Chapitre 4

Théorie de Galois

Notation : une extension $f : K \to L$ sera notée simplement $(L{:}K)$ s'il n'y a pas d'ambiguïté ; en cas de besoin on pourra préciser : $(L : K, f)$.

4.1 Extensions normales

Définition 4.1.1. Une extension $(L : K)$ est normale si et seulement si tout polynôme irréductible de $K[X]$ qui admet une racine dans L est scindé dans L.

Théorème 4.1.2. *Soit $(L : K)$ une extension. Il y a équivalence entre :*
a) l'extension est normale et de degré fini ;
b) L est corps de décomposition d'un polynôme unitaire de $K[X]$.

Définition 4.1.3. Une clôture normale d'une extension de degré fini : $(L : K)$ est une extension normale minimale $L' : L)$:
a) l'extension $(L' : K)$ est normale, et
b) si on a une tour d'extension $(L' : E : L : K)$ telle que $(E : K)$ est normale, alors : $E = L'$.

Théorème 4.1.4. *Toute extension de degré fini admet une clôture normale, et deux telles clôtures sont isomorphes.*

4.2 Extension galoisienne

Définition 4.2.1. Une extension de corps est galoisienne si et seulement si elle est normale et séparable.

Nous allons étudier les extensions galoisiennes de degré fini via leurs automorphismes.

Définition 4.2.2. a) Un automorphisme du corps K est un homomorphisme bijectif de K dans lui-même.
b) Un automorphisme d'une extension $(L : K)$ est un automorphisme de L qui est un morphisme de K-algèbre.

Proposition 4.2.3. *Les automorphismes d'un corps K forment un groupe :* $\mathrm{Aut}(K)$. *Les automorphismes d'une extension $(L : K)$ forment un groupe :* $\mathrm{Gal}(L : K)$.

Définition 4.2.4. Le groupe $\mathrm{Gal}(L : K)$ est appelé groupe de Galois de l'extension $(L : K)$.

Remarque 4.2.5. Lorsque K est le sous-corps premier de L, $\mathrm{Gal}(L : K) = \mathrm{Aut}(L)$.

Théorème 4.2.6. *Soit $L : K$ une extension de degré fini, alors il y a équivalence entre :*
a) l'extension est galoisienne,
b) $|\mathrm{Gal}(L : K)| = [L : K]$,
c) L est corps de décomposition d'un polynôme séparable sur K.

Soit H un groupe fini d'automorphismes du corps L, alors l'ensemble L^H des éléments fixés par tous les éléments de H est un sous-corps de L : le corps fixe de H. Si le groupe H est contenu dans le groupe de Galois $\mathrm{Gal}(L : K)$, alors L^H est une extension de K.

Théorème 4.2.7. *Soit H un groupe fini d'automorphismes du corps L et L^H le corps fixe associé. Alors l'extension $(L : L^H)$ est galoisienne, de groupe de Galois H.*

Démonstration. Nous allons démontrer dans le lemme qui suit que le degré $n = [L : L^H]$ est fini et majoré par le cardinal m du groupe H. On a alors :

$$H \subset \mathrm{Gal}(L : L^H) = \mathrm{Hom}_{L^H-\mathrm{alg}}(L, L) \ .$$

Le nombre de L^H-morphismes est majoré par le degré : $m \leq n$. □

Lemme 4.2.8. *Sous les hypothèses du théorème précédent,*

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

Démonstration. Notons $H = \{\sigma_1 = Id_L, \sigma_2, \ldots, \sigma_m\}$, et supposons que $m < n$. Fixons une partie libre de L sur L^H de cardinal $m+1 : x_1, \ldots, x_{m+1}$. La matrice formée par les $\sigma_i(x_j)$, $1 \leq i \leq m$, $1 \leq j \leq m+1$, a m lignes et $m+1$ colonnes : ses colonnes sont dépendantes. On renumérote éventuellement,

pour que les r premières colonnes forment une partie liée minimale (rang $r-1$). On a une relation de dépendance avec tous les coefficients $y_j \in L$ non nuls :

$$\forall i \ \sum_{j=1}^{r} \sigma_i(x_j) y_j = 0 \ .$$

On peut trouver une telle relation avec $y_1 = 1$, ce que nous supposons désormais.

$$\forall \tau \in H \ \forall i \ \sum_{j=1}^{r} \tau(\sigma_i(x_j) y_j) = 0 \ .$$

En posant $\tau\sigma_i = \sigma_k$:

$$\forall \tau \in H \ \forall k \ \sum_{j=1}^{r} \sigma_k(x_j) \tau(y_j) = 0 \ .$$

Pour chaque τ on obtient une nouvelle relation. En utilisant que le rang est égal à $r-1$, et que $\tau(y_1) = y_1 = 1$, on obtient pout tout j, $\tau(y_j) = y_j$. Chaque y_j est fixé par tous les élements de H : $y_j \in L^H$. Reprenons la relation de dépendance qui est maintenant à coefficients dans L^H :

$$\forall i \ \sum_{j=1}^{r} \sigma_i(x_j) y_j = 0 \ .$$

Avec $i = 1$, on obtient une relation de dépendance entre les x_j, ce qui donne une contradiction. On conclut : $[L : L^H] \leq m$. □

07/10/2011

Corollaire 4.2.9. *Une extension de degré fini $(L : K, f)$ est galoisienne si et seulement si $f(K) = L^{\mathrm{Gal}(L,K)}$.*

4.3 Correspondance de Galois

Théorème 4.3.1 (Galois)**.** *Soit $(L : K, f)$ une extension de degré fini galoisienne, alors :*
i) l' application : $H \mapsto L^H$, établit une bijection entre les sous-groupes H de $\mathrm{Gal}(L : K)$, et les corps E intermédiaires : $f(K) \subset E \subset L$; la bijection réciproque étant $E \mapsto \mathrm{Gal}(L : E)$.
ii) L'extension $(L^H : K)$ est galoisienne si et seulement si H est un sous-groupe distingué de $\mathrm{Gal}(L : K)$. Dans ce cas le groupe de Galois, $\mathrm{Gal}(E : K)$ est isomorphe au quotient : $\mathrm{Gal}(L : K)/H$.

La preuve du ii) dans le théorème de Galois utilise le lemme suivant :

Lemme 4.3.2. *Soient $(L : K)$ une extension galoisienne, et $E \subset L$ le sous-corps (*corps intermédiaire*) associé au sous-groupe $H \subset \mathrm{Gal}(L : K)$, alors pour tout $\sigma \in \mathrm{Gal}(L : K)$, on a $\mathrm{Gal}(L : \sigma(E)) = \sigma H \sigma^{-1}$, et la restriction définit un morphisme surjectif $N(H) \to \mathrm{Gal}(E, K)$ de noyau $\mathrm{Gal}(L : E)$. ($N(H)$ est le normalisateur de H, i.e ; le stabilisateur pour l'action de conjugaison sur les sous-groupes).*

Exercice 4.3.3. Etudier les extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, j)$ ($j = e^{i\frac{2\pi}{3}}$). Sont-elles galoisiennes ? Calculer le groupe de Galois. Déterminer les corps intermédiaires.

4.4 Un exemple élémentaire

Soit $L \subset \mathbb{C}$ le corps de décomposition (sur $\mathbb{Q}$) de $X^4 - 2$. C'est une extension galoisienne, comme corps de décomposition d'un polynôme séparable (en caractéristique zéro tout polynôme est séparable). Les racines de $X^4 - 2$ sont $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$. Le polynôme $X^4 - 2$ étant irréductible sur $\mathbb{Q}$ (justifier), l'extension $(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q})$ est de degré 4. L'extension $(L : \mathbb{Q}(\sqrt[4]{2}))$ est de degré 2 : elle est engendrée par i qui n'est pas dans $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$. On a donc : $[L : \mathbb{Q}] = 8$. Le groupe de Galois $G = \mathrm{Gal}(L : \mathbb{Q})$ est de cardinal 8. Pour $\rho \in G$, $\rho(i) = \pm i$ et $\rho(\sqrt[4]{2}) \in \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. L'application

$$\begin{array}{rccc} r : & G & \to & \{\pm i\} \times \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\} \\ & \rho & \mapsto & (\rho(i), \rho(\sqrt[4]{2})) \end{array}$$

est injective, car i et $\sqrt[4]{2}$ engendrent l'extension. C'est une application entre ensembles finis de mêmes cardinaux : elle est bijective. Les éléments $\tau = r^{-1}(-i, \sqrt[4]{2})$, $\sigma = r^{-1}(i, i\sqrt[4]{2})$ engendrent le groupe G, avec les relations :

$$\tau^2 = \sigma^4 = id \ , \ \sigma\tau = \tau\sigma^{-1} \ .$$

On reconnaît le groupe diédral D_4 (groupe des isométries du carré). Il y a 5 éléments d'ordre 2 et un élément d'ordre 4 qui engendrent des sous-groupes cycliques, et il y a deux sous-groupes de cardinal 4 non cycliques. Voir les corps correspondants dans la figure 4.1. 12/10/2011

4.5 Corps cyclotomiques

Définition 4.5.1. On appelle corps cyclotomique une extension $(\mathbb{Q}(\zeta_n) : \mathbb{Q})$, où ζ_n est une racine primitive n-ième de l'unité.

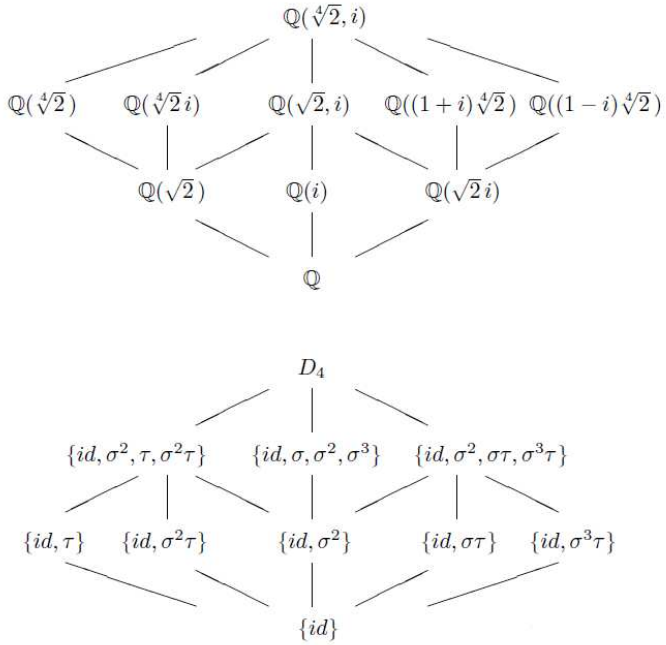

FIGURE 4.1 – Correspondance de Galois pour $X^4 - 2$

Proposition 4.5.2. *L'extension cyclotomique* $(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ *est galoisienne, de groupe de Galois isomorphe à* $(\mathbb{Z}/n\mathbb{Z})^\times$.

Démonstration. Le corps cyclotomique $\mathbb{Q}(\zeta_n)$ est le corps de décomposition sur $\mathbb{Q}$ du polynôme $X^n - 1$: c'est une extension galoisienne. Le polynôme minimal de ζ_n est le polynôme cyclotomique Φ_n dont les racines sont les ζ_n^k, $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. Notons $\tau_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ l'automorphisme correspondant à ζ_n^k. On a : $\tau_k \tau'_k = \tau_{kk'}$. Les groupes $\mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ et $(\mathbb{Z}/n\mathbb{Z})^\times$ sont isomorphes. □

Remarque 4.5.3. La structure du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ découle du théorème chinois et des résultats suivants (voir par exemple le cours d'arithmétique de Bernhard Keller, section 19, `http://www.math.jussieu.fr/~keller/mt282/arith.pdf` :

1. Pour p premier impair et $\alpha > 0$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.
2. Pour $\alpha \geq 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est isomorphe au produit de $\mathbb{Z}/2$ par un groupe cyclique.

On peut en déduire les sous-groupes et donc les sous-corps de $\mathbb{Q}(\zeta_n)$.

Exercice 4.5.4. Etudier les sous-corps de $\mathbb{Q}(\zeta_{12})$.

4.6 Corps finis

Proposition 4.6.1. *Soit $\mathbb{F}_q$, $q = p^m$, un corps à q-éléments. L'extension $(\mathbb{F}_q : \mathbb{F}_p)$ est galoisienne. Le groupe de Galois est cyclique, engendré par l'automorphisme de Frobenius.*

Démonstration. Pour un corps fini, le morphisme de Frobenius $F : x \mapsto x^p$ est un automorphisme : $F \in \mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p)$. On va montrer qu'il est d'ordre $m = [\mathbb{F}_q : \mathbb{F}_p]$. Cela justifie que l'extension est galoisienne : $\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p) = [\mathbb{F}_q : \mathbb{F}_p]$, et que F engendre le groupe de Galois.
Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique de cardinal $q - 1$. Notons α un générateur : α engendre l'extension. On a $\frac{F^\nu(\alpha)}{\alpha} = \alpha^{p^\nu - 1}$, d'où :

$$F^m = Id \text{ et } F^\nu \neq Id \text{ pour } 0 < \nu < m \ .$$

□

Remarque 4.6.2. La correspondance de Galois redonne que les sous-corps de F_q sont en bijection avec les diviseurs de m.

4.7 Groupe de Galois d'un polynôme

Définition 4.7.1. Le groupe de Galois d'un polynôme est celui d'une extension qui réalise un corps de décomposition : pour $P \in K[X]$, $\mathrm{Gal}(P) = \mathrm{Gal}(L : K)$, où L est corps de décomposition de P.

Remarque 4.7.2. L'extension qui réalise un corps de décomposition d'un polynôme P est galoisienne si et seulement si le polynôme est séparable.

Proposition 4.7.3. *Le groupe de Galois de P agit sur les racines de P, et cette action est fidèle : on obtient un isomorphisme entre* $\mathrm{Gal}(P)$ *et un sous-groupe du groupe des permutations des racines de P.*

14/10/2011

Le groupe des permutations des racines d'un polynôme P, isomorphe au groupe symétrique $\mathcal{S}_n$ contient le sous-groupe des permutations paires (isomorphe au groupe alterné $\mathcal{A}_n$.

Définition 4.7.4. Le discriminant de $P = \prod_{i=1}^n (X - x_i)$ est $D = \prod_{i \neq j}(x_i - x_j)$.

Remarque 4.7.5. Le discriminant est invariant sous l'action du groupe de Galois de P ; il appartient au corps K et plus précisément au corps engendré par les coefficients de P. L'expression précise sera donnée plus tard.

Proposition 4.7.6. *Le groupe de Galois d'un polynôme séparable $P \in K[X]$ est contenu dans le sous-groupe des permutations paires si et seulement si le discriminant de P est un carré dans K.*

Démonstration. Le discriminant de $P = \prod_{i=1}^{n}(X - x_i)$ est $D = d^2$, avec $d = \prod_{1 \leq i < j \leq n}(x_i - x_j)$. C'est un carré dans le corps K si et seulement si d est fixe par tous les élements du groupe de Galois. Pour une permutation σ des racines de P, $\sigma.d = \epsilon_\sigma d$, où ϵ_σ est la signature : le discriminant de P est un carré dans K si et seulement si tout élément du groupe de Galois induit une permutation paire. □