

AN ELEMENTARY PROOF OF THE LOCAL KRONECKER-WEBER THEOREM

BY

MICHAEL ROSEN

ABSTRACT. Let K be a local field. Lubin and Tate have shown how to explicitly construct an abelian extension of K which they prove to be the maximal abelian extension. Their proof of this result uses local class field theory. When K is a p -adic field we give an elementary proof which even avoids the use of higher ramification groups. Instead we rely on facts about the principal units in a finite abelian extension of K as a module for the Galois group.

The Kronecker-Weber theorem asserts that the maximal abelian extension of \mathbb{Q} , the rational numbers, is obtained by adjoining all the roots of unity to \mathbb{Q} . When K is a local field a similar theorem was proved by Lubin and Tate [5].

A description of the Lubin-Tate construction goes as follows. Let K be a local field, π a uniformizing parameter, p the characteristic of the residue class field, and $q = p^f$ the number of elements in the residue class field. Let $f(x) = X^q + \pi X$ and $f^n = f \circ f \circ \cdots \circ f$, i.e. f composed with itself n times. The field obtained by adjoining the roots of f^n to K will be denoted by $L_\pi^{(n)}$ and the union of these fields by L_π . Finally, denote by U the field obtained by adjoining the roots of the polynomials $X^n - 1$, n prime to p , to K . U is the maximal unramified extension of K . The theorem asserts that the compositum UL_π is the maximal abelian extension of K . It is reasonable to call this result the local Kronecker-Weber theorem.

Both the Kronecker-Weber theorem and the local version are most easily proved using class field theory. In the global case there is a long history of "elementary" proofs. In the local case there is an elementary proof due to Hazewinkel [2] and more recently one due to Lubin. The former takes place in the context of pro-algebraic groups whereas the latter uses the detailed theory of the higher ramification groups and the Hasse-Arf theorem.

In this paper we give another proof in the case where K is a p -adic field. No use will be made of the higher ramification groups.

The main idea of our proof is remarkably simple. The tools we need are Kummer theory, the structure of K^* , and in Galois extensions of K the structure of the principal units as a module for the Galois group.

1. In this section we deal with the tamely ramified extensions and reduce the proof to a question about the maximal abelian p -extension.

Received by the editors August 1, 1980.

1980 *Mathematics Subject Classification*. Primary 12B25; Secondary 12B15, 12B17.

Key words and phrases. Local field, abelian extension, Kummer theory, principal units, group ring, Lubin-Tate construction.

First, some notation. A will be the maximal abelian extension of K , Λ the maximal abelian p -extension of K , and Ω the maximal abelian p -extension of K in UL_π .

LEMMA 1. *Every abelian extension of K is contained in the compositum of an unramified extension and a totally ramified abelian extension.*

PROOF. $G(A/K)$ maps by restriction onto $G(U/K) \approx \hat{Z}$. The latter group is free in the category of profinite groups. Thus the map splits. The result follows from this.

LEMMA 2. *Every abelian tamely ramified extension of K is contained in $UL_\pi^{(1)}$.*

PROOF. The method of Lemma 1 shows that we may confine our attention to abelian extensions which are totally and tamely ramified. By a standard result, these are of the form $K(\epsilon\sqrt[e]{\gamma})$ where $e|q-1$ and γ is a uniformizing parameter. There is a unit $u \in K$ such that $\pi = -u\gamma$. It follows easily that $K(\epsilon\sqrt[e]{\gamma})$ is contained in the compositum of $L_\pi^{(1)}$ and $K(\epsilon^{-1}\sqrt[e]{u})$. The latter field is unramified over K .

LEMMA 3. *If $\Lambda = \Omega$ the theorem is true.*

PROOF. We have $A = \Lambda\Gamma$, where Γ is the maximal "prime to p " abelian extension of K . By Lemma 2, $\Gamma \subset UL_\pi$. Thus the theorem is true if $\Lambda \subset UL_\pi$, but this is equivalent to $\Lambda = \Omega$.

To prove $\Lambda = \Omega$ we use the following strategy. Clearly, $\Omega \subseteq \Lambda$ and there is an onto map $G(\Lambda/K) \rightarrow G(\Omega/K)$. If the kernel is trivial then $\Lambda = \Omega$. To show the kernel is trivial we will show that both Galois groups are finitely generated Z_p modules isomorphic to each other. The result will then follow from the fact that an onto endomorphism of a Noetherian module is necessarily one-to-one.

From Lubin-Tate theory [5], $G(L_\pi/K)$ is isomorphic to the group of units in K . We also know $G(U/K) \approx \hat{Z}$. Since U and L_π are disjoint over K it follows that $G(\Omega/K) \approx Z_p^{n+1} \times \mu_{p^s}$, where $n = [K : Q_p]$ and p^s is the maximal power of p such that K contains a p^s root of unity.

The proof now separates into two cases depending on whether $s = 0$ or not. The case $s = 0$ is technically much easier, but the idea is the same in both.

2. Suppose $s = 0$. We must show $G(\Lambda/K) \approx Z_p^{n+1}$. Since $G(\Lambda/K)$ is an abelian compact pro- p -group mapping onto $G(\Omega/K) \approx Z_p^{n+1}$ it suffices to show $G(\Lambda/K)/G(\Lambda/K)^p$ has Z/pZ dimension $n+1$. For a given field E , let E_1 be the maximal elementary abelian p -extension of E . We want to show $[K_1 : K] = p^{n+1}$. The idea is to consider $E = K(\zeta_p)$, use Kummer theory to discuss E_1 , and then recover K_1 .

Since $\zeta_p \in E$ we know $E_1 \approx E(p\sqrt[p]{E^*})$. Now, $K_1 \subset E_1$ and $[K_1E : E] = [K_1 : K]$ since $[E : K]$ is prime to p . By Kummer theory K_1E corresponds to a subgroup of E^* containing E^{*p} . Call this subgroup Δ . We want to identify Δ and show Δ/E^{*p} has dimension $n+1$ over Z/pZ .

It is easy to see that K_1E is the maximal intermediate extension of E_1/E which is abelian over K .

Let $\mathfrak{G} = G(E/K)$ and χ be the homomorphism from \mathfrak{G} to $(Z/pZ)^*$ defined by $\zeta_p^\tau = \zeta_p^{\chi(\tau)}$ for $\tau \in \mathfrak{G}$.

LEMMA 4. *An element $a \in E^*$ belongs to Δ if and only if $a^\tau \equiv a^{\chi(\tau)} \pmod{E^{*p}}$.*

PROOF. Set $F = K_1 E$. The group Δ is simply $F^{*p} \cap E$. We recall how one sets up the isomorphism between Δ/E^{*p} and the character group of $G(F/E)$.

For $a \in \Delta$ there is an $\alpha \in F$ such that $\alpha^p = a$. If $t \in G(F/E)$ we write $\Psi_a(t) = \alpha^{t-1}$. The map $a \rightarrow \Psi_a$ leads to the required isomorphism.

Suppose $\tau \in G(F/K)$ restricts to a generator of \mathfrak{G} and let $t \in G(F/E)$. Since $K(\alpha)/K$ is abelian we have $\alpha^{t\tau} = \alpha^{\tau t}$ which implies $(\alpha^{t-1})^\tau = (\alpha^\tau)^{t-1}$ and so $\Psi_a(t)^\tau = \Psi_{a^\tau}(t)$. Now, notice $\Psi_a(t)^\tau = \Psi_a(t)^{\chi(\tau)} = \Psi_{a^{\chi(\tau)}}(t)$. Thus $a^\tau \equiv a^{\chi(\tau)} \pmod{E^{*p}}$. To prove the converse, one simply reverses the steps.

This lemma is due to I. Shafarevich.

We now view E^*/E^{*p} as a module for the group ring $Z/pZ[\mathfrak{G}]$. Considered in this way the above lemma says that Δ/E^{*p} is the χ -component of E^*/E^{*p} . We wish to compute its dimension over Z/pZ . The following lemma shows we need only consider the group of principal units, $U^{(1)}$, of E .

LEMMA 5. $\Delta/E^{*p} \approx [U^{(1)}/U^{(1)p}](\chi)$.

PROOF. Suppose $\tau \in \mathfrak{G}$ is a generator and let k be an integer, $0 < k < p$, such that $k \pmod p$ is $\chi(\tau)$. If $a \in \Delta$ then $a^\tau \equiv a^k \pmod{E^{*p}}$. Let ord be the order with respect to some uniformizing parameter of E . If $s = \text{ord } a$, then we see $s = ks + pr$ for some integer r . It follows that p divides s and so we may assume a is a unit. Since $U/U^{(1)}$ has order prime to p we may even assume a is a principal unit. This completes the proof.

The principal units of E are acted on by the p -adic integers and may thus be considered as a $Z_p[\mathfrak{G}]$ module. The structure of this module is a consequence of the following result due to Krasner [3].

LEMMA 6. *Let E/K be a Galois extension of p -adic fields with group G . Suppose $[E:K]$ is prime to p . Then the principal units of E as a $Z_p[G]$ module is the direct sum of the torsion subgroup and a free module of rank $n = [K:Q_p]$.*

We will give a quick proof of this in the appendix. The important point is that the proof does not involve class field theory.

We are now in a position to complete the proof of the main theorem in the case where $\zeta_p \notin K$. The remarks at the beginning of this section reduce the proof to the assertion that Δ/E^{*p} has dimension $n + 1$ over Z/pZ . By Lemma 5 we need only prove the same assertion about $[U^{(1)}/U^{(1)p}](\chi)$. By Lemma 6 we need to compute the Z/pZ dimension of the χ -component of

$$t(E^*)/t(E^*)^p \oplus Z/pZ[\mathfrak{G}] \oplus \cdots \oplus Z/pZ[\mathfrak{G}].$$

Here $t(E^*)$ denotes the torsion subgroup of E^* and the sum is over n copies of $Z/pZ[\mathfrak{G}]$. Simple calculations reveal the following two facts.

(i) $t(E^*)/t(E^*)^p \approx \mu_p$ as \mathfrak{G} modules.

(ii) The χ -component of $Z/pZ[\mathfrak{G}]$ is cyclic over Z/pZ generated by $\sum_{\sigma} \chi(\sigma)^{-1} \sigma$.

Putting all this together we see that, indeed, the Z/pZ dimension of Δ/E^{*p} is $n + 1$ as required. The proof is complete.

3. In this section we assume $\zeta_p \in K$ but $\zeta_{p^{s+1}} \notin K$ where $s \geq 1$. If $p = 2$ we assume further that $\sqrt{-1} \in K$.

Recall that $G(\Omega/K) \approx \mu_p \times Z_p^{n+1}$ where Ω is the maximal p -extension of K in the Lubin-Tate extension UL_∞ . The Galois group $G(\Lambda/K)$, where Λ is the maximal abelian p -extension of K , is a Z_p module. Using Kummer theory we see that the Z/pZ dimension of $G(\Lambda/K)/G(\Lambda/K)^p$ is the same as that of K^*/K^{*p} . The dimension of the latter group is $n + 2$. Since $G(\Lambda/K)$ maps onto $G(\Omega/K)$ we may conclude

$$G(\Lambda/K) \approx C \times Z_p^{n+1},$$

where C is either isomorphic to Z_p or is cyclic of order p^t with $t \geq s$. To prove the theorem we need to show $t = s$. If C is bigger then clearly $[K_{s+1} : K] = (p^{s+1})^{n+2}$, where K_{s+1} is the maximal abelian p -extension of K with exponent dividing p^{s+1} . We will prove the theorem by showing $[K_{s+1} : K] < (p^{s+1})^{n+2}$.

Since $\zeta_{p^{s+1}} \notin K$, K_{s+1}/K is not a Kummer extension. As in the last section we first add the requisite root of unity to K . Let $L = K(\zeta_{p^{s+1}})$. Then L_{s+1}/L is a Kummer extension and we can use its properties to say something about K_{s+1}/K . Let M be the maximal abelian extension of K in L_{s+1} . Notice that we have the following series of inclusions $K \subset L \subset K_{s+1} \subset M \subset L_{s+1}$. Clearly $[L : K] = p$. We will show that $[M : K_{s+1}] = p$. It then follows that $[K_{s+1} : K] = [M : L]$. M/L is a Kummer extension and we will use arguments similar to those in the last section to determine $[M : L]$. The crucial piece of information necessary will be the structure of the principal units in L as a module for $\mathfrak{G} = G(L/K)$. This has been determined by Borevich in [1].

LEMMA 7. *Let M be the maximal abelian extension of K in L_{s+1} . Then $[M : K_{s+1}] = p$.*

PROOF. We first note that $K(\zeta_{p^{2s+2}})$ is in M and is cyclic of order p^{s+2} over K (recall that when $p = 2$ we are assuming that $\sqrt{-1} \in K$). Let $G = G(L_{s+1}/K)$, $H = G(L_{s+1}/L)$, and $\mathfrak{G} = G(L/K)$. Let $\tau \in G$ be an element which restricts to a generator of $G(K(\zeta_{p^{2s+2}})/K)$. Since τ restricted to L is nontrivial every element of G is of the form $\tau^i h$ where $0 \leq i \leq p$ and $h \in H$. Finally, let $\tau_0 = \tau^{p^{s+1}}$ restricted to M . τ_0 acts nontrivially on $\zeta_{p^{2s+2}}$ and so has order p . We claim $K_{s+1} = M^{\langle \tau_0 \rangle}$.

Since τ_0 is a p^{s+1} power we have $K_{s+1} \subseteq M^{\langle \tau_0 \rangle}$. Suppose $\alpha \in M$ and $\alpha^{\tau_0} = \alpha$. Consider $K(\alpha)/K$. This is an abelian extension. If λ is in the Galois group, then $\lambda = \tau^i h$ restricted to $K(\alpha)$. Since τ and h commute on $K(\alpha)$ we find $\lambda^{p^{s+1}} = \tau_0^i$ on $K(\alpha)$. But τ_0 is the identity on $K(\alpha)$ so λ has order dividing p^{s+1} . It follows that $\alpha \in K_{s+1}$ and we are done.

We denote the group ring $Z/p^{s+1}Z[\mathfrak{G}]$ by R . Let g be a generator of \mathfrak{G} . The norm element of R , namely $\sum_{i=0}^{p-1} g^i$, will be denoted by N . The homomorphism Ψ from \mathfrak{G} to $(Z/p^{s+1}Z)^*$ is defined by $\zeta_{p^{s+1}}^g = \zeta_{p^{s+1}}^{\Psi(g)}$. Since \mathfrak{G} is cyclic of order p one can choose a generator $g \in \mathfrak{G}$ such that $\Psi(g)$ is the coset of $1 + p^s$. If A is an R

module we define

$$A(\Psi) = \{a \in A \mid \tau a = \Psi(\tau)a, \tau \in \mathfrak{G}\} = \{a \in A \mid ga = (1 + p^s)a\}.$$

We note that if $(0) \rightarrow A \rightarrow B \rightarrow C \rightarrow (0)$ is an exact sequence of finite R modules, then $|B(\Psi)| \leq |A(\Psi)| + |C(\Psi)|$.

LEMMA 8. $[M:L] = |(L^*/L^{*p^{s+1}})(\Psi)|$.

PROOF. Since M/L is a Kummer extension, the character group of $G(M/L)$ is isomorphic to $M^{*p^{s+1}} \cap L^*/L^{*p^{s+1}}$. The proof now proceeds as in Lemma 4.

Let $\alpha \in M$ with $\alpha^{p^{s+1}} = a \in L$. $K(\alpha)/K$ is abelian. Let g be extended to an automorphism of M and $h \in H$. Then $\alpha^{gh} = \alpha^{hg}$ which implies $(\alpha^g)^{h-1} = (\alpha^{h-1})^g$. Thus, $\chi_{a^g}(h) = \chi_a(h)^g = \chi_a(h)^{\Psi(g)} = \chi_{a^{\Psi(g)}}(h)$. It follows that $a^g \equiv a^{\Psi(g)} \pmod{L^{*p^{s+1}}}$. The steps can be reversed so that the latter condition on an element $a \in L^*$ insures that its p^{s+1} root generates an abelian extension of K . Thus $(L^*/L^{*p^{s+1}})(\Psi)$ is isomorphic to the character group of $G(M/L)$ and the lemma follows.

Before discussing the structure of L^* as a \mathfrak{G} module we need a few technical lemmas about Ψ -components.

LEMMA 9. Let A be an R module which is acted on trivially by \mathfrak{G} and as an abelian group is cyclic of order p^{s+1} . Then $A(\Psi) = pA$. In particular, $|A(\Psi)| = p^s$.

PROOF. $a \in A(\Psi)$ if and only if $ga = (1 + p^s)a$. Since g acts trivially this is equivalent to $0 = p^s a$. This condition clearly characterizes pA .

LEMMA 10. $R(\Psi)$ is a cyclic group of order p^{s+1} generated by

$$e = \sum_{i=0}^{p-1} (1 + p^s)^{-i} g^i.$$

PROOF. This is a straightforward exercise.

LEMMA 11. Let $T = R/NR$, N the norm element. Then $T(\Psi)$ is a cyclic group of order p generated by the image of e in T .

PROOF. We first note that if $b \in T(\Psi)$ then $pb = 0$. To see this remember $gb = (1 + p^s)b$ so that

$$0 = Nb = \left(\sum_{i=0}^{p-1} (1 + p^s)^i \right) b = pb + \left(\sum_{i=0}^{p-1} i \right) p^s b.$$

If p is odd then the sum is divisible by p and the assertion is proved. If $p = 2$ then $0 = 2b + 2^s b$. Remembering that we have assumed $s \geq 2$ if $p = 2$ we can write $0 = (1 + 2^{s-1})2b$. Since $s \geq 2$, $1 + 2^{s-1}$ is a unit in T , so $2b = 0$.

Now, every element in T has a unique representative in R of the form $a = \sum_{i=1}^{p-1} a_i g^i$. Using this, and the relation $gb = (1 + p^s)b$, one is led to a recursion relation among the a_i which must hold if the image of a in T is to lie in $T(\Psi)$. These relations show that if such elements exist at all they are completely determined by a_1 . Since by the first part of the proof we must have $pa_1 = 0$ it follows that

$|T(\Psi)| \leq p$. On the other hand it is clear that the image of e in T is in $T(\Psi)$ and is not trivial. Thus $T(\Psi)$ has order p and is generated by the image of e as asserted.

REMARK. It is amusing to note that the image of e in T is $-p^s \sum_{i=1}^{p-1} g^i$ which is the same as the constant element $p^s \bmod N$.

We recall that to complete the proof we need to show $[K_{s+1} : K] < (p^{s+1})^{n+2}$. Using Lemma 7 we find $[K_{s+1} : K] = [M : L]$ and by Lemma 8 $[M : L] = |L^*/L^{*p^{s+1}}(\Psi)|$. Let U denote the units of L , and π a uniformizing parameter of L . We have an exact sequence

$$(1) \rightarrow U/U^{p^{s+1}} \rightarrow L^*/L^{*p^{s+1}} \rightarrow Z/p^{s+1}Z \rightarrow (0),$$

the third arrow being induced by taking the order of elements with respect to π . Using Lemma 9 we find

$$|L^*/L^{*p^{s+1}}(\Psi)| \leq p^s |U/U^{p^{s+1}}(\Psi)|.$$

Now, $U/U^{p^{s+1}} \approx U^{(1)}/U^{(1)p^{s+1}}$ where $U^{(1)}$ is the group of principal units of L . The theorem will be proven if we can show

$$|U^{(1)}/U^{(1)p^{s+1}}(\Psi)| = (p^{s+1})^{n+1}.$$

That this is indeed the case follows from the following result of Borevich.

LEMMA 11. (i) If L/K is unramified then $U^{(1)} \approx \mu_{p^{s+1}} \times Z_p[\mathfrak{G}]^n$.

(ii) If L/K is ramified then

$$U^{(1)} \approx \mu_{p^{s+1}} \times Z_p[\mathfrak{G}]^{n-1} \times Z \times Z_p[\mathfrak{G}]/NZ_p[\mathfrak{G}].$$

These statements are equivalent to Theorems 3 and 4 of [1]. The proof uses the fact that $U^\mathfrak{G} = NU$ in the unramified case and $|U^\mathfrak{G}/NU| = p$ in the ramified case. These statements may seem to involve class field theory but they can be demonstrated using elementary properties of the Herbrand quotient. See, for example, Lemma 4 on p. 188 of Lang's book [4].

We can now complete the proof. If L/K is unramified then by Lemma 11,

$$U^{(1)}/U^{(1)p^{s+1}} \approx \mu_{p^{s+1}} \times R^n.$$

By Lemma 9 we find that the Ψ -component has order $p^{s+1} \times (p^{s+1})^n = (p^{s+1})^{n+1}$.

If L/K is ramified then by Lemma 11,

$$U^{(1)}/(U^{(1)p^{s+1}}) \approx \mu_{p^{s+1}} \times R^{n-1} \times Z/p^{s+1}Z \times T.$$

By Lemmas 9, 10, and 11 it follows that the Ψ -component has order

$$p^{s+1} \times (p^{s+1})^{n-1} \times p^s \times p = (p^{s+1})^{n+1}.$$

4. We complete the proof by dealing with the only remaining case; K a 2-adic field and $\sqrt{-1} \notin K$.

We know $G(\Omega/K) \approx \langle \pm 1 \rangle \times Z_2^{n+1}$ and, as before, this shows $G(\Lambda/K) \approx \mu_2 \times Z_2^{n+1}$ where $1 \leq s \leq \infty$. We must show that $s = 1$.

If $s > 1$, $G(K_2/K) \approx (Z/4Z)^{n+2}$ and it follows that every quadratic extension of K is contained in a cyclic extension of degree 4. According to the following lemma this situation cannot occur.

LEMMA 12. Let K be a 2-adic field and suppose $\sqrt{-1} \notin K$. Then, not every quadratic extension of K is contained in a cyclic extension of degree 4.

PROOF. Let $a \in K$, a not a square. Let $L_0 = K(\sqrt{a})$ and suppose $L_0 \subset L$ with L/K cyclic of degree 4. We denote by σ a generator of the Galois group.

$L = L_0(\alpha)$ where $\alpha^2 = A + B\sqrt{a} \in L_0$, A and $B \in K$. Then $(\alpha^\sigma)^2 = A - B\sqrt{a}$. Since both α and α^σ generate L over L_0 we must have, by Kummer theory, $\alpha^\sigma = \alpha(C + D\sqrt{a})$ with C and $D \in K$. Applying σ to both sides of this equality shows $\alpha^{\sigma^2} = \alpha(C^2 - aD^2)$. Since σ^2 fixes L_0 we find $\alpha^{\sigma^2} = -\alpha$ and so $-1 = C^2 - aD^2$. Since $\sqrt{-1} \notin K$, $D \neq 0$. Thus $a = (1/D)^2 + (C/D)^2$.

If the lemma were false it would follow that every element of K is a norm from $K(\sqrt{-1})$. However, the norm index is 2 (see the remark following Lemma 11). This completes the proof.

Appendix. We sketch a proof of Krasner's result, Lemma 6.

By the normal basis theorem $E \approx K[G]$ as left $K[G]$ modules. It follows easily that E contains a Z_p lattice L , invariant under G , such that $L \approx Z_p[G]^n$ as right $Z_p[G]$ modules. By multiplying by a sufficiently high power of p we may assume L is in the domain of the exponential map. $\exp L$ is disjoint from the torsion subgroup of $U^{(1)}$. Thus, $U^{(1)} \bmod \text{torsion}$ contains a free $Z_p[G]$ submodule of finite index. Since $p \nmid |G|$ it follows that $Z_p[G]$ is a maximal order in the semisimple algebra $Q_p[G]$. A standard theorem says that such an order is a principal ideal ring. From this it follows that $U^{(1)} \bmod \text{torsion}$ is itself a free $Z_p[G]$ module of rank n and Krasner's result is an immediate consequence.

We remark that when G is abelian of exponent dividing $p-1$, as it is in our application, the proof is even easier since $Z_p[G]$ splits into a direct sum of ideals each of rank one over Z_p .

BIBLIOGRAPHY

1. Z. I. Borevich, *On the multiplicative group of cyclic p -extensions of a local field*, Proc. Steklov Inst. Math. **80** (1965), 15–30.
2. M. Hazewinkel, *Local class field theory is easy*, Adv. in Math. **18** (1975), 148–181.
3. M. Krasner, *Sur la representation exponentielle dans les corp relativement galoisien de nombres p -adique*, Acta Arith. **3** (1939), 133–173.
4. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1968.
5. J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. **81** (1965), 380–387.

DEPARTMENT OF MATHEMATICS, BROWN UNIVERSITY, PROVIDENCE, RHODE ISLAND 02912