Lecture 5

$K, |\ |$

1) Def: K is a local field if

   1) K is complete wrt to $|\ |$
   2) $|\ |$ is discrete valuation
   3) Residue field is finite.

$K \supset \mathcal{O} \supset I \quad \mathcal{O}/I = k$ = Residue field.

2) Normalized discrete valuation

$$|x|_I = q^{-v_I(x)} \qquad q = |k|, \quad v_I : K^{*} \to \mathbb{Z}.$$

3) Lemma: If K is local, then K is locally compact. And $\mathcal{O}$ is compact.

Proof: $\mathcal{O} \cong \varprojlim \mathcal{O}/I^n \subseteq \prod_{n=1}^{\infty} \mathcal{O}/I^n$ ← compact

A) compact $I^M/I^{M+1} \cong \mathcal{O}/I$; $|\mathcal{O}/I^n| < +\infty$.

B) $\forall a \in K \quad a + \mathcal{O}$ is open + compact.

4) Th: Let K be a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$.
Then K is local.

Proof: $| \ | = \sqrt[n]{|N_{K/L}(\alpha)|}$ where $L = \mathbb{Q}_p$ OR $\mathbb{F}_p((t))$.

Then $| \ |$ is NORM + discrete.
+ K is complete (last lecture).

K/L is of finite degree.
Then $k/\mathbb{F}_p$ is also of finite degree (k = residue field).

Indeed. If $\bar{x}_1 \dots \bar{x}_n \in k$ are linearly independent$/\mathbb{F}_p$,

then $x_1, \dots, x_n \in K$ are linearly independent$/\mathbb{Q}_L$

where $x_1 \dots x_n$ are any lifts of $\bar{x}_1 \dots \bar{x}_n$ to K.

$\sum \lambda_i x_i = 0 \Rightarrow$ divide by λ_k with largest ~~smallest~~ $| \ |$.

we MAY assume $\lambda_k \not\equiv 0 \mod I$.
$\Rightarrow \sum \bar{\lambda}_i \bar{x}_i = 0$ is a nontrivial linear dependence.

5) Th: Let K be a local field. Then either K is a finite extension of $\mathbb{Q}_p$ or K is a finite extension of $\mathbb{F}_p((t))$.

Proof: Let $p = \operatorname{char} k > 0$ ($k = \mathcal{O}/I$ as usual)

Then $v(p) > 0$, where v = exponential valuation.

We have 2 cases: $\operatorname{char} K = 0$ & $\operatorname{char} K = p$.

A) $\operatorname{char} K = 0 \Rightarrow \mathbb{Q} \subseteq K. \Rightarrow \mathbb{Q}_p \subseteq K$ because $v(p) > 0$.

$v|_{\mathbb{Q}} \sim$ p-adic valuation

Then $K/\mathbb{Q}_p$ is algebraic. Why?
By Homework Assignment 4, $K/\mathbb{Q}_p$ is finite.

B) $\operatorname{char} K = p$. Then $K = k((t))$, $I = \langle t \rangle$, $\mathcal{O} = k[[t]]$.

Since every element in K can be written as $t^m(a_0 + a_1 t + \cdots)$

$k \cong \mathbb{F}_q$ $\qquad a_i \in \mathbb{F}_q = k$

(Proposition 4.4 in the book)

(this case is easier since we know $\mathbb{F}_q = k$)

6)

$U = \mathcal{O}^*$, $U^1 = 1 + I = \{x \in K^*, |1-x| < 1\}$ IV

$U^n = 1 + I^n = \{x \in K^*, |1-x| < 1/q^{n-1}\}$

Def: U^n = higher unit groups.

Proposition: $\mathcal{O}^*/U^n \cong (\mathcal{O}/I^n)^*$

(3.10 in the book) $U^n/U^{n+1} \cong \mathcal{O}/I \quad \forall n \geq 1.$

(sometimes U_n)

7) Th: Suppose K is local.

Then $K^* = (\pi) \times \mu_{q-1} \times U^1$,

where $(\pi) = \mathbb{Z}\pi$ (multiplicative) & $I = (\pi)$,

$q = |\mathcal{O}/I|$ and $U^1 = 1 + I$.

Proof: $\forall \alpha \in K^*$ we have $\alpha = \pi^n \cdot u \quad u \in \mathcal{O}^*$.

So $K^* = (\pi) \times \mathcal{O}^*$

$x^{q-1} - 1$ splits in k. So it splits in K.

By Hensel's lemma.

$\Downarrow$

$\mu_{q-1} \subset \mathcal{O}^*$.

Homomorphism $\mathcal{O}^* \to k^*$

$u \to u \bmod I$

has kernel U^1 & maps μ_{q-1} to k^* bijectively

(by Hensel lemma)

8) Let $K = \mathbb{Q}_p$.

Then: $U \cong \mu_{p-1} \times U_1$

Theorem: If $p > 2$, then $U \cong \mathbb{Z}_p \times \mu_{p-1}$.
If $p = 2$, then $U \cong \mathbb{Z}_2 \times \mu_2$.

9) Lemma: Take $x \in U_n - U_{n+1}$, $n \geq 1$ $(p > 2)$
$n \geq 2$ $(p = 2)$.
Then $x^p \in U^{n+1} - U^{n+2}$.

Proof: $x = 1 + \alpha p^n$ & $\alpha \not\equiv 0 \mod p$.

Then $x^p = 1 + \alpha p^{n+1} + \cdots + \alpha^p p^{np}$.

So $x^p \equiv 1 + k p^{n+1} \mod p^{n+2}$.

10) Lemma: If $p \neq 2$, then $U_1 \cong \mathbb{Z}_p$.
Proof:
Pick $\alpha \in U_1 - U_2$, e.g. $1 + p$. Then $\boxed{\alpha^{p^i} \in U^{i+1} - U^{i+2}}$.
Put $\alpha_n \in U_1 / U_n$ the image of U_n.
Then $(\alpha_n)^{p^{n-2}} \neq 1$ and $(\alpha_n)^{p^{n-1}} = 1$ (in U^n)

Remark: $|U_1 / U_n| = p^{n-1}$, because $U^n / U^{n+1} \cong \mathbb{F}_p$.

Thus $U_1 / U_n = \langle \alpha_n \rangle$. $\left(\begin{matrix} \mathbb{Z}/p^{n-1}\mathbb{Z} \to U_1/U_n \\ z \to \alpha_n \end{matrix} \right)$

$U_1 = \varprojlim \mathbb{Z}/p^{n-1}\mathbb{Z} \cong \varprojlim U_1 / U_n$

11) $p=2$

Take $\alpha \in U_2 - U_3$ $(\alpha \equiv 5 \bmod 8)$

$\mathbb{Z}/2^{n-2}\mathbb{Z} \cong U_2/U_n$ as above

This gives $\mathbb{Z}_2 \cong U_2$

But we have $U_1 \to U_1/U_2 \cong \mathbb{Z}/2\mathbb{Z}$

Then $U_1 = \mathbb{Z}/2\mathbb{Z} \times U_2$.

12)
Corollary:

$$\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \quad p \neq 2$$

$$\mathbb{Q}_2^* \cong \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}.$$

13) Theorem: K-local field, $q = p^f = |k|$.

A) If char $K=0$, then $K^* = \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$

$d = [K:\mathbb{Q}_p]$

B) If char $K>0$, then $K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \times \underbrace{\mathbb{Z}_p^{\mathbb{N}}}_{\text{mult}}$

$K \cong \mathbb{F}_q((t))$. MAL

14) Logarithm.

K as above. $\mathcal{O}$, I, U^n, $k = \mathcal{O}/I$.

Th. $\exists$ continuous homomorphism $\log : K^* \to K$ s.t. $\log p = 0$ and $\log(1+x) = x - x^2/2 + x^3/3 - \cdots$ $x \in I$

Proof: v is an extension of v_p on $\mathbb{Q}_p$.

$$p^{v_p(x)} > 1. \quad p^{v_p(n)} \leq n. \implies v_p(n) \leq \frac{\ln n}{\ln p}.$$

$$\Downarrow$$

$$n v_p(x) - v_p(n) = v_p\left(\frac{x^n}{n}\right)$$

$$\vee\!/$$

$$n \frac{\ln p^{v_p(x)}}{\ln p} - \frac{\ln n}{\ln p} = \frac{\ln\left(p^{n v_p(x)}/n\right)}{\ln p} \longrightarrow +\infty$$

$$\Downarrow$$

$\frac{x^n}{n}$ is a null sequence.

15) $\log((1+x)(1+y)) = \log(1+x) + \log(1+y)$

16) $\forall \alpha \in K^*$ we have

$$\alpha = \pi^{v(\alpha)} \omega(\alpha) u_\alpha \qquad u_\alpha \in U'$$

$$\langle \pi \rangle = I \qquad \omega(\alpha) \in \mu_{p-1}$$

$v \sim v_p$ $\quad$ $p = \pi^e \cdot \omega(p) \cdot u_p \quad u_p \in U'$ so $v = e v_p$ to preserve normalizatn of v.

So we can put $\log \pi = -\frac{1}{e} \log u_p$

$$\log \alpha = v(\alpha) \log \pi + \log u_\alpha$$

17) It is unique way! (If it is given by the above series)

If $\lambda : K^* \to K$ another log,

then $\lambda(\zeta) = \frac{1}{q-1} \lambda(\zeta^{q-1}) = 0 \quad \forall \zeta \in \mu_{q-1}$

$$0 = e\lambda(\pi) + \lambda(u_p) = e\lambda(\pi) + \log u_p$$

$$\Downarrow$$

$$\lambda(\pi) = \log \pi$$

$$\Downarrow$$

$$\lambda(\alpha) = \log \alpha. \quad \forall \alpha \in K^*$$

$\square$

18)

Th. Put $e^x = 1 + x + \frac{x^2}{2!} + \cdots$

Then it converges for $|x| < q^{-\frac{e}{p-1}}$

☆ $\left(v > \frac{e}{p-1}\right)$

$$I^n \underset{\log}{\overset{\exp}{\rightleftarrows}} U^n \qquad \text{(homomor.)}$$

$$n > \frac{e}{p-1}$$

Lemma: $n = \sum_0^r a_i p^i \quad 0 \le a_i < p \Rightarrow v_p(n!) = \frac{\sum_0^r a_i(p^i - 1)}{p-1}$

(Homework).

19) We have $U^1 = \varprojlim_n U^1/U^{n+1}$

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/q^n\mathbb{Z}$$

$$|U^1/U^n| = q^n$$

$\forall z \in \mathbb{Z}$ we have $(1+x)^z \in U^1 \Rightarrow U_1 = \mathbb{Z}$-module

Then U^1 is $\mathbb{Z}_p$-module (take limits).

$U' \ldots$ $\overline{X}$

20) K, $q = p^f$, char $K = 0$, π, I

Then $K^* = \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d$.

$d = [K : \mathbb{Q}_p]$ $a \geq 0$.

SKETCH: $K^* = (\pi) \times \mu_{q-1} \times U'$

$\log : U^n \to I^n = \pi^n \mathcal{O} \cong \mathcal{O}$ isomorphisms of $\mathbb{Z}_p$-modules.

Claim: $\mathcal{O} \cong \mathbb{Z}_p^d$ (Proposition 2.10 in PART I)
Recall $\mathcal{O}$ is an integral closure of $\mathbb{Q}_p$ in K.

$U' : U^n$ is of finite index.

Thus U' is a finitely generated $\mathbb{Z}_p$-module of RANK d. Then $U' \cong \mathbb{Z}_p^d \oplus$ TORSION PART

By MAIN th of modules.
(NOTE that $\mathbb{Z}_p$ is PID)

But torsion is cyclic.

$\Rightarrow$ TORSION is $\mathbb{Z}/p^a\mathbb{Z}$ for some $a \geq 0$