On Cyclic Cubic Fields

FRANCISCA CÁNOVAS ORVAY

E.T.S. de Ingenieros Caminos, Canales y Puertos, Univ. Politécnica, Madrid, Spain

AMS Subject Class. (1980): 10B10, 14G99

Received November 13, 1990

In 1960, Godwin [3] states a conjecture about units in totally real cubic fields. Given such a field $K$, if $R$ denotes its ring of integers, he defines

$$S(\alpha) = \frac{1}{2} \left[ (\alpha - \alpha')^2 + (\alpha - \alpha^*)^2 + (\alpha' - \alpha^*)^2 \right],$$

for $\alpha \in R$; $\alpha'$ and $\alpha^*$ denote the conjugates of $\alpha$. Denoting by $E$ the subgroup of units with positive norm, Godwin's conjecture is as follows: let $\mu \in E \setminus \{1\}$ be such that $S(\mu)$ is minimum and $\tau \in U \setminus \{\mu^n : n \in \mathbb{Z}\}$ such that $S(\tau)$ is minimum; if $S(\mu) > 9$, then $\{\mu, \tau\}$ is a system of fundamental units of $K$. In 1980, Gras [4] proved this conjecture in case that $K$ is cyclic.

For three families of cyclic cubic fields we give a system of fundamental units $\{\mu, \mu'\}$. For that we use the already proved Godwin's conjecture.

In addition, the unit $\mu$ is never totally positive. Hence, every totally positive unit in $K$ is a square in $R$. We use this fact to obtain a criterion about evenness of the classnumber for fields in these families.

Precisely:

**Theorem 1.** Let $K = \mathbb{Q}(\theta), \; \text{Irr}(\theta, \mathbb{Q}) = x^3 - px + p, \; p = 3^6 p_1 \cdots p_r, \; p_1 \equiv 1 \mod{3}$ pairwise different primes, $\delta \in \{0, 2\}, \; 4p - 27 \in \mathbb{Z}^2$. The following conditions hold:

i) $\text{disc}(K) = p^2$.

ii) $K$ is monogenic with integral basis $\{1, \sigma, \sigma^2\}$.

iii) $\{\sigma, \sigma'\}$ is a system of fundamental units of $K$, where $\sigma = (m + \theta_1)/3, \sigma'$ denotes a conjugate of $\sigma, \theta_1 = (4p - 9\delta - 6\delta^2)/(4p - 27)^{1/2}$ and $m = ((4p - 27)^{1/2} - 3)/2$.

**Examples.** $p = 13, 19, 37, 63, 79, 97, 117, 139, 163, 217, 247, 279, 313, 349, 387, 427, 469, 559, 607, 657, 709, 763, 819, 877, 937, 1063, 1129, 1197, 1267, 1339, 1413, 1489.$

**Theorem 2.** Let $K = \mathbb{Q}(\theta), \; \text{Irr}(\theta, \mathbb{Q}) = x^3 - px + pq, \; p = p_1 \cdots p_r, \; p_1 \equiv 1 \mod{3}$, pairwise different primes, $q > 2, \; 4p - 27q^2 = 1$. The following conditions hold:

i) $\text{disc}(K) = p^2$.

ii) $K$ is monogenic with integral basis $\{1, \theta, \theta^2\}; \{1, \sigma, \tau = (\sigma^2 + ((q + 1)/2)\sigma)/q\}$ is another integral basis of $K$.

iii) $\{\mu, \mu'\}$ is a system of fundamental units of $K$, where $\mu = 2 + 3\sigma + 3\tau, \sigma = (-1 + \theta_1)/3$.

1 In all this paper, the rings of integer, rational and natural numbers will be denoted by $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{N}$.
ON CYCLIC CUBIC FIELDS

$\theta_1 = 4p - 9q\theta - 6\theta^2$ and $\mu' = -1 - 6\sigma + 3\tau$.

iv) $\text{Irr}(\mu, Q) = x^3 - 3((1 + 9q)/2)x^2 + ((27q - 3)/2)x + 1$.

v) $\mu$ is not totally positive.

EXAMPLES. $p = 61, 331, 547, 817, 1141, 1951, 2437, 2977, 3571, 4219, 4921, 5677, 6487, 7351, 8269, 9241, 10267, 11347, 12481, 13669, 14911, 16207, 17557, 18961$.

THEOREM 3. Let $K = \mathbb{Q}(\theta)$, $\text{Irr}(\theta, Q) = x^3 - px + pq$, $p = 9p_1 \cdots p_r$, $p_i \equiv 1 \pmod{3}$, pairwise different primes, $q > 2$, 3 $\nmid q$, $4p - 27q^2 = 9$. The following conditions holds:

i) $\text{disc}(K) = p^2$.

ii) $\{1, \sigma, \tau = (\sigma - 1)/2 \cdot \sigma + \sigma^2)/q\}$ is an integral basis of $K$ where $\sigma = \theta_1/3$ and $\theta_1 = (p + 3\theta - 2\theta^2)/3$.

iii) $\{\mu, \mu'\}$ is a system of fundamental units of $K$, where $\mu = \sigma + \tau$ and $\mu' = -2\sigma + \tau$.

iv) $\text{Irr}(\mu, Q) = x^3 - ((3 + 9q)/2)x^2 + ((9q - 3)/2)x + 1$.

v) $\mu$ is not totally positive.

EXAMPLE. $p = 171, 333, 819, 1143, 2439, 3573, 4221, 5679, 6489, 8271, 9243, 11349, 12483, 14913, 16209$.

THEOREM 4. Let $K$ be like in theorem 2. If $q \notin \mathbb{Z}^2$ but $(1 + 3q)/2 \notin \mathbb{Z}_{q_1}$ for some prime $q_1 | q$, then $h_K$ is even.

EXAMPLE. $p = 547, q = 9; p = 4219, q = 25$.

THEOREM 5. Let $K$ like in theorem 3. If $q \notin \mathbb{Z}^2$ but $(1 + 3q)/2 \notin \mathbb{Z}_{q_1}$ for some prime $q_1 | q$, then $h_K$ is even.

EXAMPLE. $p = 16209, q = 49$.

For the sake of brevity, we omit H. Cohn [2] and M. Watanabe's [5], [6] criterion about evenness of classnumber for fields in the first family.

In 1935, Siegel proved that $h_F \to +\infty$ as the absolute value of the discriminant of the imaginary quadratic fields tends to infinite. Siegel used the formula

$$\lim_{\text{disc}(F) \to 0} \frac{\log(h_F R_F)}{\log(\text{disc}(F)^{1/2})} = 1$$

where $R_F$ is the regulator of $F$.

Since Brauer [1] proved that such a formula remains true for arbitrary number fields (supposed that the degree is fixed), we use it and our previous result to obtain our last two results.

THEOREM 6. Let $K$ be like in theorem 2, then

$$\lim_{p \to +\infty} h_K = +\infty.$$ 

THEOREM 7. Let $K$ be like in theorem 3, then

$$\lim_{p \to +\infty} h_K = +\infty.$$
For the first family we have a similar result ([5]).

REFERENCES