Lecture 3-14: Review, part 3

March 14, 2025

I wrap the review with Dedekind domains and Hensel's Lemma for the ring $\mathbb{Z}_p$ of p-adic integers, with p a prime.

Let K be a finite extension of $\mathbb{Q}$. The corresponding Dedekind domain $\mathcal{O}_K$ consists of the elements in K integral over $\mathbb{Z}$, that is, satisfying a monic polynomial with coefficients in $\mathbb{Z}$. This set is closed under the ring operations (but not under division) and is such that if any $x \in K$ satisfies a monic polynomial with coefficients in $\mathcal{O}_K$, then x already lies in $\mathcal{O}_K$. Its key ring-theoretic properties are that every ideal is finitely generated, it is integrally closed in the sense just described, is a domain, and every nonzero prime ideal is maximal. Integral closure is the hardest property to intuit here, and indeed historically it was the last one whose importance was grasped; but it is essential to ensure the nice properties of Dedekind domains that you have seen. The norm $N(x)$ of any $x \in \mathcal{O}_K$, equal to the product of the images of x under the Galois group G of K, lies in $\mathbb{Z}$, as does the trace of x, which is equal to the sum of the same images.

Using these last facts, it is easy to compute $\mathcal{O}_K$ explicitly in the two most important cases, namely those of a quadratic field $K = \mathbb{Q}[\sqrt{d}]$ for $d \in \mathbb{Z}$, d square-free, and $K = \mathbb{Q}[e^{2\pi i/n}]$ for some integer n. In the first case we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \mod 4$ and $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \mod 4$; in the second case we have $\mathcal{O}_K = \mathbb{Z}[e^{2\pi i/n}]$. (In general, it is quite rare for a Dedekind domain to be generated by a single element over $\mathbb{Z}$.) The formula for the norm of an element $a + b\sqrt{d}$ in the first case is $a^2 - db^2$; note that this quantity indeed lies in $\mathbb{Z}$ even if both a and b are half-integers, rather than both being integers, provided that $d \equiv 1 \mod 4$.

In any Dedekind domain R any nonzero ideal is a product of prime ideals, which is unique up to reordering. If two ideals I, J are identified whenever there are nonzero $a, b \in R$ with $aI = bJ$, then classes of ideals form a group under multiplication, called naturally enough the class group of R. This group is finite for domains R equal to $\mathcal{O}_K$ for some K, but in general can be any abelian group. The domain R is a PID if and only if its class group is trivial. The simplest example where this fails has $K = \mathbb{Q}[\sqrt{-5}], \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$; here the class group has order two.

The theory of finitely generated modules over a Dedekind domain R closely parallels that of finitely generated modules over a PID, treated in the fall. Any such module takes the form $R^n \oplus I \oplus T$ for some nonnegative integer $n,$, nonzero ideal I, and (finitely generated) torsion submodule T; two such sums $R^n \oplus I \oplus T$ and $R^m \oplus J \oplus T'$ are isomorphic if and only if $n = m, T \cong T''$ and the ideals I, J lie in the same class. A torsion-free module is always projective; it is free if and only if the ideal I occurring in its decomposition is principal. A finitely generated torsion module takes essentially the same form as over a PID, being a direct sum of quotients $R/P_i^{n_i}$ for powers $P_i^{n_i}$ of prime ideals P_i, with two such direct sums being isomorphic if and only if they involve they involve the same prime ideals raised to the same powers.

Rounding out my treatment of representations of finite groups in the fall, I discussed semisimple Artinian rings (of which group algebras of finite groups over fields of characteristic 0 are a special case). These are Artinian rings (satisfying the descending chain condition on left or right ideals) having no nonzero nilpotent two-sided ideals. Every such ring R is a finite direct sum $\oplus M_{n_i}(D_i)$ of $n_i \times n_i$ matrix rings over a division ring D_i; if in addition R is finite-dimensional over an algebraically closed field K, then we have $D_i = K$ for all i. A simple Artinian ring (having no nonzero proper two-sided ideals) is a single matrix ring over a division ring. Going beyond semisimple rings, a commutative ring is Artinian if and only if it is Noetherian and every prime ideal in it is maximal.

.I also briefly treated discrete valuation rings (DVRs), which are principal ideal domains D with just one prime element x up to multiplication by units. The only nonzero ideals in any such R are the principal ones (x^n) generated by powers of x. The most important examples take the form R_p, the localization of R at p, where R is a PID, $p \in R$ is prime, and R_p consists of all fractions $\frac{a}{b}$ in the quotient field K of R with $p \not| b$. In particular one could take $R = \mathbb{Z}$ with p a prime integer or $R = K[x], K$ a field, with $p = x$.

In both of these last cases (in fact for any localization R_p with R a PID) one can complete R_p by forming the set of all series $\sum_{i=0}^{\infty} k_i p^i$. If $R = \mathbb{Z}$ and p is a prime number, then the coefficients k_i may be taken to lie in the set $\{0, \dots, p-1\}$ of coset representatives of $p\mathbb{Z}$ in $\mathbb{Z}$; if $R = K[x]$ one takes the coefficients to lie in K (thought of as a set of coset representatives of (x) in R). In the second case one adds and multiplies power series as with Taylor series in calculus; in the first case one does the same, but keeping track of "carrying" in the coefficients. The completed ring is the power series ring $K[[x]]$ in the second case; it is called the ring of p-adic integers and is denoted $\mathbb{Z}_p$ in the first case.

The main fact you should know about $\mathbb{Z}_p$ is Hensel's Lemma, to be proved next quarter. It states that given any polynomial $F \in \mathbb{Z}[x]$ whose reduction f in $(\mathbb{Z}/p\mathbb{Z})[x]$ has distinct roots in its splitting field has a full complement of roots in $\mathbb{Z}_p$. Thus this complete ring can do many things that $\mathbb{Z}$ cannot (but has characteristic 0, as $\mathbb{Z}$ does).

Good luck and have a nice break!