Chapitre 1. — Construction des extensions cubiques CYCLIQUES DE Q

cette méthode en donnant à Y les valeurs de 1 à 100000 et à m une centaine de valeurs pour chacune des équations a) et b).

Les résultats sont exposés aux chapitres 4 (4.1 et 4.2).

Dans un travail récent [2], M.-N. Gras obtient, par d'autres méthodes, des résultats semblables aux théorèmes 3.3 et 3.4 et donne une liste très fournie de corps cubiques cycliques dont l'anneau est soit monogène, soit non monogène.

MM. les professeurs F. Châtelet et J.-J. Payan m'ont dirigé et aidé dans ce travail; je leur exprime ici ma très vive reconnaissance.

Je remercie aussi M. R. Smadja dont un manuscrit m'a été utile dans la recherche des conditions du théorème 3.2 et M^me M. Archinard, qui a bien voulu se charger de la programmation.

Enfin, je remercie le Centre d'économétrie de l'Université de Genève qui m'a donné accès à l'ordinateur de l'Etat de Genève.

Chapitre 1. — Construction des extensions cubiques cycliques de Q

On rappelle dans ce chapitre la construction donnée par A. Châtelet. ([1], chap. 1 à IV).

1. Notations

Dans la suite, K désigne une extension cubique cyclique du corps Q des rationnels, O_K l'anneau des entiers de K, Δ_K le discriminant de K/Q et $\mathrm{Gal}(K/Q)$ son groupe de Galois. E désigne le corps $Q(j)$, où $j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, O_E l'anneau des entiers de E, τ le Q-automorphisme de E défini par $\tau j = j^2$ et β' l'élément $\tau\beta$, pour $\beta \in E$. τ désigne aussi le prolongement de τ à $K(j)$ ayant K comme corps des invariants. σ désigne à la fois un élément non trivial de $\mathrm{Gal}(K/Q)$ et son prolongement à $K(j)$ qui laisse E invariant. E est donc le corps des invariants du groupe cyclique engendré par σ.

θ étant un élément de K, on définit les expressions suivantes (résolvantes de Lagrange).

$$<\theta, \sigma> = \theta + j\sigma\theta + j^2\sigma^2\theta \quad \sigma \in \mathrm{Gal}(K/Q)$$

Ce sont des éléments de $K(j)$, qui vérifient les propriétés suivantes:

$$(1.1) \qquad \sigma^l<\theta,\sigma> = <\sigma^l\theta,\sigma> = j^{2l}<\theta,\sigma> \qquad l = 0,1,2.$$
$$\sigma^l<\theta,\sigma^2> = <\sigma^l\theta,\sigma^2> = j^l<\theta,\sigma^2> \qquad l = 0,1,2.$$

$$(1.2) \qquad \tau<\theta,\sigma> = <\theta,\sigma^2>$$

$$(1.3) \qquad \theta = \frac{1}{3}(S + <\theta,\sigma> + <\theta,\sigma^2>)$$

2. Théorèmes fondamentaux

On donne ici les résultats essentiels de la construction de Châtelet et celles de leurs conséquences techniques qui seront utilisées aux chapitres 2 et 3. Pour les démonstrations, on renvoie à [1], en notant que les principales d'entre elles font intervenir de manière systématique les propriétés de $<\theta,\sigma>$ et la théorie de Galois dans $K(j)/Q$.

Lemme 1.1 Soit θ un élément primitif de K. Alors, le nombre β défini par

$$\beta = \frac{<\sigma^l\theta,\sigma>^2}{<\sigma^l\theta,\sigma^2>}$$

est un nombre primitif de E ne dépendant pas de l et vérifiant $\beta^2\,\beta' \notin E^3$.

Si φ est un nombre algébrique engendrant un corps cubique cyclique sur Q et ρ un générateur de $\mathrm{Gal}(Q(\varphi)/Q)$ tels que

$$\frac{<\rho^l\varphi,\rho>^2}{<\rho^l\varphi,\rho^2>} = \beta, \text{ alors } \varphi = \sigma^l\theta - \frac{1}{3}(S-T), \text{ pour } l = 0$$

1 ou 2 et $\rho = \sigma$; S et T étant les traces de θ et φ.

Lemme 1.2 Soit $S \in Q$ et β un nombre primitif de E vérifiant $\beta^2\,\beta' \notin E^3$. Alors, il existe un nombre algébrique θ, de trace S, engendrant une extension cubique cyclique K/Q, et un générateurs σ de $\mathrm{Gal}(K/Q)$ tels que

$$\beta = \frac{<\theta,\sigma>^2}{<\theta,\sigma^2>}.$$

Ces deux lemmes permettent d'énoncer le théorème fondamental de cette construction des corps cubiques cycliques.

Théorème 1.1 Les formules $S = \text{trace}(\theta)$ et

$$\beta = \frac{<\theta, \sigma>^2}{<\theta, \sigma^2>}$$

définissent une surjection de l'ensemble des couples (θ, σ), formés d'un nombre algébrique engendrant un corps cubique cyclique et d'un générateur du groupe de Galois de ce corps, sur l'ensemble des couples (β, S), formés d'un nombre primitif β de E tel que $\beta^2 \beta' \notin E^3$ et d'un nombre rationnel.

Deux couples (θ, σ) et (φ, ρ) ont même image si et seulement si $\varphi = \sigma^l \theta$, pour $l = o$, 1 ou 2 et $\rho = \sigma$.

Définition 1.1 Dans la suite, lorsqu'on se référera à cette construction, on dira que (β, S) est l'image de (θ, σ), que θ est construit avec (β, S) et que β engendre $Q(\theta)$.

Remarque 1.1 Il découle de la définition de $<\theta, \sigma>$ et de la propriété (1.2) que, si (β, S) est l'image de (θ, σ), $(-\beta, -S)$ est l'image de $(-\theta, \sigma)$ et (β', S) celle de (θ, σ^2).

On est ainsi amené à la définition suivante:

Définition 1.2 Soit α et β deux éléments de E. α et β sont dits équivalents si $\alpha \in \{\beta, \beta', -\beta, -\beta'\}$.

Les résultats techniques suivants seront utiles aux chapitres 2 et 3.

Corollaire 1.1 Si θ est construit avec (β, S), θ est zéro du polynôme

$$(1.4) \quad X^3 - SX^2 + \frac{1}{3}(S^2 - \beta\beta')X - \frac{1}{27}(S^3 - 3S\beta\beta' + \beta\beta'(\beta + \beta')).$$

Corollaire 1.2 Soit θ un nombre construit avec (β, S), et soit $\Delta(\theta)$ le discriminant de $1, \theta, \theta^2$ et $\Delta(1, \theta, \sigma\theta)$ celui de $1, \theta, \sigma\theta$. On a alors:

$$(1.5) \quad \Delta(\theta) = -\frac{1}{27}(\beta\beta')^2(\beta - \beta')^2$$

$$(1.6) \quad \Delta(1, \theta, \sigma\theta) = (\beta\beta')^2$$

Corollaire 1.3 Soit (β, S) l'image de (θ, σ). On a alors:

$$(1.7) \quad 9\theta^2 = (\beta + \beta' + 4S)\theta + (j^2\beta + j\beta' - 2S)\sigma\theta + (j\beta + j^2\beta' - 2S)\sigma^2\theta + 2\beta\beta' + S^2$$

$$(1.8) \quad 9\sigma\theta\sigma^2\theta = (\beta + \beta' - 2S)\theta + (j^2\beta + j\beta' + S)\sigma\theta + (j\beta + j^2\beta' + S)\sigma^2\theta - \beta\beta' + S^2$$

Théorème 1.2 Soit (β, S) et (γ, T) les images respectives de (θ, σ) et (φ, ρ). Alors la condition

$$\frac{\gamma^2\gamma'}{\beta^2\beta'} \in E^3$$

est nécessaire et suffisante pour que $Q(\theta) = Q(\varphi)$ et $\sigma = \rho$.

Ce théorème et la remarque 1.1 permettent de reconnaître les nombres engendrant le même corps cubique cyclique.

3. L'ANNEAU O_E

On rappelle d'abord quelques résultats classiques. O_E est intègre, principal et donc factoriel.

$$O_E = Zj \oplus Zj^2 \qquad \text{(somme directe)}$$

Les unités de O_E sont $\pm 1, \pm j, \pm j^2$ et représentent les 6 classes de $O_E/(3)$ premières avec 3.

Les nombres (entiers rationnels) premiers congrus à $-1 \pmod 3$ sont irréductibles dans O_E, les nombres premiers p congrus à 1 (mod 3) sont de la forme $p = \omega_p \omega_p'$, ω_p étant irréductible et ω_p et ω_p' n'étant pas associés. Enfin, on a $3 = -(j - j^2)^2$.

Ainsi, les éléments irréductibles de O_E sont $j - j^2$, les nombres premiers congrus à $-1 \pmod 3$, les éléments ω_p et ω_p' et leurs associés.

Lemme 1.3 Soit β un élément de O_E sans facteurs rationnels et soit p un nombre premier tel que p^n divise exactement $\beta\beta'$. Alors, $p = 3$ et $n = 1$, ou $p \equiv 1 \pmod 3$ et ω_p^n divise exactement β, ω_p étant un diviseur irréductible de p.

Démonstration Si 3^n divise $\beta\beta'$, $j - j^2$ divise exactement β, donc $j - j^2$ divise aussi exactement β' et 3 divise exactement $\beta\beta'$. Il s'ensuit que $n = 1$.

Si $p \neq 3$, p est congru à 1 (mod 3), sinon p serait irréductible et diviserait β. Donc $p = \omega_p \omega_p'$ et ω_p^n et $\omega_p'^n$ divisent exactement $\beta\beta'$. Comme $\omega_p \omega_p'$ ne divise pas β, il faut que ω_p^n (ou $\omega_p'^n$) divise exactement β. C.q.f.d.

Définition 1.3 Un élément de O_E est dit entier canonique s'il n'est divisible ni par $j - j^2$, ni par un entier rationnel, ni par un facteur carré.

Un entier canonique α est de la forme $\omega_{p1} \omega_{p2} \ldots \omega_{pr}$, sa norme étant égale à $p_1 p_2 \ldots p_r$, les p_i étant des nombres premiers naturels distincts et congrus à 1 (mod 3), et satisfait la condition $\alpha^2 \alpha' \notin E^3$.

Réciproquement, un nombre de O_E dont la norme a cette forme est un entier canonique.

Un entier canonique, étant premier avec 3, appartient à l'une des 6 classes de $O_E/(3)$, premières avec 3. Il est donc congru (mod 3) à une unité.

Définition 1.4 Un entier canonique est dit unitaire positif (respectivement négatif) s'il est congru (mod 3) à 1 (respectivement à -1).

Si le signe n'intervient pas, on dit simplement que l'entier canonique est unitaire.

Tour entier canonique est le produit d'une unité et d'un entier canonique unitaire positif unique.

Théorème 1.3 Tout corps cubique cyclique K est engendré par un entier canonique, défini de manière unique à l'équivalence près.

Voir [1], chapitre III, pour une démonstration.

Des entiers canoniques équivalents étant ensemble unitaires ou non, on peut donner la définition suivante:

Définition 1.5 K est dit unitaire s'il est engendré par des entiers canoniques unitaires. (De ces entiers canoniques unitaires, deux sont positifs et deux sont négatifs).

Le théorème suivant donne la construction de bases d'entiers d'un corps K.

Théorème 1.4 Soit K le corps cubique cyclique engendré par l'entier canonique α. Alors:

a) si α est unitaire positif (respectivement négatif) et si θ est construit avec $(\alpha, 1)$ (respectivement avec $(\alpha, -1)$), θ, $\sigma\theta$, et $\sigma^2\theta$ forment une base des entiers de K;

b) si α est non unitaire et si θ est construit avec $(3\alpha, o)$, $1, \theta, \sigma\theta$ forment une base des entiers de K.

Définition 1.6 Ces bases sont dites canoniques et construites avec α.

Corollaire 1.4 On conserve les notations du théorème 1.4. Alors,

a) si K est unitaire, il est modérément ramifié et

$$\Delta_K = (\alpha\alpha')^2$$

b) si K est non unitaire, il est sauvagement ramifié et

$$\Delta_K = 81\,(\alpha\alpha')^2\,.$$

Démonstration Ces formules s'obtiennent immédiatement en prenant les discriminants des bases canoniques par la formule (1.6).

Corollaire 1.5 Soit $p_1, p_2, ..., p_r$, r nombres premiers différents de 1, distincts et congrus à 1 (mod 3). Alors il existe 2^{r-1} corps modérément ramifiés de discriminant $(p_1 p_2 ... p_r)^2$ et 2^r corps sauvagement ramifiés de discriminant $81\,(p_1 p_2 ... p_r)^2$.

Tous les corps cubiques cycliques ont leurs discriminants de cette forme, sauf un corps unique de discriminant 81.

Pour une démonstration du théorème 1.4 et du corollaire 1.5, on se reportera à [1], chapitre IV.

Chapitre 2. — Indice d'un nombre de O_K

L'indice d'un nombre θ d'une extension finie K/Q est le nombre $I(\theta) = \sqrt{\Delta(\theta)/\Delta_K}$, où $\Delta(\theta)$ est le discriminant de θ dans K et Δ_K le discriminant de K (cf. [3], chap. III, § 25 et [5]).

Comme au chapitre 1, K/Q désigne dorénavant une extension cubique cyclique et on va utiliser une base canonique (déf. 1.6) pour calculer l'indice d'un élément quelconque de O_K.

Lemme 2.1 Soit θ un élément primitif d'une base canonique de K. Alors, si $\varphi \in O_K$, il existe un nombre $\psi = X\theta + Y\sigma\theta \in O_K$ tel que $\psi - \varphi \in Z$ et $I(\psi) = I(\varphi)$.

Démonstration On considère le cas où θ est construit avec $(\alpha, 1)$, c'est-à-dire où α est unitaire positif. θ, $\sigma\theta$ et $\sigma^2\theta$ forment une base d'entiers de K, donc $\varphi = X_0\theta + X_1\sigma\theta + X_2\sigma^2\theta$, avec $X_i \in Z$, $i = 1, 2, 3$. Soit $\psi = \varphi - X_2$; alors $I(\psi) = I(\varphi)$ et $\psi = (X_0 - X_2)\theta + (X_1 - X_2)\sigma\theta$, d'après $\theta + \sigma\theta + \sigma^2\theta = 1$. ψ a la forme requise.

Les cas où α est unitaire négatif et où K est non unitaire se démontrent de manière semblable. C.q.f.d.

Donc, pour obtenir les indices de tous les nombres de O_K, il suffit de considérer les nombres de la forme $X\theta + Y\sigma\theta$ où X et Y sont des entiers.

Lemme 2.2 Soit K le corps (modérément ramifié) engendré par l'entier canonique unitaire $\alpha = a_1 j + a_2 j^2$ et soit $\theta, \sigma\theta, \sigma^2\theta$ la base canonique construite avec α. Alors, si $\psi = X\theta + Y\sigma\theta$, $\pm I(\psi)$ est égal à:

$$(2.1) \qquad \frac{a_1 - a_2}{3} X^3 + a_2 X^2 Y - a_1 X Y^2 + \frac{a_1 - a_2}{3} Y^3 .$$