October 12:

Math 432 Class Lecture Notes

- Ideal lemmas
- Invertible ideals
- Main Theorems

0.1 Ideal lemmas

The main goal today is to prove that every ideal in a Dedekind domain is invertible, that ideals factor uniquely into prime ideals, and that the ideal "classes" form a group. The main lines of the proof here are due to van der Waerden.

We start with two lemmas. Throughout let R be a Dedekind domain and F its fraction field. (There are some minor ways in which the proof could be simplified if $R = \mathbf{Z}_F$ for some number field F.) Also, in one-dimensional rings we will follow convention and reserve the word "ideal" for nonzero ideals.

Lemma 1. Any ideal contains a product of prime ideals.

Proof. The set of ideals not containing such a product has a maximal element under inclusion, since R is Noetherian. Let I be such an ideal, i.e., an ideal such that any ideal that properly contains I also contains a producdt of prime ideals.

Then I isn't a prime ideal itself, so there are elements x and y of R such that $xy \in i$ but x and y are not in I. Then $I + (x)$ is an ideal that is strictly larger than I, so it contains a product $\prod P_i$ of prime ideals, and similarly $I + (y)$ contains a product $\prod Q_j$ of prime ideals. But then

$$I \supset (I + (x))(I + (y)) \supset \prod_i P_i \prod_j Q_j$$

so that I in fact contains a product of prime ideals. □

If I is an ideal, then an element x of the fraction field F is said to be a **multiplier** for I if $xI \subset R$, i.e., x multiplies anything in I into R. Very roughly, this means that the denominator of x is an element of I.

Lemma 2. Any proper ideal (i.e., not equal too the entire ring) has a multiplier that is not in the ring.

Proof. Let I be a proper ideal, and choose a nonzero element y in I. The ideal (y) contains a product $\prod_{i=1}^{m} P_i$ of prime ideals by the previous lemma; we choose such a product in which the number m of ideals is as small as possible. Also, choose a prime ideal P that contains I, so that we have

$$P \subset I \subset (y) \subset \prod_{i=1}^{m} P_i.$$

Then $P = P_i$ for some i (if not, then for each i choose x_i in P_i by not in P; one finds that the product of the x_i, and hence one of the x_i, is in P since P is a prime ideal). Let $P = P_1$, without loss of generality.

Now choose z that is in the product $P_2 \cdots P_m$ that is not in (y) (z exists because of the minimality of m).

Then the claim is that $x = z/y$ is a multiplier for I; note that x is clearly not in R since z is not in the principal ideal (y).

On the other hand

$$xI = (z/y)I \subset (z/y)P \subset (1/y)P_1 P_2 \cdots P_m \subset R$$

by our various choices. □

0.2 Invertible ideals

An ideal I in R is said to be **invertible** if there is an ideal J such that IJ is principal. Any ideal in a Dedekind domain is invertible and, though we won't prove it, any one-dimensional integral domain with this property is in fact a Dedekind domain.

Theorem 3. If I is an ideal in R and y is a nonzero element of I, then the set

$$J := \{x \in R : xI \subset (y)\}$$

is an ideal, and $IJ = (y)$.

Proof. It is easy to check that J is an ideal, and that IJ is contained in (y). So it suffices to check that $IJ = (y)$. In order to do this, let

$$K = (1/y)IJ.$$

The set K is contained in R by our definitions, and it is then easy to check that it is an ideal. We are trying to prove that $K = R$.

Suppose that K is a proper ideal. Let x be a multiplier for K that does not lie in R.

First note that $J \subset K$. Indeed, $y \in I$ so $yJ \subset IJ$ and therefore $J \subset (1/y)IJ$.

Next, note that since $xK \subset R$ we have

$$xIJ \subset (y).$$

This means that anything in xJ (which, by the first remark is a subset of R) multiplies I into (y), i.e.,, that xJ is contained in J.

This is actually a contradiction since it implies that x is the root of a monic polynomial with coefficients in R, i.e., that (by the definition of a Dedekind domain) x is in R. Indeed, if $\alpha_1, \cdots, \alpha_k$ is a generating set for J, then each $x\alpha_i$ can be written as a linear combination of the α_i, with coefficients in R. In matrix form this gives

$$xA = MA, \qquad (xI - M)A = 0$$

where A the column vector of α_i's. A singular matrix has zero determinant, so $\det(xI - M) = 0$ and x is the root of a monic polynomial in $R[x]$, as claimed.

□

0.3 The Main Theorems

Finally, we are in a position to smoothly prove the major results about ideals in Dedekind domains.

Theorem 4. If I and J are ideals in R then $I \subset J$ if and only if I is divisible by J.

Remark 5. A smaller ideal will be divisible by more primes, so the statement is in fact not counterintuitive.

Proof. If $I = JK$ then anything in J is certainly in I (this implication is of course true in any ring).

On the other hand, if $I \subset J$ then find an ideal K such that $JK = (y)$ is principal. Then $I' := (1/y)IK$ is easily checked to be an ideal and

$$I'J = (1/y)IKJ = I.$$

So I is indeed the product of J and another ideal, i.e., I is divisible by J as claimed. □

Theorem 6. Cancellation holds for multiplication of ideals in a Dedekind domain, i.e., $IJ = IK$ implies that $J = K$.

Proof. Find an ideal I' such that $II' = (y)$. Multiplying the given equation by I' gives $(y)J = (y)K$ from which $J = K$ follows. □

Theorem 7. Every ideal in R can be uniquely represented as a product of prime ideals.

Proof. To show existence, we consider an ideal I that is as large as possible that is not a product of prime ideals. Then $I \neq R$ (since we regard R as an empty product of prime ideals). Therefore I is contained in a maximal (prime) ideal P, $I \subset P$. Clearly I is not equal to P (since we regard a prime ideal as a product of a single prime ideal) so, by the preceding result, there is a proper ideal J such that $PJ = I$. Then I is a proper subideal of J, so J is a product of prime ideals, and so is I.

To prove uniqueness we observe that if

$$\prod P_i = \prod Q_j$$

then $P_1 \supset \prod Q_j$ so that some Q_j, say Q_1 is equal to P_1. Applying cancellation enables us to prove uniqueness by induction. □

Say that two ideals I and J in R are **equivalent** if there are nonzero elements x and y of the ring such that

$$xI = yJ.$$

It is easy to check that this is an equivalence relation. Multiplication on ideals induces a multiplication on equivalence classes, and it is easily checked that this operation has an identity (the entire ring (1)), is commutative, and is associative.

Theorem 8. Equivalence classes form a group under the above operation.

Proof. If $IJ = (y)$ then
$$[I][J] = [R].$$
□

The ideal class group of a Dedekind domain R will be denoted $Cl(R)$. Later we will see that this group is finite if R is the ring of integers in a number field.