Imaginary cyclic fields of degree $p-1$ whose relative class numbers are divisible by p

By Yasuhiro Kishi

Department of Mathematics, Tokyo Metropolitan University, 1-1, Minami-Ohsawa, Hachioji, Tokyo 192-0397

(Communicated by Shokichi Iyanaga, M. J. A., April 12, 2001)

Abstract: We give a sufficient condition for an imaginary cyclic field of degree $p-1$ containing $\mathbf{Q}(\zeta+\zeta^{-1})$ to have the relative class number divisible by p. As a consequence, we see that there exist infinitely many imaginary cyclic fields of degree $p-1$ with the relative class number divisible by p.

Key words: Cyclic field; class number; Frobenius group.

1. Statement of the results. Let L be an imaginary cyclic field, and let h and h^+ be the class numbers of L and its maximal real subfield, respectively. Then h is divisible by h^+. The quotient h/h^+ is called the relative class number of L. In this paper, we study the divisibility of the relative class numbers of certain imaginary cyclic fields.

Let p be a fixed odd prime. Let ζ be a primitive p-th root of unity and put $\omega := \zeta+\zeta^{-1}$. It is expected that the class number of the cyclic field $\mathbf{Q}(\omega)$ of degree $(p-1)/2$ is not divisible by p (Vandiver's conjecture). The purpose of this paper is to give a sufficient condition for an imaginary cyclic field of degree $p-1$ containing $\mathbf{Q}(\omega)$ to have the relative class number divisible by p. As a consequence, we can get a similar result to Satgé [Sat] or Nakano [Nak]; that is, there are infinitely many imaginary cyclic fields of degree $p-1$ with the relative class number divisible by p.

Let $k=\mathbf{Q}(\sqrt{d})$ be a real quadratic field which is not contained in the cyclotomic field $\mathbf{Q}(\zeta)$. Then there exists a unique proper subextension of a bicyclic biquadratic extension $k(\zeta)/\mathbf{Q}(\omega)$ other than $\mathbf{Q}(\zeta)$ and $k(\omega)$. We denote it by M. M is an imaginary cyclic field of degree $p-1$, and its maximal real subfield coincides with $\mathbf{Q}(\omega)$ (See Fig. 1). We denote the norm map and the trace map of $k/\mathbf{Q}$ by N and Tr, respectively.

Our main results are

Theorem 1. *Let the notation be as above. Assume that there exists a unit ε of k with $\varepsilon \notin k^p$ which satisfies the condition*

$$\mathrm{Tr}(\varepsilon) \equiv 0 \pmod{p^2}. \tag{1.1}$$

Then the relative class number of M is divisible by p.

Theorem 2. *There exist infinitely many imaginary cyclic fields of degree $p-1$ whose maximal real subfields coincide with $\mathbf{Q}(\omega)$ and whose relative class numbers are divisible by p.*

Remarks 1. (1) The cases $p=3$ and 5 of Theorem 1 are included in the results of Herz [He, Theorem 6] and Parry [Pa, Theorem 5], respectively.
(2) Concerning the cases $p=3$ and 5 of Theorem 2, stronger results are known. Indeed, Nagel [Nag] (resp. Uehara [Ue]) proved that there exist infinitely many imaginary quadratic (resp. imaginary cyclic quartic) fields with relative class numbers divisible by an arbitrarily given rational integer.

2. Proofs of Theorems 1 and 2. Before proving Theorem 1, we state two propositions. First we extract some results from Sase [Sas, Proposition 2]. For a prime number p and an integer m, we denote the greatest exponent μ of p such that $p^\mu \mid m$ by $v_p(m)$.

Proposition 1 (Sase)**.** *Let p $(\neq 2)$ and q be prime numbers. Suppose that the polynomial*

$$g(X) = X^p + \sum_{j=0}^{p-2} a_j X^j, \quad a_j \in \mathbf{Z}$$

is irreducible over $\mathbf{Q}$ and satisfies the condition

$$v_q(a_j) < p-j \tag{2.1}$$

for some j, $0 \le j \le p-2$. Let θ be a root of $g(X)=0$ and put $K := \mathbf{Q}(\theta)$.

(i) *If q is different from p, then q is totally ramified*

2000 Mathematics Subject Classification. Primary 11R29; Secondary 11R20, 12F10.

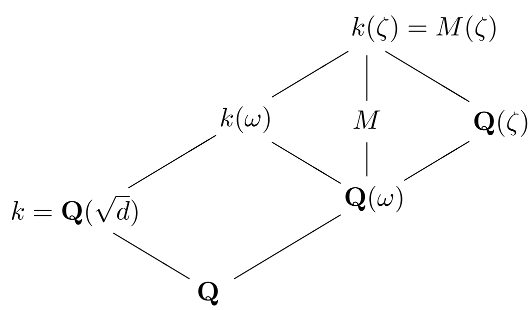

Fig. 1.

in $K/\mathbf{Q}$ if and only if

$$0 < \frac{v_q(a_0)}{p} \le \frac{v_q(a_j)}{p-j} \tag{2.2}$$

for every j, $1 \le j \le p-2$.

(ii) *Assume that $v_p(a_j) > 0$ for every j, $1 \le j \le p-2$. Then p is totally ramified in $K/\mathbf{Q}$ if and only if*

$$0 < \frac{v_p(a_0)}{p} \le \frac{v_p(a_j)}{p-j} \tag{2.3}$$

for every j, $1 \le j \le p-2$.

By applying [Im-Ki, Corollary 2.6] to the case $L_1 = \mathbf{Q}(\sqrt{d})$ and $k = \mathbf{Q}$, we give the following.

Proposition 2 (Imaoka and Kishi)**.** *Let the notation be as in Section* 1*. Let τ be a generator of* $\mathrm{Gal}(M(\zeta)/M)$*, and take an element γ of k. If $\gamma^{1-\tau} \notin M(\zeta)^p$, then the minimal splitting field E of the polynomial*

$$f(X,\gamma) = \sum_{i=0}^{(p-1)/2} (-N(\gamma))^i \frac{p}{p-2i}\binom{p-i-1}{i} \times X^{p-2i} - N(\gamma)^{(p-1)/2}\,\mathrm{Tr}(\gamma)$$

over $\mathbf{Q}$ is a cyclic extension of M of degree p and the Galois group of $E/\mathbf{Q}$ is the Frobenius group F_p of order $p(p-1)$, where $\binom{s}{j}$ denotes the binomial coefficient:

$$\binom{s}{j} = \frac{s(s-1)\cdots(s-j+1)}{j!}$$

for integers s and j, $0 \le j \le s$.

Proof of Theorem 1. Let ε be a unit of a quadratic field $\mathbf{Q}(\sqrt{d})$ with $\varepsilon \notin \mathbf{Q}(\sqrt{d})^p$, and let τ be a generator of $\mathrm{Gal}(M(\zeta)/M)$. First we will show that

$$\varepsilon^{1-\tau} \notin M(\zeta)^p. \tag{2.4}$$

Since M is the fixed field of $\langle\tau\rangle$ and does not contain ε, we have $\varepsilon^{1+\tau} = N(\varepsilon)$. Then we have

$$\varepsilon^{1-\tau} = \varepsilon^{2-(1+\tau)} = \varepsilon^2 N(\varepsilon^{-1}) = \pm\varepsilon^2. \tag{2.5}$$

On the other hand, we have $\varepsilon \notin M(\zeta)^p$ because the degree $[M(\zeta):k]$ is relatively prime to p. From this and (2.5), the condition (2.4) follows. By Proposition 2, therefore, we see that the minimal splitting field E of the polynomial $f(X,\varepsilon)$ over $\mathbf{Q}$ is an imaginary cyclic extension of M of degree p and the Galois group of $E/\mathbf{Q}$ is the Frobenius group F_p.

Next we will show that E is unramified over M. Let θ be a root of $f_p(X) = 0$. Let q be a prime number. A prime divisor of q in M is ramified in E if and only if q is totally ramified in $\mathbf{Q}(\theta)$ because $[E:M]$ and $[M:\mathbf{Q}]$ are relatively prime. Hence we have only to verify that no primes are totally ramified in $\mathbf{Q}(\theta)/\mathbf{Q}$.

The polynomial $f_p(X)$ satisfies the condition (2.1) for $j = 1$ because the coefficient of X in it is

$$(-N(\varepsilon))^{(p-1)/2}\frac{p}{p-2\cdot(p-1)/2}\binom{p-(p-1)/2-1}{(p-1)/2} = \pm p.$$

From this, moreover, we see that the condition (2.2) does not hold for every prime $q \ne p$. When $q \ne p$, therefore, we see by Proposition 1 that q is not totally ramified in $\mathbf{Q}(\theta)/\mathbf{Q}$. It is clear that all coefficient of terms of $f_p(X)$ except the highest degree X^p are divisible by p. By the assumption (1.1), the constant term is also divisible by p. On the other hand, we have

$$\frac{v_p(N(\varepsilon)^{(p-1)/2}\,\mathrm{Tr}(\varepsilon))}{p} = \frac{v_p(\mathrm{Tr}(\varepsilon))}{p} \ge \frac{2}{p}$$

and

$$\frac{v_p(-N(\varepsilon)^{(p-1)/2}p)}{p-1} = \frac{1}{p-1}.$$

Then we see that the condition (2.3) does not hold for $j = 1$ because $p \ge 3$. Hence p is not totally ramified in $\mathbf{Q}(\theta)/\mathbf{Q}$ either. Therefore E is an unramified cyclic extension of M. Hence the class number of M is divisible by p.

Let h^- denote the relative class number of M. Assume that $p \nmid h^-$. Then $E/\mathbf{Q}(\omega)$ must be abelian. This contradicts that E is an F_p-field. Hence we have $p \mid h^-$, and the proof of Theorem 1 is complete. $\square$

Let us quote a proposition which we need for the proof of Theorem 2.

Proposition 3 (Katayama [Ka]). *For every prime $q \neq 5$, $\varepsilon = (q+2+\sqrt{q(q+4)})/2$ is a fundamental unit of $\mathbf{Q}(\sqrt{q(q+4)})$.*

Proof of Theorem 2. We can take infinitely many prime integers q so that we have $q+2 \equiv 0 \pmod{p^2}$ for a fixed odd prime p. Then for each of such q, $\mathbf{Q}(\sqrt{q(q+4)})$ has a fundamental unit ε which satisfies $\mathrm{Tr}(\varepsilon) \equiv 0 \pmod{p^2}$ by Proposition 3. Therefore the statement follows from Theorem 1. □

Remarks 2. (1) Assume that p is a Fermat number; that is, p is a prime number of the form 2^t+1, $t \in \mathbf{N}$. Then every proper subfield M' of M must be contained in $\mathbf{Q}(\omega)$. If Vandiver's conjecture holds, then the class number of M' is not divisible by p. Hence every unramified cyclic extension of M of degree p which is normal over $\mathbf{Q}$, if it exists, is an F_p-field.

(2) Next consider the case that $p \equiv 3 \pmod 4$. Then M contains the imaginary quadratic field $\mathbf{Q}(\sqrt{-pd})$ as a subfield. If there exists a unit $\varepsilon \in k \setminus k^p$ with the condition (1.1) and the class number of $\mathbf{Q}(\sqrt{-pd})$ is divisible by p, then the p-rank of the ideal class group of M is greater than 1. Indeed, let E be an F_p-field containing M which is unramified over M, and let E_1 be an unramified cyclic extension of $\mathbf{Q}(\sqrt{-pd})$ of degree p. Then the composite field $E_1 \cdot M$ is also an unramified cyclic extension of M of degree p. Since both E_1 and M are normal over $\mathbf{Q}$, so is $E_1 \cdot M$. The Galois group $\mathrm{Gal}(E_1 \cdot M/\mathbf{Q})$ is not isomorphic to the Frobenius group F_p because $\mathrm{Gal}(E_1 \cdot M/\mathbf{Q})$ has a subgroup which is isomorphic to the cyclic group $C_{p(p-1)/2}$ of order $p(p-1)/2$. Therefore $E_1 \cdot M$ is different from E.

Table I

d	Exponent of ε_0 (m)	Structure of the ideal class group of $\mathbf{Q}(\sqrt{-7d})$	Structure of the ideal class group of M
73	4	[14]	[14, 7]
337	3	[28]	[28, 14, 2]
449	3	[56]	[56, 14, 2]
710	2	[14, 2, 2]	[56, 56, 2, 2, 2]
817	1	[28, 2]	[28, 28, 4, 2]
934	2	[14, 2]	[2702, 14]
986	4	[14, 2, 2]	[434, 14, 2, 2, 2]
1067	1	[28, 2, 2]	[364, 14, 2, 2, 2]
1986	2	[14, 2, 2]	[2198, 14, 2]
2001	2	[14, 2, 2]	[14, 14, 14, 2, 2]
2273	4	[154]	[2926, 7]
2274	2	[14, 2, 2]	[1022, 14, 2, 2, 2]
2334	2	[14, 2, 2]	[686, 14, 14]
2355	1	[14, 2, 2, 2]	[3206, 14, 2, 2]
2413	2	[14, 2]	[70, 70, 2, 2]
2498	1	[84, 2]	[420, 210, 3]
2642	4	[56, 2]	[7448, 14]
2838	2	[14, 2, 2, 2]	[686, 14, 2, 2, 2, 2]
3002	2	[42, 2, 2]	[882, 14, 14]
3106	2	[28, 2]	[2044, 14, 2, 2]
3323	2	[98, 2]	[1274, 182]
3603	1	[28, 2, 2]	[13132, 14, 2]
3706	4	[14, 2, 2]	[7322, 14, 2]
3722	4	[70, 2]	[490, 14, 14, 2]
4234	4	[14, 2, 2]	[2366, 14, 2, 2, 2]
4373	4	[70]	[7210, 7]
4574	1	[84, 2]	[35028, 14]
4987	2	[70, 2]	[38710, 14]

Example. In the case $p = 7$, there are 28 square free positive integers d in the range $0 \leq d \leq 5000$ for which a unit $\varepsilon_0^m \in \mathbf{Q}(\sqrt{d}) \setminus \mathbf{Q}(\sqrt{d})^7$ (for some m) satisfies the condition $\mathrm{Tr}(\varepsilon_0^m) \equiv 0 \pmod{7^2}$ and the class number of $\mathbf{Q}(\sqrt{-7d})$ is divisible by 7, where ε_0 is a fundamental unit of $\mathbf{Q}(\sqrt{d})$. In Table I, we list all of these 28 d's with the structures of the ideal class groups of $\mathbf{Q}(\sqrt{-7d})$ and of M. We denote an abelian group $C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$ by $[n_1,\ n_2, \ldots,\ n_r]$, where C_n denote a cyclic group of order n.

References

[He] Herz, C. S.: Construction of class fields. Seminar on Complex Multiplication: Seminar held at the Institute for Advanced Study, Princeton, N.J., 1957-58. (eds. Borel, A., Chowla, S., Herz, C. S., Iwasawa, K., and Serre, J.-P.). Lecture Notes in Math., no. 21, Springer, Berlin-Heidelberg-New York, pp. VII-1–VII-21 (1966).

[Im-Ki] Imaoka, M., and Kishi, Y.: Spiegelung Relations Between Dihedral Extensions and Frobenius Extensions. Tokyo Metropolitan Univ. Math. Preprint Series, no. 12, (2000).

[Ka] Katayama, S.: On fundamental units of real quadratic fields with norm +1. Proc. Japan Acad., **68A**, 18–20 (1992).

[Nag] Nagel, Tr.: Über die Klassenzahl imaginär-quadratischer Zahlköper. Abh. Math. Sem. Univ. Hamburg, **1**, 140–150 (1922).

[Nak] Nakano, S.: On the construction of certain number fields. Tokyo J. Math., **6**, 389–395 (1983).

[Pa] Parry, C. J.: Real quadratic fields with class numbers divisible by five. Math. Comp., **32**, 1261–1270 (1978).

[Sas] Sase, M.: On a family of quadratic fields whose class numbers are divisible by five. Proc. Japan Acad., **74A**, 120–123 (1998).

[Sat] Satgé, M.: Corps résolubles et divisibilité de nombres de classes d'idéaux. Enseign. Math.(2), **25**, 165–188 (1979).

[Ue] Uehara, T.: On class numbers of cyclic quartic fields. Pacific J. Math., **122**, 251–255 (1986).