

### 131. Sur le nombre de classes de sous-corps cubique cyclique de $\mathcal{Q}^{(p)}$ , $p \equiv 1 \pmod{3}$

Par Marie-Nicole MONTOUCHET\*)

(Comm. by Kunihiko KODAIRA, M. J. A., June 12, 1971)

Soit  $p$  un nombre premier congru à 1 modulo 3. Soit  $\zeta_p = e^{2\pi i/p}$  et soit  $\mathcal{Q}^{(p)} = \mathcal{Q}(\zeta_p)$  le  $p$ -ième corps cyclotomique. Il existe un sous-corps cubique cyclique et un seul  $K$  de  $\mathcal{Q}^{(p)}$ . Nous allons donner un critère permettant de déterminer la parité du nombre de classes de  $K$  ainsi que des résultats numériques.

#### 1. Notations et rappels.

Tout nombre premier  $p$ ,  $p \equiv 1 \pmod{3}$ , se met de manière unique sous la forme  $p = (a^2 + 27b^2)/4 = \varphi\bar{\varphi}$ , avec  $\varphi = (a + 3ib\sqrt{3})/2$ ,  $a \equiv 1 \pmod{3}$ .

Soit  $\chi$  un caractère modulo  $p$  de  $K$ ; soit  $\tau = \sum_{x \pmod{p}} \zeta^x \chi(x)$ . Tout élément  $z$  de  $K$  se met de manière unique sous la forme  $z = (x + y\tau + \bar{y}\bar{\tau})/3 = [x, y]$ ,  $x \in \mathcal{Q}$ ,  $y \in \mathcal{Q}(i\sqrt{3})$ .

Les coordonnées  $(x, y)$  de l'unité fondamentale  $\varepsilon$  de  $K$  sont la solution  $(x, y)$ ,  $y$  déterminé à une racine cubique de l'unité près, de l'équation  $x^3 - 3pxy\bar{y} + p(\varphi y^3 + \bar{\varphi}\bar{y}^3) = 27$  pour laquelle  $x^2 + 2py\bar{y}$  est minimum avec  $y \neq 0$  ([3]).

Soit  $\zeta_{2p} = e^{i\pi/p}$  et soit  $g$  une racine primitive modulo  $p$ . Soit  $\eta = -\prod_{n=1}^{(p-1)/6} (\zeta_{2p}^{g^{3n+1}} - \zeta_{2p}^{-g^{3n+1}}) / (\zeta_{2p}^{g^{3n}} - \zeta_{2p}^{-g^{3n}})$  l'unité cyclotomique de  $K$ . On rappelle que l'indice dans le groupe des unités de  $K$  du sous-groupe engendré par les unités cyclotomiques de  $K$  est égal à  $h$  ([4]).

#### 2. Etude de la parité du nombre de classes de $K$ .

**Théorème.** 4 divise  $h$  si et seulement si l'unité cyclotomique  $\eta$  de  $K$  est totalement positive.

La démonstration de ce théorème résulte du théorème V de J. V. Armitage et A. Fröhlich ([2]) et du fait qu'une condition nécessaire et suffisante pour que 4 divise  $h$  est que  $\eta$  soit un carré dans  $K$ .

Une généralisation de ce théorème est donné par N. Adachi dans [1].

**Proposition.** Soit  $g$  une racine primitive modulo  $p$ . On désigne par  $[g^m]$  la valeur de  $g^m$  modulo  $p$  comprise entre 1 et  $p-1$ . Pour  $i$  variant de 0 à 2 soit  $M_i$  le nombre d'entiers  $n$ ,  $1 \leq n \leq (p-1)/6$  tels que  $[g^{3n+i}]$  soit pair. 4 divise  $h$  si et seulement si  $M_0 + M_1$  et  $M_1 + M_2$  sont impairs.

\*) Institut de Mathématiques Pures, Université Scientifique et Médicale de Grenoble, B.P. 116, 38—St. Martin d'Hères, France.