*Glasgow Math. J.* **52** (2010) 575–581. © Glasgow Mathematical Journal Trust 2010.
doi:10.1017/S0017089510000431.

# ON THE IDEAL CLASS GROUP OF CERTAIN QUADRATIC FIELDS

YASUHIRO KISHI

*Department of Mathematics, Fukuoka University of Education,*
*1-1 Bunkyoumachi Akama, Munakata-shi, Fukuoka 811-4192, Japan*
*e-mail: ykishi@fukuoka-edu.ac.jp*

(Received 8 June 2009; revised 6 May 2010; accepted 28 June 2010)

**Abstract.** Let $n\,(\geq 3)$ be an odd integer. Let $k := \mathbb{Q}(\sqrt{4-3^n})$ be the imaginary quadratic field and $k' := \mathbb{Q}(\sqrt{-3(4-3^n)})$ the real quadratic field. In this paper, we prove that the class number of $k$ is divisible by 3 unconditionally, and the class number of $k'$ is divisible by 3 if $n\,(\geq 9)$ is divisible by 3. Moreover, we prove that the 3-rank of the ideal class group of $k$ is at least 2 if $n\,(\geq 9)$ is divisible by 3.

2010 *Mathematics Subject Classification.* 11R11, 11R29.

**1. Introduction.** The ideal class group is one of the most basic and mysterious objects in algebraic number theory. According to the result of Y. Yamamoto [**9**], there exist infinitely many quadratic fields whose $p$-ranks of the ideal class groups at least two for arbitrary given prime $p$. However, it is difficult to characterize quadratic fields whose Sylow $p$-subgroups of the ideal class groups are not cyclic. In [**1**], C. Erickson et al. gave a simple parametric family of quadratic fields, whose 3-ranks of the ideal class groups at least two. In this paper, we give another family of such quadratic fields.

For an odd integer $n\,(\geq 3)$, we consider two quadratic fields

$$k := \mathbb{Q}(\sqrt{4-3^n}) \text{ and } k' := \mathbb{Q}(\sqrt{-3(4-3^n)}).$$

In the case, where $4-3^n$ is square-free, we can easily see that the class number of $k$ is divisible by 3. Indeed, the splitting field of

$$f(X) = X^3 - X + 3^{(n-3)/2}$$

over $\mathbb{Q}$ is an unramified cyclic cubic extension of $k$ because the discriminant of $f$ is equal to $4-3^n$. The first aim of this paper is to remove the condition 'square-free' in the above statement; that is, we will prove

THEOREM 1. *For an odd integer $n \geq 3$, the class number of $k$ is divisible by* 3.

Next we will prove the following result concerning the divisibility of the class number of $k'$.

THEOREM 2. *For an integer $n \geq 9$ such that $n \equiv 3 \pmod 6$, the class number of $k'$ is divisible by* 3.

For a square-free negative integer $d$ in general, denote the 3-rank of the ideal class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ and the real quadratic field $\mathbb{Q}(\sqrt{-3d})$ by $r$ and $s$, respectively. It is well known that the inequalities $s \leq r \leq s+1$ hold (see e.g. [**8**]). As in our previous paper [**4**, Theorem 7.1], it follows immediately that

https://doi.org/10.1017/S0017089510000431 Published online by Cambridge University Press

PROPOSITION 1.1. *Let $d$ be a square-free negative integer with $3 \nmid d$. Then $r = s$ if and only if there are no cubic fields $K$ with $D_K = -3^3 d$, where $D_K$ is the discriminant of $K$.*

By using this proposition and Theorem 2, we will prove

THEOREM 3. *For an integer $n \geq 9$ such that $n \equiv 3 \pmod 6$, the 3-rank of the ideal class group of $k$ is at least 2.*

Recently, the author proved in his paper [**5**] that for any integer $n\,(\geq 2)$, the ideal class group of $k$ has a subgroup isomorphic to $C_n$, where $C_n$ is the cyclic group of order $n$. From this, together with Theorem 1 and Theorem 3, we immediately have

COROLLARY 1. *For an odd integer $n \geq 5$, the ideal class group of $k$ has a subgroup isomorphic to $C_n \times C_3$. In particular, therefore, the class number of $k$ is divisible by $3n$.*

**2. Proofs of theorems.** For a number field $K$, denote the discriminant, the norm map and the trace map of $K/\mathbb{Q}$ by $D_K$, $N_K$ and by $\mathrm{Tr}_K$, respectively.

For an integer $m$ and a prime $p$, $v_p(m)$ denotes the greatest exponent $\mu$ of $p$ such that $p^\mu \mid m$.

For an element $\alpha$ of a quadratic field $k$ such that $N_k(\alpha) = m^3$ for some $m \in \mathbb{Z}$, define the cubic polynomial $f_\alpha$ by

$$f_\alpha(X) = X^3 - 3mX - \mathrm{Tr}_k(\alpha).$$

The following proposition, which combined [**3**, Lemma 1] and [**4**, Proposition 6.5], is one of the main ingredients in the proofs of our theorems.

PROPOSITION 2.1. *Let $d$ be an integer with $d \notin \mathbb{Z}^2 \cup (-3\mathbb{Z}^2)$ and put $k := \mathbb{Q}(\sqrt{d})$ and $k' := \mathbb{Q}(\sqrt{-3d})$. Let $\alpha$ be an integer in $k'$ whose norm is a cube in $\mathbb{Z}$; $N_{k'}(\alpha) = m^3$ $(m \in \mathbb{Z})$. Then the polynomial $f_\alpha$ is reducible over $\mathbb{Q}$ if and only if $\alpha$ is a cube in $k'$. Moreover, if $f_\alpha$ is irreducible over $\mathbb{Q}$, then the splitting field of $f_\alpha$ over $\mathbb{Q}$ is a cyclic cubic extension of $k$ unramified outside 3 and $v_3(D_K) \neq 5$ for some cubic subfield $K$.*

REMARK 2.2. It is well known that we have $v_3(D_K) = 0, 1, 3, 4$ or $5$ for a cubic field $K$ (see e.g. [**2**, Satz 6].) The prime 3 is totally ramified in $K$ if and only if $v_3(D_K) = 3, 4$ or 5.

Next, we extract some results from P. Llorente and E. Nart [**7**, Theorem 1].

PROPOSITION 2.3. *Suppose that the cubic polynomial*

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

*is irreducible over $\mathbb{Q}$, and that either $v_3(a) < 2$ or $v_3(b) < 3$ holds. Let $\theta$ be a root of $F(X) = 0$, and put $K = \mathbb{Q}(\theta)$. Then the prime 3 is totally ramified in $K/\mathbb{Q}$ if and only if one of the following conditions holds*:

(LN-i) $1 \leq v_3(b) \leq v_3(a)$;

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

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

https://doi.org/10.1017/S0017089510000431 Published online by Cambridge University Press

*Proof of Theorem* 1. By the assumption, we can express $n = 2m + 1$, $m\,(\geq 1) \in \mathbb{Z}$. Define the element $\alpha \in k' = \mathbb{Q}(\sqrt{3^{2(m+1)} - 12})$ by

$$\alpha := \frac{3^{2m+1} - 2 + 3^m\sqrt{3^{2(m+1)} - 12}}{2}.$$

Then we have

$$N_{k'}(\alpha) = 1^3 \text{ and } \mathrm{Tr}_{k'}(\alpha) = 3^{2m+1} - 2.$$

The polynomial

$$f_\alpha(X) = X^3 - 3X - (3^{2m+1} - 2)$$

is irreducible over $\mathbb{Q}$ because

$$f_\alpha(X) \equiv X^3 - X - 1 \pmod 2$$

is irreducible over $\mathbb{F}_2$. Then by Proposition 2.1, the splitting field of $f_\alpha$ over $\mathbb{Q}$ is a cyclic cubic extension of $k$ unramified outside 3. Moreover, $f_\alpha$ does not satisfy the conditions (LN-i), (LN-ii) and (LN-iii) in Proposition 2.3. Therefore, the splitting field of $f_\alpha$ over $\mathbb{Q}$ is an unramified cyclic cubic extension of $k$, and hence the class number of $k$ is divisible by 3. □

REMARK 2.4. We will give another proof of Theorem 1 by using [**6**, Theorem]. Put $u = 3^{2(m-1)}$ and $w = 1$ in [**6**, Theorem]; we have

$$g(Z) = Z^3 - 3^{2(m-1)}Z - 3^{4(m-1)}$$

and

$$d = 4 \cdot 3^{2(m-1)} - 27 \cdot (3^{2(m-1)})^2 = 3^{2(m-1)}(4 - 3^{2m+1}).$$

We easily see that the condition (i) in [**6**, Theorem] holds. Furthermore,

$$g(Z) = Z^3 - 3^{2(m-1)}Z - 3^{4(m-1)} \equiv Z^3 - Z - 1 \pmod 2$$

is irreducible over $\mathbb{F}_2$, so $g(Z)$ is irreducible over $\mathbb{Q}$. Then the class number of $\mathbb{Q}(\sqrt{d}) = k$ is divisible by 3.

*Proof of Theorem* 2. By the assumption, we can express $n = 6u + 3$, $u\,(\geq 1) \in \mathbb{Z}$. Define the element $\alpha \in k = \mathbb{Q}(\sqrt{4 - 3^{6u+3}})$ by

$$\alpha := \frac{3^{u+1}(3^{2u+1} - 2) + \sqrt{4 - 3^{6u+3}}}{2}.$$

Then we have

$$N_k(\alpha) = (3^{2u+1} - 1)^3 \text{ and } \mathrm{Tr}_k(\alpha) = 3^{u+1}(3^{2u+1} - 2).$$

Let us show that

$$f_\alpha(X) = X^3 - 3(3^{2u+1} - 1)X - 3^{u+1}(3^{2u+1} - 2)$$

https://doi.org/10.1017/S0017089510000431 Published online by Cambridge University Press

is irreducible over $\mathbb{Q}$. In the case $u = 1$, we can verify that

$$f_\alpha(X) = X^3 - 3(3^{2+1} - 1)X - 3^{1+1}(3^{2+1} - 2) = X^3 - 78X - 225$$

is irreducible over $\mathbb{Q}$. Assume now that $u \geq 2$ and that $\alpha \in k^3$. Then we can express

$$\alpha = \left(\frac{s + t\sqrt{D}}{2}\right)^3$$

for some $s,\ t \in \mathbb{Z}$, where $D$ is the square-free part of $4 - 3^{6u+3}$. Since

$$\left(\frac{s + t\sqrt{D}}{2}\right)^3 = \frac{s(s^2 + 3t^2D)/4 + t(3s^2 + t^2D)/4 \cdot \sqrt{D}}{2},$$

we have

$$4 \cdot 3^{u+1}(3^{2u+1} - 2) = s(s^2 + 3t^2D), \tag{2.1}$$

and hence $s$ is divisible by 3. On the other hand, since the norm of $(s + t\sqrt{D})/2$ is equal to $3^{2u+1} - 1$, we have

$$t^2D = s^2 - 4(3^{2u+1} - 1), \tag{2.2}$$

and hence $t^2D$ is not divisible by 3. Therefore we get

$$v_3(s^2 + 3t^2D) = 1. \tag{2.3}$$

From (2.1) and (2.3), we have $3^u \mid s$, and hence we can express

$$s = 3^u a \tag{2.4}$$

for some $a \in \mathbb{Z}$. Substituting (2.2) and (2.4) into (2.1), it follows that

$$\begin{aligned} 4 \cdot 3^{u+1}(3^{2u+1} - 2) &= s(s^2 + 3(s^2 - 4(3^{2u+1} - 1))) \\ &= 4s(s^2 - 3^{2u+2} + 3) \\ &= 4 \cdot 3^{u+1}a(3^{2u-1}(a^2 - 9) + 1), \end{aligned}$$

and so

$$3^{2u+1} - 2 = a(3^{2u-1}(a^2 - 9) + 1). \tag{2.5}$$

If $a \leq -3$, then

$$a(3^{2u-1}(a^2 - 9) + 1) \leq 0 < 3^{2u+1} - 2.$$

This is a contradiction. If $a \geq 4$, then

$$a(3^{2u-1}(a^2 - 9) + 1) \geq 4(3^{2u-1} \cdot 7 + 1) = 28 \cdot 3^{2u-1} + 4 > 3^{2u+1} - 2.$$

This is also a contradiction. Therefore $a$ must be in the range

$$-2 \leq a \leq 3. \tag{2.6}$$

https://doi.org/10.1017/S0017089510000431 Published online by Cambridge University Press

It follows from (2.5) that

$$-2 \equiv a \pmod{3^{2u-1}}.$$

From this together with (2.6) and $u \geq 2$, we have $a = -2$. This contradicts that the left-hand side of (2.5) is odd. Hence $\alpha$ is not a cube in $k$. Therefore, by Proposition 2.1, $f_\alpha$ is irreducible over $\mathbb{Q}$. Since $f_\alpha$ does not satisfy the conditions (LN-i), (LN-ii) and (LN-iii), the splitting field of $f_\alpha$ over $\mathbb{Q}$ is an unramified cyclic cubic extension of $k'$. The proof is completed. □

*Proof of Theorem* 3. We keep the notation and situation from the proof of Theorem 2. Then the 3-rank of the ideal class group of $k'$ is at least 1. By Proposition 1.1, therefore, it is sufficient to show that there is a cubic field $K$ with $disc(K) = -3^3 D$.

Now define the element $\alpha \in k$ by

$$\alpha := 2 + \sqrt{4 - 3^{6u+3}}.$$

It follows from

$$N_k(\alpha) = (3^{2u+1})^3 \text{ and } \mathrm{Tr}_k(\alpha) = 4$$

that we have

$$f_\alpha(X) = X^3 - 3^{2u+2}X - 4.$$

Let $\theta$ be a root of $f_\alpha(X) = 0$, and put $K = \mathbb{Q}(\theta)$. Since

$$f_\alpha(X+1) = X^3 + 3X^2 - 3(3^{2u+1} - 1)X - 3(3^{2u+1} + 1),$$

we see by Eisenstein's criterion for the prime 3 that $f_\alpha$ is irreducible over $\mathbb{Q}$. Then by the last half of Proposition 2.1, the splitting field of $f_\alpha$ over $\mathbb{Q}$ is a cyclic cubic extension of $k'$ unramified outside 3. We can easily check that the condition (LN-ii) holds. Then 3 is totally ramified in $K$ and so $v_3(D_K) = 3$ by Proposition 2.1. Hence we have $D_K = -3^3 D$. By Proposition 1.1 and Theorem 2, therefore, the 3-rank of the ideal class group of $k$ is at least 2. The proof is completed. □

**3. Numerical examples.** In Table 1, we list the square-free part of $4 - 3^n$, the structure of the ideal class group of $k = \mathbb{Q}(\sqrt{4 - 3^n})$ and the class number of $k' = \mathbb{Q}(\sqrt{-3(4 - 3^n)})$ for $3 \leq n \leq 49$ with $n \equiv 1 \pmod 2$. In Table 2, we list the structure of the ideal class group of $k = \mathbb{Q}(\sqrt{4 - 3^n})$ for $50 \leq n \leq 100$ with $n \equiv 3 \pmod 6$. Here we denote an abelian group $C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$ by $[n_1, n_2, \ldots, n_r]$.

REMARK 3.1. We use computer manipulations with GP/PARI (Version 2.1.7). From these tables, we can see that for an integer $n$ in the range $9 \leq n \leq 100$ with $n \equiv 3 \pmod 6$, the ideal class group of $k$ has a subgroup isomorphic to $C_{3n} \times C_3$ (thus, in particular, $C_9 \times C_3$). However, the author has not yet proved this.

https://doi.org/10.1017/S0017089510000431 Published online by Cambridge University Press

**Table 1.**

| $n$ | Square-free part of $4-3^n$ | The structure of the ideal class group of $\mathbb{Q}(\sqrt{4-3^n})$ | The class number of $\mathbb{Q}(\sqrt{-3(4-3^n)})$ |
|---|---|---|---|
| 3 | −23 | [3] | 1 |
| 5 | −239 | [15] | 1 |
| 7 | −2183 | [42] | 6 |
| 9 | −19679 | [54, 3] | 6 |
| 11 | −177143 | [264] | 16 |
| 13 | −1594319 | [1872] | 64 |
| 15 | −14348903 | [270, 15] | 150 |
| 17 | −129140159 | [9690] | 230 |
| 19 | −1162261463 | [31350] | 1818 |
| 21 | −10460353199 | [12663, 3, 3] | 1665 |
| 23 | −94143178823 | [159942] | 7154 |
| 25 | −1601679791 | [60300] | 804 |
| 27 | −7625597484983 | [310554, 6] | 74892 |
| 29 | −68630377364879 | [4315722, 2] | 82596 |
| 31 | −617673396283943 | [32074677] | 660543 |
| 33 | −5559060566555519 | [29688714, 3] | 1050978 |
| 35 | −50031545098999703 | [52523730, 3] | 3287202 |
| 37 | −450283905890997359 | [1018421115] | 12171397 |
| 39 | −4052555153018976263 | [123043050, 3, 3] | 34215606 |
| 41 | −36472996377170786399 | [5322108033] | 47957583 |
| 43 | −328256967394537077623 | [7736038668, 2] | 373576936 |
| 45 | −2954312706550833698639 | [505223730, 18, 2, 2, 2] | 533315808 |
| 47 | −26588814358957503287783 | [21629637726, 2, 2] | 1818043912 |
| 49 | −239299329230617529590079 | [153033164592, 6] | 5545046352 |

**Table 2.**

| $n$ | The structure of the ideal class group of $\mathbb{Q}(\sqrt{4-3^n})$ |
|---|---|
| 51 | [227163157560, 6] |
| 57 | [57240211680, 18, 6, 6] |
| 63 | [42265762274736, 18] |
| 69 | [920661234127056, 6, 6] |
| 75 | [8038002712163535 0, 3, 3] |
| 81 | [2144525716486877706, 6, 2] |
| 87 | [3749039648797628651 4, 6, 2] |
| 93 | [40636390819760016643 8, 6, 6] |
| 99 | [1688615182716284910859 2, 18] |

ACKNOWLEDGEMENT. The author is grateful to the referee for his/her careful reading and for many comments on this paper.

https://doi.org/10.1017/S0017089510000431 Published online by Cambridge University Press

## REFERENCES

**1.** C. Erickson, N. Kaplan, N. Mendoza, A. M. Pacelli and T. Shayler, Parameterized families of quadratic number fields with 3-rank at least 2, *Acta Arith.* **130** (2007), 141–147.

**2.** H. Hasse, Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage, *Math. Z.* **31** (1930), 565–582.

**3.** Y. Kishi, A criterion for a certain type of imaginary quadratic fields to have 3-ranks of the ideal class groups greater than one, *Proc. Japan Acad. Ser.* A *Math. Sci.* **74** (1998), 93–97.

**4.** Y. Kishi, A constructive approach to Spiegelung relations between 3-ranks of absolute ideal class groups and congruent ones modulo $(3)^2$ in quadratic fields, *J. Number Theory* **83** (2000), 1–49.

**5.** Y. Kishi, Note on the divisibility of the class number of certain imaginary quadratic fields, *Glasgow Math. J.* **51** (2009), 187–191.

**6.** Y. Kishi and K. Miyake, Parametrization of the quadratic fields whose class numbers are divisible by three, *J. Number Theory* **80** (2000), 209–217.

**7.** P. Llorente and E. Nart, Effective determination of the decomposition of the rational primes in a cubic field, *Proc. Amer. Math. Soc.* **87** (1983), 579–585.

**8.** A. Scholz, Über die Beziehung der Klassenzahl quadratischer Körper zueinander, *J. Reine Angew. Math.* **166** (1932), 201–203.

**9.** Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.* **7** (1970), 57–76.

https://doi.org/10.1017/S0017089510000431 Published online by Cambridge University Press