GLOBAL STATEMENTS OF CLASS FIELD THEORY

ISHAN LEVY

1. The Hilbert class field

What can we say in general about the problem of for some $n > 0$ finding when $p = x^2 + ny^2$? Here we will look at the problem from a more modern perspective using orders inside number fields. A modern approach is to factor the right hand side as $(x + \sqrt{-n}y)(x - \sqrt{-n}y)$. So to say that p is of the form $x^2 + ny^2$ is exactly to say that p factors into two irreducible elements in $\mathbb{Z}[\sqrt{-n}]$. This is the not the same as saying that the ideal (p) splits in $\mathbb{Z}[\sqrt{n}]$: for example $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$, but 3 is not of the form $x^2 + 5y^2$. That is however because the ideal is not principle.

Lemma 1.1. *$p = x^2 + ny^2$ iff (p) factors in $\mathbb{Z}[\sqrt{-n}]$ into two principle ideals of norm p.*

Proof. $p = x^2 + ny^2 \iff (p) = (x + \sqrt{-n}y)(x - \sqrt{-n}y) = (N(x \pm \sqrt{-n}y))$. □

Ignoring the ramifying primes, we can split the problem into two steps: figuring out when p splits in $\mathbb{Z}[\sqrt{-n}]$, and figuring out when the ideals it splits into are principle.

Lemma 1.2. *Suppose that $p \nmid 4n = \mathrm{disc}(\mathbb{Z}[\sqrt{-n}])$. Then $-n$ is a square mod p iff (p) splits in $\mathbb{Z}[\sqrt{-n}]$.*

Proof. $\mathbb{Z}[\sqrt{-n}]/(p) = \mathbb{Z}/p\mathbb{Z}[x]/(x^2 + n)$ shows that (p) is prime in $\mathbb{Z}[\sqrt{-n}]$ iff $x^2 + n$ is irreducible mod p iff $-n$ is not a square mod p. □

Exercise 1.2.1. *Use quadratic reciprocity to show that for $p \nmid 4n$, whether or not (p) factors in $\mathbb{Z}[\sqrt{-n}]$ is a congruence condition on p modulo $4n$.*

If $\mathbb{Z}[\sqrt{-n}]$ is a PID, then this already solves our problem. For example we get that $p = x^2 + y^2$ iff $p \equiv 1 \pmod 4$. Last time, we saw that we were able to find out that $p = x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20}$, but -5 is a square mod p iff $p \equiv 1, 3, 7, 9 \pmod{20}$. So somehow, the primes that are principle are exactly the ones for which -5 is a square mod p, but also $p \equiv 1 \pmod 4$ in addition. $p \equiv 1 \pmod 4$ is also the condition for a prime to split in $\mathbb{Z}[i]$. If p splits in both $\mathbb{Z}[i], \mathbb{Z}[\sqrt{-5}]$, it splits completely in the (ring of integers of the) composite field $\mathbb{Q}[\sqrt{-5}, \sqrt{-1}]$. Thus we have found an extension of $\mathbb{Q}[\sqrt{-5}]$ that has the property that if p splits into $\mathfrak{p}\bar{\mathfrak{p}}$

in $\mathbb{Q}[\sqrt{-5}]$, it splits into principle ideals iff $\mathfrak{p}$ splits further in $\mathbb{Q}[\sqrt{-5}, \sqrt{-1}]$. This motivates the following definition:

Definition 1.3. *L is the **Hilbert class field** of K if it is a finite extension and a prime in $\mathcal{O}_K$ is principle iff there is a prime over it in L with residual degree 1.*

Exercise 1.3.1. *What is the Hilbert class field of $\mathbb{Q}[\sqrt{-6}]$?*

As of now, don't know whether it always exists and if it is unique, but we will assume this for now. In fact not only is it unique, but it is an abelian extension of the base field. This definition is good enough to solve our problem completely when $\mathbb{Z}[\sqrt{-n}]$ is the full ring of integers:

Corollary 1.4. *Let $n \equiv 2, 3 \pmod 4$ be square free, suppose $p \nmid 4n$, and let L be the Hilbert class field of $\mathbb{Q}[\sqrt{-n}]$. Then $p = x^2 + ny^2$ iff $-n$ is a square $\pmod p$ and there is a prime over p in the the Hilbert class field L with residual degree 1.*

Splitting completely in the field L might seem like an abstract condition to put on a prime, but it can be made pretty concrete. Let α be a integer in L generating the field over $\mathbb{Q}$. $\mathbb{Z}[\alpha]$ isn't *that* different from $\mathcal{O}_L$, it is a subring of finite index, and we can calculate the index by looking at the discriminant of $\mathbb{Z}[\alpha]$. In particular, after adjoining inverses of finitely many primes $p_1, \dots p_n$ dividing the discriminant of $\mathbb{Z}[\alpha]$ (this is the same as the discriminant of the minimal polynomial of α), $\mathbb{Z}[\alpha, \frac{1}{p_i}, 1 \leq i \leq n] = \mathcal{O}_K[\frac{1}{p_i}, 1 \leq i \leq n]$. Then except for these finitely many primes, we should be able to tell if p splits iff the minimal polynomial of α factors into linear factors, but since the extension is Galois, this is equivalent to the minimal polynomial having a root mod p.

Theorem 1.5. *Let $n \equiv 2, 3 \pmod 4$ be square free. Then if the Hilbert class field exists, and f is the minimal polynomial of a generating integer, there is a polynomial f such that for $p \nmid \operatorname{disc}(f)$, $p = x^2 + ny^2$ iff f has a root mod p.*

2. Global Class Field Theory

So why does the Hilbert class field exist, and why is it unique? This is a consequence of the results of class field theory. The main object that class field theory is about is the **Artin map**. Recall that given a Galois extension L/K, and an unramified prime $\mathfrak{p} \subset K$, and a prime $\mathfrak{P}$ lying over $\mathfrak{p}$, then $\mathfrak{P}$ has a decomposition group, $D(\mathfrak{P})$, the elements in the Galois group fixing $\mathfrak{P}$. If $\tilde{k}$ is the residue field of $\mathfrak{P}$, and k that of $\mathfrak{p}$, then reduction gives an isomorphism $D(\mathfrak{P}) \to \operatorname{Gal}(\tilde{k}/k)$. $\operatorname{Gal}(\tilde{k}/k)$ has a canonical generator called **Frobenius**, given by $x \to x^p$, where p is the characteristic. Via the isomorphism above, we can call the corresponding generator of $D(\mathfrak{P})$ Frobenius. It's conjugacy class only depends on $\mathfrak{p}$ and not $\mathfrak{P}$.

We can see how this relates to our discussion of the Hilbert class field.

Lemma 2.1. *The Frobenius of an unramified prime ideal $\mathfrak{p}$ in is trivial iff $\mathfrak{p}$ splits completely in the extension.*

Proof. Note that since the Frobenius generates the decomposition group, it is trivial iff the decomposition group is trivial iff the extension of residue fields is trivial, meaning the prime splits completely. □

If the extension is abelian, then the conjugacy classes are all size 1, so this only depends on $\mathfrak{p}$. If I_{ur} is a the fractional ideals generated by the unramified primes, then there is a well-defined map called the Artin map $(\frac{L/K}{-}) : I_{ur} \to \mathrm{Gal}(L/K)$ that on primes is defined to be Frobenius, and is extended to a homomorphism. Moreover, the Artin map is natural, meaning that if $M \supset L$ are two abelian extensions, and $\mathfrak{a}$ is a fractional ideal in K not ramifying in both M, L, then restricting $(\frac{M/K}{\mathfrak{a}})$ to $\mathrm{Gal}(L/K)$ yields $(\frac{L/K}{\mathfrak{a}})$.

Exercise 2.1.1. *Prove the Artin map is natural as described.*

Let's look at an example, the cyclotomic fields $\mathbb{Q}[\zeta_n]/\mathbb{Q}$. Here the Galois group is canonically identified with $\mathbb{Z}/n\mathbb{Z}^\times$ via $\sigma_a \to a$ if $\sigma_a(\zeta_n) = \zeta_n^a$. q is unramified iff $q \nmid n$, and in this case, $\sigma_q(\zeta_n) \equiv \zeta_n^q \pmod q$, so $q \in \mathbb{Z}/n\mathbb{Z}^\times$ is our candidate for Frobenius. Indeed, the polynomial $x^n - 1$ is separable over $\mathbb{Z}/q\mathbb{Z}$, so only one primitive n^{th} root of unity satisfies the congruence above, and so the Artin map sends a fractional ideal $(a) \mapsto a \in \mathbb{Z}/n\mathbb{Z}^\times$ for positive a. The kernel is then the fractional ideals relatively prime to n whose positive generator is congruent to 1 modulo n.

Now let's compute the Artin map for $\mathbb{Q}[\sqrt{n}]$. Let p be an odd prime. Then p splits in $\mathcal{O}_{\mathbb{Q}[\sqrt{n}]}$ iff it splits in $\mathbb{Z}[\sqrt{n}]$ (after inverting 2, these become the same ring), which happens iff n is a square mod p iff $(\frac{n}{p})$=1. Thus the Artin map for odd p is $(\frac{n}{p})$ and extending multiplicatively gives the Jacobi symbol $(\frac{n}{a})$.

Before moving on, let's give a quick proof of quadratic reciprocity using the cyclotomic field $\mathbb{Q}[\zeta_q]$, q odd. The $(\frac{a}{q})$ is the unique surjective homomorphism $\mathbb{Z}/q\mathbb{Z}^\times \to \mathbb{Z}/2\mathbb{Z}$ as the former group is cyclic. By Galois theory, this surjective map corresponds to the quadratic subfield of $\mathbb{Q}[\zeta_q]$. But only q ramifies in $\mathbb{Q}[\zeta_q]$, and the only quadratic number field with that property is $\mathbb{Q}[\sqrt{q^*}]$ where $q^* = (-1)^{\frac{q-1}{2}} q$. But the Artin map for this subfield is given by the Jacobi symbol $(\frac{q^*}{a})$. By naturality of the Artin map we then have, $a \mapsto (\frac{q^*}{a})$ is a surjective homomorphism from $\mathbb{Z}/q\mathbb{Z}^\times \to \mathbb{Z}/2\mathbb{Z}$ so $(\frac{q^*}{a}) = (\frac{a}{q})$.

Exercise 2.1.2. *Compute $(\frac{2}{p}), (\frac{-1}{p})$ by examining the cyclotomic field $\mathbb{Q}[\zeta_8]$.*

For another example, let's examine the Hilbert class field K of $\mathbb{Q}[\sqrt{-5}]$ again. It has two other quadratic subfields, $\mathbb{Q}[\sqrt{5}], \mathbb{Q}[\sqrt{-1}]$. Note that only 2 ramifies in one

of them, and only 5 ramifies in the other, so only $2, 5$ ramify from $\mathbb{Q}$ to K with degree 2. But they ramify in $\mathbb{Q}[\sqrt{-5}]$, so nothing can ramify from $\mathbb{Q}[\sqrt{-5}]$ to K, and so K is an unramified abelian extension of $\mathbb{Q}[\sqrt{-5}]$. The ideal class group of $\mathbb{Q}[\sqrt{-5}]$ is $\mathbb{Z}/2\mathbb{Z}$ (we will see why this can be computed using quadratic forms later), and a prime is in the kernel iff it splits iff it is principle, so the kernel is exactly the principle fractional ideals. Thus the Artin map gives an isomorphism $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) \to \mathrm{Gal}(K/\mathbb{Q}[\sqrt{-5}])$.

Class field theory says that the Artin map always gives an isomorphism between some generalized ideal class group and the Galois group of an abelian extension. More precisely, let m_0 be an ideal in $\mathcal{O}_K$, let m_∞ be a collection of real embeddings of K, and let $m = (m_0, m_\infty)$. m is called a **modulus**. Let I_m be the subgroup of fractional ideals relatively prime to m, and let P_m be the subgroup of principle ideals (α) that are congruent to 1 modulo m and have $\sigma(\alpha) > 0$ for all $\sigma \in m_\infty$. Then if H is a subgroup containing P_m, the quotient I_m/H is said to be a **generalized class group**.

The first theorem of class field theory is Artin Reciprocity.

Theorem 2.2 (Artin Reciprocity)**.** *The Artin map $I_{ur} \to \mathrm{Gal}(L/K)$ of a finite abelian extension of number fields is surjective. The kernel H always contains some P_m, where m is a suitably chosen ideal, and so the Artin map induces an isomorphism $I_m/H \to \mathrm{Gal}(L/K)$.*

For example, we can see that the kernel in the case of $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is P_m, where $m_0 = n$ and m_∞ is the unique embedding of $\mathbb{Q}$.

Exercise 2.2.1. *Find an abelian extension of $\mathbb{Q}$ such that the Artin map's kernel is P_m, $m_0 = n$, $m_\infty = \{\}$.*

Actually, given an abelian extension, there is a canonical m to be chosen, called the **conductor**.

Theorem 2.3 (Conductor Theorem)**.** *In the setup above, there is a unique m such that the Artin map induces an isomorphism for the modulus m' iff $m|m'$. Moreover, the primes dividing m are exactly the primes that ramify.*

By an embedding in m_∞ ramifying, it is meant that it extends to a complex embedding in the extension.

Finally there is a converse to Artin reciprocity, the existence theorem.

Theorem 2.4 (Existence Theorem)**.** *Given an $H \supset P_m$, there is a unique abelian extension L/K such that the Artin map induces an isomorphism $I_m/H \to \mathrm{Gal}(L/K)$.*

Corollary 2.5. *The Hilbert class field of K exists.*

Proof. Use the existence theorem when $m_0 = (1), m_\infty = \{\}$ and H is the principle fractional ideals. □