Math 538, Lecture 10, 9/2/2024

Bijection: $\left\{ \sum_{i=0}^{\infty} a_i p^i \;\middle|\; a_i \in \{0,\dots,p-1\} \right\}$

$$\updownarrow$$

$$\mathbb{Z}_p$$

Why does $\sum_{i=0}^{\infty} a_i p^i$ converge?

$|a_i p^i|_p \leq p^{-i} \xrightarrow[i\to\infty]{} 0$ so $\sum_{i=0}^{\infty} a_i p^i$ converges

---

<u>or:</u> $v_p\left(\sum_{i=0}^{\infty} a_i p^i - \sum_{i=0}^{\infty} b_i p^i\right)$ = first index i s.t. $a_i \neq b_i$

$\Rightarrow$ if $x, y \in \mathbb{Z}_p$, $x \neq y$ then $\exists k$ s.t. $x \not\equiv y \ (p^k)$

$\Rightarrow$ map $\mathbb{Z}_p \to \prod_k \mathbb{Z}/p^k\mathbb{Z}$ is injective.

<u>HW:</u>
$\mathbb{Z}_p \simeq \left\{ \underline{x} \in \prod_k \mathbb{Z}/p^k\mathbb{Z} \;\middle|\; x_{k+1} \equiv x_k \ (p^k) \right\}$

(If know image of x in $\mathbb{Z}/p^k\mathbb{Z}$, it determines the image mod p^ℓ for $\ell \leq k$)

($\mathbb{Z}_p$ is the pro-p completion of $\mathbb{Z}$)

realizes $\mathbb{Z}_p$ as $\varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$ which is cpt as a closed subset of $\prod_k \mathbb{Z}/p^k\mathbb{Z}$.

from this pov, $\sum_{i=0}^{\infty} a_i p^i$ converges because residue mod p^k is eventually constant.

<u>Last time</u>: "functional analysis":

<u>Thm</u>: F complete wrt nontrivial absolute value. Then $\exists$ unique topology on f.d. F-vsp making it a TVS, any f.d. subspace of an F-TVS is closed.

<u>Cor</u>: If L/F algebraic have at most one extension of $|\cdot|_F$ to L.

$\mathcal{O} = \{x \in F \mid |x| \leq 1\}$

Assume F is non-archimedean

<u>Thm</u>: (Hensel's lemma) for $f \in \mathcal{O}[x]$

(1) If have $\alpha \in \mathcal{O}$ st. $c = \left|\frac{f(\alpha)}{(f'(\alpha))^2}\right| < 1$.
then have $\beta \in \mathcal{O}$ st. $f(\beta) = 0$,

$$|\alpha - \beta| \leq c.$$

$\mathfrak{p} = \{x \in F : |x| < 1\}$

(2) Suppose $\bar{f}$ = image of f in $\mathcal{O}/\mathfrak{p}[x]$ has $\bar{f} \neq 0$ and that $\bar{f} = \bar{g}\bar{h}$ in $k[x]$, $(\bar{g}, \bar{h}) = 1$.

$k = \mathcal{O}/\mathfrak{p}$

Then $\exists g, h \in \mathcal{O}[x]$ lifting $\bar{g}, \bar{h}$, st. $f = gh$, $\deg g = \deg \bar{g}$.

Pf: (1) Last time (Newton's method)

(2) $d = \deg f$, $k = \deg \bar{g}$. Choose preimages g_0, h_0 of $\bar{g}, \bar{h}$ with $\deg g_0 = \deg \bar{g} = k$, $\deg h_0 = \deg \bar{h}$.

Let $\pi \in \mathfrak{p}$, to be chosen later. Suppose that for some n, have $p_i, q_i \in \mathcal{O}[x]$, $1 \le i \le n$ s.t.

$$\deg p_i < k$$
$$\deg q_i \le d \cdot k$$

s.t. for
$$g_n = g_0 + \sum_{i=1}^{n} \pi^i p_i$$
$$h_n = h_0 + \sum_{i=1}^{n} \pi^i q_i$$

have
$$f \equiv g_n h_n \ (\pi^{n+1})$$

Then for any p_{n+1}, q_{n+1} have:

$$f - g_{n+1} h_{n+1} = (f - g_n h_n) - \pi^{n+1} g_n q_{n+1} - \pi^{n+1} p_{n+1} h_n$$
$$- \pi^{2n+2} p_{n+1} q_{n+1}.$$

$$\equiv (f - g_n h_n) - \pi^{n+1} (g_n q_{n+1} + p_{n+1} h_n) \ (\pi^{n+2})$$

So $\pi^{-(n+1)}(f - g_{n+1}h_{n+1}) = \frac{f-g_nh_n}{\pi^{n+1}} - (g_nq_{n+1}+p_{n+1}h_n)$
(π)

<u>Goal:</u> choose p_{n+1}, q_{n+1} s.t. RHS is $0 \bmod \pi$.

Then $f - g_{n+1}h_{n+1} \equiv 0 \ (\pi^{n+2})$

want p_{n+1}, q_{n+1} s.t. $g_nq_{n+1} + p_{n+1}h_n \equiv \frac{f-g_nh_n}{\pi^{n+1}} \ (\pi)$

But $g_n \equiv g_0 \ (\pi)$, $h_n \equiv h_0 \ (\pi)$, so want

$$g_0q_{n+1} + p_{n+1}h_0 \equiv \frac{f-g_nh_n}{\pi^{n+1}} \ (\pi).$$

Applying Bezout in $k[x]$, have $a, b \in \mathcal{O}[x]$ s.t. $\bar{a}\bar{g} + \bar{b}\bar{h} = 1$ i.e. $ag_0 + bh_0 \equiv 1 \ (\pi)$.

May assume $1 > |\pi| \geq |ag_0 + bh_0 - 1|$.

max |coeff|

Let $r_n = \frac{f-g_nh_n}{\pi^{n+1}}$. Then since $ag_0 + bh_0 \equiv 1 \ (\pi)$

$$g_0(ar_n) + h_0(br_n) \equiv r_n \ (\pi)$$

looks like $g_0 q_{n+1} + h_0 p_{n+1} \equiv r_n \ (\pi)$ <u>except</u> $\deg(b r_n)$ could be $\geq k$.

<u>Key</u>: leading coeff of g_0 is in $\mathcal{O}^\times = \mathcal{O} \setminus \mathfrak{p}$ (e.g. has $1 \cdot 1 = 1$) since $\deg g = \deg \bar{g}$.

$\Rightarrow$ can divide with remainder:

$$b r_n = s_{n+1} g_0 + p_{n+1}, \quad \deg p_{n+1} < \deg g_0 = k$$

$$\Downarrow$$

$$g_0(a r_n + s_{n+1} h_0) + h_0 p_{n+1} \equiv r_n \ (\pi)$$

define q_{n+1} by omitting from $a r_n + s_{n+1} h_0$ any coeff divisible by π.

Then have:

$$g_0 q_{n+1} + h_0 p_{n+1} \equiv r_n \ (\pi)$$

$\deg p_{n+1} < k$.

suppose $\deg q_{n+1} = \ell > d-k$. Then highest-degree term of $g_0 q_{n+1}$ would have degree $\ell + k > d$.

But r_n has $\deg \leq d$, so leading coeff of $g_0 q_{n+1}$

would be divisible by π, so leading coeff of g_{n+1}
— " — — " — — " — — " — , contradiction.

For this to work we need: $1 > |\pi| \geq |ag_0 + bh_0 - 1|$
and need $f \equiv g_0 h_0 \ (\pi)$ i.e. $1 > |\pi| \geq |f - g_0 h_0|$

we can do this since $\bar{f} - \bar{g}_0 \bar{h}_0 \equiv 0$. ∎

<u>Cor of (2):</u> Suppose $f \in \mathcal{O}[x]$, $\alpha \in \mathcal{O}$ s.t. $\bar{f} \neq 0$, $\bar{f}(\bar{\alpha}) = 0$. Then $\exists \beta \in \mathcal{O}$ st $\beta \equiv \alpha \ (p)$ and $f(\beta) = 0$
$f'(\alpha) \in \mathcal{O}^\times$

<u>Pf:</u> Have $\bar{f}(\bar{\alpha}) = 0$, $\bar{f}'(\bar{\alpha}) \neq 0$ in k.
so $\bar{\alpha}$ is a simple root, can write $\bar{f} = (x - \bar{\alpha}) \cdot \bar{h}(x)$
with $\bar{h}(\bar{\alpha}) \neq 0$, i.e. $(x - \bar{\alpha}, \bar{h}) = 1$

By (2) have $f(x) = (x - \beta) h$ with $\beta \in \mathcal{O}$, $h \in \mathcal{O}[x]$
st. $\beta \equiv \bar{\alpha} \ (p)$

<u>Cor:</u> let $f \in \mathcal{O}[x]$ be irred, of deg d, so $a_0 a_d \neq 0$
$(f = \sum_{i=0}^{d} a_i x^i)$. Then $|f| = \max\{|a_0|, |a_d|\}$.

Pf: divide f by $|f|$ to assume wlog that $|f|=1$. If $|a_0|, |a_d|<1$ then $\bar{f}$ has degree $<d$ & vanishes at 0 so can write

$$\bar{f} = x^r \cdot \bar{h}$$

with $\bar{h}$ prime to x^r, $1 \le r < d$

$\Rightarrow$ Can write $f = gh$ with $\bar{g} = x^r$, $1 \le \deg g < d$, contradicts irreducibility of f. ∎

Cor: Let $f \in F[x]$ be irred, monic. If $a_0 \in \mathcal{O}$ then $f \in \mathcal{O}[x]$

(if not divide by $|f|$ to get poly in $\mathcal{O}[x]$, irred, with largest coeff not a_0, a_d).

Problem: L/F finite, want to extend $|\cdot|_F$ to L.

Know: if have an extension, it's unique.

Suppose that $|\cdot|_L$ is such an extension, L/F is Galois. Then for any $\sigma \in \mathrm{Gal}(L/F)$, $|\sigma x|_L$ is also an extension so $|\sigma x|_L = |x|_L$, so $|N^L_F x|_L = |\prod_{\sigma \in G} \sigma x|_L = \prod_\sigma |\sigma x|_L = |x|_L^n$

so $|x|_L = |N^L_F x|_F^{1/n}$.

Thm: Let F be complete wrt $|\cdot|_F$ which is nontrivial & non-arch. Let L/F be algebraic of degree n. Then $|\alpha|_L \overset{\text{def}}{=} |N_F^L \alpha|_F^{1/n}$ is an absolute value on L extending $|\cdot|_F$.

Pf: Certainly $|\alpha\beta|_L = |\alpha|_L |\beta|_L$ ($N(\alpha\beta) = N\alpha \cdot N\beta$)

Let $\alpha \in L^\times$ s.t. $N_F^L \alpha \in \mathcal{O}_F$. Let $f \in F[x]$ be the min poly of α. Then f is monic, const coeff is $N_F^L \alpha \in \mathcal{O}_F$, f is irred $\Rightarrow f \in \mathcal{O}[x]$

$(N_F^L \alpha = (f(0))^{[L:F]/\deg f})$

So α is integral over $\mathcal{O}_F$.

Converse immediate.

$\Rightarrow \{\alpha \in L : |\alpha|_L \leq 1\}$ is a subring of L.

$\Rightarrow$ if $|\alpha|_L \leq 1$, then $|1+\alpha|_L \leq 1$

$\Rightarrow$ if α, β have $|\alpha|_L \leq |\beta|_L$ and $\beta \neq 0$ then

$$|\alpha+\beta|_L = |\beta|_L \left|\frac{\alpha}{\beta}+1\right|_L \leq |\beta|_L.$$

$\left|\frac{\alpha}{\beta}\right|_L \leq 1 \Rightarrow \frac{\alpha}{\beta}$ is in ring. $\blacksquare$

<u>Cor</u>: Can extend to any algebraic extension.