Math 505, 1/27

Now we can finally prove that the ring R of algebraic integers in an algebraic number field L is a Dedekind domain. Given ideals I, J with $I \subset J$, we must show that $I = JK$ for some K. This trivially holds if $J = R$; if it fails for any ideal J, there must be a largest one for which it fails, so that it holds for any strictly larger ideal J'. Choose $a \neq 0$ in J and let $P_1 \cdots P_r$ be a minimal product of nonzero prime ideals lying in the principal ideal (a). Also choose a maximal ideal P containing J. Then P contains the product $P_1 \cdots P_r$, whence it contains and must equal one of the P_i, say P_1. Then the product $P_2 \cdots P_r$ of fewer than r prime ideals cannot be contained in (a), so there is $b \in R$ lying in this product but not in (a). Then $bJ \subset bP \subset P_1 \cdots P_r \subset (a)$, whence $(b/a)J \subset R$, even though the fraction b/a does not lie in R (since $b \notin (a)$). Now look at the ideal $J' = a^{-1}(a, b)J = J + (b/a)J$, where (a, b) denotes the ideal generated by a and b. Since $b/a \notin R$ we deduce by a property of ideals of R proved last time that $(b/a)J$ is not contained in J, whence the ideal J' is strictly larger than J. By the choice of J there is an ideal K' with $I = J'K'$. Now set $K = a^{-1}(a, b)K'$. This is an R-submodule of its quotient field F and $JK = a^{-1}(a, b)JK' = J'K' = I$; since $JK \subset J, K$ must be an ideal of R, not just a submodule of F. This completes the proof.

We can measure precisely how close a Dedekind domain D is to being a PID via its *class group*, the multiplicative group of (nonzero) ideal classes. For a general Dedekind domain, this can be any abelian group, but for the rings R of algebraic integers in number fields L, it turns out that this group is always finite. It is already very interesting in the simplest special case $L = \mathbf{Q}(\sqrt{-m}$ for m a positive nonsquare integer; here it turns out that the class group is trivial exactly in the cases $m = 1, 2, 3, 7, 11, 19, 43, 67, 163$ and no others! Gauss conjectured this result; it was finally proven in 1952, with the proof not acknowledged to be correct until 1967. Thus the simplest case where this ring is not a PID is the case $m = 5$: here the two essentially distinct factorizations $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ of 6 show that this ring admits nonprincipal ideals.

We now show another way in which Dedekind domains are very close to PIDs: given a nonzero proper ideal I in such a domain R, the quotient R/I is such that every ideal is principal (though this quotient generally has zero divisors). To see this let $M_1, \ldots M_k$ be the maximal ideals containing I, so that I is the product of powers of the M_i. Choose an element x_1 in M_1 but not in M_1^2. The ideals $M_1^2, M_2, \ldots, M_k$ are pairwise coprime (i.e. the sum of any two of them is R), so by the Chinese Remainder Theorem there is $y_1 \in R$ that is congruent to x_1 modulo M_1^2 and to 1 modulo any other M_i. Then the ideal generated by I and x_1 lies in M_1 but not in M_1^2 nor any other maximal ideal, so this ideal must be M_1 itself. Hence the image M_1/I in R/I is principal, being generated by y_1, and similarly the image M_i/I is also principal for all other i. Since any ideal J in R/I is a product of maximal ideals M_i/I it too must be principal. Thus every ideal in any Dedekind domain is generated by at most two elements.

It now turns out that Dedekind domains are closely related to PIDs in yet

another way, one which motivates a general construction that is a basic tool in commutative algebra. It is called *localization*; we have seen it briefly in connection with working out the behavior of $\mathbf{Z}$-modules when tensored with $\mathbf{Q}$. Let S be a multiplicatively closed subset of a (general) commutative ring A, so that $1 \in S$ and S is closed under multiplication; to avoid trivialities we also assume that $0 \notin S$. We now generalize the construction of the quotient field of an integral domain to A, even though A may contain zero divisors. Let $S^{-1}A$, the *localization of A at S*, consist of all formal fractions a/s with $a \in A, s \in S$. We decree that $a/s = b/t$ if and only if there is $u \in S$ with $u(at - bs) = 0$; one easily checks that this is an equivalence relation (but it would not be if the relation were just $at - bs = 0$). We then add and multiply fractions in the standard way from high-school algebra, checking that this is well-defined on equivalence classes. There is a natural homomorphism from A to $S^{-1}A$, sending a to $a/1$, which is *not* in general 1-1; its kernel is the set of all $a \in A$ such that $sa = 0$ for some $s \in S$. Then every ideal J of $S^{-1}A$ is generated by its intersection I with A, which is an ideal of A (look at the numerators of elements of J); if I has nonempty intersection with S, then J blows up in the sense that it is all of $S^{-1}A$. The most important example occurs when S is the *complement* in A of a (proper) prime ideal P of A (so that S is multiplicatively closed by definition of a prime ideal). We denote $S^{-1}A$ by A_P in this case and call it (by abuse of terminology) the localization of A at P. Passing from A to A_P thus cuts out all ideals not contained in P; it is not difficult to check conversely that *there is a 1-1 correspondence between prime ideals of A contained in P and prime ideals of A_P (in fact, for any multiplicatively closed subset S, there is a 1-1 correspondence between prime ideals of A not meeting S and prime ideals of $S^{-1}A$, mapping I to $S^{-1}I$*. We will say more about localization at prime ideals in the context of Dedekind domains next time.