On totally real cubic fields whose unit groups are of type $\{\theta + r, \theta + s\}$

By Kenji MINEMURA

Graduate School of Human Informatics, Nagoya University, Chikusa-ku, Nagoya 464-8601

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 14,1998)

1. Introduction. Let $f(x)$ be a cubic polynomial with rational integer coefficients, which is monic and irreducible. Suppose that all roots θ, θ' and θ'' of $f(x) = 0$ are real, and put $K = \mathbf{Q}(\theta)$. Denote by D_f the discriminant of polynomial $f(x)$. Let $\mathfrak{o}_K$ and E_K be the ring of integers and the group of units of K respectively. Moreover we denote by E_K^+ the subset of E_K consisting of the units ε with $N_{K/\mathbf{Q}}\varepsilon = 1$. It is well known by a theorem of Dirichlet [6] that there exists a system of fundamental units $\{\varepsilon_1, \varepsilon_2\}$ such that

$$E_K = \{\pm 1\} \times E_K^+ \text{ and } E_K^+ = \langle \varepsilon_1, \varepsilon_2 \rangle.$$

Our purpose is to determine totally real cubic fields such that the system of fundamental units can be given in the form $\{\theta + r, \theta + s\}$ for some integers r, s. Note that we can reduce our problem to the case that θ is a unit in K (i.e., $r = 0$).

First, for the minimal polynomial $f(x)$ of θ over $\mathbf{Q}$, we can get the following:

Proposition 1. Suppose that s is a non-zero integer and both θ and $\theta + s$ are in E_K. Then there is an integer t such that

(a) if θ and $\theta + s$ are in E_K^+, then $f(x) = x(x+s)(x+t) - 1$.

(b) if θ and $-\theta - s$ are in E_K^+, then $f(x) = x\left(x^2 + (s+t)x + \left(st - \frac{2}{s}\right)\right) - 1$.

It is easy to prove this proposition.

Conversely we should investigate whether $\{\theta, \theta + s\}$ is a system of fundamental units. As for (i), we can reduce to the case $t \geq 1$, $s \geq t + 1$ because of $\theta(\theta + t) = (\theta + s)^{-1}$. In this condition, Stender [3] and Thomas [4] proved $E_K^+ = \langle \theta, \theta + s \rangle$, but we will prove this in a different way. As for (ii), there are only four cases $s = \pm 1, \pm 2$. The case (ii) $s = 1$ was studied by Watabe [5] completely.

Our main results are as follows:

Theorem 1 (Stender [3], Thomas [4]). In the case $f(x) = x(x+t)(x+s) - 1$ $(s, t \in \mathbf{Z})$, if D_f is positive, square free and $t \geq 1$, $s \geq t + 1$, then $E_K^+ = \langle \theta, \theta + s \rangle$ holds.

Theorem 2 $(s = -1)$. In the case $f(x) = x(x^2 + (t-1)x + (-t+2)) - 1$ $(t \in \mathbf{Z})$, if D_f is positive and square free, then $E_K^+ = \langle \theta, -\theta + 1 \rangle$ holds.

Theorem 3 $(s = 2)$. In the case $f(x) = x(x^2 + (t+2)x + 2t - 1) - 1$ $(t \in \mathbf{Z})$, if D_f is square free, then $E_K^+ = \langle \theta, -\theta - 2 \rangle$ holds.

Theorem 4 $(s = -2)$. In the case $f(x) = x(x^2 + (t-2)x - 2t + 1) - 1$ $(t \in \mathbf{Z})$, if D_f is positive, both of $t + 1$ and $4t^2 + 8t - 23$ are square free and $t \not\equiv 2 \pmod 3$, then $E_K^+ = \langle \theta, -\theta + 2 \rangle$ holds.

2. Preliminaries. We define a function S from E_K to $\mathbf{Z}$ by

$$S(\varepsilon) = \frac{1}{2}\{(\varepsilon - \varepsilon')^2 + (\varepsilon' - \varepsilon'')^2 + (\varepsilon'' - \varepsilon)^2\}.$$

Moreover, define $\mathscr{A}(K)$, and $\mathscr{B}_{\varepsilon_1}(K)$ for ε_1 in $\mathscr{A}(K)$ by

$$\mathscr{A}(K) = \{\varepsilon \in E_K^+ \backslash \{1\} \mid S(\varepsilon) \text{ is minimum}\},$$
$$\mathscr{B}_{\varepsilon_1}(K) = \{\varepsilon \in E_K^+ \backslash \{\varepsilon_1^n;\, n \in \mathbf{Z}\} \mid S(\varepsilon) \text{ is minimum}\}.$$

The following lemmas will be useful for the proof of theorems.

Lemma 1 (Brunotte, Halter-Koch [2]). If ε_1 is in $\mathscr{A}(K)$ and ε_2 is in $\mathscr{B}_{\varepsilon_1}(K)$, then $(E_K^+ : \langle \varepsilon_1, \varepsilon_2 \rangle) \leq 4$ holds.

Lemma 2 (Godwin [1]). For any ε, ε_1, ε_2 in E_K^+ and integer $m \geq 2$, we have

$$S(\varepsilon)^2 < 9S(\varepsilon^2),\ S(\varepsilon)^3 < 9S(\varepsilon^3),\ S(\varepsilon)^m < \frac{3^{m+1}}{2}S(\varepsilon^m),$$
$$S(\varepsilon_1\varepsilon_2) < 3S(\varepsilon_1)S(\varepsilon_2),\ S(\varepsilon^{-1}) \leq S(\varepsilon)^2.$$

Lemma 3. In the conditions of Theorem 1, it holds that

$$S(\theta(\theta + s)) \leq S(\theta)^2,\ S(\theta^2(\theta + s)) < S(\theta)^3.$$

Proof. We can easily prove Lemma 3 by elementary calculation. □

Lemma 4. In the conditions of Theorem 1, we have $S(\theta) \geq 12$.

Proof. We have $S(\theta) = (t+s)^2 - 3st = t^2$

$- ts + s^2$ and in the case $t \geq 1$, $s \geq t + 1$, if D_f is positive and square free, then we have $(t, s) \neq (1, 2), (1, 3), (2, 3), (3, 4)$. $\square$

3. Proofs of Theorems 1 and 2. In the condition of Theorem 1, the case $s = t + 1$ can be reduced to the case $t = 1$. So we have only to prove the case $t \geq 1$, $s \geq t + 2$.

For the proof of Theorem 1, we need some lemmas. First we shall show the next lemma.

Lemma 5. In the conditions of Theorem 1, we have $\theta \in \mathscr{A}(K)$.

Proof. Since D_f is square free, we have $\mathfrak{o}_K = \mathbf{Z} + \mathbf{Z}\theta + \mathbf{Z}\theta^2$ (Cohen [7]). For any $u \in E_K^+ \backslash \{1\}$ which is expressed in the form $u = a + b\theta + c\theta^2$, $a, b, c \in \mathbf{Z}$, $(b, c) \neq (0, 0)$, we have

$$S(u) = S(\theta)b^2 + T(\theta)c^2 + U(\theta)bc,$$

where

$$\begin{aligned} T(\theta) : &= \frac{1}{2}\{(\theta^2 - \theta'^2)^2 + (\theta'^2 - \theta''^2)^2 + (\theta''^2 - \theta^2)^2\} \\ &= t^4 - s^2t^2 - 6t + s^4 - 6s, \\ U(\theta) : &= (\theta - \theta')(\theta^2 - \theta'^2) + (\theta' - \theta'')(\theta'^2 - \theta''^2) \\ &\quad + (\theta'' - \theta)(\theta''^2 - \theta^2) \\ &= -2t^3 + st^2 + s^2t - 2s^3 + 9. \end{aligned}$$

If $c = 0$, then $S(u) = S(\theta)b^2 \geq S(\theta)$. Next, suppose $|c| = 1$. Then we have

$$S(u) = S(\theta) = (t^2 - ts + s^2)b^2 \pm (-2t^3 + st^2 + s^2t - 2s^3 + 9)b + (t^4 - (s^2 + 1)t^2 + (s - 6)t + (s^4 - s^2 - 6s)).$$

If $t \geq 2$, $s \geq t + 2$, then we can see the discriminant of the above polynomial in b is negative. So we have $S(u) > S(\theta)$. If $t = 1$, $s \geq 3$, we also have $S(u) \geq S(\theta)$ because the minimum of $S(u) - S(\theta)$ is $2s - 6 \geq 0$ when $b = \pm s$. Finally, suppose $|c| \geq 2$. Then we have $S(u) - S(\theta) \geq S(u) - \frac{1}{4}S(\theta)c^2$ and we can see the discriminant of $S(u) - \frac{1}{4}S(\theta)c^2$, as a polynomial in b, is negative. So we have $S(u) > S(\theta)$. Therefore we obtain $\theta \in \mathscr{A}(K)$. $\square$

Next, we shall show the next lemma.

Lemma 6. In the conditions of Theorem 1, we have $\theta + s \in \mathscr{B}_\theta(K)$.

Proof. Since $S(\theta + s) = S(\theta)$, its minimality is obvious.

Suppose $\theta + s = \theta^m$, $m \in \mathbf{Z}$. Since $f(x) = x^3 + (t + s)x^2 + tsx - 1$, it is easy to see $m \neq 0, \pm 1, \pm 2, \pm 3$. Suppose $m \geq 4$. From Lemma 2, we have

$$S(\theta)^m < \frac{3^{m+1}}{2} S(\theta^m) = \frac{3^{m+1}}{2} S(\theta + s) = \frac{3^{m+1}}{2} S(\theta).$$

Hence we have $S(\theta) < \left(\frac{3^{m+1}}{2}\right)^{\frac{1}{m-1}} \leq \left(\frac{3^5}{2}\right)^{\frac{1}{3}} < 5$. If $m \leq -4$, again from Lemma 2, we similarly get $S(\theta) < 12$. These contradict to Lemma 4. Thus we obtain $\theta + s \in \mathscr{B}_\theta(K)$. $\square$

Proof of Theorem 1. If we put $E_0 = \langle \theta, \theta + s \rangle$, from Lemma 1 we have

$$(E_K^+ : E_0) \leq 4.$$

First, we shall show that $(E_K^+ : E_0)$ is odd. Suppose that $(E_K^+ : E_0)$ is even, then there exists $\varepsilon \in E_K^+ \backslash E_0$ such that

$$\varepsilon^2 = \theta^k(\theta + s)^l, \quad k, l \in \{0, 1\}.$$

If $(k, l) = (0, 0)$, then $\varepsilon^2 = 1$. As $\varepsilon \in E_K^+$, we have $\varepsilon = 1$. This is a contradiction. If $(k, l) = (1, 0)$, then $\varepsilon^2 = \theta$. Since

$$S(\theta)^2 \leq S(\varepsilon)^2 < 9S(\theta),$$

we have $S(\theta) < 9$. This contradicts to Lemma 4. If $(k, l) = (0, 1)$, then we obtain a contradiction similarly. If $(k, l) = (1, 1)$, then $\varepsilon^2 = \theta(\theta + s)$. So we have

$$S(\varepsilon)^2 < 9S(\varepsilon^2) = 9S(\theta(\theta + s)) < 9S(\theta)^2.$$

Hence we obtain $S(\varepsilon) < 3S(\theta)$. But we can see by elementary way that no unit ε can satisfy the following conditions simultaneously:

$$\begin{cases} \varepsilon^2 = \theta(\theta + s), \\ S(\varepsilon) < 3S(\theta), \\ \varepsilon \in E_K^+. \end{cases}$$

Finally we shall show that $(E_K^+ : E_0) \neq 3$. Suppose that $(E_K^+ : E_0) = 3$, then there exists $\varepsilon \in E_K^+ \backslash E_0$ such that

$$\varepsilon^3 = \theta^k(\theta + s)^l, \quad k, l \in \{0, 1, 2\}.$$

If $(k, l) = (0, 0)$, then $\varepsilon = 1$. This is a contradiction. If $(k, l) = (1, 0)$, then $\varepsilon^3 = \theta$. Since

$$S(\theta)^3 \leq S(\varepsilon)^3 < 9S(\theta),$$

we have $S(\theta) < \sqrt[3]{9}$. In a similar way, if $(k, l) = (0, 1), (1, 1)$, then it follows from Lemmas 2 and 3 that $S(\theta) < \sqrt[3]{9}$, 9 respectively. These contradict to Lemma 4. If $(k, l) = (2, 1)$, then $\varepsilon^3 = \theta^2(\theta + s)$. Since

$$S(\varepsilon)^3 < 9S(\varepsilon^3) = 9S(\theta^2(\theta + s)) < 9S(\theta)^3,$$

we have $S(\varepsilon) < \sqrt[3]{9}S(\theta)$. If $(t, s) \neq (2, 4), (3, 5), (4, 6), (5, 7), (2, 5)$, we can see by elementary way that no unit ε can satisfy the following conditions simultaneously:

$$\begin{cases} \varepsilon^3 = \theta^2(\theta + s), \\ S(\varepsilon) < \sqrt[3]{9}S(\theta), \\ \varepsilon \in E_K^+. \end{cases}$$

Otherwise, we can improve $S(\varepsilon) < \sqrt[3]{9}S(\theta)$, and we can also see that there is no unit ε satisfying these improved condition.

The cases $(k, l) = (2, 0), (0, 2), (1, 2)$, and $(2, 2)$ are reduced to the cases $(k, l) = (1, 0), (0, 1), (2, 1)$ and $(1, 1)$ respectively. This completes the proof of Theorem 1. □

Corollary 1. In the case $f(x) = x^3 \mp (tx + 1)(sx + 1)(t < s, t \neq 0, s \neq 0)$, if D_f is positive and square free, then E_K^+ is generated by two of the three units $\pm\theta, \pm t\theta \pm 1, \pm s\theta \pm 1$.

Proof of Corollary 1. This follows by the variable transformation $\theta := \pm \frac{1}{\theta}$ in Theorem 1. □

Proof of Theorem 2. If we put $s := -1, t := t + 1$ in Corollary 1, we obtain the polynomial in Theorem 2. So we can get Theorem 2. □

4. Proofs of Theorem 3 and 4. Proof of Theorem 3. Since we can reduce the case $t \leq 0$ to the case $t \geq 1$ and moreover the cases $t = 1, 2, 3$ do not satisfy the condition in Theorem 3, we may consider the case $t \geq 4$. In this case, we have

(1) $S(\theta) = (t+2)^2 - 3(2t-1) = t^2 - 2t + 7 > 15.$

In the conditions in Theorem 3, we have $\mathfrak{o}_K = \mathbf{Z} + \mathbf{Z}\theta + \mathbf{Z}\theta^2$ (Cohen [7]). $\theta \in \mathscr{A}(K)$ and $-\theta - 2 \in \mathscr{B}_\theta(K)$ hold by the similar way to the proof of Lemmas 5,6.

Let $E_0 = \langle\theta, -\theta - 2\rangle$. From Lemma 1 we get

$$(E_K^+ : E_0) \leq 4.$$

We shall first show that $(E_K^+ : E_0)$ is odd. Suppose that $(E_K^+ : E_0)$ is even, then there exists $\varepsilon \in E_K^+ \setminus E_0$ such that

$$\varepsilon^2 = \theta^k(-\theta - 2)^l, \quad k, l \in \{0, 1\}.$$

It follows by the same argument as in the proof of Theorem 1 that $(k, l) \neq (0, 0), (1, 0)$ and $(0,1)$. If $(k, l) = (1, 1)$, then $\varepsilon^2 = \theta(-\theta - 2)$ holds. Hence we have $\theta^2 + 2\theta + \varepsilon^2 = 0$. Since $\theta \in \mathbf{R}$, we have $1 - \varepsilon^2 > 0$. Thus we obtain $|\varepsilon| < 1$. Similarly, $|\varepsilon'| < 1, |\varepsilon''| < 1$ hold. These contradict to $\varepsilon\varepsilon'\varepsilon'' = 1$.

We shall next show that $(E_K^+ : E_0) \neq 3$. Suppose that $(E_K^+ : E_0) = 3$, then there exists $\varepsilon \in E_K^+ \setminus E_0$ such that

$$\varepsilon^3 = \theta^k(-\theta - 2)^l, \quad k, l \in \{0, 1, 2\}.$$

In the cases $(k, l) = (0, 0), (1, 0)$ and $(0,1)$, we can obtain a contradiction by the similar way to the proof of Theorem 1. If $(k, l) = (1, 1)$, then $\varepsilon^3 = \theta(-\theta - 2)$ holds. On the other hand, we can show that $S(\theta(-\theta - 2)) < S(\theta)^2$ by elementary calculation. So we have

$$S(\theta)^3 \leq S(\varepsilon)^3 < 9S(\theta(-\theta - 2)) < 9S(\theta)^2.$$

Hence we obtain $S(\theta) < 9$, which contradicts to (1). If $(k, l) = (2, 1)$, then we have $\varepsilon^3 = \theta^2(-\theta - 2)$, and so $\theta^3 + 2\theta^2 + \varepsilon^3 = 0$. Since the discriminant $-\varepsilon^3(27\varepsilon^3 + 32)$ of the above must be positive, we have $\varepsilon < 0$. Similarly $\varepsilon' < 0, \varepsilon'' < 0$ hold. These contradict to $\varepsilon\varepsilon'\varepsilon'' = 1$.

We can reduce $(k, l) = (2, 0), (0, 2), (1, 2)$ and $(2,2)$ to $(k, l) = (1, 0), (0, 1), (2, 1)$ and $(1,1)$ respectively. As a result, we have $(E_K^+ : E_0) = 1$. Therefore we obtain $E_K^+ = \langle\theta, -\theta - 2\rangle$. □

Proof of Theorem 4. From Theorems 3.1 and 3.2 in Fujisaki [8, chap. 4], we can see that D_f is the discriminant of K, so we have $\mathfrak{o}_K = \mathbf{Z} + \mathbf{Z}\theta + \mathbf{Z}\theta^2$. The rest can be proved in a similar way to the proof of Theorem 3. □

Corollary 2. In the case $f(x) = x^3 - (2t - 1)x^2 - (t + 2)x - 1$, if D_f is square free, then $E_K^+ = \langle\theta, 2\theta - 1\rangle$.

Corollary 3. In the case $f(x) = x^3 - (-2t + 1)x^2 - (t - 2)x - 1$, if D_f is positive, both of $t + 1$ and $4t^2 + 8t - 23$ are square free and $t \not\equiv 2 \pmod 3$, then $E_K^+ = \langle\theta, 2\theta - 1\rangle$.

Proof of Corollarys 2 and 3. We can get these results from Theorem 3 and 4 by the variable transformation $\theta := \frac{1}{\theta}$. □

References

[1] H. J. Godwin: The determination of units in totally real cubic fields. Proc. Cambrige Philos. Soc., **56**, 318–321 (1960).

[2] H. Brunotte and F. Halter-Koch: Zur Einheitenberechnung in totalreelen kubischen Zahlkörpern nach Godwin. J. Number Theory, **11**, 552–559 (1979).

[3] H. J. Stender: Einheiten für eine allgemeine Klasse total reeller algebraischer Zahlkörper. J. Reine Angew. Math., **257**, 151–178 (1972).

[4] E. Thomas: Fundamental units for orders in certain cubic number fields. J. Reine Angew. Math., **310**, 33–55 (1979).

[5] M. Watabe: On certain cubic fields I, III, VI. Proc. Japan Acad., **59A**, 66–69, 260–262 (1983); **60A**, 331–332 (1984).

[6] A. Fröhlich and M. J. Taylor: Algebraic Number Theory. Cambridge Univ. Press, Cambridge (1991).

[7] H. Cohen: A course in computational algebraic number theory. Second Corrected Printing,

GTM138, Springer-Verlag, (1995).
[8] G. Fujisaki: Daisūteki Seisūron Nyūmon. Shoukabou (1974) (in Japanese).