Publ. Math. Debrecen
81/3-4 (2012), 447–452
DOI: 10.5486/PMD.2012.5323

Imaginary cyclic fields of degree $p-1$ whose ideal class groups have p-rank at least two

By YASUHIRO KISHI (Aichi)

Dedicated to Professors Kálmán Győry and András Sárközy on the occasion of their 70th birthdays and to Professors Attila Pethő and János Pintz on the occasion of their 60th birthdays

Abstract. Let p be a prime number which is congruent to 3 modulo 4. For an odd positive integer n, we define a quadratic field $k_{p,n}$ by $k_{p,n} := \mathbb{Q}(\sqrt{4-p^{pn}}\,)$. Moreover let $M_{p,n}$ be the composite field of $k_{p,n}$ and the maximal real subfield of the pth cyclotomic field. Then $M_{p,n}$ is an imaginary cyclic fields of degree $p-1$. In this paper, we prove that the p-rank of ideal class groups of $M_{p,n}$ is at least 2 for any odd integer $n \geq 1$ except for $(p,n) = (3,1)$. Furthermore, we can show $M_{p,n} \neq M_{p,m}$ for any distinct two integers n and m. As a consequence, we see that there exist infinitely many imaginary cyclic field of degree $p-1$ whose ideal class group have p-rank at least 2.

1. Introduction

According to D. A. Buell's calculations [1], as for about 95% of the imaginary quadratic fields $\mathbb{Q}(\sqrt{D}\,)$ (D : fund. disc., $-4000000 < D < 0$) the ideal class group (ignore 2-part) is cyclic. So it is interesting to produce infinitely many algebraic number fields whose ideal class groups are not cyclic.

Recently, the author proved the following:

Theorem 1 ([7, Theorem 3]). *The* 3*-rank of ideal class group of imaginary quadratic field* $\mathbb{Q}(\sqrt{4-3^{3n}}\,)$ *is at least* 2 *for any odd integer* $n \geq 3$.

Mathematics Subject Classification: Primary: 11R29, 11R20; Secondary: 11D61.
Key words and phrases: ideal class group, imaginary cyclic field.

The goal of this paper is to extend this to general prime p with $p \equiv 3 \pmod 4$.

Let p be a prime with $p \equiv 3 \pmod 4$ and n odd positive integer. We define two quadratic fields $k_{p,n}$ and $k'_{p,n}$ by

$$k_{p,n} := \mathbb{Q}(\sqrt{4 - p^{pn}}\,),$$
$$k'_{p,n} := \mathbb{Q}(\sqrt{-p(4 - p^{pn})}\,) = \mathbb{Q}(\sqrt{p^{pn+1} - 4p}).$$

Let ζ be a primitive pth root of unity and put $\omega := \zeta + \zeta^{-1}$. Moreover we denote the composite field $k_{p,n}$ and $\mathbb{Q}(\omega)$ by $M_{p,n}$:

$$M_{p,n} := k_{p,n} \cdot \mathbb{Q}(\omega).$$

Then $M_{p,n}$ is an imaginary cyclic field of degree $p-1$. The following is the main theorem of this paper.

Theorem 2. *Under the above notation, the p-rank of ideal class group of $M_{p,n}$ is at least 2 for any odd integer $n \geq 1$ except for $(p, n) = (3, 1)$.*

Furthermore, we will show the following:

Proposition 1.1. *For odd positive integers n and m,*

$$n \neq m \iff M_{p,n} \neq M_{p,m}.$$

From this proposition and Theorem 2, we immediately have

Theorem 3. *For any $p \equiv 3 \pmod 4$, there exist infinitely many $M_{n,p}$ with odd $n \geq 1$ such that the p-rank of the ideal class group of $M_{n,p}$ is at least 2.*

Remark 1.2. For the case $p \equiv 1 \pmod 4$, S.-i. Katayama and the author [5] gave an infinite family of imaginary cyclic fields of degree $p-1$ whose ideal class groups have p-rank at least 2.

2. Proof of Proposition 1.1

To prove Proposition 1.1, we need the following proposition which is led from Y. Bugeaud and T. N. Shorey's result [2, Theorem 1].

Proposition 2.1. *For a positive integer D and a prime p, the number of positive integer solutions (x, y) of the equation*

$$Dx^2 + 4 = p^y$$

is at most 1 except for $(p, D) = (5, 1)$.

Let us show Proposition 1.1. If $n = m$, then it is obviously $M_{p,n} = M_{p,m}$. Conversely, we assume $M_{p,n} = M_{p,m}$. Then we easily see $k_{p,n} = k_{p,m}$. Hence there exist integers u and v such that

$$4 - p^{pn} = -du^2 \quad \text{and} \quad 4 - p^{pm} = -dv^2,$$

where d is a square free positive integer. By Proposition 2.1, therefore, we have $n = m$. Proposition 1.1 is now proved.

3. Proof of Theorem 2

We consider the case $p \geq 7$ because the case $p = 3$ is proved in [7]. We will construct to two unramified cyclic extensions L_1 and L_2 of $M_{p,n}$ of degree p such that $L_1/k_{p,n}$ (resp. $L_2/k_{p,n}$) is an abelian (resp. a non-abelian) extension.

3.1. Construction of L_1. From F. S. A. Muriefah [8] and A. Ito [4], we have

Theorem 4. *For a prime p with $p \equiv 3 \pmod 4$ and an odd positive integer n, the class number of $k_{p,n} = \mathbb{Q}(\sqrt{4 - p^{pn}}\,)$ is divisible by p.*

By this theorem, there exists an unramified cyclic extension L of $k_{p,n}$ of degree p. Put $L_1 := L \cdot M_{p,n}$. Then L_1 is an unramified cyclic extension of $M_{p,n}$ of degree p. Furthermore, it holds that $\mathrm{Gal}(L_1/k_{p,n}) \simeq C_{(p-1)/2} \times C_p$; namely, $L_1/k_{p,n}$ is an abelian extension.

3.2. Construction of L_2. First we introduce our previous results in [3] and [6]. Let p be an odd prime in general. Let ζ be a primitive pth root of unity and put $\omega := \zeta + \zeta^{-1}$. Moreover let k be a real quadratic field which is not contained in $\mathbb{Q}(\zeta)$. Then there exists a unique proper subextension of the bicyclic biquadratic extension $k(\zeta)/\mathbb{Q}(\omega)$ other than $k(\omega)$ and $\mathbb{Q}(\zeta)$. We denote it by M. Then M is a cyclic field of degree $p-1$. (In the case $p \equiv 3 \pmod 4$, M coincides with the composite field of $\mathbb{Q}(\sqrt{-pd_k})$ and $\mathbb{Q}(\omega)$, where d_k is the discriminant of k.) For an element γ of k, define the polynomial f_γ by

$$f_\gamma(X) := \sum_{i=0}^{(p-1)/2} (-N_k(\gamma))^i \frac{p}{p-2i} \binom{p-i-1}{i} X^{p-2i} - N_k(\gamma)^{(p-1)/2}\, \mathrm{Tr}_k(\gamma),$$

where N_k and Tr_k are the norm map and the trace map of $k/\mathbb{Q}$, respectively.

Proposition 3.1 ([3, Corollary 2.6], [6, Theorem 1.1])**.** *Let the notation be as above. For a unit ε of k with the conditions*

$$\begin{cases} N_k(\varepsilon) = 1, \\ \mathrm{Tr}_k(\varepsilon) \equiv \pm 2 \pmod{p^3}, \\ \varepsilon \notin k^p, \end{cases}$$

the splitting field $\mathrm{Spl}_{\mathbb{Q}}(f_\varepsilon)$ of f_ε over $\mathbb{Q}$ is an unramified cyclic extension of M of degree p and

$$\mathrm{Gal}(\mathrm{Spl}_{\mathbb{Q}}(f_\varepsilon)/\mathbb{Q}) \simeq F_p,$$

where F_p is the following group which is called Frobenius group:

$$F_p = \langle \sigma, \iota | \sigma^p = \iota^{p-1} = 1, \sigma\iota = \iota\sigma^a \rangle, \ \mathrm{ord}(a) = p-1 \quad \text{in } (\mathbb{F}_p)^\times.$$

Express $pn + 1 = 2s$ ($s \in \mathbb{Z}$) and put

$$\varepsilon_1 := \frac{p^{2s-1} - 2 + p^{s-1}\sqrt{p^{2s} - 4p}}{2} \in k'_{p,n} = \mathbb{Q}(\sqrt{p^{2s} - 4p}\,).$$

Then

$$\mathrm{Tr}_{k'_{p,n}}(\varepsilon_1) = p^{2s-1} - 2 \equiv -2 \pmod{p^3},$$

$$N_{k'_{p,n}}(\varepsilon_1) = \frac{(p^{2s-1} - 2)^2 - p^{2(s-1)}(p^{2s} - 4p)}{4} = 1.$$

Let us show that ε_1 is not a pth power in $k'_{p,n}$.

Here, we will show the following lemma.

Lemma 3.2. *For an integer $t \geq 5$, fix a unit*

$$\varepsilon = \frac{t - 2 + \sqrt{t(t-4)}}{2} = \frac{t - 2 + u\sqrt{m}}{2},$$

and denote the jth power of ε by

$$\varepsilon^j = \frac{t_j + (-1)^j 2 + u_j\sqrt{m}}{2}.$$

Then we have $t \mid t_j$ for any $j \geq 1$.

Proof. We see inductively that t_j satisfies

$$t_1 = t, \quad t_2 = t^2 - 2t, \quad t_{j+1} = (t-2)t_j - t_{j-1} + (-1)^j 2t.$$

Then it is clear that $t \mid t_j$ for any $j \geq 1$. $\square$

Now assume that ε_1 is a pth power in $k'_{p,n}$. Then we can express $\varepsilon_1 = \varepsilon_0^p$ for some $\varepsilon_0 \in k'_{p,n}$. Taking the norm, we have

$$1 = N_{k'_{p,n}}(\varepsilon_1) = N_{k'_{p,n}}(\varepsilon_0^p) = N_{k'_{p,n}}(\varepsilon_0)^p,$$

and hence

$$N_{k'_{p,n}}(\varepsilon_0) = 1.$$

Now we denote

$$\varepsilon_0 = \frac{t-2+\sqrt{t(t-4)}}{2}$$

and

$$\varepsilon_0^n = \frac{t_n + (-1)^n 2 + u_n\sqrt{m}}{2}$$

for any $n \geq 1$. Then $t_p = p^{2s-1}$ because

$$\frac{t_p + (-1)^p 2 + u_p\sqrt{m}}{2} = \varepsilon_0^p = \varepsilon_1 = \frac{p^{2s-1} - 2 + p^{s-1}\sqrt{p^{2s}-4p}}{2}.$$

Hence by Lemma 3.2, we have $t \mid p^{2s-1}$. Write

$$t = p^\alpha \ (0 \leq \alpha \leq 2s-1);$$

we have

$$\varepsilon_0 = \frac{p^\alpha - 2 + \sqrt{p^\alpha(p^\alpha-4)}}{2}.$$

Since $\varepsilon_0 \in k'_{p,n}$, we have

$$k'_{p,n} = \mathbb{Q}(\sqrt{p^\alpha(p^\alpha-4)}).$$

Remark that p is ramified in $k'_{p,n} = \mathbb{Q}(\sqrt{p^{2s}-4p})$. Then α must be odd. Write $\alpha = 2s'-1$; we obtain

$$p^\alpha(p^\alpha-4) = p^{2s'-1}(p^{2s'-1}-4) = p^{2(s'-1)}(p^{2s'}-4p).$$

Therefore we have

$$\mathbb{Q}(\sqrt{p^{2s}-4p}) = \mathbb{Q}(\sqrt{p^{2s'}-4p}).$$

It holds by Proposition 1.1 that $s = s'$. This implies $\varepsilon_0 = \varepsilon_1$, which leads a contradiction. So now we have proved $\varepsilon_1 \notin (k'_{p,n})^p$.

In the above, we verified that ε_1 satisfies three conditions

$$\begin{cases} N_{k'_{p,n}}(\varepsilon_1)=1, \\ \mathrm{Tr}_{k'_{p,n}}(\varepsilon_1)\equiv -2 \pmod{p^3}, \\ \varepsilon_1 \notin (k'_{p,n})^p. \end{cases}$$

Then by Proposition 3.1, $L_2 := \mathrm{Spl}_{\mathbb{Q}}(f_{\varepsilon_1})$ is an unramified extension of $M_{p,n}$ with $\mathrm{Gal}(L_2/\mathbb{Q}) \simeq F_p$. Since F_p does not have abelian subgroups of degree $p(p-1)/2$, $L_2/k_{p,n}$ is a non-abelian extension. Hence we have $L_1 \neq L_2$. Therefore we get two distinct unramified cyclic extensions L_1 and L_2 of $M_{p,n}$ of degree p. This completes the proof of Theorem 2.

Acknowledgments. The author wishes to thank Professor Ákos Pintér and his colleagues for their kind hospitality during the conference *Number Theory and its Applications*. Together, they made it possible to spend a wonderful week in Hungary.

References

[1] D. A. Buell, Class groups of quadratic fields, *Math. Comp.* **30** (1976), 610–623.

[2] Y. Bugeaud and T. N. Shorey, On the number of solutions of the generalized Ramanujan –Nagell equation, *J. Reine Angew. Math.* **539** (2001), 55–74.

[3] M. Imaoka and Y. Kishi, On dihedral extensions and Frobenius extensions, in "Galois theory and modular forms", Dev. Math., 11, *Kluwer Acad. Publ., Boston, MA*, 2004.

[4] A. Ito, Remarks on the divisibility of the class numbers of imaginary quadratic field $\mathbb{Q}(\sqrt{2^{2k}-q^n})$, *Glasgow Math. J.* **53** (2011), 379–389.

[5] S.-i. Katayama and Y. Kishi, Infinite family of imaginary cyclic fields of degree $p-1$ with the p-rank of the ideal class groups of at least two, *Tsinghua Sci. Technol.* **12** (2007), 475–478.

[6] Y. Kishi, On the Sylow p-subgroups of the ideal class groups of some imaginary cyclic fields of degree $p-1$, *Tokyo J. Math.* **27** (2004), 481–491.

[7] Y. Kishi, On the ideal class group of certain quadratic fields, *Glasgow Math. J.* **52** (2010), 575–581.

[8] F. S. A. Muriefah, On the Diophantine equation $Ax^2+2^{2m}=y^n$, *Int. J. Math. Math. Sci.* **25** (2001), 373–381.

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

CURRENT ADDRESS:
DEPARTMENT OF MATHEMATICS
AICHI UNIVERSITY OF EDUCATION
1 HIROSAWA, IGAYA-CHO
KARIYA-SHI AICHI 448-8542
JAPAN

E-mail: ykishi@auecc.aichi-edu.ac.jp

(Received September 5, 2011; revised January 30, 2012)