Théorie de Galois

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

Villeurbanne, le 26 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.*

Cours du mercredi 12 février 2014

Exercice : vérifier que $\mathrm{Gal}_K(P)$ agit transitivement sur les racines si et seulement si P est irréductible sur K.

Remarques :

i) Si M/L et L/K sont normales, M/K ne l'est pas forcément. Par exemple : $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = \mathbb{Q}(\sqrt[4]{2})$.

ii) Si M/L et L/K sont séparables, alors M/K est aussi séparable.

3.7 Composée de corps

section non faite en cours

Soit L/K une extension. Soient $K \leq E, E' \leq L$. On note EE' le sous-corps de L engendré par E et E'.

Proposition 3.12 *Soient L/K une extension galoisienne de groupe G, $K \leq E, E' \leq L$, $H := \mathrm{Gal}(L/E)$, $H' := \mathrm{Gal}(L/E')$. On a :*

i) $\mathrm{Gal}(L/EE') = H \cap H'$, $\mathrm{Gal}(L/E \cap E') = \langle H, H' \rangle$.

ii) Si E'/K est galoisienne, alors EE'/E aussi et $\mathrm{Gal}(EE'/E) \simeq \mathrm{Gal}(E/E \cap E')$, $s \mapsto s|_E$.

iii) Si E/K et E'/K sont galoisiennes, alors EE'/K aussi et $\mathrm{Gal}(EE'/K)$ *est isomorphe à un sous-groupe de* $\mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K)$ *via* $s \mapsto (s|_E, s|_{E'})$. *Si de plus,* $E \cap E' = K$, $\mathrm{Gal}(EE'/K) \simeq \mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K)$.

Exercice : Soient $L := k(X_1, X_2, X_3, X_4)$, $K := L^{\mathfrak{S}_4} = k(s_1, s_2, s_3, s_4)$, $E := k(x_4) = L^{\mathfrak{S}_3}$, $E' := L^{K_4}$ où $K_4 = \{1, (12)(34), (13)(24), (14)(23)\}$.

On a $H = \mathfrak{S}_3$, $H' = K_4$, $[E : K] = |\mathfrak{S}_4/\mathfrak{S}_3| = 4$, $[E' : K] = |\mathfrak{S}_4/K_4| = 6$, $EE' = L = L^{H\cap H'}$, $E \cap E' = L^{\langle H,H'} = K$. Comme H n'est pas distingué dans $\mathfrak{S}_4$, E/K n'est pas galoisienne. En revanche E'/K est galoisienne de groupe de Galois $\simeq \mathfrak{S}_4/K_4 \simeq \mathfrak{S}_3$. Vérifier que $E' = K(\beta)$ où $\beta = \sum_{\sigma\in K_4} \sigma\alpha$ où $\alpha := x_1x_2^2x_3^3x_4^4$.

4 Corps finis

4.1 Sous-groupes finis de $K^\times$

Soit G un groupe fini. On note $\omega(G)$ l'*exposant de G* : c'est le ppcm des ordres des éléments de G.

Exemple : $\omega(\mathfrak{S}_3) = 6$

Lemme 4.1 *Soient $a, b \in G$ tels que $ab = ba$. Si a, b sont d'ordres finis m, n premiers antre eux, alors ab est d'ordre mn.*

Corollaire 4.1.1 *Dans un groupe abélien fini, l'ensemble des ordres des éléments est stable par ppcm.*

Proposition 4.2 *Soit G un sous-groupe fini de $K^\times$, alors G est cyclique.*

Exemple : les $\mathbb{F}_q^\times$ sont cycliques ; les sous-groupes finis de $\mathbb{C}^\times$ sont cycliques : ce sont les $\boldsymbol{\mu_n}$.

Contre-exemple : $\mathbb{Q}_8 := \{\pm 1, \pm i, \pm j, \pm k\} \leq \mathbb{H}^\times$ n'est pas cyclique.

Exercice : déterminer les sous-groupes *d'indice fini* de $\mathbb{C}^\times$, de $\mathbb{R}^\times$.

4.2 Structure

Un anneau A est de caractéristique n si $n\mathbb{Z} = \ker(\mathbb{Z} \to A,\ n \mapsto n1_A)$. Si A est intègre, la caractéristique est un nombre premier.

Proposition 4.3 *Si A est un anneau de caractéristique p, un nombre premier, alors $\mathrm{Fr}_q : A \to A,\ x \mapsto x^q$ est un morphisme d'anneaux si q est une puissance de p.*

Soit K un corps fini. Sa caractéristique est un nombre premier p et son cardinal q une puissance de p. De plus si $q = p^n$, alors $(K, +) \simeq (\mathbb{Z}/p)^n$ et $(K^\times, \times) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.

Théorème 4.4 *Soit p un nombre premier. Si $n \geq 1$, il existe, à isomorphisme près, un unique corps de cardinal $q = p^n$ c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.*

Théorème 4.5 *Soit q une puissance d'un nombre premier p. Si $\mathbb{F}_q \leq K \leq \mathbb{F}_{q^n}$, alors K est de cardinal q^m où $m|n$. Réciproquement, si $m|n$, il existe un unique sous-corps K de $\mathbb{F}_q$ de cardinal q^m : c'est l'ensemble des racines de $X^{q^m} - X$ dans $\mathbb{F}_q$.*

Théorème 4.6 *Soit K un corps fini. Pour tout n, il existe une extension L/K de degré n. Cette extension est galoisienne, cyclique et unique à isomorphisme près.*

Démonstration : $K \simeq \mathbb{F}_q$ et $L \simeq \mathbb{F}_{q^n}$. **Q.e.d.**

Remarque : si k est un corps, alors il existe une extension algébrique $\overline{k}$ de k telle que $\overline{k}$ est algébriquement clos. Ce corps $\overline{k}$ est unique à $k-$isomorphisme près. On dit que c'est une clôture algébrique de k. Pour $\mathbb{F}_p$, on a : $\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p} \ : \ x^{p^n} = x\}$ et $\overline{\mathbb{F}_p} = \cup_n \mathbb{F}_{p^n}$.

Dans la suite, on fixe pour tout p une clôture algébrique de $\mathbb{F}_p$: notée $\overline{\mathbb{F}_p}$ et $\mathbb{F}_{p^n} := \{x \in \overline{\mathbb{F}_p} \ : \ x^{p^n} = x\}$.

4.3 Polynômes sur les corps finis

4.3.1 Nombre de polynômes irréductibles de degré donné

Théorème 4.7 *Soient p un nombre premier et q une puissance de p. Pour tout $n \geq 1$, il existe $\theta \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q[\theta]$ et il existe un polynôme irréductible de degré n sur $\mathbb{F}_q$.*

Lemme 4.8 *Soit $P \in \mathbb{F}_q[X]$ irréductible de degré m. Alors P divise $X^{q^n} - X$ sur $\mathbb{F}_q$ si et seulement si $m|n$.*

Démonstration : Si $m|n$, alors $q^m - 1 | q^n - 1$ donc $X^{q^m-1} - 1 | X^{q^n-1} - 1$ et $X^{q^m} - X | X^{q^n} - X$. **Q.e.d.**

Corollaire 4.8.1 *On a :*

i)

$$X^{q^n} - X = \prod_{d|n} \prod_{P} P(X)$$

où P décrit les polynômes irréductibles unitaires sur $\mathbb{F}_q$ de degré d.

ii) $q^n = \sum_{d|n} d\nu_d(q)$ *; où $\nu_n(q)$ est le nombre de polynômes irréductibles sur $\mathbb{F}_q$ unitaires de degré n.*

iii) $\nu_n(q) = \dfrac{\sum_{d|n} \mu(n/d) q^d}{n}$ *où μ est la fonction de Möbius.*

Rappel : si $\zeta(s) := \sum_{n\geq 1} n^{-s}$ pour $s > 1$, alors $\zeta(s)^{-1} = \sum_{n\geq 1} \mu(n) n^{-s}$ (on peut prendre cette formule comme définition de μ). Plus concrètement, on a :

$$\mu(p_1^{a_1}...p_r^{a_r}) = \begin{cases} 0 & \text{si l'un des } a_i \geq 2, \\ (-1)^r & \text{sinon.} \end{cases}$$

Exemple : dans $\mathbb{F}_3$, on a :

$$X^9 - X = X(X+1)(X+2)(X^2+X+2)(X^2+2X+2)(X^2+1)$$

et $\nu_2(3) = \frac{3^2-3}{2} = 3$.

Exercice : Donner un sens au produit infini $\prod_P (1 - t^{\deg P})^{-1}$ où P décrit l'ensemble des polynômes irréductibles unitaires sur $\mathbb{F}_q$ et montrer que :

$$\prod_P (1 - t^{\deg P})^{-1} = (1 - qT)^{-1} \ .$$

Cours du mercredi 19 février 2014

4.3.2 Ordre d'un polynôme, polynôme primitif

Théorème 4.9 *Soit $P \in \mathbb{F}_q[X]$ irréductible de degré m. Alors P est scindé à racines simples sur $\mathbb{F}_{q^m}$. Si a est l'une d'elles, les autres sont $a, ..., a^{q^{m-1}}$. En particulier, si $P \neq X$, toutes les racines de P ont le même ordre multiplicatif dans $\mathbb{F}_{q^m}^\times$.*

Démonstration : Soit a une racine de P. Le corps $\mathbb{F}_q[a]$ est une extension galoisienne de $\mathbb{F}_q$ de groupe engendré par $x \mapsto x^q$. Le groupe de Galois agit transitivement sur les racines de P. **Q.e.d.**

Soit $P \in \mathbb{F}_q[X]$ un polynôme premier à X. L'*ordre de* P est le plus petit entier $e > 0$ tel que $P | X^e - 1$. Si $P = X^h Q$ avec $h \geq 1$ et Q premier à X, on pose $\mathrm{ord}P := \mathrm{ord}Q$.

Remarque : dans le premier cas, e est l'ordre de X dans $(\mathbb{F}_q[X]/(P))^\times$ c'est aussi l'ordre commun des racines de P dans $\overline{\mathbb{F}_p}^\times$.

Proposition 4.10 *Si P est irréductible sur $\mathbb{F}_q$ de degré m, l'ordre e de P divise $q^m - 1$. De plus, si $e > 1$, m est l'ordre de q dans $(\mathbb{Z}/e\mathbb{Z})^\times$.*

Démonstration : Soit a une racine de P dans une extension de $\mathbb{F}_q$. Alors $\mathbb{F}_q[a] = \mathbb{F}_{q^m}$. Donc l'ordre de a, qui est e, divise $q^m - 1$. Si $q^n = 1 \bmod e$, alors $a^{q^n - 1} = 1$ donc $a^{q^n} = a$. Donc $a \in \mathbb{F}_{q^n}$. D'où, $\mathbb{F}_q[a] \leq \mathbb{F}_{q^n}$. Par conséquent, $m = [\mathbb{F}_q[a] : \mathbb{F}_q] | n = [\mathbb{F}_{q^n} : \mathbb{F}_q]$. Donc m est bien le plus petit entier tel que $q^m = 1 \bmod e$. **Q.e.d.**

Théorème 4.11 *Soient $e, m > 1$. Le nombre de polynômes irréductibles sur $\mathbb{F}_q$ et unitaires de degré m, d'ordre e est :*

$$N_{q,m,e} = \varphi(e)/m \text{ si } m \text{ est l'ordre de } q \text{ dans } (\mathbb{Z}/e\mathbb{Z})^\times, 0 \text{ sinon.}$$

Démonstration : Soit $\Phi_e := \prod_{\substack{x \in \mathbb{F}_{q^m} \\ x \text{ d'ordre } e}} X - x \in \mathbb{F}_q[X]$. Si P irréductible divise Φ_e, alors P est d'ordre e donc $\deg P = m$ l'ordre de q dans $(\mathbb{Z}/e\mathbb{Z})^\times$. Donc $mN_{q,m,e} = \varphi(e) =$ le nombre d'éléments d'ordre e dans le groupe cyclique $\mathbb{F}_{q^m}^\times$. **Q.e.d.**

Exemple : $2^{11} - 1 = 23.89$. On a :

$$X^{23}-1 = (X+1)(1+X^2+X^4+X^5+X^6++X^{10}+X^{11})(1+X+X^5+X^6+X^7+X^9+X^{11})$$

dans $\mathbb{F}_2[X]$. Il existe $a \in \mathbb{F}_{2^{11}}^\times$ d'ordre 23 tel que :

$$1 + X^2 + X^4 + X^5 + X^6 + X^{10} + X^{11} = \prod_{i \in \{1,2,3,4,6,8,9,12,13,16,18\}} (X - a^i) ;$$

$$1 + X + X^5 + X^6 + X^7 + X^9 + X^{11} = \prod_{i \in \{5,7,10,11,14,15,17,19,20,21,22\}} (X - a^i) .$$

Pour $e = 23$, $q = 2$, 2 est d'ordre 11 $\bmod 23$; les polynômes d'ordre 23 sur $\mathbb{F}_2$ sont de degrés 11, il y en a $\varphi(23)/11 = 2$.

Exemple : si $q = 2, m = 4$, alors $N_{2,4,e} = 1$ si $e = 5$, 2 si $e = 15$.

On a : $\Phi_5 = 1+X+X^2+X^3+X^4$ *irréductible* et $\Phi_{15} = (1+X+X^4)(1+X^3+X^4)$.

On dit qu'un polynôme $P \in \mathbb{F}_q[X]$ de degré m est *primitif* s'il est le polynôme minimal d'un générateur de $\mathbb{F}_{q^m}^\times$.

Théorème 4.12 *Un polynôme de degré m est primitif si et seulement s'il est unitaire, premier à X et d'ordre $q^m - 1$.*

Exemple : les polynômes primitifs unitaires de degré 4 sur $\mathbb{F}_2$ sont : $1 + X + X^4$ et $1 + X^3 + X^4$.

4.4 Algorithme de Berlekamp

Théorème 4.13 *Soit $P \in \mathbb{F}_q[X]$ un polynôme de degré d sur $\mathbb{F}_q$. On suppose que P est séparable. Alors P est irréductible sur $\mathbb{F}_q$ si et seulemnt si l'endomorphisme* $\mathrm{Fr}_q - \mathrm{Id}$ *du $\mathbb{F}_q-$espace vectoriel $\mathbb{F}_q[X]/(P)$ est de rang $d-1$.*

Remarque : le rang est toujours $\leq d - 1$.

Démonstration : Si le rang est $< d - 1$, il existe un polynôme $Q = a_1X + ... + a_{d-1}X^{d-1}$ non nul dans le noyau. Alors, le pgcd de P et $Q - a$ est non constant pour un certain $a \in \mathbb{F}_q$ car $P|Q^q - Q = \prod_{a\in\mathbb{F}_q}(Q - a)$.

Réciproquement, si P n'est pas irréductible, $P = P_1...P_r$ pour des polynômes irréductibles deux à deux premiers entre eux P_i et un $r > 1$. Mais alors :

$$\mathbb{F}_q[X]/(P) \simeq \oplus_i \mathbb{F}_q[X]/(P_i)$$

Les sous-espaces $E_i := \mathbb{F}_q[X]/(P_i)$ sont stables par $\mathrm{Fr}_q - \mathrm{Id}$ donc le rang est :

$$\sum_i \mathrm{rang}(\mathrm{Fr}_q - \mathrm{Id}|_{E_i}) = \sum_i \deg P_i - 1 = d - r < d - 1 \ .$$

Q.e.d.

Exemple : $q = 2$, $P = X^5 + X^4 + 1$, Dans la base $1, X, X^2, X^3, X^4 \bmod P$, la matrice de $\mathrm{Fr}_2 - \mathrm{Id}$ est :

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Le rang est $3 < 5$. Donc P est réductible. Dans le noyau, on trouve : $Q := X^2 + X^3 + X^4$. Donc $P = \mathrm{pgcd}(P, Q)\mathrm{pgcd}(P, Q + 1) = (1 + X + X^2)(1 + X + X^3)$.

5 Clôture algébrique

Soit K un corps. Une *clôture algébrique de K* est une extension akgébrique de corps $\overline{K}/K$ telle que $\overline{K}$ est algébriquement clos.

Théorème 5.1 *Soit K un corps. Il existe une clôture algébrique de K. De plus si K_1, K_2 sont deux clôtures algébriques de K, alors il existe un $K-$isomorphisme $K_1 \simeq K_2$.*

Démonstration : *Existence :* Soit I l'ensemble des polynômes unitaires de $K[X]$ de degré ≥ 1. Pour tout $f \in I$, on introduit des variables $T_{f,i}$, $1 \leq i \leq \deg f$.

On pose $A := K[T_{f,i} \ : \ f \in I, 1 \leq i \leq \deg f]$ c'est un anneau de polynômes en une infinité de variables.

Soit J l'idéal de A engendré par les coefficients des polynômes :

$$f(X) - \prod_{i=1}^{\deg f} (X - T_{f,i})$$

lorsque f décrit I.

On a $J \underset{\neq}{\subset} A$. En effet, sinon, il existe $f_1, ..., f_N \in I$ et certains coefficients $c_1, ..., c_N$ respectivement des polynômes :

$$f_j(X) - \prod_{i=1}^{\deg f_j} (X - T_{f_j,i})$$

$1 \leq j \leq N$ et des éléments $a_1, ..., a_N \in A$ tels que $a_1c_1 + ... + a_Nc_N = 1$.

Soit L une extension de K où $f_1, ..., f_N$ sont scindés :

$$f_j(X) = \prod_{i=1}^{\deg f_j} (X - r_{f_j,i})$$

pour certains $r_{f_j,i} \in L$.

Soit $\phi : A \to L$ le morphisme de $K-$algèbres tel que :

$$\phi(T_{f,i}) = \begin{cases} r_{f_j,i} & \text{si } f = f_j \\ 0 & \text{sinon.} \end{cases}$$

On étend ϕ en un morphisme $\phi : A[X] \to L[X]$.

On a : $\forall\, j$, $\phi(f_j(X) - \prod_i (X - T_{f_j,i})) = f_j(X) - \prod_{i=1}^{\deg f_j}(X - r_{f_j,i}) = 0 \in L[X]$. En particulier $\forall\, j$, $\phi(c_j) = 0$.

Donc $\phi(1) = \sum_j \phi(a_j)\phi(c_j) = 0$ *absurde !*

Soit $I \leq \mathfrak{m} < A$ un idéal maximal. On pose $\overline{K} := A/\mathfrak{m}$. C'est un corps. De plus $K \cap \mathfrak{m} = 0$ donc on peut identifier K avec son image dans $A/\mathfrak{m}$.

L'extension $\overline{K}/K$ est algébrique. En effet, $\overline{K}$ est engendré par les $t_{f,i} := T_{f,i} \bmod \mathfrak{m}$. Or par définition :

$$f(X) - \prod_{i=1}^{\deg f} (X - T_{f,i}) \in I[X] \leq \mathfrak{m}[X]$$

i.e. $f(X) = \prod_{i=1}^{\deg f}(X - t_{f,i}) \in \overline{K}[X]$. En particulier, $f(t_{f,i}) = 0$ et les $t_{f,i}$ sont algébriques sur K.

Le corps $\overline{K}$ est algébriquement clos. En effet, soit $P \in \overline{K}[X]$ un polynôme irréductible unitaire. Soit α une racine de P dans une extension Ω de $\overline{K}$. On a $K \leq \overline{K} \leq \overline{K}(\alpha)$. L'élément α est algébrique sur K. Soit Q son polynôme minimal sur K. Comme P est irréductible unitaire, P est le polynôme minimal de α sur $\overline{K}$. Donc $P|Q$ dans $\overline{K}[X]$. Or Q est scindé sur $\overline{K}$. Donc les facteurs irréductibles de P sont de degré 1 et $\deg P = 1$. **Q.e.d.**

Exemples : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$, $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ et $\cup_{n>0}\mathbb{C}((t^{1/n}))$ une clôture algébrique de $\mathbb{C}((t))$.

COURS DU MERCREDI 26 FÉVRIER 2014

5.1 Retour sur la notion de séparabilité

Soit E/F une extension finie. On fixe un corps algébriquement clos Ω et un morphisme $\sigma : F \to \Omega$. On note $[E : F]_s$ le nombre de prolongement de σ à E, c'est le *degré séparable de* E/F. *Remarque :* ce nombre ne dépend pas du corps algébriquement clos choisi ni du morphisme σ. En effet, soit $\sigma' : F \to \Omega'$ est un autre morphisme vers un corps algébriquement clos. Soient $x_1, ..., x_n \in E$ tels que $E = F(x_1, ..., x_n)$. Soient $P_1, ..., P_n$ les polynômes minimaux des x_i sur F. Soit L (*resp.*L') le corps de décomposition des polynômes $P_i^{\sigma} \in \sigma(F)[X]$ dans Ω (*resp.*$P_i^{\sigma'} \in \sigma'(F)[X]$ dans Ω'). Il est clair que tout prolongement de σ à E envoie E dans L (*resp.*de σ' ... dans L'). Il existe un prolongement $\tau : L \simeq L'$ de $\sigma' \circ \sigma^{-1} : \sigma(F) \to \sigma'(F)$. On a alors une bijection :

$$\{\widetilde{\sigma} : E \to \Omega \ : \ \widetilde{\sigma}|_F = \sigma\} \xrightarrow{1:1} \{\widetilde{\sigma'} : E \to \Omega \ : \ \widetilde{\sigma'}|_F = \sigma'\}$$

$$\Sigma \longmapsto \tau \circ \Sigma$$

Proposition 5.2 *$[E : F]_s$ est fini $\leq [E : F]$.*

Proposition 5.3 *Si $E = k(a)$, alors $[E : k]_s = [E : k] \Leftrightarrow a$ séparable sur k.*

Proposition 5.4 *Si $K \leq L \leq M$, alors $[M : K]_s = [M : L]_s[L : K]_s$.*

Proposition 5.5 *L'extension E/F est séparable $\Leftrightarrow [E:F]_s = [E:F]$.*

Corollaire 5.5.1 *Si $K \leq L \leq M$, alors M/K séparable $\Leftrightarrow$ M/L et L/K séparables. Si $E = K(x_1, ..., x_n)$ et si les x_i sont séparables sur K, alors E/K est séparable.*

6 Base normale

6.1 Éléments primitifs

Soit E/K une extension.
On dit que $x \in E$ est un élément *primitif* de E/K si $E = K(x)$.

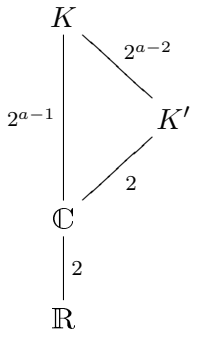
Théorème 6.1 *Si $x, y \in E$ sont algébriques sur K, si y est séparable sur K, alors il existe $z \in E$ tel que $E = K(z)$. En particulier, si $x_1, ..., x_n \in E$ sont algébriques séparables, alors $K(x_1, ..., x_n)/K$ admet un élément primitif.*

Exercice : si E/K est finie, alors E/K admet un élément primitif si et seulement s'il existe un nombre fini de corps $K \leq L \leq E$.

Contre-exemple : si $K := \mathbb{F}_p(X^p, Y^p)$, $E := \mathbb{F}_p(X, Y)$, alors les corps $K(X + tY)$, $t \in K$ sont deux à deux distincts.

Théorème 6.2 (d'Alembert-Gauss) *Le corps $\mathbb{C}$ est algébriquement clos.*

Démonstration : Le corps des réels n'admet pas d'extension de degré impair > 1. Si $K \geq C$ est une extension galoisienne de degré n, alors il existe $a \in K$ tel que $K = \mathbb{R}(a)$. Soit G son groupe de Galois, soit P un $2-$groupe de Sylow de G. Alors K^P est une extension d'ordre impair de $\mathbb{R}$ donc $K^P = \mathbb{R}$ et $P = G$. Mais alors, $|G| = 2^a$ pour un certain $a \geq 1$. Si $a > 1$, il existe un sous-groupe $H \leq \mathrm{Gal}(K/\mathbb{C}$ d'ordre 2^{a-2}. Mais alors K^H est une extension de degré 2 de $\mathbb{C}$ *absurdo !*



Q.e.d.

Exemple : soit k un corps. Soient $L := k(x_1, ..., x_n)$, $K := k(s_1, ..., s_n)$. Alors $a := x_1 x_2^2 ... x_n^n$ est un élément primitif de L sur K et x_n est un élément primitif pour $L^{\mathfrak{S}_{n-1}}/K$.

6.2 Théorème de la base normale

Soit E/K une extension galoisienne de groupe G. Une base $e_1, ..., e_n$ de E sur K est *normale* si pour tout i, il existe $\sigma \in G$ tel que $e_i = \sigma(e_1)$.

Exemple : le polynôme $P := X^4+X+1$ est primitif sur $\mathbb{F}_2$ et toute racine a de P dans $\mathbb{F}_{16}$ est un élément primitif de $\mathbb{F}_{16}/\mathbb{F}_2$. La base $1, a, a^2, a^3$ n'est pas normale (car $a^8 = \mathrm{Fr}_2^3(a) = a^2 + 1$).

Cependant :

Théorème 6.3 (de la base normale pour un corps fini) *Soient q une puissance d'un nombre premier, $d \geq 1$, $q' := q^d$. Il existe $\theta \in \mathbb{F}_{q'}$ tel que $\theta, \mathrm{Fr}_q\theta, ..., \mathrm{Fr}_q^{d-1}\theta$ est une base de $\mathbb{F}_{q'}$ sur $\mathbb{F}_q$.*

Démonstration : Soit $T^d - 1 = P_1^{r_1}...P_s^{r_s}$ la factorisation de $T^d - 1$ en irréductibles distincts dans $\mathbb{F}_q[T]$. Comme $\mathbb{F}_q-$espaces vectoriels, on a :

$$\mathbb{F}_{q'} = \oplus_i \ker(P_i^{r_i}(\mathrm{Fr}_q)) \ .$$

Comme $T^d - 1$ est le polynôme minimal de l'endomorphisme Fr_q, pour tout i, $P_i^{r_i}$ est le polynôme minimal de Fr_q sur $\ker(P_i^{r_i}(\mathrm{Fr}_q))$. Pour tout$i$, soit $x_i \in \ker(P_i^{r_i}(\mathrm{Fr}_q)) \leq \mathbb{F}'_q$ tel que $P_i^{r_i-1}(\mathrm{Fr}_q)(x_i) \neq 0$. Alors $x_i, ..., P_i^{r_i-1}(\mathrm{Fr}_q)(x_i)$ est une base de $\ker(P_i^{r_i}(\mathrm{Fr}_q))$. On pose alors $\theta := x_1 + ... + x_s$. On a :

$$\sum_{k=0}^{d-1} \lambda_k \mathrm{Fr}_q^k(\theta) = 0 \Rightarrow \forall\, i,\ \sum_{k=0}^{d-1} \lambda_k \mathrm{Fr}_q^k(x_i)$$

$$\Rightarrow \forall\, i,\ P_i^{r_i} | \sum_k \lambda_k T^k \Rightarrow T^d - 1 | \sum_k \lambda_k T^k$$

$$\Rightarrow \forall\, k,\ \lambda_k = 0 \ .$$

Q.e.d.

Remarque : si $\theta, ..., \theta^{2^{d-1}}$ est une base de $\mathbb{F}_{2^d}$ sur $\mathbb{F}_2$, alors $(a_0\theta + ... + a_{d-1}\theta^{2^{d-1}})^2 = a_{d-1}\theta + a_0\theta^2 + ... + a_{d-2}\theta^{2^{d-1}}$.

Théorème 6.4 (de la base normale pour les corps infinis) *Soit E/K une extension galoisienne. Il existe une base normale de E/K.*

Démonstration : Soit $e_1, ..., e_n$ une base de E/K. Soit $\mathrm{Gal}(E/K) =: \{\sigma_1, ..., \sigma_n\}$ avec $\sigma_1 = \mathrm{Id}$. On pose $D(T_1, ..., T_n) := \det((\sum_{k=1}^n T_k \sigma_i^{-1}\sigma_j(e_k))_{i,j}) \in E[T_1, ..., T_n]$. Comme la matrice $(\sigma_i(e_k))_{i,k} \in \mathrm{GL}_n(E)$, il existe $c_1, ..., c_n \in E$ tels que $\sum_k c_k\sigma_i(e_k) = 1$ si $i = 1$, 0 si $i \neq 1$. Mais alors $D \neq 0$. Donc comme K est infini, on peut trouver $b_1, ..., b_n \in K$ tels que $D(b_1, ..., b_n) \neq 0$. Or :

$$D(b_1, ..., b_n) = \det((\sigma_i^{-1}\sigma_j(x))_{i,j})$$

si $x := \sum_k b_k e_k$. **Q.e.d.**

Exemples :

a) $\{1+i, 1-i\}$ est une base normale pour $\mathbb{C}/\mathbb{R}$.

b) l'ensemble des conjugués de $1+\sqrt{2}+\sqrt{3}+\sqrt{6}$ est une base normale de $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ mais non celui des conjugués de $\sqrt{2}+\sqrt{3}$.

c) Si p est un nombre premier, si $z := e^{2i\pi/p}$, alors $\{z, ..., z^{p-1}\}$ est une base normale mais non $\{1, z, ..., z^{p-2}\}$.

d) Soient $E = k(x_1, ..., x_n)$, $K := k(s_1, ..., s_n)$, $x := x_1 x_2^2 ....x_n^n$. Alors, $\{\sigma(x) : \sigma \in \mathfrak{S}_n\}$ est une base normale de E/K.

Remarque : le théorème signifie que le $k[G]-$ module E est libre de rang 1 (où $G := \mathrm{Gal}(E/K)$).