

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 $\text{Gal}(K/\mathbb{Q})$ 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 $\text{Gal}(K/\mathbb{Q})$ 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 $\text{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p) \simeq D_{\mathfrak{p}} \subseteq \text{Gal}(K/\mathbb{Q})$, by Theorem 11.23, so $K_{\mathfrak{p}}$ is an abelian extension of \mathbb{Q}_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 $L = \mathbb{Q}(\zeta_m)$. 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 $\text{Gal}(L/\mathbb{Q})$ isomorphic to a subgroup of $\text{Gal}(K/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, 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 $\text{Gal}(K_i/F)$). 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

$\text{Gal}(L_{\mathfrak{q}}/F_{\mathfrak{q}})$ is isomorphic to the inertia group $I_p := I_{\mathfrak{q}} \subseteq \text{Gal}(L/\mathbb{Q})$, by Theorem 11.23 (the $I_{\mathfrak{q}}$ all coincide because L/\mathbb{Q} is abelian).

It follows from Corollary 10.18 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

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

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

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

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 14.27. Thus

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

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 $L := L_1L_2$ is Galois over K with Galois group

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

The inclusion on the RHS is an equality if and only if $L_1 \cap L_2 = K$. Conversely, if $\text{Gal}(L/K) \simeq H_1 \times H_2$ 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 $\text{Gal}(L_1/K) \simeq H_1$ and $\text{Gal}(L_2/K) \simeq H_2$.

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 extension $K(\zeta_{m_i})$, then so does L . Indeed, $L \subseteq K(\zeta_{m_1}) \cdots K(\zeta_{m_n}) = K(\zeta_m)$, where $m := m_1 \cdots m_n$.

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: $\ell \neq p$ 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 $\ell \neq p$. 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 $n \in \mathbb{Z}_{\geq 1}$, by Corollary 10.17. The extension K/F is totally ramified, and it must be tamely ramified, since the ramification index is a power of $\ell \neq p$. 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 $v_q(\text{disc}(x^e - u)) = 0$ 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 $e \mid (p-1)$, 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 $K \subseteq F(u^{1/e}) \cdot F((-p)^{1/e}) \subseteq \mathbb{Q}_p(\zeta_k) \cdot \mathbb{Q}_p(\zeta_{np}) \subseteq \mathbb{Q}_p(\zeta_{knp})$ and may take $m = knp$. \square

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

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 $u := -\pi^{p-1}/p \equiv 1 \pmod{\pi}$, 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 $g(1) \equiv 0 \pmod{\pi}$ and $g'(1) = p-1 \not\equiv 0 \pmod{\pi}$, 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

20.3 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 20.6. *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 10.17 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 10.18 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

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

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 $\text{Gal}(K(\zeta_m)/\mathbb{Q}_p(\zeta_m))$ is nontrivial and must have order p^s with $1 \leq s \leq r$.

It follows that the abelian group $\text{Gal}(K(\zeta_m)/\mathbb{Q}_p)$ 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 $(\mathbb{Z}/p\mathbb{Z})^3$. By Proposition 20.7 below, no such field exists. \square

Proposition 20.7. *For odd p every totally wildly ramified Galois extension of \mathbb{Q}_p is cyclic. In particular, there is no abelian extension of \mathbb{Q}_p with Galois group $(\mathbb{Z}/p\mathbb{Z})^3$ when p is odd.*

Proof. See Problem Set 10 for the first statement. For the second, if $\text{Gal}(K/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^3$ we can write $G := \text{Gal}(K/\mathbb{Q}_p)$ as the internal direct sum of the inertia subgroup $I \leq G$ and a cyclic subgroup $H \leq G$, since K^I is an unramified, hence cyclic extension of \mathbb{Q}_p with Galois group isomorphic to $G/I \simeq H$. Then K^H is a totally wildly ramified abelian extension of \mathbb{Q}_p whose Galois group G/H is not cyclic, and the first statement implies that no such extensions exist, which contradicts our assumption $\text{Gal}(K/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^3$. \square

Remark 20.8. There is an alternative proof to Proposition 20.7 that is more explicit. One can show that for odd p the field \mathbb{Q}_p has exactly p ramified abelian extensions of degree p , namely, $\mathbb{Q}_p[x]/(x^p + px^{p-1} + p(1 + ap))$, for integers $a \in [0, p - 1]$; see [3, Prop. 2.3.1]. Any noncyclic totally wildly ramified abelian extension of \mathbb{Q}_p would contain at least $p + 1$ ramified abelian extensions of degree p , since $(\mathbb{Z}/p\mathbb{Z})^2$ has $p + 1$ quotients of order p .

Remark 20.9. Another approach to Proposition 20.7 uses Kummer theory. One shows that for odd p the elementary abelian p -group $\mathbb{Q}_p(\zeta_p)^\times/\mathbb{Q}_p(\zeta_p)^{\times p}$ has rank at most 2, and this rules out the existence of a $(\mathbb{Z}/p\mathbb{Z})^3$ extension; see [6, Lemma 14.8].

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 20.10. *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 $\mathbb{Q}_2(\zeta_{2^{2r-1}})$ 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

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

and thus admits a quotient isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^3$. By Lemma 20.11 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 20.11. *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 extensions 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 Klasse (1896), 29–39.
- [2] Leopold Kronecker, *Über 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.