Last time

3 construction of the p-adic numbers

1. Complete $\mathbb{Q}$ w.r.t. $|\ |_p$.
2. $\left(\varprojlim \mathbb{Z}/p^n\right)\left[\frac{1}{p}\right]$
3. "Laurent series" in the variable p

   Fix S a set of coset rep's. for

   $$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p/p\mathbb{Z}_p.$$

   e.g. $S = \{0, 1, \dots, p-1\}$.

$$a_{-n}p^{-n} + a_{-n+1}p^{-n+1} \cdots + a_0 + a_1 p + a_2 p^2 + \cdots$$

$a_i \in S$

Every element in $\mathbb{Q}_p$ has a unique expression of this form.

Addition + multiplication start out like for formal power series, but then have to resolve into coset representatives.

$\mathbb{Q}_3$ $\quad 2 \quad (a_0 = 2)$

$\quad 2 \quad (a_0 = 2)$

$2 \cdot 2 \quad (\text{"}a_0 = 4\text{"})$

$1 + 3 \quad (a_0 = 1 \quad a_1 = 1)$.

This resolution step wouldn't be necessary

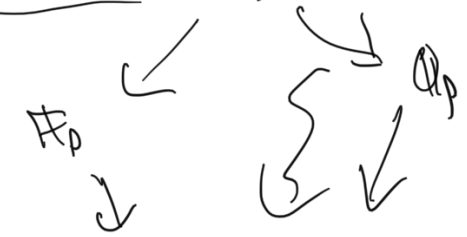
if your $S \subseteq \mathbb{Z}_p$

was a subfield isomorphic to $\mathbb{F}_p$.

this is impossible because $\operatorname{char} \mathbb{F}_p = p$

$\operatorname{char} \mathbb{Q}_p \supseteq \mathbb{Z}_p = 0$.

Side note: $\mathbb{Z}_p$ is a local ring, (complete) discrete valuation (domain)



$\mathfrak{m} = (\pi)$

$R = \varprojlim R/\pi^n$

If $R/\mathfrak{m}$ and $\operatorname{Frac} R$

↑ residue field ↑ fraction field

have same characteristic, "equicharacteristic"

otherwise mixed characteristic

E.g. equi - $\mathbb{F}_p[[t]]$

$\mathbb{C}[[t]]$

mixed - $\mathbb{Z}_p$

Fact: Every equichar. complete dvr R

is $\cong R/\mathfrak{m}[[\pi]]$

Goal for today: Explain a "best-possible" set of representatives S.

Hensel's Lemma:

$f \in \mathbb{Z}_p[x]$ $\quad a_0 + a_1 x + \cdots + a_n x^n$

$\bar{f} \in \mathbb{F}_p[x]$ $\quad \bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n x^n$.

Lemma: If $\bar{t}$ is a root of $\bar{f}$

s.t. $f'(\bar{t}) \neq 0$

then there is a unique root $t \in \mathbb{Z}_p$ of f lifting $\bar{t}$ (i.e. $t \bmod p = \bar{t}$).

Proof: Use Newton's method.

We have $\bar{t}$ ⇝ lift to t_0 s.t.

$t_0 = \bar{t}$ ⟺ $f(t_0) = 0 \bmod p$.

$f(x - t_0) = f(t_0) + f'(t_0)(x - t_0) + O((x - t_0)^2)$

$\equiv 0 \bmod p$

$$\begin{cases} f(t_0) \equiv 0 \bmod p \\ f'(t_0) \not\equiv 0 \bmod p. \end{cases} \qquad // \quad b + O(p)$$

$$f(t_0 + cp) = f(t_0) + f'(t_0)\,cp + O(p^2)$$

$$= pa + bcp + O(p^2)$$

$$c = b^{-1}a$$

$$= O(p^2).$$

Exercise: If $b \not\equiv 0 \bmod p$ then b is invertible in $\mathbb{Z}_p$.

$$t_1 = t_0 + b^{-1}a\,p$$

$$f(t_1) \equiv 0 \bmod p^2$$

Continue Newtons method yoeg

$$t_0, t_1, t_2, t_3, \ldots, t_j, t_{j+1}, \ldots$$

$f(t_j) \equiv 0 \bmod p^{j+1}$ → add a multiple of p^{j+1}

so $\lim t_i$ exists and

$$f(t) = 0.$$

Exercise Rewrite this proof analytically

Exercise [illegible]

and give better bounds for
how good of an approximate zero
you need vs. the absolute
value of the derivative

If $f \in \mathbb{Q}_p[X]$

and t_0 is s.t.

$|f(t_0)| \leq \varepsilon$ and $|f'(t_0)| \geq \delta(\varepsilon$

then Newton's method at t_0
converges to a zero of f.

Want to find coset representatives in $\mathbb{Z}_p$ for $\mathbb{F}_p$ that are multiplicati...

$0 \longleftarrow 0$ from $x^p - x = 0$

$\mu_{p-1} \longleftarrow \mathbb{F}_p^\times = x^{p-1} - 1 = 0$

μ_{p-1}

Need of $\bar{a} \in \mathbb{F}_p^\times = \mu_{p-1}(\mathbb{F}_p)$
then $\exists!$ lift
a of $\bar{a}$ in $\mu_{p-1}(\mathbb{Z}_p)$.

$\bar{a}$ is a root of $f(X) = X^{p-1} - 1$

$f'(X) = (p-1)X^{p-2}$ (in $\mathbb{F}_p[X]$)

$= -X^{p-2}$

$f'(\bar{a}) = -a^{p-2} \neq 0.$

Hensel's lemma gives unique lift.

If $s \in \mathbb{F}_p$, $[s]$ for its multiplicative lift to $\mathbb{Z}_p$

$[0] = 0$

$[s]$ = the unique $(p-1)$st root of unity lifting s

$[s_1][s_2] = [s_1 s_2]$.

$$\left(\sum [s_i] p^i\right)\left(\sum [t_i] p^i\right)$$

$$= \sum_k \left(\sum_{i+j=k} [s_i t_j]\right) p^k.$$

this will still need to be resolved.

$\sum_{i+j=k} [s_i][t_i]$ ← this for arbitrary coset representatives can be complicated

---

Let R be a complete DVR

with $\mathfrak{m} = (p)$. $\quad (p = \underbrace{1+1+\cdots+1}_{p \text{ times}})$.

$R/\mathfrak{m}$ is a field, $\mathfrak{m}$ is the only non-zero prime ideal

$R = \lim R/\mathfrak{m}^n = \lim R/p^n$

(R p-adically complete).

such that R/p is perfect

(i.e. Frobenius $x \to x^p$ is bijective on R/p)

Let R be a p-adically complete ring

$(R = \lim R/p^n)$

s.t. $R/p = \bar{R}$ is perfect.

} strict p-ring.

i.e. $\bar{R} \to \bar{R}$ is an isomorphism
$r \mapsto r^p$

Recall in char p $r \to r^p$ is always a ring homomorphism. because

$$(r_1 + r_2)^p = r_1^p + \binom{p}{1} r_1^{p-1} r_2 + \binom{p}{2} r_1^{p-2} r_2^2 + \cdots + r_2^p$$

($\binom{p}{1} = 0$, $\binom{p}{2} = 0$)

$\frac{p(p-1)\cdots(p-k+1)}{}$

$\binom{p}{k} = \frac{p!}{k!}$ when $p \neq 0$

if $1 \leq k \leq p-1$

is divisible by p.

$(r_1 + r_2)^p = r_1^p + r_2^p$ when $p = 0$.

(Isomorphism = bijection)

injective $\hookrightarrow$ R/p no nilpotents

surjective $\leftrightarrow$ R/p has pth roots

e.g. $\mathbb{F}_p$,

$\mathbb{F}_q$ for any $q = p^n$

Other examples of perfect rings:

if S is a characteristic p ring,

take its perfection

$$\operatorname{colim}\ S \xrightarrow{F} S \xrightarrow{F} S \xrightarrow{F} \cdots$$

$$s \longrightarrow s^p$$

$$s \longrightarrow s^p$$

$$\begin{array}{ccc} S & \longrightarrow & S^p \\ \uparrow & & \| \\ \text{from first copy} & & (S)^p \\ & & \uparrow \text{from second copy.} \end{array}$$

Example.

Example $\mathbb{F}_p[x] \rightsquigarrow \mathbb{F}_p[x^{1/p^\infty}]$

polynomials in x with exponents in $\mathbb{Z}[\frac{1}{p}]$.

Will define multiplicative lifts

$$R/p \to R$$
$$a \to [a].$$

take $a \rightsquigarrow a \; a^{1/p} \; a^{1/p^2} \; a^{1/p^3} \ldots$

(pth roots are unique).

$(x^{p^n} - 1) = (x-1)^{p^n}$ in char p.

Choose arbitrarily a lift

$$\tilde{a} \quad \tilde{a}^{1/p} \quad \tilde{a}^{1/p^2} \ldots$$

$\lim_{x \to a} \left(\tilde{a}^{1/p^n}\right)^{p^n}$ ← Use that p^nth power converges.

↖ Each term is a lift of

Q: Why does this exist?

Q2: Why does not depend on choices:

Given existence, independence, it's obviously multipli

$$\left(\lim_{k\to\infty} (\tilde{a}^{1/p^k})^{p^n}\right)\left(\lim_{k\to\infty} (\tilde{b}^{1/p^k})^{p^n}\right) = \lim_{k\to\infty} \left(\tilde{a}^{1/p^k}\tilde{b}^{1/p^k}\right)^{p^n}$$

$$= [a][b] \qquad \left(\tilde{a}^{1/p^k}\tilde{b}^{1/p^k} \text{ lifts } a^{1/p^k}b^{1/p^k} = (ab)^{1/p^k}\right)$$

$$= [ab].$$

Observation

$$1 \le k \le p^n$$

$$v_p\left(\binom{p^n}{k}\right) = n - v_p(k).$$

Exercise ↗

Consequence

If $x \equiv y \mod p$ (in any ring)

$$x^{p^n} \equiv y^{p^n} \mod p^n$$

$y = x + pt$

$$y^{p^n} = x^{p^n} + \sum_{k=1}^{p^n} \binom{p^n}{k} (pt)^k x^{p^n - k}$$

$\in$

(p^n)

$\binom{p^n}{k} \in (p^{n - v_p(k)})$

$(pt)^k \in p^k$

$p^{n - v_p(k)} p^k \in (p^n)$.

So $x^{p^n} \equiv y^{p^n} \mod p^n$.

(p^n power contact)