



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



# Imaginary quadratic fields whose ideal class groups have 3-rank at least three

Yasuhiro Kishi<sup>a,\*</sup>, Toru Komatsu<sup>b</sup><sup>a</sup> Department of Mathematics, Aichi University of Education, Aichi, 448-8542, Japan<sup>b</sup> Department of Mathematics, Tokyo University of Science, Chiba, 278-8510, Japan

## ARTICLE INFO

*Article history:*

Received 24 March 2016

Accepted 18 June 2016

Available online 2 August 2016

Communicated by David Goss

*MSC:*

11R11

11R29

*Keywords:*

Quadratic fields

Ideal class groups

## ABSTRACT

In this paper, we prove that the 3-rank of the ideal class group of the imaginary quadratic field  $\mathbb{Q}(\sqrt{4 - 3^{18n+3}})$  is at least 3 for every positive integer  $n$ .

© 2016 Elsevier Inc. All rights reserved.

## 1. Introduction

In 1973, Craig [1] proved that there exist infinitely many imaginary quadratic fields whose ideal class groups have 3-rank at least 3. After that Craig himself extended such lower bound replaced by 4 ([2]). However, less is known about a parametric family of such fields with high rank. On the other hand, one of the author showed in [6] that the 3-rank of the ideal class group of imaginary quadratic field  $\mathbb{Q}(\sqrt{4 - 3^{6n+3}})$  is at least 2

\* Corresponding author.

E-mail addresses: [ykishi@aeu.ac.jp](mailto:ykishi@aeu.ac.jp) (Y. Kishi), [komatsu\\_toru@ma.noda.tus.ac.jp](mailto:komatsu_toru@ma.noda.tus.ac.jp) (T. Komatsu).

for any positive integer  $n$ . The goal of the present paper is to prove that the lower bound of 3-rank for such fields can be replaced by 3 when  $n$  is divisible by 3, that is,

**Theorem 1.** *Let  $n$  be a positive integer. Then the 3-rank of the ideal class group of  $\mathbb{Q}(\sqrt{4-3^{18n+3}})$  is at least 3.*

## 2. Proof of Theorem 1

For a positive integer  $n$  we consider two quadratic fields

$$k := \mathbb{Q}(\sqrt{4-3^{18n+3}}) \quad \text{and} \quad k' := \mathbb{Q}(\sqrt{-3(4-3^{18n+3})}).$$

Denote the 3-rank of the ideal class group of  $k$  (resp.  $k'$ ) by  $r$  (resp.  $s$ ). Then it holds that  $r = s + 1$  (cf. [6, Theorem 3]). Therefore it is sufficient to show that  $s \geq 2$ .

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

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

where  $N_k$  and  $\text{Tr}_k$  denote the norm map and the trace map of  $k/\mathbb{Q}$ , respectively.

The following proposition, which combined [4, Lemma 1], [5, Proposition 6.5], [9, Theorem 1] (see Proposition 2.2) and [8, Lemma 3.2], is one of the main ingredients in the proof of our theorem.

**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  $\alpha$  and  $\beta$  be integers in  $k^\times$  whose norms are cubic in  $\mathbb{Z}$ . Then we have*

- (1) *The polynomial  $f_\alpha$  is reducible over  $\mathbb{Q}$  if and only if  $\alpha$  is cubic in  $k$ .*
- (2) *If  $f_\alpha$  is irreducible over  $\mathbb{Q}$ , then the splitting field  $E_\alpha$  of  $f_\alpha$  over  $\mathbb{Q}$  is a cyclic cubic extension of  $k'$  unramified outside  $S$  and  $E_\alpha$  has a cubic subfield  $K$  with  $v_3(D_K) \neq 5$ , where  $S$  is the set of all the prime divisors of  $3 \gcd(N_k(\alpha), \text{Tr}_k(\alpha))$  and  $D_K$  is the discriminant of  $K$ .*
- (3) *The splitting fields of  $f_\alpha$  and  $f_\beta$  over  $\mathbb{Q}$  are distinct if and only if neither  $\alpha\beta$  nor  $\bar{\alpha}\beta$  is cubic in  $k$ , where  $\bar{\alpha}$  is the conjugate of  $\alpha$  in  $k$ .*

Next we extract some results from Llorente and Nart [9, Theorem 1].

**Proposition 2.2.** *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  $v_p(a) < 2$  or  $v_p(b) < 3$  holds for every prime  $p$ . Let  $\theta$  be a root of  $F(X)$ , and put  $K = \mathbb{Q}(\theta)$ . Then we have*

- (1) The prime  $p \neq 3$  is totally ramified in  $K/\mathbb{Q}$  if and only if  $1 \leq v_p(b) \leq v_p(a)$ .  
 (2) The prime 3 is totally ramified in  $K/\mathbb{Q}$  if and only if one of the following conditions holds:

$$(\text{LN-i}) \quad 1 \leq v_3(b) \leq v_3(a);$$

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

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

**Proof of Theorem 1.** Define the elements  $\alpha, \beta \in k = \mathbb{Q}(\sqrt{4 - 3^{18n+3}})$  by

$$\alpha := \frac{3^{3n+1}(3^{6n+1} - 2) + \sqrt{4 - 3^{18n+3}}}{2},$$

$$\beta := \frac{(3^{10n+2} - 2 \cdot 3^{6n+1} + 2 \cdot 3^{4n+1} + 2 \cdot 3^{2n+1} + 2) + 3^n(2 \cdot 3^{2n} + 3)\sqrt{4 - 3^{18n+3}}}{2},$$

respectively. Then we have

$$N_k(\alpha) = (3^{6n+1} - 1)^3,$$

$$\text{Tr}_k(\alpha) = 3^{3n+1}(3^{6n+1} - 2),$$

$$N_k(\beta) = (3^{8n+1} + 3^{6n+1} - 3^{2n} + 1)^3,$$

$$\text{Tr}_k(\beta) = 3^{10n+2} - 2 \cdot 3^{6n+1} + 2 \cdot 3^{4n+1} + 2 \cdot 3^{2n+1} + 2,$$

and so

$$f_\alpha(X) = X^3 - 3(3^{6n+1} - 1)X - 3^{3n+1}(3^{6n+1} - 2),$$

$$f_\beta(X) = X^3 - 3(3^{8n+1} + 3^{6n+1} - 3^{2n} + 1)X \\ - (3^{10n+2} - 2 \cdot 3^{6n+1} + 2 \cdot 3^{4n+1} + 2 \cdot 3^{2n+1} + 2).$$

We showed in [6] that the polynomial  $f_\alpha$  is irreducible over  $\mathbb{Q}$  and the splitting field  $E_\alpha$  of  $f_\alpha$  over  $\mathbb{Q}$  is an unramified cyclic cubic extension of  $k'$ . We will guarantee the irreducibility of  $f_\beta$  at the next section. By putting  $t = 3^n$ , one has  $\text{Tr}_k(\beta) = 9t^{10} - 6t^6 + 6t^4 + 6t^2 + 2$  and  $N_k(\beta) = m^3$ , where  $m = 3t^8 + 3t^6 - t^2 + 1$ . Due to extended Euclidean algorithm as polynomials in  $t$  we have  $\lambda_1 m + \lambda_2 \text{Tr}_k(\beta) = 11^3$ , where

$$\lambda_1 = 486t^8 + 360t^6 - 501t^4 - 195t^2 + 919, \quad \lambda_2 = -162t^6 - 282t^4 - 61t^2 + 206.$$

**Proposition 2.1** shows that the splitting field  $E_\beta$  of  $f_\beta$  over  $\mathbb{Q}$  is an extension of  $k'$  unramified outside 3 and 11. We easily verify that  $f_\beta$  does not satisfy the conditions (LN-i), (LN-ii) and (LN-iii) in **Proposition 2.2** (2). Thus the prime ideal of  $k'$  above 3 does not ramify in  $E_\beta/k'$ . Let  $a_\beta$  and  $b_\beta$  be rational numbers such that  $f_\beta(X) = X^3 - a_\beta X - b_\beta$ . Note that  $3^5 \equiv 1 \pmod{11^2}$ . If  $n \equiv 0, 1, 2, 3, 4 \pmod{5}$ , then  $m \equiv 6, 82, 77, 80, 2$

(mod  $11^2$ ), respectively. Hence  $a_\beta$  is divisible by 11 if and only if  $n \equiv 2 \pmod{5}$ , and then one has  $v_{11}(a_\beta) = 1$ . When  $n \equiv 2 \pmod{5}$ , the integer  $\text{Tr}_k(\beta)$  is divisible by  $11^2$ , that is,  $v_{11}(b_\beta) \geq 2$ . Therefore, Proposition 2.2 (1) verifies that  $E_\beta/k'$  is unramified at every prime ideal above 11. Hence  $E_\beta$  is an unramified cyclic cubic extension of  $k'$ . Proposition 2.1 (1) and (3) mean that  $E_\alpha \neq E_\beta$  if and only if  $f_{\alpha\beta}$  and  $f_{\bar{\alpha}\beta}$  are both irreducible over  $\mathbb{Q}$ . The proof of Theorem 1 is complete provided  $f_\beta$ ,  $f_{\alpha\beta}$  and  $f_{\bar{\alpha}\beta}$  are all irreducible over  $\mathbb{Q}$ .  $\square$

### 3. Irreducibility of the three polynomials

The goal of this section is to prove the following proposition.

#### Proposition 3.1.

- (1) The polynomial  $f_\beta$  is irreducible over  $\mathbb{Q}$ .
- (2) The polynomial  $f_{\alpha\beta}$  is irreducible over  $\mathbb{Q}$ .
- (3) The polynomial  $f_{\bar{\alpha}\beta}$  is irreducible over  $\mathbb{Q}$ .

The polynomial  $f_\beta$  is reducible over  $\mathbb{Q}$  if and only if there exists a solution of  $f_\beta(X) = 0$  in  $\mathbb{Q}$ . We will find all solutions of  $f_\beta(X) = 0$  in  $\mathbb{Q}_3$ , the field of 3-adic numbers, and verify that such solutions do not belong to  $\mathbb{Q}$ . We put  $t = 3^n$  and  $d = 4 - 27t^{18}$ .

**Lemma 3.2.** For  $n \geq 2$ , the polynomial  $f_\beta$  has only one root  $\theta$  in  $\mathbb{Q}_3$ , and it holds that  $\theta \equiv \rho(t) \pmod{3^{14n-4}\mathbb{Z}_3}$ , where  $\rho(T)$  is a polynomial of the form

$$\rho(T) = 2 + \frac{2}{3}T^4 + \frac{10}{9}T^6 + \frac{4}{3}T^8 + \frac{19}{81}T^{10} - \frac{83}{243}T^{12}.$$

Let  $a_\beta$  and  $b_\beta$  be rational numbers such that  $f_\beta(X) = X^3 - a_\beta X - b_\beta$ . Due to Cardano's formula, all of the solutions of  $f_\beta(X) = 0$  can be expressed by  $\theta_i = \zeta^i \sqrt[3]{\xi_1} + \zeta^{-i} \sqrt[3]{\xi_2}$  for  $i = 0, 1, 2$ , where  $\zeta$  is a primitive third root of unity and

$$\begin{aligned} \xi_1 &= \frac{b_\beta}{2} + \sqrt{\left(\frac{b_\beta}{2}\right)^2 - \left(\frac{a_\beta}{3}\right)^3} = \frac{\text{Tr}_k(\beta)}{2} + \sqrt{\left(\frac{\text{Tr}_k(\beta)}{2}\right)^2 - N_k(\beta)} = \beta, \\ \xi_2 &= \frac{b_\beta}{2} - \sqrt{\left(\frac{b_\beta}{2}\right)^2 - \left(\frac{a_\beta}{3}\right)^3} = \frac{\text{Tr}_k(\beta)}{2} - \sqrt{\left(\frac{\text{Tr}_k(\beta)}{2}\right)^2 - N_k(\beta)} = \beta'. \end{aligned}$$

Here  $\beta'$  is the number such that  $\beta + \beta' = b_\beta$  and  $\beta\beta' = (a_\beta/3)^3$ . We denote the solution  $\theta_0$  by  $\theta$ . In this section we utilize Hensel's lemma not only in  $\mathbb{Q}_3$  but also in  $\mathbb{Q}[[T]]$  frequently.

**Lemma 3.3** (Hensel's lemma [3, Theorem 7.3]). Let  $R$  be a ring complete under an additive valuation  $v$ . Let  $F(X) \in R[[X]]$  and  $\eta_0 \in R$ . Put  $w = v(F(\eta_0))$  and  $w' = v(F'(\eta_0))$ ,

where  $F'$  is the derivative of  $F$ . If  $w > 2w'$ , then there exists an  $\eta \in R$  such that  $F(\eta) = 0$  and  $v(\eta - \eta_0) \geq w - w'$ .

Since  $d \equiv 2^2 \pmod{27}$ , Hensel's lemma implies that  $\sqrt{d} \in \mathbb{Q}_3$  and  $\sqrt{d} \equiv \pm 2 \pmod{27}$ . For  $n \geq 2$ , we have  $\beta \equiv \beta' \equiv 1^3 \pmod{27}$ . It follows from Hensel's lemma that  $\sqrt[3]{\beta}, \sqrt[3]{\beta'} \in \mathbb{Q}_3$ . This shows that  $\theta \in \mathbb{Q}_3$ . Because of the binomial coefficient  ${}_{1/3}C_j$  appearing below, it is complicated to approximate values in  $\mathbb{Q}_3$  each time the computation proceeds. To evade such complications, we replace the calculating ring with  $\mathbb{Q}[[T]]$ , the ring of formal power series over  $\mathbb{Q}$ , in lifting  $t$  to  $T$ . After approximating  $\theta$  in  $\mathbb{Q}[[T]]$ , we substitute  $t$  for  $T$  of the approximation and measure its precision by Hensel's lemma. For a number  $z \in \mathbb{Q}_3$  with expression as a formal power series in  $t$  over  $\mathbb{Q}$ , let  $L(z, T) \in \mathbb{Q}[[T]]$  be a lift for  $z$ , that is,  $L(z, t) = z$ . We will find a polynomial  $\rho(T)$  such that  $\rho(T) \equiv L(\theta, T) \pmod{T^{14}}$ . Here the scale of  $T^{14}$  is sufficient to prove [Proposition 3.1](#) (1). Since  $L(d, T) = 4 - 27T^{18} \equiv 2^2 \pmod{T^{14}}$ , we may have  $L(\sqrt{d}, T) \equiv 2 \pmod{T^{14}}$ . Then it satisfies that

$$L(\beta, T) \equiv 1 + 3T + 3T^2 + 2T^3 + 3T^4 - 3T^6 + \frac{9}{2}T^{10} \pmod{T^{14}},$$

$$L(\beta', T) \equiv 1 - 3T + 3T^2 - 2T^3 + 3T^4 - 3T^6 + \frac{9}{2}T^{10} \pmod{T^{14}}.$$

The following lemma is convenient to solve a third root in  $\mathbb{Q}[[T]]$ . Let  $g \in \mathbb{Q}[[T]]$  with  $g \equiv 0 \pmod{T}$ . For a positive integer  $l$ , we define  $B(g)_l \in \mathbb{Q}[[T]]$  of degree less than  $l$  such that

$$B(g)_l \equiv \sum_{j=0}^{l-1} {}_{1/3}C_j g^j \pmod{T^l},$$

where  ${}_{1/3}C_j$  are the binomial coefficients, that is,  ${}_{1/3}C_j = \Gamma(4/3)/(\Gamma(j+1)\Gamma(4/3-j))$  for the Gamma function  $\Gamma$ .

**Lemma 3.4** ([7, Chap. IV.1]). *The sequence  $\{B(g)_l\}$  converges in  $\mathbb{Q}[[T]]$ , and the limit  $B(g) = \lim_{l \rightarrow \infty} B(g)_l$  satisfies that  $B(g)^3 = 1 + g$  and  $B(g) \equiv B(g)_l \pmod{T^l}$  for every  $l$ .*

The following finite sequence  $\{H_j\}$  is a practical tool to calculate  $B(g)_l$ . Fix a positive integer  $l$ . We define polynomials  $H_1, H_2, \dots, H_l$  of degree less than  $l$  by the initial term  $H_1 = 1$  and the recurrence relation  $H_j \equiv 1 + {}_{1/3}D_{l-j}gH_{j-1} \pmod{T^l}$  for  $2 \leq j \leq l$ , where  ${}_{1/3}D_{l-j} = {}_{1/3}C_{l-j+1}/{}_{1/3}C_{l-j} = (1/3 - l + j)/(l - j + 1)$ .

**Lemma 3.5.** *We have  $H_l = B(g)_l$ .*

**Proof.** By the definition of  $H_j$ , the term  $H_l$  is congruent to

$$1 + \frac{{}_{1/3}C_1}{{}_{1/3}C_0} g H_{l-1} \equiv 1 + \frac{{}_{1/3}C_1}{{}_{1/3}C_0} g \left( 1 + \frac{{}_{1/3}C_2}{{}_{1/3}C_1} g (\cdots (1 + \frac{{}_{1/3}C_{l-1}}{{}_{1/3}C_{l-2}} g H_1) \cdots) \right) \pmod{T^l},$$

which agrees with the definition of  $B(g)_l$ .  $\square$

**Remark 3.6.** The sequence  $\{H_j\}_{j=1}^l$  is different from  $\{B(g)_j\}_{j=1}^l$  when  $g \not\equiv 0 \pmod{T^l}$  and  $l \geq 3$ . Indeed, one has  $H_2 \equiv 1 + {}_{1/3}D_{l-2}g \not\equiv 1 + {}_{1/3}C_1g \equiv B(g)_2 \pmod{T^l}$  for  ${}_{1/3}D_{l-2} = (1/3 - l + 2)/(l - 1) \neq 1/3 = {}_{1/3}C_1$ .

By Lemma 3.5, one computes that

$$\begin{aligned} B(L(\beta, T) - 1)_{14} &= 1 + T + \frac{1}{3}T^3 + \frac{1}{3}T^4 - T^5 + \frac{5}{9}T^6 - \frac{4}{9}T^7 + \frac{2}{3}T^8 - \frac{4}{81}T^9 \\ &\quad + \frac{19}{162}T^{10} - \frac{2}{9}T^{11} - \frac{83}{486}T^{12} + \frac{107}{243}T^{13}, \\ B(L(\beta', T) - 1)_{14} &= 1 - T - \frac{1}{3}T^3 + \frac{1}{3}T^4 + T^5 + \frac{5}{9}T^6 + \frac{4}{9}T^7 + \frac{2}{3}T^8 + \frac{4}{81}T^9 \\ &\quad + \frac{19}{162}T^{10} + \frac{2}{9}T^{11} - \frac{83}{486}T^{12} - \frac{107}{243}T^{13}. \end{aligned}$$

Thus we have

$$\begin{aligned} L(\theta, T) &= L(\sqrt[3]{\beta}, T) + L(\sqrt[3]{\beta'}, T) \\ &= B(L(\beta, T) - 1) + B(L(\beta', T) - 1) \equiv \rho(T) \pmod{T^{14}}, \end{aligned}$$

where

$$\rho(T) = 2 + \frac{2}{3}T^4 + \frac{10}{9}T^6 + \frac{4}{3}T^8 + \frac{19}{81}T^{10} - \frac{83}{243}T^{12}.$$

**Proof of Lemma 3.2.** The number  $\theta = \theta_0$  is a root of  $f_\beta$  in  $\mathbb{Q}_3$ . It follows from  $\theta_0 + \theta_1 + \theta_2 = 0$  that  $\theta_1 \in \mathbb{Q}_3$  if and only if  $\theta_2 \in \mathbb{Q}_3$ . The discriminant  $\text{disc}(f_\beta)$  of  $f_\beta$  satisfies that  $v_3(\text{disc}(f_\beta)) = 2n + 5 \equiv 1 \pmod{2}$ . This means that  $\mathbb{Q}_3(\theta_0, \theta_1, \theta_2)$  has a ramified quadratic field and  $\theta_1, \theta_2 \notin \mathbb{Q}_3$ . Thus  $\theta$  is only one root of  $f_\beta$  over  $\mathbb{Q}_3$ . Let us measure the distance between  $\theta$  and  $\rho(t)$  in  $\mathbb{Q}_3$ . The direct computation yields that

$$\begin{aligned} f_\beta(\rho(t)) &= -17t^{14}/3^2 + 97t^{16}/3^4 + \cdots - 571787t^{36}/3^{15} \\ &\equiv -17 \cdot 3^{14n-2} \pmod{3^{16n-4}\mathbb{Z}} \end{aligned}$$

for  $n \geq 2$ . This shows that  $v_3(f_\beta(\rho(t))) = 14n - 2$ . On the other hand, one has  $f'_\beta(\rho(t)) \equiv 3 \cdot 2^2 - 3 \equiv 9 \pmod{27}$  and  $v_3(f'_\beta(\rho(t))) = 2$ . Hensel's lemma implies that  $\theta \equiv \rho(t) \pmod{3^{14n-4}}$ .  $\square$

**Proof of Proposition 3.1 (1).** Assume  $n \geq 2$ . By Lemma 3.2, there exists a 3-adic integer  $\delta$  such that  $\theta = \rho(t) + 3^{14n-4}\delta$ . It follows from  $f_\beta(\rho(t)) \neq 0$  that  $\delta \neq 0$ . Now suppose that  $f_\beta$  is reducible over  $\mathbb{Q}$ . Then  $\theta$  belongs to  $\mathbb{Z}$ , and so does  $3^{14n-4}\delta$  for  $\rho(t) \in \mathbb{Z}$ . By  $\delta \in \mathbb{Z}_3$ , we have  $\delta \in \mathbb{Z}$ . It is well-known that every root of  $f_\beta$  in  $\mathbb{Q}$  is an integer dividing the constant term  $-b_\beta$  of  $f_\beta$ . In particular,  $|\theta|$  is not greater than  $|b_\beta|$ , where  $|\cdot|$  is the absolute value in  $\mathbb{R}$ . However, it holds that

$$\begin{aligned} |\theta| - |b_\beta| &\geq \frac{|\delta|}{81}t^{14} - |\rho(t)| - |b_\beta| \\ &> \frac{1}{81}t^{14} - \frac{83}{243}t^{12} - 10(t^{10} + t^8 + t^6 + t^4 + t^2 + 1) \\ &> \frac{1}{81}t^{14} - t^{12} = \frac{t^{12}(t+9)(t-9)}{81} \geq 0 \end{aligned}$$

for  $t \geq 9$ . This is a contradiction. Hence  $f_\beta$  is irreducible over  $\mathbb{Q}$  if  $n \geq 2$ . For  $n = 1$ , we have  $f_\beta(X) \equiv X^3 - X - 4 \pmod{13}$ , which is irreducible over  $\mathbb{F}_{13}$ . Therefore  $f_\beta$  is irreducible over  $\mathbb{Q}$  for every  $n \geq 1$ .  $\square$

Let us analyze the second  $f_{\alpha\beta}$ . For

$$\begin{aligned} \alpha\beta &= (-t(27t^{20} + 27t^{14} - 27t^{10} - 27t^8 + 18t^6 + 18t^4 + 2t^2 - 6) \\ &\quad + (9t^{12} + 18t^{10} - 9t^6 - 6t^4 + 3t^2 + 1)\sqrt{4 - 27t^{18}})/2 \end{aligned}$$

and  $N_k(\alpha\beta) = (3t^6 - 1)^3(3t^8 + 3t^6 - t^2 + 1)^3$ , we have

$$\begin{aligned} f_{\alpha\beta}(X) &= X^3 - 3(3t^6 - 1)(3t^8 + 3t^6 - t^2 + 1)X \\ &\quad + t(27t^{20} + 27t^{14} - 27t^{10} - 27t^8 + 18t^6 + 18t^4 + 2t^2 - 6) \\ &= X^3 - a_{\alpha\beta}X - b_{\alpha\beta}. \end{aligned}$$

**Lemma 3.7.** For  $n \geq 2$  the polynomial  $f_{\alpha\beta}(X)$  has only one root  $\theta$  in  $\mathbb{Q}_3$ , and it holds that  $\theta \equiv \rho(t) \pmod{3^{25n-10}\mathbb{Z}_3}$ , where

$$\begin{aligned} \rho(T) &= 2T - \frac{4}{3}T^3 - 2T^5 - \frac{32}{9}T^7 - \frac{179}{81}T^9 + \frac{2}{9}T^{11} + \frac{184}{243}T^{13} \\ &\quad - \frac{115}{729}T^{15} + \frac{143}{243}T^{17} - \frac{12755}{6561}T^{19} + \frac{23227}{19683}T^{21} + \frac{6752}{6561}T^{23} \in \mathbb{Q}[T]. \end{aligned}$$

**Proof.** Let  $\theta_0, \theta_1, \theta_2$  be the roots of  $f_{\alpha\beta}$  as that of  $f_\beta$ . Then one sees that  $\theta_0 \in \mathbb{Q}_3$ . For  $L(d, T) \equiv (2 - 27T^{18}/4)^2 \pmod{T^{25}}$ , we may have that  $L(\sqrt{d}, T) \equiv 2 - 27T^{18}/4 \pmod{T^{25}}$ . Note that  $\sqrt[3]{-1-g} = -\sqrt[3]{1+g}$ . Computing the lift  $L(\theta_0, T)$  of  $\theta_0$  in the same way as that for  $f_\beta$ , one sees that  $L(\theta_0, T) \equiv \rho(T) \pmod{T^{25}}$ . The direct calculation implies that

$$\begin{aligned} f_{\alpha\beta}(\rho(t)) &= 52636t^{25}/3^9 + 5688712t^{27}/3^{12} - \cdots + 307820331008t^{69}/3^{24} \\ &\equiv 52636 \cdot 3^{25n-9} \pmod{3^{27n-12}} \end{aligned}$$

for  $n \geq 2$ . Thus it holds that  $v_3(f_{\alpha\beta}(\rho(t))) = 25n - 9$ . Since  $f'_{\alpha\beta}(\rho(t)) \equiv 3 \cdot 0^2 + 3 \equiv 3 \pmod{9}$ , one has  $v_3(f'_{\alpha\beta}(\rho(t))) = 1$ . Hensel's lemma shows that  $\theta_0 \equiv \rho(t) \pmod{3^{25n-10}}$ . Since  $v_3(\text{disc}(f_{\alpha\beta})) = 3 \equiv 1 \pmod{2}$ , there exists at most one root of  $f_{\alpha\beta}$  in  $\mathbb{Q}_3$ . Thus  $f_{\alpha\beta}$  has only one root in  $\mathbb{Q}_3$ .  $\square$

**Proof of Proposition 3.1 (2).** Assume  $n \geq 6$ . Suppose that  $f_{\alpha\beta}$  is reducible over  $\mathbb{Q}$ . In the same way as in the proof for  $f_\beta$ , it follows from Lemma 3.7 that  $\theta = \rho(t) + \delta t^{25} 3^{-10}$  for some  $\delta \in \mathbb{Z}$ . Then it holds that

$$\begin{aligned} |\theta| - |b_{\alpha\beta}| &\geq \frac{|\delta|}{3^{10}} t^{25} - |\rho(t)| - |b_{\alpha\beta}| \\ &> \frac{1}{3^{10}} t^{25} - \frac{6752}{6561} t^{23} - 30(t^{21} + t^{19} + \cdots + t^3 + t) \\ &> \frac{1}{3^{10}} t^{25} - 3^2 t^{23} = \frac{t^{23}(t + 3^6)(t - 3^6)}{3^{10}} \geq 0 \end{aligned}$$

for  $t \geq 3^6$ . This is contrary to the fact that  $|\theta| \leq |b_{\alpha\beta}|$ . Hence  $f_{\alpha\beta}$  is irreducible over  $\mathbb{Q}$  for  $n \geq 6$ . When  $n = 1, 2, 3, 4, 5$ , the polynomials  $f_{\alpha\beta}(X)$  are congruent to  $X^3 - 2X - 3 \pmod{13}$ ,  $X^3 - X - 2 \pmod{5}$ ,  $X^3 - 10X - 7 \pmod{13}$ ,  $X^3 - X - 3 \pmod{5}$ ,  $X^3 - 3X - 1 \pmod{11}$ , respectively. Since they are irreducible over such finite fields, and so are over  $\mathbb{Q}$ . Therefore  $f_{\alpha\beta}$  is irreducible over  $\mathbb{Q}$  for any  $n \geq 1$ .  $\square$

Let us study the third  $f_{\overline{\alpha}\beta}$ . For

$$\begin{aligned} \overline{\alpha}\beta &= (t(27t^{20} + 81t^{18} - 27t^{14} + 27t^{10} + 27t^8 - 18t^6 - 18t^4 - 10t^2 - 6) \\ &\quad + (9t^{12} + 9t^{10} - 3t^6 - 12t^4 - 3t^2 - 1)\sqrt{4 - 27t^{18}})/2 \end{aligned}$$

and  $N_k(\overline{\alpha}\beta) = (3t^6 - 1)^3(3t^8 + 3t^6 - t^2 + 1)^3$ , we have

$$\begin{aligned} f_{\overline{\alpha}\beta}(X) &= X^3 - 3(3t^6 - 1)^3(3t^8 + 3t^6 - t^2 + 1)X \\ &\quad - t(27t^{20} + 81t^{18} - 27t^{14} + 27t^{10} + 27t^8 - 18t^6 - 18t^4 - 10t^2 - 6) \\ &= X^3 - a_{\overline{\alpha}\beta}X - b_{\overline{\alpha}\beta}. \end{aligned}$$

**Lemma 3.8.** For  $n \geq 2$  the polynomial  $f_{\overline{\alpha}\beta}(X)$  has only one root  $\theta$  in  $\mathbb{Q}_3$ , and it holds that  $\theta \equiv \rho(t) \pmod{3^{25n-10}\mathbb{Z}_3}$ , where

$$\begin{aligned} \rho(T) &= -2T - \frac{8}{3}T^3 + 2T^5 + \frac{20}{9}T^7 - \frac{55}{81}T^9 - \frac{26}{9}T^{11} - \frac{352}{243}T^{13} \\ &\quad + \frac{829}{729}T^{15} - \frac{353}{243}T^{17} + \frac{16364}{6561}T^{19} + \frac{20606}{19683}T^{21} + \frac{601}{6561}T^{23} \in \mathbb{Q}[T]. \end{aligned}$$



**Proof.** Computing  $L(\theta_0, T)$  of  $\theta_0 \in \mathbb{Q}_3$  for  $f_{\bar{\alpha}\beta}$  in the same way as for  $f_{\alpha\beta}$ , we have  $L(\theta_0, T) \equiv \rho(T) \pmod{T^{25}}$ . The direct computation yields that

$$\begin{aligned} f_{\bar{\alpha}\beta}(\rho(t)) &= -23497t^{25}/3^9 - 895510t^{27}/3^{12} + \cdots + 217081801t^{69}/3^{24} \\ &\equiv -23497 \cdot 3^{25n-9} \pmod{3^{27n-12}} \end{aligned}$$

for  $n \geq 2$ . One has  $f'_{\bar{\alpha}\beta}(\rho(t)) \equiv 3 \pmod{9}$ . By  $v_3(f_{\bar{\alpha}\beta}(\rho(t))) = 25n - 9$  and  $v_3(f'_{\bar{\alpha}\beta}(\rho(t))) = 1$ , Hensel's lemma implies that  $\theta \equiv \rho(t) \pmod{3^{25n-10}}$ . It follows from  $v_3(\text{disc}(f_{\bar{\alpha}\beta})) = 3 \equiv 1 \pmod{2}$  that  $f_{\alpha\beta}$  has only one root  $\theta_0$  in  $\mathbb{Q}_3$ .  $\square$

**Proof of Proposition 3.1 (3).** Assume  $n \geq 4$ . Suppose that  $f_{\bar{\alpha}\beta}$  is reducible over  $\mathbb{Q}$ . In the same way as in the proof for  $f_{\alpha\beta}$ , by Lemma 3.8 we have  $\theta = \rho(t) + \delta t^{25}3^{-10}$  for some  $\delta \in \mathbb{Z}$ . Then it holds that

$$\begin{aligned} |\theta| - |b_{\bar{\alpha}\beta}| &\geq \frac{|\delta|}{3^{10}} t^{25} - |\rho(t)| - |b_{\bar{\alpha}\beta}| \\ &> \frac{1}{3^{10}} t^{25} - \frac{601}{6561} t^{23} - 84(t^{21} + t^{19} + \cdots + t^3 + t) \\ &> \frac{1}{3^{10}} t^{25} - \frac{1}{3^2} t^{23} = \frac{t^{23}(t + 3^4)(t - 3^4)}{3^{10}} \geq 0 \end{aligned}$$

for  $t \geq 3^4$ . This conflicts with the fact that  $|\theta| \leq |b_{\bar{\alpha}\beta}|$ . Hence  $f_{\bar{\alpha}\beta}$  is irreducible over  $\mathbb{Q}$  provided  $n \geq 4$ . For  $n = 1, 2, 3$ , the polynomials  $f_{\bar{\alpha}\beta}(X)$  are congruent to  $X^3 - 26X - 19 \pmod{31}$ ,  $X^3 - X - 2 \pmod{5}$ ,  $X^3 - 5X - 6 \pmod{11}$ , respectively. Since they are irreducible over such finite fields, and so are over  $\mathbb{Q}$ . Therefore  $f_{\bar{\alpha}\beta}$  is irreducible over  $\mathbb{Q}$  for arbitrary  $n \geq 1$ .  $\square$

## References

- [1] M. Craig, A type of class group for imaginary quadratic fields, *Acta Arith.* 22 (1973) 449–459.
- [2] M. Craig, A construction for irregular discriminants, *Osaka J. Math.* 14 (1977) 365–402.
- [3] D. Eisenbud, *Commutative Algebra, With a View Toward Algebraic Geometry*, Grad. Texts in Math., vol. 150, Springer-Verlag, New York, 1995.
- [4] 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.
- [5] 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.
- [6] Y. Kishi, On the ideal class group of certain quadratic fields, *Glasg. Math. J.* 52 (2010) 575–581.
- [7] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*, second edition, Grad. Texts in Math., vol. 58, Springer-Verlag, New York, 1984.
- [8] T. Komatsu, On unramified cyclic cubic extensions of real quadratic fields, *Jpn. J. Math.* 27 (2001) 353–386.
- [9] P. Llorente, E. Nart, Effective determination of the decomposition of the rational primes in a cubic field, *Proc. Amer. Math. Soc.* 87 (1983) 579–585.