Math 505, 1/25

We now take up the study of commutative rings, starting with a particular class of them rather than such rings in general. Rings in this class are a little but not much more complicated than PIDs in some sense, and in particular finitely generated modules over them admit a very similar classification to the PID case. These rings are called *Dedekind domains*; we will begin with a quite nonstandard definition of them which is however equivalent to the standard one and most convenient for our purposes. Call a (commutative) integral domain R a Dedekind domain if for any ideals I, J of R with $I \subset J$ there is an ideal K of R with $I = JK$. We note at once that the ideal K is unique, except for the trivial case $I = J = 0$; indeed, if $JK = JK' \neq 0$, then we can choose $a \in J$ with $a \neq 0$ and then there is an ideal L with $LJK = LJK' = aK = aK'$, forcing $K = K'$ since R is an integral domain. We say that nonzero ideals I, J of R lie in the same *ideal class* if there are nonzero $a, b \in R$ with $aI = bJ$; one checks immediately that this is an equivalence relation and the ideals equivalent to R itself are exactly the principal ones. Then the ideals J in the same class as I are exactly those isomorphic as R-modules to I, for if $\pi : I \to J$ is an isomorphism and $x \in I, x \neq 0$, then we have $x\pi(y) = \pi(xy) = \pi(x)y$ for $y \in I$, whence $xJ = \pi(x)I$. Note that ideal classes form a group under multiplication; the definition of Dedekind domain guarantees that every ideal class has an inverse. Next we show that every ideal I in a Dedekind domain is finitely generated. If $I \neq 0$, choose a nonzero element a of it and write $(a) = IJ$ for some ideal J. By definition of the ideal product, there are finitely many elements $x_1, \ldots, x_n$ in $I, y_1, \ldots, y_n$ in J with $a = x_1y_1 + \ldots + x_ny_n$. The ideal I' generated by the x_i then satisfies $I'J \subset IJ = (a)$, but it contains the generator a, so $IJ = I'J$, whence $I = I'$ is finitely generated. From this it follows that R is *Noetherian*: every nonempty set of ideals of R has a maximal element, or equivalently there are no infinite strictly ascending chains $I_1 \subset I_2 \subset \cdots$ of ideal in R: indeed, given such a chain, its union I would be an ideal and this finitely generated; but then for i large enough I_i contains all generators of I and thus I itself, whence $I_i = I_j$ for $j > i$, a contradiction. Next, I claim that *every nonzero ideal I of R is uniquely (up to reordering) a finite product of maximal ideals*. Given I, if it is not maximal already, then it lies in a maximal ideal M_1, whence $I = M_1I_2$ for an ideal I_2 strictly containing I; if I_2 is not maximal, we write $I_2 = M_2I_3$ for some maximal ideal M_2 and ideal I_3 strictly containing I_2, and so on; since there are no infinite strictly ascending chains of ideals in R, the process terminates, realizing I as a finite product of maximal ideals $M_1 \cdots M_n$. For the uniqueness, observe that if also $I = N_1 \cdots N_r$ with the N_i maximal, then N_1, as a prime ideal of R, contains the product $M_1 \cdots M_n$ and thus M_i for some i, whence by maximality $N_1 = M_i$. Cancelling M_i, N_1 from both products equalling I, we see that $n = r$ and the N_i are a permutation of the M_j (note that the M_i need not be distinct, and similarly for the N_j). As a consequence, *every nonzero prime ideal P of R is maximal*, for P must be a product $M_1 \cdots M_n$ of maximal ideals, whence P contains and must equal M_i for some i. Finally, one last ideal-theoretic property of R: *given any nonzero ideal I of R and f in the* *quotient field of R, if $fI \subset I$, then $f \in R$.* Indeed, if $fI \subset I$, then fI is an ideal of R contained in R, whence $fI = IRf = IJ$ for some ideal J of R, whence by cancellation the R-submodule Rf of F generated by f equals J, forcing f to lie in R. We express this trio of properties (R a Noetherian integral domain, every nonzero prime ideal of R is maximal, any f in the quotient field of R that maps a nonzero ideal to itself actually lies in R) by saying that R is an *integrally closed Noetherian domain of dimension one*; here "integrally closed" means that every element of the quotient field F of R satisfying a monic polynomial with coefficients in R actually lies in R, a property equivalent to the third one above; while "dimension one" expresses the maximality of every nonzero prime ideal; we will give a general account of dimension for commutative rings later. The standard definition of Dedekind domain is then an integrally closed Noetherian domain of dimension one.

Now we are ready to exhibit our main example of Dedekind domains. Let L be an algebraic number field (a finite extension of $\mathbf{Q}$, not necessarily Galois). Let R consist of the algebraic integers in L (roots of monic polynomials over $\mathbf{Z}$). Then we claim that R is a Dedekind domain. This will take some work to prove. Begin by noting (as we did when discussing characters of finite groups) that R is at least a ring. Next we claim that R is a free $\mathbf{Z}$-module of finite rank. To prove this note first that by clearing denominators we see that for any $x \in L$ there is a nonzero $n \in \mathbf{Z}$ with $nx \in R$. Let $x_1, \ldots, x_m$ be a basis of L over $\mathbf{Q}$ and for each i choose a nonzero integer n_i with $y_i = n_i x_i \in R$, so that the y_i also form a basis of L over $\mathbf{Q}$. For any $y \in R$, the products yy_i lie in R and therefore have traces that are rational algebraic integers and thus integers. But any $y \in L$ is completely determined by the traces of the yy_i, since the trace is a nondegenerate (symmetric) bilinear form on L. It follows that as an additive group R is isomorphic to a subgroup of $\mathbf{Z}^m$, whence it like $\mathbf{Z}^m$ is free and finitely generated over $\mathbf{Z}$ (in fact of rank exactly m).

We now claim that *every nonzero proper ideal I in R contains a product of nonzero prime ideals.* If this failed, there would be a largest ideal I for which it failed, so that I contains no such product, but any larger ideal does contain such a product. But then I cannot itself be prime; if $a, b \in R$ are such that $ab \in I$ but $a, b \notin I$, then the larger ideals $I + (a), I + (b)$ of R contain products of nonzero prime ideals, whence so too does their product $(I + (a))(I + (b))$, which lies in I, a contradiction. Now we need our last property above of any nonzero ideal I of $R :$ if an element f of the quotient field of R satisfies $fI \subset I$, then $f \in R$. To see this we note that I is necessarily a free module of finite rank over $\mathbf{Z}$; under the hypothesis multiplication by f defines a $\mathbf{Z}$-linear transformation from this module to itself, whence by the Cayley-Hamilton Theorem it satisfies its own characteristic polynomial, which is monic with integer coefficients, forcing f to lie in R, as desired. We will complete the proof that R is a Dedekind domain next time.