OUKA
Osaka University Knowledge Archive

Title	On unramified Galois extensions of quadratic number fields
Author(s)	Yamamoto, Yoshihiko
Citation	Osaka Journal of Mathematics. 1970, 7(1), p. 57-76
Version Type	VoR
URL	https://doi.org/10.18910/10165
rights	
Note	

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

Yamamoto, Y.
Osaka J. Math.
7 (1970), 57-76

ON UNRAMIFIED GALOIS EXTENSIONS OF QUADRATIC NUMBER FIELDS

YOSHIHIKO YAMAMOTO

(Received September 8, 1969)

Introduction

Let n be a given natural number greater than 1. It was shown by several authors that there exist infinitely many imaginary quadratic number fields whose ideal class numbers are multiples of n (Nagel [9], Humbert [7], Ankeny and Chowla [1], Kuroda [8]). For real quadratic number fields, however, there seems to be no corresponding result except special cases $n=2^i$ ($i=1, 2, \cdots$) (Gauss [4]) and $n=3$ (Honda [6]).

In part I of this paper we show the infiniteness of the number of such real quadratic number fields for every natural number n (Corollary 1 of Theorem 2), by modifying the method used in [9]. At the same time we get an infinite number of imaginary quadratic number fields F each of which has a subgroup of order n^2 isomorphic to the direct product of two cyclic groups of order n in its ideal class group. Moreover we can impose certain conditions on the behaviour of finite number of primes in F. Our method is sketched as follows: In the first place, we construct a quadratic number field which has two ideal classes $\mathfrak{a}$, $\mathfrak{a}'$ and satisfies some local conditions on its discriminant D. In case $D<0$, both of them are of order n and independent. In case $D>0$, neither of them may be of order n because of the existence of non-trivial units but the subgroup $\langle \mathfrak{a}, \mathfrak{a}' \rangle$ generated by them contains at least an ideal class $\mathfrak{b}$ of order n. Next we show that such fields exist infinitely for either case, using the local conditions on D.

According to the class field theory, the ideal class group of a number field is closely related to the maximal unramified abelian extension of the field. In part II we study other types of unramified Galois extensions of quadratic number fields. First, as a special case of Hibert's irreducibility theorm, we construct (infinitely many) Galois extensions of the rational number field $\boldsymbol{Q}$ whose Galois groups are isomorphic to the symmetric group S_n of degree n and each of which is defined as a minimal splitting field of a trinomial equation

$$X^n+aX+b=0 \qquad (a, b \in \boldsymbol{Z}).$$

These fields are unramified over the quadratic number fields corresponding to

the alternating group A_n of degree n, under the condition $((n-1)a, nb)=1$ (Proposition 1). Then we get infinitely many imaginary (resp. real) quadratic number fields each of which has an unramified (resp. unramified at all finite prime spots) Galois extension with the Galois group isomorphic to A_n (called an A_n-extension in the following). This is a generalization of the result in Honda [6], where the case $n=3$ are treated. In the rest of this part, we study the cases of other types of unramified Galois extensions, the dihedral group D_n and the symmetric group S_n, for instance.

The author wishes to express his sincere gratitude to Professor Y. Akagawa and Professor T. Honda for their valuable suggestions. He also wishes to thank Professor H. Nagao and Professor Y. Nakai for their continuous encouragement.

PART I

1. Let n be a natural number. We fix n throughout this part. Denote by $\boldsymbol{Z}$ and $\boldsymbol{Q}$ the ring of rational integers and the rational number field respectively. Let F be a quadratic number field with discriminant D, we assume $D\neq -3$ or -4 in order to simplify our argument in the following, and σ be the non-trivial automorphism of F over $\boldsymbol{Q}$. Define ε by

$$\varepsilon=\begin{cases}\text{a fundamental unit of } F & \text{if } D>0,\\ 1 & \text{if } D<-4.\end{cases}$$

Lemma 1. *Let x, y, z be a solution in $\boldsymbol{Z}$ of the Diophantine equation*

$$X^2-Y^2D=4Z^n \tag{1}$$

satisfying $(x, z)=1$, then there exist an (integral) ideal $\mathfrak{a}$ in F such that

(a) $\left(\frac{x+y\sqrt{D}}{2}\right)=\mathfrak{a}^n$,

(b) $\mathfrak{a}$ *and* $\mathfrak{a}^\sigma$ *are relatively prime,*

where (α) means the principal ideal in F generated by an element α of F.

Proof. Set $\alpha=\frac{x+y\sqrt{D}}{2}$. It is an integer in F. It follows from (1) that $\alpha+\alpha^\sigma=x$ and $\alpha\alpha^\sigma=z^n$. We have $(\alpha)(\alpha^\sigma)=(z)^n$. On the other hand, we have $(\alpha, \alpha^\sigma)=1$, since $(\alpha, \alpha^\sigma)\ni x, z^n$ and $(x, z)=1$. Decomposing the ideal (z) into the product of prime ideals in F, we get easily that $(\alpha)=\mathfrak{a}^n$ for a suitable integral ideal $\mathfrak{a}$. Condition (b) follows from $(\alpha, \alpha^\sigma)=1$.

2. Let p be a prime factor of n. Take another prime number l such that

$$l\equiv 1 \quad \begin{cases}(\text{mod. } p) & \text{if } p\neq 2,\\ (\text{mod. } 4) & \text{if } p=2.\end{cases} \tag{2}$$

It follows from (2) that -1 is a p-th power residue mod. l.

Suppose we have a solution x, y, z of the Diophantine equation (1) satisfying

(i) $(x, z)=1$,
(ii) $l \mid z$,
(iii) x is a p-th power non-residue mod. l.

We get $\left(\frac{D}{l}\right)=1$ from (1) and condition (i), where the left side is the Kronecker symbol. By the decomposition law of primes we have $l=\mathfrak{r}\mathfrak{r}^{\sigma}$ where $\mathfrak{r}$ and $\mathfrak{r}^{\sigma}$ are conjugate prime ideals in F different from each other. Put $\alpha=\frac{x+y\sqrt{D}}{2}$. We have $\mathfrak{r}\mathfrak{r}^{\sigma} \mid (\alpha)(\alpha^{\sigma})$, hence we may assume $\mathfrak{r} \mid (\alpha^{\sigma})$ but $\mathfrak{r} \nmid (\alpha)$ since (α) and (α^{σ}) are relatively prime from Lemma 1. Then we have:

Lemma 2. *If $\mathfrak{E}$ is a p-th power residue mod. $\mathfrak{r}$, then ideal (α) is the p-th power of no principal ideal in F.*

Proof. Since $\alpha^{\sigma} \in \mathfrak{r}$, we get $x \equiv y\sqrt{D}$ (mod. $\mathfrak{r}$), hence $\alpha \equiv x$ (mod. $\mathfrak{r}$). Therefore α is a p-th power non-residue mod. $\mathfrak{r}$, because the residue class field mod. $\mathfrak{r}$ is canonically isomorphic to the prime field Z/lZ. Assume $(\alpha)=(\beta)^{p}$ with a principal ideal (β) in F. As α is an integer in F, β is also an integer in F. We have

$$\alpha = \pm \mathfrak{E}^{k} \beta^{p} \tag{3}$$

for some $k \in \boldsymbol{Z}$. So it follows from (3) and the assumption of the lemma α must be a p-th power residue mod. $\mathfrak{r}$. This is a contradiction. So we get our lemma.

REMARK. In case p=odd prime, Nagel [9] used the following condition (iv);

(iv) $p \| x$

in place of conditions (ii) and (iii).

3. Let

$$n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} \tag{4}$$

be the prime decomposition of n. For each i $(1 \leqq i \leqq s)$ we fix a prime number l_i satisfying

$$(2)' \qquad \begin{cases} l_i \equiv 1 \pmod{p_i} & \text{if } p_i \neq 2, \\ l_i \equiv 1 \pmod{4} & \text{if } p_i = 2. \end{cases}$$

Suppose we have a solution x, y, z of (1) satisfying

(i)′ $(x, z)=1$,
(ii)′ $l_i \mid z$ for $i=1, 2, \cdots, s$,
(iii)′ x is a p_i-th power non-residue mod. l_i for $i=1, 2, \cdots, s$.

Put $\alpha=\frac{x+y\sqrt{D}}{2}$. From Lemma 1 we have $(\alpha)=\mathfrak{a}^n$ with an ideal $\mathfrak{a}$ in F. It follows from §2 that every l_i is decomposed in F: $l_i=\mathfrak{r}_i\mathfrak{r}_i^{\sigma}$. Assume $\mathfrak{r}_i \mid (\alpha^{\sigma})$. Denote by $[\mathfrak{a}]$ the ideal class containing $\mathfrak{a}$. We have

$$[\mathfrak{a}]^n = [(\alpha)] = 1 .$$

Proposition 1. *Let notations and assumptions be as above. If ε is a p_i-th power residue mod. $\mathfrak{r}_i$ for every i $(1 \leqq i \leqq s)$, then the order of $[\mathfrak{a}]$ is equal to n.*

Proof. Assume $[\mathfrak{a}]^m=1$ for some m $(1 \leqq m<n)$. It is obvious that m is a divisor of n, so there exists at least a prime divisor p_i of n such that $mp_i \mid n$. Then $[\mathfrak{a}]^{n/p_i}=1$. So there exists an integer β in F such that $\mathfrak{a}^{n/p_i}=(\beta)$. Then $(\alpha)=\mathfrak{a}^n=(\beta)^{p_i}$. But this is impossible from Lemma 2. So we have $[\mathfrak{a}]^m \neq 1$ for $m=1, 2, \cdots, n-1$. Therefore the order of $[\mathfrak{a}]$ is equal to n.

REMARK. In case $D<-4$, we do not need the condition on ε in Lemma 2 or Proposition 1, since $\varepsilon=1$.

Theorem 1. *For given finite sets S_1, S_2, S_3 of prime numbers satisfying $S_i \cap S_j=\phi$ $(i \neq j)$, there exist infinitely many imaginary quadratic number fields F such that*

(a) *the ideal class group of F has a class of order n,*
(b) *all primes contained in S_i* $\begin{cases} \text{are decomposed in } F & (i=1), \\ \text{remain prime} \quad \text{,,} & (i=2), \\ \text{are ramified} \quad \text{,,} & (i=3). \end{cases}$

Proof. Let $F(S_1, S_2, S_3)$ be the set of all imaginary quadratic number fields which satisfy the conditions (a), (b). It is sufficient to prove the case $S_3-\{2, 3\} \neq \phi$. Fix a prime number l such that

$$(5) \qquad \begin{cases} l \equiv 1 \pmod{q} & \text{for } q \in S \cup S_2, \\ l \equiv 1 \pmod{q^2} & \text{for } q \in S_3 \cup \{2\}, \end{cases}$$

where S is the set of all prime factors of n. Let k be the product of all primes in S_1. Take a rational integer x satisfying

(i) x is a p_i-th power non-residue mod. l for $p_i \in S$,
(ii) $(x, k)=1$,
(iii) x^2-4 is a quadratic non-residue mod. q for $q \in S_2-\{2\}$ and x is odd if $2 \in S_2$,
(iv) $x \equiv q+2 \pmod{q^2}$ for $q \in S_3$.

Using the condition (5) on l, it is easy to see the existence of such x. Then put

$$F = \boldsymbol{Q}(\sqrt{x^2-4z^n})$$

where z is a rational integer satisfying

(v) $(x, z)=1$,
(vi) $kl \mid z$,
(vii) $z \equiv 1 \pmod{q^2}$ for $q \in S_2 \cup S_3$,
(viii) $x^2-4z^n<0$.

This time also we see easily the existence of such z, since z is determined by a congruence condition and the coefficient of z^n in (viii) is negative. Let D be the discriminant of F and put

$$x^2-4z^n = y^2D \qquad (y \in \boldsymbol{Z}).$$

If $q \in S_1$, from (v) and (vi), we have $\left(\frac{D}{q}\right)=1$. If $q \in S_2$, from (iii) and (vii), we have $\left(\frac{D}{q}\right)=-1$. In the case $q \in S_3$, from (iv) and (vii), we get

$$x^2-4z^n = (q+2)^2-4 \equiv 4q \pmod{q^2}$$

and further if $q=2$, we get

$$\frac{x^2-4z^n}{4} \equiv -1 \pmod{4}.$$

So all primes in S_3 are ramified in F. It follows from Proposition 1 that F has an ideal class of order n, since we have $D<-4$ from the assumption on S_3. Therefore F satisfies the conditions (a) and (b). So we have $F(S_1, S_2, S_3) \neq \phi$. The infiniteness follows directly from the existence: Assume there exist only a finite number of such F's. Let them be $F_1, F_2, \cdots, F_t$, and S_1' be the set of all prime numbers which are ramified in at least one of F_i's. S_3' is a finite set since only a finite number of primes are ramified in F_i. Let q' be a prime number which is not contained in $S_1 \cup S_2 \cup S_3' \cup \{2, 3\}$. And put $S_3'' = S_3' \cup \{q\}$. We have shown already that $F(S_1, S_2, S_3'') \neq \phi$. Take an $F'' \in F(S_1, S_2, S_3'')$. Obviously $F'' \in F(S_1, S_2, S_3)$. So we get $q' \in S_3'$. This contradict the choice of q'. Therefore $F(S_1, S_2, S_3)$ must be an infinite set. This completes the proof.

REMARK In Kuroda [8], the case $S_1=S_2=\phi$ is treated and the infiniteness is proved by an analytic method.

4. Take two systems of prime number $\{l_i\}$ and $\{l_i'\}$, each satisfying the condition (2)′ in § 3. We assume, moreover, that $l_i \neq l_i'$ for every $i (1 \leqq i \leqq s)$.

The following proposition is fundamental for our purpose.

Proposition 2. *Let x, z, x', z' be a non-trivial solution of the following Diophantine equation*

$$X^2-4Z^n = X'^2-4Z'^n \tag{6}$$

such that

(i)″ $(x, z)=(x', z')=1$,
(ii)″ $l_i \mid z$ *and* $l_i' \mid z'$ $(1\leqq i\leqq s)$,
(iii)″ x *(resp.* x'*) is a* p_i*-th power non-residue mod.* l_i *(resp. mod.* l_i'*)* $(1\leqq i\leqq s)$,
(iv)″ $\dfrac{x+x'}{2}$ *is a* p_i*-th power residue mod.* l_i $(1\leqq i\leqq s)$.

Then the ideal class group H of the field

$$F = \boldsymbol{Q}(\sqrt{x^2-4z^n})$$

has a subgroup N such that

$$N \cong \begin{cases} \boldsymbol{Z}/n\boldsymbol{Z}\oplus\boldsymbol{Z}/n\boldsymbol{Z} & \text{if } D<-4, \\ \boldsymbol{Z}/n\boldsymbol{Z} & \text{if } D>0, \end{cases}$$

where D is the discriminant of F.

Proof. From the equation (6) we set

$$x^2-4z^n = x'^2-4z'^n = y^2D \tag{7}$$

for some $y\in\boldsymbol{Z}$. Hence we have

$$x^2-y^2D = 4z^n, \tag{8}$$
$$x'^2-y^2D = 4z'^n. \tag{9}$$

So we get two solutions x, y, z and x', y', z' of the Diophantine equation (1). It follows from Lemma 1 that there are ideals $\mathfrak{a}$, $\mathfrak{a}'$ in F such that $(\alpha)=\mathfrak{a}^n$ and $(\alpha')=\mathfrak{a}'^n$ where $\alpha=\dfrac{x+y\sqrt{D}}{2}$ and $\alpha'=\dfrac{x'+y\sqrt{D}}{2}$. Let $\mathfrak{r}_i$, $\mathfrak{r}_i'$ $(1\leqq i\leqq s)$ be the prime ideals in F such that

$$l_i = \mathfrak{r}_i\mathfrak{r}_i^{\sigma} \qquad \mathfrak{r}_i \mid (\alpha^{\sigma}),$$
$$l_i' = \mathfrak{r}_i'\mathfrak{r}_i'^{\sigma} \qquad \mathfrak{r}_i' \mid (\alpha'^{\sigma}),$$

(cf. § 2). Let R_i (resp. R_i') be the set of all integers in F which are p_i-th power residues mod. $\mathfrak{r}_i$ (resp. mod. $\mathfrak{r}_i'$). Since

$$\alpha \equiv x \,(\text{mod. } \mathfrak{r}_i), \quad \alpha' \equiv x' \,(\text{mod. } \mathfrak{r}_i')$$

and

$$\alpha' \equiv \frac{x+x'}{2} \,(\text{mod.}\mathfrak{r}_i)\,,$$

it follows from (iii)″ and (iv)″ that

$$\alpha \notin R_i,\ \alpha' \notin R_i',\ \text{and}\ \ \alpha' \in R_i \qquad (1 \leqq i \leqq s)\,. \tag{10}$$

The case $D<-4$. By Proposition 1, both ideal classes $[\mathfrak{a}]$ and $[\mathfrak{a}']$ have the same order n. Suppose the following equation holds for $m>0$ and $m'>0$;

$$[\mathfrak{a}]^m[\mathfrak{a}']^{m'} = 1\,. \tag{11}$$

Then there exists a number $\beta \in F$ such that

$$\mathfrak{a}^m\mathfrak{a}^{m'} = (\beta)\,. \tag{12}$$

Taking n-th power of both sides of (12),

$$\alpha^m\alpha^{m'} = \pm\beta^n\,. \tag{13}$$

Define d_i by $\mathfrak{p}_i^{d_i} \| (m, m')$, and e_i by $\mathfrak{p}_i^{e_i} \| n$ $(1 \leqq i \leqq s)$. We claim that $d_i \geqq e_i$ for all i. Suppose $d_i < e_i$ holds for some i, and set

$$m = \mathfrak{p}_i^{d_i} m_0,\ m' = \mathfrak{p}_i^{d_i} m_0',\ n = \mathfrak{p}_i^{d_i} n_0\,, \tag{14}$$

where $\mathfrak{p}_i \mid \mathfrak{n}_0$. From (13) we have

$$\alpha^{m_0}\alpha'^{m_0'} = \pm\beta^{n_0}\,,$$

since F has no root of 1 except ± 1. As $\alpha'^{m_0'} \in R_i$ and $\pm\beta^{n_0} \in R_i$, we have $\alpha^{m_0} \in R_i$. But $\alpha \notin R_i$, so we have $\mathfrak{p}_i \mid \mathfrak{m}_0$. Then we have $\alpha^{m_0} \in R_i'$ and $\pm\beta^{n_0} \in R_i'$, so we also get $\mathfrak{p}_i \mid \mathfrak{m}_0'$ using $\alpha' \notin R_i'$. Hence and from (14) we have $\mathfrak{p}_i^{d_i+1} \mid (m, m')$. This contradicts the definition of d_i. Therefore we have $d_i \geqq e_i$ for every i, accordingly we have $n \mid m$ and $n \mid m'$. Let N be the subgroup of the ideal class group H generated by $[\mathfrak{a}]$ and $[\mathfrak{a}']$. Then N is isomorphic to the direct sum $\boldsymbol{Z}/n\boldsymbol{Z} \oplus \boldsymbol{Z}/n\boldsymbol{Z}$.

The case $D>0$. Set $I=\{i \mid \varepsilon \in R_i,\ 1 \leqq i \leqq s\}$, where ε is a fixed fundamental unit of F. Let m and m' be the orders of the ideal class $[\mathfrak{a}]$ and $[\mathfrak{a}']$ respectively $(m \mid n$ and $m' \mid n)$. It follows from Lemma 2 that m is a multiple of $\prod_{i \in I} \mathfrak{p}_i^{e_i}$. We claim that m' is a multiple of $\prod_{i \notin I} \mathfrak{p}_i^{e_i}$. Assume $\mathfrak{p}_i m' \mid n$ for some $i \notin I$, then there exists a number β in F such that

$$\mathfrak{a}'^n = (\alpha') = (\beta)^{\mathfrak{p}_i}\,.$$

So we have

$$\alpha' = \pm\varepsilon^k\beta^{p_i} \qquad \text{for some} \quad k\in\boldsymbol{Z}.$$

Since $\alpha'\in R_i$, $\beta^{p_i}\in R_i$, and $\varepsilon\notin R_i$, we get $p_i \mid k$. Hence $\pm\varepsilon^k\beta^{p_i}\in R_i'$. So we get $\alpha'\in R_i'$, while from (10), $\alpha'\notin R_i'$. This is a contradiction. Therefore we have $p_i m' \nmid n$ for all $i\notin I$. So m' is a multiple of $\prod_{i\notin I} p_i^{e_i}$. Set

$$m = m_0 \prod_{i\in I} p_i^{e_i} \quad \text{and} \quad m' = m_0' \prod_{i\notin I} p_i^{e_i}.$$

It is easy to see that the ideal class

$$[\mathfrak{a}^{m_0}\mathfrak{a}'^{m_0'}]$$

has the order just equal to n. So the proof is completed.

REMARK. In the case $D>0$, we see that the subgroup N generated by $[\mathfrak{a}]$ and $[\mathfrak{a}']$ is isomorphic to $\boldsymbol{Z}/n\boldsymbol{Z}\oplus\boldsymbol{Z}/n\boldsymbol{Z}$ if a fundamental unit ε of F is a p_i-th power residue mod. $\mathfrak{r}_i$ and mod. $\mathfrak{r}_i'$ for every $i=1, 2, \cdots, s$.

5. We need one more lemma before we state our main theorem.

Lemma 3. *For a given prime number p, there exist infinitely many prime number l's such that*

(a) $l\equiv 1 \pmod{p}$ *if* $p\neq 2$, $l\equiv 1 \pmod{4}$ *if* $p=2$,
(b) *both 2 and -1 are p-th power residues mod. l,*
(c) *3 is a p-th power non-residue mod. l.*

Proof. Set

$$K = \begin{cases} \boldsymbol{Q}(1^{1/p}) & \text{if} \quad p\neq 2, \\ \boldsymbol{Q}(\sqrt{-1}) & \text{if} \quad p=2, \end{cases}$$
$$\bar{K} = K(2^{1/p}, 3^{1/p}).$$

Then $\bar{K}/\boldsymbol{Q}$ is a Galois extension of degree $p^2(p-1)$ or 8 according as $p\neq 2$ or $p=2$. It follows from the density theorem that there exist infinitely many prime number l's whose decomposition fields are all equal to $K(2^{1/p})$. We can see easily that such l's satisfy the conditions of the lemma.

Theorem 2. *For given finite sets S_1, S_2, S_3 of prime numbers satisfying $S_i\cap S_j=\phi$ if $i\neq j$, there exist infinitely many imaginary (resp. real) quadratic number fields F such that*

(a) *the ideal class group H of F has a subgroup N which is isomorphic to $\boldsymbol{Z}/n\boldsymbol{Z}\oplus\boldsymbol{Z}/n\boldsymbol{Z}$ (resp. $\boldsymbol{Z}/n\boldsymbol{Z}$),*

(b) *all primes contained in S_i* $\begin{cases} \text{are decomposed in } F & (i=1), \\ \text{remain prime} \quad \text{"} & (i=2), \\ \text{are ramified} \quad \text{"} & (i=3). \end{cases}$

Proof. As in the proof of Theorem 1 we may assume that S_3 contains at

least one prime $\neq 2, 3$. Let S be the set of all prime factors of n as in § 3. For each $p_i \in S$ fix two prime numbers l_i and l_i' satisfying the three conditions in Lemma 3 with $p=p_i$. We may assume that $l_i \neq l_i'$ and $l_i, l_i' \notin S_1 \cup S_2 \cup S_3$ for all $i (1 \leqq i \leqq s)$. Define a number e_p by $p^{e_p} || n$ for every prime number p. And take two rational integers a, b satisfying

$$
(15)\quad \begin{cases} a \not\equiv 0,\ b \equiv 0 \pmod{l_i} \\ a \equiv 0,\ b \not\equiv 0 \pmod{l_i'} \end{cases} \text{for } i = 1, 2, \cdots, s, \\
a \equiv b \not\equiv 0 \pmod{q} \quad \text{for } q \in S_1 - \{2\}, \\
\begin{cases} a \equiv a_q q^{f_q} \pmod{q^{f_q+1}} \\ b \equiv 0 \pmod{q^{f_q+1}} \end{cases} \text{for } q \in S_2 \cup S_3 - \{2\}, \\
\begin{cases} a \equiv a_2 2^{e_2+5} \pmod{2^{e_2+8}} \\ b \equiv 0 \pmod{2^{e_2+8}} \end{cases} \text{if } 2 \in S_1 \cup S_2 \cup S_3, \\
a \equiv b \equiv 0 \pmod{2} \quad \text{if } 2 \notin S_1 \cup S_2 \cup S_3,
$$

where a_q is a rational integer such that

$$
(16)\quad \begin{cases} 2na_q q^{-e_q} \text{ is a quadratic non-residue mod. } q & \text{for } q \in S_2 - \{2\}, \\ a_q \not\equiv 0 \pmod{q} & \text{for } q \in S_3 - \{2\}, \\ na_2 2^{-e_2} \equiv 1 \pmod{8} & \text{if } 2 \in S_1, \\ \equiv 5 \pmod{8} & \text{if } 2 \in S_2, \\ \equiv 3 \pmod{4} & \text{if } 2 \in S_3, \end{cases}
$$

and f_q is defined by

$$
(17)\quad f_q = \begin{cases} e_q + 2 & \text{for } q \in S_2 - \{2\}, \\ e_q + 1 & \text{for } q \in S_3 - \{2\}. \end{cases}
$$

Then take another rational integer t such that

$$
(18)\quad \begin{cases} t \equiv a \pmod{l_i} & (1 \leqq i \leqq s), \\ t \equiv b \pmod{l_i'} & (1 \leqq i \leqq s), \\ t \equiv a \pmod{q} & \text{for } q \in S_1 - \{2\}, \\ t \equiv 1 \pmod{q} & \text{for } q \in S_2 \cup S_3 - \{2\}, \\ t \equiv 1 \pmod{8}, \\ (t, a^n - b^n) = 1, \\ (t-a, 2a^n - \frac{1}{2}(a-b)^n) = 1, \\ (t-b, 2b^n - \frac{1}{2}(b-a)^n) = 1. \end{cases}
$$

Referring to the choice of l_i, l_i' and a, b, we see easily that such t's exist infinitely

and they are determined by a congruence condition. Set

$$x = 2t^n + \frac{1}{2}\{(t-a)^n - (t-b)^n\},$$

$$x' = 2t^n - \frac{1}{2}\{(t-a)^n - (t-b)^n\},$$

$$z = t(t-a),$$

$$z' = t(t-b).$$

Then we have

$$x^2 - 4z^n = x'^2 - 4z'^n$$

and

$$x \equiv \frac{3}{2}a^n \pmod{l_i},$$

$$x' \equiv \frac{3}{2}b^n \pmod{l_i'},$$

$$x + x' \equiv 4a^n \pmod{l_i}.$$

It follows from this that x, z, x', z' is a solution of the equation (6) in Proposition 2 satisfying all the conditions (i)″, (ii)″, (iii)″ and (iv)″. Since it holds that

$$x^2 - 4z^n = 2n(a+b)t^{2n-1} + \{\text{terms with lower degrees on } t\}$$

and t is determined by a congruence condition, we can let the value $x^2 - 4z^n$ be negative (resp. positive) by taking t suitably. Put $F = \boldsymbol{Q}(\sqrt{x^2 - 4z^n})$. Let D be the discriminant of F. For $q \in S_1 - \{2\}$, we get $q \mid z$ from (18), so $\left(\frac{D}{q}\right) = 1$. As $x^2 - 4z^n$ is a homogeneous polynomial with respect to a, b, t, we have

$$x^2 - 4z^n \equiv \begin{cases} 2na_q q^{f_q} \pmod{q^{e_q + f_q + 1}} & \text{for } q \in S_2 \cup S_3 - \{2\}, \\ na_2 2^{e_2+6} \pmod{2^{2e_2+9}} & \text{if } 2 \in S_1 \cup S_2 \cup S_3. \end{cases}$$

From (16) and (17), $\left(\frac{D}{q}\right) = -1$ or $\left(\frac{D}{q}\right) = 0$ holds if $q \in S_2$ or $q \in S_3$ respectively. And we have $\left(\frac{D}{2}\right) = 1$ for the case $2 \in S_1$. Therefore there exists at least one imaginary (resp. real) field F which satisfies the conditions (a), (b) of the theorem. The infiniteness is shown in the same way as in the proof of Theorem 1.

Corollary 1. *There exist infinitely many real quadratic number fields each with the class number divisible by a given number n.*

Corollary 2. *For a given number n and a given prime number p, there exist infinitely many imaginary quadratic number field F's such that*

(a) *p is decomposed into the product of two distinct prime ideals* $\mathfrak{p}$, $\mathfrak{p}^\sigma$ *in F*

(b) *the cyclic subgroup generated by the class* $[\mathfrak{p}]$ *has the index divisible by n.*

REMARK. In a sense, Corollary 1 can be regarded as a special case when p=infinity of Corollary 2. In this connection it is conjectured that there exist infinitely many imaginary quadratic number field F's whose ideal class groups are cyclic and generated by the class $[\mathfrak{p}]$.

PART II

1. Throughout this part we fix a natural number $n \geqq 3$. Let

$$g(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \qquad (a_0 \neq 0),$$
$$h(X) = b_0X^n + b_1X^{n-1} + \cdots + b_n$$

be two polynomials of degrees n and $n'(n \geqq n')$ with coefficients in a field (in the above, both polynomials are written as those of degree n, so it may happen that $b_0=0$). Set

$$R = R(g, h) = \begin{array}{c} \overbrace{\hphantom{0 \quad \cdot \quad \cdot \quad \cdot \quad 0}}^{n-1} \\ \begin{vmatrix} a_0 & a_1 & \cdot & \cdot & \cdot & a_n & 0 & \cdot & \cdot & \cdot & 0 \\ b_0 & b_1 & \cdot & \cdot & \cdot & b_n & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & a_0 & \cdot & \cdot & \cdot & a_{n-1} & a_n & 0 & \cdot & \cdot & 0 \\ 0 & b_0 & \cdot & \cdot & \cdot & b_{n-1} & b_n & 0 & \cdot & \cdot & 0 \\ \cdot & & & & & \cdot & & & & & \cdot \\ \cdot & & & & & \cdot & & & & & \cdot \\ \cdot & & & & & \cdot & & & & & \cdot \\ 0 & \cdot & \cdot & 0 & a_0 & a_1 & \cdot & \cdot & \cdot & \cdot & a_n \\ 0 & \cdot & \cdot & 0 & a_0 & b_1 & \cdot & \cdot & \cdot & \cdot & b_n \end{vmatrix} \end{array}$$

and let $R_k = R_k(g, h)$ be the determinant derived from R by deleting the last $2k$ rows and the last $2k$ columns.

Lemma 1. *The degree of the greatest common divisor of $g(X)$ and $h(X)$ is equal to d, if and only if $R=0$, $R_1=0$, $\cdots$, $R_{d-1}=0$ and $R_d \neq 0$.*

We get this lemma from classical theory of equations (see, for example, Dickson [2]).

2. We consider trinomials of the form

$$(*) \qquad X^n + aX + b \qquad (a, b \in \boldsymbol{Z}).$$

Let $f(X)$ be given by $(*)$ and $f'(X)$ be its derivative. By simple calculations we get

$$(1) \qquad R = R(f, f') = (-1)^{n(n-1)/2}\{(-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}\},$$
$$(2) \qquad R_1 = R_1(f, f') = (-1)^{(n-1)(n-2)/2} n(n-1)^{n-2} a^{n-2}.$$

From (1) and (2), it follows;

Lemma 2. *If $(n-1)a$ and nb are relatively prime, then R and R_1 are also relatively prime.*

Let p be a prime number. Denote by $f(X)$ *mod.* p the image of $f(X)$ by the canonical homomorphism

$$\boldsymbol{Z}[X]\to(\boldsymbol{Z}/p\boldsymbol{Z})[X]\,.$$

Lemma 3. *If $(n-1)a$ and nb are relatively prime, then, for every prime number p, $f(x)$ mod. p has at most one multiple root, which is of multiplicity 2 if there exists.*

Proof. Let $\bar{g}(X)$ be the greatest common divisor of $f(X)$ mod. p and $f'(X)$ mod. p. If α is a root of $f(X)$ mod. p of multiplicity m, then it is a root of $\bar{g}(X)$ of multiplicity not less than $m-1$. From Lemma 1 and Lemma 2, it follows that the degree of $g(X)$ is equal to 0 or 1. So all roots of $f(X)$ mod. p are of multiplicity 1 or 2. And among them there is at most one which is of multiplicity 2.

3. Let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be n roots of $f(X)$. Denote the discriminant of $f(X)$ by $D(f)$. It holds that

$$D(f)=\prod_{i<j}(\alpha_i-\alpha_j)^2=R(f,f')$$

Let K be the (minimal) splitting field of $f(X)$ over the rational number field $\boldsymbol{Q}$. We have

$$K=\boldsymbol{Q}(\alpha_1,\alpha_2,\cdots,\alpha_n)\,.$$

K is a Galois extension over $\boldsymbol{Q}$ and the Galois group $G=G(K/\boldsymbol{Q})$ is isomorphic to a subgroup (also denoted by G, if there is no confusion) of the symmetric group S_n of degree n as a permutation group acting on the set $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$.

Proposition 1. *If*

(i) *$(n-1)a$ and nb are relatively prime*

and

(ii) *$G(K/\boldsymbol{Q})$ is isomorphic to S_n,*

then K is an A_n-extension of $\boldsymbol{Q}(\sqrt{D(f)})$ unramified at all finite prime spots, where an A_n-extension means a Galois extension whose Galois group is isomorphic to the alternating group A_n of degree n.

Proof. From the definition of $D(f)$, we see easily that $\boldsymbol{Q}(\sqrt{D(f)})$ is the fixed field of A_n in $K/\boldsymbol{Q}$. So K is an A_n-extension over $\boldsymbol{Q}(\sqrt{D(f)})$. Set $F=$

$\boldsymbol{Q}(\sqrt{D(f)})$. Take any prime ideal $\mathfrak{p}$ in F. Let p be the prime number such that $p=\mathfrak{p}\cap \boldsymbol{Z}$. By Lemma 3, $f(X)$ mod. p has *case* 1) no multiple root or *case* 2) one double root and $n-1$ simple roots. In case 1), p is not ramified in $\boldsymbol{Q}(\alpha_i)/\boldsymbol{Q}$ for $i=1, 2, \cdots, n$, accordingly so in $K/\boldsymbol{Q}$. Hence $\mathfrak{p}$ is not ramified in K/F. In case 2), we have

$$f(X) \equiv (X-c)^2 h(X) \qquad (\text{mod. } p)$$

for some $c\in \boldsymbol{Z}$ and a polynomial $h(X)\in \boldsymbol{Z}[X]$ of degree $n-2$ such that $h(X)$ mod. p has no multiple root and $h(c)\not\equiv 0$ (mod. p). By Hensel's lemma, we get

$$f(X) = \tilde{g}(X)\tilde{h}(X)\,,$$

where $\tilde{g}(X)$ and $\tilde{h}(X)$ are polynomials of degrees 2 and $n-2$ respectively with coefficients in the p-adic number field $\boldsymbol{Q}_p$ such that

$$\tilde{g}(X) \equiv (X-c)^2 \qquad (\text{mod. } p)\,,$$
$$\tilde{h}(X) \equiv h(X) \qquad (\text{mod. } p)\,.$$

Let $\mathfrak{P}$ be a prime ideal in K satisfying $\mathfrak{P}\mid\mathfrak{p}$ and $K_{\mathfrak{P}}$ be the $\mathfrak{P}$-completion of K. $K_{\mathfrak{P}}$ contains $\boldsymbol{Q}_p$ canonically and then it is a Galois extension over $\boldsymbol{Q}_p$. Let L and L' be the splitting fields of $\tilde{g}(X)$ and $\tilde{h}(X)$ respectively over $\boldsymbol{Q}_p$. We may set $K_{\mathfrak{P}}=L\cup L'$. Let $Z_{\mathfrak{P}}$ and $T_{\mathfrak{P}}$ be the decomposition group and the inertia group of $\mathfrak{P}$ with respect to $\boldsymbol{Q}$. $Z_{\mathfrak{P}}$ is ,dentified with the Galois group $G(K_{\mathfrak{P}}/\boldsymbol{Q}_p)$. Since $L'/\boldsymbol{Q}_p$ is unramified, $K_{\mathfrak{P}}/\boldsymbol{Q}_p$ is ramified or not according as $L/\boldsymbol{Q}_p$ is ramified or not. The Galois group $Z_{\mathfrak{P}}$ being regarded as a permutation group on n roots of $f(X)$, we see that $T_{\mathfrak{P}}$ is either a cyclic group of order 2 generated by a transposition of two roots of $f(X)$ or the trivial group 1 according as the extension $L/\boldsymbol{Q}_p$ is ramified or not. In either case, the inertia group of $\mathfrak{P}$ with respect to F, which is given by $T_{\mathfrak{P}}\cap A_n$, is equal to 1. So $\mathfrak{p}$ is not ramified in K. Therefore K/F is unramified at all finite prime spots. This completes the proof.

4. Let $f(X)$ be a trinomial of the form (*) and K be the splitting field of $f(X)$ over $\boldsymbol{Q}$. In order to determine the Galois group $G=G(K/\boldsymbol{Q})$ which is called *the Galois group of* $f(X)$ in the following, we use the following

Lemma 4 (cf. [11], § 61). *If there exist three prime numbers* l_1, l_2, l_3 *which satisfy the following conditions*:

(i) $f(X)$ *mod.* l_1 *is irreducible.*
(ii) $f(X)$ *mod.* l_2 *is the product of two irreducible polynomials of degrees* 1 *and* $n-1$.
(iii) $f(X)$ *mod.* l_3 *is the product of distinct* $n-2$ *polynomials of degree* 1 *and an irreducible polynomial of degree* 2.

Then G *is isomorphic to* S_n.

Conversely, from the density theorem of the prime ideals with a given type of decomposition in a Galois extension, we get

Lemma 5. *If G is isomorphic to S_n, then, for each one of conditions* (i), (ii), (iii) *of Lemma* 4, *there exist infinitely many prime numbers which satisfy the condition.*

The following is fundamental in this part together with Proposition 1.

Proposition 2. *There exist infinitely many trinomials of the form* (*) *whose Galois groups are isomorphic to S_n.*

Proof. Let l_1 be a prime number such that $l_1 \equiv 1 \pmod{n}$ and c_1 be a primitive root mod. l_1. Then polynomial $X^n - c_1$ is irreducible mod. l_1. Let l_2 and c_2 be a prime number such that $l_2 \equiv 1 \pmod{n-1}$ and a primitive root mod. l_2, then $X^n - c_2X$ satisfies the condition (ii) of Lemma 4. Finally, let's find a trinomial $f(X)$ of the form (*) which satisfies the condition (iii) of Lemma 4. Let p be a prime number such that $p \equiv 1 \pmod{4}$ and $p \nmid n(n-1)$. Take $c, d \in \boldsymbol{Z}$ satisfying $c^2 - 4d = p$. Let

$$\frac{1}{1+ct+dt^2} = 1 + e_1t + e_2t^2 + \cdots \tag{3}$$

be the formal expansion with respect to t, then we have

$$\begin{aligned} &e_i \in \boldsymbol{Z} \qquad \text{for} \quad i = 1, 2, \cdots \\ &e_1 = -c, \\ &e_2 = -(ce_1 + d), \\ &e_i = -(ce_{i-1} + de_{i-2}) \qquad \text{for} \quad i \geqq 3. \end{aligned}$$

Put $g(X) = X^2 + cX + d$ and $h(X) = X^{n-2} + e_1X^{n-3} + \cdots + e_{n-2}$. We have

$$g(X)h(X) = X^n - e_{n-1}X + de_{n-2}.$$

Here we claim that discriminants $D(g)$ and $D(h)$ are relatively prime. Since $D(g) = c^2 - 4d = p$ and $D(gh) = D(g)D(h)R(g, h)^2$, it is sufficient to show that $D(gh)$ is divisible by p but not by p^2. Equation $g(X) = 0$ gives a ramified quadratic extension k_p over $\boldsymbol{Q}_p$. Let $\alpha, \beta \in k_p$ be roots of $g(X)$, then it holds

$$(\alpha - \beta)^2 = c^2 - 4d = p,$$

and $\pi = \alpha - \beta$ is a prime element of k_p while α and β are both units. Calculating the expansion (3) in the ring of formal power series with coefficients in k_p,

$$\frac{1}{1+ct+dt^2} = \frac{1}{(1-\alpha t)(1-\beta t)}$$
$$= \frac{1}{(\alpha-\beta)t}\left\{\frac{1}{1-\alpha t} - \frac{1}{1-\beta t}\right\}$$
$$= \frac{1}{\alpha-\beta}\sum_{k=0}^{\infty}(\alpha^{k+1}-\beta^{k+1})t^k,$$

we get

$$e_k = \frac{\alpha^{k+1}-\beta^{k+1}}{\alpha-\beta} \qquad \text{for} \quad k = 1, 2, \cdots.$$

Replace α by $\beta+\pi$, and we get

$$e_k \equiv (k+1)\beta^k + \binom{k+1}{2}\beta^{k-1}\pi + \binom{k+1}{3}\beta^{k-2}\pi^2 \qquad (\text{mod. } \pi^3).$$

Applying this congruence relation to $D(gh)$,

$$D(gh) = (-1)^{n(n-1)/2}\{(-1)^{n-1}(n-1)^{n-1}(-e_{n-1})^n + n^n(de_{n-2})^{n-1}\}$$
$$\equiv (-1)^{(n-1)(n-2)/2}\frac{1}{8}n^{n+1}(n-1)^n\beta^{(n+1)(n-2)}\pi^2 \qquad (\text{mod. } \pi^3).$$

In the last member of the congruence, the coefficient of π^2 being a unit of k_p, $D(gh)$ is not divisible by π^3. Hence, returning to $\boldsymbol{Z}$, $D(gh)$ is just divisible by p and not by p^2, since $\pi^2=p$. Now that $D(g)$ and $D(h)$ are relatively prime, two splitting fields K_g and K_h of $g(X)$ and $h(X)$ over $\boldsymbol{Q}$ are independent, that is, $K_g \cap K_h = \boldsymbol{Q}$. From the density theorem it follows that there exist infinitely many prime numbers which remain prime in K_g but are decomposed completely in K_h. Let l_3 be one of them such that $l_3 \nmid l_1 l_2\, D(gh)$, then $f(X)=g(X)h(X)$ satisfies the condition (iii) of Lemma 4. Now take $a, b \in \boldsymbol{Z}$ such that

$$\begin{aligned} a &\equiv 0, & b &\equiv -c_1 & (\text{mod. } l_1)\\ a &\equiv -c_2, & b &\equiv 0 & (\text{mod. } l_2)\\ a &\equiv -e_{n-1}, & b &\equiv de_{n-2} & (\text{mod. } l_3). \end{aligned}$$

By Lemma 4, the polynomial X^n+aX+b has the Galois group isomorphic to S_n. It is obvious that there are infinitely many pair (a, b) which satisfy above conditions. So the proof is completed.

5. Now we prove our main theorem:

Theorem 1. *Let S be the set of all prime factors of $n(n-1)$, and S' be a given finite set of prime numbers satisfying $S \cap S' = \phi$. Then there exist infinitely many imaginary (resp. real) quadratic number field F's which satisfy the following conditions (a), (b), (c).*

(a) *F has an A_n-extension K which is unramified at all prime (resp. all finite prime) spots of F.*
(b) *K is an S_n-extension of $\boldsymbol{Q}$.*
(c) *All primes in S' are ramified in F.*

Proof. From Proposition 2, there is a trinomial

$$f(X) = X^n + a_0X + b_0$$

whose Galois group is isomorphic to S_n. Take three prime numbers l_1, l_2, l_3 which satisfy the conditions (i), (ii), (iii) of Lemma 4 respectively. By Lemma 5, we may assume that $l_i \notin S \cup S'$ for $i=1, 2, 3$. First we consider the case n is odd. Take and fix $b \in \boldsymbol{Z}$ such that

$$\begin{aligned} &b \equiv b_0 \quad (\text{mod. } l_i) \quad \text{for} \quad i=1, 2, 3\,, \\ &b \equiv n-1 \quad (\text{mod. } p^2) \quad \text{for} \quad p \in S'\,, \\ &(b, n-1) = 1\,, \end{aligned}$$

and then take $a \in \boldsymbol{Z}$ such that

$$\begin{aligned} &a \equiv a_0 \quad (\text{mod. } l_i) \quad \text{for} \quad i = 1, 2, 3\,, \\ &a \equiv p-n \quad (\text{mod. } p^2) \quad \text{for} \quad p \in S'\,, \\ &(a, nb) = 1\,. \end{aligned}$$

Set

$$f(X) = X^n + aX + b\,.$$

As a is determined by a suitable congruence condition, we may safely assume that $D(f)<0$ (resp.>0). Then it is easily seen that $f(X)$ satisfies the conditions (i), (ii) of Proposition 1. Moreover for $p \in S'$, it holds that

$$\begin{aligned} D(f) &\equiv (-1)^{n(n-1)/2}(n-1)^{n-1}\{(p-n)^n + n^n\} \quad (\text{mod. } p^2) \\ &\equiv (-1)^{n(n-1)/2}(n-1)^{n-1}n^n p \quad (\text{mod. } p^2) \end{aligned}$$

This implies that $p \| D(f)$. Hence $F=\boldsymbol{Q}(\sqrt{D(f)})$ and the splitting field K of $f(X)$ over $\boldsymbol{Q}$ satisfy the conditions (a), (b), (c) of the theorem. The case n is even is discussed in almost same way by exchanging the roles of a and b. And the infiniteness is shown in the same way as in the proof of Theorem 1 of part I.

REMARK. Theorem 1 is considered a sort of generalizations of [6], where the case $n=3$ is treated.

6. Here is an interesting example. Set

$$f(X) = X^5 + 2X + 1\,.$$

Then we get

$$f(X) \equiv (X+1)(X^4+X^3+X^2+X+1) \pmod 2,$$
$$f(X) \equiv X^5+2X+1 \pmod 3,$$
$$f(X) \equiv (X^2+9X+10)(X^3+8X^2+3X+12) \pmod{17},$$

where each factor in the right sides is irreducible with respect to its modulus. Hence the Galois group of $f(X)$ over $\boldsymbol{Q}$ is isomorphic to S_5 (cf. [11] § 61). Let K be the splitting field of $f(X)$ over $\boldsymbol{Q}$ and $F=\boldsymbol{Q}(\sqrt{D(f)})$ where $D(f)=11317$ (prime number). It follows from Proposition 1 that K is an A_5-extension of F and all finite prime spots of F are unramified in K. Since K is imaginary, however, the two infinite prime spots of F are ramified in K.

On the other hand, after a little tedious calculations on continuous fractions, we see that the ideal class number of F is equal to 1 and the norm of the fundamental unit of F is equal to -1. So there is no *abelian* extension of F which is unramified at all finite prime spots of F. (for another example, cf. Fujisaki [3], but the real quadratic field in it has a fundamental unit with norm 1)

7. In this section we consider the case $n=3$. Put

$$\begin{cases} a_1 = -2t^2+18t \\ b_1 = t^3-16t^2-432 \end{cases} \qquad \begin{cases} a_2 = -2t^2-18t \\ b_2 = t^3+16t^2+432 \end{cases}$$

where $t \in \boldsymbol{Z}$ satisfying

$$(4) \qquad \begin{cases} t \equiv 37 \pmod{210} \\ t \not\equiv \pm 9 \pmod{37} \end{cases}$$

For $i=1, 2$ set

$$f(X) = X^3+a_iX+b_i\,.$$

Then we get

$$\begin{aligned} D(f_1) &= D(f_2) \qquad (\text{set} = D(t)) \\ &= 5\,t^6+2^5 3^3 t^4-2^9 3^6 t^2-2^8 3^9 \end{aligned}$$

and

$$\begin{aligned} (2a_1,\ 3b_1) &= (t-9,\ t^3-16t^2-432) \\ &= (t-9,\ 3^3 37) \\ &= 1\,, \\ (2a_2,\ 3b_2) &= (t+9,\ t^3+16t^2+432) \\ &= (t+9,\ 3^3 37) \\ &= 1\,. \end{aligned}$$

Moreover for every t satisfying condition (4) we get

$$f_1(X) \equiv X^3+3X+2 \quad (\text{mod. } 5),$$
$$f_2(X) \equiv X^3+X+4 \quad (\text{mod. } 5),$$

where both trinomials in the right sides are irreducible mod. 5. So both $f_1(X)$ and $f_2(X)$ are irreducible over $\boldsymbol{Q}$ and have the Galois group isomorphic to S_3 (cf. [6]). Let K_i be the splitting field of $f_i(X)$ over $\boldsymbol{Q}$ ($i=1, 2$). Then K_i is a cyclic extension of $F_t=\boldsymbol{Q}(\sqrt{D(t)})$ of degree 3 and unramified at all finite prime spots. On the other hand we have

$$f_1(X) \equiv X^3+2 \equiv \text{irreducible} \quad (\text{mod. } 7)$$
$$f_2(X) \equiv X^3+5X \equiv X(X+3)(X+4) \quad (\text{mod. } 7).$$

So K_1 must be different from K_2, since prime ideal 7 in $\boldsymbol{Q}$ has different types of prime decompositions in K_1 and K_2.

Consider the following Diophantine equation:

$$dY^2 = 5X^6+2^5 3^3 X^4-2^9 3^6 X^2-2^8 3^9 \tag{5}$$

where d is a fixed rational integer. Since the affine curve defined by (5) has genus 2, from Siegel's theorem (cf. [10]) the equation has only a finite number of integral solutions. Hence, for infinitely many values of t satisfying (4), F_t represents infinitely many real quadratic number fields. So we get the following theorem, which is a supplement of Theorem 2 of Part I.

Theorem 2. *There exist infinitely many real quadratic number fields whose ideal class groups have non-cyclic 3-subgroups.*

REMARK. For imaginary case we have the corresponding result by setting, for example,

$$\begin{cases} a_1 = t+9 \\ b_1 = t^2+25 \end{cases} \qquad \begin{cases} a_2 = t-9 \\ b_2 = t^2+29 \end{cases}$$

where $t \in \boldsymbol{Z}$ satisfying

$$\begin{cases} t \equiv 2 & (\text{mod. } 30), \\ t \not\equiv 9 & (\text{mod. } 11), \\ t \not\equiv -9 & (\text{mod. } 53). \end{cases}$$

But we have got more stronger results in part I.

REMARK. We can add a local conditions to this theorem as in part I. For that purpose we need further investigations on the ramifications of the spots $p=2$ or 3.

8. In the rest of this paper, we shall study other types of unramified Galois extensions of quadratic number fields.

Lemma 6. (cf. Herz [5]). *Every unramified abelian extension A of a quadratic number field F is absolutely normal and the Galois group $G(A/\boldsymbol{Q})$ is isomorphic to the semi-direct product of $G(F/\boldsymbol{Q})$ and $G(A/F)$. Moreover if $G(A/F)$ is cyclic then $G(A/\boldsymbol{Q})$ is dihedral.*

Proposition 3. *Let F_0 be a quadratic number field with discriminant D_0 and K_0 be a Galois extension of F_0 unramified at all finite prime spots. If K_0 is absolutely normal then, for a quadratic number field F with discriminant D satisfying $D_0 | D$ and $D_0 \neq D$, the field $K=K_0 \cup F$ is a Galois extension of F such that*

(a) $G(K/F) \cong G(K_0/\boldsymbol{Q})$.
(b) *All finite prime spots of F are unramified in K.*

Proof. Since $F_0 \cap F=\boldsymbol{Q}$, it is easily seen that there is a canonical isomorphism $G(K/F) \cong G(K_0/\boldsymbol{Q})$ and $K/F_0 \cup F$ is unramified except at infinite prime spots. On the other hand, $F_0 \cup F/F$ also is unramified except at the infinities, so K/F is unramified at all finite prime spots. So the proof is completed.

Corollary 1. *For a group G such that*

$$G = \prod_{i=1}^{r} D_{m_i} \times \prod_{j=1}^{s} S_{n_j} \qquad (\textit{direct product})$$

where D_m is the dihedral group of order $2m$ and

$$\begin{cases} 2 \leqq m_1 \leqq m_2 \leqq \cdots \leqq m_r \\ 4 \leqq n_1 \leqq n_2 \leqq \cdots \leqq n_s , \end{cases}$$

there exist infinitely many imaginary (resp. real) quadratic number fields each of which has an unramified (resp. unramified except at infinities) Galois extension with Galois group isomorphic to G.

This is a direct consequence of Theorem 1 and Theorem 2 of part I, Theorem 1, Lemma 6 and Proposition 3 of this part. Moreover for a little more complicated group G the corresponding results can be proved. The precise proofs of all these facts will be left to the interested reader.

OSAKA UNIVERSITY

References

[1] N.C. Ankeny and S. Chowla: *On the divisibility of the class number of quadratic fields*, Pacific J. Math. **5** (1955), 321–324.
[2] L.E. Dickson: Elementary Theory of Equations, John Wiley, 1914.
[3] G. Fujisaki: *On an example of an unramified Galois extension* (in Japanese), Sûgaku **9** (1957), 97.

[4] C.F. Gauss: Werke, I, Göttingen, 1863.
[5] C.S. Herz: *Construction of class fields* (Seminar on Complex Multiplication), Springer, 1966.
[6] T. Honda: *On real quadratic fields whose class numbers are multiples of* 3, J. Reine Angew. Math. **233** (1968), 101–102.
[7] P. Humbert: *Sur les nombres de classes de certains corps quadratiques*, Comment. Math. Helv. **12** (1939/40), 233–245; also **13** (1940/41), 67.
[8] S. Kuroda: *On the class number of imaginary quadratic number fields*, Proc. Japan Acad. **40** (1964), 365–367.
[9] T. Nagel: *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **1** (1922), 140–150.
[10] C.L. Siegel: *Über einige Anwendungen Diophantischer Approximationen*, Gesammelte Abhandlungen Band I, 209–266.
[11] B.L. van der Waerden: Moderne Algebra, Springer, 1940.

Note added in proof: Therem 1 in Part II. is shown independently by K. Uchida in almost the same way. His paper is to appear in the *Tôhoku Mathematical Journal.*