Lecture 5-24: Dedekind domains

May 24, 2024

Going beyond discrete valuation rings, we develop the properties of non-local integrally closed Noetherian domains of dimension one, or Dedekind domains.

Before specializing down to the main objects of study, we introduce a general definition that is very useful in the study of ideals in integral domains.

Definition, p. 760

Let R be an integral domain with quotient field K. A *fractional ideal* I of R is an R-submodule A of K such that $dA \subseteq R$ for some nonzero $d \in R$ (or equivalently $A \subset d^{-1}R$ for some $d \in R$). A fractional ideal A is said to be *invertible* if there is another fractional ideal B with $AB = R$.

The simplest example of an R-submodule of K that is *not* a fractional ideal is the subgroup S of $\mathbb{Q}$ consisting of all rational numbers whose denominator is a power of 2. If A is invertible, then its inverse B is unique, for if $AB = AC = R$, then $B = B(AC) = (BA)C = C$.

The set of invertible ideals then forms a group under multiplication; as Rk is invertible for every nonzero $k \in K$, the set of principal fractional ideals Rk is a subgroup of this group. The quotient group is called the class group of R (p. 761). In general the class group can be any abelian group. We can get more control on fractional ideals if we assume more about R.

Definition, p. 764

A *Dedekind domain* R is an integrally closed Noetherian domain of dimension one (so that every element of the quotient field EK of R that is integral over R already lies in R).

For example, any PID is a Dedekind domain (since any PID is a UFD and IUFDs are integrally closed).

cf. Theorem 15, p. 765

Every nonzero fractional ideal I in a Dedekind domain R is invertible.

Let K be the quotient field of R. Given $I \neq 0$, define $I^{-1} = \{x \in K : xI \subset R\}$. Then clearly I^{-1} is a nonzero fractional ideal and II^{-1} is an ideal of R. If $II^{-1} \neq R$, then we have $II^{-1} \subseteq M$ for some maximal ideal M. Now the localization R_M is a local Noetherian domain of dimension one which is easily seen to be integrally closed; by a result proved last time it is a DVR. But then the localization I_M of I is principal, say generated by y, which we can take to lie in I. Then $y^{-1} \in K$ sends I and I_M to R, contradicting $II^{-1} \subset M$.

As a simple corollary we get

Theorem; cf. Theorem 15, p. 765

Every nonzero ideal I in a Dedekind domain is a product $P_1 \cdots P_m$ of prime ideals, with the P_i unique up to reordering.

Proof.

If I is not already prime then it lies in a maximal ideal M and we have $M^{-1})M = I, IM^{-1} \subseteq R$. We cannot have $IM^{-1} = I$, for then $IM = I, IMR_M = IR_M$, and then fixing a minimal set of generators $i_1, \ldots, i_m$ of I and arguing as we did last time to show that $M^2 \neq M$ for the maximal ideal M of a local Dedekind domain (we are invoking Nakayama's Lemma, which is Proposition 1 on p. 751), we get a contradiction. Since $1 \in M^{-1}$ we get that IM^{-1} is an ideal of R properly containing I; iterating this process we eventually write I as a finite product $P_1 \cdots P_m$ of maximal ideals P_i, all of them prime. If there is another product $Q_1 \cdots Q_r$ of maximal ideals equalling I, then primeness forces Q_1 to contain one of the P_i, whence $Q_1 = P_i$. Multiplying by $P_i^{-1} = Q_1^{-1}$ and continuing inductively, we deduce the uniqueness. □

Thus we get unique factorization of *ideals* (not of elements) as products of primes in a Dedekind domain. The simplest example of a Dedekind domain for which unique factorization of elements fails (or equivalently, not every ideal is principal) is the integral closure $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ of $\mathbb{Z}$ in $\mathbb{Q}[\sqrt{-5}]$. Here the element 6 has two essentially distinct factorizations into primes, namely $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. The factors $2, 3, 1 \pm \sqrt{-5}$ really are prime in R, since if we define the norm $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2 \in \mathbb{Z}$, as for Gaussian integers, then we have the product rule $N(zw) = N(z)N(w)$. Thus the only way that one of $2, 3, 1 \pm \sqrt{-5}$ could fail to be prime is if there were an element R of norm 2 or 3; but no such element exists.

More generally, the integral closure R of $\mathbb{Z}$ in a finite Galois extension K of $\mathbb{Q}$ (often called the ring of integers in K) is a Dedekind domain, being integrally closed, a domain, and of dimension one (like $\mathbb{Z}$). It is Noetherian because it is in fact a finitely generated $\mathbb{Z}$-module (Theorem 29, p. 676). In this case the class group is known to be finite (for general Dedekind domains it can be any abelian group); its order is called the class number of R (see the definition on p. 761). The class number provides a precise measure of how far the Dedekind domain is from being a PID (or a UFD; it turns out that Dedekind domains are PIDs if and only if they are UFDs). The class number of the ring R above is 2.

Much is known about rings of integers $\mathcal{O}_d$ in quadratic extensions $\mathbb{Q}[\sqrt{d}]$ of $\mathbb{Q}$, where $d \in \mathbb{Z}$ is square-free, particularly (oddly enough) for imaginary extensions (ones with $d < 0$). Here $\mathcal{O}_d$ is spanned over $\mathbb{Z}$ by 1 and $\sqrt{d}$ if $d \equiv 2$ or $3 \mod 4$ and by 1 and $\frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \mod 4$. A striking result obtained only in 1967 is that $\mathcal{O}_d$ is a UFD for $d < 0$ if and only if d is one of the values $-1, -2, -3, -7, -11, -19, -43, -67, -163$. As an interesting historical aside, an earlier proof of this result announced in 1952 but not generally accepted at the time was later acknowledged to be correct after all by the author of the 1967 proof.

Another well-studied case is that of rings $\mathcal{O}_p$ of integers in a cyclotomic field $\mathbb{Q}[e^{2\pi i/p}]$, the splitting field of $x^p - 1$ over $\mathbb{Q}$, where p is prime. Here $\mathcal{O}_p$ is generated by 1 and $e^{2\pi i/p}$ as a $\mathbb{Z}$-algebra. This case is historically important becausethe incorrect assumption that $\mathcal{O}_p$ is always a UFD lay at the heart of many false proofs of Fermat's Last Theorem. In fact $\mathcal{O}_p$ is a UFD only for $p \leq 19$.

In algebraic geometry Dedekind domains arise as coordinate rings of nonsingular curves (Corollary 13, p. 763). Integral closedness of such ring turns out to be equivalent to nonsingularity of the curve. In general integral closedness of the coordinate ring $k[V]$ of a variety V implies but is not equivalent to the codimension of the set of singular points in V being at least 2.

The last week of the course will be devoted entirely to review.