Lecture 4

① Let K be a field.
Let $|\ |: K \to \mathbb{R}_{\geq 0}$ be a valuation.

Def: K is complete if every Cauchy sequence in K converges to an element in K.

If K is not complete, we can construct its completion – $\hat{K}$ with $|\ |: \hat{K} \to \mathbb{R}_{\geq 0}$ valuation by

1) R = Ring of All Cauchy sequences in K
2) $I \subset R$ the ideal of sequences $\to 0$
3) $\hat{K} = R/I$
4) $K \subset \hat{K}$ constant sequences
5) $|a| = \lim_{n \to \infty} |a_n|$ $a = \{a_n\}$

Remark: $(\hat{K}, |\ |)$ is unique up to isomorphism

If $(\hat{K}', |\ |')$ is another completion, then $\exists f: \hat{K} \to \hat{K}'$ s.t. $|a|' = |f(a)|$ $\forall a \in \hat{K}$
isomorphism of fields

Ex: $\mathbb{C}, \mathbb{R}$

(2) Th (Ostrowski)

Suppose $|\ |$ is Archimedean and K is complete.

Then either $K = \mathbb{R}$ or $K = \mathbb{C}$ (and $|\ |$ is usual) $|\ |_\infty^s$, $s \in (0,1]$.

Proof: We may assume $\mathbb{R} \subseteq K$ and $|\ |\big|_{\mathbb{R}} = |\ |_\infty$.

Why?

Let $x \in K$ s.t. $x \notin \mathbb{R}$. Let us show that "$x \in \mathbb{C}$" "satisfies a quadratic equation".

Let $f : \mathbb{C} \to \mathbb{R}$ be $f(z) = |x^2 - (z+\bar{z})x + z\bar{z}|$.

Then f is continuous. And $\exists$ its minimum $= m$.

Claim: $\exists N > 0$ s.t. $f(z) > m$ $\forall z \in \mathbb{C}$ s.t. $|z| \geq N$.

Put $S = \{ z \in \mathbb{C} : f(z) = m \}$.

Then S is bounded by Claim. And closed.

Then $\exists\, z_0 \in S$ with greatest $|z_0|$.

If we show that $m = 0$, we are done.

Thus, we suppose $m > 0$.

2 cont Put $g(t) = t^2 - (z_0 + \bar{z}_0)t + z_0\bar{z}_0 + \varepsilon$ for $\varepsilon \in (0, m)$.

Let z_1 and $\bar{z}_1 \in \mathbb{C}$ be its roots.

Then $\underbrace{z_1\bar{z}_1}_{= |z_1|^2} = z_0\bar{z}_0 + \varepsilon > |z_0|^2$. Then $\boxed{f(z_1) > m}$

Put $G(t) = (g(t) - \varepsilon)^n - (-\varepsilon)^n = \prod_{i=1}^{2n} (x - \alpha_i)$

Then $G(z_1) = 0$. $\alpha_1 \ldots \alpha_{2n} \in \mathbb{C}$

wlog, $\boxed{z_1 = \alpha_1}$. Put x into $G^2(t) = \prod_{i=1}^{2n} (x^2 - (\alpha_i + \bar{\alpha}_i)x + \alpha_i\bar{\alpha}_i)$

$$|G(x)|^2 = \prod^{2n} f(\alpha_i) \geq f(\alpha_1) \cdot m^{2n-1}$$

$\wedge|$

$$(|g(x) - \varepsilon|^n + |\varepsilon|^n)^2 = (|f(z_0)^n| + \varepsilon^n)^2 = (m^n + \varepsilon^n)^2$$

$\Downarrow$

$$\frac{f(\alpha_1)}{m} \leq \left(1 + \left(\frac{\varepsilon}{m}\right)^n\right)^2$$

$\lim_{n \to \infty} \Rightarrow f(\alpha_1) \leq m$. But $f(\alpha_1) > m$.

$\square$

(3) From now on $| \, |$ is not Archim. IV

$K \subset \hat{K}$ $\begin{cases} v(x) = -\log|x| \\ \forall x \neq 0 \text{ in } K. \end{cases}$ in $v(a_n) = v(a)$

Remark: $|x| \neq |y| \Rightarrow |x+y| = \max\{|x|, |y|\}$

Then $a_n \to a$ $|a_n|$ "stabilizes" (unless $a=0$) because $|a_n - a| < |a|$ $\forall n \gg 0$, so that

$$|a_n| = \max\{|a_n - a|, |a|\} = |a|.$$

So we do not have "new" $|a|$.

Corollary: Cauchy $\{a_n\} \Leftrightarrow a_{n+1} - a_n \to 0$

$\sum a_i$ converge $\Leftrightarrow$ $a_i \to 0$.

As before $\hat{O} \subseteq \hat{K}$ $\{x \in \hat{K} \text{ s.t. } |x| \leq 1\}$

$\hat{I} \subseteq \hat{O}$ $\{x \in \hat{K} \text{ s.t. } |x| < 1\}$

Corollary: $\hat{O}/\hat{I} \cong O/I$ & $\hat{I}$ = maximal ideal.

where $O \subseteq K$ $I \subseteq O$ are defined in the same way.

(4) Now we assume $|\ |$ is discrete. $\underline{\overline{V}}$

And normalized $(v(K^*) = \mathbb{Z})$

$\exists \varpi \in K$ s.t. $v(\varpi) = 1$.

ϖ is in O. ϖ is prime.

$\forall x \in K^*$ $x = u\varpi^m$, $u \in O^*$ $m \in \mathbb{Z}$.

Proposition: Let $R \subseteq O$ be a system of representatives for O/I. Suppose $0 \in R$.

$\forall x \in \hat{K}^*$ $x = \varpi^m(a_0 + a_1\varpi + a_2\varpi^2 \dots)$

$a_i \in R$, $a_0 \neq 0$, $m \in \mathbb{Z}$.

Proof: $x = \varpi^m u$ $u \in \hat{O}^*$.

$\exists a_0 \equiv u \mod \hat{I}$ $u = a_0 + \varpi \cdot b_1$ $b_1 \in \hat{O}$

Apply the same for b_1 instead of x.

Use convergence.

$\square$

Ex: $\mathbb{Q}$ $|\ |_p$ $\mathbb{Q}_p$

Ex: $\mathbb{C}[t]$ $a \in \mathbb{C}$ $I = \langle t-a \rangle$ ... $\mathbb{C}((x))$ Laurent series.

(1) Proposition: $\hat{O} \cong \varprojlim O/I^n$

(6) BASIC VERSION:

Th: $f(x) \in \mathbb{Z}_p[x]$ s.t. $f(a) \equiv 0 \mod p$

$a \in \mathbb{Z}_p$ $\qquad f'(a) \not\equiv 0 \mod p$.

Then $\underline{\exists! \alpha} \in \mathbb{Z}_p$ s.t. $f(\alpha) = 0$, $\alpha \equiv a \mod p$.

Proof: Put $a_1 = a$.

Let $a_2 = a_1 + pt_1$ s.t. $f(a_2) \equiv 0 \mod p^2$.

Why t_1 exists?

$$f(a_2) = f(a_1) + f'(a_1)pt_1 + \frac{f''(a_1)}{2}(pt_1)^2 + \cdots$$

Now by induction $a_1 \cdots a_n$ s.t.

- $f(a_n) \equiv 0 \mod p^n$
- $a_n \equiv a \mod p$.

Put $a_{n+1} = a_n + p^n t_n$. The

$$f(a_{n+1}) = f(a_n) + f'(a_n)p^n t_n + \cdots$$

Q: $f'(a_n)p^n t_n \equiv ? \mod p^{n+1}$

A: $\equiv f'(a)p^n t_n$

DONE $\square$

Ex: SQUARE ROOTS mod $p > 2$.

(7) $K, |\ |$ complete, (~~discrete~~)

VI

$\mathcal{O}$ = Ring of x with $|x| \le 1$.

I = ideal with $|x| < 1$.

Th. Let $f(x) \in \mathcal{O}[x]$ s.t. $f \not\equiv 0 \bmod I$.

Suppose that $f(x) \equiv \bar{g}(x)\bar{h}(x) \bmod I$

and $\bar{g}, \bar{h} \in \mathcal{O}/_I[x]$ are relatively prime.

Then $f(x) = g(x)h(x)$ for some $f, g \in \mathcal{O}[x]$ s.t.

- $g \equiv \bar{g}(x) \bmod I$
- $h(x) \equiv \bar{h}(x) \bmod I$
- $\deg g = \deg \bar{g}$.

Proof: Put $d = \deg f$, $m = \deg \bar{g}$. Then $\deg \bar{h} \le d - m$.

Let g_0, h_0 be some polynomial in $\mathcal{O}[x]$

s.t. $g_0 \equiv \bar{g} \bmod I$, $h_0 \equiv \bar{h} \bmod I$ $\deg g_0 = m$.

Then $\exists\ a(x), b(x) \in \mathcal{O}[x]$ s.t. $ag_0 + bh_0 \equiv 1 \bmod I$

$$\left\{\begin{array}{l} f - g_0h_0 \\ ag_0 + bh_0 - 1 \end{array}\right. \text{ are } 0 \text{ in } \bmod I.$$

Let π be "biggest" coef of these poly.

Then they are $\equiv 0 \bmod \pi$ $\quad \pi \in I$.

(7 cont) VII

We are looking for

$$\begin{cases} g = g_0 + p_1 \pi + p_2 \pi^2 + \cdots \\ h = h_0 + q_1 \pi + q_2 \pi^2 \cdots \end{cases}$$

$p_i, q_i \in \mathcal{O}[x]$ of $\boxed{\deg \leq m}$, $\leq d-m$.

$$\begin{cases} g_{n-1} = g_0 + p_1 \pi + \quad + p_{n-1} \pi^{n-1} \\ h_{n-1} = h_0 + q_1 \pi + \quad + q_{n-1} \pi^{n-1} \end{cases} \quad \text{s.t.}$$

$$\star \quad f \equiv g_{n-1} h_{n-1} \mod \pi^n \qquad \text{by induction}$$

$$\begin{cases} g_n = g_{n-1} + p_n \pi^n \\ h_n = h_{n-1} + q_n \pi^n \end{cases}$$

$$\star \quad f - g_{n-1} h_{n-1} \equiv (g_{n-1} q_n + h_{n-1} p_n) \pi^n \mod \pi^{n+1}$$

$$\Updownarrow$$

$$g_0 q_n + h_0 p_n \equiv f_n \mod \pi$$

? But $g_0 a + h_0 b \equiv 1 \mod \pi$ $\left(f_n = \dfrac{f - g_{n-1} h_{n-1}}{\pi^n} \right)$

$$g_0 a f_n + h_0 b f_n \equiv f_n \mod \pi$$

$q \in \mathcal{O}[x]$ $\Leftarrow$ $b_m f_n = q(x) g_0(x) + p_n$ $\quad \deg p_n < \deg g_0 = m$

highest coef of g_0 is unit
$g_0 \equiv \bar{g} \mod J$
$\deg g_0 = \deg \bar{g}$

$$g_0 a f_n + h_0 (q g_0 + p_n) \equiv f_n$$

$$g_0 (a f_n + h_0 q) + h_0 p_n \equiv f_n \mod \pi$$

8 VII

Corollary: $\mathbb{Q}_p$ has $(p-1)$-th roots of unity $(p-1)$ of th

Corollary: $f(x) = a_0 + a_1 x + \quad + a_n x^n \in K[x]$ (complete, non-Archimedean).

Suppose $a_0 \neq 0$ and $a_n \neq 0$, f is IRRED.

Then $\max\{|a_0|, .. |a_n|\} = \max\{|a_0|, |a_n|\}$

(If $a_0 \in \mathcal{O}$ and $a_0 = 1$, then $f \in \mathcal{O}[x]$)

Proof: We may assume $f \in \mathcal{O}[x]$, and $\max\{|a_0| .. |a_n|\} = 1$.

Let a_r be the first coeff s.t. $|a_r| = 1$

$f(x) = x^r(a_r + a_{r+1}x + \ldots + a_n x^{n-r}) \bmod I$.

If $|a_0| < 1$ and $|a_n| < 1$, then $r \in (0, n)$.

$\neq$ Hensel lemma

$\square$

(9) $K, |\ |$ as before (complete non-archimedean)

$K \subset L$ algebraic extension.

Remark. If L is finite, put $N_{L|K} : K \to L$ by

$$N_{L|K}(\alpha) = \det(T_\alpha)$$

where ~~k_α~~ $T_\alpha : \in \mathrm{End}_K(L)$ multiplication by α.

Theorem: Suppose $L|K$ finite.
Put $|\alpha| = \sqrt[n]{|N_{L|K}(\alpha)|}$ $\forall \alpha \in L$.

Then, • $|\ | : L \to \mathbb{R}_{\geq 0}$ valuation.
•• L is complete and $|\ |'|_K = |\ |$
••• this is the only way to extend $|\ |$ to L.

Ex: $\mathbb{R} \subset \mathbb{C}$.
$\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}_p$, $p \equiv 3 \bmod 4$

EXISTENCE

(10) $\boxed{\text{Proof}}$: $O_K \subset K$ is integrally closed. IX

. Put $O_L \subset L$ the integral closure of O_K in L.

Claim: $O_L = \{\alpha \in L \text{ s.t. } N_{L/K}(\alpha) \in O_K\}$

Proof: $\alpha \in O_L \Rightarrow N_{L/K}(\alpha) \in O_K$ (use Chapter I Sectn 2)

$\Leftarrow$ Take $\alpha \in L^*$ s.t. $N_{L/K}(\alpha) \in O_K$.

$\begin{cases} \alpha^d + a_{d-1}\alpha^{d-1} + \dots + a_0 = 0 \text{ in } K[x] \\ \text{minimal polynomial.} \end{cases}$

$N_{L/K}(\alpha) = \pm a_0^m \in O_K$ (characteristic Tα poly is a power of minimal)

$\Downarrow$

$|a_0| \leq 1$, $a_0 \in O_K$

$\alpha \in O_L$

$\Uparrow$ $\qquad$ $\Downarrow$

$f(x) \in O_K[x] \Leftarrow$ Corollary of Hensel Lemma

$\Downarrow$

- $|\alpha| = 0 \Leftrightarrow \alpha = 0$
- $|\alpha\beta| = |\alpha||\beta|$
- $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\} \Leftrightarrow |\alpha| \leq 1 \Rightarrow |\alpha + 1| \leq 1$

(ii) Uniquness $\qquad$ X

$K \subset L \quad |\ |'$ another extension.

$\mathcal{O}_K \subset \mathcal{O}_L \quad I_L \subset \mathcal{O}_L$ max ideal

Similarly, Let $\mathcal{O}'_L, I'_L \subset \mathcal{O}'_L$ be valuation ring and ideal.

$|\ |' \leq 1$

$|\ |' < 1$

Take $\alpha \in \mathcal{O}_L$ s.t. $\alpha \notin \mathcal{O}'_L$.

Let $f(x) = x^d + a_1 x^{d-1} + \dots + a_d$ be minimal $/K$ polynomial of α.

Then $a_1 \dots a_d \in \mathcal{O}_K$ (we just proved this).

$$\alpha \notin \mathcal{O}'_L \Rightarrow \alpha^{-1} \in I_L \Rightarrow 1 = \underbrace{-a_1 \alpha^{-1} - \dots - a_d (\alpha^{-1})^d}_{\in I_L}$$

$\Downarrow$

$|\alpha| < 1 \Rightarrow |\alpha|' \leq 1$.

Approximation Theorem: $\exists\, \alpha$ s.t. $|\alpha| \leq 1$, $|\alpha|' > 1$. if not equivalent

$\Downarrow$

equivalent $\quad |\ |' = |\ |^s$

But on K they are the same!

(12) Completeness. XI

This follows from general result.

Th: $\underline{K, |\ |}$ complete.

Then all norms on K^n are equivalent ~~to~~ (say to $\max\{|x_i|\}$.)

Proof: $(x_1 \quad x_n)$ $\quad \|\ \| = \max\{|x_i|\}$.

$|\ |$ = any other norm.

Then $|\ | \leq (\sum |(0 \ldots i \ldots)|) \|\ \|$.

Want $|\ | \geq \rho \|\ \|$. $\quad n = 1 \quad \rho = |V_1|$.

~~$V_i = (\ldots 0_{i \text{ place}} \ldots) \cong K^{n-1}$~~ $\quad V_i = (\ldots\ 0, \ldots)$ with K^{n-1} (0 in i-th pl)

$\Downarrow$

$V_i = (\ldots, 1, \ldots) \subseteq K^n \quad \Longleftarrow$ complete

SH closed

$\exists \rho$ s.t. all vectors lying there $|\ | \geq \rho$.

$|(x_1 \ldots x_n) \cdot \frac{1}{x_r}| \geq \rho$

$|x_r| = \max\{|x_i|\}$