THE KRONECKER-WEBER THEOREM

CHARLIE JIANG

Abstract. In this expository paper, we provide a complete proof of the Kronecker-Weber theorem, a foundational result in algebraic number theory. Our approach will make use of local techniques and class field theory. The only prior experience in algebraic number theory required is a first course covering the ramification theory of Dedekind domains and the definition of completions.

Contents

1. Introduction

A common practice in mathematics is to simplify the study of an abstract object by embedding it into some concrete, well-understood "ambient" object. In algebra, one embeds a group G into $\mathrm{Aut}_{\mathsf{Set}}(G)$ and a ring R into $\mathrm{End}_{\mathsf{Ab}}(R)$—both are of course subsumed under the general paradigm of embedding a category C into its free cocompletion (the presheaf category $\mathsf{Set}^{\mathsf{C}}$) via the Yoneda embedding. On the geometric side of things, the Whitney embedding theorem allows any smooth manifold to be viewed as a properly embedded submanifold of an Euclidean space; further examples abound. An instance of this paradigm in the context of algebraic number theory is the *Kronecker-Weber theorem*, which places every abelian extension of $\mathbb{Q}$ into an ambient cyclotomic field. The precise statement is as follows:

Theorem 1.1 (Kronecker-Weber-Hilbert)**.** *For any finite abelian extension $L/\mathbb{Q}$, there exists some $n > 1$ for which $L \subseteq \mathbb{Q}(\zeta_n)$.*

Our goal in this expository paper is to a proof of this result by way of reduction to local fields. Before delving into the proof, let us take a step back and consider the class of embedding problems to which the theorem belongs:

Definition 1.2. Fix K a field, $\mathcal{P}$ a property of finite field extensions of K. The **$\mathcal{P}$-embedding problem for K** asks whether there exist a class $\mathcal{C}$ of field extensions of K such that for every finite extension L/K satisfying $\mathcal{P}$, there exists $F \in \mathcal{C}$ such that $L \subseteq F$.

Phrased in this language, the Kronecker-Weber Theorem is the abelian-embedding problem for $\mathbb{Q}$. One step of generalization leads us to *Hilbert's twelfth problem*, which concerns the abelian-embedding problem for arbitrary number fields and is solved in very few cases besides for $\mathbb{Q}$. The subject of what was historically known as *Kronecker's Jugendtraum* is the problem for when the base field is $\mathbb{Q}(i)$, for which a satisfying answer has been obtained through the theory of *complex multiplication*, which we will briefly explore towards the end of the paper.

In any case, the first conceivable reduction to be made for the abelian-embedding problem proceeds by way of Galois theory, translating the decomposition of the Galois group into a statement about the field extension:

Proposition 1.3. *For K a field, if $\mathcal{C}$ is closed under composita and solves the embedding problem for cyclic p-extensions of K, then it also solves the abelian-embedding problem for K.*

Proof. Let L/K be an abelian extension with $\mathrm{Gal}(L/K) \cong \bigoplus \mathbb{Z}_{p_i^{n_i}}$, a decomposition furnished by the structure theorem for finite abelian groups. For each i, denote the subgroup of $\mathrm{Gal}(L/K)$ corresponding to $\bigoplus_{j \neq i} \mathbb{Z}_{p_j^{n_j}}$ by H_i, and whose fixed field by L_i, which is a cyclic extension as $\mathrm{Gal}(L_i/K) \cong \mathrm{Gal}(L/K)/H_i \cong \mathbb{Z}_{p_i^{n_i}}$. It will then suffice to show that $L_1 \dots L_n = L$, whence L would be contained in the compositum of the fields in $\mathcal{C}$ containing each L_i. Now since the compositum is but the fixed field of $\bigcap H_i$, this amounts to that $\bigcap H_i = \{1\}$. To this end, let $\varphi \in H_i$ for all i. Then for $\pi_i \colon G \to \mathbb{Z}_{p_i^{n_i}}$ the canonical projection, $\pi_i(\varphi) = 1$ for all i, whereby φ is itself 1, as needed. □

It is by virtue of this result that we may study solely the *cyclic*-embedding problem in the sequel, in both the local and global case. Indeed, recall that $\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{\mathrm{lcm}(m,n)})$. On the other hand, if one wishes to study the general embedding problem, one might ask if a similar reduction is possible: after, finite simple groups have been fully classified!

While solving the embedding problem for each class of finite simple extension could already itself prove an insurmountable task, collating the results into a solution for the general embedding problem can also no longer be done with such a simple maneuver as taking the compositum. Indeed, the Jordan-Hölder theorem merely furnishes a filtration with simple factors, not a decomposition by finite simple groups. Given a field extension L/K whose Galois group admits the composition series

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G,$$

we have by the Galois correspondence a tower of fields

$$K = L^G \subseteq L^{G_{n-1}} \subseteq \cdots \subseteq L^0 = L.$$

Now although $\mathrm{Gal}(L^{G_m}/L^{G_{m+1}}) = G_{m+1}/G_m$ is simple, to say anything useful we need a solution to the simple-embedding problem for $L^{G_{m+1}}$, not just L. Even with this, embeddings lower down the tower may not be compatible with ones higher up, and in general it is not clear what sort of sufficient conditions allowing one to move from $\mathcal{C}_k$ to $\mathcal{C}_l$, for $k > l$, are to be deemed satisfactory. Given this complexity, we will focus exclusively on the abelian case, where the tools of completion and class field theory are available to us.

2. General Theory of Henselian DVRs

We officially begin making way towards a proof of Theorem 1.1, following [8]. As stated earlier, instead of tackling it directly, we will take a roundabout approach and first show an analogous *local* statement, taking completions at each point and studying the resulting extensions individually. The statement is none other than the abelian-embedding problem for $\mathbb{Q}_p$:

Theorem 2.1 (Local Kronecker-Weber)**.** *For any finite abelian extension $L/\mathbb{Q}_p$, for p a prime number, there exists some $n > 1$ for which $L \subseteq \mathbb{Q}_p(\zeta_n)$.*

To understand why working locally should bring about a simplification, we observe a crucial difference between when one has a general Dedekind domain as the base ring versus when one has a Henselian DVR, that while in the former the discrete valuation downstairs may be extended in as many ways as there are primes upstairs, of which there could be many, in the latter a unique prime ideal, hence a unique extension may be obtained.

For ease of notation, we introduce the following shorthand: whenever we "assume $ABKL$," we let A be a Dedekind domain, K its field of fractions, L a finite separable extension of K, and B the integral closure of A therein.

Lemma 2.2. *Assume ABKL, and let $\mathfrak{p}$ be a prime of A. Then the map $\mathcal{P} \rightsquigarrow \nu_{\mathcal{P}}$ yields a bijection between the primes of B lying above $\mathfrak{p}$ and the discrete valuations on B extending $\nu_{\mathfrak{p}}$. In particular, $\nu_{\mathcal{P}}$ extends $\nu_{\mathfrak{p}}$ with index $e(\mathcal{P}/\mathfrak{p})$.*

Proof. Given a prime $\mathcal{P}$ lying above $\mathfrak{p}$, that $\nu_{\mathcal{P}}$ extends $\nu_{\mathfrak{p}}$ follows immediately from that $\nu_{\mathcal{P}}(\mathfrak{p}B) = \nu_{\mathcal{P}}(\prod \mathcal{P}_i^{e(\mathcal{P}_i/\mathfrak{p})}) = e(\mathcal{P}/\mathfrak{p})$, as $\mathcal{P}$ lies above no other prime and $\nu_{\mathcal{P}}$ distributes over products of ideals. To see injectivity, note that given distinct prime ideals $\mathcal{P}$, $\mathcal{P}'$, there exists $x \in \mathcal{P} \setminus \mathcal{P}'$, on which $\nu_{\mathcal{P}}$ and $\nu_{\mathcal{P}'}$ evidently cannot agree. Now let ω be a discrete valuation extending $\nu_{\mathfrak{p}}$ with index e, valuation ring $R = \{ x \in L \colon \omega(x) \geq 0 \}$, and maximal ideal $\mathfrak{m} = \{ x \in L \colon \omega(x) > 0 \}$. Since $\omega|_K = e\nu_{\mathfrak{p}}$ and for all $a \in A$ (resp. $\mathfrak{p}$), $\nu_{\mathfrak{p}}(a) \geq 0$ (resp. > 0), $A \subseteq R$, and $\mathfrak{m}$ lies above $\mathfrak{p}$. But R is a DVR, hence integrally closed in L, so we have furthermore that $B \subseteq R$. For $\mathcal{P} := \mathfrak{m} \cap B = \iota_B^{-1}(\mathfrak{m})$, we claim that $B_{\mathcal{P}} = R$, from which the result evidently follows. It in fact suffices to show the forward inclusion, as $R \subseteq L = K(B_{\mathcal{P}})$, and there are no proper intermediate rings between a DVR and its fraction field (else the intermediate ring would contain an element $u\pi^n$ for $n < 0$, u a unit, and multiplying by π^{-1-n} yields π^{-1}). To this end, note that every element of $B_{\mathcal{P}}$ can be written as b/s, for $b \in B, s \in B \setminus \mathfrak{q}$. Then as $s \notin \mathcal{P} \implies s \notin \mathfrak{p}$, $\omega(s) = 0$, whereby $b/s \in R$. □

Theorem 2.3. *Assume ABKL, with $(A, \mathfrak{p}, \nu_{\mathfrak{p}})$ a Henselian DVR. Then B is a DVR whose unique maximal ideal $\mathcal{P}$ lies above $\mathfrak{p}$, whereby $\nu_{\mathcal{P}}$ is the unique discrete valuation on B extending $\nu_{\mathfrak{p}}$. Furthermore, if A is complete with respect to $\nu_{\mathfrak{p}}$, then so is B with respect to $\nu_{\mathcal{P}}$.*

Proof. Since B is in general a Dedekind domain, it will suffice to show that it is local, i.e. there is a single prime lying above $\mathfrak{p}$. Suppose to the contrary that there are distinct prime $\mathcal{P}, \mathcal{P}'$ lying above $\mathfrak{p}$, and let $b \in \mathcal{P} \setminus \mathcal{P}'$. As b is an integral element, the minimal polynomial f of b lies in $A[x]$, whence $A[b] \cong A[x]/(f)$. We claim that f is reducible. Writing $k := A/\mathfrak{p}$, we have $A[b]/\mathfrak{p}A[b] \cong A[x]/(\mathfrak{p}, f) \cong k[x]/(\overline{f})$, where $\overline{f}$ is the reduction of f to $k[x]$. Then $\mathcal{P} \cap A[b]$ and $\mathcal{P}' \cap A[b]$ are sent to distinct prime ideals of $k[x]/(\overline{f})$, whereby $\overline{f}$ has at least two distinct irreducible factors, with $k[x]$ a PID. But since A is Henselian, one may lift these factors to show that f is reducible.
The uniqueness of $\nu_{\mathcal{P}}$ as an extension of $\nu_{\mathfrak{p}}$ now follows from the preceding lemma, whereas the final assertion about completeness follows if we consider the norm on L induced by $\nu_{\mathcal{P}}$ and invoke the fac that every norm on a finite-dimensional vector space V over a complete field induces the same topology, in which V is complete. □

The move to the purely local setting pays dividends in part through a significant simplification of the `ref`-identity, where the `r` is all but annihilated and a single product alone suffices for computing $[L : K]$. On the one hand, from this *monogenicity*, i.e. the existence of a power basis, is guaranteed whenever a separable residue field extension can be procured. This is by no means the case when working globally: although given a separable l/k one could always find a primitive element, from it alone no clean description of B can be deduced in general.

Theorem 2.4. *Assume ABKL. If A and B are DVRs, with residue fields l, k, respectively, then l/k being separable implies that $B = A[\alpha]$ for some $\alpha \in B$. If furthermore L/K is unramified, then α may be taken to be any lift of a primitive element $\overline{\alpha}$ with $l = k(\overline{\alpha})$.*

Proof. The primitive element theorem furnishes an $\overline{\alpha} \in l$ such that $l = k(\overline{\alpha})$ with minimal polynomial $\overline{g} \in k[x]$. Let $g \in A[x]$ be a monic lift of $\overline{g}$, $\alpha_0 \in B$ a lift of $\overline{\alpha}$, so that $g(\alpha_0) \equiv \overline{g}(\overline{\alpha}) = 0 \mod \mathcal{P}$, whereby $\nu_{\mathcal{P}}(g(\alpha_0)) \geq 1$. If $\nu_{\mathcal{P}}(g(\alpha_0)) = 1$, put $\alpha := \alpha_0$. Otherwise, let π_0 be a uniformizer in B, and put $\alpha := \alpha_0 + \pi_0$. Taking the first-order formal Taylor expansion, we have $g(\alpha) = g(\alpha_0) + \pi_0 g'(\alpha_0) + \pi_0^2 h(\alpha_0)$, for some $h \in A[x]$. Now while evidently $\nu_{\mathcal{P}}(g(\alpha_0))$ and $\nu_{\mathcal{P}}(\pi_0^2 h(\alpha_0))$

are both greater than 1, $\nu_{\mathcal{P}}(\pi_0 g'(\alpha_0)) = 1$, as $g'(\alpha_0) \in \mathcal{P}$ would imply that $\overline{g}'(\overline{\alpha}) = 0$, contradicting the separability of $\overline{g}$. It follows that $\nu_{\mathcal{P}}(g(\alpha)) = 1$, as the discrete valuation of a sum is *equal* to the minimum of that of each term, if there is a unique one. We thus put $\pi := g(\alpha)$, so that it is a uniformizer in either case.
We claim that $\left\{ 1, \alpha, \dots, \alpha^{n-1} \right\}$ generates B as an A-module. Consider the filtration

$$B/\pi^e B \supseteq \pi B/\pi^e B \supseteq \dots \supseteq \pi^{e-1} B/\pi^e B \supseteq 0.$$

For each $(\pi^k B/\pi^e B)/(\pi^{k+1} B/\pi^e B) \cong \pi^k B/\pi^{k+1} B$, multiplication by π^k yields a k-linear isomorphism $l = B/\pi B \to \pi^k B/\pi^{k+1} B$. Hence $S := \left\{ \pi^i \alpha^j : 0 \leq i \leq e-1, 0 \leq j \leq f-1 \right\}$ is a k-generating set for $B/\pi^e B$ (as it is one for the associated graded object), whence Nakayama's lemma asserts that it is an A-generating set for B. But since $\pi = g(\alpha)$ is a monic polynomial in α, we have $\pi^i \alpha^j \in A[\alpha]$, whereby $S \subseteq A[\alpha] \implies B \subseteq A[\alpha]$, as needed.
When L/K is unramified, $[L : K] = f$, whereby π need not be involved, α need not be adjusted, and Nakayama's lemma directly yields the result. □

On the other hand, this allows us to *canonically* decompose any extension L/K into an unramified part and a totally ramified part. One might wonder what the replacement is for the *decomposition subfield* that is present in the case of global fields: in the local setting it is trivialized, as $r = 1$ and $[L^{D(\mathcal{P}/\mathfrak{p})} : K] = r$. When the extension is Galois, this intermediate field is given by $L^{I_0(\mathcal{P}/\mathfrak{p})}$, which we will henceforth denote by L^{ur} and call the **maximal unramified subfield**. Note that it is possible to define L^{ur} even when the extension is *not* Galois, but this will not be needed for our present purposes.

Remark. To see how this dichotomy will be relevant to our proof of Theorem 2.1, note that if the embedding problem is solved for L^{ur}/K and L/L^{ur}, i.e. if L^{ur} embeds into $K(\zeta_n)$ and L embeds into $L^{\mathrm{ur}}(\zeta_m)$ for $n, m \in \mathbb{Z}^+$, then L manifestly embeds into $K(\zeta_{\mathrm{lcm}(m,n)})$. This also justifies our working in complete generality, as it is necessary to account for changes in the base field.

By virtue of Theorem 2.4, characterizations of unramified and totally ramified extensions may be given in terms of their monogenic generator, i.e. with conditions on the α for which $B = A[\alpha]$. Having such a concrete form for the extensions allows us to better embed them into cyclotomic fields, as only the generator needs to be accounted for. The realization of this premise in the unramified case hinges on the following result, which we motivate by noting that via the `ref`-identity, L/K is unramified iff l/k is separable and $[L : K] = f$, whence a *functorial* way to go from separable l/k to unramified L/K may be expected.

Theorem 2.5. *Fix a Henselian DVR $(A, \mathfrak{p})$ with residue field k and fraction field K. Denote by C the subcategory of K-Alg of finite unramified extensions of K, D the subcategory of k-Alg of finite separable extensions of k. The functor $F\colon \mathsf{C} \to \mathsf{D}$ sending each unramified extension L, wherein the integral closure of A is $(B, \mathfrak{q})$, to the residue field $l := B/\mathfrak{q}$ and each K-algebra morphism $\varphi\colon L_1 \to L_2$ to the morphism $\overline{\varphi}\colon l_1 \to l_2$ induced from $B_1 \xrightarrow{\varphi} B_2 \xrightarrow{\pi} l_2$ is an equivalence of categories.*

Proof. That $\overline{\varphi}$ is well-defined follows from the injectivity of φ as a morphism of fields: for then B_2 is a finite extension of $\varphi(B_1)$, whereby $\mathfrak{q}_2$ is the unique maximal ideal lying over $\varphi(\mathfrak{q}_1)$, as shown in the Theorem 2.3. The map also admits an explicit description: it sends $[a]$ to $[\varphi(a)]$. Since F is manifestly functorial, it remains to show essential surjectivity and fully faithfulness.
Given a finite separable l/k, the primitive element theorem furnishes an $\overline{\alpha} \in l$ for which $l \cong k(\overline{\alpha}) \cong k[x]/(\overline{f})$, for $\overline{f} \in k[x]$ the minimal polynomial of $\overline{\alpha}$. It follows that any monic lift $f \in A[x]$ is irreducible, whereby the subsequent Lemma 2.6 shows that l is the residue field of $L := K[x]/(f)$. That L/K is unramified then follows, as $[L : K] = \deg(f) = \deg\left(\overline{f}\right) = [l : k]$, and l/k is separable.
Now given finite unramified extensions L_1, L_2, we have $\mathrm{Hom}_K(L_1, L_2) \cong \mathrm{Hom}_A(B_1, B_2)$, so it suffices to show that $\pi^\sharp\colon \mathrm{Hom}_A(B_1, B_2) \to \mathrm{Hom}_k(l_1, l_2)$ is also a bijection. By Theorem 2.4, we may write

$B_1 = A[\alpha] \cong A[x]/(g)$, $l_1 = k[\overline{\alpha}] \cong k[x]/(\overline{g})$. Then an A-algebra homomorphism $B_1 \to B_2$ (resp. k-algebra homomorphism $l_1 \to l_2$) is determined by the image of α (resp. $\overline{\alpha}$), whereby

$$\operatorname{Hom}_A(B_1, B_2) \cong \{\text{ roots of } g \text{ in } B_2\,\}, \quad \operatorname{Hom}_k(l_1, l_2) \cong \{\text{ roots of } \overline{g} \text{ in } l_2\,\}.$$

But B_2 is Henselian and $\overline{g}$ is separable, so Hensel lifting furnishes a bijection from the set of roots of $\overline{g}$ to that of g, whence an inverse to $\pi^\sharp$. □

Lemma 2.6. *Assume ABKL, with A and B DVRs. Let $\pi\colon A[x] \to k[x]$ be the canonical projection. If for some monic $f \in A[x]$, $L = K[x]/(f)$ and $\overline{f} := \pi(f)$ is irreducible, then $l = k[x]/(\overline{f})$.*

Proof. Let α be a root of f in K, so that $A[x]/(f) \cong A[\alpha]$. Evidently π restricts to a map $A[x]/(f) \twoheadrightarrow k[x]/(\overline{f})$, with kernel given by $\mathfrak{p}A[x]/(f)$. Hence $A[x]/(f, \mathfrak{p}) \cong k[x]/(\overline{f})$. Denote by B the integral closure of A in L, a DVR with unique maximal ideal $\mathcal{P}$. Since α is integral, $A[\alpha] \subseteq B$, yielding a k-algebra homomorphism $\iota\colon A[\alpha]/\mathfrak{p}A[\alpha] \hookrightarrow B/\mathcal{P}$, necessarily injective as a morphism of fields. But since $[l : k] = f \leq [L : K] = [k[x]/(\overline{f}) : k]$, ι is an isomorphism. □

From this, Theorem 2.4 immediately yields the following characterization:

Theorem 2.7. *Assume ABKL, with (A, k) a Henselian DVR. Then the L/K is unramified iff there exists a primitive element $\alpha \in B$ whose minimal polynomial has separable reduction in $k[x]$, in which case $B = A[\alpha]$.*

Proof. The forward direction and the implication follow immediately from the unramified case of Theorem 2.4. To see the converse, write $f \in A[x]$ for the minimal polynomial, $\overline{f}$ for its reduction in $k[x]$. Then by Hensel's lemma, $\overline{f}$ is irreducible, so $l = k[x]/(\overline{f})$ by the preceding lemma. Hence l/k is separable with $[l : k] = \deg\left(\overline{f}\right) = \deg(f) = [L : K]$, and that L/K is unramified follows from the theorem. □

Not too much can be said about elements with minimal polynomial separable modulo $\mathfrak{p}$ in complete generality, but in §3 we will see that these are precisely cyclotomic extensions of suitable degree in our case of interest. As such, we now move on to study totally ramified extensions. The answer in terms of monogenic generators turns out to be surprisingly simple (and completely analogous to Theorem 2.7), involving only the following axiomatization of Eisenstein's criterion:

Definition 2.8. Fix a DVR $(A, \mathfrak{p})$. A monic polynomial $\sum a_i x^i \in A[x]$ is **Eisenstein** if $\nu_{\mathfrak{p}}(a_i) > 0$ for all $0 \leq i < n$ and a_0 is a uniformizer.

Remark. The same elementary proof of Eisenstein's criterion may be transplanted verbatim to yield the result that Eisenstein polynomials are irreducible in $A[x]$ and $K[x]$.

Theorem 2.9. *Assume ABKL, with A a Henselian DVR. Then L/K is totally ramified iff $L = K(\pi)$ and the minimal polynomial of π is Eisenstein, in which case π is a uniformizer of B and $B = A[\pi]$.*

Proof. This is Theorem 6.11 in Chapter 6 of the lecture notes. □

We conclude the section by introducing a further dichotomy for ramified extensions that will prove useful in the next section:

Definition 2.10. Assume $ABKL$, with (A, k) a Henselian DVR. L/K is said to be **tamely ramified** if l/k is separable and $\operatorname{char} k \nmid e$. Otherwise, L/K is said to be **wildly ramified**.

As to be seen, quite a bit can still be said about tamely ramified extensions generically; but whenever one treads near the borders of wild ramification, general theory fails, and one must work on a case-by-case basis.

3. Proof via Local Techniques

In this section, we apply the machinery developed in §2 to $\mathbb{Q}_p$ to derive a proof of Theorem 2.1, from which Theorem 1.1 will in turn be deduced using a prototypical local-to-global argument.

Lemma 3.1. *Fix a Henselian DVR A with residue field k and fraction field K, a primitive nth root of unity ζ_n in some algebraic closure of K. If $\gcd(n, \operatorname{char} k) = 1$, then $K(\zeta_n)/K$ is unramified.*

Proof. By Theorem 2.7, it suffices to show that the reduction $\overline{f}$ of the minimal polynomial f of ζ_n is separable. Indeed, since $f \mid x^n - 1$, also $\overline{f} \mid x^n - 1$. Now $\gcd(n, \operatorname{char} k) = 1$ implies that $n \neq 0$ in k, whereby $x^n - 1$ is coprime to its derivative nx^{n-1}. As such, $x^n - 1$, hence $\overline{f}$, is separable in k. □

Proposition 3.2. *Fix a Henselian DVR A with finite residue field $\mathbb{F}_q$ and fraction field K. Then a degree n extension L/K is unramified iff $L \cong K(\zeta_{q^n-1})$. In this case, L/K is an $\mathbb{Z}/n\mathbb{Z}$-extension.*

Proof. Since L/K is unramified, Theorem 2.7 furnishes an $\alpha \in B$ whose minimal polynomial $f \in A[x]$ has separable, hence irreducible reduction $\overline{f}$ in $\mathbb{F}_q[x]$. By Lemma 2.6, $l \cong \mathbb{F}_q[x]/(\overline{f}) \cong \mathbb{F}_{q^n}$, whereby $\overline{f}$ divides $x^{q^n-1} - 1$ in $\mathbb{F}_q[x]$. Lifting this divisibility with Hensel's lemma, with $\overline{f}$ being separable, we conclude that α is a $(q^n - 1)$-th root of unity. Hence $L = K(\alpha) \subseteq K(\zeta_{q^n-1})$. But since $[L : K] = n$, this is in fact an equality. The reverse implication follows immediately from the preceding lemma, and from this the Galois group is easily seen to be $\mathbb{Z}/n\mathbb{Z}$. □

This is certainly very good news: the problem has been essentially trivialized in the unramified case, whereby only the totally ramified case continues to call for our attention.

Proposition 3.3. *Assume ABKL, with (A, k) a Henselian DVR. If $\operatorname{char} k \nmid n := [L : K]$, then L/K is totally tamely ramified iff $L = K(\pi^{1/n})$ for some uniformizer π of A, in which case $B = A[\pi^{1/n}]$.*

Proof. Let us denote $\operatorname{char} k$ by p, the maximal ideals of A, B by $\mathfrak{p}, \mathcal{P}$, and their uniformizers by π_A, π_B, respectively. Since $\nu_{\mathcal{P}}$ extends $\nu_{\mathfrak{p}}$ with index $e = n$, we may write $\pi_B^n = u\pi_A$ for some $u \in B^\times$. It suffices to exhibit some $r \in B$ with $r^n = u$, for then $(\pi_B/r)^n = \pi_B^n/u = \pi_A$, and π_B/r is a uniformizer, with r being a unit; thence the result follows immediately from Theorem 2.9. As the choice of π_A is immaterial, multiplying π_A by $\overline{u}$ (recall that $B/\mathcal{P} \cong A/\mathfrak{p}$) allows us to assume without loss of generality that $u \equiv 1 \mod \mathcal{P}$. As such, $x^n - u$ reduces to $x^n - 1$, for which 1 is a simple root, as $p \nmid n$, whereby Hensel's lemma furnishes the desired root. For the reverse implication, note that the minimal polynomial of $\pi^{1/n}$, $x^n - p$, is Eisenstein, whereby Theorem 2.9 asserts that L/K is totally ramified, with $B = A[\pi^{1/n}]$. Tameness follows, as $p \nmid n = e$. □

We are finally ready to prove Theorem 2.1. To set the stage, fix a prime p and an abelian extension $L/\mathbb{Q}_p$. The residue field of $\mathbb{Q}_p$ is, of course, $\mathbb{F}_p$, and the tower of residue field extensions is of characteristic p. By Proposition 1.3, we may take $\operatorname{Gal}(K/\mathbb{Q})$ to be $\mathbb{Z}/q^n\mathbb{Z}$ for some prime q. Put $K := L^{\mathrm{ur}}$, so that $f = [K : \mathbb{Q}_p]$ is q^r for some $r \in \mathbb{N}$, whereby $e = [L : K] = q^{n-r}$, and $K = \mathbb{Q}_p(\zeta_{p^{q^r}-1})$.

It suffices to consider three cases:

3.1. **Case 1: $p \neq q$.** Evidently $e = q^{n-r}$ is coprime to p, so L/K is tamely ramified. Let π be a uniformizer of $\mathcal{O}_K$. Then by Proposition 3.3, $L = K(\pi^{1/e})$. But since $K/\mathbb{Q}_p$ is unramified, $\mathcal{P}_K = p\mathcal{O}_K$, whence there exists some $u \in \mathcal{O}_K^\times$ for which $\pi = -up$. Now $L = K(u^{1/e}(-p)^{1/e}) \subseteq K(u^{1/e}) \cdot K((-p)^{1/e})$, so it suffices to show that either extension in the compositum is contained in a cyclotomic extension of $\mathbb{Q}_p$.

We first claim that $K(u^{1/e})/K$ is unramified; since K is itself cyclotomic over $\mathbb{Q}_p$, that $K(u^{1/e})$ is cyclotomic as well would follow from Proposition 3.2. By Theorem 2.7, it suffices to show that $x^e - u$ has separable reduction in $k_K[x]$; the same then holds for the minimal polynomial of $u^{1/e}$. This is manifestly the case, as e is a unit in k_K, whereby $\gcd\big(x^e - u, ex^{e-1}\big) = 1$.

It remains to show that $K((-p)^{1/e})$ is contained in a cyclotomic extension of $\mathbb{Q}_p$. Since K is cyclotomic, this would of course follow from the same statement for $\mathbb{Q}_p((-p)^{1/e})$. We first show that $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}$ is an abelian extension by realizing it as a subextension of another abelian extension. Indeed, consider $M := L(u^{1/e})$, which is abelian as the compositum of L and $\mathbb{Q}_p(\zeta_e)$. Then $\mathbb{Q}_p(p^{1/e}) \subseteq M$, with $(-p)^{1/e} = (\pi/u)^{1/e} = \pi^{1/e}/u^{1/e}$. Now since $x^e + p$ is Eisenstein, $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}$ is totally ramified by Theorem 2.9.

By taking the ratio of two eth roots of p, which belong to $\mathbb{Q}_p((-p)^{1/e})$ as it is Galois over $\mathbb{Q}_p$, we see that $\zeta_e \in \mathbb{Q}_p((-p)^{1/e})$. Phrased more evocatively, $\mathbb{Q}_p(\zeta_e) \subseteq \mathbb{Q}_p((-p)^{1/e})$. But $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ is totally ramified, forcing $[\mathbb{F}_p(\zeta_e) : \mathbb{F}_p] = f(\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p) = 1$. This happens only if $e \mid (p-1)$, whereby $\mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p((-p)^{1/(p-1)})$.

By virtue of this result, we have detached ourselves entirely from the relative situation and reduced the problem to the following statement, which is entirely about $\mathbb{Q}_p$:

Proposition 3.4. *For p a prime, $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$.*

Proof. Put $\pi := \zeta + 1$, and notice that its minimal polynomial $x^{p-1} + px^{p-2} + \cdots + p$ is Eisenstein. We then have $\pi^{p-1} + p\pi^{p-2} + \cdots = -p$, and dividing by p and reducing modulo π, we have a $u := -\pi^{p-1}/p$ that is $1 \pmod{\pi}$, hence a unit. That is, $x^{p-1} = u$ reduces to $x^{p-1} = 1$, and with 1 being a simple root of the latter (as $p - 1 \nmid p$), Hensel's lemma furnishes a $(p-1)$-th root $r \in \mathbb{Q}_p^\times$ of u. It follows that $(\pi/r)^{p-1} = \pi^{p-1}/u = -p$, whence $(-p)^{1/(p-1)} \in \mathbb{Q}_p(\zeta_p)$, which concludes the proof as $[\mathbb{Q}_p((-p)^{1/(p-1)}) : \mathbb{Q}_p] = p - 1$, with $x^{p-1} + p$ being Eisenstein. □

We may thus mark this case as completed. □

3.2. **Case 2: $p = q > 2$.** An attempt to mimic our work in the previous case would falter at the very first step: Proposition 3.3 does not apply, and no explicit form for L can be secured with these elementary means. It is therefore necessary for us to take a step back and take a structural look at the situation. Since the local Kronecker-Weber theorem concerns *all* abelian extensions of $\mathbb{Q}_p$, it is possible to study them not individually but all at once. The requisite gadget for this is the following:

Definition 3.5. Let K be a local field, and fix a separable closure K^{sep}. The **maximal abelian extension** of K is the subextension $K^{\text{ab}} = \bigcup_{L/K \text{ finite abelian}} L$.

Note that $\mathbb{Q}_p^{\text{ur}} \subseteq \mathbb{Q}_p^{\text{ab}}$ by virtue of Proposition 3.2. In this language, the theorem essentially concerns whether the cyclotomic extensions form a cofinal system. Our present case in turn concerns the subextension that is the union of all $\mathbb{Z}/p^r\mathbb{Z}$-extensions $L/\mathbb{Q}_p$, but as a priori these extensions are not known to be linearly disjoint or bear any sort of relation with each other, we will benefit from slightly broadening our scope and considering the **maximal p^r-exponent extension**, denoted $K^{\text{ab},p^r}/K$, that is the union of all extensions with finite abelian p^r-exponent Galois groups. Concretely, these are groups A wherein for all $a \in A$, $a^{p^r} = 1$, or equivalently finite direct sums $\bigoplus \mathbb{Z}/p^{r_i}\mathbb{Z}$, where $r_0 = r$ and $r_{i+1} \leq r_i$ for all i. Being able to embed K^{ab,p^r} into a cyclotomic field will of course imply the same for $(\mathbb{Z}/p^r\mathbb{Z})$-extensions.

As with any problem in field theorem, the solution usually presents itself when one passes to group theory via Galois theory. The Galois groups in question are profinite groups and already admit somewhat explicit descriptions: $\text{Gal}(K^{\text{ab}}/K)$ is both the projective limit over all finite abelian Galois groups and the abelianization of the absolute Galois group $\text{Gal}(K^{\text{sep}}/K)$, and by the same token $\text{Gal}(K^{\text{ab},p^r}/K)$ is the projective limit over p^r-exponent $\text{Gal}(L/K)$'s.

Hitherto we have done nothing but recast the problem in a more systematic way. This, however, allows us to shift our attention from an infinite set of extensions to a single, maximal one, the knowledge of whose Galois group would allow us to decompose it into a hopefully finite set of explicit subextensions which we can try to embed one by one. Suppose, for instance, that we have shown

$\mathrm{Gal}(K^{\mathrm{ab},p^r}/K) \cong (\mathbb{Z}/p^r\mathbb{Z})^d$. Then K^{ab,p^r} is the compositum of exactly d linearly disjoint $\mathbb{Z}/p^{r_i}\mathbb{Z}$-extensions over K. This is by virtue of the exact same argument we have made in Proposition 1.3.

The solution has already surfaced: once we compute the Galois group (to be say a finite product $\bigoplus G_i$), we simply need to determine each of the d "basic" G_i-extensions, show their linear disjointness, and embed each into a cyclotomic field. This is, of course, all contingent on the highly non-obvious (and generally false) assumption that $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab},p^r}/\mathbb{Q}_p)$, an object we presently lack any ability to compute, is well-behaved. The one glimmer of hope is supplied by the fact that when we restrict to the case of $r = 1$, the Galois group is necessarily a direct product. This is indeed, in some sense, the classical approach, where one deduces the non-existence of certain extensions of $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^d$, from where to derive a contradiction. This, however, suffers from the major pitfall that it obfuscates the conceptual picture, i.e. its non-constructive nature precludes the specification of an actual cyclotomic extension containing $\mathbb{Q}_p^{\mathrm{ab},p^r}$.

Classically, the tool for computing such abelian absolute Galois groups is Kummer theory, but as a result of its independence of base field, whence limited strength, it has largely been superseded by the machine of *local class field theory* (LCFT), whose goal is to provide for each abelian Galois extension of local fields L/K an explicit description of $\mathrm{Gal}(L/K)$. In our present case, their main results will coincide, but we still opt to give an introduction—a laughably brief one—to LCFT in hopes of conveying the full conceptual picture. The author's absurd proclivity to broach the unknown, against all odds, is by itself plenty of evidence to validate the transpiration of the mythological original sin, whose impact, despite emanating from the distant past, can still be palpably felt today.

The somewhat vague and idyllic objective of LCFT may be formalized with a list of desiderata elegantly conveyed with the following characterizing property for the *local Artin map*, the central object of study in this theory:

Definition 3.6 (c.f. [5, Theorem 1.1])**.** Fix a non-archimedean local field K. The **local Artin map** is a homomorphism $\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisfying the following properties:

(1) for any uniformizer π of K, the restriction of $\phi_K(\pi)$ to K^{ur} is $\mathrm{Frob}_{K^{\mathrm{ur}}/K}$;
(2) for any finite abelian extension L/K, ϕ_K induces an isomorphism $\phi_{L/K} : K^\times/N_{L/K}(L^\times) \to \mathrm{Gal}(L/K)$.

In particular, $\{ \phi_{L/K} \}$ constitutes a morphism of projective system, thereby giving rise to an isomorphism $\widehat{\phi_K} : \widehat{K^\times} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

It holds that ϕ_K is *characterized* by these properties, and that such a map does exist. This is in some sense the main result of local class field theory, and thus far beyond the scope of this paper. (We note that both Kummer theory and LCFT may be proven using the machinery of group cohomology, a common ground that somewhat justifies their mutual effectiveness in our case.) Nevertheless, let us take a leap of faith and tentatively take these for granted; the question then is to understand the subgroup of $\widehat{K^\times}$ corresponding to $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab},p^r}/\mathbb{Q}_p)$.

Proposition 3.7. *For p an odd prime,* $\mathrm{Gal}(\mathbb{Q}_p^{ab,p^r}/\mathbb{Q}_p) \cong (\mathbb{Z}/p^r\mathbb{Z})^2$.

Proof. The result has thus been reduced to computing $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^{p^r}$, where by $(\mathbb{Q}_p^\times)^{p^r}$ we understand the subgroup generated by $\{ u^{p^r} : u \in \mathbb{Q}_p^\times \}$. To this end, we must first understand the structure of $\mathbb{Q}_p^\times$. □

Remark. As can be seen, the correspondence needed from LCFT in order to prove the proposition is practically identical to [3, Cor 5.7], the main result of Kummer theory.

We may now complete the proof of this case. As argued earlier, it suffices to determine two linearly disjoint p^r-extensions which may be embedded in cyclotomic fields. Natural candidates are $\mathbb{Q}(\zeta_{p^{p^r}-1})$, the unique unramified p^r-extension, and the unique p^r-subextension of the totally ramified $\mathbb{Q}(\zeta_{p^{r+1}})$. Since one is unramified while the other is totally ramified, the two are manifestly linearly disjoint. □

3.3. **Case 3: $p = q = 2$.** While the computation of Proposition 3.7 does not carry over verbatim to when $p = 2$, an analogous one can still be done using LCFT, and our subsequent strategy will be identical to the one in the previous case.

Proposition 3.8. *LCFT yields an isomorphism* $\mathrm{Gal}(\mathbb{Q}_2^{ab,2^r}/\mathbb{Q}_2) \cong (\mathbb{Z}/2^r\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2^r\mathbb{Z})$.

Proof. The same argument as in Proposition 3.7 reduces the problem to computing $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^{2^r}$. □

Like in the former case, it suffices to exhibit three linearly disjoint 2^r-exponent fields with Galois groups being each of the factors. The first will still be the unramified extension $\mathbb{Q}_2(\zeta_{2^{2^r}-1})$ of degree 2^r. For the latter two, we play a little trick and construct a p^r-exponent field extension whose Galois group is *a priori* their direct sum. This extension is, of course, $\mathbb{Q}_2(\zeta_{2^{r+2}})$. Indeed, $\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^{r+2}})/\mathbb{Q}_2) \cong (\mathbb{Z}/2^{r+2}\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^r\mathbb{Z}$. Notice how the extra flexibility supplied by allowing for p^r-exponent fields plays a critical role; $\mathbb{Q}_2(\zeta_{2^{r+2}})$ is not a $(\mathbb{Z}/2^r\mathbb{Z})$-extension. □

3.4. **Deriving Theorem 1.1.** Fix a finite abelian extension $K/\mathbb{Q}$. For each *ramified* prime $p \in \mathbb{Z}$, of which there are finitely many, fix a prime $\mathfrak{p}$ lying above, so that $K_\mathfrak{p}/\mathbb{Q}_p$ constitutes an abelian extension with Galois group isomorphic to $D(\mathfrak{p}/p)$, by virtue of Theorem 6.8 in the course notes. The local Kronecker-Weber then furnishes a ζ_{m_p} for which $K_\mathfrak{p} \subseteq \mathbb{Q}_p(\zeta_{m_p})$. Put $n_p := \nu_p(m_p)$, $m := \prod p^{n_p}$. We claim that $L := K(\zeta_m) = \mathbb{Q}(\zeta_m)$, from which it would follow that $K \subseteq \mathbb{Q}(\zeta_m)$, as desired.

Since $L = K \cdot \mathbb{Q}(\zeta_m)$, it will suffice to show that $[L : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$. We are thus interested in the Galois group $\mathrm{Gal}(L/\mathbb{Q})$, which is abelian as a subgroup of $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_m))$. We again apply the technique of completion: let $\mathcal{P}$ be a prime in L lying above $\mathfrak{p}$, and consider the abelian extension $L_\mathcal{P}/\mathbb{Q}_p$, which has Galois group isomorphism to $D(\mathcal{P}/p)$. Write $M_\mathcal{P}$ for the fixed field of $I_0(\mathcal{P}/p)$, so that $L_\mathcal{P}/M_\mathcal{P}$ is totally ramified while $M_\mathcal{P}/\mathbb{Q}_p$ is unramified. Note that we can write $I_p := I_0(\mathcal{P}/p)$, as the choice of some other $\mathcal{P}'$ would yield a conjugate, hence equal subgroup by abelianness.

Now $L_\mathcal{P} = K_\mathfrak{p}(\zeta_m) = K_\mathfrak{p}(\zeta_{m/p^{n_p},\zeta_{p^{n_p}}}) = M_\mathcal{P}(\zeta_{p^{n_p}})$, as $K_\mathfrak{p} \subseteq \mathbb{Q}_p(\zeta_{m_p}) \subseteq M_\mathcal{P}(\zeta_{p^{n_p}})$ and $\mathbb{Q}_p(\zeta_{m/p^{n_p}})$ is unramified by Lemma 3.1. Hence $I_p \cong \mathrm{Gal}(L_\mathcal{P}/M_\mathcal{P}) \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n_p}})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^{n_p}\mathbb{Z})^\times$. Let I be the subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ generated by $\bigcup_{p \mid m} I_p$. Then evidently

$$[L : L^I] = |I| \leq \left| \prod_{p \mid m} I_p \right| = \prod_{p \mid m} |I_p| = \prod_{p \mid m} \varphi(p^{n_p}) = \varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}],$$

where by φ we understand the Euler totient function. But L^I is a subfield of each L^{I_p}, hence unramified over $\mathbb{Q}$, and since $\mathbb{Q}$ has no non-trivial unramified extension, we have $[L : L^I] = [L : \mathbb{Q}]$, as needed.

4. Generalizations

To conclude the paper, we will briefly survey alternative proof strategies for the Kronecker-Weber theorem and discuss some known generalizations or variants, including the Kronecker Jugendtraum, as promised in the introduction.

While our proof is local in nature, it is possible work exclusively with global fields. This was the approach of Kronecker and Weber, after whom the theorem is named, but who both failed to provide a full proof. It is not until 1986 that O. Neumann corrected their attempts in [7], still using their technique of *Lagrange resolvents* and central extensions, thereby proving a somewhat more general result than the present one.

The first correct proof was given by Hilbert, for which a detailed exposition can be found in [1]. The proof is surprisingly elementary and makes use of only the machinery covered in this course, primarily higher ramification groups. Structurally, it bears remarkable semblance to our approach, beginning also by dealing with the case of tame ramification: for each $L/\mathbb{Q}$ they construct an associated $L'/\mathbb{Q}$ such that every tamely ramified prime in L is unramified in L', and for which there exists a $\mathbb{Q}(\zeta_n)$ which, if containing L', also contains L. Note that this L' is constructed as the fixed field of a certain inertia group. In the case of wild ramification, it is also necessary to separately consider when $p = 2$, but here things turn out be significantly simpler as one could consider the fixed field of complex conjugation.

Another approach is via global class field theory [2]. Although the main results here are more complex than those in local class field theory, involving moduli and adèles, the spirit of the proof is analogous to ours: they compute the Galois group of the abelianized absolute Galois group and translate it to a statement about fields using infinite Galois theory.

We now discuss some generalizations of the result. The first question is of course if an analogous statement holds for local fields in general, namely for function fields. The answer is a somewhat tenuous yes, in the sense that it is no longer $\mathbb{F}_q(t)[\zeta_n]$ into which they embed, but what is known as *Carlitz cyclotomic fields*. This is carried out in [4]; incidentally, Hayes was a professor at UMass Amherst. A clue for why the naive conjecture would fail to hold can already be found in Proposition 3.2 not holding for DVRs with infinite residue fields, which applies to function fields at the "point at infinity".

Finally, the solution to Hilbert's twelfth problem for imaginary quadratic number fields may be viewed in tandem with the classical result in the following way: the roots of units ζ_n may be chosen to lie in the image of $e^{2\pi i/n}$, and it turns out the proper elements to adjoin are specific elements in *modular* and *elliptic* functions. The author lacks the ability to expound further on this deep subject and will refer the reader to [6].

References

[1] L. Culler. The kronecker-weber theorem. *UChicago VIGRE*, 2007.
[2] E. Ghate. The kronecker-weber theorem, 1999.
[3] K. Harper. Group cohomology and kummer theory. *UChicago VIGRE*, 2010.
[4] D. R. Hayes. Explicit class field theory for rational function fields. *Transactions of the American Mathematical Society*, 189:77–91, 1974.
[5] J.S. Milne. *Class Field Theory (v4.03)*. J.S. Milne, 2020.
[6] J.S. Milne. *Complex Multiplication*. J.S. Milne, 2020.
[7] Olaf Neumann. Two proofs of the kronecker-weber theorem "according to kronecker, and weber". *Journal für die reine und angewandte Mathematik*, 323:105–126, 1981.
[8] A. Sutherland. The kronecker-weber theorem, 2021.