Completions and Hensel's lemma

Notes on the last two weeks of Commutative Algebra

Daniel Koizumi

November 24, 2021

1 November 11

Today we will examine limits and colimits, with the eventual goal being to show that the dimension of $k[\![x_1, \ldots, x_n]\!]$ is n.

Let I be a **directed set**. In particular, there is a partial order on I, denote it $\leq$. Directed sets required that, given any $i, j \in I$, there exists k such that $i \leq k$, $j \leq k$.

$$\begin{tikzcd}
i \arrow[dr] & \\
& k \\
j \arrow[ur] &
\end{tikzcd}$$

Definition 1. Let A be a ring, and I be a directed set. A **colimit system** (in A-modules) is a family of A-modules

$$\{M_i\}_{i \in I}$$

with a functor from I to A-mod by $\mathcal{F}(i) = M_i$.

We talk of maps between colimit systems as natural transformations of the corresponding functors.

$$\begin{tikzcd}
M_i \arrow[r] \arrow[d, "\tau(i)"'] & M_j \arrow[d, "\tau(j)"'] \\
N_i \arrow[r] & N_j
\end{tikzcd}$$

Given such a system, the **colimit** is a module M with maps $M_i \to M$ that are compatible with the system. In other words, they satisfy

$$\begin{tikzcd}
M_i \arrow[rr] \arrow[dr] & & M_j \arrow[dl] \\
& M &
\end{tikzcd}$$

and M is universal with the property. In other words, given any other compatible family $M_i \to N$, there exists a unique map $M \to N$ such that the composition

$$M_i \to M \to N$$

is the map $M_i \to N$ from the family. For any A-module M, there is a constant diagram, where we take $cM_i = M$ for all i and $cM_i \to cM_j$ is the identity for all $i \leq j$.

$$\begin{tikzcd} M_\bullet \arrow[rr] \arrow[dr] & & cM \arrow[dl, dashed] \\ & cN & \end{tikzcd}$$

In the category A-mod for any ring A, the colimit exists and is unique up to isomorphism. To prove existence, consider

$$\bigoplus_{i \in I} M_i$$

identify M_i as a submodule of $\bigoplus_{i \in I} M_i$. Consider the A-submodule generated by

$$W = \left(x_i - f_{ij}(x_i) \mid x_i \in M_i, M_i \xrightarrow{f_{ij}} M_j \right)$$

The $\bigoplus M_i / W$ is the colimit. We have the structure maps

$$M_i \hookrightarrow \bigoplus M_i \twoheadrightarrow \frac{\bigoplus M_i}{W}$$

Check that this is compatible with $\{M_i\}$. It satisfies the universal property because the direct sum does.

Notation: We write $\mathrm{Colim}_{i \in I} M_i$ for the colimit of $\{M_i\}$.

Exercise

If $M_i \subset U$ for some A-module U, and $M_i \to M_j$ are the inclusions, the colimit should be the union. Check

$$\mathrm{Colim}_{i \in I} M_i = \bigcup_{i \in I} M_i$$

Can construct $\mathbb{Q}$ from $\mathbb{Z}$ using colimits. More generally: $a \in A$, consider

$$A \xrightarrow{a} A \xrightarrow{a} A \xrightarrow{a} \dots$$

indexed by $\mathbb{N}$.

Exercise

What is the colimit of the above? Use this to create localizations as colimits? Also think about what happens when a is nilpotent.

Definition 2. Limits Let I be a directed set. An **inverse/limit system** is a contravariant functor from I to A-mod. Or a functor $I^{op} \to A$-mod. We have a family $\{M_i\}$ of A-modules such that given $i \to j$ ($i \leq j$), we have a map $M_j \xrightarrow{f_{ji}} M_i$. The **limit** of such a system is an A-module M with maps $M \to M_i$ respecting the family with respect to composition. In other words the following diagram commutes:

$$\begin{tikzcd} M_i & & M_j \arrow[ll] \\ & M \arrow[ul] \arrow[ur] & \end{tikzcd}$$

That is universal with respect to this property. Given any other A-module N and maps $N \to M_i$, there is a unique map $N \to M$ such that the composition

$$N \to M \to M_i$$

is the map $N \to M_i$.

$$\begin{tikzcd} cM & & cN \arrow[ll, dashed, "\exists!"] \\ & M_\bullet \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Theorem 1. The limit exists and is unique up to isomorphism.

Proof. Uniqueness is from the universal property. We show existence: given system $\{M_i\}$, whenever $i \leq j$, we have a map $M_i \to M_j$. Consider

$$\prod_{i \in I} M_i$$

and consider the submodule of compatible sequences

$$Z = \{(a_i)_{i \in I} \mid f_{ji}(a_j) = a_i \forall f_{ji}\}$$

We have

$$Z \hookrightarrow \prod M_i \twoheadrightarrow M_i$$

$$\begin{tikzcd} M_i & & M_j \arrow[ll, "f_{ji}"] \\ & Z \arrow[ul] \arrow[ur] & \end{tikzcd}$$

commutes. Check that Z is the limit of $\{M_i\}$, and denote it $\lim\limits_{i} M_i$. ☐

Say $0 \to \{L_i\} \to \{M_i\} \to \{N_i\} \to 0$ is an exact sequence of inverse systems. In other words, the maps are morphisms of diagrams and at each level they are exact.

$$0 \to L_i \to M_i \to N_i \to 0$$

are exact for all i. This induces

$$0 \to \lim_i L_i \to \lim_i M_i \to \lim_i N_i$$

but the last map is not necessarily surjective. ie the functor by taking limits is left exact.

Focus on $I = \mathbb{N} = \{0, 1, 2, \dots\}$ with $n \leq n + 1$. An $\mathbb{N}$-induced inverse system is a family

$$\dots \to M_2 \xrightarrow{f_2} M_1 \xrightarrow{f_1} M_0$$

We look at $\prod_{i\geq 0} M_i \xrightarrow{\theta} \prod_{i\geq 0} M_i$ defined by

$$\theta[(x_i)_{i\in I}] = (x_i - f_{i+1}(x_{i+1}))_{i\in I}$$

We know $\theta = \mathrm{id} - f_\bullet$ where

$$f_\bullet : \prod M_i \to \prod M_i$$

induced by $M_i \to M_{i+1}$. The kernel of θ is $(x_i)_{i\in I}$ where

$$\ldots \to x_2 \to x_1 \to x_0$$

so $\ker\theta = \lim_i M_i$. We have

$$0 \to \lim M_i \to \prod_i M_i \xrightarrow{\theta} \prod M_i$$

The cokernel is denoted $\lim^1(M_i) = \mathrm{coker}\theta$.

Exercise

0 $\lim^1(M_i) = 0$ if $\{M_i\}$ is surjective, ie $M_{i+1} \twoheadrightarrow M_i$. This would go to show that taking limits by the below argument preserves the short exact sequence.

Now given an exact sequence

$$0 \to \{L_i\} \to \{M_i\} \to \{N_i\} \to 0$$

we will have

$$0 \to \prod L_i \to \prod M_i \to \prod N_i \to 0$$

so now we can apply the snake lemma to

$$\begin{tikzcd}
0 \arrow[r] & \prod L_i \arrow[r] \arrow[d, "\theta"] & \prod M_i \arrow[r] \arrow[d, "\theta"] & \prod N_i \arrow[r] \arrow[d, "\theta"] & 0 \\
0 \arrow[r] & \prod L_i \arrow[r] & \prod M_i \arrow[r] & \prod N_i \arrow[r] & 0
\end{tikzcd}$$

We have

$$0 \to \lim L_i \to \lim M_i \to \lim N_i \to \lim^1 L_i \to \lim^1 M_i \to \lim^1 N_i \to 0$$

Let A be a ring, M be an A-module with a topology such that addition and scalar multiplication are continuous maps

$$M \times M \to M$$

and

$$M \to M$$

respectively. This means the open neighborhoods are determined by the neighborhoods around 0. In other words, U is an open neighborhood of 0 if and only if $U + x$ is an open neighborhood of x for all $x \in M$.

We'll discuss completions with respect to the topology, Cauchy sequences, convergence, etc. We define completions using an inverse limit. M

2 November 16

- Let $\mathcal{G}$ be a topological group.
- The topology is determined by neighborhoods of the origin. If $U \supset 0$ then $\forall a \in \mathcal{G}$, $U + a$ is an open neighborhood of a.

- $\mathcal{G}$ is Hausdorff if and only if $\{0\}$ is closed.
- In general, $\overline{\{0\}} \subset \mathcal{G}$ is a subgroup and $\mathcal{G} \mid_{\overline{0}}$ is a Hausdorff topological group.

Hence $\mathcal{G}$ will be **first countable**. In other words it has a countable basis for the neighborhoods of 0.

Definition 3. A sequence (g_n) in $\mathcal{G}$ **converges** to 0 means that given an open neighborhood U of 0, there exists N such that for all $n \geq N$, $g_n \in U$.

A sequence (g_n) is Cauchy if for every neighborhood of 0, U, there exists N such that $i, j \geq N$ implies

$$g_i g_j^{-1} \in U$$

Example. Consider $\mathbb{Z}$ with the p-adic topology when p is prime. Neighborhoods of the origin are $U_n = (p^n)$.

$$\mathbb{Z} = U_0 = U_1 \supset U_2 \supset U_3 \supset \dots$$

say $g_n = 1 + p + \dots + p^n$. Then (g_n) is a Cauchy sequence but it does not converge in $\mathbb{Z}$.

Consider

$$\hat{\mathcal{G}} = \{(g_n) \mid \text{ where } (g_n) \text{ is a Cauchy sequence}\} / \sim$$

where $(g_n) \sim (h_n)$ if $(g_n - h_n) \to 0$.

Example. $\hat{\mathcal{G}}$ is also an abelian group with topology induced by the one on $\mathcal{G}$. For each U open about 0 consider the collection of equivalence classes

$$\left\{[(g_n)] \in \hat{\mathcal{G}} \mid g_n \in U \text{ for } n \gg 0\right\}$$

This should define a neighborhood of $\hat{\mathcal{G}}$.

Example. Considering $\mathbb{Z}$ with the p-adic topology. The completion in $\mathbb{Z}_p$ (p-adic integers). We can consider a map

$$\mathcal{G} \to \hat{\mathcal{G}}$$

defined by $g \mapsto [(g)]$. Check that this map is a group homomorphism. The kernel is $\overline{0}$ (note that it need to be $\{0\}$).

Now suppose $\mathcal{G}$ has a fundamental system of neighborhoods given by $\{\mathcal{G}_n\}$ where the $\mathcal{G}_n$ are subgroups. We can assume

$$\mathcal{G} \supset \mathcal{G}_1 \supset \mathcal{G}_2 \supset \dots$$

(Conversely, any such nested sequence of subgroups defines a topology on $\mathcal{G}$). Hence we can construct completions algebraically. We consider the inverse limit system

$$\dots \twoheadrightarrow \frac{\mathcal{G}}{\mathcal{G}_{n+1}} \twoheadrightarrow \frac{\mathcal{G}}{\mathcal{G}_n} \to \dots \to \frac{\mathcal{G}}{\mathcal{G}_1}$$

This is an inverse limit system.

Lemma 1. $\hat{\mathcal{G}} = \lim\limits_{n} \left(\frac{\mathcal{G}}{\mathcal{G}_n}\right)$.

Proof. By construction, $\lim\limits_{n} \left(\frac{\mathcal{G}}{\mathcal{G}_n}\right)$ consists of compatible sequences in

$$\prod_{n \geq 1} \left(\frac{\mathcal{G}}{\mathcal{G}_n}\right)$$

(i.e. sequences $(\hat{g_n})$ where $g_n \in \mathcal{G}$ such that

$$g_{n+1} - g_n \in \mathcal{G}_n$$

Then (g_n) is a Cauchy sequence. Conversely, any Cauchy sequence is equivalent to one such element. □

Corollary 1. Given a subgroup $\mathcal{H} \subset \mathcal{G}$, with the subspace topology given by the one on $\mathcal{G}$. The sequence

$$0 \to \mathcal{H} \to \mathcal{G} \to \frac{\mathcal{G}}{\mathcal{H}} \to 0$$

induces exact sequence

$$0 \to \hat{\mathcal{H}} \to \hat{\mathcal{G}} \to \left(\frac{\hat{\mathcal{G}}}{\mathcal{H}}\right) \to 0$$

Proof. The neighborhoods of $\mathcal{H}$ are $\{\mathcal{H} \cap \mathcal{G}_n\}_{n\geq 1}$. In $\mathcal{G}/\mathcal{H}$ this would be $\left\{\frac{(\mathcal{G}_n+\mathcal{H})}{\mathcal{H}}\right\}_{n\geq 1}$. We have

$$\begin{tikzcd}
0 \arrow[r] & \frac{\mathcal{H}}{\mathcal{H}\cap\mathcal{G}_n} \arrow[r] \arrow[d, two heads] & \frac{\mathcal{G}}{\mathcal{G}_{n+1}} \arrow[r] \arrow[d] & \frac{\mathcal{G}}{\mathcal{G}_{n+1}+\mathcal{H}} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \frac{\mathcal{H}}{\mathcal{H}\cap\mathcal{G}_n} \arrow[r] & \frac{\mathcal{G}}{\mathcal{G}_n} \arrow[r] & \frac{\mathcal{G}}{\mathcal{G}_n+\mathcal{H}} \arrow[r] & 0
\end{tikzcd}$$

. By last lecture, this means the system is surjective, so it induces exact

$$0 \to \hat{\mathcal{H}} \to \hat{\mathcal{G}} \to (\mathcal{G} \hat{/} \mathcal{H}) \to 0$$

□

If A is a commutative ring $I \subset A$ is an ideal, M is an A-module. A filtration $M \supset M_1 \supset M_2 \supset \dots$ by A-submodules is an I-filtration if

$$IM_n \subset M_{n+1}$$

It is ***I*-stable** if equality holds for $n \gg 0$.

Example. Take $M_i = M$ for all i, so this defines an I filtration that is not I-stable.

An example of an I-stable filtration is where you take $M_i = I^i M$ (called the ***I*-adic filtration**).

Suppose $N \subset M$ is a submodule. We would like to relate the I-adic filtration on N (defined by $\{I^n N\}$) with the induced filtration $\{N \cap I^n M\}$ by M on N.

Remark. Say (M_n) and (M'_n) are both I-stable filtrations on M. Then there exists N such that

$$M_{i+N} \subset M'_i \text{ and } M'_{i+N} \subset M_i$$

Exercise

Prove that the above claim. In other words, the filtrations above have bounded difference. This is a stronger statement than the idea that they have the same topology.

In particular, any I-stable filtration and (I^nM) have bounded difference.

Given $I \subset A$ an ideal. There is a construction called the **Rees ring**

$$\mathcal{R}_I(A) = \bigoplus_{n \geq 0} I^n$$

which is a graded A algebra. Given an I-filtration $\mathcal{M} = (M_n)$ on an A-module M, set

$$\mathcal{R}_{\mathcal{M}}(M) = \bigoplus_{n \geq 0} M_n$$

where $M_0 = M$. Because $\mathcal{M}$ is an I-filtration,

$$\mathcal{R}_{\mathcal{M}}(M)$$

is a graded $\mathcal{R}_I(A)$-module.

Proposition 1. Let A be a Noetherian ring. Consider an I-filtration $\mathcal{M} = (M_n)$. Then $\mathcal{M}$ is I-stable if and only if $\mathcal{R}_{\mathcal{M}}(M)$ is finitely generated.

Proof. For each n, consider the submodule $X(n)$ of $\mathcal{R}_{\mathcal{M}}(M)$ generated by

$$\bigoplus_{i=0}^{n} M_i$$

(this is not necessarily a submodule). We have

$$X(n) = M_0 \oplus M_1 \oplus \ldots \oplus M_n \oplus IM_n \oplus I^2M_n \oplus \ldots$$

We have an increasing filtration

$$X(n) \subset X(n+1) \subset X(n+2) \subset \ldots$$

Because $\mathcal{R}_{\mathcal{M}}(M)$ is Noetherian, there exists N such that

$$X(n) = X(N) \text{ for all } n \geq N$$

In other words, $X(n)$ is

$$\ldots \oplus M_N \oplus IM_N \oplus \ldots$$

which implies

$$I^{n-N}M_N = M_n \text{ for all } n \geq N$$

which implies that $\mathcal{M}$ is I-stable.

Now suppose $\mathcal{M}$ is I-stable. Since A is noetherian, $\mathcal{R}_I(A)$ is noetherian by Hilbert's basis theorem. Now if M is I-stable, then

$$\mathcal{R}_{\mathcal{M}}(M) = X(N)$$

for some N where the latter is finitely generated over $\mathcal{R}_I(A)$. $\square$

Theorem 2. (Artin-Rees) Consider a Noetherian ring A, $I \subset A$ ideal, and M a finitely generated A-module. Then for any submodule $N \subset M$, the filtrations (I^nN) and $(I^nM \cap N)$ have bounded differences.

Proof. It suffices to prove that $(I^n M \cap N)$ is I-stable. We look at

$$\mathcal{R}_I(M) = M \oplus IM \oplus I^2M \oplus \dots$$

and the $\mathcal{R}_I(A)$-submodule

$$N \oplus N \cap IM \oplus N \cap I^2M \oplus \dots$$

We know $\mathcal{R}_I(A)$ is Noetherian and $\mathcal{R}_I(M)$ is finitely generated by $\mathcal{R}_I(M)_0$. Hence

$$N \oplus N \cap IM \oplus \dots$$

is a finitely geenrated $\mathcal{R}_I(A)$-module. ☐

Corollary 2. If A is noetherian, $I \subset A$ is an ideal, given any exact sequence of A-modules

$$0 \to N \to M \to L \to 0$$

for which each module is finitely generated, completing with respect to the I-adic topologies induces exact sequence

$$0 \to \hat{N} \to \hat{M} \to \hat{L} \to 0$$

(each topology is the I-adic topology)

Proof. The preceding theorem states that the I-adic topology on $\hat{M}$ induces the I-adic topology on N. In other words, I-adic completions is exact as a functor on the category of finitely generated modules. ☐

Note that this fails for general modules. Consider

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \frac{\mathbb{Q}}{\mathbb{Z}} \to 0$$

The p-adic completion of $\mathbb{Q}$ is $\lim \left(\frac{\mathbb{Q}}{p^n\mathbb{Q}}\right) = 0$ (we are considering $\mathbb{Q}$ as a $\mathbb{Z}$-module).

Theorem 3. Let A be noetherian and M be a finitely generated A-module. Also let $I \subset A$ be an ideal. Consider

$$M \to \hat{M}^I$$

(the latter is the I-adic completion). THe kernel is

$$\cap_{i \geq 0} I^n M = \{x \in M \mid (1-a)x = 0 \text{ for } a \in I\}$$

Proof. Let K be the kernel of $M \to \hat{M}^I$. Now $K \subset M$. The topology on K induced by the I-adic topology on M is $(I^n M \cap K) = (K)$. But this is the trivial topology. By Artin-Rees, the topology is also the topology on K. Nakayama (rather, the determinant trick) gives us the conclusion. ☐

Corollary 3. (Krull intersection theorem) If $I \subset J(A)$, one has $\cap I^n M = 0$. In other words the topology is Hausdorff.

3 November 18

Theorem 4. If A is Noetherian, $\hat{A}$ is Noetherian.

Corollary 4. If A is a Noetherian ring, $A[\![x_1, \dots, x_n]\!]$ is Noetherian.

In fact, one can prove the corollary first (along with the proof of Hilbert's basis theorem) and deduce the theorem from it.

Theorem 5. When A is Noetherian,

$$\dim(A[\![x_1, \dots, x_n]\!]) = \dim(A) + n$$

We will prove this theorem later, but we will show it can be used to prove the first theorem.

Theorem 6. If A is Noetherian, $I \subset A$ is an ideal, then the map $A \to \hat{A}$ is flat. In other words, if

$$0 \to L \to M \to N \to 0$$

is an exact sequence of A-modules, then

$$0 \to \hat{A} \otimes_A L \to \hat{A} \otimes_A M \to \hat{A} \otimes_A N \to 0$$

is exact.

Key point in proof: There is a natural map $\hat{A} \otimes_A M \to \hat{M}$. And the map is surjective if M is finitely generated (A Noetherian)

Given commutative A, ideal $I \subset A$ and I-adic completion $\hat{A}$, $x \in I$ makes

$$s = 1 + x + x^2 + x^3 + \dots$$

a defined element of $\hat{A}$, since the series is Cauchy. That is, $s_n = 1 + x + \dots + x^n$ makes a Cauchy sequence. Or

$$\frac{A}{I^{n+1}} \to \frac{A}{I^n}$$

(s_n) defines a coherent system. Hence $s \cdot (1 - x) = 1 = \lim_n s_n(1 - x) = 1$. This means $1 - x$ is a unit in the completion. In other words, $1 - x \in J(\hat{A})$.

Proposition 2. $I\hat{A} \subset J(\hat{A})$

We can call $I\hat{A} = \hat{I}^n$ for all n when A is Noetherian, since we have

$$0 \to I^n \to A \to \frac{A}{I^n} \to 0$$

yields

$$0 \to \hat{I}^n \to \hat{A} \to \frac{\hat{A}}{I^n \hat{A}}$$

Example. Let A be a commutative ring, $m \in Max(SpecA))$. Let $A \to \hat{A}$ be the m-adic completion. $m\hat{A} \subset J(\hat{A})$ and $\hat{A}/m\hat{A} = \frac{A}{m}$ is a field (this condition may require A is Noetherian). This implies $\hat{A}$ is a local ring with maximal ideal $m\hat{A}$.

Example. Let k be a field, $A = k[x_1, \dots, x_n]$ and $m = (x)$. Then

$$\hat{A} = k[x]^{\wedge}_{(x)} = k[\![x_1, \dots, x_n]\!]$$

Theorem 7. If A is Noetherian, $I \subset A$ is an ideal, then $\hat{A}$ is Noetherian

Proof. Step 1: Prove $A[\![x]\!]$ is Noetherian where x is indeterminate. (This was an exercise, but we can use Hilbert's basis theorem's proof, a possible presentation after/before thanksgiving).

Step 2: Deduce that $A[\![x_1, \dots, x_n]\!]$ is Noetherian by observing

$$A[\![x_1, \dots, x_n]\!] = A[\![x_1, \dots, x_{n-1}]\!][\![x_n]\!]$$

Step 3: Say $I = (a_1, \dots, a_n)$. Consider

$$ev : A[\![x_1, \dots, x_n]\!] \to \hat{A}$$

by the evaluation map $x_i \mapsto a_i$. Check well definedness (Exercise). Check that this map is also surjective (we can use power series to cook up a term that is equal to 1). Elements of $\hat{A}$ can be represented

$$q_0 + q_1 + q_2 + \dots$$

where $q_i \in I^i$. Each partial sum can be realized as a sum of polynomials such that $p_i(a) = q_i$. Surjectivity yields the result, since $\hat{A}$ must be a quotient of a Noetherian ring. $\square$

Exercise

You always have a map $A[x_1, \dots, x_n] \to A$ where $x_i \mapsto a_i$. This map is surjective (it even has a right inverse $A \subset A[x_1, \dots, x_n]$). This suggests, given $(B, J) \to (A, I)$ where $B \to A$ and $J \to I$, and induces

$$\hat{B}^J \to \hat{A}^J$$

which is surjective if $B \twoheadrightarrow A$ and $J \twoheadrightarrow I$. Show that this happens.

Exercise

Suppose A is Noetherian and $I \subset A$ is an ideal. Let

$$f : M \to N$$

be an A-linear map such that M, N are finitely generated. If the induced map $f \otimes_A \frac{A}{I} : \frac{M}{IM} \to \frac{M}{IN}$ is surjective, then $\hat{f} : \hat{M} \to \hat{N}$ is surjective.

4 November 23

Theorem 8. (Hensel's lemma) Let (A, m, k) be complete, local, $f(x) \in A[x]$ be a monic polynomial. Let $F(x)$ be the image of $f(x)$ in $\frac{A}{m}[x] = k[x]$. If $F(x) = G(x)H(x)$ where G, H are monic and $\gcd(G, H) = 1$, then there exists monic polynomials $g(x), h(x) \in A[x]$ with

$$\deg(g) = \deg(G)$$

and

$$\deg(h) = \deg(H)$$

with $f(x) = g(x)h(x)$ and g, h are uniquely determined subject to these constraints. We also have g, h lift G, H.

Corollary 5. If (A, m, k) and $f(x)$ satisfies the above conditions, and $\alpha \in k$ is a **simple** root of $F(x)$, then it lifts to a root of $f(x)$ in A.

Proof. Because α is a simple root,

$$F(x) = (x - \alpha)H(x)$$

with $(x - \alpha, H(x)) = 1$. Hensel's lemma implies that $f(x)$ splits

$$f(x) = (x - \hat{\alpha})h(x)$$

for $\hat{\alpha} \in A$. $f(\hat{\alpha}) = 0$. □

Example. Consider $x^2 - 2 \in \mathbb{Z}[x]$. This has an integer solution if and only if it has a rational solution. Consider $x^2 - 2$ in $\mathbb{F}_7[x]$, which has simple root 3. In fact,

$$x^2 - 2 = (x + 3)(x - 3)$$

This is connected with quadratic reciprocity

But there is no root in $\mathbb{Z}_{(7)}[x]$. Hensel's lemma implies $x^2 - 2$ has a root in $\mathbb{Z}_7 = \hat{\mathbb{Z}}_7$, the 7-adic completion of $\mathbb{Z}$. (potential exercise: finding the root by following Hensel's lemma). Idea of potential exercise: We know there is a root in $\frac{\mathbb{Z}}{7\mathbb{Z}}$. Could we find a root in

$$\frac{\mathbb{Z}}{7^3\mathbb{Z}} \twoheadrightarrow \frac{\mathbb{Z}}{7^2\mathbb{Z}} \twoheadrightarrow \frac{\mathbb{Z}}{7\mathbb{Z}}$$

Preimages of 3 are $3 + 7a$ for $0 \leq a < 7$. If you square $3 + 7a$,

$$(3 + 7a)^2 = 9 + 42a \cong 2 \mod 7^2$$

we are looking for a that satisfies the above congruence. In fact, $a = 1$ works. Likewise, Hensel's lemma ensures that we have some b such that

$$3 + 7 + 7^2 b$$

functions as a root to the polynomial.

Proof. (Hensel's Lemma): Consider

$$\frac{A}{m^{n+1}}[x] \twoheadrightarrow \frac{A}{m^n}[x] \to \ldots \to k[x]$$

. Will construct families of monic polynomials $(g_n(x)_{n\geq 1}$ and $(h_n(x))_{n\geq 1}$ in $A[x]$ such that

- $f(x) = g_n(x)h_n(x) \mod m^n A[x]$.
- $g_{n+1}(x) \equiv g_n(x) \mod m^n A[x]$

  $h_{n+1}(x) \equiv h_n(x) \mod m^n A[x]$
- $g_1(x) \equiv G(x)$ and $h_1(x) \equiv H(x) \mod mA[x]$.

Then $g(x) = \lim g_n(x)$ and $h(x) = \lim h_n(x)$. Then $f(x) - g(x)h(x) \in nm^n A[x] = 0$ by Krull. Pick $g_1(x)$ and $h_1(x)$ in $A[x]$ mapping to $g(x)$ and $h(x)$ respectively. Assume we have constructed g_n and h_n. Consider $f(x) - g_n(x)h_n(x) \in m^n A[x]$. We want to find $a(x), b(x)$ such that

$$a(x), b(x) \equiv 0 \mod m^n A[x]$$

$$f(x) - (g_n(x) + a(x))(h_n(x) + b(x)) \in m^{n+1} A[x]$$

We have

$$[f(x) - g_n(x)h_n(x)] - [g_n(x)b(x) - h_n(x)a(x)] - a(x)b(x) \equiv 0 \mod m^{n+1} A[x]$$

By choosing coefficients for a, b in some high enough power of m, we dont have to worry about the $a(x)b(x)$ term. Call

$$d(x) = f(x) - g_n(x)h_n(x)$$

we choose $u(x), v(x) \in A[x]$ monic such that

$$g_n(x)u(x) + h_n(x)v(x) \equiv 1 \mod mA[x]$$

modding by m, g_n and G are the same, and $h_n \equiv H$. Hence we can have the equation above since G, H are coprime. We have

$$d(x) - (g_n(x)u(x)d(x) + h_n(x)v(x)d(x)) \equiv 0 \mod m^{n+1}A[x]$$

Set $ud = b'$ and $vd = a'$. We would like to take $g_{n+1}(x) = g_n(x) + a'(x)$, $h_{n+1}(x) = h_n(x) + b'(x)$. Both are in $m^nA[x]$. These may not be monic. If this is the case (ie $\deg(a') \geq \deg(g_n)$), use the division algorithm to write

$$a'(x) = q(x)g_n(x) + a(x)$$

and

$$b'(x) = q(x)h_n(x) + b(x)$$

which is possible because g_n, h_n are monic. Set $g_{n+1}(x) = g_n(x) + a(x)$ and $h_{n+1}(x) = h_n(x) + b(x)$. Claim: Let $a(x), b(x) \equiv 0 \mod m^nA[x]$. We also claim $a'(x) \equiv a(x) \mod m^{n+1}A[x]$ and $b'(x) \equiv b(x)$. Consider

$$a'(x) = q(x)g_n(x) + a(x)$$

Because $g_n(x)$ is monic and $\deg(a) < \deg(g_n)$, $q(x) \equiv 0 \mod m^nA[x]$ hence $a(x) \equiv 0 \mod m^nA[x]$. We have

$$f(x) - g_{n+1}(x)h_{n+1}(x)$$

$$= f(x) - (g_n(x) + a(x))(h_n(x) - b(x))$$

$$\equiv f(x) - g_n(x)h_n(x) - g_n(x)b(x) - h_n(x)b(x)$$

I have

$$f(x) - g_n(x)h_n(x) - g_n(x)[b'(x) - q(x)h(x)] - h_n(x)[a'(x) - q(x)g_n(x)]$$

$$q_n(x)h_n(x)[q_b(x) + q_a(x)]$$

We repair this lemma later. $\square$