Lecture 5-9: Hensel's Lemma and the Cohen Structure Theorem

May 9, 2025

Having established the basic properties of completions, I turn to their major computational application, namely Hensel's Lemma (stated last quarter). I am following the treatment in Chapter 7 of Eisenbud's book "Commutative Algebra with a View to Algebraic Geometry".

Hensel's Lemma

Let R be a ring complete with respect to an ideal I. Let $F(x) \in R[x]$ be a monic polynomial and let $f(x)$ be its reduction mod I (in $(R/I)[x]$. If f factors in $(R/I)[x]$as $g_1 g_2$ with g_1, g_2 coprime polynomials and g_1 monic, then there is a unique factorization $F = G_1 G_2 \in R[x]$ with G_1 monic and G_i reducing to g_i mod I.

The proof will require a lemma. Let S be a commutative ring and $g_1, g_2 \in S[x]$ with g_1 monic of degree d and g_1, g_2 coprime in $S[x]$.

Lemma

In this situation, if $h \in S[x]$ is any polynomial then there is a unique combination $h = h_1 g_1 + h_2 g_2$ with $h_1, h_2 \in S[x]$ and $\deg h_2 < d$. Moreover, if $S = R/I$ for some ring R and ideal I contained in its Jacobson radical, if $G_1, G_2 \in R[x]$ reduce to g_1, g_2, and G_1 is monic, then G_1, G_2 are coprime in $R[x]$.

We first write $h = h_1' g_1 + h_2' g_2$ for $h_1', h_2' \in S[x]$, since g_1, g_2 are coprime. We then write $h_2' = q g_1 + h_2$ with $\deg h_2 < d$; this is possible since g_1 is monic. Then $h = (h_1' + q g_2) h g_1 + h_2 g_2 = (h_1' + q g_2) g_1 + (h_2' - q g_1) g_2$ expresses h in the desired form. If also $h = f_1 g_1 + f_2 g_2$, then g_1 divides $(f_2 - h_2) g_2$, forcing g_1 to divide $f_2 - h_2$ since g_1, g_2 are coprime. This implies $f_2 = h_2, f_1 = h_1$ by the degree condition on $f_2 - h_2$. To prove the second assertion, we must show that G_2 generates $R[x]/(G_1)$; since G_1 is monic, $R[x]/(G_1)$ is finitely generated. Then the result follows from Nakayama's Lemma.

Proof.

Begin by choosing any polynomials $G_1', G_2' \in R[x]$ with G_1 monic and G_i' reducing to g_i. Then write $F - G_1'G_2' \in I[x]$ by the lemma as $G_1'H_1 + G_2'H_2$ with $H_i \in R[x]$, $\deg H_2 < \deg G_1'$; we are using that I lies in Jacobson radical of $R = \hat{R}$. Setting $G_1'' = G_1' + H_2, G_2'' = G_2 + H_1$, we have $F - G_1''G_2'' = -H_1H_2$ and $H_i \in I[x]$ by the uniqueness assertion in the lemma. Then $F - G_1''G_2'' \in I^2[x]$; iterating the above step, we find $G_1^{(3)}, G_2^{(3)}$ reducing to g_1, g_2 with $F - G_1^{(3)}G_2^{(3)} \in I^3[x]$. Iterating, we get a sequences of polynomials $G_1^{(i)}, G_2^{(i)}$ which converge in $R[x]$ to polynomials G_1, G_2 of the desired form. Uniqueness follows from the uniqueness assertion in the lemma, which shows that G_1, G_2 are uniquely determined mod $I^n[x]$ for all n, so are unique. □

In particular, if p is prime, then any polynomial over $\mathbb{Z}/p\mathbb{Z}$ with distinct roots in its splitting field has a full complement of roots in the p-adic integers $\mathbb{Z}_p$. Also if $f(t, x)$ is a polynomial in two variables over a field k and $x = a$ is a simple root of $f(0, x)$, then there is a unique power series $x(t)$ with $x(0) = a$ such that $f(t, x(t)) = 0$; the implicit equation $f(x, t) = 0$ is solved by the explicit power series.

Next I extend a well-known property of polynomial rings (namely that any map from a finite set $\{x_1, \ldots, x_n\}$ to a K-algebra A extends uniquely to a K-algebra homomorphism from the polynomial ring $K[x_1, \ldots, x_n]$ to A) to power series rings mapping into complete ones.

Theorem

Let R be a ring and S an R-algebra complete with respect to an ideal I. Given $f_1, \ldots, f_n \in I$ we have

1. There is a unique R-algebra homomorphism ϕ from the power series ring $R[[x_1, \ldots, x_n]]$ to S mapping x_i to f_i and taking convergent sequences to convergent sequences. It is continuous in the adic topologies on $R[[x_1, \ldots, x_n]]$ and S,
2. If the induced map $R \to S/I$ is onto and $f_1, \ldots, f_n$ generate I, then ϕ is onto.
3. If the induced map $G(\phi)$ of graded rings from $R[x_1, \ldots, x_n]$ to $G(S)$ is one-to-one, then so is ϕ.

Proof.

The unique R-algebra map from $R[x_1, \ldots, x_n]$ to S/I^ℓ sending x_i to the image of f_i induces a map from $R[x_1, \ldots, x_n]/(x_1, \ldots, x_n)^\ell$ to S/I^ℓ and this induces a unique map from $R[[x_1, \ldots, x_n]]$ to S/I^ℓ sending x_i to the image of f_i. Since S is the inverse limit of the S/I^ℓ, there is a unique map $\phi : R[[x_1, \ldots, x_n]] \to S$ sending x_i to f_i, as required. For the second assertion, since the f_i generate I, the map from $(x_1, \ldots, x_n)/(x_1, \ldots, x_n)^2$ to I/I^2 is a surjection, so the induced map $G(\phi)$ from $G(R)[x_1, \ldots, x_n] \cong R[x_1, \ldots, x_n]$ to $G(S)$ is also a surjection; here $G(R[x_1, \ldots, x_n]$ is graded with respect to the ideal $(x_1, \ldots, x_n)$ and $G(S)$ is graded with respect to I. Given nonzero $g \in S$ there is a largest i with $g \in I^i$, since $\cap I^i = 0$. Then there is a polynomial g_1 of degree i in the x_i mapping to the image of g in $I^i/I^{i+1} \subset G(S)$, so that $g_1 - \phi(f_1) \in I^{i+1}$. □

Proof.

Iterating this process, we get a sequence of elements $g_j \in (x_1, \ldots, x_n)^{i+j-1}$ such that $g = \sum_{j=1}^{\infty} \phi(g_j)$. Since g preserves infinite sums, this implies that $g = \phi(\sum_{j=1}^{\infty} g_j$ and the second assertion follows. Finally, for the third assertion, if $g \in R[[x_1, \ldots, x_n]]$ is a nonzero power series with homogeneous term g_1 of lowest degree d, then $G(\phi)(g_1) \neq 0$ in the degree d part of $G(S)$. But then $g \equiv g_1 \mod (x_1, \ldots, x_n)^{d+1}$ and $\phi(g) \equiv G(\phi)(g_1) \mod I^{d+1}$, whence $\phi(g) \neq 0$ as well. □

Now I can state and prove the Cohen Structure Theorem, which severely constrains the structure of complete local Noetherian rings containing copies of their residue fields.

Theorem

Let R be a complete local Noetherian ring with maximal ideal M and residue field $K \cong R/M$. If R contains a copy of K mapping onto the residue field, then $R \cong K[[x_1, \ldots, x_n]]/I$ for some n and ideal I of $K[[x_1, \ldots, x_n]]$.

I previously showed that a Noetherian regular local ring R with maximal ideal M is such that its graded ring $G(R)$ with respect to M is a polynomial ring over the residue field $K = R/M$: to a first approximation, any two Noetherian local rings with the same residue field and the same dimension look the same. This result says that completions of Noetherian local rings containing a copy of their residue fields (called a coefficient field) have a similar rigid behavior. It can be shown that in fact R always contains a coefficient field. Next time I will show that quotients of power series rings have a rather restricted structure.

Proof.

Choosing a coefficient field K for R and a set of generators $a_1, \ldots, a_n$ for its maximal ideal, this follows at once from the previous theorem. □

There is also a more general version of Hensel's Lemma that applies to polynomials that are not given as products of coprime polynomials. It applies to any complete ring, Noetherian or not. To state it I first need a simple consequence of the above theorem about extending maps to power series rings.

Lemma

Let R be any ring, $f \in xR[[x]]$ a power series over R. If ϕ is the map from $R[[x]]$ to itself that is the identity on R and sends x to f, then ϕ is an isomorphism if and only if the derivative $f'(0)$ (defined in the obvious way) is a unit in R.

Proof.

If ϕ is an isomorphism, then the elements of $R[[x]]$ not in (x) are those with nonzero constant term and ϕ preserves this subset; since ϕ is an isomorphism we must have $\phi((x)) = (x)$. In particular the image $\phi(x) = f$ of the generator x of (x) also generates (x). Hence $f + (x^2)$ generates $(x)/(x^2)$. Since $f \equiv f'(0)x \mod x^2$, we see that $f'(0)$ is a unit in R. Conversely, if $f'(0) = u$ is a unit, then $G(R[[x]]) \cong R[x]$, where G is defined relative to the ideal (x),and $G(\phi) : R[x] \to R[x]$ is an isomorphisms because it sends x to ux. By the theorem, ϕ is injective and we can write $f = ux + hx^2$ for some $h \in R[[x]]$. Since $u + hx$ is a unit in $R[[x]]$, it follows that f generates (x), whence by the theorem again ϕ is surjective and thus an isomorphism. $\square$

Then we have

Generalized Hensel's Lemma

Let R be a ring complete with respect to an ideal I and let $f(x) \in R[x]$ be a polynomial. If $a \in R$ is an approximate root of f in the sense that $f(a) \equiv 0 \mod f'(a)^2 I$, then there is a root b of f near a in the sense that $f(b) = 0$ and $b \equiv a \mod f'(a)I$. If $f'(a)$ is not a zero divisor in R, then b is unique.

I will prove this next time.