

Théorie de Galois

Alexis TCHOUDJEM

Institut Camille Jordan

Université Claude Bernard Lyon I

Boulevard du Onze Novembre 1918

69622 Villeurbanne

FRANCE

Villeurbanne, le 24 octobre 2017

Cours du mercredi 20/1/15

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 : Vérifier que $2 \cos(2\pi/5) = \frac{-1+\sqrt{5}}{4}$ et $2 \sin(2\pi/5) = \sqrt{\frac{5-\sqrt{5}}{2}}$.

0.2 Méthode de Lagrange

0.2.1 Degré 3

Soit $P(X) := X^3 + pX + q \in \mathbb{C}[X]$. On note r_1, r_2, r_3 ses racines.

On pose $a := r_1 + jr_2 + j^2r_3$. Si on applique tous les $s \in \mathfrak{S}_3$ à a^3 , on obtient seulement deux valeurs :

$$a^3 \text{ et } b^3$$

où $b = r_1 + j^2r_2 + jr_3$.

Donc $(X - a^3)(X - b^3)$ s'exprime simplement en fonction de p, q .

Explicitement :

$$(X - a^3)(X - b^3) = X^2 + 27qX - 27p^3$$

Ce polynôme a pour discriminant $\Delta = 4 \cdot (27)^2 \left(\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 \right)$.

Remarque : on a aussi $ab = -3p$.

On peut exprimer r_1, r_2, r_3 en fonction de a, b :

$$r_1 = \frac{a+b}{3}, r_2 = \frac{j^2a+jb}{3}, r_3 = \frac{ja+j^2b}{3},$$

Réciproquement, soient a, b des racines cubiques :

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

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

telles que $ab = -3p$.

Exercice : vérifier que c'est possible!

Alors si on pose :

$$r_1 = \frac{a+b}{3}, r_2 = \frac{j^2a+jb}{3}, r_3 = \frac{ja+j^2b}{3}$$

on a bien $(X - r_1)(X - r_2)(X - r_3) = X^3 + pX + q$.

On a donc bien résolu notre équation avec des radicaux.

Exemples :

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

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

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

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

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

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

0.2.2 Degré 4

Il y a aussi des formules avec des radicaux mais qui prennent beaucoup de places ...

Soient $p, q, r \in \mathbb{C}$.

On note r_1, r_2, r_3, r_4 les racines du polynôme $P := X^4 + pX^2 + qX + r$
i.e. :

$$P(X) = (X - r_1)(X - r_2)(X - r_3)(X - r_4) .$$

On pose $t_1 := (r_1 + r_2)(r_3 + r_4)$, $t_2 := (r_1 + r_3)(r_2 + r_4)$, $t_3 := (r_1 + r_4)(r_2 + r_3)$. On a alors :

$$R(X) := (X - t_1)(X - t_2)(X - t_3) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2 .$$

Remarque : $(t_1 - t_2)^2(t_2 - t_3)^2(t_1 - t_3)^2 = (r_1 - r_2)^2(r_2 - r_3)^2(r_3 - r_4)^2(r_1 - r_3)^2(r_2 - r_4)^2(r_1 - r_4)^2 = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$.

Comme $r_1 + r_2 + r_3 + r_4 = 0$, on a aussi :

$$(r_1 + r_2)^2 = -t_1, (r_1 + r_3)^2 = -t_2, (r_1 + r_4)^2 = -t_3 .$$

On peut donc retrouver r_1, r_2, r_3, r_4 à partir de t_1, t_2, t_3 .
On choisit des racines carrées des $-t_i$ de sorte que :

$$r_1 + r_2 = \sqrt{-t_1}, \quad r_1 + r_3 = \sqrt{-t_2}, \quad r_1 + r_4 = \sqrt{-t_3} .$$

Remarque : on a forcément $\sqrt{-t_1}\sqrt{-t_2}\sqrt{-t_3} = -q$.

On a alors :

$$\begin{aligned} r_1 &= \frac{\sqrt{-t_1} + \sqrt{-t_2} + \sqrt{-t_3}}{2} \\ r_2 &= \frac{\sqrt{-t_1} - \sqrt{-t_2} - \sqrt{-t_3}}{2} \\ r_3 &= \frac{-\sqrt{-t_1} + \sqrt{-t_2} - \sqrt{-t_3}}{2} \\ r_4 &= \frac{-\sqrt{-t_1} - \sqrt{-t_2} + \sqrt{-t_3}}{2} . \end{aligned}$$

Réciproquement, si on note t_1, t_2, t_3 les racines du polynôme :

$$R(X) := X^3 - 2pX^2 + (p^2 - 4r)X + q^2$$

si on choisit trois racines carrées $\sqrt{-t_1}, \sqrt{-t_2}, \sqrt{-t_3}$ telles que $\sqrt{-t_1}\sqrt{-t_2}\sqrt{-t_3} = -q$, et si on pose :

$$\begin{aligned} r_1 &:= \frac{\sqrt{-t_1} + \sqrt{-t_2} + \sqrt{-t_3}}{2} \\ r_2 &:= \frac{\sqrt{-t_1} - \sqrt{-t_2} - \sqrt{-t_3}}{2} \\ r_3 &:= \frac{-\sqrt{-t_1} + \sqrt{-t_2} - \sqrt{-t_3}}{2} \\ r_4 &:= \frac{-\sqrt{-t_1} - \sqrt{-t_2} + \sqrt{-t_3}}{2} , \end{aligned}$$

alors :

$$X^4 + pX^2 + qX + r = (X - r_1)(X - r_2)(X - r_3)(X - r_4) .$$

On a donc résolu notre équation par des radicaux.

0.3 Autres méthodes

0.3.1 Cardan

Pour résoudre $x^3 + px + q = 0$, on peut utiliser la méthode de Cardan qui est facile à retenir (ou à retrouver) :

On cherche une racine sous la forme $x = u + v$:

$$(u + v)^3 + p(u + v) + q = 0 \Leftrightarrow u^3 + v^3 + (u + v)(3uv + p) + q = 0 .$$

Ça se simplifie si on impose $3uv = -p$:

$$u^3 + v^3 + q = 0 .$$

Donc si u, v vérifient

$$\begin{cases} u^3 + v^3 = -q \\ uv = -p/3 \end{cases}$$

alors $u + v, ju + j^2v, j^2u + jv$ sont racines. Plus précisément :

$$X^3 + pX + q = (X - (u + v))(X - (ju + j^2v))(X - (j^2u + jv))$$

où u^3, v^3 sont des racines de $T^2 + qT - p^3/27$ telles que $uv = -p/3$.

0.3.2 Euler

Pour résoudre $x^4 + px^2 + qx + r$ Euler procède ainsi :

On cherche une racine sous la forme $x = \sqrt{u} + \sqrt{v} + \sqrt{w}$.

Or,

$$x = \sqrt{u} + \sqrt{v} + \sqrt{w} \Rightarrow x^2 - u - v - w = 2(\sqrt{u}\sqrt{v} + \sqrt{u}\sqrt{w} + \sqrt{v}\sqrt{w})$$

$$\Rightarrow x^4 - 2(u+v+w)x^2 + (u+v+w)^2 = 4(uv+uw+vw) + 8(\sqrt{u}+\sqrt{v}+\sqrt{w})\sqrt{u}\sqrt{v}\sqrt{w}$$

Donc :

$$x^4 + px^2 + qx + r = (p + 2(u+v+w))x^2 + (q + 8\sqrt{u}\sqrt{v}\sqrt{w})x + r - (u+v+w)^2 + 4(uv+uw+vw).$$

Par conséquent :

$$x^4 + px^2 + qx + r = 0 \iff \begin{cases} u + v + w = -p/2 \\ \sqrt{u}\sqrt{v}\sqrt{w} = -q/8 \\ -(u + v + w)^2 + 4(uv + uw + vw) = -r \end{cases}$$

$$\iff \begin{cases} u + v + w = -p/2 \\ \sqrt{u}\sqrt{v}\sqrt{w} = -q/8 \\ (uv + uw + vw) = \frac{(p/2)^2 - r}{4} \end{cases}$$

Il suffit donc de trouver (*) u, v, w trois racines du polynôme $T^3 + \frac{p}{2}T^2 + \frac{(p/2)^2 - r}{4}T - (\frac{q}{8})^2$ et trois racines carrées $\sqrt{u}, \sqrt{v}, \sqrt{w}$ telles que $\sqrt{u}\sqrt{v}\sqrt{w} = -q/8$.

On a ainsi résolu l'équation $x^4 + px^2 + qx + r = 0$ car on peut vérifier que si u, v, w et $\sqrt{u}, \sqrt{v}, \sqrt{w}$ vérifient (*), alors :

$$\begin{aligned} & x^4 + px^2 + qx + r = \\ & (x - (\sqrt{u} + \sqrt{v} + \sqrt{w}))(x - (\sqrt{u} - \sqrt{v} - \sqrt{w}))(x - (-\sqrt{u} + \sqrt{v} - \sqrt{w}))(x - (-\sqrt{u} - \sqrt{v} + \sqrt{w})). \end{aligned}$$

0.4 Degré ≥ 5

On a : $x^5 - 2 = (x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5)$ où $x_k = \sqrt[5]{2}(\cos(2k\pi/5) + i \sin(2k\pi/5)) = \sqrt[5]{2} \left(\frac{1+\sqrt{5}}{4} + \frac{\sqrt{-1}}{2} \sqrt{\frac{5-\sqrt{5}}{2}} \right)^k$. Donc $x^5 - 2 = 0$ est une équation « résoluble par radicaux ».

En revanche nous verrons plus tard que l'équation $x^5 - x - 1 = 0$ n'est pas résoluble par radicaux.

0.5 Caractéristique

Soit K un corps.

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

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

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

0.6 Polynômes symétriques

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

On note $\sigma_k(X_1, \dots, X_n) := \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}$ les *polynômes symétriques élémentaires*. On peut aussi les définir aussi par l'égalité :

$$(T - X_1) \dots (T - X_n) = T^n - \sigma_1 T^{n-1} + \dots + (-1)^n$$

dans $K[X_1, \dots, X_n][T]$.

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

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

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

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

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

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

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

conséquence : si par exemple $P(X) = X^n + a_1X^{n-1} + \dots + a_n \in \mathbb{Z}[X]$ si on note $r_1, \dots, r_n \in \mathbb{C}$ ses racines, alors tout polynôme $f \in \mathbb{Z}[X_1, \dots, X_n]$ symétrique vérifie $f(r_1, \dots, r_n) \in \mathbb{Z}$.

Exercice : $X^n - X - 1$ est irréductible sur \mathbb{Q} pour tout $n \geq 2$.

Exercice :

- soit $P(X) := X^3 + pX + q = (X - r_1)(X - r_2)(X - r_3)$. Montrer que $(r_1 - r_2)^2(r_2 - r_3)^2(r_1 - r_3)^2 = -4p^3 - 27q^2$;
- soit $P(X) := X^3 + a_1X^2 + a_2X + a_3 = (X - r_1)(X - r_2)(X - r_3)$, alors $(r_1 - r_2)^2(r_2 - r_3)^2(r_1 - r_3)^2 = a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3$
- soit $P(X) := X^4 + pX^2 + qX + r = (X - r_1)(X - r_2)(X - r_3)(X - r_4)$. Montrer que $(r_1 - r_2)^2(r_2 - r_3)^2(r_3 - r_4)^2(r_1 - r_3)^2(r_2 - r_4)^2(r_1 - r_4)^2 = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$.

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* et on le note parfois L/K .

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

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

Démonstration : Supposons $n = 3$. Soit $(x_i)_i$ une base de K_2 comme K_1 -espace vectoriel. Soit $(y_j)_j$ une base de K_3 comme K_2 -espace vectoriel. Alors $(x_i y_j)_{i,j}$ est une base de K_3 comme K_1 -espace vectoriel. **Q.e.d.**

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

1.3 Éléments algébriques

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

- (i) il existe $0 \neq P \in K[X]$ tel que $P(x) = 0$;
- (ii) $\dim_K K[x]$ est finie;
- (iii) $K[x] = K(x)$.

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

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

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

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

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

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

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

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

COURS DU MARDI 27 JANVIER 2015

Rappels sur les morphismes de corps

Soient K, L deux corps. Une application $\phi : K \rightarrow L$ est un morphisme de corps si $\forall x, y \in K$, $\phi(x + y) = \phi(x) + \phi(y)$, $\phi(xy) = \phi(x)\phi(y)$, $\phi(1) = 1$.

Exercice : tout morphisme de corps est injectif!

Exercice : $\text{Aut}(\mathbb{Q}) = \{\text{Id}\}$, $\text{Aut}(\mathbb{R}) = \{\text{Id}\}$, $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})) = \{\text{Id}\}$, $\text{Aut}(\mathbb{Q}(\sqrt{2})) = \{\text{Id}, \sigma : \sqrt{2} \mapsto -\sqrt{2}\}$, $\text{Aut}(\mathbb{Q}(\sqrt[4]{2})) = \{\text{Id}, \tau : \sqrt[4]{2} \mapsto -\sqrt[4]{2}\}$.

1.4 Corps de rupture

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

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

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

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

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

Corollaire 1.6.1 *Si $P \in K[X]$ est irréductible, il existe toujours un corps de rupture de P sur K , unique à isomorphisme près.*

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 :

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

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

1.5 Corps de décomposition

Soit $0 \neq P \in K[X]$. On suppose que $E \geq K$ est un corps où P est scindé : $P = c(X - x_1)\dots(X - x_n)$, $c \in K^\times$. On dit que $K(x_1, \dots, x_n)$ est le *corps de décomposition* de P dans E .

Proposition 1.7 *Un corps de décomposition existe toujours.*

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

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

Théorème 1.8 (prolongement d'isomorphisme) *Soit $\sigma : K \rightarrow K'$ 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 des extensions de K, K' , alors σ se prolonge en un isomorphisme $K(\alpha) \simeq K'(\alpha')$ qui envoie α sur α' .*

Théorème 1.9 (unicité du corps de décomposition) Soit $\sigma : K \rightarrow K'$ 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 1.9.1 Soient L, L' deux corps de décomposition de P sur K . Alors il existe un K -isomorphisme $L \simeq L'$.

Exemples : soient q une puissance d'un nombre premier p ; le corps \mathbb{F}_q est un corps de décomposition de $X^q - X$ sur \mathbb{F}_p et on a donc l'unicité à isomorphisme près des corps finis de cardinaux donnés.

Définition 2 On dit qu'un corps K est algébriquement clos si tout polynôme non constant est scindé sur K .

Théorème 1.10 Soit K un corps. Il existe une extension algébrique \overline{K} de K qui est un corps algébriquement clos. C'est une clôture algébrique de K . L'extension \overline{K} est unique à K -isomorphisme près.

Démonstration :

Existence : soit \mathcal{P} l'ensemble des polynômes irréductibles unitaires de $K[X]$. Pour tout $p \in \mathcal{P}$, on choisit une variable X_p . Soit $A := K[X_p : p \in \mathcal{P}]$. Soit I l'idéal de A engendré par les polynômes $p(X_p)$, $p \in \mathcal{P}$. Alors I est propre donc contenu dans un idéal maximal M . Le corps A/M est une extension algébrique de K et tout polynôme p irréductible sur K a une racine ($X_p \bmod M$) dans A/M . Cela suffit pour dire que A/M est algébriquement clos (comme nous le verrons plus tard) ...

Unicité : on utilise le lemme de Zorn ...

Q.e.d.

Exemples : \mathbb{C} (resp. $\overline{\mathbb{Q}}$ (resp. $\bigcup_{n \geq 1} \mathbb{C}((t^{1/n}))$)) est une clôture algébrique de \mathbb{R} (resp. de \mathbb{Q} (resp. de $\mathbb{C}((t))$)).

2 Théorème d'indépendance des caractères d'Artin

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 (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 $\sigma_1, \dots, \sigma_m$ m morphismes distincts $E \rightarrow E'$. Alors si $F := E^{\{\sigma_1, \dots, \sigma_m\}} := \{x \in E : \sigma_1(x) = \dots = \sigma_m(x)\}$, $[E : F] \geq m$.

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

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

Remarque : comme G contient l'identité, $E^G = \{x \in E : \forall g \in G, g(x) = x\}$.

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

Définition 3 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 .

Exemples : \mathbb{C}/\mathbb{R} , $\mathbb{F}_{q^n}/\mathbb{F}_q$, $\mathbb{Q}(\zeta)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{C}(X)/\mathbb{C}(X^3)$; *contre-exemple* : $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{F}_p(X)/\mathbb{F}_p(X^p)$, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$.

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

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 $F = E^G$, $G = \{\sigma_1, \dots, \sigma_n\}$. Soient g_1, \dots, g_n les éléments de G . Si e_1, \dots, e_{n+1} sont des éléments de E , alors les colonnes de la matrices $(g_i(e_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n+1}} \in \mathcal{M}_{n,n+1}$ sont liées. Donc $\forall i, \sum_j x_j g_i(e_j) = 0$ pour certains $x_j \in E$. D'où :

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

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

COURS DU MARDI 3 FÉVRIER 2015

Exemples :

- a) $k(x_1, \dots, x_n)^{\mathfrak{S}_n} = k(s_1, \dots, s_n)$ (où k est un corps et où les s_i sont les polynômes symétriques élémentaires) car $k(x_1, \dots, x_n) \geq k(x_1, \dots, x_n)^{\mathfrak{S}_n} \geq k(s_1, \dots, s_n)$ et $[k(x_1, \dots, x_n) : k(x_1, \dots, x_n)^{\mathfrak{S}_n}] = |\mathfrak{S}_n| = n! \geq [k(x_1, \dots, x_n) : k(s_1, \dots, s_n)]$,
- b) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est galoisienne de groupe de Galois $G := \langle s, t \rangle \simeq \mathfrak{S}_3$ où s est le $\mathbb{Q}(j)$ -automorphisme qui envoie $\sqrt[3]{2}$ sur $j\sqrt[3]{2}$ et t le $\mathbb{Q}(\sqrt[3]{2})$ -automorphisme qui envoie j sur j^2 ;
- c) soit G le sous-groupe des automorphismes de $\mathbb{C}(t)$ engendré par les changements de variables $t \mapsto t^{-1}$ et $t \mapsto 1 - t$. On vérifie que G est d'ordre 6, isomorphe à \mathfrak{S}_3 .

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

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

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

En déduire que l'extension :

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

est galoisienne de groupe de Galois S_3 .

Exercice : on pose $y_1 := x_1 + jx_2 + j^2x_3$, $y_2 := x_1 + j^2x_2 + jx_3$. Montrer que $\mathbb{C}(x_1, x_2, x_3)^{\mathfrak{A}_3} = \mathbb{C}(y_1^2/y_2, y_2^2/y_1, \sigma_1)$.

On peut retrouver les polynômes symétriques à partir des fractions rationnelles symétriques ...

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

- a) $[L_{i-1} : L_i] = i$ et $1, \dots, x_i^{i-1}$ est une base de L_{i-1}/L_i .
- b) $\{x_1^{a_1} \dots x_n^{a_n} : \forall i, a_i \leq i - 1\}$ est une base de $k(x_1, \dots, x_n)/L$.
- c) tout $g \in k[x_1, \dots, x_n]$ est une combinaison $k[s_1, \dots, s_n]$ -linéaire de monômes $x_1^{a_1} \dots x_n^{a_n} : \forall i, a_i \leq i - 1$.
- d) On retrouve que $k[x_1, \dots, x_n]^{\mathfrak{S}_n} = k[s_1, \dots, s_n]$.

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

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

3.2 Injectivité

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

3.3 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 $E^H = B$.

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

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

3.4 Théorème fondamental

Théorème 3.3 Soit E/F une extension galoisienne de groupe G .

i) On a 2 bijections réciproques :

$$\begin{aligned} \{H \leq G\} &\xleftrightarrow{1:1} \{F \leq B \leq E\} \\ H &\mapsto E^H \\ \text{Gal}(E/B) &\leftarrow B \end{aligned}$$

- 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, $\text{Gal}(B/F) \simeq G/\text{Gal}(E/B)$.

Démonstration : Si $\text{Gal}(E/B) \triangleleft G$, si $\sigma \in G$, alors $\sigma(B) = B$: en effet, $\text{Gal}(E/\sigma(B)) = \sigma \text{Gal}(E/B) \sigma^{-1} = \text{Gal}(E/B) \Rightarrow \sigma(B) = B$. Notons G' l'image du morphisme $\sigma \mapsto \sigma|_B$. On a $B^{G'} = F$. Réciproquement si B/F est galoisienne, alors pour tout $\sigma \in G$, $\sigma|_B \in \text{Gal}(B/F)$ (cf. le corollaire 3.1.1). On a alors $\text{Gal}(E/B) = \ker(G \rightarrow \text{Gal}(B/F), \sigma \mapsto \sigma|_B)$ qui est un noyau donc distingué. **Q.e.d.**

Proposition 3.4 Soit E/K une extension galoisienne. On suppose que $K \leq B \leq B' \leq E$. On note $U := \text{Gal}(E/B)$, $U' := \text{Gal}(E/B')$. Alors B'/B est galoisienne $\Leftrightarrow U' \triangleleft U$. Et dans ce cas, $\text{Gal}(B'/B) \simeq U/U'$.

Exercice : démontrer cette proposition.

3.5 Caractérisation des extensions galoisiennes

Théorème 3.5 Soit E/K une extension finie. On a toujours : $|\text{Aut}_K(E)| \leq [E : K]$. L'extension E/K est galoisienne $\Leftrightarrow |\text{Aut}_K(E)| = [E : K]$. Dans ce cas, $\text{Gal}(E/K) = \text{Aut}(E/K)$.

Contre-exemples :

- a) si $E = \mathbb{Q}(\sqrt[4]{2})$, alors $|\text{Aut}(E/\mathbb{Q})| = 2 < 4 = [E : \mathbb{Q}]$.
- b) si p est premier et $E = \mathbb{F}_p(T)$ et $K = \mathbb{F}_p(T^p)$; alors $[\mathbb{F}_p(T) : \mathbb{F}_p(T^p)] = p$ mais $\text{Aut}_{\mathbb{F}_p(T^p)}(\mathbb{F}_p(T)) = \{\text{Id}\}$.

3.6 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). Dans ce cas, on dit que P est un *polynôme séparable*

Définition 4 (séparable) 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 3.6 Si $P \in K[X]$ est irréductible, alors P est séparable si $P' \neq 0$. En particulier, en caractéristique nulle ou sur un corps fini, tout polynôme irréductible est séparable.

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

Théorème 3.7 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 3.8 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 , noté $\text{Gal}_K(P)$. De plus $\text{Gal}_K(P)$ s'identifie à un sous-groupe de \mathfrak{S}_r où $r = \deg P$.

Démonstration : \Rightarrow : Soit e_1, \dots, e_n une base de E/K . Soient $P_1, \dots, P_n \in K[X]$ les polynômes minimaux correspondants. Alors les P_i sont scindés sur E et leurs racines engendrent E car les e_i sont parmi elles. Donc E est le corps de décomposition du polynôme séparable $\prod_i P_i \in K[X]$ où on ne choisit qu'une seule fois chaque facteur irréductible.

\Leftarrow : Soit P un polynôme séparable. Soit E un corps de décomposition de P sur K . On raisonne par récurrence sur le nombre de racines qui ne sont pas dans K . Soit x_1 une racine qui n'est pas dans K . Alors par hypothèse de récurrence, $E/K(x_1)$ est galoisienne de groupe $H \leq \text{Aut}_K(E)$. On sait que $G := \text{Aut}_K(E)$ est fini. Soit $x \in E^G$. On a $x \in K(x_1)$. On a $x = a_0 + \dots + a_{d-1}x_1^{d-1}$ pour certains $a_i \in K$ où $d := [K(x_1) : K]$. Notons x_2, \dots, x_d les autres racines du polynôme minimal de x_1 sur K . Les isomorphismes : $K(x_1) \simeq K(x_i)$, $x_1 \mapsto x_i$ se prolongent en des éléments $s_i \in G$. Comme $s_i(x) = x$, on a :

$$\forall i, a_0 - x + a_1x_i + \dots + a_{d-1}x_i^{d-1} = 0$$

Donc le polynôme $a_0 - x + \dots + a_{d-1}X^{d-1}$ a au moins d racines donc est nul donc $a_0 = x \in K$. **Q.e.d.**

COURS DU MARDI 24 FÉVRIER 2015

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

Corollaire 3.8.1 *Soit a un élément algébrique séparable sur K . Alors l'extension $K(a)/K$ est séparable.*

Démonstration : Soit P le polynôme minimal de a sur K . Soit L/K un corps de décomposition de P sur K contenant a . Alors L/K est galoisienne donc séparable. Comme $K(a) \leq L$, $K(a)/K$ est aussi séparable. **Q.e.d.**

Exemple : on retrouve ainsi que toute extension finie d'un corps fini est séparable.

3.7 Normalité

Théorème 3.9 *Soit E/K une extension algébrique. Si $\sigma : E \rightarrow E$ est un K -endomorphisme de corps, alors σ est un automorphisme.*

Démonstration : Il suffit de démontrer la surjectivité. Soit $x \in E$. Soit $P \in K[X]$ le polynôme minimal de x sur K . On peut prolonger σ à $E[X]$. Alors $P^\sigma = P$. Soit $P = \prod_i P_i$ la factorisation de P en produits d'irréductibles unitaires dans $E[X]$. On a $P^\sigma = \prod_i P_i^\sigma$. Par unicité de la factorisation en irréductible, $P^\sigma = P \Rightarrow \exists i, P_i^\sigma = X - x$. Soit $x' \in E$ tel que $X - x' = P_i$.

On a $\sigma(x') = x$.

Q.e.d.

Exercice : donner un contre-exemple si E/F n'est pas algébrique.

Théorème 3.10 (de prolongement) Soit E/K une extension algébrique. On suppose que $E = K(x_i : i \in I)$ pour une certaines familles $x_i, i \in I$ d'éléments de E . Pour tout i , soit P_i le polynôme minimal de x_i sur K . On suppose qu'il existe un morphisme de corps $\sigma : K \rightarrow \Omega$ où Ω est un corps où tous les polynômes P_i^σ sont scindés (par exemple c'est le cas si Ω est algébriquement clos). Alors σ se prolonge à E .

Démonstration : dans le cas où I est fini. Il suffit de raisonner par récurrence. Il suffit donc de traiter le cas où I est un singleton. C'est facile ...

Q.e.d.

Définition 5 On dit qu'une extension algébrique E/F est normale si tout polynôme irréductible $P \in F[X]$ qui a une racine dans E est scindé sur E .

Exemples : les extensions de degré 2 sont toujours normales.

Contre-exemples : $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ et $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ne sont pas normales.

Proposition 3.11 Soit E/F une extension algébrique. Sont équivalentes :

- (i) l'extension E/F est normale ;
- (ii) pour toute extension Ω de F , et pour tous F -morphisme $\sigma, \tau : E \rightarrow \Omega$, $\sigma(E) = \tau(E)$. ;
- (iii) pour toute extension Ω de E , et pour tout F -morphisme $\sigma : E \rightarrow \Omega$, $\sigma(E) = E$. ;

Démonstration : (i) \Rightarrow (ii) : soit $x \in E$. Soit P le polynôme minimal unitaire de x sur F . On peut prolonger σ, τ à $E[X]$. Comme $P \in F[X]$, $P^\sigma = P^\tau$. Or $X - x$ est un facteur irréductible de P dans $E[X]$. Donc $X - \sigma(x) | P^\sigma \Rightarrow \exists y \in E, \sigma(x) = \tau(y)$. Donc $\sigma(x) \in \tau(E)$. D'où $\sigma(E) \leq \tau(E)$. De même, $\tau(E) \leq \sigma(E)$.

ii \Rightarrow *iii* : facile ;

iii \Rightarrow *i* : soit $P \in F[X]$ un polynôme irréductible sur F avec une racine $x \in E$. Soit Ω un corps algébriquement clos qui contient E . Soit $x' \in \Omega$ une autre racine de P . Alors le F -morphisme $F(x) \rightarrow \Omega, x \mapsto x'$ se prolonge en un morphisme $\sigma : E \rightarrow \Omega$. On a donc $\sigma(E) = E$ et $x' \in E$. Donc toutes les racines de P sont dans E .

Q.e.d.

Proposition 3.12 Si E/F est un corps de décomposition, E/F est normale.

Démonstration : Supposons que $P \in F[X]$ est irréductible avec une racine x dans E . Soit $\Omega \geq E$ un corps algébriquement clos (si E/F est engendré par un nombre fini d'éléments x_1, \dots, x_n , il suffit de prendre une extension où tous les polynômes minimaux des x_i et le polynôme P sont scindés). Soit x' une racine de P . Le F -morphisme $F(x) \rightarrow \Omega, x \mapsto x'$ se prolonge en un morphisme $E \rightarrow \Omega$ d'image E' . Donc $x' \in E'$ et toutes les racines de P sont dans E' .

Q.e.d.

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

Théorème 3.13 Soit E/F une extension finie. Alors l'extension E/F est galoisienne si et seulement si elle est normale et séparable.

Démonstration : \Rightarrow : déjà fait.

\Leftarrow : Soit E/F une extension finie normale et séparable. Soit e_1, \dots, e_n une base de E/F . Soit P le produit des polynômes minimaux distincts des e_i sur F . Alors E est un corps de décomposition de P qui est un polynôme séparable. Donc E/F est galoisienne.

Q.e.d.

Remarques :

- i) Si M/L et L/K sont normales, M/K ne l'est pas forcément. Par exemple : $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}), M = \mathbb{Q}(\sqrt[4]{2})$.
- ii) Si M/L et L/K sont séparables, alors M/K est aussi séparable (nous le démontrerons plus tard).

3.8 Composée de corps

section non faite en cours

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

Proposition 3.14 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, $E \cap E' = K, \text{Gal}(EE'/K) \simeq \text{Gal}(E/K) \times \text{Gal}(E'/K)$.

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 $H = \mathfrak{S}_3$, $H' = K_4$, $[E : K] = |\mathfrak{S}_4/\mathfrak{S}_3| = 4$, $[E' : K] = |\mathfrak{S}_4/K_4| = 6$, $EE' = L = L^{H \cap H'}$, $E \cap E' = L^{\langle H, H' \rangle} = K$. 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

Exemples : $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}[i]/(7)$, $\mathbb{Z}[\sqrt{2}]/(3)$, $\left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}/5\mathbb{Z} \right\}$, $\mathbb{F}_2[X]/(X^3 + X + 1)$.

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.

Démonstration : Soit x d'ordre $m = p_1^{a_1} \dots p_r^{a_r}$ et soit y d'ordre $n = p_1^{b_1} \dots p_r^{b_r}$ où les p_i sont des nombres premiers deux à deux non associés et où les $a_i, b_i \in \mathbb{N}$. Alors pour tout i , $x^{\prod_{j \neq i} p_j^{a_j}}$ est d'ordre $p_i^{a_i}$ et $y^{\prod_{j \neq i} p_j^{b_j}}$ est d'ordre $p_i^{b_i}$. Donc il existe z_i d'ordre $p_i^{c_i}$ pour tout i , où $c_i := \max\{a_i, b_i\}$. On a $z_1 \dots z_r$ d'ordre $\prod_i p_i^{c_i} = \text{ppcm}(m, n)$. Q.e.d.

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

Démonstration : Soit N le ppcm des ordres des éléments de G . Alors il existe un élément $g \in G$ d'ordre N . Or $X^N = 1$ a au plus N solutions dans K . Comme $\langle g \rangle \leq G \leq \{x \in K^\times : x^N = 1\}$, on a $\langle g \rangle = G = \{x \in K^\times : x^N = 1\}$ et G cyclique. Q.e.d.

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

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 $\overline{\mathbb{F}_p} = \bigcup_n \mathbb{F}_{p^n}$.

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 (de l'élément primitif) *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 .*

Démonstration : En effet, il suffit de choisir pour θ un générateur du groupe cyclique $\mathbb{F}_{q^n}^\times$.

Q.e.d.

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

Démonstration : Si $m|n$, alors $q^m - 1 | q^n - 1$ donc $X^{q^m-1} - 1 | X^{q^n-1} - 1$ et $X^{q^m} - X | X^{q^n} - X$. Réciproquement, si $P | X^{q^n} - X$ alors si $x \in \mathbb{F}_{q^n}$ est une racine de P , on a :

$$\mathbb{F}_q \leq \mathbb{F}_q[x] \leq \mathbb{F}_{q^n}$$

donc $m = \deg P = [\mathbb{F}_q[x] : \mathbb{F}_q]$ divise $n = [\mathbb{F}_{q^n} : \mathbb{F}_q]$. Réciproquement, $m|n \Rightarrow q^m - 1 | q^n - 1 \Rightarrow X^{q^m-1} - 1 | X^{q^n-1} - 1 \Rightarrow X^{q^m} - X | X^{q^n} - X$. Or, si on pose $K := \mathbb{F}_q[X]/(P)$ et $x := X \bmod P$, on a $|\mathbb{F}_q[X]/(P)| = q^m \Rightarrow x^{q^m} = x \Rightarrow x^{q^m} - x = 0 \Rightarrow P | X^{q^m} - X$. Q.e.d.

COURS DU MARDI 3 MARS 2015

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 :

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

L'égalité précédente s'écrit :

$$\prod_{n \geq 1} (1 - t^n)^{-\nu_n(q)} = (1 - qT)^{-1} .$$

Exercice : Vérifier : $\nu_n(q) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right)$. En déduire

$$\left| \{P \in \mathbb{F}_q[X] : P \text{ irréductible unitaire } \deg P \leq n\} \right| \sim \frac{q}{q-1} \frac{q^n}{n} .$$

4.3.2 Ordre d'un polynôme, polynôme primitif

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

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

Soit $P \in \mathbb{F}_q[X]$ un polynôme irréductible premier à X . L'ordre de P est le plus petit entier $e > 0$ tel que $P|X^e - 1$.

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

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

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

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

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

Démonstration : Soit $\Phi_e := \prod_{\substack{x \in \mathbb{F}_{q^m} \\ x \text{ d'ordre } e}} X - x \in \mathbb{F}_q[X]$. En effet, on le démontre par récurrence en utilisant la formule :

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

si $n|q^m - 1$. 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 : $2^{11} - 1 = 23 \cdot 89$. 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 unitaire irréductible de degré m est primitif si et seulement s'il est premier à X et d'ordre $q^m - 1$.*

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

4.4 Algorithme de Berlekamp

Théorème 4.13 *Soit $P \in \mathbb{F}_q[X]$ un polynôme de degré d sur \mathbb{F}_q . On suppose que P est séparable. Alors P est irréductible sur \mathbb{F}_q si et 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 $a \in \mathbb{F}_q$ car $P|Q^q - Q = \prod_{a \in \mathbb{F}_q} (Q - a)$. Donc P est divisible par un polynôme non constant de degré $< d = \deg P$ donc est réductible.

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

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

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

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

Q.e.d.

Exemple : $q = 2$, $P = X^5 + X^4 + 1$, Dans la base $1, X, X^2, X^3, X^4 \pmod P$, 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

Pas fait en cours Soit K un corps. Une *clôture algébrique* de K est une extension algébrique 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 $f_1, \dots, f_N \in I$ 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.**

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

5.1 Retour sur la notion de séparabilité

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

$$\{\tilde{\sigma} : E \rightarrow \Omega : \tilde{\sigma}|_F = \sigma\} \xrightarrow{1:1} \{\tilde{\sigma}' : E \rightarrow \Omega : \tilde{\sigma}'|_F = \sigma'\}$$

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

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

Démonstration : On a $E = F(x_1, \dots, x_r)$ pour certains $x_i \in E$. Soit $\sigma : F \rightarrow \Omega$. Soit P_1 le polynôme minimal de x_1 sur F . Alors il y a une bijection entre les prolongements de σ à $F(x_1)$ et le nombre de racines distinctes du polynôme P_1^σ dans Ω . Donc $[F(x_1) : F]_s \leq [F(x_1) : F] = \deg P_1$. Soit \mathcal{P} l'ensemble des prolongements de σ à E . On a $\mathcal{P} = \cup_{\sigma_i} \mathcal{P}_{\sigma_i}$ où σ_i décrit les prolongements de σ à $F(x_1)$. On a donc $[E : F]_s = \sum_i [E : F(x_1)]_s \leq \sum_i [E : F(x_1)] = [F(x_1) : F]_s [E : F(x_1)] \leq [F(x_1) : F] [E : F(x_1)] = [E : F]$. **Q.e.d.**

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

Démonstration : $[E : k]_s$ = le nombre de racines du polynôme minimal de a sur k . De plus, si a est séparable, E est contenu dans un corps de décomposition du polynôme minimal de a sur k qui est séparable et donc E est dans une extension galoisienne ... **Q.e.d.**

COURS DU MARDI 10 MARS 2015

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

Démonstration : Soit Ω un corps algébriquement clos et soit $\sigma : K \rightarrow \Omega$ un morphisme de corps. Notons $\mathcal{P}_{K,L,\sigma}$ l'ensemble des prolongements de σ à L .

On a : $\mathcal{P}_{K,M,\sigma} = \sqcup_{\tau \in \mathcal{P}_{K,L,\sigma}} \mathcal{P}_{L,M,\tau}$. Donc $[M : K]_s = \sum_{\tau \in \mathcal{P}_{K,L,\sigma}} [M : L]_s [L : K]_s$. Q.e.d.

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

Démonstration : Soient $x_1, \dots, x_r \in E$ tels que $E = F(x_1, \dots, x_r)$. Si $r = 1$: c'est déjà fait. Si $r > 1$: si $[E : F] = [E : F]_s$, alors pour tout $x \in E$, on a : $[E : F] = [E : F]_s \Rightarrow [F(x) : F] = [F(x) : F]_s$ donc x est séparable sur F . Réciproquement, si E/F est séparable, on a : $E/F(x_1)$ séparable et $F(x_1)/F$ séparable donc :

$$[E : F] = [E : F(x_1)][F(x_1) : F] = [E : F(x_1)]_s [F(x_1) : F]_s = [E : F]_s .$$

Q.e.d.

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

6 Base normale

6.1 Éléments primitifs

Soit E/K une extension.

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

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

Démonstration : Si K est fini, alors $K(x, y)$ aussi donc $K(x, y)^\times$ est cyclique et il suffit de prendre pour z un générateur du groupe $K(x, y)^\times$!

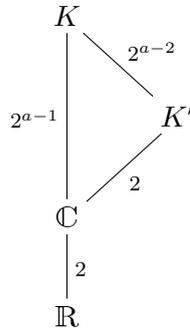
Si K est infini : notons P_x, P_y les polynômes minimaux de x et y sur K . Notons y_j les racines distinctes de P_y et x_i celles de P_x (dans une extension). Soit $0 \neq t \in K$ tel que les $x_i + ty_j$ soient deux à deux distincts (il suffit que $t \in K \setminus \left\{ \frac{x_{i'} - x_i}{y_j - y_{j'}} : i, i', j, j', y_j \neq y_{j'} \right\}$). Posons $z := x + ty$. Alors $P_x(z - tY) \in K(z)[Y]$ a une seule racine en commun avec $P_y(Y) : y$. Donc le pgcd de $P_x(z - tY)$ et P_y est $Y - y$. Or, $P_y, P_x(z - tY) \in K(z)[Y]$ donc $Y - y \in K(z)[Y] \Rightarrow y \in K(z) \Rightarrow x, y \in K(z) \Rightarrow K(z) = K(x, y)$. Q.e.d.

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

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

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

Démonstration : Le corps des réels n'admet pas d'extension de degré impair > 1 . Si $K \geq \mathbb{C}$ est une extension de degré n , alors il existe $a \in K$ tel que $K = \mathbb{R}(a)$ car K/\mathbb{R} est séparable (caractéristique nulle). Quitte à remplacer K par un corps de décomposition sur \mathbb{R} du polynôme minimal de a , on peut supposer que K/\mathbb{R} est galoisienne. Soit G son groupe de Galois, soit P un 2-groupe de Sylow de G . Alors K^P est une extension d'ordre impair de \mathbb{R} donc $K^P = \mathbb{R}$ et $P = G$. Mais alors, $|G| = 2^a$ pour un certain $a \geq 1$. Si $a > 1$, il existe un sous-groupe $H \leq \text{Gal}(K/\mathbb{C})$ d'ordre 2^{a-2} . Mais alors K^H est une extension de degré 2 de \mathbb{C} *absurdo!*



Q.e.d.

Exemple : soit k un corps. Soient $L := k(x_1, \dots, x_n)$, $K := k(s_1, \dots, s_n)$. 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 a, a^2, a^3, a^4 n'est pas normale (car $a^8 = \text{Fr}_2^3(a) = a^4 + a^2 + a$).

Cependant :

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

Lemme 6.4 *Le polynôme minimal du \mathbb{F}_q -endomorphisme Fr_q sur \mathbb{F}_{q^d} est le polynôme $T^d - 1$.*

Démonstration : Il est clair que $\text{Fr}_q^d = \text{Id}$ sur \mathbb{F}_{q^d} . Si $P(\text{Fr}_q) = 0$ avec $0 \neq P = a_0 + \dots + a_N T^N \in \mathbb{F}_q[X]$, alors le polynôme $a_0 X + \dots + a_N X^{q^N}$ s'annule sur \mathbb{F}_q^d donc a au moins q^d racines donc son degré $q^N \geq q^d$ et $N \geq d$.

Q.e.d.

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

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

Comme $T^d - 1$ est le polynôme minimal de l'endomorphisme Fr_q , pour tout i , $P_i^{r_i}$ est le polynôme minimal de Fr_q sur $\ker(P_i^{r_i}(\text{Fr}_q))$. Pour tout i , soit $x_i \in \ker(P_i^{r_i}(\text{Fr}_q)) \leq \mathbb{F}_{q'}$ tel que $P_i^{r_i-1}(\text{Fr}_q)(x_i) \neq 0$. Alors l'idéal $\{P \in \mathbb{F}_q[X] : P(\text{Fr}_q)(x_i) = 0\}$ contient $P_i^{r_i}$ mais non $P_i^{r_i-1}$. Donc il est engendré par $P_i^{r_i}$!

On pose alors $\theta := x_1 + \dots + x_s$. On a :

$$\begin{aligned} \sum_{k=0}^{d-1} \lambda_k \text{Fr}_q^k(\theta) = 0 &\Rightarrow \forall i, \sum_{k=0}^{d-1} \lambda_k \text{Fr}_q^k(x_i) \\ &\Rightarrow \forall i, P_i^{r_i} \mid \sum_{k=0}^{d-1} \lambda_k T^k \Rightarrow T^d - 1 \mid \sum_{k=0}^{d-1} \lambda_k T^k \\ &\Rightarrow \forall k, \lambda_k = 0 . \end{aligned}$$

Q.e.d.

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

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

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

si $x := \sum_k b_k e_k$.

Q.e.d.

Exemples :

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

- b) l'ensemble des conjugués de $1 + \sqrt{2} + \sqrt{3} + \sqrt{6}$ est une base normale de $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ mais non celui des conjugués de $\sqrt{2} + \sqrt{3}$.
- c) Si p est un nombre premier, si $z := e^{2i\pi/p}$, alors $\{z, \dots, z^{p-1}\}$ est une base normale mais non $\{1, z, \dots, z^{p-2}\}$.
- d) 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 .

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

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 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.

Exercice : Trouver une base normale de $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$.

COURS DU MERCREDI 17 MARS 2015

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 : L'extension $K(\zeta_n)/K$ est galoisienne car c'est le corps de décomposition sur K du polynôme séparable $X^n - 1$.

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 $\simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Démonstration : Il suffit de montrer que ζ_n est de degré $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ sur \mathbb{Q} . cf. la proposition suivante ... **Q.e.d.**

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 de ζ , une racine primitive n -ième de 1, sur \mathbb{Q} . On montre que si p est un nombre premier tel que $p \nmid n$, $P(\zeta^p) = 0$.

Cela suffit car toute racine de Φ_n s'écrit $\zeta^{p_1 \dots p_m} = \zeta^{p_1 \dots p_m}$ pour certains nombres premiers p_i qui ne divisent pas n . En effet, soit Δ le discriminant de $X^n - 1$. On a :

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

car $\zeta^{1+\dots+n} = \zeta^{n(n+1)/2} = \pm 1$ (vu que $(\zeta^{n(n+1)/2})^2 = 1$). Donc :

$$\Delta = \pm \left(\frac{X^n - 1}{X - 1} (1) \right)^n = \pm (1 + \dots + X^{n-1})(1)^n = \pm n^n .$$

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

$p|n^n$ dans $\mathbb{Z}[\zeta]$ donc dans \mathbb{Z} car $\mathbb{Q} \cap \mathbb{Z}[\zeta] = \mathbb{Z}$. 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 : $\Phi_{105}(X) = X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - X^{40} - X^{39} + X^{36} + X^{35} + X^{34} + X^{33} + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} - X^{22} - X^{20} + X^{17} + X^{16} + X^{15} + X^{14} + X^{13} + X^{12} - X^9 - X^8 - 2X^7 - X^6 - X^5 + X^2 + X + 1$.

Exercice : $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\text{ppcm}(m,n)})$; $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\text{pgcd}(m,n)})$;
 $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m) \Leftrightarrow \{n, m\} \subseteq \{k, 2k\}$ pour un k impair. Si $K = \mathbb{Q}(\sqrt{3})$,
 $K(\zeta_3) = K(\zeta_4)$; $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\cos(2\pi/n))$.

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 $a \in \mathbb{Z}$, $\chi(a) := \chi(a \bmod N)$ 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 $\ker((\mathbb{Z}/N\mathbb{Z})^\times \rightarrow (\mathbb{Z}/M\mathbb{Z})^\times)$), 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 :

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

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.

On en déduit que $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(i, \sqrt{\left(\frac{-1}{p}\right)}) \subseteq \mathbb{Q}(i, \zeta_p) \subseteq \mathbb{Q}(\zeta_{4p}) \dots$ **Q.e.d.**

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

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 $\text{Tr}_{E/K}(\alpha) = -r a_1$.
- (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 :

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

Exercice : en utilisant la trace et la norme, montrer que $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$ et que $1 + \sqrt[3]{2}$ n'est pas un carré dans $\mathbb{Q}(\sqrt[3]{2})$.

Démonstration : Soit $\chi_{\alpha, E/K}$ le polynôme caractéristique de $m_\alpha : E \rightarrow E$. On a $\chi_{\alpha, E/K} = (\chi_{\alpha, K(\alpha)/K})^{[E:K(\alpha)]}$.

Pour la transitivité, on se ramène au cas où $E = L(x)$. Soit $X^r + a_1 X^{r-1} + \dots + a_r \in L[X]$ le polynôme minimal de x sur L . Soit e_1, \dots, e_m une base de L/K . On a une base de $E/K : e_i x^j, 1 \leq i \leq m, 0 \leq j \leq r-1$. Dans cette base la matrice de la multiplication par x est donnée par :

$$\begin{pmatrix} 0 & \cdots & 0 & -A_r \\ & \ddots & & \vdots \\ I_m & & & 0 \\ & \ddots & & \vdots \\ 0 & & & I_m \\ & \ddots & & \vdots \\ 0 & \cdots & 0 & -A_1 \end{pmatrix}$$

où les $A_i \in \mathcal{M}_m(K)$ sont les matrices des m_{a_i} dans la base e_i .

On a alors : $N_{E/K}(x) = (-1)^{mr} \det A_r = (-1)^{mr} N_{L/K}(a_r) = (-1)^{mr} N_{L/K}((-1)^r N_{E/L}(x)) = N_{L/K}(N_{E/L}(x))$. Q.e.d.

9 Extensions cycliques

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

Exemples : les extensions des corps finis, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, si p premier (où $\zeta_p := e^{2i\pi/p}$, $\mathbb{C}(t^{1/n})/\mathbb{C}(t)$ est galoisienne cyclique de groupe de Galois $\mathbb{Z}/n\mathbb{Z}$.

Contre-exemple : $\mathbb{Q}(\zeta_8)/\mathbb{Q}$.

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 $a \in E^\times$.

Démonstration : Soit c tel que $a := bc + b\sigma(b)\sigma(c) + \dots + \prod_{i=0}^{n-1} \sigma^i(b)\sigma^{n-1}(c) \neq 0$ où $n := [E : K]$. On a $b = a/\sigma a$. Q.e.d.

Théorème 9.2 (Kummer) Soit E/K une extension finie. 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 E/K est galoisienne cyclique et 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 .

Démonstration :

- (i) on a $N(\zeta^{-1}) = \zeta^{-n} = 1$. Donc il existe $\alpha \in E$ tel que $\sigma\alpha/\alpha = \zeta$. Alors le polynôme minimal de α sur K P_α est de degré $\leq n$ et a au moins n racines distinctes :

$$\alpha, \sigma\alpha = \zeta\alpha, \dots, \sigma^{n-1}\alpha = \zeta^{n-1}\alpha .$$

Donc $P_\alpha = (T - \alpha)\dots(T - \zeta^{n-1}\alpha) = T^n - \alpha^n$. En particulier, $\alpha^n \in K$ et $E = K(\alpha)$.

- (ii) Il est clair que E/K est le corps de décomposition du polynôme séparable $X^n - \alpha^n$ sur K . Donc E/K est galoisienne. On a un morphisme injectif de groupes : $G := \text{Gal}(E/K) \rightarrow \mathbb{Z}/n\mathbb{Z}$ $s \mapsto k_s$ où $s\alpha/\alpha = \zeta^{k_s}$. Donc $\text{Gal}(E/K)$ est cyclique. Soit $d := |\text{Gal}(E/K)|$. Soit s un générateur de G . On a $s(\alpha) = \zeta^{k_s}\alpha$ où $s^d = \text{Id} \Rightarrow k_s = 0 \pmod{n/d}$. Mais alors $s(\alpha^d) = \alpha^d$ et $\alpha^d \in K$. Donc $d = [K(\alpha) : K] \Rightarrow T^d - \alpha^d$ est le polynôme minimal de α sur K .

Q.e.d.

Exercice : soit p un nombre premier. Vérifier que l'extension $\mathbb{Q}(\zeta_n, \sqrt[p]{p})/\mathbb{Q}(\zeta_n)$ est galoisienne cyclique de groupe de Galois $\simeq \mathbb{Z}/n\mathbb{Z}$ si n est impair (on note $\zeta_n := e^{2i\pi/n}$). Si $n = 8$, déterminer $[\mathbb{Q}(\sqrt[8]{2}, \zeta_8) : \mathbb{Q}(\zeta_8)]$.

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 $\alpha^p - \alpha - a = 0$.

COURS DU MARDI 7 AVRIL 2015

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 de sous-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 $|G|$.

Remarque : cela revient à dire que $\mathcal{D}^n(G) = 0$ si $n \gg 0$.

Exemple : le groupe \mathfrak{S}_4 est résoluble mais non le groupe \mathfrak{S}_5 .

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

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 :

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

Si $\text{car}(K) = 0$, si $f \in K[X]$, on dit que f est résoluble par radicaux s'il existe une tour d'extensions $K = K_0 \leq \dots \leq K_m$ telle que :

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

et f est scindé dans K_m .

Exemple : le polynôme $X^7 - 1$ est résoluble par radicaux sur \mathbb{Q} car ...

Théorème 10.1 *Soit K de caractéristique nulle. Une extension finie L/K est résoluble par radicaux si et seulement si elle est résoluble.*

Lemme 10.2 *On suppose $\text{car}(K) = 0$. Soit L/K une extension galoisienne de groupe de Galois G . Soit $K' \geq K$. Soit E un corps qui contient L, K' . Alors LK'/K' est galoisienne de groupe de Galois isomorphe à un sous-groupe de G .*

Démonstration : On peut supposer que E/K est galoisienne. Montrons que $\text{Gal}(E/LK') \triangleleft \text{Gal}(E/K')$. Soient $s \in \text{Gal}(E/LK')$, $t \in \text{Gal}(E/K')$. On a $tst^{-1}(x) = x$ si $x \in K'$. Si $x \in L$, $t^{-1}(x) \in L$ car L/K est galoisienne donc $tst^{-1}(x) = tt^{-1}(x) = x$. Donc $tst^{-1} \in \text{Gal}(E/LK')$. De plus, le morphisme de groupes $\text{Gal}(LK'/K') \rightarrow \text{Gal}(L/K)$, $s \mapsto s|_L$ est injectif. **Q.e.d.**

Démonstration :

résoluble \Rightarrow résoluble par radicaux :

Supposons L/K galoisienne de groupe de Galois G résoluble. Nous allons montrer par récurrence sur $n = |G| = [L : K]$ que L/K est résoluble par radicaux. Si $n = 1$, il n'y a rien à faire. Si $n > 1$...

Il existe des sous-groupes $G = G_0 \geq G_1 \geq \dots \geq G_N = e$ tels que $\forall i, G_{i+1} \triangleleft G_i$ et G_i/G_{i+1} est cyclique d'ordre premier p_i . Posons $n' := \prod_{p_i \text{ distincts}} p_i \leq n$. Soit ζ une racine primitive n' ième de l'unité dans une extension de K . On a $[K(\zeta) : K] \leq \varphi(n') < n' \leq n$. Donc par hypothèse de récurrence il existe une suite d'extensions par radicaux :

$$K = K_0 \leq \dots \leq K_N \geq K(\zeta) .$$

Soit $K' := K_N$. Posons $L_i := L^{G_i}$. On a L_{i+1}/L_i galoisienne de groupe de Galois cyclique G_i/G_{i+1} . Pour tout i , $L_{i+1}K'/L_iK'$ est galoisienne de groupe de Galois trivial ou isomorphe à G_i/G_{i+1} d'après le lemme ci-dessus.

Dans ce dernier cas, d'après le théorème de Kumer, $L_{i+1}K' = L_iK'(\alpha_i)$ pour un certain $\alpha_i \in L_{i+1}K'$ tel que :

$$[L_{i+1}K'/L_iK'] = p_i \text{ et } \alpha_i^{p_i} \in L_iK' .$$

On a donc une tour d'extensions radicales :

$$K = K_0 \leq K_1 \leq \dots \leq K_N \leq K_{N+1} \leq \dots \leq K_{N+M} \geq LK' \geq L$$

où $K_{N+j} := L_jK'$.

Donc L/K est résoluble par radicaux.

Réciproquement, démontrons d'abord le lemme suivant :

Lemme 10.3 *Soient $K \leq L \leq M$. On suppose $\text{car}(K) = 0$. L 'extension M/K est résoluble 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, soit M' le sous-corps de E engendré par les $\sigma(M)$ où σ décrit $\text{Gal}(E/L)$. Alors, $E \geq M' \geq M \geq L$ 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.**

On suppose que l'on a une tour d'extensions :

$$K = K_0 \leq \dots \leq K_N \geq L$$

où $\forall i, K_{i+1} = K_i(\alpha_i)$ pour un $\alpha_i \in K_{i+1}$ tel que $[K_{i+1} : K_i] = n_i$ et $\alpha_i^{n_i} \in K_i$. Posons $n := \prod_i n_i$ et ζ une racine primitive n -ième de l'unité dans une extension de K . On a les inclusions :

$$K = K_0 \leq K(\zeta) \leq K_1(\zeta) \leq \dots \leq K_N(\zeta) .$$

Pour tout i , l'extension $K_{i+1}(\zeta)/K_i(\zeta)$ est résoluble car galoisienne cyclique (cf. le théorème de Kummer). L'extension $K(\zeta)/K$ aussi est résoluble car galoisienne de groupe de Galois abélien (isomorphe à un sous-groupe de $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/n'\mathbb{Z})^\times$). Donc par le lemme précédent, on en déduit par récurrence que $K_N(\zeta)/K$ est résoluble.

Q.e.d.

Rappelons le :

Théorème 10.4 *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) i.e. toutes les racines de P sont dans une extension résoluble par radicaux sur K .

Exemple : $X^7 - 1$ est résoluble par radicaux sur \mathbb{Q} car $e^{2i\pi/7} = \frac{x + \sqrt{x^2 - 4}}{2}$ où $x := -\frac{1}{3} + \frac{1}{3} \left(\sqrt[3]{\frac{7+21i\sqrt{3}}{2}} + \sqrt[3]{\frac{7-21i\sqrt{3}}{2}} \right)$.

Théorème 10.5 (Galois) *Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré p premier. Alors sont équivalentes :*

- (i) P est résoluble par radicaux ;
- (ii) 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 ;
- (iii) 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 .

Démonstration : $ii \Rightarrow iii$: facile ; $iii \Rightarrow i$: le groupe de Galois G de $\mathbb{Q}(x_1, x_2)/\mathbb{Q}$ est d'ordre $\leq p(p-1)$ car $\sigma \in G$ est déterminé par $\sigma(x_1)$ et $\sigma(x_2)$. Donc G contient un seul p -groupe par exemple : $H := \langle (12\dots p) \rangle$. Donc $H \triangleleft G$ et $G \leq N_{\mathfrak{S}_p}(H)$. Or $N_{\mathfrak{S}_p}(H)/H$ est cyclique comme nous allons le voir.

Q.e.d.

Théorème 10.6 *Soit p un nombre premier. Soit Aff_p le groupe des bijections affines $\mathbb{F}_p \rightarrow \mathbb{F}_p$, $z \mapsto az + b$, où $a \in \mathbb{F}_p^\times$, $b \in \mathbb{F}_p$. On peut identifier Aff_p avec un sous-groupe de \mathfrak{S}_p en associant à $x \mapsto ax + b$ la permutation : $i \mapsto [ai + b]$, représentant de $ai + b$ dans $\{1, \dots, p\}$. Alors Aff_p est le normalisateur de $\langle (12\dots p) \rangle$ et $\text{Aff}_p / \langle (12\dots p) \rangle \simeq \mathbb{F}_p^\times$ est cyclique (donc Aff_p est résoluble).*

Tout sous-groupe transitif et résoluble de \mathfrak{S}_p est conjugué à un sous-groupe de Aff_p .

Démonstration :

Dans \mathfrak{S}_p , il y a $(p-2)!$ sous-groupes d'ordre p donc le normalisateur du sous-groupe engendré par le p -cycle $(12\dots p)$ est d'ordre $p(p-1)$. Or Aff_p est d'ordre $p(p-1)$ et est contenu dans le normalisateur de $\langle(12\dots p)\rangle$. Donc $\text{Aff}_p = N_{\mathfrak{S}_p}(\langle(12\dots p)\rangle)$. De plus Aff_p est résoluble car $\text{Aff}_p/\langle(12\dots p)\rangle \simeq (\mathbb{F}_p)^\times$.

Soit $H \subseteq \mathfrak{S}_p$ un sous-groupe transitif. Si $H' \triangleleft H$, alors les H' -orbites dans $\{1, \dots, p\}$ sont H -stables et de même cardinal car $H'hx = hH'x$. Il y en a donc p ou 1 . Donc $H' = 1$ ou H' est encore transitif. On en déduit que si $1 \neq H'$, H' contient autant de p -Sylow que H (car H' est distingué et les p -Sylow sont conjugués). Donc si H est résoluble transitif, H contient un seul p -sous-groupe de Sylow. Donc est contenu dans le normalisateur du groupe engendré par un p -cycle qui est conjugué à Aff_p . **Q.e.d.**

Corollaire 10.6.1 *Si H est un sous-groupe transitif et résoluble de \mathfrak{S}_p , alors si $h \in H$ a deux points fixes dans $\{1, \dots, p\}$, $h = 1$.*

Démonstration : Il suffit de vérifier que si $h \in \text{Aff}_p$ a deux points fixes, alors $h = 1$. **Q.e.d.**

Fin de la démonstration du théorème de Galois : $i \Rightarrow ii$: soit L un corps de décomposition de P sur \mathbb{Q} , soient x_1, x_2 deux racines de P , si $\sigma \in \text{Gal}(L/\mathbb{Q}(x_1, x_2))$, σ est dans un sous-groupe résoluble transitif de \mathfrak{S}_p avec au moins deux points fixes donc $\sigma = 1$. Donc $L = \mathbb{Q}(x_1, x_2)$ *q.e.d.*

Corollaire 10.6.2 *Si $P \in \mathbb{Q}[X]$ est un polynôme résoluble par radicaux irréductible de degré p premier, alors P a une seule ou toutes ses racines réelles.*

Démonstration : S'il y a au moins 2 racines réelles x_1, x_2 , alors $\mathbb{Q}(x_1, \dots, x_p) = \mathbb{Q}(x_1, x_2) \leq \mathbb{R}$ et tous les x_i sont réels! **Q.e.d.**

Exemple : le polynôme $X^5 - 4X + 2$ n'est pas résoluble par radicaux sur \mathbb{Q} .

COURS DU MARDI 21 AVRIL 2015

11 Calcul du groupe de Galois

11.1 Discriminant

Soit $P \in K[X]$ un polynôme de degré n et de coefficient dominant $a_n \in K^\times$ sur un corps K de caractéristique $\neq 2$. On note x_1, \dots, x_n les racines de P dans un corps de décomposition. Alors :

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

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

Remarque : si P est unitaire, alors on a $\Delta_P = (-1)^{n(n-1)/2} \prod_{i=1}^n P'(x_i)$.

Exercice 1 Si P est unitaire de degré n , alors $\Delta_P = (-1)^{n(n-1)/2} n^n \prod_{j=1}^{n-1} P(\eta_j)$ où les η_j sont les racines de P' .

Exercice 2 Si $P = aX^2 + bX + c$ avec $a \neq 0$, $\Delta_P = b^2 - 4ac$. Si $P = a_3X^3 + a_2X^2 + a_1X + a_0$ est de degré 3, alors : $\Delta_P = a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 + 18a_0a_1a_2a_3 - 27a_0^2a_3^2$.

Exercice 3 Si P est de degré n , alors Δ_P est un polynôme à coefficients entiers, homogène de degré $2n - 2$ en les coefficients de P .

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

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

Démonstration : Soit L le corps de décomposition de P sur K . Posons $\delta := \prod_{1 \leq i < j \leq n} (x_i - x_j) \in L$. Alors $\Delta \in (K^\times)^2 \Leftrightarrow \delta \in K \Leftrightarrow \delta \in L^G$. Or si $\sigma \in G$, $\sigma(\delta) = \epsilon(\sigma)\delta$. Donc $\delta \in K \Leftrightarrow \forall \sigma \in G, \epsilon(\sigma) = 1$. **Q.e.d.**

Exercice : déterminer le discriminant de $P := X^5 + 20X + 16$ et en déduire que le groupe de Galois de P est contenu dans A_5 (*indication* : vérifier que $\Delta_P = 2^{16} \cdot 5^6$).

11.2 Réduction modulo un nombre premier

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

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 :

$$\theta := u_1a_1 + \dots + u_na_n \in L[u_1, \dots, u_n]$$

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

Remarque : les θ^s , $s \in \mathfrak{S}_n$ sont deux à deux distincts.

On note $F(T, u) := \prod_{s \in \mathfrak{S}_n} (T - \theta^s) \in L[u_1, \dots, u_n, T]$. Alors $F(T, u) \in K[T, u]$. En effet, $\forall s \in \mathfrak{S}_n, \theta^s = u_1a_{s^{-1}(1)} + \dots + u_na_{s^{-1}(n)}$. Donc $F(T, u) \in \mathbb{Z}[T, u, \sigma_1, \dots, \sigma_n]$ où $\sigma_1, \dots, \sigma_n$ sont les fonctions symétriques élémentaires en les a_i :

$$\forall k, \sigma_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} a_{i_1} \dots a_{i_k}$$

$$= \pm \text{le coefficient de degré } n - k \text{ de } P(T) = (T - a_1) \dots (T - a_n) .$$

En particulier, $F(T, u) \in K[T, u]$.

Remarque : si $P(T) \in A[T]$ où A est un anneau intègre de corps des fractions K , alors $F(T, u) \in A[T, u]$.

Soit

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

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

On pose :

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

Théorème 11.2 *Supposons que F_1 est le facteur irréductible qui annule θ . On peut identifier $G := \text{Gal}_P := \text{Gal}(L/K)$ à un sous-groupe de \mathfrak{S}_n via :*

$$\sigma(a_i) = a_{\sigma(i)}$$

pour tout i et tout $\sigma \in G$.

Avec cette identification, on a $\mathfrak{g} = G$.

Démonstration : Soit $s \in G$. On a $F_1^s(\theta^s) = (F_1(\theta))^s = 0$. Or $\theta^s = u_1 a_{s^{-1}(1)} + \dots + u_n a_{s^{-1}(n)} = s^{-1} \cdot_G(\theta) = s^{-1}(\theta)$ (où on considère l'action de G sur $L[u][T]$ induite par l'action de G sur L). Donc $F_1^s(s^{-1}(\theta)) = 0 \Rightarrow s^{-1}(F_1^s(\theta)) = 0 \Rightarrow F_1^s(\theta) = 0$. Donc F_1^s (qui est l'un des F_i) et F_1 ont une racine commune donc sont égaux!

Réciproquement soit $s \in \mathfrak{g}$. Comme $F_1(\theta) = 0$, F_1 s'annule en tous les $\sigma(\theta)$, $\sigma \in G$. Donc F_1 est divisible dans $L[u][T]$ par $\prod_{\sigma \in G} (T - \sigma(\theta)) \in K[u][T]$. Or F_1 est irréductible donc $F_1 = \prod_{\sigma \in G} (T - \sigma(\theta))$. En particulier les racines de F_1 sont les $\sigma(\theta) = \theta^{\sigma^{-1}}$, $\sigma \in G$, où on voit σ^{-1} dans \mathfrak{S}_n . Mais $F_1^s = F_1 \Rightarrow F_1$ s'annule en $\theta^s \Rightarrow \theta^s = \theta^{\sigma^{-1}}$ pour un $\sigma \in G \Rightarrow s = \sigma^{-1} \in G$.

Q.e.d.

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 conjugué dans \mathfrak{S}_n 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 \overline{P} dans un corps de décomposition \overline{L} de \overline{K} . Soient $\theta := u_1 a_1 + \dots + u_n a_n$ et $\overline{\theta} := u_1 b_1 + \dots + u_n b_n$.

Soient $F(u, T) := \prod_{s \in \mathfrak{S}_n} (T - \theta^s)$ et $\overline{F}(u, T) := \prod_{s \in \mathfrak{S}_n} (T - \overline{\theta}^s) \in A/\mathfrak{p}[u, T]$. Ce sont des polynômes séparables : en effet, les racines b_i sont 2 à 2 distinctes donc les racines de \overline{F} aussi ; de même pour F . De plus, \overline{F} est la réduction de F mod \mathfrak{p} . En effet, soit $S(u, Y, T) := \prod_{s \in \mathfrak{S}_n} (T - (u_{s(1)} Y_1 + \dots + u_{s(n)} Y_n))$. Alors $S(u, Y, T) = \prod_{s \in \mathfrak{S}_n} (T - (u_1 Y_{s^{-1}(1)} + \dots + u_n Y_{s^{-1}(n)})) \in \mathbb{Z}[u, \Sigma_1, \dots, \Sigma_n, T]$ où les Σ_i sont les fonctions symétriques élémentaires en les Y_i . Si $P = T^n - \sigma_1 T^{n-1} + \dots + (-1)^n \sigma_n$, 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 σ_i . De même pour \overline{F} avec $\sigma_i \bmod \mathfrak{p}$ à la place de σ_i .

Soit $F = F_1 \dots F_r$ la décomposition de F en produits d'irréductibles de $K[u, T]$. On suppose que $F_1(\theta) = 0$ où $\theta := u_1 a_1 + \dots + u_n a_n$. Quand on identifie G à un sous-groupe de \mathfrak{S}_n via l'action sur les racines a_i , on a $G = \{s \in \mathfrak{S}_n : F_1^s = F_1\}$. On pose $\overline{\theta} := u_1 b_1 + \dots + u_n b_n$. Quitte à renuméroter les b_i , on peut supposer que $\overline{F}_1(\overline{\theta}) = 0$. Comme \overline{F} est séparable, les \overline{F}_i sont deux à deux premiers entre eux. Soit \overline{H} le facteur irréductible de \overline{F} dans $\overline{K}[u, T]$ qui annule $\overline{\theta}$. On a $\overline{H} | \overline{F}_1$. Donc si $s \in \mathfrak{S}_n$, représente un élément de \overline{G} , on a $\overline{H}^s = \overline{H}$ qui divise $\overline{F}_1^s = \overline{F}_1$. Or $F_1^s = F_i$ pour un certain $1 \leq i \leq r$ et comme les \overline{F}_j sont deux à deux premiers entre eux, \overline{F}_i et \overline{F}_1 ont un facteur commun (\overline{H}) donc sont égaux et $i = 1$ i.e. $F_1^s = F_1 \Leftrightarrow s \in G$.

Q.e.d.

Application : Soit $P \in \mathbb{Z}[T]$ un polynôme séparable. Soit p un nombre premier. On suppose que $P \bmod p$ est séparable sur \mathbb{F}_p . Soit $\overline{P} = \phi_1 \dots \phi_r$ 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 \overline{G} le groupe de Galois de \overline{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 : $P := T^5 - T - 1$ est irréductible modulo 5 et $P = (T^2 + T + 1)(T^3 + T^2 + 1) \bmod 2$ 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 à supports disjoints : $c\tau$. Donc $(c\tau)^3 = \tau \in G$ et G contient un 5-cycle et une transposition. Cela suffit pour dire que $G = \mathfrak{S}_5$.

Exercice : Montrer que le groupe de Galois sur \mathbb{Q} de $X^5 + 20X + 16$ est $\simeq \mathfrak{A}_5$ (indication : réduire modulo 3 et modulo 7).

12 Théorie de la ramification

12.1 Éléments entiers sur un anneau

Soient $A \leq B$ deux anneaux. On dit que $b \in B$ est entier sur A s'il existe $a_1, \dots, a_n \in A$ tels que :

$$b^n + a_1 b^{n-1} + \dots + a_n = 0 .$$

Si tous les éléments de B sont entiers sur A , on dit que B est entier sur A .

Exemple : $\sqrt{2}$ est entier sur \mathbb{Z} mais non $1/\sqrt{2}$.

Proposition 12.1 Soit $b \in B$. Sont équivalentes :

- (i) b est entier sur A ;
- (ii) $A[b]$ est un A -module de type fini ;
- (iii) il existe un $A[b]$ -module fidèle qui est un A -module de type fini.

Démonstration : $iii \Rightarrow i$: soit M un $A[b]$ -module fidèle qui est un A -module de type fini. Soient e_1, \dots, e_n des générateurs. Il existe des coefficients $a_{i,j} \in A$ tels que :

$$\forall j, be_j = \sum_i a_{i,j} e_i .$$

On en déduit par récurrence sur n que $\forall j, b^n e_j = \sum_i (M^n)_{i,j} e_i$ où $M := (a_{i,j})$. Mais alors, $\chi_M(b) e_j = \sum_i \chi_M(M)_{i,j} e_i = 0$ pour tout j . Donc $\chi_M(b) M = 0 \Rightarrow \chi_M(b) = 0$ car M est fidèle. Or, $\chi_M(X)$ est unitaire à coefficients dans A . Q.e.d.

Corollaire 12.1.1 *L'ensemble des éléments $b \in B$ entiers sur A est un sous-anneau de B .*

Démonstration : Si b_1, b_2 sont entiers sur A , alors $A[b_1]$ est un A -module de type fini tout comme $A[b_2]$. Donc $A[b_1, b_2]$ est un A -module de type fini. Si $x = b_1 \pm b_2$ ou $b_1 b_2$, alors $A[x] \subseteq A[b_1, b_2]$ qui est un $A[x]$ -module fidèle. Donc x est entier sur A . Q.e.d.

COURS DU MARDI 28 AVRIL 2015

Exercice 4 *Soient $A \leq B \leq C$ trois anneaux. Alors C entier sur B et B entier sur $A \Rightarrow C$ entier sur A .*

Exercice : si $x \in \mathbb{C}$, alors x est entier sur \mathbb{Z} si et seulement si son polynôme minimal unitaire est à coefficients entiers.

12.2 Anneaux de Dedekind

Soit K/\mathbb{Q} une extension finie. On note \mathcal{O}_K l'anneau des éléments de K entiers sur \mathbb{Z} .

Exemples : $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$, $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$.

Proposition 12.2 *i) L'anneau \mathcal{O}_K est intègre ;*

ii) l'anneau \mathcal{O}_K est nœthérien i.e. toute suite croissante d'idéaux $I_1 \leq \dots \leq I_k \leq \dots$ a un élément maximal i.e. tout idéal I de \mathcal{O}_K peut être engendré par un nombre fini d'éléments ;

- iii) l'anneau \mathcal{O}_K est int egralement clos i.e. si $x \in K = \text{Frac}(\mathcal{O}_K)$, est entier sur \mathcal{O}_K , alors $x \in \mathcal{O}_K$;
- iv) tout id eal premier non nul de \mathcal{O}_K est maximal.

D emonstration : ii : soit e_1, \dots, e_n une base de K/\mathbb{Q} . On peut choisir les $e_i \in \mathcal{O}_K$. Consid erons : $K \rightarrow \mathbb{Q}^n, x \mapsto (\text{Tr}_{K/\mathbb{Q}}(xe_1), \dots, \text{Tr}_{K/\mathbb{Q}}(xe_n))$. C'est K -lin eaire et  a envoie \mathcal{O}_K dans \mathbb{Z}^n . C'est injectif car $\text{Tr}_{K/\mathbb{Q}}(xe_i) = 0$ pour tout $i \Rightarrow \text{Tr}(xK) = 0 \Rightarrow x = 0$ ou $\text{Tr} = 0$ absurde ! Donc \mathcal{O}_K est un \mathbb{Z} -module de type fini. Si $I \leq \mathcal{O}_K$ est un id eal, c'est aussi un \mathbb{Z} -module de type fini.

iv : soit P un id eal premier non nul. \mathcal{O}_K/P est entier sur $\mathbb{Z}/(P \cap \mathbb{Z})$. Soit $x \in P$ non nul. $x^n + a_1x^{n-1} + \dots + a_n = 0$ pour certains entiers a_i avec $a_n \neq 0$. Alors $0 \neq a_n \in P \cap \mathbb{Z}$. Donc $P \cap \mathbb{Z} = (p)$ pour un certain nombre premier p . Donc \mathcal{O}_K/P est un corps et P est maximal. **Q.e.d.**

D efinition 6 Un anneau int egre A qui est int egralement clos, n eth erien et dont tous les id eaux premiers non nuls sont maximaux est un anneau de Dedekind.

Exemple : les corps, $\mathbb{Z}, \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$, les anneaux de la forme $\mathbb{C}[X, Y]/(f)$ o u $f \in \mathbb{C}[X, Y]$ est irr eductible et $(f, \partial_X f, \partial_Y f) = 1$.

Th eor eme 12.3 (Factorisation unique en produit d'id eaux premiers)
 Tout id eal non nul \mathfrak{a} de \mathcal{O}_K s' ecrit :

$$\mathfrak{a} = P_1 \dots P_r$$

pour certains P_i id eaux premiers non nuls de \mathcal{O}_K uniques   permutation pr es des termes.

Exemple : dans $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ donc \mathcal{O} n'est pas factoriel, mais on a bien : $(6) = P_1^2 P_2 P_3$ avec $P_1 = (2, 1 + \sqrt{-5}), P_2 = (3, 2 + \sqrt{-5}), P_3 = (3, 2 - \sqrt{-5})$.

Lemme 12.4 Soit $\mathfrak{a} \leq \mathcal{O}_K$ un id eal non nul. Il existe P_1, \dots, P_r des id eaux premiers non nuls tels que $\mathfrak{a} \geq P_1 \dots P_r$.

D emonstration : Par l'absurde : soit I un id eal maximal parmi ceux qui n'ont pas la propri et e voulue. Alors I n'est pas premier. Soient x, y tels que $xy \in I$ mais $x, y \notin I$. Par maximalit e, $I + (x) \geq P_1 \dots P_r$ et $I + (y) \geq Q_1 \dots Q_s$ pour certains id eaux premiers non nuls P_i, Q_j . Mais alors $I \geq (I + (x))(I + (y)) \geq P_1 \dots P_r Q_1 \dots Q_s$ d'o u la contradiction ! **Q.e.d.**

Lemme 12.5 Soit $P \leq \mathcal{O}_K$ un idéal premier non nul. On pose :

$$P^{-1} := \{x \in K : xP \leq \mathcal{O}_K\} .$$

Alors $\mathcal{O}_K \subsetneq P^{-1}$ et si $\mathfrak{a} \leq \mathcal{O}_K$ est un idéal non nul, $\mathfrak{a} \subsetneq \mathfrak{a}P^{-1}$.

Remarque : $P^{-1} \geq \mathcal{O}_K$.

Démonstration : On montre d'abord que $P^{-1} \neq \mathcal{O}_K$. Soit $a \in P$ non nul. Soient P_1, \dots, P_r des idéaux premiers non nuls avec r minimal tels que $P_1 \dots P_r \leq (a) \leq P$. Comme P est premier, l'un des P_i par ex. P_1 est P . Comme r est minimal, il existe $b \in P_2 \dots P_r$ tel que $b \notin (a)$. Mais alors $a^{-1}b \notin \mathcal{O}_K$. Or $bP = bP_1 \leq (a) \Rightarrow a^{-1}bP \leq \mathcal{O}_K \Rightarrow a^{-1}b \in P^{-1}$.

Supposons par l'absurde qu'il existe $a \leq \mathcal{O}_K$ un idéal non nul tel que $aP^{-1} = a$. Soient x_1, \dots, x_n des générateurs de a comme \mathbb{Z} -modules. Si $y \in P^{-1}$, on a :

$$yx_i = \sum_j a_{i,j} x_j$$

pour certains $a_{i,j} \in \mathcal{O}_K$. Soit $A := (a_{i,j}) \in \mathcal{M}_n(\mathcal{O}_K)$. On a $\chi_A(y)x_i = \sum_j \chi_A(A)_{i,j} x_j = 0$ pour tout i . Donc $\chi_A(y) = 0$ et y est entier sur \mathcal{O}_K . Donc $y \in \mathcal{O}_K$. donc $P^{-1} \leq \mathcal{O}_K$ absurde!

Q.e.d.

Démonstration du théorème de factorisation :

Existence : par l'absurde : soit $\mathfrak{a} \leq \mathcal{O}_K$ un idéal maximal pour la propriété de n'être pas factorisable en produits d'idéaux premiers. Il existe P un idéal maximal (premier non nul) tel que $\mathfrak{a} \leq P$. On a :

$$\mathfrak{a} \leq \mathfrak{a}P^{-1} \leq PP^{-1} \leq \mathcal{O}_K .$$

Comme $PP^{-1} \neq P$, on a $PP^{-1} = \mathcal{O}_K$. Or $\mathfrak{a}P^{-1} \neq \mathfrak{a}$. Par maximalité, $\mathfrak{a}P^{-1} = P_1 \dots P_r$ pour certains idéaux premiers non nuls P_i . Mais alors :

$$\mathfrak{a} = PP_1 \dots P_r .$$

Contradiction!

Unicité : Si $\mathfrak{a} = P_1 \dots P_r = Q_1 \dots Q_s$ pour certains idéaux premiers non nuls P_i, Q_j . Alors P_1 contient l'un des Q_j par exemple Q_1 . Par maximalité, $P_1 = Q_1$. En multipliant par P_1^{-1} , on trouve : $P_2 \dots P_r = Q_2 \dots Q_s$. On conclut par récurrence. **Q.e.d.**

COURS DU MARDI 5 MAI 2015

Exercice 5 Soit A un anneau de Dedekind.

a) Tout idéal I de A est inversible : $II^{-1} = A$ où $I^{-1} = \{x \in K : xI \leq A\}$.

- b) Un anneau de Dedekind avec un nombre fini d'idéaux maximaux est principal (par exemple un anneau de Dedekind local).
- c) Si I est un idéal non nul, alors A/I est principal.
- d) Tout idéal peut être engendré par deux éléments.

Soit A un anneau de Dedekind (par ex. : $A = \mathbb{Z}$), soit K (par ex. : $K = \mathbb{Q}$) le corps des fractions de A . Soit L/K une extension finie *séparable*, soit $B := \overline{A}^L$ la fermeture intégrale de A dans L i.e. B est l'anneau des éléments de L entiers sur A (par ex. : $B = \mathcal{O}_L$). Alors B est un anneau de Dedekind (exo)

Soit \mathfrak{p} un idéal premier non nul de A . Il existe P_1, \dots, P_g des idéaux premiers non nuls de B deux à deux distincts tels que $B\mathfrak{p} = P_1^{e_1} \dots P_g^{e_g}$ pour certains entiers $e_i \geq 1$, $g \geq 1$. Tout cela est uniquement déterminé.

Définition 7 Les entiers e_i sont les indices de ramification de \mathfrak{p} dans L . Si tous les e_i sont 1, on dit que \mathfrak{p} est non ramifié dans L , si l'un des $e_i > 1$, on dit que \mathfrak{p} est ramifié dans L .

Exemple : si $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $B = \mathbb{Z}[i]$, alors on a :

	e	f	g
$p = 2$	2	1	1
$p = 1 \pmod{4}$	1	1	2
$p = -1 \pmod{4}$	1	2	1

car $2\mathbb{Z}[i] = (1+i)^2$, si p est premier de la forme $1 \pmod{4}$, $p\mathbb{Z}[i] = P_1P_2$ pour certains idéaux premiers distincts P_1, P_2 de $\mathbb{Z}[i]$, si p est premier de la forme $-1 \pmod{4}$, $p\mathbb{Z}[i]$ reste premier. Donc 2 est le seul nombre premier qui se ramifie dans $\mathbb{Q}(i)$.

12.3 Égalité fondamentale

Théorème 12.6 Si L/K est galoisienne, alors $e_1 = \dots = e_g$. Autrement dit $B\mathfrak{p} = (P_1 \dots P_g)^e$ pour un certain $e \geq 1$.

Démonstration : Soit $G := \text{Gal}(L/K)$. Le groupe G préserve B . De plus, G permute les P_i car ce sont les idéaux premiers non nuls de B qui contiennent \mathfrak{p} . Posons $P := P_1$. Soit $\mathcal{P} := \{\sigma(P) : \sigma \in G\}$. Supposons par l'absurde qu'il existe un i tel que $P_i \notin \mathcal{P}$. D'après le théorème des restes chinois, $B/P_1 \dots P_r \simeq \prod_j B/P_j$. Donc il existe $\alpha \in P$ tel que $\alpha = 0 \pmod{P_i}$ et $\alpha = 1 \pmod{\sigma P}$ pour tout $\sigma \in G$.

Soit $a := \prod_{\sigma \in G} \sigma \alpha = N_{L/K}(\alpha)$. On a $a \in A \cap P_i = \mathfrak{p} \leq P_1^{e_1} \dots P_g^{e_g}$. Donc $a \in P$ et il existe un des facteurs $\sigma \alpha$, $\sigma \in G$, tel que $\sigma \alpha \in P$. Mais alors $\alpha \in \sigma^{-1}P$ ce qui contredit $\alpha = 1 \pmod{\sigma^{-1}P}$ ($\forall \sigma \in G$).

On dit que les P_i sont les idéaux conjugués de P .

Donc $B\mathfrak{p} = \sigma(P_1^{e_1} \dots P_g^{e_g}) = \sigma(P_1)^{e_1} \dots \sigma(P_g)^{e_g}$. Soit i , soit σ tel que $\sigma(P_1) = P_i$. On trouve : $e_1 = e_i$. **Q.e.d.**

Considérons le corps résiduel B/P_i . C'est une extension finie du corps fini A/\mathfrak{p} . Soit $f_i := [B/P_i : A/\mathfrak{p}]$.

Théorème 12.7 *Si L/K est galoisienne, tous les corps résiduels B/P_i ont le même degré $f = f_1 = \dots = f_g$.*

Démonstration : Si $\sigma(P_1) = P_i$, alors σ induit un isomorphisme $B/P_1 \simeq B/P_i$. **Q.e.d.**

Théorème 12.8 (égalité fondamentale) *Soit $n = |G|$. Alors $B\mathfrak{p} = (P_1 \dots P_g)^e$ et $n = efg$.*

Démonstration : Dans le cas où $A = \mathbb{Z}$:

Soit p le nombre premier > 0 tel que $\mathfrak{p} = (p)$.

$\mathcal{O}_L/(p) \simeq \prod_i \mathcal{O}_L/P_i^e$. Or \mathcal{O}_L est un \mathbb{Z} -module libre de rang n . Donc $\mathcal{O}_L/(p) \simeq (\mathbb{Z}/p\mathbb{Z})^n$ est de cardinal p^n . Pour tout j , P_i^j/P_i^{j+1} est un \mathcal{O}_L/P_i -espace vectoriel de dimension 1 : en effet, soit $x \in P_i^j \setminus P_i^{j+1}$ alors $(x) = \prod_{k \neq i} P_k^{r_k} P_i^{r_i}$ pour certains idéaux premiers non nuls deux à deux distincts et certains entiers r_k . Comme $(x) \leq P_i^j$, $r_i \geq j$ (si $r_i < j$, on multiplie par $P_i^{-r_i}$ et on trouve une contradiction). Comme $x \notin P_i^{j+1}$, $r_i = j$. Donc $x\mathcal{O}_L/P_i^{j+1} = P_i^j/P_i^{j+1}$ car si $P \neq P_i$, $P/P_i^{j+1} = \mathcal{O}_L/P_i^{j+1}$. On en déduit que $\mathcal{O}_L/P_i \rightarrow P_i^j/P_i^{j+1}$, $t \mapsto tx$ est surjectif. De plus, si $t \in \mathcal{O}_L$, $tx \in P_i^{j+1} \Rightarrow t \in P_i$ (en effet, si $t \notin P_i$, t est inversible dans \mathcal{O}_L/P_i donc il existe $s \in \mathcal{O}_L$ tel que $st = 1 \pmod{P_i}$ mais alors d'une part, $stx \in P_i^{j+1}$ et d'autre part, $stx = x \pmod{P_i^{j+1}} \Rightarrow x \in P_i^{j+1}$ absurde !) donc on a un isomorphisme $\mathcal{O}_L/P_i \simeq P_i^j/P_i^{j+1}$.

Comme $\mathcal{O}_L/P_i^e \geq P_i/P_i^e \geq \dots \geq P_i^{e-1}/P_i^e \geq 0$ et pour tout $j = 0$ à $e-1$,

$$P_i^j/P_i^e/P_i^{j+1}/P_i^e \simeq P_i^j/P_i^{j+1} \simeq \mathcal{O}_L/P_i,$$

on a $|\mathcal{O}_L/P_i^e| = \prod_{j=0}^{e-1} |\mathcal{O}_L/P_i| = p^{ef}$. Donc $p^n = p^{efg}$.

Cas général : Soient $S := A \setminus \mathfrak{p}$, $A' := S^{-1}A := \{a/s : a \in A, s \in S\}$, $B' := S^{-1}B := \{b/s : b \in B, s \in S\}$. Alors A' est principal, $\text{Frac}(A') = K$ et $B' = \overline{A'}^L$ est un A' -module libre de rang $n = [L : K]$ (exo). On peut raisonner comme pour \mathbb{Z} : $B/B\mathfrak{p} \simeq B'/B'\mathfrak{p}$, $A'/\mathfrak{p}A' \simeq A/\mathfrak{p}$, $B'/B'\mathfrak{p}$ est un $A'/A'\mathfrak{p}$ -espace vectoriel de rang n . De plus, dans l'anneau de Dedekind

B' , on a la décomposition $B'\mathfrak{p} = \prod_{i=1}^g (B'P_i)^{e_i}$ où les idéaux $B'P_i$ sont premiers, non nuls, deux à deux distincts. Donc $n = \sum_i e_i [B'/B'P_i : A'/A'\mathfrak{p}] = \sum_i e_i f_i = efg$. Q.e.d.

12.4 Discriminant

Définition 8 Soient $A \leq B$ deux anneaux commutatifs tels que B est un A -module libre de rang n . Si $x_1, \dots, x_n \in B$, on note $D_{B/A}(x_1, \dots, x_n) := \det(\text{Tr}_{B/A}(x_i x_j))_{1 \leq i, j \leq n}$. On note $\mathcal{D}_{B/A}$ l'idéal principal de A engendré par $D(x_1, \dots, x_n)$ où x_1, \dots, x_n est une A -base de B .

Si L/K est une extension finie séparable. On note $\Delta_{L/K}$ l'idéal de \mathcal{O}_K engendré par les $D_{L/K}(x_1, \dots, x_n)$ où (x_1, \dots, x_n) est une K -base de L contenue dans \mathcal{O}_L .

Exercice 6 Si $A \leq B$ sont deux anneaux commutatifs tels que B est un A -module libre, si x_1, \dots, x_n et x'_1, \dots, x'_n sont deux bases du A -module B , alors :

$$D_{B/A}(x'_1, \dots, x'_n) = (\det P)^2 D_{B/A}(x_1, \dots, x_n)$$

où P est la matrice de passage de la base des x_i dans la base des x'_i .

Proposition 12.9 Si L/K est une extension séparable et si $\sigma_1, \dots, \sigma_n$ sont les n K -plongements de L dans Ω une extension algébriquement close de L , alors pour toute base x_1, \dots, x_n de L/K , on a :

$$D_{L/K}(x_1, \dots, x_n) = \det(\sigma_i(x_j))_{i,j}^2 \neq 0 .$$

Démonstration : Soit Q la matrice $(\sigma_i(x_j))_{1 \leq i, j \leq n}$. Pour tous i, j , on a $\text{Tr}_{L/K}(x_i x_j) = \sum_{k=1}^n \sigma_k(x_i x_j) = \sum_{k=1}^n \sigma_k(x_i) \sigma_k(x_j) = ({}^t Q Q)_{i,j}$. Q.e.d.

Remarque : en particulier, si L/K est une extension finie séparable, la K -forme quadratique $L \rightarrow K$, $x \mapsto \text{Tr}_{L/K}(x^2)$ est non dégénérée.

Exemple : si $L = K[x]$ est une extension finie séparable de degré n , alors $D_{L/K}(1, \dots, x^{n-1}) = (-1)^{n(n-1)/2} N_{L/K}(F'(x)) = \text{Disc}(F)$ où F est le polynôme minimal de x sur K .

Définition 9 (discriminant absolu) Soit K/\mathbb{Q} une extension finie de degré n . On note $D_{K/\mathbb{Q}} := D(x_1, \dots, x_n)$ où x_1, \dots, x_n est une \mathbb{Z} -base de \mathcal{O}_K .

Exercice : c'est indépendant de la \mathbb{Z} -base choisie.

Exemple : si $K = \mathbb{Q}(\sqrt{d})$ où d est un entier $\neq 1$ sans facteur carré, alors :

d	\mathcal{O}_K	$D_{K/\mathbb{Q}}$
$1 \pmod 4$	$\mathbb{Z} \oplus \mathbb{Z} \frac{1+\sqrt{d}}{2}$	d
$2 \pmod 4$	$\mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$	$4d$
$-1 \pmod 4$	$\mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$	$4d$

En particulier, si K/\mathbb{Q} est une extension quadratique où 2 est le seul nombre premier ramifié, alors $K = \mathbb{Q}(i)$ ou $\mathbb{Q}(\sqrt{-2})$ ou $\mathbb{Q}(\sqrt{2})$.

Théorème 12.10 (Hermite-Minkowski) *Si K/\mathbb{Q} est une extension finie de degré > 1 , alors $|D_{K/\mathbb{Q}}| > 1$.*

Démonstration : cf. Pierre Samuel, *Théorie algébrique des nombres*, §4.3, th. 1 Q.e.d.

12.5 Discriminant et ramification

Lemme 12.11 *Soient A un anneau et B_1, \dots, B_r des anneaux contenant A qui sont des A -modules libres de rang fini. On note $B := \prod_{i=1}^r B_i$. Alors $\mathcal{D}_{B/A} = \prod_{i=1}^r \mathcal{D}_{B_i/A}$.*

Lemme 12.12 *Soient $A \leq B$ deux anneaux tels que B est un A -module libre ayant une base x_1, \dots, x_n . Soit \mathfrak{a} un idéal de A . Si on note $\bar{x}_i := x_i \bmod \mathfrak{a}$, alors on a :*

$$D(\bar{x}_1, \dots, \bar{x}_n) = D(x_1, \dots, x_n) \bmod \mathfrak{a} .$$

Lemme 12.13 *Soient K un corps fini ou un corps de caractéristique nulle et L une K -algèbre de dimension finie. L'algèbre L/K est réduite si et seulement si $\mathcal{D}_{L/K} \neq 0$.*

Démonstration : Supposons L non réduite. Il existe $0 \neq x_1 \in L$ nilpotent. On complète en x_1, \dots, x_n une base de L/K . Pour tout j , la multiplication par $x_1 x_j$ est un endomorphisme nilpotent de L donc de trace nulle : la matrice $(\text{Tr}(x_i x_j))_{i,j}$ a donc une première ligne nulle et son déterminant est 0. Réciproquement, supposons L réduite. Alors l'idéal (0) contient un produit fini d'idéaux premiers (éventuellement nuls!) : $(0) = P_1^{e_1} \dots P_g^{e_g}$ où les P_i sont des idéaux premiers deux à deux distincts. Soit $x \in P_1 \cap \dots \cap P_g$. On a $x^{e_1 + \dots + e_g} \in P_1^{e_1} \dots P_g^{e_g} \Rightarrow x^{e_1 + \dots + e_g} = 0 \Rightarrow x = 0$ car L est réduite. Donc $0 = P_1 \cap \dots \cap P_g$. Les L/P_i sont des K -algèbres de dimension finie intègres donc sont des corps et les P_i sont maximaux. On a donc $L = L/0 \simeq \prod_i L/P_i$. Donc $\mathcal{D}_{L/K} = \prod_i \mathcal{D}_{L_i/K} \neq 0$ (où $L_i := L/P_i$).

Q.e.d.

Théorème 12.14 *Soit K/\mathbb{Q} une extension finie. Le nombre premier $p \in \mathbb{Z}$ se ramifie dans \mathcal{O}_K si et seulement si $p | D_{K/\mathbb{Q}}$.*

Démonstration : On a p qui se ramifie si et seulement si l'algèbre $\mathcal{O}_K/p\mathcal{O}_K$ est non réduite i.e. $\mathcal{D}_{\mathcal{O}_K/p} = (D_{K/\mathbb{Q}} \bmod p) = 0$ i.e. $p | D_{K/\mathbb{Q}}$.

Q.e.d.

Corollaire 12.14.1 Si K/\mathbb{Q} est une extension finie où aucun nombre premier ne se ramifie alors $K = \mathbb{Q}$.

Plus généralement, on a :

Théorème 12.15 Soit A un anneau de Dedekind, soit K le corps des fractions de A . Soit L/K une extension finie séparable, soit $B := \overline{A}^L$ la fermeture intégrale de A dans L . Alors un idéal premier \mathfrak{p} de A est ramifié dans L si et seulement si $\mathcal{D}_{B/A} \leq \mathfrak{p}$ (où $\mathcal{D}_{B/A}$ est l'idéal de A engendré par les $D_{L/K}(x_1, \dots, x_n)$, (x_1, \dots, x_n) base de L comme K -ev contenue dans B).

Exercice 7 Soient trois corps $K \leq K' \leq K''$ tels que $[K'' : K]$ est finie. On a la formule de transitivité suivante :

$$\mathcal{D}_{K''/K} = N_{K'/K}(\mathcal{D}_{K''/K'}) \cdot \mathcal{D}_{K'/K}^{[K'' : K']}$$

où pour tout idéal \mathfrak{a}' de $\mathcal{O}_{K'}$, on note $N_{K'/K}(\mathfrak{a}')$ l'idéal de \mathcal{O}_K engendré par les $N_{K'/K}(a')$, $a' \in \mathfrak{a}'$.

Exercice 8 Soient p un nombre premier et ζ une racine primitive p -ième de l'unité. On a $D_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \pm p^{p-2}$, l'anneau des entiers de $\mathbb{Q}(\zeta)$ est $\mathbb{Z}[\zeta]$ et p est le seul nombre premier p ramifié dans $\mathcal{O} := \mathbb{Z}[\zeta]$. L'idéal $(1 - \zeta)$ est premier dans \mathcal{O} , c'est le seul idéal premier au-dessus de p et on a $p\mathcal{O} = (1 - \zeta)^{p-1}$ et $\mathbb{Z}[\zeta]/(1 - \zeta) \simeq \mathbb{Z}/p\mathbb{Z}$. On a donc $e(\mathbb{Q}(\zeta)/\mathbb{Q}) = p-1$, $f(\mathbb{Q}(\zeta)/\mathbb{Q}) = 1$ et $g(\mathbb{Q}(\zeta)/\mathbb{Q}) = 1$.

12.6 Groupes de décomposition et d'inertie

Soit L/K une extension galoisienne finie de groupe de Galois G . Soit P un idéal premier de \mathcal{O}_L . On note $Z_P := \{s \in G : s(P) = P\}$.

Proposition 12.16 $[G : Z_P] = g$ le nombre d'idéaux premiers de \mathcal{O}_L au-dessus de $\mathfrak{p} := P \cap \mathcal{O}_K$ et $|Z_P| = ef$.

Définition 10 (groupe d'inertie) Soient $k_L := \mathcal{O}_L/P$ et $k_K := \mathcal{O}_K/\mathfrak{p}$. On note I_P le noyau du morphisme $Z_P \rightarrow \text{Gal}(k_L/k_K)$.

Proposition 12.17 Le morphisme $Z_P \rightarrow \text{Gal}(k_L/k_K)$ est surjectif. En particulier, $[Z_P : I_P] = f$ et $|I_P| = e$.

Démonstration :

On suppose d'abord que $G = Z_P$. Soit $x \in \mathcal{O}_L$ tel que $k_L = k_K[\overline{x}]$ où $\overline{x} := x \bmod P$. Soit $s \in \text{Gal}(k_K/k_L)$. Soit f le polynôme minimal de x sur K . Notons x_1, \dots, x_m , $m \leq n$ ses racines. Notons $\overline{f} := (X - \overline{x}_1) \dots (X - \overline{x}_m) \in k_K[X]$. On a $\overline{f}(\overline{x}) = 0 \Rightarrow \overline{f}(s(\overline{x})) = 0$. Donc il existe i tel que $s(\overline{x}) = \overline{x}_i$. Soit $\sigma \in G$ tel que $\sigma(x) = x_i$. On a bien $\overline{\sigma} = s$.

Cas général : Soit $K' := L^{Z_P}$. Soit $P' := P \cap \mathcal{O}_{K'}$. On a $P' \mathcal{O}_L = P^{e(L/K')} \dots$ et $\mathfrak{p} \mathcal{O}_{K'} = P'^{e'}$... pour un certain $e' \geq 1$. Comme $\mathcal{O}_K \leq \mathcal{O}_{K'} \leq \mathcal{O}_L$, $\mathfrak{p} \mathcal{O}_L = P^{e(L/K)} \dots$ avec $e(L/K) = e' e(L/K') \geq e(L/K')$.

On a aussi :

$$k_K \leq \mathcal{O}_{K'}/P' \leq \mathcal{O}_L/P$$

donc $[k_L : k_K] = f(L/K) = [\mathcal{O}_L/P : \mathcal{O}_{K'}/P'] [\mathcal{O}_{K'}/P' : k_K] \geq f(L/K')$.

Or si on considère l'extension galoisienne L/K' , comme $\text{Gal}(L/K') = Z_P$, on a $g(L/K') = 1$. D'où :

$$[L : K'] = e(L/K') f(L/K') = |Z_P| = [L : K] / g(L/K) = e(L/K) f(L/K) .$$

Comme $e(L/K') \leq e(L/K)$ et $f(L/K') \leq f(L/K)$, on a forcément $e(L/K') = e(L/K)$ et $f(L/K') = f(L/K)$. En particulier $\mathcal{O}_{K'}/P' = \mathbb{F}_p$. Donc on peut raisonner avec L/K' à la place de L/K et dans ce cas, $\text{Gal}(L/K') = Z_P$.

Q.e.d.

En déduire :

Exercice 9 Soit K/F une extension galoisienne de corps de nombres. Soit P un idéal premier de \mathcal{O}_K , soit $I := I_P$ et $K_I := K^I$. Alors $f(K/K_I) = 1$ et $g(K/K_I) = 1$; si $\mathfrak{p} := P \cap \mathcal{O}_F$, alors \mathfrak{p} est non ramifié dans K_I et K_I contient toutes les extensions $F \leq K' \leq K$ où \mathfrak{p} est non ramifié. En particulier, si $F \leq F', F'' \leq K$, si \mathfrak{p} un idéal premier non nul de \mathcal{O}_F est non ramifié dans F' et dans F'' , \mathfrak{p} est non ramifié dans le compositum $F'F''$ (indication : en utilisant la première partie : soit M/F une extension galoisienne contenant F, F' , soit I le groupe d'inertie d'un idéal premier au-dessus de \mathfrak{p} , alors $F, F' \leq M^I \Rightarrow FF' \leq M^I$!).

12.7 Théorème de Kronecker-Weber

Pour tout $n > 1$, on pose $\zeta_n := e^{2i\pi/n}$.

Nous allons démontrer :

Théorème 12.18 (de Kronecker-Weber) Soit K/\mathbb{Q} une extension galoisienne finie de groupe de Galois abélien. Alors il existe n tel que $K \leq \mathbb{Q}(\zeta_n)$.

Puisque tout groupe abélien fini est produit de groupes cycliques, il suffit de traiter le cas où $G := \text{Gal}(K/\mathbb{Q})$ est cyclique d'ordre une puissance d'un nombre premier !

En effet, si K/\mathbb{Q} est une extension galoisienne de groupe $G_1 \times G_2$, si on pose $K_i := K^{G_i}$, alors K_1/\mathbb{Q} (resp. K_2/\mathbb{Q}) est galoisienne de groupe de Galois $\simeq G_2$ (resp. G_1) et $K = K_1 K_2$ car $\text{Gal}(K/K_1 K_2) = \text{Gal}(K/K_1) \cap \text{Gal}(K/K_2) = G_1 \times 1 \cap 1 \times G_2 = 1$.

Lemme 12.19 Soit K/\mathbb{Q} une extension finie abélienne. Soit p un nombre premier qui ne divise pas $[K : \mathbb{Q}]$. Soit I le groupe d'inertie d'un idéal premier P au-dessus de p dans K . Alors, I est cyclique d'ordre qui divise $p - 1$.

Démonstration : Soit D le groupe de décomposition de P au-dessus de \mathbb{Q} . Soit $k_K := \mathcal{O}_K/P$ le corps résiduel. Soit $\pi \in P \setminus P^2$. Si $\sigma \in D$, on note $\bar{\sigma} \in \text{Gal}(k_K/\mathbb{F}_p)$ l'automorphisme induit sur k_K . Considérons l'application :

$$f : D \rightarrow k_K^\times$$

définie par $f(\sigma) := \sigma(\pi)/\pi \bmod P$ pour un certain élément $\pi \in P \setminus P^2$ fixé. On vérifie que :

$$\forall \sigma, \tau \in D, f(\sigma\tau) = f(\sigma)\bar{\sigma}(f(\tau)) .$$

En particulier, $f|_I$ est un morphisme de groupes. Soit $\sigma \in \ker(f|_I)$. Soit m l'ordre de σ . Alors $p \nmid m$. De plus $\sigma(\pi) = \pi \bmod P^2$. supposons que $\sigma(\pi) = \pi + a\pi^k \bmod P^{k+1}$ pour un certain $a \in \mathcal{O}_K$ et un $k \geq 2$. Comme $\mathcal{O}_{K^I}/(P \cap \mathcal{O}_{K^I}) \simeq \mathcal{O}_K/P$ (exo), on peut supposer que a est fixé par I . On a :

$$\pi = \sigma^m(\pi) = \pi + a(\pi^k + \dots + \sigma^{m-1}(\pi)^k) \bmod P^{k+1} .$$

Or, $\forall k, \sigma(\pi)^k = \pi^k \bmod P^{k+1}$. Donc $\pi = \pi + am\pi^k \bmod P^{k+1}$. D'où, $a = 0 \bmod P$. On a donc montré que $\sigma(\pi) - \pi \in \bigcap_{k \geq 2} \pi^k = 0$. Donc $\sigma(\pi) = \pi$. On en déduit que $\sigma = \text{Id}$ sur \mathcal{O}_K et donc sur K (en effet, pour tout $x \in \mathcal{O}_K$, pour tout $n \geq 0$, il existe $a_0, \dots, a_n \in \mathcal{O}_{K^I}$ tels que $x = a_0 + a_1\pi + \dots + a_n\pi^n \bmod P^{n+1}$; donc $\sigma(x) - x \in \bigcap_n P^n = 0$).

ainsi $f|_I$ est injective. Pour terminer, il suffit de montrer que $f(I) \leq \mathbb{F}_p^\times$. OR, si $\sigma \in I$ et $\tau \in D$, comme D est abélien, $f(\sigma\tau) = f(\tau\sigma) = f(\tau)\bar{\tau}(f(\sigma)) \Rightarrow f(\sigma)f(\tau) = f(\tau)\bar{\tau}(f(\sigma)) \Rightarrow f(\sigma) = \bar{\tau}(f(\sigma))$. Donc $f(\sigma)$ est fixé par tous les éléments de $\text{Gal}(k_K/\mathbb{F}_p)$. **Q.e.d.**

Corollaire 12.19.1 Si K/\mathbb{Q} est une extension finie abélienne de degré impair, alors 2 n'est pas ramifié dans K .

Lemme 12.20 Soit K/\mathbb{Q} une extension finie cyclique de degré l' où l est un nombre premier. Il existe K'/\mathbb{Q} une autre extension finie cyclique de degré une puissance de l telle que l est le seul nombre premier ramifié dans K'/\mathbb{Q} et telle que :

K est inclus dans un corps cyclotomique si et seulement si K' l'est aussi.

Démonstration : Supposons que $p \neq l$ est un nombre ramifié dans K . Alors si $l \neq 2$, p est impair d'après le corollaire précédent. Soit l^a la plus grande puissance de l divisant $p - 1$. Soit F le sous-corps de $\mathbb{Q}(\zeta_p)$ de degré

l^a sur \mathbb{Q} . Soit $E := FK$. Soit K_I le corps d'inertie de E/\mathbb{Q} pour p (pour un idéal premier P de \mathcal{O}_E au-dessus de p , $K_I := E^{I_P}$). Alors $E = FK_I$, donc K est inclus dans un corps cyclotomique si et seulement si K_I l'est aussi. De plus, p n'est plus ramifié dans K_I et un nombre premier non ramifié dans K reste non ramifié dans K_I ... en un nombre fini d'étapes on arrive donc à un K' comme dans l'énoncé à partir de K . **Q.e.d.**

Il reste donc à démontrer :

Théorème 12.21 *Soit K/\mathbb{Q} une extension finie cyclique de degré l^r pour un nombre premier l et un $r \geq 1$. On suppose que l est le seul nombre premier ramifié dans K . Alors K est contenu dans un corps cyclotomique.*

Démonstration : On distingue les cas :

si $l = 2$

Supposons que K/\mathbb{Q} est une extension cyclique de degré 2^r pour un certain $r \geq 1$ et que 2 est le seul nombre premier ramifié dans K . Comme K/\mathbb{Q} est cyclique, K contient une seule extension quadratique de degré 2 (où 2 est le seul nombre premier ramifié). Donc $\mathbb{Q}(i)$ ou $\mathbb{Q}(i\sqrt{2}) \not\subseteq K$. Par exemple si $i \notin K$, considérons $K_1 := K(i) \cap \mathbb{R}$ qui est de degré 2^r sur \mathbb{Q} . Soit $F := \mathbb{Q}(\zeta_{2^{r+2}}) \cap \mathbb{R}$. On a aussi $[F : \mathbb{Q}] = 2^r$. Considérons le corps $E := FK_1$. Alors K est inclus dans un corps cyclotomique $\Leftrightarrow K_1$ l'est $\Leftrightarrow E$ l'est. Si E/\mathbb{Q} est cyclique, alors E contient une unique extension de \mathbb{Q} de degré 2^r donc $F = K_1$ est contenu dans une extension cyclotomique et K aussi! Si E/\mathbb{Q} n'est pas cyclique, alors E contient une extension de \mathbb{Q} de groupe de Galois $\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En particulier, E contient au moins deux extensions quadratiques réelles où 2 est le seul nombre premier ramifié. Or $\mathbb{Q}(\sqrt{2})$ est la seule extension de la sorte!

Q.e.d.

si l impair

Q.e.d.

Lemme 12.22 *Soit p un nombre premier impair. Il existe une unique extension cyclique K/\mathbb{Q} de degré p où p est le seul nombre premier ramifié (i.e. dont le discriminant est une puissance de p). Il s'agit de l'unique sous-corps de $\mathbb{Q}(\zeta_{p^2})$ de degré p sur \mathbb{Q} .*

Démonstration : *Existence* : exo!

Unicité : soit K' comme dans l'énoncé. Soit K l'unique sous-corps de $\mathbb{Q}(\zeta_{p^2})$ de degré p sur \mathbb{Q} . Soit $L = \mathbb{Q}(\zeta)$ où $\zeta := \zeta_p \neq 1$ est une racine p -ième

de l'unité. Il est clair que $KL = \mathbb{Q}(\zeta_{p^2})$. D'après le théorème de Kummer 9.2, $K'L = L(\sqrt[p]{\alpha})$ pour un $\alpha \in L$. On peut supposer que $\alpha \in \mathcal{O}_L$ (en effet, $n\alpha \in \mathcal{O}_L$ pour un certain entier $n > 0$ et donc $n^p\alpha \in \mathcal{O}_L$ convient aussi. Soit $\lambda := 1 - \zeta \in L$. On a $N_{L/\mathbb{Q}}(\lambda) = p$ donc (λ) est l'unique idéal premier de \mathcal{O}_L au-dessus de p . On va montrer que l'on peut choisir $\alpha = 1 \pmod{\lambda^p}$ dans \mathcal{O}_L . En effet, soit τ un générateur de $\text{Gal}(L/\mathbb{Q})$ qu'on prolonge à $K'L$. Soit σ un générateur de $\text{Gal}(K'L/L) \simeq \text{Gal}(K'/(K' \cap L)) = \text{Gal}(K'/\mathbb{Q})$ si on suppose $K' \neq \mathbb{Q}$. Comme $\text{Gal}(K'L/\mathbb{Q})$ est abélien (exo), $\sigma(\tau(\sqrt[p]{\alpha})) = \tau(\sigma(\sqrt[p]{\alpha})) = \tau(\zeta \sqrt[p]{\alpha}) = \zeta^l \tau(\sqrt[p]{\alpha})$ pour un certain l générateur de $\mathbb{Z}/p\mathbb{Z}$. Donc $\tau(\sqrt[p]{\alpha})$ est un vecteur propre de σ associé à la valeur propre ζ^l . Or $\sigma(\sqrt[p]{\alpha}) = \zeta \sqrt[p]{\alpha}$ donc $\sigma(\sqrt[p]{\alpha^l}) = \zeta^l \sqrt[p]{\alpha^l}$ et $\sqrt[p]{\alpha^l}$ est aussi un vecteur propre associé à ζ^l . Donc $\tau(\sqrt[p]{\alpha}) = c \sqrt[p]{\alpha}$ pour un $c \in L$. Mais alors : $\tau(\alpha) = c^p \alpha^l$. Donc $\tau(\alpha)/\alpha \in \mathcal{O}_L$. On a donc $L(\sqrt[p]{\tau(\alpha)/\alpha}) = L(\sqrt[p]{\alpha^{l-1}}) \leq L(\sqrt[p]{\alpha})$. Comme $\sqrt[p]{\alpha^{l-1}} \notin L$ (car $\sigma(\sqrt[p]{\alpha^{l-1}}) = \zeta^{l-1} \sqrt[p]{\alpha^{l-1}}$ et $\zeta^{l-1} \neq 1 \Leftrightarrow l-1 \neq 0 \pmod{p} \Leftrightarrow l \neq 1 \pmod{p}$). Comme l'idéal (λ) est stable par τ , on voit que $\tau(\alpha)/\alpha$ est premier à p . Quitte à remplacer α par $\tau(\alpha)/\alpha$ on peut donc supposer α premier à p . Quitte à remplacer α par α^{p-1} , on peut supposer que $\alpha = 1 \pmod{\lambda}$ (en effet : $|(\mathcal{O}_L/\lambda)^\times| = p-1$). Puisque $\mathcal{O}_L/(\lambda) \simeq \mathbb{Z}/p\mathbb{Z}$, $\alpha = 1 + a\lambda \pmod{\lambda^2}$ pour un certain entier a . Or, $\zeta^a = 1 - a\lambda \pmod{\lambda^2}$ (exo). Donc en remplaçant α par $\zeta^a \alpha$, on obtient un $\alpha' := \zeta^a \alpha = 1 \pmod{\lambda^2}$ dans \mathcal{O}_L . Supposons que $\alpha' = 1 + a\lambda^e \pmod{\lambda^{e+1}}$ pour un $2 \leq e < p$. Comme $L(\sqrt[p]{\alpha'}) \leq KK'L$ et comme $KK'L/\mathbb{Q}$ est abélienne, $L(\sqrt[p]{\alpha'})/\mathbb{Q}$ aussi. Donc comme précédemment, on peut trouver un $c \in L$ tel que $\tau(\alpha') = c^p \alpha'^l = c^p \pmod{\lambda^2}$ pour un certain l générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Or, $\tau(\lambda) = 1 - \zeta^l = \lambda(1 + \dots + \zeta^{l-1}) = l\lambda \pmod{\lambda^2}$. Donc $\tau(\alpha') = 1 + a(l\lambda)^e \pmod{\lambda^{e+1}} = c^p \pmod{\lambda^2} \Rightarrow c^p = 1 \pmod{\lambda}$. Mais $c^p = c \pmod{\lambda}$ car $\mathcal{O}_L/\lambda \simeq \mathbb{Z}/p\mathbb{Z}$. Donc $c = 1 \pmod{\lambda} \Rightarrow c^p = 1 \pmod{p}$ ($(1 + t\lambda)^p = 1 \pmod{p}$). Par conséquent :

$$1 + a(l\lambda)^e = \tau(\alpha') = \alpha'^l = 1 + al\lambda^e \pmod{\lambda^{e+1}}$$

d'où : $a = 0$ ou $l^e = l \Rightarrow p-1|e-1$ absurde ! Ainsi $\alpha' = 1 \pmod{\lambda^{e+1}}$. On peut recommencer ... finalement, on trouve $\alpha' = 1 \pmod{\lambda^p}$.

On va en déduire que $K' = K$. Sinon : posons $\xi := \frac{1 - \sqrt[p]{\alpha'}}{\lambda} \in KK'L$. C'est une racine du polynôme $f(X) = (X - 1/\lambda)^p - \alpha'/\lambda^p$. D'après ce qui précède, $f(X)$ est un polynôme unitaire dans $\mathcal{O}_L[X]$. Donc ξ est entier (sur \mathbb{Z}). Le discriminant de l'extension $KK'L/KL$ contient l'idéal engendré par $N_{KK'L/KL}(f'(\xi)) = N_{KL}(p(\xi - 1/\lambda)^{p-1}) = \epsilon \alpha'^{p-1}$ où ϵ est une unité. Mais alors, c'est premier à p . Donc l'idéal premier de \mathcal{O}_{KL} au-dessus de p est non ramifié ! Mais alors le groupe d'inertie I d'un idéal premier de $\mathcal{O}_{KK'L}$ au-dessus de p est d'ordre $< [KK'L : \mathbb{Q}] = p(p^2 - p)$. Soit $T := (KK'L)^I$ le corps des invariants. Le nombre premier p n'est pas ramifié dans T et aucun autre nombre premier ne peut l'être car aucun autre n'est ramifié ni dans K , ni dans K' ni dans L . Donc $T = \mathbb{Q}$ absurde ! **Q.e.d.**

Soit K/\mathbb{Q} une extension cyclique de degré l^r où l est premier et l est le seul premier ramifié dans K . Soit F le sous-corps de $\mathbb{Q}(\zeta_{l^{r+1}})$ de degré l^r sur \mathbb{Q} . Soit $E := FK$. L'extension E/\mathbb{Q} est cyclique $\Leftrightarrow F = K$ (car $\text{Gal}(FK/K) \simeq \text{Gal}(F/(K \cap F))$ est de même ordre que $\text{Gal}(FK/F) \simeq \text{Gal}(K/(K \cap F)) : l^r/[K \cap F : \mathbb{Q}]$; donc si $\text{Gal}(FK/\mathbb{Q})$ ce groupe ne contient qu'un seul sous-groupe d'un ordre donné et $\text{Gal}(FK/K) = \text{Gal}(FK/F)$ d'où en prenant les invariants : $F = K$). Si E/\mathbb{Q} n'est pas cyclique, il existe un quotient de $\text{Gal}(E/\mathbb{Q})$ isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (exo) *i.e.* un corps $\mathbb{Q} \leq D \leq E$ tel que $\text{Gal}(D/\mathbb{Q}) \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Clairement l est le seul nombre premier ramifié dans D' si $\mathbb{Q} < D' < D$ avec $[D' : \mathbb{Q}] = p$. D'après le lemme précédent, il existe un unique D' tel que : $\mathbb{Q} < D' < D$ et $[D' : \mathbb{Q}] = p$. Donc il existe un unique sous-groupe d'ordre p dans $\text{Gal}(D/\mathbb{Q}) \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ *absurdo!*
Q.e.d.

FIN DU COURS 2015

12.8 Application : le polynôme $X^n - X - 1$

Soit $P := X^n - X - 1 \in \mathbb{Q}[X]$. C'est un polynôme irréductible sur \mathbb{Q} (cf. TD) avec des racines x_1, \dots, x_n . On note $K \subseteq \mathbb{C}$ le corps de décomposition de P sur \mathbb{Q} .

Théorème 12.23 *On a $\text{Gal}_{\mathbb{Q}}(P) = \mathfrak{S}_n$.*

Lemme 12.24 *Soit p un nombre premier et I_P le groupe d'inertie d'un idéal $P \leq \mathcal{O}_K$ au-dessus de p . Alors I_P est soit trivial soit engendré par une transposition.*

Démonstration : On note \bar{P} la réduction de $P \pmod{p}$.

Dans $\mathbb{F}_p[X]$, on a :

$$X\bar{P}' - \bar{P} = (n-1)X + n .$$

Comme p ne divise pas en même temps n et $n-1$, on en déduit que le pgcd de \bar{P}' et \bar{P} est de degré ≤ 1 . Donc \bar{P} est soit séparable soit avec une seule racine double et $n-2$ racines simples dans \mathcal{O}_K/P .

Soit $e \neq s \in I_P$. Il existe $i \neq j$ tel que $s(x_i) = x_j$. Alors $s(\bar{x}_i) = \bar{x}_j = \bar{x}_i$ car $s \in I_P$. Donc $\bar{x}_i = \bar{x}_j$ est l'unique racine double de \bar{P} . De plus si $\bar{x}_k \neq \bar{x}_i$, $s(\bar{x}_k) = \bar{x}_k$. Donc $s = (ij)$.
Q.e.d.

Lemme 12.25 *Le groupe $G := \text{Gal}_{\mathbb{Q}}(P)$ est engendré par les groupes d'inertie I_P , $P \leq \mathcal{O}_K$ idéal premier.*

Démonstration : Soit H le sous-groupe de G engendré par les I_P où P décrit les idéaux maximaux de \mathcal{O}_K . C'est un sous-groupe distingué de G . En effet, si p est un nombre premier, l'ensemble des idéaux maximaux de \mathcal{O}_K au-dessus de p est stable par l'action de G . Si $\sigma \in G$, $I_{\sigma(P)} = \sigma I_P \sigma^{-1}$.

Soit $k := K^H$. Nous allons montrer que $k = \mathbb{Q}$. Si $k \neq \mathbb{Q}$, d'après le théorème d'Hermite-Minkowski, il existe un nombre premier p qui se ramifie dans \mathcal{O}_k . Soit P' un idéal maximal de \mathcal{O}_k tel que $P' \cap \mathbb{Z} = p\mathbb{Z}$. Soit P un idéal maximal de \mathcal{O}_K tel que $P \cap \mathcal{O}_k = P'$. Soit $\sigma \in I_{P'} \leq \text{Gal}(k/\mathbb{Q})$. Soit $\sigma_1 \in G$ tel que $\sigma_1|_k = \sigma$. On peut supposer que $\sigma_1(P) = P$ en effet, il existe $t \in \text{Gal}(K:k)$ tel que $t\sigma_1(P) = P$ (cf. la démonstration du théorème 12.6 en l'adaptant à K/k au lieu de K/\mathbb{Q}) et on peut ramplacer σ_1 par $t\sigma_1$. On peut aussi supposer que $\sigma_1 \in I_P$ en effet, il existe $t \in \text{Gal}(K/k)$ tel que $\bar{t} : \mathcal{O}_K/P \rightarrow \mathcal{O}_K/P$ coïncide avec $\bar{\sigma}_1 : \mathcal{O}_K/P \rightarrow \mathcal{O}_K/P$ et on peut remplacer σ_1 par $t^{-1}\sigma_1$. Mais alors $\sigma_1 \in H$ et $\sigma = \sigma_1|_k$ est trivial. Donc $|I_{P'}| = 1$ et p n'est pas ramifié! Q.e.d.

Lemme 12.26 Soit $G \subseteq \mathfrak{S}_n$ un sous-groupe transitif engendré par des transpositions. Alors $G = \mathfrak{S}_n$.

Démonstration : Soit T l'ensemble des transpositions de G . Soient $1 \leq a \neq b \leq n$. On va montrer que $(ab) \in G$. On choisit $s \in G$ tel que $s(a) = b$. On écrit $s = t_1 \dots t_p$ avec $t_i \in T$. On choisit $s \in G$ tel que $s(a) = b$ et p est minimal.

On a b dans le support de t_1 . Sinon $t_2 \dots t_p(a) = t_1(b) = b$ ce qui contredit la minimalité de p . On a aussi :

$$s = t_j t'_1 \dots t'_{j-1} t_{j+1} \dots t_p$$

où $t'_k := t_j t_k t_j^{-1}$. On en déduit que b est dans le support de t_j pour tout j et donc de t_p . De même, on montre que a est dans le support de t_p . Donc $t_p = (ab) \in G$ car t_p est une transposition. Q.e.d.

Sections non traitées en cours :

13 Cohomologie galoisienne

13.1 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.

13.2 Groupes de cohomologie

13.2.1 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 13.1 (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 13.1.1 *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 13.2 *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.*

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.**

13.2.2 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 11 *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 13.3 *Pour tout $n, d^n d^{n-1} = 0$.*

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

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 :

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

Q.e.d.

Définition 12 (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 13.4 (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 :

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

14 Théorie de Kummer

L'objectif est de généraliser la bijection suivante :

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

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

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 14.1 *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 :

$$G_C \rightarrow \text{Hom}((C/(K^\times)^n), \mu_n)$$

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

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 14.2 *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 14.2.1 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 :

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

15 Extensions d'Artin-Schreier

15.1 Forme additive du théorème 90 de Hilbert

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

Théorème 15.1 $H^n(G, L) = \begin{cases} L^G = K & \text{si } n = 0; \\ 0 & \text{si } n > 0. \end{cases}$

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 15.1.1 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.**

15.2 Théorie des extensions d'exposant p en caractéristique p

Soit K un corps de caractéristique p .

Lemme 15.2 *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 \bar{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 \bar{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 $\phi : \bar{K} \rightarrow \bar{K}$, $x \mapsto x^p - x$. 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 15.3 *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 15.3.1 *On a deux bijections réciproques l'une de l'autre :*

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

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 $x^p - x = c$.

15.3 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 15.4 *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 15.5 *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 15.6 *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 15.5 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.

Index

- 90 (forme additive du théorème de Hilbert), 61
- 90 (théorème de Hilbert), 34
- G -module, 57
- caractéristique d'un corps, 6
- cyclique (extension), 34
- algébriquement clos, 10
- Artin-Schreier (extensions), 61
- Artin-Schreier (théorème), 63
- Berlekamp (algorithme), 22
- casus irreducibilis, 3
- cobords, 59
- cocycles, 58, 59
- cohomologie, 59
- corps de décomposition, 9
- corps de rupture, 9
- cyclotomique (extension), 29
- cyclotomique (polynôme), 30
- Dedekind, 44
- degré (d'un élément), 8
- degré séparable, 25
- exposant d'un groupe, 18
- galoisienne (extension), 11
- indépendance des caractères, 10
- Kronecker-Weber, 32
- Kummer (théorème sur les extensions cycliques), 34
- normale (base), 27
- normale (extension), 16
- polynôme minimal, 8
- primitif (polynôme), 22
- primitif (élément), 26
- ramification (indice), 46
- ramifié, 46
- ramifié (non), 46
- résoluble (extension), 35
- résoluble (groupe), 35
- résoluble par radicaux, 36
- résoluble par radicaux réels, 3
- symétriques élémentaires, 6
- séparable (élément), 14

Table des matières

Introduction	2
0.1 Équations de degré 2	2
0.2 Méthode de Lagrange	2
0.2.1 Degré 3	2
0.2.2 Degré 4	3
0.3 Autres méthodes	4
0.3.1 Cardan	4
0.3.2 Euler	5
0.4 Degré ≥ 5	6
0.5 Caractéristique	6
0.6 Polynômes symétriques	6
1 Extensions, algébricité	7
1.1 Polynômes irréductibles	7
1.2 Extensions, degré	7
1.3 Éléments algébriques	8
1.4 Corps de rupture	8
1.5 Corps de décomposition	9
2 Théorème d'indépendance des caractères d'Artin	10
2.1 Indépendance	10
2.2 Corps des invariants	11
3 Correspondance de Galois	11
3.1 Extensions galoisiennes	11
3.2 Injectivité	13
3.3 Surjectivité	13
3.4 Théorème fondamental	13
3.5 Caractérisation des extensions galoisiennes	14
3.6 Séparabilité	14
3.7 Normalité	15
3.8 Composée de corps	17
4 Corps finis	18
4.1 Sous-groupes finis de \mathbf{K}^\times	18
4.2 Structure	19
4.3 Polynômes sur les corps finis	19
4.3.1 Nombre de polynômes irréductibles de degré donné	19
4.3.2 Ordre d'un polynôme, polynôme primitif	21
4.4 Algorithme de Berlekamp	22
5 Clôture algébrique	23
5.1 Retour sur la notion de séparabilité	25

6	Base normale	26
6.1	Éléments primitifs	26
6.2	Théorème de la base normale	27
7	Extensions cyclotomiques	29
7.1	Racines primitives n -ièmes	29
7.2	Polynômes cyclotomiques sur \mathbb{Q}	30
7.3	Théorème de Kronecker-Weber	32
8	Norme et trace	33
9	Extensions cycliques	34
9.1	Théorème 90 de Hilbert	34
10	Résolubilité par radicaux	35
11	Calcul du groupe de Galois	39
11.1	Discriminant	39
11.2	Réduction modulo un nombre premier	40
12	Théorie de la ramification	42
12.1	Éléments entiers sur un anneau	42
12.2	Anneaux de Dedekind	43
12.3	Égalité fondamentale	46
12.4	Discriminant	48
12.5	Discriminant et ramification	49
12.6	Groupes de décomposition et d'inertie	50
12.7	Théorème de Kronecker-Weber	51
12.8	Application : le polynôme $X^n - X - 1$	55
13	Cohomologie galoisienne	57
13.1	G -modules	57
13.2	Groupes de cohomologie	57
13.2.1	En degré 1	57
13.2.2	En tout degré	58
14	Théorie de Kummer	60
15	Extensions d'Artin-Schreier	61
15.1	Forme additive du théorème 90 de Hilbert	61
15.2	Théorie des extensions d'exposant p en caractéristique p	62
15.3	Théorème d'Artin-Schreier	63