20 The Kronecker-Weber theorem

In the previous lecture we established a relationship between finite groups of Dirichlet characters and subfields of cyclotomic fields. Specifically, we showed that there is a one-to-one-correspondence between finite groups H of primitive Dirichlet characters of conductor dividing m and subfields K of $\mathbb{Q}(\zeta_m)$ under which H can be viewed as the character group of the finite abelian group $\mathrm{Gal}(K/\mathbb{Q})$ and the Dedekind zeta function of K factors as

$$\zeta_K(s) = \prod_{\chi\in H} L(s,\chi).$$

Now suppose we are given an arbitrary finite abelian extension $K/\mathbb{Q}$. Does the character group of $\mathrm{Gal}(K/\mathbb{Q})$ correspond to a group of Dirichlet characters, and can we then factor the Dedekind zeta function $\zeta_K(s)$ as a product of Dirichlet L-functions?

The answer is yes! This is a consequence of the *Kronecker-Weber theorem*, which states that every finite abelian extension of $\mathbb{Q}$ lies in a cyclotomic field. This theorem was first stated in 1853 by Kronecker [2], who provided a partial proof for extensions of odd degree. Weber [7] published a proof 1886 that was believed to address the remaining cases; in fact Weber's proof contains some gaps (as noted in [5]), but in any case an alternative proof was given a few years later by Hilbert [1]. The proof we present here is adapted from [6, Ch. 14]

20.1 Local and global Kronecker-Weber theorems

We now state the (global) Kronecker-Weber theorem.

Theorem 20.1. *Every finite abelian extension of* $\mathbb{Q}$ *lies in a cyclotomic field* $\mathbb{Q}(\zeta_m)$.

There is also a local version.

Theorem 20.2. *Every finite abelian extension of* $\mathbb{Q}_p$ *lies in a cyclotomic field* $\mathbb{Q}_p(\zeta_m)$.

We first show that the local version implies the global one.

Proposition 20.3. *The local Kronecker-Weber theorem implies the global Kronecker-Weber theorem.*

Proof. Let $K/\mathbb{Q}$ be a finite abelian extension. For each ramified prime p of $\mathbb{Q}$, pick a prime $\mathfrak{p}|p$ and let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$ (the fact that $K/\mathbb{Q}$ is Galois means that every $\mathfrak{p}|p$ is ramified with the same ramification index; it makes no difference which $\mathfrak{p}$ we pick). We have $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) \simeq D_\mathfrak{p} \subseteq \mathrm{Gal}(K/\mathbb{Q})$, by Theorem 11.23, so $K_\mathfrak{p}$ is an abelian extension of $\mathbb{Q}_\mathfrak{p}$ and the local Kronecker-Weber theorem implies that $K_\mathfrak{p} \subseteq \mathbb{Q}_p(\zeta_{m_p})$ for some $m_p \in \mathbb{Z}_{\geq 1}$. Let $n_p := v_p(m_p)$, put $m := \prod_p p^{n_p}$ (this is a finite product), and let $L = K(\zeta_m)$. We will show $L = \mathbb{Q}(\zeta_m)$, which implies $K \subseteq \mathbb{Q}(\zeta_m)$.

The field $L = K \cdot \mathbb{Q}(\zeta_m)$ is a compositum of Galois extensions of $\mathbb{Q}$, and is therefore Galois over $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q})$ isomorphic to a subgroup of $\mathrm{Gal}(K/\mathbb{Q})\times\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, hence abelian (as recalled below, the Galois group of a compositum $K_1\cdots K_r$ of Galois extensions K_i/F is isomorphic to a subgroup of the direct product of the $\mathrm{Gal}(K_i/F)$). Let $\mathfrak{q}$ be a prime of L lying above a ramified prime $\mathfrak{p}|p$; as above, the completion $L_\mathfrak{q}$ of L at $\mathfrak{q}$ is a finite abelian extension of $\mathbb{Q}_p$, since $L/\mathbb{Q}$ is finite abelian, and we have $L_\mathfrak{q} = K_\mathfrak{p}\cdot\mathbb{Q}_p(\zeta_m)$. Let $F_\mathfrak{q}$ be the maximal unramified extension of $\mathbb{Q}_p$ in $L_\mathfrak{q}$. Then $L_\mathfrak{q}/F_\mathfrak{q}$ is totally ramified and $\mathrm{Gal}(L_{\mathfrak{q}}/F_{\mathfrak{q}})$ is isomorphic to the inertia group $I_p := I_{\mathfrak{q}} \subseteq \mathrm{Gal}(L/\mathbb{Q})$, by Theorem 11.23 (the $I_{\mathfrak{q}}$ all coincide because $L/\mathbb{Q}$ is abelian).

It follows from Corollary 10.20 that $K_{\mathfrak{p}} \subseteq F_{\mathfrak{q}}(\zeta_{p^{n_p}})$, since $K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_{m_p})$ and $\mathbb{Q}_p(\zeta_{m_p/p^{n_p}})$ is unramified, and that $L_{\mathfrak{q}} = F_{\mathfrak{q}}(\zeta_{p^{n_p}})$, since $\mathbb{Q}_p(\zeta_{m/p^{n_p}})$ is unramified. Moreover, we have $F_{\mathfrak{q}} \cap \mathbb{Q}_p(\zeta_{p^{n_p}}) = \mathbb{Q}_p$, since $\mathbb{Q}_p(\zeta_{p^{n_p}})/\mathbb{Q}_p$ is totally ramified, and it follows that

$$I_p \simeq \mathrm{Gal}(L_{\mathfrak{q}}/F_{\mathfrak{q}}) \simeq \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n_p}})/\mathbb{Q}_p) \simeq (\mathbb{Z}/p^{n_p}\mathbb{Z})^\times.$$

Now let I be the group generated by the union of the groups $I_p \subseteq \mathrm{Gal}(L/\mathbb{Q})$ for $p|m$. Since $\mathrm{Gal}(L/\mathbb{Q})$ is abelian, we have $\bigcup I_p \subseteq \prod I_p$, thus

$$\#I \le \prod_{p|m} \#I_p = \prod_{p|m} \#(\mathbb{Z}/p^{n_p}\mathbb{Z})^\times = \prod_{p|m} \phi(p^{n_p}) = \phi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}].$$

Each inertia field L^{I_p} is unramified at p (see Proposition 7.12), as is $L^I \subseteq L^{I_p}$. So $L^I/\mathbb{Q}$ is unramified, and therefore $L^I = \mathbb{Q}$, by Corollary 14.25. Thus

$$[L : \mathbb{Q}] = [L : L^I] = \#I \le [\mathbb{Q}(\zeta_m) : \mathbb{Q}],$$

and $\mathbb{Q}(\zeta_m) \subseteq L$, so $L = \mathbb{Q}(\zeta_m)$ as claimed and $K \subseteq L = \mathbb{Q}(\zeta_m)$. $\square$

To prove the local Kronecker-Weber theorem we first reduce to the case of cyclic extensions of prime-power degree. Recall that if L_1 and L_2 are two Galois extensions of a field K then their compositum $L \coloneqq L_1L_2$ is Galois over K with Galois group

$$\mathrm{Gal}(L/K) \simeq \{(\sigma_1, \sigma_2) : \sigma_1|_{L_1\cap L_2} = \sigma_2|_{L_1\cap L_2}\} \subseteq \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K).$$

The inclusion on the RHS is an equality if and only if $L_1 \cap L_2 = K$. Conversely, if $\mathrm{Gal}(L/K) \simeq H_1 \times H_2$ then by defining $L_2 := L^{H_1}$ and $L_1 := L^{H_2}$ we have $L = L_1L_2$ with $L_1 \cap L_2 = K$, and $\mathrm{Gal}(L_1/K) \simeq H_1$ and $\mathrm{Gal}(L_2/K) \simeq H_2$.

It follows from the structure theorem for finite abelian groups that we may decompose any finite abelian extension L/K into a compositum $L = L_1 \cdots L_n$ of linearly disjoint cyclic extensions L_i/K of prime-power degree. If each L_i lies in a cyclotomic field $\mathbb{Q}(\zeta_{m_i})$, then so does L. Indeed, $L \subseteq \mathbb{Q}(\zeta_{m_1}) \cdots \mathbb{Q}(\zeta_{m_n}) = \mathbb{Q}(\zeta_m)$, where $m \coloneqq m_1 \cdots m_n$.

To prove the local Kronecker-Weber theorem it thus suffices to consider cyclic extensions $K/\mathbb{Q}_p$ of prime power degree ℓ^r. There two distinct cases: $\ell \ne p$ and $\ell = p$.

20.2 The local Kronecker-Weber theorem for $\ell \neq p$

Proposition 20.4. *Let $K/\mathbb{Q}_p$ be a cyclic extension of degree ℓ^r for some prime $\ell \ne p$. Then K lies in a cyclotomic field $\mathbb{Q}_p(\zeta_m)$.*

Proof. Let F be the maximal unramified extension of $\mathbb{Q}_p$ in K; then $F = \mathbb{Q}_p(\zeta_n)$ for some $n \in \mathbb{Z}_{\ge 1}$, by Corollary 10.19. The extension K/F is totally ramified, and it must be tamely ramified, since the ramification index is a power of $\ell \ne p$. By Theorem 11.10, we have $K = F(\pi^{1/e})$ for some uniformizer π, with $e = [K : F]$. We may assume that $\pi = -pu$ for some $u \in \mathcal{O}_F^\times$, since $F/\mathbb{Q}_p$ is unramified: if $\mathfrak{q}|p$ is the maximal ideal of $\mathcal{O}_F$ then the valuation $v_{\mathfrak{q}}$ extends v_p with index $e_{\mathfrak{q}} = 1$ (by Theorem 8.20), so $v_{\mathfrak{q}}(-pu) = v_p(-p) = 1$. The field $K = F(\pi^{1/e})$ lies in the compositum of $F((-p)^{1/e})$ and $F(u^{1/e})$, and we will show that both fields lie in a cyclotomic extension of $\mathbb{Q}_p$.

The extension $F(u^{1/e})/F$ is unramified, since $v_{\mathfrak{q}}(\operatorname{disc}(x^e - u)) = 0$ for $p \nmid e$, so $F(u^{1/e})/\mathbb{Q}_p$ is unramified and $F(u^{1/e}) = \mathbb{Q}_p(\zeta_k)$ for some $k \in \mathbb{Z}_{\geq 1}$. The field $K(u^{1/e}) = K \cdot \mathbb{Q}_p(\zeta_k)$ is a compositum of abelian extensions, so $K(u^{1/e})/\mathbb{Q}_p$ is abelian, and it contains the subextension $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$, which must be Galois (since it lies in an abelian extension) and totally ramified (by Theorem 11.5, since it is an Eisenstein extension). The field $\mathbb{Q}_p((-p)^{1/e})$ contains ζ_e (take ratios of roots of $x^e + p$) and is totally ramified, but $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$ is unramified (since $p \nmid e$), so we must have $\mathbb{Q}_p(\zeta_e) = \mathbb{Q}_p$. Thus $e|(p-1)$, and by Lemma 20.5 below,

$$\mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p).$$

It follows that $F((-p)^{1/e}) = F \cdot \mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p(\zeta_n) \cdot \mathbb{Q}_p(\zeta_p) \subseteq \mathbb{Q}_p(\zeta_{np})$. We then have $K \subseteq F(u^{1/e}) \cdot F((-p)^{1/e}) \subseteq \mathbb{Q}(\zeta_k) \cdot \mathbb{Q}(\zeta_{np}) \subseteq \mathbb{Q}(\zeta_{knp})$ and may take $m = knp$. $\square$

Lemma 20.5. *For any prime p we have $\mathbb{Q}_p\big((-p)^{1/(p-1)}\big) = \mathbb{Q}_p(\zeta_p)$.*

Proof. Let $\alpha = (-p)^{1/(p-1)}$. Then α is a root of the Eisenstein polynomial $x^{p-1} + p$, so the extension $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\alpha)$ is totally ramified of degree $p-1$, and α is a uniformizer (by Lemma 11.4 and Theorem 11.5). Let $\pi = \zeta_p - 1$. The minimal polynomial of π is

$$f(x) := \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \cdots + p,$$

which is Eisenstein, so $\mathbb{Q}_p(\pi) = \mathbb{Q}_p(\zeta_p)$ is also totally ramified of degree $p-1$, and π is a uniformizer. We have $u := -\pi^{p-1}/p \equiv 1 \bmod \pi$, so u is a unit in the ring of integers of $\mathbb{Q}_p(\zeta_p)$. If we now put $g(x) = x^{p-1} - u$ then $g(1) \equiv 0 \bmod \pi$ and $g'(1) = p - 1 \not\equiv 0 \bmod \pi$, so by Hensel's Lemma 9.15 we can lift 1 to a root β of $g(x)$ in $\mathbb{Q}_p(\zeta_p)$.

We then have $p\beta^{p-1} = pu = -\pi^{p-1}$, so $(\pi/\beta)^{p-1} + p = 0$, and therefore $\pi/\beta \in \mathbb{Q}_p(\zeta_p)$ is a root of the minimal polynomial of α. Since $\mathbb{Q}_p(\zeta_p)$ is Galois, this implies that $\alpha \in \mathbb{Q}_p(\zeta_p)$, and since $\mathbb{Q}_p(\alpha)$ and $\mathbb{Q}_p(\zeta_p)$ both have degree $p-1$, the two fields coincide. $\square$

To complete the proof of the local Kronecker-Weber theorem, we need to address the case $\ell = p$. Before doing so, we first recall some background on Kummer extensions.

20.3 A brief introduction to Kummer theory

Let n be a positive integer and let K be a field of characteristic prime to n that contains a primitive nth root of unity ζ_n. While we are specifically interested in the case where K is a local or global field, in this section K can be any field that satisfies these conditions.

For any $a \in K$, the field $L = K(\sqrt[n]{a})$ is the splitting field of $f(x) = x^n - a$ over K; the notation $\sqrt[n]{a}$ denotes a particular nth root of a, but it does not matter which root we pick because all the nth roots of a lie in L (if $f(\alpha) = f(\beta) = 0$ then $\alpha/\beta \in \zeta_n^i \in K$ for some $0 \leq i < n$ and $K(\alpha) = K(\beta)$). The polynomial $f(x)$ is separable, since n is prime to the characteristic of K, so L is a Galois extension of K, and $\operatorname{Gal}(L/K)$ is cyclic, since we have an injective homomorphism

$$\begin{aligned} \operatorname{Gal}(L/K) &\hookrightarrow \langle \zeta_n \rangle \simeq \mathbb{Z}/n\mathbb{Z} \\ \sigma &\mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}. \end{aligned}$$

This homomorphism is an isomorphism if and only if $x^n - a$ is irreducible.

Kummer's key observation is that the converse holds. In order to prove this we first recall a basic (but often omitted) lemma from Galois theory, originally due to Dedekind.

Lemma 20.6. *Let L/K be a finite extension of fields. The set $\operatorname{Aut}_K(L)$ is a linearly independent subset of the L-vector space of functions $L \to L$.*

Proof. Suppose not. Let $f := c_1\sigma_1 + \cdots + c_r\sigma_r = 0$ with $c_i \in L$, $\sigma_i \in \operatorname{Aut}_K(L)$, and r minimal; we must have $r > 1$, the c_i nonzero, and the σ_i distinct. Choose $\alpha \in L$ so $\sigma_1(\alpha) \neq \sigma_r(\alpha)$ (possible since $\sigma_1 \neq \sigma_r$). We have $f(\beta) = 0$ for all $\beta \in L$, and the same applies to $f(\alpha\beta) - \sigma_1(\alpha)f(\beta)$, which yields a shorter relation $c_2'\sigma_2 + \cdots + c_r'\sigma_r = 0$, where $c_i' = c_i\sigma_i(\alpha) - c_i\sigma_1(\alpha)$ with $c_1' = 0$, which is nontrivial because $c_r' \neq 0$, a contradiction. $\square$

Corollary 20.7. *Let L/K be a cyclic field extension of degree n with Galois group $\langle\sigma\rangle$ and suppose L contains an nth root of unity ζ_n. Then $\sigma(\alpha) = \zeta_n\alpha$ for some $\alpha \in L$.*

Proof. The automorphism σ is a linear transformation of L with characteristic polynomial $x^n - 1$; by Lemma 20.6, this must be its minimal polynomial, since $\{1, \sigma^1, \ldots, \sigma^{n-1}\}$ is linearly independent. Therefore ζ_n is eigenvalue of σ, and the lemma follows. $\square$

Remark 20.8. Corollary 20.7 is a special case of HILBERT'S THEOREM 90, which replaces ζ_n with any element u of norm $\mathrm{N}_{L/K}(u) = 1$; see [4, Thm. VI.6.1], for example.

Lemma 20.9. *Let K be a field, let $n \geq 1$ be prime to the characteristic of K, and assume $\zeta_n \in K$. If L/K is a cyclic extension of degree n then $L = K(\sqrt[n]{a})$ for some $a \in K$.*

Proof. Let L/K be a cyclic extension of degree n with $\operatorname{Gal}(L/K) = \langle\sigma\rangle$. By Corollary 20.7, there exists an element $\alpha \in L$ for which $\sigma(\alpha) = \zeta_n\alpha$. We have

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta_n\alpha)^n = \alpha^n,$$

thus $a = \alpha^n$ is invariant under the action of $\langle\sigma\rangle = \operatorname{Gal}(L/K)$ and therefore lies in K. Moreover, the orbit $\{\alpha, \zeta_n\alpha, \ldots, \zeta_n^{n-1}\alpha\}$ of α under the action of $\operatorname{Gal}(L/K)$ has order n, so $L = K(\alpha) = K(\sqrt[n]{a})$ as desired. $\square$

Definition 20.10. Let K be a field with algebraic closure $\overline{K}$, let $n \geq 1$ be prime to the characteristic of K, and assume $\zeta_n \in K$. The *Kummer pairing* is the map

$$\begin{aligned}\langle\cdot,\cdot\rangle\colon \operatorname{Gal}(\overline{K}/K) \times K^\times &\to \langle\zeta_n\rangle\\ (\sigma, a) &\mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\end{aligned}$$

where $\sqrt[n]{a}$ is any nth root of a in $\in \overline{K}^\times$. If α and β are two nth roots of a, then $(\alpha/\beta)^n = 1$, so $\alpha/\beta \in \langle\zeta_n\rangle \subseteq K$ is fixed by σ and $\sigma(\beta)/\beta = \sigma(\beta)/\beta \cdot \sigma(\alpha/\beta)/(\alpha/\beta) = \sigma(\alpha)/\alpha$, so the value of $\langle\sigma, a\rangle$ does not depend on the choice of $\sqrt[n]{a}$. If $a \in K^{\times n}$, then $\langle\sigma, a\rangle = 1$ for all $\sigma \in \operatorname{Gal}(\overline{K}/K)$, so the Kummer pairing depends only on the image of a in $K^\times/K^{\times n}$; thus we may also view it as a pairing on $\operatorname{Gal}(\overline{K}/K) \times K^\times/K^{\times n}$.

Theorem 20.11. *Let K be a field, let $n \geq 1$ be prime to the characteristic of K with $\zeta_n \in K$. The Kummer pairing induces an isomorphism*

$$\begin{aligned}\Phi\colon K^\times/K^{\times n} &\to \operatorname{Hom}\bigl(\operatorname{Gal}(\overline{K}/K), \langle\zeta_n\rangle\bigr)\\ a &\mapsto \bigl(\sigma \mapsto \langle\sigma, a\rangle\bigr).\end{aligned}$$

Proof. For each $a \in K^\times - K^{\times n}$, if we pick an nth root $\alpha \in \overline{K}$ of a then the extension $K(\alpha)/K$ will be non-trivial and some $\sigma \in \operatorname{Gal}(\overline{K}/K)$ must act nontrivially on α. For this σ we have $\langle \sigma, a\rangle \neq 1$, so $a \notin \ker \Phi$; thus Φ is injective.

Now let $f\colon \operatorname{Gal}(\overline{K}/K) \to \langle \zeta_n\rangle$ be a homomorphism, and put $d := \#\operatorname{im} f$, $H := \ker f$, and $L := \overline{K}^H$. Then $\operatorname{Gal}(L/K) \simeq \operatorname{Gal}(\overline{K}/K)/H \simeq \mathbb{Z}/d\mathbb{Z}$, so L/K is a cyclic extension of degree d, and Lemma 20.9 implies that $L = K(\sqrt[d]{a})$ for some $a \in K$. If we put $e = n/d$ and consider the homomorphisms $\Phi(a^{me})$ for $m \in (\mathbb{Z}/d\mathbb{Z})^\times$, these homomorphisms are all distinct (because the a^{me} are distinct modulo $K^{\times n}$ and Φ is injective), and they all have the same kernel and image as f (their kernels have the same fixed field L because L contains all the dth roots of a). There are $\#(\mathbb{Z}/d\mathbb{Z})^\times = \#\operatorname{Aut}(\mathbb{Z}/d\mathbb{Z})$ distinct isomorphisms $\operatorname{Gal}(\overline{K}/K)/H \simeq \mathbb{Z}/d\mathbb{Z}$, one of which corresponds to f, and each corresponds to one of the $\Phi(a^{me})$. It follows that $f = \Phi(a^{me})$ for some $m \in (\mathbb{Z}/d\mathbb{Z})^\times$, thus Φ is surjective. $\square$

Given a finite subgroup A of $K^\times/K^{\times n}$, we can choose $a_1, \ldots, a_r \in K^\times$ so that the images $\bar{a}_i$ of the a_i in $K^\times/K^{\times n}$ form a basis for the abelian group A; this means

$$A = \langle \bar{a}_1\rangle \times \cdots \times \langle \bar{a}_r\rangle \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z},$$

where $n_i | n$ is the order of $\bar{a}_i$ in A. For each a_i, the fixed field of the kernel of $\Phi(\bar{a}_i)$ is a cyclic extension of K isomorphic to $L_i := K(\sqrt[n_i]{a_i})$, as in the proof of Theorem 20.11. The fields L_i are linearly disjoint over K (because the a_i correspond to independent generators of A), and their compositum $L = K(\sqrt[n_1]{a_1}, \ldots \sqrt[n_r]{a_r})$ has Galois group $\operatorname{Gal}(L/K) \simeq A$, an abelian group whose exponent divides n; such fields L are called *n-Kummer extensions* of K.

Conversely, given an n-Kummer extension L/K, we can iteratively apply Lemma 20.9 to put L in the form $L = K(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r})$ with each $a_i \in K^\times$ and $n_i | n$, and the images of the a_i in $K^\times/K^{\times n}$ then generate a subgroup A corresponding to L as above. We thus have a 1-to-1 correspondence between finite subgroups of $K^\times/K^{\times n}$ and (finite) n-Kummer extensions of K (this correspondence also extends to infinite subgroups provided we put a suitable topology on the groups).

So far we have been assuming that K contains all the nth roots of unity. To help handle situations where this is not necessarily the case, we rely on the following lemma.

Lemma 20.12. *Fix $n \in \mathbb{Z}_{>1}$, let F be a field of characteristic prime to n, let $K = F(\zeta_n)$, and let $L = K(\sqrt[n]{a})$ for some $a \in K^\times$. Define the homomorphism $\omega\colon \operatorname{Gal}(K/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ by $\zeta_n^{\omega(\sigma)} = \sigma(\zeta_n)$. If L/F is abelian then $\sigma(a)/a^{\omega(\sigma)} \in K^{\times n}$ for all $\sigma \in \operatorname{Gal}(K/F)$.*

Proof. Let $G = \operatorname{Gal}(L/F)$, let $H = \operatorname{Gal}(L/K) \subseteq G$, and let A be the subgroup of $K^\times/K^{\times n}$ generated by a. The Kummer pairing induces a bilinear pairing $H \times A \to \langle \zeta_n\rangle$ that is compatible with the Galois action of $\operatorname{Gal}(K/F) \simeq G/H$. In particular, we have

$$\langle h, a^{\omega(\sigma)}\rangle = \langle h, a\rangle^{\omega(\sigma)} = \sigma(\langle h, a\rangle) = \langle h^\sigma, \sigma(a)\rangle = \langle h, \sigma(a)\rangle$$

for all $\sigma \in \operatorname{Gal}(K/F)$ and $h \in H$; the Galois action on H is by conjugation (lift σ to G and conjugate there), but it is trivial because G is abelian (so $h^\sigma = h$). The isomorphism Φ induced by the Kummer pairing is injective, so $a^{\omega(\sigma)} \equiv \sigma(a) \bmod K^{\times n}$. $\square$

20.4 The local Kronecker-Weber theorem for $\ell = p > 2$

We are now ready to prove the local Kronecker-Weber theorem in the case $\ell = p > 2$.

Theorem 20.13. *Let $K/\mathbb{Q}_p$ be a cyclic extension of odd degree p^r. Then K lies in a cyclotomic field $\mathbb{Q}_p(\zeta_m)$.*

Proof. There are two obvious candidates for K, namely, the cyclotomic field $\mathbb{Q}_p(\zeta_{p^{p^r}-1})$, which by Corollary 10.19 is an unramified extension of degree p^r, and the index $p-1$ subfield of the cyclotomic field $\mathbb{Q}_p(\zeta_{p^{r+1}})$, which by Corollary 10.20 is a totally ramified extension of degree p^r (the p^{r+1}-cyclotomic polynomial $\Phi_{p^{r+1}}(x)$ has degree $\phi(p^{r+1}) = p^r(p-1)$ and remains irreducible over $\mathbb{Q}_p$). If K is contained in the compositum of these two fields then $K \subseteq \mathbb{Q}_p(\zeta_m)$, where $m := (p^{p^r}-1)(p^{r+1})$ and the theorem holds. Otherwise, the field $K(\zeta_m)$ is a Galois extension of $\mathbb{Q}_p$ with

$$\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_p) \simeq \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z},$$

for some $s > 0$; the first factor comes from the Galois group of $\mathbb{Q}_p(\zeta_{p^{p^r}-1})$, the second two factors come from the Galois group of $\mathbb{Q}_p(\zeta_{p^{r+1}})$ (note $\mathbb{Q}_p(\zeta_{p^{r+1}}) \cap \mathbb{Q}_p(\zeta_{p^{p^r}-1}) = \mathbb{Q}_p$), and the last factor comes from the fact that we are assuming $K \not\subseteq \mathbb{Q}_p(\zeta_m)$, so $\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_p(\zeta_m))$ is nontrivial and must have order p^s for some $s \in [1, r]$.

It follows that the abelian group $\mathrm{Gal}(K(\zeta_m)/\mathbb{Q}_p)$ has a quotient isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$, and the subfield of $K(\zeta_m)$ corresponding to this quotient is an abelian extension of $\mathbb{Q}_p$ with Galois group isomorphic $(\mathbb{Z}/p\mathbb{Z})^3$. By Lemma 20.14 below, no such field exists. $\square$

To prove that $\mathbb{Q}_p$ admits no $(\mathbb{Z}/p\mathbb{Z})^3$-extensions our strategy is to use Kummer theory to show that the corresponding subgroup of $\mathbb{Q}_p(\zeta_p)^\times/\mathbb{Q}_p(\zeta_p)^{\times p}$ given by Theorem 20.11 must have p-rank 2 and therefore cannot exist. For an alternative proof that uses higher ramification groups instead of Kummer theory, see Problem Set 10.

Lemma 20.14. *For $p > 2$ no extension of $\mathbb{Q}_p$ has Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$.*

Proof. Suppose for the sake of contradiction that K is an extension of $\mathbb{Q}_p$ with Galois group $\mathrm{Gal}(K/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^3$. Then $K/\mathbb{Q}_p$ is linearly disjoint from $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$, since the order of $G := \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ is not divisible by p, and $\mathrm{Gal}(K(\zeta_p)/\mathbb{Q}_p(\zeta_p)) \simeq (\mathbb{Z}/p\mathbb{Z})^3$ is a p-Kummer extension. There is thus a subgroup $A \subseteq \mathbb{Q}_p(\zeta_p)^\times/\mathbb{Q}_p(\zeta_p)^{\times p}$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$, for which $K(\zeta_p) = \mathbb{Q}_p(\zeta_p, A^{1/p})$, where $A^{1/p} := \{\sqrt[p]{a} : a \in A\}$ (here we identify elements of A by representatives in $\mathbb{Q}_p(\zeta_p)^\times$ that are determined only up to pth powers).

For any $a \in A$, the extension $\mathbb{Q}_p(\zeta_p, \sqrt[p]{a})/\mathbb{Q}_p$ is abelian, so by Lemma 20.12, we have

$$\sigma(a)/a^{\omega(\sigma)} \in \mathbb{Q}_p(\zeta_p)^{\times p} \tag{1}$$

for all $\sigma \in G$, where $\omega\colon G \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times$ is the isomorphism defined by $\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}$.

The field $\mathbb{Q}_p(\zeta_p)$ is a totally tamely ramified extension of $\mathbb{Q}_p$ of degree $p-1$ with residue field $\mathbb{Z}/p\mathbb{Z}$; as shown in the proof of Lemma 20.5, we may take $\pi := \zeta_p - 1$ as a uniformizer. For each $a \in A$ we have

$$v_\pi(a) = v_\pi(\sigma(a)) \equiv \omega(\sigma)v_\pi(a) \bmod p,$$

thus $(1-\omega(\sigma))v_\pi(a) \equiv 0 \bmod p$, for all $\sigma \in G$, hence for all $\omega(\sigma) \in \omega(G) = (\mathbb{Z}/p\mathbb{Z})^\times$; for $p > 2$, this implies $v_\pi(a) \equiv 0 \bmod p$. Now a is determined only up to pth-powers, so after multiplying by $\pi^{-v_\pi(a)}$ we may assume $v_\pi(a) = 0$, and after multiplying by a suitable power of $\zeta_{p-1}^p = \zeta_{p-1}$, we may assume $a \equiv 1 \bmod \pi$, since the image of ζ_{p-1} generates the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of the residue field.

We may thus assume that $A \subseteq U_1/U_1^p$, where $U_1 := \{u \equiv 1 \bmod \pi\}$. Each $u \in U_1$ can be written as a power series in π with integer coefficients in $[0, p-1]$ and constant coefficient 1.

We have $\zeta_p \in U_1$, since $\zeta_p = 1 + \pi$, and $\zeta_p^b = 1 + b\pi + O(\pi^2)$ for integers $b \in [0, p-1]$.[1] For $a \in A \subseteq U_1$, we can choose b so that for some integer $c \in [0, p-1]$ and $e \in \mathbb{Z}_{\geq 2}$ we have

$$a = \zeta_p^b(1 + c\pi^e + O(\pi^{e+1})).$$

For $\sigma \in G$ we have

$$\frac{\sigma(\pi)}{\pi} = \frac{\sigma(\zeta_p - 1)}{\zeta_p - 1} = \frac{\zeta_p^{\omega(\sigma)} - 1}{\zeta_p - 1} = \zeta_p^{\omega(\sigma)-1} + \cdots + \zeta_p + 1 \equiv \omega(\sigma) \bmod \pi,$$

since each term in the sum is congruent to 1 modulo $\pi = (\zeta_p - 1)$; here we are representing $\omega(\sigma) \in (\mathbb{Z}/p\mathbb{Z})^\times$ as an integer in $[1, p-1]$. Thus $\sigma(\pi) \equiv \omega(\sigma)\pi \bmod \pi^2$ and

$$\sigma(a) = \zeta_p^{b\omega(\sigma)}(1 + c\omega(\sigma)^e\pi^e + O(\pi^{e+1})).$$

We also have

$$a^{\omega(\sigma)} = \zeta_p^{b\omega(\sigma)}(1 + c\omega(\sigma)\pi^e + O(\pi^{e+1})).$$

As we showed for a above, any $u \in U_1$ can be written as $u = \zeta_p^b u_1$ with $u_1 \equiv 1 \bmod \pi^2$. Each interior term in the binomial expansion of $u_1^p = (1 + O(\pi^2))^p$ other than leading 1 is a multiple of $p\pi^2$ with $v_\pi(p\pi^2) = p - 1 + 2 = p + 1$, and it follows that $u^p = u_1^p \equiv 1 \bmod \pi^{p+1}$. Thus every element of U_1^p is congruent to 1 modulo π^{p+1}, and as you will show on the problem set, the converse holds, that is, $U_1^p = \{u \equiv 1 \bmod \pi^{p+1}\}$.

We know from (1) that $\sigma(a)/a^{\omega(\sigma)} \in U_1^p$, so $\sigma(a) = a^{\omega(\sigma)}(1 + O(\pi^{p+1}))$ and therefore

$$\sigma(a) \equiv a^{\omega(\sigma)} \bmod \pi^{p+1}.$$

For $e \leq p$ this is possible only if $\omega(\sigma) = \omega(\sigma)^e$ for every $\sigma \in G$, equivalently, for every $\omega(\sigma) \in \sigma(G) = (\mathbb{Z}/p\mathbb{Z})^\times$, but then $e \equiv 1 \bmod (p-1)$ and we must have $e \geq p$, since $e \geq 2$.

We have shown that every $a \in A$ is represented by an element $\zeta_p^b(1 + c\pi^p + O(\pi^{p+1})) \in U_1$ with $b, c \in \mathbb{Z}$, and therefore lies in the subgroup of U_1/U_1^p generated by ζ_p and $(1 + \pi^p)$, which is an abelian group of exponent p generated by 2 elements, hence isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^2$. But this contradicts $A \simeq (\mathbb{Z}/p\mathbb{Z})^3$. $\square$

Remark 20.15. In the proof of Lemma 20.14 above, the elements of $\mathbb{Q}_p(\zeta_p)^\times/\mathbb{Q}_p(\zeta_p)^{\times p}$ that lie in A are quite special. For most $a \in \mathbb{Q}_p(\zeta_p)^\times$ the extension $\mathbb{Q}_p(\zeta_p, \sqrt[p]{a})/\mathbb{Q}_p$ will not be abelian, even though the extensions $\mathbb{Q}_p(\sqrt[p]{a})/\mathbb{Q}_p(\zeta_p)$ and $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ both are, and we typically will not have $v_\pi(a) \equiv 0 \bmod p$ (consider $a = \pi$). The key point is that we started with an abelian extension $K/\mathbb{Q}_p$, so $K(\zeta_p) = K \cdot \mathbb{Q}_p(\zeta_p)$ is an abelian extension containing $A^{1/p}$; this ensures that for $a \in A$ the fields $\mathbb{Q}_p(\zeta_p, \sqrt[p]{a})$ are abelian.

Remark 20.16. There is an alternative proof to Lemma 20.14 that is much more explicit. One can show that for $p > 2$ the field $\mathbb{Q}_p$ admits exactly $p + 1$ cyclic extensions of degree p: the unramified extension $\mathbb{Q}_p(\zeta_{p^p - 1})$ and the extensions $\mathbb{Q}_p[x]/(x^p + px^{p-1} + p(1 + ap))$, for integers $a \in [0, p-1]$; see [3, Prop. 2.3.1]. This implies that $\mathbb{Q}_p$ cannot have a $(\mathbb{Z}/p\mathbb{Z})^3$ extension, since this would imply the existence of $p^2 + p + 1$ cyclic extensions of degree p, one for each index p subgroup of $(\mathbb{Z}/p\mathbb{Z})^3$.

[1] The expression $O(\pi^n)$ denotes a power series in π that is divisible by π^n.

For $p = 2$ there is an extension of $\mathbb{Q}_2$ with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$, the cyclotomic field $\mathbb{Q}_2(\zeta_{24}) = \mathbb{Q}_2(\zeta_3) \cdot \mathbb{Q}_2(\zeta_8)$, so the proof we used for $p > 2$ will not work. However we can apply a completely analogous argument.

Theorem 20.17. *Let $K/\mathbb{Q}_2$ be a cyclic extension of degree 2^r. Then K lies in a cyclotomic field $\mathbb{Q}_2(\zeta_m)$.*

Proof. The unramified cyclotomic field $\mathbb{Q}_2(\zeta_{2^{2^r}-1})$ has Galois group $\mathbb{Z}/2^r\mathbb{Z}$, and the totally ramified cyclotomic field $\mathbb{Q}_2(\zeta_{2^{r+2}})$ has Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$ (up to isomorphism). Let $m = (2^{2^r} - 1)(2^{r+2})$. If K is not contained in $\mathbb{Q}_2(\zeta_m)$ then

$$\operatorname{Gal}(K(\zeta_m)/\mathbb{Q}_2) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^r\mathbb{Z})^2 \times \mathbb{Z}/2^s\mathbb{Z} & \text{with } 1 \le s \le r \\ \text{or} & \\ (\mathbb{Z}/2^r\mathbb{Z})^2 \times \mathbb{Z}/2^s\mathbb{Z} & \text{with } 2 \le s \le r \end{cases}$$

and thus admits a quotient isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^3$. By Lemma 20.18 below, no extension of $\mathbb{Q}_2$ has either of these Galois groups, thus K must lie in $\mathbb{Q}_2(\zeta_m)$. $\square$

Lemma 20.18. *No extension of $\mathbb{Q}_2$ has Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^3$.*

Proof. As you proved on Problem Set 4, there are exactly 7 quadratic extensions of $\mathbb{Q}_2$; it follows that no extension of $\mathbb{Q}_2$ has Galois group $(\mathbb{Z}/2\mathbb{Z})^4$, since this group has 15 subgroups of index 2 whose fixed fields would yield 15 distinct quadratic extension of $\mathbb{Q}_2$.

As you proved on Problem Set 5, there are only finitely many extensions of $\mathbb{Q}_2$ of any fixed degree d, and these can be enumerated by considering Eisenstein polynomials in $\mathbb{Q}_2[x]$ of degrees dividing d up to an equivalence relation implied by Krasner's lemma. One finds that there are 59 quartic extensions of $\mathbb{Q}_2$, of which 12 are cyclic; you can find a list of them here. It follows that no extension of $\mathbb{Q}_2$ has Galois group $(\mathbb{Z}/4\mathbb{Z})^3$, since this group has 28 subgroups whose fixed fields would yield 28 distinct cyclic quartic extensions of $\mathbb{Q}_2$. $\square$

References

[1] David Hilbert, *Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klass (1896), 29–39.

[2] Leopold Kronecker, *Uber die algebraisch auflösbaren Gleichungen I* (1853), in *Leopold Kronecker's Werke, Part 4* (ed. K. Hensel), AMS Chelsea Publishing, 1968.

[3] John W. Jones and David P. Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), 80–97.

[4] Serge Lang, *Algebra*, 3rd edition, Springer, 2002.

[5] Olaf Neumann, *Two proofs of the Kronecker-Weber theorem "according to Kronecker, and Weber"*, J. Reine Angew. Math. **323** (1981),105–126.

[6] Lawrence C. Washington, *Introduction to cyclotomic fields*, 2nd edition, Springer, 1997.

[7] Heinrich M. Weber, *Theorie der Abel'schen Zahlkörper*, Acta Mathematica **8** (1886), 193–263.