J. Math. Soc. Japan
Vol. 36, No. 1, 1984

Leopoldt's conjecture and Reiner's theorem

By Hiroo MIKI and Hirotaka SATO

(Received Oct. 6, 1982)
(Revised Nov. 22, 1982)

§1. Introduction.

Let p be a prime number and let k be a finite algebraic number field. Let k_v be the completion of k with respect to a prime divisor v of k, and let S_k be the set of all prime divisors of k lying over p. Let E_k be the group of units ε of k such that $\varepsilon \in U_v^{(1)}$ for all $v \in S_k$, where $U_v^{(1)}$ is the group of principal units of k_v. Imbed E_k into $\prod_{v \in S_k} U_v^{(1)}$ in the natural way and take the topological closure $\bar{E}_k$ of E_k in $\prod_{v \in S_k} U_v^{(1)}$. Put $\delta_k = \mathrm{rank}_{\boldsymbol{Z}} E_k - \mathrm{rank}_{\boldsymbol{Z}_p} \bar{E}_k$, where $\boldsymbol{Z}$ and $\boldsymbol{Z}_p$ are the rings of integers and p-adic integers respectively. Leopoldt [4] conjectured that $\delta_k = 0$ for any prime number p.

Let K/k be a finite Galois p-extension with Galois group G. In [**7**, Corollary to Theorem 2], we proved the Leopoldt conjecture for (K, p) under certain strong conditions on k and the ramification of K/k. The purpose of the present paper is to give another proof of this theorem by considering the $\boldsymbol{Z}_p[G]$-module structure of the Galois group X_K^* of the composite of all $\boldsymbol{Z}_p$-extensions of K based on Reiner's theorem [**1**, Theorem (74.3)] when K/k is a cyclic extension of degree p (Theorem and its Corollary).

§2. The G-module structure of the Galois group of the composite of $\boldsymbol{Z}_p$-extensions of K.

Let M_k be the maximal p-ramified abelian p-extension of k and let M_k^* be the composite of all $\boldsymbol{Z}_p$-extensions of k. Let L_k and L_k^* be the maximal elementary abelian p-extension of k in M_k and M_k^* respectively. Put $X_k = G(M_k/k)$ and $X_k^* = G(M_k^*/k)$. Then M_K^*/k is a Galois extension and X_K^* becomes a G-module by $\sigma\tau = \tilde{\sigma}\tau\tilde{\sigma}^{-1}$ $(\tau \in X_K^*)$, where σ is a generator of G and $\tilde{\sigma}$ is an extension of σ to M_K^*. From now on, we assume that K/k is unramified at all infinite primes of k if $p=2$. By [**2**, Theorem 3], X_K^* is a free $\boldsymbol{Z}_p$-module of rank $(pr_2 + 1 + \delta_K)$, where $r_2 = r_2(k)$ is the number of complex places of k. Hence by Reiner's theorem [**1**, Theorem (74.3)],

(1) $X_K^* \cong \boldsymbol{Z}_p[G]^\alpha \oplus R^\beta \oplus \boldsymbol{Z}_p^\gamma$ $(\alpha, \beta, \gamma \geqq 0)$ as $\boldsymbol{Z}_p[G]$-modules, and

(2) $$p\alpha+(p-1)\beta+\gamma=pr_2+1+\delta_K,$$

where $R=\boldsymbol{Z}_p[\zeta]$ (ζ: a primitive p-th root of unity) is a $\boldsymbol{Z}_p[G]$-module by $\sigma x= \zeta x$ $(x \in R)$ and $\boldsymbol{Z}_p$ is a $\boldsymbol{Z}_p[G]$-module by $\sigma x=x$ $(x \in \boldsymbol{Z}_p)$.

LEMMA 1. *Let the notation and assumptions be as above. Then*

(3) $$\alpha+\gamma=r_2+1+\delta_k.$$

PROOF. Let M' be the maximal abelian extension of k in M_K^*. Put $\tilde{G}= G(M'/K)$ and $G^*=G(M'/k)$. Then

$$\begin{aligned}\tilde{G}&=X_K^*/(\sigma-1)X_K^*\\ &\cong(\boldsymbol{Z}_p[G]/(\sigma-1)\boldsymbol{Z}_p[G])^\alpha \oplus (R/(\zeta-1)R)^\beta \oplus \boldsymbol{Z}_p^\gamma.\end{aligned}$$

Hence

(4) $$\tilde{G} \cong \boldsymbol{Z}_p^{\alpha+\gamma} \oplus \boldsymbol{F}_p^\beta.$$

Hence $\mathrm{rank}_{\boldsymbol{Z}_p}\tilde{G}=\alpha+\gamma$. Since $G(M'/M_k^*)$ is the torsion subgroup of G^*, we have

$$\mathrm{rank}_{\boldsymbol{Z}_p}G^*=\mathrm{rank}_{\boldsymbol{Z}_p}G(M_k^*/k)=r_2+1+\delta_k.$$

Since $[G^*: \tilde{G}]=p$, we have $\mathrm{rank}_{\boldsymbol{Z}_p}\tilde{G}=\mathrm{rank}_{\boldsymbol{Z}_p}G^*$. Hence we obtain the equality (3). Q.E.D.

Let T be a finite set of finite prime divisors of k such that $S_k \cap T=\emptyset$. Put $t=|T|$ (the number of elements of T) and $t'=\mathrm{Max}(t-1, 0)$.

LEMMA 2. *Let the notation and assumptions be as above. Moreover, assume the following* (i) *and* (ii):

(i) *K/k is unramified outside $S_k \cup T$ and ramified at T.*

(ii) $\dim_{\boldsymbol{F}_p} X_k/X_k^p=r_2+1$, *where $\boldsymbol{F}_p$ is the field of p elements.*

Then $\beta \leqq t'$.

PROOF. By [7, Lemma 9 (Kubota, Šafarevič and Iwasawa)], the condition (ii) is equivalent to that $\delta_k=0$ and X_k is torsion free. Let K_1 be the fixed field by $\boldsymbol{Z}_p^{\alpha+\gamma}$ in M' by the isomorphism (4). Then $G(K_1/K) \cong \boldsymbol{F}_p^\beta$, $M'=(KM_k^*)K_1$ and

(5) $$K_1 \cap KM_k^*=K.$$

We see that $G(K_1/k)^p=0$ if $t=0$. In fact, if there exists a cyclic extension K_2 of k of degree p^2 such that $K \subset K_2 \subset K_1$, then the condition (ii) implies that there exists a $\boldsymbol{Z}_p$-extension k_∞ of k such that $K_2 \subset k_\infty$, so $K_2 \subset M_k^*K$. This contradicts (5). Let k_1 $(\subset K_1)$ be an extension of k such that $G(K_1/k)=G(K_1/K) \times G(K_1/k_1)$, or the inertia field of $\mathfrak{Q}$ with respect to k according as $t=0$ or $t \geqq 1$, where $\mathfrak{Q}$ is an extension of a fixed $\mathfrak{q} \in T$ to K_1. Since K/k is ramified at $\mathfrak{q}$ and K_1/K is unramified at $\mathfrak{Q}$, we have $G(K_1/k_1)=(p)$ and $K \cap k_1=k$, so $K_1=Kk_1$.

Hence $[K_1:K]=[k_1:k]$. Let L'_k be the maximal elementary abelian p-extension of k which is unramified outside $S_k\cup(T-\{\mathfrak{q}\})$. Then $k_1\subset L'_k$ and $L_k\subset L'_k$. By the condition (ii), $L_k\subset M_k^*$, so (5) implies that $L_k\cap k_1=k$. Hence

$$[L_kk_1:k]=[L_k:k][k_1:k]\leqq[L'_k:k].$$

By (ii), $[L_k:k]=p^{r_2+1}$ and $[L'_k:k]=p^{r_2+1+t'}$ by [8, Theorem 1] or [3] (see also [6, Corollary 1 to Theorem 1]). Thus $p^{\beta}=[K_1:K]=[k_1:k]\leqq p^{t'}$, so $\beta\leqq t'$.

Q.E.D.

LEMMA 3. *Let $V\in S_K$ be an extension of a $v\in S_k$. Put $K'_V=K_V(\zeta)$ and $k'_v=k_v(\zeta)$. Let τ_v be a generator of $G(k'_v/k_v)$ and let $m_v\in\boldsymbol{Z}$ be such that $\zeta^{\tau_v}=\zeta^{m_v}$. Assume that $\zeta\notin k_v$. Let $x\in k'_v$ be such that $x^{\tau_v-m_v}\in k'^p_v$. Then $x\in N_{K'_V/k'_v}(K'_V)$.*

PROOF. By taking $N_{k'_v/k_v}$ of $x^{\tau_v-m_v}\in k'^p_v$, we have $N_{k'_v/k_v}(x)^{1-m_v}\in k_v^p$. Since $\zeta\notin k_v$, we have $1-m_v\not\equiv 0 \pmod p$. Hence $N_{k'_v/k_v}(x)\in k_v^p$. By translation theorem in local class field theory, $x\in N_{K'_V/k'_v}(K'_V)$. Q.E.D.

Let L be an elementary abelian p-ramified p-extension of k and let $L(T)$ be the maximal extension of k in L which is completely decomposed at T (if $T=\emptyset$, then put $L(T)=L$). Put $k'=k(\zeta)$, $K'=K(\zeta)$, $L'=L(\zeta)$, $L(T)'=L(T)(\zeta)$, $V=\{x\in k'^{\times}\mid \sqrt[p]{x}\in L'\}$ and $V(T)=\{x\in k'^{\times}\mid \sqrt[p]{x}\in L(T)'\}$.

LEMMA 4. *Let the notation and assumptions be as above. Assume the condition* (i) *in Lemma* 2. *Then the following* (i) *and* (ii) *hold.*

(i) $\dim_{F_p}(V\cap N_{K'/k'}(K'^{\times})/(k'^{\times})^p)\leqq\dim_{F_p}G(L(T)/k)$.

(ii) *Moreover assume one of the following* (a) *and* (b).

(a) $\zeta\notin k_v$ *for all* $v\in S_k$.

(b) $\zeta\in k$ *and* $|S_k|$ (*the number of elements in* S_k)$=1$.

Then $\dim_{F_p}(V\cap N_{K'/k'}(K'^{\times})/(k'^{\times})^p)=\dim_{F_p}G(L(T)/k)$.

PROOF. (i) If $x\in V\cap N_{K'/k'}(K'^{\times})$, then $x\in N_{K'_{\mathfrak{q}'}/k'_{\mathfrak{q}'}}(K'_{\mathfrak{q}'})$ for any $\mathfrak{q}'\in T'$, where T' is the extension of T to k'. Hence $x\in(k'_{\mathfrak{q}'})^p$ for any $\mathfrak{q}'\in T'$, so $x\in V(T)$. Hence $V\cap N_{K'/k'}(K'^{\times})\subset V(T)$. Since $\dim_{F_p}V(T)/(k'^{\times})^p=\dim_{F_p}G(L(T)/k)$, we have the assertion.

(ii) Let $x\in V$. Let τ be a generator of $G(k'/k)$ and let $m\in\boldsymbol{Z}$ be such that $\zeta^{\tau}=\zeta^m$. Then by Kummer theory, $x^{\tau-m}\in k'^p$ for $x\in V$, so $x^{\tau_v-m_v}\in k'^p_v$ for any $v\in S_k$. Hence by Hasse's norm theorem and Lemma 3, $x\in N_{K'/k'}(K')$ if and only if $x\in N_{K'_{\mathfrak{q}'}/k'_{\mathfrak{q}'}}(K'_{\mathfrak{q}'})$ for any $\mathfrak{q}'\in T'$. This is equivalent to that $x\in(k'_{\mathfrak{q}'})^p$ for any $\mathfrak{q}'\in T'$, and to that $x\in V(T)$. Hence $V\cap N_{K'/k'}(K'^{\times})=V(T)$. Since $\dim_{F_p}V(T)/(k'^{\times})^p=\dim_{F_p}G(L(T)/k)$, we have the assertion. Q.E.D.

LEMMA 5. *Assume the condition* (i) *in Lemma* 2. *Put* $p^{t^*}=[L_k^*:L_k^*(T)]$. *Then* $\alpha\leqq r_2+1+\delta_k-t^*$, *i.e.*, $\gamma\geqq t^*$.

PROOF. Let K_α be the fixed field by $R^\beta\oplus\boldsymbol{Z}_p^\gamma$ in M_K^*, by the isomorphism of (1). Then $G(K_\alpha/K)\cong\boldsymbol{Z}_p[G]^\alpha$ as a $\boldsymbol{Z}_p[G]$-module. Put $V=\{x\in K'^{\times}\mid\sqrt[p]{x}\in$

$K_\alpha(\zeta)\}$ and $V^*=\{x\in k'^{\times}|\sqrt[p]{x}\in L_k^*(\zeta)\}$. Then $V/(K'^{\times})^p\cong \boldsymbol{F}_p[G]^\alpha$ as a $\boldsymbol{F}_p[G]$-module. By taking $N=1+\sigma+\cdots+\sigma^{p-1}$ of both members, $N_{K'/k'}(V)(K'^{\times})^p/(K'^{\times})^p \cong \boldsymbol{F}_p^\alpha$, so $\dim_{\boldsymbol{F}_p} N_{K'/k'}(V)(K'^{\times})^p/(K'^{\times})^p=\alpha$. On the other hand, since $N_{K'/k'}(V) \subset V^*$, we have

$$\begin{aligned}\dim_{\boldsymbol{F}_p} N_{K'/k'}(V)(K'^{\times})^p/(K'^{\times})^p &\leqq \dim_{\boldsymbol{F}_p} N_{K'/k'}(V)(k'^{\times})^p/(k'^{\times})^p\\ &\leqq \dim_{\boldsymbol{F}_p}(V^*\cap N_{K'/k'}(K'))/(k'^{\times})^p\\ &\leqq \dim_{\boldsymbol{F}_p}(G(L_k^*(T)/k)\\ &\leqq r_2+1+\delta_k-t^*,\end{aligned}$$

by (i) of Lemma 4. Hence $\alpha\leqq r_2+1+\delta_k-t^*$, i.e., $\gamma\geqq t^*$ by Lemma 1.

Q.E.D.

ANOTHER PROOF OF LEMMA 5. We may suppose that $t^*\geqq 1$. Since $G(L_k^*/L_k^*(T))$ is generated by $\{G_\mathfrak{q}|\mathfrak{q}\in T\}$ ($G_\mathfrak{q}$: the decomposition group of $\mathfrak{q}$ for L_k^*/k) and since $|G_\mathfrak{q}|=1$ or p, there exists $T_0\subset T$ such that $G(L_k^*/L_k^*(T))=\prod_{\mathfrak{q}\in T_0} G_\mathfrak{q}$ (direct product). Then $L_k^*(T)=L_k^*(T_0)$ and $|T_0|=t^*$. Take a subfield k' of L_k^* such that $L_k^*=k'L_k^*(T_0)$ and $k'\cap L_k^*(T_0)=k$. Since $\dim_{\boldsymbol{F}_p} G(k'/k)=t^*$ and $k'\subset L_k^*$, there exists a Galois extension k_∞/k such that $G(k_\infty/k)\cong \boldsymbol{Z}_p^{t^*}$ and $k'\subset k_\infty$. Put $K'=k'K$ and $K_\infty=k_\infty K$. Since K/k is fully ramified at T_0, we have $K\cap k_\infty=k$, so $G(K_\infty/K)\cong \boldsymbol{Z}_p^{t^*}$ as a $\boldsymbol{Z}_p[G]$-module. Let $K(T_0)$ be the maximal extension of K in M_K^* which is completely decomposed at T_0', where T_0' is the extension of T_0 to K. Put $G(T_0)=G(M_K^*/K(T_0))$. Then $K(T_0)/k$ is a Galois extension. Since $k'\cap L_k^*(T_0)=k$ and since K/k is fully ramified at T_0, we have $K'\cap K(T_0)=K$, so $K_\infty\cap K(T_0)=K$. Hence

$$\mathrm{rank}_{\boldsymbol{Z}_p} G(T_0)\geqq \mathrm{rank}_{\boldsymbol{Z}_p} G(K_\infty/K)=t^*.$$

On the other hand, since $G(T_0)$ is generated by $\{D_\mathfrak{q}|\mathfrak{q}\in T_0'\}$ ($D_\mathfrak{q}$: the decomposition group of $\mathfrak{q}$ for M_K^*/K) and since $D_\mathfrak{q}$ is a cyclic $\boldsymbol{Z}_p$-module, we have

$$\mathrm{rank}_{\boldsymbol{Z}_p} G(T_0)\leqq |T_0'|=t^*.$$

Hence $\mathrm{rank}_{\boldsymbol{Z}_p} G(T_0)=t^*$ and $M_K^*=K_\infty K(T_0)$, so $X_K^*\cong G(K_\infty/K)\times G(K(T_0)/K)$ as a $\boldsymbol{Z}_p[G]$-module. Hence $\gamma\geqq t^*$. Q.E.D.

THEOREM. *Let K/k be a cyclic extension of degree p and let T be a finite set of finite prime divisors of k such that $S_k\cap T=\emptyset$. Assume the following* (i), (ii) *and* (iii).

(i) $[L_k^*: L_k^*(T)]=p^t$, *where* $t=|T|$.

(ii) $\dim_{\boldsymbol{F}_p} X_k/X_k^p=r_2+1$.

(iii) *K/k is unramified outside $S_k\cup T$ and ramified at any $\mathfrak{q}\in T$.*

Then $X_K^* \cong \boldsymbol{Z}_p[G]^{r_2-t'} \oplus R^{t'} \oplus \boldsymbol{Z}_p^{t'+1}$ *with* $t'=\mathrm{Max}(t-1, 0)$.

PROOF. (I) The case where $t=0$. By Lemma 2, $\beta=0$. Hence by (2)–(3), we obtain $(p-1)\alpha=(p-1)r_2+\delta_K$ and $r_2 \leqq \alpha \leqq r_2+1$. Hence

(6) $$\alpha=r_2, \quad \gamma=1 \quad \text{and} \quad \delta_K=0, \quad \text{or}$$

(7) $$\alpha=r_2+1, \quad \gamma=0 \quad \text{and} \quad \delta_K=p-1.$$

Suppose (7). Then $X_K^* \cong \boldsymbol{Z}_p[G]^{r_2+1}$ by (1). L_K^*/k is a Galois extension and $G(L_K^*/K) \cong \boldsymbol{F}_p[G]^{r_2+1}$. Since $H^2(G, \boldsymbol{F}_p[G]^{r_2+1})=0$, the exact sequence

$$0 \longrightarrow G(L_K^*/K) \longrightarrow G(L_K^*/k) \longrightarrow G \longrightarrow 0$$

is split, so $G(L_K^*/k)=G \ltimes G(L_K^*/K)$ (semi-direct product). Let L'/k be the maximal abelian extension in L_K^*. Then

(*) $$G(L'/k) \cong G \times (\boldsymbol{F}_p[G]/(\sigma-1)\boldsymbol{F}_p[G])^{r_2+1} \cong G \times \boldsymbol{F}_p^{r_2+1}.$$

Since K/k is p-ramified, so is L'/k. Hence (*) contradicts the condition (ii). Thus we obtain (6), and $X_K^* \cong \boldsymbol{Z}_p[G]^{r_2} \oplus \boldsymbol{Z}_p$ by (1).

(II) The case where $t \geqq 1$. By (2)–(3), we obtain $(p-1)(\alpha+\beta-r_2)=\delta_K$, so $\alpha+\beta \geqq r_2$. On the other hand, by Lemmas 2 and 5, $\alpha+\beta \leqq r_2$. Hence $\alpha+\beta=r_2$, $\delta_K=0$ and $\alpha=r_2+1-t$, $\beta=t-1$ and $\gamma=t$. Q.E.D.

COROLLARY (a special case of [7, Corollary to Theorem 2]). *Under the same notation and assumptions in Theorem, the Leopoldt conjecture is valid for* (K, p).

References

[1] C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Interscience, New York, 1962.

[2] K. Iwasawa, On $\boldsymbol{Z}_l$-extensions of algebraic number fields, Ann. of Math., **98** (1973), 246-326.

[3] T. Kubota, Galois group of the maximal abelian extension over an algebraic number field, Nagoya Math. J., **12** (1957), 177-189.

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

[5] H. Miki, On the maximal abelian l-extension of a finite algebraic number field with given ramification, Proc. Pre-conference of Intern. Symp. on Algebraic Number Theory, December 1975 Kyoto.

[6] ———, ————, Nagoya Math. J., **70** (1978), 183-202 (this is the details of [5]).

[7] ———, On the Leopoldt conjecture on the p-adic regulators, preprint.

[8] I. R. Šafarevič, Extensions with given points of ramification, I. H. E. S. Publ. Math., **18** (1963), 71-95 (=A. M. S. Transl. Ser. 2, **59** (1966), 128-149).

Hiroo MIKI
Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Setagaya-ku, Tokyo 158
Japan

Hirotaka SATO
Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Setagaya-ku, Tokyo 158
Japan