M. Ozaki
Nagoya Math. J.
Vol. 169 (2003), 179–190

AN APPLICATION OF IWASAWA THEORY TO CONSTRUCTING FIELDS $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$ WHICH HAVE CLASS GROUP WITH LARGE p-RANK

MANABU OZAKI*

Abstract. Let p be an odd prime number. By using Iwasawa theory, we shall construct cyclotomic fields whose maximal real subfields have class group with arbitrarily large p-rank and conductor with only four prime factors.

§1. Introduction

The class group of the n-th cyclotomic field $\mathbf{Q}(\zeta_n)$ is a much studied classical and fascinating object in algebraic number theory. The class group of $\mathbf{Q}(\zeta_n)$ can be divided into two "parts": the relative class group (or the minus part of the class group) and the real class group, the latter being the class group of the maximal real subfield of $\mathbf{Q}(\zeta_n)$. The relative class group is easier to manage than the real class group. For example, the order h_n^- of the relative class group has an "elementary" expression, namely, the product of generalized Bernoulli numbers. In contrast to this, the real class number h_n^+ is much harder to calculate since the formula for h_n^+ includes a mysterious quantity related to units, namely, the regulator of the maximal real subfield $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$. This gives a hint of the difficulty of the study of the real class group. The number h_n^+ is so difficult to compute that we only know the exact value of h_n^+ for small n (However, R. Schoof calculated certain factors $\tilde{h}_p^+$ of h_p^+ for prime numbers $p < 10000$, which are very likely the exact values (see [8, pp.420–423])), and h_n^+ is quite small compared to h_n^-. Consequently one would like to find large h_n^+, and refining this problem, one would like to find real class groups with large p-rank for given prime p. In [1] and [2], Cornell and Rosen studied the p-rank of the class group of the maximal real subfield of cyclotomic fields. By using the genus theory,

Received March 17, 2000.
2000 Mathematics Subject Classification: Primary 11R23, 11R18, 11R29.
*This research is partially supported by the Grant-in-Aid for Encouragement of Young Scientists, Ministry of Education, Science, Sports and Culture, Japan.

https://doi.org/10.1017/S0027763000008485 Published online by Cambridge University Press

they gave methods to construct fields $\mathbf{Q}(\zeta_n+\zeta_n^{-1})$ which have class group with arbitrarily large p-rank. Specifically, they proved that if the number of distinct prime factors l of n with $l\equiv 1 \pmod p$ increases, then the p-rank of the class group of $\mathbf{Q}(\zeta_n+\zeta_n^{-1})$ also increases.

In the present paper, we shall construct cyclotomic fields whose maximal real subfields have class groups with arbitrarily large p-rank and conductors with only four prime factors. Usually, one would try to apply the genus theory to the construction of fields with the above properties. In fact, Lemmermeyer [6] recently done such construction by using the genus theory. However, interestingly, our method is based on Iwasawa theory of cyclotomic $\mathbf{Z}_p$-extensions, specifically, Iwasawa's main conjecture for totally real number fields, which was proved by Wiles [9].

In section 2, by using Iwasawa theory we shall give a criterion for the p-divisibility of the class number of a certain type of totally real number fields. In section 3, we shall apply the result obtained in section 2 to the construction of the maximal real subfield of a cyclotomic field with class group whose p-rank is arbitrarily large and also whose conductor has only four prime factors. In section 4, applying our construction, we shall give a lower bound of the order of the p-rank of the class group of $\mathbf{Q}(\zeta_n+\zeta_n^{-1})$ as $n\to\infty$.

§2. Criterion for the p-divisibility of the class number of a certain totally real number field

Let p be a fixed odd prime number, and let K be a totally real finite abelian extension of a totally real number field k. We assume that $p\nmid [K:k]$. We denote by K_∞ the cyclotomic $\mathbf{Z}_p$-extension of K, and let K_n be its n-th layer. Put $\Gamma=\mathrm{Gal}(K_\infty/K)$, fixing a topological generator γ of Γ. For any field $F\subseteq\overline{\mathbf{Q}}$, we denote by $L(F)$ and $M(F)$ the maximal unramified pro-p abelian extension over F and the maximal pro-p abelian extension over F which is unramified outside p, respectively, and by $A(F)$ the Sylow p-subgroup of the class group of F. Put $\Delta=\mathrm{Gal}(K/k)$ and $\widehat{\Delta}=\mathrm{Hom}(\Delta,\overline{\mathbf{Q}}_p^\times)$. For any $\mathbf{Z}_p[\Delta]$-module M and $\chi\in\widehat{\Delta}$, we define the χ-part of M by $M^\chi=(\#(\Delta)^{-1}\sum_{\sigma\in\Delta}\mathrm{Tr}_{\mathbf{Q}_p(\chi(\Delta))/\mathbf{Q}_p}(\chi(\sigma))\sigma^{-1})M$. Then we have $M=\bigoplus_\chi M^\chi$, where χ runs over $\chi\in\widehat{\Delta}$ modulo $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-conjugacy, namely, representatives of one dimensional factors over $\overline{\mathbf{Q}}_p$ of every irreducible $\mathbf{Q}_p$-character of Δ.

In this section, using Iwasawa's main conjecture proved by Wiles [9] and the idea given in [7], we shall give a criterion for the p-divisibility of the class number of K_n for $n \geq 1$ under some assumption on K. Actually, we shall give a criterion for non-triviality of the χ-part of $A(K_n)$ by means of estimating the value of p-adic L-function of k for $n \geq 1$ and $\chi \in \widehat{\Delta}$, which can be regarded as a totally real analogue of the theorems of Herbrand and Ribet for the minus part of the class group of the p-th cyclotomic field (see [8, Theorems 6.17 and 6.18]).

Our aim in this section is to prove the following theorem:

THEOREM 1. *Let notations be as above. We assume that the prime p is completely decomposed in K. Then the following two statements are equivalent for every $\chi \in \widehat{\Delta}$:*

(i) $A(K_n)^\chi \neq 0$ *for all* $n \geq 1$,

(ii) $$\begin{cases} L_p(0, \chi, k) \equiv 0 \pmod{p} & (\textit{if } \chi \neq 1), \\ p\zeta_p(0, k) \equiv 0 \pmod{p} & (\textit{if } \chi = 1), \end{cases}$$

where $L_p(s, \chi, k)$ and $\zeta_p(s, k)$ are the p-adic L-function of k and the p-adic zeta function of k, respectively.

In order to prove Theorem 1, we need the following lemma:

LEMMA 1. *Let K be as in the statement of Theorem 1. Then $M(K)/K$ is the maximal abelian sub-extension of $L(K_\infty)/K$.*

Proof. We denote by $I_\mathfrak{p} \subseteq \mathrm{Gal}(M(K)/K)$ the inertia group for a prime $\mathfrak{p}$ of K lying above p. It follows from the assumption on K that the pro-p part of the local unit group of $K_\mathfrak{p}$ is isomorphic to $\mathbf{Z}_p$, where $K_\mathfrak{p}$ stands for the completion of K at $\mathfrak{p}$. Hence class field theory shows that $I_\mathfrak{p}$ is isomorphic to a quotient group of $\mathbf{Z}_p$. Since $\mathfrak{p}$ is infinitely ramified in $K_\infty \subseteq M(K)$, we see that $I_\mathfrak{p} \simeq \mathbf{Z}_p$, and that $I_\mathfrak{p} \cap \mathrm{Gal}(M(K)/K_\infty) = 0$. This equality implies that the primes of K_∞ lying above $\mathfrak{p}$ are unramified in $M(K)$. Therefore $M(K)/K_\infty$ is an unramified extension, and $M(K) \subseteq L(K_\infty)$. Thus we obtain Lemma 1. $\square$

Let $\mathfrak{X} = \mathrm{Gal}(M(K_\infty)/K_\infty)$, $X = \mathrm{Gal}(L(K_\infty)/K_\infty)$, and $Y = \mathrm{Gal}(L(K_\infty)/K_\infty L(K_0))$. Then these Galois groups are finitely generated torsion Λ-modules, where $\Lambda = \mathbf{Z}_p[\Delta][[\Gamma]]$ (see [4] or [8]).

We need the following theorem proved by Wiles [9].

https://doi.org/10.1017/S0027763000008485 Published online by Cambridge University Press

Theorem A (Iwasawa's Main Conjecture). *Let settings and notations be as above. We put* $\Lambda = \mathbf{Z}_p[\Delta][[\Gamma]]$. *Let* $\tilde{\gamma} \in \mathrm{Gal}(K_\infty(\zeta_p)/K(\zeta_p))$ *be the image of* $\gamma \in \Gamma$ *by the natural isomorphism* $\Gamma \simeq \mathrm{Gal}(K_\infty(\zeta_p)/K(\zeta_p))$. *We let* $\kappa \in 1+p\mathbf{Z}_p$ *be the number such that* $\zeta^{\tilde{\gamma}} = \zeta^\kappa$ *for any p-power-th root of unity* ζ. *Let* $F_\chi(T) \in \mathbf{Z}_p[\Delta]^\chi[[T]] \simeq \mathbf{Z}_p[\chi(\Delta)][[T]]$ *be the power series such that*

$$L_p(s,\chi,k) = \begin{cases} F_\chi(\kappa^{1-s}-1) & (\textit{if } \chi \neq 1), \\ \dfrac{F_\chi(\kappa^{1-s}-1)}{\kappa^{1-s}-1} & (\textit{if } \chi = 1) \end{cases}$$

for $s \in \mathbf{Z}_p$. *Then*

$$\mathrm{char}_{\Lambda^\chi}\mathfrak{X}^\chi = F_\chi(\gamma-1)\Lambda^\chi,$$

where $\mathrm{char}_{\Lambda^\chi}\mathfrak{X}^\chi$ *denotes the characteristic ideal of the* Λ^χ*-module* $\mathfrak{X}^\chi$ *and* $F_\chi(\gamma-1)$ *is the image of* $F_\chi(T)$ *by the isomorphism* $\mathbf{Z}_p[\chi(\Delta)][[T]] \simeq \Lambda^\chi$ *sending* T *to* $\gamma - 1$.

Proof of Theorem 1. Let $\nu_n = \frac{\gamma^{p^n}-1}{\gamma-1} \in \Lambda = \mathbf{Z}_p[\Delta][[\Gamma]]$. Then

$$A(K_n)^\chi \simeq X^\chi/\nu_n Y^\chi$$

by [4, Theorem 6]. Since X is finitely generated over Λ, we have

$$A(K_n)^\chi \neq 0 \text{ for all } n \geq 1 \Longleftrightarrow X^\chi \neq 0 \tag{1}$$

by the above isomorphism and Nakayama's lemma. We denote by $L(K_\infty)^{\mathrm{ab}}/K$ the maximal abelian sub-extension of $L(K_\infty)/K$. Then

$$\mathrm{Gal}(L(K_\infty)^{\mathrm{ab}}/K_\infty) \simeq X/(\gamma-1)X.$$

Since $L(K_\infty)^{\mathrm{ab}} = M(K)$ by Lemma 1, and $\mathrm{Gal}(M(K)/K_\infty) \simeq \mathfrak{X}/(\gamma-1)\mathfrak{X}$, we have

$$X^\chi/(\gamma-1)X^\chi \simeq \mathfrak{X}^\chi/(\gamma-1)\mathfrak{X}^\chi.$$

Hence we see that

$$X^\chi \neq 0 \Longleftrightarrow \mathfrak{X}^\chi \neq 0 \tag{2}$$

by Nakayama's lemma. Since $\mathfrak{X}^\chi$ has no non-trivial finite Λ^χ-submodules (see [3]), $\mathfrak{X}^\chi \neq 0$ is equivalent to $\mathrm{char}_{\Lambda^\chi}(\mathfrak{X}) \neq \Lambda^\chi$, which in turn is equivalent to $F_\chi(T) \notin \mathbf{Z}_p[\chi(\Delta)][[T]]^\times$ by Theorem A. This is also equivalent to $F_\chi(\kappa -$

1) $\equiv 0 \pmod{p}$. We note that the number κ in Theorem A satisfies $\kappa \notin 1 + p^2\mathbf{Z}_p$ by the assumption on K. It follows from

$$F_\chi(\kappa - 1) = \begin{cases} L_p(0, \chi, k) & (\text{if } \chi \neq 1), \\ (\kappa - 1)\zeta_p(0, k) & (\text{if } \chi = 1) \end{cases}$$

that

$$\mathfrak{X}^\chi \neq 0 \Longleftrightarrow \begin{cases} L_p(0, \chi, k) \equiv 0 \pmod{p} & (\text{if } \chi \neq 1), \\ p\zeta_p(0, k) \equiv 0 \pmod{p} & (\text{if } \chi = 1). \end{cases} \tag{3}$$

Combining (1), (2) and (3), we obtain Theorem 1. □

§3. Construction of the maximal real subfield of a cyclotomic field which has class group with large p-rank

In this section, by using Theorem 1 in the previous section, we shall find n with four prime factors for which the class group of the maximal real subfield of the n-th cyclotomic field has arbitrarily large p-rank.

Let p be a fixed odd prime, and let k and k' be a pair of real abelian number fields satisfying the following three conditions:

(a) The conductor of k is a prime q which splits completely in k', and $[k : \mathbf{Q}] = p$.

(b) The prime p does not divide $[k' : \mathbf{Q}]$.

(c) The prime p splits completely in kk'.

We note that $q \equiv 1 \pmod{p}$ from (a).

Lemma 2. *Let k and k' be real abelian number fields with properties* (a), (b) *and* (c). *Then we have*

$$B_{1,\chi\psi\omega^{-1}} = \frac{1}{pqf_\chi} \sum_{a=1}^{pqf_\chi} a\chi\psi\omega^{-1}(a) \equiv 0 \pmod{(1 - \zeta_p)}$$

for any p-adic Dirichlet characters $\chi \in \mathrm{Gal}(k'/\mathbf{Q})\widehat{\ } - \{1\}$ and $\psi \in \mathrm{Gal}(k/\mathbf{Q})\widehat{\ } - \{1\}$, where f_χ is the conductor of χ, ω is the Teichmüller character for the prime p and ζ_p is a primitive p-th root of unity. If we assume $q \equiv 1 \pmod{p^2}$, then the above congruence also holds for $\chi = 1 \in \mathrm{Gal}(k'/\mathbf{Q})\widehat{\ }$.

Proof. We first note that p, q and f_χ are pairwise coprime by conditions (a) and (c).

$$\begin{aligned} B_{1,\chi\psi\omega^{-1}} &= \frac{1}{pqf_\chi} \sum_{\substack{a=1 \\ (a,pqf_\chi)=1}}^{pqf_\chi} a\omega^{-1}(a)\chi(a)\psi(a) \\ &= \frac{1}{pqf_\chi} \sum_{\substack{a=1 \\ (a,pqf_\chi)=1}}^{pqf_\chi} a\omega^{-1}(a)\chi(a)(\psi(a)-1) \\ &\qquad\qquad + \frac{1}{pqf_\chi} \sum_{\substack{a=1 \\ (a,pqf_\chi)=1}}^{pqf_\chi} a\omega^{-1}(a)\chi(a). \end{aligned}$$

We write S for the latter term of the bottom row in the above expression. Since $\psi(a)^p = 1$ and $a\omega^{-1}(a) \equiv 1 \pmod{p}$, we have

$$(4) \qquad B_{1,\chi\psi\omega^{-1}} \equiv \frac{1}{pqf_\chi} \sum_{\substack{a=1 \\ (a,pqf_\chi)=1}}^{pqf_\chi} \chi(a)(\psi(a)-1) + S \pmod{(1-\zeta_p)}.$$

We can easily see that

$$(5) \qquad \begin{aligned} &\sum_{\substack{a=1 \\ (a,pqf_\chi)=1}}^{pqf_\chi} \chi(a)\psi(a) \\ &\quad = \sum_{\substack{a=1 \\ (a,qf_\chi)=1}}^{pqf_\chi} \chi(a)\psi(a) - \chi(p)\psi(p) \sum_{\substack{b=1 \\ (b,qf_\chi)=1}}^{qf_\chi} \chi(b)\psi(b) = 0 - 0 = 0, \end{aligned}$$

since $\chi\psi$ is a non-trivial character. Also we have

$$(6) \qquad \sum_{\substack{a=1 \\ (a,pqf_\chi)=1}}^{pqf_\chi} \chi(a) = \begin{cases} 0 & (\text{if } \chi \neq 1), \\ (p-1)(q-1) & (\text{if } \chi = 1). \end{cases}$$

Now we shall calculate S:

$$S = \frac{1}{pqf_\chi} \sum_{\substack{a=1 \\ (a,pqf_\chi)=1}}^{pqf_\chi} a\omega^{-1}(a)\chi(a)$$

https://doi.org/10.1017/S0027763000008485 Published online by Cambridge University Press

$$= \frac{1}{pqf_\chi}\left\{ \sum_{\substack{a=1\\(a,pf_\chi)=1}}^{pqf_\chi} a\omega^{-1}(a)\chi(a) - q\omega^{-1}(q)\chi(q) \sum_{\substack{b=1\\(b,pf_\chi)=1}}^{pf_\chi} b\omega^{-1}(b)\chi(b) \right\}.$$

We see that

$$\begin{aligned}
\sum_{\substack{a=1\\(a,pf_\chi)=1}}^{pqf_\chi} a\omega^{-1}(a)\chi(a) &= \sum_{b=0}^{q-1} \sum_{\substack{a=1\\(a,pf_\chi)=1}}^{pf_\chi} (a+bpf_\chi)\omega^{-1}(a)\chi(a) \\
&= \sum_{b=0}^{q-1} \sum_{\substack{a=1\\(a,pf_\chi)=1}}^{pf_\chi} a\omega^{-1}(a)\chi(a) \\
&= q \sum_{\substack{a=1\\(a,pf_\chi)=1}}^{pf_\chi} a\omega^{-1}(a)\chi(a),
\end{aligned}$$

since the conductor of the non-trivial character $\omega^{-1}\chi$ is pf_χ. Hence we find that

$$\begin{aligned}
S &= \frac{1}{pqf_\chi}\left\{ q \sum_{\substack{a=1\\(a,pf_\chi)=1}}^{pf_\chi} a\omega^{-1}(a)\chi(a) - q\omega^{-1}(q)\chi(q) \sum_{\substack{a=1\\(a,pf_\chi)=1}}^{pf_\chi} a\omega^{-1}(a)\chi(a) \right\} \\
&= 0,
\end{aligned}$$

since $\omega^{-1}(q)\chi(q) = 1$ from condition (a). Therefore it follows from (4), (5) and (6) that

$$B_{1,\omega^{-1}\chi\psi} \equiv \begin{cases} 0 & (\text{if } \chi \neq 1), \\ -\dfrac{1}{pq}(p-1)(q-1) & (\text{if } \chi = 1), \end{cases} \pmod{(1-\zeta_p)}$$

which completes the proof of Lemma 2. □

We shall give real abelian number fields k and k' satisfying conditions (a), (b) and (c) in the following. Given an odd prime p, we choose a prime q satisfying

$$(7) \qquad \begin{cases} q \equiv 1 & (\text{mod } p), \\ p^{\frac{q-1}{p}} \equiv 1 & (\text{mod } q). \end{cases}$$

https://doi.org/10.1017/S0027763000008485 Published online by Cambridge University Press

Since (7) is equivalent to the statement that a prime q splits completely in $\mathbf{Q}(\zeta_p, \sqrt[p]{p})$ (ζ_n denotes a primitive n-th root of unity for $n \geq 1$), there exist infinitely many primes q satisfying (7) by the Chebotarev density theorem. If k denotes the unique subfield of $\mathbf{Q}(\zeta_q)$ with $[k : \mathbf{Q}] = p$, then p splits completely in k by (7). Take a prime number r with $(r, pq) = 1$, and let k' be a subfield of $\mathbf{Q}(\zeta_r + \zeta_r^{-1})$ with $p \nmid [k' : \mathbf{Q}]$ in which both primes p and q split completely. Then the real abelian number fields k and k' satisfy conditions (a), (b) and (c).

Theorem 2. *Let q, r, and k' be as above. Then we have*

$$p\text{-rank}\, A(\mathbf{Q}(\zeta_{p^2qr} + \zeta_{p^2qr}^{-1})) \geq [k' : \mathbf{Q}] - 1.$$

To prove Theorem 2, we need the following lemma:

Lemma 3. *Let p be a prime and M a finite $\mathbf{Z}_p$-module on which a finite abelian group G with $p \nmid \#G$ acts. Then $\#\{\chi^\sigma | \sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)\}$ divides p-rank M^χ for any $\chi \in \widehat{G} = \mathrm{Hom}(G, \overline{\mathbf{Q}}_p^\times)$.*

Proof. Put $\overline{G} = G/\mathrm{Ker}\chi$. Then the cyclic group $\overline{G}$ acts on $M^\chi = e_\chi M$ since $he_\chi = e_\chi$ for $h \in \mathrm{Ker}\chi$, where $e_\chi = (\#G)^{-1}\sum_{g\in G}\mathrm{Tr}_{\mathbf{Q}_p(\chi(G))/\mathbf{Q}_p}(\chi(g))g^{-1}$. We define $\mathrm{N}_{\overline{H}} = \sum_{h\in\overline{H}} h$ for any non-trivial subgroup $\overline{H}$ of $\overline{G}$. Then we have

$$\mathrm{N}_{\overline{H}} \sum_{g\in G} \chi^\sigma(g)g^{-1} = \sum_{h\in\overline{H}} \chi^\sigma(h) \sum_{g\in G} \chi^\sigma(g)g^{-1} = 0$$

for every $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ since χ is a faithful character of $\overline{G}$. Hence $\mathrm{N}_{\overline{H}}$ annihilates M^χ for any non-trivial subgroup $\overline{H} \subseteq \overline{G}$. Therefore a similar argument to the proof of [8, Theorem 10.8] shows that the order of $p \bmod \#\overline{G}$ divides p-rank M^χ. Since the order of $p \bmod \#\overline{G}$ is equal to $\#\{\chi^\sigma | \sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)\}$, we obtain the lemma. □

Proof of Theorem 2. Let $K = kk'$. Then the prime p splits completely in K by condition (c), and $p \nmid [K : k] = [k' : \mathbf{Q}]$ by condition (b). Thus we can apply Theorem 1 to K/k. For $\chi \in \mathrm{Gal}(K/k)^\wedge - \{1\}$ we have

$$L_p(0, k, \chi) = \prod_{\psi\in\mathrm{Gal}(k/\mathbf{Q})^\wedge} L_p(0, \mathbf{Q}, \chi\psi) = \prod_{\psi\in\mathrm{Gal}(k/\mathbf{Q})^\wedge} (-B_{1,\chi\psi\omega^{-1}}),$$

where we identify $\mathrm{Gal}(K/k)\widehat{\ }$ with $\mathrm{Gal}(k'/\mathbf{Q})\widehat{\ }$ by the natural isomorphism. Hence we find that

$$L_p(0, k, \chi) \equiv 0 \pmod p$$

by Lemma 2. Therefore it follows from Theorem 1 that $A(K_1)^\chi \neq 0$ for every $\chi \in \mathrm{Gal}(K/k)\widehat{\ } - \{1\}$. This and Lemma 3 imply

$$p\text{-rank } A(K_1)^\chi \geq \#\{\chi^\sigma | \sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)\}$$

for every $\chi \in \mathrm{Gal}(K/k)\widehat{\ } - \{1\}$. Therefore

$$\begin{aligned} p\text{-rank } A(K_1) &\geq {\sum_{\chi}}' \#\{\chi^\sigma | \sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)\} \\ &= [K : k] - 1 = [k' : \mathbf{Q}] - 1, \end{aligned} \tag{8}$$

where χ runs over $\chi \in \mathrm{Gal}(K/k)\widehat{\ } - \{1\}$ modulo $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-conjugacy in ${\sum_\chi}'$. We consider the ascending chain of fields $K_1 \subseteq K(\zeta_{p^2})^+ \subseteq K(\zeta_{p^2 r})^+ \subseteq \mathbf{Q}(\zeta_{p^2qr} + \zeta_{p^2qr}^{-1})$, where F^+ denotes the maximal real subfield of F for any abelian number field F. Since $p \nmid [K(\zeta_{p^2})^+ : K_1] = \frac{p-1}{2}$ and the primes of $K(\zeta_{p^2})^+$ (resp. $K(\zeta_{p^2 r})^+$) lying above r (resp. q) are totally ramified in $K(\zeta_{p^2 r})^+$ (resp. $\mathbf{Q}(\zeta_{p^2qr} + \zeta_{p^2qr}^{-1})$), the norm map from $A(\mathbf{Q}(\zeta_{p^2qr} + \zeta_{p^2qr}^{-1}))$ to $A(K_1)$ is surjective. Hence we obtain Theorem 2 by (8). $\square$

Now we shall derive the following our main result from Theorem 2:

THEOREM 3. *Let p be an odd prime number. For any given positive integer N, there exist prime numbers q and r such that p-rank $A(\mathbf{Q}(\zeta_{p^2qr} + \zeta_{p^2qr}^{-1})) \geq N$. More precisely, if primes q and r satisfy*

$$\begin{cases} q \equiv 1 & \pmod p, \\ p^{\frac{q-1}{p}} \equiv 1 & \pmod q, \\ r \equiv 1 & \pmod N \\ p^{\frac{r-1}{N}} \equiv 1 & \pmod r, \\ q^{\frac{r-1}{N}} \equiv 1 & \pmod r, \end{cases} \tag{9}$$

for a positive integer N prime to $2p$, then p-rank $A(\mathbf{Q}(\zeta_{p^2qr} + \zeta_{p^2qr}^{-1})) \geq N-1$.

https://doi.org/10.1017/S0027763000008485 Published online by Cambridge University Press

Proof. Assume that primes q and r satisfies condition (9). Let k' be the subfield of $\mathbf{Q}(\zeta_r + \zeta_r^{-1})$ with $[k' : \mathbf{Q}] = N$. Then the primes p and q splits completely in k' and $p \nmid [k' : \mathbf{Q}]$. Hence we have

$$p\text{-rank}\, A(\mathbf{Q}(\zeta_{p^2qr} + \zeta_{p^2qr}^{-1})) \geq [k' : \mathbf{Q}] - 1 = N - 1,$$

from Theorem 2. Since (9) is equivalent to the statement that the prime q splits completely in $\mathbf{Q}(\zeta_p, \sqrt[p]{p})$ and the prime r splits completely in $\mathbf{Q}(\zeta_N, \sqrt[N]{p}, \sqrt[N]{q})$, we can find primes q and r with condition (9) by the Chebotarev density theorem. Thus we have the theorem. □

§4. Behavior of the p-rank of the class group of the maximal real subfield of cyclotomic fields

In this section, we shall give the following theorem concerning the behavior of the p-rank $r_p(n)$ of the class group of the maximal real subfield of the n-th cyclotomic field as $n \to \infty$ by applying our construction in section 3:

THEOREM 4. *Let p be an odd prime. Denote by $r_p(n)$ the p-rank of the class group of $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$. We assume that the generalized Riemann hypothesis holds. Then we have*

$$r_p(n) \neq O(n^{1/6-\varepsilon})$$

for any $\varepsilon > 0$. Here $O(\ )$ stands for Landau's symbol. In other words, for any $c > 0$ and $\varepsilon > 0$, there exists $n \geq 1$ such that

$$r_p(n) \geq cn^{1/6-\varepsilon}.$$

To prove Theorem 4, we recall the following theorem from analytic number theory:

THEOREM B (LAGARIAS-ODLYZKO [5]). *There exists an absolute constant $c_0 \geq 0$ with the following property:*
Let L/K be a finite Galois extension of number fields. If the generalized Riemann hypothesis holds for the Dedekind zeta function of L, then for every conjugacy class C of $\mathrm{Gal}(L/K)$, there exists a prime ideal $\mathfrak{p}$ of K such that

$$[\mathfrak{p}, L/K] = C$$

and

$$\mathrm{N}(\mathfrak{p}) \leq c_0(\log d_L)^2(\log\log d_L)^4.$$

https://doi.org/10.1017/S0027763000008485 Published online by Cambridge University Press

Here $[\mathfrak{p}, L/K]$ *denotes the conjugacy class of* $\mathrm{Gal}(L/K)$ *which consists of Frobenius automorphisms for primes of* L *lying above* $\mathfrak{p}$*, and* d_L *is the absolute value of the discriminant of* L*.*

We also need the following lemma:

Lemma 4. *Let* K_1 *and* K_2 *be number fields. Then we have*

$$d_{K_1K_2} \leq d_{K_1}^{[K_2:\mathbf{Q}]} d_{K_2}^{[K_1:\mathbf{Q}]}.$$

Proof. For any extension of number fields L/K, we denote by $\mathfrak{D}(L/K)$ the different of L/K. Then we have $d_L\mathbf{Z} = \mathrm{N}_{L/\mathbf{Q}}\mathfrak{D}(L/\mathbf{Q})$. Also we write for $\mathfrak{D}_{L/K}(\alpha)$ the different of $\alpha \in L$ relative to L/K. Since $\mathfrak{D}(K_1K_2/\mathbf{Q}) = \mathfrak{D}(K_1K_2/K_1)\mathfrak{D}(K_1/\mathbf{Q})$, we have by taking the norm $\mathrm{N}_{K_1K_2/\mathbf{Q}}$

$$\begin{aligned} d_{K_1K_2}\mathbf{Z} &= (\mathrm{N}_{K_1K_2/\mathbf{Q}}\mathfrak{D}(K_1K_2/K_1))d_{K_1}^{[K_1K_2:K_1]} \\ &\supseteq (\mathrm{N}_{K_1K_2/\mathbf{Q}}\mathfrak{D}(K_1K_2/K_1))d_{K_1}^{[K_2:\mathbf{Q}]}. \end{aligned}$$

We shall show that $d_{K_2}^{[K_1:\mathbf{Q}]}\mathbf{Z} \subseteq \mathrm{N}_{K_1K_2/\mathbf{Q}}\mathfrak{D}(K_1K_2/K_1)$, which implies Lemma 4. We recall that $\mathfrak{D}(L/K)$ is the greatest common divisor of $\{\mathfrak{D}_{L/K}(\alpha) | \alpha$ is an integer in $L\}$ for any extension of number fields L/K. Hence it follows from $\mathfrak{D}_{K_1K_2/K_1}(\alpha) | \mathfrak{D}_{K_2/\mathbf{Q}}(\alpha)$ for every integer $\alpha \in K_2$ that $\mathfrak{D}(K_2/\mathbf{Q}) \subseteq \mathfrak{D}(K_1K_2/K_1)$. Taking the norm $\mathrm{N}_{K_1K_2/\mathbf{Q}}$, we have

$$d_{K_2}^{[K_1:\mathbf{Q}]}\mathbf{Z} \subseteq d_{K_2}^{[K_1K_2:K_2]}\mathbf{Z} \subseteq \mathrm{N}_{K_1K_2/\mathbf{Q}}\mathfrak{D}(K_1K_2/K_1).$$

Thus we obtain Lemma 4. $\square$

Proof of Theorem 4. Let $\delta > 0$ be fixed. In the following, $c_i > 0$ denotes a constant depending only on δ and p. For the prime p, we choose a prime q satisfying condition (7) in section 3, and fix q once for all. Next we choose a prime r satisfying condition (9) for the above fixed prime q and $N > 0$ prime to $2p$. Since $d_{\mathbf{Q}(\zeta_N)} \leq N^N$, $d_{\mathbf{Q}(\sqrt[N]{p})} \leq N^N p^{N-1}$ and $d_{\mathbf{Q}(\sqrt[N]{q})} \leq N^N q^{N-1}$, we can find that

$$d_{\mathbf{Q}(\zeta_N, \sqrt[N]{p}, \sqrt[N]{q})} \leq (N^{N^2}(N^N p^{N-1})^N)^N (N^N q^{N-1})^{N^2} \leq N^{c_1 N^3}$$

by Lemma 4. Hence we can choose r with

$$r \leq c_2(N^3 \log N)^{(2+\delta/2)} \leq c_3 N^{3(2+\delta)} \tag{10}$$

by Theorem B. Now we shall deal with $\mathbf{Q}(\zeta_{p^2qr} + \zeta_{p^2qr}^{-1})$. By Theorem 3,

$$r_p(p^2qr) \geq N - 1. \tag{11}$$

On the other hand, we have

$$p^2qr \leq c_4 N^{3(2+\delta)} \tag{12}$$

from (10). If we choose $\delta > 0$ with $3(2+\delta)(\frac{1}{6} - \varepsilon) < 1$ and let N go to infinity, then we obtain Theorem 4 by (11) and (12). □

Acknowledgements. The author wishes to thank Prof. Franz Lemmermeyer for his valuable advice.

References

[1] G. Cornell, *Exponential growth of the l-rank of the class group of the maximal real subfield of cyclotomic fields*, Bull. Amer. Math. Soc., **8** (1983), 55–58.

[2] G. Cornell and M. Rosen, *The l-rank of the real class group of cyclotomic fields*, Compositio Math., **53** (1984), 133–141.

[3] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math., **47** (1978), 85–99.

[4] K. Iwasawa, *On $\mathbf{Z}_l$-extensions of algebraic number fields*, Ann. of Math., **98** (1973), 246–326.

[5] J.C. Lagarias and A.M. Odlyzko, *Effective version of the Chebotarev density theorem*, Algebraic number fields, (Durham Symposium, 1975; ed. by A.Fröhlich), Academic Press, London, 1977, 409–464.

[6] F. Lemmermeyer, *Ideal class groups of cyclotomic number fields II*, Acta. Arith., **84** (1998), 59–70.

[7] M. Ozaki, *The class group of $\mathbf{Z}_p$-extensions over totally real number fields*, Tôhoku Math. J., **49** (1997), 431-435.

[8] L.C. Washington, Introduction to Cyclotomic Fields (2nd. edition), Graduate Texts in Math. 83, Springer-Verlag, New York, 1997.

[9] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math., **131** (1990), 493–540.

Department of Mathematics
Faculty of Science and Engineering
Shimane University
1060, Nishikawatsu-cho, Matsue 690-8504 Japan
ozaki@math.shimane-u.ac.jp