Journal of Number Theory 170 (2017) 46–54

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 [a,*], Toru Komatsu [b]

[a] *Department of Mathematics, Aichi University of Education, Aichi, 448-8542, Japan*

[b] *Department of Mathematics, Tokyo University of Science, Chiba, 278-8510, Japan*

A R T I C L E   I N F O

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

A B S T R A C T

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.

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@auecc.aichi-edu.ac.jp (Y. Kishi), komatsu_toru@ma.noda.tus.ac.jp (T. Komatsu).

http://dx.doi.org/10.1016/j.jnt.2016.06.019
0022-314X/

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

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

where N_k and 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 α and β be integers in $k^\times$ whose norms are cubic in $\mathbb{Z}$. Then we have*

(1) *The polynomial f_α is reducible over $\mathbb{Q}$ if and only if α is cubic in k.*
(2) *If f_α is irreducible over $\mathbb{Q}$, then the splitting field E_α of f_α over $\mathbb{Q}$ is a cyclic cubic extension of k' unramified outside S and E_α has a cubic subfield K with $v_3(D_K) \neq 5$, where S is the set of all the prime divisors of $3\gcd(N_k(\alpha), \mathrm{Tr}_k(\alpha))$ and D_K is the discriminant of K.*
(3) *The splitting fields of f_α and f_β over $\mathbb{Q}$ are distinct if and only if neither $\alpha\beta$ nor $\overline{\alpha}\beta$ is cubic in k, where $\overline{\alpha}$ is the conjugate of α 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 θ be a root of $F(X)$, and put $K = \mathbb{Q}(\theta)$. Then we have