250B: Commutative Algebra
For the Morbidly Curious

Nir Elber

Spring 2022

Contents

Theme 1
Working in Chains

But this is like trying to scale a glacier. It's hard to get your footing, and your fingertips get all red and frozen and torn up.

—Anne Lamott

1.1 March 10

We continue discussing completion.

1.1.1 Completion for Modules

Recall that we had a notion of completion for modules as follows.

Definition 1.1 (Completion, modules)**.** Fix R a ring and M a module with a filtration $\mathcal{J}$ given by

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots.$$

Then we define the *completion* as the inverse limit $\varprojlim M/M_i$.

Here is our primary example.

Example 1.2. If we fix an ideal $I \subseteq R$, then we are granted an I-adic filtration of M, which gives the I-adic completion of M. In particular, this is an $\widehat{R}_I$-module.

Here is a nice lemma.

Lemma 1.3. Suppose we have two filtrations of an R-module M given by $\mathcal{J}$

$$M \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

and $\mathcal{J}'$ given by

$$M \supseteq M_1' \supseteq M_2' \supseteq \cdots .$$

Further, suppose that, for all i, there exists j such that $M_i \supseteq M_j'$ and perhaps another j such that $M_i' \supseteq M_j'$. Then we have an isomorphism

$$\varprojlim M/M_i \cong \varprojlim M/M_i'$$

Remark 1.4. Of course, any subsequence of a filtration $\mathcal{J}$ will give rises to the same inverse limit. Intuitively, this is fairly clear because any given term in the inverse limit is just some sequence where earlier terms are fixed by later ones, so we can just build the isomorphism explicitly.

Proof. In general, if we have two inverse limits, the way to define an inverse limit is to define a map into each of the components. To manifest this idea, we pick up strictly increasing $\alpha, \beta, \gamma : \mathbb{N} \to \mathbb{N}$ such that

$$M_j \supseteq N_{\alpha(j)} \supseteq M_{\beta(j)} \supseteq N_{\gamma(j)}. \tag{$*$}$$

These embeddings give us surjections

$$M/N_{\gamma(j)} \twoheadrightarrow M/M_{\beta(j)} \twoheadrightarrow M/M_{\alpha(j)} \twoheadrightarrow M/M_j.$$

This gives rise to morphisms

$$\varprojlim M/N_{\gamma(j)} \to \varprojlim M/M_{\beta(j)} \to \varprojlim M/M_{\alpha(j)} \to \varprojlim M/M_j.$$

Now, these are subsequences, so the terms are isomorphic to the terms without the injective functions, so we get morphisms

$$\varprojlim M/N_j \to \varprojlim M/M_j \to \varprojlim M/M_j \to \varprojlim M/M_j.$$

We can check by hand that the composite of any consecutive map is the identity by tracking through $(*)$ on the inclusions $M_j \subseteq M_{\beta(j)}$ and $N_{\alpha(j)} \subseteq N_{\gamma(j)}$. This provides us with our isomorphisms. ∎

Here is another lemma which we will want for abstract nonsense reasons.

Lemma 1.5. Fix R a Noetherian ring and an ideal I. Further, suppose that we have a short exact sequence

$$0 \to A \to B \to C \to 0$$

of finitely generated R-modules. Then we have a short exact sequence

$$0 \to \widehat{A} \to \widehat{B} \to \widehat{C} \to 0$$

of completions.

Proof. We start with the short exact sequence

$$0 \to A \to B \to C \to 0$$

and tensor by $- \otimes R/I^s$ to get a right-exact sequence

$$A/I^s A \to B/I^s B \to C/I^S C \to 0.$$

We can show by hand that this gives us a surjection $\widehat{B} \twoheadrightarrow \widehat{C}$, but we need this to be exact on the left. Well, the next best thing that we can write down is

$$0 \to \frac{A}{A \cap I^s B} \to \frac{B}{I^s B} \to \frac{C}{I^s C},$$

so because taking inverse limits is left exact, we have a left-exact sequence

$$0 \to \varprojlim \frac{A}{A \cap I^s B} \to \varprojlim \frac{B}{I^s B} \to \varprojlim \frac{C}{I^s B}.$$

It remains to show that our left term is $\widehat{A}$. Well, by the Artin–Rees lemma (!), we see that the filtration

$$A \cap I^s B$$

is an I-stable filtration. In other words, there is an n such that $I^k(A \cap I^n B) = A \cap I^{n+k} B \subseteq I^k A$ for sufficiently large k. Applying Lemma 1.3 finishes. ∎

The point of this is that we see completion is an exact functor. In fact, as with localization, there is a flat module hiding in the background.

Theorem 1.6. Fix R a Noetherian ring with an ideal $I \subseteq R$ and M a finitely generated R-module.

(a) We have that $\widehat{M_I} \cong \widehat{R}_I \otimes_R M$, and this isomorphism is natural in M.

(b) We have that $\widehat{R}_I$ is a flat R-module.

Proof. So we show (a). If $M \cong R$, then we are done. Because tensoring and completion commutes with taking direct sums, we see that (a) remains true for $M \cong R^n$ for $n \in \mathbb{N}$. Otherwise, because we live in a Noetherian world, M is finitely presented, so we have a right-exact sequence

$$G \to F \to M \to 0$$

where F and G are both free of finite rank. Tensoring with $\widehat{R}_I$, we see that

$$G \otimes_R \widehat{R}_I \to G \otimes_R \widehat{R}_I \to M \otimes_R \widehat{R} \to 0.$$

We also have the short exact sequence

$$\widehat{G}_I \to \widehat{F}_I \to \widehat{M_I} \to 0,$$

so we slap them on top of each other to build the following diagram.

$$\begin{array}{ccccccc} G \otimes_R \widehat{R}_I & \longrightarrow & F \otimes_R \widehat{R}_I & \longrightarrow & M \otimes_R \widehat{R}_I & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ \widehat{G}_I & \longrightarrow & \widehat{F}_I & \longrightarrow & \widehat{M_I} & \longrightarrow & 0 \end{array}$$

In particular, the two left maps are isomorphisms, so the right map is also an isomorphism by the Snake lemma.

We now show (b). We would like to use the previous lemma, but it only works for finitely generated modules instead of general short exact sequences. But have no fear—it suffices to show that the natural inclusion

$$J \otimes_R \widehat{R}_I \to \widehat{R}_I$$

is an inclusion for any finitely generated J by our flatness criterion, which we do have, so we are done. ∎

1.1.2 Examples of Hensel's Lemma

Let's continue talking about number theory. Hensel's lemma is a way to lift solutions to polynomial equations from quotients up to complete rings. More precisely, we have the following.

Theorem 1.7 (Hensel's lemma)**.** Suppose that R is a ring complete with respect to an I-adic filtration, and pick up a polynomial $f(x) \in R[x]$. Now, suppose we have $a \in R$ such that

$$f(a) \equiv 0 \pmod{f'(a)^2 m}.$$

Then there exists $b \in R$ such that $b \equiv a \pmod{f'(a)m}$ and $f(b) = 0$.

We do a few examples before proving the lemma.

Exercise 1.8. We solve $x^2 = 1 + t$ in $R[[t]]$, where $k[[t]]$ is complete with respect to (t).

Proof. Note that $x_0 = 1$ is a solution in $R/(t)$. So we hope that we can find a solution $u \in k[[t]]$ such that $u \equiv 1 \pmod{t}$ such that $u^2 = 1 + t$. Well, from the general binomial theorem, we can write

$$\sqrt{1+t} = \sum_{k=0}^{\infty} \binom{1/2}{k} t^k.$$

We can check that this works. ∎

Exercise 1.9. Fix $a \in \mathbb{Z}_p$ for an odd prime p. We discuss when we can solve $x^2 \equiv a$.

Proof. If $a = 0$, then we are done. Otherwise, write $a = bp^n$ where $b \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. If n is odd, there is no solution; so we let $n = 2k$ and write

$$\left(x/p^k\right)^2 = b,$$

so we are solving $y^2 = b$, where $b \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Now, if a solution is to exist, then we require $b \pmod{p}$ to be a perfect square, so find $x_0 \in \mathbb{F}_p$ such that

$$x_0^2 \equiv b \pmod{p}.$$

To check that we can lift by Hensel's lemma, we need to check the derivative, but when p is odd, then our derivative is $2x_0$, which is nonzero because x_0 is nonzero.

Let's actually show how we can solve this. Well, expand out x in a p-adic series as

$$\left(\sum_{k=0}^{\infty} x_k p^k\right)^2 = b =: \sum_{k=0}^{\infty} b_k p^k.$$

We already have x_0. For x_1, we check the linear term to find

$$2x_0 x_1 \equiv b_1 \pmod{p},$$

from which we extract b_1. More generally, this term reads as

$$x_0 x_n + \sum_{k=1}^{n} x_k x_{n-k} = b_n,$$

from which we can solve for x_n recursively. ∎

Exercise 1.10. We show that $x^2 = b$ has a solution in $\mathbb{Z}_2$ if b is an odd perfect square $\pmod 8$. In other words, we require $b \equiv 1 \pmod 8$.

Proof. Simply use Hensel's lemma, but now $f'(a)^2 \cdot 2$ is divisible by a factor of 8. ∎

1.1.3 Proof of Hensel's Lemma

With sufficient motivation, we now turn to a proof of Theorem 1.7. We have the following universal property.

Proposition 1.11. Fix S an R-algebra such that S is complete with respect to an ideal $I \subseteq S$. If $I = (f_1, \dots, f_n)$ is finitely generated, then there is a unique homomorphism

$$\varphi : R[[x_1, \dots, x_n]] \to S$$

such that $x_\bullet \mapsto f_\bullet$, and φ is continuous under the induced I-adic topology. In fact, the following hold.

- If $R \to S/I$ is surjective, then φ is surjective.
- If the induced map $R[x_1, \dots, x_n] \to \operatorname{gr}_I S$, then φ is injective.

Remark 1.12. This is intended to be an analog for the universal property of polynomial algebras.

Proof. To construct φ, it suffices to note that $R[[x_1, \dots, x_n]]$ is the completion of $R[x_1, \dots, x_n]$ with respect to the ideal $\mathfrak{m} = (x_1, \dots, x_n)$ and then construct a system of maps

$$\varphi_k : \frac{R[x_1, \dots, x_n]}{\mathfrak{m}^k} \to \frac{S}{I^k}.$$

Alternatively, we can note that the restricted map on $R[x_1, \dots, x_n] \to S$ is forced and use continuity to fill in for the rest of $R[[x_1, \dots, x_n]]$.

For the surjectivity check, we note that we can lift to

$$\varphi_k : \frac{R[x_1, \dots, x_n]}{\mathfrak{m}^k} \to \frac{S}{I^k}$$

is surjective, so going to the completion provides the result.

Lastly, we note that the condition tells us that

$$\bigcap_i I^i = 0 \implies \bigcap \mathfrak{m}^i = 0.$$

To finish our injectivity check, we note more generally that if $\varphi : A \to B$ is a map of filtered algebras, then we can build an associated map $\operatorname{gr} \varphi : \operatorname{gr} A \to \operatorname{gr} B$. Then if $\operatorname{gr} \varphi$ is injective (as seen above), then φ is also injective. This gives the result after some care. ∎

Corollary 1.13. Fix $\varphi : R[[x]] \to R[[x]]$ some morphism. Further, find $f \in (x)$ such that $f \equiv x \pmod{x^2}$. Then if $\varphi(x) = f$ and $\varphi(r) = r$ for $r \in R$, then φ is an isomorphism.

Proof. Use the previous lemma to construct φ and then run the previous surjectivity and injectivity check. ∎

Remark 1.14. In fact, there is an explicit inverse map for this φ.

We are now ready to prove Theorem 1.7.

Proof of Theorem 1.7. We use Newton's lemma to build our solution b. For ease of mind, we set $e := f'(a)$ so that we know

$$f(a) \equiv 0 \pmod{e^2 m}.$$

Now, we can write $f(a+ex)$, which upon expansion via the binomial theorem looks like

$$f(a+ex) = f(a) + f'(a)ex + h(x)(ex)^2$$

for some $h \in R[x]$. Using $f'(a) = e$, we get

$$f(a+ex) = f(a) + e^2\left(x + x^2 h(x)\right).$$

Now, consider the homomorphism $\varphi : R[[x]] \to R[[x]]$ by $\varphi(x) := x + x^2 h(x)$, but the previous corollary tells us that φ is an isomorphism! So we see

$$f\left(a + e\varphi^{-1}(x)\right) = f(a) + e^2 x$$

by plugging in. To finish, we build $\psi : R[[x]] \to R$ by $\psi(x) = -c$, where $f(a) = e^2 c$ and can compute that

$$f\left(a + e\psi\varphi^{-1}(x)\right) = f(a) - e^2 c = 0,$$

which finishes. ∎

Remark 1.15. We can show that the solution above is unique, provided that $f'(a)$ is not a zero-divisor. We will omit this proof.

List of Definitions