

Théorie de Galois

Alexis TCHOUDJEM

Institut Camille Jordan

Université Claude Bernard Lyon I

Boulevard du Onze Novembre 1918

69622 Villeurbanne

FRANCE

Villeurbanne, le 17 avril 2013

Table des matières

Introduction	3
0.1 Équations de degré 2	5
0.2 Degré 3	5
0.3 Degré ≥ 5	6
1 Extensions, algébricité	6
1.1 Polynômes irréductibles	6
1.2 Extensions, degré	6
1.3 Éléments algébriques	7
1.4 Corps de rupture, corps de décomposition	7
2 Caractères et morphismes de corps	9
2.1 Indépendance	9
2.2 Corps des invariants	10
3 Correspondance de Galois	10
3.1 Extensions galoisiennes	10
3.2 Surjectivité	11
3.3 Théorème fondamental	12
3.4 Caractérisation des extensions galoisiennes	12
3.5 Séparabilité	13
3.6 Normalité	13
3.7 Composée de corps	14
4 Corps finis	15
4.1 Sous-groupes finis de K^\times	15
4.2 Structure	15
4.3 Polynômes sur les corps finis	16
4.3.1 Nombre de polynômes irréductibles de degré donné	16
4.4 Ordre d'un polynôme, polynôme primitif	18
4.5 Algorithme de Berlekamp	19
5 Clôture algébrique	19
6 Base normale	21
6.1 Éléments primitifs	21
6.2 Théorème de la base normale	21
7 Extensions cyclotomiques	22
7.1 Racines primitives n -ièmes	22
7.2 Polynômes cyclotomiques sur \mathbb{Q}	22
7.3 Théorème de Kronecker-Weber	23

8	Norme et trace	25
9	Extensions cycliques	25
9.1	Théorème 90 de Hilbert	25
10	Résolubilité par radicaux	26
11	Calcul du groupe de Galois	28
11.1	Discriminant	28
11.2	Réduction	28
12	Cohomologie galoisienne	29
12.1	G -modules	29
12.2	Groupes de cohomologie	30
12.2.1	En degré 1	30
12.2.2	En tout degré	31
13	Théorie de Kummer	32
14	Extensions d'Artin-Schreier	34
14.1	Forme additive du théorème 90 de Hilbert	34
14.2	Théorie des extensions d'exposant p en caractéristique p . . .	34
14.3	Théorème d'Artin-Schreier	35

Index

- 90 (forme additive du théorème de Hilbert), 34
- 90 (théorème de Hilbert), 25
- G -module, 29

- cyclique (extension), 25

- Artin-Schreier (extensions), 34
- Artin-Schreier (théorème), 35

- Berlekamp (algorithme), 19

- casus irreducibilis, 6
- cobords, 32
- cocycles, 31, 32
- cohomologie, 32
- corps de décomposition, 9
- corps de rupture, 7
- cyclotomique (extension), 22
- cyclotomique (polynôme), 22

- exposant d'un groupe, 15

- galoisienne (extension), 10

- indépendance des caractères, 9

- Kronecker-Weber, 23
- Kummer (théorème sur les extensions cycliques), 25

- normale (base), 21
- normale (extension), 13

- polynôme minimal, 7
- primitif (polynôme), 19
- primitif (élément), 21

- résoluble (extension), 26
- résoluble (groupe), 26
- résoluble par radicaux, 26
- résoluble par radicaux réels, 6

- séparable (élément), 13

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 $K_1 \leq \dots \leq K_n$ des corps. Alors $[K_n : K_1] = [K_n : K_{n-1}] \dots [K_2 : K_1]$.

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 $\{x \in E : x \text{ est algébrique sur } K\}$ 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 $K[X]/(P) \rightarrow k[\alpha]$, $Q(X) \bmod P \mapsto Q(\alpha)$ 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 $P(X) = X^n + a_1X^{n-1} + \dots + a_n \in K[X]$ est irréductible, alors $K[X]/(P) \simeq K[A]$ où A est la matrice :

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

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

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 $1, \alpha, \dots, \alpha^{\deg P - 1}$ 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 : $P = c(X - x_1)\dots(X - x_n)$. On dit que $K(x_1, \dots, x_n)$ est le corps de décomposition de P dans E .

Théorème 1.7 (prolongement d'isomorphisme) Soit $\sigma : K \rightarrow K'$ 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 $\sigma : K \rightarrow K'$ un isomorphisme de corps. Soit $P \in K[X]$. Soit $E \geq K$ un corps où P est scindé : $P = c(X - x_1)\dots(X - x_n)$. Soit $E' \geq K'$ un corps où P^σ est scindé : $P^\sigma = c'(X - x'_1)\dots(X - x'_n)$. Soient $B := K(x_1, \dots, x_n), B' := K'(x'_1, \dots, x'_n)$. 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 caractère de G dans K est un morphisme de groupes $G \rightarrow K^\times$. L'ensemble des caractères est une partie du K -espace vectoriel des fonctions $G \rightarrow K$.

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 $\sigma_1, \dots, \sigma_n$ 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 $\sigma_1, \dots, \sigma_n$ sont n morphismes distincts de corps $E \rightarrow E'$. 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, $|\text{Hom}(G, K^\times)| \leq |G|$.

2.2 Corps des invariants

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

Corollaire 2.2.1 Si G est un sous-groupe fini de $\text{Aut}(E)$, 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 $G \leq \text{Aut}(E)$ fini. On dit que E/E^G est une *extension galoisienne* de groupe de Galois G .

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

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 $G \leq \text{Aut}(E)$ un groupe fini. Alors $[E : E^G] = |G|$.

Démonstration : On utilise la forme F -linéaire $\text{Tr} : E \rightarrow F, x \mapsto \sigma_1(x) + \dots + \sigma_n(x)$ où $F = E^G, G = \{\sigma_1, \dots, \sigma_n\}$. **Q.e.d.**

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

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

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

$$H \mapsto E^H$$

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

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

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

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

3.4 Caractérisation des extensions galoisiennes

Théorème 3.4 Soit E/K une extension finie. On a toujours : $|\text{Aut}(E/K)| \leq [E : K]$. L'extension E/K est galoisienne $\Leftrightarrow |\text{Aut}(E/K)| = [E : K]$. Dans ce cas, $\text{Gal}(E/K) = \text{Aut}(E/K)$.

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

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, \dots, x_r , $r \leq n$ les images distinctes de x par les $\sigma \in G$. Le polynôme $(X - x_1) \dots (X - x_r)$ 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 $\text{Gal}(E/K)$ est le groupe de Galois de P sur K . De plus $\text{Gal}_K(P)$ s'identifie à un sous-groupe de \mathfrak{S}_r où $r = \deg P$.*

Exercice : vérifier que $\text{Gal}_K(P)$ 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 -morphisme $\sigma, \tau : E \rightarrow \Omega$, $\sigma(E) = \tau(E)$.

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 , $K \leq E, E' \leq L$, $H := \text{Gal}(L/E)$, $H' := \text{Gal}(L/E')$. On a :*

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

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 $H = \mathfrak{S}_3$, $H' = K_4$, $[E : K] = |\mathfrak{S}_4/\mathfrak{S}_3| = 4$, $[E' : K] = |\mathfrak{S}_4/K_4| = 6$, $EE' = L = L^{H \cap H'}$, $E \cap E' = L^{H, H'} = K$. 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 $\alpha := x_1 x_2^2 x_3^3 x_4^4$.

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 entre 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 μ_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 $n\mathbb{Z} = \ker(\mathbb{Z} \rightarrow A, n \mapsto n1_A)$. 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 $\text{Fr}_q : A \rightarrow A, x \mapsto x^q$ 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 \bar{k} de k telle que \bar{k} est algébriquement clos. Ce corps \bar{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) $\nu_n(q) = \frac{\sum_{d|n} \mu(n/d) q^d}{n}$ 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 :

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

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, \dots, 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 $\text{ord} P := \text{ord} Q$.

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 $m N_{q,m,e} = \varphi(e) =$ le nombre d'éléments d'ordre e dans le groupe cyclique $\mathbb{F}_{q^m}^\times$. **Q.e.d.**

Exemple : $2^{11} - 1 = 23 \cdot 89$. 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 seulement si l'endomorphisme $\text{Fr}_q - \text{Id}$ 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 $Q = a_1X + \dots + a_{d-1}X^{d-1}$ 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 $\text{Fr}_2 - \text{Id}$ 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 $P = \text{pgcd}(P, Q)\text{pgcd}(P, Q + 1) = (1 + X + X^2)(1 + X + X^3)$.

5 Clôture algébrique

Soit K un corps. Une *clôture algébrique de K* est une extension algébrique de corps \bar{K}/K telle que \bar{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 $f_1, \dots, f_N \in I$ et certains coefficients c_1, \dots, 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 $a_1, \dots, a_N \in A$ tels que $a_1 c_1 + \dots + a_N c_N = 1$.

Soit L une extension de K où f_1, \dots, 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 $\phi : A \rightarrow L$ 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 $\phi : A[X] \rightarrow L[X]$.

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.**

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

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

Exemple : soit k un corps. Soient $L := k(x_1, \dots, x_n)$, $K := k(s_1, \dots, s_n)$. Alors $a := x_1 x_2^2 \dots x_n^n$ 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, \dots, 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 $a^8 = \text{Fr}_2^3(a) = a^2 + 1$).

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 $\theta, \text{Fr}_p \theta, \dots, \text{Fr}_p^{d-1} \theta$ est une base de \mathbb{F}_q sur \mathbb{F}_p .*

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

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 :

- $\{1 + i, 1 - i\}$ est une base normale pour \mathbb{C}/\mathbb{R} .
- Soient $E = k(x_1, \dots, x_n)$, $K := k(s_1, \dots, s_n)$, $x := x_1 x_2^2 \dots x_n^n$. 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 $\text{car}(K)$ 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 $\sigma \in \text{Gal}(K(\zeta_n)/K)$, $\sigma(\zeta_n) = \zeta_n^{m_\sigma}$ 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) $T^n - 1 = \prod_{d|n} \Phi_d(X)$.

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

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 $p \nmid n$, $P(\zeta_n^p) = 0$.

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

$$\begin{aligned} \Delta &= \prod_{1 \leq i < j \leq n} (\zeta_n^i - \zeta_n^j)^2 = \pm \prod_{\substack{1 \leq i, j \leq n \\ i \neq j}} (\zeta_n^i - \zeta_n^j) \\ &= \pm \prod_{1 \leq i \leq n} \zeta_n^i \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (1 - \zeta_n^{j-i}) \\ &= \pm \left(\prod_{1 \leq k \leq n-1} (1 - \zeta_n^k) \right)^n \\ &= \pm ((X^n - 1)'(1))^n = \pm n^n. \end{aligned}$$

Notons z_1, \dots, z_r les racines de P . Comme $P|X^n - 1$ dans \mathbb{Q} , $P \in \mathbb{Z}[X]$. Donc $P(X^p) = P(X) \pmod{p\mathbb{Z}[X]}$. Si $P(\zeta_n^p) \neq 0$, $\zeta_n^p \notin \{z_1, \dots, z_r\}$ et $P(\zeta_n^p) = \prod_{i=1}^r (\zeta_n^p - z_i)$ divise Δ dans $\overline{\mathbb{Z}}$. Or $P(\zeta_n^p) = P(\zeta_n)^p = 0 \pmod{p\overline{\mathbb{Z}}}$. 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 $p \nmid n$. **Q.e.d.**

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

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

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, $K \leq \mathbb{Q}(\zeta_n)$ pour une certaine racine primitive n -ième ζ_n .

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

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

si $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ est un caractère, on pose pour tout $a \in \mathbb{Z}$, $\chi(a) := \chi(a \pmod N)$ 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 $\ker((\mathbb{Z}/N\mathbb{Z})^\times \rightarrow (\mathbb{Z}/M\mathbb{Z})^\times)$), alors on a :

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

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

$$\begin{aligned} G_a(\chi) &= \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(x)\zeta_N^{ax} = \sum_{y \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(ya^{-1})\zeta_N^y \\ &= \chi(a^{-1}) \sum_{y \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(y)\zeta_N^y \\ &= \overline{\chi(a)}G_1(\chi) . \end{aligned}$$

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

$$\begin{aligned} G_a(\chi) &= \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(x)\zeta_N^{da'x} \\ &= \chi(a'^{-1}) \sum_{y \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(y)\zeta_N^{dy} \\ &= \chi(a'^{-1}) \sum_{i=1}^r \sum_{h \in H_d} \chi(y_i h)\zeta_N^{dy_i h} \end{aligned}$$

où $H_d := \ker \left((\mathbb{Z}/N\mathbb{Z})^\times \rightarrow (\mathbb{Z}/(N/d)\mathbb{Z})^\times \right)$ et y_1, \dots, 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 :

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

Exemple : $N_{\mathbb{C}/\mathbb{R}}(z) = |z|^2$, $\text{Tr}_{\mathbb{C}/\mathbb{R}}(z) = 2\Re z$.

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 :

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

- (i) Si $E = K(\alpha)$, alors $N_{E/K}(\alpha) = (-1)^n a_n$ et $\text{Tr}_{E/K}(\alpha) = -a_1$.
- (ii) Si $[E : K(\alpha)] = r$, alors $N_{E/K}(\alpha) = (-1)^{nr} a_n^r$ et $\text{Tr}_{E/K}(\alpha) = -ra_1$.
- (iii) Transitivité : si $K \leq L \leq E$, $N_{E/K} = N_{L/K} \circ N_{E/L}$ et $\text{Tr}_{E/K} = \text{Tr}_{L/K} \circ \text{Tr}_{E/L}$.
- (iv) Si E/K est galoisienne de groupe de Galois $G = \{\sigma_1, \dots, \sigma_m\}$, alors :

$$N_{E/K}(\alpha) = \sigma_1(\alpha) \dots \sigma_m(\alpha), \quad \text{Tr}_{E/K}(\alpha) = \sigma_1(\alpha) + \dots + \sigma_m(\alpha)$$

9 Extensions cycliques

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

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

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 $\text{Gal}(E/K)$. 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 $p = \text{car}(K)$, 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 :

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

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 $K = K_0 \leq \dots \leq K_m = E \geq L$ telle que :

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

Lemme 10.1 Soient $K \leq F, L \leq E$. On suppose $\text{car}(K) = 0$ 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 $\text{Gal}(E/K)$. Alors $E \geq L' \geq L \geq K$ et L'/K est galoisienne de groupe de Galois $\text{Gal}(L'/K)$ résoluble. De même il existe $E \geq M' \geq M \geq L$ tel que M'/L est galoisienne de groupe de Galois $\text{Gal}(M'/L)$ résoluble. Soit M'' le sous-corps de E engendré par les $\sigma(M')$ où σ décrit $\text{Gal}(E/K)$. Alors $M'' \geq M, L' \geq K$ et M''/K est galoisienne. Or, $\text{Gal}(M''/L')$ est résoluble car isomorphe à un sous-groupe de :

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

Comme $\text{Gal}(M''/K)/\text{Gal}(M''/L') \simeq \text{Gal}(L'/K)$ est aussi résoluble, $\text{Gal}(M''/K)$ 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 $p(p-1)$ ($\simeq \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in (\mathbb{Z}/p\mathbb{Z})^\times, b \in \mathbb{Z}/p\mathbb{Z} \right\}$).

11 Calcul du groupe de Galois

11.1 Discriminant

Soit $P \in k[X]$ un polynôme unitaire. On suppose que $P = (X - x_1) \dots (X - x_n)$ dans $\Omega[X]$ pour une certaine extension Ω de K . Alors :

$$\Delta_P := \prod_{1 \leq i < j \leq n} (x_i - x_j)^2$$

est le discriminant de P . On a $\Delta_P \in k$.

Théorème 11.1 *Si P est séparable, si G est le groupe de Galois de P sur k , vu comme sous-groupe de \mathfrak{S}_n , alors*

$$G \leq \mathfrak{A}_n \Leftrightarrow \Delta \in (k^\times)^2 .$$

Exemple : déterminer le discriminant de $X^5 + 20X + 16$.

COURS DU MERCREDI 10 AVRIL

11.2 Réduction

Soit $P \in K[T]$, un polynôme séparable *unitaire* de degré n . On pose :

$$S(u, y, T) := \prod_{s \in \mathfrak{S}_n} (T - (u_{s(1)}y_1 + \dots + u_{s(n)}y_n)) \in \mathbb{Z}[u, y, T] .$$

Soit L un corps de décomposition sur K du polynôme P . Soient a_1, \dots, a_n les racines de P dans L . On pose :

$$\theta := u_1 a_1 + \dots + u_n a_n \in L[u_1, \dots, u_n]$$

$$\forall s \in \mathfrak{S}_n, \theta^s := u_{s(1)} a_1 + \dots + u_{s(n)} a_n .$$

On note $F(T, u) := S(u, a_1, \dots, a_n, T) = \prod_{s \in \mathfrak{S}_n} (T - \theta^s) \in K[u_1, \dots, u_n, T]$ (le vérifier : *exo*) et

$$F(T, u) = F_1(T, u) \dots F_r(T, u)$$

la décomposition de F en produits d'irréductibles dans $K[u_1, \dots, u_n, T]$.

On pose :

$$\mathfrak{g} := \{s \in \mathfrak{S}_n : s(F_1) = F_1\}$$

Théorème 11.2 *Le sous-groupe \mathfrak{g} est isomorphe à $G := \text{Gal}_P := \text{Gal}(L/K)$.*

Corollaire 11.2.1 *Soient A un anneau factoriel, $\mathfrak{p} \leq A$ un idéal premier, $K := \text{Frac}(A)$, $\overline{K} := \text{Frac}(A/\mathfrak{p})$. Soit $P \in A[T]$ unitaire, séparable sur K de degré n tel que \overline{P} est aussi séparable sur \overline{K} . Alors le groupe $\overline{G} := \text{Gal}_{\overline{P}/\overline{K}}$ est isomorphe à un sous-groupe de $\text{Gal}_{P/K}$.*

Démonstration : Soient a_1, \dots, a_n les racines de P dans un corps de décomposition L de K . Soient b_1, \dots, b_n les racines de \bar{P} dans un corps de décomposition \bar{L} de \bar{K} .

Soient $F(u, T) := S(u, a_1, \dots, a_n, T) \in A[u, T]$, $\bar{F}(u, T) := S(u, b_1, \dots, b_n, T) \in \bar{A}[u, T]$. Ce sont des polynômes séparables : en effet, les racines b_i sont 2 à 2 distinctes donc les racines de \bar{F} aussi ; de même pour F . De plus, \bar{F} est la réduction de $F \pmod{\mathfrak{p}}$. En effet, $S(u, y, T) \in \mathbb{Z}[u, \sigma_1, \dots, \sigma_n, T]$ où les σ_i sont les fonctions symétriques élémentaires en les y_i . Si $P = T^n - \lambda_1 T^{n-1} + \dots + (-1)^n \lambda_n$, F est le polynôme obtenu à partir de $S(u, y, T) \in \mathbb{Z}[u, \sigma_1, \dots, \sigma_n, T]$ en remplaçant σ_i par λ_i . De même pour \bar{F} avec $\lambda_i \pmod{\mathfrak{p}}$ à la place de λ_i .

Q.e.d.

Application : Soit $P \in \mathbb{Z}[T]$ un polynôme séparable. Soit p un nombre premier. On suppose que $P \pmod{p}$ est séparable sur \mathbb{F}_p . Soit $\bar{P} = \phi_1 \dots \phi_r$ la décomposition en facteurs irréductibles dans $\mathbb{F}_p[T]$. Alors le groupe de Galois de P sur \mathbb{Q} contient un $\sigma = c_1 \dots c_r$ où les c_i sont des cycles à supports disjoints de longueurs respectives les $\deg \phi_i$. En effet soit \bar{G} le groupe de Galois de \bar{P} sur \mathbb{F}_p . C'est un groupe cyclique ; soit c un générateur. Pour tout i , l'action de c sur l'ensemble des racines de ϕ_i est transitive. Donc c est un produit de s cycles à supports disjoints de longueurs respectives les $\deg \phi_i$.

Exemple : $T^5 - T - 1 = (T^2 + T + 1)(T^3 + T^2 + 1) \pmod{2}$, est irréductible mod 3 donc son groupe de Galois G , vu comme sous-groupe de \mathfrak{S}_5 contient un 5-cycle et un produit d'un 3-cycle et d'une transposition : c'est \mathfrak{S}_5 .

Exercice : Montrer que le groupe de Galois sur \mathbb{Q} de $X^5 + 20X + 16$ est $\simeq \mathfrak{A}_5$.

12 Cohomologie galoisienne

12.1 G -modules

Soit G un groupe fini. Un G -module est un groupe abélien A sur lequel G opère et tel que :

- (i) $1a = a$;
- (ii) $s(a + b) = sa + sb$;
- (iii) $(st)a = s(ta)$;

pour tous $a, b \in A$, $s, t \in G$.

Si A, B sont des G -modules, on dit qu'une application $f : A \rightarrow B$ est un G -morphisme si $\forall g \in G, \forall a \in A, f(ga) = gf(a)$.

Remarque : si $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ est une suite exacte, alors la suite $0 \rightarrow A^G \rightarrow B^G \rightarrow C^G$ est exacte.

12.2 Groupes de cohomologie

12.2.1 En degré 1

On note $Z^1(G, A) := \{f : G \rightarrow A : \forall s, t \in G, f(st) = f(s) + sf(t)\}$.

Si $a \in A$, on note : $f_a : G \rightarrow A, g \mapsto ga - a$ et $B^1(G, A) := \{f_a : a \in A\}$.

On pose ensuite : $H^1(G, A) := Z^1(G, A)/B^1(G, A)$.

Exercice : soient G un groupe cyclique et A un G -module. Soit s un générateur de G . On pose :

$$N_G : A \rightarrow A, a \mapsto \sum_{i=0}^{|G|-1} s^i a .$$

Montrer que $H^1(G, A) \simeq \ker N_G / (s-1)(A)$ (indication : si $N_G x = 1$, considérer le 1-cocycle : $z_x : s^i \mapsto (1 + \dots + s^{i-1})(x)$.)

Théorème 12.1 (90 de Hilbert) Soit L/K une extension galoisienne. On a :

$$H^1(G(L/K), L^\times) = 1$$

où $G(L/K) = \text{Gal}(L/K)$.

Démonstration : Soit $f \in Z^1(G(L/K), L^\times)$. D'après le théorème d'indépendance des caractères, il existe un $x \in L$ tel que $y := \sum_{g \in G} f(g)^g x \neq 0$. Alors $f = f_{y^{-1}}$. **Q.e.d.**

Corollaire 12.1.1 On retrouve le théorème 90 de Hilbert si L/K est cyclique.

Démonstration : Il suffit d'appliquer le théorème et l'exercice ci-dessus. **Q.e.d.**

Soit $f : A \rightarrow B$ un morphisme de G -modules. Si $c \in Z^1(G, A)$, alors $f \circ c \in Z^1(G, B)$. De même, si $b \in B^1(G, A)$, alors $b \circ c \in B^1(G, B)$. On en déduit un morphisme : $H^1(f) : H^1(G, A) \rightarrow H^1(G, B) : c \bmod B^1(G, A) \mapsto f \circ c \bmod B^1(G, B)$.

Proposition 12.2 Si $0 \rightarrow A \xrightarrow{i} B \xrightarrow{j} C \rightarrow 0$ est une suite exacte*, alors il existe un morphisme $\delta : C^G \rightarrow H^1(G, A)$ telle que la suite $0 \rightarrow A^G \xrightarrow{i} B^G \xrightarrow{j} C^G \xrightarrow{\delta} H^1(G, A) \xrightarrow{H^1(i)} H^1(G, B) \xrightarrow{H^1(j)} H^1(G, A)$ est exacte.

*. i.e. i est injective, $\text{im } i = \ker j$ et j est surjective.

Démonstration : On définit δ : soit $c \in C^G$. Il existe $b \in B$ tel que $c = j(b)$. Alors, $\forall s \in G$, $j(sb - b) = sc - c = 0$. Donc il existe $a \in A$ tel que $sb - b = i(a)$. On pose $f : G \rightarrow A$, $s \mapsto sb - b$ et $\delta(c) := f \bmod B^1(G, A)$.
Q.e.d.

COURS DU 17 AVRIL

12.2.2 En tout degré

Si $n \geq 0$, on pose :

$$C^n(G, A) := \{f : G^n \rightarrow A\}$$

c'est un groupe abélien (addition point par point) qu'on appelle le groupe des n -cocycles. Si $n < 0$, on pose $C^n(G, A) := 0$.

Définition 1 Soit $n \geq 0$. Soit $f \in C^n(G, A)$. Pour tous $g_1, \dots, g_{n+1} \in G$, on pose :

$$d^n(f)(g_1, \dots, g_{n+1}) := g_1 f(g_2, \dots, g_{n+1}) + \sum_{i=1}^n (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) + (-1)^{n+1} f(g_1, \dots, g_n) .$$

On obtient un morphisme $d^n : C^n(G, A) \rightarrow C^{n+1}(G, A)$ pour tout n (si $n < 0$, $d^n = 0$).

Proposition 12.3 Pour tout n , $d^n d^{n-1} = 0$.

Démonstration : Posons $\partial^i f(g_1, \dots, g_{n+1}) := \begin{cases} g_1 f(g_2, \dots, g_{n+1}) & \text{si } i = 0 ; \\ f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) & \text{si } 1 \leq i \leq n ; \\ f(g_1, \dots, g_n) & \text{si } i = n + 1 ; \end{cases}$

On a alors :

$$\begin{aligned} d^n d^{n-1} f(g_1, \dots, g_{n+1}) &= \sum_{i=0}^{n+1} (-1)^i \partial^i d^{n-1} f(g_1, \dots, g_{n+1}) \\ &= \sum_{i=0}^{n+1} \sum_{j=0}^n (-1)^{i+j} \partial^i \partial^j f(g_1, \dots, g_{n+1}) . \end{aligned}$$

Or, si $j < i$, on a : $\partial^i \partial^j = \partial^j \partial^{i-1}$. Donc :

$$d^n d^{n-1} f(g_1, \dots, g_{n+1}) = \sum_{\substack{0 \leq i \leq n+1 \\ 0 \leq j \leq n \\ j < i}} (-1)^{i+j} \partial^i \partial^j + \sum_{\substack{0 \leq i \leq n+1 \\ 0 \leq j \leq n \\ i \leq j}} (-1)^{i+j} \partial^i \partial^j$$

$$\begin{aligned}
& \sum_{\substack{0 \leq i \leq n+1 \\ 0 \leq j \leq n \\ j < i}} (-1)^{i+j} \partial^j \partial^{i-1} + \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq n \\ i \leq j}} (-1)^{i+j} \partial^i \partial^j \\
& \sum_{\substack{0 \leq i' \leq n \\ 0 \leq j' \leq n \\ i' \leq j'}} (-1)^{i'+j'-1} \partial^{i'} \partial^{j'} + \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq n \\ i \leq j}} (-1)^{i+j} \partial^i \partial^j \\
& = 0 .
\end{aligned}$$

Q.e.d.

Définition 2 (cocycles, cobords et cohomologie) *Le groupe $Z^n(G, A) := \ker d^n$ est le groupe des n -cocycles et $B^n(G, A) := \text{im}(d^{n-1})$ celui des n -cobords. Le groupe $H^n(G, A) := Z^n(G, A)/B^n(G, A)$ est le n -ième groupe de cohomologie.*

Exercice : $H^0(G, A) = A^G$ et on retrouve la définition de $H^1(G, A)$ précédente.

Soit $f : A \rightarrow B$ un morphisme de G -modules. Le morphisme f induit des morphismes $f^n : C^n(G, A) \rightarrow C^n(G, B)$ qui « commutent aux d^n ». en particulier on obtient des morphismes $H^n(f) : H^n(G, A) \rightarrow H^n(G, B)$.

Proposition 12.4 (suite exacte longue de cohomologie) *Soit $0 \rightarrow A \xrightarrow{i} B \xrightarrow{j} C \rightarrow 0$ une suite exacte de G -modules. On a une suite exacte :*

$$\begin{aligned}
0 \rightarrow H^0(G, A) \xrightarrow{H^0(i)} H^0(G; B) \xrightarrow{H^0(j)} H^0(G, C) \xrightarrow{\delta^0} H^1(G, A) \xrightarrow{H^1(i)} H^1(G, B) \rightarrow \dots \\
\rightarrow H^n(G, A) \xrightarrow{H^n(i)} H^n(G; B) \xrightarrow{H^n(j)} H^n(G, C) \xrightarrow{\delta^n} H^{n+1}(G, A) \rightarrow \dots
\end{aligned}$$

COURS DU 17 AVRIL

13 Théorie de Kummer

L'objectif est de généraliser la bijection suivante :

$$\left\{ \text{extensions } \mathbb{Q} \leq K \leq \overline{\mathbb{Q}} \atop [K:\mathbb{Q}] \leq 2 \right\} \xleftrightarrow{1:1} \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$$

$$d \in \mathbb{Z} \text{ sans facteur carré} \xrightarrow{\mathbb{Q}(\sqrt{d})} d \bmod (\mathbb{Q}^\times)^2.$$

Soit K un corps contenant le groupe μ_n des racines n -ièmes de l'unité. On suppose que la caractéristique de K est nulle ou première à n . Soit

$(K^\times)^n \leq C \leq K^\times$ un sous-groupe tel que $C/(K^\times)^n$ soit fini. Pour tout $c \in K^\times$, l'extension $K(c^{1/n})/K$ est cyclique d'ordre un diviseur de n (cf. le théorème de Kummer 9.2). On pose $L := K(C^{1/n})$ le corps engendré par les $K(c^{1/n})$ (dans une certaine extension algébriquement close Ω de K fixée). On a un morphisme injectif de groupes :

$$G_C := \text{Gal}(L/K) \rightarrow \prod_{c \in C/(K^\times)^n} \text{Gal}(K(c^{1/n})/K) .$$

En particulier, l'extension L/K est abélienne.

Proposition 13.1 *L'application :*

$$\langle \cdot, \cdot \rangle : G_C \times C/(K^\times)^n \rightarrow \mu_n(s, c) \mapsto \langle s, c \rangle := s(c^{1/n})/c^{1/n}$$

est bimultiplicative et non dégénérée i.e. induit des isomorphismes :

$$\begin{aligned} G_C &\rightarrow \text{Hom}(C/(K^\times)^n, \mu_n) \\ C/(K^\times)^n &\rightarrow \text{Hom}(G_C, \mu_n) . \end{aligned}$$

Démonstration :

Soit $G := \text{Gal}(L/K)$. Soit $C = (L^\times)^n \cap K^\times$. La suite exacte courte $1 \rightarrow \mu_n \rightarrow L^\times \rightarrow (L^\times)^n \rightarrow 1$ induit une suite exacte :

$$1 \rightarrow \mu_n \rightarrow (L^\times)^G \cap K^\times \rightarrow (L^\times)^{nG} = C \rightarrow H^1(G, \mu_n) = \text{Hom}(G, \mu_n) \rightarrow H^1(G, L^\times) = 1.$$

Q.e.d.

Lemme 13.2 *Soit L/K une extension abélienne d'exposant un diviseur de n . Il existe $c_1, \dots, c_l \in K^\times$ tel que L soit le corps de décomposition du polynôme :*

$$(X^n - c_1) \dots (X^n - c_l) .$$

Démonstration : On raisonne par récurrence sur le degré $[L : K]$. Soit $G := \text{Gal}(L/K)$. Si G est cyclique on applique le théorème de Kummer 9.2. Sinon, il existe $H_1, H_2 < G$ tels que $G = H_1 H_2 \simeq H_1 \times H_2$. Alors $L = L_1 L_2$ avec $L_i := L^{H_i}$. On applique l'hypothèse de récurrence à L_1/K et L_2/K .

Q.e.d.

Corollaire 13.2.1 *Soit K un corps contenant le groupe μ_n des racines n -ièmes de l'unité. On suppose que la caractéristique de K est nulle ou première à n . On a deux bijections réciproques l'une de l'autre :*

$$\begin{array}{ccc} L^n \cap K^\times & \left\{ \begin{array}{l} \text{Sous-groupes } (K^\times)^n \leq C \leq K^\times \\ \text{tels que } C/(K^\times)^n \text{ est fini} \end{array} \right\} & C \\ \uparrow \Psi & \updownarrow \Psi, \Phi & \downarrow \Phi \\ \underline{L} & \left\{ \begin{array}{l} \text{extensions abéliennes finies} \\ \text{d'exposant un diviseur de } n \end{array} \right\} & K(C^{1/n}) \end{array}$$

14 Extensions d'Artin-Schreier

14.1 Forme additive du théorème 90 de Hilbert

Soit L/K une extension galoisienne de groupe de Galois G .

Théorème 14.1 $H^n(G, L) = \begin{cases} L^G = K & \text{si } n = 0; \\ 0 & \text{si } n > 0. \end{cases}$

Démonstration : Montrons que $H^1(G, L) = 0$. Soit $a \in L$ tel que $\text{Tr}_{L/K}(a) = 1$. Soit $f \in Z^1(G, L)$. On pose $b := \sum_{g \in G} f(g)^g a \in L$. Pour tout $\sigma \in G$, ${}^\sigma b = b - f(\sigma)$. Q.e.d.

Corollaire 14.1.1 Si L/K est cyclique et si σ est un générateur de $\text{Gal}(L/K)$, alors si $x \in L$, on a :

$$\text{Tr}_{L/K}(x) = 0 \Leftrightarrow \exists y \in L, x = {}^\sigma y - y .$$

Démonstration : L'application $\text{Gal}(L/K) \rightarrow L, \sigma^i \mapsto (1 + \dots + \sigma^{i-1})(x)$ est un 1-cocycle. Q.e.d.

14.2 Théorie des extensions d'exposant p en caractéristique p

Soit K un corps de caractéristique p .

Lemme 14.2 Si $c \in K$, alors le polynôme $X^p - X - c \in K[X]$ est séparable et scindé sur K ou séparable et irréductible sur K de groupe de Galois $\simeq \mathbb{Z}/p\mathbb{Z}$.

Démonstration : Si a est une racine de $X^p - X - c$, alors les autres racines sont les $a + i, i \in \mathbb{F}_p$. Q.e.d.

Soit \overline{K} une clôture algébrique de K . Soient $c_1, \dots, c_n \in K$. Pour tout i , soit L_i le corps de décomposition sur K (dans \overline{K}) des polynômes $X^p - X - c_i$. Soit $L = L_1 \dots L_n$. On a un morphisme injectif de groupes :

$$\text{Gal}(L/K) \rightarrow \prod_{i=1}^n \text{Gal}(L_i/K)$$

donc $\text{Gal}(L/K)$ est abélien fini d'exposant p .

Posons $\phi : \overline{K} \rightarrow \overline{K}, x \mapsto x^p - x$. Soit C un sous-groupe de K tel que $\phi(K) \leq C \leq K$ et $C/\phi(K)$ est fini. Notons $L := K(\phi^{-1}(C))$ l'extension galoisienne engendré par les racines de $X^p - X - c, c \in C$ et $G_C := \text{Gal}(K(\phi^{-1}(C))/K)$.

On considère :

$$G_C \times C \rightarrow \mathbb{F}_p, \sigma, c \mapsto \langle \sigma, c \rangle := \sigma(\phi^{-1}(c)) - \phi^{-1}(c) .$$

Proposition 14.3 *L'application $\langle \cdot, \cdot \rangle$ est biadditive et induit des isomorphismes de groupes :*

$$G_C \rightarrow \text{Hom}(C/\phi(K), \mathbb{F}_p)$$

$$C/\phi(K) \rightarrow \text{Hom}(G_C, \mathbb{F}_p) .$$

Corollaire 14.3.1 *On a deux bijections réciproques l'une de l'autre :*

$$\begin{array}{ccc}
 \phi(L) \cap K & \left\{ \begin{array}{l} \text{Sous-groupes } \phi(K) \leq C \leq K \\ \text{tels que } C/\phi(K) \text{ est fini} \end{array} \right\} & C \\
 \uparrow \Psi & \Psi \updownarrow \Phi & \downarrow \Phi \\
 L & \left\{ \begin{array}{l} \text{extensions abéliennes finies} \\ \text{d'exposant un diviseur de } p \end{array} \right\} & K(\phi^{-1}(C))
 \end{array}$$

Démonstration : La suite exacte $0 \rightarrow \mathbb{F}_p \rightarrow L \rightarrow \phi(L) \rightarrow 0$ induit une suite exacte :

$$K \xrightarrow{\phi} K \cap \phi(L) \rightarrow H^1(\text{Gal}(L/K), \mathbb{F}_p) \rightarrow 0$$

Or, $H^1(\text{Gal}(L/K), \mathbb{F}_p) = \text{Hom}(\text{Gal}(L/K), \mathbb{F}_p)$ car $\text{Gal}(L/K)$ agit trivialement sur \mathbb{F}_p . **Q.e.d.**

Remarque : en particulier, si L/K est galoisienne de degré p , alors il existe $x \in L \setminus K$, $c \in K$ tels que $x^p - x = c$.

14.3 Théorème d'Artin-Schreier

Il n'existe pas de sous-corps F de \mathbb{C} tel que $[\mathbb{C} : F] = 3$. En effet, on a le :

Théorème 14.4 *Soit Ω un corps algébriquement clos. Soit $F \leq \Omega$ un sous-corps tel que $1 < [\Omega : F] < \infty$. Alors F est de caractéristique nulle, $\Omega = F(i)$ pour un i tel que $i^2 = -1$. En particulier $[\Omega : F] = 2$. De plus, si $a \in F^\times$, il y a un unique carré parmi $a, -a$ et toute somme finie non vide de carrés non nuls est encore un carré non nul dans F^\times .*

Lemme 14.5 *Soit F un corps de caractéristique p . Si $a \in F \setminus F^p$, alors pour tout $m \geq 1$, $X^{p^m} - a$ est irréductible dans $F[X]$ pour tout $m \geq 1$.*

Lemme 14.6 Soit F un corps où -1 n'est pas un carré (en particulier, F est de caractéristique $\neq 2$) et tel que chaque élément de $F(\sqrt{-1})$ est un carré. Alors une somme finie de carrés dans F est un carré dans F et F est de caractéristique 0.

Démonstration : Si $(a + \sqrt{-1}b) = (c + \sqrt{-1}d)^2$, alors $a^2 + b^2 = (c^2 + d^2)^2$. Q.e.d.

Démonstration du théorème : Si K est de caractéristique p et si $[\Omega : F] = p$, alors $F = F^p$ d'après le lemme 14.5 donc Ω/F est séparable. Dans tous les cas, Ω/F est galoisienne. Si $[\Omega : F] \neq 2$, on peut supposer que $[\Omega : F] = p$ un nombre premier impair ou 4. Dans le premier cas, si $\text{car}(F) \neq p$, d'après le théorème de Kummer, $\Omega = F(\alpha)$ pour un certain α tel que $\alpha^p = a \in F$. On a alors $N_{\Omega/F}(\alpha) = (-1)^{p+1}a$. Soit $\beta \in \Omega$ tel que $\beta^p = \alpha$. on a $N(\beta)^p = a$ absurde ! Si $\text{car}(F) = p$, alors $\Omega = F(\alpha)$ pour un $\alpha \in \Omega$ tel que $\alpha^p - \alpha = a \in F$. Mais alors en considérant un $\beta \in \Omega$ tel que $\beta^p - \beta = a\alpha^{p-1}$, on obtient $\lambda_{p-1}^p - \lambda_{p-1} = a$ où $\beta = \lambda_0 + \dots + \lambda_{p-1}\alpha^{p-1}$ pour certains $\lambda_i \in F$: absurde ! car $X^p - X - a$ est irréductible sur F

Si $[\Omega : F] = 4$, on peut trouver $\Omega \geq K \geq F$ tel que $[\Omega : K] = 2$. On a $\text{car}(F) \neq 2$ comme ci-dessus et en raisonnant avec la norme comme précédemment, on voit que $i \notin K$. En raisonnant avec $F(i)$ à la place de K , on trouve $i \notin F(i)$ absurde ! Q.e.d.