16 Uniqueness of Ideal Factorization

16.1 Properties of Ideal Multiplication

Last time, we began discussing the uniqueness of factorization into ideals in the ring of algebraic integers of an imaginary quadratic field. We let $F = \mathbb{Q}[\sqrt{d}]$ for a squarefree integer $d < 0$, and we saw that then the ring of algebraic integers in F is

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\} & \text{if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\sqrt{d} \mid a, b \in \frac{1}{2}\mathbb{Z} \text{ and } a + b \in \mathbb{Z}\right\} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

We then proved the key lemma:

Lemma 16.1
If $I \subset R$ is an ideal, then $I\overline{I} = (n)$ for some $n \in \mathbb{Z}$.

We can assume $n > 0$ (since n and $-n$ generate the same ideal), giving the following definition:

Definition 16.2
The **norm** of an ideal I, denoted $\mathrm{N}(I)$, is the positive integer n with $I\overline{I} = (n)$.

Note that when $I = (\alpha)$ is principal, then $I\overline{I} = (\alpha\overline{\alpha})$, so $\mathrm{N}(I) = \alpha\overline{\alpha}$. So this coincides with the usual concept of the norm of a complex number. It's also clear from the definition that N is multiplicative, meaning that $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$ — this is because

$$IJ \cdot \overline{IJ} = I\overline{I} \cdot J\overline{J}.$$

Last time, we also stated the following key proposition:

Proposition 16.3
Multiplication of ideals has the following two properties:

(a) Cancellation: if $IJ = I'J$ and $J \neq 0$, then $I = I'$.

(b) If $I \subset J$, then $I = JJ'$ for some J'.

As stated last time, the second condition is actually an *if and only if* statement — we've seen already that if $I = JJ'$, then $I \subset J$.

Student Question. *Is this only true for imaginary quadratic number fields?*

Answer. *It's true for other rings of algebraic integers; it's also true for some other examples, such as a ring of polynomials in one variable (which we'll discuss next class) and its extensions; but it doesn't hold in general. For example, it doesn't hold for polynomials in two variables.*

Proof of Proposition 16.3. The main idea is that in the case where J is principal, this is almost obvious; and using Lemma 16.1, we can reduce to the case where J is principal.

First consider the case where J is principal. Then for (a), it's clear that

$$\alpha I = \alpha I' \implies I = I'.$$

This is because multiplying by α is easily inverted, just by multiplying by α^{-1}, if we think of these sets as belonging to the field F and not the ring R.

Similarly, for (b), if we have $I \subset (\alpha)$, then $x/\alpha \in R$ for all $x \in I$. Then we can take

$$J' = \frac{I}{\alpha} = \left\{\frac{x}{\alpha} \mid x \in I\right\},$$

which is an ideal of R.

Now consider the more general case. For (a), if we have $IJ = I'J$, then we can multiply by $\overline{J}$ to get

$$I(J\overline{J}) = I'(J\overline{J}) \implies I(n) = I'(n),$$

where $n = \mathrm{N}(J)$. Since $n \neq 0$ if $J \neq 0$, then by the principal case of (a), we have that $I = I'$ in the general case as well.

For (b), we use the same trick. Suppose $I \subset J$, and multiply both sides by $\overline{J}$. Then

$$I\overline{J} \subset J\overline{J} = (n).$$

As before, now set $J' = I\overline{J}/n$ (which is an ideal for the same reason as in the principal case). Then

$$J'(J\overline{J}) = J'(n) = I\overline{J},$$

and by (a) we can cancel out $\overline{J}$ to get $J'J = I$. □

Student Question. *For rings of general algebraic integers, can we get a principal ideal by multiplying by* all *conjugates?*

Answer. *Yes — if the field is Galois, then we can multiply by all the Galois conjugates. But we haven't yet learned the relevant theory.*

Finally, before proving unique factorization, we'll need the following lemma (which will essentially allow us to use (b) to find a prime ideal dividing *any* ideal, so that we can factor repeatedly):

Lemma 16.4
Every non-unit ideal I in R is contained in a maximal ideal.

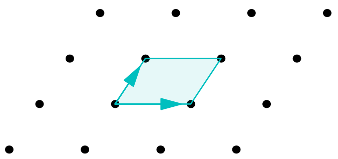
This lemma is actually true for *any* ring. But we'll only prove it in our case (since the proof is harder in general).

Proof. Assume without loss of generality that $I \neq 0$, since the zero ideal is contained in *any* ideal. Then we know that R/I is finite — this means there are finitely many ideals in R/I.

But ideals in R/I are in bijection with ideals in R containing I, by the correspondence theorem for rings. And since R/I is finite, it must have a maximal ideal — if we have an ideal that isn't maximal (or the unit ideal), we can find a bigger one, and we can't keep on doing this forever since there's only finitely many ideals. □

Student Question. *Why is R/I finite?*

Answer. *As discussed last time, this is because R and I are both lattices in $\mathbb{C}$, and the index of any lattice in another is finite. In fact, for any lattice, we can take two vectors which generate it, and compute the area of the parallelogram formed by those two vectors:*



Then the index of I in R is the ratio of the areas of their corresponding parallelograms.

Note 16.5
Lemma 16.4 is true in any ring. But in this proof, we used the fact that the poset of ideals in R/I under inclusion is finite, and therefore has a maximal element; this isn't true for a general poset — for example, the positive integers don't have a maximal element.

But the poset of ideals has the additional property that any increasing chain of ideals is majorated by an element of the set — if we have a chain $I_1 \subset I_2 \subset I_3 \cdots$, their union $I_1 \cup I_2 \cup \cdots$ is again an ideal, which contains all the I_n.

Then it's possible to use Zorn's Lemma from set theory, which applies to partially ordered sets with this property. Although Zorn's Lemma is needed in the general case, we'll see a weaker finiteness property in which case there *is* an easier proof. That finiteness property will be much more general than the one used here — in particular, it will apply to polynomial rings and their quotients.

16.2 Proof of Unique Factorization

Finally, we are ready to prove the uniqueness of ideal factorization for imaginary quadratic number fields:

Theorem 16.6
Every nonzero ideal $I \subset R$ factors uniquely (up to permutation of factors) as a product of prime ideals.

Proof. First, we'll prove the existence of a prime factorization. Let $I \subset R$ be an ideal which is neither the zero ideal nor the unit ideal. Then by Lemma 16.4, there is a maximal ideal $\mathfrak{m}$ with $I \subset \mathfrak{m}$, and therefore by Proposition 16.3, we can factor $I = \mathfrak{m} \cdot J$ for some ideal J. Since $\mathfrak{m}$ is maximal, it is also prime; so we can think of this as the first step in the factorization process, and now it suffices to factor J (unless J is the unit ideal, in which case we're done).

It then suffices to show that this factorization process terminates. To do so, we can consider the norm — we have

$$\mathrm{N}(I) = \mathrm{N}(\mathfrak{m}) \cdot \mathrm{N}(J).$$

We must have $\mathrm{N}(\mathfrak{m}) > 1$ (since $1 \notin \mathfrak{m}$), so then $\mathrm{N}(J) < \mathrm{N}(I)$. This means the norm of our ideal decreases, so the process must eventually terminate, meaning that J must eventually become the unit ideal. (This argument can also be phrased by induction on the norm.)

Now we'll prove uniqueness of factorization. Suppose

$$I = P_1 \cdots P_n = Q_1 \cdots Q_n,$$

where the P_i and Q_i are all ideals. It's enough to show that $P_1 = Q_i$ for some i, since then by part (a) of Proposition 16.3, we can cancel out the common factor (this is the same way we proved uniqueness in the case of integers or polynomials, except that now we're dealing with ideals instead of elements).

Assume for contradiction that $Q_i \neq P_1$ for all i. Then $Q_i \not\subset P_1$ for all i — since Q_i is maximal, the only ideals containing it are itself and the unit ideal. So for each i, we can find an element $x_i \in Q_i$ with $x_i \notin P_1$. But now consider their product $x_1 x_2 \cdots x_n$. By definition, this product lies in $Q_1 \cdots Q_n$. But since P_1 is prime and none of the x_i are in P_1, their product cannot be either; contradiction. □

The last step can instead be worded using the following lemma:

Lemma 16.7
If P is a prime ideal, and I and J are ideals with $I \not\subset P$ and $J \not\subset P$, then $IJ \not\subset P$.

Proof. The same proof works — pick $x \in I$ and $y \in J$ with $x, y \notin P$. Then we have $xy \in IJ$, but $xy \notin P$. □

16.3 Classification of Prime Ideals

We can look more concretely at the structure of these prime ideals. In a future class, we'll see that the classification of prime ideals actually works quite similarly to the classification of primes we saw in the Gaussian integers — by looking at all integer primes p, and trying to factor (p) into prime ideals. We'll see that there are three possibilities:

- (p) remains prime in R — such primes are called **inert primes**;
- (p) factors as $Q_1 Q_2$, where Q_1 and Q_2 are distinct (they must then be conjugate) — such primes are called **splitting primes**;
- (p) factors as Q^2 — such primes are called **ramified primes**. (In the case of Gaussian integers, the only ramified prime was 2; in general, the ramified primes come from divisors of d.)

All prime ideals in this list are distinct, and this gives a full list of the prime ideals.

16.4 Similarity Classes of Ideals

We'll now discuss another important concept regarding ideals.

Definition 16.8
Two nonzero ideals $I, J \subset R$ are **similar** if there exists some $\lambda \in F$ such that $\lambda I = J$.

(We only consider nonzero ideals when discussing similarity.)

Note that it would be equivalent to state $\lambda \in \mathbb{C}$ in the definition, since if $\lambda \in \mathbb{C}$ were the quotient of two elements in R, then we must have $\lambda \in F$. Meanwhile, two lattices L_1 and L_2 in $\mathbb{C}$ are similar if $L_2 = \lambda L_1$ for some $\lambda \in \mathbb{C}$ — geometrically, multiplication by a complex number corresponds to scaling and rotation. So the algebraic notion of similarity of ideals coincides with the geometric notion of similarity of their lattices.

Similarity is an equivalence relation — if $I_2 = \lambda I_1$ and $I_3 = \mu I_2$, then $I_3 = \lambda\mu I_1$. So we will use the notation $I \sim J$ to denote that two ideals are similar. Then we can think about ideals in terms of their equivalence classes, which are called **ideal classes**.

Example 16.9
The similarity class of the unit ideal (1) consists of ideals $I = \lambda(1)$ for $\lambda \in F$. But since $\lambda \cdot 1 \in R$, then we must have $\lambda \in R$. So then $I = \lambda(1) = (\lambda)$ is a principal ideal — so the similarity class of (1) consists of exactly the principal ideals.

In particular, this example implies that in a PID, all ideals are similar. But there are many cases which are *not* PIDs — and in some sense, the number of equivalence classes is a measure of the ring's failure to be a PID.

Proposition 16.10
If $I \sim I'$, then $IJ \sim I'J$.

This is straightforward from the definitions, but it's important — it means that taking the product of ideals gives a commutative and associative operation on the set of ideal classes. In fact, the set of ideal classes, along with ideal multiplication, is an abelian group — the class of (1) is the unit, and every nonzero class is invertible because $I\overline{I}$ is principal, so the class of $\overline{I}$ is the inverse of the class of I. This group is called the **ideal class group**, and denoted $\mathrm{Cl}(F)$.

An important theorem about the ideal class group, which we'll look at in more detail later, is the following:

Theorem 16.11
The ideal class group $\mathrm{Cl}(F)$ is finite.

Example 16.12
For $R = \mathbb{Z}[\sqrt{-5}]$, the class group is $\mathbb{Z}/2\mathbb{Z}$ — the only two ideals up to similarity are (1) and $(2, 1+\sqrt{-5})$.

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