15 Ideal Factorization

This class, we'll consider unique factorization in rings of algebraic integers, primarily imaginary quadratic number fields. Unique factorization is a useful property — for example, we used unique factorization in $\mathbb{Z}[i]$ to classify which n can be written as a sum of squares. However, unique factorization doesn't hold in general — for example, we've seen that it fails in $\mathbb{Z}[\sqrt{-5}]$.

But instead, we can prove a weaker statement — instead of unique factorization as a product of prime *elements*, we'll prove unique factorization as a product of prime *ideals*.

15.1 Motivation

The motivation for ideal factorization is that we've seen that unique factorization doesn't hold in a general ring of algebraic integers, so we'd like to modify the property of unique factorization in order to find one that *does* hold. So instead of thinking about products of prime elements, we can think of products of something else — which we can call "ideal prime factors," or "ideal divisors."

We don't yet know what these "ideal divisors" are, but we can think about how they *should* behave. Given an ideal divisor, it should appear in the prime decomposition of various actual numbers. And if it enters the factorization of different numbers, perhaps it should arise as a gcd of different numbers — in an ideal theory where we've restored unique factorization and therefore the existence of a gcd, we would want our ideal divisor to arise as $\gcd(a_1, \ldots, a_n)$ where the a_i are actual elements of the ring.

So along these lines, we could introduce *formal* gcd's of several elements (similarly to how when going from $\mathbb{R}$ to $\mathbb{C}$, we add a formal variable whose square is -1), and figure out how to operate with them. Then given a formal gcd such as $\gcd(a_1, \ldots, a_n)$, we can think about the set of *actual* numbers (in the ring) which are divisible by that gcd. But we've seen that set before — it's the ideal generated by $a_1, \ldots, a_n$! In fact, in the case of a PID (where unique factorization into elements does hold), $\gcd(a_1, \ldots, a_n)$ in the usual sense is the generator of the ideal $(a_1, \ldots, a_n)$.

This was the approach taken by Kummer in the 19th century, when initially developing the concept of ideal factorization. Later, Noether and others realized that a good way to think about this is to declare the gcd to *be* that ideal. In fact, this is where the term "ideal" comes from — we defined them by looking at the kernels of homomorphisms, but the term initially comes from "ideal divisors" and the idea that you can define the ideal divisors as ideals in the sense we've discussed.

Definition 15.1
Given elements $a_1, \ldots, a_n$ in a ring, we define $\gcd(a_1, \ldots, a_n)$ as the ideal $(a_1, \ldots, a_n)$ (meaning the ideal generated by $a_1, \ldots, a_n$).

This definition is where the shorthand (a, b) for $\gcd(a, b)$ comes from as well.

15.2 Prime Ideals

To understand factorization into ideals, we need to understand what the "building blocks" are in such a factorization. A prime *element* is an element p such that if $p \mid ab$, then $p \mid a$ or $p \mid b$. The definition of a prime *ideal* is similar.

Definition 15.2
A **prime ideal** $I \subset R$ is an ideal other than R itself such that whenever $ab \in I$, either $a \in I$ or $b \in I$.

There are a few observations we can make about this definition:

Example 15.3
If I is principal with $I = (a)$, then I is prime if and only if a is prime (by directly applying the definitions).

Lemma 15.4
An ideal I is prime if and only if R/I is an integral domain.

Proof. Recall that an integral domain is a ring where the product of any two nonzero elements must be nonzero. Then this is clear from the definition as well — if we use $\overline{a}$ to denote a mod I, then $\overline{a} = 0$ if and only if $a \in I$. So the definition of a prime ideal states that

$$\overline{ab} = 0 \implies \overline{a} = 0 \text{ or } \overline{b} = 0.$$

But this is exactly the definition of an integral domain. □

Lemma 15.5
A maximal ideal is always prime.

Proof. As we've seen before, an ideal I is maximal if and only if R/I is a field. But all fields are integral domains, so if I is maximal, it must be prime as well (by the above observation). □

Note that by definition, the unit ideal is not prime. Meanwhile, the zero ideal may or may not be prime — in fact, it's prime if and only if R is an integral domain.

15.3 Multiplying Ideals

Of course, to perform factorization using ideals, we also need a way to multiply them.

Definition 15.6
Given two ideals I and J, we define their product as

$$I \cdot J = \left\{ \sum a_i b_i \mid a_i \in I, b_i \in J \right\}.$$

It's clear that multiplication of ideals is commutative and associative. It's also immediate from the definition that if $I = (a_1, \dots, a_n)$ and $J = (b_1, \dots, b_m)$, then IJ is generated by the elements $a_i b_j$.

Example 15.7
If $I = (a)$ is principal, then $IJ = (ab_1, \dots, ab_m)$. In particular, if $I = (a)$ and $J = (b)$, then $IJ = (ab)$ — this means the product of ideals is compatible with the usual product of elements.

Note that IJ is always contained in $I \cap J$ (since I is closed under addition and under multiplication by *any* element of R, then any element $\sum a_i b_i$ must be in I, and the same is true for J). On the other hand, we don't necessarily have $IJ = I \cap J$.

Example 15.8
In $\mathbb{Z}$, if $I = (n)$ and $J = (m)$, then $IJ = (nm)$, while $I \cap J = (\text{lcm}(m, n))$. We always have $\text{lcm}(m, n) \mid mn$, but they're only equal if m and n are relatively prime.

Now that we have defined how to factor with ideals, we are ready to state the main theorem for this section.

Theorem 15.9
Let R be the ring of algebraic integers in a number field. Then every nonzero ideal $I \subset R$ factors uniquely (up to permutation of factors) as a product of prime ideals.

We'll only prove the theorem in the case where the number field F is a *imaginary quadratic field*, but it is true for any number field.

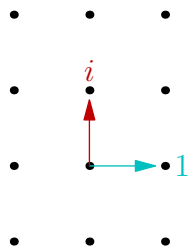
15.4 Lattices

Since we are working with imaginary quadratic number fields, from now we'll assume $F = \mathbb{Q}[\sqrt{d}]$ for an integer $d < 0$. Without loss of generality we may assume d is squarefree. We'll also use R to denote the ring of algebraic

integers in F. As we saw last time, we have

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

In either case, we can think of R as a *lattice* in $\mathbb{C}$ (a lattice is the additive subgroup of $\mathbb{C}$ generated by two non-collinear vectors), generated by 1 and $\sqrt{d}$ in the first case, and 1 and $(1+\sqrt{d})/2$ in the second. For example, $\mathbb{Z}[i]$ is the square lattice (and more generally, in the first case, the lattice is always rectangular):



We'll first state a few elementary properties of lattices that will be useful:

Proposition 15.10
Suppose that L and L' are lattices, with $L' \subset L$.

- The quotient L/L' is finite.
- If L'' is a subgroup of L (under addition) with $L' \subset L'' \subset L$, then L'' is also a lattice.

The proof is left as an exercise; it's possible to see this by thinking about the example $\mathbb{Z}^2$, since these properties don't depend on which lattice L is.

Corollary 15.11
Every nonzero ideal of R is again a lattice.

Proof. First, this is clear for *principal* ideals — if $I = (\alpha)$, then we can write $I = \alpha R$, so I is obtained by multiplying the lattice of R by α. It's clear from the definition that multiplying a lattice by a complex number will still produce a lattice; it's also possible to see this geometrically, since multiplication by a complex number is just a rotation and dilation.

But if I is an arbitrary nonzero ideal, then $R \supset I \supset \alpha R$ for each nonzero $\alpha \in I$, so by Proposition 15.10, since I sits between two lattices, I must itself be a lattice. □

Note 15.12
As we'll see later, trying to understand how these lattices look geometrically (up to similarity — multiplication by a complex number) gives rise to an important number theoretic concept.

15.5 Proof of Unique Factorization

To prove uniqueness of ideal factorization for $R \subset \mathbb{Q}[\sqrt{d}]$, we will first make a few observations.

Lemma 15.13
A nonzero ideal in R is prime if and only if it is maximal.

We've already seen that all maximal ideals are prime; in general, the converse is false, but in the situation here (and more generally, in rings of algebraic integers in a number field) it turns out to be true.

Proof. It's enough to show that every prime ideal is maximal. But note that R/I is finite for every nonzero ideal, since I and R are lattices (by Proposition 15.10). Additionally, since I is prime, R/I is an integral domain — so there are no zero divisors.

But in a *finite* ring S, any element a which is not a zero divisor is necessarily invertible — this can be proven by a counting argument. Consider the list of values ab for all $b \in S$; these must all be distinct, as if $ab = ac$, then we would have $a(b-c) = 0$. But there are $|S|$ such values, so they must cover *all* of S; and in particular, there exists b with $ab = 1$. □

Student Question. *Does this mean that a finite ring of prime order is a field?*

Answer. *Yes — the only ring of order p is $\mathbb{Z}/p\mathbb{Z}$, which is a field. This doesn't generalize to prime powers, though — we'll later see that for each prime power p^k, there's one field with order p^k, but there are other rings with order p^k.*

Student Question. *In general, if we have a prime ideal I for which R/I is finite, then do we know I is also maximal?*

Answer. *Yes. In fact, there's also a generalization of this lemma which replaces "finite" with "finite-dimensional vector space."*

The key proposition, from which most of the proof follows formally, is the following:

Proposition 15.14
Multiplication of ideals has the *cancellation property* — if we have ideals I, I', and J (with $J \neq 0$), then

$$IJ = I'J \implies I = I'.$$

Furthermore, divisibility is the same as inclusion — if $I \subset J$, then there exists an ideal J' such that $I = JJ'$.

It's clear that multiplication of ideals gives us a smaller ideal; the second statement tells us that here, the converse is true as well.

To prove these two properties, we'll first establish the following key lemma. This lemma will essentially allow us to reduce to the case of principal ideals, which are easier to work with.

Lemma 15.15
If $I \subset R$ is an ideal, then $I\overline{I}$ is a principal ideal generated by an integer $n \in \mathbb{Z}$.

Here $\overline{I} = \{\overline{z} \mid z \in I\}$ — it's clear that this is also an ideal.

Proof. Since I is a lattice, we can pick two elements α and β which generate I as a lattice. Then they also generate I as an ideal; this means $I = (\alpha, \beta)$ and $\overline{I} = (\overline{\alpha}, \overline{\beta})$. This means

$$I\overline{I} = (\alpha\overline{\alpha}, \beta\overline{\beta}, \alpha\overline{\beta}, \beta\overline{\alpha}).$$

Note that $\alpha\overline{\alpha}$, $\beta\overline{\beta}$, and $\alpha\overline{\beta} + \beta\overline{\alpha}$ are all integers; so we can define n to be their gcd, in the sense of the usual integers.

Then we claim that $I\overline{I} = (n)$. It's clear that $n \in I\overline{I}$, since n is in the smaller ideal $(\alpha\overline{\alpha}, \beta\overline{\beta}, \alpha\overline{\beta} + \beta\overline{\alpha}) \subset I$. So it suffices to check that n generates the entire ideal, or equivalently that (n) contains all the generators of I; and since we already know that n divides $\alpha\overline{\alpha}$, $\beta\overline{\beta}$, and $\alpha\overline{\beta} + \beta\overline{\alpha}$, it's enough to check that n divides $\alpha\overline{\beta}$.

To do so, we'll check that $\alpha\overline{\beta}/n$ is an algebraic integer, which will imply that it's in R; it suffices to check that it's the root of a monic polynomial with integer coefficients.

But we can take

$$P = \left(x - \frac{\alpha\overline{\beta}}{n}\right)\left(x - \frac{\overline{\alpha}\beta}{n}\right) = x^2 - \frac{\alpha\overline{\beta} + \overline{\alpha}\beta}{n} \cdot x + \frac{\alpha\overline{\alpha} \cdot \beta\overline{\beta}}{n}.$$

By the definition of n, both coefficients are integers, so we are done. □

Resource: Algebra II Student Notes

Spring 2022

Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng