J. Math. Soc. Japan
Vol. 42, No. 2, 1990

Remarks on connections between the Leopoldt conjecture, p-class groups and unit groups of algebraic number fields

By Hiroshi YAMASHITA

(Received June 18, 1988)
(Revised Feb. 17, 1989)

Introduction.

Let p be a prime number. Leopoldt [8] showed that the p-adic rank r_p of the unit group of a totally real abelian number field K equals the number of non-trivial characters of K such that the p-adic L-functions associated to them have not value 0 at 1. Moreover, he obtained the p-adic class number formula in case where the p-adic rank equals the total number of non-trivial characters which is equal to the rank of the unit group. The Leopoldt conjecture comes from this. This equality of the p-adic rank and the rank of the unit group for an abelian field was verified by Ax [1] for several special cases, and was proved completely by Brumer [2] in the general case.

We define the p-adic rank of the unit group of an algebraic number field to which we refered above. Let $\mathcal{O}$ be an integral domain and $\mathcal{K}$ be its field of quotients. For an $\mathcal{O}$-module M, we define the essential $\mathcal{O}$-rank of M to be the value of $\dim_{\mathcal{K}} M\otimes_{\mathcal{O}}\mathcal{K}$, and denote it by ess. $\mathcal{O}$-rank M.

Let k denote a finite algebraic number field throughout this paper. Let E_1 be the group of units which are congruent to 1 modulo every prime $\mathfrak{p}$ lying over p, and let $U_{\mathfrak{p}}(1)$ be the group of the local units u such that $u\equiv 1 \bmod \mathfrak{p}$. Then E_1 is embedded into $\prod_{\mathfrak{p}|p}U_{\mathfrak{p}}(1)$ by $\varepsilon\rightarrow(\varepsilon, \varepsilon, \cdots, \varepsilon)$. Denote by $\bar{E}_1$ the closure of E_1 in $\prod U_{\mathfrak{p}}(1)$. Since $U_{\mathfrak{p}}(1)$ are multiplicative $\boldsymbol{Z}_p$-modules, where $\boldsymbol{Z}_p$ is the ring of p-adic integers, $\bar{E}_1$ is also a $\boldsymbol{Z}_p$-module. We refer to the ess. $\boldsymbol{Z}_p$-rank of $\bar{E}_1$ as the p-adic rank of the unit group of k, and denote it by r_p in this paper.

The Leopoldt conjecture predicts that the p-adic rank equals the essential $\boldsymbol{Z}$-rank of the unit group in any algebraic number field. We know by Brumer [2] that this equality holds for an abelian extension of an imaginary quadratic number field, and also know by Miyake [10] for certain non-abelian extensions of imaginary quadratic number fields.

Let r be the essential $\boldsymbol{Z}$-rank of the unit group of k, and we set $\delta_p=r-r_p$.

The Leopoldt conjecture is true if and only if $\delta_p=0$. We call this δ_p the defect value of the Leopoldt conjecture. Note that δ_p is a non-negative integer.

Throughout this paper, let E denote the group of units of k which are p-th powers at every infinite place. When p is odd, or when k is totally imaginary, E is the whole unit group. Let S be a finite set of finite places of k which contains the set P of all places lying over p. Let $U_S=\prod_{\mathfrak{p}\in S}U_{\mathfrak{p}}$, where $U_{\mathfrak{p}}$ are the local unit groups. By embedding E into U_S, we consider E as a subgroup of U_S. Denote by E_S the closure of E in U_S. It is a totally disconnected compact group. Note that $E_S=E\cdot E_S^n$ for an arbitrary positive integer n.

Let ζ_p be a primitive p-th root of unity, and G be the Galois group $\mathrm{Gal}(k(\zeta_p)/k)$. For each $\sigma\in G$, there exists $m\in(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ such that $\zeta_p^\sigma=\zeta_p^m$, where $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ is the multiplicative group of $\boldsymbol{Z}/p\boldsymbol{Z}$. Since $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ is naturally embedded into the multiplicative group of $\boldsymbol{Z}_p$, we obtain a $\boldsymbol{Z}_p$-valued character ω of G by putting $\omega(\sigma)=m$. Let ε_ω be the idempotent of the group ring $\boldsymbol{Z}_p[G]$ associated to ω, that is $\varepsilon_\omega=(1/|G|)\sum_{\sigma\in G}\omega(\sigma)\sigma^{-1}$.

Let C be the ideal class group of $k(\zeta_p)$, and let D be the subgroup generated by all of the extensions of ideals of S to $k(\zeta_p)$. Put $C_S=C/D\cdot C^p$; this is naturally considered a $\boldsymbol{Z}_p[G]$-module. Denote by $C_{S,\omega}$ the submodule of C_S generated by $\varepsilon_\omega(x)$, $x\in C_S$. This is an ω-eigenspace, that is, the submodule consisting of $x\in C_S$ such that $x^\sigma=x^{\omega(\sigma)}$ for all $\sigma\in G$.

Let S_∞ be the union of S and the set of all infinite places. Denote by $B_{S_\infty}(p)$ the subgroup of $k^\times/k^p$ generated by all those $\alpha\in k^\times$ which are locally p-th powers at every $\mathfrak{p}\in S_\infty$ and whose principal ideals (α) are p-th powers of ideals of k. We shall prove that $C_{S,\omega}$ and $B_{S_\infty}(p)$ are dual to each other (Proposition 1).

For an abelian group A, we denote the subgroups of p^n-torsion points by $t_p^{(n)}(A)$ and the union of $t_p^{(n)}(A)$ for $n=1, 2, 3, \cdots$ by $t_p(A)$. Let $\boldsymbol{F}_p$ be the finite field with p-elements. We consider A/A^p an $\boldsymbol{F}_p$-linear space. If A is a torsion group, we call its dimension the p-rank of A and denote it by p-rank A.

Let G_P^{ab} be the Galois group over k of the maximal abelian p-extension of k unramified outside P. We have the following formula of δ_p from Theorem I2 of Gras [5] if p is odd.

$$\delta_p = p\text{-rank}\, t_p(U_P)+p\text{-rank}\, C_{P,\omega}-p\text{-rank}\, t_p(k^\times)-p\text{-rank}\, t_p(G_P^{ab}).$$

Therefore, if p-rank $t_p(U_P)=p$-rank $t_p(k^\times)$ and $C_{P,\omega}=\{1\}$, then $\delta_p=0$. We obtain the same consequence also for $p=2$ from Theorem I3 of Gras [5] if k is totally imaginary. This sufficient condition for $\delta_p=0$ was shown in Gras [4], Miki [9] and Sands [12].

We shall refine the formula on δ_p (Theorem 2) and prove that there exists a certain unramified abelian p-extension over $k(\zeta_{p^n})$ whose Galois group is isomorphic to $(\boldsymbol{Z}/p^{n-a}\boldsymbol{Z})^{\delta_p}$ if n is greater than a certain non-negative integer a determined only by k; here ζ_{p^n} denotes a primitive p^n-th root of unity (Theorem 3). It follows from this, in particular, that $\delta_p=0$ if there is a positive integer $n>a$ such that the ideal class group of $k(\zeta_{p^n})$ have no classes of order p^{n-a}. Moreover we see that the λ-invariant of the $\boldsymbol{Z}_p$-extension $\bigcup_{n\geq 1}k(\zeta_{p^n})$ over $k(\zeta_p)$ is greater than δ_p-1 if $\delta_p\neq 0$. This was proved in Gillard [3] by using the Kummer pairing over $\bigcup k(\zeta_{p^n})$.

The purpose in the present paper is to study δ_p in connection with $t_p(E_S)$ and $C_{S,\omega}$, and to obtain sufficient conditions for $\delta_p=0$. Here we state out the main results.

THEOREM 1. *The Leopoldt conjecture for p is true for k if and only if there is a finite set S of finite places of k containing P and satisfying the following three conditions.*

(1) *$C_{S,\omega}$ vanishes.*

(2) *The p-ranks of $t_p(E_S)$ and $t_p(E)$ are equal.*

(3) *E^p contains $E_S{}^p\cap E'^p$, where E' is the whole unit group of k.*

COROLLARY. *Suppose k is totally imaginary when $p=2$. If p-rank $t_p(U_S)=$ p-rank $t_p(k^\times)$ and $C_{S,\omega}=\{1\}$, then the Leopoldt conjecture for p is true for every finite p-extensions of k unramified outside S.*

THEOREM 2. *Let S be a finite set of finite places of k containing P, and let S_∞ be the union of S and the set of all infinite places. For $\alpha\cdot k^p\in B_{S_\infty}(p)$, there exists an ideal $\mathfrak{a}$ of k such that $\mathfrak{a}^p=(\alpha)$; let $A_{S_\infty}^{(0)}$ denote the subgroup of the ideal class group of k generated by all such ideals $\mathfrak{a}$. Then we have the following equality*

$$\delta_p = p\text{-rank}\, t_p(U_S)-p\text{-rank}\, t_p(E)+p\text{-rank}\, C_{S,\omega}-p\text{-rank}\, A_{S_\infty}^{(0)} -p\text{-rank}\, t_p(U_S/E_S)+p\text{-rank}\, E'^p/E^p\,.$$

THEOREM 3. *Let k be a finite algebraic number field such that $\delta_p\geqq 1$. Suppose that $E\cdot t_p^{(1)}(k^\times)$ is equal to the whole unit group of k. Let K_t denote the cyclotomic extension $k(\zeta_{p^t})$ of k, where ζ_{p^t} is a primitive p^t-th root of unity. Let n be a positive integer satisfying $K_{n+1}\neq K_n$. Suppose that $\boldsymbol{Q}_n\cap k$ is totally imaginary when $p=2$ and $n\geqq 2$. Then we have the following statements.*

(1) *Let a be the smallest non-negative integer such that $x^{p^a}=1$ for every $x\in t_p(E_P)$. If $n>a$, then there exists an unramified abelian extension M_n of K_n whose Galois group* Gal(M_n/K_n) *is isomorphic to $(\boldsymbol{Z}/p^{n-a}\boldsymbol{Z})^{\delta_p}$ and in which every place lying over p is completely decomposed over K_n.*

(2) *Suppose $t_p(E_P)=t_p(E)$. Let n be a positive integer such that there is a ramified place in K_{n+1}/K_n. Let C_n be the ideal class group of K_n. Put $t=$ p-rank $C_n^{p^n}$, $s=p$-rank $C_n^{p^{n-1}}-t$ and $r=p$-rank C_n-t-s. Then there exists an*

unramified abelian extension M_n' *of* K_n *whose Galois group* $\mathrm{Gal}(M_n'/K_n)$ *is isomorphic to* $(\boldsymbol{Z}/p^n\boldsymbol{Z})^{\delta_p}$ *and in which every place lying over* $\mathfrak{p}$ *is completely decomposed over* K_n. *Moreover, if the p-ranks of the ideal class groups of* K_n *and* K_{n+1} *are equal, we have* $\delta_p \leqq s+\min(r, t)$.

COROLLARY. *Under the same assumptions as in* (2) *of Theorem* 3, *we have* $\delta_p=0$ *if* $s+\min(r, t)=0$.

In §1, we shall prove a basic formula of δ_p and show Theorem 1 by virtue of it. In §2, we shall show the formula of Theorem 2, which is a natural consequence from §1. As an application of this formula, we shall show Proposition 2. In the last section, we shall construct Kummer extensions of degree p^{n-a} over K_n by certain subgroups of E which are determined from $t_p(E_S)$, and prove Theorem 3.

The author is very grateful to the referee for looking the drafts over and checking the results many times.

1. The basic formula of δ_p and the proof of Theorem 1.

For a place $\mathfrak{q}\in S$, let $N\mathfrak{q}$ denote the absolute norm of $\mathfrak{q}$, and $m_{\mathfrak{q}}$ be the highest power of p dividing $N\mathfrak{q}-1$. Let T be the complement of P in S and put $V_S=\prod_{\mathfrak{p}\in P} V_{\mathfrak{p}}\times\prod_{\mathfrak{q}\in T} U_{\mathfrak{q}}^{m_{\mathfrak{q}}}$, where $V_{\mathfrak{p}}$ denote the subgroups of $U_{\mathfrak{p}}$ generated by a primitive $(N\mathfrak{p}-1)$-th root of unity. Put $F_S=E_S\cap V_S$ and $\tilde{E}_S=E_S/F_S$. Since U_S/V_S is a $\boldsymbol{Z}_p$-module, $\tilde{E}_S$ is also a $\boldsymbol{Z}_p$-module. Set $m=\mathrm{l.c.m.}\{N\mathfrak{p}-1\mid\mathfrak{p}\in P\}$. Note that U_P^m is the direct product of the groups of the principal local units $U_{\mathfrak{p}}(1)$ for all $\mathfrak{p}\in P$. We recall that $\bar{E}_1$ is the closure of E_1 in U_P^m, where E_1 is the group of units of k which are congruent to 1 modulo every $\mathfrak{p}\in P$. Since $E_1\supset E^m$ and $E\supset E_1^2$, the subgroup E_P^m of $\bar{E}_1$ is of finite index. Therefore we have $r_p=\mathrm{ess.}\ \boldsymbol{Z}_p\text{-rank}\ E_P^m$. It follows from this that

$$r_p=\mathrm{ess.}\ \boldsymbol{Z}_p\text{-rank}\ \tilde{E}_P.$$

Let $\pi: E_S\to E_P$ be the restriction onto E_S of the canonical projection from U_S to U_P. Since E_S is compact, $\pi(E_S)$ is also compact. Hence $E_P=\pi(E_S)$, because E is dense in $\pi(E_S)$. π induces the surjection $\tilde{\pi}: \tilde{E}_S\to\tilde{E}_P$ defined by $\tilde{\pi}(\varepsilon F_S)=\pi(\varepsilon)F_P$, and the kernel of $\tilde{\pi}$ is $(E_S\cap U_T\cdot V_P)\cdot F_S/F_S$, where $U_T=\prod_{\mathfrak{p}\in T}U_{\mathfrak{p}}$. We see $(E_S\cap U_T\cdot V_P)^n\subset E_S\cap V_T\subset F_S$ for $n=\mathrm{l.c.m.}\{N\mathfrak{p}-1\mid\mathfrak{p}\in P\}\cdot\mathrm{l.c.m.}\{m_{\mathfrak{q}}\mid\mathfrak{q}\in T\}$. This means that $\ker\tilde{\pi}$ is finite. Hence we obtain the equality

$$\mathrm{ess.}\ \boldsymbol{Z}_p\text{-rank}\ \tilde{E}_S=\mathrm{ess.}\ \boldsymbol{Z}_p\text{-rank}\ \tilde{E}_P.$$

Therefore, the essential $\boldsymbol{Z}_p$-rank of $\tilde{E}_S$ equals r_p.

LEMMA 1. *We have the following equality of the p-adic rank* r_p *of the unit* *group of* k.

$$r_p = p\text{-rank}\, E_S/E_S{}^p - p\text{-rank}\, t_p(E_S).$$

PROOF. If we prove $\tilde{E}_S/\tilde{E}_S \cong E_S{}^p/E_S{}^p$ and $t_p(\tilde{E}_S) \cong t_p(E_S)$, the lemma follows from the equality

$$\text{ess. } \boldsymbol{Z}_p\text{-rank}\, \tilde{E}_S = p\text{-rank}\, \tilde{E}_S/\tilde{E}_S{}^p - p\text{-rank}\, t_p(\tilde{E}_S).$$

We shall show these isomorphisms. We observe $V_S{}^p = V_S$ and that $\{V_S{}^n \mid n = 1, 2, 3, \cdots\}$ forms a base for the open neighborhood system of unity in V_S. Hence for every n, $V_S/V_S{}^n$ are finite abelian groups whose orders are prime to p. Since $F_S \cdot V_S{}^n/V_S{}^n$ are subgroups of $V_S/V_S{}^n$, we have $F_S{}^p \cdot V_S{}^n/V_S{}^n = F_S \cdot V_S{}^n/V_S{}^n$. Thus $F_S{}^p \cdot V_S{}^n = F_S \cdot V_S{}^n$, and hence

$$\bigcap_{n=1}^{\infty} (F_S{}^p \cdot V_S{}^n) = \bigcap_{n=1}^{\infty} (F_S \cdot V_S{}^n).$$

This means the closures of $F_S{}^p$ and F_S are equal. Since both of them are compact, we have $F_S{}^p = F_S$. Hence $F_S{}^{p^m} = F_S$ for every positive integer m. Moreover, $t_p(F_S) = \{1\}$, because $t_p(F_S)$ is a finite abelian group.

We obtain the first isomorphism, $E_S/E_S{}^p \cong \tilde{E}_S/\tilde{E}_S{}^p$, because $E_S{}^p \supset F_S{}^p = F_S$. Let g be an element of E_S such that $g^{p^m} \in F_S$ for a certain positive integer m. There is $h \in F_S$ such that $h^{p^m} = g^{p^m}$. We see $g \cdot h^{-1} \in t_p(E_S)$. This means $t_p(\tilde{E}_S) \cong t_p(E_S) \cdot F_S/F_S$. Hence $t_p(\tilde{E}_S) \cong t_p(E_S)/t_p(F_S)$. Thus we obtain the second isomorphism, $t_p(\tilde{E}_S) \cong t_p(E_S)$. Q. E. D.

We note ess. $\boldsymbol{Z}$-rank E equals p-rank $E/E^p - p$-rank $t_p(E)$. From this and Lemma 1 follows a formula of δ_p:

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

Let X be the complete system of representatives of E/E^p in E. Since $\bigcup_{\varepsilon \in X} \varepsilon E_S{}^p$ is a compact subset of E_S containing E, it must be equal to E_S itself. Hence we obtain a surjection f from E/E^p onto $E_S/E_S{}^p$ by $f(\varepsilon E^p) = \varepsilon E_S{}^p$, $\varepsilon \in X$. Since $\ker f = E \cap E_S{}^p/E^p$, we have an exact sequence

$$(1.1) \qquad 1 \longrightarrow E \cap E_S{}^p/E^p \longrightarrow E/E^p \xrightarrow{f} E_S/E_S{}^p \longrightarrow 1.$$

Let $A_{S_\infty}^{(2)}$ denote the subgroup of $k^\times/k^p$ generated by $E \cap E_S{}^p$, where S_∞ is the union of S and the set of all infinite places of k. Then

$$(1.2) \qquad p\text{-rank}\, A_{S_\infty}^{(2)} = p\text{-rank}\, E \cap E_S{}^p/E^p - p\text{-rank}\, E'^p \cap E_S{}^p/E^p,$$

where E' is the whole unit group of k. We note that this last term p-rank $E'^p \cap E_S{}^p/E^p$ vanishes when p is odd or when k is totally imaginary.

We obtain the following basic formula of δ_p from the above formula of δ_p, the exact sequence (1.1) and the equality (1.2).

(1.3) $\delta_p = p\text{-rank}\, t_p(E_S) - p\text{-rank}\, t_p(E) + p\text{-rank}\, A_{S_\infty}^{(2)} + p\text{-rank}\, E'^p \cap E_S{}^p / E^p$.

Since $t_p(E_S) \supset t_p(E)$, we see $p\text{-rank}\, t_p(E_S) - p\text{-rank}\, t_p(E) \geqq 0$. Hence δ_p vanishes if and only if $p\text{-rank}\, t_p(E_S) = p\text{-rank}\, t_p(E)$, $A_{S_\infty}^{(2)} \cong \{1\}$ and $E'^p \cap E_S{}^p \subset E^p$.

Let $C_{S,\omega}$ and $B_{S_\infty}(p)$ be as in the introduction. We shall show by using the Kummer pairing that $C_{S,\omega} \cong \{1\}$ implies $A_{S_\infty}^{(2)} \cong \{1\}$. We will prove the duality between $C_{S,\omega}$ and $B_{S_\infty}(p)$. Put $K = k(\zeta_p)$, where ζ_p is a primitive p-th root of unity. Let S_K be the set of all extensions to K of every places contained in S_∞. Let $B_{S_K}(p)$ be the subgroup of $K^\times/K^p$ generated by those $\alpha \in K^\times$ which are locally p-th powers at every $\mathfrak{P} \in S_K$ and whose principal ideals (α) are p-th powers of ideals of K. We recall that $C_S = C/D \cdot C^p$, where C is the ideal class group of K and where D is the subgroup generated by all ideals of places of S_K.

Let L be the unramified abelian p-extension of K corresponding to C_S by class field theory. Let $\mathfrak{G}$ be the Galois group of L/K and ϕ: $C_S \to \mathfrak{G}$ be the isomorphism. Then we have the Kummer pairing

$$\langle c, \bar{\alpha} \rangle = \sqrt[p]{\alpha}^{\,\phi(c)-1}, \tag{1.4}$$

where $\bar{\alpha} = \alpha K^p$ is the coset of $B_{S_K}(p)$ generated by α. This gives the perfect duality, and the Galois group $G = \mathrm{Gal}(K/k)$ acts by

$$\langle c^\tau, \bar{\alpha}^\tau \rangle = \langle c, \bar{\alpha} \rangle^{\omega(\tau)}, \qquad \tau \in G.$$

LEMMA 2. *Let N_G denote the norm map of G-module. Then $B_{S_\infty}(p)$ is isomorphic to the subgroup $N_G(B_{S_K}(p))$ of $B_{S_K}(p)$.*

PROOF. Let j: $k^\times/k^p \to K^\times/K^p$ be the homomorphism induced from the inclusion map from $k^\times$ into $K^\times$. We see $j(B_{S_\infty}(p))^{|G|} \subset N_G(B_{S_K}(p)) \subset j(B_{S_\infty}(p))$ and $\ker j = k^\times \cap K^p/k^p$. Since the order of G is prime to p, j maps $B_{S_\infty}(p)$ onto $N_G(B_{S_K}(p))$. On the other hand, j is injective, because $N_G(\ker j) = \ker j$ and $N_G(k^\times \cap K^p) \subset k^p$. This completes the proof.

PROPOSITION 1. *$B_{S_\infty}(p)$ is the dual of $C_{S,\omega}$ with respect to the pairing* (1.4).

PROOF. We have

$$\langle \varepsilon_\omega(c), \bar{\alpha} \rangle^{|G|} = \langle c, N_G(\bar{\alpha}) \rangle,$$

for $c \in C_S$ and $\bar{\alpha} \in K^\times/K^p$. The proposition follows from this and Lemma 2.

Q. E. D.

LEMMA 3. *For $\alpha \cdot k^p \in B_{S_\infty}(p)$, there is an ideal $\mathfrak{a}$ of k such that $\mathfrak{a}^p = (\alpha)$. Let $A_{S_\infty}^{(0)}$ denote the subgroup of the ideal class group of k generated by all such ideals $\mathfrak{a}$. Let $A_{S_\infty}^{(1)} = (E \cap U_S{}^p) \cdot k^p / (E \cap E_S{}^p) \cdot k^p$ and $A_{S_\infty}^{(2)} = (E \cap E_S{}^p) \cdot k^p / k^p$ Then*

$$B_{S_\infty}(p) \cong A_{S_\infty}^{(0)} \times A_{S_\infty}^{(1)} \times A_{S_\infty}^{(2)}. \tag{1.5}$$

(1.6) $$p\text{-rank}\, C_{S,\omega}=\sum_{i=0}^{2} p\text{-rank}\, A_{S_\infty}^{(i)}.$$

PROOF. Let $B_{S_\infty}^0(p)$ be the subgroup of $B_{S_\infty}(p)$ generated by $E\cap U_S{}^p$. For each $\alpha\cdot k^p\in B_{S_\infty}(p)$, take an ideal $\mathfrak{a}$ of k so that $\mathfrak{a}^p=(\alpha)$. Let c_α be the ideal class containing $\mathfrak{a}$. We define a surjection from $B_{S_\infty}(p)$ onto $A_{S_\infty}^{(0)}$ by $f(\bar{\alpha})=c_\alpha$. We see the kernel of f is $B_{S_\infty}^0(p)$, hence $B_{S_\infty}(p)/B_{S_\infty}^0(p)\cong A_{S_\infty}^{(0)}$. Since $B_{S_\infty}(p)$ is an elementary abelian p-group, we have

$$B_{S_\infty}(p)\cong A_{S_\infty}^{(0)}\times B_{S_\infty}^0(p).$$

Similarly, since $B_{S_\infty}^0(p)/A_{S_\infty}^{(2)}=A_{S_\infty}^{(1)}$, we have

$$B_{S_\infty}^0(p)\cong A_{S_\infty}^{(1)}\times A_{S_\infty}^{(2)}.$$

Hence we obtain (1.5). (1.6) follows from (1.5) and Proposition 1, immediately.
Q. E. D.

PROOF OF THEOREM 1. Assume S satisfies all of the conditions (1), (2) and (3). By Proposition 1 and (1.5), we see that the condition (1) implies $A_{S_\infty}^{(2)}\cong\{1\}$. Hence, by the basic formula (1.3), we obtain $\delta_p=0$ from the conditions (2) and (3). Conversely assume $\delta_p=0$. Then, by the basic formula (1.3), we see that the conditions (2) and (3) hold for any S containing all places lying over p. Take a prime ideal from each ideal class c of $k(\zeta_p)$ and let $\mathfrak{p}_c$ denote its restriction to k. Let S be the union of the set of all places of such prime ideals $\mathfrak{p}_c$ and the set of all places of k lying over p. This S obviously satisfies the condition (1), and is the desired finite set of places of k. Q. E. D.

We prove the corollary to Theorem 1. Let k_S be the maximal p-extension of k unramified outside S, and put $G=\mathrm{Gal}(k_S/k)$. G is a pro-p-group. The value of $\dim_{F_p}H^2(G,F_p)$ equals the number of the relations of a minimal generator system of G as a pro-p-group (see Serre [**13**], Corollary to Proposition 27 in Chap. I). Denote it by $r(G)$. G is a free pro-p-group if and only if $r(G)=0$. We note that the cohomological p-dimension $\mathrm{cd}_p(G)$ is less than 2 if and only if $r(G)=0$. If G is a free pro-p-group, an arbitrary subgroup H of G is also free, because $\mathrm{cd}_p(H)\leqq\mathrm{cd}_p(G)$ (see Serre [**13**], Proposition 14 in Chap. I).

Assume k is totally imaginary when $p=2$. We observe no infinite places are ramified in k_S/k. For such k and p, we obtain the following formula by Corollary 2 of the main theorem of Neumann [**11**]:

$$r(G)=p\text{-rank}\, B_{S_\infty}(p)+p\text{-rank}\, t_p(U_S)-p\text{-rank}\, t_p(E).$$

Since $B_{S_\infty}(p)\cong C_{S,\omega}$, we see $r(G)$ equal 0 if and only if $C_{S,\omega}=\{1\}$ and $p\text{-rank}\, t_p(U_S)=p\text{-rank}\, t_p(E)$. Hence we have $C_{S,\omega}=\{1\}$ and $p\text{-rank}\, t_p(E_S)=p\text{-rank}\, t_p(E)$ if $r(G)$ vanishes, because $p\text{-rank}\, t_p(U_S)\geqq p\text{-rank}\, t_p(E_S)$. It follows from Theorem 1 that the Leopoldt conjecture is true for k if $\mathrm{Gal}(k_S/k)$ is a free pro-p-group.

Let K be a finite extension of k contained in k_S. Let L be a Galois p-extension of K unramified outside S. Let L' be any conjugate field of L over k. We observe that every ramified place of k in L'/k is contained in S. Thus the Galois closure of L over k is contained in k_S. Hence k_S is also the maximal p-extension of K unramified outside S_K, where S_K denotes the set of all extensions of places contained in S. Assume $C_{S,\omega}=\{1\}$ and p-rank $t_p(U_S)=$ p-rank $t_p(E)$ for k. Then $\mathrm{Gal}(k_S/k)$ is a free pro-p-group, and hence, $\mathrm{Gal}(k_S/K)$ is also free. It follows from this that the Leopoldt conjecture is true for K.

Q. E. D.

2. The proof of Theorem 2 and its application.

We recall that $A_{S_\infty}^{(1)}$ is the factor group $(E\cap U_S{}^p)\cdot k^p/(E\cap E_S{}^p)\cdot k^p$. We have an exact sequence of elementary abelian p-groups

$$1 \longrightarrow E'^p/E'^p\cap E_S{}^p \longrightarrow E\cap U_S{}^p/E\cap E_S{}^p \longrightarrow A_{S_\infty}^{(1)} \longrightarrow 1, \tag{2.1}$$

where E' is the whole unit group of k. We can describe $E\cap U_S{}^p/E\cap E_S{}^p$ as follows.

LEMMA 4. *We have the following exact sequence.*

$$1 \longrightarrow t_p^{(1)}(U_S)\cdot E_S/E_S \longrightarrow t_p^{(1)}(U_S/E_S) \longrightarrow E\cap U_S{}^p/E\cap E_S{}^p \longrightarrow 1.$$

PROOF. Let W_S denote the subgroup of U_S consisting of those elements whose p-th powers are contained in E_S. Obviously, $t_p^{(1)}(U_S/E_S)=W_S/E_S$. For $u\in W_S$, there are $\varepsilon\in E$ and $\alpha\in E_S$ such that $u^p=\varepsilon\cdot\alpha^p$, because E is dense in E_S. Let f be a homomorphism from W_S onto $E\cap U_S{}^p/E\cap E_S{}^p$ defined by $f(u)=\varepsilon\cdot(E\cap E_S{}^p)$. Since the kernel of f is $t_p^{(1)}(U_S)\cdot E_S$, we have the exact sequence by f. Q. E. D.

PROOF OF THEOREM 2. The following equality follows from Lemma 4 and the exact sequence (2.1).

$$\begin{aligned} p\text{-rank}\, t_p^{(1)}(E_S) = {} & p\text{-rank}\, t_p^{(1)}(U_S) - p\text{-rank}\, t_p^{(1)}(U_S/E_S) \\ & + p\text{-rank}\, A_{S_\infty}^{(1)} + p\text{-rank}\, E'^p/E'^p\cap E_S{}^p. \end{aligned} \tag{2.2}$$

We obtain the formula of Theorem 2 from the basic formula (1.3) as follows. Eliminate the term p-rank $t_p(E_S)$ from (1.3) by using (2.2), and replace the term p-rank $A_{S_\infty}^{(1)}+p$-rank $A_{S_\infty}^{(2)}$ with p-rank $C_{S,\omega}-p$-rank $A_{S_\infty}^{(0)}$ by using (1.6). Q. E. D.

We recall the equivalent statement to the Leopoldt conjecture given by Iwasawa [7]. Let $\mathfrak{q}$ be a finite place of k such that $\mathfrak{q}\nmid p$, and $N\mathfrak{q}$ denote the absolute norm of $\mathfrak{q}$. If n is a natural number, we shall denote by $(n)_p$ the highest power of p dividing n. Let

$$e(\mathfrak{q}, a)=\max(p^a, (N\mathfrak{q}-1)_p)$$

for a natural number a. A finite abelian extension K over k will be called a $(\mathfrak{q}, a)$-field if K/k is unramified outside $p\mathfrak{q}$ and if

$$e(\mathfrak{q}, a)\leqq e(\mathfrak{q};\, K/k)$$

where $e(\mathfrak{q};\, K/k)$ denote the ramification index of $\mathfrak{q}$ in K/k. The Leopoldt conjecture is equivalent to the existence of a $(\mathfrak{q}, a)$-field for every $(\mathfrak{q}, a)$ such that $N\mathfrak{q}\equiv 1 \bmod p$ and $p^a\leqq(N\mathfrak{q}-1)_p$ (see Iwasawa [7] and Sands [**12**]).

Concerning with the $(\mathfrak{q}, 1)$-field, we obtain the following proposition from Theorem 2.

PROPOSITION 2. *Let T be the subset of $S\setminus P$ consisting of all places $\mathfrak{q}$ such that $(\mathfrak{q}, 1)$-fields exist. Then*

$$\begin{aligned}\delta_p \lneqq\, & p\text{-rank}\, t_p(U_S)-\#T+p\text{-rank}\, C_{S,\omega}-p\text{-rank}\, A_S^{(0)} \\ & -p\text{-rank}\, t_p(E)+p\text{-rank}\, E'^p/E^p\,.\end{aligned}$$

PROOF. Let $\tilde{k}_{S_\infty}^{ab}$ be the maximal abelian extension of k unramified outside S_∞, where S_∞ is the union of S and the set of all infinite places. Let H be the absolute class field of k. We can prove $U_S/E_S\cong\text{Gal}(\tilde{k}_{S_\infty}^{ab}/H)$ by means of class field theory. Let $k_{S_\infty}^{ab}$ be the maximal p-extension of k contained in $\tilde{k}_{S_\infty}^{ab}$. We note that $k_{S_\infty}^{ab}$ is a finite extension over $k_{P_\infty}^{ab}$, where P is the set of all places of k lying over p, because every $\boldsymbol{Z}_p$-extension of k are contained in $k_{P_\infty}^{ab}$ and $\text{Gal}(k_{S_\infty}^{ab}/k)$ is a finitely generated $\boldsymbol{Z}_p$-module. Hence we obtain

$$p\text{-rank}\, t_p(U_S/E_S)=p\text{-rank}\, t_p(\text{Gal}(\tilde{k}_{S_\infty}^{ab}/H))\geqq p\text{-rank Gal}(k_{S_\infty}^{ab}/k_{P_\infty}^{ab})\,.$$

Let $k(T)=\bigcup_{\mathfrak{q}\in T} k(\mathfrak{q})$, where $k(\mathfrak{q})$ is a $(\mathfrak{q}, 1)$-field. We observe $p\text{-rank Gal}(k(T)k_{P_\infty}^{ab}/k_{P_\infty}^{ab})=\#T$. Hence

$$p\text{-rank}\, t_p(\text{Gal}(k_{S_\infty}^{ab}/k_{P_\infty}^{ab}))\gneqq \#T\,.$$

Therefore, we obtain the inequality.

$$p\text{-rank}\, t_p(U_S/E_S)\gneqq \#T\,.$$

The proposition follows from Theorem 2. Q.E.D.

3. The construction of unramified extensions and the proof of Theorem 3.

In this section, we suppose that the defect value δ_p of k is different from 0, and show that the existence of a characteristic unramified abelian p-extension over $k(\zeta_{p^n})$, where ζ_{p^n} is a primitive p^n-th root of unity. We write δ for δ_p in this section.

If F is a finite algebraic number field or its completion at a certain finite place, we denote the exponent of the order of $t_p(F^\times)$ by $e(F)$, that is, $|t_p(F^\times)| = p^{e(F)}$.

Let u be an element of $t_p(E_S)$ and p^a be the order of u. We see $u=(\zeta_\mathfrak{p} \mid \mathfrak{p}\in S) \in U_S$, where $\zeta_\mathfrak{p}$ are p^a-th roots of unity in $k_\mathfrak{p}$. Since E is dense in E_S, there exists $\varepsilon\in E$ for each integer $m\geqq 1$ such that

$$u = \varepsilon\cdot\alpha^{p^m}, \quad \text{where} \quad \alpha\in E_S. \tag{3.1}$$

Set $K_n=k(\zeta_{p^n})$. Suppose that m satisfies the inequality $m\leqq e(K_n)$. Put $L=K_n(\sqrt[p^m]{\varepsilon})$. Then L/K_n is a Kummer extension which is unramified outside p. We consider the ramifications of places lying over p. Let $\mathfrak{P}$ be a finite place of K_n lying over p. Let $\mathfrak{p}$ be the restriction of $\mathfrak{P}$ to k and $\mathcal{P}$ an extension of $\mathfrak{P}$ to L. Denote the $\mathfrak{p}$-components of u and α by $u_\mathfrak{p}$ and $\alpha_\mathfrak{p}$, respectively. Let p^b be the order of $u_\mathfrak{p}$. The completion of K_n at $\mathfrak{P}$ is $k_\mathfrak{p}(\zeta_{p^n})$. Since ε is a product of a p^b-th root of unity and $\alpha_\mathfrak{p}^{p^m}\in k_\mathfrak{p}$, the completion of L at $\mathcal{P}$ is $k_\mathfrak{p}(\zeta_{p^n}, \zeta_{p^{b+m}})$. Hence we have the following lemma.

LEMMA 5. *Under the above notation, $\mathfrak{P}$ is completely decomposed in L/K_n if and only if $b+m\leqq e(k_\mathfrak{p}(\zeta_{p^n}))$.*

We suppose that S satisfies the following condition.

$$E\cap U_S{}^p = E^p. \tag{3.2}$$

Recall that E' is the whole unit group of k. Since $E'\subset U_S$, we have $E'^p\cap E = E^p$ by (3.2). Thus $E'^p=E^p$. This implies $E'=E\cdot t_p^{(1)}(k^\times)$. Further, we have $E\cap E_S{}^p=E^p$ because $E\cap U_S{}^p\supset E\cap E_S{}^p$. Hence by (1.2) and the basic formula (1.3), we obtain an equality

$$\delta = p\text{-rank}\, t_p(E_S) - p\text{-rank}\, t_p(E). \tag{3.3}$$

LEMMA 6. *Suppose $\delta\geqq 1$ and that S satisfies* (3.2). *Then there is a subgroup T_S of $t_p(E_S)$ such that $t_p(E_S)$ is a direct sum of T_S and $t_p(E)$.*

PROOF. If $t_p(E)=\{1\}$, the statement is obvious. Assume $t_p(E)\neq\{1\}$, and let p^d be the order. Note that $t_p(E)\neq\{1\}$ means k is totally imaginary when $p=2$. Hence $E=E'$.

We shall prove that the following equality holds for every positive integer t:

$$t_p(E)\cap t_p(E_S)^{p^t} = t_p(E)^{p^t}.$$

Firstly, we prove this equality for $t\leqq d$. Let η be a generator of $t_p(E)\cap t_p(E_S)^{p^t}$. $k(\sqrt[p^t]{\eta})$ is an unramified abelian p-extension over k in which every place in S is completely decomposed. We assume $k(\sqrt[p^t]{\eta})\neq k$. Then, $k(\sqrt[p^t]{\eta})$ must contain a primitive p^{d+1}-th root ζ. ζ^p is an element of $U_S{}^p$, because every place contained in S is completely decomposed in $k(\zeta)/k$. However, this is impossible, because $t_p(E)\cap U_S{}^p=t_p(E)^p$ from the assumption (3.2). Therefore $k(\sqrt[p^t]{\eta})=k$, namely $\eta\in t_p(E)\cap k^{p^t}=t_p(E)^{p^t}$. We have proved the above equality for $t\leqq d$.

In the case of $t>d$, the equality follows immediately because

$$t_p(E)\cap t_p(E_S)^{p^t}=(t_p(E)\cap t_p(E_S)^{p^d})\cap t_p(E_S)^{p^t}=\{1\}.$$

Let $\{u_0, u_1, \cdots, u_\delta\}$ be a basis of $t_p(E_S)$. For a primitive p^d-th root ξ of unity, there are $a_i\in \boldsymbol{Z}$ such that

$$\xi=u_0^{a_0}\cdot u_1^{a_1}\cdot \cdots \cdot u_\delta^{a_\delta}.$$

Put $I=\{i\,|\,a_i \text{ is prime to } p\}$. Since $\xi\notin t_p(E)\cap t_p(E_S)^p$, I is not empty. Put $p^a=\max\{\mathrm{ord}(u_i)\,|\,i\in I\}$. Then we see $\xi^{p^a}\in t_p(E_S)^{p^{a+1}}$. By the fact that we proved above, this means $\xi^{p^a}=1$. Hence there is $i\in I$ such that the orders of ξ and u_i are equal. This implies that there is a basis of $t_p(E_S)$ which contains ξ.

Q. E. D.

By this lemma and (3.3), we see

$$\delta=p\text{-rank}\, T_S. \tag{3.4}$$

Let $u_1, \cdots, u_\delta$ be a basis of T_S. Then for each $m\geqq 1$, we obtain a system of units $\varepsilon_1, \cdots, \varepsilon_\delta$ of E such that

$$u_i=\varepsilon_i\cdot\alpha_i^{p^m}, \qquad \alpha_i\in E_S,$$

by means of (3.1). We fix one of such systems of units for each m. Let $T_{S,m}$ denote the subgroup of E generated by this system $\{\varepsilon_1, \cdots, \varepsilon_\delta\}$.

We see $K_m=K_n$ for all integers m such that $n\leqq m\leqq e(K_n)$. Hence, in the following, we assume that n satisfies $e(K_n)=n$.

LEMMA 7. (1) *Suppose k contains $\sqrt{-1}$ when $p=2$. Then the* 1-*cohomology group* $H^1(\mathrm{Gal}(K_n/k), t_p(K_n^\times))=\{0\}$.

(2) *Suppose $p=2$, $k\not\ni\sqrt{-1}$. For a positive integer n such that $n=e(K_n)$, we have* $H^1(\mathrm{Gal}(K_n/k), t_2(K_n^\times))=\{0\}$ *if and only if $n=1$ or $k_0=k\cap \boldsymbol{Q}(\zeta_{2^n})$ is imaginary.*

PROOF. K_n/k is a cyclic extension when $p\geqq 3$, or when $p=2$ and $k\ni\sqrt{-1}$. Then the order of 1-dimensional cohomology group $H^1(\mathrm{Gal}(K_n/k), t_p(K_n^\times))$ equals that of the 0-dimensional Tate cohomology group $H^0(\mathrm{Gal}(K_n/k), t_p(K_n^\times))$. Hence the 1-dimensional cohomology group vanishes. (1) is proved.

We shall prove (2). When $n=1$, the cohomology group is always trivial. We consider the case of $n\geqq 2$. Let $\boldsymbol{Q}_n$ denote the 2^n-th cyclotomic field. There is an integer s, $2\leqq s\leqq n$, such that $k(\sqrt{-1})=K_s$ and $K_{s+1}\neq K_s$. Note that $k_0=$

$\boldsymbol{Q}_s \cap k$. We have a cohomology exact sequence

$$0 \longrightarrow H^1(\mathrm{Gal}(K_s/k), t_2(K_s^\times)) \longrightarrow H^1(\mathrm{Gal}(K_n/k), t_2(K_n^\times)) \longrightarrow$$
$$H^1(\mathrm{Gal}(K_n/K_s), t_2(K_n^\times)).$$

The last term of this exact sequence vanishes, because K_s contains $\sqrt{-1}$ and K_n/K_s is a cyclic extension. Further, we have

$$H^1(\mathrm{Gal}(K_s/k), t_2(K_s^\times)) \cong H^1(\mathrm{Gal}(\boldsymbol{Q}_s/k_0), t_2(\boldsymbol{Q}_s^\times)).$$

Since $\boldsymbol{Q}_s/k_0$ is a cyclic extension of degree 2, we have the equality

$$|H^1(\mathrm{Gal}(K_n/k), t_2(K_n^\times))| = |H^0(\mathrm{Gal}(\boldsymbol{Q}_s/k_0), t_2(\boldsymbol{Q}_s^\times))| = 2\cdot|N_G(t_2(\boldsymbol{Q}_s^\times))|^{-1},$$

where $G=\mathrm{Gal}(\boldsymbol{Q}_s/k_0)$ and N_G is the norm map. Let τ be the generator of G and ζ be a primitive 2^s-th root of unity. Then $H^1(\mathrm{Gal}(K_n/k), t_2(K_n^\times))\cong\{1\}$ if and only if $\zeta^{1+\tau}=-1$. ζ^τ equals either ζ^{-1} or $\zeta^{-(1+2^{s-1})}$ because $k\not\ni\sqrt{-1}$. In the case of $\zeta^\tau=\zeta^{-1}$, we see $N_G(t_2(\boldsymbol{Q}_s^\times))=\{1\}$ and k_0 is real. In the other case, we see $\zeta^{\tau+1}=\zeta^{-2^{s-1}}=-1$ and that k_0 is imaginary. Therefore, we complete the proof.

LEMMA 8. *Let n be a positive integer such that $n=e(K_n)$. Suppose that S satisfies* (3.2) *and that $k\cap\boldsymbol{Q}(\zeta_{2n})$ is totally imaginary when $p=2$ and $n\geqq 2$. Let m and l be integers such that $1\leqq m\leqq e(K_n)$ and $m\leqq l$. Then we have $T_{S,l}^{p^m}=T_{S,l}\cap K_n^{p^m}$ and an isomorphism*

$$T_{S,l}\cdot K_n^{p^m}/K_n^{p^m} \cong (\boldsymbol{Z}/p^m\boldsymbol{Z})^\delta.$$

PROOF. By the exact sequence (1.1), we observe that E/E^p is isomorphic to E_S/E_S^p because $E\cap E_S^p/E^p=\{1\}$ from the assumption (3.2). Hence the homomorphism f in (1.1) induces an isomorphism

$$T_{S,l}\cdot t_p(E)\cdot E^p/E^p \cong t_p(E_S)\cdot E_S^p/E_S^p.$$

This isomorphism implies the following one.

$$T_{S,l}\cdot t_p(E)\cdot E^p/t_p(E)\cdot E^p \cong t_p(E_S)\cdot E_S^p/t_p(E)\cdot E_S^p.$$

Thus we obtain

$$p\text{-rank } T_{S,l}\cdot t_p(E)\cdot E^p/t_p(E)\cdot E^p = \delta.$$

Since $T_{S,l}$ is generated by just δ elements, this means

(3.5) $$T_{S,l}\cap t_p(E)\cdot E^p = T_{S,l}^p.$$

It follows from this that $t_p(T_{S,l})=T_{S,l}\cap t_p(E)\subset t_p(T_{S,l})^p$. Hence $T_{S,l}$ is p-torsion free.

Next, we shall show the following equality for $m\geqq 2$.

$$T_{S,l} \cap t_p(E) \cdot E^{p^m} = T_{S,l}^{p^m}. \tag{3.6}$$

Let t be the maximal exponent of p such that

$$T_{S,l} \cap t_p(E) \cdot E^{p^m} \subset T_{S,l}^{p^t}.$$

Assume $t<m$. Take $z \in T_{S,l} \cap t_p(E) \cdot E^{p^m}$ which is not contained in $T_{S,l}^{p^{t+1}}$. There are $\zeta \in t_p(E)$ and $y \in E$ such that $z=\zeta \cdot y^{p^m}$, and there is $w \in T_{S,l}$ such that $z=w^{p^t}$. Hence $w=\zeta' \cdot y^{p^{m-t}}$ for a certain $\zeta' \in t_p(E)$. By (3.5), we see that w is contained in $T_{S,l}^p$, hence $z \in T_{S,l}^{p^{t+1}}$. This contradicts the choice of z. Therefore we have the equality (3.6) because the converse inclusion is clear.

Now we shall prove the lemma by virtue of (3.5) and (3.6). For $\alpha \in T_{S,l} \cap K_n^{p^m}$, there is $\beta \in K_n$ such that $\alpha=\beta^{p^m}$. By Lemma 7, the 1-dimensional cohomology group $H^1(\mathrm{Gal}(K_n/k), t_p(K_n^\times))$ is trivial. This implies that there are $\beta_0 \in E'$ and $\zeta \in t_p(K_n^\times)$ such that $\beta=\zeta \cdot \beta_0$. Since (3.2) implies $E'=E \cdot t_p^{(1)}(k^\times)$, we have $\alpha \in E^{p^m} \cdot t_p(E)$. Thus $T_{S,l} \cap K_n^{p^m} \subset t_p(E) \cdot E^{p^m}$. It follows from (3.5) and (3.6) that $T_{S,l} \cap K_n^{p^m}$ is contained in $T_{S,l}^{p^m}$. Since the converse inclusion is clear, the lemma is proved.

PROOF OF (1) OF THEOREM 3. We see that $K_n \neq K_{n+1}$ means $n=e(K_n)$. We see $E'^p=E^p$ from the assumption, $E \cdot t_p^{(1)}(k^\times)=E'$. Let S be a finite set of finite places of k which contains all places lying over p and which satisfies $C_{S,\omega}=\{1\}$. (See the latter half of the proof of Theorem 1.) Then by Lemma 3, we have $E \cap U_S{}^p=E'^p$, and hence $E \cap U_S{}^p=E^p$. Thus the condition (3.2) holds for this S. Let p^a be the exponent of $t_p(E_P)$. Since $n>a$ by the assumption, we set $m=n-a$ and put $M_n=K_n(\sqrt[p^m]{\varepsilon} \mid \varepsilon \in T_{S,m})$. By Lemma 8, we have

$$\mathrm{Gal}(M_n/K_n) \cong (\boldsymbol{Z}/p^m\boldsymbol{Z})^\delta.$$

By Lemma 5, M_n is an unramified extension of K_n in which every place lying over p is completely decomposed. This completes the proof.

We proceed to the proof of (2) of Theorem 3. Let L_n be the maximal unramified abelian p-extension of K_n. By class field theory, $\mathrm{Gal}(L_n/K_n)$ is isomorphic to the p-class group of K_n. Let $X(L_n)$ be the character group of $\mathrm{Gal}(L_n/K_n)$. For each $\sigma \in \mathrm{Gal}(L_{n+1}/K_{n+1})$, $\mathrm{res}(\sigma)$ denotes the restriction of σ onto L_n. Then for $\chi \in X(L_n)$, $\chi \circ \mathrm{res}$ is a character of $\mathrm{Gal}(L_{n+1}/K_{n+1})$. Let ext denote the homomorphism from $X(L_n)$ to $X(L_{n+1})$ defined by $\mathrm{ext}(\chi)=\chi \circ \mathrm{res}$ for $\chi \in X(L_n)$. We note that the corresponding abelian extension of K_{n+1} to $\mathrm{ext}(\chi)$ is an abelian extension of K_n.

Now suppose that $t_p(E_P)=t_p(E)$. Let l be a positive integer. We recall $T_{S,l} \cdot E_S{}^{p^l}=T_S \cdot E_S{}^{p^l}$ for a certain subgroup T_S of $t_p(E_S)$. Let π be the canonical projection from U_S to U_P. We showed in § 1 that π maps E_s onto E_p. Thus we have $\pi(T_{S,l}) \subset \pi(T_S) \cdot E_P{}^{p^l}=t_p(E) \cdot E_P{}^{p^l}$. Let $\{\varepsilon_1, \cdots, \varepsilon_\delta\}$ be a set of generators of

$T_{S,l}$. Take $\zeta_i \in t_p(E)$ for each ε_i so that $\pi(\varepsilon_i) \in \zeta_i \cdot E_P{}^{p^l}$, and put $\varepsilon_i' = \varepsilon_i \cdot \zeta_i^{-1}$. Let $T'_{S,l}$ be the subgroup of E generated by $\{\varepsilon_1', \cdots, \varepsilon_\delta'\}$. Note $\pi(\varepsilon) \in E_P{}^{p^l}$ for $\varepsilon \in T'_{S,l}$.

LEMMA 9. *Assume S satisfies* (3.2). *Assume $t_p(E_P) = t_p(E)$ and $n = e(K_n)$. Assume also that $k \cap \boldsymbol{Q}(\zeta_{2n})$ is totally imaginary when $p=2$ and $n \geqq 2$. Let m and l be integers such that $1 \leqq m \leqq n$ and $m \leqq l$. Put $M_{n,l}^{(m)} = K_n(\sqrt[p^m]{\varepsilon} \mid \varepsilon \in T'_{S,l})$. Then $M_{n,l}^{(m)}$ is an unramified extension of K_n in which every place lying over p is completely decomposed and* $\mathrm{Gal}(M_{n,l}^{(m)}/K_n)$ *is isomorphic to* $(\boldsymbol{Z}/p^m\boldsymbol{Z})^\delta$.

PROOF. Since $\pi(\varepsilon) \in E_P{}^{p^m}$ for each $\varepsilon \in T'_{S,l}$, $K_n(\sqrt[p^m]{\varepsilon})$ is an unramified extension of K_n in which every place lying over p is completely decomposed. Put $N_n = K_n(\sqrt[p^m]{\alpha} \mid \alpha \in T_{S,l})$. We have $M_{n,l}^{(m)} K_{n+m} = N_n K_{n+m}$ because $K_n(\sqrt[p^m]{\varepsilon_i'}) \subset K_n(\sqrt[p^m]{\varepsilon_i}, \sqrt[p^m]{\zeta_i})$ for each generator ε_i' of $T'_{S,l}$, where $\zeta_i \in t_p(E)$. Since the character group of $\mathrm{Gal}(N_n K_{n+m}/K_{n+m})$ is isomorphic to $T_{S,l} K_{n+m}^{p^m}/K_{n+m}^{p^m}$, we have $[N_n K_{n+m} : K_{n+m}] = p^{\delta m}$ by Lemma 8. Hence $[M_{n,l}^{(m)} : K_{n+m} \cap M_{n,l}^{(m)}] = p^{\delta m}$. On the other hand, we see $[M_{n,l}^{(m)} : K_n] \leqq p^{\delta m}$, because $T'_{S,l}$ is generated by δ elements. Therefore we have $[M_{n,l}^{(m)} : K_n] = p^{\delta m}$. Thus we obtain $[T'_{S,l} K_n^{p^m} : K_n^{p^m}] = p^{\delta m}$, and this implies the following isomorphism.

$$T'_{S,l} K_n^{p^m}/K_n^{p^m} \cong (\boldsymbol{Z}/p^m\boldsymbol{Z})^\delta. \tag{3.7}$$

Since $\mathrm{Gal}(M_{n,l}^{(m)}/K_n)$ is the dual group of $T'_{S,l} K_n^{p^m}/K_n^{p^m}$ by the Kummer pairing, we obtain an isomorphism

$$\mathrm{Gal}(M_{n,l}^{(m)}/K_n) \cong (\boldsymbol{Z}/p^m\boldsymbol{Z})^\delta. \qquad \text{Q.E.D.}$$

Take $\varepsilon \in T'_{S,n+1}$ and let $\chi_\varepsilon^{(n)}$ be the Kummer character defined by $\chi_\varepsilon^{(n)}(\sigma) = \sqrt[p^n]{\varepsilon}^{(\sigma-1)}$ for $\sigma = \mathrm{Gal}(L_n/K_n)$. Since $K_n(\sqrt[p^n]{\varepsilon}) \subset L_n$, we have $\chi_\varepsilon \in X(L_n)$. Let $\chi_\varepsilon^{(n+1)}$ denote the Kummer character defined by $\chi_\varepsilon^{(n+1)}(\sigma) = \sqrt[p^{n+1}]{\varepsilon}^{(\sigma-1)}$ for $\sigma \in \mathrm{Gal}(L_{n+1}/K_{n+1})$. Suppose that there is $\theta \in X(L_n)$ such that $\theta^p = \chi_\varepsilon^{(n)}$. Then $\mathrm{ext}(\theta^p) = \chi_\varepsilon^{(n+1)p}$. Hence there is $\eta \in X(L_{n+1})$ such that $\mathrm{ext}(\theta) \cdot \eta = \chi_\varepsilon^{(n+1)}$ and $\eta^p = 1$. Let $K_{n+1}(\eta)$ be the intermediate field of L_{n+1}/K_{n+1} corresponding to η. Since $K_{n+1}(\sqrt[p^{n+1}]{\varepsilon}) \subset L_n \cdot K_{n+1}(\eta)$ and since $K_{n+1}(\eta) \subset L_n \cdot K_{n+1}(\sqrt[p^{n+1}]{\varepsilon})$, we have $K_{n+1}(\sqrt[p^{n+1}]{\varepsilon})$ is an abelian extension of K_n if and only if $K_{n+1}(\eta)$ is abelian over K_n.

LEMMA 10. *Suppose S satisfies* (3.2). *Let n be a positive integer such that $n = e(K_n)$. Suppose that $k \cap \boldsymbol{Q}(\zeta_{p^{n+1}})$ is totally imaginary when $p=2$ and $n \geqq 2$. Take $\varepsilon \in T'_{S,n+1}$ so that $\varepsilon \notin T'^{\,p}_{S,n+1}$. Then $K_{n+1}(\sqrt[p^{n+1}]{\varepsilon})/K_n$ is never an abelian extension.*

PROOF. It follows from (3.7) that $K_{n+1}(\sqrt[p^{n+1}]{\varepsilon})/K_{n+1}$ is a cyclic extension of degree p^{n+1}. Let τ be a generator of the Galois group such that $\tau(\sqrt[p^{n+1}]{\varepsilon})$

$={}^{p^{n+1}}\sqrt{\varepsilon}\cdot\zeta$ for a certain primitive p^{n+1}-th root ζ of unity. Let σ be an extension to $K_{n+1}(^{p^{n+1}}\sqrt{\varepsilon})$ of a generator of the Galois group of K_{n+1}/K_n. Let a be an integer such that $\zeta^\sigma=\zeta^a$. Since $\varepsilon^\sigma=\varepsilon$, we have $\chi_\varepsilon^{(n+1)}(\sigma\tau\sigma^{-1})=\chi_\varepsilon^{(n+1)}(\tau)^a$. Hence $\sigma\cdot\tau\cdot\sigma^{-1}=\tau^a$. Assume that $K_{n+1}(^{p^{n+1}}\sqrt{\varepsilon})/K_n$ is abelian. Then $a\equiv 1 \bmod p^{n+1}$. Therefore σ has to be the identity in K_{n+1}. However, this is not the case. Hence $K_{n+1}(^{p^{n+1}}\sqrt{\varepsilon})/K_n$ is not abelian. Q.E.D.

LEMMA 11. *Assume S satisfies* (3.2). *Assume* $t_p(E_P)=t_p(E)$. *Let n be a positive integer such that $n=e(K_n)$. Assume also that $k\cap\boldsymbol{Q}(\zeta_{2^{n+1}})$ is totally imaginary when $p=2$ and $n\geqq 2$. Put $M_{n,n+1}^{(n)}=K_n(^{p^n}\sqrt{\varepsilon}\mid\varepsilon\in T'_{S,n+1})$; this is a subfield of the p-Hilbert class field L_n of K_n. Let $X(L_n)$ be the character group of* $\mathrm{Gal}(L_n/K_n)$ *and $X(M_{n,n+1}^{(n)})$ be that of* $\mathrm{Gal}(M_{n,n+1}^{(n)}/K_n)$. *If* $t_p^{(1)}(X(L_{n+1}))\subset \mathrm{ext}(X(L_n))$, *we have* $X(M_{n,n+1}^{(n)})\cap X(L_n)^p=X(M_{n,n+1}^{(n)})^p$.

PROOF. We have $M_{n,n+1}^{(n)}\subset L_n$ by Lemma 9. Take $\theta\in X(L_n)$ and $\varepsilon\in T'_{S,n+1}$ so that $\theta^p=\chi_\varepsilon^{(n)}$. Then there is $\eta\in t_p^{(1)}(X(L_{n+1}))$ such that $\mathrm{ext}(\theta)=\eta\cdot\chi_\varepsilon^{(n+1)}$. Since the p-ranks of $t_p^{(1)}(X(L_{n+1}))$ and $t_p^{(1)}(\mathrm{ext}(X_n(L_n)))$ are equal, we have $\chi_\varepsilon^{(n+1)}\in\mathrm{ext}(X(L_n))$. This means that $K_{n+1}(^{p^{n+1}}\sqrt{\varepsilon})/K_n$ is abelian. By Lemma 10, we have $\varepsilon\in T'^{p}_{S,n+1}$, that is $\chi_\varepsilon^{(n)}\in X(M_{n,n+1}^{(n)})^p$. Q.E.D.

PROOF OF (2) OF THEOREM 3. We have shown in the proof of (1) of Theorem 3 that there exists a finite set S of finite places of k containing P and satisfying (3.2). Take such an S and put $M'_n=M_{n,n+1}^{(n)}$. Then we obtain the first assertion by Lemma 9.

Let $\phi_n: C_n\to\mathrm{Gal}(L_n/K_n)$ be the isomorphisms defined by class field theory. C_n and $X(L_n)$ are dual to each other by the pairing

$$\langle\chi, c\rangle_n=\chi(\phi_n(c))$$

where $\chi\in X_n(L_n)$ and $c\in C_n$. Hence they are of the same type as finite abelian groups. We have the following equalities.

$$t=p\text{-rank}\,X(L_n)^{p^n},$$
$$s=p\text{-rank}\,X(L_n)^{p^{n-1}}-t,$$
$$r=p\text{-rank}\,X(L_n)-t-s.$$

Moreover, ext is the dual map of the norm map $N_{K_{n+1}/K_n}: C_{n+1}\to C_n$, because

$$\langle\mathrm{ext}(\chi), c\rangle_{n+1}=\langle\chi, N_{K_{n+1}/K_n}(c)\rangle_n$$

for $\chi\in X(L_{n+1})$ and $c\in C_{n+1}$.

Since there is a ramified place in K_{n+1}/K_n, we see N_{K_{n+1}/K_n} is surjective. Thus ext is injective. This implies $t_p^{(1)}(X(L_{n+1}))\subset\mathrm{ext}(X(L_n))$, because the p-ranks of C_n and C_{n+1} are equal by the assumption.

Put $Y=X(M_{n,n+1}^{(n)})$. Since $Y\cong(\boldsymbol{Z}_p/p^n\boldsymbol{Z}_p)^\delta$ by Lemma 9, we obtain

$$\delta \leqq p\text{-rank}\, X(L_n)^{p^{n-1}} = s+t.$$

Next we shall prove $\delta\leqq r+s$. Let $(p^{n-a_1}, \cdots, p^{n-a_r}, \cdots, p^n, \cdots, p^n, p^{n+b_1}, \cdots, p^{n+b_t})$ be the type of $X(L_n)$ as an abelian group, where $a_1\geqq\cdots\geqq a_r\geqq 1$ and $1\leqq b_1\leqq\cdots\leqq b_t$. There are three subgroups X_1, X_2 and X_3 of $X(L_n)$ such that $X(L_n)$ is a direct product of them and

$$X_1 \cong \boldsymbol{Z}/p^{n-a_1}\boldsymbol{Z}\times \cdots \times\boldsymbol{Z}/p^{n-a_r}\boldsymbol{Z},$$
$$X_2 \cong (\boldsymbol{Z}/p^n\boldsymbol{Z})^s,$$
$$X_3 \cong \boldsymbol{Z}/p^{n+b_1}\boldsymbol{Z}\times \cdots \times\boldsymbol{Z}/p^{n+b_t}\boldsymbol{Z}.$$

Then Y is contained in $X_1\times X_2\times X_3^p$. Since $Y\cap X(L_n)^p=Y^p$ by Lemma 11, we have

$$p\text{-rank}\, Y/Y^p \leqq p\text{-rank}\, X_1\times X_2\times X_3^p/X_1^p\times X_2^p\times X_3^p = r+s.$$

Thus we have proved (2) of Theorem 3.

References

[1] J. Ax, On the units of an algebraic number field, Illinois J. Math., **9** (1965), 584-589.

[2] A. Brumer, On the units of algebraic number fields, Mathematika, **14** (1967), 121-124.

[3] R. Gillard, Formulations de la conjecture de Leopoldt et étude d'une condition suffisante, Abh. Math. Sem. Univ. Hamburg, **48** (1979), 125-138.

[4] G. Gras, Remarques sur la conjecture de Leopoldt, C. R. Acad. Sci. Paris (A), **274** (1972), 377-380.

[5] ———, Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'un corps de nombres, J. Reine Angew. Math., **333** (1982), 86-132.

[6] ———, Une interpretétation de la conjecture de Leopoldt, C. R. Acad. Sci. Paris (I), **302** (1986), 607-610.

[7] K. Iwasawa, On Leopoldt's conjecture (in Japanese), Seminar Note on Algebraic Number Theory, Sūrikaiseki-kenkyūsho, Kyoto, 1984.

[8] H. W. Leopoldt, Zur Arithmetik in abelschen Zahlkörpern, J. Reine. Angew. Math., **209** (1962), 54-71.

[9] H. Miki, On the Leopoldt conjecture on the p-adic regulators, J. Number Theory, **26** (1987), 117-128.

[10] K. Miyake, On the units of an algebraic number field, J. Math. Soc. Japan, **34** (1982), 515-525.

[11] O. Neumann, On p-closed algebraic number fields with restricted ramifications, Math. USSR-Izv., **9** (1975), 243-254.

[12] J. W. Sands, Kummer's and Iwasawa's version of Leopoldt's conjecture, Canad. Math. Bull., to appear.

[13] J. P. Serre, Cohomologie galoisienne, Lecture Notes in Math., **5**, Springer, 1964.

Hiroshi YAMASHITA
Kanazawa Women's College
Kanazawa 920-13
Japan