# Algebraic Number Theory, a Computational Approach

William Stein

May 31, 2019

# Chapter 1

# The Weak Mordell-Weil Theorem

## 1.1 Kummer Theory of Number Fields

Suppose $K$ is a number field and fix a positive integer $n$. Let $\mu_n$ denote the $n$th roots of unity in $\overline{K}$ as a group under multiplication. Consider the exact sequence

$$1 \to \mu_n \to \overline{K}^* \xrightarrow{n} \overline{K}^* \to 1,$$

where $n$ denotes the map $a \mapsto a^n$.

The corresponding long exact sequence from Theorem **??** is

$$1 \to \mu_n(K) \to K^* \xrightarrow{n} K^* \to H^1(K, \mu_n) \to H^1(K, \overline{K}^*) = 0,$$

where $\mu_n(K)$ is the $n$th roots of unity contained in $K$. The last equality follows from Theorem **??**.

Assume now that the group $\mu_n$ is contained in $K$. Using Galois cohomology we obtain a relatively simple classification of all abelian extensions of $K$ with cyclic Galois group of order dividing $n$. Moreover, since the action of $\mathrm{Gal}(\overline{K}/K)$ on $\mu_n$ is trivial, by our hypothesis that $\mu_n \subset K$, Exercise **??** implies

$$H^1(K, \mu_n) = \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n).$$

Thus we obtain an exact sequence

$$1 \to \mu_n \to K^* \xrightarrow{n} K^* \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n) \to 1,$$

or equivalently, an isomorphism

$$K^*/(K^*)^n \cong \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n).$$

By Galois theory, homomorphisms $\mathrm{Gal}(\overline{K}/K) \to \mu_n$ (up to automorphisms of $\mu_n$) correspond to cyclic abelian extensions of $K$ with Galois group a subgroup of the cyclic group $\mu_n$. Unwinding the definitions, this says that every cyclic abelian extension of $K$ of degree dividing $n$ is of the form $K(a^{1/n})$ for some element $a \in K$.

One can prove via calculations that $K(a^{1/n})$ is unramified outside $n$ and the primes that divide $\mathrm{Norm}(a)$. Moreover, and this is a much bigger result, one can combine this with facts about class groups and unit groups to prove the following theorem:

**Theorem 1.1.1.** *Suppose $K$ is a number field with $\mu_n \subset K$, where $n$ is a positive integer. Let $L$ be the maximal extension of $K$ such that*

*(i)* $\mathrm{Gal}(L/K)$ *is abelian,*

*(ii)* $n \cdot \mathrm{Gal}(L/K) = 0$, *and*

*(iii)* $L$ *is unramified outside a finite set $S$ of primes.*

*Then $L/K$ is of finite degree.*

*Sketch of Proof.* Note that we may enlarge $S$ as needed. To see why, choose a finite set $S' \supseteq S$ and let $L'$ the maximal extension with respect to $S'$ as in the statement of the theorem. Because $L$ is unramified outside of $S$, it is certainly unramified outside of $S'$. By maximality of $L'$ this implies $L \subseteq L'$. Therefore it's sufficient to show the larger extension $L'/K$ is finite.

We first argue that we can enlarge $S$ so that the ring

$$\mathcal{O}_{K,S} = \{a \in K^* \colon \mathrm{Ord}_{\mathfrak{p}}(a\mathcal{O}_K) \geq 0 \text{ for all } \mathfrak{p} \notin S\} \cup \{0\}$$

is a principal ideal domain. One can show that for any $S$, the ring $\overline{K}K,S$ is a Dedekind domain. The condition $\mathrm{Ord}_{\mathfrak{p}}(a\mathcal{O}_K) \geq 0$ means that in the prime ideal factorization of the fractional ideal $a\mathcal{O}_K$, we have that $\mathfrak{p}$ occurs to a nonnegative power. Thus we are allowing denominators at the primes in $S$. Since the class group of $\mathcal{O}_K$ is finite, there are primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ that generate the class group as a group (for example, take all primes with norm up to the Minkowski bound). Enlarge $S$ to contain the primes $\mathfrak{p}_i$.

possible exercise?

Note that we have used that *the class group of $\mathcal{O}_K$ is finite*.

Next we want to show $\mathfrak{p}_i\mathcal{O}_{K,S}$ is the unit ideal. To see this, let $m$ be the order of $\mathfrak{p}_i$ in the class group of $\mathcal{O}_K$ so that $\mathfrak{p}_i^m = (\alpha)$ for some $\alpha \in \mathcal{O}_K$. Note the factorization of $\frac{1}{\alpha}\mathcal{O}_K$ is $\mathfrak{p}_i^{-m}$ so by construction $\frac{1}{\alpha} \in \mathcal{O}_{K,S}$. Since $\alpha \in (\mathfrak{p}_i\mathcal{O}_{K,S})^m$ this shows $(\mathfrak{p}_i\mathcal{O}_{K,S})^m$ is the unit ideal. It follows from the unique factorization of ideals in the Dedekind domain $\mathcal{O}_{K,S}$ that $\mathfrak{p}_i\mathcal{O}_{K,S}$ is the unit ideal.

Now we can show $\mathcal{O}_{K,S}$ is a principal ideal domain. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_{K,S}$. Since the $\mathfrak{p}_i$ generate the class group of $\mathcal{O}_K$, the restriction of $\mathfrak{P}$ to $\mathcal{O}_K$ is equivalent modulo a principal ideal to a product of the primes $\mathfrak{p}_i$. Therefore $\mathfrak{P}$ is equivalent modulo a principal ideal to a product of ideals of the form $\mathfrak{p}_i\mathcal{O}_{K,S}$. Because we showed $\mathfrak{p}_i\mathcal{O}_{K,S}$ was the unit ideal, this means $\mathfrak{P}$ is principal.

Next enlarge $S$ so that all primes over $n\mathcal{O}_K$ are in $S$. Note that $\mathcal{O}_{K,S}$ is still a PID. Let

$$K(S,n) = \{a \in K^*/(K^*)^n \colon n \mid \mathrm{Ord}_{\mathfrak{p}}(a) \text{ for all } \mathfrak{p} \notin S\}.$$

Then a refinement of the arguments at the beginning of this section show that $L$ is generated by all $n$th roots of the elements of $K(S,n)$ (specifically, their representatives in $K$). Thus it suffices to prove that $K(S,n)$ is finite.

If $a \in \mathcal{O}_{K,S}^*$ then $\mathrm{Ord}_{\mathfrak{p}}(a) = 0$ for all $\mathfrak{p} \notin S$. So there is a natural map

$$\phi : \mathcal{O}_{K,S}^* \to K(S,n)$$

sending $a$ to it's residue class in $K^*/(K^*)^n$. Suppose $a \in K^*$ is a representative of an element in $K(S,n)$. The ideal $a\mathcal{O}_{K,S}$ has a factorization which is a product of $n$th powers, so it is an $n$th power of an ideal. Since $\mathcal{O}_{K,S}$ is a PID, there is $b \in \mathcal{O}_{K,S}$ and $u \in \mathcal{O}_{K,S}^*$ such that

$$a = b^n \cdot u.$$

Thus $u \in \mathcal{O}_{K,S}^*$ maps to $[a] \in K(S,n)$. This shows $\phi$ is surjective.

Recall *Dirichlet's unit theorem* (Theorem **??**), which asserts that the group $\mathcal{O}_K^*$ is a finitely generated abelian group of rank $r+s-1$. More generally, we now show that $\mathcal{O}_{K,S}^*$ is a finitely generated abelian group of rank $r+s+\#S-1$. Because we showed $\phi$ is surjective this would imply $K(S,n)$ is finitely generated. Since $K(S,n)$ is also a torsion group it must be finite which proves the theorem.

The fact that $\mathcal{O}_{K,S}^*$ has rank $r+s-1+\#S$ is sometimes referred to as the *$S$-unit theorem* or the *Dirichlet $S$-unit theorem.* To prove this theorem, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be the primes in $S$ and define a map $\phi : \mathcal{O}_{K,S}^* \to \mathbb{Z}^m$ by

$$\phi(u) = (\mathrm{Ord}_{\mathfrak{p}_1}(u), \ldots, \mathrm{Ord}_{\mathfrak{p}_m}(u)).$$

First we show that $\ker(\phi) = \mathcal{O}_K^*$. We have that $u \in \ker(\phi)$ if and only if $u \in \mathcal{O}_{K,S}^*$ and $\mathrm{Ord}_{\mathfrak{p}_i}(u) = 0$ for all $i$; but the latter condition implies that

$u$ is a unit at each prime in $S$. But $u \in \mathcal{O}_{K,S}^*$ implies $\mathrm{Ord}_{\mathfrak{p}}(u) = 0$ for all $\mathfrak{p} \notin S$, so it follows that $\mathrm{Ord}_{\mathfrak{p}}(u) = 0$ for all primes $\mathfrak{p}$ in $\mathcal{O}_K$ and therefore $u \in \mathcal{O}_K^*$. Thus we have an exact sequence

$$1 \to \mathcal{O}_K^* \to \mathcal{O}_{K,S}^* \xrightarrow{\phi} \mathbb{Z}^m.$$

Next we show that the image of $\phi$ has finite index in $\mathbb{Z}^m$. Let $h$ be the class number of $\mathcal{O}_K$. For each $i$ there exists $\alpha_i \in \mathcal{O}_K$ such that $\mathfrak{p}_i^h = (\alpha_i)$. But $\alpha_i \in \mathcal{O}_{K,S}^*$ since $\mathrm{Ord}_{\mathfrak{p}}(\alpha_i) = 0$ for all $\mathfrak{p} \notin S$ (by unique factorization). Then

$$\phi(\alpha_i) = (0, \ldots, 0, h, 0, \ldots, 0).$$

It follows that $(h\mathbb{Z})^m \subset \Im(\phi)$, so the image of $\phi$ has finite index in $\mathbb{Z}^m$. It follows that $\mathcal{O}_{K,S}^*$ has rank equal to $r + s - 1 + \#S$. $\square$

TODO delete this comment?

## 1.2 Proof of the Weak Mordell-Weil Theorem

Suppose $E$ is an elliptic curve over a number field $K$, and fix a positive integer $n$. Just as with number fields, we have an exact sequence

$$0 \to E[n] \to E \xrightarrow{n} E \to 0.$$

Then we have an exact sequence

$$0 \to E[n](K) \to E(K) \xrightarrow{n} E(K) \to H^1(K, E[n]) \to H^1(K, E)[n] \to 0.$$

Note the last term comes from replacing the codomain of $H^1(K, E[n]) \to H^1(K, E)$ by the kernel of $H^1(K, E) \xrightarrow{n} H^1(K, E)$. From this we obtain a short exact sequence

$$0 \to E(K)/nE(K) \to H^1(K, E[n]) \to H^1(K, E)[n] \to 0. \tag{1.1}$$

Now assume, in analogy with Section 1.1, that $E[n] \subset E(K)$, i.e., all $n$-torsion points are defined over $K$. Then the Galois action on $E[n]$ is trivial so by exercise **??** we have

TODO non-canonical iso?

$$H^1(K, E[n]) = \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), E[n]) \cong \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), (\mathbb{Z}/n\mathbb{Z})^2),$$

and the sequence (1.1) induces an inclusion

$$E(K)/nE(K) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), (\mathbb{Z}/n\mathbb{Z})^2). \tag{1.2}$$

Explicitly, this homomorphism sends a point $P$ to the homomorphism defined as follows: Choose $Q \in E(\overline{K})$ such that $nQ = P$; then send each $\sigma \in \mathrm{Gal}(\overline{K}/K)$ to $\sigma(Q) - Q \in E[n]$.

**Exercise 1.2.1.** Consider the map $E(K) \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), E[n])$ defined above. First show this map is well defined, i.e., $\sigma(Q) - Q \in E[n]$ for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then show it does not depend on the choice of $P$ modulo $nE(K)$ so it indeed descends to a homomorphism on $E(K)/nE(K)$.

Because $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$, given a point $P \in E(K)$, we obtain a homomorphism $\varphi : \mathrm{Gal}(\overline{K}/K) \to (\mathbb{Z}/n\mathbb{Z})^2$, whose kernel defines an abelian extension $L$ of $K$ that has exponent $n$. The amazing fact is that $L$ can be ramified only at the primes of bad reduction for $E$ and the primes that divide $n$. Thus we can apply theorem 1.1.1 to see that there are only finitely many such $L$.

TODO non-canonical iso?

**Theorem 1.2.2.** *Let $P \in E(K)$ and $L$ be the field obtained by adjoining the coordinates of all points $Q \in E(\overline{K})$ such that $nQ = P$. Then $L/K$ is unramified outside the set of primes dividing $n$ and primes of bad reduction for $E$.*

*Sketch of Proof.* This sketch closely follows [Sil92, Prop. VIII.1.5b].

Fix a prime $\mathfrak{p}$ of $K$ such that $\mathfrak{p} \nmid n$ and $E$ has good reduction at $\mathfrak{p}$. Let $\mathfrak{q}$ be a prime of $L$ lying over $\mathfrak{p}$. Note that $\mathfrak{q}$ is again a prime of good reduction for $E$ since we may use the same Weierstrass equation for $E$ as an elliptic curve over $L$.

First one proves that for any extension $K'/K$ and any prime $\mathfrak{p}'$ of $K'$ such that $\mathfrak{p}' \nmid n$ and $\mathfrak{p}'$ is a prime of good reduction for $E/K'$, the natural reduction map $\pi : E(K')[n] \to \tilde{E}(\mathcal{O}_{K'}/\mathfrak{p}')$ is injective. The argument that $\pi$ is injective uses *formal groups*, whose development is outside the scope of this course.[1]

Next, fix some $Q \in E[n]$ such that $nQ = P$. From Exercise 1.2.1 we have that $\sigma(Q) - Q \in E[n]$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Let $I_\mathfrak{q} \subset \mathrm{Gal}(L/K)$ be the inertia group for $\mathfrak{q}/\mathfrak{p}$. The action of $I_\mathfrak{q}$ is trivial on $\tilde{E}(\mathcal{O}_L/\mathfrak{q})$ so for each $\sigma \in I_\mathfrak{q}$ we have

$$\pi(\sigma(Q) - Q) = \sigma(\pi(Q)) - \pi(Q) = \pi(Q) - \pi(Q) = 0.$$

Since $\pi$ is injective, it follows that $\sigma(Q) = Q$ for $\sigma \in I_\mathfrak{q}$, i.e., that $Q$ is fixed under $I_\mathfrak{q}$. Repeating this argument for each $Q$ implies $I_\mathfrak{q}$ is trivial and hence $\mathfrak{q}/\mathfrak{p}$ is unramified. □

**Theorem 1.2.3** (Weak Mordell-Weil)**.** *Let $E$ be an elliptic curve over a number field $K$, and let $n$ be any positive integer. Then $E(K)/nE(K)$ is finitely generated.*

[1] For a proof using formal groups see [Sil92, Prop. VII.3.1b].

*Proof.* First suppose all elements of $E[n]$ have coordinates in $K$. Then the homomorphism (1.2) provides an injection of $E(K)/nE(K)$ into

$$\mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), (\mathbb{Z}/n\mathbb{Z})^2).$$

By Theorem 1.2.2, the image consists of homomorphisms whose kernels cut out an abelian extension of $K$ unramified outside $n$ and primes of bad reduction for $E$. Since this is a finite set of primes, Theorem 1.1.1 implies that the homomorphisms all factor through a finite quotient $\mathrm{Gal}(L/K)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Thus there can be only finitely many such homomorphisms, so the image of $E(K)/nE(K)$ is finite. Thus $E(K)/nE(K)$ itself is finite, which proves the theorem in this case.

Next suppose $E$ is an elliptic curve over a number field, but do *not* make the hypothesis that the elements of $E[n]$ have coordinates in $K$. Since the group $E[n](\mathbb{C})$ is finite and its elements are defined over $\overline{\mathbb{Q}}$, the extension $L$ of $K$ got by adjoining to $K$ all coordinates of elements of $E[n](\mathbb{C})$ is a finite extension. It is also Galois, as we saw when constructing Galois representations attached to elliptic curves. By Proposition **??**, we have an exact sequence

$$0 \to H^1(L/K, E[n](L)) \to H^1(K, E[n]) \to H^1(L, E[n]).$$

The kernel of the restriction map $H^1(K, E[n]) \to H^1(L, E[n])$ is finite, since it is isomorphic to the finite cohomology group $H^1(L/K, E[n](L))$. By the argument of the previous paragraph, the image of $E(K)/nE(K)$ in $H^1(L, E[n])$ under

$$E(K)/nE(K) \hookrightarrow H^1(K, E[n]) \xrightarrow{\mathrm{res}} H^1(L, E[n])$$

is finite, since it is contained in the image of $E(L)/nE(L)$. Thus $E(K)/nE(K)$ is finite, since we just proved the kernel of res is finite. □

# Bibliography

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.