Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
The Kronecker-Weber Theorem

Reference. Our approach follows Washington, *Introduction to Cyclotomic Fields*, Chapter 14. A variety of other methods can be found in other texts.

Abelian extensions of $\mathbb{Q}$.

Though class field theory has its origins in the law of quadratic reciprocity discovered by Gauss, its proper beginning is indicated by the Kronecker-Weber theorem, first stated by Kronecker in 1853 and proved by Weber in 1886. Although one could skip this theorem and deduce it as a consequence of more general results later on, I prefer to work through it explicitly. It will provide a "trailer" for the rest of the course, giving us a preview of a number of key elements:

- Reciprocity laws
- Passage between local and global fields, using Galois theory
- Group cohomology, and applications to classifying field extensions
- Computations in local fields

An *abelian extension* of a field is a Galois extension with abelian Galois group. An example of an abelian extension of $\mathbb{Q}$ is the cyclotomic field $\mathbb{Q}(\zeta_n)$ (where ζ_n is a primitive n-th root of unity), whose Galois group is $(\mathbb{Z}/n\mathbb{Z})^*$, or any subfield thereof. Amazingly, there are no other examples!

Theorem 1 (Kronecker-Weber). *If $K/\mathbb{Q}$ is a finite abelian extension, then $K \subseteq \mathbb{Q}(\zeta_n)$ for some positive integer n.*

For example, every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic field, a fact known to Gauss.

The smallest n such that $K \subseteq \mathbb{Q}(\zeta_n)$ is called the *conductor* of $K/\mathbb{Q}$. It plays an important role in the splitting behavior of primes of $\mathbb{Q}$ in K, as we will see a bit later.

We will prove this theorem in the next few lectures. Our approach will be to deduce it from a local analogue.

Theorem 2 (Local Kronecker-Weber). *If $K/\mathbb{Q}_p$ is a finite abelian extension, then $K \subseteq \mathbb{Q}_p(\zeta_n)$ for some n, where ζ_n is a primitive n-th root of unity.*

Before proceeding, it is worth noting explicitly a nice property of abelian extensions that we will exploit below. Let L/K be a Galois extension with Galois group G, let $\mathfrak{p}$ be a prime of K, let $\mathfrak{q}$ be a prime of L over $\mathfrak{p}$, and let $G_\mathfrak{q}$ and $I_\mathfrak{q}$ be the decomposition and inertia groups of $\mathfrak{q}$, respectively. Then any other prime $\mathfrak{q}'$ over $\mathfrak{p}$ can be written as $\mathfrak{q}^g$ for some $g \in G$, and the decomposition and inertia groups of $\mathfrak{q}'$ are the conjugates $g^{-1}G_\mathfrak{q}g$ and $g^{-1}I_\mathfrak{q}g$, respectively. (Note: my Galois actions will always be right actions, denoted by superscripts.) If L/K

is *abelian*, though, these conjugations have no effect. So it makes sense to talk about *the* decomposition and inertia groups of $\mathfrak{p}$ itself!

A reciprocity law.

Assuming the Kronecker-Weber theorem, we can deduce strong results about the way primes of $\mathbb{Q}$ split in an abelian extension. Suppose $K/\mathbb{Q}$ is abelian, with conductor m. Then we get a surjective homomorphism

$$(\mathbb{Z}/m\mathbb{Z})^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}).$$

On the other hand, suppose p is a prime not dividing m, so that $K/\mathbb{Q}$ is unramified above p. As noted above, there is a well-defined decomposition group $G_p \subseteq \mathrm{Gal}(K/\mathbb{Q})$. Since there is no ramification above p, the corresponding inertia group is trivial, so G_p is generated by a Frobenius element F_p, which modulo any prime above p, acts as $x \mapsto x^p$. We can formally extend the map $p \mapsto F_p$ to a homomorphism from S_m, the subgroup of $\mathbb{Q}$ generated by all primes not dividing m, to $\mathrm{Gal}(K/\mathbb{Q})$. This is called the *Artin map* of $K/\mathbb{Q}$.

The punchline is that the Artin map factors through the map $(\mathbb{Z}/m\mathbb{Z})^* \to \mathrm{Gal}(K/\mathbb{Q})$ we wrote down above! Namely, note that the image of r under the latter map takes ζ_m to ζ_m^r. For this image to be equal to F_p, we must have $\zeta_m^r \equiv \zeta_m^p \pmod{\mathfrak{p}}$ for some prime $\mathfrak{p}$ of K above p. But $\zeta_m^r(1-\zeta_m^{r-p})$ is only divisible by primes above m (see exercises) unless $r - p \equiv 0 \pmod{m}$. Thus F_p must be equal to the image of p under the map $(\mathbb{Z}/m\mathbb{Z})^* \to \mathrm{Gal}(K/\mathbb{Q})$.

The *Artin reciprocity law* states that a similar phenomenon arises for any abelian extension of any number field; that is, the Frobenius elements corresponding to various primes are governed by the way the primes "reduce" modulo some other quantity. There are several complicating factors in the general case, though:

- Prime ideals in a general number field are not always principal, so we can't always take a generator and reduce it modulo something.
- There can be lots of units in a general number field, so even when a prime ideal is principal, it is unclear which generator to choose.
- It is not known in general how to explicitly construct generators for all of the abelian extensions of a general number field.

Thus our approach will have to be a bit more indirect.

Reduction to the local case.

Our reduction of Kronecker-Weber to local Kronecker-Weber relies on a key result from last semester. (See Neukirch III.2.)

Theorem 3 (Minkowski). *There are no nontrivial extensions of $\mathbb{Q}$ which are unramified everywhere.*

Local KW implies KW. For each prime p over which K ramifies, pick a prime $\mathfrak{p}$ of K over p; by local Kronecker-Weber, $K_\mathfrak{p} \subseteq \mathbb{Q}_p(\zeta_{n_p})$ for some positive integer n_p. Let p^{e_p} be the largest power of p dividing n_p, and put $n = \prod_p p^{e_p}$. (This is a finite product since only finitely many primes ramify in K.)

We will prove that $K \subseteq \mathbb{Q}(\zeta_n)$, by proving that $K(\zeta_n) = \mathbb{Q}(\zeta_n)$. Write $L = K(\zeta_n)$ and let I_p be the inertia group of p in L. If we let U be the maximal unramified subextension of $L_\mathfrak{q}$ over $\mathbb{Q}_p$ for some prime $\mathfrak{q}$ over p, then $L_\mathfrak{p} = U(\zeta_{p^{e_p}})$ and $I_p \cong \mathrm{Gal}(L_\mathfrak{p}/U) \cong (\mathbb{Z}/p^{e_p}\mathbb{Z})^*$. Let I be the group generated by all of the I_p; then

$$|I| \leq \prod |I_p| = \prod \phi(p^{e_p}) = \phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

On the other hand, the fixed field of I is an everywhere unramified extension of $\mathbb{Q}$, which can only be $\mathbb{Q}$ itself by Minkowski's theorem. That is, $I = \mathrm{Gal}(L/\mathbb{Q})$. But then

$$[L : \mathbb{Q}] = |I| \leq [\mathbb{Q}(\zeta_n) : \mathbb{Q}],$$

and $\mathbb{Q}(\zeta_n) \subseteq L$, so we must have $\mathbb{Q}(\zeta_n) = L$ and $K \subseteq \mathbb{Q}(\zeta_n)$, as desired. $\square$

Exercises.

1. For $m \in \mathbb{Z}$ not a perfect square, determine the conductor of $\mathbb{Q}(\sqrt{m})$. (Hint: first consider the case where $|m|$ is prime.)

2. Recover the law of quadratic reciprocity from the Artin reciprocity law, using the fact that $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ has conductor p.

3. Prove that if m, n are coprime integers in $\mathbb{Z}$, then $1 - \zeta_m$ and n are coprime in $\mathbb{Z}[\zeta_m]$. (Hint: look at the polynomial $(x-1)^m - 1$ modulo a prime divisor of n.) Optional: prove that if m is not a prime power, $1 - \zeta_m$ is actually a unit. (Hint: see last semester's final exam for a key special case.)