Lecture 4

Corollary 3.7: (i) $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$

(ii) Every element $x \in \mathbb{Q}_p$ can be written uniquely as $\sum_{i=n}^{\infty} a_i p^i$, $a_i \in \{0, 1, \ldots, p-1\}$.

Proof: (i) It suffices by Prop. 3.5 to show that $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

Let $f_n : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ be the natural map.

We have $\ker(f_n) = \{x \in \mathbb{Z} \mid |x|_p \leq p^{-n}\}$

$$= p^n\mathbb{Z}.$$

Thus $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ is injective.

Let $\bar{c} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ and $c \in \mathbb{Z}_p$ a lift.

Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, $\exists x \in \mathbb{Z}$ s.t.

$x \in c + p^n\mathbb{Z}_p \leftarrow$ open in $\mathbb{Z}_p$.

Then $f_n(x) = \bar{c}$

$\Rightarrow \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ is surjective.

ii) Follows directly from Prop. 3.5(ii) using $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. $\square$

Eg. $\frac{1}{1-p} = 1 + p + p^2 + p^3 + \ldots$ in $\mathbb{Q}_p$.

Remark: Prop 3.5 implies $\mathbb{F}_p((t))$ and $\mathbb{Q}_p$ both in bijection with

$$\{(a_i)_{i=-\infty}^{\infty} \mid a_i \in \{0,\dots,p-1\},\ a_i = 0 \text{ for } i << -\infty\}$$

2 ring structures very different.

~~II Complete valued fields~~

§4 Hensel's Lemma

Theorem 4.1: (Hensel's Lemma version 1)
Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(X) \in \mathcal{O}_K[X]$ and assume $\exists a \in \mathcal{O}_K$ s.t. $|f(a)| < |f'(a)|^2$.

Then there exists a unique $x \in \mathcal{O}_K$ s.t. $f(x) = 0$ and $|x - a| < |f'(a)|$.

$f'(a)$ formal derivative
E.g. $f(X) = X^n$
$f'(X) = nX^{n-1}$

Proof: Let $\pi \in \mathcal{O}_K$ be a uniformizer and let $r = v(f'(a))$. v normalized valuation ($v(\pi) = 1$)

We construct a sequence $(x_n)_{n=1}^{\infty}$ in $\mathcal{O}_K$ s.t.

(i) $f(x_n) \equiv 0 \mod \pi^{n+2r}$

(ii) $x_{n+1} \equiv x_n \mod \pi^{n+r}$

Take $x_1 = a$; then $f(x_1) \equiv 0 \mod \pi^{1+2r}$

Suppose have constructed $x_1, \dots, x_n$ satisfying (i) and (ii).

3 Define $x_{n+1} := x_n - \dfrac{f(x_n)}{f'(x_n)}$

Since $\underline{x_n \equiv x_1 \bmod \pi^{r+1}}$, $v(f'(x_n)) = r$

and hence $\dfrac{f(x_n)}{f'(x_n)} \equiv 0 \bmod \pi^{n+r}$ by (i).

It follows that $x_{n+1} \equiv x_n \bmod \pi^{n+r}$ so (ii) holds.

Note that for X, Y indeterminates.

$f(X+Y) = f_0(X) + f_1(X)Y + f_2(X)Y^2 + \dots$

where $f_i(X) \in \mathcal{O}_K[X]$ and

$f_0(X) = f(X)$, $f_1(X) = f'(X)$,

Thus $f(x_{n+1}) = f(x_n) + f'(x_n)c + \underbrace{f_2(x_n)c^2 + \cdot}_{\in \pi^{n+2r+1}}$

$c = -\dfrac{f(x_n)}{f'(x_n)}$

Since $c \equiv 0 \bmod \pi^{n+r}$ and $v(f_i(x_n)) \geq 0$,

we $f(x_{n+1}) \equiv f(x_n) + f'(x_n)c \bmod \pi^{n+2r+1}$

$\equiv 0 \bmod \pi^{n+2r+1}$

so (i) holds.

This gives construction of $(x_n)_{n=1}^{\infty}$.

* Property (ii) $\Rightarrow (x_n)_{n=1}^{\infty}$ is Cauchy,

so let $x \in \mathcal{O}_K$ s.t. $x_n \to x$.

Then $f(x) = \lim_{n \to \infty} f(x_n) = 0$ by (i).

Moreover (ii) implies

$a = x_1 \equiv x_n \bmod \pi^{r+1} \ \forall n$

$\Rightarrow a \equiv x \mod \pi^{r+1}$

$\Rightarrow |x-a| < |f'(a)|$. This proves existence

Uniqueness: Suppose x' also satisfies

$f(x') = 0, \quad |x'-a| < |f'(a)|$.

Set $\delta = x' - x \neq 0$.

Then $|x'-a| < |f'(a)|$, $|x-a| < |f'(a)|$

and the ultrametric inequality implies

$$|\delta| = |x - x'| < |f'(a)| = |f'(x)|$$

But $0 = f(x') = f(x+\delta)$

$$= \underset{0}{\underset{\parallel}{f(x)}} + f'(x)\delta + \underbrace{\cdots}_{|\cdot| \leq |\delta|^2}$$

Hence $|f'(x)\delta| \leq |\delta|^2$

$$\Rightarrow |f'(x)| \leq |\delta| \quad \# \qquad \square$$

Corollary 4.2: Let $(K, |\cdot|)$ complete discretely valued field. Let $f(X) \in \mathcal{O}_K[X]$ and $\bar{c} \in k := \mathcal{O}_K/\mathfrak{m}$ a simple root of $\bar{f}(X) := f(X) \mod \mathfrak{m} \in k[X]$. Then $\exists!$ $x \in \mathcal{O}_K$ s.t. $f(x) = 0$ $x \equiv \bar{c} \mod \mathfrak{m}$.

Proof: Apply Theorem 4.1 to a lift $c \in \mathcal{O}_K$ of $\bar{c}$. Then $|f(c)| < |f'(c)|^2 = 1$ since $\bar{c}$ is a simple root. $\square$

Example: $f(X) = X^2 - 2$ has a simple root mod 7. Thus $\sqrt{2} \in \mathbb{Z}_7 \subseteq \mathbb{Q}_7$.

Corollary 4·3:

$$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p > 2 \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p = 2. \end{cases}$$

Proof: Case $p > 2$.

Let $b \in \mathbb{Z}_p^\times$. Applying Corollary 4·2 to $f(X) = X^2 - b$, we find that

$$b \in (\mathbb{Z}_p^\times)^2 \text{ iff } b \in (\mathbb{F}_p^\times)^2.$$

Thus $\mathbb{Z}_p^\times / (\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$ since $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

We have an isomorphism $\mathbb{Z}_p^\times \times \underset{\uparrow}{\mathbb{Z}} \cong \mathbb{Q}_p^\times$ given by $(u, n) \mapsto up^n$ $\quad (\mathbb{Z}, +)$

Thus $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Case $p = 2$:

Let $b \in \mathbb{Z}_2^\times$. Consider $f(X) = X^2 - b$.

$f'(X) = 2X \equiv 0 \bmod 2$.

Let $b \equiv 1 \bmod 8$. $|f(1)|_2 \leq 2^{-3} < |f'(1)|_2^2 = 2^{-2}$

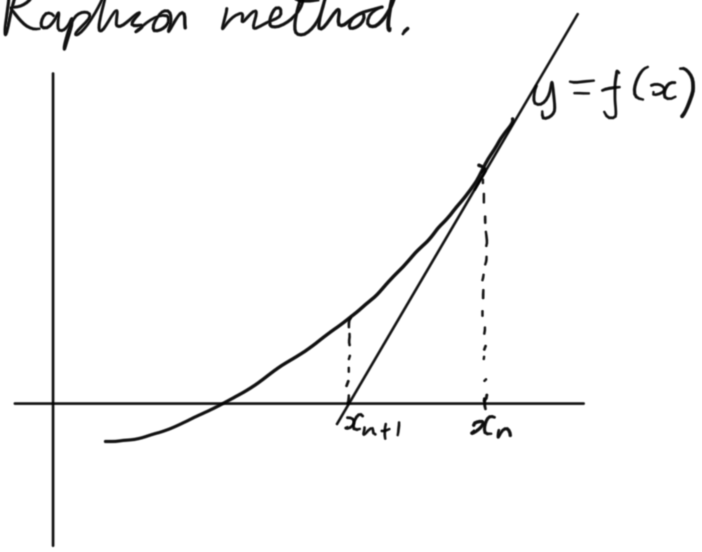
Hensel's Lemma $\Rightarrow f(X)$ has a root in $\mathbb{Z}_2$

$\Rightarrow b \in (\mathbb{Z}_p^\times)^2$ iff $b \equiv 1 \bmod 8$.

Thus $\mathbb{Z}_2^\times / (\mathbb{Z}_2^\times)^2 \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2$

Again using $\mathbb{Q}_2^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}$, we find that $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$ $\square$

Remark: Proof uses the iteration $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$
$\leadsto$ non-archimedean analogue of Newton-Raphson method.



We need for later.

Theorem 4.4: (Hensel's Lemma version 2)
Let $(K, |\cdot|)$ be a complete discretely valued field and $f(X) \in \mathcal{O}_K[X]$. Suppose $\bar{f}(X) := f(X) \bmod \mathfrak{m}$ factorizes as

$$\bar{f}(X) = \bar{g}(X)\bar{h}(X) \quad \text{in } k[X],$$

with $\bar{g}(X)$, $\bar{h}(X)$ coprime.
Then there is a factorisation

$$f(X) = g(X)h(X) \quad \text{in } \mathcal{O}_K[X],$$

with $\bar{g}(X) = g(X) \bmod \mathfrak{m}$, $\bar{h}(X) = h(X) \bmod \mathfrak{m}$

and $\deg \bar{g} = \deg g$.

Proof: Example sheet 1.