p-adics, power series, and Hensel's lemma

Let k be a field.

What is the equivalence relation on $\frac{k[t]}{(t^n)}$ $(n \geq 1)$?

$f \equiv g \bmod (t^n) \iff t^n \mid f-g$

$\iff$ f and g have the same coefficients up to degree $n-1$

$f = \sum_{i \geq 0} a_i t^i$, $g = \sum_{i \geq 0} b_i t^i$

$a_i = b_i$ $\forall\, 0 \leq i < n$

if $\operatorname{char}(k) = 0$,

or really if $\frac{1}{i!}$ exists $\forall\, 0 \leq i < n$

$\iff$ $f(0) = g(0)$ 0^{th} order

$f'(0) = g'(0)$ 1^{st} order

$\vdots$

$f^{(n-1)}(0) = g^{(n-1)}(0)$ $(n-1)^{st}$ order

for $k = \mathbb{R}$ or $\mathbb{C}$

$\iff (f-g) = O(t^n)$

So $\operatorname{mod}(t) \iff$ eval @ 0

$\operatorname{mod}(t^2) \iff$ eval + differentiate @ 0

$\operatorname{mod}(t^3) \iff$ " " twice @ 0.

We have maps

$$\frac{k[t]}{(t^n)} \longrightarrow \frac{k[t]}{(t^m)}$$

$$f+(t^n) \longmapsto f+(t^m)$$

If $n \geq m$, the kernel is $\frac{(t^m)}{(t^n)}$

This forgets all the information $\geq$ degree m

What if we want to remember it all?

Def. $\varprojlim_n k[t]/(t^n) = \left\{ (f_n+(t^n)) \in \prod_{n\geq 1} \frac{k[t]}{(t^n)} \;\middle|\; f_n \equiv f_m \bmod t^m \text{ whenever } n \geq m \right\}$

$$\varprojlim_n \frac{k[t]}{(t^n)} \longrightarrow \cdots \longrightarrow \frac{k[t]}{(t^4)} \to \frac{k[t]}{(t^3)} \to \frac{k[t]}{(t^2)} \longrightarrow \frac{k[t]}{(t)} \quad (\text{with } \frac{k[t]}{(t)} \cong k)$$

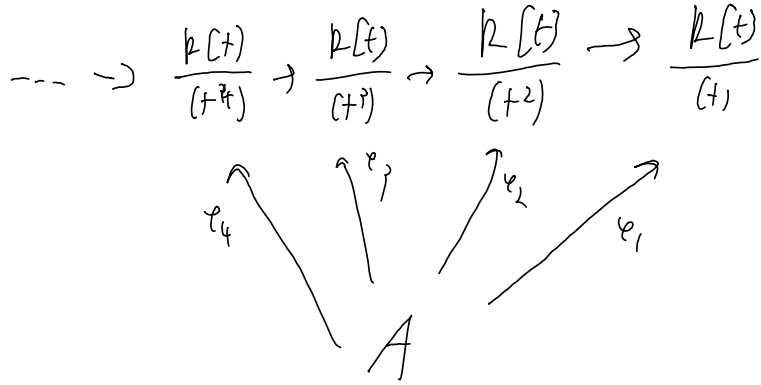
The "inverse limit" of this sequence of ring maps.

Let's call this $R = \varprojlim_n \frac{k[t]}{(t^n)}$.

Let A be a ring with maps

$$\varphi_n : A \longrightarrow k[t]/(t^n)$$

$\forall n \geq 1$ s.t. all the triangles commute



i.e. $\varphi_n(a) \equiv \varphi_m(a) \bmod t^m \quad \forall\, n \geq m$

Thus, $\varphi = (\varphi_n)_n$ is a map $A \longrightarrow \varprojlim_n \frac{k[t]}{(t^n)}$.

This determines precisely how to map into the inverse limit

Prop. ("Universal property of $\varprojlim$")
A ring map $A \longrightarrow \varprojlim_n \frac{k[t]}{(t^n)}$ is uniquely and totally specified by a family $(\varphi_n : A \longrightarrow \frac{k[t]}{(t^n)})$ s.t. $\varphi_n \equiv \varphi_m \bmod t^m$ $\forall n \geq m$, i.e. so the triangles all commute.

In fancy terms,

$$\underline{\mathrm{Ring}}\left(A, \varprojlim_h \frac{k[t]}{(f^n)}\right) \cong \left\{(\varphi_n) \in \prod_n \underline{\mathrm{Ring}}\left(A, \frac{k[t]}{(f^n)}\right) \;\middle|\; \varphi_{n+1} \equiv \varphi_n \bmod f^n \right\}$$

$$\| \quad \text{''} \quad \|$$

$$\varprojlim_n \underline{\mathrm{Ring}}\left(A, \frac{k[t]}{(f^n)}\right)$$

an "inverse limit" in $\underline{\mathrm{Set}}$

$\Big\downarrow$

(of the diagram before $\wr$ $\underline{\mathrm{Ring}}(A, -)$ applied to it)

$\varprojlim_n \frac{k[t]}{(f^n)}$ contains "∞ order differential data".

Let $f = (f_n + (f^n))_n \in \varprojlim_n \frac{k[t]}{(f^n)}$

$f_n + (f^n)$ may be represented as $\sum_{i=0}^{n-1} q_i t^i$ uniquely

$f_{n+1} \equiv f_n \bmod f^n$, so f_{n+1} is $\sum_{i=0}^{n} q_i t^i$ uniquely

etc.

Thus, f is determined wholly and uniquely by a sequence $(q_i)_{i \geq 0} \in k^{\mathbb{N}}$. We write $f = \sum_{i \geq 0} q_i t^i$, a power series.

More formally, we have a map

$$k[[t]] \longrightarrow \varprojlim_n \frac{k[t]}{(t^n)}$$

defined via universal property by taking the maps φ_n

$$k[[t]] \longrightarrow \frac{k[[t]]}{(t^n)} \cong \frac{k[t]}{(t^n)}$$

Explicitly, this takes

$$\sum_{i\geq 0} a_i t^i \longmapsto \left(\sum_{i=0}^{n-1} a_i t^i + (t^n) \right)_n$$

Prop. This is an iso.

pf. If $f \in k[[t]]$ maps to 0, then $f \equiv 0 \bmod (t^n)$ for all n, i.e. $f \in \bigcap_{n\geq 1} (t^n)$, which is (0), so this is $1-1$.

Surjectivity is clear by what we said before. $\square$

Over to arithmetic land...

We have $\mathbb{Z}/p^n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^m\mathbb{Z}$ for $n \geq m$

Def. $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} := \left\{ (a_n + (p^n))_n \in \prod_n \mathbb{Z}/p^n\mathbb{Z} \;\middle|\; a_n \equiv a_m \bmod p^m \text{ for } n \geq m \right\}$

$$\mathbb{Z}_p \to \cdots \to \mathbb{Z}/p^3\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$

We have the same universal property

$$\underline{\mathrm{Ring}}(A, \mathbb{Z}_p) \cong \left\{ (b_n)_n \in \prod_n \underline{\mathrm{Ring}}(A, \mathbb{Z}/p^n\mathbb{Z}) \;\middle|\; b_n \equiv b_m \bmod p^m \text{ for } n \geq m \right\}$$

$$\| !$$

$$\varprojlim_n \underline{\mathrm{Ring}}(A, \mathbb{Z}/p^n\mathbb{Z})$$

How to represent elements of $\mathbb{Z}_p$?

At degree 1, represent $\mathbb{Z}/p\mathbb{Z}$ by $\{0, \ldots, p-1\}$

At degree 2, represent $\mathbb{Z}/p^2\mathbb{Z}$ by $\{0, \ldots, p^2-1\}$

specifically, these are elements of the form $a_0 + pa_1$ for $a_0, b_0 \in \{0, \ldots, p-1\}$, i.e. base p expansions of the form $a_1 a_0$

$\| \quad \| \quad \}$ $\| \quad \|$ $\{0, \ldots, p^3-1\}$

$a_0 + a_1 p + a_2 p^2$, $a_i \in \{0, \ldots, p-1\}$,

so base p expansion of the form $a_2 a_1 a_0$.

$\mathbb{Z}/p^n\mathbb{Z}$ is represented by base p expansions of length n.

$\mathbb{Z}/p^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ truncates the base p expansion

$$\sum_{i=0}^{n} q_i p^i \longmapsto \sum_{i=0}^{n-1} q_i p^i$$

So elts of $\mathbb{Z}_p$ are of the form

$$\sum_{i\geq 0} q_i p^i, \quad q_i \in \{0, \dots, p-1\}$$

i.e. ∞ base p expansions

$$\cdots q_3 q_2 q_1 q_0$$

e.g. $\cdots 111$ in $\mathbb{Z}_2$ is $\sum_{i\geq 0} 2^i$.

$$\begin{aligned} 1 + \sum_{i\geq 0} 2^i &= 1 + 1 + 2 + 4 + 8 + \cdots = 1 + (\cdots 1111) \\ &= 2 + 2 + 4 + 8 + \cdots = 10 + (\cdots 1110) \\ &= 4 + 4 + 8 + \cdots = 100 + (\cdots 1100) \\ &\vdots \\ &= 2^k + \sum_{i\geq k} 2^k = 10\cdots 0 + (\cdots 10\cdots 0) \end{aligned}$$

so all terms are eventually 0, Essentially we carry the 2 off to infinity.

Thus, in $\mathbb{Z}_2$, $\sum_{i\geq 0} 2^i = -1$. Recall the geometric series, $\frac{1}{1-2} = \sum_{i\geq 0} 2^i 1^i$.

$\mathbb{Z}_p$ roughly looks like power series

w/ p as a power series variable and the

set $\{0, \dots, p-1\}$ as coefficients

But this is not $\mathbb{F}_p[\mathbb{Z}[[t]]$!

The addition is different - we do not "carry" in $\mathbb{F}_p[\mathbb{Z}[[t]]$.

$\underline{\text{char } \mathbb{Z}_p = 0}$; $\text{char } \mathbb{F}_p[\mathbb{Z}[[t]]) = p$

By $\left(\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}\right)_{n \geq 0}$

induces a map

$\mathbb{Z} \longrightarrow \mathbb{Z}_p$, by UP

w/ kernel $\bigcap_{n \geq 1} p^n\mathbb{Z} = 0$

Regardless, the power series analogy is very fruitful,

and a fuller exploitation of it is a key to

modern number theory research on "perfectoid spaces"

by Peter Scholze, an acclaimed arithmetic geometer.

The map $\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ takes $\sum_{i \geq 0} a_i p^i \mapsto \sum_{i=0}^{n-1} a_i p^i$,

which is like the order $n-1$ differential in fn.

mod (p) $\leftrightarrow$ evaluating $p=0$

mod (p^2) $\leftrightarrow$ " " and taking a "derivative wrt p"

mod (p^3) $\leftrightarrow$ " " " " 2 "derivatives wrt p"

etc.

$\mathbb{Z}_p$ and $k[[t]]$ are very similar rings

theoretically

Both are local PIDs. In fact, they are "complete" local PID,

(also called a discrete valuation ring, or DVR)

Here's an application of this analogy,

Thm (Hensel's lemma), Let R be either $\mathbb{Z}_p$ or $k[[t]]$,

Let $\pi = \begin{cases} p & R = \mathbb{Z}_p \\ t & R = k[[t]] \end{cases}$, which is

generator of the unique maximal ideal

$m = (\pi)$ of R,

Now, let $f \in R[x]$ be s.t. its reduction mod π (and has the same degree as f)

$\bar{f} \in R/(\pi)[x]$ has a simple root $\bar{a} \in R/(\pi)$, i.e. $\bar{f}(\bar{a}) = 0$

and $\bar{f}$ is indivisible by $(x-\bar{a})^2$.

Then $\exists!\ a \in R$ s.t. $f(a) = 0$ and $a \equiv \bar{a} \bmod \pi$

pf. we recall in both cases that $R = \varprojlim_n R/(\pi^n)$

we will construct a recursively.

(e.g. $f = x^2 - 24$ in $\mathbb{Z}_5$, $\bar{\alpha} = 2 + 5\mathbb{Z}$)

Base case: $\alpha_0 \in R$ any lift of $\bar{\alpha}$, e.g. a degree 0 power series in π.
(e.g. $\alpha_0 = 2 \in \mathbb{Z}_5$)

Inductive step: Suppose we have found $\alpha_k \in R$ for $0 \le k \le n$ such that
- $\alpha_n \equiv \alpha^k \bmod (\pi^{2^k})$ $\forall k$
- $f(\alpha_n) \equiv 0 \bmod (\pi^{2^n})$,

Write $f = \sum_{i=0}^{m} a_i x^i$, $a_m \neq 0$

$f(\alpha_n + \gamma) - (f(\alpha_n) + f'(\alpha_n)\gamma)$ is divisible by γ^2 in $R[\gamma]$.
Indeed, plugging in $\gamma = 0$ yields 0, so the 0th coeff is 0
differentiating then plugging in $\gamma = 0$ also yields 0, so the 1st coeff is 0
(linear approx to f is $O(x^2)$)

Expanding yields

$$f(\alpha_n + \gamma) - (f(\alpha_n) + f'(\alpha_n)\gamma) = \sum a_i (\alpha_n + \gamma)^i + \sum a_i \alpha_n^i + \sum a_i i \alpha_n^{i-1} \gamma$$

This is divisible by γ^2 in $R[\gamma]$, so it is divisible by $(\pi^{2^n})^2 = \pi^{2^{n+1}}$ upon evaluating $\gamma = \beta \pi^{2^n}$ for any $\beta \in R$, i.e.

$$f(\alpha_n + \beta \pi^{2^n}) \equiv f(\alpha_n) + f'(\alpha_n)\beta \pi^{2^n} \bmod \pi^{2^{n+1}}$$

Now, $f'(\alpha_n) \equiv \bar{f}'(\bar{\alpha}) \neq 0$ in R/π, so $f'(\alpha_n)$ is a unit mod $\pi^{2^{n+1}}$, as it is coprime to π.

Choose $\beta \in R$ s.t. $\beta \equiv \dfrac{-f(\alpha_n)}{f'(\alpha_n)} \mod \pi^{2^{n+1}}$

Then $f(\alpha_n + \beta\pi^{2^n}) \equiv 0 \mod \pi^{2^{n+1}}$

Let $\alpha_{n+1} = \alpha_n + \beta\pi^{2^n}$, then

- $\alpha_{n+1} \equiv \alpha_n \mod \pi^{2^n}$
- $f(\alpha_{n+1}) \equiv 0 \mod \pi^{2^{n+1}}$

Rmk: $\alpha_{n+1} \equiv \alpha_n - \dfrac{f(\alpha_n)}{f'(\alpha_n)} \mod \pi^{2^{n+1}}$ (Newton's method!)

Thus, α_{n+1} is unique mod $\pi^{2^{n+1}}$ s.t. the above two hold.

eg. for $f = x^2 - 24$ in $\mathbb{Z}_5$, $\alpha_0 = 2$,

$f(2) = 2^2 - 24 = -20$

$f'(2) = 4$, which has inverse 19 in $\mathbb{Z}/25\mathbb{Z}$

so we take α_1 to be $2 - \underbrace{(-20)\cdot 19}_{20 \cdot b} \mod 25$

$= (-5)(-6)$

$= 30$

$= 5$

So $\alpha_1 = 2 + 5$, i.e. 12 in base 5.

for α_2,

$f(\alpha_1) = 7^2 - 24 = 25$

$f'(\alpha_1) = 14$, which has inverse 134 mod $25^2 = 625$

$$\alpha_2 = \alpha_1 - \frac{f(\alpha_1)}{f'(\alpha_1)} \mod 625$$

$$(-25)(134) \equiv 400 \mod 625$$

$400 = (31)00$ in base 7)

so $\alpha_2 = 3112$ base 7

Rmk. only compute $-\frac{f(x_n)}{f'(x_n)}$ in each step!

To conclude, let $\alpha \in \mathbb{R}$ be the system $(\alpha_n)_n$.

Then $f(\alpha) \equiv f(\alpha_n) \mod 7^{2^n}$

$\equiv 0 \mod 7^{2^n}$ $\forall n$

so $f(\alpha) \equiv 0 \mod 7^{2^n}$ $\forall n$, so $f(\alpha) = 0$. $\square$

The "convergence" rate here is exponential!!

On Completeness

the p-adic valuation

On $\mathbb{Z}$ we define $v_p(n)$ to be the power of p in its prime factorization, and 0 if it doesn't appear. Thus, $n = \prod_{p \text{ prime}} p^{v_p(n)}$ $\forall n \in \mathbb{Z}$

the p-adic norm

$v_p(n/m) := v_p(n) - v_p(m)$ on $\mathbb{Q}$

$|\alpha|_p = p^{-v_p(\alpha)}$ is a norm on $\mathbb{Q}$, and

$\{\alpha \in \mathbb{Q} \mid |\alpha|_p \leq 1\} = \mathbb{Z}_{(p)}$

The p-adic valuation and norm extend to $\mathbb{Z}_p$ in the same way

$$v_p\left(\sum_{i \geq 0} a_i p^i\right) = \text{the least } i \text{ s.t. } a_i \neq 0.$$

Then $p\mathbb{Z}_p = \{\alpha \in \mathbb{Z}_p \mid |\alpha|_p < 1\}$ and is hence open in $\mathbb{Z}_p$. More generally, $p^e\mathbb{Z}_p = \{\alpha \in \mathbb{Z}_p \mid |\alpha|_p < p^{-(e-1)}\}$, which is also open. These define a basis for a topology around 0 in $\mathbb{Z}_p$, making it a topological ring. It is complete wrt topology

Two p-adic integers are close if they are congruent mod a large power of p.

The Hensel's lemma iteration approaches a root of f w/ initial guess x_0 by shrinking the diameter by a factor of 2 on each step, then taking a p-adic limit.

Exc. Rewrite the above in terms of $\mathbb{R}[[t]]$, or better yet, in terms of R and π.