mathbb{Q}$. Soit p un nombre premier ne divisant pas n. Assertion : ζ^p est une racine de $f(X)$. On procède par l'absurde. On suppose que ζ^p est racine de $g(X)$. Donc ζ est racine de $h(X)=g(X^p)$. Comme f est le polynome minimal, $f(X)|h(X)$:

$$g(X^p) = h(X) = f(X)k(X).$$

Tous ce polynomes sont a coefficients entier. Posons $g(X)=\sum_i b_i X^i$. On réduit modulo p. On a

$$\begin{aligned}\bar{h}(X) &= \bar{g}(X^p) \\ &= \sum_i \bar{b}_i X^{ip} \\ &= \sum_i \bar{b}_i^p X^{ip} \\ &= \left(\sum_i \bar{b}_i X^i\right)^p \\ &= \bar{g}(X)^p.\end{aligned}$$

Par ailleurs, $X^n - 1 = \bar{f}(X)\bar{g}(X)$, et $\bar{f}(X)|\bar{h}(X) = \bar{g}(X)^p$. Donc $\bar{f}(X)$ et $\bar{g}(X)$ partagent un facteur commun ($\mathbb{F}_p[X]$ est factoriel, considérer la décomposition en facteur premiers). Donc $X^n - 1 = \bar{f}(X)\bar{g}(X)$ a une racine double dans une extension bien choisie de $\mathbb{F}_p$. C'est donc une racine du polynome dérivé $\bar{n}X^{n-1}$. Or, $p \not| n$, et donc $\bar{n} \neq 0$. Ceci est impossible car $X^n - 1$ et X^{n-1} n'ont pas de racine commune. Ainsi, on a prouvé l'assertion.

Soit $1 \leq i \leq n$, avec $\text{pgcd}(i, n) = 1$. Alors i s'écrit $i = p_1 \cdots p_s$, avec $p_j \not| n$ premier. On a que ζ est une racine de $f(X)$. Donc par l'assertion, ζ^{p_1} est une racine de $f(X)$. De plus, p_1 est premier avec n, et ζ^{p_1} est de nouveau une racine primitive. Donc, de nouveau par l'assertion, $\zeta^{p_1 p_2}$ est une racine de $f(X)$, et ainsi de suite jusqu'à ζ^i. Donc f est multiple de Φ_n. Par ailleurs $\mathbb{Q}[\zeta]$ est une extension galoisienne de degré divisant $\phi(n)$, car $\text{Gal}(\mathbb{Q}[\zeta], \mathbb{Q})$ s'injecte dans $(\mathbb{Z}/n\mathbb{Z})^*$. Donc $f = \min(\zeta, \mathbb{Q})$ est de degré divisant $\phi(n)$. Comme f est multiple de Φ_n qui est justement de degré $\phi(n)$, on a $f = \Phi_n$. En particulier, $\Phi_n \in \mathbb{Z}[X]$.

2. Clair par le point précédent.
3. Clair par un lemme précédent.

□

Théorème 6.1.7 (Kronecker–Weber)**.** *Toute extension abélienne finie de $\mathbb{Q}$ est une sous extension d'une certaine extension cyclotomique de $\mathbb{Q}$.*

Démonstration. Nope. □

6.2 Extensions cycliques

Soit E une extension cyclique de K de degré n, de groupe de Galois $\text{Gal}(E, K) = \langle\sigma\rangle$, avec $\sigma^n = 1$. On définit la *norme* de E sur K par

$$\begin{aligned} N_K^E : E^* &\longrightarrow K^* \\ \alpha &\longmapsto \prod_{i=0}^{n-1} \sigma^i(\alpha), \end{aligned}$$

le produit de tous les conjugués de α. L'image est bien dans K^* car fixée point par point sous l'action du groupe de Galois. C'est bien un homomorphisme de groupe, car σ est un homomorphisme.

Lemme 6.2.1 (Indépendance linéaire des automorphismes)**.** *Soit F un corps, et $\sigma_1, \ldots, \sigma_n \in \text{Aut}\, F$ distincts. Alors ils sont linéairement indépendants dans $\mathcal{F}(F, F)$, le F-espace vectoriel des fonctions de F dans F.*

Démonstration. On suppose qu'il existe une combinaison linéaire nulle de k d'entre eux, et on montre qu'elle doit être triviale par récurrence sur k. Le cas $k = 1$ est clair. Si $k \geq 2$, notons les $\sigma_1, \ldots, \sigma_k$. On a $\sum_i \lambda_i \sigma_i = 0$. On sait que $\sigma_{k-1} \neq \sigma_k$, et soit z tel que $\sigma_{k-1}(z) \neq \sigma_k(z)$. On évalue sur xz :

$$\begin{aligned} \sum_i \lambda_i \sigma_i(xz) &= 0 \\ &= \sum_i \lambda_i \sigma_i(x)\sigma_i(z). \end{aligned}$$

Par ailleurs,

$$\begin{aligned}\sum_i \lambda_i \sigma_i(x) &= 0 \\ &= \sum_i \lambda_i \sigma_k(z)\sigma_i(x).\end{aligned}$$

En soustrayant on obtient

$$\sum_{i=1}^{k-1} \lambda_i(\sigma_k(z) - \sigma_i(z))\sigma_i(x) = 0.$$

Par hypothèse de récurrence, $\lambda_i(\sigma_k(z) - \sigma_i(z)) = 0$, et en particulier, $\lambda_{k-1}(\sigma_k(z) - \sigma_{k-1}(z))$. Donc $\lambda_{k-1} = 0$. Il reste

$$\sum_{i \neq k-1} \lambda_i \sigma_i,$$

qui comporte $k-1$ termes. Par hypothèse de récurrence, $\lambda_i = 0$. □

Théorème 6.2.2 (90 de Hilbert)**.** *Soit $\beta \in E^*$. On a que $N_K^E(\beta) = 1$ si et seulement si $\exists \alpha \in E^*$ tel que $\beta = \alpha\sigma(\alpha)^{-1}$.*

Démonstration. $\Longleftarrow$ Supposons $\beta = \alpha\sigma(\alpha)^{-1}$. Alors

$$\begin{aligned}N_K^E(\beta) &= N_K^E(\alpha) N_K^E(\sigma(\alpha))^{-1} \\ &= 1.\end{aligned}$$

$\Longrightarrow$ On a $\mathrm{Gal}(E, K) = \{1, \sigma, \ldots, \sigma^{n-1}\}$, qui sont n automorphismes linéairement indépendents. On considère

$$1 + \beta\sigma + (\beta\sigma(\beta))\sigma^2 + \cdots + (\beta\sigma(\beta)\cdots\sigma^{n-2}(\beta))\sigma^{n-1} \neq 0.$$

Il existe $x \in E$ tel que la combinaison ci-dessus ne s'annulle pas, et posons α cette évaluation. On calcule $\beta\sigma(\alpha)$:

$$\beta\sigma(\alpha) = \beta\sigma(x) + \beta\sigma(\beta)\sigma(x) + \cdots + (\beta\sigma(\beta)\sigma^2(\beta)\cdots\sigma^{n-1}\beta))\sigma^n(x).$$

Le dernier terme vaut $N_K^E(\beta)x = x$. Finallement,

$$\begin{aligned}\beta\sigma(\alpha) &= \beta\sigma(x) + \cdots + (\beta\sigma(\beta)\cdots\sigma^{n-2}(\beta))\sigma^{n-1}(x) + x \\ &= \alpha.\end{aligned}$$

Donc $\beta = \alpha\sigma(\alpha)^{-1}$. □

Théorème 6.2.3 (Classification des extension cycliques)**.** *Soit K un corps. On suppose qu'il contient les racines n-ièmes de 1, et qu'elles sont toutes distinctes.*

1. *On se donne $a \in K$, et $\beta \in \bar{K}$ une racine de $X^n - a$. Alors $K[\beta]$ est un extension cyclique de K de degré d divisant n. De plus, $\min(\beta, K) = X^d - c$, pour un certain $c \in K$.*

2. *Si E est un extension cyclique de K, de degré n, alors $E = K[\beta]$, pour un certain $\beta \in E$ une racine de $X^n - a$, pour un certain $a \in K$.*

Démonstration. 1. Les racines de $X^n - a$ sont : $\beta, \zeta\beta, \zeta^2\beta, \ldots, \zeta^{n-1}\beta$, où ζ est une racine primitive n-ième de l'unité. Soit $E = K[\beta]$, et $\tau \in \mathrm{Gal}(E, K)$. Remarquons que E est une extension galoisienne de K. Alors $\tau(\beta)$ est racine de $X^n - a$, donc $\tau(\beta) = \zeta^k\beta$, pour un certain $k \in \mathbb{N}$. Donc τ est entièrement caractérisé par k. On considère $\mathrm{Gal}(E, K) \longrightarrow \mathbb{Z}/n\mathbb{Z} : \tau \longmapsto k$, où k est définit comme avant. C'est évidemment un homomorphisme injectif. Donc $\mathrm{Gal}(E, K)$ est isomorphisme à un sous groupe de $\mathbb{Z}/n\mathbb{Z}$. C'est donc un groupe cyclique d'ordre $d|n$, engendré par la classe de n/d. Ainsi $\mathrm{Gal}(E, K) = \langle\sigma\rangle$ est cyclique d'ordre d, et $\sigma(\beta) = \zeta^{n/d}\beta$. De plus $\sigma(\beta^d) = \beta^d$. Donc β^d est invariant sous l'action du groupe de galois, ce qui force $\beta^d \in K$. On pose $c = \beta^d$. Alors $X^d - c$ est un polynome annulateur de degré d de β, donc le polynome minimal.

2. Réciproquement, soit σ un générateur de $\mathrm{Gal}(E, K)$, qui est cyclique par hypothèse. On considère $\zeta^{-1} \in K$. On a que $K_K^E(\zeta^{-1}) = \prod_{i=0}^{n-1} \sigma^i(\zeta^{-1}) = \zeta^{-n} = 1$. Par le théorème 90 le Hilbert, $\exists\beta \in E$ tel que $\zeta^{-1} = \beta\sigma(\beta)^{-1}$. En d'autres termes, $\sigma(\beta) = \zeta\beta$. Les conjugués de β sont donc $\beta, \zeta\beta, \ldots, \zeta^{n-1}\beta$, tous discincts. De plus, $\sigma(\beta^n) = \beta^n$, et donc $\beta^n \in K$. Les conjugués de β sont tous racines de $X^n - \beta^n$, un polynome de degré n. Donc $\min(\beta, K) = X^n - \beta^n$.

□

Chapitre 7

Résolubilité par radicaux

7.1 Théorème de Galois

Définition 7.1.1 (Groupe résoluble)**.** Un groupe G est dit *résoluble* s'il existe une suite de sous groupes emboités

$$G = G_0 \geq G_1 \geq \cdots G_{r-1} \geq G_r = \{1\}$$

telle que

1. $G_{i+1} \trianglelefteq G_i$, $0 \leq i \leq r-1$,
2. G_i/G_{i+1} est un groupe abélien.

Définition 7.1.2 (Groupe dérivé)**.** Les sous groupes dérivés de G sont définis comme suit :

1. $D_0(G) = G$,
2. $D_1(G) = [G, G]$, le sous groupe des comutateurs de G,
3. $D_{n+1}(G) = [D_n(G), D_n(G)]$.

Rappel 7.1.3. Dans un groupe G, $[G, G]$ est le plus petit sous groupe normal de G avec quotient abélien.

Lemme 7.1.4. *Un groupe G est résoluble si et seulement si $\exists r \in \mathbb{N}$ tel que $D_r(G) = \{1\}$.*

Rappel 7.1.5. En général, G_i n'et pas toujours normal dans G, mais $D_i(G)$, lui, l'est.

Lemme 7.1.6. *Si G est fini, alors il est résoluble si et seulement si il existe une suite $G = G_0 \geq \cdots \geq G_n = \{1\}$ avec quotients cycliques d'ordre premier.*

Démonstration. Si un telle suite existe, alors clairement G est résoluble. Réciproquement, si G est résoluble avec une suite de résolubilité $G = G_0 \geq \cdots \geq G_r = \{1\}$. Le groupe G_i/G_{i+1} est abélien, non trivial sans perte de généralité. Donc il contient un élément non trivial a d'ordre fini $k > 1$. Soit $p|k$ un nombre premier, alors $b = a^{k/p}$ est d'ordre p. Alors $H = \langle b \rangle \leq G_i/G_{i+1}$ est d'ordre p, et normal (car groupe abélien). En prenant les images réciproques, on a $G_i \geq \pi^{-1}(H) = H' \geq G_{i+1}$, avec $G_{i+1} \trianglelefteq H' \trianglelefteq G_i$, et H/G_{i+1} cyclique d'ordre p. De plus $G_i/H \cong (G_i/G_{i+1})/(H/G_{i+1})$ est abélien. Ainsi, on peut raffiner la suite entière (car G fini) de manière à ce qu'elle satisfasse les hypothèses. □

Remarque 7.1.7. Avec l'exigence de quotients successifs cycliques, on ne peut pas avoir en général que $G_i \trianglelefteq G$. Par exemple, $G = \mathfrak{S}_4$, on a $\mathfrak{S}_4 \geq A_4 \geq V_4 = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \geq \{1\}$. Alors tous les termes de la suites sont normaux dans $\mathfrak{S}_4$, et $\mathfrak{S}_4/A_4 \cong C_2$, $A_4/V_4 \cong C_3$, $V_4/\{1\} = V_4$ non cyclique. On peut rajouter $V_4 \geq \langle(1\,2)(3\,4)\rangle \cong C_2 \geq \{1\}$ pour obtenir des quotients cycliques, mais $C_2 \not\trianglelefteq \mathfrak{S}_4$.

Lemme 7.1.8. *1. Tout sous groupe d'un groupe résoluble est résoluble.*

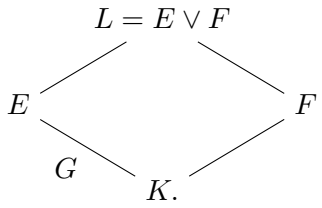
2. Tout quotient d'un groupe résoluble est résoluble.

3. Si $H \trianglelefteq G$, avec H et G/H résolubles, alors G est résoluble.

Définition 7.1.9 (Extension radicale)**.** 1. Une extension *radicale simple* d'un corps K est une extension $K[\alpha]$, où α est une racine d'un polynome de la forme $X^n - a$, où $a \in K$.

2. Une extension E de K est dite *radicale* si elle est obtenue par une tour d'extensions radicales simples.
3. Une extension finie E de K est dite *résoluble par radicaux* si elle est contenue dans une extension radicale.
4. Soit $f \in K[X]$. Le *groupe de Galois* de f est le groupe de Galois de son corps de décomposition (comme extension de K).
5. Soit $f \in K[X]$. On dit que l'équation $f(X) = 0$ est résoluble par radicaux si le groupe de Galois de f est résoluble par radicaux.

Lemme 7.1.10. *Soit L une extension finie de K, obtenue en composant deux extensions E et F. Supposons E galoisienne sur K, de groupe de Galois G.*



1. L est une extension galoisienne de F ;

2. $\mathrm{Gal}(L, F)$ est isomorphe à une sous groupe de G.

Démonstration. 1. On a que E est le corps de décomposition d'un polynome irréductible séparable $f \in K[X]$, avec racines $\alpha_1, \ldots, \alpha_n$. Donc $E = K[\alpha_1, \ldots, \alpha_n]$, et $L = F[\alpha_1, \ldots, \alpha_n]$, qui est le corps de décomposition de $f \in F[X]$. Ainsi, L est galoisienne sur F.

2. Posons

$$\begin{aligned} \mathrm{Gal}(L, F) &\longrightarrow \mathrm{Gal}(E, K) = G \\ \sigma &\longmapsto \sigma|_E. \end{aligned}$$

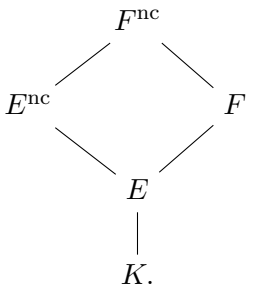
Si $\sigma \in \mathrm{Gal}(L, F)$, alors $\sigma|_K = \mathrm{id}_K$, et $\sigma|_E(E) = E$, car E est normal sur K. Donc $\sigma|_E \in \mathrm{Gal}(E, K)$. Il est alors clair que c'est un homomorphisme de groupes. il est injectif car si $\sigma|_E = \mathrm{id}_E$, alors $\sigma = \mathrm{id}_{E\vee F}$, car $\sigma|_F = \mathrm{id}_F$.

□

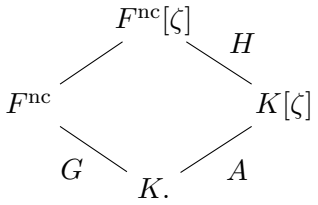
Remarque 7.1.11. Si E est une extension algébrique de K, alors sa cloture normale E^{nc} peut etre obtenue en rajoutant toutes les racines de tous les polynomes de $K[X]$ ayant l'une de leur racine dans E. De manière équivalente, E^{nc} est le composé de tous les corps de la forme $\sigma(E)$, où $\sigma : E \longrightarrow \bar{K}$ est un K-homomorphisme. De plus, si $E = K[\alpha_1, \ldots, \alpha_n]$, alors E^{nc} est le corps de décomposition des $\min(\alpha_i, K)$.

Théorème 7.1.12 (Galois)**.** *Soit K un corps de caractéristique 0 (pour simplifier), et une extension finie E de K. Alors E est résoluble par radicaux si et seulement si $\text{Gal}(E^{\text{nc}}, K)$ est résoluble.*

Démonstration. $\implies$ Supposons que E est résoluble par radicaux. Par définition, $E \leq F$, pour une certaine extension radicale F de K.



Si $F = K[\alpha_1, \ldots, \alpha_n]$, avec α_i racine de $X^{m_i} - a_i$. Alors F^{nc} est engendré par K et par toutes les autres racines de ces polynomes. Donc F^{nc} est aussi une extension radicale de K, qui est de plus galoisienne. Il suffit alors de montrer que $\text{Gal}(F^{\text{nc}}, K)$ est résoluble, car $\text{Gal}(E^{\text{nc}}, K)$ est un quotient de $\text{Gal}(F^{\text{nc}}, K)$. On a que F^{nc} est obtenue par une tour d'extensions radicales simples, correspondants a des polynomes $X^{m_i} - a_i$. On pose $N = \text{ppcm}(m_1, \ldots, m_n)$, et ζ une racine primitive N-ième de l'unité. On considère



Par le lemme, $F^{\text{nc}}[\zeta]$ est galoisienne sur $K[\zeta]$, et son groupe de Galois H est isomorphe à un sous groupe de G. Remarquer $F^{\text{nc}}[\zeta]$ est aussi un extension radicale de $K[\zeta]$. Donc $F^{\text{nc}}[\zeta]$ est une tour d'extensions

$$F^{\text{nc}}[\zeta] = L_k \geq L_{k-1} \geq \cdots \geq L_0 = K[\zeta],$$

où $L_i = L_{i-1}[\beta_i]$, avec β_i une racine de $X^{n_i} - a_i \in Li - 1[X]$. Par choix de n, les racines m_i-ièmes de 1 sont dans $K[\zeta]$. Par le théorème sur les extensions cycliques, l'extension L_i de L_{i-1} est cyclique de groupe de galois H_i, avec $|H_i||m_i$. Par le théorème de correspondance de Galois, on obtient une suite de sous groupes emboités

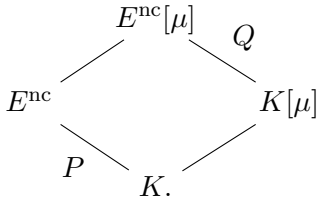
$$H = \text{Gal}(F^{\text{nc}}[\zeta], K[\zeta]) = S_0 \geq \cdots S_k = \{1\},$$

avec $S_i = \mathrm{Gal}(F^{\mathrm{nc}}[\zeta], L_i)$. De plus, $S_i \trianglelefteq S_{i-1}$, car l'extension L_i de L_{i-1} est galoisienne. De plus, S_{i-1}/S_i est cyclique car isomorphe à $\mathrm{Gal}(L_i, L_{i-1})$. Ainsi, $H = \mathrm{Gal}(F^{\mathrm{nc}}[\zeta], K[\zeta])$ est résoluble. On considère maintenant $A = \mathrm{Gal}(K[\zeta], K)$, groupe de galois d'une extension cyclotomique, donc abélien. On a

$$\mathrm{Gal}(F^{\mathrm{nc}}[\zeta], K) \geq \underbrace{\mathrm{Gal}(F^{\mathrm{nc}}[\zeta], K[\zeta])}_{H} \geq \{1\},$$

et $H \trianglelefteq \mathrm{Gal}(F^{\mathrm{nc}}[\zeta], K)$, car $K[\zeta]$ galoisienne sur K, et $\mathrm{Gal}(F^{\mathrm{nc}}[\zeta], K)/H \cong A$. Donc $\mathrm{Gal}(F^{\mathrm{nc}}[\zeta], K)$ est résoluble, car H et A le sont. Enfin, remarquer que G est un quotient de $\mathrm{Gal}(F^{\mathrm{nc}}[\zeta], K)$, donc lui-même résoluble.

$\Longleftarrow$ Supposons que $P = \mathrm{Gal}(E^{\mathrm{nc}}, K)$ est résoluble. Soit μ une racine primitive k-ième de l'unité, où $k = |P|$.



Par le lemme, $E^{\mathrm{nc}}[\mu]$ est une extension galoisienne de $K[\mu]$, et $Q = \mathrm{Gal}(E^{\mathrm{nc}}[\mu], K[\mu])$ est isomorphe à un sous groupe de P. Donc Q est résoluble et fini, et on se donne une suite de résolubilité

$$Q = Q_0 \trianglerighteq \cdots \trianglerighteq Q_s = \{1\}$$

avec quotients successifs cycliques. Donc par correspondance de Galois, $E^{\mathrm{nc}}[\mu]$ est obtenu à partir de $K[\mu]$ par une tour d'extensions cycliques

$$E^{\mathrm{nc}}[\mu] = M = M_s \geq \cdots \geq M_0 = K[\mu],$$

avec M_{i+1} une extension cyclique de M_i. Par le théorème sur les extensions cycliques, $M_{i+1} = M_i[\gamma_i]$, où γ_i est racine de $X^{r_i} - c_i \in M_i[X]$. De plus, $K[\mu]$ est une extension radicale simple de K, donc $E^{\mathrm{nc}}[\mu]$ est radicale. Comme $E \leq E^{\mathrm{nc}}[\mu]$, on a que E est une extension résoluble par radicaux.

□

Corollaire 7.1.13. *Soit K un corps de caractéristique 0. Toute équation $f(X) = 0$ de degré au plus 4 est résoluble par radicaux.*

Démonstration. Soit E le corps de décomposition de f, et $G = \mathrm{Gal}(E, K)$. Alors G permute les racines de f, donc G est isomorphe à un sous groupe de $\mathfrak{S}_4$ (ex. 1, série 11). Or $\mathfrak{S}_4$ est résoluble :

$$\mathfrak{S}_4 \geq A_4 \geq V_4 = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \geq \{1\},$$

donc G aussi. Par le thorème précédent, E est résoluble par radicaux. □

Lemme 7.1.14. *1. Le groupe A_n est engendré par les 3-cycles.*

2. Si $n \geq 5$, $[A_n, A_n] = A_n$. En particulier, A_n et $\mathfrak{S}_n$ ne sont pas résoubles.

Démonstration. 1. $\forall \sigma \in A_n$, σ est un produit d'un nombre pair de transpositions. On a

$$(a\ b)(b\ c) = (a\ b\ c),$$
$$(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d).$$

Ainsi, σ est un produit de 3-cycles.

2. Soit $(a\ b\ c) \in A_n$. Comme $n \geq 5$, il existe d, e, distincts de a, b et c. Puis,

$$(a\ b\ c) = (b\ c\ e)(a\ d\ b)(b\ c\ e)^{-1}(a\ d\ b)^{-1}.$$

Donc tout 3-cycle est un commutateur, et donc $A_n = [A_n, A_n]$.

□

Corollaire 7.1.15. *Si $f \in K[X]$ est un polynome irréductible de degré $n \geq 5$ dont le groupe de Galois est A_n ou $\mathfrak{S}_n$, alors l'équation $f(X) = 0$ n'est pas résoluble par radicaux.*

Il reste à trouver de tels polynomes...

7.2 Equation générale de degré n

Soit $K[X_1, \ldots, X_n]$ l'anneau des polynomes à n indéterminées, et $K(t_1, \ldots, t_n)$ son corps des fractions. Le groupe $\mathfrak{S}_n$ agit sur $K(t_1, \ldots, t_n)$ par permutation des intéterminées :

$$\sigma \cdot f(t_1, \ldots, t_n) = f(t_{\sigma(1)}, \ldots, t_{\sigma(n)}), \qquad \forall f \in K(t_1, \ldots, t_n), \forall \sigma \in \mathfrak{S}_n.$$

L'action définit un automorphisme $\sigma : K(t_1, \ldots, t_n) \longrightarrow K(t_1, \ldots, t_n)$. Donc $\mathfrak{S}_n$ agit que $K(t_1, \ldots, t_n)$ par automorphisme, et par the théorème d'Artin, $K(t_1, \ldots, t_n)$ est une extension galoisienne de $K(t_1, \ldots, t_n)^{\mathfrak{S}_n}$. Posons

$$g(X) = \prod_{i=1}^{n} (X - t_i) \in K(t_1, \ldots, t_n)[X].$$

Alors $g(X)$ est fixé par l'action de $\mathfrak{S}_n$. On peut écrire

$$g(X) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^{n-1} s_{n-1} X + (-1)^n s_n,$$

où $s_1, \ldots, s_n \in K(t_1, \ldots, t_n)^{\mathfrak{S}_n}$ sont les fonctions symétriques élémentaires en $t_1, \ldots, t_n$:

$$s_k = \sum_{1 \leq i_1 < \ldots < i_k \leq n} \prod_{j=1}^{k} X_j^{i_j}.$$

L'équation $g(X) = 0$ s'appelle *l'équation générale de degré n.*

Lemme 7.2.1. *1. $K(t_1, \ldots, t_n)^{\mathfrak{S}_n} = K(s_1, \ldots, s_n)$.*

2. $s_1, \ldots, s_n$ sont algébriquement indépendants.

Démonstration. 1. On a

$$K(s_1,\dots,s_n) \leq K(t_1,\dots,t_n)^{\mathfrak{S}_n} \leq K(t_1,\dots,t_n).$$

On sait que $[K(t_1,\dots,t_n) : K(t_1,\dots,t_n)^{\mathfrak{S}_n}] = |\mathfrak{S}_n| = n!$, par le théorème d'Artin. Puis, $K(t_1,\dots,t_n)$ est le corps de décomposition du polynome $g(X)$, à coefficient dans $K(s_1,\dots,s_n)$. Or, le degré du corps de décomposition de $g(X)$ est au plus $n!$. Donc

$$\begin{aligned}&\underbrace{[K(t_1,\dots,t_n) : K(t_1,\dots,t_n)^{\mathfrak{S}_n}]}_{=n!}[K(t_1,\dots,t_n)^{\mathfrak{S}_n} : K(s_1,\dots,s_n)]\\ &= [K(t_1,\dots,t_n) : K(s_1,\dots,s_n)]\\ &\leq n!.\end{aligned}$$

Ainsi, $K(t_1,\dots,t_n)^{\mathfrak{S}_n} = K(s_1,\dots,s_n)$.

2. (Esquisse) Si $s_1,\dots,s_n$ étaient algébriquement dépendants, il existerait un polynome non nul qui s'annulerait en $s_1,\dots,s_n$, et donc on aurait un polynome en $t_1,\dots t_n$ qui serait nul.

□

Corollaire 7.2.2. *$K(t_1,\dots,t_n)$ est une extension galoisienne de $K(s_1,\dots,s_n)$ de groupe de Galois $\mathfrak{S}_n$. Le polynome $g(X) = \sum_{i=0}^{n}(-1)^i s_i X^{n-i} \in K(s_1,\dots,s_n)[X]$ a comme groupe de Galois $\mathfrak{S}_n$. Ainsi, $g(X) = 0$ est résoluble par radicaux si et seulement si $n \leq 4$.*

Question : sur $\mathbb{Q}$, existe-t-il des polynomes de groupe de Galois non résolubles ? Oui, on va construire des polynomes $f \in \mathbb{Q}[X]$ avec groupe de Galois $\mathfrak{S}_p$, avec p premier.

Théorème 7.2.3. *Soit p un nombre premier, et $f \in \mathbb{Q}[X]$ irréductible de degré p. On suppose que f possède $p-2$ racines réelles, et 2 racines complexe conjuguées distinctes (donc non réelles). Alors le groupe de Galois de f est $\mathfrak{S}_p$.*

Démonstration. Soit α_1 une racine f. Alors $\mathbb{Q} \leq \mathbb{Q}[\alpha_1] \leq E$, où E est le corps de décomposition de f. Alors $[\mathbb{Q}[\alpha_1],\mathbb{Q}] = p$ car f est irréductible. Soit $G = \mathrm{Gal}(E,\mathbb{Q})$. Rappelons que G s'injecte dans $\mathfrak{S}_p$ par permutation des racines de f. Comme $p \mid [E:\mathbb{Q}]$, $p \mid |G|$, et donc G possède un élément σ d'ordre p (théorème de Sylow). La permutation correspondante doit forcément être un p-cycle $(a_1\ a_2 \cdots a_p) \in \mathfrak{S}_p$. On numérote les racines de sorte que les deux racines comlpexes (conjuquées) aient les numéros 1 et 2. Sans perde de généralité, $a_1 = 1$, et $a_k = 2$, pour un certain $1 < k \leq p$. Alors $\sigma^{k-1}(1) = a_k$, et $\rho = \sigma^{k-1}$ est de nouveau un p-cycle, car $k-1 < p$, et p est premier, et donc $\langle\sigma\rangle = \langle\rho\rangle$. Ainsi, $\rho = (1\ 2\ b_3 \cdots b_p)$. On choisi la numérotation des $p-2$ racines réelles de sorte que $b_i = i$, i.e. $\rho = (1\ 2\ 3 \cdots p)$. Maintenant, la conjugaison complexe $\tau : \mathbb{C} \longrightarrow \mathbb{C}$ restreinte à E est un élément de $\mathrm{Gal}(E,\mathbb{Q})$, et a pour permutation correspondante $(1\ 2)$. On considère le sous groupe $H = \langle\rho,\tau\rangle \leq \mathfrak{S}_p$. On a

$$\begin{aligned}\rho^i\tau\rho^{-i} &= (\rho^i(1)\ \rho^i(2)) = (i+1\ i+2) \in H,\\ (k-1\ k)(1\ k-1)(k-1\ k) &= (k-1\ k) && \text{par rec. } (1\ k) \in H,\\ (1\ i)(1\ k)(1\ i) &= (i\ k) \in H.\end{aligned}$$

Donc au bout du compte, toutes les transpositions sont dans H, et $H = \mathfrak{S}_p$. Donc $G \cong \mathfrak{S}_p$. □

Il faut maintenant construire un tel polynome. Soit $p \geq 5$ un nombre premier. Soient $n_1 < n_2 < \cdots < n_{p-2}$ des entiers pairs, soit $m \geq \sum_i \frac{n_i^2}{2}$ un entier pair. Posons $g(X) = (X^2 + m)\prod_i (X - n_i) \in \mathbb{Z}[X]$, et $f(X) = g(X) - 2$. Le coefficient constant de f est divisible par 2 mais pas par 4, et tous les autres coefficients non dominant sont pairs. Donnnnc par le critère d'Eisenstein, f est irréductible, de degré p. On a

$$g(n_i - 1) \begin{cases} < -2 & \text{si } i \text{ est impair,} \\ > -2 & \text{si } i \text{ est pair.} \end{cases}$$

Donc

$$f(n_i - 1) \begin{cases} < 0 & \text{si } i \text{ est impair,} \\ > 0 & \text{si } i \text{ est pair.} \end{cases}$$

Il y a $p-2$ changement de signe, donc en tout cas $p-2$ racines réelles. Soit $\alpha_1, \ldots, \alpha_p$ les racines de f. Alors

$$\sum_i \alpha_i = -\text{coeff. de } X^{p-1} = -\sum_{i=0}^{p-2} n_i,$$
$$\sum_{i,j} \alpha_i \alpha_j = \text{coeff. de } X^{p-2} = \sum_{i \neq j \leq p-2} n_i n_j + m.$$

Alors

$$\begin{aligned} \sum_i \alpha_i^2 &= \left(\sum_i \alpha_i\right)^2 - 2\sum_{i \neq j} \alpha_i \alpha_j \\ &= \left(\sum_{i=1}^{p-2} n_i\right)^2 - 2\left(\sum_{i \neq j \leq p-2} n_i n_j + m\right) \\ &= \sum_{i=1}^{p-2} n_i^2 - 2m. \end{aligned}$$

Par le choix de m, on trouve un nombre négatif. Si les deux dernières racines étainent réelles, on aurait une somme négative de carré de réels, ce qui est impossible. Donc les deux dernières racines sont complexes, nécessairement conjuguées, non réelles. Le théorème précédent s'applique, et $f \in \mathbb{Q}[X]$ a pour groupe de Galois $\mathfrak{S}_p$, et l'équation $f(X) = 0$ n'est pas résoluble par radicaux.

Chapitre 8

Corps finis

8.1 Rappels

Lemme 8.1.1. *Soit K un corps fini.*

1. *La caractéristique de K est un nombre premier.*
2. *K est une extension finie de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, où $p = \operatorname{car} K$.*

Démonstration. 1. Si K est de caractéristique 0, alors il existe une injection $\mathbb{Z} \hookrightarrow K$, ce qui est absurde. De plus, K est un anneau intègre, donc de caractéristique première.

2. Comme $\operatorname{car} K = p$, on a $\underbrace{1 + \cdots + 1}_{p \text{ fois}} = 0$, donc $\underbrace{\{0, \ldots, p-1\}}_{\cong \mathbb{Z}/p\mathbb{Z}} \subseteq K$.

□

Lemme 8.1.2. *Soit K un corps fini de caractéristique p.*

1. *$|K| = p^r$, pour un certain $r \in \mathbb{N}^*$.*
2. *$\forall x \in K^*$, $x^{p^r-1} = 1$.*
3. *$\forall x \in K$, $x^{p^r} = x$.*
4. *K est le corps de décomposition du polynome $X^{p^r} - X$.*

Démonstration. 1. K est une extension finie de $\mathbb{F}_p$. Soit $r = [K, \mathbb{F}_p]$. Alors K est un $\mathbb{F}_p$-espace vectoriel de dimension r, et donc $|K| = |\mathbb{F}_p^r| = p^r$.

2. K^* est un groupe d'ordre $|K| - 1 = p^r - 1$.

3. Découle du point précédent.

4. $X^{p^r} - X$ a p^r racines distinctes dans $\overline{\mathbb{F}_p}$, car $(X^{p^r} - X)' = -1$, et donc il n'a aucune racine multiple. Il les a déja dans K, donc K est bien le corps de décomposition de $X^{p^r} - X$.

□

Théorème 8.1.3 (Existence et unicité)**.** *Soit p un nombre premier, et $r \in \mathbb{N}^*$.*

1. *Il existe un corps K de cardinalité p^r.*

2. *Un tel K est unique à isomorphisme près. Dans une cloture algébrique $\overline{\mathbb{F}_p}$, un tel K est unique.*
3. *K est le corps de décomposition de $X^{p^r} - X \in \mathbb{F}_p[X]$.*

Démonstration. 1. Soit E un corps de décomposition de $X^{p^r} - X \in \mathbb{F}_p[X]$. Soit $R \subseteq E$ l'ensemble de ses racines. On a $\mathbb{F}_p \subseteq R$. On montre que R est un sous corps de E :

$$(x \pm y)^{p^r} = x^{p^r} \pm y^{p^r} = x \pm y,$$
$$(xy)^{p^r} = x^{p^r} y^{p^r} = xy.$$

Donc R est stable sous addition et multiplication. Comme il est fini, il est aussi stable par inversion, et donc c'est un sous corps de E. Le polynome $X^{p^r} - X$ se décompose dans R, donc $R = E$. De plus, $|E| = |R| = p^r$.

2. Par unicité d'un corps de décomposition.
3. Déja prouvé dans le point 1.

□

Théorème 8.1.4. *1. Tout sous groupe fini du groupe multiplicatif d'un corps K (non nécessairement fini) est cyclique, et constiué de racines de l'unité.*

2. Si K est un corps fini, alors K^* est cyclique.

Démonstration. 1. Soit A un sous groupe fini de K^*. Alors A est abélien, et isomorphe à un produit de groupes cycliques $\prod_{i=1}^{m} A_i$, avec $|A_i| \mid |A_{i+1}|$. Soit $a = (1, \ldots, 1, g)$, où g est un générateur de A_n. Alors a est d'ordre s, où $s = |A_m|$. Tous les éléments a^i sont racines du polynome $X^s - 1$, où $0 \leq i < s$. Or tout élément $x \in A$ satisfait aussi $x^s = 1$. Donc $m = 1$, et $A = A_m$ est cyclique.

2. Clair à partir du point précédent.

□

Notation 8.1.5. Si $q = p^r$ est une puissance d'un nombre premier p, on note $\mathbb{F}_q$ le corps fini à q éléments.

8.2 Et Galois dans tout ca ?

Théorème 8.2.1 (Extensions de corps finis)**.** *Soit $\mathbb{F}_q$ un corps fini à $q = p^r$ éléments, et soit $\mathbb{F}_{q'}$ un corps fini à $q' = p^s$ éléments, tous les deux dans une même cloture algébrique $\overline{\mathbb{F}_p}$. Alors $\mathbb{F}_{q'}$ est une extension de $\mathbb{F}_q$ si et seulement si $r \mid s$. De plus, l'extension est galoisienne.*

Démonstration. Supposons $\mathbb{F}_{q'}$ est une extension de $\mathbb{F}_q$ de degré m. Alors $\mathbb{F}_{q'}$ est un $\mathbb{F}_q$ espace vectoriel de dimension m, donc $q' = q^m$, et on a bien $r \mid s$. De plus, c'est un extension normale (car $\mathbb{F}_{q'}$ est un corps de décomposition) et séparable (car corps finis), donc galoisienne. □

Théorème 8.2.2 (Groupe de Galois des corps finis)**.** *Soient $q = p^r$, $q' = p^{nr}$, avec p premier. Alors* $\mathrm{Gal}(\mathbb{F}_{q'}, \mathbb{F}_q)$ *est cyclique d'ordre n, engendré par l'*automorphisme de Frobenius *:*

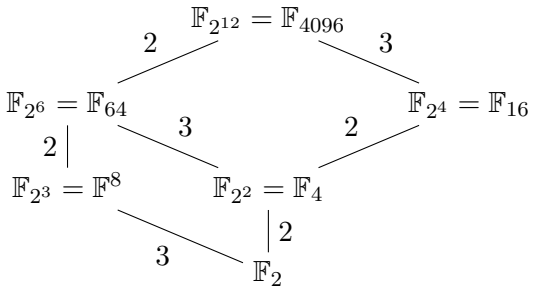
$$\sigma : \mathbb{F}_{q'} \longrightarrow \mathbb{F}_{q'}$$
$$x \longmapsto x^q.$$

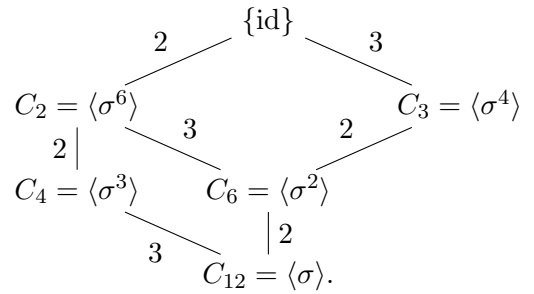
Démonstration. σ est bien un automorphisme de corps, d'inverse $x \longmapsto x^{q^{n-1}}$. De plus, $\sigma|_{\mathbb{F}_q} = \mathrm{id}_{\mathbb{F}_q}$, car tout élément de $\mathbb{F}_q$ est d'ordre q. Ainsi, $\sigma \in \mathrm{Gal}(\mathbb{F}_{q'}, \mathbb{F}_q)$. On a $\sigma^k(x) = x^{q^k}$. De plus, si $k < n$, $\sigma^k(g) \neq g$, où g est un générateur de $\mathbb{F}_{q'}^*$. Ainsi, σ est d'ordre n. Or, $|\mathrm{Gal}(\mathbb{F}_{q'}, \mathbb{F}_q)| = [\mathbb{F}_{q'}, \mathbb{F}_q] = n$. Donc $\mathrm{Gal}(\mathbb{F}_{q'}, \mathbb{F}_q) = \langle\sigma\rangle$ est cyclique. □

Pour tout diviseur d de n, il existe un unique sous groupe de $\mathrm{Gal}(\mathbb{F}_{q'}, \mathbb{F}_q)$ cyclique d'ordre n/d engndré par σ^d. Donc il existe une unique extension intermédiaire de degré d, à savoir $\mathbb{F}_{q^d}$.

$$\begin{array}{c} \mathbb{F}_{q'} = \mathbb{F}_{q^n} \\ \Big| \langle\sigma^d\rangle \\ \mathbb{F}_{q^d} \\ \Big| \\ \mathbb{F}_q. \end{array}$$

Exemple 8.2.3. 1.





2.

$$\begin{array}{c} \mathbb{F}_{2^{13}} \\ 13 \Big| \\ \mathbb{F}_2 \end{array} \qquad \begin{array}{c} \{\mathrm{id}\} \\ 13 \Big| \\ C_{13}. \end{array}$$

Chapitre 9

Constructions à la règle et au compas

On part de deux points $(0,0),(0,1) \in \mathbb{R}^2$. Quels points du plan sont constructibles à la règle et au compas ?

9.1 Le théorème

Rappel 9.1.1. A la règle et au compas, on peut construire les choses suivantes :
- la médiatrice d'un segment,
- le milieu d'un segment,
- la parallèle d'un segment en un point donné,
- la perpendiculaires d'un segment en un point donné,
- le 4ème point d'un parallélogramme, ce qui permet de reporter une ditance déja construite à partir d'un autre point déja constuit.

Théorème 9.1.2. *Soit $(\alpha,\beta) \in \mathbb{R}^2$. Alors on peut construire (α,β) à partir de nos deux points donnés en un nombre fini de constructions la règle et au compas si et seulement si $\alpha,\beta \in E$, où E et une tour d'extensions de degré 2, partant de $\mathbb{Q}$.*

Démonstration. Supposons (α,β) constructible (toujours à la règle et au compas). Il suffit de montrer que chaque construction successive correspond à une extension de degré 1 ou 2.
- Si (α,β), (γ,δ) sont construtis, alors la droite qui les relie a poir équation $(\delta-\beta)(x-\alpha)-(\gamma-\alpha)(y-\beta)=0$. Si $\alpha,\beta,\gamma,\delta \in K \geq \mathbb{Q}$, alors la droite précédente est de la forme $ax+by+c=0$, avec $a,b,c \in K$.
- Si (α,β), (γ,δ) sont construtis, alors le cercle de centre (α,β) passant par (γ,δ) a pour équation $(x-\alpha)^2+(y-\beta)^2=(\gamma-\alpha)^2+(\delta-\beta)^2$, i.e. une équation de second degré en x et y, à coefficients dans K.

Puis :
- Intersection de deux droites : on a un système

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

et donc x et y sont dans le meme corps que a,b,c,a',b',c'.

— Intersection d'une droite et d'un cercle : on a un système

$$\begin{cases} ax + by + c = 0 \\ (x-u)^2 + (y-v)^2 - r^2 = 0, \end{cases}$$

on substitue $y = \frac{-ax-c}{b}$, si $b \neq 0$, et on trouve une équation du second degré. Donc x est dans une extension de degré 1 ou 2 de K, et y aussi.

— Intersection de deux cercles : on a un système

$$\begin{cases} (x-u)^2 + (y-v)^2 - r^2 = 0 \\ (x-u')^2 + (y-v')^2 - (r')^2, \end{cases}$$

on soustrait les deux équations pour obtenir une équation de degré 1 (une droite). On est ramené à l'intersection d'une droite avec l'un des deux cercles.

Si on fait n constructions successives, cela correspond à n extensions de corps successives, chacunes de degré 1 ou 2. Réciproquement, on se donne une extension E de $\mathbb{Q}$, obtenue par une tour d'extensions de degré 2. Soient $\alpha, \beta \in E$, et on veut montrer que $(\alpha, \beta) \in \mathbb{R}^2$ est constructible. Par définition de E, α et β peuvent d'écrire à l'aide de

— l'addition,
— la soustraction,
— a multiplication,
— la division (avec un diviseur non nul),
— l'extraction de racines carrés, car toute extension de degré 2 est de la forme $K[\alpha]$, avec $\alpha^2 - c = 0$, $c \in K$.

Il faut montrer que chacune de ces opérations est réalisable à la règle et au compas. Remarquer que (x, y) est constructible si et seulement si $(x, 0)$ et $(0, y)$ sont constructibles, si et seulement si $(x, 0)$ et $(y, 0)$ sont constructibles.

— Addition : Soient $(x_1, 0)$ et $(x_2, 0)$, et considérer le cercle de centre $(\max\{x_1, x_2\}, 0)$, et de rayon $|x_1 - x_2|$.
— Soustraction : on additionne par l'opposé (construit au compas), en utilisant le point précédent.
— Division : on utilise le théorème de Thalès pour les triangles $(0,0), (x_1, 0), (0, 1)$ et $(0, 0), (x_2, 0), (0, x_2/x_1)$, le deuxième étant construit par parallèle.
— Multiplication : on divise par l'inverse en utilisant le point pécédent.
— Extraction de racine carré : considérer le segment $[(-1, 0), (x, 0)]$, et le cercle admettant le segment précédent pour diamètre. On a un triangle rectangle inscrit admettant le segment précédent comme hypothénuse, de hauteur (verticale) h. Alors $(1+x)^2 = (1+h^2) + (h^2 + x^2)$, i.e. $h = \sqrt{x}$.

□

9.2 Problèmes classiques des grècs

— Duplication du carré : Possible car $2x^2 = (\sqrt{2}x)^2$.
— Duplication du cube : Impossible car $\sqrt[3]{2}$ n'est pas constructible, car $X^3 - 2$ est irréductible, donc $[\mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}] = 3$.

— Quadrature du cercle : Impossible car $\sqrt{\pi}$ n'est pas constructible, car π est transcendant (théorème de Lindemann, fin 19ème).
— Bisection d'un angle : Possible par médiatrice.
— Trisection d'un angle : Impossible, car à partir de $e^{i\pi/3} = (1/2, \sqrt{3}/2)$ (qui est constructible), on pourrait construire $e^{i\pi/9}$ (par trisection), et

$$\cos(\pi) = 4\cos(\pi/9)^3 - 3\cos(\pi/9)$$

donne un polynome irréductible $4X^3 - 3X - 1/2$ admettant une racine constructible, ce qui est absurde.

9.3 Polygones réguliers

Définition 9.3.1 (Nombre permier de Fermat)**.** Un nombre est *permier de Fermat* s'il est de la forme $2^m + 1$.

Lemme 9.3.2. *Si $p = 2^m + 1$ est premier, alors m est un puissance de 2.*

Démonstration. Par contraposition, si m n'est pas une puissance de 2, alors $m = ab$, avec $a \geq 3$ impair. Alors $2^b \equiv -1$ $(2^b + 1)$, et donc $2^m = 2^{ab} \equiv (-1)^a = -1$ $(2^b + 1)$. Ainsi $2^b + 1 \mid 2^m + 1$, et $1 < 2^b + 1 < 2^m + 1$. □

Théorème 9.3.3 (Gauss)**.** *On peut construire un polygone régulier à n cotés (inscrit dans le cercle unité spdg) si et seulement si $n = 2^k p_1 \cdots p_r$, où $k \geq 0$, et p_i sont des nombres premiers de Fermat distincts.*

Démonstration. Si on a un n-gone et un m-gone constructibles, avec n et m premiers entre eux, alors on a un mn-gone constructible. En effet, $un + vm = 1$ (Bézout), et

$$e^{\frac{2i\pi}{mn}} = \left(e^{\frac{2i\pi}{m}}\right)^u \left(e^{\frac{2i\pi}{n}}\right)^v.$$

Cela réduit l'analyse au car $n = p^k$, avec p premier.
— Si $p = 2$, alors le $n = 2^k$-gone est constructible par bisections successives.
— Si p est impair, et si un p^k-gone est constructible, alors un p-gone aussi (facile). On peut donc se restrenidre au cas où $n = p$. On a que $\zeta_p = e^{\frac{2i\pi}{p}}$ est une racine primitive p-ième de l'unité. Donc $[\mathbb{Q}[\zeta_p], \mathbb{Q}] = \phi(p) = p - 1$. Donc si $p - 1$ n'est pas une puissance de 2, ζ_p n'est pas constructible. Si $p - 1$ est une puissance de 2, alors $p = 2^m + 1$ est un nombre premier de Fermat. Or $\mathbb{Q}[\zeta_p]$ est une extension galoisienne de $\mathbb{Q}$ avec groupe de Galois $G = (\mathbb{Z}/p\mathbb{Z})^*$, ui est cyclique (donc abélien) d'ordre $p - 1$. On applique le théorème de structure des groupes abéliens finis : $G = G_0 > \cdots G_r = \{1\}$, avec G_{i+1} d'indice 2 dans G_i. Par correspondance de Galois, le corps $\mathbb{Q}[\zeta_p]$ est obtenu par une tour d'extensions de degré 2 à partir de $\mathbb{Q}$. Donc ζ_p est constructible. En revache, ζ_{p^2} n'est pas constructible, car $\phi(p^2) = p(p-1)$ n'est pas une puissance de 2.

□

Exemple 9.3.4. 1. $\cos\left(\frac{2\pi}{5}\right)$ est de degré 2 sur $\mathbb{Q}$, donc constructible.

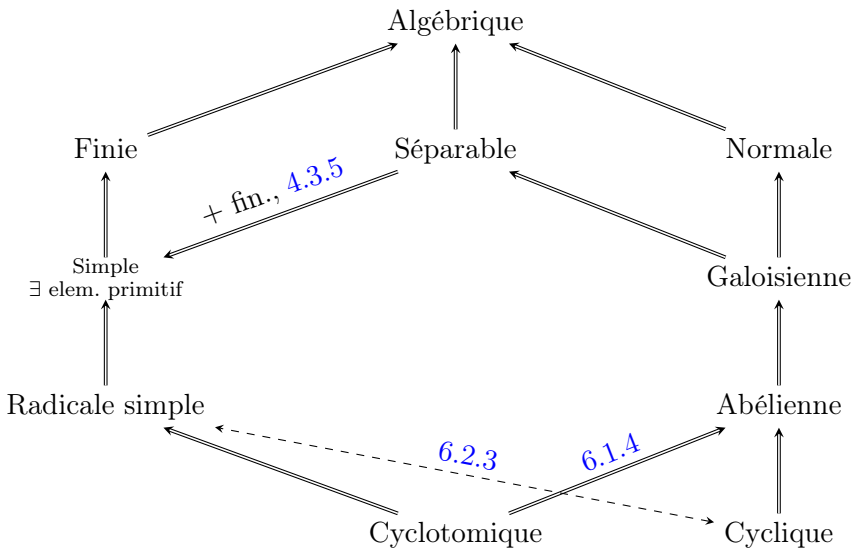
2. $\cos\left(\frac{2\pi}{17}\right)$ est constructible, car $17 = 2^{2^2} + 1$ est premier de Fermat.

$$\cos\left(\frac{2\pi}{17}\right) = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

Merci Gauss...

Annexe A

Petit diagramme des types d'extensions



Index