Chapitre 7

Théorie de Galois

Notation : On note $(F : K)$ l'extension $K \subset F$.

7.1 Automorphismes de corps

Définition 7.1.1. a) Un automorphisme du corps K est un homomorphisme bijectif de K dans lui-même.
b) Un automorphisme d'une extension $(F : K)$ est un automorphisme de F qui fixe les éléments de K (dont la restriction à K est l'identité).

Proposition 7.1.2. *Les automorphismes d'un corps K forment un groupe :* $\mathrm{Aut}(K)$. *Les automorphismes d'un extension $(F : K)$ forment un groupe qu'on appelle groupe de Galois de l'extension :* $\mathrm{Gal}(F : K)$.

Remarque 7.1.3. Lorsque K est le sous-corps premier de F, $\mathrm{Gal}(F : K) = \mathrm{Aut}(F)$.

Proposition 7.1.4. *Soit H un sous-groupe d'un groupe de Galois* $\mathrm{Gal}(F : K)$, *alors l'ensemble L^H des éléments fixés par tous les éléments de H est un sous-corps de L qui contient K : le corps fixe de H.*

Proposition 7.1.5. *Soit $\sigma \in \mathrm{Gal}(L : K)$, et $\alpha \in L$ un élément algébrique sur K, alors $\sigma(\alpha)$ est une racine du polynôme minimal de α.*

Corollaire 7.1.6. *Si l'extension $(L : K)$ est de degré fini ou plus généralement engendrée par un nombre fini d'éléments algébriques : $L = K(\alpha_1, \ldots, \alpha_m)$, alors le groupe de Galois* $\mathrm{Gal}(L : K)$ *est fini.*

Théorème 7.1.7. *Si F est corps de décomposition d'un polynôme $Q \in K[X]$, alors on a l'inégalité :*

$$|\mathrm{Gal}(F : K)| \leq [F : K] \ ,$$

et l'égalité a lieu si et seulement si Q est séparable (produit de polynômes irréductibles séparables).

Démonstration. On peut supposer que Q est produit de facteurs irréductibles distints. On procède par récurrence sur $n = [F : K]$. Pour $n = 1$, on a $F = K$ et $\mathrm{Gal}(F : K) = \{\mathrm{Id}_K\}$. Supposons le résultat établi pour tout corps de décomposition réalisant une extension de degré strictement inférieur à n. Soit L un corps de décomposition de $Q \in K[X]$, avec $[L : K] = n$, et soit P un diviseur irréductible de Q. On a une tour d'extension :

$$K \subset K(\alpha) \subset L \ .$$

On considère le morphisme de restriction :

$$j : \mathrm{Gal}(L : K) \to \mathrm{Gal}(K(\alpha) : K) \ .$$

Le noyau de j est égal au groupe $\mathrm{Gal}(L : K(\alpha))$. On déduit :

$$\begin{array}{rcl} |\mathrm{Gal}(L : K)| & = & |\mathrm{Gal}(K(\alpha) : K)| \times |\mathrm{Im}(j)| \\ & \leq & |\mathrm{Gal}(K(\alpha) : K)| \times |\mathrm{Gal}(L : K(\alpha))| \end{array} \ .$$

On a : $|\mathrm{Gal}(K(\alpha) : K)| \leq \deg(P) = [K(\alpha) : K]$, et par hypothèse de récurrence : $|\mathrm{Gal}(L : K(\alpha))| \leq [L : K(\alpha)]$, d'où l'inégalité :

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

Pour être plus précis et déterminer le cas d'égalité, observons que pour chaque racine β de P dans L, il y a exactement un homorphisme f_β de $K(\alpha)$ dans L qui fixe les éléments de K. On considère le diagramme suivant :

$$\begin{array}{ccc} K(\alpha) & \longrightarrow & L \\ {\scriptstyle f_\beta}\downarrow & & \downarrow{\scriptstyle g_\beta} \\ K(\beta) & \longrightarrow & L \end{array}$$

L'existence d'un isomorphisme g_β qui induit f_β résulte du théorème d'unicité du corps de décomposition. D'autre part : $g : F \to F$ est un isomorphisme qui induit f_β si et seulement si : $g_\beta^{-1} g \in \mathrm{Gal}(L : K(\alpha)$. Finalement le cardinal du groupe $\mathrm{Gal}(L : K)$ est égal au produit du nombre de racines de P par le cardinal de $\mathrm{Gal}(L : K(\alpha))$. Le nombre de racines de P est égal au degré de P si et seulement si P est séparable, et par hypothèse de récurrence le cardinal de $\mathrm{Gal}(L : K(\alpha))$ est égal à $[L : K(\alpha)]$ si et seulement si Q est séparable. On obtient le cas d'égalité si et seulement si Q est séparable. $\square$

7.2 Correspondance de Galois

Définition 7.2.1. Une extension $(L : K)$ de degré fini est galoisienne si et seulement le cardinal du groupe de Galois est égal au degré $[L : K]$.

Remarque 7.2.2. Dans le cas général, la définition habituelle est : *normale et séparable*. On va voir qu'en degré fini il y a équivalence avec ci-dessus.

Théorème 7.2.3. *Soit H un groupe fini d'automorphisme du corps L et F^H le corps fixe associé. Alors l'extension $(F : F^H]$ est galoisienne, de groupe de Galois H.*

Etablissons d'abord :

Lemme 7.2.4 (Lemme de Dedekind)**.** *Des homomorphismes de corps distincts de K dans L forment une partie libre dans l'ensemble des applications de K dans L.*

Démonstration. Supposons qu'il existe une famille liée. On peut trouver une sous-famille liée minimale, c'est à dire une famille de m homorphismes distincts $\sigma_1, \ldots, \sigma_m$ qui a pour rang $m-1$. Dans ce cas toutes les relations sont proportionnelles : on a une relation avec tous les coefficients non nuls

$$\sum_{i=1}^{m} \lambda_i \sigma_i = 0 \ ;$$

et si

$$\sum_{i=1}^{m} \mu_i \sigma_i = 0 \ ,$$

alors les $\frac{\mu_i}{\lambda_i}$ sont tous égaux. On obtient :

$$\forall x \in K, \forall y \in K, \ \sum_{i=1}^{m} \lambda_i \sigma_i(yx) = 0 \ ;$$

$$\forall x \in K, \forall y \in K, \ \sum_{i=1}^{m} \lambda_i \sigma_i(y) \sigma_i(x) = 0$$

$$\forall y \in K, \ \sum_{i=1}^{m} \lambda_i \sigma_i(y) \sigma_i = 0 \ .$$

On déduit que pour, tout $y \in K$, tous les $\sigma_i(y)$ sont égaux. Les σ_i étant supposés distincts, il ne reste que la possibilité $m = 1$, exclue également car un homomorphisme de corps n'est pas nul. □

Démonstration. Démontrons le théorème. Posons $n = [F : F^H]$, $m' = |\mathrm{Gal}(F : F^H)|$ et $m = |H|$. Notons que : $H \subset \mathrm{Gal}(F : F^H)$, donc : $m \leq m'$. On applique le lemme précédent à $K = F : H' = \mathrm{Gal}(F : F^H)$ forme une partie libre dans l'ensemble des applications de F dans F. Notons B une base de F sur F^H. Comme les éléments de H' sont F^H-linéaires, les restrictions des éléments de H' à la base B forment aussi une partie libre, et ceci dans un espace vectoriel de dimension n. Donc : $n \geq m' \geq m$.
Supposons que $m < n$. On fixe une partie libre de F sur F^H de cardinal $m+1$: $x_1, \ldots, x_{m+1}$. La matrice formée par les $\sigma(x_j)$, $\sigma \in H$, $1 \leq j \leq m+1$, a m lignes et $m+1$ colonnes : ses colonnes sont dépendantes. Quitte à réordonner, on suppose que les r premières colonnes forment une partie liée minimale (rang $r-1$). On a une relation de dépendance avec tous les coefficients $y_j \in F$ non nuls :

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

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

En posant $\tau\sigma = \gamma$:

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

Pour chaque τ on obtient une nouvelle relation, proportionnelle à la première : pout tout j, $\frac{\tau(y_j)}{\tau(y_1)} = \frac{y_j}{y_1}$.

$$\forall \gamma \in H \ \forall \tau \in H \ \sum_{j=1}^{r} \gamma(x_j) \frac{\tau(y_1)}{y_1} y_j = 0 \ .$$

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

Avec $\gamma = \mathrm{Id}$, on a une relation de dépendance entre les x_j, ce qui donne une contradiction. On conclut : $n = m = m'$, et $H = \mathrm{Gal}(F : F^H)$. □

Corollaire 7.2.5. *Pour toute extension de degré fini, on a :*

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

Corollaire 7.2.6. *Une extension de degré fini $(F : K)$ est galoisienne si et seulement si $K = F^H$, où $H = \mathrm{Gal}(F : K)$.*

Théorème 7.2.7. *Une extension de degré fini est galoisienne si et seulement si c'est le corps de décomposition d'un polynôme séparable.*

Théorème 7.2.8 (Galois)**.** *Soit* $(L : K)$ *une extension de degré fini galoisienne, alors :*
i) l' application : $H \mapsto F^H$ *, établit une bijection entre les sous-groupes* H *de* $\mathrm{Gal}(F : K)$*, et les corps* E *intermédiaires :* $K \subset E \subset F$ *; la bijection réciproque étant* $E \mapsto \mathrm{Gal}(F : E)$ *.*
ii) L'extension $(F^H : K)$ *est galoisienne si et seulement si* H *est un sous-groupe distingué de* $\mathrm{Gal}(F : K)$ *et dans ce cas la resrtiction induit un isomorphisme* $\mathrm{Gal}(F : K)/H \approx \mathrm{Gal}(F^H : K)$*.*

7.3 Exemples

...

Corps cyclotomiques

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

Corps finis

Pour $q = p^m$, l'extension $(\mathbb{F}_q : \mathbb{F}_p)$ est galoisienne. Le groupe de Galois est cyclique, engendré par l'automorphisme de Frobenius.

Fin du cours du 30 novembre

7.4 Compléments

Proposition 7.4.1. *Soit* $(F : K)$ *une extension de degré fini galoisienne. Tout élément* $\beta \in F$ *est séparable sur* K*.*

Corollaire 7.4.2. *Soit* $F = K(\alpha_1, \ldots, \alpha_n)$ *une extension algébrique engendrée par les éléments* α_i *séparables, alors tout* $\beta \in F$ *est séparable sur* K*.*

Ceci complète la preuve du théorème 6.6.12.

7.5 Groupe de Galois d'un polynôme séparable

Définition 7.5.1. Le groupe de Galois d'un polynôme séparable est celui de l'extension qui réalise le corps de décomposition : pour $P \in K[X]$, $\mathrm{Gal}(P) = \mathrm{Gal}(F : K)$, où F est le corps de décomposition de P.

Théorème 7.5.2. *Le groupe de Galois du polynôme générique à coefficient dans $K(\sigma_1, \ldots, \sigma_n)$:*

$$X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n \ ,$$

est isomorphe au groupe symétrique $\mathcal{S}_n$.

On note $\mathcal{A}_n$ le groupe alterné (formé des permutations paires).

Proposition 7.5.3. *Pour $P \in K[X]$ séparable, on a :* $\mathrm{Gal}(P) \subset \mathcal{A}_n$ *si et seulement si le discriminant de P est un carré dans K.*

Polynômes de petit degré ...

7.6 Résolubilité par radicaux

Définition 7.6.1. Une extension $(F : K)$ est cyclique si et seulement si elle est galoisienne et son groupe de Galois est cyclique.

Proposition 7.6.2. *Soit K un corps de caractéristique nulle ou première avec n qui contient les racines n-ièmes de l'unité. Pour $a \in K$ l'extension $K(b)$ où b est racine n-ième de a (dans le corps de décomposition de $X^n - a$) est cyclique de degré d diviseur de n.*

Proposition 7.6.3. *Soit $(F : K)$ une extension cyclique de degré n sur un corps de caractéristique première avec n qui contient les racines n-ièmes de l'unité, alors $F = K(b)$ avec b de polynôme minimal $X^n - a$. On note $F = K(\sqrt[n]{a})$.*

Définition 7.6.4. Un polynôme à coefficient dans un corps de caractéristique nulle est résoluble par radicaux si et seulement si son corps de décomposition est obtenu par une suite d'extensions, chacune obtenue par adjonction d'une racine :

$$K = K_0 \subset K_1 \subset \ldots K_m = L \ ,$$

avec $K_i = K_{i-1}(\sqrt[n_i]{a_i})$.

Théorème 7.6.5. *Un polynôme P à coefficient dans un corps de caractéristique nulle est résoluble par radicaux si et seulement si son groupe de Galois G est résoluble, c'est à dire qu'il existe une suite :*

$$G = G_0 \supset G_1 \supset \cdots \supset G_{m+1} = \{e\} \ ,$$

avec G_{i+1} sous-groupe distingué de G_i, et G_i/G_{i+1} abélien.

Théorème 7.6.6. *Pour $n \geq 5$, le polynôme générique de degré n n'est pas résoluble par radicaux.*

Fin du cours du 4 décembre