17 Ideals in Quadratic Fields

17.1 Prime Ideals

Guiding Question

What are the prime ideals in $R \subset \mathbb{Q}[\sqrt{d}]$?

The answer is similar to the case $R = \mathbb{Z}[i]$, which we've seen earlier.

Lemma 17.1

If P is a prime (nonzero) ideal in R, then either $P = (q)$ for an integer prime q, or $P\overline{P} = (q)$ for an integer prime q.

Proof. Suppose $P\overline{P} = (n)$, where n is not prime. Then we can factor $n = ab$ with $a, b \neq \pm 1$. But then by unique ideal factorization (since P and $\overline{P}$ are prime), it follows that $(a) = P$ and $(b) = \overline{P}$, or vice versa. Then we must have $a = b = q$ for a prime q. □

Lemma 17.2

An odd integer prime q remains prime in R if and only if the equation $\overline{a}^2 = d\overline{b}^2$ has no solutions in $\mathbb{F}_q$ except $(0, 0)$, or equivalently, if d is neither 0 nor a square mod q.

Proof. First, suppose (q) is prime, and there exists a solution in $\mathbb{F}_q$ to $\overline{a}^2 = d\overline{b}^2$. Then

$$q \mid (a - b\sqrt{d})(a + b\sqrt{d}).$$

Since q is prime, then q must divide one of $a \pm b\sqrt{d}$, and therefore $q \mid a$ and $q \mid b$.

Conversely, if q is not prime, then we can find α and β such that $q \mid \alpha\beta$ but q does not divide either α or β. But since $q \mid \alpha\beta$, we have

$$q \mid \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta).$$

So since q is an integer prime, it must divide one of the factors on the right; without loss of generality, $q \mid \mathrm{N}(\alpha)$. Now write $\alpha = a + b\sqrt{d}$, so we get that

$$q \mid a^2 - db^2.$$

(It's possible that a and b are half-integers instead of integers; if so, we can replace them with $(2a, 2b)$ without affecting the rest of the argument.) Since q doesn't divide α in R, then q cannot divide both a and b; so $(a, b) \neq (0, 0)$ is a solution to $\overline{a}^2 = d\overline{b}^2$. □

Student Question. *In the first lemma, how did we conclude that P and $\overline{P}$ are (a) and (b)?*

Answer. *We know that (n) is the product of two primes, P and $\overline{P}$. But then the only way to factor it (where neither factor is the unit ideal) is as the product of those two primes — and since it also factors as $(a)(b)$, then (a) and (b) must be those two primes. As an analogy in $\mathbb{Z}$, the only way to factor 6 is as $2 \cdot 3$.*

Student Question. *Did we use the fact that d was negative here?*

Answer. *Somewhat — our proof involved complex conjugation, which relies on d being negative. But if we modify our operation of conjugation, then this analysis works for real quadratic fields as well — we'll discuss this later today.*

Student Question. *Why is $q = 2$ a special case?*

Answer. *It has to do with the fact that if $d \equiv 1 \pmod 4$, then we may have half-integers, such as $(1 + \sqrt{d})/2$. In the case where q was odd, this didn't really matter; but we have to be more careful when $q = 2$. In particular, in the first direction knowing that 2 divides $a + b\sqrt{d}$ in R does not necessarily imply that 2 divides a and b in $\mathbb{Z}$.*

Combining these two results, we get a full list of primes in R:

- For each integer prime $q \nmid d$ where d is not a square mod q (equivalently, there are no solutions to $\overline{a}^2 = d\overline{b}^2$), we get the prime q itself.
- For all other primes, we can factor $q = P\overline{P}$. In most cases, P and $\overline{P}$ are distinct, and this gives two prime ideals. But there's finitely many ramification primes where $P = \overline{P}$, and we get one prime ideal. In fact, these ramification primes are the divisors of d, along with 2 if $d \not\equiv 1 \pmod 4$.

17.2 The Ideal Class Group

Previously, we introduced the ideal class group $\mathrm{Cl}(F)$, which consists of the nonzero ideals in R up to similarity.

Theorem 17.3
The ideal class group $\mathrm{Cl}(F)$ is finite.

We'll prove this in a future class; but for now, we'll look at a few examples.

Example 17.4
In the cases of $\mathbb{Z}[i] \subset \mathbb{Q}[i]$ and $\mathbb{Z}[\omega] \subset \mathbb{Q}[\sqrt{-3}]$ (where ω is a primitive third root of unity), the class group is trivial, since both $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$ are PIDs. But in fact, there are finitely many negative d for which $\mathrm{Cl}(\mathbb{Q}[\sqrt{d}])$ is trivial.

For a more interesting example:

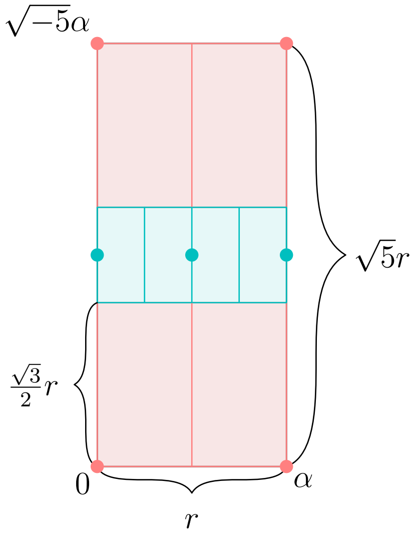
Lemma 17.5
In the case of $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{Q}[\sqrt{-5}]$, the class group is $\mathbb{Z}/2\mathbb{Z}$. The two similarity classes of ideals are represented by (1), and by $(2, 1+\sqrt{-5})$.

Proof. Let I be a nonzero ideal, and let α be a nonzero element of I with minimal norm. Let L be the lattice generated by α and $\sqrt{-5}\alpha$, or equivalently, the lattice corresponding to the ideal (α); then $L \subset I$.

If $L = I$, then I is principal. Now assume $L \neq I$, so there is an element $\beta \in I$ with $\beta \notin L$. Without loss of generality, we can assume that β is in the rectangle spanned by α and $\sqrt{-5}\alpha$ — otherwise, we can subtract multiples of α and $\sqrt{-5}\alpha$ to translate β into this rectangle)

Claim. *We must have $\beta = \alpha \cdot (1 + \sqrt{-5})/2$.*

Proof. Let $r = |\alpha|$. Then split the rectangle into smaller rectangles as shown (note that the rectangle will not generally be horizontal, but it is drawn this way for convenience):



By straightforward calculation, it can be shown that every point in one of the red rectangles is at a distance less than r from one of the red dots, corresponding to 0, α, $\sqrt{-5}\alpha$, and $(1+\sqrt{-5})\alpha$. Meanwhile, every point in one of the blue rectangles is at a distance less than $r/2$ from one of the blue dots, corresponding to $\sqrt{-5}\alpha/2$, $(1+\sqrt{-5})\alpha/2$, and $(2+\sqrt{-5})\alpha/2$.

In the first case, let γ be this red dot. Then $\beta \in I$ and $\gamma \in I$, so $\beta - \gamma \in I$ as well. But we have $|\beta - \gamma| < |\alpha|$, contradiction.

In the second case, again let γ be this blue dot. Then $\beta \in I$ and $2\gamma \in I$, so $2\beta - 2\gamma \in I$ as well. But we have $|2\beta - 2\gamma| < |\alpha|$, which is again a contradiction unless $2\beta - 2\gamma = 0$.

Now suppose $\beta = \gamma$. We now claim that β can't be either of the two blue dots on the ends — either case would imply that $\sqrt{-5}\alpha/2 \in I$. But multiplying by $\sqrt{-5}$ would give that $-5\alpha/2 \in I$, and therefore $\alpha/2 \in I$; this would contradict the choice of α as the element of smallest length.

So then β must be the dot in the center, which is $(1+\sqrt{-5})\alpha/2$. □

So in this case, there is only one element of I inside this rectangle, which is $\beta = \alpha \cdot (1+\sqrt{-5})/2$; then

$$I = (\alpha, \beta) = \frac{\alpha}{2}(2, 1+\sqrt{-5}).$$ □

Here, we saw a proof that there's only two ideals in $\mathrm{Cl}(\mathbb{Q}[\sqrt{-5}])$ up to similarity which looked geometrically at lattices. In fact, the proof of finiteness in general *also* involves looking at lattices. We'll see this proof next class; but today we'll conclude by looking at a few generalizations, where we consider similar questions in fields similar to imaginary quadratic number fields.

17.3 Real Quadratic Number Fields

So far, we've discussed the case $F = \mathbb{Q}[\sqrt{d}]$ when $d < 0$.

Guiding Question
What if we instead have $\mathbb{Q}[\sqrt{d}]$ with $d > 0$?

We can then write $F = \mathbb{Q}[\delta]$, where $\delta^2 = d$.

This case is quite similar, but there are some differences. First, it doesn't make sense to talk about complex conjugation, since all our numbers are real. But there is still a type of "conjugation" in F — the map $a + b\delta \to a - b\delta$. (This is an example of a general construction that we'll discuss in a much later class, related to the Galois group.) This is still a field automorphism.

Moreover, R is not a lattice in $\mathbb{C}$, but it can be embedded as a lattice in $\mathbb{R}\times\mathbb{R}$, a ring where addition and multiplication are done componentwise. To perform this embedding, we send

$$a + b\delta \mapsto (a + b\sqrt{d}, a - b\sqrt{d}) \in \mathbb{R}^2.$$

In fact, the reason we're using the notation with δ is because we can think of it as an abstract square root of d — then we can write it as the *positive* square root $\sqrt{d}$, or the *negative* square root $-\sqrt{d}$.

Another important difference is that in imaginary quadratic fields, there are very few units. However, in this case, the group of units is infinite — there are infinitely many solutions to $a^2 - b^2 d = 1$ (which is known as a Pell equation).

Although there are some differences, our arguments used in imaginary quadratic fields mostly work here as well. In principle, those arguments can be generalized to rings of algebraic integers in *arbitrary* number fields; but that generalization is more difficult and requires theory we have not yet discussed.

17.4 Function Fields

There is a second generalization we'll discuss.

Guiding Question
What if we replace $\mathbb{Z}$ by $k[t]$ for a field k?

Then we replace $\mathbb{Q}$ with $k(t)$, the field of rational functions in t over the field k — in other words, $k(t) = \text{Frac}(k[t])$.

In this case, we consider fields F containing $k(t)$ which are finite-dimensional over $k(t)$, similarly to how a number field is a field containing $\mathbb{Q}$ which is finite-dimensional over $\mathbb{Q}$. We then have

$$R = \{\alpha \in F \mid P(\alpha) = 0 \text{ for a monic } P \in k[t][x]\}.$$

Here P is a polynomial in *two* variables, but it's supposed to be monic as a polynomial in x. This is again similar to how in the number field setting, where R is the set of $\alpha \in F$ which are roots of a monic polynomial in $\mathbb{Z}[x]$.

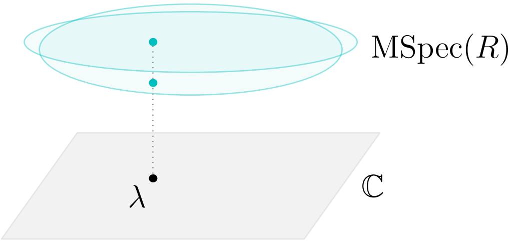
The especially relevant examples are $k = \mathbb{C}$ and $k = \mathbb{F}_p$. We'll focus on the case $k = \mathbb{C}$.

In the case of imaginary quadratic number fields, we looked at primes in $\mathbb{Z}$ and analyzed how they factored in R — we can try to perform a similar analysis here.

First, as we've seen earlier, $k[t]$ is a PID for any k. So in the case $k = \mathbb{C}$, the primes in $\mathbb{C}[t]$ are exactly $(t - \lambda)$ for $\lambda \in \mathbb{C}$, since the only irreducible polynomials in $\mathbb{C}$ are linear.

Meanwhile, to describe the nonzero primes in R, we can use Hilbert's Nullstellensatz. It's possible to write R as a quotient of $\mathbb{C}[t, t_2, \ldots, t_n]$ by polynomials — for example, in the case of quadratic number fields, we have $\mathbb{Z}[\sqrt{d}] = \mathbb{Z}[x]/(x^2 - d)$, and it's possible to perform a similar construction here. We still have unique factorization into ideals in R, and in particular, prime ideals are maximal; so the nonzero primes in R correspond to points in $\text{MSpec}(R)$, which we can think of as a subset of $\mathbb{C}^n$ by Nullstelensatz.

Now this gives a ramified covering, where we can cover $\mathbb{C}$ by $\text{MSpec}(R) \subset \mathbb{C}^n$. More explicitly, if we write R as a quotient of $\mathbb{C}[t, t_2, \ldots, t_n]$, then the elements of $\text{MSpec}(R)$ correspond to points in $\mathbb{C}^n$ which are roots of all the polynomials we quotient out by. In this ramified covering, a point $t \in \mathbb{C}$ lies below all the points in $\text{MSpec}(R)$ with that value of t.



Factoring $(t - \lambda)$ as a product of prime ideals in R then amounts to enumerating the points in the pre-image of λ in this ramified covering. (We'll see this in more detail next class.)

The term *ramified* is used in a similar sense here as when discussing ramified primes. In this setting, if for example our ramified cover corresponds to the map $z \mapsto z^2$, then most points in $\mathbb{C}$ have *two* points in their pre-image (since there's two square roots), but 0 only has one — so 0 is a ramification point. This is similar to how in the number field setting, when we factor (q) as a product of prime ideals in R, usually these prime ideals are distinct, but they're the same ideal for the ramified primes.

A famous mathematician, André Weil, proposed a metaphor between this situation and the Rosetta Stone. The Rosetta Stone contained a script written in three languages. Here our languages are the finite extensions of $\mathbb{Q}$ (or in other words, number fields), finite extensions of $\mathbb{F}_q(t)$ for a finite field $\mathbb{F}_q$, and finite extensions of $\mathbb{C}(t)$. In all of these situations, it's possible to consider how normal primes (in $\mathbb{Z}$, $\mathbb{F}_q[t]$, and $\mathbb{C}[t]$ respectively) factor as a product of ideals in the corresponding ring R. There are analogies between the three settings, and Weil wondered how results in each setting could be "translated" to the others.

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