

**ON THE MAXIMAL ABELIAN  $\ell$ -EXTENSION OF A FINITE  
ALGEBRAIC NUMBER FIELD WITH  
GIVEN RAMIFICATION**

HIROO MIKI<sup>\*)</sup>

Let  $k$  be a finite algebraic number field and let  $\ell$  be a fixed odd prime number. In this paper, we shall prove the equivalence of certain rather strong conditions on the following four things (1) ~ (4), respectively:

- (1) the class number of the cyclotomic  $Z_\ell$ -extension of  $k$ ,
- (2) the Galois group of the maximal abelian  $\ell$ -extension of  $k$  with given ramification,
- (3) the number of independent cyclic extensions of  $k$  of degree  $\ell$ , which can be extended to finite cyclic extensions of  $k$  of any  $\ell$ -power degree, and
- (4) a certain subgroup  $B_k(m, S)$  (cf. § 2) of  $k^\times / (k^\times)^{\ell^m}$  for any natural number  $m$  (see the main theorem in § 3).

Bertrandias-Payan [2] made some examples of  $k$  satisfying our condition on (3), which implies the non-vanishing of the  $\ell$ -adic regulator of  $k$  (Leopoldt's conjecture for  $(\ell, k)$ ), and satisfying the condition  $|S_k| = 2$ , for  $\ell = 3$  and 5, where  $|S_k|$  is the number of places of  $k$  lying above  $\ell$ . In § 4, we shall prove the existence of  $k$  satisfying our condition on (1) and the condition  $|S_k| \geq n$ , for each natural number  $n$  and each regular odd prime number  $\ell$ .

In § 1, we shall transform Kubota's theorem [16] into our useful form to prove the equivalence of our conditions on (2), (3) and (4) in § 3.

In § 2, we shall discuss a certain relation between  $B_k(m, S)$  and the class number of a cyclotomic  $Z_\ell$ -extension. It is already noted in Satz 8.1 of Neukirch [20] that our condition on (1) implies our condition

---

Received June 24, 1977.

<sup>\*)</sup> Partly supported by Fūjukai Foundation.

on (4). The converse can be proved by using Iwasawa-Yokoyama's method [10], [24] (cf. Theorem 2 in § 2).

In § 3, by using the results of § 1 and 2, we shall give a complete proof of the main theorem.

In § 4, we shall also prove the following statement: *Let  $\zeta_i$  be a primitive  $\ell^i$ -th root of unity, and put  $k_i = k_0(\zeta_i)$ , where  $k_0/\mathbf{Q}$  is a totally real finite Galois extension such that  $\ell$  is completely decomposed in  $k_0$ . Suppose that the class number of  $k_1$  is not divisible by  $\ell$ . Then the class number of  $k_i$  is not divided by  $\ell$  for any  $i \geq 1$ .* Note that this statement is a generalization of Iwasawa [10].

In § 5, we shall give another proof of a part of the main theorem, based on Kummer theory (cf. [17], Proposition 3)<sup>(1)</sup> and a cohomology theoretic method of Iwasawa [9].

I wish to express my sincere thanks to Professors Y. Kawada, T. Kubota and S. -N. Kuroda for their helpful advice and encouragement.

### Notation and terminology

(1)  $\mathbf{Z}$ : the ring of rational integers.  $N = \{n \in \mathbf{Z} \mid n \geq 1\}$ .  $N' = N \cup \{0\} \cup \{\infty\}$ .  $\mathbf{Z}_\ell$ : the ring of  $\ell$ -adic integers.  $\mathbf{Q}_\ell$ : the field of  $\ell$ -adic numbers.  $F_\ell$ : the finite field with  $\ell$  elements.  $|X|$ : the cardinal number of a set  $X$ .  $(\ell^m)$ : the cyclic group of order  $\ell^m$  for each non-negative integer  $m$ .  $(\ell^\infty)$ : the additive group of  $\mathbf{Z}_\ell$ .  $C(m, s)$ : the direct product of  $s$  copies of  $(\ell^m)$  for each  $m, s \in N'$ .  $G(K/k)$ : the Galois group of a Galois extension  $K$  of a field  $k$ .  $K^\times$ : the multiplicative group of a field  $K$ .

(2)  $\ell$ : a fixed odd prime number.  $\zeta_i$ : a primitive  $\ell^i$ -th root of unity for  $i \geq 0$ .  $k$ : a finite algebraic number field.  $n_0$ : the non-negative integer such that  $\zeta_{n_0} \in k$  and  $\zeta_{n_0+1} \notin k$ .  $r_1$ : the number of real places of  $k$ .  $r_2$ : the number of complex places of  $k$ .  $k_i = k(\zeta_i)$ .  $k_v$ : the completion of  $k$  with respect to a prime divisor  $v$  of  $k$ .  $U_v$ : the group of units of  $k_v$  if  $v$  is non-archimedean, and  $k_v^\times$  otherwise.  $S_k$ : the set of all the prime divisors of  $k$  lying above  $\ell$ .  $S$ : a finite set of non-archimedean prime divisors of  $k$ , containing  $S_k$ .  $S_i = \{v \in S \mid \zeta_i \in k_v, \zeta_{i+1} \notin k_v\}$  for each  $i \geq 0$ .  $s_i = |S_i|$ .  $S^i$ : the set of all prime divisors of  $k_i$  lying

(1) Note that Corollary to Proposition 3 of [17] is the same as Theorem 1 of Bertrandias-Payan [2] when the basic field contains a primitive  $\ell$ -th root of unity. The author did not know their result when he wrote [17].

above  $S$  for each  $i \geq 0$ .  $T$ : a finite set of prime divisors of  $k$ . An algebraic extension  $K$  of  $k$  is called  $T$ -ramified (or unramified outside  $T$ ) if  $K/k$  is unramified for any prime divisor  $v \notin T$ .

$k(T)$ : the maximal  $T$ -ramified abelian  $\ell$ -extension of  $k$ .  $G_k(T) = G(k(T)/k)$ .  $U_k(m, T) = \{x \in k^\times \mid (x) = \alpha^{\ell^m}, \alpha \in k_v^{\times \ell^m} \text{ for } v \in T\}$ , where  $(x)$  is a principal ideal of  $k$  generated by  $x$ ,  $\alpha$  denotes a fractional ideal of  $k$ .  $B_k(m, T) = U_k(m, T)/k^{\times \ell^m}$ .  $I_k$ : the group of ideals of  $k$ .  $P_k$ : the group of principal ideals of  $k$ .  $Cl_k$ : the ideal class group of  $k$ , i.e.,  $Cl_k = I_k/P_k$ .  $Cl_k(S) = Cl_k/\langle S \rangle$ , where  $\langle S \rangle$  is the subgroup of  $Cl_k$  generated by all ideal classes containing prime ideals in  $S$ .  $J$ : the idele group of  $k$ .  $C_k$ : the idele class group of  $k$ .  $W$ : the group of  $\ell$ -power roots of unity in  $k$ .  $W_v$ : the group of  $\ell$ -power roots of unity in  $k_v$  for a prime divisor  $v$  of  $k$ .  $n_v$ : the non-negative integer such that  $\zeta_{n_v} \in k_v$  and  $\zeta_{n_v+1} \notin k_v$ , i.e.,  $\zeta_{n_v}$  is a generator of  $W_v$ .  $U_T = \{x = (x_v) \in J \mid x_v \in U_v \text{ for } v \notin T, x_v = 1 \text{ for } v \in T\}$ .  $E_k$ : the group of units in  $k$ .  $E_k(S) = \{x \in k^\times \mid x \in U_v \text{ for any } v \notin S\}$ .

**§ 1. Kubota’s theorem and its corollaries**

To introduce some of Kubota’s results [16], we need some notations. Let  $\ell, k, S_k, T$  and  $B_k(\nu, T)$  be as in Notation. For each  $\nu \in N$ , let  $k(\nu, T)$  be the maximal  $T$ -ramified abelian  $\ell$ -extension of  $k$  such that  $\sigma^{\ell^\nu} = 1$  for all  $\sigma \in G(k(\nu, T)/k)$ , and let  $k(\nu)/k$  be the composite field of all cyclic extensions  $K$  of  $k$  of degree  $\ell^m$  with  $m \leq \nu$  such that for any  $n \in N, K/k$  can be extended to a cyclic extension  $\tilde{K}$  of  $k$  of degree  $\ell^{m+n}$ . Let  $G_k(\nu, T) = G(k(\nu, T)/k)$  and  $H_k(\nu) = G(k(\nu)/k)$ . Let  $N = [k: \mathbf{Q}]$ . For each  $v \in T$ , let  $N_v = [k_v: \mathbf{Q}_\ell]$  or 0 according as  $v \mid \ell$  or  $v \nmid \ell$ , and let  $w_{v, \nu}$  be the number of roots of unity in  $k_v^\times$  whose orders divide  $\ell^\nu$ . Let  $h_v$  be the  $\ell^\nu$ -class number of  $k$ , i.e., the number of the ideal classes of  $k$  whose orders divide  $\ell^\nu$ . Put

$$U_k^*(\nu, T) = \{x \in k^\times \mid (x) = \alpha^{\ell^\nu}, \alpha \in W_v(k_v^\times)^{\ell^\nu} \text{ for all } v \in T\}$$

and  $B_k^*(\nu, T) = U_k^*(\nu, T)/(k^\times)^{\ell^\nu}$ , where  $W_v$  is as in Notation.

**THEOREM 1** (Kubota [16]). *Under the above notation and assumptions, the following two statements hold:*

(i)  $|G_k(\nu, T)| = h_\nu \cdot \prod_{v \in T} (\ell^{\nu N_v w_{v, \nu}} \cdot (B_k(\nu, \phi) : B_k(\nu, T))^{-1};$

$$(ii) \quad |H_k(\nu)| = h_\nu \cdot \ell^{N\nu} (B_k(\nu, \phi) : B_k^*(\nu, S_k))^{-1} .$$

*Remark 1.* Kubota [16] stated the statement (i) in Theorem 1 when  $T = S_k$ , but in the same way as his, the general case follows.

Now we transform Kubota's result quoted above into a useful form for our purpose. For this we need the following elementary

LEMMA 1. *Under the above notation and assumptions,*

$$|B_k(\nu, \phi)| = h_\nu \ell^{(r_1+r_2-1)\nu} w_\nu ,$$

where  $w_\nu$  is the number of roots of unity in  $k^\times$  whose orders divide  $\ell^\nu$ .

*Proof.* We have an exact sequence

$$1 \longrightarrow E_k/E_k^{\ell^\nu} \xrightarrow{\phi_1} B_k(\nu, \phi) \xrightarrow{\phi_2} H_\nu \longrightarrow 1 ,$$

where  $H_\nu$  is the group of the ideal classes of  $k$  whose orders divide  $\ell^\nu$ ,  $\phi_1(\varepsilon) = \varepsilon \pmod{(k^\times)^{\ell^\nu}}$  with  $\varepsilon = \varepsilon \pmod{E_k^{\ell^\nu}}$ ,  $\varepsilon \in E_k$ , and  $\phi_2(\tilde{x}) = \alpha \pmod{P_k}$  with  $\tilde{x} = x \pmod{(k^\times)^{\ell^\nu}}$ ,  $x \in U_k(\nu, \phi)$ ,  $(x) = \alpha^{\ell^\nu}$  and  $\alpha \in I_k$ . From this exact sequence, we obtain  $|B_k(\nu, \phi)| = |H_\nu| \cdot |E_k/E_k^{\ell^\nu}|$ . From this equality and Dirichlet's unit theorem, the assertion follows.

*Remark 2.* When  $\nu = 1$ , the above Lemma 1 is contained in the proof of Theorem 1 of Šafarevič [22], and the above proof is the same as his.

By Theorem 1 and Lemma 1, we obtain immediately the following

COROLLARY 1. *Under the above notation and assumptions, the following two statements hold:*

$$(i) \quad |G_k(\nu, T)| = \prod_{v \in T} (\ell^{\nu N_v} \cdot w_{\nu, v}) \cdot |B_k(\nu, T)| \cdot (\ell^{(r_1+r_2-1)\nu} \cdot w_\nu)^{-1} ;$$

*In particular,*

$$|G_k(\nu, T)| = \ell^{(r_2+1)\nu} \left( \prod_{v \in T} w_{\nu, v} \right) w_\nu^{-1} |B_k(\nu, T)| \quad \text{if } T \supset S_k ;$$

$$(ii) \quad |H_k(\nu)| = |B_k^*(\nu, S_k)| \cdot \ell^{(r_2+1)\nu} w_\nu^{-1} .$$

*Proof.* If  $T \supset S_k$ , then  $\sum_{v \in T} N_v = N$  and  $N = r_1 + 2r_2$ . From this equality, Theorem 1 and Lemma 1, the assertion follows.

*Remark 3.* The statement (i) in the above Corollary is the same as Theorem 1 of Šafarevič [22], when  $\nu = 1$ .

**COROLLARY 2.** *Let the notation be as in Notation. Then the following three statements are equivalent:*

(i) *The essential rank of  $G_k(S)$  is  $r_2 + 1$ , i.e., the number of independent  $\mathbb{Z}_\ell$ -extensions of  $k$  is equal to  $r_2 + 1$ .*

(ii) *There exists an integer  $c$  depending only on  $k$  and  $S$  such that  $|B_k(m, S)| < c$  for all  $m \geq 1$ .*

(iii) *There exist integers  $c$  and  $m_0$  depending only on  $k$  and  $S$  such that  $|B_k(m, S)| = c$  for all  $m \geq m_0$ .*

*Proof.* It is obvious that the statement (i) is equivalent to that  $|G_k(m + 1, S)|/|G_k(m, S)| = \ell^{r_2+1}$  for sufficiently large  $m$ . By the statement (i) of Corollary 1 to Theorem 1,

$$|G_k(m + 1, S)|/|G_k(m, S)| = \ell^{r_2+1} \cdot |B_k(m + 1, S)| \cdot |B_k(m, S)|^{-1}$$

for sufficiently large  $m$ . Hence the statement (i) is equivalent to that there exists an integer  $m_0$  such that  $|B_k(m + 1, S)| = |B_k(m, S)|$  for all  $m \geq m_0$ , i.e., that the statement (iii) holds. It is clear that (iii) implies (ii). Now suppose that the statement (ii) holds. By Lemma 2,  $|B_k(m + 1, S)| \geq |B_k(m, S)|$  for sufficiently large  $m$ . Hence the condition (ii) implies the condition (iii).

*Remark 4.* (1) According to Iwasawa, the condition (i) in the above Corollary 2 is equivalent to the non-vanishing of the  $\ell$ -adic regulator of  $k$  (Leopoldt’s conjecture for  $(\ell, k)$ ) (see [12], p. 254).

(2) By Corollary 1 to Theorem 1 and Lemma 2,

$$|G_k(m + 1, S)|/|G_k(m, S)| = \ell^{r_2+1} |B_k(m + 1, S)| |B_k(m, S)|^{-1}$$

and  $|B_k(m + 1, S)| \geq |B_k(m, S)|$  for sufficiently large  $m$ . This gives that the essential rank of  $G_k(S) \geq r_2 + 1$  (a part of Theorem 2 of Iwasawa [12]).

**LEMMA 2.** *Let the notation and assumptions be as in Notation. Then the  $\ell$ -th power homomorphism  $f$  from  $U_k(m, S)$  to  $U_k(m + 1, S)$  induces the injection from  $B_k(m, S)$  to  $B_k(m + 1, S)$  for sufficiently large  $m$ . In particular,  $|B_k(m, S)| \leq |B_k(m + 1, S)|$  for sufficiently large  $m$ .*

*Proof.* By definition,  $U_k(m, S)^\ell \subset U_k(m + 1, S)$  for  $m \geq 1$ . Let  $x \in U_k(m, S)$  be such that  $x^\ell \in (k^\times)^{\ell^{m+1}}$ . Then  $x^\ell = y^{\ell^{m+1}}$  with a  $y \in k^\times$ , hence  $x = \zeta_1^r y^{\ell^m}$  with an  $r \in \mathbb{Z}$ . Let  $v_0 \in S_k$ . Then we see easily that

$\zeta_1 \in (k_{v_0}^\times)^{\ell^m}$  for sufficiently large  $m$ . Since  $S \supset S_k$ ,  $x \in U_k(m, S)$  implies that  $\zeta_1^r \in (k_{v_0}^\times)^{\ell^m}$ , hence  $r \equiv 0 \pmod{\ell}$ , i.e.,  $x = y^{\ell^m} \in (k^\times)^{\ell^m}$ . Therefore we have the assertion.

To apply Theorem 1 to the proof of the part “(iii)  $\Leftrightarrow$  (v)” of the main theorem, we need moreover the following Lemma 4, and for the proof of Lemma 4 we need the following

**LEMMA 3.** *Let the notation and assumptions be as above. Moreover suppose that  $\zeta_{n_0} \in k$  and  $\zeta_{n_0+1} \in k$  with  $n_0 \geq 1$ . Then  $B_k(1, S) = 0$  implies that  $B_k(\nu, S) = 0$  for  $1 \leq \nu \leq n_0$ .*

*Proof.* It suffices to prove that  $B_k(\nu + 1, S) = 0$  with a  $\nu \leq n_0 - 1$  under the assumption that  $B_k(m, S) = 0$  for  $1 \leq m \leq \nu$ . Let  $x \in U_k(\nu + 1, S)$ . Then  $B_k(\nu, S) = 0$  implies that  $x = y^{\ell^\nu}$  with a  $y \in k^\times$ . Then  $x \in U_k(\nu + 1, S)$  implies that  $y = \zeta_{v_0}^{r_\nu} z_{v_0}^{\ell}$  with  $r_\nu \in \mathbf{Z}$ ,  $z_{v_0} \in k_{v_0}^\times$  for each  $v \in S$ . Since  $\nu \leq n_0 - 1$ ,  $y \in k_{v_0}^{\ell}$  for each  $v \in S$ , hence  $y \in U_k(1, S)$ . Hence  $B_k(1, S) = 0$  implies that  $y = z^\ell$  with a  $z \in k^\times$ , hence  $x = y^{\ell^\nu} = z^{\ell^{\nu+1}}$ . This implies that  $B_k(\nu + 1, S) = 0$ .

**LEMMA 4.** *Let the notation and assumptions be as above. If  $\zeta_1 \in k$ , then suppose moreover that there exists  $v_0 \in S_k$  such that  $\zeta_{n_0+1} \in k_{v_0}$ . Then the following three statements are equivalent:*

- (i)  $B_k(\nu, S_k) = 0$  for all  $\nu \geq 1$ .
- (ii)  $|B_k^*(1, S_k)| = \ell$  or  $1$  according as  $\zeta_1 \in k$  or not.
- (iii)  $U_k^*(1, S_k) = \langle \zeta_{n_0} \rangle (k^\times)^\ell$ .

*Proof.* The equivalence of (ii) and (iii) is obvious. First suppose that (i). Let  $x \in U_k^*(1, S_k)$ . Then there exists a positive integer  $n$  such that  $x^{\ell^n} \in U_k(n + 1, S_k)$ . By (i),  $x^{\ell^n} = y^{\ell^{n+1}}$  with a  $y \in k^\times$ . Hence  $x = \zeta_{n_0}^r y^\ell$  with an  $r \in \mathbf{Z}$ . This implies that  $U_k^*(1, S_k) = \langle \zeta_{n_0} \rangle (k^\times)^\ell$ , i.e., the statement (iii) follows. Conversely suppose that (iii). We prove the assertion (i) by induction on  $\nu$ . Since  $U_k(1, S_k) \subset U_k^*(1, S_k)$ , (iii) implies that  $U_k(1, S_k) = (k^\times)^\ell$ , i.e.,  $B_k(1, S_k) = 0$ , when  $\zeta_1 \in k$ . When  $\zeta_1 \in k$ , by the assumption that  $\zeta_{n_0} \in k_{v_0}^{\ell}$  with a  $v_0 \in S_k$ , we have  $\zeta_{n_0} \in U_k(1, S_k)$ . Hence (iii) gives  $U_k(1, S_k) = (k^\times)^\ell$ , i.e.,  $B_k(1, S_k) = 0$ . Then by Lemma 3,  $B_k(n_0, S_k) = 0$  if  $n_0 \geq 1$ . Now suppose that  $B_k(\nu, S_k) = 0$  for a  $\nu \geq \max(n_0, 1)$ . Let  $x \in U_k(\nu + 1, S_k)$ . Then it follows from  $B_k(\nu, S_k) = 0$  that  $x = z^{\ell^\nu}$  for a  $z \in k^\times$ . By definition,  $z \in U_k^*(1, S_k)$ . From (iii), we obtain  $z = \zeta_{n_0}^s w^\ell$  with  $s \in \mathbf{Z}$ ,  $w \in k^\times$ . Hence  $x = z^{\ell^\nu} = w^{\ell^{\nu+1}}$ , since

$\nu \geq \max(n_0, 1)$ . This implies that  $B_k(\nu + 1, S_k) = 0$ . Therefore by induction on  $\nu$ , we obtain (i).

*Remark 5.* (1) In the above proof, we use the assumption that  $\zeta_{n_0+1} \notin k_{v_0}$  with a  $v_0 \in S_k$  if  $n_0 \geq 1$ , only to prove that (ii) implies (i).

(2) If  $B_k(1, S) = 0$  and if  $\zeta_1 \in k$ , then there exists  $v_0 \in S$  such that  $\zeta_{n_0} \in k_{v_0}^\ell$ . In fact, if  $\zeta_{n_0} \in k_v^\ell$  for all  $v \in S$ , then  $\zeta_{n_0} \in U_k(1, S)$  and  $\zeta_{n_0} \in k^\ell$ ; this implies that  $B_k(1, S) \neq 0$ ; this is a contradiction.

**§2. A relation between  $B_k(m, S)$  and the class number of a cyclotomic  $Z_\ell$ -extension**

**LEMMA 5.** *Let  $\ell, k, \zeta_i, n_0, S$  and  $B_k(m, S)$  be as in Notation and let  $m$  be a positive integer. Suppose that there exists a  $v_0 \in S$  such that  $\zeta_{n_0+1} \notin k_{v_0}$ . Then  $B_k(m, S) = 0$  implies that  $B_k(i, S) = 0$  for  $1 \leq i \leq m$ .*

*Proof.* Let  $x \in U_k(i, S)$ , and put  $z = x^{\ell^{m-i}}$ , then  $z \in U_k(m, S)$ . Since  $B_k(m, S) = 0$ , there exists a  $y \in k^\times$  such that  $z = y^{\ell^m}$ , hence  $x = \zeta_{n_0}^r y^{\ell^i}$  with some  $r \in Z$ . Since  $x \in U_k(i, S)$ ,  $\zeta_{n_0}^r \in k_{v_0}^{\ell^i}$ . This implies  $\zeta_{n_0}^r = \zeta_{n_0}^{s\ell^i}$  with some  $s \in Z$ , since  $\zeta_{n_0} \in k_{v_0}$  and  $\zeta_{n_0+1} \notin k_{v_0}$ ; hence  $x \in k^{\ell^i}$ . Therefore  $B_k(i, S) = 0$ .

**LEMMA 6.** *Let  $\ell, k, S$  and  $\zeta_i$  be as in Notation, and let  $m_0 \in N$  be such that  $\zeta_{m_0} \notin k_v$  for all  $v \in S$ . Then  $B_k(m_0, S) = 0$  implies that  $B_k(m, S) = 0$  for all  $m \geq m_0$ .*

*Proof.* We shall prove the lemma by induction on  $m$ . If  $m = m_0$ , then the assertion is valid by assumption. Suppose  $m > m_0$ , and let  $x \in U_k(m, S)$ . Since  $B_k(m - 1, S) = 0$  by the induction hypothesis, there exists a  $y \in k^\times$  such that  $x = y^{\ell^{m-1}}$ . Since  $x \in k_v^{\ell^m}$  for all  $v \in S$ , there exists  $r_v \in Z$  and  $a_v \in k_v^\times$  such that  $y = \zeta_{n_0}^{r_v} \cdot a_v^\ell$ . We have  $n_v < m_0$  for all  $v \in S$ , since  $\zeta_{m_0} \notin k_v$ . Hence  $y^{\ell^{m_0-1}} = a_v^{\ell^{m_0}}$  all  $v \in S$ , so  $y^{\ell^{m_0-1}} \in U_k(m_0, S)$ . Since  $B_k(m_0, S) = 0$ , there exists a  $z \in k^\times$  such that  $y^{\ell^{m_0-1}} = z^{\ell^{m_0}}$ , hence  $x = z^{\ell^m} \in k^{\ell^m}$ . This implies  $B_k(m, S) = 0$ . By induction on  $m$ , we have the assertion.

**LEMMA 7 (Iwasawa, Yokoyama).** *Let  $\ell$  and  $k$  be as in Notation and let  $K/k$  be a finite Galois extension of  $\ell$ -power degree. Let  $v_0$  be a non-archimedean prime divisor of  $k$  and let  $V_0$  be an extension of  $v_0$  to  $K$ . Let  $M/k$  (resp.  $M'/k$ ) be a finite Galois extension of  $\ell$ -power degree containing  $K$  such that  $V_0$  is unramified in  $M$  (resp.  $V_0$  is completely*

decomposed in  $M'$ ). Assume that  $M \cong K$  (resp.  $M' \cong K$ ). Then there exists a cyclic extension  $L$  of  $k$  of degree  $\ell$  in  $M$  (resp.  $M'$ ) where  $v_0$  is unramified (resp.  $v_0$  is completely decomposed).

The above Lemma 7 follows directly from the proofs of Iwasawa [8] and [Yokoyama [24], Theorem 4] (see also [Iwasawa [11], § 6–3, Lemma, (ii)]).

**THEOREM 2.** *Let  $\ell$  be a prime number. Let  $k, n_0, S, S^i, k_i$  and  $Cl_k(S)$  be as in Notation and assume that  $k$  contains a primitive 4-th root of unity if  $\ell = 2$ . Let  $m$  be a positive integer. Then the following statements hold:*

(1) (Remark in Neukirch [20], Satz (8.1)). *If  $|Cl_{k_m}(S^m)| \equiv 0 \pmod{\ell}$ , then  $B_k(m, S) = 0$ .*

(2) *Assume moreover that  $\zeta_1 \in k$  and that there exists a  $v_0 \in S$  such that  $\zeta_{n_0+1} \notin k_{v_0}$ . Then  $B_k(m, S) = 0$  implies  $|Cl_{k_m}(S^m)| \equiv 0 \pmod{\ell}$ .*

*Proof.* (2) It is sufficient to prove that  $B_k(m, S) \neq 0$  under the assumption  $|Cl_{k_m}(S^m)| \equiv 0 \pmod{\ell}$ . Let  $M/k_m$  be the maximum unramified abelian  $\ell$ -extension of  $k_m$  where any prime divisor in  $S^m$  is completely decomposed. Clearly  $M/k$  is a Galois extension. By class field theory,  $|Cl_{k_m}(S^m)| \equiv 0 \pmod{\ell}$  implies that  $M \cong k_m$ . Hence by Lemma 7, there exists a cyclic extension  $K$  of  $k$  of degree  $\ell$  in  $M$  where  $v_0$  is completely decomposed. Since  $\zeta_{n_0+1} \notin k_{v_0}$ ,  $v_0$  is not completely decomposed in  $k_{n_0+1}/k$ . Therefore  $k_m \cap K = k$ , so  $[Kk_m : k_m] = \ell$ . Let  $x \in k^\times$  be such that  $K = k(\sqrt[\ell]{x})$ . Since  $k_m/k$  is  $S$ -ramified,  $K/k$  is  $S$ -ramified. Put  $z = x^{\ell^{m-1}}$ . Let  $v \in S$ , and let  $V$  be an extension of  $v$  to  $k_m$ . Since  $V$  is completely decomposed in  $M/k_m$  and  $Kk_m \subset M$ , we have  $x \in (k_m)_V^\ell$ . Hence by Kummer theory,  $x = a^\ell \zeta_i^j$  with  $a \in k_v^\times$ ,  $j \in \mathbf{Z}$ ,  $i \in \mathbf{N}$ ,  $i < m$ . Hence  $z = x^{\ell^{m-1}} = a^{\ell^m} \in k_v^{\ell^m}$ . Now let  $v \in S$  be any non-archimedean prime divisor of  $k$ . Since  $K/k$  is  $S$ -ramified,  $\text{ord}_v(x) \equiv 0 \pmod{\ell}$ , so  $\text{ord}_v(z) \equiv 0 \pmod{\ell^m}$ , where  $\text{ord}_v$  is the normalized additive valuation of  $k$  with respect to  $v$ . Therefore  $z \in U_k(m, S)$ . On the other hand,  $z \notin k^{\ell^m}$ . In fact, if  $z \in k^{\ell^m}$ , then  $z = x^{\ell^{m-1}} = w^{\ell^m}$  with a  $w \in k^\times$ , hence  $x = \zeta_{m-1}^r w^\ell$  with some  $r \in \mathbf{Z}$ ; this implies  $K \subset k_m$ , but this contradicts that  $[Kk_m : k_m] = \ell$ ; so  $z \notin k^{\ell^m}$ . Therefore  $B_k(m, S) \neq 0$ .

**LEMMA 8.** *Let  $\ell, k, n_0, \zeta_i, k_i, S_k, S, S^m$  and  $Cl_k(S)$  be as in Notation and let  $m \geq n_0$  be a rational integer. Assume that  $\zeta_1 \in k$ . Assume more-*

over that any prime divisor in  $S^m - S_{k_m}$  is not decomposed in  $k_{m+1}/k_m$  and that there exists a  $v_0 \in S_{k_m}$  not decomposed in  $k_{m+1}/k_m$ . Then  $|Cl_{k_{m+1}}(S^{m+1})| \equiv 0 \pmod{\ell}$  implies that  $|Cl_{k_m}(S_{k_m})| \equiv 0 \pmod{\ell}$ .

*Proof.* It is sufficient to prove that  $|Cl_{k_{m+1}}(S^{m+1})| \equiv 0$  under the assumption that  $|Cl_{k_m}(S_{k_m})| \equiv 0 \pmod{\ell}$ . By class field theory, this condition implies that there exists an unramified cyclic extension  $K/k_m$  of degree  $\ell$  where any prime divisor in  $S_{k_m}$  is completely decomposed. From the existence of  $v_0$ , it follows that  $Kk_{m+1}/k_{m+1}$  is an unramified cyclic extension of degree  $\ell$  where any prime divisor in  $S_{k_{m+1}}$  is completely decomposed. Now suppose that there exists a  $V_1 \in S^{m+1} - S_{k_{m+1}}$  not decomposed in  $Kk_{m+1}/k_{m+1}$ . Let  $v_1$  be the restriction of  $V_1$  to  $k_m$ . Since any prime divisor in  $S^m - S_{k_m}$  is not decomposed in  $k_{m+1}/k_m$ ,  $v_1$  is unramified and not decomposed in  $Kk_{m+1}/k_m$ , hence  $Kk_{m+1}/k_m$  is cyclic of degree  $\ell^2$ . But this is a contradiction. Therefore any prime divisor in  $S^{m+1}$  is completely decomposed in  $Kk_{m+1}/k_{m+1}$ , so by class field theory,  $|Cl_{k_{m+1}}(S^{m+1})| \equiv 0 \pmod{\ell}$ .

By Lemmas 5, 6, 8 and Theorem 2, we obtain the following

**THEOREM 3.** *Let  $\ell, k, S_k, S, \zeta_i, n_0, k_i, S^i, Cl_k(S)$  and  $B_k(m, S)$  be as in Notation. Assume that  $\zeta_1 \in k$  and that there exists a  $v_0 \in S_k$  such that  $\zeta_{n_0+1} \in k_{v_0}$ . Then the following statements (1) ~ (8) are equivalent:*

- (1)  $B_k(m, S) = 0$  for all  $m \in N$ .
- (2)  $B_k(m, S_k) = 0$  for all  $m \in N$ .
- (3)  $|Cl_{k_m}(S^m)| \equiv 0 \pmod{\ell}$  for all  $m \in N$ .
- (4)  $|Cl_{k_m}(S_{k_m})| \equiv 0 \pmod{\ell}$  for all  $m \in N$ .
- (5)  $B_k(m_0, S) = 0$  for some  $m_0 \geq 1$  such that  $\zeta_{m_0} \in k_v$  for all  $v \in S$ .
- (6)  $B_k(m_0, S_k) = 0$  for some  $m_0 \geq 1$  such that  $\zeta_{m_0} \in k_v$  for all  $v \in S_k$ .
- (7)  $|Cl_{k_{m_0}}(S^{m_0})| \equiv 0 \pmod{\ell}$  for some  $m_0 \geq 1$  such that  $\zeta_{m_0} \in k_v$  for all  $v \in S$ .
- (8)  $|Cl_{k_{m_0}}(S_{k_{m_0}})| \equiv 0 \pmod{\ell}$  for some  $m_0 \geq 1$  such that  $\zeta_{m_0} \in k_v$  for all  $v \in S_k$ .

**§ 3. Main Theorem**

**MAIN THEOREM.** *Let the notation be as in Notation and suppose that  $k$  contains a primitive  $\ell$ -th root of unity and that there exists  $v_0 \in S_k$  such that  $W_{v_0} = W$ . Then the following statements (i) ~ (vi) are equivalent:*

- (i)  $|Cl_{k_i}(S_k)| \equiv 0 \pmod{\ell}$  for all  $i \geq 1$ ;
- (ii)  $|Cl_{k_i}(S)| \equiv 0 \pmod{\ell}$  for all  $i \geq 1$ ;
- (iii)  $B_k(m, S_k) = 0$  for all  $m \geq 1$ ;
- (iv)  $B_k(m, S) = 0$  for all  $m \geq 1$ ;
- (v) The number of independent cyclic extensions of  $k$  of degree  $\ell$ , which can be extended to cyclic extensions of  $k$  of degree  $\ell^n$  for any  $n \in \mathbb{N}$ , is equal to  $r_2 + 1$ ;
- (vi)  $G_k(S) \cong (\prod_{v \in S - \{v_0\}} W_v) \times \mathbb{Z}_\ell \times \cdots \times \mathbb{Z}_\ell$  ( $r_2 + 1$  copies).

*Proof.* It is contained in Theorem 3 that the statements (i), (ii), (iii) and (iv) are equivalent each other. It is easily verified that the statement (vi) in the main theorem is equivalent to that

$$|G_k(\nu, S)| = \ell^{\nu(r_2+1)} \left( \prod_{v \in S} w_{\nu, v} \right) w_\nu^{-1} \quad \text{for all } \nu \geq 1.$$

By (i) of Corollary 1 to Theorem 1, this is equivalent to that  $|B_k(\nu, S)| = 1$  for all  $\nu \geq 1$ , i.e., the statement (iv) in the main theorem. Under the assumption that  $\zeta_{n_0} \notin k_{v_0}^\ell$  with a  $v_0 \in S_k$ , it is obvious that the statement (v) is equivalent to that  $|H_k(1)| = \ell^{r_2+1}$ . By (ii) of Corollary 1 to Theorem 1, this is equivalent to  $|B_k^*(1, S_k)| = \ell$ , since  $\zeta_1 \in k$ . Hence by Lemma 4, this is equivalent to (iii).

*Remark 6.* (1) If  $|Cl_k(S_k)| \equiv 0 \pmod{\ell}$  and if  $\zeta_1 \in k$ , then there exists a  $v_0 \in S_k$  such that  $W_{v_0} = W$ . In fact, if  $W_v \neq W$  for all  $v \in S_k$ , then  $k_{n_0+1} = k(\sqrt[\ell]{\zeta_{n_0}})$  is an unramified cyclic extension of  $k$  of degree  $\ell$  where any place  $v \in S_k$  is fully decomposed. By class field theory, this implies that  $|Cl_k(S_k)| \equiv 0 \pmod{\ell}$ , and this is a contradiction. Hence there exists a  $v_0 \in S_k$  such that  $W_{v_0} = W$ .

(2) The above proof of the statements of “(iii)  $\Leftrightarrow$  (v)” and “(iv)  $\Leftrightarrow$  (vi)” of the main theorem are also valid in the case where  $\zeta_1 \notin k$ .

**§4. Existence of finite algebraic number fields  $k$  satisfying the condition (i) in the main theorem and the condition  $|S_k| \geq n$  for each  $n \geq 1$  and each regular prime number  $\ell$**

By Iwasawa [10], we see easily that for each regular prime number  $\ell$  there exist infinitely many finite algebraic number fields  $k$  satisfying the condition (i) in the main theorem and the condition  $|S_k| = 1$ . But when  $S = S_k$  and  $|S_k| = 1$ , the part “(i)  $\Leftrightarrow$  (vi)” of the main theorem

follows also from [Šafarevič [22], § 4] and [Brumer [4], Corollary 3.3], hence it is natural to consider whether there exists a finite algebraic number field  $k$  satisfying the condition (i) in the main theorem and the condition  $|S_k| > 1$ . Note that Bertrandias-Payan [2] gave some examples satisfying the condition (v) in the main theorem and the condition  $|S_k| = 2$  for  $\ell = 3, 5$ .

The purpose of this section is to prove the following two theorems.

**THEOREM 4.** *Let  $\ell$  and  $\zeta_i$  be as in Notation. Let  $k/\mathbf{Q}$  be a finite Galois extension where  $\ell$  is completely decomposed. Put  $k_i = k(\zeta_i)$  with  $i \geq 1$ . Suppose that  $|Cl_{k_1}| \not\equiv 0 \pmod{\ell}$ . Then the following two statements are equivalent:*

- (i)  $|Cl_{k_i}| \equiv 0 \pmod{\ell}$  for all  $i \geq 2$ .
- (ii)  $k$  is totally real.

**THEOREM 5.** *For each regular prime number  $\ell \neq 2$  and each  $n \in \mathbf{N}$ , there exist infinitely many finite algebraic number fields  $k$  satisfying the following conditions (1) ~ (4):*

- (1)  $\zeta_1 \in k$ ;
- (2)  $k/\mathbf{Q}(\zeta_1)$  is not a Galois extension, and  $[k:\mathbf{Q}(\zeta_1)] = \ell^s$  with some  $s \geq 2$ .
- (3)  $|Cl_{k_i}| \equiv 0 \pmod{\ell}$  for all  $i \geq 1$ ;
- (4)  $|S_k| \geq n$ ,

where  $\zeta_i, k_i, Cl_{k_i}$  and  $S_k$  are as in Notation.

**EXAMPLES.** (1) Put  $\ell = 3$  and  $k = \mathbf{Q}(\sqrt{7})$ . Then  $\ell$  is decomposed in  $k$  and  $|Cl_{k_1}| \equiv 0 \pmod{\ell}$ . Therefore by Theorem 4,  $|Cl_{k_i}| \equiv 0 \pmod{\ell}$  for all  $i \geq 2$ .

(2) Put  $\ell = 3$  and  $k = \mathbf{Q}(\sqrt{-2})$ . Then  $\ell$  is decomposed in  $k$  and  $|Cl_{k_1}| \equiv 0 \pmod{\ell}$ . But by Theorem 4,  $|Cl_{k_2}| \equiv 0 \pmod{\ell}$ , hence  $|Cl_{k_i}| \equiv 0 \pmod{\ell}$  for all  $i \geq 2$ .

(3) Put  $\ell = 3$  and  $k = \mathbf{Q}(\zeta_1, \sqrt[3]{(2 + 3\sqrt{-3})(4 + 3\sqrt{-3})})$ . Then exactly two primes  $(2 + 3\sqrt{-3})$  and  $(4 + 3\sqrt{-3})$  in  $\mathbf{Q}(\zeta_1)$  are ramified in  $k/\mathbf{Q}(\zeta_1)$ , and  $|S_k| = 3$ . Since any prime in  $S_k$  is not decomposed in  $k_2$  and since  $|Cl_{\mathbf{Q}(\zeta_i)}| \equiv 0 \pmod{\ell}$  for all  $i \geq 1$ , we see by Lemma 10 that  $|Cl_{k_i}| \equiv 0 \pmod{\ell}$  for all  $i \geq 1$ . Therefore by the main theorem,  $G_k(S_k) \cong \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times (3) \times (3)$ . We can make many such examples in the way of the proof of Theorem 5.

**5.1. Generalizations of Iwasawa-Yokoyama’s theorem on class numbers.**

In this section, we state two lemmas on the  $\ell$ -rank of the ideal class group and class numbers (see Lemmas 9 and 10), which are considered as generalizations of Iwasawa [10] and [Yokoyama [24], Theorem 4]. In §§ 5.2–5.3, we shall use these lemmas for the proofs of Theorems 4 and 5.

**LEMMA 9 ([18], Theorem).** *Let  $\ell$  be a prime number and let  $k$  be a finite algebraic number field. Let  $Cl_k$  denote the ideal class group of  $k$ . Let  $k_n/k$  be a ramified cyclic extension of degree  $\ell^n$  with  $n \in \mathbb{N}$  and let  $k_i/k$  be the sub-extension of degree  $\ell^i$  for  $0 \leq i \leq n$ . Suppose that the following two conditions are satisfied:*

- (i) *Any archimedean prime divisor of  $k$  is unramified in  $k_n$ ;*
- (ii) *Any prime divisor of  $k$  ramified in  $k_n$  is fully ramified in  $k_n$ .*

*Then the equality  $\ell$ -rank  $Cl_k = \ell$ -rank  $Cl_{k_1}$  implies that  $\ell$ -rank  $Cl_k = \ell$ -rank  $Cl_{k_i}$  for  $1 \leq i \leq n$ . In particular, the conditions  $|Cl_k| \equiv 0 \pmod{\ell}$  and  $|Cl_{k_1}| \equiv 0 \pmod{\ell}$  imply that  $|Cl_{k_i}| \equiv 0 \pmod{\ell}$  for  $1 \leq i \leq n$ .*

Note that the condition (i) in Lemma 9 is always satisfied if  $\ell \neq 2$  and that there exists a finite cyclic extension  $k_n/k$  of degree  $\ell^n$  such that  $|Cl_k| \equiv 0 \pmod{\ell}$  and  $|Cl_{k_1}| \equiv 0 \pmod{\ell}$  (cf. (2) of Examples of Theorem 4).

**LEMMA 10.** *Let  $\ell, k, \zeta_i, n_0$  and  $Cl_k$  be as in Notation and let  $v_1$  and  $v_2$  be two distinct non-archimedean prime divisors of  $k$  such that  $\zeta_{n_0+1} \in k_{v_2}$  and such that  $v_2$  does not lie above  $\ell$ . Let  $K$  be a finite Galois extension of  $k$  of  $\ell$ -power degree, unramified outside  $v_1$  and  $v_2$ , and let  $G = G(K/k)$ . Then the following two statements hold:*

- (1) *If  $|Cl_k| \equiv 0 \pmod{\ell}$ , then  $|Cl_K| \equiv 0 \pmod{\ell}$ .*
- (2) *Suppose moreover that  $K/k$  is cyclic and that  $v_2$  is fully ramified in  $K/k$ . Then  $|Cl_K^G| = |Cl_k|$ , where  $Cl_K^G$  is the subgroup of  $Cl_K$  of all elements invariant by  $G$ .*

For the proof of Lemma 10, we use Iwasawa-Yokoyama’s Lemma 7 and the following

**LEMMA 11.** *Let  $\ell, k, \zeta_i$  and  $n_0$  be as in Lemma 10 and let  $v_0$  be a non-archimedean prime divisor of  $k$  not lying above  $\ell$ . Suppose that  $\zeta_{n_0+1} \in k_{v_0}$ . Let  $K/k$  be a cyclic extension of degree  $\ell$ , unramified outside*

$v_0$ . Then  $K/k$  is unramified.

*Proof.* Let  $J$  and  $U_T$  be as in Notation. Let  $N$  be the subgroup of  $J$  associated with  $K$ , by class field theory. Since  $K/k$  is unramified outside  $v_0$ ,  $U_S J^{\ell} k^{\times} \subset N$ , where  $S = \{v_0\}$ . Let  $a = (a_v) \in J$  be such that  $a_{v_0} = 1$  and  $a_v = \zeta_{n_0}$  for  $v \neq v_0$ , and let  $b = (b_v) \in J$  such that  $b_{v_0} = \zeta_{n_0}$  and  $b_v = 1$  for  $v \neq v_0$ . Then  $\zeta_{n_0} = ab$  in  $J$ .  $a \in U_S$  implies that  $b \in U_S k^{\times}$ , so  $b \in N$ . Since  $v_0$  does not lie above  $\ell$ ,  $U_{v_0}^{(1)} \subset J^{\ell} \subset N$ , where  $U_{v_0}^{(1)}$  is the subgroup of  $U_{v_0}$  of principal units of  $k_{v_0}$ . Since  $\zeta_{n_0} \notin k_{v_0}^{\ell}$ , the conditions  $b \in N$  and  $U_{v_0}^{(1)} \subset N$  imply that  $U_{v_0} \subset N$ . Therefore  $v_0$  is unramified in  $K$ .

*Remark 7.* Lemma 11 can be also proved by using [Šafarevič [22], Theorem 1].

*Proof of Lemma 10.* (1) It is enough to prove that  $|Cl_k| \equiv 0 \pmod{\ell}$  under the assumption that  $|Cl_k| \equiv 0 \pmod{\ell}$ . Let  $M$  be the maximum unramified abelian extension of  $K$  of  $\ell$ -power degree. Obviously  $M/k$  is a Galois extension. Then by class field theory,  $|Cl_K| \equiv 0 \pmod{\ell}$  implies that  $M \neq K$ , so by Lemma 7, there exists a cyclic extension  $L$  of  $k$  in  $M$  where  $v_1$  is unramified. Since  $L \subset M$ ,  $L/k$  is unramified outside  $v_2$ , so by Lemma 11,  $L/k$  is unramified; hence by class field theory,  $|Cl_k| \equiv 0 \pmod{\ell}$ .

(2) Put  $N_{K/k}(K^{\times}) \cap E_k = A$  and  $[K:k] = \ell^n$ , where  $E_k$  is the group of units of  $k$ . Since  $v_2$  is fully ramified in  $K$ , it follows from Lemma 11 that  $v_1$  is fully ramified in  $K$ . Hence by the well-known formula of  $|Cl_K^G|$  (see Yokoi [23]), we have  $|Cl_K^G| = [E_k:A]^{-1} \ell^n |Cl_k|$ . Now we shall show that  $E_k/A$  is generated by  $\zeta_{n_0} \pmod A$  and that  $[E_k:A] = \ell^n$ . Since  $\zeta_{n_0} \notin k_{v_2}^{\ell}$  and since  $v_2$  does not lie above  $\ell$ , we see easily that for any  $\varepsilon \in E_k$  there exists an  $r \in \mathbb{Z}$  such that  $\varepsilon \zeta_{n_0}^{-r} \in k_{v_2}^{\ell^n}$ . So, since  $K/k$  is unramified outside  $v_1$  and  $v_2$ ,  $\varepsilon \zeta_{n_0}^{-r} \in N_{K_V/k_V}(K_V^{\times})$  for all  $v \neq v_1$ , where  $V$  is an extension of  $v$  to  $K$ . Therefore by Hasse's norm theorem,  $\varepsilon \zeta_{n_0}^{-r} \in N_{K/k}(K^{\times})$ . This implies that  $E_k/A$  is generated by  $\zeta_{n_0} \pmod A$ . Suppose that  $\zeta_{n_0}^s \in A$  with an  $s \in \mathbb{Z}$ . Then  $\zeta_{n_0}^s \in N_{K_{V_2}/k_{v_2}}(K_{V_2}^{\times})$ , where  $V_2$  is an extension of  $v_2$  to  $K$ . Since  $K_{V_2}/k_{v_2}$  is fully ramified and cyclic of degree  $\ell^n$  and since  $v_2$  does not lie above  $\ell$ ,  $\zeta_{n_0}^s \in N_{K_{V_2}/k_{v_2}}(K_{V_2}^{\times})$  implies  $\zeta_{n_0}^s \in (k_{v_2}^{\times})^{\ell^n}$ , so  $s \equiv 0 \pmod{\ell^n}$ , since  $\zeta_{n_0} \notin k_{v_2}^{\ell}$ ; hence  $[E_k:A] = \ell^n$ . Therefore by the above formula,  $|Cl_K^G| = |Cl_k|$ .

5.2. Proof of Theorem 4.

We prove Theorem 4, using Lemma 9, a formula of the number of ambig ideals (see Yokoi [23]), Hasse’s norm theorem and the well-known translation theorem in local class field theory (see e.g., Weil [26], Chap. XII, § 3, Corollary 3 to Theorem 4).

*Proof of Theorem 4.* Put  $g = [k : \mathbf{Q}]$ . Let  $v_1, \dots, v_g$  denote all the primes of  $k$  lying above  $\ell$ . Then  $v_j$  is fully ramified in  $k_1$  for  $1 \leq j \leq g$ . Let  $V_j$  denote a unique extension of  $v_j$  to  $k_1$  for  $1 \leq j \leq g$ . Let  $E$  and  $E_i$  denote the group of units of  $k$  and  $k_i$  with  $i \geq 1$ , respectively. Since  $\ell$  is completely decomposed in  $k$  and since  $\ell$  is fully ramified in  $\mathbf{Q}(\zeta_1)$ ,  $k \cap \mathbf{Q}(\zeta_1) = \mathbf{Q}$ . Put  $A = E_1 \cap N_{k_2/k_1}(k_2^\times)$ . First we shall show that  $A = E_1 \cap N_{k_1/k}^{-1}(E^\ell)$ . Since  $N_{\mathbf{Q}_\ell(\zeta_2)/\mathbf{Q}_\ell}(\mathbf{Q}_\ell(\zeta_2)^\times) = \ell^{\mathbf{Z}} \times \{x \in \mathbf{Q}_\ell^\times \mid x \equiv 1 \pmod{\ell^2}\}$ , we see by Hasse’s norm theorem and the translation theorem in local class field theory that

$$(*) \quad A = \{x \in E_1 \mid N_{(k_1)_{V_j}/\mathbf{Q}_\ell}(x) \equiv 1 \pmod{\ell^2} \text{ for } 1 \leq j \leq g\}.$$

Let  $x \in E_1 \cap N_{k_1/k}^{-1}(E^\ell)$ . Then  $N_{k_1/k}(x) \in E^\ell$ . Since  $(k_1)_{V_j} = \mathbf{Q}_\ell(\zeta_1)$  and  $k_{v_j} = \mathbf{Q}_\ell$ ,  $N_{(k_1)_{V_j}/\mathbf{Q}_\ell}(x) \equiv 1 \pmod{\ell}$ . Hence  $N_{k_1/k}(x) \in E^\ell$  implies that  $N_{(k_1)_{V_j}/k_{v_j}}(x) \equiv 1 \pmod{\ell^2}$ , i.e., that  $x \in A$ . Conversely let  $x \in A$ , and put  $y = N_{k_1/k}(x)$ . Then (\*) implies that  $y \in k_{v_i}^\ell$  for  $1 \leq i \leq g$ . Hence  $k_1(\ell\sqrt{y})/k_1$  is unramified. Since  $|Cl_{k_1}| \equiv 0 \pmod{\ell}$ ,  $k_1(\ell\sqrt{y}) = k_1$ , hence  $y \in k_1^\ell$ , so  $y \in E_1^\ell$ . Making  $N_{k_1/k}$  operate on  $y \in E_1^\ell$ ,  $y^{\ell-1} \in E^\ell$ , so  $y \in E^\ell$ , i.e.,  $x \in E_1 \cap N_{k_1/k}^{-1}(E^\ell)$ . Therefore

$$(**) \quad A = E_1 \cap N_{k_1/k}^{-1}(E^\ell).$$

The norm map  $N_{k_1/k}$  induces a linear map  $f$  from a vector space  $E_1/E_1^\ell$  to a vector space  $E/E^\ell$  over  $F_\ell$  in the natural way. Since  $E^{\ell-1} \subset N_{k_1/k}(E_1)$  and since  $E^{\ell-1}E^\ell = E$ ,  $f$  is surjective. Since  $A \supset E_1^\ell$ , (\*\*) implies that  $\text{Ker } f = A/E_1^\ell$ . Hence  $[E_1 : A] = [E : E^\ell] = \ell^{r_1+r_2-1}$ , where  $r_1$  and  $r_2$  denote the numbers of real places and complex places of  $k$ , respectively. By the formula of the number of ambig ideal classes (see Yokoi [23]),

$$|Cl_{k_2}^G| = |Cl_{k_1}| \frac{\ell^{g-1}}{[E_1 : A]} = |Cl_{k_1}| \ell^{r_2},$$

where  $G = G(k_2/k_1)$ . By the theory of  $\ell$ -groups,  $|Cl_{k_2}^G| \equiv 0 \pmod{\ell}$  if and only if  $|Cl_{k_2}| \equiv 0 \pmod{\ell}$ , hence this implies that  $|Cl_{k_2}| \equiv 0 \pmod{\ell}$  if and only if  $r_2 = 0$ . By Lemma 9,  $|Cl_{k_2}| \equiv 0 \pmod{\ell}$  is equivalent to

that  $|Cl_{k_i}| \equiv 0 \pmod{\ell}$  for all  $i \geq 2$ .

**5.3. Proof of Theorem 5.**

We use the following two lemmas and Theorem 6.

**LEMMA 12.** *Let  $\ell, k, \zeta_i$  and  $Cl_k$  be as in Notation. Put  $|Cl_k| = h$  and assume that  $h \equiv 0 \pmod{\ell}$ . Let  $T$  be a finite set of non-archimedean prime divisors of  $k$  not lying above  $\ell$ , and let  $K$  be a cyclic extension of  $k$  of degree  $\ell$ , unramified outside  $T$ . Let  $\mathfrak{p}$  be a prime ideal of  $k$  lying above  $\ell$  and let  $y \in k^\times$  be such that  $(y) = \mathfrak{p}^h$ . Suppose that  $y \in k_v^\ell$  for all  $v \in T$ . Then  $\mathfrak{p}$  is completely decomposed in  $K$ .*

*Proof.* Let  $N$  be the subgroup of  $J$  associated with  $K$ , by class field theory. Since  $K/k$  is unramified outside  $T$ ,  $N \supset U_T J^\ell k^\times$ . Let  $a = (a_v) \in J$  be such that  $a_v = y$  if  $v = \mathfrak{p}$  and  $a_v = 1$  otherwise, let  $b = (b_v) \in J$  be such that  $b_v = 1$  if  $v \in T \cup \{\mathfrak{p}\}$  and  $b_v = y$  otherwise, and let  $c = (c_v) \in J$  be such that  $c_v = y$  if  $v \in T$  and  $c_v = 1$  otherwise. Since  $b \in U_T$  by definition and since  $c \in J^\ell$  by assumption, the equation  $y = abc$  in  $J$  implies that  $a \in U_T J^\ell k^\times$ . Since  $(y) = \mathfrak{p}^h$ , we can write  $y = u\pi_v^h$  in  $k_v$  with a  $u \in U_v$  and a prime element  $\pi_v$  of  $k_v$ . Since  $U_v \subset U_T J^\ell k^\times$ ,  $a \in U_T J^\ell k^\times$  implies that  $\pi_v^h \in U_T J^\ell k^\times$ . Since  $h \equiv 0 \pmod{\ell}$ , there exists an  $h' \in \mathbb{Z}$  such that  $h'h \equiv 1 \pmod{\ell}$ . By taking the  $h'$ -th power of  $\pi_v^h \in U_T J^\ell k^\times$ , we have  $\pi_v \in U_T J^\ell k^\times$ . Hence  $k_v^\times \subset U_T J^\ell k^\times \subset N$ . By class field theory, this implies that  $\mathfrak{p}$  is completely decomposed in  $K$ .

**LEMMA 13.** *Let  $\ell, k, r_1, r_2, \zeta_i, n_0$  and  $Cl_k$  be as in Notation. Assume that  $\zeta_1 \in k$  and that  $h \equiv 0 \pmod{\ell}$ , where  $h = |Cl_k|$ . Let  $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_s$  be all the prime ideals of  $k$  lying above  $\ell$ , and let  $y_i \in k^\times$  be such that  $(y_i) = \mathfrak{p}_i^h$  for  $i = 1, 2, \dots, s$ . Let  $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{r-1}$  be a system of the fundamental units of  $k$ , where  $r = r_1 + r_2$ . Then there exist infinitely many prime divisors  $v$  of  $k$  satisfying the following conditions (1) ~ (4):*

- (1)  $v$  does not lie above  $\ell$ .
- (2)  $\varepsilon_i \in k_v^\ell$  for  $i = 1, 2, \dots, r - 1$ , and  $y_j \in k_v^\ell$  for  $j = 1, 2, \dots, s$ .
- (3)  $\zeta_{n_0} \notin k_v^\ell$ .
- (4) The degree of  $v$  is 1.

*Proof.* Put  $M = k(\sqrt[\ell]{\varepsilon_1}, \dots, \sqrt[\ell]{\varepsilon_{r-1}}, \sqrt[\ell]{y_1}, \dots, \sqrt[\ell]{y_s})$ . Clearly  $M$  and  $k(\zeta_{n_0+1})$  are linearly disjoint over  $k$ . Put  $M_1 = M(\zeta_{n_0+1})$  and let  $\sigma$  be a generator of  $G(M_1/M)$ . By Čebotarev's density theorem, there exist

infinitely many prime divisors  $V$  of  $M_1$  such that the Frobenius automorphism of  $V$  with respect to  $k$  is  $\sigma$ . If  $v$  is the restriction of  $V$  to  $k$ , then  $v$  satisfies the above conditions (2) and (3). We can take such  $v$  satisfying (1) and (4).

**THEOREM 6.** *Let the notation and assumptions be as in Lemma 13. Let  $v_1$  and  $v_2$  be two distinct prime divisors of  $k$  satisfying the conditions (1) ~ (3) in Lemma 13. Then there exists one and only one cyclic extension  $K$  of  $k$  of degree  $\ell$ , unramified outside  $v_1$  and  $v_2$ . The extension  $K/k$  satisfies the following four conditions (a) ~ (d):*

- (a)  $v_1$  and  $v_2$  are fully ramified in  $K$ .
- (b) Any prime divisor in  $S_k$  is completely decomposed in  $K$ .
- (c)  $v_1$  and  $v_2$  are not decomposed in  $k_\infty$ , where  $k_i = k(\zeta_i)$  and  $k_\infty = \bigcup_{i=1}^\infty k_i$ .
- (d)  $|Cl_K| \not\equiv 0 \pmod{\ell}$ . If  $|Cl_{k_i}| \equiv 0 \pmod{\ell}$  for an  $i \in N$ , then  $|Cl_{K_i}| \equiv 0 \pmod{\ell}$ , where  $K_i = K(\zeta_i)$ .

*Proof.* Put  $T = \{v_1, v_2\}$  and  $T_i = \{v_i\}$  for  $i = 1, 2$ . By [Šafarevič [19], Theorem 1],  $\text{rank } G_k(T) = 2 - r_2 + \dim_{F_i} B_k(1, T)$ . Since  $|Cl_k| \not\equiv 0 \pmod{\ell}$ , we see easily that  $B_k(1, T) \cong \{\varepsilon \in E_k \mid \varepsilon \in k_v^\ell \text{ for all } v \in T\} / E_k^\ell$ . Hence by the definition of  $T$ ,  $\dim_{F_i} B_k(1, T) = r_2 - 1$ . Therefore  $\text{rank } G_k(T) = 1$ . This implies that there exists one and only one cyclic extension  $K$  of  $k$  of degree  $\ell$ , unramified outside  $v_1$  and  $v_2$ . Similarly,  $\text{rank } G_k(T_i) = 0$  for  $i = 1, 2$ . This implies the condition (a). Note that the condition (a) follows also from Lemma 11. The condition (b) follows from Lemma 12 and the condition (2) in Lemma 13. The condition (c) follows from the condition (3) in Lemma 13 and that  $k_\infty/k$  is a  $Z_\ell$ -extension. The condition (d) follows from the condition (c) and Lemma 10.

*Proof of Theorem 5.* We shall prove the theorem by induction on  $n$ . If  $k = \mathbf{Q}(\zeta_1)$ , then by Iwasawa [8], we see that  $k$  satisfies the conditions (1) and (3). Now let  $k$  satisfy the conditions (1) ~ (4). By Lemma 13 and Theorem 6, there exists a cyclic extension  $K$  of  $k$  of degree  $\ell$  such that  $|Cl_{K_i}| \equiv 0 \pmod{\ell}$  for all  $i \geq 1$  and such that  $|S_K| \geq \ell n$ , where  $K_i = K(\zeta_i)$ . Let  $v_1$  and  $v_2$  be two prime divisors of  $K$  which are not conjugate each other over  $k$ , satisfying the conditions (1) ~ (4) of Lemma 13 (replacing  $k$  by  $K$ ). Then by Theorem 6, there exists a unique cyclic extension  $L$  of  $K$  of degree  $\ell$ , unramified outside  $v_1$  and  $v_2$ , satisfying the conditions (a) ~ (d) in Theorem 6 (replacing  $K$  and  $k$  by  $L$  and

$K$ , respectively). Then  $|S_L| = \ell |S_K| \geq \ell^2 n$ . Since the degree of  $v_i$  is 1 for  $i = 1, 2$ ,  $\{v_1, v_2\} \not\cong \{v_1^\sigma, v_2^\sigma\}$  for  $\sigma \in G(K/k)$ , with  $\sigma \neq 1$ . From this, it follows that  $L \not\cong L^{\bar{\sigma}}$  for any extension  $\bar{\sigma}$  of  $\sigma$  to the Galois closure of  $L/k$ . This implies that  $L/k$  is not a Galois extension, so  $L/\mathbb{Q}(\zeta_1)$  is not a Galois extension. Hence by induction on  $n$ , we have the assertion.

**§ 5. Remark**

In this section, we note that the part “(ii)  $\Leftrightarrow$  (vi)” of the main theorem can be proved by using Galois theory, Kummer theory and the same cohomology theoretic method as in Iwasawa [9]. The key lemma is Proposition 3 of [17], which connects such a cohomology theoretic method with our problem. We shall omit the details and sketch the proof.

LEMMA 14 ([17], Proposition 3). *Let  $\ell$  be a prime number and let  $\zeta_i$  be a primitive  $\ell^i$ -th root of unity for each  $i \in \mathbb{N}$ . Let  $k$  be a field of characteristic different from  $\ell$ . Assume that  $\zeta_1 \in k$  and that  $\zeta_2 \in k$  if  $\ell = 2$ . Fix  $n \in \mathbb{N}$  and put  $K = k(\zeta_n)$ . Let  $\sigma$  be a generator of  $G(K/k)$  and let  $s \in \mathbb{Z}$  be such that  $\zeta_n^\sigma = \zeta_n^s$ . Put  $\Sigma = \sigma^{N-1} + \sigma^{N-2}s + \dots + \sigma s^{N-2} + s^{N-1}$ , where  $N = [K:k]$ . Let  $L/K$  be a cyclic extension of  $K$  of degree  $\ell^n$  and let  $y \in K^\times$  be such that  $L = K(\ell^n \sqrt{y})$ . Then the following three statements are equivalent:*

- (1)  $L/k$  is an abelian extension whose Galois group is the direct product of  $G(L/K)$  and a cyclic subgroup of  $G(L/k)$  of order  $N$ .
- (2) There exists a  $w \in K^\times$  such that  $L = K(\ell^n \sqrt{w^s})$ .
- (3)  $y^{\sigma-s} = w^{\ell^n}$  with a  $w \in K^\times$ , and  $L = K(\ell^n \sqrt{w^s})$ .

The equivalence of (2) and (3) follows from the proof of [[17], Proposition 3].

Remark 8. We can prove that Grunwald-Hasse-Wang’s theorem ([7], [8], [25]; see also [1], Chap. 10) holds also in the case where the base field is an arbitrary field with discrete valuations, by generalizing and refining the above Lemma 14 (see [19]).

As an application of Lemma 14, we have the following

LEMMA 15. *Let  $\ell, k, \zeta_i, k_i, S, S^i, Cl_k(S)$  and  $E_k(S)$  be as in Notation. Let  $m$  be a positive rational integer. Assume that  $|Cl_k(S)| \equiv 0 \pmod{\ell}$  and that  $|Cl_{k_m}(S^m)| \equiv 0 \pmod{\ell}$ . Assume moreover that  $\zeta_1 \in k$  and that*

$\zeta_2 \in k$  if  $\ell = 2$ . Let  $K/k$  be an  $S$ -ramified cyclic extension of  $k$  of degree  $\ell$ , and let  $\varepsilon \in E_k(S)$  be such that  $K = k(\sqrt[\ell]{\varepsilon})$ . Then the following two statements are equivalent:

- (1) There exists an  $S$ -ramified cyclic extension  $L/k$  of degree  $\ell^m$  containing  $K$ ;
- (2)  $\varepsilon \in E_k(S)^\ell N_{k_m/k}(E_{k_m}(S^m))$ .

*Remark 9.* (1) If  $|Cl_k(S)| \not\equiv 0 \pmod{\ell}$ , then for any  $S$ -ramified cyclic extension  $K$  of  $k$  of degree  $\ell$ , there exists  $\varepsilon \in E_k(S)$  such that  $K = k(\sqrt[\ell]{\varepsilon})$ .

(2) The above Lemma 15 can be also proved by using the proof of [Bertrandias-Payan [2], Theorem 1].

*Proof of Lemma 15.* Obviously we may suppose that  $K \not\subset k_{n_0+1}$ . Suppose that the statement (2) holds. Put  $K_m = k_m(\sqrt[\ell^m]{\varepsilon_1^{\Sigma}})$ , where  $\Sigma$  is as in Lemma 14 for the extension  $k_m/k$  and where  $\varepsilon_1 \in E_{k_m}(S^m)$  is such that  $\varepsilon/N_{k_m/k}(\varepsilon_1) \in E_k(S)^\ell$ . Since  $s \equiv 1 \pmod{\ell}$ ,  $\Sigma \equiv \sigma^{N-1} + \sigma^{N-2} + \dots + \sigma + 1 \pmod{\ell}$ . Hence  $N_{k_m/k}(\varepsilon_1)/\varepsilon_1^\Sigma \in k_m^\ell$ , so  $\varepsilon/\varepsilon_1^\Sigma \in k_m^\ell$ . This implies that  $K_m \supset K$ . By Lemma 14,  $K_m/k$  is abelian and  $G(K_m/k) \cong G(K_m/k_m) \times (N)$ , so by Galois theory, there exists a cyclic extension  $L/k$  of degree  $\ell^m$  such that  $K \subset L \subset K_m$ . Since  $\varepsilon_1 \in E_{k_m}(S^m)$  and since  $k_m/k$  is  $S_k$ -ramified,  $K_m/k$  is  $S$ -ramified, so  $L/k$  is also  $S$ -ramified. Conversely suppose that the statement (1) holds. Put  $L_m = Lk_m$ . Since  $L_m/k_m$  is  $S^m$ -ramified and since  $|Cl_{k_m}(S^m)| \not\equiv 0 \pmod{\ell}$ , there exists  $\varepsilon_1 \in E_{k_m}(S^m)$  such that  $L_m = k_m(\sqrt[\ell^m]{\varepsilon_1})$ . By (3) of Lemma 14, there exists  $\varepsilon_2 \in k_m^\times$  such that  $\varepsilon_1^{\sigma-s} = \varepsilon_2^{\ell^m}$  and  $L_m = k_m(\sqrt[\ell^m]{\varepsilon_2^{\Sigma}})$ . Since  $\varepsilon_1 \in E_{k_m}(S^m)$ ,  $\varepsilon_2 \in E_{k_m}(S^m)$ . Since  $\varepsilon_2^\Sigma/N_{k_m/k}(\varepsilon_2) \in k_m^\ell$  and since  $k_m(\sqrt[\ell^m]{\varepsilon_2^{\Sigma}}) = k_m(\sqrt[\ell]{\varepsilon})$ , we have  $N_{k_m/k}(\varepsilon_2^r)/\varepsilon \in k_m^\ell$  with an  $r \in \mathbb{Z}$  such that  $r \not\equiv 0 \pmod{\ell}$ , hence by using Kummer theory we see easily that  $\zeta_{n_0}^i N_{k_m/k}(\varepsilon_2^r)/\varepsilon \in k^\ell$  with an  $i \in \mathbb{Z}$ . Put  $\varepsilon' = \zeta_{n_0}^i \varepsilon_2^r$ , then  $\varepsilon' \in E_{k_m}(S^m)$  and  $N_{k_m/k}(\varepsilon')/\varepsilon \in k^\ell$ , hence  $N_{k_m/k}(\varepsilon')/\varepsilon \in E_k(S)^\ell$ . This implies that the statement (2) holds.

The following lemma can be proved by using the same cohomology theoretic method as in Iwasawa [9], hence we omit the proof.

**LEMMA 16.** *Let the notation and assumptions be as in Lemma 15 and let  $t_m$  be the number of prime divisors in  $S$  completely decomposed in  $k_m$ . Then  $\text{rank } \hat{H}^0(G(k_m/k), E_{k_m}(S^m)) = |S| - t_m - 1$ , i.e.,  $\text{rank } E_k(S)/N_{k_m/k}(E_{k_m}(S^m))E_k(S)^\ell = |S| - t_m - 1$  for all  $m \geq n_0 + 1$ , where  $\hat{H}^0$  means*

*Tate-cohomology group of dimension 0.*

*Outline of another proof of the part “(ii)  $\Rightarrow$  (vi)” of the main theorem.* Obviously there exists an  $m_0 \in \mathbb{N}$  such that  $t_m = 0$  for all  $m \geq m_0$ . Put  $N_i = N_{k_i/k}(E_{k_i}(S^i))E_k(S)^\ell/E_k(S)^\ell$  for all  $i \geq 0$ . Regard  $N_i$  as a vector space over  $F_\ell$  in the natural way. Then  $\dim_{F_\ell} N_{n_0} = r_2 + |S|$ , and by Lemma 16,  $\dim_{F_\ell} N_i = r_2 + 1 + t_i$  for all  $i \geq n_0 + 1$ . Let  $A = \{a_\lambda\}_{\lambda \in A}$  be a basis of  $N_{n_0}$  over  $F_\ell$  such that  $A \cap N_i$  is a basis of  $N_i$  over  $F_\ell$  for any  $i \geq n_0$ . For each  $\lambda \in A$ , let  $\varepsilon_\lambda \in E_k(S)$  be such that  $\varepsilon_\lambda \bmod E_k(S)^\ell = a_\lambda$ , and put  $k_\lambda = k(\sqrt[\ell]{\varepsilon_\lambda})$ . Let  $K_\lambda/k$  be a maximal  $S$ -ramified cyclic extension of  $k$  of  $\ell$ -power degree containing  $k_\lambda$ . Then by Lemma 15,  $[K_\lambda : k] = \ell^{m_\lambda}$ , where  $m_\lambda \geq 0$  is such that  $a_\lambda \in N_{m_\lambda}$  and  $a_\lambda \notin N_{m_\lambda+1}$  if  $N_{m_\lambda} \supseteq N_{n_0}$  and where  $m_\lambda = \infty$  if  $a_\lambda \in N_{n_0}$ . Put  $M = \prod_{\lambda \in A} K_\lambda$ , then by Galois theory,  $G(M/k) \cong C(\infty, r_2 + 1) \times C(n_0, s_{n_0} - 1) \times \prod_{i=n_0+1}^\infty C(i, s_i)$ , since  $t_i - t_{i+1} = s_i$  for  $i \geq n_0 + 1$  and  $s_{n_0} = |S| - t_1$ . By using Galois theory, Kummer theory and Lemma 15, we can prove that  $k(S) = M$ . Hence the assertion follows.

#### REFERENCES

- [ 1 ] Artin, E. and Tate, J., *Class Field Theory*, Benjamin, New York, 1967.
- [ 2 ] Bertrandias, F. and Payan, J.-J.,  $\Gamma$ -extensions et invariants cyclotomiques, *Ann. scient. Éc. Norm. Sup.*, 4<sup>e</sup> série, **5** (1972), 517–543.
- [ 3 ] Brumer, A., On the units of algebraic number fields, *Mathematika* **14** (1967), 121–124.
- [ 4 ] —, Galois groups of extensions of number fields with given ramification, *Mich. Math. J.* **13** (1966), 33–40.
- [ 5 ] Cassels, J. W. S. and Frohlich, A. (Editors), *Algebraic number theory*, Academic Press, London, 1967.
- [ 6 ] Gras, M. G., Remarques sur la conjecture de Leopoldt, *C. R. Acad. Sc. Paris*, t. **274**, Série A (1972), 377–380.
- [ 7 ] Grunwald, W., Ein allgemeines Existenztheorem für algebraische Zahlkörper, *J. reine angew. Math.* **169** (1933), 103–107.
- [ 8 ] Hasse, H., Zum Existenzsatz von Grunwald in der Klassenkörpertheorie, *J. reine angew. Math.* **188** (1950), 40–64.
- [ 9 ] Iwasawa, K., A note on the group of units of an algebraic number field, *J. Math. pures appl.* **35** (1956), 189–192.
- [10] —, A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 189–192.
- [11] —, Introduction to  $Z_\ell$ -extensions, *Lecture notes at Princeton Univ.*, 1971.
- [12] —, On  $Z_\ell$ -extensions of algebraic number fields, *Ann. of Math.* **98** (1973), 246–326.
- [13] Kawada, Y., Class formations, *Number theory institute, Amer. Math. Soc. Proc. of Symp. in pure Math. Vol. XX*, 1969, 1971, 96–114.
- [14] Koch, H.,  $\ell$ -Erweiterungen mit vorgegebenen Verzweigungsstellen, *J. reine angew. Math.* **219** (1965), 30–61.

- [15] —, Galois Theorie der  $p$ -Erweiterungen, Springer, Berlin, 1970.
- [16] Kubota, T., Galois group of the maximal abelian extension over an algebraic number field, Nagoya Math. J. **12** (1957), 177–189.
- [17] Miki, H., On  $Z_p$ -extensions of complete  $p$ -adic power series fields and function fields, J. Fac. Univ. Tokyo Sec. IA, Vol. **21** (1974), 377–393.
- [18] —, A note on the  $p$ -rank of ideal class groups of finite algebraic number fields.
- [19] —, On Grunwald-Hasse-Wang's theorem, J. Math. Soc. Japan **30** (1978), No. 2.
- [20] Neukirch, J., Über das Einbettungsproblem der algebraischen Zahlentheorie, Invent. Math. **21** (1973), 59–116.
- [21] Roquette, P., On class field towers, [5], Chap. IX, 231–249.
- [22] Šafarevič, I. R., Extensions with given points of ramification, Inst. Hautes Études Sci. Publ. Math. **18** (1963), 71–95 = A.M.S. Transl. Ser. 2, **59** (1966), 128–149.
- [23] Yokoi, H., On the class number of a relatively cyclic number field, Nagoya Math. J. **29** (1967), 31–44.
- [24] Yokoyama, A., On class numbers of finite algebraic number fields, Tôhoku Math. J. **17** (1965), 349–357.
- [25] Wang, S., On Grunwald's Theorem, Ann. of Math. **51** (1950), 471–484.
- [26] Weil, A., Basic Number Theory, Springer, Berlin, 1967.

*Department of Mathematics*  
*Faculty of Engineering*  
*Yokohama National University*