Canad. Math. Bull. Vol. **31** (3), 1988

KUMMER'S AND IWASAWA'S VERSION OF LEOPOLDT'S CONJECTURE

BY

JONATHAN W. SANDS

ABSTRACT. We present a refinement of Iwasawa's approach to Leopoldt's conjecture on the non-vanishing of the p-adic regulator of an algebraic number field K. As an application, the conjecture for K implies the conjecture for a solvable extension L of degree g over K if g is relatively prime to $p - 1$ and p does not divide g, the discriminant of K, and the quotient of class numbers $h(L(\zeta_p))/h(K(\zeta_p))$, where ζ_p is a primitive pth root of unity. This can be viewed as generalizing a theorem of Kummer on cyclotomic units.

1. **Introduction.** In 1847, Kummer rather precociously proved Leopoldt's conjecture for the field $K = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$ and the regular prime p ($\zeta_p = e^{2\pi i/p}$). In fact, Kummer's theorem that a unit of K congruent to a rational integer (mod p) is a pth power anticipated an especially simple statement of the conjecture (cf. 2.2). Using this statement and basic class field theory, Iwasawa [10] developed a new approach to Leopoldt's conjecture which does not seem to be well known. Here we present a refinement and an application of this approach, seeking to show the insight available from classical notions.

Our application concerns the question of "going up": if Leopoldt's conjecture holds for a fixed prime p and field K (e.g. K absolutely abelian and p arbitrary [4]), does it hold for a cyclic extension $\mathscr{K}$ of K? Miki and Sato [12], [13] have studied this situation when $[\mathscr{K}:K] = p$; we restrict attention to the case of $[\mathscr{K}:K]$ prime to p. Primarily, our result says that Leopoldt's conjecture holds for $\mathscr{K}$ and $p \neq 2$ if the p-part of the class number is the same for $\mathscr{K}(\zeta_p)$ as for $K(\zeta_p)$, and (e.g.) p is unramified in $\mathscr{K}$. It should be remarked that another proof of this result arises from work of Gras [8] concerning the maximal abelian p-ramified pro-p-extension of K.

In studying the connection between Leopoldt's conjecture and class numbers, we take the opportunity to note a direct proof of a motivating result (3.1) which has appeared in various forms before [2], [3], [6], [7]. An appendix supplies proofs of "well-known" results for which there seems to be no adequate reference.

Received by the editors February 18, 1987, and, in revised form, July 7, 1987.

Research supported in part by NSF grant MCS-8108814.

AMS Subject Classification (1980): 11R27.

https://doi.org/10.4153/CMB-1988-049-0 Published online by Cambridge University Press

I am indebted to my colleagues Warren Sinnott, Bob Gold, and Karl Rubin at Ohio State for ideas on these matters, but especially to K. Iwasawa for considerable direction during my stay in Princeton. The hospitality of the Institute for Advanced Study and funding from the National Science Foundation are most appreciated for making this stay possible.

2. **Kummer's version of Leopoldt's conjecture.** Let K be a fixed algebraic number field and E_K be its group of units. We fix a prime number p and for each positive integer m we let $E_K(p^m)$ be the group of units of K which are congruent to 1 (mod p^m). Leopoldt's conjecture may be stated as follows.

2.1 CONJECTURE. LC(K, p). *Given any positive integer a, there exists a positive integer m such that* $E_K(p^m) \subset E_K^{p^a}$.

In A.3 of the appendix, 2.1 is shown to be equivalent to a perhaps more familiar statement of Leopoldt's conjecture.

Henceforth we take p to be an *odd* prime. Now let ζ_p be a pth root of unity and $K_0 = K(\zeta_p)$. The next two propositions originate from Iwasawa [10].

2.2 PROPOSITION. *Assume that no divisor of p splits completely in* K_0/K. *Then* LC(K, p) *holds if and only if* $E_K(p^m) \subset E_K^p$ *for some positive integer m.*

PROOF. The "only if" statement follows directly from 2.1.

Assume then that m is fixed so that $E_K(p^m) \subset E_K^p$. Given a positive integer a, we show that $E_K(p^{mp^a}) \subset E_K^{p^a}$. So suppose $\epsilon \in E_K(p^{mp^a})$. First $\epsilon \in E_K(p^m) \subset E_K^p$, so that $\epsilon = \eta^p$ in E_K. Let ν be a normalized valuation of K_0 with $\nu(p) = 1$. Then $\nu(1 - \eta^p) = \nu(1 - \epsilon) \geqq mp^a$. Factoring $1 - \eta^p = \prod_{i=0}^{p-1} (1 - \zeta_p^i\eta)$, we see that $\nu(1 - \zeta\eta) \geqq mp^{a-1}$ for some $\zeta = \zeta_p^i$. By assumption, there exists an element σ of the Galois group Gal(K_0/K) such that σ fixes ν and has order $d \neq 1$. Then $\nu(1 - \zeta^{\sigma^i}\eta) \geqq mp^{a-1}$ for each i. The sum

$$(1 - \zeta\eta) + \zeta\eta(1 - \zeta^\sigma\eta) + \zeta^{1+\sigma}\eta^2(1 - \zeta^{\sigma^2}\eta) + \dots$$
$$+ \zeta^{1+\sigma+\dots+\sigma^{d-2}}\eta^{d-1}(1 - \zeta^{\sigma^{d-1}}\eta)$$

telescopes to $1 - \zeta^{1+\sigma+\dots+\sigma^{d-1}}\eta^d$. But $\zeta^{1+\sigma+\dots+\sigma^{d-1}}$ is a pth root of unity in an extension of K strictly smaller than $K(\zeta_p)$, hence it must be 1. Each parenthesized term in the sum has valuation $\geqq mp^{a-1}$, so $\nu(1 - \eta^d) \geqq mp^{a-1}$.

Now $1 - \eta^d = \prod(1 - \zeta_d^i\eta)$ and $1 - \zeta_d^i\eta = (1 - \eta) + \eta(1 - \zeta_d^i)$, with $\nu(1 - \eta) > 0$, $\nu(\eta) = 0$, and $\nu(1 - \zeta_d^i) = 0$ unless $\zeta_d^i = 1$, since $d | p - 1$. Hence $\nu(1 - \zeta_d^i\eta) = 0$ for $\zeta_d^i \neq 1$, and from $\nu(1 - \eta^d) \geqq mp^{a-1}$ we see that $\nu(1 - \eta) \geqq mp^{a-1}$. This holds for each ν with $\nu(p) = 1$, therefore $\eta \in E_K(p^{mp^{a-1}})$. Hence $\epsilon \in E_K(p^{mp^{a-1}})^p$, or $E_K(p^{mp^a}) \subset E_K(p^{mp^{a-1}})^p$. By iteration, $E_K(p^{mp^a}) \subset E_K(p^m)^{p^a} \subset E_K^{p^a}$.

We call 2.2 "Kummer's version of Leopoldt's conjecture," because the assumption holds when $K = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$, for which Kummer proved that $E_K(p) \subset E_K^p$ when p is a regular prime; thus Leopoldt's conjecture holds in this case.

The assumption in 2.2 has appeared often enough in the literature [7], [12]. Note that it is satisfied if $2 \neq p \nmid d_K$, the discriminant of K, or, more generally, if (as in [7]) $p - 1$ does not divide the ramification index of p in $K/\mathbf{Q}$. Our next proposition involves a similarly familiar simplifying assumption.

2.3 Proposition. *Assume $K = K_0$ and only one prime of K divides p. Then* LC(K, p) *holds if and only if $E_K(p^m) \subset E_K^p$ for some positive integer m.*

Proof. The "only if" statement follows directly from 2.1.

Assume that m is fixed so that $E_K(p^m) \subset E_K^p$. Given a positive integer a, we again show that $E_K(p^{mp^a}) \subset E_K^{p^a}$. Suppose then that $\epsilon \in E_K(p^{mp^a})$. Then $\epsilon \in E_K(p^m) \subset E_K^p$, *and* $\epsilon = \eta^p$, $\eta \in E_K$. Let ν be a valuation of K such that $\nu(p) = 1$. From $\nu(1 - \epsilon) \geqq mp^a$, $1 - \epsilon = \prod_{i=0}^{p-1} (1 - \zeta_p^i\eta)$, we see that $\nu(1 - \zeta_p^i\eta) \geqq mp^{a-1}$ for some i. Replace η by $\zeta_p^i\eta$ to have $\nu(1 - \eta) \geqq mp^{a-1}$, or $\eta \in E_K(p^{mp^{a-1}})$. Thus $E_K(p^{mp^a}) \subset E_K(p^{mp^{a-1}})$, and the proof concludes as in 2.2.

3. **The connection with class groups.** Let $S = S(K_0)$ be the set of primes of K_0 dividing p, and let $C_{K_0,S}$ be the "S-ideal class group" of K_0, i.e., the quotient of the ideal class group C_{K_0} by the subgroup generated by those ideal classes containing elements of S. We define $h_{K_0,S}$, the S-class number, to be the order of $C_{K_0,S}$. Clearly $h_{K_0,S}$ divides the class number h_{K_0}. Finally put ${}_pC_{K_0,S} = C_{K_0,S}/C_{K_0,S}^p$. Via class field theory, $C_{K_0,S}$ corresponds to the maximal abelian unramified extension of K_0 in which all primes in S split completely, and ${}_pC_{K_0,S}$ corresponds to the maximal such elementary p-extension.

There is a natural action of $\Delta = \mathrm{Gal}(K_0/K)$ on the modified class groups we have just defined. On the isomorphic Galois groups (Artin isomorphism of class field theory), the compatible action is induced by conjugation. Since ${}_pC_{K_0,S}$ is an abelian p-group, it is a $\mathbf{Z}_p$-module, where $\mathbf{Z}_p$ denotes the p-adic integers. Further, it is then a $\mathbf{Z}_p[\Delta]$-module and hence decomposes via the idempotents of $\mathbf{Z}_p[\Delta]$, which we now describe.

Let $\omega:\Delta \to \mathbf{Z}_p^\times$ be the character such that $\zeta_p^\sigma = \zeta_p^{\omega(\sigma)}$ for each $\sigma \in \Delta$. If the order of Δ is $d = |\Delta|$, then an orthogonal system of idempotents of $\mathbf{Z}_p[\Delta]$ is

$$\left\{\epsilon_i = \frac{1}{d} \sum_{\sigma \in \Delta} \omega^i(\sigma)\sigma^{-1} : i = 1, \ldots, d\right\}.$$

ϵ_i has the property that $\sigma\epsilon_i = \omega^i(\sigma)\epsilon_i$ for each σ in Δ.

It is interesting to discover how classical a proof one can give for the following proposition, cases of which are found in [2], [3], [6], [7]. The full proposition is also a corollary of [8, Théorème I.2].

https://doi.org/10.4153/CMB-1988-049-0 Published online by Cambridge University Press

3.1 PROPOSITION. *Assume that no prime dividing p splits completely in K_0/K or that $K_0 = K$ and only one prime of K divides p. If $\epsilon_1({}_pC_{K_0,S})$ is trivial, then* LC(K, p) *holds.*

PROOF. Hecke [9, p. 136] shows that if $\epsilon \in E_K(p^3)$, then in $K_0(\epsilon^{1/p})/K_0$, every divisor of p splits completely. The extension is abelian and no other finite primes ramify, by Kummer theory. No infinite primes ramify because p is odd. By class field theory, $K_0(\epsilon^{1/p})$ corresponds to a quotient of ${}_pC_{K_0,S}$. Since $\epsilon \in K$, one in fact finds that $K_0(\epsilon^{1/p})$ corresponds to a quotient of $\epsilon_1({}_pC_{K_0,S})$. This last group is trivial by assumption, so we have $\epsilon \in E_{K_0}^p$. As the degree $[K_0{:}K]$ is prime to p, taking the norm to K shows that $\epsilon \in E_K^p$. Now ϵ is arbitrary, so $E_K(p^3) \subset E_K^p$, and the proof concludes with an application of 2.2 or 2.3.

4. **Iwasawa's version of Leopoldt's conjecture.** This section refines ideas of Iwasawa in [10]. With p and K as before, let $\mathbf{q}$ be a prime ideal of the ring of integers $\mathcal{O}_K$ of K, $\mathbf{q}$ not containing p. First we motivate the key concept of a $\mathbf{q}$-field for K and p.

4.1 LEMMA. *Let L be a finite abelian extension of K, and I be the inertia group of $\mathbf{q}$ for L/K. If I_p is the p-Sylow subgroup of I, then I_p is isomorphic to a subgroup of $(\mathcal{O}_K/\mathbf{q})^\times$, hence is cyclic of order dividing* $\mathbf{Nq} - 1$.

PROOF. [11, p. 94] or [15, p. 67].

Let $e(\mathbf{q}, L/K)$ denote the ramification index of $\mathbf{q}$ in L/K. If N is an integer, we will write N_p for the highest power of p dividing N. So $e(\mathbf{q}, L/K)_p = |I_p|$, and we put $e(\mathbf{q}) = (\mathbf{Nq} - 1)_p$, $e(\mathbf{q})d(\mathbf{q}) = \mathbf{Nq} - 1$.

4.2 COROLLARY. *For any finite abelian extension L of K, $e(\mathbf{q}, L/K)$ divides $e(\mathbf{q})$.*

4.3 DEFINITION. *A number field L is called a weak $\mathbf{q}$-field for K (and p) if it satisfies these two conditions*:

(a) *L is a finite abelian extension of K, unramified at each infinite prime and each finite prime other than $\mathbf{q}$ and the divisors of p.*

(b) *$e(\mathbf{q}, L/K)_p > 1$ if $e(\mathbf{q}) > 1$.*

(*L is called a $\mathbf{q}$-field for K if L is a weak $\mathbf{q}$-field and $e(\mathbf{q}, L/K) = e(\mathbf{q})$.*)

Let $K_\mathbf{q}$ be the completion of K at $\mathbf{q}$, and $U_\mathbf{q}$ be the group of units of $K_\mathbf{q}$.

4.4 LEMMA (Iwasawa). *A weak $\mathbf{q}$-field exists for K if and only if $E_K(p^m) \subset U_\mathbf{q}^p$ for some positive integer m.*

PROOF. Note that if $p \nmid (\mathbf{Nq} - 1)$, then the pth power map is an isomorphism on $(\mathcal{O}_K/\mathbf{q})^\times$, and $x^p - \epsilon$ has a root (mod $\mathbf{q}$) for each ϵ in E_K. So $E_K \subset U_\mathbf{q}^p$ by Hensel's lemma, and our lemma holds. We now assume that $p \mid (\mathbf{Nq} - 1)$.

For non-negative integers m and n, let $K_{m,n}$ be the ray class field of K (mod

https://doi.org/10.4153/CMB-1988-049-0 Published online by Cambridge University Press

$p^m\mathbf{q}^n$). If L is a weak $\mathbf{q}$-field, then $L \subset K_{m,n}$ for some m and n. But $p \nmid [K_{m,n}:K_{m,1}]$ since $p \nmid \mathbf{Nq}$, and we may assume $L \subset K_{m,1}$. In fact, $K_{m,1}$ is then a weak $\mathbf{q}$-field and we will use $L = K_{m,1}$. Then $e(\mathbf{q}, L/K)_p = e(\mathbf{q}, K_{m,1}/K)_p = [K_{m,1}:K_{m,0}]_p$. Clearly $K_{m,1}$ is a weak $\mathbf{q}$-field if and only if $p \mid [K_{m,1}:K_{m,0}]_p$.

Fix m and let $A = \{\alpha \in K^\times: \alpha \text{ is prime to } p\mathbf{q} \text{ and } \alpha \equiv 1 \bmod^\times p^m\}$ and $B = \{\alpha \in A: \alpha \equiv 1 \bmod^\times \mathbf{q}\}$, while (A) and (B) denote the groups of ideals they generate. Then by class field theory, $\mathrm{Gal}(K_{m,1}/K_{m,0}) \cong (A)/(B) \cong A/B \cdot (A \cap E_K) = A/B \cdot E_K(p^m)$. So it suffices to consider whether p divides the order $|A/B \cdot E_K(p^m)|$. Now $A/B \cong (\mathcal{O}_K/\mathbf{q})^\times$ is cyclic of order divisible by p, hence $A^p \cdot B/B$ is the maximal subgroup of index divisible by p. We see that p divides $|A/B \cdot E_K(p^m)|$ if and only if $E_K(p^m) \subset A^p \cdot B$.

The lemma will be established once we show that $E_K(p^m) \subset A^p \cdot B$ if and only if $E_K(p^m) \subset U_\mathbf{q}^p$. First, $B \subset U_\mathbf{q}^p$ by Hensel's lemma, so that $A^p \cdot B \subset U_\mathbf{q}^p$, and one implication is clear. Suppose then that $E_K(p^m) \subset U_\mathbf{q}^p$, and $\epsilon \in E_K(p^m)$. Then $\epsilon = u^p$ for some $u \in U_\mathbf{q}$, and we choose $a \in A$ such that $a \equiv u \pmod{\mathbf{q}}$. Then $\epsilon/a^p \equiv 1 \bmod^\times p^m\mathbf{q}$, so $\epsilon/a^p \in B$ and $\epsilon \in A^p \cdot B$; therefore $E_K(p^m) \subset A^p \cdot B$.

4.5 Remark. Similarly, one can prove that a $\mathbf{q}$-field exists for K if and only if $E_K(p^m)^{d(\mathbf{q})} \subset E_K(\mathbf{q})$ for some positive integer m.

Let $D = D_K = \{u \in E_K\text{: each prime of } S \text{ splits completely in } K_0(u^{1/p})/K_0\}$. Then D is a subgroup of E_K, $D \supset E_K^p$.

4.6 Theorem. *Suppose that for each u in D, there exists a prime ideal $\mathbf{q}_0$ of K_0 satisfying two conditions*:

(a) *$\mathbf{q}_0$ is inert in $K_0(u^{1/p})$*

(b) *a weak $\mathbf{q}$-field exists for K, where $\mathbf{q} = \mathbf{q}_0 \cap K$.*

Then $E_K(p^m) \subset E_K^p$ for some positive integer m. Conversely, if $E_K(p^m) \subset E_K^p$ for some m, then a weak $\mathbf{q}$-field exists for each prime ideal $\mathbf{q}$ of K.

Proof (After Iwasawa [10], Chevalley [5]). Let $\{u_i: i = 1, \ldots, r\}$ be a full set of representatives for the finite group D/E_K^p. Then for each i, let $\mathbf{q}_0^{(i)}$ satisfy (a) and (b). By 4.4, $E_K(p^m) \subset U_{\mathbf{q}^{(i)}}^p$ for some $m \geqq 1$. We may clearly assume that the same m applies for each i, and that $m \geqq 3$. If $\epsilon \in E_K(p^m)$, then each prime of S splits completely in $K_0(\epsilon^{1/p})/K_0$ [9, p. 136]. Hence $\epsilon \in D$, and $K_0(\epsilon^{1/p})$ must be one of the $K_0(u_i^{1/p})$. However, $\epsilon \in E_K(p^m) \subset U_{\mathbf{q}^{(i)}}^p$. Consequently, each $\mathbf{q}_0^{(i)}$ splits completely in $K_0(\epsilon^{1/p})$ while $\mathbf{q}_0^{(i)}$ remains inert in $K_0(u_i^{1/p})$. We conclude that $K_0(\epsilon^{1/p}) = K_0$, so $\epsilon \in E_{K_0}^p$. Taking the norm to K shows that $\epsilon^{p-1} \in E_K^p$, and thus $\epsilon \in E_K^p$. For the converse, simply note that $E_K^p \subset U_\mathbf{q}^p$ for each $\mathbf{q}$. Lemma 4.4 completes the proof.

4.7 Remark. Similarly [10], one can prove that $\mathrm{LC}(K, p)$ holds if and only if a $\mathbf{q}$-field exists for each $\mathbf{q}$ of K.

https://doi.org/10.4153/CMB-1988-049-0 Published online by Cambridge University Press

4.8 THEOREM. *Suppose* LC(K, p) *holds. Let* $\mathscr{K}$ *be a cyclic Galois extension of* K *with* $\mathscr{K} \cap K_0 = K$ *and* $[\mathscr{K}:K] = g$ *prime to* p. *Assume that no prime dividing* p *splits completely in* $\mathscr{K}_0/\mathscr{K}$, *or that* $\mathscr{K}_0 = \mathscr{K}$ *and only one prime of* $\mathscr{K}$ *divides* p. *Identify* $\mathrm{Gal}(\mathscr{K}_0/\mathscr{K})$ *with* $\mathrm{Gal}(K_0/K) = \Delta$, *and let* $\mathscr{S}$ *be the set of primes of* $\mathscr{K}_0$ *dividing* p. *If* $\epsilon_1({}_pC_{K_0,S}) \cong \epsilon_1({}_pC_{\mathscr{K}_0,\mathscr{S}})$, *then* LC($K$, p) *holds.*

4.9 REMARK. Since $(g, p) = 1$, we always have for any $j \in \mathbf{Z}$ that $\epsilon_j({}_pC_{K_0,S})$ is isomorphic to a subgroup of $\epsilon_j({}_pC_{\mathscr{K}_0,\mathscr{S}})$ via extension of ideals. Likewise ${}_pC_{K_0} \subset {}_pC_{\mathscr{K}_0}$.

4.10 REMARK. $p^j \mid (\epsilon_1({}_pC_{\mathscr{K}_0,\mathscr{S}}):\epsilon_1({}_pC_{K_0,S}))$ for $j = 1 \Leftrightarrow$ for $j =$ order of $p \pmod g$ (cf. [14, Ch. IV]).

PROOF OF 4.8. Let u in $D_{\mathscr{K}}$ represent an arbitrary nontrivial element of $D_{\mathscr{K}}/E_{\mathscr{K}}^p$. We will find a prime ideal $\mathscr{Q}_0$ of $\mathscr{K}_0$ satisfying (a) and (b) of 4.6.

By class field theory, our assumption on class groups implies that every unramified, cyclic, degree p extension of $\mathscr{K}_0$ in which $\mathscr{S}$ splits completely and Δ acts via ω arises by composition from such an extension of K_0. $\mathscr{K}_0(u^{1/p})$ fits this description, so $\mathscr{K}_0(u^{1/p}) = \mathscr{K}_0 \cdot M$, with M/K_0 cyclic of degree p. Also $\mathrm{Gal}(\mathscr{K}_0/K_0) \cong \mathrm{Gal}(\mathscr{K}/K)$ is cyclic of degree g, since $\mathscr{K} \cap K_0 = K$. Hence $\mathscr{K}_0(u^{1/p})/K_0$ is cyclic of degree pg, as $(p, g) = 1$. Thus (Tchebotarev density) we can choose a *first degree* prime $\mathbf{q}_0$ of K_0 which is inert in $\mathscr{K}_0(u^{1/p})$. Then $\mathscr{Q}_0 = \mathbf{q}_0\mathscr{O}_{\mathscr{K}_0}$ is inert in $\mathscr{K}_0(u^{1/p})$, so (a) of 4.6 is satisfied.

Putting $\mathscr{Q} = \mathscr{Q}_0 \cap \mathscr{K}$ and $\mathbf{q} = \mathbf{q}_0 \cap K$, we know that $\mathbf{q}_0$ has residue degree 1 over $\mathbf{q}$, since it is a first degree prime. As $\mathscr{Q}_0$ over $\mathbf{q}_0$ has residue degree g, it is an easy exercise in decomposition groups to discover that $\mathscr{Q}$ over $\mathbf{q}$ has residue degree g, or $\mathbf{q}\mathscr{O}_{\mathscr{K}} = \mathscr{Q}$. By the assumption of LC(K, p) and by 4.6 (converse part), a weak $\mathbf{q}$-field L exists for K and p. But then $L \cdot \mathscr{K}$ becomes a weak $\mathbf{q}\mathscr{O}_{\mathscr{K}} = \mathscr{Q}$-field for $\mathscr{K}$ and p, so (b) of 4.6 is satisfied. Since $u \in D_{\mathscr{K}}$ was arbitrary, this all implies that $E_{\mathscr{K}}(p^m) \subset E_{\mathscr{K}}^p$, for some m, and LC($\mathscr{K}$, p) holds by 2.2 and 2.3.

4.11 COROLLARY. *Suppose* p *is odd and* LC(K, p) *holds. Let* $\mathscr{K}/K$ *be a Galois extension of degree* g *with* $(g, p - 1) = 1$ *and* $\mathrm{Gal}(\mathscr{K}/K)$ *solvable. If* p *does not divide* (*the numerator of*) $(d_K)(g)(h_{\mathscr{K}_0,\mathscr{S}}/h_{K_0,S})$, *then* LC($\mathscr{K}$, p) *holds.*

PROOF. Since p is unramified in K and totally ramified in $\mathbf{Q}_0$, all primes in S ramify totally in K_0/K, and $[K_0:K] = p - 1$.

Let $K = M^{(1)}, \ldots, M^{(n)} = \mathscr{K}$ be a sequence of fields such that $M^{(i+1)}/M^{(i)}$ is a cyclic extension for each i. Put $S^{(i)}$ equal to the set of primes in $M^{(i)}$ which divide p. As $(g, p - 1) = 1$, $M^{(i+1)} \cap M_0^{(i)} = M^{(i)}$ for each i, and all primes in $S^{(i)}$ ramify (totally) in $M_0^{(i+1)}/M^{(i+1)}$. From 4.9 and the assumption,

https://doi.org/10.4153/CMB-1988-049-0 Published online by Cambridge University Press

${}_pC_{K_0,S} \cong {}_pC_{\mathscr{K}_0,\mathscr{S}}$ and ${}_pC_{M_0^{(i)},S^{(i)}} \cong {}_pC_{M_0^{(i+1)},S^{(i+1)}}$. The conclusion follows by application of 4.8 to $M^{(i+1)}/M^{(i)}$; $i = 1, \ldots, n-1$.

As an application, we note a relation with a conjecture in Iwasawa theory.

Fix a prime number l and let $K_0^{(\infty)}$ denote the cyclotomic $\mathbf{Z}_l$-extension of the number field K_0, with $K_0^{(n)}$ denoting the nth layer (cf. [18, Chapter 13], for definitions). For $p \neq l$, Washington conjectured [16] (and proved for K absolutely abelian [17]) that there exists an integer $N > 0$ such that $p \nmid (h_{K_0^{(n)}}/h_{K_0^{(N)}})$ whenever $n \geqq N$. Of course this implies that $p \nmid (h_{K_0^{(n)},S^{(n)}}/h_{K_0^{(N)},S^{(N)}})$ by 4.9.

4.12 Corollary. *Suppose* $p \not\equiv 1 \pmod{l}$, $p \nmid 2d_K l$, *and the conjecture of Washington holds for* K_0 *and* p. *Then either* $\mathrm{LC}(K^{(n)}, p)$ *is true for all* $n \geqq 0$ *or it is false for all* $n \geqq N$.

Proof. If $\mathrm{LC}(K^{(N)}, p)$ is true, we apply 4.11 and A.4. If $\mathrm{LC}(K^{(N)}, p)$ is false, we apply the contrapositive of A.4.

Appendix. Allow p to be 2, and in that case put $q = 4$, otherwise $q = p$. Then $E_K(q)$ is torsion free of $\mathbf{Z}$-rank $r = r_K$. We prove (A.3) that the statement 2.1 of Leopoldt's conjecture is equivalent to the maximality of the (free) $\mathbf{Z}_p$-rank of $\overline{E_K(q)}$, the closure of $E_K(q)$ embedded diagonally in the product of completions of K at primes dividing p (cf. [18]). The method leads to a simple proof (A.4) of the fundamental "going down" theorem for Leopoldt's conjecture.

By the rank, $\mathrm{rank}_R\, M$, of a finitely generated module M over an integral domain R, we mean the rank of the free module obtained as the quotient of the original modulo torsion. All other notation is that set out in section II.

A.1 Lemma. *Given a positive integer* c, *there exists a positive integer* a *such that*

$$E_K(q) \cap E_K^{p^a} \subset E_K(q)^{p^c}.$$

Proof. By the Artin-Rees lemma [1, Chapter 10], there exists $A \geqq 0$ such that

$$E_K(q) \cap E_K^{p^{A+c}} = (E_K(q) \cap E_K^{p^A})^{p^c}$$

for all positive c. Given c, put $a = A + c$.

A.2 Lemma. $\mathrm{LC}(K, p)$ *holds* $\Leftrightarrow$ *for each positive integer* c *there exists a positive integer* m *such that*

$$E_K(p^m) \subset E_K(q)^{p^c}.$$

Proof. ($\Leftarrow$) Clear.

($\Rightarrow$) Given c, choose a as in A.1. Then (taking $m \geqq 2$ when $p = 2$)

https://doi.org/10.4153/CMB-1988-049-0 Published online by Cambridge University Press

$$E_K(p^m) \subset E_K^{p^a} \Rightarrow E_K(p^m) \subset E_K(q) \cap E_K^{p^a} \subset E_K(q)^{p^c}.$$

A.3 PROPOSITION. LC(K, p) *holds* $\Leftrightarrow \operatorname{rank}_{\mathbf{Z}_p} \overline{E_K(q)} = \operatorname{rank}_{\mathbf{Z}} E_K(q) = r$.

PROOF. Since $\mathbf{Z}$ is a Noetherian ring, E_K is a finitely generated module, and $\mathbf{Z}_p$ is compact, it is straightforward [1, Chapter 10] to check that one has a commutative diagram of commutative pro-p-groups (all maps are continuous homomorphisms) and hence of $\mathbf{Z}_p$ modules:

$$\begin{tikzcd}
\mathbf{Z}_p \otimes_{\mathbf{Z}} E_K(q) \arrow[r, "\simeq"] \arrow[d, "\alpha"'] & \varprojlim_n E_K(q)/E_K(q)^{p^n} \arrow[d, "\beta"] \\
\overline{E_K(q)} \arrow[r, "\simeq"] & \varprojlim_n E_K(q)/E_K(p^{n+1})
\end{tikzcd}$$

The vertical maps α and β are surjective.

Since $\operatorname{rank}_{\mathbf{Z}_p} \mathbf{Z}_p \otimes_{\mathbf{Z}} E_K(q) = r$, we have $\operatorname{rank}_{\mathbf{Z}_p} \overline{E_K(q)} = r \Leftrightarrow \alpha$ is a topological isomorphism $\Leftrightarrow \beta$ is a topological isomorphism $\Leftrightarrow \{E_K(q)^{p^n} : n = 1, 2, \ldots\}$ and $\{E_K(p^{n+1}) : n = 1, 2, \ldots\}$ define the same topology on $E_K(q) \Leftrightarrow$ for each positive integer c, there exists a positive integer m such that $E_K(p^m) \subset E_K(q)^{p^c}$. (Given m, $c = m - 1$ always provides the reverse inclusion.)

A.4 COROLLARY. *If F is a subfield of K, then* LC(K, p) $\Rightarrow$ LC(F, p).

PROOF. We have the commutative diagram [1, Chapter 10]

$$\begin{tikzcd}
\mathbf{Z}_p \otimes_{\mathbf{Z}} E_F(q) \arrow[r] \arrow[d, "\gamma"'] & \mathbf{Z}_p \otimes_{\mathbf{Z}} E_K(q) \arrow[d, "\alpha"] \\
\overline{E_F(q)} \arrow[r] & \overline{E_K(q)}
\end{tikzcd}$$

where the horizontal maps are injective. Then by the proof of A.3, LC(K, p) $\Leftrightarrow$ α is injective $\Rightarrow \gamma$ is injective $\Leftrightarrow$ LC(F, p)

A.5 REMARK. A similar proof shows that LC(K^+, p) $\Rightarrow$ LC(K, p) when K is a CM-field.

REFERENCES

1. M. F. Atiyah and I. G. McDonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Mass. 1969.

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

3. F. Bertrandias and J. J. Payan, *Γ-extensions et invariants cyclotomiques*, Ann. Scient. Ec. Norm. Sup. 4ᵉ ser. **5** (1972), pp. 517-543.

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

5. C. Chevalley, *Deux théorèmes d'arithmetique*, J. Math. Soc. Japan **31** (1951), pp. 36-44.

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

7. G. Gras, *Remarques sur la conjecture de Leopoldt*, C.R. Acad. Sc. Paris (A) **274** (1972), pp. 377-380.

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

9. E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer-Verlag, New York, 1981.

10. K. Iwasawa, *A simple remark on Leopoldt's conjecture*, (in Japanese), R.I.M.S. Kyoto U. (1984), pp. 45-54.

11. R. Long, *Algebraic Number Theory*, Marcel Dekker, New York, 1977.

12. H. Miki and H. Sato, *Leopoldt's conjecture and Reiner's theorem*, J. Math. Soc. Japan **361** (1984), pp. 47-51.

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

14. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, P.W.N. Polish Scientific Publishers, Warsaw, 1973.

15. J. P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.

16. L. Washington, *Class numbers and* $\mathbf{Z}_p$*-extensions*, Math. Ann. **214** (1975), pp. 177-193.

17. ———, *The non-p-part of the class number in a cyclotomic* $\mathbf{Z}_p$*-extension*, Inv. Math. **49** (1979), pp. 87-97.

18. ———, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1982.

UNIVERSITY OF VERMONT
BURLINGTON, VT 05405