October 10

Math 431 Class Lecture Notes

- Factorization
- Dedekind domains

0.1 Factorization

In $\mathbf{Z}[i]$ every element factors uniquely into primes (irreducibles), up to units. The primes were easy to ascertain: any prime element in $\mathbf{Z}[[i]$ divides a rational prime number p, So we can find all primes in $\mathbf{Z}[i]$ (up to associates) by factoring rational primes. There were 3 possible factorizations, up to units.

The caveats about units can be avoided by working with principal ideals. Thus the statements become: any prime ideal can be found by factoring the ideals $(p) = p\mathbf{Z}[i]$ for rational primes p, and one finds

$$(2) = (1+i)^2$$

$$(p) \quad \text{is a prime ideal if} \quad p \equiv 3 \bmod 4$$

$$(p) = (a-bi)(a+bi) \quad \text{if} \quad p \equiv 1 \bmod 4.$$

And any ideal factors uniquely into prime ideals.

As we saw earlier, unique factorization does not hold in $\mathbf{Z}[\sqrt{-5}]$, and the problem seemed to be that there weren't "enough" elements. However, it turns out that unique factorization into prime ideals does hold.

This property turns out to hold in any number ring $\mathbf{Z}_F$, i.e, any ring of integers in a number field F. Thus even if unique factorization into irreducible elements does not hold, unique factorization of ideals into prime ideals does hold, and this is a crucial tool in working with the number theory of the rings $\mathbf{Z}_F$.

0.2 Dedekind domains

In fact, unique factorization of ideals holds more generally in "Dedekind domains." These rings are "one-dimensional" and posess a nice theory of ideals. There are several ways that they can be defined, and we choose one of the standard ones.

Definition 1. An integral domain R is a Dedekind domain if R satisfies the following three conditions:

- 1) R is Noetherian,
- 2) if $P \subset R$ is a (nonzero) ideal of R, then P is a maximal ideal,
- 3) R is integrally closed in its fraction field.

The last condition means that if an element x of the fraction field F of F satisfies a monic polynomial with coefficients in R, then x is in R.

Theorem 2. If F is a number field then its ring of integers Z_F is a Dedekind domain.

Proof. Let $n = [F : \mathbf{Q}]$. Then any ideal I of $\mathbf{Z}_F$ is a subgroup of a free abelian group of rank n and is itself finitely generated, so $\mathbf{Z}_F$ is certainly Noetherian.

In fact, if $\alpha_1, \cdots, \alpha_n$ is a basis of $\mathbf{Z}_F$ and α is any nonzero element of an ideal I, then I contains n linearly independent elements $\alpha\alpha_i$, so the rank of I is n. By our general results on fabs, this means that $\mathbf{Z}_F/I$ is finite.

Lemma 3. Any finite integral domain is a field.

Proof. Let x belong to A, where A is a finite integral domain and $x \neq 0$. Then the sequence $1, x, x^2, ...$ is finite, and so $x^{m+n} = x^n$ for some integer m. Therefore, $x^n(x^m - 1) = 0$. Since A is an integral domain, $x^m - 1 = 0$, and $x \cdot x^{m-1} = 1$. Thus any nonzero element has a multiplicative inverse, and A is a field as claimed. □

Thus if P is a prime ideal of $\mathbf{Z}_F$ then $\mathbf{Z}_F/P$ is an integral domain (by the definition of a prime ideal), and it is finite by the earlier remarks; by the lemma the quotient is a field and P is a maximal ideal. This finishes the verification of the first two Dedekind domain properties.

The third property is easy. If $\alpha \in F$ satisfies a monic integral equation with coefficients in $\mathbf{Z}_F$ then by an earlier exercise it is an algebraic integer. It follows that α is in $\mathbf{Z}_F$. □

0.3 Ideals

If I and J are ideals in a ring R then so are

$$\begin{aligned} I+J &:= \{x+y : x \in I, y \in J\} \\ IJ &:= \{\sum x_i y_i : x_i \in I, y_i \in J\} \\ I \cap J &:= \{x : x \in I, x \in J\} \end{aligned}$$

Example 4. If $R = \mathbf{Z}$ is the ring of (rational) integers, and $I = (m)$ and $J = (n)$ then

$$\begin{aligned} I+J &= (\gcd(m,n)) \\ IJ &= (mn) \\ I \cap J &= (\mathrm{lcm}(m,n)) \end{aligned}$$

The main fact that will underlie all of our results on ideals in Dedekind domains is that every (nonzero) ideal I is invertible in the sense that there is an ideal J such that IJ is principal.

Theorem 5. If R is a Dedekind domain then every ideal is invertible.

This will be proved next time; it requires all of the properties of a Dedeking domain, and in fact this invertibility property is more or less equivalent to being a Dedekind domain.

One of its crucial corollaries is that divisibility and inclusion are inversely related.

Corollary 6. If I and J are ideals in a Dedekind domain, then $I \subset J$ if and only if there is an ideal K such that $I = JK$.

Proof. If $I = JK$ then anything in I is of the form $i = \sum j_r k_r$ where the j_r are in J, so $i \in J$. This direction of the corollary is of course true in any ring.

On the other hand, suppose that $I \subset J$. Choose an ideal J' such that $JJ' = (\alpha)$. Then since $I \subset J$, every element of IJ' is contained in (α) and the set $K := (1/\alpha)IJ'$ is contained in R. An easy computation shows that K is an ideal, and a further easy computation shows that $JK = I$. □

As we will see next time, this will enable us to prove that ideals factor uniquely into prime ideals.

0.4 The ideal class group

The above theorem also lets us prove that "ideals modulo principal ideals" form a group under (the operation induced by) multiplication. This group is called the class group and provides a measure of how far a Dedekind ring R is from being a principal ideal domain (PID).

First we define the desired equivalence relation.

Definition 7. If I and J are ideals in a Dedeking domain, then we say that I and J are equivalent, written $I \sim J$, if there are elements α and β in the ring such that

$$\alpha \cdot I = \beta \cdot J \ .$$

This is easily checked to be an equivalence relation. For instance, if $\alpha I = \beta J$ and $\alpha' J = \beta' K$ then

$$\alpha\alpha' I = \alpha'\beta J = \beta\beta' K.$$

Theorem 8. Multiplication of ideals induces a well defined operation on the equivalence classes of ideals, and the set of equivalence classes forms a group under this operation.

The identity element of the group is the equivalence class of principal ideals. The existence of inverses follows immediately from the invertibility of ideals.

Later we will see that if $R = \mathbf{Z}_F$ is a number ring then the class group, denoted $\mathrm{Cl}(F)$, is finite. This group arises in numerous situations. Historically, it first arose in Gauss's study of which numbers n could be represented

by binary quadratic forms $f(x, y) = ax^2 + bxy + cy^2$. It also arose in early investigations of Fermat's Last Theorem; indeed algebraic number theory is sometimes described as a subject that arose out of efforts to prove this theorem. The basic idea is that in the equation $x^p + y^p = z^p$ (where p is an odd prime), the LHS factors over the ring $\mathbf{Z}[\omega] = \mathbf{Z}[e^{2\pi i/p}]$:

$$x^p + y^p = \prod_{i=0}^{[p-1} (x + \omega^i y) = z^p.$$

If the class number is relatively prime to p then with some work one can show that each of the factors on the LHS must be a p-th power and that this leads to a contradiction. The class number is prime to p for all but two primes less than 100.