Class Field Theory

Linus Setiabrata

Lecture 1. Feb 10, 2019

I will try to give a very quick review of "basic" algebraic number theory and then hopefully get through the beginning of Kedlaya's notes, which is a preamble on Kronecker-Weber. In this chapter, Kedlaya follows Lawrence Washington's book (which GTM are you?); Kedlaya's proofs are super condensed, but Washington's are more detailed. Guillot's book also builds up to this theorem, so regardless of whether we want to follow the Brian group or do our own thing, it doesn't hurt to flesh out this theorem.

Let me begin by stealing the following definition from MIT number theory lecture notes. This perspective is different from the definition Zywina used in his 6370, so I was caught off guard a little the first time I saw it:

Definition 1. Let $A \subseteq B$ be rings. An element $b \in B$ is integral over A if b is a root of a monic polynomial in $A[x]$. The ring B is integral over A if all its elements are.

Definition 2. Given a ring extension B/A, the ring $\tilde{A} := \{b \in B : b \text{ is integral over } A\}$ is the integral closure of A in B. When $\tilde{A} = A$ we say that A is integrally closed in B.

Definition 3. A number field K is a finite extension of $\mathbb{Q}$. Its ring of integers $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.

And then sometimes instead of $\mathbb{Z}$ you want to put other rings, which gives this $AKLB$-setup: in general we let A be a Dedekind domain with field of fractions K, and L a finite separable extension, and B the integral closure of A in L. By the way, a Dedekind domain is a integrally closed, Noetherian domain of Krull dimension 1 (i.e., this is equivalent to having all nonzero ideals factor uniquely as a product of prime ideals).

Proposition 4. *If B is an integral extension of A, then $\dim(B) = \dim(A)$. Hence $\mathcal{O}_K$ has dimension 1 for any number field K.*

Some highlights of 6370, which hopefully suffice as a refresher:

Definition 5. A fractional ideal of K is a nonzero finitely generated $\mathcal{O}_K$ submodule $I \subseteq K$. The set of fractional ideals is denoted J_K and they form an abelian group under multiplication.

Definition 6. The ideal class group Cl_K of K is J_K/P_K, where P_K is the subgroup of J_K consisting of those fractional ideals which are principal. The ideal class group Cl_K happens to also be the Picard group of $\mathrm{Spec}(\mathcal{O}_K)$.

Theorem 7. *The ideal class group Cl_K is finite. Specifically, every class in the class group contains an ideal J of $\mathcal{O}_K$ with norm at most*

$$\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\mathrm{disc}(K)|}.$$

Proof. This rests on the fact that if I is a nonzero ideal of $\mathcal{O}_K$, then I contains an element α satisfying

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\mathrm{disc}(K)|} \cdot N(I),$$

which pops out of some Minkowski Theory (geometry of numbers).

Afterwards it is a matter of trickery to conclude that Cl_K is finite (e.g. there are only finitely many ideals of a given norm, bla bla bla...). □

Theorem 8. *Let K be a number field of degree n with r real embeddings and s pairs of complex embeddings. Then $\mathcal{O}_K^\times$ is isomorphic to $\mu_K \times \mathbb{Z}^{r+s-1}$, where μ_K denotes the roots of unity of $\mathcal{O}_K$.*

Proof. You can define a map $\psi\colon K^\times \to \mathbb{R}^{r+s}$ with some nice properties, in particular that $\psi|_{\mathcal{O}_K^\times}$ has kernel μ_K, and that $\psi(\mathcal{O}_K^\times)$ is a lattice in the subspace $\{x \in \mathbb{R}^{r+s} \colon x_1 + \cdots + x_{r+s} = 0\}$. The rest is a long, painful computation. □

Let's talk about field extensions and get more into CFT.

Definition 9. Let L/K be a separable extension. We say L/K is Galois if K is the fixed field of $\mathrm{Aut}(L/K) =: \mathrm{Gal}(L/K)$.

Definition 10. We say L/K is abelian if $\mathrm{Gal}(L/K)$ is abelian.

For example, you have all the cyclotomic fields $\mathbb{Q}(\zeta_n)$, whose Galois group is $(\mathbb{Z}/n\mathbb{Z})^\times$, and all of its subfields (which correspond to subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$ by the fundamental theorem of Galois theory). Kronecker-Weber states that this is the complete list of abelian extensions of $\mathbb{Q}$:

Theorem 11. *If $K/\mathbb{Q}$ is an abelian extension, then $K \subseteq \mathbb{Q}(\zeta_n)$ for some n.*

Then given an abelian extension $K/\mathbb{Q}$, there is a smallest n for which $K \subseteq \mathbb{Q}(\zeta_n)$; this n is called its conductor.

You can easily deduce this theorem from a local analogue, which we'll rove:

Theorem 12. *If $K/\mathbb{Q}_p$ is an abelian extension, then $K \subseteq \mathbb{Q}_p(\zeta_n)$ for some n.*

Recall (hopefully)

Definition 13. Let L/K be a Galois extension and say that $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_L$ so that $\mathfrak{q}$ lies over $\mathfrak{p}$ in $\mathcal{O}_K$. The decomposition group of $\mathfrak{q}$, called $D_\mathfrak{q}$, is the subgroup of $\mathrm{Gal}(L/K)$ that fixes $\mathfrak{q}$.

Thus if $\sigma \in D_\mathfrak{q}$ you get an automorphism

$$\begin{aligned} \mathcal{O}_L/\mathfrak{q} &\to \mathcal{O}_L/\mathfrak{q} \\ x + \mathfrak{q} &\mapsto \sigma(x) + \mathfrak{q} \end{aligned}$$

and hence a homomorphism

$$\varphi\colon D_\mathfrak{q} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}),$$

where $\mathbb{F}_\mathfrak{q} := \mathcal{O}_L/\mathfrak{q}$ (it's a field because $\mathcal{O}_L$ has dimension 1) and $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$. This homomorphism is apparently surjective (Mehrle's 6.17). In any case, we can now define

Definition 14. The kernel of this homomorphism φ is the inertia group $I_\mathfrak{q}$ of $\mathfrak{q}$.

Now the Galois group $\mathrm{Gal}(L/K)$ acts transitively on the set of primes $\mathfrak{q}$ of L dividing a fixed $\mathfrak{p}$ of K; hence if $\mathfrak{q}' = \sigma(\mathfrak{q})$ we have $D_{\mathfrak{q}'} = \sigma D_\mathfrak{q} \sigma^{-1}$ and $I_{\mathfrak{q}'} = \sigma I_\mathfrak{q} \sigma^{-1}$ and if L/K is abelian then $D_{\mathfrak{q}'} = D_\mathfrak{q}$ and $I_{\mathfrak{q}'} = I_\mathfrak{q}$. Hence we can talk about $D_\mathfrak{p}$ and $I_\mathfrak{p}$ instead.

Okay, let's let $K/\mathbb{Q}$ be an abelian extension, with conductor m. There is a surjective homomorphism

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

If p is a prime not dividing m, then $K/\mathbb{Q}$ is unramified above p, and the homomorphism $\varphi\colon D_p \to \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ is injective and hence an isomorphism. Thus D_p is cyclic and, like $\mathrm{Gal}(K/\mathbb{Q})$, is generated by the Frobenius element $\sigma_p\colon x \mapsto x^p \pmod{\mathfrak{p}}$ for any $\mathfrak{p}$ over p. Thus we can define a map $p \mapsto \sigma_p$, which we can formally extend to to the group $S_m \subseteq \mathbb{Q}$ generated by primes not dividing m (as an example, the element $6/5 \in S_7$ gets mapped to $\sigma_2\sigma_3(\sigma_5)^{-1} \in \mathrm{Gal}(K/\mathbb{Q})$).

Definition 15. This map $S_m \to \mathrm{Gal}(K/\mathbb{Q})$ is the Artin map of $K/\mathbb{Q}$.

The Artin map factors through $\varphi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(K/\mathbb{Q})$, that is to say, note that $\varphi(r) \mapsto \{\zeta_m \mapsto \zeta_m^r\}$. If the automorphism $\{\zeta_m \mapsto \zeta_m^r\}$ is equal to the automorphism F_p we need $\zeta_m^r \equiv \zeta_m^p \pmod{\mathfrak{p}}$ for some $\mathfrak{p}$ over p, and this is only true when $r \equiv p \pmod{m}$ ("see exercises", thanks Kedlaya).

Anyways, the Artin reciprocity law states that a similar phenomenon arises for abelian extensions over any number field: Frobenius elements of primes are governed by how they "reduce" modulo some other quantity.

Okay, let's prove Kronecker-Weber from its local analogue.

Proof. Fix a field $K/\mathbb{Q}$; for each prime p where K ramifies pick a $\mathfrak{p}$ over p and note that $K_\mathfrak{p}$, the completion of K with respect to $\mathfrak{p}$, is such that $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) \cong D_\mathfrak{p} \subseteq \mathrm{Gal}(K/\mathbb{Q})$ (the isomorphism is magic) and hence $K_\mathfrak{p}$ is an abelian extension of $\mathbb{Q}_p$. Hence by local Kronecker-Weber we have $K_\mathfrak{p} \subseteq \mathbb{Q}_p(\zeta_{n_p})$ for some n_p. Let e_p be the highest power of p dividing n_p and define $n = \prod_p p^{e_p}$. We show that $L := K(\zeta_n) = \mathbb{Q}(\zeta_n)$.

Note that L is the compositum of K and $\mathbb{Q}(\zeta_n)$ and hence $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and is hence an abelian extension; pick a $\mathfrak{q}$ in L lying above p, and let U be the maximal unramified subextension of $L_\mathfrak{q}$ over $\mathbb{Q}_p$. Then $L_\mathfrak{q}/U$ is totally ramified, and $\mathrm{Gal}(L_\mathfrak{q}/U) \cong I_p$. Notice that $L_\mathfrak{q} \supseteq U(\zeta_{p^{e_p}})$ and that $K_\mathfrak{p} \subseteq \mathbb{Q}_p(n_p) \subseteq U(\zeta_{p^{e_p}})$, so $L_\mathfrak{q} = K_\mathfrak{p}(\zeta_n) \subseteq U(\zeta_{p^{e_p}})$. It follows that $L_\mathfrak{q} = U(\zeta_{p^{e_p}})$ so $I_p \cong (\mathbb{Z}/p^{e_p}\mathbb{Z})^\times$. Now if I is the group generated by all the I_p, we have

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

The fixed field $L^I/\mathbb{Q}$ of I is contained in $L^{I_p}/\mathbb{Q}$ for all p, and $L^{I_p}/\mathbb{Q}$ is unramified at p. Hence $L^I/\mathbb{Q}$ is unramified everywhere and so $L^I = \mathbb{Q}$. So $I = \mathrm{Gal}(L/\mathbb{Q})$ and

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

Because $\mathbb{Q}(\zeta_n) \subseteq L$, we get $\mathbb{Q}(\zeta_n) = L$ as desired. □