18 The Ideal Class Group

18.1 Review — Function Fields

Last time, we discussed a generalization where we replace $\mathbb{Q}$ and $\mathbb{Z}$ with $k(t)$ and $k[t]$, for a field k — instead of working with finite extensions of $\mathbb{Q}$ (or number fields), we work with finite extensions of $k(t)$ (or function fields). For concreteness, we'll focus on $k = \mathbb{C}$.

In order to keep the same level of generality as we had when working with number fields, we will take F to be a *quadratic* extension of $\mathbb{C}(t)$, so

$$F = \mathbb{C}(t)[z]/(z^2 - P(t))$$

for some polynomial $P(t)$, which we may without loss of generality assume to be squarefree. Here $P(t)$ plays the same role as d did when we considered quadratic *number* fields $\mathbb{Q}[\sqrt{d}]$, which could also be described as $\mathbb{Q}[x]/(x^2 - d)$. In this setting, the analog of the ring of algebraic integers, which was $\mathbb{Z}[\sqrt{-d}] = \mathbb{Z}[x]/(x^2 - d)$ in the quadratic number field setting, is

$$R = \mathbb{C}[t][z]/(z^2 - P(t)).$$

In this setting, unique factorization into ideals still holds, although we will not discuss the proof:

Theorem 18.1
Every ideal in R can be factored uniquely as a product of prime ideals.

In particular, all prime ideals are maximal — in fact, this can be proven using a similar argument to the one we saw for number fields, but using that R mod an ideal is finite-dimensional as a $\mathbb{C}$-vector space, rather than that it is finite.

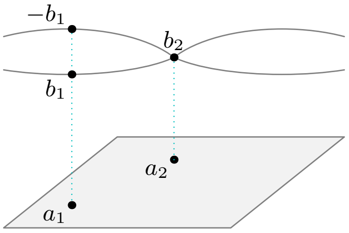
In number fields, we described how prime ideals (q) in the original ring $\mathbb{Z}$ factor as a product of ideals in the new ring R. We can ask the same question in this setting as well.

Guiding Question
How do the prime ideals in $\mathbb{C}[t]$ factor as a product of prime ideals in R?

In both cases, the prime ideals are exactly the maximal ones. Describing the maximal ideals in $\mathbb{C}[t]$ is simple — the only irreducible polynomials in $\mathbb{C}[t]$ are linear, so these prime ideals are of the form $(t - \lambda)$ for $\lambda \in \mathbb{C}$.

Meanwhile, to understand the maximal ideals in R, we can use Nullstelensatz! So far we have been thinking of R as a quadratic extension, but we could instead think of it as the quotient of a two-variable polynomial ring — we have $R = \mathbb{C}[t, z]/(z^2 - P(t))$. Hilbert's Nullstelensatz tells us that the maximal ideals of $\mathbb{C}[t, z]$ are exactly $\mathfrak{m}_{a,b} = (t - a, z - b)$ for $(a, b) \in \mathbb{C}$, so the maximal ideals of R are exactly those $\mathfrak{m}_{a,b}$ for which $b^2 = P(a)$.

So maximal ideals in $\mathbb{C}[t]$ are in bijection with $\mathbb{C}$, and maximal ideals in R are in bijection with solutions in $\mathbb{C}^2$ to $b^2 = P(a)$. This gives a **ramified double cover** — each value of a corresponds to two values of b, except the roots of P, which correspond to one value of b. In the case of imaginary quadratic number fields, we had complex conjugation; the analog in this setting is the map $b \mapsto -b$.



Now that we have a description of what the maximal (and therefore prime) ideals in $\mathbb{C}[t]$ and R are, we can answer our question. A prime ideal $(t - \lambda) \subset \mathbb{C}[t]$ is contained in $\mathfrak{m}_{a,b}$ if and only if $a = \lambda$. So if λ is not a root of P, we get two prime ideals of R containing $(t - \lambda)$, while if λ is a root of P, we get only one. In either case, we can check that

$$(t - \lambda) = \mathfrak{m}_{\lambda,b}\mathfrak{m}_{\lambda,-b},$$

where b is a root of $b^2 = P(\lambda)$. Similarly to the case of integers, $(t - \lambda)$ is a **splitting prime** if λ is not a root of P, since it factors as a product of two distinct ideals; and $(t - \lambda)$ is a **ramified prime** if λ is a root of P, since it factors as a product of two copies of the same ideal. Note that there are no inert (or non-splitting) primes in this situation, since $\mathbb{C}$ is algebraically closed; if we instead worked with a field such as $\mathbb{F}_p$, there would be inert primes as well.

Just as in the case of quadratic number fields, R will not usually have unique factorization in *elements*. But there are some examples where there *is* unique factorization into elements; then all ideals are principal (which is not true in general), and factorization into ideals just becomes factorization into elements.

Example 18.2
When $P(t) = t$, we have $R = \mathbb{C}[z, t]/(z^2 - t) \cong \mathbb{C}[z]$. In this case, $(t - \lambda)$ factors as

$$(t - \lambda) = (z - \sqrt{\lambda})(z + \sqrt{\lambda}).$$

Here is a table of the counterparts between $\mathbb{Z}$ and $\mathbb{C}[t]$ (assume $d \not\equiv 1 \pmod 4$ for simplicity):

$\mathbb{Z}$	$\mathbb{Z}[\sqrt{d}]$	primes	ramified primes	splitting primes
$\mathbb{C}[t]$	$\mathbb{C}[t, z]/(z^2 - P(t))$	$t - \lambda$	$t - \lambda$ where $P(\lambda) = 0$	$t - \lambda$ where $P(\lambda) \neq 0$

Now we'll return to number fields. We previously defined the **ideal class group** $\mathrm{Cl}(F)$. We've already discussed that it's a group, but today we'll see that it's finite.

18.2 Application to Fermat's Last Theorem

Before we discuss the proof of finiteness, we'll circle back to an application to Fermat's Last Theorem. It suffices to consider the case where the exponent is prime. So suppose we want to solve $a^p + b^p = c^p$ over the integers, where p is an odd prime.

Then if ζ is a pth root of unity, in the field $F = \mathbb{Q}[\zeta]$ we can factor

$$(a + b)(a + \zeta b) \cdots (a + \zeta^{p-1} b) = c^p.$$

Assuming that no two factors have a common divisor, we want to conclude that each factor is a pth power — just as we would over the integers, since in that case every prime must have exponent divisible by p — meaning that $a + \zeta^n b = c_n^p \cdot u_n$ for a unit u_n.

We can do this if R is a PID, which is equivalent to $\mathrm{Cl}(F)$ being trivial — the unit in $\mathrm{Cl}(F)$ corresponds to principal ideals, so the group is trivial if and only if all ideals are principal. But this only happens for very few primes (which are all at most 19). However, it turns out that there's a more general condition we can use instead:

Definition 18.3
A prime p is **regular** if $p \nmid \# \mathrm{Cl}(F)$.

There are many regular primes: in fact, the only irregular primes $p \leq 100$ are 37, 59, and 67. So this covers many more cases than the requirement that $\mathbb{Z}[\zeta]$ be a PID. It's still unknown whether there's infinitely many regular primes, though.

Proposition 18.4
We can still conclude each factor is a pth power if p is regular.

Proof. First, using unique factorization for ideals, we see that the *ideal* $(a + \zeta^n b)$ is a pth power, meaning that $(a + \zeta^n b) = I^p$ for some ideal I.

Now it remains to check that I is principal, or equivalently, that its class $[I]$ is trivial. But we know I^p is principal, so $[I]^p = 1$. Now using regularity, no element of the class group has order p; so we must have $[I] = 1$ as well. □

There are still further steps — we then have to consider the case where the factors are *not* coprime as well. In the case where a, b, and c are not divisible by p, the factors are always coprime, and we can use this argument and get a contradiction with a bit more work. When one of them is divisible by p, a different argument is needed. But this is the key ingredient — the rest is clever but elementary.

18.3 Finiteness of the Class Group

Theorem 18.5
The class group $\mathrm{Cl}(F)$ is finite.

As usual, we'll see how to prove this for imaginary quadratic number fields. The key claim is the following:

Proposition 18.6
Every ideal class has a representative with bounded norm — more precisely, with norm at most

$$\mu = \begin{cases} \sqrt{|d|/3} & \text{if } d \equiv 1 \pmod 4 \\ 2\sqrt{|d|/3} & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

It's clear that this proposition implies the class group is finite, since there are finitely many ideals of any given norm. In fact, it also gives us an effective way to *compute* the class group — it implies that the class group is generated by the classes of ideals with norm $p \le \mu$ for primes p. For each prime p, there are at most two ideals with norm p, which can be found by attempting to factor (p) as a product of ideals; then it's enough to find all these ideals and the relations between them.

To prove this proposition, we'll first prove the following lemma:

Lemma 18.7
An ideal I of norm n contains a nonzero element $\alpha \neq 0$ with $\alpha\overline{\alpha} \le \mu n$.

The lemma itself can be proved by elementary geometry on lattices, so we'll first look at how it implies the proposition.

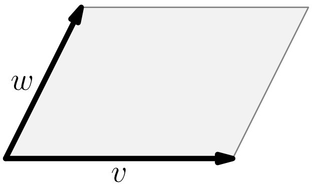
Proof of Proposition 18.6. Choose some nonzero ideal I of norm n in the given class, and find $\alpha \in \overline{I}$ with $|\alpha|^2 \le \mu n$. We saw previously that inclusion of ideals implies divisibility, so then since $(\alpha) \subset \overline{I}$, we can write $(\alpha) = \overline{I}J$ for some ideal J.

But then $[J] = [I] = [\overline{I}]^{-1}$, because $J\overline{I} = (\alpha)$ and $I\overline{I} = (n)$ are both principal.

On the other hand, norm is multiplicative, so we have $\mathrm{N}(J)\,\mathrm{N}(\overline{I}) = \mathrm{N}(\alpha)$. So then

$$\mathrm{N}(J) = \frac{|\alpha|^2}{n} \le \mu. \qquad \square$$

Proof of Lemma 18.7. For a lattice $L \subset \mathbb{R}^2$, define Δ_L as the area of its **fundamental parallelogram**, the parallelogram spanned by two vectors v and w for which $L = \{nv + mw \mid n, m \in \mathbb{Z}\}$.



By elementary linear algebra, we can show that Δ_L doesn't depend on the choice of basis vectors. Furthermore, if $L' \subset L$, then one fundamental paralellogram of L can be obtained by taking the union of $[L : L']$ copies of the fundamental parallelogram of L', so $\Delta_{L'} = [L : L']\Delta_L$.

Now let $v \in L$ be a vector of minimal length.

Claim. *We have the bound* $|v|^2 \cdot \sqrt{3}/2 \leq \Delta_I$.

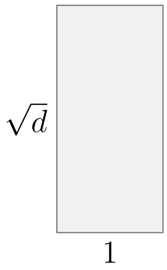
Proof. If v is the shortest vector, and w the shortest vector with $w \neq cv$, then v and w must span the lattice. Without loss of generality we can assume the angle α between v and w is at most $\pi/2$. Then we must have $\alpha \geq \pi/3$, or else $w - v$ has smaller length. Then

$$\Delta_I = |w| \cdot |v| \cdot \sin\alpha \geq \frac{\sqrt{3}}{2}|v|^2. \qquad \square$$

Now it remains to relate Δ_I to $\mathrm{N}(I)$: we claim that

$$\Delta_I = \begin{cases} \mathrm{N}(I)\sqrt{d} & \text{if } d \not\equiv 1 \pmod 4 \\ \mathrm{N}(I)\sqrt{d}/2 & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

This is true when $I = (1)$ — for example, if $d \not\equiv 1 \pmod 4$, then the fundamental parallelogram is a rectangle.



So now we can attempt to reduce the general case to the case $I = (1)$, using the following claim:

Claim. *We have* $\mathrm{N}(I) = [R : I]$.

Proof. It suffices to show that if P is a prime ideal and J any ideal, then $[J : PJ] = \mathrm{N}(P)$ — then we can factor I as a product of primes, and use this property repeatedly. This is obvious when P is principal, so now suppose $P\overline{P} = (q)$ for a prime q. Then we have

$$[J : PJ] \cdot [PJ : P\overline{P}J] = [J : qJ] = q^2,$$

since for any lattice L and integer n, we have $L/nL \cong (\mathbb{Z}/n)^2$. Then q^2 is the product of two integers, both not equal to 1; so each must be q. $\square$

Now we have $\Delta_I = [R : I]\Delta_R = \mathrm{N}(I)\Delta_R$. This gives the claimed expression for Δ_I, and therefore for $|v|$ using the previous claim. $\square$

This concludes the proof of the finiteness of the class group for imaginary quadratic number fields.

Resource: Algebra II Student Notes
Spring 2022
Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng