Lecture 3-7: Completions of rings

March 7, 2025

As indicated last time, I will show how to enlarge a DVR (and in fact any commutative ring) to a larger ring which is complete with respect to a certain topology; thus this larger ring can do many things that the original ring could not, just as completions of metric spaces can do many things the original metric spaces could not. I will give just a brief treatment of completions now, returning to them in much more detail next quarter.

Rather than give the general construction at the outset, I will warm up to it with a couple of examples. For any field K, it is well known that the only units in the polynomial ring $K[x]$ are the nonzero constant polynomials. The power series ring $K[[t]]$, consisting by definition of all formal power series $\sum_{i=0}^{\infty} a_i x^i$ with $a_i \in K$, has many more units; in fact any power series $\sum_{i=0}^{\infty} a_i x^i$ with $k_0 \neq 0$ is a unit. To see this, recall that $(\sum a_i x^i)(\sum b_i x^i) = \sum_{i=0}^{\infty} c_i x^i$, where $c_n = \sum_{i=0}^{n} a_i b_{n-i}$ (or take this as the definition, motivated by the distributive law for polynomials). If $a_0 \neq 0$, then we can take $b_0 = a_0^{-1}$; assuming inductively that $b_0, \ldots, b_{n-1}$ have been defined, one can solve the equation $c_n = \sum_{i=0}^{n} a_i b_{n-i} = 0$ for b_n, since its coefficient is a_0.

Similarly, the ring of Laurent series $\sum_{i=-m}^{\infty} a_i x^i$ (for some $m \in \mathbb{Z}$), studied in complex analysis, is actually a field. Now consider a variation of this construction. For p a fixed (positive) prime integer, consider the set of formal series $\sum a_i p^i$, where each $a_i \in [p] = \{0, \dots, p-1\}$. To add two such series $s = \sum a_i p^i, t = \sum b_i p^i$, start with the sum $\sum (a_i + b_i) p^i$ and then replace each $a_i + b_i$ by a finite polynomial $\sum c_{ij} p^j$, where the c_{ij} again lie in $[p]$; (in effect just rewrite $a_i + b_i$ in base p). Combining terms in the resulting series, further rewrite $s + t = \sum (a_i + b_i) p^i$ as a single series $\sum d_i p^i$ with $d_i \in [p]$. Define the product st similarly.

This ring is called the ring of p-adic integers and is denoted $\mathbb{Z}_p$; of course this must be carefully distinguished form the ring $\mathbb{Z}/p\mathbb{Z}$ of integers modulo p. Similarly, the ring of Laurent series $\sum_{i=m}^{\infty} a_i p^o$ with $a_i \in [p]$ is denoted $\mathbb{Q}_p$ and called the ring of p-adic rationals. For example, in $\mathbb{Z}_p$ we have $-1 = \sum_{i=1}^{\infty}(p-1)p^i$ and $(1-p)^{-1} = \sum_{i=0}^{\infty} p^i$.

More generally, let R be any commutative ring and let I be an ideal of R. The main example to keep in mind is the case where R is a DVR and M its maximal ideal. Define the I-adic topology on R by decreeing that a neighborhood of any point x is a subset of R containing the coset $x + I^n = \{x + +i : i \in I^n\}$ for some n. A subset of R is then by definition open if and only if it is a neighborhood of all of its points. The ring operations in R are continuous with respect to this topology. A Cauchy sequence (r_i) of elements of R in this topology is then one such that for any n we have a positive integer N with $r_i - r_j \in I^n$ for any indices $i, j > N$.

I want to create a larger ring $\hat{R}$ for which any Cauchy sequence (r_i) converges, so that there is $r \in R$ such that for every index n there is N with $r - r_m \in I^n$ for all $m > N$. To do this I use an inverse limit construction, as I did earlier when constructing Galois groups of infinite algebraic extensions. Start with the direct product $\prod_{i=0}^{\infty} R/I^i$ and take the subring $\hat{R}$ consisting of all tuples $(r_0, r_1, \ldots)$ such that $r_i \equiv r_j$ modulo I^i whenever $i < j$. Clearly $\hat{R}$ is closed under the ring operations. In the two particular cases $R = \mathbb{Z}, I = (p)$ and $R = K[x], I = (x)$ mentioned above one can check directly that $\hat{R}$ becomes $\mathbb{Z}_p$ and $K[[x]]$, respectively. The ring operations are more complicated for $\mathbb{Z}_p$ than they are for $K[[x]]$ because $\mathbb{Z}$ has no additive subgroup complementary to the subgroup $(p)^n = p^n\mathbb{Z}$, whereas $K[x]$ admits a natural subgroup complementary to (x^n).

In general there is an obvious map $R \to \hat{R}$, sending r to $(r, r, \ldots)$; its kernel is 0 provided that $\cap I^n = 0$. If this map is an isomorphism then R is called *I-adically complete*. I will return to completions in much more detail next quarter, when I will verify that $\hat{R}$ is indeed I-adically complete..

To get a flavor of what I-adic completion can do, let me mention one of the most basic and frequently used results, called *Hensel's lemma*.

Lemma

Let R be a commutative ring and M a maximal ideal in R. Let $f \in R[x]$ be a monic polynomial such that the reduction $\bar{f}$ of f in $(R/M)[x]$ admits a factorization $\bar{g}\bar{h}$ with $\bar{g}, \bar{h}$ coprime polynomials. Then the image $\hat{f}$ of f in $\hat{R}[x]$, with $\hat{R}$ the M-adic completion of R, factors as $\hat{g}\hat{h}$, where $\hat{g}, \hat{h}$ have the same respective degrees as $\bar{g}, \bar{h}$.

As an example, since 2 has the distinct square roots 3 and 4 modulo 7, it also has a square root in the ring $\mathbb{Z}_7$ of 7-adic integers.

As completion is more familiar in the context of metric spaces than arbitrary topological spaces I will indicate how to recover the topology introduced above on a commutative ring R from a metric. Let M be a maximal ideal of R with $\cap_n M^n = 0$. For $r \in R, r \neq 0$, set $v(r) = n$ if $r \in M^n$ but $r \notin M^{n+1}$. Then the function $\rho : R \times R \to \mathbb{R}^+$ defined by $\rho(x, y) = 2^{-v(x-y)}$ if $x \neq y, \rho(x, x) = 0$, is easily seen to be a metric. In fact it satisfies a stronger version of the usual triangle inequality: for $x, y, z \in R$ we have $\rho(x, z) \leq \max(\rho(x, y), \rho(y, z))$ instead of just $\rho(x, z) \leq \rho(x, y) + \rho(y, z)$. Such a function is called an ultrametric, or non-Archimedean. The completion of R as a metric space then coincides with the completion $\hat{R}$ with respect to the M-adic topology. (In case $R = \mathbb{Z}$ and $M = (p)$ for p prime, one generally replaces 2 by p in the definition of ρ.)

If in addition R is an integral domain with quotient field K, then any unit $u \in R$ does not lie in M, so that $v(u) = 0$. Thus one can extend v to K^* by decreeing that $v(x^{-1}) = -v(x)$ and extend ρ to an ultrametric on K similarly. More generally, K is a field, then a function $f : K \times K \to \mathbb{R}^+$ with $f(a+b) \leq f(a) + f(b)$ for $a, b, a+b \neq 0$, is called an absolute value. Given such a function the function $\rho : K \times K \to \mathbb{R}^+$ defined by $\rho(x,y) = 2^{-f(x-y)}$ for $x \neq y, \rho(x,x) = 0$, is a metric. The completion of K with respect to this metric is again a field. Two absolute values f, g are called equivalent if they induce the same topology on K. As examples, wih $K = \mathbb{Q}$, we have the usual absolute value and the p-adic absolute value v defined as in the previous slide, taking $M = (p)$. An absolute value is called trivial if it induces the discrete topology on K.

The completions of $\mathbb{Q}$ with respect to each of these absolute values are $\mathbb{R}$ and $\mathbb{Q}_p$, respectively; note that the usual (Euclidean) topology on $\mathbb{Q}$ is *not* induced from any I-adic topology on $\mathbb{Z}$ since it is not defined by neighborhoods that are cosets of subgroups. A remarkable result called Ostrowski's theorem asserts that the only nontrivial absolute values up to equivalence on $\mathbb{Q}$ are the ones given above. The completions $\mathbb{R}$ and $\mathbb{Q}_p$ are called places of $\mathbb{Q}$; sometimes $\mathbb{R}$ is denoted by $\mathbb{Q}_\infty$ in this context.

The rings $\mathbb{Z}_p$ and $\mathbb{Q}_p$ of p-adic integers and rationals play a crucial role (as one might expect) in number theory. For example, the famous Hasse principle attempts to decide whether a polynomial equation with rational coefficients, possibly with several variables, has a solution in $\mathbb{Q}^n$ if it has one in both $\mathbb{R}^n$ and $\mathbb{Q}_p^n$ for all p.