Lecture 5-22: Wrapping up prime spectra and discrete valuation rings

May 22, 2024

We wrap up the discussion of prime spectra with a couple of important examples and then consider a class of rings whose prime spectrum consists of two points.

We present two final examples of prime spectra, following Examples 2 and 3 in DF, pp. 735-6. First take $R = \mathbb{Z}[x]$, the polynomial ring in one variable over $\mathbb{Z}$. Any prime ideal P of R has prime contraction to $\mathbb{Z}$, which must be either 0 or the ideal (p) generated by a prime number p. In the first case P does not meet the multiplicatively closed set $\mathbb{Z}^*$ of nonzero integers, so it is the contraction to R of a prime ideal in $\mathbb{Q}[x]$. Any such ideal is principal, either 0 or generated by an irreducible polynomial $f \in \mathbb{Z}[x]$ which is moreover *primitive* in the sense that the greatest common divisor of its coefficients is 1; recall by Gauss's Lemma that a primitive polynomial in $\mathbb{Z}[x]$ is irreducible if and only if it is irreducible in $\mathbb{Q}[x]$. The ideal (f) is not maximal.

In the second case, where P contracts to (p), P is the preimage in R of a prime ideal in $R' = \mathbb{Z}_p[x]$, a principal ideal domain; so P must take the form (p, g), where g is a monic polynomial in R whose reduction mod p is irreducible in R'. The ideal (p, g) is then maximal.

Following the picture on p. 737, we can portray Spec R by showing how it projects by contraction to Spec $\mathbb{Z}$. For example, take $f = x^4 + 1 \in R$. This polynomial is irreducible, but becomes reducible upon reduction modulo any prime p. Modulo 2, this polynomial is the fourth power of $x + 1$, so there is just one closed point in $\mathcal{Z}(f)$ lying over $(2) \in$ Spec $\mathbb{Z}$. Modulo a prime $p \equiv 1 \mod 8$, f has four distinct roots, so there are four such closed points; modulo all other primes p, there are just two such closed points.

The picture is much the same (but perhaps geometrically more satisfying) for $R = k[x, y]$, the polynomial ring in two variables over an algebraically closed field k; the point is that R can be viewed as a polynomial ring in one variable y over the PID $k[x]$. The elements of Spec R consist of the generic point (0); the principal ideal (f) generated by an irreducible polynomial f in R, of height 1; and the closed points $(x - a, y - b)$ for $a, b) \in k^2$. The closure of an "intermediate" point like (f) consists of this point together with the closed points corresponding to the zero locus of f.

Finally, we mention that for three or more variables all hell breaks loose; for $n \geq 3$ there are prime ideals in $k[x_1, \ldots, x_n]$ requiring arbitrarily many generators.

Now we shift gears significantly, looking at rings whose prime spectra have exactly two points.

Definition; DF, p. 755

A *discrete valuation* on a field K is a surjective map $\nu : K^* \to \mathbb{Z}$ such that $\nu(xy) = \nu(x) + \nu(y)$ and $\nu(x+y) \geq \min(\nu(x), \nu(y))$ for all $x, y \in K^*$ with $x + y \neq 0$. The subring $R = \{x \in K : \nu(x) \geq 0\} \cup \{0\}$ is called the *valuation ring* of ν; we also say that R is a *discrete valuation ring* or *DVR*.

Sometimes one extends ν to all of K by decreeing that $\nu(0) = \infty$. The field of tropical geometry studies the operations of addition and taking the minimum on the right side of the definition of valuation, (roughly) using them in place of ordinary multiplication and addition.

Example

Fixing a prime $p \in \mathbb{Z}$, we can define a valuation on $\mathbb{Q}$ via $\nu(\frac{p^n a}{b}) = n$ for all integers a, b relatively prime to p and all $n \in \mathbb{Z}$. The corresponding DVR is the localization $\mathbb{Z}_{(p)}$ at the prime ideal (p). Similarly, if F is a field and $f \in F[x]$ is irreducible, we can define a valuation ν on the rational function field $F(x)$ via $\nu(\frac{f^n p}{q}) = n$ for all polynomials p, q relatively prime to f and all $n \in \mathbb{Z}$; the corresponding DVR is the localization $F[x]_{(f)}$. Taking K to be the field $k((t))$ of Laurent series over a field k, that is, power series $f = \sum_{i=m}^{\infty} k_i x^i$ with $k_i \in k, k_m \neq 0$, and m an integer (possibly negative), we can define $\nu(f) = m$. Then the DVR is the ring $k[[x]]$ of power series $\sum_{i=0}^{\infty} k_i x^i$ (with the obvious ring operations). See pp. 755-6.

Example

Finally, putting these examples together, if $p \in \mathbb{Z}$ is prime, we define the field $\mathbf{Q}_p$ of p-adic numbers as the set of formal series $\sum_{i=m}^{\infty} a_i p^i$, where the a_i lie in $\mathbb{Z}/p\mathbb{Z}$, the integers mod p, m is an integer, and the ring operations are as in $\mathbb{Z}/p\mathbb{Z}$ in each coefficient, but with carrying, so that for example the sum of $1 = 1p^0 + \sum_{i=1}^{\infty} 0p^i$ and $\sum_{i=0}^{\infty}(p-1)p^i$ is 0. Then one can check that $\mathbb{Q}_p$ is indeed a field; the valuation ν on it is such that if $f = \sum_{i=m}^{\infty} a_i p^i$ with $a_m \neq 0$, then $\nu(f) = m$. The ring of p-adic integers (usually denoted $\mathbb{Z}_p$, but one must of course be careful not to confuse this with the integers mod p) then consists of all sums $f = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Q}_p$.

The basic structural properties of DVRs are given by

Proposition 5, p. 756

Let R be a DVR with quotient field K, corresponding to the valuation ν, and choose $t \in R$ with $\nu(t) = 1$.

- Every nonzero element r of R can be written as ut^n for some unit $u \in R$ and $n \in \mathbb{Z}, n \geq 0$; r is a unit if and only if $n = 0$. Every nonzero element in the quotient field K of R takes the form ut^n for some $n \in \mathbb{Z}$ and unit u.
- The principal ideals (t^n) for $n \geq 0$ exhaust the nonzero ideals of R; in particular, R is a Noetherian local ring with just two prime ideals.

The element t in the proposition is called a uniformizing (or local) parameter for R (p. 756).

Proof.

If $u \in R$ is a unit then there is $v \in R$ with $uv = 1$; since $\nu(1) = \nu(1) + \nu(1)$ we must have $\nu(1) = 0$ and then $\nu(u) = \nu(v) = 0$. Conversely, if $u \in K$ has $\nu(u) = 0$, then $v = u^{-1} \in K$ and we must have $\nu(v) = 0$, so $u, v \in R$ and u is a unit. Given any $r \in R$ with $\nu(r) = n$, we have $\nu(rt^{-n}) = 0$ whence $rt^{-n} = u \in R$ is a unit and r takes the desired form. Taking quotients we see that any $x \in K$ takes the given form as well. Thus the products ut^n are exactly the elements $r \in R$ with $\nu(r) = n \geq 0$; if I is a nonzero ideal and we choose $r \in I$ with $\nu(r)$ minimal we see at once that $I = (r)$, as claimed. $\square$

Conversely, if R is a PID having only one nonzero prime ideal $P = (x)$, then x is the only prime element of R up to unit multiples and unique factorization shows that every element of R takes the form ux^n for a unique $n \geq 0$ and unit u. We can define a valuation ν on the quotient field K of R via $\nu(ux^n) = n$ for all $n \in \mathbb{Z}$ and units u and then recover R as the DVR corresponding to K and ν. In particular DVRs are integrally closed (being UFDs, by an earlier argument). It is a remarkable fact that the properties of integral closure, localness, and Krull dimension 1 characterize DVRs (for integral domains).

Theorem 7, p. 757

Any local integrally closed Noetherian domain of Krull dimension 1 (so that every nonzero prime ideal is maximal) is a DVR.

Proof.

Let R be such a domain with maximal ideal M. We claim first that we must have $M^2 \neq M$. Indeed, M is finitely generated; let $m_1, \ldots, m_n$ be a minimal set of generators. If we had $M^2 = M$ then we would get $m_n = r_1 m_1 + \cdots + r_n m_n$ for some $r_i \in M$, whence $m_n(1 - r_n) = r_1 m_1 + \cdots r_{n-1} m_{n-1}$. But all the nonunits of R lie in its maximal ideal M while $1 - r_n$ cannot lie in M, so it must be a unit. This forces m_n to be generated by $m_1, \ldots, m_{n-1}$, contradicting minimality. Hence there is $t \in M$ with $t \notin M^2$. The radical $\sqrt{(t)}$ of the principal ideal generated by t is an intersection of prime ideals, so it must be all of M since M is the only nonzero prime ideal. Now any ideal I in a Noetherian ring S contains a power J^m of its radical J; to see this, let $j_1, \ldots, j_r$ be a set of generators of J, with $j_i^{n_i} \in I$. By the multinomial theorem, $(s_1 j_1 + \cdots + s_r j_r)^N \in I$ for any $s_i \in S$ if $N > n_1 + \cdots + n_r$, since every term of the sum giving this power involves some j_i raised to a power at least n_i. $\square$

Proof.

Now we claim that $M = (t)$. If not, then there would be some $n \geq 2$ with $M^n \subseteq (t), M^{n-1} \not\subseteq (t)$, and there is $x \in M^{n_1}, x \notin (t)$ with $xM \subset (t)$. Since $t \neq 0$ the element $y = x/t$ lies in the quotient field K of R and we have $y \notin R$ since $x = ty \notin (t)$. By the choice of x we have $yM \subseteq R$, so that yM is an ideal of R. We cannot have $1 = ym$ for any $m \in M$ as that would force $t = xm \in M^2$, whence yM is a proper ideal, necessarily contained in M. Looking at the matrix of the action of y on M relative to a set of generators of M, as in the proof that the elements of an extension B integral over a subring A form a subring, we see that this forces some monic polynomial $p \in R[x]$ to have $p(y) = 0$, forcing $y \in R$ since R is integrally closed. We conclude finally that $M = (t)$ is principal. We next show as in the proof that $M \neq M^2$ that $\cap_n M^n = 0$. A similar argument to one above then shows that every ideal of R is principal. Then since R has only one prime ideal M, it is a DVR by the preceding result. $\square$