Math 505, 1/30

Having explored some of the properties of localization for general commutative rings last time, we now look at how it works for integral domains D. The first point is that the definition last time that two fractions $a/s, b/t$ are equal if and only if there is u in our multiplicatively closed subset S with $u(at - bs) = 0$ simplifies to just $at - bs = 0$ (as in the construction of the full quotient field of D), since $0 \notin S$ and D has no zero divisors. In particular, the map from D to $S^{-1}D$ sending x to $x/1$ is 1-1 in this case. Now specialize to the case where D is a Dedekind domain. We have seen that nonzero prime ideal P of D is maximal. The localization D_P of D at P, cutting out as it does all primes ideals of D not contained in P, leaves only two remaining prime ideals in D_P, namely 0 and $Q = PD_P$ (the ideal of D_P generated by P). But every nonzero ideal of D_P, like every nonzero ideal of D, is a product of prime ideals, so *every nonzero ideal in D_P is a power of Q*: the ideal structure of D_P is drastically simpler than it would be even for a general PID. In fact, D_P is a PID: we know that $Q \neq Q^2$ in D_P, as in D, and if $x \in Q, x \notin Q^2$, then the principal ideal (x) is not contained in Q^2 or any higher power of Q, so it must be all of Q. Thus *every element of D_P is a power of x times a unit in D_P*. We call D_P a *discrete valuation ring*, or DVR for short; in fact we could have called it a DVD, since it is an integral domain, but that abbreviation has been co-opted for another purpose. We will give the reason for this terminology later. Perhaps the simplest example is $\mathbf{Z}_{(p)}$ for p a prime; this ring is not the ring of integers mod p, but rather the the ring of all rational numbers whose denominators are not divisible by p. A "naturally occurring" example (not arising by explicitly localizing another ring) is the ring $K[[x]]$ of formal power series $\sum_{n=0}^{\infty} a_n x^n$ in one variable x over a field K; here we impose no convergence requirement on the power series. We add two power series $\sum a_n x^n, \sum_n b_n x^n$ in the obvious way and multiply them via the rule $\sum_n a_n x^n \sum_n b_n x^n = \sum_n c_n x^n$, where $c_m = \sum_{n=0}^{m} a_n b_{m-n}$. At first you might think that the structure of $K[[x]]$ would be more complicated than that of the polynomial ring $K[x]$; in fact, it is much simpler, since an easy inductive argument shows that any power series $\sum_{n=0}^{\infty} a_n x^n$ with $a_0 \neq 0$ is a unit in $K[[x]]$, so that any element of $K[[x]]$ is a power of x times a unit, so that the only nonzero ideals of $K[[x]]$ are powers of (x). Returning now to a general discrete valuation ring R whose maximal ideal is generated by a single element x, we define a map v from R to the nonnegative integers by decreeing that $v(x^n u) = n$ if u is a unit in R, while $v(0)$ is undefined (or sometimes is taken to be $-\infty$). Then we have $v(ab) = v(a) + v(b)$ for $a, b \neq 0 in R$, while $v(a + b) \geq \min(v(a), v(b))$ if $a, b, a + b \neq 0$ in R. Such a map v is called a *discrete valuation* (discrete since its range lies in a discrete set). We extend it to the quotient field K of R by decreeing that $v(x^m u) = m$ for any integer m, positive or negative; then we can recover R from K as the set of elements x with $v(x) \geq 0$. In fact, given any field K and a valuation v from K^* to $\mathbf{Z}$, the subring R consisting of all $x \in K$ with $v(x) \geq 0$ is a discrete valuation ring; if $y \in R$ is such that $v(y) = k > 0$ and k is minimal, then it is not difficult to check that the principal ideal (y) contains all $x \in K$ with $v(x) \geq k$

and powers of this ideal account for all the nonzero ideals of R. (Nondiscrete valuation rings, having valuations with ranges in other ordered groups, can have a more complicated structure.) A famous example of a discrete valuation ring, combining the features of the modular integers and power series, is the ring of *p-adic integers* for p a prime. As a set this is just $\mathbf{Z}_p[[x]]$, the power series ring over $\mathbf{Z}_p$; the ring operations are those of $\mathbf{Z}_p[[x]]$ with "carrying", so that whenever a coefficient of a power of p exceeds p, we subtract off the appropriate multiple kp of p from it and then add k to the coefficient of the next higher power of p. Thus for example the sum of 1 and the series $\sum_{n=0}^{\infty}(p-1)p^n$ is 0, so that this series equals -1, the additive inverse of 1, while the product of $1+(p-1)p$ and the series $\sum_{n=0}^{\infty} p^n$ is 1, so the series is the multiplicative inverse of $1+(p-1)p$ in the p-adic integers. The quotient field $\mathbf{Q}_p$ of the p-adic integers consists of all Laurent series in p (involving finitely many negative powers of p). It is usually denoted $\mathbf{Q}_p$; similarly one often uses the notation $\mathbf{Z}_p$ for the p-adic integers; but we will have no further occasion to use them and so will reserve this notation for the integers mod p.

Before leaving Dedekind domains we mention one other result that will be needed in this week's homework: given a nonzero ideal I, J in a Dedekind domain D, there is an ideal I' in the ideal class of I that is coprime to J (so that $I' + J = D$). To prove this, begin as usual by choosing $a \in I, a \neq 0$ and write $IK = (a)$ for some ideal K of D. Then we have seen that K is generated by JK and one other element, say x. Multiplying the equation $K = JK + (x)$ by I and dividing by a, we get $R = J + Ix/a$, whence $I' = Ix/a$ is an ideal coprime to J in the class of I, as desired. This result is needed to complete the classification of finitely-generated torsion-free modules (and ultimately all finitely generated modules) over D.