Local Fields

Jia Shi

Spring 2021

1 Local Fields notes- Jane Shi

1.1 Week 1 Day 1

Basic Theory

Example 1.1:
$f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ and $f(x_1, \ldots x_n) = 0$. Instead of solutions, you might want to find congruences. I.e. Take the poly $f(x_1, \ldots x_n)$ modulo $p, p^2, p^3, \ldots$.
This leads to the study of $p-$adic numbers, which are example of local fields. Local fields packages all of these information together.

1.2 Absolute values

Definition 1.1 (Absolute value): Let K be a field, and absolute value $|\cdot|$ on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that

- $|x| = 0 \iff x = 0$
- $|xy| = |x||y|$
- $|x + y| \leq |x| + |y|$

Now, compare absolute values to norms and metric. Metrics are more general than norm spaces, and norms are on vector spaces. So they are different in this sense. **norms induce a metric** on vector space. Normed spaces need to be on a vector space, whereas metric spaces can be on anyting.
Example: $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with usual absolute value where $|a + bi| = \sqrt{a^2 + b^2}$. We write $|\cdot|_\infty$.
Consider the trivial absolute value where

$$|x| = \begin{cases} 0 \text{ if } x = 0 \\ 1 \text{ if } x \neq 0 \end{cases}$$

If K is a finite field then its absolute value must be trivial. i.e. if $x^n = 1$ then say if $x = x^n$, so $|x| = |x^n| = |x|^n$. This means that absolute values on finite fields are boring and trivial.

Definition 1.2 (The p-adic absolute value):

for $0 \neq x \in \mathbb{Q}$, write $x = p^n \frac{a}{b}$ where $(a,p) = 1, (b,p) = 1$. Then the p-adic absolute value is as follows:

$$|x|_p = \begin{cases} 0 & \text{if } x = 0 \\ p^{-n} & \text{if } x = p^n \frac{a}{b} \end{cases}$$

Lemma 1.2 (p-adic absolute value is an absolute value):

1. clear
2. write out the equations
3. write out the equations

Note 3 gives you the ultrametric inequality, which is stronger than the triangle inequality.

Note that an absolute value induces a metric on the field K. Once you get a field, you get a topology.

Definition 1.3 (Equivalent absolute values): Let $|\cdot|, |\cdot|'$ be non-trivial absolute values on K. They are equivalent absolute values if they induce the same topology.

Definition 1.4 (Place): Equivalent classes of absolute values.

Proposition 1.3 (Three equivalent conditions for equivalent metric spaces):
TFAE:

1. $|\cdot|, |\cdot|'$ are equivalent
2. $|x| < 1 \iff |x|' < 1, \forall x \in K$
3. There exist $s \in \mathbb{R}_{\geq 0}$ such that $\forall x \in K$,

$$|x|^s = |x|'$$

Proof :

- $1 \to 2$:

$$\begin{aligned} |x| < 1 &\iff |x|^n \to 0 \\ &\iff (|x|)'^n \to 0 \text{ by the metric induced topology} \\ &\iff |x|' < 0 \end{aligned}$$

- $2 \to 3$

  3 being true implies that

$$s \log|x| = \log|x|'$$

  so that the ratio

$$\frac{\log|x|}{\log|x|'}$$

is constant. Going for contradiction. Suppose not. Then let $a, x \in K$ be two elements such that

$$\frac{\log|x|}{\log|x|'} < \frac{\log|a|}{\log|a|'}$$

therefore

$$\frac{\log|x|}{\log|a|} < \frac{\log|x|'}{\log|a|'}$$

Then there exists rational $\frac{m}{n}$ such that

$$\frac{\log|x|}{\log|a|} < \frac{m}{n} < \frac{\log|x|'}{\log|a|'}$$

then

$$n\log|x| < m\log|a|$$
$$m\log|a|' < n\log|x|'$$

so

$$|x|^n < |a|^m, |a|'^m < |x|'^n$$

so

$$|\frac{x^n}{a^m}| < 1, |\frac{x^n}{a^m}|' > 1$$

contradiction.

- $3 \to 1$ Open balls form a basis of topology. If there is an open ball it must be open in the other metric. So they are equivalent.

□

Note that $|\cdot|_\infty^2$ on $\mathbb{C}$ is not an absolute value by our definition.
In this course, we mainly are interested in non-archimedean absolute values.

Definition 1.5 (Non-archimedean): An absolute value is non-archimedean if

$$|x+y| \leq \max\{|x|, |y|\}, \forall x, y$$

For example $|\cdot|_\infty$ on $\mathbb{R}$ is archimedean, and $|\cdot|_p$ on $\mathbb{Q}$ is non-archimedean.

Example 1.4:
Our geometric intuition breaks down in non-archimedean norms. For example, all triangles are isosceles. But congruences are easier to study, unlike archimedean cases.

Lemma 1.5 (All triangles are isosceles):
Let $(K, |\cdot|)$ be a non-archimedean value field. Let $x, y \in K$. If $|x| < |y|$ then $|x-y| = |y|$

Proof :

$$|x-y| \leq \max\{|x|,|y|\} = |y|$$
$$|y| \leq \max\{|y-x|,|x|\} = |y-x|$$

□

Lemma 1.6 (Weird convergence in non-archimedean sequence):
Let $(x_n)_{n=0}^{\infty}$ a sequence on K and $|x_n - x_{n+1}| \to 0$ then x_n is cauchy. In particular, if K is complete then it converges.

Proof : For $\epsilon > 0$, choose N such that $\forall n > N, |x_n - x_{n+1}| < \epsilon$. Then for all m, n such that $N < n < m$ we have

$$|x_n - x_m| = |x_n - x_{n+1} + \ldots + x_{m-1} - x_m| < \epsilon$$

□

Example 1.7:
$K = \mathbb{Q}, p = 5, |\cdot| = |\cdot|_5$.
Consider the sequence $a_1 = 3, a_2 = 33, a_3 = 333, a_4 = 3333, \ldots$
We have $a_m \equiv a_n \pmod{5^n}$, $\forall m \geq n$. So $|a_m - a_n| \leq 5^{-n}, \forall m \geq n$. This is a cauchy sequence. But $a_n = \frac{1}{3}(10^n - 1)$ so $|a_n + \frac{1}{3}| = 5^{-n} \to 0$ as $n \to \infty$. So $a_n \to -\frac{1}{3}$ w.r.t $|\cdot|_5$.

Example 1.8:
We want to construct sequence $(a_n)_{n=1}^{\infty} \in \mathbb{Q}$ such that the following holds. This is a sequence that is cauchy in $5-$adic norm but also square converges to -1.

$$a_n^2 + 1 \equiv 0 \pmod{5^n}$$

$$a_n \equiv a_{n+1} \pmod{5^n}$$

Take $a_1 = 2$, suppose that a_n is already chosen, then write $a_n^2 + 1 = 5^n c$, $c \in \mathbb{Z}$, then

$$(a_n + b5^n)^2 + 1 = a_n^2 + 1 + 2 \cdot 5^n b a_n + 5^{2n} b^2 \equiv 5^n (c + 2a_n b) \pmod{5^{n+1}}$$

So c is picked. a_n is known. want to figure out b to make it possible. Indeed it is. we pickk $b \in \mathbb{Z}$ so $c + 2a_n b \equiv 0 \pmod 5$. This is possible since $(2a_n, 5) = 1$. So we pick $a_{n+1} = a_n + 5^n b$.
We know from construction it is cauchy. Now suppose $a_n \to L$, $L \in \mathbb{Q}$. Then

$$|L^2 + 1| \leq |L^2 - a_n^2| + |a_n^2 - 1| \to 0, n \to \infty$$

but this gives you a contradiction as $L^2 = -1$. So L not in $\mathbb{Q}$. So $(\mathbb{Q}, |\cdot|_5)$ is not complete.

Definition 1.6: The p-adic numbers $\mathbb{Q}_p$ are defined to be the completion of $\mathbb{Q}$ with respect to the $p-$adic metric $|\cdot|_p$.

There's an analogy: $\mathbb{Q}$'s completion w.r.t. $|\cdot|_\infty$ is $\mathbb{R}$. $\mathbb{Q}$'s completion w.r.t. $|\cdot|_p$ is $\mathbb{Q}_p$.

1.3 Lecture 2

Terminologies:
Let $(K, |\cdot|)$ be a non-archimedean valued field. For $x \in K$, and $r \in \mathbb{R}_{\geq 0}$, we can denote:

- $B(x,r) = \{y \in K \mid |x-y| < r\}$
- $\overline{B}(x,r) = \{y \in K \mid |x-y| \leq r\}$

Lemma 1.9 (Four funny properties of non-arch-val-fields):

1. If $z \in B(x,r)$, then $B(z,r) = B(x,r)$
2. If $z \in \overline{B}(x,r)$, then $\overline{B}(z,r) = \overline{B}(x,r)$
3. $B(x,r)$ is closed
4. $\overline{B}(x,r)$ is open

So open and closed balls don't have centers, and open balls are closed, and closed balls are open.

Proof :

1. Let $y \in B(x,r)$ then $|z-y| \leq \max\{|z-x|, |x-y|\} < r$ so $y \in B(x,z)$. So $B(x,r) \subseteq B(z,r)$. The other direction is done by reversing the roles of x, r.
2. Proven by changing $<$ to $\leq$ in the above.
3. Want to show that complement is open. We let $y \notin B(x,r)$. We claim that $B(y,r)$ is an open nbhd of y that does not intersect $B(x,r)$. Indeed if some $z \in B(y,r) \cap B(x,r)$ then $y \in B(y,r) = B(z,r) = B(x,r)$, so contradicting the two balls have empty intersection.
4. Let $z \in \overline{B}(x,r)$, then we will show that the ball $B(z,r)$ is a subset of $\overline{B}(x,r)$.

$$z \in B(x,r) \subseteq \overline{B}(z,r) = \overline{B}(x,r)$$

□

2 Valuation Rings

Remark 1: With a field with non-archimedean absolute value, you will get a very rich algebraic structure.

Definition 2.1 (Valuation): Let K be a field. A valuation on K is a function $V : K^\times \to \mathbb{R}$ such that

1. $V(xy) = V(x) + V(y)$
2. $V(x+y) \geq \min\{V(x), V(y)\}$

We fix $0 < \alpha < 1$, if V is valuation on K, then we get absolute value

$$|x| = \begin{cases} \alpha^{V(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

This determines a non-arch abs.val on K.

Conversely, a non-arch abs value on K determines a valuation $V(x) = \log_\alpha |x|$. Note there is no negative sign here!

Remark 2: Note that valuations and absolute-values are quite-equivalent. But a valuation is just more flexible and easier to use.

We also ignore trivial valuation $V(x) = 0$, $\forall x \in \hat{K}$. Say V_1, V_2 are equivalent if there exists $c \in \mathbb{R}_{\geq 0}$ such that $V_1(X) = cV_2(X)$, $\forall x \in K^\times$.

For example, $K = \mathbb{Q}$, define $v_p(x) = -\log_p |x|_p$ to be the $P-$adic valuation. SO the integer p has valuation 1.

Think about the $t-$adic valuation. (Note that something-adic, the something can be a prime p or an ideal I or the ideal (t).

Example 2.1 (t-adic):
Let k be a field. $K = k(t) = \text{Frac}(k[t])$ (rational functional field).

Then $V\left(t^n \frac{f(t)}{g(t)}\right) = n$ where f, g are polynomials such that $f(0) \neq 0 \neq g(0)$. This is called the $t-$adic valuation.

Example 2.2 (Laurent Series):

$$K = k((t)) = \text{Frac}(K[[x]]) = \left\{ \sum_{i=1}^{\infty} a_i t^i \mid a_i \in K, n \in \mathbb{Z} \right\}$$

be the formal Laurent series over K.
Then, we get the valuation

$$v\left(\sum_i a_i t^i\right) = \min\{i \mid a_i \neq 0\}$$

is the $t-$adic valuation K. Completion of rational fractional field.

Definition 2.2 (Valuation ring): Let $(K, |\cdot|)$ be non-archemedean valuation field, define the valuation ring of K, to be

$$\begin{aligned} \mathcal{O}_K &= \{x \in K \mid |x| \leq 1\} \\ &= \overline{B}(0,1) \\ &= \{x \in K^\times \mid V(x) \geq 0\} \cup \{0\} \end{aligned}$$

Proposition 2.3:

1. $\mathcal{O}_K$ is an open subring of K
2. the subsets
$$\{x \in K \mid |x| \leq r\}$$
and
$$\{x \in K \mid |x| < r\}$$
for $r \leq 1$, are open ideals in $\mathcal{O}_K$.
3.
$$\mathcal{O}_K^\times = \{x \in K \mid |x| = 1\}$$

Proof :

1. It is open because it's a closed ball. It's a subring, to check that $|0| = 0.|1| = 1$ so $0, 1 \in \mathcal{O}_K$.
Check closed under additive inverse:
$$x \in \mathcal{O}_K \implies |-x| = |-1||x| = |x| \leq 1, \text{ so } -x \in \mathcal{O}_K$$
Check closed under addition
$$x, y \in \mathcal{O}_K, |x + y| \leq \max\{|x|, |y|\} \leq 1 \implies x + y \in \mathcal{O}_K$$
Check closed under multiplication
$$x, y \in \mathcal{O}_K, |xy| = |x||y| \leq 1 \implies xy \in \mathcal{O}_K$$
2. They are open, yes. Them being ideals in $\mathcal{O}_K$ is a similar check than 1.
3. Note that for any x, $|x||x^{-1}| = 1$. So
$$|x| = 1 \iff |x^{-1}| = 1 \iff x, x^{-1} \in \mathcal{O}_K \iff x \in \mathcal{O}_K^\times$$
The third iff is that if $x, x^{-1} \in \mathcal{O}_K$, both them need to have abs values ≤ 1, but they reciprocals. (quick reminder $R^\times$ is the multiplicative subgroup.)

□

Proposition 2.4 (The maximal ideal of the valuation ring):
Denote the following
$$m = \{x \in \mathcal{O}_K \mid |x| < 1\}$$
a max ideal in $\mathcal{O}_K$. Then
$$K = \mathcal{O}_K/m$$
is the residue field.

Proof : If it were any bigger, then we have x with $|x| = 1 \in m$, then $x^{-1} \in m$, then $1 \in m$, then we get the whole thing. $\square$

Corollary 2.5 ($\mathcal{O}_K$ being a local ring with unique max ideal):
Note that $\mathcal{O}_K$ is a local ring (ring with a unique maximal ideal) with unique max ideal m.

Example 2.6 (Example of a valuation ring):
Let $K = \mathbb{Q}$ with $|\cdot|_p, \mathcal{O}_K = \mathbb{Z}_p = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}$ this is a valuation ring with $m = p\mathbb{Z}_p, K = \mathbb{F}_p$.

Definition 2.3 (discrete valuation): Let $V : K^\times \to \mathbb{R}$ be a valuation. Then $V(K^\times) \cong \mathbb{Z}$. We say V is a discrete valuation, and K is said to be discretely valued.

Definition 2.4 (Uniformizer): An element in $\mathcal{O}_K$ is said to be uniformizer is $V(\pi) > 0$ and $V(\pi)$ generates $V(K^\times)$. For example

- $K = \mathbb{Q}$ with $p-$adic valuation
- $K = k(t)$ with $t-$adic valuation.

Both of which are discrete valued fields.

Remark 3: If V is a discrete valuation, one can replace with equivalent one such that $V(K^\times) = \mathbb{Z}$. All such V normalize valuation, then $V(\pi) = 1 \iff \pi$ is a unit.

Lemma 2.7:
Let V be a valuation ring on K. TFAE:

1. V is discrete
2. $\mathcal{O}_K$ is PID (consider this the strongest argument)
3. $\mathcal{O}_K$ is Noethertian
4. m is principal

Proof :

- $1 \implies 2$: Suppose that V is discrete. Want to show that $\mathcal{O}_K$ is a pid. Need to show that it's an ID and it's principal.
  - It is an ID because K is a field and $\mathcal{O}_K \subseteq K$. So it must be an ID.
  - Now show it's principal. Let I be an ideal in $\mathcal{O}_K$. Then let $x \in I$ be an element that $v(x) = \min\{v(a) \mid a \in I\}$. The element $x \in I$ exists since V is discrete.

We claim that $x\mathcal{O}_k = I$. Note that $x\mathcal{O}_K = \{a \in \mathcal{O}_K \mid v(a) \geq x\}$ is equal to I.

* $x\mathcal{O}_K \subseteq I$: LHS is a smaller ideal than RHS. I is an ideal. So we are done
* $x\mathcal{O}_K \supseteq I$: Let $y \in I$, then $v(x^{-1}y) \geq 0$, so $0 \neq x^{-1}y \in \mathcal{O}_k$, so $y = x(x^{-1}y) \in x\mathcal{O}_K$. Note here we use the valuation ring definition: $V(x^{-1}y) \geq 0 \iff |x^{-1}y| < 1$.

- $2 \implies 3$ Clear, every ideal is finitely generated hence $\mathcal{O}_K$ have to be noetherian.
- $3 \implies 4$ since $\mathcal{O}_K$ is Noetherian, then it is finitely generated.

$$m = x_1\mathcal{O}_K + \ldots + x_n\mathcal{O}_K$$

WLOG $V(x_1) \leq \ldots \leq V(x_n)$.Then, $x_2, \ldots, x_n \in x_1\mathcal{O}_K$. But similarly to previous argument, each $x_i, i > 1$ we have $x_1^{-1}x_i \in \mathcal{O}_K$, so $x_i \in \mathcal{O}_K$ so $m = x_1\mathcal{O}_k$.

- $4 \implies 1$

Let $m = \pi\mathcal{O}_K$ for some $\pi \in \mathcal{O}_K$.

We will show that $v(K^\times) = v(\pi)\mathbb{Z}$.

Let $c = v(\pi)$. then, for all x s.t. $v(x) > 0$, we would have $x \in m$, then $v(x) \geq c$. (because $v(xy) \geq v(x) + v(y)$) Then, $V(K^\times) \cap (0, c) = \varnothing$. That is, the valuations of other items in the ideal m is either 0 or greater than c. But it' generated by c. Since $V(K^\times)$ is a subgroup of $(\mathbb{R}, +)$, we have $v(K^\times) = c\mathbb{Z}$. hence it is discrete.

□

2.1 Week 1 lecture 3

Let $(K, |\cdot|)$ be a non-archimedean value field. Then $\mathcal{O}_K\left[\frac{1}{x}\right] = K$, $\forall x \in m$. i.e. by taking the adjoint of the inverse of any element in the maximal ideal, you get back your original field. In particular, $K = \text{Frac}(\mathcal{O}_K)$

Definition 2.5 (DVR): A ring R is called a dicrete valuation ring if it is a PID and it has exactly one non-zero prime ideal. (necessarily maximal)

Compare this definition to the above TFAE conditions. This one is exactly the TFAE ones.

Lemma 2.8:

1. Let v be a discrete valuation on a field K. Then $\mathcal{O}_K$ is a DVR.
2. Let R be a DVR, then there exists a valuation v on $K = \text{Frac}(R)$ such that $R = \mathcal{O}_K$.

Proof :

1. To show that $\mathcal{O}_K$ is a DVR, it suffices to show that it is a PID and that it has exactly one non-zero prime ideal.
   (a) It is a PID by the previous lemma. i.e. V being discrete implies $\mathcal{O}_K$ is PID.
   (b) Remember in the inclusions of rings, PID is where prime ideals and maximal ideals coincide. It suffices to show it has exactly one non-zero max ideal. But by previous theory, we know $\mathcal{O}_K$ has a unique max ideal. Therefore, the proof is done.
2. Elements in R can be written uniquely

   Let R be a DVR with maximal ideal m. Since it's a PID let $m = (\pi)$. Since PIDs are also UFDs we can write $x \in R \setminus \{0\}$ uniquely as
   $$\pi^m u, u \in R^\times, m \geq 0$$
   For any $y \in K \setminus \{0\}$, we can write it uniquely as $\pi^n u, u \in R^\times, m \in \mathbb{Z}$ (up to multiplication by units?)

   Now define the valuation
   We define $v(\pi^m u) = m$. It is easy to check that v defines a valuation and $\mathcal{O}_K = R$.

□

Question: inside PIDs, max ideals and prime ideals coincide. How about outside of PIDs? Can you define similar notions for rings outside of PIDs?

Remark 4: Before, we are going from a field K, we made an absolute value on that field $|\cdot|_p$ on that field. With that absolute value, we also had an equivalent notion, which are negative-log, called valuations. Then, from that valuation, we made a ring called the $p-$adic integers. For this ring, we found a maximal ideal and a residue field. Also, the valuation is discrete.

Now, forgetting about the field, forgetting about the absolute value and the valuation, we now only have a ring that has two properties: being a PID and have exactly one non-zero prime ideal. Now, we are going to construct the field $K = \text{Frac}(R)$ and the valuation v, such that the similar construction, i.e. the valuation ring of K, $\mathcal{O}_K$ is equal to R.
This is quite interesting as we can go from

$$\text{Field} + \text{Valuation} \to \text{Ring} = \mathcal{O}_K$$

and we can go back from

$$\text{Ring} \to (\text{Field} + \text{Valuation}) \text{ such that } \mathcal{O}_K = R$$

Example 2.9:
$\mathbb{Z}_{(p)}, K[|t|]$ are DVRs (R is a field)

2.2 p-adic numbers

Recall that $\mathbb{Q}_p$ is a completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$. In Example sheet 1,we will show that $\mathbb{Q}_p$ is a field. $|\cdot|_p$ extends to $\mathbb{Q}_p$ and the associated valuation is discreet.

Definition 2.6 (Ring of p-adic integers): The ring of p-adic integers is valuation ring $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$.

Note that for a fact, $\mathbb{Z}_p$ is a DVR, maximal ideal $p\mathbb{Z}_p$ and non-zero ideals are given by $p^n\mathbb{Z}_p, n \geq 0$.

Proposition 2.10:
$\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$. In particular, $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ w.r.t. $|\cdot|_p$.

Remark 5:

1. $\mathbb{Q}_p$: The $p-$adic numbers. The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. This is quite mysterious because we haven't learnt any thing about it. (Imagine only knowing $\mathbb{Q}$ and defining $\mathbb{R}$ based on limits in $\mathbb{Q}$.) Many of them dont live in $\mathbb{Q}$.
2. $\mathbb{Z}_p$: The $p-$adic integers, $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$. Many of them dont live in $\mathbb{Z}$.
3. $\mathbb{Z}_{(p)}$: $\mathbb{Z}_p \cap \mathbb{Q}$, which is $\{x \in \mathbb{Q} \mid |x|_p \leq 1\}$. We know this is concrete because it lives in $\mathbb{Q}$.
4. $\mathbb{Q}$: we know it's concrete
5. $\mathbb{Z}$: we know it's concrete

Proof : We need to show that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

We just need to show the following inclusions

$$\mathbb{Z} \underset{\text{dense}}{\subseteq} \mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p \underset{\text{dense}}{\subseteq} \mathbb{Z}_p$$

- The right dense: We know $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. (By definition, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ w.r.t. $p-$adic). Since $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ is open (i.e. the close ball with absolute value ≤ 1), we know $\mathbb{Z}_p \cap \mathbb{Q}$ is dense in $\mathbb{Z}_p$.
- The left dense: What is $\mathbb{Z}_{(p)}$? it is

$$\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p = \left\{ \frac{a}{b} \mid \left| \frac{a}{b} \right|_p \leq 1 \right\} = \left\{ \frac{a}{b} \mid p \nmid b \right\}$$

  Now we want to show that we can create a sequence for any $\frac{a}{b} \in \mathbb{Z}_{(p)}$, where $a, b \in \mathbb{Z}, p \nmid b$. We can indeed make this sequence. For any $n \in \mathbb{N}$, we can pick $y_n \in \mathbb{Z}$ such that $by_n \equiv a \pmod{p}^n$. So $y_n \to \frac{a}{b}$ as $n \to \infty$.

In particular, we know that $\mathbb{Z}_p$ is complete because it's intersection of a closed ball and $\mathbb{Q}_p$. So $\mathbb{Z} \subseteq \mathbb{Z}_p$, is dense, so it is $\mathbb{Z}$s completion within $\mathbb{Q}_p$. □

Question: We know that $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$. But what are some elements that are in $\mathbb{Z}_p$ but not in $\mathbb{Q}$?

Here is an answer:
`https://math.stackexchange.com/questions/1583418/finding-an-example-of-a-non-rational-p-adic-number`
Note that the $p-$adic numbers encode information about higher dimensional power of p.

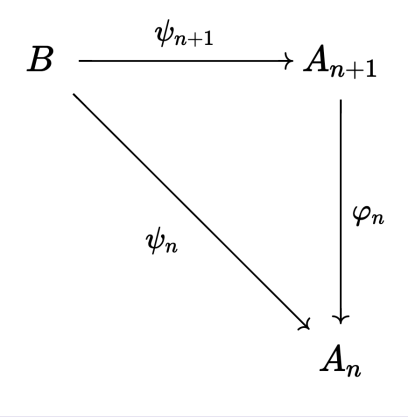
Definition 2.7 (Inverse limits): Let $(A_n)_{n=1}^{\infty}$ be a sequence of sets/groups/rings. Together with homomorphisms $\varphi_n : A_{n+1} \to A_n$, the transition maps.
Then the inverse limit of $(A_n)_{n=1}^{\infty}$ is the set/groups/rings:

$$\varprojlim_n A_n = \{(a_n) \in A_n \mid \varphi_n(a_{n+1}) = a_n\} \subseteq \Pi_{n=1}^{\infty} A_n.$$

Fact: if A_n is a group/ring, then $\varprojlim_n A_n$ is a group/ring. Define group/ring operations components.

Let $\Theta_m : \varprojlim_n A_n \to A_m$ denote the natural projection. Then the inverse limit satisfies the following universal property:

Proposition 2.11:
For any set/group/rings B together with homomorphism $\psi_n : B \to A_n$ such that the following commutes $\forall n$,



Then there exists a unique homomorphism

$$\psi : B \to \varprojlim_n A_n$$

such that $\Theta_m \circ \psi = \psi_m$.

Proof : Define $\psi : B \to \prod_{n=1}^{\infty} A_n$ by $b \mapsto \prod_{n=1}^{\infty} \psi_n(b)$.
Then $\psi_n = \varphi_n \circ \psi_{n+1} \implies \psi(b) \in \varprojlim_n A_n$.
The map is clearly unique, (determine by $\Theta_m \circ \psi = \psi_m$) and is a homomorphism (of sets/ groups/ rings).□

Definition 2.8 (I-adic completion, I-adic complete): Let $I \subseteq R$ be an ideal in a ring. Then we define the $I-$adic completion of R with respect to I to be the ring

$$\hat{R} = \varprojlim_n R/I^n$$

where $R/I^{n+1} \to R/I^n$ is the natural projection.
Note that there exists a natural map $R \to \hat{R}$ by universal property ($\exists$ maps $R \to R/I^n$). We say R is a I-adically complete if i is an isomorphism.
Fact: $\ker(i : R \to \hat{R}) = \bigcap_{n=1}^{\infty} I^n$

Proposition 2.12:
Now, let $(K, |\cdot|)$ be a non-archimedean valued field and let $\pi \in \mathcal{O}_K$ such that $|\pi| < 1$. Assume that K is complete w.r.t. $|\cdot|$.

- $\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n\mathcal{O}_K$ ($\mathcal{O}_K$ is $\pi-$adically complete)
- every $x \in \mathcal{O}_K$ can be written uniquely as $x = \sum_{i=0}^{\infty} a_i\pi^i$, $a_i \in A \subseteq \mathcal{O}_K$ is a set of cosets representation for $\mathcal{O}_K/\pi\mathcal{O}_K$.
  Moreover, any such power series $\sum_{i=0}^{\infty} a_i\pi^i, a_i \in A$ converges.

Proof : O_K is closed, and K is complete, this implies that $\mathcal{O}_K$ is complete.

- Show injectivity.
  Let $x \in$ the kernel. So $x \in \bigcap_{n=0}^{\infty} \pi^n\mathcal{O}_K$ implies that $\forall n, v(x) \geq nv(\pi)$. This implies that $x = 0$.
  Is it because $v(x) = -\log_\alpha(x)$? Because valuation is only defined for nonzero x.
  Hence $\mathcal{O}_K \to \varprojlim_n \mathcal{O}_K/\pi^n$ is injective.
- Show surjectivity.
  Let $(x_n)_{n=1}^{\infty} \in \varprojlim_n \mathcal{O}_K/(\pi^n\mathcal{O}_K)$ and for each n, let $y_n \in \mathcal{O}_K$ be a lift of $x_n \in \mathcal{O}_K/\pi^n\mathcal{O}_K$.
  Then, $y_n - y_{n+1} \in \pi^n\mathcal{O}_K$ so that $v(y_n - y_{n+1}) \geq nv(\pi)$.
  Thus $(y_n)_{n=0}^{\infty}$ is a cauchy sequence in $\mathcal{O}_K$. We let $y_n \to y \in \mathcal{O}_K$. Then y maps to $(y_n)_{n=0}^{\infty}$ in $\varprojlim_n \mathcal{O}_K/(\pi^n\mathcal{O}_K)$.
  Then $\mathcal{O}_K \to \varprojlim \mathcal{O}_K/\pi^n\mathcal{O}_K$ is surjective.

The proof for the second part is on example sheet, and it is quite similar. □

warning: if $(K, |\cdot|)$ is not discretely valued, then $\mathcal{O}_K$ is not necessarily m-adically complete.

Corollary 2.13:
K is as in part *ii* of the above proposition. Then every $x \in K$ can be written uniquely as $\sum_{i=-n}^{\infty} a_i\pi^i, a_i \in A$. Conversely, any such expression $\sum_{i=1}^{\infty} a_i\pi^i$ converges, defines an element in K.

Proof : Apply the second part of the previous theorem to $\pi^{-n}x, n \in \mathbb{Z}$, such that $\pi^{-n}x \in \mathcal{O}_K$.
Not quite get why this works? □

3 Local Fields notes- Jane Shi

3.1 Week 2 lecture 1

.

Corollary 3.1 (3.7):

1. $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ (Encoding congruences)
2. Every element $x \in \mathbb{Q}_p$ can be written uniquely as $\sum_{i=n}^{\infty} a_i p^i$ where $a_i \in \{0, 1, \ldots, p-1\}$

Proof :

1. Since we already know by the previous proposition, that $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}_p/p^n\mathbb{Z}_p$, it just suffices to show that $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$.

   Let $f_n : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ be the natural map. We will show that f is indeed the homomorphism that we use such that we have domain mod kernel equals the image.

   We have $\ker(f_n) = \{x \in \mathbb{Z} \mid |x|_p \leq p^{-n}\} = p^n\mathbb{Z}$.

   We now let $\bar{c} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ and $c \in \mathbb{Z}_p$ be a lift. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, $\exists x \in \mathbb{Z}$ such that $x \in c + p^n\mathbb{Z}_p$, which is a (closed but) open ball in $\mathbb{Z}_p$. Namely the ball $\overline{B}(c, p^{-n})$. Then $f_n(x) = \bar{c}$. This means that f_n is surjective.
2. It follows form the previous proposition (every x can be written uniquely...) using $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. ($\mathbb{Z}_p$ playing the role of $\mathcal{O}_k$ and $p\mathbb{Z}_p$ playing the role of $\pi\mathcal{O}_K$).

   For example, consider $\frac{1}{1-p} = 1 + p + p^2 + \ldots \in \mathbb{Q}_p$.

□

The above concludes the first part of the course, which is basic theory.
Now we go into complete valued fields.

4 Complete Valued Fields

4.1 Hensel's Lemma

Theorem 4.1 (Hensel's Lemma 4.1):
Let $(K, |\cdot|)$ be a complete, discretely valued field. Let $f(x) \in \mathcal{O}_K[x]$ and assume that there exists $a \in \mathcal{O}_K$ such that

$$|f(a)| < |f'(a)|^2$$

where the prime is the formal derivative. Then there exists unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and that $|x - a| < |f'(a)|$.

Remark 6 (A few ways to think of valuation and absolute values):

- Recall $v(x) = -\log_p |x|_p$
- How to think of π? we have $v(\pi) = 1$ so $1 = -\log_p |\pi|_p$, so $|\pi|_p = \frac{1}{p}$. So exactly one power of p divides π. So think of it as the integer p.
- Now, what is $\pi^{v(x)}$? Note that if $|x|_p = p^{-n}$ then

$$\pi^{v(x)} = \pi^{-\log_p |x|_p} = \pi^{-\log_p p^{-n}} = \pi^n$$

  where n is the biggest power of p dividing x.
- i.e. $v(x)$ is the biggest power of p dividing x.
- Intuition for the following proof: $r = v(f'(a))$ so working in π^{r+1} guarantees that $f'(a)$ is nonzero in this modulo.

The remark is that polynomials are quite likely to have solutions.

Proof : Let $\pi \in \mathcal{O}_K$ be a uniformizer. Let $r = v(f'(a))$, where v is normalized valuation, where $v(\pi) = 1$. We construct sequence $(x_n)_{n=1}^{\infty}$ in $\mathcal{O}_K$ such that

1. $f(x_n) \equiv 0 \pmod{\pi^{n+2r}}$ (getting closer and closer to the solution)
2. $x_n \equiv x_{n+1} \pmod{\pi^{n+r}}$ (guarantees the cauchiness)

The specific construction

Base Construction We take $x_1 = a$, then $f(x_1) = f(a)$. But

$$\begin{aligned} |f(a)| &< |f'(a)|^2 \\ \log|f(a)| &< 2\log|f'(a)| \\ 2v(f'(a)) &< v(f(a)) \\ 2r+1 = 2v(f'(a)) + 1 &\leq v(f(a)) \\ \pi^{2r+1} &\mid \pi^n \end{aligned}$$

Now if we raise π to their powers, we get π^{2r+1} is a factor of $\pi^{v(f(a))}$. But by our remark, that means it is π^n where n is the biggest power of p dividing x. Therefore, we have $f(a) \equiv 0 \pmod{\pi^{2r+1}}$. This proves the claim $f(a) \equiv 0 \pmod{\pi^{2r+1}}$.

Inductive construction

We make this sequence by using induction. Suppose that we have constructed $x_1, \ldots, x_n$ satisfying the two above. We define $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$.

Now we need to show that this construction works.

1. Show property 2 holds.
2. Since $x_n \equiv x_1 \pmod{\pi^{r+1}}$ then $v(f'(x_n)) = r$. The reason is as follows:

   Since $x_n \equiv x_1 \pmod{\pi^{r+1}}$, we have $f'(x_n) \equiv f'(x_1) \pmod{\pi^{r+1}}$. But we know $v(f'(x_1)) = v(f'(a)) = r$. So r is the biggest power that divides $f'(a)$. Note that $f'(a), f'(x_n)$ are equivalent π^{r+1}, so we know π^r divides $f'(x_n)$ as well but π^{r+1} cannot divide it. Hence $v(f'(x_n)) = r$.
3. Then, $\frac{f(x_n)}{f'(x_n)} \equiv 0 \pmod{\pi^{n+r}}$. This is because the biggest power dividing $f(x_n)$ is at least $n+2r$, and

the biggest power dividing $f'(x_n)$ is at most r. Therefore, the quotient is at least divisible by $n+r$.

4. So, property 2 holds.
$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$
It's because both $\frac{f(x_n)}{f'(x_n)} = x_{n+1} - x_n = 0$ modulo π^{n+r}.
5. Now show property 1 holds.
6. Consider a fact for general polynomials in general rings, this identity is like Taylor expansions.
7. Note that for X, Y inderterminants, you can write the following style
$$f(X+Y) = f_0(X) + f_1(X)Y + f_2(X)Y^2 + \dots$$
where each $f_i(x) \in \mathcal{O}_K[x]$.
Then we have $f_0(x) = f(x)$ and $f_1(x) = f'(x)$. (not quite sure why latter equality holds)
8. Thus that we can write
$$f(x_{n+1}) = f\left(x_n + \frac{-f(x_n)}{f'(x_n)}\right) = f(x_n) + f'(x_n)c + \underbrace{f_2(x_n)c^2 + \dots}_{\in \pi^{n+2r+1}\mathcal{O}_K}$$
where $c = \frac{-f(x_n)}{f'(x_n)}$. Note that the bracketed part is in $\pi^{n+2r+1}\mathcal{O}_K$ as $c \equiv 0 \pmod{\pi^{n+r}}$ and that $v(f_i(x_n)) \geq 0$, (they all lie in valuation ring $\mathcal{O}_K$), so we know they wont' make the power of each term any less.
9. Now we can reduce $\pmod{\pi^{n+2r+1}}$.
We have $f(x_{n+1}) \equiv f(x_n) + f'(x_n)c \equiv 0 \pmod{\pi^{n+2r+1}}$. So that 1 holds.

This proves the existence of the sequences with respect to property 1 and 2.
Note that the second property shows that (x_n) is Cauchy. Note that $x \in \mathcal{O}_K$, $\mathcal{O}_K$ is complete, so that $x_n \to x$. Then by continuity, $f(x) = \lim_{n\to\infty} f(x_n) = 0$ by (i). Moreover, ii implies that
$$a \equiv x_1 \equiv x_n \pmod{\pi^{r+1}}, \forall n$$
$$\implies a \equiv x \pmod{\pi^{r+1}}$$
So π^{r+1} divides $x - a$. But $|f'(a)| = r$. So p to the power of $x - a$ will be less than p to the power of $f'(a)$. This completes that construction:
$$|x - a| < |f'(a)|$$
Now we will show the uniqueness
Suppose that x' also satisfies $f(x') = 0$ where $|x' - a| < |f'(a)|$. We set $\delta = x' - x \neq 0$.
So we get $|x' - a| < |f'(a)|$, and $|x - a| < |f(a)|$. Then by ultrametric inequality $|\delta| = |x - x'| < |f'(a)|$.
But on the other hand $0 = f(x') = f(x+\delta) = f(x)^{=0} + f'(x)\delta + \underbrace{\delta^2 + \dots}_{|\cdot| \leq |\delta|^2}$ Hence $|f'(x)\delta| \leq |\delta^2|$ (again by ultrametric), so $|f'(x)| < |\delta|$.
But $x \equiv a \pmod{\pi^{1+r}}$.so $f'(x) \equiv f'(a) \pmod{\pi^{1+r}}$. But these residues are nonzero, as $v(f'(a)) = r$, so they have same absolute values. This means $|f'(x)| = |f'(a)|$. So $|f'(a)| = |f'(x)| < |\delta|$. This gives contradiction and proves uniqueness. $\square$

Definition 4.1 (Simple root): Simple root of a polynomial is a root with degree 1.

Corollary 4.2:
Let $(K, |\cdot|)$ be complete, discretely valued field. Let $f(x) \in \mathcal{O}_K[x]$ and $\bar{c} \in k := \mathcal{O}_K/m$ (the residue field). A simple root is a root of $\bar{f}(x) = f(x) \pmod{m}$ in $k[x]$.
Then there exists a unique $x \in \mathcal{O}_K$ such that $f(x) = 0$ and $x = \bar{c} \pmod{m}$.

Another way to say this is roots in the residue field lift to roots in the big field.

Proof : Let $c \in \mathcal{O}_k$ be any lift of $\bar{c}$. We will show that this c acts as the role of a in Hensel's lemma. Since c is a simple root, we know $|f(c)| < |f'(c)|^2 < 1$, as m is $\pi\mathcal{O}_k$ and $f(c)$ is zero mod π but $f'(c)$ is nonzero mod π due to the non-simpleness. This gives us a unique solution $x \in \mathcal{O}_K$..

□

Example 4.3:
Note that $f(x) = x^2 - 2$ has a simple root modulo 7, which is $\sqrt{2} \in \mathbb{Z}_7$.

Corollary 4.4 (Multiplicative structure of p-adic integers):
Consider units of the p-adic numbers:

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } p > 2 \\ (\mathbb{Z}/2\mathbb{Z})^3 & \text{if } p = 2 \end{cases}$$

Proof :

- Case $p > 2$

  Let $b \in \mathbb{Z}_p^\times$, apply the previous corollary to $f(x) = x^2 - b$, then we know that

  $$b \in (\mathbb{Z}_p^\times)^2 \iff \bar{b} \in (\mathbb{F}_p^\times)^2$$

  thus

  $$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 = \mathbb{Z}/2\mathbb{Z}$$

  The LHS equality is given by, consider the natural homomorphism, it works and is surjective. But roots in the RHS also lifts uniquely to roots in the LHS. The second equality is the multiplicative group of size $p-1$ vs the squares, which are ones of $(p-1)/2$.

  We have an isomorphism between

  $$\mathbb{Z}_p^\times \times \mathbb{Z} \cong \mathbb{Q}_p^\times$$

  given by

  $$(u, n) \mapsto up^n$$

Therefore,

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Not quite understanding the inequality here. If i expand it out, not sure about the quotient ring correspondence

- Case $p = 2$

  Let $b \in \mathbb{Z}_2^\times$. Consider $f(x) = x^2 - b$.

  Why are these groups different? Because $f'(x) = 2x \equiv 0 \pmod 2$. So, this polynomial, modulo 2, you won't find a simple root. Then we need the full strength of Hensel's lemma instead of just needing a corollary.

  Let $b \equiv 1 \pmod 8$. Recall $f(x) = x^2 - b$. Then

  $$|f(1)|_2 = |1^2 - b|_2 \leq 2^{-3} < |f'(1)|_2^2 = |2 \cdot 1|_2^2 = 2^{-2}$$

  Then Hensel's lemma implies that $f(x)$ has a root in $\mathbb{Z}_2$.

  This tells us that $b \in (\mathbb{Z}_p^\times)^2$ iff $b \equiv 1 \pmod 8$. I know b 1 mod 8 implies in the Zp2, but why does it in Zp2 imply it is 1 mod 8?

  Thus

  $$\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \cong (\mathbb{Z}/\mathbb{Z}_8)^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

  I dont get both of the equivalences Again using

  $$\mathbb{Q}_2^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}$$

  we find that

  $$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^3$$

□

Remark 7 (having solutions and reducing it modulo higher powers of uniformizer):
Consider question 7 in local fields example sheet 1
Usually two cases:

- Exists a simple root downstairs, then u lift it to a root upstairs using Hensel's lemma
- In the case that no roots exists, then think of

  $$\mathbb{Z}_p/\pi^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

  especially use $n = 1$. If there is a solution x downstairs, you can try to lift it by using $x + k$ where $k \in \pi^n\mathbb{Z}_p$. Then try to get a contradiction in the upper ring $\mathbb{Z}_p$ using the fact that $\mathbb{Z}_p$ is an integral domain. (so can divide by powers of p.) Another method is to show that in hensel's lemma, you can write such solution in as a cauchy sequence in $\mathcal{O}_k$ where $f(x_i) = 0 \pmod{\pi^{n+2r}}$ and $x_i \equiv x_{i+1} \pmod{\pi^{n+2r}}$. So this means we can examine solutions modulo π^k for $k > 1$.

Remark 8: Note that the proof uses $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ is the non-archimedean analogue of the Newton Rapsen method.

Theorem 4.5 (Hensel's lemma version 2):
Let $(K, |\cdot|)$ be a complete and discretely valued field. Let $f(x) \in \mathcal{O}_K[x]$. Suppose $\bar{f}(x) = f(x) \mod m$ in $k[x]$ (polynomial with coefficients in the residue field) can be factored as

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x), \text{ in } k[x]$$

with $\bar{g}, \bar{h}$ coprime, then there is a factorization (or a lift) $f(x) = g(x)h(x)$ in $\mathcal{O}_k[x]$ with $\bar{g}(x) \equiv g(x) \mod m$ and $\bar{h}(x) \equiv h(x) \mod m$ and $\deg g = \deg \bar{g}$.

Proof : See example sheet. □

4.2 Week 2 lecture 2

Corollary 4.6 (A cor of the second ver Hensel's lemma):
Let $f(x) = a_n x^n + \ldots + a_0 \in K[x]$.
Note that $(K, |\cdot|)$ is a complete, discretely valued field. With $a_0, a_n \neq 0$. If $f(x)$ is irreducible, then

$$|a_i| \leq \max\{|a_0|, |a_n|\}, \forall i$$

Proof : Upon scaling, we can say $f(x) \in \mathcal{O}_k$ with $\max|a_i| = 1$. So we wish to show that either it's a_0 or a_n that satisfies that max absolute value. If not, let r be a minimal value such that $|a_r| = 1$. Then $0 < r < n$. We then have modulo the maximal ideal m (recall maximal ideal are elements in $\mathcal{O}_k$ with $|x| < 1$ so the terms below r disappear.)
Thus we have

$$\bar{f}(x) = x^r(a_r + \ldots + a_n x^{n-r}) \mod m$$

note that $a_r \neq 0$ because we are taking mod m.This is reducible, with two polynomial factors coprime. Then the theorem 4.4 (second version of Hensel) implies that this lifts to a solution $f(x) = g(x)h(x)$ in $\mathcal{O}_K[x]$, with $0 < \deg g < n$. This is a contradiction as f is irred. □

5 Teichmüller Lifts

Intuition behind Teichmüller lifts: earlier we see that we can write integers in $\mathbb{Q}_p$ as a laurent series, where each of the coefficients is a lift, by taking a representative of cosets $\mathcal{O}_K/(\pi^n\mathcal{O}_k)$, i.e. the $0, 1, 2, \ldots p-1$. They are the natural lift. But they are actually not natural? they don't preserve the additive and multiplicative structure. So we want a lift that does that.

Definition 5.1 (Perfect ring): A ring R of characteristic $p > 0$ (p prime) is a perfect ring if the Frobenius $x \mapsto x^p$ is a bijection. A field of char p is a perfect field if it is a perfect as a ring.

Remark 9: Since $charR = p$, we have $(x + y)^p = x^p + y^p$ so that the Frobenius map is a ring homomorphism.

Example 5.1:

1. $\mathbb{F}_{p^n}, \bar{\mathbb{F}}_p$ are perfect fields
2. $\mathbb{F}_p[t]$ is not perfect because $t \notin Im(frob)$
3. $\mathbb{F}_p(t)$ is not perfect but
$$\mathbb{F}_p(t^{1/p^\infty}) = \mathbb{F}_p(t, t^{1/p}, t^{1/p^2}, \ldots)$$
is perfect. It is the perfection of $\mathbb{F}_p(t)$.

A fact: a field K of char $p > 0$ is perfect if and only if any finite extension is separable. (separable: if min poly for any element in field is separable).
Think of perfection as: given non-perfect field, we throw in all possible separable field extensions.

Theorem 5.2:
$(K, |\cdot|)$ be complete, discrete valued field. such that its residue field $k : \mathcal{O}_K/m$ is perfect of char p. then there exists unique map

$$[-] : k \mapsto \mathcal{O}_k$$

such that

1. $a \equiv [a] \mod m, \forall a \in K$
2. $[ab] = [a][b], \forall a, b \in K$

So we say it preserves algbraic structure. If $\operatorname{char} K = p$, then $[-]$ is a ring homomorphism. i.e. in generally, addition is NOT reserved. But in the special case, when the char of big field K is p, you get your addition preserved.

Lemma 5.3:
Let $(K, |\cdot|)$ be as in the theorem. Fix $\pi \in \mathcal{O}_K$ be a uniformizer. Let $x, y \in \mathcal{O}_K$. Suppose that

$$x \equiv y \mod \pi^k (k \geq 1)$$

we get

$$x^p \equiv y^p \mod \pi^{k+1}$$

Proof : Let $x = y + u\pi^k$ with $u \in \mathcal{O}_k$. Then

$$x^p = (y + u\pi^k)^p = \sum_{i=0}^{p} \binom{p}{p-i} y^{p-i} (u\pi^k)^i = y^p + \sum_{i=1}^{p} \binom{p}{p-i} y^{p-i} (u\pi^k)^i$$

Since $\mathcal{O}_K/\pi\mathcal{O}_K$ has characteristic p, we have $p \in \pi\mathcal{O}_K$. Thus $\binom{p}{p-i} y^{p-i} (u\pi^k)^i \in \pi^{k+1}\mathcal{O}_K, \forall i \geq 1$. Hence $x^p \equiv y^p \mod \pi^{k+1}$. □

Proof (Now proof of the theorem): The proof idea is to take roots downstairs, lift it upstairs, and then power it back. Then you claim this sequence converges to the lift you want. Note that this lift is not natural and really troublesome, but what's good about it is that it preserves algebraic structure.
Let $a \in K$. For each $i \geq 0$, we pick a lift $y_i \in \mathcal{O}_k$ of a^{1/p^i}. Note that a^{1/p^i} exists because the field is perfect. (not familiar w perfect fields)
We define $x_i = y_i^{p^i}$. We claim that $(x_i)_{i=0}^{\infty}$ is a cauchy sequence and its limit $x_i \to x$ is independent of the choice of y_i.
By the construction, we have $y_i \equiv y_{i+1}^p \mod \pi$. (taking both to power p^i gives $a \equiv a$? not sure why they are equal.)
By previous lemma and induction on r we have

$$y_i^{p^r} \equiv y_{i+1}^{p^{r+1}} \mod \pi^{r+1}$$

and hence $x_i \equiv x_{i+1} \mod \pi^{i+1}$, take $(r = i)$.
This implies (x_n) is cauchy so $x_i \to x \in \mathcal{O}_K$ as $\mathcal{O}_K$ is complete.
Now show that it is independent of choice of y_is.
Suppose that $(x_i')_{i=1}^{\infty}$ arises from another choice of y_i' lifting a^{1/p^i}, then get (x_i') is also cauchy and

$x_i' \to x' \in \mathcal{O}_K$.

Now we consider a third sequence

$$x'' = \begin{cases} x_i & i \text{ even} \\ x_i' & i \text{ odd} \end{cases}$$

then x_i'' arise from lifting $y_i'' : \begin{cases} y_i & i \text{ even} \\ y_i' & i \text{ odd} \end{cases}$
then apply the previous argument of cauchiness again, we show that x'' is cauchy as $x'' \to x, x'' \to x'$, this implies $x = x'$. hence x is independent of the y_is. We denote $[a] = x$.
(That is, if you have another converging sequence, you can build an alternating sequence, which also satisfies cauchyness, so it converges to both limits, so both limits are same.)
Then we get

$$x_i = y^{p^i} \equiv (a^{1/p^i})^{p^i} \equiv a \mod \pi$$

so $x \equiv a \mod \pi$ hence 1 is satisfied.
Now we show 2 We let $b \in k$ and we choose $u_i \in \mathcal{O}_k$, a lift of b^{1/p^i}, let $z_i = u_i^{p^i}$. Then $\lim_{i\to\infty} z_i = [b]$.
Now $u_i y_i$ is a lift of $(ab)^{1/p^i}$, hence

$$[ab] = \lim_{i\to\infty} x_i z_i = \lim_{i\to\infty} x_i \lim_{i\to\infty} z_i = [a][b]$$

(I think the reason why you're allowed to distribute limit is due to something on example sheet.) This means 2 is satisfied.

Big field char p, get a ring hom:
Now we will show the addition is satisfied in char $K = p$ where K is the big field.
If char $K = p$, $y_i + u_i$ is a lift of $a^{1/p^i} + b^{1/p^i} = (a+b)^{1/p^i}$. Then

$$\begin{aligned} [a+b] &= \lim (y_i + u_i)^{p^i} \\ &= \lim y_i^{p^i} + u_i^{p^i} \\ &= \lim x_i + z_i \\ &= [a] + [b] \end{aligned}$$

It is easy to check $[0] = 0, [1] = 1$ so $[-]$ gives you a ring homomorphism.
uniqueness of the $[-]$
We still need to check uniqueness. Say we have another lifting satisfying the multiplicative property. Let $\phi : k \to \mathcal{O}_K$ be another such map. Then for $a \in k, \phi(a^{1/p^i})$ is a lift of a^{1/p^i}. It follows that

$$[a] = \lim \phi(a^{1/p^i})^{p^i} = \lim \phi(a_i) = \phi(a)$$

The LHS equality comes from that we know it's a lift (so by previous argument we know it must converge to $[a]$). The second equality is the multiplicative property of ϕ. □

Example 5.4:
If $K = \mathbb{Q}_p$, $[-] : \mathbb{F}_p \to \mathbb{Z}_p$, $a \in \mathbb{F}_p^\times, [a]^{p-1} = [a^{p-1}] = [1] = 1$. So $[a]$ is a $p-1$ root of unity.

Lemma 5.5:
$(K, |\cdot|)$ a complete discretely valued field. Then if $k : \mathcal{O}_K/m \subseteq \overline{\mathbb{F}_p}$, then $[a] \in \mathcal{O}_K$ is a root of unity.

Proof : $a \in K$ implies that $a \in \mathbb{F}_{p^n}$ for some n (is it because the closure of $\mathbb{F}_p$ is $\mathbb{F}_{p^n}$ for some n). Then

$$[a]^{p^n-1} = [a^{p^n-1}] = [1] = 1$$

□

Theorem 5.6:
Let $(K, |\cdot|)$ be a complete, discretely valued field. with $\operatorname{char} K = p > 0$. Assume k is perfect, then $K \cong k((t))$. (the field of formal laurent series)

Proof : Since $K = \operatorname{Frac} \mathcal{O}_K$, it suffices to show $\mathcal{O}_K \cong K[[t]]$. This is formal power series as rings.
For $\pi \in \mathcal{O}_K$ be uniformizer, let

$$[-] : k \to \mathcal{O}_k$$

be the Teichmüller lift.
Define

$$\phi : k[[t]] \to \mathcal{O}_k$$

by

$$\phi(\sum_{i=0}^{\infty} a_i t^i) = \sum_{i=0}^{\infty} [a_i]\pi^i$$

ϕ if a ring homomorphism beacuse Teichmüller is, and it is a bijection by prop 2.2. □

5.1 Week 2 lecture 3

6 Extensions of complete valued fields

The following is a big theorem that would take 1-2 lectures

Theorem 6.1 (Extension of complete valued field theorem):
Given a $(K, |\cdot|)$, complete, discretely valued field and L/K a finite extension of degree n then

- $|\cdot|$ extends uniquely to an absolute value on L $|\cdot|_L$ defined by

$$|y|_L = |N_{L/K}(y)|^{1/n}, \forall y \in L$$

- L is complete w.r.t.$|\cdot|_L$

Remark 10: Some basic facts:

- L/K finite, and $N_{L/K} : L \to L$ defined by

$$N_{L/K}(y) = \det_k(mult\ y)$$

  where $mult\ y : L \to L$ is the k linear map of multiplication by y.

- $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$
- $N_{L/K}(x) = 0 \iff x = 0$

This proof is mainly two parts, the first is uniqueness and the second is completeness.

Definition 6.1 (Norm on a $(K, |\cdot|)$, equivalent norms): Same old norm with a ultrametric $\triangle$ ineq. Same old definitioin on equivalent norms. Also note that equivalent norms induce the same topology.

Proposition 6.2 (Vec spaces are complete via sup norm):
Let $(K, |\cdot|)$ be complete and non-arch. Then let V be a finite dimensional vector space over K. Then V is complete w.r.t. $\|\cdot\|_\infty$.

Proof : Idea is if a sequence is cauchy over V then each position converges in K and V is complete w.r.t. sup norm. □

Theorem 6.3:
$(K, |\cdot|)$ complete, non-arch. V be a f.d.v.s. over K. then any two norms on V is equivalent. In particular V is complete w.r.t. any norm.

Proof : Proof idea is to show that any norm is equivalent to $\|\cdot\|_\infty$.
For D, i.e. $\|x\| \leq D\|x\|_\infty$, $D = \max_i \|e_i\|$ suffices.

For C, we need induction. The $C\|x\|_\infty < \|x\|$. For $n = 1$ we get $\|e_i\|$. For $n > 1$, use the construction $V_i = \text{Span}\{e_1, \ldots, \hat{e_i}, \ldots, e_n\}$. Take $S = \bigcup_{i=1}^n e_i + V_i$. Pick some interesting c such that $B(0, C)$ does not intersect S.

□

Lemma 6.4:
Let $(K, |\cdot|)$ be nonarchimedean valued field, then $\mathcal{O}_K$ is integrally closed in K. (proof is just some expansion of monic poly.)

Lemma 6.5:
$\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ over L.

Now we are ready to prove the big theorem 6

Proof : First two axioms are just quick expansions.
But for the third axiom (ultrametric), we had to define what it means for a super ring to be integral over subring. Show that $R \subseteq S$ are rings then $R^{\int(S)}$ is integrally closed in S.
We need the two lemmas above, and then we could use the fact that $\mathcal{O}_L$ is a ring. fill in the proof later.

□

7 Local Fields notes- Jane Shi

7.1 Week 3 lecture 1

.

Lemma 7.1:
$\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.

Proof : Proof not quite 100 % understand, should revisit. Requires quite a lot of previous theorems/lemmas.□

$(K, |\cdot|)$ is complete, non-archimedean, and discretely valued. We get a family of corollaries.

Corollary 7.2:
Let L/K be a finite extension. Then

- L is discretely valued w.r.t. $|\cdot|_L$
- $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.

Proof : Fill it in. One follows from a lemma and another is just using the definition of the extension of norm. □

Corollary 7.3:
Let $\overline{K}/K$ be the algebraic closure. Then $|\cdot|$ extends uniquely to an absolute value $|\cdot|_{\overline{K}}$ on $\overline{K}$.

Proof : Just requires the uniqueness coming from the big theorem. Also requires to check that the axioms are met. □

Remark 11: Warning: $|\cdot|_{\overline{K}}$ is actually never discrete as it joins roots of the uniformizers. Note that it is actually also not complete. i.e. $\overline{\mathbb{Q}_p}$ is not complete with respect to $|\overline{\mathbb{Q}}_p|$. But $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}_p}$ and $\mathbb{C}_p$ is algebraically closed.

Proposition 7.4:
Let L/K be a finite extension of complete, discretely valued fields. Assume that

- $\mathcal{O}_k$ is compact
- the extension $k_{L/K}$ of residue is finite and separable.

Then there exists $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

Proof : review separability
The proof scheme is as follows:

- Separable implies $\exists, \overline{\alpha} \in k_L$ such that $K_L = k(\overline{\alpha})$
- pick $\alpha \in L$ a lift of $\overline{\alpha}$
- fix a uniformizer $\pi_l \in \mathcal{O}_L$
- Show that the valuation $V_L(g(\alpha)) = 1$ by taking a lift. How to take a lift? pick any lift $\overline{\alpha}$. Uniformizers are those who can be divided by at most one copy of π_L. If it is 0 in π_L^2, then we can do $g(\alpha + \pi_L)$ so it is no longer in 0 modulo π_L^2.
- use a polynomial argument to show that $\mathcal{O}_k[\alpha]$ is compact, hence closed
- Get coset representatives, and give $y \in \mathcal{O}_L$ arbitrary, using the closed-ness to show $y \in \mathcal{O}_k[\alpha]$.

Not quite understanding the proof! □

7.2 Week 3 lecture 2

8 III. Local Fields

Definition 8.1 (Local field): Let $(K, |\cdot|)$ be a valued field. K is a local field if it is complete and locally compact. Locally compact at point x implies that there exists an open neighbourhood U of x such that U sits inside some compact subset.

Proposition 8.1:
Let $(K, |\cdot|)$ be a non-arch complete valued field. TFAE:

- K is locally compact
- $\mathcal{O}_K$ is compact
- V is discretely valued. and that the residue field $k := \mathcal{O}_K/m$ is finite.

Example 8.2 (Two examples of local fields):
Heard that there're only two nontrivial examples?

- $\mathbb{Q}_p$ is a local field
- $\mathbb{F}_p((t))$ is a local field

Definition 8.2 (Profinite topology): Assume A_n are finite. Then the profinite topology on $A : \varprojlim_n A_n$ is the weakest topology on A such that $A \to A_n$ is cnotinuous $\forall n$, where A_n is equipped with the discrete topology.

Fact: that $A := \varprojlim_n A_n$ with profinite topology is compact, totally disconnected, and Hausdorff.

Proposition 8.3:
Let K be a non-archimedean local field under isomorphism

$$\mathcal{O}_k \cong \varprojlim_n \mathcal{O}_k/\pi^n\mathcal{O}_k$$

where π is a uniformizer. Then the topology on $\mathcal{O}_K$ coincides with the profinite topology.

Proof : One checks that the sets

$$B = \{a + \pi^n\mathcal{O}_k \mid n \in \mathbb{Z}_{\geq 1}, a \in \mathcal{O}_k\}$$

is a basis of open sets in both topologies. In $|\cdot|$, they are clear. In profinite top, consider the projection, which is continuous.

□

Lemma 8.4:
Let K be a non-archimedean local field. L/K is a finite extension, then L/K is also a local field.

Proof : Idea: show that it is finitely generated module over the residue field in K □

Definition 8.3 (Characteristics of local fields): A non-archimedean valued field $(K, |\cdot|)$ has equal characteristic if $\text{char}(K) = \text{char}(k)$. Otherwise it has mixed characteristic. i.e. $\mathbb{Q}_p$ has mixed characteristic while $\mathbb{F}_p((t))$ has equal characteristic.

Theorem 8.5 (Non-archimedean local fields of equal char):
K be a non-arch local field of equal char $p > 0$, then

$$K \cong \mathbb{F}_{p^n}((t))$$

Proof : Main idea is from $k = \mathbb{F}_{p^n}$ being finite hence perfect. Then you use the Teichmuller lift. fill in □

Lemma 8.6 (non-archimedean abs value):
An absolute value on a field K is non-archimedian iff $|n|$ is bounded $\forall n \in \mathbb{Z}$.

9 Week 3 lecture 3

Theorem 9.1 (Ostrowski's lemma):
Any nontrivial abs value on $\mathbb{Q}$ is either equivalent to either the absolute value $|\cdot|_\infty$ or the $p-$adic absolute value $|\cdot|_p$ for some prime p.

Proof :

- When $|\cdot|$ is archimedean. In this case, fix an integer $b > 1$ such that $|b| > 1$. Let a be another integer > 1, and write b^n in base a. Then using some bounds and some logarithms, you are able to to get a λ as a ratio of logs. Then switch logs you get that they are equivalent to $|\cdot|_\infty$.
- When $|\cdot|$ is non-archimedean. Pick n such that $|n| < 1$, and decompose n into prime factors. Claim exactly one of those primes have abs < 1. If for contradiction, another prime also does, then use relatively prime to obtain contradiction

□

Theorem 9.2 (Non-arch, local field of mixed char):
Let $(K, |\cdot|)$ be a non-arch, local field of mixed char, then K is a finite extension of $\mathbb{Q}_p$. (For some prime p.)

Proof :

- Since by earlier defns and theorems, we know it's an extension, we just need to show finite extension
- $\mathcal{O}_k/p\mathcal{O}_k$ is finite. it's a fin diml v.s. over $\mathbb{F}_p$. Then pick coset representatives and build something
- Then let $y \in \mathcal{O}_k$, can write as an infinite sum, but rearranging shows the elements of sum in $\mathbb{Z}_p$. So $\mathcal{O}_k$ is finite over $\mathbb{Z}_p$.

□

In summary, if K is a local field, then there are only three options

1. archimedean: $K \cong \mathbb{R}, \mathbb{C}$.
2. non-arch, equal char: $K \cong \mathbb{F}_{p^n}((t))$.
3. non-arch, mixed char: K is a finite extension $\mathbb{Q}_p$.

9.1 Global Fields

Definition 9.1 (Global field): A global field is either

- an algebraic number field
- a global function field i.e. a finite extension of $\mathbb{F}_p(t)$.

Lemma 9.3:
Let $(K, |\cdot|)$ be complete, discrete value field. L/K a finite Galois extension with $|\cdot|_L$ extending $|\cdot|$. Then for $x \in L$, $\sigma \in \mathrm{Gal}(L/K)$, we have $|\sigma(x)|_L = |x|_L$.

Proof : one-liner □

Lemma 9.4 (Krasner's Lemma):
Let $(K, |\cdot|)$ be a complete discretely valued field. Let $f(x) \in K[x]$ be a separable, irreducible, poly with $\alpha_1, \ldots, \alpha_n \in \overline{K}$. Then suppose $\beta \in \overline{K}$ with $|\beta - \alpha_1| < |\beta - \alpha_i|$ for $i = 2, 3, \ldots, n$. Then $K(\alpha_1) \subseteq K(\beta)$.

Proof : not complicated but requires some galois extension properties. □

Proposition 9.5 (Nearby polynomials define same extensions):
$(K, |\cdot|)$ a complete, discretely valued field. $f(x) \in \mathcal{O}_k[x]$ separable, monic, and irreducible. Fix $x \in \overline{K}$, a root of f, pick $\epsilon > 0$ such that for any $g(x) \in \mathcal{O}_k[x]$ monic, with $|a_i - b_i| < \epsilon$ same degree, there exists a root β of $g(x)$ such that $K(\alpha) = K(\beta)$.

Proof : more complicated, uses Hensel's and Krasner's. □

10 Week 4 Lecture 1

Theorem 10.1 (8.5):
Let K be a local field. Then, K is the completion of a global field.

11 Dedekind domains

The idea of dedkind domain is that it's the global setting of a DVR.

Definition 11.1 (Dedekind domain): It's a ring R such that

- R is a Noetherian integral domain
- R is integrally closed in $\mathrm{Frac}(R)$
- Every nonzero prime ideal is maximal

FOr example, any PID hence DVR is a dedekind domain. THe ring of integers in a number field is also one.

Theorem 11.1 (9.2. Main theorem of this lecture):
A ring R is a DVR $\iff$ R is a Dedekind domain with exactly one nonzero prime ideal.

Lemma 11.2 (9.3):
Let R be Noetherian, and $I \subseteq R$ nonzero ideal. Then there exists nonzero prime ideal $p_1, \ldots, p_r \subseteq R$ such that $p_1 p_2 \ldots p_r \subseteq I$.

Lemma 11.3 (9.4):
Let R be an ID which is integrally closed in $K = \mathrm{Frac}(R)$. Let $I \subseteq R$ be a non-zero finitely generated ideal and $x \in K$. Then if $xI \subseteq I$, we have $x \in R$.

Definition 11.2 (Multiplicative sets and localization): Two faces:

- R noetherian implies $S^{-1}R$ noetherian
- there exists bijection between prime ideals in $S^{-1}R$ and prime ideals $p \in R$ such that $p \cap S = \varnothing$.

Corollary 11.4:
Let R be a dedekind domain. $P \subseteq R$ is a prime ideal. Then $R_{(p)}$ is a DVR.

11.1 Week 4 lecture 2

Definition 11.3 (9.6): If R is a dedekind domain, $P \subseteq R$, a nonzero prime ideal, write v_p for normalized valuation on $\mathrm{Frac}(R) = \mathrm{Frac}(R_{(p)})$ corresponding to the DVR $R_{(p)}$.

Proposition 11.5 (Factorization property for ideals):
Let R be a dedkind domain. Then every nonzero ideal $I \subseteq R$ can be written uniquely as a product of prime ideals. $I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$. with the $\mathfrak{p}$s distinct.

12 Dedekind domains and extensions

If L/K is separable of degree n and $\sigma_1, \dots, \sigma_n : L \to \overline{K}$ denote the set of embeddings of L into algebrac closure of R. Then $Tr_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$.

Lemma 12.1 (10.1. Big theorem of the lecture):
Let L/K be a finite separable extension of fields. Then the symmetric bilinear pairing

$$(\bullet, \bullet) : L \times L \to R$$

$$(x, y) \mapsto Tr_{L/K}(xy)$$

is non-degenerate.

Lemma 12.2 (10.2):
Let $\mathcal{O}_k$ be a dedekind domain and L a finite separable extension of $k := \mathrm{Frac}\, \mathcal{O}_k$. Then the integral closure $\mathcal{O}_L$ of $\mathcal{O}_k$ in L is a dedekind domain.

Proof : a relatively long proof. related to example sheets □

Corollary 12.3 (10.3):
The ring of integers of number field is a Dedekind domain.

12.1 Week4 lecture 3

Some background info: Let $\mathcal{O}_k$ be a dedekind domain with $k = \mathrm{Frac}(\mathcal{O}_k)$. L/K a finite separable extension. $\mathcal{O}_L \subseteq L$ integral over $\mathcal{O}_K$ in L, be as in theorem 10.2.
Then

Lemma 12.4 (10.4.):
let $0 \neq x \in \mathcal{O}_k$. Then

$$(x) = \prod_{p \neq 0, p \text{ prime}} \wp^{V_p(x)}$$

Remark 12 (Notation): If $\mathcal{P} \subseteq \mathcal{O}_L$, $\wp \subseteq \mathcal{O}_K$ are prime ideals, then

$$\mathcal{P} \mid \wp$$

if $\wp\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$ and $\mathcal{P} \in \{\mathcal{P}_1, \dots, \mathcal{P}_r\}, e_r > 0$.

Theorem 12.5 (10.5.):
Let $\mathcal{O}_K, \mathcal{O}_L, K, L$ as above, for $\wp$ a nonzero prime ideal of $\mathcal{O}_K$. If we can write

$$\wp\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}, e_i > 0$$

then the absolute value on L extending $|\cdot|_\wp$ up to equivalence are precisely $|\cdot|_{\mathcal{P}_1}, \dots, |\cdot|_{\mathcal{P}_r}$

Corollary 12.6 (Classification of abs value on number fields):
Let K be a number field with ring of integers $\mathcal{O}_K$. Then any absolute value on K is equivalent to

- $|\cdot|_\wp$ for some non-zero prime ideal $\wp \subseteq \mathcal{O}_K$
- $|\cdot|_\gamma$ for some $\gamma : K \to \mathbb{R}$ or $\mathbb{C}$.

13 Completions (of Dedekind domains)

Let $\mathcal{O}_K$ be a dedekind domain, L/K a finite separable extension. Let $\wp \subseteq \mathcal{O}_k, \mathcal{P} \subseteq \mathcal{O}_L \neq 0$ be prime ideals. Say $\mathcal{P} \mid \wp$. We write $K_\wp$ and $L_\mathcal{P}$ for the completion of K, L w.r.t. abs value of $|\cdot|_\wp$, $|\cdot|_P$ respectively.

Lemma 13.1 (10.9):

1. the natural map
$$\pi_\mathcal{P} : L \otimes_K K_\wp \to L_\mathcal{P}$$
is surjective
2. $$[L_p : K_\wp] \leq [L : K]$$

Lemma 13.2 (10.8 CRT):

Theorem 13.3 (10.9):
The natural map $L \otimes_K K_\wp \to \prod_{\mathcal{P}|\wp} L_\mathcal{P}$ is an isomorphism
Note that $K_\wp$ means the completion of K w.r.t. $\wp$.

14 Week 5 Lecture 1

Corollary 14.1 (10.10):
For $x \in L$,

$$N_{L/K}(x) = \prod_{\mathcal{P}|\wp} N_{L_\mathcal{P}/k_\wp}(x)$$

these subscripts mean the completion with respect to $|\cdot|_\wp$. NOT localization.

15 Decomposition groups

Let $0 \neq \wp$ be a prime ideal of $\mathcal{O}_K$. then write $\wp\mathcal{O}_L = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$ for distinct products of prime ideals in $\mathcal{O}_L, e_i > 0$.
Note that for any i, $\wp \subseteq \mathcal{O}_k \cap \mathcal{P}_i \subsetneq \mathcal{O}_k$. Since $\wp$ is maximal, $\wp = \mathcal{O}_k \cap \mathcal{P}_i$.

Definition 15.1 (11.1. Ramification):

1. e_i is the ramification index of $\mathcal{P}_i$ over $\wp$.
2. we say K ramifies in L if some $e_i > 1$.

Definition 15.2 (11.2 Residue class degree):

$$f_i := [\mathcal{O}_L/\mathcal{P}_i : \mathcal{O}_k/\wp]$$

is the residue class degree of $\mathcal{P}_i$ over $\wp$.

Theorem 15.1 (11.3):

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

This theory is more interesting when $[L : K]$ is Galois. Note that $\mathrm{Gal}(L/K)$ acts on $\{\mathcal{P}_1, \dots, \mathcal{P}_r\}$.

Proposition 15.2 (11.4):
The action of $\mathrm{Gal}(L/K)$ on $\{\mathcal{P}_1, \dots, \mathcal{P}_r\}$ is transitive.

Corollary 15.3 (11.5):
Suppose L/K is Galois, then $e := e_1 = \ldots = e_r, f_1 = \ldots = f_r := f$. Then we have $n = efr$.

If L/K is extension of complete, discrete valued fields, normalized valuation V_L, V_K, with valuation π_L, π_K, then the ramification index

$$e := e_{L/K} = V_L(\pi_k)$$

and

$$f := f_{L/K} = [k_L : k]$$

where the ks are residue fields.

Corollary 15.4 (11.6):
L/K is a finite separable extension, then $[L : K] = ef$. Note that corollary holds without the assumption of separability.

Definition 15.3 (11.7. decomposition grouup):
$\mathcal{O}_L$ a ddk domain, L/K finite Galois extension. Then decomposition group at prime $\mathcal{P}$ of $\mathcal{O}_L$ is the susbgroup of $\mathrm{Gal}(L/K)$ defined by

$$G_{\mathcal{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathcal{P}) = \mathcal{P}\}$$

15.1 Week 5 lecture 2

Proposition 15.5 (11.8):
Suppose that L/K is Galois, the $\mathcal{P}/_{\wp}$ prime ideal of $\mathcal{O}_L$. Then

- $L_{\mathcal{P}}/k_{\wp}$ is Galois
- There is a natural map
$$res : \mathrm{Gal}(L_{\mathcal{P}}/k_{\wp}) \to \mathrm{Gal}(L/K)$$
which is injective and has image $G_{\mathcal{P}}$. (recall this is the decomposition group, the Gal of L/K that fixes $\mathcal{P}$.)

16 Ramification theory

16.1 Different and discriminant

Let L/K be an extension of algebraic number fields, $[L : K] = n$.
Let $x_1, \ldots, x_n \in L$, set

$$\Delta(x_1, \ldots, x_n) = \det\big(\mathrm{Tr}_{L/K}\, x_i x_j\big) \in K = \det(\sigma_i(x_j))^2 \in K$$

where $\sigma_i : L \to \bar{K}$ are distinct embeddings.
Note: with $x_1, \ldots, x_n$, you first make matrix $x_i x_j$. Then you replace each entry of the matrix with $\det(x_i x_j)$. Now you obtain a matrix, and then you compute its determinant.
If $y_i = (a_{ij})x_j$ where the (a_{ij}) is the matrix form, then

$$\Delta(y_1, \ldots, y_n) = \det\big(A^2\big)\Delta(x_1, \ldots, x_n), A = (a_{ij})$$

This is how you perform change of coordinate w.r.t. the Δ. if all elements are in $\mathcal{O}_L$ then the Δ is in $\mathcal{O}_K$, `https://en.wikipedia.org/wiki/Perfect_field`

Lemma 16.1 (12.1):
Let K be a perfect field. R is a $k-$algebra, finite dimensional as a $k-$vector space. then the trace form

$$(,) : R \times R \to K$$

$$(x, y) \to Tr(xy) := Tr_R(mult(xy))$$

is nondegenerate iff $R \cong R_1 \times \ldots \times R_n$ where k_i/k are finite hence separable extensions.
This is more of a linear algebra result. This holds for general rings.

Theorem 16.2 (12.2):
Let $0 \neq \wp \subseteq \mathcal{O}_k$ be prime ideals.
If $\wp$ ramifies in L, then for every $x_1, \ldots, x_n \in \mathcal{O}_L$, $\wp \mid \Delta(x_1, \ldots x_n)$.
If $\wp$ is unfamified in L, then $\exists x_1, \ldots, x_n \in \mathcal{O}_L$ such that $p \nmid \Delta(x_1, \ldots, x_n)$.

Definition 16.1 (12.3): The discriminant is the ideal $d_{L/K} \subseteq \mathcal{O}_K$ generated by $\Delta(x_1, \ldots x_n)$ for all choices of $x_1, \ldots, x_k \in \mathcal{O}_L$.

Corollary 16.3 (12.4):
$\wp$ ramifies in $L \iff \wp \mid d_{L/K}$. In particular, only finitely many primes ramify.

Definition 16.2 (12.5): The inverse different is $D^{-1}_{L/K} = \{y \in L : Tr_{L/K}(xy) \in \mathcal{O}_K, \forall x \in \mathcal{O}_L\}$ is an $\mathcal{O}_L$ submodule of L containing $\mathcal{O}_L$. The inverse of the inverse different ideal is the different ideal.

Lemma 16.4 (12.6):
$D^{-1}_{L/K}$ is a fractional ideal.

16.2 Week 5 lecture 3

Remark 13 (Commute): Note that there is a commutative diagram of $L^\times, K^\times, I_L, I_K$ where the Is are groups of fractional ideals.

Theorem 16.5 (12.7):

$$N_{L/K}(D_{L/K}) = d_{L/K}$$

Theorem 16.6 (12.8):
If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ and α has monic minimal polynomial $g(x) \in \mathcal{O}_k[x]$ then $D_{L/K} = (g'(\alpha))$.

Theorem 16.7 (12.9):

$$D_{L/K} = \prod_{\mathcal{P}} D_{L_{\mathcal{P}}/k_{\wp}}$$

Corollary 16.8 (12.10):

$$d_{L/K} = \prod_{\mathcal{P}|\wp} d_{L\mathcal{P}/k_{\wp}}$$

16.3 Unramified and totally ramified extensions of local fields

Lemma 16.9 (13.1):
Tower law for the e indices and the f indices.

Definition 16.3 (Unramified, ramified, and totally ramified):

16.4 Week 6 lecture 1

L/K a finite separable extension of local fields.
In this lecture, we will show that unram and ram extensions are the building blocks of those extensions.

Theorem 16.10 (13.3):
There exists a field K_0 $K \subseteq K_0 \subseteq L$ such that

- K_0/K is unramified
- L/K_0 is totally ramified

Moreover $[K_0 : K] = f_{L/K}$ and $[L : K_0] = e_{L/K}$ and K_0/K is Galois.

Theorem 16.11 (13.4):
Unramified extensions are easy to understand. You just look at the residue fields!
Let $k = \mathbb{F}_q$. for each $n \geq 1$, there exists a unique unramified extension L/K of degree n. Moreover, L/K is Galois and the natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ is an isomorphism. $\mathrm{Gal}(L/K) = \langle Frob_{L/K} \rangle$ is cyclic, where $Frob_{L/K}(x) \equiv x^q \mod m_L, \forall x \in \mathcal{O}_L$.

Corollary 16.12 (13.5):
L/K finite Galois. Then the map

$$res : \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$$

is surjective.

Definition 16.4 (13.6. Intertial subgroup): L/K be finite and Galois. The inertia subgroup is

$$I_{L/K} = \ker(\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k))$$

we have $|I_{L/K}| = e_{L/K}$. Also $I_{L/K} = \mathrm{Gal}(L/K_0)$.

The totally ramified polynomials are controlled by Eisenstein polynomials.

Definition 16.5 (13.7): A polynomial in $\mathcal{O}_k[x]$ is eisenstein if $V_k(a_i) \geq 1, \forall i, V_k(a_0) = 1$. i.e. all other coefficient has valuation at least 1 while constant coefficient exactly 1.

Theorem 16.13 (13.8):

1. Let L/K be finite and totally ramified. $\pi_L \in \mathcal{O}_L$ uniformizer. Then the min poly of π_L is Eisenstein and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. and $L = K(\pi_L)$.
2. Conversely, if $f(x) \in \mathcal{O}_k[x]$ is Eisenstein, and α is a root of f, then $L = K(\alpha)/K$ is totally ramified and α is a unif in L.

16.5 Structure of units

Let $[K : \mathbb{Q}_p] < \infty$. $e := e_{L/\mathbb{Q}_p}$ be the absolute ram index. Let π be unit in k.

Proposition 16.14 (14.1):
If $r > \frac{e}{p-1}$, $\exp(x) = \sum_{i=0}^{\infty} \frac{x^n}{n!}$ converges in $\pi^r \mathcal{O}_k$ and induces an isomorphism between

$$(\pi^r \mathcal{O}_k, +) \cong (1 + \pi^r \mathcal{O}_k, \times)$$

17 Week 6 Lec 2

Definition 17.1 (13.10): Filtration: for $s \in \mathbb{Z}_{\geq 1}$, the sth unit group $U_k^{(s)}$ is defined by

$$U_K^{(s)} = (1 + \pi^s \mathcal{O}_k, \times)$$

set $U_k^{(0)} = U_k$. Then we have filtration

$$\ldots \subseteq U_K^{(s)} \subseteq \ldots \subseteq U_K^{(1)} \subseteq U_K^{(0)} = U_K$$

Proposition 17.1 (13.11):

- $U_K^{(0)}/U_K^{(1)} \cong (k^\times, \times), k := \mathcal{O}_k/\pi$
- $U_K^{(s)}/U_k^{(s+1)} \cong (k^\times, +), s \geq 1$

Corollary 17.2 (5.2.4.):
Let $[K : \mathbb{Q}_p] < \infty$. Then $\mathcal{O}_K^\times$ has a subgroup of finite index isomorphic to $(\mathcal{O}_k, +)$.
Note that this is not true for K of equal char, where exp is not well defined.

17.1 Higher Ramification groups

Let L/K be a finite Galois extension of local fields. We define an analogous filtration of $\mathrm{Gal}(L/K)$.

Definition 17.2 (14.1): v_L be the normalized valuation on L. For $s \in \mathbb{R}_{\geq 1}$ we define the sth ramification group

$$G_s(L/R) = \{\sigma \in \mathrm{Gal}(L/K) \mid v_L(\sigma(x) - x) \geq s + 1, \forall x \in \mathcal{O}_L.\}$$

Note that $G_{-1}(L/K) = \mathrm{Gal}(L/K)$ and $G_0(L/K) = I_{L/K}$.
For $s \in \mathbb{Z}_{\geq 0}$,

$$G_s(L/K) = \ker(\mathrm{Gal}(L/K) \to Aut(\mathcal{O}_L/\pi_L^{s+1}\mathcal{O}_L))$$

so $G_s(L/K)$ is a normal subgroup of $\mathrm{Gal}(L/K)$.

$$G_s \subseteq G_{s-1} \subseteq \ldots \subseteq G_{-1} = \mathrm{Gal}(L/K)$$

Note that G_s only change at integers.

Theorem 17.3 (14.2. three big theorems about higher rami groups):

1. for $s \geq 1$, $G_s = \{\sigma \in G_0 \mid v_L(\sigma(\pi_L) - \pi_L) \geq s + 1\}$
2. $\bigcap_{s=0}^{\infty} G_s = \{1\}$.
3. let $s \in \mathbb{Z}_{\geq 0}$. Then there exists injective group hom

$$G_s/G_{s+1} \hookrightarrow U_L^{(s)}/U_L^{(s+1)}$$

induced by $\sigma \mapsto \frac{\sigma(\pi_L)}{\pi_L}$. This map independent in choice of π_L.

17.2 Week 6 lecture 3

Corollary 17.4 (14.3):
Given a finite Galois extension of local fields, $\mathrm{Gal}(L/K)$ is solvable.

G_1 is the unique (since normal) Sylow-p subgroup of $G_L = I_{L/K}$.

Definition 17.3 (14.4):
The group G is the wild inertia group. and G_0/G_1 is the tame quotient. If L/K is finite seprable extension of local fields, we say L/K is tamely ramified if $\operatorname{char} k \nmid e_{L/K}$ ($\iff$ $G_1 = \{1\}$ if L/K is Galois) otherwise it is wildly ramified.

Theorem 17.5 (14.5):
$[K : \mathbb{Q}_p] < \infty$, L/K finite, $D_{L/K} = (\pi_L)^{\delta(L/K)}$ therefore $\delta(L/K) \geq e_{L/K} - 1$ with equality iff L/K is tamely ramified.

Corollary 17.6 (14.6):
L/K is an extension of number fields. $\mathcal{P} \subseteq \mathcal{O}_L, \mathcal{P} \cap \mathcal{O}_K = \wp$, then $e(\mathcal{P}/\wp) > 1 \iff \mathcal{P} \mid D_{L/K}$

Remark 14: Explicitly what the group G_i looks like.

18 Local class field theory

Infinite Galois theory. Let L/K be an algebraic extension of any field.

Definition 18.1 (5.2.): definition of

- separable
- normal
- Galois: separable and normal
- the Galois correspondence
- Let $(I, \leq)$ a partially ordered set. It is a directed set if for all $i, j \in I, \exists k \in I$, such that $i \leq k, j \leq k$
- profinite topology on an inverse limit is the weakest topology such that the projection maps are continuous.

Proposition 18.1 (16.2):
Let $(I, \leq)$ be direct set, and $(G_i)_{i\in I}$ a collection of groups together with maps $\phi_{ij} : G_j \to G_i$ such that

- $\phi_{ij} = \phi_{ij} \circ \phi_{jk}, \forall i \leq j \leq b$
- $\phi_{ii} = id.$

We say $((G_i)_{i\in I}, \phi_{ij})$ is an inverse system.
Inverse limit of $((G_i)_{i\in I}, \phi_{ij})$

$$\varprojlim_{i\in I} G_i = \left\{ (g_i)_{i\in I} \in \prod_{i\in I} G_i \mid \phi_{ij}(g_j) = g_i \right\}$$

Proposition 18.2 (16.3):
Let L/K be Galois. then

- the set $I = \{F/K \text{ is finite Galois}, F \subseteq L\}$ is directed under $\subseteq$.
- for $F, F' \in I$, such that $F \subseteq F'$, there is a restriction map $res_{F,F}$

$$\mathrm{Gal}(F'/K) \to \mathrm{Gal}(F/K)$$

and the natural map $\mathrm{Gal}(L/K) \to \varprojlim_{F\in I} \mathrm{Gal}(F/K)$ is an isomorphism.

18.1 Week 7 lecture 1

Theorem 18.3 (16.4):
This is practically the fundamental theorem of Galois theory extended to infintie extensions. Endow $\mathrm{Gal}(L/K)$ with profinite topology and then we get the usual bijection between F/K, subextensions of L/K to the closed subgroups of $\mathrm{Gal}(L/K)$. F/K is finite iff $\mathrm{Gal}(L/K)$ is open. F/K is Galois iff $\mathrm{Gal}(L/F)$ is normal in $\mathrm{Gal}(L/K)$.

18.2 The Weil group

Let K be a local field and let L/K be separable algebraic extension. then

Definition 18.2 (16.5):

- L/K is unram if F/K is unram for all F/K finite ext
- L/K is totally ram if F/K is totally ram for all F/K finite ext.

Proposition 18.4 (16.6):
Let L/K be unram. Then L/K is Galois and

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k)$$

Remark 15: For any Galois extension L/K we can find a max unram subextension of K_0/K.

We then move onto the Weil group

Definition 18.3 (16.7 The Weil group): Let L/K be Galois, the Weil group $W(L/K) \subseteq \mathrm{Gal}(L/K)$ is $res\langle Fr_{K_l/K}\rangle$
The Weil group for finite extension if equal to the Gal group but for infinite one it's strict containment.

Definition 18.4 (The topology of $W(L/K)$): It is the weakest topology such that $W(L/K)$ is a topological subgroup and that $I_{L/K} = \mathrm{Gal}(L/K_0)$ is equipped with profinite topology. Note that the subspace topology inherited on Gal is not fine enough for $I_{L/K}$ to be open.

Proposition 18.5 (16.8):
Let L/K be Galois. The ideal is that from Gal to W we dont lose information.

- $W(L/K)$ is dense in $\mathrm{Gal}(L/K)$.
- If F/K is finite extension of L/K then

$$W(L/F) = W(L/K) \cap \mathrm{Gal}(L/F)$$

- If F/K is finite Galois then

$$\frac{W(L/K)}{W(L/F)} \cong \mathrm{Gal}(F/K)$$

18.3 Week 7 Lecture 2

19 Statements of Local Class Field Theory

Definition 19.1 (17.1): An extension L/K is Abelian if it's Galois and $\mathrm{Gal}(L/K)$ is abelian.

Remark 16 (Facts): If $L_1/K, K_2/K$ are abelian then

- L_1L_2/K is abelian
- If $L_1 \cap L_2 = K$ then there exists canonical isomorphism $\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

Definition 19.2:

- K^{ab} is the maximal abelian extension of K inside K^{sep}
- K^{sep} is the separable closure of K.
- K^W is the maximum unramified extension of K inside K^{sep}

There exists an exact sequence.

$$0 \longrightarrow I_{K^{ab}/K} \longrightarrow W(K^{ab}/K) \longrightarrow \begin{array}{c} < Fr_{K^W/k} > \\ = \\ \mathbb{Z} \end{array} \longrightarrow 0$$

Theorem 19.1 (17.2):
Local Artin reciprocity, Art_K induces an isomorphism, Existence Theorem, Norm functoriality,

Proposition 19.2 (17.3):
L/K finite abelian of degree n, then $e_{L/K} = [\mathcal{O}_K^\times : N_{L/K}(\mathcal{O}_L^\times)]$

Corollary 19.3 (17.4):
Let L/K be finite abelian. Then L/K is unramified iff $N_{L/K}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$.

Theorem 19.4 (17.5. Local Kronecker - Weber):

$$\mathbb{Q}_p^{ab} = \mathbb{Q}_p^{un}\mathbb{Q}_p(\zeta_{p^\infty})$$

19.1 Week 7 lec 3

Now we are in a place to construct Art_K. Let K be a local field, and π a uniformizer of K. For $n \geq 1$, we can construct $K_{\pi,n}$ totally ramified Galois extension such that

1. $K \subseteq K_{\pi,1} \subseteq K_{\pi,2} \subseteq \ldots$,
2. for $n \geq m \geq 1$ there exists a diagram

$$\begin{array}{ccc} \mathrm{Gal}\,(K_{\pi,n}/K) & \longrightarrow\!\!\!\!\!\rightarrow & \mathrm{Gal}\,(K_{\pi,m}/K) \\ {\scriptstyle \psi_n}\downarrow{\scriptstyle \sim} & & {\scriptstyle \sim}\downarrow{\scriptstyle \psi_m} \\ \mathcal{O}_K^\times/\mathrm{U}_K^{(n)} & \xrightarrow[\text{mod } m]{}\!\!\!\!\!\rightarrow & \mathcal{O}_K^\times/\mathrm{U}_K^{(m)} \end{array},$$

3. setting $K_{\pi,\infty} = \bigcup_{n=1}^{\infty} K_{\pi,n}$, we have

$$K^{\mathrm{ab}} = K^{\mathrm{ur}} K_{\pi,\infty}.$$

(Picture fetched from David Kurniadi Angdinata)
The existence of the map ψ will help you construct the Artin map. The rest of the course focuses on this.

20 Lubin- Tate theory

Definition 20.1 (Ring for formal power series):

$$R[|x_1, \ldots, x_n|]$$

Definition 20.2 (18.1): A $1-$dimensional commutative formal group law over R is a power series $F(X,Y) \subseteq R[[X,Y]]$ satisfying

- $F(X,Y) \equiv X + Y$ mod degree 2
- $F(X, F(X,Y)) = F(F(X,Y), Z)$, associativity
- $F(X,Y) = F(Y,X)$ commutativity

Moreover,
1. $\hat{G_\alpha}(X;Y) = X + Y$ is the formal additive group
2. $\hat{G_m}(X,Y) = X + Y + XY$ is the formal multiplicative group.

Lemma 20.1 (18.2):
F a formal group law over R.
1. $F(X,0) = X, F(0,Y) = Y$
2. $\exists$ a unique $i(X) \in XR[[X]]$ such that $F(X, i(X)) = 0$.

Definition 20.3 (Homomorphism between formal group laws): Let F, G be formal group laws over R. A homomorphism $f : F \to G$ is an element $f(x) \in XR[[X]]$ such that

$$f(F(X,Y)) = G(f(X), f(X))$$

a homomorphism $f : F \to G$ is an iso if there is an $g : G \to F$ such that $f(g(X)) = g(f(X))$. Define $\mathrm{End}_R(F)$ be the set of homomorphisms $f : F \to F$.

Proposition 20.2 (18.4):
R be a $\mathbb{Q}$ algebra. There is an isomorphism of formal group laws

$$\exp : \hat{G_a} \to \hat{G_m}$$

$$\exp(x) = \sum_{i=0}^{n} \frac{x^n}{n!}$$

Proposition 20.3 (18.4):
$\text{End}_R(F)$ is a ring (in general, non-commutative) with addition $f +_F g(x) = F(f(x), g(x))$ and multiplication given by composition.

Now let K be a local field. Let $|k| = q$.
Then

Definition 20.4 (19.1): A formal $\mathcal{O}_K$ module of $\mathcal{O}_K$ is a formal group law $F(X, Y) \in \mathcal{O}_K[[X, Y]]$ together with a ring hom

$$[\cdot]_F : \mathcal{O}_K \to \text{End}_{O_K} F$$

such that $\forall a \in \mathcal{O}_K$, $[a]_F(x) \equiv aX \mod X^2$.
An hom or iso is a hom/iso of group laws $f \circ [a]_F = [a]_G \circ f, \forall a \in \mathcal{O}_K$.

Definition 20.5 (19.2): Let $\pi \in \mathcal{O}_k$ be a uniformizer. Then a Lubin-Tate series for π is a power series $f(x) \in \mathcal{O}_k[[x]]$ such that

- $f(X) \equiv \pi X \mod X^2$
- $f(X) \equiv X^q \pmod{\pi}$

20.1 Week 8 Lec 1

Let K be a local field π a unif, and $|k| = q$.

Theorem 20.4 (19.3):
Let $f(X)$ be a Lubin-tate series for π. Then

1. $\exists$ a unique formal group law F_f over $\mathcal{O}_k$ such that $f \in \text{End}_{\mathcal{O}_K}(F_f)$
2. $\exists$ a ring hom
$$[\cdot]_f : \mathcal{O}_k \to \text{End}_{\mathcal{O}_K}(F_f)$$
which implies F_g is a formal $\mathcal{O}_k$-module over $\mathcal{O}_k$.
3. if $g(x)$ is another formal Lubin-tate series for π, then $F_f \cong F_g$ as formal $\mathcal{O}_k$ modules. F_f is the Lubin-Tate formal group law for π. (only depends on π up to isomorphism.)

Lemma 20.5 (19.4. Key Lemma):
Let $f(x), g(x)$ be Lubin-tate series for π. Let $L(x_1, \dots, x_n) = \sum_{i=1}^{n} a_i x_i$, $a_i \in \mathcal{O}_k$. There $\exists$ a unique power series $F(x_1, \dots, x_n) \in \mathcal{O}_k[[x_1, \dots, x_n]]$ such that

- $F(x_1 \dots x_n) \equiv L(x_1, \dots, x_n) \bmod \deg 2$
- $f(F(x_1, \dots, x_n)) = F(g(x_1), \dots, g(x_n))$.

20.2 Week 8 Lec 2

20.3 Lubin- Tate Extensions

K non-arch local fields. $|K| = q$ and π a uniformizer. Let $\overline{K}$ be the algebraic closure of K and $\overline{\mathfrak{m}} \subseteq \mathcal{O}_{\overline{K}}$.

Lemma 20.6 (20.1):
Let F be a formal $\mathcal{O}_K$-module over $\mathcal{O}_K$. Then $\overline{\mathfrak{m}}$ becomes a genuine $\mathcal{O}_K$ module with

$$x +_F y = F(x, y), x, y \in \overline{\mathfrak{m}}$$

$$a_F x = [a]_F(x), x \in \overline{\mathfrak{m}}, a \in \mathcal{O}_K$$

Definition 20.6 (20.2. π^n Torsion group):
Let $f(X)$ be Lubin Tate series for $\mathfrak{m}$. Let F_f be Lubin Tate formal group law. The π^n- torsion group is

$$\mu_{f,n} = \{x \in \overline{\mathfrak{m}} \mid \pi^n \cdot_{F_f} x = 0\}$$

$$= \{x \in \overline{\mathfrak{m}} \mid f_n(x) = \underbrace{f \circ f \circ \dots f}_{n\text{times}} = 0\}$$

Note that $\mu_{f,n}$ is an $\mathcal{O}_k-$module and that $\mu_{f,n} \subseteq \mu_{f,n+1}$.

Proposition 20.7 (20.3):
Set $h_n(X) = \frac{f_n(X)}{f_{n-1}(X)} = \pi + f_{n-1}(x)^{q-1}$ and $f_0(x) = x$. $h_n(X)$ is a separable Eisenstein polynomial of degree $q^{n-1}(q-1)$.

Proposition 20.8 (20.4):

- $\mu_{f,n}$ is a free module of rank 1 over $\mathcal{O}_k/\pi^n\mathcal{O}_k$.
- If g is another Lubin-Tate series for π then $\mu_{f,n} \cong \mu_{g,n}$ as $\mathcal{O}_K$modules and $K(\mu_{f,n}) = K(\mu_{g,n})$

Definition 20.7 (20.5): $K_{\pi,n} = K(\mu_{f,n})$ is called the Lubin-tate extensions.
Note that it does not depend on f and that $K_{\pi,n} \subseteq K_{\pi,n+1}$.

Proposition 20.9 (20.6):
Note that $K_{\pi,n}$ are totall ramfiied and Galois extensoins of degree $q^{n-1}(q-1)$.

20.4 Week 8 Lec 3

Setup: Let K be local field. $|K| = q$, π a uniformizer, and $f-$ a Lubin-Tate series $\pi x + x^q$.

Theorem 20.10 (20.7.):
There are isomorphisms

$$\psi_n : \mathrm{Gal}(K_{\pi,n}/K) \cong (\mathcal{O}_k/\pi^n\mathcal{O}_k)^\times$$

determined by

$$\phi_n(\sigma) \cdot_{F_f} x = \sigma(x), \forall x \in \mu_{f,n}, \sigma \in \mathrm{Gal}(K_{\pi,n}/K)$$

note that ψ_n does not depend on f.

Note that we set $K_{\pi,\infty} := \bigcup_{n=1}^{\infty} K_{\pi,n}$,

$$\psi : \mathrm{Gal}(K_{\pi,\infty}/K) \cong \varprojlim_n (\Theta_k/\pi^n)^\otimes \cong \mathcal{O}_k k^\times$$

Theorem 20.11 (20.8 Generalized Local Kronecker-Weber):
We have

$$K^{ab} = K_{\pi,\infty} K^{un}$$

the proof is omitted.

THen we can define the Artin map:

$$K^\times \cong \mathbb{Z} \times \mathcal{O}_k^\times \to \mathrm{Gal}(K^{un}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K) \cong \mathrm{Gal}(K^{ab}/K)$$

where

$$(n, \mu) \leftarrow\!\shortmid \pi^n \mu \mapsto (Fr^n_{K^{ur}/K}, \psi^{-1}(u))$$

The image is $W(K^{ab}/K)$. This is independent of choice of π.

21 Non-examinable materials

- Upper numbering of ramification groups.
- $\phi(s)$ as an integral of piecewise linear functions.
- upper numbering system
- example of the upper numbering of the Cyclotomic extension, after computation