WEEK 5.

Extension Thm.: K complete, with $|\cdot|$, non-archimedean. E/K finite, $n=[E:K]$.
Then $|\cdot|$ extends uniquely to an abs-value $\|\cdot\|$ on E.
Formula: $\forall x\in E$, ok by Cor. above.

$$\|x\| = \left|N_{E/K}(x)\right|^{1/n}.$$

PROOF. Define $f: E \longrightarrow [0,\infty)$ by $f(x) = |N(x)|^{1/n}$.
Strong triangle inequality? (multiplicative ✓)
- Equivalently, $f(\alpha)\leq 1 \Longrightarrow f(\alpha+1)\leqslant 1$? $\forall \alpha\in E$.

Suppose $f(\alpha)\leqslant 1$. Minimal polynomial:

$$h(t) = \operatorname{Irr}(\alpha,K,t) = a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} + t^m$$

Here (204A): $(m=[K(\alpha):K])$ $K[t]$.

$$a_0 = \pm N_{K(\alpha)/K}(\alpha)$$

Observe: $N_{E/K}(\alpha) = N_{K(\alpha)/K}\left(N_{E/K(\alpha)}(\alpha)\right) = N_{K(\alpha)/K}(\alpha)^{[E:K(\alpha)]}$.

Therefore,

$$|a_0| = \left|N_{K(\alpha)/K}(\alpha)\right| = f(\alpha)^m \leqslant 1, \quad \text{i.e. } a_0\in R.$$

By Hensel–Kürschák all $a_i\in R$.
So, $h(t-1) = \operatorname{Irr}(\alpha+1,K,t)\in R[t]$

$h(t-1)$ has constant term: $\pm N_{K(\alpha)/K}(\alpha+1)$.

$\Uparrow$

R

$\Rightarrow f(\alpha+1)^m \leq 1$

$\Rightarrow f(\alpha+1) \leq 1$.

done $\square$

$\|$ as above obs.

$\pm N_{E/K}(\alpha+1)^{m/n}$ — has abs. value:

$\|$

$\pm f(\alpha+1)^m \cdot (\text{unit})$

- **Remark**: $|\cdot|$ extends uniquely to $\overline{K}$,
  - but not complete (fact); consider $\widehat{\overline{K}}$.

  e.g. $\mathbb{C}_p := \widehat{\overline{\mathbb{Q}_p}}$.

Exc K with $|\cdot|$ complete, non-arch.

- For $\alpha \in \overline{K}$ T.F.A.E.:
  - (1) $|\alpha| \leq 1$
  - (2) $\mathrm{Irr}(\alpha, K, t) \in R[t]$
  - (3) α integral over R.

(**Hint**: (1) $\Rightarrow$ (2): Constant term $a_0 = \pm N_{K(\alpha)/K}(\alpha)$ has $|a_0| = |\alpha|^{[K(\alpha):K]} \leq 1$. Done by Hensel–Kurschak.

(2) $\Rightarrow$ (3): Obvious.

(3) $\Rightarrow$ (1): Suppose $\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0 = 0$ with all $a_i \in R$.
If $|\alpha| > 1$, $|\alpha|^m \leq \max\{|a_0|, \ldots, |a_{m-1}\alpha^{m-1}|\} \leq |\alpha|^{m-1}$
(contradiction))

K with $|\cdot|$, possibly incomplete
(ex. $\mathbb{Q}$ with $|\cdot|_p$)
E = number field, g/p.

$$\begin{array}{c} E \\ \text{finite } \Big| \; n = [E:K]. \\ \text{\& separable } \; \\ K \end{array}$$

Thm. (a) $|\cdot|$ extends to E.
(b) $|\cdot|$ has $\leq n$ extensions to E, say $|\cdot|_i$ with $i = 1, 2, \ldots, r$.
(c) Let $\hat{E}_i$ be the i^{th} completion.
Then:

$$E \otimes_K \hat{K} \xrightarrow{\sim} \prod_{i=1}^{r} \hat{E}_i$$

(isom. of $\hat{K}$-alg.)

— In particular, $[E:K] = \sum_{i=1}^{r} [\hat{E}_i : \hat{K}]$.

PROOF. $C = \hat{K}^{alg}$ with the $|\cdot|_C$ extending $\|\cdot\|$ on $\hat{K}$ (complete).

$\sigma \in \mathrm{Hom}_K(E, C) = \{\sigma_1, \ldots, \sigma_n\}$ (sep.)

Note: $x \longmapsto |\sigma(x)|_C$ is abs. value on E ext. $|\cdot|$ on K.
$\qquad\quad \| $
$\quad |x|_\sigma \qquad\qquad \Rightarrow$ (a).

Claim. Any $|\cdot|'$ on E ext. $|\cdot|$ on K is of the form $|\cdot|_\sigma$ $\Rightarrow$ (b).
(may have repetitions i.e., may happen: $|\cdot|_\sigma = |\cdot|_\tau$ for $\sigma \neq \tau$)

– why? E' = completion of E rel. $|\cdot|'$
K' = closure of K in E'.

$$\begin{array}{ccc} E & — & E' \\ | & & | \\ K & — & K' \end{array}$$

• Observe that $E' = EK'$. (RHS finite/K' thus complete, contains E as dense subf.)
(thus E'/K' finite)

Since $|\cdot|'$ extends $|\cdot|$ on K,
K' is another completion of K. Unique: Pick

$$\gamma : K' \xrightarrow{\sim} \widehat{K}$$ isometric K-linear isomorphism of fields.

Extend it to embedding

$$\sigma : E' \longrightarrow \mathbb{C}.$$

Since $\underset{E'}{\underset{\in}{x}} \mapsto \underset{\underset{|x|'}{\|}}{|\sigma(x)|_{\mathbb{C}}}$ extends $|\cdot|'$ on K' (complete)
— unique...

Certainly for $x \in E \subseteq E'$: $\quad |x|' = |\sigma(x)|_{\mathbb{C}} = |x|_{\sigma_E}$.

(C): E/K sep., choose primitive element: $E = K(\alpha)$.

$$f(t) = \operatorname{Irr}(\alpha, K, t) = f_1(t) \cdots f_s(t)$$

— factor in $\widehat{K}[t]$

w. $f_i \in \widehat{K}[t]$ irreducible, distinct.

Pick a root $\alpha_i \in \mathbb{C}$ for each f_i.

Let $\sigma_i : E \longrightarrow \mathbb{C}$ be the embedding $\sigma_i(\alpha) = \alpha_i$.

$$\alpha \longmapsto \alpha_i$$

Consider an arbitrary $\sigma \in \operatorname{Hom}_K(E, \mathbb{C})$.

$\sigma(\alpha)$ is a root of precisely one of the f_i

$$\hat{K}(\alpha_i) \xleftarrow{\sim} \hat{K}[t]/(f_i(t)) \xrightarrow{\sim} \hat{K}(\sigma\alpha).$$

Find Galois auto. $\tau \in \mathrm{Gal}(\mathbb{C}/\hat{K})$ sending $\tau(\alpha_i) = \sigma(\alpha)$.

$$\tau(\alpha_i) = \sigma(\alpha) = \tau\sigma_i(\alpha)$$

– Shows: $\sigma = \tau\sigma_i$.

Thus, $\forall x \in E$,

$$|x|_\sigma = |\tau\sigma_i(x)| = |\sigma_i(x)| = |x|_{\sigma_i}$$

obs. $|\tau(c)| = |c|$ for all $c \in \mathbb{C}$ (both sides ext. $\|\cdot\|$ on $\hat{K}$)

– So any ext. of $|\cdot|$ on K to E is among $|\cdot|_{\sigma_1}, \ldots, |\cdot|_{\sigma_s}$. — so $r \leq s$.

<u>Claim</u> $r = s$ (i.e., they're <u>distinct</u>).

Extend $\sigma_i : E \to \mathbb{C}$ to $\hat{\sigma}_i : \hat{E}_i \to \mathbb{C}$ ~~(multiple~~ (possible? $\sigma_i : E \to \hat{K}(\alpha_i)$ is isometric into complete field.) $\hat{E}_i$ = completion of E rel. $|\cdot|_{\sigma_i}$.

Suppose $|\cdot|_{\sigma_i} = |\cdot|_{\sigma_j}$, some $1 \leq i, j \leq s$.

Then,

$$\hat{\sigma}_j \circ \hat{\sigma}_i^{-1} : \hat{K}(\alpha_i) \xrightarrow{\sim} \hat{E}_i = \hat{E}_j \xrightarrow{\sim} \hat{K}(\alpha_j)$$

extends to a $\tau \in \mathrm{Gal}(\mathbb{C}/\hat{K})$ with $\tau(\alpha_i) = \alpha_j$.

$\Rightarrow \alpha_j$ is a root of f_j <u>and</u> f_i $\Rightarrow i = j$. ✓

$$\hat{E}_i \cong \hat{K}[t]/(f_i)$$

~ Knowing $r = s$, and $E \cong K[t]/(f)$,

$$\begin{tikzcd}
\hat{K}[t]/(f) \arrow[r, "\sim", "\text{CRT}"'] & \prod_{i=1}^{r} \hat{K}[t]/(f_i) \arrow[d, "\wr"] \\
E \otimes_K \hat{K} \arrow[u, "\wr"] \arrow[r, "\text{composition of isoms..}"'] & \prod_{i=1}^{r} \hat{E}_i
\end{tikzcd}$$

<u>Remark</u>: In general, if E/K is possibly <u>inseparable</u>, $|\cdot|$ has $\leq [E:K]_{sep}$ extensions (<u>unique</u> if <u>purely</u> insep.), and

$$(E \otimes_K \hat{K})_{red} \xrightarrow{\sim} \prod_{i=1}^{r} \hat{E}_i$$

so here $[E:K] \geq \sum [\hat{E}_i : \hat{K}]$.

$$\begin{array}{c} \text{field} \\ F = (E \otimes \hat{K})/\mathfrak{m} \\ \Big| \text{ fin.} \\ \hat{K} \end{array}$$

<u>Exc</u>: Pick any max $\mathfrak{m} \subseteq E \otimes \hat{K}$, consider: ext. $|\cdot|$ on $\hat{K}$ to F, restrict to $E \hookrightarrow F$.

Complete: $\hat{E}$.

If $x \in \ker(\dots)$, diagram shows $x \in \mathfrak{m}$.

$$\begin{tikzcd}
0 & \hat{E} \arrow[r, hook] & F \\
x \in \arrow[u, mapsto] & E \otimes \hat{K} \arrow[u] \arrow[ur] &
\end{tikzcd}$$

— conclude $\ker(\dots) = \bigcap \mathfrak{m} = \mathrm{Rad}(0)$.

App.: Ostrowski for number fields $\overset{E}{K}/\mathbb{Q}$.

$|\cdot|_\infty$ and $|\cdot|_p$ on $\mathbb{Q}$ extend to E.

I) Archimedean: Extensions of $|\cdot|_\infty$ are $|\cdot|_\sigma$ for some $\sigma: E \longrightarrow \mathbb{C}$. (cf. proof above)

[Minkowski Theory $\Longrightarrow$ $|\cdot|_\sigma$ and $|\cdot|_\tau$ are inequivalent unless $\sigma \in \{\tau, \bar\tau\}$]

II) Non-arch.: Ext. of $|\cdot|_p$ are $|\cdot|_\sigma$ for $\sigma: E \longrightarrow \overline{\mathbb{Q}_p}$

$\mathfrak{p} = \{x \in \overset{\mathcal{O}}{E} : |x|_\sigma < 1\}$ max id. in $\mathcal{O}_E$, $\mathfrak{p} | p$.
(nonz. prime)

gives $|\cdot|_\mathfrak{p}$ on E:

$$|x|_\mathfrak{p} = N(\mathfrak{p})^{-v_\mathfrak{p}(x)}.$$

Note: $|\cdot|_\sigma \cong |\cdot|_\mathfrak{p}$.

Why? They're equivalent since they have the same unit ball $\mathfrak{p}$.

- Summary: Up to equivalence, the non-triv. $|\cdot|$ on a number field $E/\mathbb{Q}$ are:
  - I) $|\cdot|_\sigma$ for $\sigma: E \to \mathbb{C}$
  - II) $|\cdot|_\mathfrak{p}$ for $\mathfrak{p} \subseteq \mathcal{O}_E$.

- Moreover, $E \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\sim} \prod_{\mathfrak{p}|p} E_\mathfrak{p}$.

next understand:

$$\begin{array}{c} E_\mathfrak{p} \\ | \\ \mathbb{Q}_p \end{array}$$

K with non-arch. $|\cdot|$, $\quad k = \mathcal{O}/\mathfrak{m}$.

E/K finite, with <u>some</u> $|\cdot|$ ext. $|\cdot|$ on K.
(unique if K complete)

<u>Get:</u>
$\mathcal{O}_E$, $\mathfrak{m}_E$, k_E.

<u>Note</u>: $\mathcal{O}_K = K \cap \mathcal{O}_E$, $\quad \mathfrak{m}_K = K \cap \mathfrak{m}_E$, $\quad k_K \hookrightarrow k_E$.

<u>Def</u>: 1) "inertia degree" $f(E/K) = [k_E : k_K]$
2) "ramification index" $e(E/K) = [|E^\times| : |K^\times|]$.

both (possibly ∞) — a priori.

cf.

<u>Obs</u>: ∘ Both f and e are <u>multiplicative</u> in <u>towers</u>.

∘ —— " —— <u>insensitive</u> to <u>completion</u>.
(recall $k_K \simeq k_{\hat{K}}$ and $|K^\times| = |\hat{K}^\times|$)

∘ In general $[E:K] \geq [\hat{E}:\hat{K}]$.

<u>Lemma</u>. If E/K finite, so are $e(E/K)$ and $f(E/K)$, and

$$\boxed{e(E/K) \cdot f(E/K) \leq [E:K]}$$

PF. Choose $x_1, \dots, x_f \in \mathcal{O}_E$ s.t. $\{\overline{x_i}\}$ is a k_K-basis (just <u>lin. independent</u>) for k_E.
Choose $y_1, \dots, y_e \in E^\times$ s.t. $|y_j|$ lie in different cosets mod $|K^\times|$.

CLAIM: $\{x_i y_j\}$ lin. <u>independent</u> over K $\left(\Rightarrow ef \leq \underset{[E:K]}{\overset{\shortparallel}{n}}\right)$

*) <u>Prelim.</u> <u>obs.</u>: $\left|\sum_{i=1}^{f} a_i x_i\right| = \max\{|a_1|, \dots, |a_f|\}$.
$(a_i \in K)$

scaling: enough to show $\left|\sum_{i=1}^{f} a_i x_i\right| = 1$
when <u>all</u> $a_i \in \mathcal{O}_K$
and <u>some</u> $a_i \in \mathcal{O}_K^\times$.

If not, $\sum_{i=1}^{f} \overline{a_i}\,\overline{x_i} = 0$ in k_E, so
all $\overline{a_i} = 0$. But some $\overline{a_i} \neq 0$. ✓

Back to claim: Supp. $\exists$ relation

$$\sum c_{ij} x_i y_j = 0. \quad \text{I.e., } \sum_j \underbrace{\left(\sum_i c_{ij} x_i\right)}_{\overset{\text{df.}}{=}\, a_j} y_j = 0.$$

$c_{ij} \in K$

By obs *) deduce $\forall j$:

$$|a_j| = \max\{|c_{1j}|, \dots, |c_{fj}|\}$$

— visibly <u>lies</u> <u>in</u> $|K^\times|$ (if nonz.)

Assumption on y_j's tells us all (nonz) terms of $\sum_j a_j y_j$ have <u>distinct</u> $|\cdot|$:

$$|a_r y_r| \neq |a_s y_s|. \quad (\text{if nonz.})$$

Therefore "max achieved once", so

$$0 = \left|\sum_j a_j y_j\right| \overset{\downarrow}{=} \max\{|a_j y_j| : j = 1, \dots, e\}$$

Conclude all $a_j = 0$, which by ~~indep~~ (obs *) means all $c_{ij} = 0$. $\square$

Strengthening: E/K finite, suppose $|\cdot|_1, \ldots, |\cdot|_r$ are <u>all</u> the extns. of $|\cdot|$ on K.

w. corr. f_i and e_i.

– Then,

$$\sum_{i=1}^{r} e_i f_i \leqslant [E:K].$$

equal if E/K sep.

(Why? $e_i = e(\hat{E}_i/\hat{K})$ and sim. for f_i.

By lemma, $e_i f_i \leqslant [\hat{E}_i : \hat{K}]$. Also, $\sum_{i=1}^{r} [\hat{E}_i : \hat{K}] \leqslant [E:K]$)

Next GOAL:

<u>Thm</u>. E/K finite and separable, $|K^\times|$ <u>discrete</u>.

Then:

$$\sum_{i=1}^{r} e_i f_i = [E:K].$$

– Above argument reduces to showing: – apply to $\hat{E}_i/\hat{K}$.

<u>Lemma</u> E/K finite, <u>complete</u>, $|K^\times|$ <u>discrete</u>.

Then:

$$e(E/K) \cdot f(E/K) = [E:K].$$

(non-arch.)

E/K finite, K complete, $|K^\times|$ discrete. $(= |\pi|^{\mathbb{Z}})$.

<u>Lemma</u>: Suppose $v_1, \dots, v_r \in \mathcal{O}_E$ reduce to a k_K-basis for $\mathcal{O}_E/\pi\mathcal{O}_E$. Then:

(just <u>span</u>)

$$\mathcal{O}_E = \sum_{i=1}^{r} \mathcal{O}_K \cdot v_i \qquad (\oplus)$$

Pf. Denote RHS by $M \subseteq \mathcal{O}_E$. <u>Assumption</u>: $\mathcal{O}_E = M + \pi\mathcal{O}_E$.

$\forall\, x \in \mathcal{O}_E$, write $x = \sum_{i=1}^{r} \underset{\mathcal{O}_K}{\underset{\Uparrow}{x_i}} v_i + \pi y$, with $y \in \mathcal{O}_E$.

— do the same for y, continue:

$$x = \sum_{i=1}^{r} x_i^{(n)} v_i + \pi^n y^{(n)}$$

such that $x_i^{(n+1)} \equiv x_i^{(n)} \pmod{\pi^n}$

K complete, let $c_i = \lim_{n\to\infty} x_i^{(n)}$.

Then $x = \sum_{i=1}^{r} c_i v_i$ $\square$

<u>Exc</u>: Check "<u>freeness</u>", so $\mathcal{O}_E$ is <u>finite</u> <u>free</u> $\mathcal{O}_K$-module of rank $= \dim_{k_K} \mathcal{O}_E/\pi\mathcal{O}_E$.

$\boxed{ef = n}$: Uniformizers $\pi \in K$, $\Pi \in E$.

— write $\pi = (\text{unit})\cdot \Pi^e$, $e = v_E(\pi)$ (ram. idx.)

$\left(|K^\times| = |\pi|^{\mathbb{Z}} \leq |E^\times| = |\Pi|^{\mathbb{Z}} \infty\ |E^\times|/|K^\times| \simeq \mathbb{Z}/e\mathbb{Z} \right)$

- Pick $v_1, \dots, v_f \in \mathcal{O}_E$ reducing to a k_K-basis for k_E (modulo $m_E = (\Pi)$.)

(f = inertia degree)

(*) Claim: $v_i \Pi^j$ ($i = 1, \dots, f$ and $j = 0, \dots, e-1$) generate $\mathcal{O}_E$ as an $\mathcal{O}_K$-module.

- introduce $M = \mathcal{O}_K v_1 + \dots + \mathcal{O}_K v_f$.

By assumption,

M

$$\begin{aligned} \mathcal{O}_E &= M + \Pi \mathcal{O}_E \\ &= M + \Pi M + \Pi^2 \mathcal{O}_E \\ &\vdots \\ &= \underbrace{M + \Pi M + \dots + \Pi^{e-1} M}_{\text{- must be } \mathcal{O}_E \text{ by the lemma.}} + \underbrace{\Pi^e \mathcal{O}_E}_{\pi \mathcal{O}_E}. \end{aligned}$$

(proves claim)

Certainly these $v_i \Pi^j$ then span E as K-vs.,

- so $\underset{\underset{n}{\parallel}}{[E:K]} \leq ef$. $\square$

Corollary $\mathcal{O}_E$ is free over $\mathcal{O}_K$ of rank $n = [E:K]$.

Pf. $|\mathcal{O}_E / \pi \mathcal{O}_E| = q_E^e = q_K^{ef}$ so $\dim_{k_K} \mathcal{O}_E / \pi \mathcal{O}_E = ef = n$ $\square$