PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 104, Number 1, September 1988

LEOPOLDT'S CONJECTURE IN PARAMETERIZED FAMILIES

JOHANNES BUCHMANN AND JONATHAN W. SANDS

(Communicated by Larry J. Goldstein)

ABSTRACT. For each fixed prime $p \neq 5$, we prove Leopoldt's conjecture in two infinite families of fields of degree five whose normal closure has Galois group over the rationals isomorphic to S_5. The units of these fields were determined by Maus [**4**]; we develop and apply a simple reformulation of Leopoldt's conjecture to obtain the result. We also observe that Leopoldt's conjecture in one field can imply the same in a second field related by congruence conditions.

I. Introduction. Let K be an algebraic number field with ring of integers $\mathcal{O}_K$ and unit group E_K. If $\mathfrak{I}$ is an ideal of $\mathcal{O}_K$, we let $E_K(\mathfrak{I})$ be the group of units which are congruent to 1 modulo $\mathfrak{I}$. When $\mathfrak{I} = (\alpha)$ is principal, we also write this as $E_K(\alpha)$. A simple statement of Leopoldt's conjecture [**2**] for K and a rational prime p is that there exists an integer m such that $E_K(p^m) \subset E_K(p^2)^p$. We denote this conjecture by $\mathrm{LC}(K,p)$, and further reformulate it in §II. A fundamental result of Brumer [**1**] states that $\mathrm{LC}(K,p)$ holds for all primes p when K lies in an abelian extension of an imaginary quadratic field.

Strong interest in Leopoldt's conjecture derives from its connections with Iwasawa theory [**3**], p-adic L-functions [**6**], and Galois cohomology [**5**]. Thus it is desirable to have many examples of fields where the conjecture is known to hold. Our approach in this note is elementary.

In §III we explicitly describe two families of fifth degree fields for each prime $p \neq 5$, and prove $\mathrm{LC}(K,p)$ for each K in either of these families. This result is made possible by the work of Maus [**4**], who determined maximal systems of independent units in these fields. A general principle suggests itself in the proof: $\mathrm{LC}(K,p)$ is equivalent to $\mathrm{LC}(L,p)$ when $\mathcal{O}_L$ and $\mathcal{O}_K$ are isomorphic modulo some power p^k of p and have unit groups sufficiently similar modulo p^k. In this way, Leopoldt's conjecture for one field can imply the conjecture for infinitely many fields. We make this precise in §IV, and give another application to the fields of Maus. Finally, §V completes our discussion by proving that the specific families of fields we have considered are in fact infinite. Thus we have Leopoldt's conjecture in infinitely many new fields of degree five, for any fixed prime. The interesting problem of proving Leopoldt's conjecture for a particular one of these fields and infinitely many primes still remains.

We thank Avner Ash for suggesting this collaboration, and the Alexander von Humboldt foundation and the Ohio State University Department of Mathematics

Received by the editors March 2, 1987 and, in revised form, August 31, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R27; Secondary 11R21.
Supported by a Feodor Lynen research fellowship of the Alexander von Humboldt foundation and the Ohio State University.

0002-9939/88 $1.00 + $.25 per page

for making it possible. We also thank M. Ram Murty for his major contribution to the proof of (5.1).

II. Reformulations of Leopoldt's conjecture. Fix K and a rational prime p, and put $q = p$ if p is odd, $q = 4$ if $p = 2$. As $E_K(q)$ is torsion free and finite index in E_K, it is a free abelian group of rank $r = r_K$, the rank of E_K modulo torsion. Fix a subgroup $D = D_K$ of finite index in $E_K(q)$, and let $D(\mathfrak{I}) = D \cap E_K(\mathfrak{I})$ for each ideal $\mathfrak{I}$ of K; $D(\alpha) = D((\alpha))$ for each α in $\mathcal{O}_K$. Each $D(\mathfrak{I})$ is then also free of rank r. This notation will be in force throughout the paper.

PROPOSITION 2.1. LC(K,p) *holds if and only if there exists an integer* $m \geq 2$ *such that* $D(p^m) \subset D^p$.

LEMMA 2.2. *Suppose* $\varepsilon \in D$ *and* k *is a positive integer. Then* $\varepsilon^p \in D(p^{k+1})$ *if and only if* $\varepsilon \in D(p^k)$.

These are proved in [**2**]. Note that $D(p^k)/D(p^{k+1})$ is then a module over $\mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$.

PROPOSITION 2.3. *Let* k *be a positive integer. The following three statements are equivalent.* (1) $D(p^{k+1}) \subset D^p$. (2) $D(p^{k+1}) = D(p^k)^p$. (3) $D(p^k)/D(p^{k+1})$ *has dimension* r *as an* $\mathbf{F}_p$*-vector space.*

PROOF. The equivalence of (1) and (2) follows from the lemma. Note that $D(p^k)/D(p^{k+1})$ is in general a quotient of the r-dimensional $\mathbf{F}_p$-vector space $D(p^k)/D(p^k)^p$. The equivalence of (2) and (3) is now clear.

For each positive integer k we let $\phi_k\colon D(p^k) \to \mathcal{O}_K/p\mathcal{O}_K$ be the homomorphism of abelian groups (the first, multiplicative; the second, additive) defined by $\phi_k(1 + p^k\alpha) = \alpha \pmod p$.

COROLLARY 2.4. LC(K,p) *holds if and only if there exists a positive integer* k *such that either of the following two equivalent conditions holds*: (1) $D(p^k)/D(p^{k+1})$ *has dimension* $r = r_K$ *as an* $\mathbf{F}_p$*-vector space.* (2) *The image of* ϕ_k *in* $\mathcal{O}_K/p\mathcal{O}_K$ *has dimension* r *as an* $\mathbf{F}_p$*-vector space.*

PROOF. That Leopoldt's conjecture is equivalent to (1) follows directly from the propositions. ϕ_k induces an isomorphism from $D(p^k)/D(p^{k+1})$ to the image of ϕ_k; this demonstrates the equivalence of (1) and (2).

III. Leopoldt's conjecture in the fifth degree fields of Maus. Assume now that $p \neq 5$. We will prove LC(K,p) first for a family of fifth degree fields (depending on p) with $r = 2$, and then for a family of fifth degree fields (depending on p) with $r = 3$.

Let $A \geq 1$ (resp. $B \geq 2$) be an integer, and $\varepsilon = \varepsilon_A$ (resp. $\xi = \xi_B$) be a root of $f_A(x) = x^5 + 4A^4x + 1$ (resp. $g_B(x) = x^5 - B^4x + 1$) in an algebraic closure of $\mathbf{Q}$. We put $K_A = \mathbf{Q}(\varepsilon)$ (resp. $L_B = \mathbf{Q}(\xi)$). The ambiguity in choosing ε (resp. ξ) will have no effect on our considerations, which depend only on the isomorphism class of K_A. We collect the necessary facts from [**4**] in the following theorem.

THEOREM 3.1 (MAUS). (1) *The discriminant of* $f_A(x)$ *(resp.* $g_B(x)$*) is* $d_A = 5^5 + 4^9A^{20}$ *(resp.* $d_B = 5^5 - 4^4B^{20}$*).*

(2) *The Galois group of the splitting field of* $f_A(x)$ *(resp.* $g_B(x)$*) over* $\mathbf{Q}$ *is isomorphic to the symmetric group* S_5.

(3) $r(K_A) = 2$ *and two independent units are* $\varepsilon_1 = \varepsilon$ *and* $\varepsilon_2 = \varepsilon^2 - 2A\varepsilon + 2A^2$. $r(L_B) = 3$ *and three independent units are* $\xi_1 = \xi$, $\xi_2 = \xi + B$, *and* $\xi_3 = \xi - B$.

Consider first the fields K_A. With ε_1 and ε_2 as in the theorem, let $\eta_1 = -\varepsilon_1^5$ and $\eta_2 = \varepsilon_2^{10}$. Let D_A be the subgroup of E_{K_A} generated by η_1 and η_2.

LEMMA 3.2. $\eta_1 = 1+4A^4\varepsilon$ *and* $\eta_2 \equiv 1+20A\varepsilon^4 \bmod (2A)^2$, *so* $D_A \subset E_{K_A}(4A)$.

PROOF. The statement about η_1 is clear from the definitions. Now $\varepsilon_2 \equiv \varepsilon^2 - 2A\varepsilon \pmod{2A^2}$, so $\varepsilon_2^5 \equiv \varepsilon^{10} - 10A\varepsilon^9 \pmod{2A^2}$, upon expanding via the binomial theorem. We substitute in $-\eta_1$ for ε^5 where possible and use the equality just observed to continue: $\eta_1^2 + 10A\varepsilon^4\eta_1 \equiv 1 + 10A\varepsilon^4 \pmod{2A^2}$. Thus $\varepsilon_2^5 = 1 + 10A\varepsilon^4 + 2A^2\beta$, $\beta \in \mathcal{O}_{K_A}$. Upon squaring, we see that $\eta_2 = \varepsilon_2^{10} \equiv 1 + 20A\varepsilon^4 \bmod (2A)^2$.

THEOREM 3.3. LC(K_A, p) *holds whenever* $p = 2$ *or* p *divides* A $(p \neq 5)$.

PROOF. Let $\delta_1 = \eta_1 = 1 + 4A^4\varepsilon$ and $\delta_2 = \eta_2^{A^3}$. From the lemma, we have $\eta_2 = 1 + 20A\varepsilon^4 + 4A^2\gamma$, $\gamma \in \mathcal{O}_{K_A}$. Consequently, one finds (with special attention to the factors of 2 and 3) that $\delta_2 \equiv 1 + 20A^4\varepsilon^4 \bmod 4A^5$. Now suppose that p^t exactly divides A, $t \geq 1$. Then δ_1 and δ_2 are in $D_A(p^{4t})$ (and in $D_A(p^{4t+2})$ for $p = 2$). We therefore consider $\phi_{4t}(\delta_1)$ and $\phi_{4t}(\delta_2)$ (or $\phi_{4t+2}(\delta_1)$ and $\phi_{4t+2}(\delta_2)$ for $p = 2$). Our expression for δ_1 and our congruence for δ_2 show that their images are $(A/p^t)^4\varepsilon$ and $5(A/p^t)^4\varepsilon^4 \pmod p$, or 4 times these when p is odd. Now $r = 2$ by (3) of (3.1), and the coefficients of ε and ε^4 are prime to p in any case. Hence (2.3) implies that we need only show that ε and ε^4 have independent images in the $\mathbf{F}_p$-vector space $\mathcal{O}_{K_A}/p\mathcal{O}_{K_A}$. But this follows from the fact that the powers ε^j; $j = 0, 1, 2, 3, 4$; form a basis for an order in $\mathcal{O}_{K_A}$ of index dividing $d_A = 5^5 + 4^9A^{20}$, which is prime to the divisor p of A.

When p equals 2 and does not divide A, we use $\varepsilon_2 = \varepsilon^2 - 2A\varepsilon + 2A^2$ to find $\varepsilon_2^5 \equiv \varepsilon^{10} + 2A\varepsilon^9 + 2A^2\varepsilon^8 \equiv 1 + 2A\varepsilon^4 + 2A^2\varepsilon^3 \pmod 4$. Similarly, $\eta_2 = \varepsilon_2^{10} \equiv 1 + 4A^4\varepsilon + 4A\varepsilon^4 \pmod 8$, while $\eta_1 = 1 + 4A^4\varepsilon$. The images under ϕ_2 are then $A^4\varepsilon + A\varepsilon^4$, and $A^4\varepsilon \pmod 2$. The argument concludes as before, since we still have d_A not divisible by $p = 2$.

Consider now the fields L_B. With ξ_1, ξ_2, and ξ_3 as in (3.1); let $\theta_1 = -\xi_1^5 = -\xi^5 = 1 - B^4\xi$, $\theta_2 = -\xi_2^5 = -\xi^5 - 5B\xi^4 + B^2\gamma' = 1 - 5B\xi^4 + B^2\gamma$, and $\theta_3 = (\xi_2\xi_3)^5 = (\xi^2 - B^2)^5 = \xi^{10} - 5B^2\xi^8 + B^3\beta' = 1 + 5B^2\xi^3 + B^3\beta$ (γ', γ, β', and β in $\mathcal{O}_{L_B}$).

THEOREM 3.4. LC(L_B, p) *holds whenever* p *divides* B, $p \neq 5$.

PROOF. Let $\rho_1 = \theta_1$, $\rho_2 = \theta_2^{B^3} = 1 - 5B^4\xi^4 - 25((B^4 - B)/2)B^4\xi^3 + B^5\lambda$, $\rho_3 = \theta_3^{B^2} = 1 + 5B^4\xi^3 + B^5\tau$; $\lambda, \tau \in \mathcal{O}_{L_B}$. Suppose that p^t exactly divides B, so $t \geq 1$. Then the ρ_i lie in $E_{L_B}(p^{4t})$, hence so does the group D_B they generate. Now $\phi_{4t}(\rho_1) = (B/p^t)^4\xi$, $\phi_{4t}(\rho_2) = -5(B/p^t)^4\xi^4 - 25((B^4 - B)/2)(B/p^t)^4\xi^3$, and $\phi_{4t}(\rho_3) = 5(B/p^t)^4\xi^3 \pmod p$. Again p does not divide the discriminant d_B, so the powers ξ^i, $i = 0, 1, 2, 3, 4$, form a basis mod p, and we see that these values ϕ_{4t} are linearly independent. An application of (2.4) completes the proof.

IV. Fields related by congruence conditions. In this section we assume LC(K, p) and consider LC(L, p) for L in a family of fields related to K. Let α be an

algebraic integer such that $K = \mathbf{Q}(\alpha)$, and let $f(x) \in \mathbf{Z}[x]$ be the monic irreducible polynomial satisfied by α. The order $\mathbf{Z}[\alpha]$ has finite index i_α in $\mathscr{O}_K$, and its unit group is of the same free rank $r(K)$. (For some M, $E_K^M \subset 1 + i_\alpha \mathscr{O}_K \subset \mathbf{Z}[\alpha]$.)

We also assume now that D is chosen to lie in $\mathbf{Z}[\alpha]$. If $(p, i_\alpha) = 1$, then $\mathbf{Z}[\alpha]/p^k\mathbf{Z}[\alpha]$ is naturally isomorphic to $\mathscr{O}_K/p^k\mathscr{O}_K$ for each k, and $D(p^k)$ is the same whether we understand congruence modulo p^k to hold in $\mathscr{O}_K$ or in $\mathbf{Z}[\alpha]$. Let d_f be the discriminant of $f(x)$ and d_K be the discriminant of K, so $d_f = i_\alpha^2 d_K$.

THEOREM 4.1. *Suppose $K = \mathbf{Q}(\alpha)$, α a root of the monic irreducible polynomial $f(x)$ of degree n with rational integer coefficients, and suppose p is a prime with p^2 not dividing the discriminant d_f. Let $\varepsilon_i = \sum_{j=0}^{n-1} a_{i,j}\alpha^j$; $i = 1, \ldots, r$, be a maximal system of independent units congruent to 1 modulo q in $\mathbf{Z}[\alpha]$, and define D to be the group they generate. Assume* $\mathrm{LC}(K, p)$ *holds, and choose $m \geq 2$ so that $D(p^m) \subset D^p$. Now choose a monic polynomial $g(x)$ of degree n which is congruent to $f(x)$ modulo p^m, coefficient by coefficient. Let K' be the field obtained by adjoining a root β of $g(x)$ to $\mathbf{Q}$, and assume that K' has a maximal system of independent units $\delta_i = \sum_{j=0}^{n-1} b_{i,j}\beta^j$, $j = 1, \ldots, r$; where $b_{i,j} \equiv a_{i,j} \bmod p^m$ for each pair of indices i and j. Then Leopoldt's conjecture also holds for K' and the prime p.*

PROOF. We of course define D' to be the group generated by the δ_j. The discriminant d_g of $g(x)$ is an integral polynomial in the coefficients of $g(x)$: these being the same modulo p^2 as the coefficients of $f(x)$, we have that $d_g \equiv d_f$ modulo p^2. In particular, the fact that p^2 does not divide d_f implies that p^2 does not divide d_g, so $(p, i_\alpha) = 1$ and $(p, i_\beta) = 1$. By the preceding discussion, we have natural isomorphisms $\mathscr{O}_K/p^m\mathscr{O}_K \cong \mathbf{Z}[\alpha]/p^m\mathbf{Z}[\alpha]$ and $\mathscr{O}_{K'}/p^m\mathscr{O}_{K'} \cong \mathbf{Z}[\beta]/p^m\mathbf{Z}[\beta]$. However these quotients on the right hand side are naturally isomorphic to $\mathbf{Z}[x]/(p^m, f(x))$ and $\mathbf{Z}[x]/(p^m, g(x))$, *which are the same ring.* Taking the images of D and D' in this ring, we find that $D/D(p^m) \cong D'/D'(p^m)$. Then $D(p^{m-1})/D(p^m) \cong D'(p^{m-1})/D'(p^m)$, and both have the same rank $r = r(K) = r(K')$, by (2.3). $\mathrm{LC}(K', p)$ follows by application of (2.4).

REMARK 4.2. In fact, one can easily see that the result holds if we assume that p is prime to i_α and i_β, but make no assumption on d_f.

COROLLARY 4.3. *Suppose that A is an integer such that $LC(K_A, p)$ holds and p^2 does not divide $d_A = 5^5 + 4^9 A^{20}$. Choose $D_A \subset E_{K_A}(q)$ to be generated by ε_1^a and ε_2^b for some appropriate positive integers a and b. Fix m such that $D_A(p^m) \subset D_A^p$. Let $\mathscr{F}$ be the family of fields $K_{A'}$ such that $A' \equiv A \pmod{p^m}$. Then* $\mathrm{LC}(F, p)$ *holds for each F in $\mathscr{F}$.*

PROOF. Using (3) of (3.1) and defining $D_{A'}$ via the same exponents a and b, it is easy to verify the hypotheses of the theorem with $f(x) = f_A(x)$, $g(x) = f_{A'}(x)$, $\alpha = \varepsilon_A$, and $\beta = \varepsilon_{A'}$.

COROLLARY 4.4. *Suppose that B is an integer such that* $\mathrm{LC}(L_B, p)$ *holds and p^2 does not divide $d_B = 5^5 - 4^4 B^{20}$. Fix m such that $D_B(p^m) \subset D_B^p$. Let $\mathscr{G}$ be the family of fields $L_{B'}$ such that $B' \equiv B \pmod{p^m}$. Then* $\mathrm{LC}(F, p)$ *holds for each F in $\mathscr{G}$.*

PROOF. Clear, by modifying the proof of (4.3).

REMARK 4.5. To obtain an application of (4.3) or (4.4), one can use the algorithm of [**2**] to computationally verify $\mathrm{LC}(K_A, p)$ or $\mathrm{LC}(L_B, p)$. As an example, for $p = 7$, the discriminant hypotheses are satisfied by all fields under consideration. We report that the computer verifies Leopoldt's conjecture with $m = 2$ when $1 \leq A \leq 49$ or $2 \leq B \leq 50$ (we discover that $m = 5$ is not necessary when 7 divides A or B, if D_A and D_B are chosen differently). Hence the corollaries imply that Leopoldt's conjecture holds with $p = 7$ for *all* K_A and L_B. Similarly, $\mathrm{LC}(L_B, 3)$ is deduced for all B, as is $\mathrm{LC}(K_A, 3)$ for all $A \not\equiv \pm 4$ modulo 9. (The discriminant condition is not met in the exceptional cases.)

V. The infinitude of fields in certain families. We now show that the families of fields considered in (3.3), (3.4), (4.3) and (4.4) are infinite.

PROPOSITION 5.1. *Fix a positive integer modulus M and a congruence class representative $a \geq 0$; consider $A = a + Mn$ (resp. $B = a + Mn$). If l is a prime number congruent to* 3 *or* 7 *(modulo* 20*) (resp. congruent to* -1 *(modulo* 20*)) and not dividing M, then there exists a nonnegative integer $n < 2l$ such that l ramifies in K_A (resp. L_B).*

PROOF. By the familiar equality immediately preceding (4.1), it suffices to ensure that l exactly divides $d_A = 5^5 + 4^9 A^{20}$ (resp. $d_B = 5^5 - 4^4 B^{20}$). As n ranges from 0 to $l-1, Mn$ and $A = B = a + Mn$ both range over complete residue systems (modulo l). Our congruence conditions on l then imply that $-4^9 A^{20}$ ranges twice over the nonsquares (modulo l), of which 5^5 is one (resp. $4^4 B^{20}$ ranges twice over the squares (modulo l), of which 5^5 is one), by quadratic reciprocity. Hence we can choose $n < l$ such that l divides d_A (resp. d_B). If n is replaced by $n + l$, it is easy to see that the difference in d_A (resp. d_B) is exactly divisible by l, so that replacing n by $n + l$ if necessary completes the proof.

COROLLARY 5.2. *For A (resp. B) is any arithmetic progression, there are infinitely many distinct fields K_A (resp. L_B).*

PROOF. Arguing by contradiction, the set of primes which ramify in at least one of these fields would otherwise be finite. (5.1) and Dirichlet's theorem on primes in an arithmetic progression show that this is not so.

The following corollaries are now clear.

COROLLARY 5.3. *When p is fixed, the family of fields $\{K_{p^n} : n = 1, 2, \dots\}$ (or K_n if $p = 2$) for which Leopoldt's conjecture holds by* (3.3) *is infinite.*

COROLLARY 5.4. *When p is fixed, the family of fields $\{L_{p^n} : n = 0, 1, 2, \dots\}$ for which Leopoldt's conjecture holds by* (3.4) *is infinite.*

COROLLARY 5.5. *For a fixed prime p and positive integer A, the family of fields $\{K_{A'}\}$ considered in* (4.3) *is infinite.*

COROLLARY 5.6. *For a fixed prime p and positive integer B, the family of fields $\{L_{B'}\}$ considered in* (4.4) *is infinite.*

REFERENCES

1. A. Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124.
2. J. Buchmann and J. W. Sands, *An algorithm for testing Leopoldt's conjecture*, J. Number Theory **27** (1987), 92–105.

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. E. Maus, *Zur Arithmetik einiger Serien nichtauflösbarer Gleichungen* 5. *Grades*, Abh. Math. Sem. Univ. Hamburg **54** (1984), 227–250.
5. T. Nguyen-Quang-Do, *Sur la structure Galoisienne des corps locaux et la théorie d'Iwasawa*, Comp. Math. **46** (1982), 85–119.
6. J.-P. Serre, *Sur le résidue de la fonction zêta p-adique d'une corps de nombres*, C.R. Acad. Sci. Paris **287** (1978), 183–188.

MATHEMATISCHES INSTITUT, UNIVERSITAT DUSSELDORF, 4000 DUSSELDORF, WEST GERMANY

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF VERMONT, BURLINGTON, VERMONT 05405