Journal of Number Theory **80**, 209–217 (2000)
Article ID jnth.1999.2455, available online at http://www.idealibrary.com on IDEAL®

Parametrization of the Quadratic Fields Whose Class Numbers are Divisible by Three

Yasuhiro Kishi and Katsuya Miyake[1]

Department of Mathematics, Tokyo Metropolitan University, Minami-Ohsawa 1-1, Hachioji-shi, Tokyo 192-0397, Japan
E-mail: ykishi@comp.metro-u.ac.jp and miyakek@comp.metro-u.ac.jp

Communicated by A. C. Woods

Received August 18, 1998

of $g(Z)=Z^3-uwZ-u^2$.

1. THE MAIN THEOREM

We consider a polynomial of the form

$$g(Z)=Z^3-uwZ-u^2, \qquad u, w \in \mathbf{Z},$$

where u and w are relatively prime, $d:=4uw^3-27u^2$ is not a square in Z, and one of the following conditions holds:

$$\begin{aligned} &\text{(i)} \quad 3 \nmid w; \\ &\text{(ii)} \quad 3 \mid w, \quad uw \not\equiv 3 \pmod 9, \quad u \equiv w \pm 1 \pmod 9; \\ &\text{(iii)} \quad 3 \mid w, \quad uw \equiv 3 \pmod 9, \quad u \equiv w \pm 1 \pmod{27}. \end{aligned} \tag{1.1}$$

The discriminant of $g(Z)$ is

$$D=u^2d,$$

and is not a square in Z by the assumption. If $g(Z)$ is irreducible over Q, then the minimal splitting field of $g(Z)$ contains the quadratic field $\mathbf{Q}(\sqrt{d})$, and its Galois group over Q is the symmetric group S_3.

[1] This author was partially supported by Grant-in-Aid for Scientific Research (A) (No. 08304004), Ministry of Education, Science and Culture.

0022-314X/00 $35.00

MAIN THEOREM. *Let the notation and the assumptions be as above. If* $g(Z)$ *is irreducible over* Q, *then the roots of* $g(Z)=0$ *generate an unramified cyclic cubic extension of the quadratic field* $\mathrm{Q}(\sqrt{d})$. *Conversely, every quadratic field whose class number is divisible by* 3 *and every unramified cyclic cubic extension of it are given in this way by a suitable pair of integers* u *and* w.

2. PROOF

It is well-known that every unramified cyclic cubic extension of a quadratic field is normal over Q and is an S_3-extension of Q. Every S_3-extension of Q is given by a cubic equation of the form

$$X^3 - tX - t = 0, \qquad t \in \mathrm{Q}. \tag{2.1}$$

Indeed, we suppose that the polynomial

$$Irr(\theta; X) = X^3 - aX - b, \qquad a, b(\neq 0) \in \mathrm{Q},$$

generate the cubic field $\mathrm{Q}(\theta)$. If $a=0$, then we see

$$Irr\left(\theta + \frac{1}{\theta}; X\right) = X^3 - 3X - b - \frac{1}{b}.$$

Hence we may assume that $ab \neq 0$. And then we have

$$Irr\left(\frac{a}{b}\theta; X\right) = X^3 - \frac{a^3}{b^2}X - \frac{a^3}{b^2}.$$

Express $t = v/u$ $(u, v \in \mathrm{Z},\ (u, v) = 1)$, and multiply both sides of (2.1) by u^3. If we put $Y = uX$, then we obtain

$$f(Y) := Y^3 - uvY - u^2v = 0. \tag{2.2}$$

Let p be a prime number. It is easy to see that a prime divisor of p in $\mathrm{Q}(\sqrt{d})$ is ramified in the minimal splitting field of $f(Y)$ if and only if p is totally ramified in a cubic field generated by a root of $f(Y)=0$. Hence we determine the conditions under which no primes are totally ramified in the cubic field.

For a prime number p and an integer m, we denote the greatest exponent μ of p such that $p^\mu \mid m$ by $V_p(m)$. Here we extract some results from P. Llorente and E. Nart [Ll-Nar].

PROPOSITION (Llorente and Nart). *Suppose that the cubic polynomial*

$$F(X) = X^3 - aX - b, \qquad a, b \in \mathbf{Z},$$

is irreducible over Q, *and that either* $V_p(a) < 2$ *or* $V_p(b) < 3$ *holds for a prime* p. *Let* θ *be a root of* $F(X) = 0$, *and put* $K = \mathbf{Q}(\theta)$.

(a) *When* $p \neq 3$, p *is totally ramified in* $K/\mathbf{Q}$ *if and only if*

$$1 \leqslant V_p(b) \leqslant V_p(a).$$

(b) *When* $p = 3$, 3 *is totally ramified in* $K/\mathbf{Q}$ *if and only if one of the following conditions holds*:

(i) $1 \leqslant V_3(b) \leqslant V_3(a)$;

(ii) $3 \mid a$, $a \not\equiv 3 \pmod 9$, $3 \nmid b$, *and* $b^2 \not\equiv a + 1 \pmod 9$;

(iii) $a \equiv 3 \pmod 9$, $3 \nmid b$, *and* $b^2 \not\equiv a + 1 \pmod{27}$.

To utilize this proposition, let us closely investigate the Eq. (2.2). Take a root θ of $f(Y) = 0$ and put $K = \mathbf{Q}(\theta)$.

LEMMA 1. *Let* p *be a prime factor of* v. *If* $p \neq 3$, *then* p *is totally ramified in* $K/\mathbf{Q}$ *if and only if* $V_p(v) \not\equiv 0 \pmod 3$. *If* $p = 3$, 3 *is totally ramified in* $K/\mathbf{Q}$ *if* $V_3(v) \not\equiv 0 \pmod 3$.

Proof. Suppose that $V_p(v) = 3n + \alpha \geqslant 1$ ($\alpha = 0$, 1 or 2), and put $v = p^{3n+\alpha}v'$. Then $(p, v') = 1$. We have

$$Y^3 - p^{3n+\alpha}uv'Y - p^{3n+\alpha}u^2v' = 0.$$

Divide both sides by p^{3n}, and put $Z = Y/p^n$; then we get

$$Z^3 - p^{n+\alpha}uv'Z - p^{\alpha}u^2v' = 0.$$

When $p \neq 3$, we see by the proposition that p is totally ramified in $K/\mathbf{Q}$ if and only if $\alpha \neq 0$. For $p = 3$, it follows from (i) of the proposition that 3 is totally ramified in $K/\mathbf{Q}$ if $\alpha \neq 0$. ∎

Hence to obtain the condition under which no primes are totally ramified in $K/\mathbf{Q}$, we assume $V_p(v) \equiv 0 \pmod 3$ for every prime p. Then v is a cube in Z. Take $w \in \mathbf{Z}$ so that we have $v = w^3$. Put $Y = wZ$ in (2.2) and divide both sides by w^3; then we obtain

$$g(Z) := Z^3 - uwZ - u^2 = 0, \qquad (u, w) = 1.$$

It is clear that $g(\theta/w) = 0$ and $K = \mathbf{Q}(\theta/w)$.

If $p \nmid uw$, then the proposition assures us that p is not totally ramified in $K/\mathbf{Q}$.

LEMMA 2. *No prime factors of u are totally ramified in $K/\mathbf{Q}$.*

Proof. Suppose that $V_p(u) = 2n + \beta \geqslant 1$ ($\beta = 0$ or 1), and put $u = p^{2n+\beta}u'$. Then $(p, u') = (p, w) = 1$. We have

$$g(Z) = Z^3 - p^{2n+\beta}u'wZ - p^{4n+2\beta}u'^2 = 0.$$

Divide both sides by p^{3n}, and put $W = Z/p^n$; then we get

$$W^3 - p^{\beta}u'wW - p^{n+2\beta}u'^2 = 0.$$

It is now clear by the proposition that p is not totally ramified in $K/\mathbf{Q}$. ∎

If $p \mid w$ and $p \neq 3$, it is clear by the proposition that p is not totally ramified in $K/\mathbf{Q}$.

Now suppose $3 \mid w$. Then $3 \nmid u$ because $(u, w) = 1$. Therefore $u \equiv \pm 1 \pmod 3$. It follows from the proposition that 3 is not totally ramified in $K/\mathbf{Q}$ if and only if either

$$uw \not\equiv 3 \pmod 9, \qquad u^4 \equiv uw + 1 \pmod 9,$$

or

$$uw \equiv 3 \pmod 9, \qquad u^4 \equiv uw + 1 \pmod{27}.$$

Since $u \equiv \pm 1 \pmod 3$, we have $u^3 \equiv \pm 1 \pmod 9$. Take $x \in \mathbf{Z}$ so that we have $ux \equiv 1 \pmod 9$. Then in $\mathbf{Z}/9\mathbf{Z}$, we see

$$\begin{aligned} u - (w \pm 1) - (u^3 - (w + x)) &= u \mp 1 - u^3 + x \\ &\equiv u \mp 2 + x \\ &\equiv x(u^2 \mp 2u + 1) \\ &= x(u \mp 1)^2 \\ &\equiv 0. \end{aligned}$$

Therefore we have

$$u^4 \equiv uw + 1 \pmod 9 \Leftrightarrow u^3 \equiv w + x \pmod 9 \Leftrightarrow u \equiv w \pm 1 \pmod 9.$$

Assume now $uw \equiv 3 \pmod 9$. Since $u \equiv \pm 1 \pmod 3$, we have $w \equiv \pm 3 \pmod 9$. Put

$$u = 3u' \pm 1, \qquad w = 9w' \pm 3.$$

Since

$$u^4 = (3u' \pm 1)^4 \equiv \pm 12u' + 1 \pmod{27},$$

we see

$$\begin{aligned} u^4 \equiv uw + 1 \pmod{27} &\Leftrightarrow \pm 12u' + 1 \equiv (3u' \pm 1)(9w' \pm 3) + 1 \pmod{27} \\ &\Leftrightarrow \pm 12u' + 1 \equiv \pm 9u' \pm 9w' + 3 + 1 \pmod{27} \\ &\Leftrightarrow \pm 3u' + 1 \equiv \pm 9w' + 3 + 1 \pmod{27} \\ &\Leftrightarrow \pm (3u' \pm 1) \equiv \pm (9w' \pm 3) + 1 \pmod{27} \\ &\Leftrightarrow \pm u \equiv \pm w + 1 \pmod{27} \\ &\Leftrightarrow u \equiv w \pm 1 \pmod{27}. \end{aligned}$$

This completes the proof of the main theorem.

3. ON SOME KNOWN RESULTS

There are known families of quadratic fields whose class numbers are divisible by 3. In this section, we exhibit four such families, and show how they are related with our theorem. The class number of a quadratic field k is denoted by $h(k)$.

THEOREM 1 (Honda [Ho]). *Let m and n be rational integers, and suppose that* (a) $(m, 3n) = 1$, (b) $4m^3 - 27n^2$ *is not square, and* (c) m *cannot be expressed as* $(n + a^3)/a$ *with* $a \in \mathbf{Z}$. *Then the class number of* $\mathbf{Q}(\sqrt{4m^3 - 27n^2})$ *is divisible by* 3.

In this case, put $u = n^2$ and $w = m$ in our main theorem. Then we have

$$Z^3 - n^2 m Z - n^4 = 0,$$

and $d = 4n^2m^3 - 27n^4$. Divide both sides of the equation by n^3, and put $X = Z/n$; then we get

$$f(X) := X^3 - mX - n = 0.$$

The assumption (c) implies that $f(X)$ is irreducible over Q. It follows from the assumption (a) that the condition (i) of (1.1) holds. Hence we have

$$3 \mid h(\mathbf{Q}(\sqrt{4n^2m^3 - 27n^4})) = h(\mathbf{Q}(\sqrt{4m^3 - 27n^2}))$$

also by the main theorem.

THEOREM 2 (Hartung [Ha]). *Let m be a square free integer. If $m \equiv 7 \pmod{12}$ and if m is of the form $(n^2-4)/27$ where n is an integer, then the class number of $\mathbf{Q}(\sqrt{-m})$ is divisible by 3.*

Put $u = n^2$ and $w = 3$ in our main theorem. Then we have

$$Z^3 - 3n^2 Z - n^4 = 0,$$

and $d = 4 \cdot 27n^2 - 27n^4$. Divide both sides by n^3, and put $X = Z/n$; then we get

$$f(X) := X^3 - 3X - n = 0.$$

Since $n^2 = 27m + 4$ and m is a square free integer, n cannot be even. Assume that $f(X)$ is reducible; then there exists $a \in \mathbf{Z}$ such that $a^3 - 3a - n = 0$; therefore

$$n = a^3 - 3a = a(a^2 - 3),$$

and n is even. This is a contradiction. Therefore $f(X)$ is irreducible. Since

$$uw = 3n^2 \equiv 3 \pmod{9},$$

and

$$u = n^2 \equiv 4 = w + 1 \pmod{27},$$

the condition (iii) of (1.1) holds. Hence by the main theorem we have

$$3 \mid h(\mathbf{Q}(\sqrt{4 \cdot 27n^2 - 27n^4})) = h\left(\mathbf{Q}\left(\sqrt{-\frac{n^2-4}{27}}\right)\right) = h(\mathbf{Q}(\sqrt{-m})).$$

For our argument here, the condition $m \equiv 7 \pmod{12}$ is not necessary. We give a table of integers n for which $m = (n^2-4)/27$ is not a square, and the class number of $k = \mathbf{Q}(\sqrt{-m})$.

n	m	k	$h(k)$	n	m	k	$h(k)$
25	23	$\mathbf{Q}(\sqrt{-23})$	3	133	655	$\mathbf{Q}(\sqrt{-655})$	12
29	31	$\mathbf{Q}(\sqrt{-31})$	3	137	695	$\mathbf{Q}(\sqrt{-695})$	24
56	116	$\mathbf{Q}(\sqrt{-29})$	6	160	948	$\mathbf{Q}(\sqrt{-237})$	12
79	231	$\mathbf{Q}(\sqrt{-231})$	12	164	996	$\mathbf{Q}(\sqrt{-249})$	12
83	255	$\mathbf{Q}(\sqrt{-255})$	12	187	1295	$\mathbf{Q}(\sqrt{-1295})$	36
106	416	$\mathbf{Q}(\sqrt{-26})$	6	191	1351	$\mathbf{Q}(\sqrt{-1351})$	24
110	448	$\mathbf{Q}(\sqrt{-7})$	1	214	1696	$\mathbf{Q}(\sqrt{-106})$	6

In the table, only $n=29$, 133 and 191 satisfy the condition $m\equiv 7 \pmod{12}$. In case of $n=110$, the class number of k is equal to 1 and is not divisible by 3. This is because the polynomial $f(X)$ is reducible over Q:

$$f(X)=X^3-3X-110=(X-5)(X^2+5X+22).$$

THEOREM 3 (Ohta [Oh]). *Let a and b be rational integers and $p_1, \dots, p_r$ be prime numbers different from each other, and suppose that we have $(6ab, p_1\cdots p_r)=1$ and $(3a, 4b)=1$. Let $\alpha_1, \dots, \alpha_r$ be positive integers. If we have either*

$$\begin{cases} ap_1^{\alpha_1}\cdots p_r^{\alpha_r}\equiv \pm 1 \pmod 3 \\ bp_1\cdots p_r\equiv 1 \pmod 3 \end{cases} \tag{3.1}$$

or

$$\begin{cases} ap_1^{\alpha_1}\cdots p_r^{\alpha_r}\equiv \pm 2 \pmod 5 \\ bp_1\cdots p_r\equiv 1 \pmod 5, \end{cases} \tag{3.2}$$

then the class number of the quadratic field

$$\mathrm{Q}(\sqrt{p_1\cdots p_r(4^4b^3-3^3a^4p_1^{4\alpha_1-3}\cdots p_r^{4\alpha_r-3})})$$

is divisible by 3.

In this case, put $u=a^4p_1^{4\alpha_1-3}\cdots p_r^{4\alpha_r-3}$ and $w=4b$ in our main theorem. Then we have

$$g(Z)=Z^3-4a^4bp_1^{4\alpha_1-3}\cdots p_r^{4\alpha_r-3}Z-a^8p_1^{2(4\alpha_1-3)}\cdots p_r^{2(4\alpha_1-3)}, \tag{3.3}$$

and

$$\begin{aligned} d&=4a^4p_1^{4\alpha_1-3}\cdots p_r^{4\alpha_r-3}\cdot 4^3b^3-27a^8p_1^{2(4\alpha_1-3)}\cdots p_r^{2(4\alpha_1-3)} \\ &=(a^2p_1^{2\alpha_1}\cdots p_r^{2\alpha_r})^2\, p_1\cdots p_r(4^4b^3-3^3a^4p_1^{4\alpha_1-3}\cdots p_r^{4\alpha_r-3}). \end{aligned}$$

Dividing both sides of the Eq. (3.3) by $(ap_1^{\alpha_1-1}\cdots p_r^{\alpha_r-1})^6$ and putting $X=Z/(ap_1^{\alpha_1-1}\cdots p_r^{\alpha_r-1})^2$, we have

$$f(X):=X^3-4bp_1\cdots p_rX-(ap_1^{\alpha_1}\cdots p_r^{\alpha_r})^2.$$

If the condition (3.1) holds, then we have

$$f(X)\equiv X^3-X-1 \pmod 3.$$

Since X^3-X-1 is irreducible with respect to modulo 3, $f(X)$ is also irreducible over Q. Similarly, if the condition (3.2) holds, then we see that $f(X)$ is irreducible over Q because

$$f(X) \equiv X^3+X+1 \pmod 5.$$

By the assumptions, we have $(u, w)=1$ and $3 \nmid w$. Hence the condition (i) of (1.1) holds. Therefore our Main Theorem implies

$$3 \mid h(\mathrm{Q}(\sqrt{p_1 \cdots p_r(4^4b^3-3^3a^4p_1^{4\alpha_1-3} \cdots p_r^{4\alpha_r-3})}).$$

THEOREM 4 (Brinkhuis [Br]). *Let m be a rational integer which cannot be written in the form n^3-n^2 for any integer n. Then the class number of $\mathrm{Q}(\sqrt{-4m-27m^2})$ is divisible by* 3.

This theorem follows from the main theorem if we put $u=m$ and $w=-1$. In fact, we have

$$Z^3+mZ-m^2=0,$$

and $d=-4m-27m^2$. Multiply both sides of the equation by m/Z^3, and put $X=m/Z$; then we get

$$f(X) := X^3-X^2-m=0.$$

By the assumption, we see that $f(X)$ is irreducible over Q. Since $w=-1$ is not divisible by 3, the condition (i) of (1.1) holds. Hence we have

$$3 \mid h(\mathrm{Q}(\sqrt{-4m-27m^2})).$$

Remark. Hendy [He], Mollin [Mo], Nakahara [Nak] and Uehara [Ue] also gave families of infinitely many quadratic fields with class numbers divisible by 3. All of their results are proved by means of constructing an ideal class of order 3. The authors have not yet found any clear expressions of their families by means of our Main Theorem.

REFERENCES

[Br] J. Brinkhuis, Normal integral bases and the spiegelungssatz of Scholz, *Acta Arithmetica* **69** (1995), 1–9.

[Ha] P. Hartung, Explicit construction of a class of infinitely many imaginary quadratic fields whose class number is divisible by 3, *J. Number Theory* **6** (1974), 279–281.

[He] M. D. Hendy, Class number divisors for some real quadratic fields, *Occ. Pub. Math.* **5** (1977), 1–3.

[Ho] T. Honda, On real quadratic fields whose class numbers are multiples of 3, *Reine Angew. Math.* **273** (1968), 101–102.

[Ll-Nar] P. Llorente and E. Nart, Effective determination of the decomposition of the rational prime in a cubic field, *Proc. American Math. Soc.* **87** (1983), 579–585.

[Mo] R. A. Mollin, Solutions of diophantine equations and divisibility of class numbers of complex quadratic fields, *Glasgow Math. J.* **38** (1996), 195–197.

[Nak] T. Nakahara, On real quadratic fields whose ideal class groups have a cyclic p-subgroup, *Reports Fac. Sci. Eng. Saga Univ. Math.* **6** (1978), 15–26.

[Oh] K. Ohta, On algebraic number fields whose class numbers are multiples of 3, *Mem. Gifu Tech. Coll.* **17** (1981), 51–54.

[Ue] T. Uehara, On class numbers of imaginary quadratic and quartic fields, *Archiv der Math.* **41** (1983), 256–260.