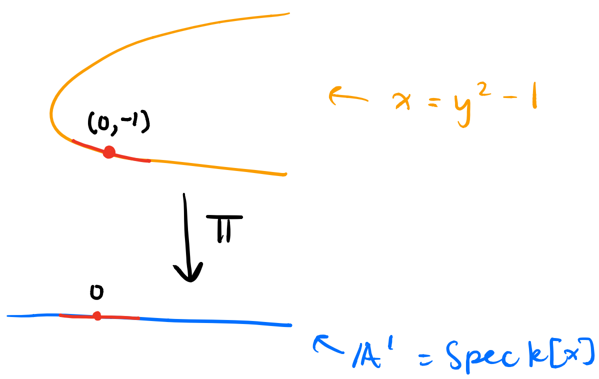
Completions

Idea: If R is a ring, $m \subseteq R$ an ideal, the localization R_m tells us about Zariski open neighborhoods. The "completion" $\hat{R}_m$ tells us about smaller neighborhoods. In the k-algebra case, it tells us about Euclidean neighborhoods.

We will see that if $R = k[x_1, x_2, \ldots, x_n]$, $m = (x_1, \ldots, x_n)$, then $\hat{R}_m = k[[x_1, \ldots, x_n]]$, the formal power series ring, and $\widehat{(R/I)}_m = k[[x_1, \ldots, x_n]] / I\,k[[x_1, \ldots, x_n]]$

Ex: $R = k[x,y]/(y^2 - x - 1)$. Then $k[x] \hookrightarrow R$, and this induces the map



In k^2, π is just the projection onto the x-axis.

In the standard Euclidean topology, π has nonzero derivative at $(0,-1)$, so the inverse function theorem (say $k = \mathbb{C}$ or $\mathbb{R}$) says there is a neighborhood U of 0 on the line and a neighborhood V of $(0,-1)$ s.t. there is an (analytic) inverse

$$U \to V. \qquad x \mapsto (x, -\sqrt{x+1})$$

However, there is no algebraic inverse since y would have to be a square root of $x+1$, which is not a polynomial. However, there is a power series expansion $-\sqrt{x+1} = -1 - x/2 + x^2/8 - \ldots$, which converges for $|x| < 1$.

So we do have an inverse at the level of power series!

We'll see that the above actually holds in a more general setting.

Before we get to the definition of completions, we need the following construction.

Let $\{A_i\}_{i\in J}$ be a collection of groups, w/ J partially ordered s.t. if $i \le j$ $\exists$ $\varphi_{ij} : A_j \to A_i$ a homomorphism with the following properties:

1.) φ_{ii} = identity

2.) $\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$ $\forall$ $i \le j \le k$.

i.e.
$$\begin{tikzcd} A_k \arrow[d] \arrow[dr] & \\ A_i & A_j \arrow[l] \end{tikzcd}$$
commutes.

This is called an <u>inverse system</u>. The <u>inverse limit</u> of the inverse system is

$$\varprojlim A_i = \left\{ \vec{a} \in \prod_{i\in J} A_i \;\middle|\; a_i = \varphi_{ij}(a_j) \;\forall\; i \le j \text{ in } J \right\}$$

For the completion of a ring, let R be a ring, and $m \subseteq R$ an ideal

Then $\{R/m^i\}_{i\in\mathbb{Z}_+}$ is an inverse system, w/ $\varphi_{ij} : R/m^j \to R/m^i$ the quotient.

Then we define the completion w/ respect to m to be

$$\hat{R}_m := \varprojlim R/m = \left\{ g = (g_1, g_2, \dots) \in \prod_i R/m^i \;\middle|\; g_j \equiv g_i \pmod{m^i} \text{ for } j > i \right\}$$

It's clear that $\hat{R}_m$ is also a ring with coordinate-wise addition and multiplication.

For each i, define

$\hat{m}_i := \{g = (g_1, g_2, \ldots) \in \prod R/m^i \mid g_j = 0 \text{ for } j \leq i\}$. Each g_j is equiv. mod m^i,

so $\hat{R}/\hat{m}_i = R/m^i$, since each elt of $\hat{R}/\hat{m}_i$ is a choice of a single equivalence class mod m^i.

If $m \subseteq R$ is maximal, then $\hat{R}_m/\hat{m}_1 = R/m$, a field, so $\hat{m}_1$ is maximal.

If $g = (g_1, g_2, \ldots) \in \hat{R}_m$, but not in $\hat{m}_1$, then $g_1 \neq 0$.

Thus, each $g_i \notin m/m^i \subseteq R/m^i$, so each g_i is a unit (the only max'l ideal containing m^i is m)

Since $g_j = g_i \pmod{m^i}$, it follows that $g_j^{-1} \equiv g_i^{-1} \pmod{m^i}$, so $h = (g_1^{-1}, g_2^{-1} \ldots) \in \hat{R}_m$ and is the inverse of g, so g is a unit.

Thus, $\hat{R}_m$ is local in this case, w/ max'l ideal $\hat{m}_1$.

$R/m_i = (R/m^i)_m = R_m/m^i_m$, so we get the same completion if we first localize at m.

Ex: $R = S[x_1, \ldots, x_n]$, $m = (x_1, \ldots, x_n)$. We want to show that, in fact, $\hat{R}_m \cong S[[x_1, \ldots, x_n]]$.

Note that $S[[x_1, \dots, x_n]] / m^i = R/m^i$, so we have a natural map

(ideal gen by m^i)

$$S[[x_1, \dots, x_n]] \longrightarrow \hat{R}_m$$
$$f \longmapsto (f + m, f + m^2, \dots)$$

In the other direction, if $(f_1 + m, f_2 + m^2, \dots) \in \hat{R}_m$, where for $i > j$, $f_i = f_j$ + terms of deg $> j$.

Then $(f_1 + m, f_2 + m^2, \dots) \longmapsto f_1 + \underbrace{(f_2 - f_1)}_{\deg > 1} + \underbrace{(f_3 - f_2)}_{\deg > 2} + \dots \in S[[x_1, \dots, x_n]]$.

Thus, this is infact a formal power series, and it's straightforward to check that the map is well-defined (i.e. independent of choice of f_i).

Another standard example comes from number theory:

Ex: Let $p \in \mathbb{Z}$ be prime. The ring $\hat{\mathbb{Z}}_{(p)}$, written $\mathbb{Z}_p$ is the ring of p-adic integers. We can do a similar construction as above:

let $(a_1 + (p), a_2 + (p^2), \dots) \in \mathbb{Z}_p$. Where $0 \leq a_i < p^i$.

Then for each i, $a_{i+1} \equiv a_i \pmod{p^i}$, so $p^i \mid a^{i+1} - a^i$, so set

$$a^{i+1} - a^i = b_i p^i, \quad b_i < p$$

and we write this as a power series, called a p-adic expansion.

$a_1 + b_1 p + b_2 p^2 + \dots$, so that the partial sums give the sequence:

$a_1 + b_1 p = a_1 + a_2 - a_1 = a_2$, etc.

However, $\mathbb{Z}/(p^i)$ has torsion (as an abelian group), so addition of power series works a little differently:

$$(a_1, a_2, \dots) + (a_1', a_2', \dots) = (a_1 + a_1' \pmod{p}, a_2 + a_2' \pmod{p^2}, \dots)$$

So, for example in $\mathbb{Z}_2$,

$$(1, 1, 1, 9, 9, \dots) + (1, 1, 1, 1, \dots) = (0, 2, 2, 10, 10, \dots)$$

and the corr. power series expansions are

$$(1 + 0\cdot 2 + 0\cdot 2^2 + 1\cdot 2^3) + (1) = (0 + 1\cdot 2 + 0\cdot 2^2 + 1\cdot 2^3)$$

so addition is not term by term! Instead, we have to "carry".

$$(1 + 2\cdot 3 + 2\cdot 3^2) + (1 + 2\cdot 3 + 1\cdot 3^2) = 2 + 4\cdot 3 + 3\cdot 3^2 = 2 + 1\cdot 3 + 1\cdot 3^2 + 1\cdot 3^3.$$

Note that $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ naturally, since for $r > 0$, $r < p^a$, some a, so $r \pmod{p^a} \neq 0$. i.e. the kernel is 0.

e.g. in $\mathbb{Z}_2$, $1 = (1, 1, 1, \dots)$ and the power series expansion

$1 + 2 + 2^2 + 2^3 + \dots$ corresponds to the element $(1, 2^2 - 1, 2^3 - 1, 2^4 - 1, \dots)$

But $(1, 1, 1, \dots) + (1, 2^2 - 1, \dots) = 0$, so $1 + 2 + 4 + 8 + \dots = -1$.

Note that $\mathbb{Z} \not\cong \mathbb{Z}_p$. Any p-adic expansion

$a_0 + a_1 p + a_2 p^2 + \cdots$ w/ $0 \le a_i < p$, corresponds to the element

$(a_0, a_0 + a_1 p, a_0 + a_1 p + a_2 p^2, \ldots) \in \mathbb{Z}_p$, so this gives a bijection between

p-adic expansions and $\mathbb{Z}_p$. In particular, $\mathbb{Z}_p$ is uncountable!

Properties of Completion

Def: If R is a ring, $m \subseteq R$ an ideal, then if the natural map $R \to \hat{R}_m$ is an isomorphism, we say R is complete with respect to m. When m is max'l, we say R is a complete local ring.

Note: $\bigcap_j m^j$ goes to 0 in $\hat{R}_m$, so if R is complete w.r.t. m, then $\bigcap_j m^j = 0$.

Let $m \subseteq R$ an ideal, and denote $\hat{R} = \hat{R}_m$.

We have a natural map $\hat{R} \to R/m^n$.

$$(f_1, f_2, \ldots) \longmapsto f_n$$

Then $\hat{m}_n$ is the kernel.

Recall: $\hat{m}_n$ is the elements of $\hat{R}$ whose j^{th}-coordinate is in m^n $\forall j$ (and is thus 0 if $j \le n$)

Note: The elements of $m^n \hat{R}$ are generated by elts of the form $(ar_1, ar_2, \ldots)$ where $a \in m^n$, and $(r_1, \ldots) \in \hat{R}$.

In particular, $ar_i \in m^n$, so it's 0 for $i \leq n$.

$\Rightarrow m^n \hat{R} \subseteq \hat{m}_n$. This is an equality if R is Noetherian, but in general, they may be different!!

Claim: $\hat{R}$ is complete with respect to the filtration by the $\hat{m}_n$.

Pf: By definition, $\hat{R}/\hat{m}_n \cong R/m^n$, so

$$\hat{R} = \varprojlim R/m^n = \varprojlim \hat{R}/\hat{m}_n = \text{completion of } \hat{R} \text{ w.r.t. } \hat{m}_1 \supset \hat{m}_2 \supset \dots \quad \square$$

In the Noetherian case, we get the following:

Thm: Let R be Noetherian, $m \subseteq R$ an ideal, and $\hat{R}$ the completion with respect to m.

a.) $\hat{R}$ is complete with respect to $m\hat{R}$.

b.) $\hat{R}$ is Noetherian.

c.) $\hat{R}$ is a flat R-module.

Pf: See Eisenbud.

Limits

Note that in the cases we've looked at, $\hat{R}$ can be thought of as "limits" of sequences in R.

Ex: in $R[x]$, the sequence $a_0, a_0+a_1x, a_0+a_1x+a_2x^2, \ldots$ "converges" to $\sum a_i x^i \in R[[x]]$.

Ex: In $\mathbb{Z}_2$, $\underset{\underset{1}{\shortparallel}}{1}, \underset{\underset{3}{\shortparallel}}{1+2}, \underset{\underset{7}{\shortparallel}}{1+2+2^2}, \ldots$ converges to

$1+2+2^2+\ldots = -1.$

More generally, we define convergence as follows:

Def: A sequence $a_1, a_2, \ldots \in \hat{R}$ <u>converges</u> to an element $a \in \hat{R}$ if $\forall\ n \in \mathbb{Z}$, there is an integer $i(n)$ s.t.

$$a - a_j \in \hat{m}_n \quad \forall\ j \geq i(n)$$

In this case, if $i, j \geq i(n)$, then

$a_i - a_j \in \hat{m}_n$, so it's a Cauchy sequence.

In fact, the converse holds! (Exercise)

In this case, we write $\lim a_i = a$.

(In fact, this is the usual definition of a Cauchy sequence if we put on $\hat{R}$ the topology generated by the basis of sets $a + \hat{m}_n$.)