Math 250A Lecture 18 Notes

Daniel Raban

October 26, 2017

1 Formal power series

1.1 Definition, inverse limit, and multiplicative inverses

Definition 1.1. Let R be a ring. The ring of *Formal power series*, $R[\![x]\!]$, is the ring of series of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots$$

with $a_i \in R$.

When we say "formal," we mean that we don't care about convergence. So these usually do not define a function.

Example 1.1. Consider the formal power series in $\mathbb{C}[\![x]\!]$

$$1 + 1!x + 2!x^2 + 3!x^3 + \cdots .$$

This only converges for $x = 0$.

$R[\![x]\!]$ is the inverse limit of the rings $R[x]/(x^n)$, the polynomial rings truncated at degree n. The homomorphism $R[x]/(x^n) \to R[x]/(x^{n-1})$ just removes the x^n term. We also say that $R[\![x]\!]$ is the *completion* of R at the ideal (x). More generally, we can take $\varprojlim R/I^n$ for any ideal I.

Example 1.2. The map $R \to \varprojlim R/I^n$ need not be injective. Let

$$R = \mathbb{C}[x^{1/n}, \text{all } n > 0],$$

$$I = (x^{1/2}, x^{1/3}, x^{1/4}, \dots).$$

So $R/I^n = R/I = \mathbb{C}$ for all n, which makes $\varprojlim R/I^n = \mathbb{C}$.

We also consider $R[\![x_1, x_2, \dots, x_n]\!]$, the ring of formal power series in n variables. This is just the ring defined recursively as $R[\![x_1, \dots, x_{n-1}]\!][\![x_n]\!]$.

Proposition 1.1. *Let $K[\![x]\!]$ be a field. Suppose that $f(x) = a_0 + a_1 x + \cdots$ with $a_0 \neq 0$. Then f has an inverse.*

Proof. Put $a_0 = 1$ for simplicity. Then $f(x) = 1 + g(x)$, where $g(x) = a_1 x + a_2 x^2 + \cdots$. Then

$$1/f = 1/(1+g) = 1 - g + g^2 - g^3 + \cdots,$$

which makes sense because the coefficient of x^n is a finite sum for every n. □

Example 1.3. Let $f = 1 + x + x^2$. The inverse is $1 - x + x^3 - x^4$.

1.2 Ideals of $R[\![x]\!]$

Proposition 1.2. *The only ideals of $K[\![x]\!]$ are (0), (1), and (n) for $n \geq 1$.*

Proof. Any element $a_n x^n + a_{n+1} x^{n+1} = x^n(a_n + a_{n+1}x + \cdots) = x^n u$ for a unit u. □

Corollary 1.1. *$K[\![x]\!]$ is a PID, and a UFD.*

What about $K[\![x, y]\!]$? This is not a principal ideal domain because it has the nonprincipal ideal (x, y). However, we have the following result.

Theorem 1.1. *If R is Noetherian, so is $R[\![x]\!]$.*

Proof. This is similar to the proof for polynomials. Let I be an ideal. Let I_n be the ideal of the coefficients of x^n in series with smallest term x^n. Then $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$. This stabilizes because R is Noetherian. Each of these is finitely generated, so I is finitely generated. □

Corollary 1.2. *If R is Noetherian, so is $R[\![x_1, \ldots, x_n]\!]$.*

Proof. Induct on n. □

1.3 Unique factorization

Recall that $K[x_1, \ldots, x_n]$ is a UFD. We want to prove the corresponding fact for formal power series. But this is not as straightforward to prove.

A bad attempt would be to try to show that if R is a UFD, so is $R[x]$; this is not true in general.[1]

If we try to copy the proof for $R[x]$, we need to define the content of a formal power series. But this need not exist.

Example 1.4. Let $R = Z$ and $f = 1 + x/p + x^2/p^2 + x^3/p^3 + \cdots$, where p is prime. Then the content would have to be $p^{-\infty}$ times something.

[1] Lang made this mistake in a previous version of the book. According to Professor Borcherds, there are many papers that point out various errors in Lang's book.

The following theorem lets us reduce formal power series proofs to polynomial proofs. We treat the $n = 2$ case, but the proof for n variables is similar but with more bookkeeping.

Theorem 1.2 (Weierstrass preparation)**.** *Suppose $f \in K[\![x, y]\!]$, were K is a field. Then $f = ug$, where u is a unit, g is a polynomial in y with coefficients in $K[\![x]\!]$, and the leading coefficient is a power of x.*

Proof. Pick the monomial $x^m y^n$ so that $a_{m,n} \neq 0$ and if $a_{b,c} = 0$, then $b < m$, or $b = m$ and $b < n$; this is the same as saying that (m, n) is least in the lexicographic ordering on the degrees of polynomials with nonzero coefficients.

$$\begin{array}{ccccc} \vdots & \vdots & \vdots & \vdots & \\ 0 & a_{1,0} & a_{2,0} & a_{3,0} & \cdots \\ 0 & a_{1,3} & a_{2,3} & a_{3,3} & \cdots \\ 0 & \boxed{a_{1,2}} & a_{2,2} & a_{3,2} & \cdots \\ 0 & 0 & a_{2,1} & a_{3,1} & \cdots \\ 0 & 0 & a_{2,0} & a_{3,0} & \cdots \end{array}$$

By multiplying by units, $1 + cx^i y^j$, we can make the coefficients of every term $x^m y^k$ zero for $k > n$; we can do this infinitely many times because the infinite product just defines a power series.

$$\begin{array}{ccccc} \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & * & * & \cdots \\ 0 & 0 & * & * & \cdots \\ 0 & a_{1,2} & * & * & \cdots \\ 0 & 0 & * & * & \cdots \\ 0 & 0 & * & * & \cdots \end{array}$$

We can then kill all the coefficients $x^{m+1} y^k$ with $k \geq 1$. Similarly, kill off the other coefficients of $x^\ell y^k$ with $k \geq m$.

$$\begin{array}{ccccc} \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ 0 & a_{1,2} & 0 & 0 & \cdots \\ 0 & 0 & * & * & \cdots \\ 0 & 0 & * & * & \cdots \end{array}$$

So f is a unit times $x^m y^n + \sum b_{i,j} x^i y^j$ with $i \geq m + 1$ and $j \leq m$. Note that we have to kill all the coefficients in this order; if you kill $x^i y^j$ before you kill $x^{i-k} y^{j-\ell}$, when you kill $x^{i-k} y^{j-\ell}$, you might make $x^i y^j$ nonzero. □

It turns out that the Weierstrass preparation theorem is what we needed.

Theorem 1.3. *$K[\![x_1, \ldots, x_n]\!]$ is a UFD.*

Proof. We will treat the case of $n = 2$, $R[\![x, y]\!]$. We first show that every element has a factorization into irreducibles. The proof we gave for $R[x]$ works for any Noetherian ring, and $R[\![x]\!]$ is Noetherian.

To prove uniqueness, the key step is to show that irreducible elements are prime. Irreducible means that $g \neq gh$ with g, h not units, and prime means that if f divides gh, then f divides g or h. This follows from the Weierstrass preparation theorem. Suppose that f divides gh; we can assume f, g, h are polynomials in y with coefficients in $K[\![x]\!]$. By induction, $K[\![x]\!]$ is a UFD, so $K[\![x]\!][y]$ is a UFD since it is a polynomial ring over a UFD. So f divides g or h in $K[\![x]\!][y]$ and hence in $K[\![x]\!][\![y]\!]$. □

Example 1.5. Let $f(x, y) = y^2 - x^2 - x^3$. This is irreducible as a polynomial in $K[x, y]$, but it is not irreducible as a power series in $K[\![x, y]\!]$.

$$y^2 - x^2 - x^3 = (y + x\sqrt{1+x})(y - x\sqrt{1+x}),$$

where $\sqrt{1+x}$ is the formal power series

$$\sqrt{1+x} = 1 + \frac{1}{2}x + \frac{\frac{1}{2} \cdot \frac{-1}{2}}{2!}x^2 + \cdots .$$

Geometrically, the curve $y^2 = x^2 - x^3$ only has 1 component. Near 0, the curve looks reducible, however, because it looks like two intersecting curves, $y = x\sqrt{1+x}$ and $y = -x\sqrt{1+x}$. So this polynomial is reducible in $K[\![x, y]\!]$ iff the curve $y^2 - x^2 = x^3 = 0$ has two branches near $x = y = 0$ (the point where the ideal (x, y) vanishes).

1.4 Hensel's lemma

Lemma 1.1 (Hensel)**.** *Suppose $f(x, y) \in K[\![x, y]\!]$, and suppose the smallest nonzero coefficients are of degree d and form a polynomial $f_d(x, y)$. Suppose that $f_d(x, y) = g(x, y)h(x, y)$ with g, h coprime. Then $f(x, y) = G(x, y)H(x, y)$, where g and h are the smallest degree terms of G and H, respectively.*

We will not prove this. Instead, here are some examples.

Example 1.6. Let $f(x) = y^2 - x^2 - x^3$. Then $d - 2$ and $f_2 = y^2 - x^2$. So

$$fy^2 - x^2 = (y - x)(y + x),$$

which lifts to

$$y^2 - x^2 - x^3 = (y - x\sqrt{1+x})(y - x\sqrt{1+x}) = (y - x + \cdots)(y + x + \cdots).$$

Example 1.7. Let $f(x) = y^2 - x^3$. Then $d = 2$ and $f_d = y^2 = y \cdot y$. However, $y^2 - x^3$ does not factorize! This is because x^3 has no square root as a formal power series. Geometrically, $y^2 - x^3 = 0$ looks like a cusp, so we don't get two different curves around 0.

Here is an analogue of Hensel's lemma in number theory.

Lemma 1.2 (Hensel (number theory version))**.** *Suppose $f(x) = (x-a)g(x)$, and $f(x) = 0$ around p, where $f \in \mathbb{Z}[x]$. If $f'(x) \neq 0 \pmod{p}$ has a root in $\mathbb{Z}_p$ ($f(x) \equiv 0 \mod p^n$ for all $n \geq 1$).*

Example 1.8. Let $f(x) = x^2 = 7$ and $p = 3$. Then $f(1) = 1^2 - 7 \equiv 0 \pmod{3}$, and $f'(1) = 2 \not\equiv 0 \pmod{3}$. So $x^2 - 6 \equiv 0 \pmod{p}^n$ has a root for all $n \geq$. We get

$$x^2 - 7 = (x - \sqrt{7})(x + \sqrt{7})$$

Example 1.9. Let $f(x) = x^2 - 7$ and $p = 2$. $f(1) \equiv 0 \pmod{2}$, and $x^2 - 7$ has no roots $\pmod{2}^3 = 8$. And $f'(1) = 2 \equiv 0 \pmod{2}$.