Théorie de Galois

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

Villeurbanne, le 27 mars 2013

Table des matières

Index

Cours du mercredi 30/1/13

Introduction

0.1 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 : Calculer $\cos(2\pi/5)$ et $(\sin(2\pi/5)$.

0.2 Degré 3

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

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

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 :

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

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

Donc :

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

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

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

où à chaque ligne, la deuxième racine cubique est choisie de sorte que le produit des 2 racines cubiques est $-3p$.

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 :

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

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* $(2\cos 3t) = (2\cos t)^3 - 3(2\cos t)$*).*

0.3 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 *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

Soit $K \leq E$ une extension de corps. Soit $x \in E$. 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 1.3 *L'ensemble* $\{x \in E : x$ *est algébrique sur* $K\}$ *est un sous-corps de* E.

Proposition 1.4 *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, corps de décomposition

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 1.5 *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.

Réalisation du corps de rupture

Si $P(X) = X^n + a_1X^{n-1} + ... + a_n \in K[X]$ est irréductible, alors $K[X]/(P) \simeq K[A]$ où A est la matrice :

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

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

Cours du mercredi 6/2/13

Théorème 1.6 *Soit K un corps. Soit $P \in K[X]$ irréductible. Soit $L \geq K$ un corps qui contient une racine α de P. Alors $K[\alpha] = K(\alpha) \simeq K[X]/(P)$.*

On dit que $K(\alpha)$ est un corps de rupture de P sur K.

En particulier $1, \alpha, ..., \alpha^{\deg P - 1}$ est une $K-$base de α. Ça existe toujours ! *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 $\mathbb{Q}$.

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.

Théorème 1.7 (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 une extension de K, K', alors σ se prolonge en $K(\alpha) \simeq K'(\alpha')$.*

Théorème 1.8 (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 1.8.1 *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 $\mathbb{F}_q$.

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 $F := E^{\{\sigma_1,...,\sigma_n\}}$, $[E : F] \geq n$.*

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

Cours du mercredi 13 février 2013

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 $F = E^G$, $G = \{\sigma_1, ..., \sigma_n\}$. **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 particlier, $G = \mathrm{Aut}_F(E)$.*

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

Exemple : $k(x_1, ..., x_n)^{\mathfrak{S}_n} = k(s_1, ..., s_n)$, $\mathbb{Q}(\sqrt[3]{2}, j) \geq \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(j\sqrt[3]{2}), \mathbb{Q}(j^2\sqrt[3]{2}), \mathbb{Q}(j)$; 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.

3.2 Surjectivité

Théorème 3.2 *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 $E^H = B$.*

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

3.3 Théorème fondamental

Théorème 3.3 *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, $\mathrm{Gal}(B/F) \simeq G/\mathrm{Gal}(E/B)$.

3.4 Caractérisation des extensions galoisiennes

Théorème 3.4 *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 $|\mathrm{Aut}(E/\mathbb{Q})| = 2 < 4 = [E : \mathbb{Q}]$.

Cours du 20 février 2013

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

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

Théorème 3.6 *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 3.7 *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 $r = \deg P$.*

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

3.6 Normalité

On dit qu'une extension E/F est *normale* si 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 3.8 *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 3.9 *Soit E/F une extension finie. Alors l'extension E/F est galoisienne si et seulement si elle est normale et séparable.*

3.7 Composée de corps

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 3.10 *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,* $E \cap E' = K$, $\mathrm{Gal}(EE'/K) \simeq \mathrm{Gal}(E/K) \times \mathrm{Gal}(E'/K)$.

Cours du mercredi 27 février

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 $\mu_{\mathbf{n}}$.

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

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 6 mars

4.4 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 $\mathbb{F}_{q^m}^\times$.*

Corollaire 4.9.1 *Le corps de décomposition de tout polynôme irréductible de degré m sur $\mathbb{F}_q$ est $\mathbb{F}_{q^m}$.*

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 $(\mathbb{F}_q[X]/(P))^\times$.

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 $(\mathbb{Z}/e\mathbb{Z})^\times$.*

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 $\mod 23$; 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 $q^m - 1$.*

4.5 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 $a \in \mathbb{F}_q$. **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 $J \subsetneq A$. 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 dur 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.**

Cours du mercredi 13 mars

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 $x_1, ..., x_n \in E$ sont algébriques séparables, alors $K(x_1, ..., x_n)/K$ admet un élément primitif.*

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

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 p un nombre premier, $d \geq 1$, $q := p^d$. Il existe $\theta \in \mathbb{F}_q$ tel que $\theta, \mathrm{Fr}_p\theta, ..., \mathrm{Fr}_p^{d-1}\theta$ est une base de $\mathbb{F}_q$ sur $\mathbb{F}_p$.*

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.*

Exemples :

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

b) 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.

Cours du mercredi 20 mars

Remarque : soit E/K une extension galoisienne de groupe de Galois G. D'après le théorème de la base normale, $E \simeq K[G]$ comme $G-$module sur K.

Exercice : Montrer que $1+\epsilon_1\sqrt{2}+\epsilon_2\sqrt{3}+\epsilon_3\sqrt{6}$, $\epsilon_i = \pm 1$, $\epsilon_1\epsilon_2\epsilon_3 = 1$ est une base normale pour $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

7 Extensions cyclotomiques

7.1 Racines primitives $n-$ièmes

Soit K un corps. Pour tout $n \geq 1$, on note $\mu_n(K)$ le sous-groupe de $K^\times$ formé des racines de $T^n - 1$.

Remarque : si L contient un corps de décomposition de $T^n - 1$ sur K et si $\mathrm{car}(K)$ ne divise pas n, $\mu_n(L)$ est cyclique d'ordre n. Les générateurs de $\mu_n(L)$ sont les *racines primitives $n-$ièmes de* 1.

Une *extension cyclotomique* est une extension de la forme $K(\zeta_n)/K$ où K est un corps de caractéristique première à n et ζ_n une racine primitive $n-$ième de 1 (dans un corps de décomposition de $T^n - 1$ sur K).

Théorème 7.1 *Soit une extension cyclotomique $K(\zeta_n)/K$ où K est un corps de caractéristique première à n et ζ_n une racine primitive $n-$ième de 1. Alors $K(\zeta_n)/K$ est galoisienne de groupe de galois isomorphe à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Démonstration : Si $\sigma \in \mathrm{Gal}(K(\zeta_n)/K)$, $\sigma(\zeta_n) = \zeta_n^{m_\sigma}$ pour un $m_\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$. Le morphisme $\sigma \mapsto m_\sigma$ est injectif. **Q.e.d.**

Corollaire 7.1.1 *Une extension cyclotomique est toujours abélienne.*

7.2 Polynômes cyclotomiques sur $\mathbb{Q}$

Théorème 7.2 *Soit $\zeta_n \in \mathbb{C}^\times$ un élément d'ordre n. L'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est galoisienne de groupe de Galois $\simeq (\mathbb{Z}/n\mathbb{Z})^\times$.*

On note $\Phi_n(X) := \prod_{k\in(\mathbb{Z}/n\mathbb{Z})^\times}(X - e^{2ik\pi/n})$. C'est le *$n-$ième polynôme cyclotomique* .

Proposition 7.3 *(i)* $\Phi_n \in \mathbb{Z}[X]$ *est unitaire irréductible sur $\mathbb{Q}$, c'est le polynôme minimal de ζ_n sur $\mathbb{Q}$ pour tout ζ_n d'ordre n.*

(ii) $\deg \Phi_n = \varphi(n)$.

(iii) $T^n - 1 = \prod_{d|n} \Phi_d(X)$.

(iv) $\Phi_n(X) = \prod_{d|n}(X^d-1)^{\mu(n/d)}$.

Démonstration : Si on suppose que $\Phi_d(X)$ est unitaire à coefficients entiers, pour $d<n$, alors le quotient de la division euclidienne de X^n-1 par $\prod_{\substack{d|n\\ d<n}} \Phi_d(X)$ est un polynôme à coefficients entiers (unitaire). Or ce quotient est précisément $\Phi_n(X)$. Pour montrer l'irréductibilité de Φ_n, on considère P le polynôme minimal d'une racine primitive $n-$ième de 1 ζ_n sur $\mathbb{Q}$. On montre que si p est un nombre premier tel que $p \not| n$, $P(\zeta_n^p)=0$.

En effet, soit Δ le discriminant de X^n-1. On a :

$$\Delta = \prod_{1\le i<j\le n}(\zeta_n^i-\zeta_n^j)^2 = \pm \prod_{\substack{1\le i,j\le n\\ i\neq j}}(\zeta_n^i-\zeta_n^j)$$

$$= \pm \prod_{1\le i\le n}\zeta_n^i \prod_{\substack{1\le j\le n\\ j\neq i}}(1-\zeta_n^{j-i})$$

$$= \pm(\prod_{1\le k\le n-1}(1-\zeta_n^k))^n$$

$$= \pm((X^n-1)'(1))^n = \pm n^n \ .$$

Notons $z_1,...,z_r$ les racines de P. Comme $P|X^n-1$ dans $\mathbb{Q}$, $P\in\mathbb{Z}[X]$. Donc $P(X^p)=P(X) \bmod p\mathbb{Z}[X]$. Si $P(\zeta_n^p)\neq 0$, $\zeta_n^p \notin \{z_1,...,z_r\}$ et $P(\zeta_n^p)=\prod_{i=1}^r(\zeta_n^p-z_i)$ divise Δ dans $\overline{\mathbb{Z}}$. Or $P(\zeta_n^p)=P(\zeta_n)^p=0 \bmod p\overline{\mathbb{Z}}$. Donc $p|n^n$ dans $\overline{\mathbb{Z}}$ donc dans $\mathbb{Z}$ car $\mathbb{Q}\cap\overline{\mathbb{Z}}=\mathbb{Z}$. C'est absurde car $p\not| n$. **Q.e.d.**

Exemple : si p premier, $\Phi_p = 1+...+X^{p-1}$.

Exercice : déterminer $\Phi_n(X)$ si $1\le n\le 8$.

Exemple : $\Phi_{105}(X) = X^{48}+X^{47}+X^{46}-X^{43}-X^{42}-2X^{41}-X^{40}-X^{39}+X^{36}+X^{35}+X^{34}+X^{33}+X^{32}+X^{31}-X^{28}-X^{26}-X^{24}-X^{22}-X^{20}+X^{17}+X^{16}+X^{15}+X^{14}+X^{13}+X^{12}-X^9-X^8-2X^7-X^6-X^5+X^2+X+1$.

7.3 Théorème de Kronecker-Weber

Théorème 7.4 *Soit $K/\mathbb{Q}$ une extension abélienne. Alors, $K\le\mathbb{Q}(\zeta_n)$ pour une certaine racine primitive $n-$ième ζ_n.*

Exemple : $\mathbb{Q}(i)=\mathbb{Q}(\zeta_4)$, $\mathbb{Q}(\sqrt{2})\le\mathbb{Q}(\zeta_8)$.

Démonstration : Dans le cas où $K/\mathbb{Q}$ est quadratique : on introduit les sommes de Gauss :

si $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ est un caractère, on pose pour tout $a\in\mathbb{Z}$), $\chi(a) := \chi(a \bmod N$ si $(a,N)=1$, 0 sinon.

Pour tout $a\in\mathbb{Z}$, soit $G_a(\chi) := \sum_{x=1}^{N-1}\chi(x)\zeta_N^{ax}$ où $\zeta_N := e^{2i\pi/N}$.

Proposition 7.5 *Si χ est primitif (*i.e. *si $M>1$ est un diviseur strict de N, χ n'est pas trivial sur* $\ker((\mathbb{Z}/N\mathbb{Z})^\times\to(\mathbb{Z}/M\mathbb{Z})^\times)$*, alors on a :*

(i) $\forall\, a \in \mathbb{Z}$, $G_a(\chi) = \overline{\chi}(a) G_1(\chi)$;
(ii) $\overline{G_1(\chi)} = \chi(-1) G(\overline{\chi})$;
(iii) $|G_1(\chi)|^2 = N$.

Démonstration : Si $(a, N) = 1$), on a :

$$G_a(\chi) = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(x) \zeta_N^{ax} = \sum_{y \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(y a^{-1}) \zeta_N^{y}$$

$$= \chi(a^{-1}) \sum_{y \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(y) \zeta_N^{y}$$

$$= \overline{\chi(a)} G_1(\chi) \ .$$

Si $(a, N) = d > 1$, alors : $a = da'$ avec $a' \in (\mathbb{Z}/N\mathbb{Z})^\times$ et :

$$G_a(\chi) = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(x) \zeta_N^{da'x}$$

$$= \chi(a'^{-1}) \sum_{y \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(y) \zeta_N^{dy}$$

$$= \chi(a'^{-1}) \sum_{i=1}^{r} \sum_{h \in H_d} \chi(y_i h) \zeta_N^{dy_i h}$$

où $H_d := \ker \left(\ \mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/(N/d)\mathbb{Z})^\times \ \right)$ et $y_1, ..., y_r$ est un système de représentants de $(\mathbb{Z}/N\mathbb{Z})^\times / H_d$.

Donc $G_a(\chi) = \chi(a'^{-1}) \sum_{i=1}^{r} \chi(y_i) \zeta_N^{dy_i} \underbrace{\sum_{h \in H_d} \chi(h)}_{=0} = 0$ si on suppose $\chi|_{H_d}$ non trivial. Or, $\chi(a) = 0$ si $(a, N) = d > 1$. **Q.e.d.**

Corollaire 7.5.1 *Si p est un nombre premier impair, alors $G_1(\chi_p) = \pm\sqrt{\left(\frac{-1}{p}\right) p}$, où $\chi_p : a \mapsto \left(\frac{a}{p}\right)$ est le symbole de Legendre.*

Q.e.d.

Exercice : vérifier que $2\sin(2\pi/7) + 2\sin(3\pi/7) - 2\sin(\pi/7) = \sqrt{7}$.

Cours du 27 mars

8 Norme et trace

Soit E/K une extension finie. Si $\alpha \in E$, on note :

$$N_{E/K}(\alpha) := \det_K m_\alpha,\ \mathrm{Tr}_{E/K}(\alpha) := \mathrm{Tr}_K(m_\alpha)\ .$$

Exemple : $N_{\mathbb{C}/\mathbb{R}}(z) = |z|^2$, $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(z) = 2\Re z$.
Remarque : la norme est à valeurs dans $K^\times$ et la trace dans K.

Proposition 8.1 *Soient E/K une extension finie et $\alpha \in E$ de polynôme minimal sur K :*

$$T^n + a_1 T^{n-1} ... + a_n\ .$$

(i) Si $E = K(\alpha)$, alors $N_{E/K}(\alpha) = (-1)^n a_n$ et $\mathrm{Tr}_{E/K}(\alpha) = -a_1$.

(ii) Si $[E : K(\alpha)] = r$, alors $N_{E/K}(\alpha) = (-1)^{nr} a_n^r$ et $\mathrm{Tr}_{E/K}(\alpha) = -ra_1$.

(iii) Transitivité : si $k \leq L \leq E$, $N_{E/K} = N_{L/K} \circ N_{E/L}$ et $\mathrm{Tr}_{E/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{E/L}$.

(iv) Si E/K est galoisienne de groupe de Galois $G = \{\sigma_1, ..., \sigma_m\}$, alors :

$$N_{E/K}(\alpha) = \sigma_1(\alpha)...\sigma_m(\alpha),\ \mathrm{Tr}_{E/K}(\alpha) = \sigma_1(\alpha) + ... + \sigma_m(\alpha)$$

9 Extensions cycliques

Une extension *cyclique* est une extension galoisienne de groupe de Galois cyclique.

Exemples : les extensions des corps finis, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, $\mathbb{Q}(\zeta_n, \sqrt[n]{p})/\mathbb{Q}(\zeta_n)$.
Contre-exemple : $\mathbb{Q}(\eta_8)/\mathbb{Q}$.

9.1 Théorème 90 de Hilbert

Théorème 9.1 *Soit E/K une extension cyclique. Soit σ un générateur de $\mathrm{Gal}(E/K)$. Si $b \in E$, alors sont équivalentes :*

i) $N_{E/K}(b) = 1$;

ii) $b = a\sigma(a)^{-1}$ pour un certain $a \in E^\times$.

Théorème 9.2 (Kummer) *Soit E/K une extension galoisienne. On suppose que la caractéristique de K est première à n et que K contient une racine primitive $n-ième$ de l'unité.*

(i) Si E/K est cyclique de degré n, alors il existe $\alpha \in E$ tel que $E = K(\alpha)$ et $\alpha^n \in K$.

(ii) S'il existe $\alpha \in E$ tel que $E = K(\alpha)$ et $\alpha^n \in K$, alors il existe d tel que $d|n$, E/K est de degré d, $\alpha^d \in K$ et $T^d - \alpha^d$ est le polynôme minimal de α sur K.

Exercice : vérifier que l'extension $\mathbb{Q}(\zeta_n, \sqrt[n]{p})/\mathbb{Q}(\zeta_n)$ est galoisienne cyclique de groupe de Galois $\simeq \mathbb{Z}/n\mathbb{Z}$.

Exercice : si E/K est galoisienne cyclique de degré $p = \mathrm{car}(K)$, alors il existe $\alpha \in E$, $a \in K$ tels que $E = K(\alpha)$ et $\alpha^p - \alpha - a = 0$.

10 Résolubilité par radicaux

Une extension L/K est *résoluble* s'il existe $E \geq L \geq K$ telle que E/K est galoisienne de groupe de Galois résoluble.

On rappelle qu'un groupe fini G est *résoluble* s'il existe une suite desous-groupes :

$$G = G_0 \geq ... \geq G_n = 1$$

tels que $G_{i+1} \triangleleft G_i$ et G_i/G_{i+1} est cyclique d'ordre un nombre premier p qui divise $|G|$.

Exercice : si $H \triangleleft G$, G est résoluble $\Leftrightarrow$ H et G/H résolubles.

Remarque : soient $K \leq L \leq M$. Si M/L et L/K sont résolubles, alors M/K aussi.

Soit K un corps de caractéristique nulle. On dit qu'une extension L/K est *résoluble par radicaux* s'il existe une tour d'extensions $K = K_0 \leq .... \leq K_m = E \geq L$ telle que :

$$\forall\, j \geq 1,\ \exists\, \alpha_j \in K_{j+1},\ n_j > 0,\ K_{j+1} = K_j(\alpha_j) \text{ et } \alpha_j^{n_j}\ .$$

Lemme 10.1 *Soient $K \leq F, L \leq E$. On suppose $\mathrm{car}(K) = 0$ et E/K galoisienne. Si L/K est résoluble (resp.par radicaux), alors FL/F aussi.*

Cours du mercredi 3 avril

Lemme 10.2 *Soient $K \leq L \leq M$. L'extension M/K est résoluble (resp.par radicaux) si et seulement si M/L et L/K le sont.*

Attention ! si $K \leq L \leq M$ et si L/K et M/L sont galoisiennes, M/K n'est pas forcément galoisienne : par ex. : $\mathbb{Q}(\sqrt[4]{2}) \geq \mathbb{Q}(\sqrt{2}) \geq \mathbb{Q}$.

Démonstration :

Supposons L/K et M/L résolubles. Soit $E \geq M \geq L \geq K$ avec E/K galoisienne. Soit L' le sous-corps de E engendré par les $\sigma(L)$ où σ décrit $\mathrm{Gal}(E/K)$. Alors $E \geq L' \geq L \geq K$ et L'/K est galoisienne de groupe de Galois $\mathrm{Gal}(L'/K)$ résoluble. De même il existe $E \geq M' \geq M \geq L$ tel que M'/L est galoisienne de groupe de Galois $\mathrm{Gal}(M'/L)$ résoluble. Soit M" le sous-corps de E engendré par les $\sigma(M')$ où σ décrit $\mathrm{Gal}(E/K)$. Alors $M" \geq M, L' \geq K$ et $M"/K$ est galoisienne. Or, $\mathrm{Gal}(M"/L')$ est résoluble car isomorphe à un sous-groupe de :

$$\prod_{\sigma \in \mathrm{Gal}(E/K)} \mathrm{Gal}(\sigma(M')/L') \leq \prod_{\sigma \in \mathrm{Gal}(E/K)} \underbrace{\mathrm{Gal}(\sigma(M')/\sigma(L))}_{\simeq \mathrm{Gal}(M'/L)} .$$

Comme $\mathrm{Gal}(M"/K)/\mathrm{Gal}(M"/L') \simeq \mathrm{Gal}(L'/K)$ est aussi résoluble, $\mathrm{Gal}(M"/K)$ est résoluble.

Par ex. : si $M = \mathbb{Q}(\sqrt[4]{2}), L = \mathbb{Q}(\sqrt{2}), K = \mathbb{Q}$, $M" = \mathbb{Q}(\sqrt[4]{2}, i)$. **Q.e.d.**

Théorème 10.3 *Soit K de caractéristique nulle. Une extension L/K est résoluble si et seulement si elle est résoluble par radicaux.*

Si $P \in K[X]$ est un polynôme séparable, on dit que P est résoluble par radicaux si le corps de décomposition de P sur K est résoluble par radicaux (sur K).

Théorème 10.4 *Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré p premier. Alors sont équivalentes :*

(i) *P est résoluble par radicaux ;*

(ii) *il existe x_1, x_2 racines de P telles que $\mathbb{Q}(x_1, x_2)$ est le corps de décomposition sur $\mathbb{Q}$ de P ;*

(iii) *pour toutes racines $x_1 \neq x_2$ de P, $\mathbb{Q}(x_1, x_2)$ est le corps de décomposition sur $\mathbb{Q}$ de P.*

Théorème 10.5 *Soit C un $p-$cycle dans $\mathfrak{S}_p$. Alors le normalisateur de $N = N_{\langle c \rangle}(\mathfrak{S}_p)$ est un groupe résoluble d'ordre $p(p-1)$ ($\simeq \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbb{Z}/p\mathbb{Z})^\times, b \in \mathbb{Z}/p\mathbb{Z} \right\}$).*