WEEK 4.

<u>Corollary</u> (K complete) $f \in R[X]$. Suppose $\alpha_0 \in R$ sat.

$$f(\alpha_0) \equiv 0 \pmod{m} \quad \underline{\text{and}} \quad f'(\alpha_0) \not\equiv 0 \pmod{m}$$

[i.e., $\overline{\alpha_0} \in k$ is a <u>simple</u> root of $\overline{f} \in k[X]$].

Then $\exists\, \alpha \in R$ s.t. (1) $f(\alpha) = 0$ and

(2) $\alpha \equiv \alpha_0 \pmod{m}$.

[i.e., $\overline{\alpha_0}$ <u>lifts</u> to a root of f in R]

— This α is nec. <u>unique</u> (and simple): If $\alpha \neq \beta$ both work

$$f(X) = (X-\alpha)(X-\beta)\, q(X)$$

$$\Rightarrow \overline{f}(X) = (X - \overline{\alpha_0})^2\, \overline{q}(X)$$

contradicts $\overline{\alpha_0}$ is <u>simple</u>.

— In other words, $R = \mathcal{O}_K$ is <u>HENSELIAN</u>.

<u>Def</u>. Let (R, m, k) be a local ring.
We say R is <u>Henselian</u> if $\forall$ monic $f \in R[X]$,
and every <u>simple root</u> $\rho \in k$ of $\overline{f}$,
there exists an $\alpha \in R$ s.t. $f(\alpha) = 0$ and $\rho = \overline{\alpha}$.

("<u>strictly</u> Henselian" when $k = k^{sep}$)

Lem. 10.149.3

- Commutative algebra (cf. Stacks project, tag 04GE):
R Henselian iff following holds: "Hensel's Lemma"

> For any $f \in R[X]$ and any factorization:
> $$\bar{f} = g_0 h_0 \text{ with } GCD(g_0, h_0) = 1,$$
> there's a factorization $f = gh$ in $R[X]$ s.t.
> $$g_0 = \bar{g} \text{ and } h_0 = \bar{h}$$
> (moreover, $\deg(g) = \deg(g_0)$).

"if" is obvious: $\bar{f}(x) = (x-\rho)h_0(x)$ lifts to
$f(x) = (x-\alpha)h(x)$.
coprime if ρ simple

Application: Consider $x^{p-1} - 1 = \prod_{\rho \in \mathbb{F}_p^\times} (x-\rho)$ in $\mathbb{F}_p[X]$.
By Hensel for $\mathbb{Z}_p$,
each $\rho \in \mathbb{F}_p^\times$ lifts uniquely
to a root $\hat{\rho} \in \mathbb{Z}_p^\times$ of $x^{p-1}-1$.
$(p-1)^{st}$ root of unity in $\mathbb{Q}_p$.

$$1 \to 1 + p\mathbb{Z}_p \to \mathbb{Z}_p^\times \to \mathbb{F}_p^\times \to 1$$
splits: As top. groups,
Teichmüller lift (representatives)
$$\mathbb{Z}_p^\times \cong \mu_{p-1}(\mathbb{Q}_p) \times (1 + p\mathbb{Z}_p)$$

<u>Hensel</u>–<u>Kurschak</u> <u>Lemma</u>: K complete, non-arch.

$f(X) = a_0 + a_1 X + \cdots + a_N X^N \in K[X]$.

Assume (i) f <u>irreducible</u>, <u>monic</u> ($a_N = 1$)

(ii) $a_0 \in R$.

Then <u>all</u> $a_i \in R$. for $i = 0, 1, \dots, N-1$.

PROOF. More <u>general</u> statement:

If $f \in K[X]$ is <u>any</u> polynomial,

let (not nec. irr./monic)

$$\|f\| := \max\{|a_0|, |a_1|, \dots, |a_N|\}.$$

Assume ($a_N \neq 0$)

(a) $\|f\| > |a_N|$ and

(b) $\|f\| = |a_i|$ for some $i > 0$.

Then f is <u>reducible</u>.

— <u>Remark</u>: (will use it to extend $|\cdot|$ on K to <u>finite</u> E/K).

<u>Why</u>? May assume $\|f\| = 1$. — in this case (a) & (b) amount to: $|a_N| < 1$ and some $|a_i| = 1$ for $i > 0$.

Thus $f \in R[X]$ and $a_i \in R^\times$ for <u>some</u> $0 < i < N$.

Let r be the <u>largest</u> such i.

Thus $a_i \in \mathfrak{m}$ for $r < i \leq N$, and therefore

$$\overline{f}(X) = (\overline{a_0} + \overline{a_1} X + \cdots + \underbrace{\overline{a_r}}_{\text{nonzero}} X^r) \cdot \overline{1}$$

nonzero.

Factors obviously coprime, so by <u>HENSEL</u>: $f = gh$ where $\overline{g} = \overline{f}$ and $\overline{h} = \overline{1}$. (moreover $\deg(g) = \deg(\overline{g}) = r$)

$\Rightarrow f$ <u>reducible</u>. ✓

– back to our <u>special case</u>: If $f \in K[X]$ <u>irreducible</u> and $a_N = 1$, either (a) or (b) <u>fails</u>.

I.e., either $\|f\| \leq 1$ or $\|f\| = |a_0|$. ≤ 1 (by (ii))

In both cases $\|f\| \leq 1$. Equivalently, $f \in R[X]$ (so all $a_i \in R$). $\square$

Extension Thm. $K, |\cdot|$ complete. E/K finite, $n = [E:K]$. There's a unique $\|\cdot\|$ on E extending $|\cdot|$ on K, and $E, \|\cdot\|$ is complete.

- Formula: $\|x\| = |N_{E/K}(x)|^{1/n}$.
  ($x \in E$)

[therefore $|\cdot|$ also extends uniquely to $\bar{K}$ = alg. closure].

— Formula follows immediately from uniqueness:

First suppose E/K Galois, $G = \mathrm{Gal}(E/K)$, $|G| = n$.

Then $\forall \gamma \in G$, $x \longmapsto \|\gamma(x)\|$ abs. value ext. $|\cdot|$

$$\Rightarrow |N_{E/K}(x)| = \prod_{\gamma \in G} \underbrace{\|\gamma(x)\|}_{=\|x\|}$$

$$= \|x\|^n.$$

[If not Galois pass to normal closure and use above obs. for $\tilde{E}/K$].

$$\left.\begin{array}{c} \tilde{E} \\ | \\ E \\ | \\ K \end{array}\right) \text{Galois}$$

★ Difficulty: $x \mapsto |N_{E/K}(x)|^{1/n}$ sat. strong triangle ineq.

Exc: A multiplicative function $f: E \longrightarrow [0, \infty)$ sat. strong triangle ineq. iff

$$f(\alpha) \leq 1 \implies f(\alpha + 1) \leq 1, \quad \text{all } \alpha \in E.$$

[hint: only if obvious. "if" suppose $\alpha, \beta \in E^\times$ and $f(\alpha) \leqslant f(\beta)$. Then,

$$f(\alpha+\beta) = f(\beta) f\left(\frac{\alpha}{\beta}+1\right) \leqslant f(\beta)\cdot 1 \quad = \max$$

<u>note</u>: $f\left(\frac{\alpha}{\beta}\right) = \frac{f(\alpha)}{f(\beta)} \leqslant 1.$]

<u>Note</u>: $|\cdot|_\infty$ on $\mathbb{C}$ does <u>not</u> extend to $\mathbb{C}(t)$

$$\begin{array}{c} \mathbb{C}(t) \\ | \ \text{trans.} \\ \mathbb{C} \end{array}$$

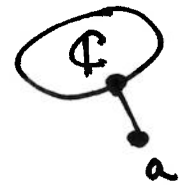
— follows from:

<u>Prop.</u> $E \supset \mathbb{C}$ with $\|\cdot\|$ extending $|\cdot|_\infty$. Then $E = \mathbb{C}$.

Pf (sketch): If $E \neq \mathbb{C}$ pick any $a \in E \setminus \mathbb{C}$.

Has a "<u>nearest</u>" point $z_0 \in \mathbb{C}$: $\quad d(a, \mathbb{C}) = \|a - z_0\|$
(exc)

That is, $\|a - z\| \geqslant \|a - z_0\| \quad \forall z \in \mathbb{C}$.



Then $\underset{\substack{\rotatebox{90}{$\in$} \\ E \setminus \mathbb{C}}}{\tilde{a}} := a - z_0$ sat. $\quad \|\tilde{a} - z\| \geqslant \|\tilde{a}\|$ for all $z \in \mathbb{C}$.

Scaling $\tilde{a}$ by $c > 0$ arrange that $\|\tilde{a}\| > 1$.

<u>Summary</u>: Found $b \in E \setminus \mathbb{C}$ s.t.

$$\|b - z\| \geqslant \|b\| > 1 \quad \forall z \in \mathbb{C}.$$

Using $b^n - 1 = \prod_{i=0}^{n-1} (b - \zeta^i)$ for $n \in \mathbb{N}$ arbitrary,

$$\|b - 1\| = \frac{\|b^n - 1\|}{\prod_{i=1}^{n-1} \|b - \zeta^i\|} \underset{\substack{\uparrow \\ z = \zeta^i}}{\leqslant} \frac{\|b^n - 1\|}{\|b\|^{n-1}} = \left\| b - \frac{1}{b^{n-1}} \right\|$$

$\left\| b - \frac{1}{b^{n-1}} \right\| \to 0$ as $n \to \infty$ — since $\|b\| > 1$.

Letting $n \to \infty$,

$$\|b - 1\| \leqslant \|b\|$$

$\uparrow$ <u>equality</u> ($z = 1$ above)

$\Rightarrow \boxed{\|b-1\| = \|b\|}$. Repeating the argument for $b-1$ etc. yields $\|b-n\| = \|b\|$ $\forall n \in \mathbb{N}$.

Then,

$$n = |n|_\infty = \|n\| \leq \|b-n\| + \|b\| = 2\|b\|$$

— contradiction $\square$.

Ostrowski's 2^{nd} thm.: $K, |\cdot|$ archimedean & complete. Then $K = \mathbb{R}$ or $K = \mathbb{C}$ with $|\cdot| \sim |\cdot|_\infty$.

Idea: archimedean, so $\mathbb{Q} \subseteq K$ (char $= 0$) and $|\cdot| \sim |\cdot|_\infty$ on $\mathbb{Q}$.

complete — so in fact $\mathbb{R} \subseteq K$.

If $\mathbb{C} \subseteq K$ the above prop. shows $\mathbb{C} = K$.

(otherwise more work — omit).

~ Assume $K, |\cdot|$ non-archimedean & complete.

$$\begin{array}{c} E \\ | \text{ finite} \\ K \end{array}$$

Def. V = vector space over K (eventually $V = E$)

A "norm" on V is $\|\cdot\| : V \longrightarrow [0, \infty)$ s.t.

1) $\|x\| = 0 \iff x = 0$
2) $\|cx\| = |c| \cdot \|x\|$ $\quad (c \in K, x \in V)$
3) $\|x+y\| \leq \|x\| + \|y\|$

(usually assume ultrametric)

Ex $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ basis, $\|\sum_{i=1}^{n} x_i v_i\| := \max\{|x_1|, \dots, |x_n|\}$.

Prop. K with $|\cdot|$ complete, $\dim_K V < \infty$.
Let $|\cdot|_1$ and $|\cdot|_2$ be norms on V. Then $\exists a, b > 0$:

$$a|x|_1 \leq |x|_2 \leq b|x|_1 \qquad \forall x \in V.$$

(so any two norms def. same topology on V, $|\cdot|_1 \sim |\cdot|_2$, rel. to which V is complete).

PROOF. May assume $|\cdot|_1 = |\cdot|_{\mathcal{B}}$ rel. (ordered) basis $\mathcal{B}$. (transitivity) $\mathcal{B} = \{e_1, \dots, e_n\}$.

take a max-norm, e.g. $|\cdot|_{\mathcal{B}}$

[and non-arch. if K is].

"any two norms are equivalent on n-dim space"

- Induction on $n = \dim V$. ($n=0$ ok)

Suppose $n > 0$ and ok for $\dim < n$.

Note: Any $x = \sum_{i=1}^{n} x_i e_i$ has – for any norm $\|\cdot\|$,

$$\|x\| \leq \sum_{i=1}^{n} |x_i| \cdot \|e_i\| \leq \underbrace{\left(\sum_{i=1}^{n} \|e_i\|\right)}_{b} \cdot \underbrace{\max|x_i|}_{|x|_{\mathcal{B}}}$$

- Finding $a > 0$:
  - introduce subspaces

$$W_i = \operatorname{span}\{e_1, \dots, \hat{e}_i, \dots, e_n\} \qquad (i = 1, \dots, n)$$

$\dim W_i = n-1$. By induction all norms on W_i are $\sim$ and each W_i is complete rel. any $\|\cdot\|$

May restrict $\|\cdot\|$ on V to W_i. In particular $W_i \subseteq V$ closed (rel. $\|\cdot\|$).

$\Rightarrow$ $\underbrace{e_i + W_i}_{}$ closed.

0 not in here; find open ball $B_\varepsilon(0)$ s.t.

$$B_\varepsilon(0) \cap (e_i + W_i) = \emptyset$$

for all i (shrink ε if necessary).

★) CLAIM: $a = \varepsilon$ works (i.e., $\varepsilon |x|_B \leq \|x\|$ for all $x \in V$).

Let $x \in V \setminus \{0\}$. Pick i s.t. $|x|_B = |x_i|$. Then

$x_i^{-1} x = \cdots + 1 e_i + \cdots$ lies in $e_i + W_i$,

therefore not in $B_\varepsilon(0)$: $\|x_i^{-1} x\| \geq \varepsilon$. done. $\square$

Corollary. K with $|\cdot|$ complete (non-trivial), E/K finite.
If $|\cdot|_1$ and $|\cdot|_2$ are abs. val. on E ext. $|\cdot|$ on K, $|\cdot|_1 = |\cdot|_2$ (and E complete)

PROOF. By Prop., $|\cdot|_2 = |\cdot|_1^c$, some $c > 0$.

Pick $a \in K^\times$ with $|a| \neq 1$. Then $|a|_2 = |a| = |a|_1^c = |a|^c$ shows $c = 1$. $\square$