CLASS NUMBERS OF QUADRATIC EXTENSIONS
OF ALGEBRAIC NUMBER FIELDS

JIN NAKAGAWA

(Received March 5, 1985)

Introduction. For a number field $K$, denote by $C_K$ the ideal class group of $K$. Let $n$ be a given natural number greater than 1. In [5], Nagell proved that there exist infinitely many imaginary quadratic fields with class numbers divisible by $n$. The corresponding result for real quadratic fields was obtained by Yamamoto [11] and Weinberger [10]. In the same paper, Yamamoto constructed infinitely many imaginary quadratic fields $K$ such that $C_K$ contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$. These results were recently generalized for non totally real fields of arbitrary degrees by Azuhata-Ichimura [1], and for totally real fields of arbitrary degrees by Nakano [7]. To be more precise, they constructed, for any integers $m$, $n > 1$ and $r_1, r_2 \geq 0$ with $r_1 + 2r_2 = m$, infinitely many number fields $K$ of degree $m$ with just $r_1$ real primes such that $C_K$ contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{r_2+1}$.

The main purpose of this paper is to prove certain relative versions of the above results. In this direction, Naito obtained a generalization of Yamamoto's result on imaginary quadratic fields. He constructed in [6], for a given totally real field $F$, infinitely many totally imaginary quadratic extensions $K/F$ such that $C_K$ contains a subgroup $H$ isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ with $H \cap C_F = 1$. On the other hand, we obtain a generalization of Yamamoto's result on real quadratic fields (Theorem 1). Our second result is an analogue of Nakano's result over quadratic fields (Theorem 2). For $n = 3, 5$ or 7, it was known that there exist infinitely many real quadratic fields $K$ such that $C_K$ contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ (for $n = 3$ by Yamamoto [11, Part II], for $n = 5$ or 7 by Mestre [4]). We note that a stronger result for $n = 3$ was obtained by Craig [2]. Our third result is a relative version of the above result for $n = 3$ (Theorem 3).

The author wishes to express his gratitude to Professor Yasuo Morita for his continuous encouragement.

Statement of the results.

THEOREM 1. Let $F$ be a number field of finite degree with $r_z = 0$ or 1, where $r_z$ is the number of imaginary primes of $F$. Then for any
integer $n > 1$, there exist infinitely many quadratic extensions $K/F$ with the following properties:

(i) the number of real primes of $F$ decomposed in $K$ is 1 or 0 according as $r_2 = 0$ or 1,

(ii) the ideal class group of $K$ contains a subgroup $H$ which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and satisfies $N_{K/F}(H) = 1$, where $N_{K/F}$ is the norm map of the ideal class group of $K$ to that of $F$.

**Theorem 2.** Let $F$ be a quadratic field, $m$ be an odd prime number and $n$ be an integer with $n > 1$. Then there exist infinitely many extensions $K/F$ of degree $m$ with the following properties:

(i) both of the infinite primes of $F$ are decomposed into one real and $(m - 1)/2$ imaginary primes in $K$ if $F$ is real,

(ii) the ideal class group of $K$ contains a subgroup $H$ which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and satisfies $N_{K/F}(H) = 1$.

**Theorem 3.** Let $F$ be a number field of finite degree and let $S$ be a set of real primes of $F$ ($S$ may be empty). Then there exist infinitely many quadratic extensions $K/F$ with the following properties:

(i) a real prime of $F$ is ramified in $K$ if and only if it belongs to $S$,

(ii) the ideal class group of $K$ contains a subgroup $H$ which is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$ and satisfies $N_{K/F}(H) = 1$.

**Remark.** We can impose the following additional condition on $K$ in the above three theorems:

(iii) for any proper subfield $F'$ of $F$, $K$ is not a composition of $F$ with any extension of degree $m$ over $F'$ ($m = [K:F]$).

**Notation.** As usual, we denote by $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ the ring of rational integers, the rational number field and the real number field, respectively. For a field $k$, denote by $k^*$ the multiplicative group of $k$. For a number field $k$ of finite degree, denote by $\mathcal{O}_k$, $C_k$, $E_k$ and $W_k$ the ring of integers of $k$, the ideal class group of $k$, the group of units of $k$ and the group of roots of unity contained in $k$, respectively. For a prime ideal $\mathfrak{p}$ of $k$, denote by $N\mathfrak{p}$ the absolute norm of $\mathfrak{p}$. If $N\mathfrak{p}$ is congruent to 1 modulo a natural number $\nu$, denote by $\left(\frac{x}{\mathfrak{p}}\right)_\nu$ the $\nu$-th power residue symbol, that is,

$$\left(\frac{x}{\mathfrak{p}}\right)_\nu = x^{(N\mathfrak{p} - 1)/\nu} \mod \mathfrak{p} \in (\mathcal{O}_k/\mathfrak{p})^*$$

for any integer $x$ of $k$ prime to $\mathfrak{p}$. For a natural number $n$, $\zeta_n$ means a primitive $n$-th root of unity.
1. Some lemmas. Let $F$ be a number field of finite degree, $m$ be a prime number and $n$ be a natural number greater than 1. Let $\mathcal{L}$ be the set of all prime numbers dividing $n$. We fix $F$, $m$ and $n$ throughout this section. We begin with the following lemma which is easily deduced from the theorem on elementary divisors.

Lemma 1. Let $K/F$ be an extension of degree $m$ satisfying (i) $W_K = W_F$ and (ii) $K \subset F(\zeta_m, E_F^{1/m})$. Then a system of fundamental units of $F$ is extended to that of $K$.

The second lemma is a relative version of [7, Lemma 1]. Using Lemma 1 above, it is proved by the same argument as in the proof of [7, Lemma 1].

Lemma 2. Let $K/F$ be an extension of degree $m$ satisfying the assumptions in Lemma 1. Let $R$ and $r$ be the $\mathbb{Z}$-rank of $E_K$ and $E_F$, respectively. Suppose that there exist $\alpha_1, \ldots, \alpha_s \in K^*$ ($s > R - r$) satisfying the following conditions:

(i) $(\alpha_i) = a_i^* \text{ for some ideal } a_i \text{ of } K \text{ such that } N_{K/F}a_i \text{ is a principal ideal of } F$ ($1 \leq i \leq s$),

(ii) $\alpha_1, \ldots, \alpha_s$ are independent in $K^*/E_FK^*$ for all $l \in \mathcal{L}$.

Then $C_K$ contains a subgroup $H$ which is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{s-R+r}$ and satisfies $N_{K/F}(H) = 1$.

We must have $m - (R - r) > 0$ so that we can apply the above lemma with $s = m$. It is easy to see that this occurs only in the following four cases (under the assumption that $m$ is a prime):

(a) $m = 2$, $F$ is totally real and $K$ is totally imaginary,

(b) $m = 2$, $F$ and $K$ are as in Theorem 1,

(c) $m \geq 3$, $F = \mathbb{Q}$ and $K$ is arbitrary,

(d) $m \geq 3$, $F$ is a quadratic field and $K$ is as in Theorem 2.

The cases (a) and (c) were discussed by Naito and by Nakano, respectively. We discuss the case (b) in §2, the case (d) in §3. We note that $m - (R - r) = 1$ in both cases.

We shall consider a number of congruence conditions in the proof of our theorems. The next lemma will be often used for the existence of integers of $F$ satisfying such congruence conditions.

Lemma 3. Let $F_q$ be the finite field with $q$ elements. Let $d$ be an integer with $d \geq 2$ and $g(X) \in F_q[X]$ be a polynomial of degree $n \geq 1$. Suppose that $Y^d - g(X)$ is absolutely irreducible. Put

$N = \sharp\{(x, y) \in F_q \times F_q; y^d = g(x)\},$

$N_1 = \#\{x \in F_q; g(x) = y^d \text{ for some } y \in F_q^*\},$

$N_2 = \#\{x \in F_q; g(x) \neq y^d \text{ for any } y \in F_q\}.$
where \#A means the cardinality of a finite set A. Then we have
\[ |N - q| \leq (d - 1)(n - 1)q^{1/2}. \]

If \( d \) divides \( q - 1 \), then we have
\[ N_1 \geq \frac{q}{d} - (2n - 1)q^{1/2}, \]
\[ N_2 \geq (d - 1)q/d - (2n - 1)q^{1/2}. \]

**Proof.** The first inequality is a special case of Weil's famous theorem (the "Riemann Hypothesis for Curves over Finite Fields"). See [8, Chapter I, Theorem 2A] and [8, Chapter II, §11]. Let \( N_0 \) be the number of \( x \in F_q \) with \( g(x) = 0 \), and assume \( d \mid (q - 1) \). Then we have \( N_0 + N_1 + N_2 = q \), \( N_0 + dN_1 = N \), and \( 0 \leq N_0 \leq n \). Hence the second and third inequalities follow from the first one. q.e.d.

**Remark.** (i) If \( (d, n) = 1 \) or \( g(X) \) has a simple root, then \( Y^d - g(X) \) is absolutely irreducible (cf. [8, p. 11]).

(ii) By Lemma 3, we have \( N_1 \geq 0 \) and \( N_2 \geq 0 \) if \( q \geq 0 \).

We use Lemma 3 in this form in our later applications.

2. **Proof of Theorem 1.** Let \( F \), \( n \) and \( \mathcal{L} \) be as in §1 and let \( m = 2 \). Further we assume that \( F \) has at most one imaginary prime. Following Yamamoto [11], we consider the Diophantine equation
\[ x_1^2 - 4z_1^n = x_2^2 - 4z_2^n \]
and a solution in \( \mathcal{D}_F \) of the form
\[ x_1 = 2t^n + \frac{(t - a)^n - (t - b)^n}{2}, \]
\[ x_2 = 2t^n - \frac{(t - a)^n - (t - b)^n}{2}, \]
\[ z_1 = t(t - a), \]
\[ z_2 = t(t - b), \quad (a, b, t \in \mathcal{D}_F, a \equiv b \mod 2\mathcal{D}_F). \]

Put \( D = x_1^2 - 4z_1^n = x_2^2 - 4z_2^n \), \( K = F(\sqrt{D}) \) and \( \alpha_i = \frac{x_i + \sqrt{D}}{2} (i = 1, 2) \).

We impose some appropriate conditions on \( a \), \( b \), and \( t \) so that \( \alpha_i \), \( \alpha_i \) satisfy the conditions (i) and (ii) in Lemma 2. For each \( l \in \mathcal{L} \), take two prime ideals \( p_{i,l} \) and \( p_{i,l} \) of \( F \) which split completely in \( F(\zeta_l, 2^{1/l}, E_{1/l}^{1/l}) \). There are infinitely many such prime ideals by Tchebotarev's density theorem. We therefore assume that \( p_{i,l} \) (\( i = 1, 2, l \in \mathcal{L} \)) are all distinct, prime to \( 6n \) and have sufficiently large absolute norms. By the choice of \( p_{i,l} \), we have
\[ Np_{i,l} = 1 \mod l, \]
\[ \left( \frac{\varepsilon}{p_{i,l}} \right) = 1, \quad \left( \frac{2}{p_{i,l}} \right) = 1 \quad (i = 1, 2, l \in \mathcal{L}, \varepsilon \in E_{1/l}). \]
Take two integers $a$, $b$ of $F$ satisfying

\[ a \not\equiv -b \mod 2\mathcal{O}_F, \quad a \equiv 0 \mod 3\mathcal{O}_F, \quad a \equiv b \mod 5\mathcal{O}_F, \]
\[ 2a^n - (a - b)^n/2 \text{ is an } l\text{-th power non-residue mod } p_{i,l}, \]
\[ 2b^n - (a - b)^n/2 \text{ is an } l\text{-th power non-residue mod } p_{i,l}, \]
\[ a \equiv 0 \mod p_{i,l}, \quad b \equiv 0 \mod p_{i,l} \quad (l \in \mathcal{L}). \]

The existence of such integers $a$, $b$ is observed as follows. For each $p_{i,l}$, take any $a \not\equiv 0 \mod p_{i,l}$ and apply Lemma 3 to the case $d = l$, $g(X) = 2a^n - (a - X)^n/2 \mod p_{i,l}$. Then the third inequality of the lemma shows the existence of such $b \mod p_{i,l}$. For each $p_{i,l}$, repeat the same argument exchanging $a$ and $b$.

We fix such $a, b \in \mathcal{O}_F$ and take an integer $t$ of $F$ satisfying

\[ t \equiv a \mod p_{i,l}, \quad t \equiv b \mod p_{i,l} \quad (l \in \mathcal{L}), \]
\[ (t, a^n - b^n) = 1, \]
\[ (t - a, 2a^n - (a - b)^n/2) = 1, \]
\[ (t - b, 2b^n - (b - a)^n/2) = 1. \]

Then the integers $x_i, z_i$ ($i = 1, 2$) of $F$ defined by (2) satisfy

\[ (x_i, z_i) = 1, \quad p_{i,l} | z_i \quad (i = 1, 2), \]
\[ x_i \text{ is an } l\text{-th power non-residue mod } p_{i,l} \quad (i = 1, 2), \]
\[ (x_1 + x_2)/2 \text{ is a non-zero } l\text{-th power residue mod } p_{i,l} \quad (l \in \mathcal{L}). \]

Now we assume that $K$ is a quadratic extension of $F$ satisfying the condition (i) in Theorem 1, $W_K = W_F$ and $K \not\subset F(E^{1/2}_F)$. Then it follows from (3) and (6) that $\alpha_1, \alpha_2$ satisfy the conditions (i) and (ii) in Lemma 2 by the same argument as in the proof of [11, Proposition 2]. Hence $C_K$ has a subgroup $H$ which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and satisfies $N_{K/F}(H) = 1$, by Lemma 2.

Now we ensure the above assumptions by imposing further conditions on $t$. We note that $D = D(t)$ is a polynomial in $\mathcal{O}_F[t]$ of the form

\[ D(t) = 2n(a + b)t^{2n-1} + \text{ (terms with lower degrees in } t) \].

Put

\[ c = (6n)(a + b)(a^n - b^n)(2a^n - (a - b)^n/2)(2b^n - (b - a)^n/2) \prod_{l \in \mathcal{L}} p_{i,l}p_{t,l}. \]

Take a prime ideal $q$ of $F$ which splits completely in $F(E^{1/2}_F)$, is prime to $c$ and has a sufficiently large absolute norm. Since $2n(a + b)$ is prime to $q$, $D(t) \mod q$ has degree $2n - 1$ and $Y^2 - D(X) \mod q$ is absolutely irreducible by the remark after Lemma 3. Applying Lemma 3 to the case $d = 2$,
\(g(X) = D(X) \mod q\), \(D(t)\) is a quadratic non-residue \(\mod q\) for a suitable choice of \(t \mod q\). Then \(D \in F^{\times 2}\) and \(K = F(\sqrt{D})\) is a quadratic extension of \(F\). Moreover \(K\) is not contained in \(F(E_{1/2}^{2})\), since \(q\) remains prime in \(K\) while \(q\) splits completely in \(F(E_{1/2}^{2})\). Since \(D\) is a polynomial in \(t\) of odd degree, the condition (i) in Theorem 1 is satisfied by a suitable choice of the signs of \(t\) and sufficiently large absolute values of \(t\) (for the real primes of \(F\)). If \(F = Q\), then \(K\) is a real quadratic field, hence \(W_{K} = W_{F} = \{\pm 1\}\). If \(F \neq Q\), then we take a sufficiently large prime number \(p\) which splits completely in \(F\) and is prime to \(cq\). Let \(p_{j} (1 \leq j \leq [F: Q])\) be the prime ideals of \(F\) lying above \(p\). Applying Lemma 3 again, we see that \(D(t)\) is a quadratic non-residue \(\mod p_{j}\) and is a non-zero quadratic residue \(\mod p_{j} (2 \leq j \leq [F: Q])\) for a suitable choice of \(t \mod pDF\). Then it is easy to see that \(W_{K} = W_{F}\) and \(K\) does not come from any quadratic extension of any proper subfield of \(F\).

It remains only to show the existence of infinitely many quadratic extensions \(K/F\) with the properties in the theorem. We claim that \(K = F(\sqrt{D(t)})\) represents infinitely many such quadratic extensions as \(t\) takes infinitely many values in \(DF\) satisfying all the above conditions (for fixed \(a, b\)). Suppose \(K_{1}, \ldots, K_{s}\) are such quadratic extensions. Take a prime ideal \(\tau\) of \(F\) which splits completely in the composition \(K_{1} \cdots K_{s}\) and has a sufficiently large absolute norm. By Lemma 3, we can choose \(t\) so that \(\tau\) remains prime in \(K\) and \(K\) has the properties in the theorem. Then \(K\) is not contained in \(K_{1} \cdots K_{s}\). This proves our claim, and the proof of Theorem 1 is completed.

3. Proof of Theorem 2. We fix a quadratic field \(F\), an odd prime number \(m\) and a natural number \(n > 1\). Let \(\mathcal{L}\) be the set of all prime numbers dividing \(n\). We denote by \(\tau\) the non-trivial automorphism of \(F\). If \(F\) is a real quadratic field, we fix an embedding of \(F\) into \(R\). The following lemma is a relative version of [7, Lemma 2] and is proved similarly.

**Lemma 4.** Let \(f(X) \in \mathcal{O}_{F}[X]\) be a monic irreducible polynomial of degree \(m\), \(\theta\) be a root of \(f(X)\) and put \(K = F(\theta)\). Suppose there exist prime ideals \(p_{i,i}\) of \(F\) with \(Np_{i,i} \equiv 1 \mod l (1 \leq i \leq m, l \in \mathcal{L})\) and integers \(A_{j}, C_{j} (1 \leq j \leq m)\) of \(F\) such that

(i) \(f(A_{j}) = C_{j} (1 \leq j \leq m)\),

(ii) \((f'(A_{j}), C_{j}) = 1 (1 \leq j \leq m, l \in \mathcal{L})\),

(iii) \(f(0) \equiv 0, f'(0) \equiv 0 \mod p_{i,i} (1 \leq i \leq m, l \in \mathcal{L})\),

(iv) \(\left(\frac{A_{j}}{p_{i,i}}\right)_{l} = 1, \left(\frac{A_{j}}{p_{i,i}}\right)_{l} \neq 1 (1 \leq j < i \leq m, l \in \mathcal{L})\),
\( (v) \) \( \left( \frac{\epsilon}{\mathfrak{p}_{i,l}} \right) = 1 \) \( (\epsilon \in E_r, \ 1 \leq i \leq m, \ \ell \in \mathfrak{L}) \),

where \( f'(X) \) is the derivative of \( f(X) \). Then the \( m \) elements \( \alpha_j = \theta - A_j \) \( (1 \leq j \leq m) \) satisfy the conditions (i), (ii) in Lemma 2.

Following Nakano [7], we try to use a polynomial \( f(X) \) which is defined by

\[
(*) \quad f(X) = \prod_{j=0}^{m-1} (X - A_j) + C^n \ (A_j, C \in \mathfrak{O}_F)
\]

and satisfies

\[
(**) \quad f(A_m) = D^n \text{ for some } A_m, D \in \mathfrak{O}_F.
\]

The following lemma is deduced from Lemmas 2 and 4.

**Lemma 5.** If there exist prime ideals \( \mathfrak{p}_{i,l} \) of \( F \) with \( N\mathfrak{p}_{i,l} \equiv 1 \mod \ell \) \( (1 \leq i \leq m, \ \ell \in \mathfrak{L}) \) and integers \( A_j \) \( (0 \leq j \leq m) \), \( C, D \) of \( F \) satisfying the following conditions (C.1) through (C.11), then \( K = F(\theta) \) is an extension of degree \( m \) over \( F \) with the three properties (i), (ii), (iii) in Theorem 2, where \( f(X) \) is defined by (\( * \)) and \( \theta \) is a root of \( f(X) \).

(C.1) \( \prod_{j=0}^{m-1} (A_m - A_j) = D^n - C^n. \)

(C.2) \( \prod_{j=0}^{m-1} (-A_j) + C^n \equiv 0 \mod \mathfrak{p}_{i,l} \) \( (1 \leq i \leq m, \ \ell \in \mathfrak{L}) \).

(C.3) \( \left( \sum_{k=0}^{m-1} \prod_{0 \leq j \leq m-1, j \neq k} A_j, \prod_{l \in \mathfrak{L}} \prod_{1 \leq i \leq m} \mathfrak{p}_{i,l} \right) = 1. \)

(C.4) \( \left( \frac{A_j}{\mathfrak{p}_{i,l}} \right) = 1, \ \left( \frac{A_j}{\mathfrak{p}_{i,l}} \right) \neq 1 \) \( (1 \leq j < i \leq m, \ \ell \in \mathfrak{L}) \).

(C.5) \( \left( \frac{\epsilon}{\mathfrak{p}_{i,l}} \right) = 1 \) \( (\epsilon \in E_r, \ 1 \leq i \leq m, \ \ell \in \mathfrak{L}) \).

(C.6) \( (A_k - A_j, C) = 1 \) \( (1 \leq j < k \leq m - 1) \).

(C.7) \( \left( \sum_{k=0}^{m-1} \prod_{0 \leq j \leq m-1, j \neq k} (A_m - A_j), D \right) = 1. \)

(C.8) \( f(X) \) is irreducible over \( F \).

(C.9) \( K \) is not a composition of \( F \) with any extension of degree \( m \) over \( \mathbb{Q} \).

If \( F \) is a real quadratic field, we add the following two conditions.

(C.10) \( K \nmid F(\zeta_m, \eta^{1/m}) \), where \( \eta \) is a fundamental unit of \( F \).

(C.11) both \( f(X) \) and \( f'(X) \) have just one real root.

**Remark.** The conditions (C.8) and (C.9) imply \( W_K = W_F \), since \( m \) is an odd prime number.

First we must consider the global condition (C.1) which is viewed as
a Diophantine equation. We use the following solution of (C.1) in \( \mathcal{O}_F \)
which is different from Nakano's and has a simpler form.

\[
\begin{align*}
A_0 &= w^n - 1 + (t - u)^n - (t - v)^n, \\
A_j &= w^n - 1 - (t - a_j)^n \quad (1 \leq j \leq m - 1), \\
A_m &= w^n - 1, \\
C &= (t - u) \prod_{j=1}^{m-1} (t - a_j), \\
D &= (t - v) \prod_{j=1}^{m-1} (t - a_j) \quad (a_j, t, u, v, w \in \mathcal{O}_F).
\end{align*}
\]

For each \( l \in \mathcal{L} \), take \( m \) distinct prime ideals \( \mathfrak{p}_{i,l} \) \((1 \leq i \leq m)\) of \( F \)
which split completely in \( F(\zeta_l, E_{j/l}) \). We may assume that \( \mathfrak{p}_{i,l} \) \((1 \leq i \leq m, l \in \mathcal{L})\) are all distinct, prime to \( n \) and have sufficiently large absolute norms. In particular, we may assume \( N\mathfrak{p}_{i,l} > m + 1 \). Then the condition (C.5) is satisfied.

Now we impose some congruence conditions modulo \( \mathfrak{p}_{i,l} \) on \( a_j, t, u, v \)
and \( w \) so that the conditions (C.2), (C.3) and (C.4) are satisfied. Take an
integer \( w \) of \( F \) satisfying

\[
\begin{align*}
wn - 1 & \text{ is an \( l \)-th power non-residue mod } \mathfrak{p}_{m,l} \quad (l \in \mathcal{L}), \\
w(w^{n(m-1)} - 1) & \equiv 0 \mod \mathfrak{p}_{i,l} \quad (1 \leq i \leq m, l \in \mathcal{L}).
\end{align*}
\]

The existence of such \( w \) is guaranteed by Lemma 3 (apply the lemma to the case \( d = l, g(X) = X^n - 1 \mod \mathfrak{p}_{m,l} \)). Next we take integers \( a_j \) \((1 \leq j \leq m - 1)\) of \( F \) satisfying

\[
\begin{align*}
a_j & \equiv 0 \mod \mathfrak{p}_{i,l} \quad (1 \leq i \leq m, 1 \leq j \leq m - 1, j \neq i, l \in \mathcal{L}), \\
w^n - 1 - (w - a_j)^n & \text{ is an \( l \)-th power non-residue mod } \mathfrak{p}_{i,l}, \\
(w - a_i)(w^{n(m-2)} - 1) + w^n - 1 & \not\equiv 0 \mod \mathfrak{p}_{i,l}, \\
a_i & \equiv w \mod \mathfrak{p}_{i,l} \quad (1 \leq i \leq m - 1, l \in \mathcal{L}).
\end{align*}
\]

The existence of such \( a_j \)'s is also guaranteed by Lemma 3 (apply the lemma to the case \( d = l, g(X) = w^n - 1 - (w - X)^n \mod \mathfrak{p}_{m,l} \)). Take an
integer \( t \) of \( F \) satisfying

\[
(10) \quad t \equiv w \mod \mathfrak{p}_{i,l} \quad (1 \leq i \leq m, l \in \mathcal{L}).
\]

In view of (7), (9) and (10), we have

\[
\begin{align*}
A_i & \equiv -1 \mod \mathfrak{p}_{i,l} \quad (1 \leq i \leq m, 1 \leq j \leq m - 1, j \neq i, l \in \mathcal{L}), \\
A_i & \equiv w^n - 1 - (w - a_i)^n \mod \mathfrak{p}_{i,l} \quad (1 \leq i \leq m - 1, l \in \mathcal{L}).
\end{align*}
\]

Then it follows from (8), (9) and (11) that (C.4) is satisfied. Put
\[ b_i = (w - a_i)^n(w^{n(m-2)} - 1) + w^n - 1, \]
\[ c_i = w^{n(m-1)}(w - a_i)^n(1 - (m - 2)A_i). \]

Take two integers \( u, v \) of \( F \) satisfying
\[
(w - v)^n \equiv (1 - w^{n(m-1)})(w - u)^n + w^n - 1 \mod p_{m,l},
\]
\[
(m - 1)w^{n(m-1)}(w - u)^n \not\equiv 1 \mod p_{m,l} \quad (l \in \mathcal{L}),
\]
\[
A_i(w - v)^n \equiv b_i(w - u)^n + A_i(w^n - 1) \mod p_{i,l},
\]
\[
u \not\equiv w, \quad v \not\equiv w \mod p_{i,l},\]
\[
c_i(w - u)^n \not\equiv A_i \mod p_{i,l} \quad (1 \leq i \leq m - 1, l \in \mathcal{L}).
\]

In view of (8), (9) and (11), we have
\[
(1 - w^{n(m-1)})(w^n - 1) \equiv 0 \mod p_{m,l} \quad (l \in \mathcal{L}),
\]
\[b_i A_i(w^n - 1) \equiv 0 \mod p_{i,l} \quad (1 \leq i \leq m - 1, l \in \mathcal{L}).\]

Hence the existence of such \( u, v \) is also guaranteed by Lemma 3. Then it follows from (7), (10), (11) and (12) that (C.2) and (C.3) are satisfied.

Now we consider the conditions (C.8), (C.9) and (C.10). Put
\[ f_0(X) = X^m - mX^{m-1} + 1 \in \mathbb{Q}[X]. \]

Since \((X - 1)^m f_0(1/(X - 1)) = X^m - mX^{m-1} + \cdots + m\) is an Eisenstein polynomial with respect to \( m \), \( f_0(X) \) is irreducible over \( \mathbb{Q} \), hence over \( F \). Let \( \theta_0 \) be a root of \( f_0(X) \) and put \( K_0 = F(\theta_0) \). If \( F \) is imaginary, take a prime ideal \( q \) of \( F \) which remains prime in \( K_0 \). Since \( m \) is a prime number, there exist infinitely many such prime ideals by the density theorem. If \( F \) is real, we have \( K_0 \cap F(\zeta_m, \gamma/m) = F \) since \( f_0(X) \) has just three real roots. Hence we can take a prime ideal \( q \) of \( F \) which remains prime in \( K_0 \) and splits in \( F(\zeta_m, \gamma/m) \) by the density theorem. We may assume in both cases that \( q \not\equiv q^* \), \( N_q \) is prime to \((n) \prod p_{i,l} \) and \( N_q \) is sufficiently large. We may also assume that \( q \) is prime to the discriminant of \( f_0(X) \). Then \( f_0(X) \mod q \) is irreducible, and \( X^m - \gamma \mod q \) is not if \( F \) is real. We impose the following condition on \( a_j \)'s.
\[(13) \quad a_j \equiv 0 \mod qq^* \quad (1 \leq j \leq m - 1). \]

Further we impose the following conditions on \( u, v \) and \( w \).
\[(14) \quad v \not\equiv w \mod q,
\]
\[(w - u)w^{m-1} \equiv 1 \mod q,
\]
\[w(w^{n(m-1)} - 1) \not\equiv 0 \mod q^*,
\]
\[(w - v)^n + (w^{n(m-1)} - 1)(w - u)^n \equiv w^n - 1 \mod q^*,
\]
\[(15) \quad u \not\equiv w, \quad v \not\equiv w \mod q^*,
\]
\[(m - 1)w^{n(m-1)}(w - u)^n \not\equiv 1 \mod q^*.\]
The existence of such \( u, v, w \mod q^r \) is guaranteed by Lemma 3. If \( t \) satisfies

\[(16) \quad t \equiv w \mod q^r,\]

then it follows from (7) and (13) that

\[
\begin{align*}
A_j &\equiv -1 \mod q^r \quad (1 \leq j \leq m - 1), \\
A_0 &\equiv w^n - 1 + (w - u)^n - (w - v)^n \mod q^r, \\
C &\equiv (w - u)w^{m-1} \mod q^r.
\end{align*}
\]

Hence we obtain

\[(17) \quad f(X-1) \equiv \{X - w^n - (w - u)^n + (w - v)^n\}X^{m-1} + w^{n(m-1)}(w - u)^n \mod q^r.\]

In view of (14) and (17), we have \( f(X - 1) \equiv f_0(X) \mod q \). Hence \( f(X) \) is irreducible over \( F' \), that is, the condition (C.8) is satisfied. In case \( F \) is real, \( f(X) \mod q \) is irreducible while \( X^m - \gamma \mod q \) is not. Hence (C.10) is satisfied. In view of (15) and (17), we have \( f(0) \equiv 0, f'(0) \not\equiv 0 \mod q^r. \) Hence \( q^r \) splits in \( K \) while \( q \) remains prime in \( K \). Hence (C.9) is satisfied.

Now we consider the conditions (C.6) and (C.7). We impose the following condition on \( a_j's, u \) and \( v \).

\[(18) \quad u \equiv v \equiv a_i \equiv \cdots \equiv a_{m-1} \equiv 0 \mod p\]

for all prime ideals \( p \) of \( F \) with \( Np \leq m + 1. \) This condition is consistent with the other ones, since \( Np_i, i \) and \( Nq \) are sufficiently large. If \( t \) satisfies (10) and (16), then it follows from (8), (9), (12), (14) and (15) that \( CD \) is prime to \( q^r \prod p_i, \). Now we fix \( u, v, w \) and \( a_j's \) satisfying (8), (9), (12) through (15) and (18). Then \( f'(A_j) \) is a polynomial in \( t \), so we write it as \( f'(A_j)(t) \quad (1 \leq j \leq m). \) It is clear that there exist infinitely many \( t \in \mathcal{O}_F \) satisfying (10), (16) and the following condition (19).

\[
\begin{align*}
(t - u, f'(A_j)(u)) &= 1 \quad (1 \leq j \leq m - 1), \\
(t - v, f'(A_j)(v)) &= 1, \\
(t - a_i, f'(A_j)(a_i)) &= 1 \quad (1 \leq i \leq m - 1, 1 \leq j \leq m).
\end{align*}
\]

If \( t \) satisfies (10), (16) and (19), then the conditions (C.6) and (C.7) are satisfied.

It remains only to ensure the condition (C.11) in case \( F \) is real. We claim that (C.11) is satisfied if \( t \) and \( t' \) are sufficiently large. In general, we consider a polynomial \( h(X) \in R[X] \) defined by

\[h(X) = \prod_{j=0}^{m-1} (X - B_j) + L \quad (B_j, L \in R).\]

We may assume \( B_0 \leq B_1 \leq \cdots \leq B_{m-1}. \) Since \( m \) is odd, we see from the
graph of $Y = h(X)$ that $h(X)$ has just one real root if the following inequality holds.

\[(20) \quad \text{Max} \left\{ \prod_{j=0}^{m-1} |x - B_j|; B_0 \leq x \leq B_{m-1} \right\} < |L|.
\]

If $B_k \leq x \leq B_{k+1}$, then we have

\[|x - B_k||x - B_{k+1}| \leq |B_{k+1} - B_k|^2/4.
\]

This inequality and trivial estimates yield

\[(21) \quad \text{Max} \left\{ \prod_{j=0}^{m-1} |x - B_j|; B_0 \leq x \leq B_{m-1} \right\} \leq |B_{m-1} - B_0|^m/4.
\]

We return to our case. In view of (7), we see that $A_0$ is a polynomial in $t$ of degree $n - 1$, $A_j$ ($1 \leq j \leq m - 1$) are of degree $n$ with leading coefficient $-1$ and $C$ is monic of degree $m$. Hence we have

\[(22) \quad \lim_{t \to 0} \left( \text{Max}_{0 \leq j \leq m-1} A_j \right)^{m/|C|} = 1.
\]

The same holds if we replace $A_j$, $C$ and $t$ by their conjugates. If we let $t$ and $t^*$ be sufficiently large, then the inequality (20) holds for $h(X) = f(X)$, $f^*(X)$ by (21) and (22). This proves our claim.

We have just proved the existence of at least one extension $K/F$ of degree $m$ satisfying (C.1) through (C.11) for any given natural number $n$. By Lemma 5, such a $K/F$ has the properties in Theorem 2. Then there exist infinitely many such extensions because of the finiteness of class numbers. This completes the proof of Theorem 2.

4. Proof of Theorem 3. Let $F$ be a given number field of finite degree. We prove Theorem 3 by the same method as in the proof of [11, Part II, Theorem 2]. We need the following lemma.

**Lemma 6.** Let $a$, $b$ be integers of $F$ such that $f(X) = X^3 - ax + b$ is irreducible over $F$. Let $L$ be the splitting field of $f(X)$ over $F$ and put $D = 4a^3 - 27b^2$, $K = F(\sqrt[3]{D})$. If $(a, 3b) = 1$ and $D \not\in F^{*2}$, then $L/K$ is an unramified cyclic extension of degree 3 and $\text{Gal}(L/F)$ is isomorphic to the symmetric group $S_3$ of degree 3.

This lemma is well-known. For example, see Honda [3]. Put

\[
\begin{align*}
  a_1 &= t^3 + 9t \\
  a_2 &= t^3 - 9t \\
  b_1 &= t^4 + 2t^3 + 27, \\
  b_2 &= t^4 - 2t^3 + 27
\end{align*}
\]

$t \in \mathbb{C}_F$.

For $i = 1, 2$ set $f_i(X, t) = X^3 - a_i X + b_i$. Then the two polynomials $f_i(X, t)$ and $f_3(X, t)$ have the common discriminant

\[D(t) = 2t^6 - 3t^4 + 2t^2 + 27t^2 - 2 \cdot 3t^4 - 3.
\]
By a simple computation, we see that $D(t)$ has no multiple roots as a polynomial in $t$. Hence the affine curve $Y^2 = D(X)$ has genus 4.

Let $t_0$ be a rational integer satisfying

$$t_0 \equiv 1 \mod 3, \quad t_0 \equiv 0 \text{ or } 4 \mod 5, \quad t_0 \equiv 3 \mod 7.$$

Then we have $D(t_0) \equiv 2$ or $3 \mod 5$. Hence $K_0 = \mathbb{Q}(\sqrt{D(t_0)})$ is a quadratic field. Further we have

$$f_1(X,t_0) \equiv X(X-1)(X-2) \mod 3,$$
$$f_1(X,t_0) \equiv X^3 - 5X + 1 \mod 7 \quad \text{(irreducible over } \mathbb{F}_7),$$
$$f_1(X,t_0) \equiv X^3 - X - 1 \mod 3 \quad \text{(irreducible over } \mathbb{F}_3).$$

Hence both $f_1(X,t_0)$ and $f_2(X,t_0)$ are irreducible over $\mathbb{Q}$ and have the Galois group isomorphic to $S_3$. Let $L_{i,0}$ be the splitting field of $f_i(X,t_0)$ over $\mathbb{Q}$ ($i = 1, 2$). Then we have $L_{1,0} \neq L_{2,0}$ by the above congruences. Hence $\text{Gal}(L_{1,0}/L_{2,0})$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$. Since the affine curve $Y^2 = D(X)$ has genus 4, there exist only a finite number of integral points on the curve in a fixed number field of finite degree by Siegel’s theorem (cf. [9]). Hence, for infinitely many values of $t_0$ satisfying (23), $K_0$ represents infinitely many quadratic fields. On the other hand, we see easily that a prime number $p$ is ramified in each subfield ($\neq \mathbb{Q}$) of $L_{1,0}L_{2,0}$ if $p$ is ramified in $K_0$. Hence we have $L_{1,0}L_{2,0} \cap F = \mathbb{Q}$ for a suitable choice of $t_0$. We fix such a $t_0$. By the density theorem, we can take two prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ of $F$ such that the decomposition field of $\mathfrak{p}_i$ for $L_{1,0}L_{2,0}F/\mathbb{F}$ is $L_{i,0}F$ ($i = 1, 2$). We may assume that $N\mathfrak{p}_i$ is prime to $D(t_0)$ ($i = 1, 2$). Then we have

$$f_i(X,t_0) \mod \mathfrak{p}_i \text{ splits completely},$$
$$f_i(X,t_0) \mod \mathfrak{p}_j \text{ is irreducible} \quad (i, j = 1, 2, \ i \neq j).$$

Take a sufficiently large prime number $q$ which splits completely in $F$ and is prime to $30N\mathfrak{p}_1N\mathfrak{p}_2$. Let $q_j$ ($1 \leq j \leq [F: \mathbb{Q}]$) be the prime ideals of $F'$ lying above $q$. By Lemma 3, we can take an integer $t$ of $F$ satisfying

$$D(t) \text{ is a quadratic non-residue mod } q_1,$$
$$D(t) \text{ is a non-zero quadratic residue mod } q_j \quad (2 \leq j \leq [F: \mathbb{Q}]),$$

$$t \equiv t_0 \mod \mathfrak{p}_1 \mathfrak{p}_2,$$
$$t \equiv 4 \mod 6\mathfrak{O}_F,$$
$$t - 1, 5 = 1.$$

Then $K = F(\sqrt{D(t)})$ is a quadratic extension of $F$. Moreover $K$ does not come from any quadratic extension of any proper subfield of $F$. Let $L_i$ be the splitting field of $f_i(X,t)$ over $F$ ($i = 1, 2$). In view of (24) and
We have
\[(25) \quad Gal(L_i/F) = S_3, \quad (a_i, 3b_i) = 1 \quad (i = 1, 2), \quad L_1 \neq L_2.\]

By Lemma 6 and class field theory, (26) implies that the 3-rank of \(C_K\) is greater than or equal to 2, where \(C_K = \text{Ker}(N_{K/F} : C_K \to C_F)\). Hence \(C_K\) has a subgroup \(H\) which is isomorphic to \((\mathbb{Z}/3\mathbb{Z})^2\) and satisfies \(N_{K/F}(H) = 1\).

Since \(D(t)\) is a polynomial in \(t\) of odd degree, the condition (i) in Theorem 3 is satisfied by a suitable choice of the signs of \(t\) and sufficiently large absolute values of \(t\) for the real primes of \(F\). Finally, since the affine curve \(Y^2 = D(X)\) has genus 4, for infinitely many values of \(t\) satisfying (25) and the above condition on the signs of \(D(t)\), \(K = F(\sqrt[3]{D(t)})\) represents infinitely many quadratic extensions with the properties in Theorem 3 by Siegel’s theorem. This completes the proof of Theorem 3.

**REFERENCES**


MATHEMATICAL INSTITUTE
Tohoku University
Sendai 980
Japan