

On sufficient conditions for the Leopoldt conjecture

山下 浩 (Hiroshi Yamasita)

Introductions.

Let p be a prime number. Let k be an algebraic number fields of finite degree over the rational number field $\mathbf{Q}$. Let S be a non-empty finite set of prime divisors of k , and let $U_S = \prod_{p \in S} U_p$, where U_p is the unit group of the completion of k at p . Let E be the global unit group of k and $i : E \longrightarrow U_S$ be the canonical injection. We denote by E_S the topological closure of $i(E)$ in U_S . Let P be the set of all prime divisors of k dividing p . Let r be the $\mathbf{Z}$ -free rank of E and r_p be the $\mathbf{Z}_p$ -free rank of E_p . Then it is equivalent to $r = r_p$ that the Leopoldt conjecture holds for (k, p) . Put $\delta_p = \delta(k, p) = r - r_p$. Then $\delta_p \geq 0$ and it is the defect value for the Leopoldt conjecture. We study the conditions for $\delta_p = 0$ in this paper. Now we explain notation which uses in this paper and state main results of this paper. Let ξ_p be a primitive p -th root of unity and let $K = k(\xi_p)$. We denote by $\bar{S}$ the set of all prime divi-

sors of K which divide the prime divisors of k contained in S . Let C be the divisor class group of K and D_S be its subgroup generated by all divisor classes containing the prime divisors in $\bar{S}$. Put $C_S = C/D_S \cdot C^p$. Put $G = \text{Gal}(K/k)$. Let $\omega : G \longrightarrow \mathbb{Z}_p^\times$ be a homomorphism to the multiplicative group of the ring of p -adic integers $\mathbb{Z}_p$ defined by $\xi_p^\tau = \xi_p^{\omega(\tau)}$ for any $\tau \in G$. Put $\varepsilon_\omega = (\sum_{\tau \in G} \omega(\tau) \tau^{-1}) / |G|$, which is an idempotent element of group ring $\mathbb{Z}_p[G]$ associated with ω . Since C_S is a $\mathbb{Z}_p[G]$ -module, we set $C_{S,\omega} = \varepsilon_\omega(C_S)$. For an abelian group A , we denote by $t_p(A)$ the maximal p -group contained in the maximal torsion subgroup of A . We prove in Theorem 1 that $\delta_p = 0$ is equivalent to existence of a finite set S of prime divisors of k satisfying the following three conditions. (1) $S \supset P$. (2) $C_{S,\omega} \simeq \{1\}$. (3) $p\text{-rank}(t_p(E_S)) = p\text{-rank}(t_p(E))$. Put $e_p = \#\{p \mid p \in S \text{ and } \xi_p \in k_p\}$. We estimate δ_p in Theorem 2 and see that $\delta_p \leq p\text{-rank}(C_{P,\omega}) + e_p - p\text{-rank}(t_p(E))$ holds. We prove in Proposition 1 that the condition (3) holds if $e_p = p\text{-rank}(t_p(E))$. If the condition (2) also holds for P , the Leopoldt conjecture is true. This was known in Gras [2], Gillard [1] and Sands [8]. Miki [6] showed that the following two conditions (4) and (5) are equivalent. (4) the Galois group of the maximal p -ramified p -abelian extension of k is torsion free and the Leopoldt conjecture holds for (k, p) . (5) the condition (2) holds for P and $e_p = p\text{-rank}(t_p(E))$ holds. We assume in Theorem 4 that k is totally imaginary if $p = 2$ and prove that the Galois group over k of the maximal p -extension of k which

is unramified outside S is a pro- p -free group if and only if the condition (2) holds for S and $e_S = p\text{-rank}(t_p(E))$.

1. the necessary and sufficient condition of

$$\delta(k : p) = 0.$$

Let N be the set of the natural numbers. Let i, j be elements of N . Let A be an abelian group. Put $A_i = A/A^{p^i}$ for $i \in N$. For $i \geq j$, we denote by $\varphi_{i,j}$ a homomorphism from A_i to A_j defined by $\varphi_{i,j}(a \cdot A^{p^i}) = a \cdot A^{p^j}$ for $a \in A$. Then $(A_i, \varphi_{i,j})$ is a projective system of abelian groups. We denote by $\bar{A}$ its projective limit, which is a $\mathbb{Z}_p$ -module. Put $r(A) = \dim_{\mathbb{Q}_p}(\bar{A} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$, where we denote by $\mathbb{Q}_p$ the field of p -adic numbers. We observe that $r = r(E)$ and $r_p = r(E_p)$. We abbreviate $r(E_S)$ to r_S .

Theorem 1. $\delta(k : p) = 0$ is equivalent to existence of the finite set S of prime divisors of k satisfying the following three conditions. (1) $S \supset P$. (2) $C_{S, \omega} \simeq \{1\}$. (3) $p\text{-rank}(t_p(E_S)) = p\text{-rank}(t_p(E))$.

To prove this theorem, we need some lemmas.

Lemma 1. $r_P = r_S$ if $P \subset S$.

Proof. Let $\pi : U_S \longrightarrow U_P$ be the canonical projection. Let S' be the subset of S consisting of all elements which are not contained in P . The kernel of π is $U_{S'}$. Let V_1 resp. V_2 be any open subgroup of U_P resp. $U_{S'}$. We have $E \cdot V_1 \cdot V_2 = E_S \cdot V_1 \cdot V_2$ since $V_1 \cdot V_2$ is an open subgroup of U_S . Hence $\pi(E) \cdot V_1 = \pi(E_S) \cdot V_1$. Therefore the topological closure in U_P of $\pi(E)$ is equal to that of $\pi(E_S)$. Since E_S is compact, $\pi(E_S)$ is also compact. Thus we have $E_P = \pi(E_S)$. Put $V(p) = t_p(k_p^\times)$ for $p \in S$. Put $p^m = \max\{|V(p)| \mid p \in S'\}$. Then we have

$$(U_{S'} \cap E_S) \cdot (E_S)^{p^n} / (E_S)^{p^n} \simeq t_p(U_{S'} \cap E_S).$$

Hence we have an exact sequence

$$1 \longrightarrow t_p(U_{S'} \cap E_S) \longrightarrow E_S / E_S^{p^n} \xrightarrow{\pi_n} E_P / E_P^{p^n} \longrightarrow 1,$$

where π_n is a homomorphism defined by $\pi_n(\varepsilon \cdot E_S^{p^n}) = \pi(\varepsilon) \cdot E_P^{p^n}$ for $\varepsilon \in E_S$. We take the projective limit of this exact sequence. Then we see $r_P = r_S$ by the definition. Q. E. D.

Put $A_S^{(2)} = (E \cap (E_S)^p) / E^p$.

Lemma 2. Suppose $S \supset P$. Then we have

$$\delta_p = p\text{-rank}(t_p(E_S)) - p\text{-rank}(t_p(E)) + p\text{-rank}(A_S^{(2)}).$$

Proof. Let X be a set of representatives of all left coset in E with respect to E^p . Then X is a finite set.

Put $F = \bigcup_{\varepsilon \in X} \varepsilon \cdot E_S^p$. Then F is compact because it is a finite union of compact sets $\varepsilon \cdot E_S^p$. Hence we have $F = E_S$ because $E_S \supset F \supset E$. Let $f : E/E^p \longrightarrow E_S/E_S^p$ be a homomorphism defined by $f(\varepsilon \cdot E) = \varepsilon \cdot E_S^p$ for $\varepsilon \in X$. Then f is surjective and $\ker(f) = \{ \varepsilon \cdot E^p \mid \varepsilon \in E_S^p \} = (E \cap E_S^p)/E^p$. Therefore we have $E/(E \cap E_S^p) \simeq E_S/E_S^p$. Since E/E^p is an elementary p -abelian group, we have $E/E^p \simeq E/(E \cap E_S^p) \oplus A_S^{(2)}$. Hence $E/E^p \simeq E_S/E_S^p \oplus A_S^{(2)}$. Since $r = p\text{-rank}(E/E^p) - p\text{-rank}(t_p(E))$ and $r_S = p\text{-rank}(E_p/E_p^p) - p\text{-rank}(t_p(E_S))$, We have

$$\delta_p = r - r_S = p\text{-rank}(t_p(E_S)) - p\text{-rank}(t_p(E)) + p\text{-rank}(A_S^{(2)}).$$

Q. E. D.

We define $U_k^S(p)$ by

$$U_k^S(p) = \{ \alpha \in k^\times \mid \text{There exists an ideal } \alpha \text{ of } k \text{ such}$$

$$\text{that } \alpha^p = (\alpha), \text{ and } \alpha \in (k_p^\times)^p \text{ for any } p. \},$$

where we denote by k_p the completion of k at p . We denote by $\bar{S}$ the set $\{ \mathfrak{P} \mid \mathfrak{P} \text{ is a prime divisor of } K \text{ which divides a prime divisor of } k \text{ contained in } S. \}$. Let $U_K^{\bar{S}}(p)$ be a set of elements of $K^\times$ such that there exists an ideal $\mathfrak{A}$ of K satisfying $\mathfrak{A}^p = (\alpha)$, and $\alpha \in (K_{\mathfrak{P}}^\times)^p$ for any $\mathfrak{P} \in \bar{S}$, where we denote by $K_{\mathfrak{P}}$ the completion of K at $\mathfrak{P}$.

$$\text{Lemma 3. } U_k^S(p) \simeq N_{K/k}(U_K^{\bar{S}}(p)) \cdot (K^\times)^p / (K^\times)^p,$$

where we denote by $N_{K/k}$ the norm map from K to k .

Proof. Let $\alpha \in U_K^S(p)$ and $\mathfrak{A}$ be an ideal of K such that $\mathfrak{A}^p = (\alpha)$. We denote by J_p the semi-local product $\prod_{\mathfrak{p} \mid p} K_{\mathfrak{p}}^{\times}$. Since $N_{K/k}(\mathfrak{A})^p = N_{K/k}((\alpha))$ and $N_{K/k}(\alpha) \in N_{K/k}(J_p^p) \subset (K^{\times})^p$, we have $N_{K/k}(U_K^S(p)) \subset U_k^S(p)$. Since $(U_k^S(p))^{[K:k]} \subset N_{K/k}(U_K^S(p)) \subset U_k^S(p)$ and $(p, [K:k]) = 1$, we have $U_k^S(p) \cdot (K^{\times})^p = N_{K/k}(U_K^S(p)) \cdot (K^{\times})^p$. Let $j : K^{\times}/(K^{\times})^p \longrightarrow K^{\times}/(K^{\times})^p$ be a homomorphism defined by $j(\alpha \cdot (K^{\times})^p) = \alpha \cdot (K^{\times})^p$ for $\alpha \in K^{\times}$. Let $\bar{k}$ be the algebraic closure of k , and let μ_p be the group of all p -th roots of unity in K . Since we have the isomorphisms $H^1(\bar{k}/k, \mu_p) \simeq K^{\times}/(K^{\times})^p$ and $H^1(\bar{k}/K, \mu_p) \simeq K^{\times}/(K^{\times})^p$, we see that the injection of the cohomology groups $\text{Inf} : H^1(\bar{k}/k, \mu_p) \longrightarrow H^1(\bar{k}/K, \mu_p)$ induces j . Hence $\ker(j) \simeq H^1(K/k, \mu_p)$ by the exact sequence of the restriction and the injection of the first cohomology groups. Since $[K:k]$ is prime to p , we have $\ker(j) \simeq \{1\}$. Thus $U_k^S(p)/(K^{\times})^p$ is isomorphic to $U_k^S(p) \cdot (K^{\times})^p / (K^{\times})^p$ by j . Therefore we have $U_k^S(p)/(K^{\times})^p \simeq N_{K/k}(U_K^S(p)) \cdot (K^{\times})^p / (K^{\times})^p$.

Q. E. D.

Put $L = K(\sqrt[p]{\alpha} \mid \alpha \in U_K^S(p))$. Then L is the maximal elementary p -abelian extension of K such that any prime divisor contained in $\bar{S}$ is completely decomposed and $\text{Gal}(L/K)$ is isomorphic to C_S by class field theory. Thus we identify C_S with $\text{Gal}(L/K)$.

Lemma 4. $\text{Hom}(C_{S,\omega}, \mu_p) \simeq N_{K/k}(U_K^{\bar{S}}(p)) \cdot (K^\times)^p / (K^\times)^p,$

where we denote by μ_p the group of all p -th roots of unity contained in K .

Proof. Denote by $\bar{\alpha}$ the left coset $\alpha \cdot (K^\times)^p$ for $\alpha \in U_K^{\bar{S}}(p)$. Let $x \in C_S$. Set $\langle \bar{\alpha}, x \rangle = \sqrt{\alpha} x^{-1}$. Then it defines a non-degenerate pairing on $(U_K^{\bar{S}}(p) / (K^\times)^p) \times C_S$. Let $\sigma \in G$. Then $\langle \sigma(\bar{\alpha}), \sigma(x) \rangle = \langle \bar{\alpha}, x \rangle^{\omega(\sigma)}$. Hence we have $\langle \bar{\alpha}, \varepsilon_\omega(x) \rangle^m = \langle N_G(\bar{\alpha}), x \rangle$, where we denote by N_G the norm map of a G -module, and $m = [K:k]$. Let $H = \{\alpha \in U_K^{\bar{S}}(p) \mid N_G(\alpha) \in (K^\times)^p\}$. Then we see that $H / (K^\times)^p$ is the annihilator of $C_{S,\omega}$. Therefore we have

$$\text{Hom}(C_{S,\omega}, \mu_p) \simeq N_{K/k}(U_K^{\bar{S}}(p)) \cdot (K^\times)^p / (K^\times)^p,$$

since $\text{Hom}(C_{S,\omega}) \simeq U_K^{\bar{S}}(p) / H \cdot (K^\times)^p \simeq N_G(U_K^{\bar{S}}(p)) \cdot (K^\times)^p / (K^\times)^p$.

Q. E. D

Corollary. $U_K^{\bar{S}}(p) / (K^\times)^p \simeq C_{S,\omega}$.

Proof of Theorem 1. By Corollary to Lemma 4, we see that $U_K^{\bar{S}}(p) = (K^\times)^p$ is equivalent to $C_{S,\omega} = \{1\}$. Assume that S satisfies the condition (1), (2) and (3) of Theorem 1. Since $U_K^{\bar{S}}(p) = (K^\times)^p$, we have $A_S^{(2)} = \{1\}$ by the proof of Corollary to Lemma 7. Hence $\delta_p = p\text{-rank}(t_p(E_S)) - p\text{-rank}(t_p(E))$. Therefore $\delta_p = 0$ by the condition (3). Conversely we assume that $\delta_p = 0$. Let S be a finite set of prime divisors of k

containing P . Since $t_p(E_S) \supset t_p(E)$, we have $p\text{-rank}(t_p(E_S)) - p\text{-rank}(t_p(E)) \geq 0$. Hence we have $p\text{-rank}(t_p(E_S)) - p\text{-rank}(t_p(E)) = 0$ by Lemma 2. The condition (3) holds for any S containing P . We take a sufficiently large set S so that $C_{S,\omega} \simeq \{1\}$. Then the condition (2) holds. Q. E. D.

2. Some sufficient conditions for the conditions of Theorem 1.

Put $e_P = \#\{p \mid p \in P \text{ and } \xi_p \in k_p\}$.

Proposition 1. $p\text{-rank}(t_p(E_P)) = p\text{-rank}(t_p(E))$ if $e_P = p\text{-rank}(t_p(E))$ or if $\xi_p \notin k_p$ for any $p \in P$.

Proof. Since $e_P \geq p\text{-rank}(t_p(E_P)) \geq p\text{-rank}(t_p(E))$, we have $p\text{-rank}(t_p(E_P)) = p\text{-rank}(t_p(E))$ if $e_P = p\text{-rank}(t_p(E))$. We see that $e_P = p\text{-rank}(t_p(E))$ holds if $\xi_p \in k$ and $|P| = 1$ or if $\xi_p \notin k_p$ for any $p \in P$.

Q. E. D.

Proposition 2. Suppose that $\xi_p \notin k_p$ for any $p \in P$ and that the p -class field tower of K is finite. Then the Leopoldt conjecture holds for (k, p) .

Proof. Let $K = K_0 \subsetneq K_1 \subsetneq K_2 \cdots \subsetneq K_n = K_{n+1}$ be the p -class field tower of K . Then K_n/k is a Galois extension. Since K_n/K is a p -extension and K/k is a cyclic extension

whose extension degree is prime to p , there exists $\tau \in \text{Gal}(K/k)$ whose order is just $[K:k]$. Let M be the fixed field of τ in K_n . Since $[K_n:M] = [K:k]$ and $K_n \supset M(\xi_p)$, we have $[K_n:M(\xi_p)] \mid [K:k]$. On the other hand, since $M(\xi_p) \supset K$, we have $[K_n:M(\xi_p)] \mid [K_n:K]$. Since $[K:k]$ is prime to $[K_n:K]$, we have $[K_n:M(\xi_p)] = 1$. Hence $K_n = M(\xi_p)$. Let P_M be the set of all prime divisors of M dividing p . Then we see that the condition (2) of Theorem 1 holds for (M, P_M) . Let $\mathfrak{P} \in P_M$ and $M_{\mathfrak{P}}$ be the completion of M at $\mathfrak{P}$. Let $\mathfrak{p}$ be a prime divisor of k divided by $\mathfrak{P}$. Since $\xi_p \notin k_{\mathfrak{p}}$ and $M_{\mathfrak{P}}/k_{\mathfrak{p}}$ is a p -extension, we have $\xi_p \notin M_{\mathfrak{P}}$. By Proposition 1, we have that the condition (3) holds for (M, P) . Therefore the Leopoldt conjecture holds for M . Hence it also holds for k . Q. E. D.

Propositin 3. Let k_0 be an algebraic number field such that $[k : \mathbb{Q}]$ is finite. Suppose that k_0 is a cyclic extension of k of degree p . Let S_0 be the finite set of prime divisors of k_0 such that the condition (2) of Theorem 1 holds for (k_0, S_0) . Let S be the set of all prime divisors of k which divide prime divisors contained in S_0 . Put $K_0 = k_0(\xi_p)$. Let R be the set of primes divisors $\mathfrak{p}$ of k_0 satisfying the following two conditions. (1) $\mathfrak{p}$ is contained in S_0 or an extension of $\mathfrak{p}$ to K is ramified at K/K_0 . (2) $\mathfrak{p}$ is completely decomposed at K_0 .

Then the condition (2) of Theorem 1 for (k_0, S_0) implies that for (k, S) if $R = \emptyset$.

Put $X_\omega = \varepsilon_\omega(X)$ for a $\mathbb{Z}_p[G]$ -module X . To prove this proposition, we need the following two lemmas.

Lemma 5. Let $0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$ be an exact sequence of $\mathbb{Z}_p[G]$ -modules. Then we have the exact sequence

$$0 \longrightarrow N_\omega \longrightarrow M_\omega \longrightarrow P_\omega \longrightarrow 0.$$

Proof. We regard N as a submodule of M . We have an exact sequence $0 \longrightarrow N \cap M_\omega \longrightarrow M_\omega \longrightarrow P_\omega \longrightarrow 0$. Let y be an element of M such that $\varepsilon_\omega(y) \in N$. Then $\varepsilon_\omega(y) = \varepsilon_\omega \cdot \varepsilon_\omega(y) \in N_\omega$ since $\varepsilon_\omega \cdot \varepsilon_\omega = \varepsilon_\omega$. Hence $N \cap M_\omega \subset N_\omega$. Since $N \subset N \cap M_\omega$, we have $N_\omega = N \cap M_\omega$. Q. E. D.

Let L be the class field of K whose Galois group over K is isomorphic to C_S by class field theory. We denote by L^* the maximal abelian extension of k contained in L . Let J_K be the idèle group of $K = k(\xi_p)$ and U_K be its unit group. Put $W_K = U_K \cdot \prod_{\mathfrak{p} \in \bar{S}} K_{\mathfrak{p}}^\times$, where we denote by $\bar{S}$ the set of all prime divisors of K dividing prime divisors contained in S_0 . Then we have $C_S \simeq J_K / W_K \cdot (J_K)^p \cdot K^\times$. Put $K_0 = k_0(\xi_p)$.

Lemma 6. Let σ be a generator of $\text{Gal}(K/K_0)$. Then we have

$$C_S / (C_S)^{\sigma-1} \simeq N_{K/K_0} (J_K) \cdot K_0^\times / N_{K/K_0} (W_K \cdot (J_K^p)) \cdot K_0^\times$$

Proof. We identify $\text{Gal}(L/K)$ to C_S . Let M be the fixed field of $C_S^{\sigma^{-1}}$ in L . $\text{Gal}(M/K_0)$ is an abelian group since K/K_0 is a cyclic extension. Hence $L^* \supset M$. Put $H = \text{Gal}(L/L^*)$. Then $H \supset (C_S)^{\sigma^{-1}}$ because σ acts trivially on $\text{Gal}(L^*/K)$. Hence $L^* \subset M$. Thus we have $L^* = M$ and $\text{Gal}(L^*/K) \simeq C_S / (C_S)^{\sigma^{-1}}$. On the other hand, we have $\text{Gal}(L^*/K) \simeq N_{K/K_0}(J_K) \cdot K_0^\times / N_{K/K_0}(W_K \cdot (J_K^D)) \cdot K_0^\times$ by translation theorem of class field theory, because $\text{Gal}(L/K) \simeq J_K / W_K \cdot (J_K)^D \cdot K^\times$. Q. E. D.

Proof of Proposition 3. We denote by $\mathfrak{p}$ resp. $\mathfrak{P}$ a prime divisor of K_0 resp. K . We denote by $K_{0\mathfrak{p}}$ resp. $K_{\mathfrak{P}}$ the completion of K_0 resp. K at $\mathfrak{p}$ resp. $\mathfrak{P}$. Let $U_{\mathfrak{p}}$ resp. $U_{\mathfrak{P}}$ be its unit group. Let $\mathfrak{p}_0$ be a prime divisor of k_0 . We define $V_{\mathfrak{p}_0}$ and $W_{\mathfrak{p}_0}$ by

$$V_{\mathfrak{p}_0} = \prod_{\mathfrak{p}|\mathfrak{p}_0} K_{0\mathfrak{p}}^\times, \quad W_{\mathfrak{p}_0} = \prod_{\mathfrak{P}|\mathfrak{p}_0} K_{\mathfrak{P}}^\times \quad \text{if } \mathfrak{p}_0 \in S_0,$$

$$V_{\mathfrak{p}_0} = \prod_{\mathfrak{p}|\mathfrak{p}_0} U_{\mathfrak{p}}, \quad W_{\mathfrak{p}_0} = \prod_{\mathfrak{P}|\mathfrak{p}_0} U_{\mathfrak{P}} \quad \text{if } \mathfrak{p}_0 \notin S_0.$$

For each $\mathfrak{p}$, we choose a prime divisor $\mathfrak{P}$ of K dividing $\mathfrak{p}$ and denote by $Z_{\mathfrak{p}}$ the decomposition group of $\mathfrak{P}$ in $\text{Gal}(K/K_0)$. If $\mathfrak{P}$ is ramified at K/K_0 , then $Z_{\mathfrak{p}}$ is also the inertia group of $\mathfrak{P}$. Hence we have by class field theory

$$(2.1) \quad v_{p_0} / N_{K/K_0} (w_{p_0}) \simeq \prod_{p|p_0} Z_p.$$

for any prime divisor p_0 of k_0 . We consider the $Z_p[G]$ -module structure of this group. We see $Z_p \simeq \{1\}$ if p is decomposed at K/K_0 or if p_0 is not contained in S_0 and p is not ramified at K/K_0 . Now we consider the group of (2.1) for p_0 whose extension $\mathfrak{P}$ to K is not decomposed if $p_0 \in S_0$ or which is ramified at K/k if $p_0 \notin S_0$. Let p be a fixed prime divisor of K_0 dividing p_0 . We denote by G_{p_0} be the decomposition group of p in $\text{Gal}(K_0/k_0)$. Let $G = \cup_{i=1}^t \sigma_i \cdot G_{p_0}$ be the decomposition of G to left cosets. We assume $\sigma_1 \in G_{p_0}$. Let τ_1 be a generator of Z_p . Then $\tau_i = \sigma_i \cdot \tau_1 \cdot \sigma_i^{-1}$ is a generator of $Z_{p^{\sigma_i}}$. We use the additive notation for Z_p in the followings. Then

$$\prod_{p|p_0} Z_p \simeq \{ (n_1 \cdot \tau_1, n_2 \cdot \tau_2, \dots, n_t \cdot \tau_t) \mid n_i \in \mathbb{Z}/p\mathbb{Z} \}$$

for $i = 1, \dots, t$.

Let $\varphi : \prod_{p|p_0} Z_p \longrightarrow (\mathbb{Z}/p\mathbb{Z})[G/G_p]$ be a $Z_p[G]$ -isomorphism defined by $\varphi((n_1 \cdot \tau_1, \dots, n_t \cdot \tau_t)) = \sum_{i=1}^t n_i \cdot \sigma_i \cdot G_p$. Then we have

$$(2.2) \quad \left(\prod_{p|p_0} Z_p \right)_{\omega} \simeq ((\mathbb{Z}/p\mathbb{Z})[G/G_p])_{\omega}.$$

This module is $\{0\}$ if $G_p \neq \{1\}$, and is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ if $G_p \simeq \{1\}$. By (2.1) and (2.2), we have $(v_{p_0} / N_{K/K_0} (w_{p_0}))_{\omega} \simeq \{1\}$ if and only if p_0 is not completely decomposed at

K_0/k_0 . Hence we have $(v_{p_0}/N_{K/K_0}(w_{p_0}))_\omega \simeq \{1\}$ for any p_0 because $R = \emptyset$. Put $v_{K_0} = \prod_{p_0} v_{p_0}$ and $w_K = \prod_{p_0} w_{p_0}$, where p_0 runs through the set of all prime divisors of k_0 . Then we have

$$(2.3) \quad (v_{K_0}/N_{K/K_0}(w_K))_\omega \simeq \{1\}.$$

We define $\mathbb{Z}_p[G]$ -modules N, M, P, Z, Y by

$$N = v_{K_0} \cdot N_{K/K_0}(J_K^p) \cdot K_0^\times / N_{K/K_0}(w_K \cdot (J_K^p)) \cdot K_0^\times,$$

$$M = v_{K_0} \cdot (J_{K_0}^p) \cdot K_0^\times / N_{K/K_0}(w_K \cdot (J_K^p)) \cdot K_0^\times,$$

$$P = v_{K_0} \cdot (J_{K_0}^p) \cdot K_0^\times / v_{K_0} \cdot N_{K/K_0}(J_K^p) \cdot K_0^\times,$$

$$Y = N_{K/K_0}(J_K) \cdot K_0^\times / N_{K/K_0}(w_K \cdot (J_K^p)) \cdot K_0^\times,$$

$$Z = J_{K_0}/N_{K/K_0}(w_K \cdot (J_K^p)) \cdot K_0^\times.$$

Then we have exact sequences of $\mathbb{Z}_p[G]$ -modules

$$(2.4) \quad 1 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 1,$$

$$(2.5) \quad 1 \longrightarrow M \longrightarrow Z \longrightarrow Z/M \longrightarrow 1,$$

$$(2.6) \quad 1 \longrightarrow Y \longrightarrow Z \longrightarrow J_{K_0}/N_{K/K_0}(J_K) \cdot K_0^\times \longrightarrow 1.$$

Since N is a homomorphic image of $v_{K/K_0}/N_{K/K_0}(J_K) \cdot K_0^\times$ as

$\mathbb{Z}_p[G]$ -module, we see $N_\omega \simeq \{1\}$ by Lemma 5 and (2.3). Let $f :$

$J_{K_0}/N_{K/K_0}(J_K) \cdot K_0^\times \longrightarrow P$ be a $\mathbb{Z}_p[G]$ -homomorphism defined by

$f(a \cdot N_{K/K_0}(J_K) \cdot K_0^\times) = a^p \cdot v_{K_0} \cdot N_{K/K_0}(J_K^p) \cdot K_0^\times$. Then f is a sur-

jection. Since $J_{K_0}/N_{K/K_0}(J_K) \cdot K_0$ is a trivial G -module, we have $(J_{K_0}/N_{K/K_0}(J_K) \cdot K_0^\times)_\omega \simeq \{1\}$. Hence $\text{image}(f)_\omega = P_\omega \simeq \{1\}$ by Lemma 5. Then we have $M_\omega \simeq \{1\}$ by Lemma 5 and (2.4). Hence we have $Z_\omega \simeq (Z/M)_\omega$ by Lemma 5 and (2.5). Since it is equivalent to $(J_{K_0}/V_{K_0} \cdot (J_{K_0}^p) \cdot K_0^\times)_\omega \simeq \{1\}$ that the condition (2) of Theorem 1 holds for (K_0, S_0) , we have $(Z/M)_\omega \simeq \{1\}$ by the assumption of Proposition. Hence we see $Z_\omega \simeq \{1\}$. Therefore $Y_\omega \simeq \{1\}$ by (2.6). Since $Y \simeq C_S/(C_S)^{\sigma-1}$ by Lemma 6, we have $(C_S/C_S^{\sigma-1})_\omega \simeq \{1\}$. Since $\text{Gal}(K/k_0)$ is an abelian group, we have $\sigma \cdot \tau = \tau \cdot \sigma$ for any $\tau \in G$. Hence $\sigma \cdot \varepsilon_\omega = \varepsilon_\omega \cdot \sigma$. Thus $(C_S^{\sigma-1})_\omega = (C_{S,\omega})^{\sigma-1}$. Therefore we have $C_{S,\omega}/(C_{S,\omega})^{\sigma-1} \simeq \{1\}$ because $(C_S/C_S^{\sigma-1})_\omega \simeq C_{S,\omega}/(C_{S,\omega})^{\sigma-1}$. This implies $C_{S,\omega} \simeq \{1\}$. Q. E. D.

3. Some theorems concerned with $\delta_p(K : p)$.

We define groups V_S , W_S and $A_S^{(1)}$ by

$$V_S = \{ u \in U_S \mid u^p \in E_S \},$$

$$W_S = \{ u \in U_S \mid u^p = 1 \},$$

$$A_S^{(1)} = E \cap (U_S^p)/E \cap (E_S^p).$$

Lemma 8. $1 \longrightarrow W_S/W_S \cap t_p(E_S) \longrightarrow V_S/W_S \longrightarrow A_S^{(1)} \longrightarrow 1.$

Proof. Let $u \in V_S$. Then there exists $\delta \in E_S$ such that

$u^p = \delta$. Since $E \cdot (E_S^p) = E_S$, we have $\varepsilon \in E$ and $\delta_1 \in E_S$ such that $\delta = \varepsilon \cdot \delta_1^p$. Then we see $\varepsilon \in E \cap (U_S^p)$. Let $f : V_S \longrightarrow A_S^{(1)}$ be a homomorphism defined by $f(u) = \varepsilon \cdot (E \cap (E_S^p))$. Then $\ker(f) = W_S \cdot E_S$. Let $\varepsilon \in E \cap (U_S^p)$. Then there exists $u \in U_S$ such that $u^p = \varepsilon$. We have $f(u) = \varepsilon \cdot (E \cap (E_S^p))$. Hence f is surjective. Since $W_S \cdot E_S / E_S \simeq W_S / W_S \cap t_p(E_S)$, we have an exact sequence

$$1 \longrightarrow W_S / W_S \cap t_p(E_S) \longrightarrow V_S / E_S \longrightarrow A_S^{(1)} \longrightarrow 0.$$

Q. E. D.

Let T be a finite set of prime divisors of k . We permit in the case $T = \emptyset$. Let A be the maximal subgroup of the ideal class group of k whose exponent is divided by p . We define $U_k^T(p)$ for $T = \emptyset$ by $U_k^\emptyset(p) = \{ \alpha \in k \mid \text{There exists an ideal } \alpha \text{ of } k \text{ such that } \alpha^p = (\alpha) \}$. We define a subgroup $A_T^{(0)}$ of A by

$$A_T^{(0)} = \{ c \in A \mid c \text{ contains an ideal } \alpha \text{ of } k \text{ such that } \alpha^p = (\alpha) \text{ for some } \alpha \in U_k^T(p) \}.$$

Lemma 9. $U_k^T(p) / (E \cap (U_k^T(p))) \cdot (k^\times)^p \simeq A_T^{(0)}$.

Proof. Let $\alpha \in U_k^T(p)$. Then there exists an ideal α of k such that $\alpha^p = (\alpha)$. Let c be the divisor class containing α . This divisor class is contained in $A_S^{(0)}$. We define a homomorphism $f : U_k^T(p) \longrightarrow A_S^{(0)}$ by $f(\alpha) = c$. Then f is

surjective by the definition of $A_S^{(0)}$. Since $\ker(f) = \{ \alpha \in U_k^T(p) \mid \text{There exists } \beta \in k \text{ such that } (\alpha) = (\beta^p) \}$, we have $\ker(f) = (E \cdot (k^\times)^p) \cap U_k^T(p) = (E \cap U_k^T(p)) \cdot (k^\times)^p$. Therefore we see $\text{image}(f) \simeq U_k^T(p) / (E \cap U_k^T(p)) \cdot (k^\times)^p$.

Q. E. D.

Corollary. Suppose S is a non-empty finite set of prime divisors of k . Then we have

$$U_k^S(p) / (k^\times)^p \simeq A_S^{(0)} \oplus A_S^{(1)} \oplus A_S^{(2)}.$$

Proof. Since $E \cap U_k^S(p) = E \cap U_S^p$, we have a chain of abelian groups $U_k^S(p) / (k^\times)^p \supset (E \cap U_k^S(p)) \cdot (k^\times)^p / (k^\times)^p \supset (E \cap E_S^p) \cdot (k^\times) / (k^\times)^p$. The sequence of the quotient groups of this chain is isomorphic to $A_S^{(0)}, A_S^{(1)}, A_S^{(2)}$. Since the exponent of $U_k^S(p) / (k^\times)^p$ divides p , it is isomorphic to $A_S^{(0)} \oplus A_S^{(1)} \oplus A_S^{(2)}$.

Q. E. D.

Put $e_S = \{ p \mid p \in S \text{ and } \xi_p \in k_p \}$. We see that e_S is equal to $p\text{-rank}(W_S)$.

Theorem 2. We have for $S \supset P$,

$$\begin{aligned} \delta_p &= e_S + p\text{-rank}(C_{S, \omega}) - p\text{-rank}(t_p(E)) - p\text{-rank}(V_S/E_S) \\ &\quad - p\text{-rank}(A_S^{(0)}). \end{aligned}$$

Proof. By Lemma 2. we have

$$(3.1) \quad \delta_p = p\text{-rank}(t_p(E_S)) - p\text{-rank}(t_p(E)) + p\text{-rank}(A_S^{(2)}).$$

By Lemma 8, we have

$$(3.2) \quad p\text{-rank}(t_p(E_S)) = e_S - p\text{-rank}(W_S/E_S) + p\text{-rank}(A_S^{(1)})$$

since $p\text{-rank}(t_p(E_S)) = p\text{-rank}(W_p \cap t_p(E_S))$.

We substitute $p\text{-rank}(t_p(E_S))$ in (3.1) by the right hand side of (3.2). Then

$$(3.3) \quad \delta_p = e_S - p\text{-rank}(V_S/E_S) + p\text{-rank}(t_p(E)) + \\ (p\text{-rank}(A_S^{(1)}) + p\text{-rank}(A_S^{(2)})).$$

By Corollary to Lemma 9 and Corollary to Lemma 4,

$$(3.4) \quad p\text{-rank}(A_S^{(1)}) + p\text{-rank}(A_S^{(2)}) = p\text{-rank}(C_{S,\omega}) - p\text{-rank}(A_S^{(0)})$$

We substitute $(p\text{-rank}(A_S^{(1)}) + p\text{-rank}(A_S^{(2)}))$ in (3.3) by the right hand side of (3.4). Then

$$\delta_p = e_S - p\text{-rank}(V_S/E_S) - p\text{-rank}(t_p(E)) + p\text{-rank}(C_{S,\omega}) \\ - p\text{-rank}(A_S^{(0)}).$$

Q. E. D.

Corollary. We have $\delta_p \leq p\text{-rank}(C_{S,\omega}) + e_S - p\text{-rank}(t_p(E))$ for $P \subset S$.

Let k_S be the maximal p -extension of k unramified outside S . Put $G_S = \text{Gal}(k_S/k)$ and $G_S^* = G_S/[G_S, G_S]$, where

$[G_S, G_S]$ is the comutator subgroup of G_S . Put $\hat{G}_S = \text{Hom}(G_S^*, \mathbb{Q}/\mathbb{Z})$. Let f_p be an endomorphism of $\mathbb{Q}/\mathbb{Z}$ defined by $f_p(x) = p \cdot x$ for $x \in \mathbb{Q}/\mathbb{Z}$. We have an exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{f_p} \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

Then we have the following cohomology long exact sequence

$$H^1(G_S, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f_p^{(1)}} H^1(G_S, \mathbb{Q}/\mathbb{Z}) \longrightarrow H^2(G_S, \mathbb{Z}/p\mathbb{Z}) \longrightarrow$$

$$H^2(G_S, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f_p^{(2)}} H^2(G_S, \mathbb{Q}/\mathbb{Z}),$$

where we denote by $f_p^{(1)}$ and $f_p^{(2)}$ the induced homomorphism of the cohomology groups by f_p . Since G_S acts trivially on $\mathbb{Q}/\mathbb{Z}$, we have $H^1(G_S, \mathbb{Q}/\mathbb{Z}) \simeq \hat{G}_S$. Then $\text{coker}(f_p^{(1)}) = \hat{G}_S/p \cdot \hat{G}_S$ and $\ker(f_p^{(2)}) = \{c \in H^2(G_S, \mathbb{Q}/\mathbb{Z}) \mid p \cdot c = 0\}$. Put $H^2(G_S, \mathbb{Q}/\mathbb{Z})_p = \ker(f_p^{(2)})$ and $G_{S,p}^* = \{x \in G_S^* \mid x^p = 1\}$. Then $G_{S,p}^*$ is equal to $\{x \in G_S^* \mid x^p = 1\}$. Put $\hat{G}_{S,p} = \text{Hom}(G_{S,p}^*, \mathbb{Q}/\mathbb{Z})$. Then $\text{coker}(f_p^{(1)}) \simeq \hat{G}_S/p \cdot \hat{G}_S$ is equal to $\hat{G}_{S,p}$. Hence we have a short exact sequence

$$(3.5) \quad 0 \longrightarrow \hat{G}_{S,p} \longrightarrow H^2(G_S, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^2(G_S, \mathbb{Q}/\mathbb{Z})_p \longrightarrow 0.$$

Put $g^S = p\text{-rank}(H^1(G_S, \mathbb{Z}/p\mathbb{Z}))$, $r^S = p\text{-rank}(H^2(G_S, \mathbb{Q}/\mathbb{Z}))$ and $t^S = p\text{-rank}(t_p(G_S^*))$.

Theorem 3. Suppose that k is totally imaginary if $p = 2$. Suppose $P \subset S$. Let r_2 be the number of the complex places of k . Then we have

$$(1) \quad p\text{-rank}(H^2(G_S, \mathbb{Z}/p\mathbb{Z})) = g^S - (r_2 + 1) = \delta_p + t^S,$$

$$(2) \quad p\text{-rank}(H^2(G_S, \mathbb{Q}/\mathbb{Z})_p) = \delta_p.$$

Proof. Let S_1 be the union of S and the set of all infinite prime divisors of k . We see $k_S = k_{S_1}$ in case of $p = 2$ because k is totally imaginary. If there exists an intermediate field k' of k_{S_1}/k of finite degree over k such that the infinite prime divisors are ramified, then we see $[\bar{k}':k] \equiv 0 \pmod{2}$, where we denote by $\bar{k}'$ the Galois closure of k' . Since $\bar{k}' \subset k_{S_1}$, such k' does not exist in case of $p \neq 2$. Thus $k_S = k_{S_1}$. Therefore we have, by Corollary 1 to the main theorem of Neumann [7],

$$\sum_{i=0}^2 (-1)^i p\text{-rank}(H^i(G_S, \mathbb{Z}/p\mathbb{Z})) = -r_2.$$

Hence $p\text{-rank}(H^2(G_S, \mathbb{Z}/p\mathbb{Z})) = p\text{-rank}(H^1(G_S, \mathbb{Z}/p\mathbb{Z})) - (r_2 + 1)$. Since the $\mathbb{Z}_p$ -free rank of G_S^* equals $r_2 + 1 + \delta_p$ by the theory of $\mathbb{Z}_p$ -extensions, we see

$$p\text{-rank}(G_S^*/(G_S^*)^p) = (r_2 + 1 + \delta_p) + t^S.$$

Since $g^S = p\text{-rank}(H^1(G_S, \mathbb{Z}/p\mathbb{Z})) = p\text{-rank}(G_S^*/(G_S^*)^p)$, we have

$$p\text{-rank}(H^2(G_S, \mathbb{Z}/p\mathbb{Z})) = g^S - (r_2 + 1) = \delta_p + t^S.$$

Hence we have $p\text{-rank}(H^2(G_S, \mathbb{Q}/\mathbb{Z})_p) = \delta_p$ by (3.5), because $p\text{-rank}(\hat{G}_{S,p}) = p\text{-rank}(G_{S,p}^*) = p\text{-rank}(t_p(G_S^*))$.

Q. E. D.

Corollary. Suppose k is totally imaginary if $p = 2$. Suppose $P \subset S$. Then G_S is a pro- p -free group if and only if $\delta_p = 0$ and $t^S = 0$.

Proof. By Satz 4.12 of Koch [5], we have that G_S is the pro- p -free group if and only if $H^2(G_S, \mathbb{Z}/p\mathbb{Z}) = \{0\}$. By (1) of Theorem 3, we have that $H^2(G_S, \mathbb{Z}/p\mathbb{Z}) = \{0\}$ is equivalent to $\delta_p = t^S = 0$. Q. E. D.

Lemma 10. Suppose $P \subset S$. Let r_2 be the number of complex places of k . Then we have

$$g^S = e_S - p\text{-rank}(t_p(E)) + p\text{-rank}(C_{S, \omega}) + r_2 + 1.$$

Proof. Let J be the idèle group of k , and U be its unit group. Put $U(S) = \prod_{p \in S} U_p$, which is contained in U .

By §3 in Miki [6], we have an exact sequence

$$(3.6) \quad 1 \longrightarrow U_k^S(p)/(k^\times)^p \longrightarrow U_k^\phi(p)/(k^\times)^p \longrightarrow U/U(S) \cdot U^p \\ \longrightarrow J/U(S) \cdot J^p \cdot k^\times \longrightarrow J/U \cdot J^p \cdot k^\times \longrightarrow 1.$$

Since $G_S^*/(G_S^*)^p \simeq J/U(S) \cdot J^p \cdot k^\times$ by class field theory, we have $p\text{-rank}(J/U \cdot J^p \cdot k^\times) = g_S$. We compute g^S by (3.6). We have $U_k^\phi(p)/E \cdot (k^\times)^p \simeq A_\phi^{(0)}$ by Lemma 9. Let h_p be the p -rank of the p -Sylow subgroup of the ideal class group of k . Then h_p

$= p\text{-rank}(J/U \cdot J^p \cdot k^\times)$ by the definition of h_p . Since h_p is also equal to $p\text{-rank}(A_\phi^{(0)})$, we have $p\text{-rank}(J/U \cdot J^p \cdot k^\times) = p\text{-rank}(A_\phi^{(0)})$. Hence

$$\begin{aligned}
 (3.7) \quad & p\text{-rank}(J/U \cdot J^p \cdot k^\times) - p\text{-rank}(U_k^\phi(p)/(k^\times)^p) = \\
 & p\text{-rank}(J/U \cdot J^p \cdot k^\times) - (p\text{-rank}(U_k^\phi(p)/E \cdot (k^\times)^p) + \\
 & p\text{-rank}(E \cdot (k^\times)^p/(k^\times)^p)) \\
 & = p\text{-rank}(E \cdot (k^\times)^p/(k^\times)^p) = -p\text{-rank}(E/E^p).
 \end{aligned}$$

We have $p\text{-rank}(U/U(S) \cdot U^p) = e_S + [k:\mathbf{Q}]$ because $U/U(S) \cdot U^p$ is isomorphic to U_S/U_S^p . Therefore by (3.6), (3.7) and corollary to Lemma 4, we have

$$\begin{aligned}
 g^S &= p\text{-rank}(U_k^S(p)/(k^\times)^p) + (e_S + [k:\mathbf{Q}]) - p\text{-rank}(E/E^p) \\
 &= p\text{-rank}(C_{S,\omega}) + e_S + r_2 + 1 - p\text{-rank}(t_p(E)).
 \end{aligned}$$

Q. E. D.

Theorem 4. Put $r^S = p\text{-rank}(H^2(G_S, \mathbf{Z}/p\mathbf{Z}))$. Suppose that k is totally imaginary if $p = 2$. Suppose that $P \subset S$. Then $r^S = 0$ if and only if $p\text{-rank}(C_{S,\omega}) = 0$ and $e_S = p\text{-rank}(t_p(E))$.

Proof. By (1) of Theorem 3 and Lemma 10, we have $r^S = 0$ holds if and only if $e_S - p\text{-rank}(t_p(E)) + p\text{-rank}(C_{S,\omega}) = 0$. Since $e_S - p\text{-rank}(t_p(E)) \geq 0$, we have $r^S = 0$ if and only if $e_S - p\text{-rank}(t_p(E)) = 0$ and $p\text{-rank}(C_{S,\omega}) = 0$. Q. E. D.

Remark. We see $e_S \geq p\text{-rank}(t_p(E_S)) \geq p\text{-rank}(t_p(E))$.
Hence the condition (3) of Theorem 1 holds if $e_S = p\text{-rank}(t_p(E))$.

References

- [1] R. Gillard, Formulations de la conjecture de Leopoldt et étude d'une condition suffisante, Abh. Math. Sem. Univ. Hamburg **48**(1979), 125-138.
- [2] G. Gras, Remarques sur la conjecture de Leopoldt, C. R. Acad. Sc. Paris (A) **274**(1972), 377-380.
- [3] F.-P. Heider, Zahlentheoretische Koten unendlicher Erweiterungen, Arch. Math. **37**(1981), 341-352.
- [4] _____, Kapitulationsproblem und Kotentheorie, Manuscripta Math. **46**(1984), 227-272.
- [5] H. Koch, Galoissche Theorie der p -Erweiterungen, Springer-Verlag: Berlin-Heidelberg-New York, 1970.
- [6] H. Miki, On the Leopoldt conjecture on the p -adic regulators, to appear.
- [7] O. Neumann, On p -closed algebraic number fields with restricted ramifications, Math. USSR Izvestija **9**(1975), 234-254.
- [8] J. W. Sands, Kummer's and Iwasawa's version of Leopoldt's conjecture, preprint.
- [9] L. Washington, Introductions to Cyclotomic Fields,

Graduate Texts in Mathematics, no 83, Springer-Verlag:New
York-Heidelberg-Berlin, 1980.

Hiroshi Yamashita
Kanazawa Women's Junior College
Kanazawa 920-13
Japan