Théorie de Galois

Alexis TCHOUDJEM
Institut Camille Jordan
Université Claude Bernard Lyon I
Boulevard du Onze Novembre 1918
69622 Villeurbanne
FRANCE

Villeurbanne, le 5 février 2014

Table des matières

Cours du mercredi 22/1/14

Introduction

0.1 Caractéristique

Soit K un corps.

Définition 1 *Soit $p \geq 0$ tel que $p\mathbb{Z} = \ker(\varphi : \mathbb{Z} \to K, n \mapsto n1_K)$. Le nombre p est la caractéristique du corps K.*

Proposition 0.1 *La caractéristique de K est 0 ou un nombre premier > 0.*

Remarque : si $p = 0$, $\mathbb{Q}$ est le plus petit sous-corps de K si $p > 0$, c'est $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

0.2 Polynômes symétriques

Soit K un corps. Si $s \in \mathfrak{S}_n$, si $P \in K[X_1, ..., X_n]$, on note $P^s(X_1, ..., X_n) := P(X_{s(1)}, ..., X_{s(n)})$. (*C'est une action à droite*). On note $K[X_1, ..., X_n]^{\mathfrak{S}_n}$ les polynômes invariants ou *polynômes symétriques.*

On note $\sigma_k(X_1, ..., X_n) := \sum_{1 \leq i_1 < ... < i_k \leq n} X_{i_1}...X_{i_k}$ les *polynômes symétriques élémentaires* :

Proposition 0.2 $K[X_1, ..., X_n]^{\mathfrak{S}_n} = K[\sigma_1, ..., \sigma_n]$

Démonstration : Par récurrence sur le degré donné par l'ordre lexicographique $X_1 > ... > X_n$. **Q.e.d.**

Remarque : c'est vrai si on remplace K par $\mathbb{Z}$!

Exercice : Si K est de caractéristique $\neq 2$, alors $K[X_1, ..., X_n]^{A_n} = K[\sigma_1, ..., \sigma_n] + \delta K[\sigma_1, ..., \sigma_n]$ où $\delta := \prod_{1 \leq i < j \leq n}(X_i - X_j)$ (*indication : soit P tel que $\forall\, \sigma$, $P^\sigma = \epsilon(\sigma)P$, alors P est divisible par δ (en effet, le monôme dominant de P est de la forme X^α avec $\alpha_1 > .... > \alpha_n$ qui est divisible par $X_1^{n-1}....X_{n-1}$, monôme dominant de δ)*).

Proposition 0.3 (relations coefficients-racines) *Soit $P(X) := X^n + a_1X^{n-1} + ... + a_n \in K[X]$. On suppose que P a n racines $x_1, ..., x_n$ dans une extension de K* i.e. *:*

$$P = (X - x_1)...(X - x_n) \ .$$

Alors $a_k = (-1)^k\sigma_k(x_1, ..., x_n)$.

0.3 Équations de degré 2

$$f(x) = x^2 + px + q = (x - x_1)(x - x_2)$$

$$\Rightarrow x_1 + x_2 = -p, x_1 x_2 = q, x_1 - x_2 = \pm\sqrt{\Delta}$$

où $\Delta = (x_1 - x_2)^2 = p^2 - 4q$.

Donc :

$$x_1, x_2 = \frac{-p \pm \sqrt{\Delta}}{2} \ .$$

Exercice : Vérifier que $2\cos(2\pi/5) = \frac{1+\sqrt{5}}{2}$ et $2\sin(2\pi/5) = \sqrt{\frac{5-\sqrt{5}}{2}}$.

0.4 Degré 3

$$f(x) = x^3 + px + q = (x - x_1)(x - x_2)(x - x_3)$$

$$\Rightarrow \delta^2 = ((x_1 - x_2)(x_2 - x_3)(x_1 - x_3))^2 = -4p^3 - 27q^2 \ .$$

c'est le *discriminant de* $x^3 + px + q$. Soient $a := x_1 + jx_2 + j^2x_3$, $b := x_1 + j^2x_2 + jx_3$.

Alors :

$$x_1 = \frac{a+b}{3},\ x_2 = \frac{j^2a + jb}{3},\ x_3 = \frac{ja + j^2b}{3},$$

et : $a^3 = -\frac{27q}{2} + \frac{\sqrt{-27}\delta}{2}$, $b^3 = -\frac{27q}{2} - \frac{\sqrt{-27}\delta}{2}$ et $ab = -3p$.

Réciproquement, si on choisit une racine carrée : $\sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$ et une racine cubique : $\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$, on peut choisir une racine cubique $\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$ telle que :

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}\ \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} = -3p \ .$$

Si on pose :

$$x_1, x_2, x_3 = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}},$$

$$j^2\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + j\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}},$$

$$j\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+j^2\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}},$$

on a : $(X-x_1)(X-x_2)(X-x_3)=X^3+pX+q$.

Exemples :

i) l'unique racine réelle de x^3-x-1 est :

$$\sqrt[3]{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{23}{27}}}+\sqrt[3]{\frac{1}{2}-\frac{1}{2}\sqrt{\frac{23}{27}}}\ .$$

ii) x^3-3x+1 a 3 racines réelles mais aucune n'est *résoluble par radicaux réels* : c'est le *casus irreducibilis*. Une des racines est :

$$2\cos\left(\frac{2\pi}{9}\right)=\sqrt[3]{j}+\sqrt[3]{j^2}\ .$$

où on pose $\sqrt[3]{re^{it}}:=r^{\frac{1}{3}}e^{\frac{it}{3}}$ *si* $r>0$ *et* $-\pi<t<\pi$.

Exercice : Montrer que $2\cos(2\pi/7)=-\frac{1}{3}+\frac{1}{3}\left(\sqrt[3]{\frac{7+21i\sqrt{3}}{2}}+\sqrt[3]{\frac{7-21i\sqrt{3}}{2}}\right)$ *(indication :* $1+2\cos(2\pi/7)+2\cos(4\pi/7)+2\cos(6\pi/7)=0$ *et* $(2\cos 3t)=(2\cos t)^3-3(2\cos t)$*).*

Exercice : Si $P=X^3+a_1X^2+a_2X+a_3$, alors $\Delta=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3$.

0.5 Degré 4

Il y a aussi des formules avec des radicaux mais la place me manque ...

0.6 Degré ≥ 5

$x^5-2=(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)$ où $x_k=\sqrt[5]{2}(\cos(2k\pi/5)+i\sin(2k\pi/5))$ donc x^5-2 est résoluble par radicaux.

En revanche nous verrons plus tard que x^5-x-1 n'est pas résoluble par radicaux.

1 Extensions, algébricité

1.1 Polynômes irréductibles

Proposition 1.1 *Soit K un corps. soit $P\in K[X]$. Alors P est irréductible $\Leftrightarrow$ $K[X]/(P)$ est un corps.*

Remarque : $K[X]/(P)$ est un $K-$espace vectoriel de dimension $d=\deg P$.

1.2 Extensions, degré

Soient $K \leq L$ deux corps. On dit que L est une *extension de* K.

Dans ce cas L est aussi un $K-$espace vectoriel. On note $[L : K] := \dim_K L$: c'est le *degré de* L *sur* K.

Proposition 1.2 (multiplicativité des degrés) *Soient* $K_1 \leq ... \leq K_n$ *des corps. Alors* $[K_n : K_1] = [K_n : K_{n-1}]...[K_2 : K_1]$.

Exemple : $[\mathbb{Q}(\sqrt[3]{2}, j) : \mathbb{Q}] = 6$.

1.3 Éléments algébriques

Proposition 1.3 *Soit* $K \leq E$ *une extension de corps. Soit* $x \in E$. *Sont équivalentes :*

(i) *il existe* $0 \neq P \in K[X]$ *tel que* $P(x) = 0$ *;*

(ii) $\dim_K K[x]$ *est finie ;*

(iii) $K[x] = K(x)$.

On dit que x est *algébrique sur* K s'il existe un polynôme $P \in K[X]$ non nul tel que $P(x) = 0$.

Dans ce cas, $K[x] = K(x)$, $K[x]$ est un $K-$espace vectoriel de dimension finie.

De plus, l'idéal $\{P \in K[X] \ : \ P(x) = 0\}$ est un idéal premier non nul engendré par un unique polynôme unitaire P_x : le *polynôme minimal* de x sur K.

Remarque, P_x est irréductible sur K et si P est un polynôme irréductible sur K qui annule x, $P = cP_x$ pour un $c \in K^\times$.

On a : $[K[x] : K] = \deg P_x$: c'est le *degré de* x *sur* K.

Proposition 1.4 *L'ensemble* $\{x \in E : x$ *est algébrique sur* $K\}$ *est un sous-corps de* E.

Proposition 1.5 *Si* $K \leq E$ *est une extension finie (*i.e. $[E : K]$ *est fini), alors* E *est algébrique sur* K i.e. *tous les éléments de* E *sont algébriques sur* K.

Remarque : $\overline{\mathbb{Q}}$ est une extension algébrique infinie de $\mathbb{Q}$.

1.4 Corps de rupture

Soit $P \in K[X]$ un polynôme irréductible. Dans le corps $K[X]/(P)$, l'élément $\overline{X} := X \bmod P$ est une racine de P car $P(\overline{X}) = P(X) = 0 \bmod P$.

Théorème 1.6 *Soit L une extension de K et $\alpha \in L$ une racine de P telle que $K[\alpha] = L$. Alors $K[X]/(P) \to k[\alpha]$, $Q(X) \bmod P \mapsto Q(\alpha)$ est un isomorphisme de corps.*

Une extension L de K comme dans le théorème est un *corps de rupture de P sur K.*

En particulier $1, \alpha, ..., \alpha^{\deg P - 1}$ est une $K-$base de α.

Exemple : $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q}(j^2\sqrt[3]{2})$ sont des corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.

Réalisation du corps de rupture

Si $P(X) = X^n + a_1 X^{n-1} + ... + a_n \in K[X]$ est irréductible, alors $K[X]/(P) \simeq K[A]$ où A est la matrice :

$$\begin{pmatrix} 0 & \cdots & 0 & -a_n \\ 1 & \ddots & \vdots & \vdots \\ 0 & \ddots & 0 & \vdots \\ \vdots & \ddots & & \vdots \\ 0 & \cdots & 0 & -a_1 \end{pmatrix} \in \mathscr{M}_n(\mathbb{K})$$

Par exemple : $\mathbb{C} \simeq \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ et $\mathbb{F}_{25} \simeq \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_5 \right\}$

1.5 Corps de décomposition

Soit $P \in K[X]$. On suppose que $E \geq K$ est un corps où P est scindé : $P = c(X - x_1)...(X - x_n)$. On dit que $K(x_1, ..., x_n)$ est le *corps de décomposition* de P dans E.

Proposition 1.7 *Un cops de décomposition existe toujours.*

Démonstration : PAr récurrence sur $\deg P$ en utilisant l'existence de corps de rupture. **Q.e.d.**

Nous allons voir qu'il y a unicité à isomorphisme près.

Théorème 1.8 (prolongement d'isomorphisme) *Soit $\sigma : K \to K'$ un isomorphisme de corps. Soit $P \in K[X]$ un polynôme irréductible. Alors $P^\sigma \in K'[X]$ est irréductible. Si α, α' sont des racines de P et P^σ dans des extensions de K, K', alors σ se prolonge en un isomorphisme $K(\alpha) \simeq K'(\alpha')$ qui envoie α sur α'.*

Théorème 1.9 (unicité du corps de décomposition) *Soit $\sigma : K \to K'$ un isomorphisme de corps. Soit $P \in K[X]$. Soit $E \geq K$ un corps où P est scindé :$P = c(X - x_1)...(X - x_n)$. Soit $E' \geq K'$ un corps où P^σ est scindé : $P^\sigma = c'(X - x'_1)....(X - x'_n)$. Soient $B := K(x_1, ..., x_n), B' := K'(x'_1, ..., x'_n)$. Alors σ se prolonge en un isomorphisme $B \simeq B'$.*

Corollaire 1.9.1 *Soient L, L' deux corps de décomposition de P sur K. Alors il existe un $K-$isomorphisme $L \simeq L'$.*

Exemples : $\mathbb{F}_{q^n}$ est un corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}_q$ et on a donc l'unicité à isomorphisme près des corps finis de cardinaux donnés.

Cours du mercredi 29 janvier 2014

2 Caractères et morphismes de corps

Si G est un groupe et K un corps, un carctère de G dans K est un morphisme de groupes $G \to K^\times$. L'ensemble des caractères est une partie du $K-$espace vectoriel des fonctions $G \to K$.

Exemple : $G = \mathbb{Z}/n\mathbb{Z}$, $K = \mathbb{C}$, les caractères de G dans $\mathbb{C}$ sont les $k \mapsto \zeta^k$ où $\zeta = \exp(2i\pi/n)$.

2.1 Indépendance

Théorème 2.1 (d'indépendance des caractères d'Artin) *Soient $\sigma_1, ..., \sigma_n$ n caractères distincts de G dans K. Alors les σ_i sont $K-$linéairement indépendants.*

Corollaire 2.1.1 *Soient E, E' deux corps. Si $\sigma_1, ..., \sigma_n$ sont n morphismes distincts de corps $E \to E'$. Alors les σ_i sont $E'-$linéairement indépendants.*

Exercice : si G abélien, on pose $G^\vee$ le groupe des caractères de G dans $\mathbb{C}$. Montrer que $G^\vee \simeq G$ *(non canonique).*

Exercice : si G fini, $|\mathrm{Hom}(G, K^\times)| \leq |G|$.

2.2 Corps des invariants

Théorème 2.2 *Soient $\sigma_1, ..., \sigma_n$ n morphismes distincts $E \to E'$. Alors si $F := E^{\{\sigma_1,...,\sigma_n\}}$, $[E : F] \geq n$.*

Démonstration : Si $e_1, ..., e_m$ est une famille génératrice de E comme $F-$espace vectoriel, alors les lignes de la matrice $(\sigma_i(e_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \in \mathscr{M}_{n,m}(E')$ sont indépendantes. Donc $n \leq m$. **Q.e.d.**

Corollaire 2.2.1 *Si G est un sous-groupe fini de* $\mathrm{Aut}(E)$*, alors* $[E : E^G] \geq |G|$.

Exemple : $E = \mathbb{C}, G = \{1, \sigma\}$ où σ est la conjugaison complexe, $[\mathbb{C} : \mathbb{R}] = 2$.

3 Correspondance de Galois

3.1 Extensions galoisiennes

Soit E un corps. Soit $G \leq \mathrm{Aut}(E)$ fini. On dit que E/E^G est *une extension galoisienne* de groupe de Galois G.

Notation : si $F = E^G$, $G =: \mathrm{Gal}(E/F)$.

Exemples : $\mathbb{C}/\mathbb{R}$, $\mathbb{F}_{q^n}/\mathbb{F}_q$, $\mathbb{Q}(\zeta)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, *contre-exemple :* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Exemple : $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$.

Théorème 3.1 *Soit E un corps. Soit $G \leq \mathrm{Aut}(E)$ un groupe fini. Alors* $[E : E^G] = |G|$.

Démonstration : On utilise la forme $F-$linéaire $\mathrm{Tr} : E \to F$, $x \mapsto \sigma_1(x) + ... + \sigma_n(x)$ où $F = E^G$, $G = \{\sigma_1, ..., \sigma_n\}$. Soient $g_1, ..., g_n$ les éléments de G. Si $e_1, ..., e_{n+1}$ sont des éléments de E, alors les colonnes de la matrices $(g_i(e_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n+1}} \in \mathscr{M}_{n,n+1}$ sont liées. Donc $\forall\, i$, $\sum_j x_j g_i(e_j) = 0$ pour certains $x_j \in E$. D'où :

$$\forall\, i, \sum_j g_i^{-1}(x_j) e_j = 0$$

et $\sum_i \sum_j g_i^{-1}(x_j) e_j = 0 \Rightarrow \sum_j \mathrm{Tr}(x_j) e_j = 0$. C'est encore vrai si on remplace x_j par $x x_j$, $x \in E$. Donc on peut choisir les x_j tels que $x_1 \in E$ et $\mathrm{Tr}(x_1) \neq 0$ par exemple. Mais alors, les e_j sont liés sur E^G. **Q.e.d.**

Corollaire 3.1.1 (Maximalité du groupe de Galois) *Soit E/F galoisienne de groupe G. Alors si $\sigma : E \to E'$ est un $F-$morphisme de corps, $\sigma \in G$. En particulier,* $G = \mathrm{Aut}_F(E)$.

Corollaire 3.1.2 (Injectivité) *Si E/F est galoisienne de groupe G si $H_1, H_2 \leq G$, alors* $E^{H_1} = E^{H_2} \Leftrightarrow H_1 = H_2$.

Exemples :

a) $k(x_1, ..., x_n)^{\mathfrak{S}_n} = k(s_1, ..., s_n)$,

b) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est galoisienne de groupe de Galois $G := \langle s, t \rangle \simeq \mathfrak{S}_3$ où s est le $\mathbb{Q}(j)-$automorphisme qui envoie $\sqrt[3]{2}$ sur $j\sqrt[3]{2}$ et t le $\mathbb{Q}(\sqrt[3]{2})-$automorphisme qui envoie j sur j^2 ;

c) soit G le sous-groupe des automorphismes de $\mathbb{C}(t)$ engendré par les changements de variables $t \mapsto t^{-1}$ et $t \mapsto 1-t$. Montrer que G laisse stable l'ensemble des 3 fonctions :

$$f_1 := t + t^{-1},\ f_2 := 1 - t + (1-t)^{-1},\ f_3 := 1 - t^{-1} + (1-t^{-1})^{-1}\ .$$

En déduire que G est isomorphe au groupe S_3.

Soit K le sous-corps des fractions rationnelles $f \in \mathbb{C}(t)$ invariantes par les changements de variables

$$t \mapsto 1-t \text{ et } t \mapsto t^{-1}\ .$$

Montrer que $K = \mathbb{C}\left(\frac{(t^2-t+1)^3}{t^2(t-1)^2}\right)$.

En déduire que l'extension :

$$\mathbb{C}\left(\frac{(t^2-t+1)^3}{t^2(t-1)^2}\right) \subset \mathbb{C}(t)$$

est galoisienne de groupe de Galois S_3.

Exercice : on pose $y_1 := x_1 + jx_2 + j^2x_3$, $y_2 := x_1 + j^2x_2 + jx_3$. Montrer que $\mathbb{C}(x_1,x_2,x_3)^{A_3} = \mathbb{C}(y_1^2/y_2, y_2^2/y_1, \sigma_1)$.

Proposition 3.2 *On pose $L := k(s_1,...,s_n)$ et $L_i := L(x_{i+1},...,x_n)$, $0 \leq i \leq n$ ($L_n = L$).*

a) $[L_{i-1} : L_i] = i$ *et* $1, ..., x_i^{i-1}$ *est une base de* L_{i-1}/L_i.

b) $\{x_1^{a_1}...x_n^{a_n}\ :\ \forall\, i,\ a_i \leq i-1\}$ *est une base de* $k(x_1,....,x_n)/L$.

c) tout $g \in k[x_1,...,x_n]$ *est une combinaison* $k[s_1,...,s_n]-$*linéaire de monômes* $x_1^{a_1}...x_n^{a_n}\ :\ \forall\, i,\ a_i \leq i-1$.

d) On retrouve que $k[x_1,...,x_n]^{\mathfrak{S}_n} = k[s_1,...,s_n]$.

3.2 Surjectivité

Théorème 3.3 *Soit E/F une extension galoisienne de groupe de Galois G. Si $F \leq B \leq E$, alors il existe $H \leq G$ tel que $E^H = B$.*

Démonstration : Soit $H := \mathrm{Aut}_B(E)$. On a : $B \leq E^H$. Soit $s_1,...,s_r$ un système de représentants de G/H. On a $B^{\{s_1,...,s_r\}} = F$ donc $[B:F] \geq r$ et $[E:B] \leq [E:F]/r = |H| = [E:E^H]$ d'où $B = E^H$. **Q.e.d.**

Exercice : donner la liste des sous-corps de $\mathbb{Q}(\sqrt[3]{2}, j)$.
(*réponse :* $\mathbb{Q}(\sqrt[3]{2},j) \geq \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q}(j^2\sqrt[3]{2}), \mathbb{Q}(j) \geq \mathbb{Q}$).

Cours du mercredi 5 février 2014

3.3 Théorème fondamental

Théorème 3.4 *Soit E/F une extension galoisienne de groupe G.*

i) On a 2 bijections réciproques :

$$\{H \leq G\} \overset{1:1}{\longleftrightarrow} \{F \leq B \leq E\}$$

$$H \mapsto E^H$$

$$\mathrm{Gal}(E/B) \leftarrow B \ .$$

ii) L'extension E/B est galoisienne et $[E:B] = |\mathrm{Gal}(E/B)|$;

iii) $[B:F] = |G/\mathrm{Gal}(E/B)|$;

iv) l'extension B/F est galoisienne si et seulement si $\mathrm{Gal}(E/B) \triangleleft G$. Dans ce cas, $\mathrm{Gal}(B/F) \simeq G/\mathrm{Gal}(E/B)$.

Proposition 3.5 *Soit E/K une extension galoisienne. On suppose que $K \leq B \leq B' \leq E$. On note $U := \mathrm{Gal}(E/B)$, $U' := \mathrm{Gal}E/B'$. Alors B'/B est galoisienne $\Leftrightarrow U' \triangleleft U$. Et dans ce cas, $\mathrm{Gal}(B'/B) \simeq U/U'$.*

3.4 Caractérisation des extensions galoisiennes

Théorème 3.6 *Soit E/K une extension finie. On a toujours : $|\mathrm{Aut}(E/K)| \leq [E:K]$. L'extension E/K est galoisienne $\Leftrightarrow |\mathrm{Aut}(E/K)| = [E:K]$. Dans ce cas, $\mathrm{Gal}(E/K) = \mathrm{Aut}(E/K)$.*

Exemple : si $E = \mathbb{Q}(\sqrt[4]{2})$, alors $|\mathrm{Aut}(E/\mathbb{Q})| = 2 < 4 = [E:\mathbb{Q}]$.

3.5 Séparabilité

Soit $P \in K[X]$. Alors : P est premier avec P' si et seulement s'il n'existe pas d'extension où P a une racine multiple (*i.e.* d'ordre > 1).

Si E/K est une extension. On dit que $\alpha \in E$ est *algébrique séparable* si $P(\alpha) = 0$ pour un polynôme séparable $P \in K[X] \Leftrightarrow$ le polynôme minimal de α est séparable.

Une extension est *séparable* si tous ses éléments le sont.

Proposition 3.7 *Si $P \in K[X]$ est irréductible, alors P est séparable si $P' \neq 0$. En particulier, en caractéristique nulle ou sur un corps fini, tout polynôme irréductible est séparable.*

Contre-exemple : $X^p - t$ est irréductible non séparable sur $\mathbb{F}_p(t)$.

Théorème 3.8 *Soit E/F une extension galoisienne de groupe G. Soit $x \in E$. Soient $x_1, ..., x_r$, $r \leq n$ les images distinctes de x par les $\sigma \in G$. Le polynôme $(X - x_1)....(X - x_r)$ est le polynôme minimal de x sur F. En particulier, E/F est séparable.*

Théorème 3.9 *Une extension finie E/K est galoisienne $\Leftrightarrow$ E est le corps de décomposition sur K d'un polynôme $P \in K[X]$ séparable. Dans ce cas, on dit que* $\mathrm{Gal}(E/K)$ *est le groupe de Galois de P sur K. De plus* $\mathrm{Gal}_K(P)$ *s'identifie à un sous-groupe de $\mathfrak{S}_r$ où $r = \deg P$.*

3.6 Normalité

On dit qu'une extension E/F est *normale* si pour toute extension Ω de F, et pour tous $F-$morphismes $\sigma, \tau : E \to \Omega$, $\sigma(E) = \tau(E)$.

Exercice : Cela revient à dire que $\sigma(E) = E$ si ci-dessus $\Omega \geq E$.

Proposition 3.10 *Si E/F est un corps de décomposition, E/F est normale.*

Exemple : $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$, *contre-exemple :* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

Théorème 3.11 *Soit E/F une extension finie. Alors l'extension E/F est galoisienne si et seulement si elle est normale et séparable.*