Part III Local Fields 2014

Part III Local Fields 2014

Contents

Chapter 1

Introduction

These are lecture notes for the 2014 Part III Local Fields course taught by Dr. Tom Fisher.

The recommended books are:

- Cassels
- Serre
- Koblitz

Generated: May 22, 2015, 12:34:22 (Z)

Chapter 2

p-adic numbers

Definition 2.0.1 (Absolute value)**.** An **absolute value** on a field K is a function $|\cdot|\colon K \to \mathbf{R}$ such that

1. $|x| \geq 0$ and $|x| = 0 \iff x = 0$.
2. $|xy| = |x||y|$.
3. $|x+y| \leq |x| + |y|$.

Example 2.0.2. 1. $K \subset \mathbf{C}$, $|a+bi|_\infty = \sqrt{a^2+b^2}$.

2. K any field, $|x| = 0$ if $x = 0$ and $|x| = 1$ otherwise, this is called the **trivial absolute value**.

Remark 2.0.3. 1. If $x^n = 1$ then $|x| = 1$ and hence finite fields can only be given the trivial absolute value.

2. In particular $|-1| = 1$ and so $|x| = |-x|$ for all $x \in K$.

A valued field $(K, |\cdot|)$ becomes a metric space with $d(xy,) = |x-y|$, and hence a topological space, i.e. open sets are unions of open balls $B(x,r) = \{y \in K : |x-y| < r\}$.

Exercise 2.0.4. Show that the functions $+, \cdot\colon K \times K \to K$ and $|\cdot|\colon K \to \mathbf{R}$ are continuous with respect to this topology.

Example 2.0.5. Let $K = \mathbf{Q}$, p be a prime and $0 < \alpha < 1$. For $x \in \mathbf{Q}^*$ let $\nu_p(x) = r$ where $x = p^r u/v$ and $p \nmid uv$. Then the p-adic absolute value if given by

$$|x|_p = \begin{cases} 0 & x = 0, \\ \alpha^{\nu_p(x)} & \text{otherwise.} \end{cases}$$

Usually we take $\alpha = 1/p$. In this case we get the inequality $|x+y|_p \leq \max\{|x|_p, |y|_p\}$, this is the **ultrametric triangle inequality**.

Definition 2.0.6 ((non-)Archimidean absolute values)**.** Absolute values are called **non-archimidean** if this inequality holds, otherwise they are called **archimidean**.

Recall that if R is any ring then there exists a unique ring homomorphism $\mathbf{Z} \to R$.

Lemma 2.0.7. $|\cdot|$ *is non-archimidean if and only if* $|n|$ *is bounded for all* $n \in \mathbf{Z}$.

Proof. ($\Rightarrow$) $|n| \leq \max\{|1|\} = 1$.
($\Leftarrow$) Suppose $|n| \leq B$ for all $n \in \mathbf{Z}$ then

$$|x+y|^m = \left|\sum_{r=0}^{m} \binom{m}{r} x^{m-r} y^r\right| \leq \sum_{r=0}^{m} \left|\binom{m}{r}\right| |x|^{m-r}|y|^r \leq (m+1)B \max\{|x|^m, |y|^m\}.$$

Now letting $m \to \infty$ we get that $|x+y| \leq \max\{|x|, |y|\}$. □

Corollary 2.0.8. *All absolute values on fields of characteristic p are non-archimidean.*

Example 2.0.9.

1. $K = \mathbf{Q}$, $p = 5$ $|\cdot| = |\cdot|_5$. Let $a_1 = 3, a_2 = 33, a_3 = 33$, etc. So $a_n \equiv a_m \pmod{5^n}$ for all $m \geq n$. Then $|a_n - a_m|_5 \leq 5^{-n}$ for all $m \geq n$ and so $(a_n)_{n\geq 1}$ is a Cauchy sequence. Now $a_n = \frac{10^n - 1}{3}$ so $|a_n - \frac{1}{3}| = 5^{-n} \to 0$ as $n \to \infty$ i.e. $a_n \to -\frac{1}{3}$ w.r.t. $|\cdot|_5$

2. We'll construct (a_n) such that for all $n \geq 1$

$$\begin{cases} a_n^2 + 1 \equiv 0 \pmod{5^n} \\ a_{n+1} \equiv a_n \pmod{5^n} \end{cases}$$

Take $a_1 = 2$. Suppose a_n is chosen and it satisfies $a_n^2 + 1 = 5^n c$. $(a_n + 5^n b)^2 + 1 \equiv a_n^2 + 1 + 2 \cdot 5^n a_n b \equiv 5^n(c + 2ba_n) \pmod{5^{n+1}}$. We solve for b s.t. $2ba_n + c \equiv 0 \pmod 5$. Since $(2a_n, 5) = 1$ this is always possible. Now put $a_{n+1} = a_n + 5^n b$. Condition (ii) implies that a_n is Cauchy. Suppose it converges and $a_n \to l \in \mathbf{Q}$. Then $|l^2 + 1|_5 \leq |a_n^2 + 1|_5 + |a_n^2 - l^2|_5$, both of these terms tend to 0 which gives $l^2 = -1$ a contradiction. This shows that $\mathbf{Q}$ is not complete under $|\cdot|_5$.

Definition 2.0.10. $\mathbf{Q}_p$ is the completion of $\mathbf{Q}$ w.r.t. $|\cdot|_p$. Note that $\mathbf{Q}_p$ has $+, \cdot, |\cdot|_p$ as they extend from $\mathbf{Q}$ by continuity. It is easy to check that $(\mathbf{Q}_p, |\cdot|_p)$ is a non-archimidean valued field.

Definition 2.0.11. $\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x|_p \leq 1\}$.

Lemma 2.0.12. $\mathbf{Z}$ *is dense in* $\mathbf{Z}_p$*, in particular* $\mathbf{Z}_p$ *is the completion of* $\mathbf{Z}$ *w.r.t.* $|\cdot|_p$.

Proof. $\mathbf{Q} \cap \mathbf{Z}_p = \{x \in \mathbf{Q} : |x|_p \leq 1\} = \{\frac{a}{b} \in \mathbf{Q} : p \nmid b, a, b \in \mathbf{Z}\} = \mathbf{Z}_{(p)}$. Let $\frac{a}{b} \in \mathbf{Z}_{(p)}$ i.e. $a, b \in \mathbf{Z}$, $p \nmid b$. For each $n \geq 1$ we can pick $y_n \in \mathbf{Z}$ s.t. $by_n \equiv 1 \pmod{p^n}$ implying $by_n \to_p 1$ as $n \to \infty$. This implies that $ay_n \to \frac{a}{b}$ as $n \to \infty$. Hence $\mathbf{Z}$ is dense in $\mathbf{Z}_{(p)}$.

Now for$\mathbf{Q}$ is dense in $\mathbf{Q}_p$ and $\mathbf{Z}_p \subset \mathbf{Q}_p$ being open give that $\mathbf{Q} \cap \mathbf{Z}_p$ is dense in $\mathbf{Z}_p$. □

The global situation is as follows. $[K : \mathbf{Q}] < \infty$ $\mathcal{O}_K$ = integral closure of $\mathbf{Z}$ in K. $\mathcal{O}_K$ need not be a UFD.

The local situation is as follows. $[K : \mathbf{Q}] < \infty$ $\mathcal{O}_K$ = integral closure of $\mathbf{Z}_p$ in K. $\mathcal{O}_K$ is always a UFD! In fact it is a DVR. K number field $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal $0 < \alpha < 1$. For $x \in K^*$ $v_{\mathfrak{p}}(x)$ = power of $\mathfrak{p}$ in the factorisation of $x\mathcal{O}_K$. Define

$$|x|_p = \begin{cases} \alpha^{v_p(x)} \text{if } x \neq 0 \\ 0 \text{otw} \end{cases}$$

$|\cdot|_{\mathfrak{p}}$ is an absolute value on K. $K_{\mathfrak{p}}$ is the completion of K w.r.t. $|\cdot|_{\mathfrak{p}}$. Note that for a suitable choice of α $|\cdot|_{\mathfrak{p}}$ extends $|\cdot|_p$ on $\mathbf{Q}$ (where $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$).

Remark 2.0.13. $[K_{\mathfrak{p}} : \mathbf{Q}_p] \leq [K : \mathbf{Q}]$. Every finite extension of$\mathbf{Q}_p$ arises as the completion of some number field. Proofs later.

Lemma 2.0.14. *Let $|\cdot|_1$ and $|\cdot|_2$ be non-trivial absolute values on a field K then TFAE:*

1. *$|\cdot|_1$ and $|\cdot|_2$ define the same topology on K.*
2. *$|x|_1 < 1 \iff |x|_2 < 1$.*
3. *$|x|_2 = |x|_1^c$ for some $c > 0$.*

If these conditions hold we say that $|\cdot|_1$ and $|\cdot|_2$ are equivalent.

Proof. 1) $\implies$ 2) $|x|_1 < 1 \iff x^n \to 0$ as $n \to \infty$ w.r.t. $|\cdot|_1 \iff x^n \to 0$ w.r.t. $|\cdot|_2$ iff $|x|_2 < 1$.
2) $\implies$ 3) Pick $a \in K^*$ with $|a|_1 < 1$. Let $x \in K^* m, n \in \mathbf{Z} n > 0$. □

Definition 2.0.15. A **place** of K is an equivalence class of absolute values on K.

Theorem 2.0.16. *A non-trivial absolute value on $\mathbf{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p.*

Proof. First let $|\cdot|$ be archimidean. Let $a, b > 1$ be integer. Write b^n in base a

$$b^n = c_m a^m + \cdots + c_1 a + c_0$$

where $0 \leq c_i < a$ and $m \leq n \log_a b$. Let $B = \max\{c : 0 \leq c < a\}$ then $|b^n| \leq (m+1) B \max\{|a|^m, 1\}$. This implies $|b| \leq ((n \log_a b + 1)B)^{\frac{1}{n}} \max(|a|^{\frac{m}{n}}, 1)$ taking the limit as$n \to \infty$ gives that $|b| \leq \max(|a|^{\log_a b}, 1)$. Since $|\cdot|$ is archimidean we may pick an integer $b > 1$ s.t. $|b| > 1$. Applying the above inequality for any integer $a > 1$ we get $|b| \leq |a|^{\log_a b}$. So $|a| > 1$. Swapping a and b in the inequality we get $|a| \leq |b|^{\log_b a}$. So

$$\frac{\log |a|}{\log a} = \frac{\log |b|}{\log b} = \lambda.$$

Then $|a| = a^\lambda$ for all $a \in \mathbf{Z}_{\geq 1}$ implying $|\cdot| \sim |\cdot|_\infty$.
Now for non-archimidean $|\cdot|$. The ultrametric law implies that $|n| \leq 1$ for all $n \in \mathbf{Z}$, $|\cdot|$ being non-trivial implies that $|u| < 1$ for some $n \in \mathbf{Z}_{>1}$. Writing $n = p_1^{e_1} \cdots p_k^{e_k}$ we get $|p| < 1$ for some p. Suppose that $|p| < 1$ and $|q| < 1$ for $p \neq q$. Write $1 = rp + sq$ so that $1 = |rp + sq| \leq \max < 1$ a contradiction. So $|p| = \alpha$ for some p and $|\cdot|$ is 1 for all other primes. Hence $|\cdot| \sim |\cdot|_p$. □

Remark 2.0.17. If $(K, |\cdot|)$ is archimidean then $\mathrm{char}(K) = 0$ and so $\mathbf{Q} \subset K$. Ostrowski then impliees that restriction of $|\cdot|$ to $\mathbf{Q}$ is equivalent to $|\cdot|_\infty$. so if K is complete then it contains a copy of $\mathbf{R}$.

Fact: If $(K, |\cdot|)$ is complete and archimidean then $K = \mathbf{R}$ or $K = \mathbf{C}$ and $|\cdot| \sim |\cdot|_\infty$ (see Cassels).
From now on we take K non-archimidean.

Lemma 2.0.18. *Let $(K, |\cdot|)$ be non-archimidean. Then*

1. *$|x| > |y|$ implies $|x + y| = |x|$.*
2. *$|x_1 + \cdots + x_n| \leq \max\{|x_i|\}$ with equality only .*
3. *If $(K, |\cdot|)$ is complete then $\sum_{n=1}^\infty a_n$ converges iff $a_n \to 0$.*

Proof.

1. $|x + y| \leq \max(|x|, |y|) = |x| \leq \max(|x + y|, |y|) = |x + y|$.
2. Ultrametric + induction. Apply (i) with $x = x_1$ and $y = x_1 + \cdots + x_n$.

3. Let $s_n = \sum_{i=0}^n a_i$, if $s_n \to l$ then $a_n = s_n - s_{n-1} \to 0$ as $n \to \infty$, conversely for $m \geq n$ we have $s_m - s_n = |a_{n+1} + \cdots + a_m| \leq \max_{i=n+1,\ldots,m}(|a_i|) < \max_{i>n} |a_i| \to 0$ as $n \to \infty$ so s_n is Cauchy, hence convergent.

□

For $x \in L$ $r > 0$ we let $B(x,r) = \{y \in K : |x-y| < r\}$ and $\overline{B}(x,r) = \{y \in K : |x-y| \leq r\}$.

Lemma 2.0.19. *1. If $y \in B(x,r)$ then $B(x,r) = B(y,r)$.*

2. If $y \in \bar{B}(x,r)$ then $\bar{B}(x,r) = \bar{B}(y,r)$.

3. $B(x,r)$ is both open and closed.

4. $\bar{B}(x,r)$ is both open and closed.

5. K is totally disconnected (i.e. the only connected subsets are singletons).

Proof. 1. Ultrametric.

2. Ultrametric.

3. $B(x,r)$ is open, it is closed since if $y \notin B(x,r)$ then $B(x,r) \cap B(y,r) = \emptyset$ as they are not the same ball.

4. $\bar{B}(x,r)$ is closed since if $y \in \bar{B}(x,r)$ then $B(y,r/2) \subset \bar{B}(y,) = \bar{B}(x,r)$.

5. Given any $x, y \in K$ distinct, let $r = |x-y|/2 > 0$ then $B(x,r)$ and its complement are open sets, one containing x, the other y.

□

Chapter 3

Valuations

3.1 Valuations

Let K be a field.

Definition 3.1.1 (Valuations, discrete, normalised, valuation ring, units maximal ideal)**.** $v\colon K^* \to \mathbf{R}$ is called a valuation if

1. $v(xy) = v(x) + v(y)$
2. $v(x + y) \geq \min(v(x), v(y))$.

Fix some $0 < \alpha < 1$, then a valuation v determines a non-archimidean absolute value, via

$$|x| = \begin{cases} \alpha^{v(x)} \text{ if } x \neq 0, \\ 0 \text{ if } x = 0. \end{cases}$$

Conversely given some $|\cdot|$ we can put $v(x) = \log |x| / \log \alpha$. We ignore the trivial valuation. We say two valuations v_1, v_2 are equivalent if for some $c \in \mathbf{R}_{>0} v_1(x) = cv_2(x)$ for all $x \in K^*$. The image $v(K^*)$ is a subgroup of $\mathbf{R}$. If it is discrete (i.e. isomorphic to $\mathbf{Z}$) we say that v is a discrete valuation, we say it is normalised if $v(K^*) = \mathbf{Z}$. We let $\mathcal{O}_v = \{x \in K : v(x) \leq 1\}$ be the valuation ring. $\mathcal{O}_v^* = \{x \in K : v(x) = 1\}$ is its unit group. $m = \{x \in K : |x| < 1\}$ is a maximal ideal. $k = \mathcal{O}_v/m$ is the residue field.

Remark 3.1.2.

1. $m = \mathcal{O}_v \smallsetminus \mathcal{O}_v^*$ so m is the unique maximal ideal, hence $\mathcal{O}_v$ is a local ring.
2. Let $x, y \in K^*$, then $x\mathcal{O}_v \subset y\mathcal{O}_v \iff x/y \in \mathcal{O}_v \iff |x/y| \leq 1 \iff |x| \leq |y|$.
3. If $0 \neq x \in m$ then $K = \mathcal{O}_v[1/x] = \mathrm{Frac}(\mathcal{O}_v)$.
4. $\mathcal{O}_v$ is integrally closed in K. This is as if $x \in K$ satisfies $x^n + \cdots + a_0 = 0$ with $a_i \in \mathcal{O}_v$ then $|x^n| \leq \max_{i=0,\ldots,n-1} |a_i x^i| \leq \max(1, |x|^{n-1})$ which implies $|x| \leq 1$ i.e. $x \in \mathcal{O}_v$.

Lemma 3.1.3. *TFAE:*

1. *v is discrete.*
2. *$\mathcal{O}_v$ is a PID.*
3. *$\mathcal{O}_v$ is a Noetherian.*

4. m is principal.

Proof. Note that $x\mathcal{O}_v \subset u\mathcal{O}_v \iff |x| \leq |y|$. For i) $\implies$ ii) Take $I \subset \mathcal{O}_v$ and pick $a \in I$ with $|a| = \max\{|x| : x \in I\}$ equivalently $v(a) = \min\{v(x) : x \in I\}$. This minimum exists as v is discrete. Then $I = a\mathcal{O}_v$. ii) $\implies$ iii) is clear. For iii) $\implies$ iv) assume $m = x_1\mathcal{O}_v + \cdots + x_n\mathcal{O}_v$ wlog $|x_1| \geq \cdots \geq |x_n|$ then $m = x_1\mathcal{O}_v$. For iv) $\implies$ i) Write $m = \pi\mathcal{O}_v$ and let $c = v(\pi) > 0$. If $x \in K^*$ with $v(x) > 0$ then $x \in m$ and so $v(X) \geq c$ and therefore v is discrete. ☐

Definition 3.1.4 (DVR)**.** A DVR is a PID with exactly one non-zero prime ideal.

Lemma 3.1.5. *1. If v is discrete then $\mathcal{O}_v$ is a DVR.*

2. Let R be a DVR, then there exists a discrete valuation on $K = \mathrm{Frac}(R)$ s.t. $R = \mathcal{O}_v$ with v unique up to normalisation.

Proof. 1. $\mathcal{O}_v$ is a local ring, lemma 2.1 implies that $\mathcal{O}_c$ is a PID, this gives that $\mathcal{O}_v$ is a DVR

2. Let R be a DVR with prime element π. Every $x \in R \setminus \{0\}$ can be written as $u\pi^m$ with $u \in R^*$, $m \geq 0$. Every $x \in K^*$ can be written as $u\pi^m$ with $u \in R^*$, $m \in \mathbf{Z}$. We define $v\colon K^* \to \mathbf{Z}$ by $u\pi^m \mapsto m$, this is a discrete valuation with $\mathcal{O}_v = R$.

☐

Example 3.1.6. $\mathbf{Z}_{(p)} = \{x \in \mathbf{Q} : |x|_p \leq 1\}$ is a DVR with field of fractions $\mathbf{Q}$. $\mathbf{Z}_{(p)} = \{x \in \mathbf{Q}_p : |x|_p \leq 1\}$ is a DVR with field of fraction $\mathbf{Q}_p$. In both of these examples the residue field is $\mathbf{F}_p$.

For the rest of this section let $v\colon K^* \to \mathbf{Z}$ be a normalised discrete valuation. Additionally pick $\pi \in K^*$ with $v(\pi) = 1$ so that $m = \pi\mathcal{O}_v$ (π is called the uniformiser).

Lemma 3.1.7 (Hensel's lemma (version 1))**.** *Assume K is complete w.r.t. v and let $f \in \mathcal{O}[x]$. Suppose that the reduction $\bar{f} \in k[x]$ has a simple root in k i.e. there exists $a \in \mathcal{O}$ s.t. $f(a) \equiv 0 \pmod{\pi}$ (i.e $|f(a)| < 1$) and $f'(a) \not\equiv 0 \pmod{\pi}$ (i.e $|f'(a)| = 1$). Then there exists a unique $x \in \mathcal{O}$ s.t. $f(x) = 0$ and $x \equiv a \pmod{\pi}$.*

Proof. Follows from version 2 of Hensel's Lemma . ☐

Lemma 3.1.8 (Hensel's lemma (version 2))**.** *Assume K is complete w.r.t. v and let $f \in \mathcal{O}[x]$. Suppose that there exists $a \in \mathcal{O}$ s.t. $|f(a)| < |f'(a)|^2$). Then there exists a unique $x \in \mathcal{O}$ s.t. $f(x) = 0$ and $|x - a| < |f'(a)|$.*

Proof. Let $r = v(f'(a))$. We construct a sequence $(x_n) \in \mathcal{O}$ s.t.

1. $f(x_n) \equiv 0 \pmod{\pi^{n+2r}}$,
2. $x_{n+1} \equiv x_n \pmod{\pi^{n+r}}$.

We put $x_1 = a$. Let $n \geq 1$ and suppose x_n satisfies 1, i.e. $f(x_n) = c\pi^{n+2r}$ for some $c \in \mathcal{O}$. We'll put $x_{n+1} = x_n + b\pi^{n+r}$ for some $b \in \mathcal{O}$. We have that

$$f(X+Y) = f_0(X) + f_1(X)Y + f_2(X)Y^2 + \cdots$$

for some $f_i \in \mathcal{O}[X]$. We have $f_0 = f$, $f_1 = f'$. $f(x_{n+1}) = f(x_n + b\pi^{n+r}) \equiv f(x_n) + f'(x_n)b\pi^{n+r} \pmod{\pi^{n+2r+1}}$ But $x_n \equiv a \pmod{\pi^{r+1}}$ which implies that $f'(x_n) \equiv f'(a) \pmod{\pi^{r+1}}$, implying $f'(x_n) = u\pi^r$ for some $u \in \mathcal{O}^*$. Note that this argument shows that if $x \in \mathcal{O}$ and $|x-a| < |f'(a)|$ then $|f'(a)| = |f'(x)|$. Therefore $f(x_{n+1}) \equiv c\pi^{n+2r} + u\pi^r b\pi^n \pmod{\pi^{n+2r+1}} \equiv (c+ub)\pi^{n+2r} \pmod{\pi^{n+2r+1}}$. Taking $b = -c/u$

(note $b \in \mathcal{O}$) gives that $f(x_{n+1}) \equiv 0 \pmod{\pi^{n+2r+1}}$, so the first property holds for $n+1$. The second property implies that (x_n) is Cauchy and the first gives that $x = \lim_{n\to\infty} x_n$ is a root of f. Note that $x_n \equiv a \pmod{\pi^{n+1}}$ for all n implies that $x \equiv a \pmod{\pi^{r+1}}$ and so $|x - a| < f'(a)|$.
To see uniqueness suppose x and y both satisfy the above note . Assume moreover that $s = x - y \neq 0$. The inequalities $|x-a| < |f'(a)|$ and $|y-a| < |f'(a)|$ together imply that $|s| < |f'(a)|$. Now $0 = f(y) = f(x+s) = f(x) + f'(x)s + \cdots$ and therefore $|f'(x)s| < |s|^2$ and so $|f'(a)| = |f'(x)| \leq |s|$ which contradicts the above. □

Remark 3.1.9. In the proof of Hensel's lemma $x_{n+1} = x_n - f(x_n)/f'(x_n)$ which is as in the Newton-Raphson method.

Remark 3.1.10. Uniqueness in Hensel's . We saw that every element of K^* is of the form $u\pi^r$ for some $u \in R^*$ and $m \in \mathbf{Z}$. If $R = \mathcal{O}_v$ for some valuation $v\colon K^* \to \mathbf{R}$ then $v(x) \geq 0$ for all $x \in R$. So if $u \in R^*$ then $v(u) = 0$. In particular $v(u\pi^m) = mv(\pi)$, i.e. v is uniquely determined by $v(\pi)$ so it is unique if we normalise it.

Lemma 3.1.11. *Let $A \subset \mathcal{O}_v$ be a set of coset representatives for $k = \mathcal{O}_v/m$. Then every $x \in \mathcal{O}_v$ can be written uniquely as*

$$x = \sum_{n=0}^{\infty} a_n \pi^n$$

with $a_n \in A$.

Proof. There exists a unique $a_0 \in A$ s.t. $x \equiv a_0 \pmod{\pi}$. So $x = a_0 + \pi x_1$ for some $x_1 \in \mathcal{O}_v$. There now exists a unique $a_1 \in A$ s.t. $x_1 \equiv a_1 \pmod{\pi}$. So $x = a_0 + \pi a_1 + \pi^2 x_2$ for some $x_2 \in \mathcal{O}_v$. We may continue this process. Letting $s_N = \sum_{n=0}^{\infty} a_n \pi^n$ we get $v(x - s_N) > N$. This gives that $s_N \to x$ as $N \to \infty$. So $x = \lim_{N\to\infty} s_N = \sum_{n=0}^{\infty} a_n \pi^n$. Uniqueness is clear. □

Remark 3.1.12. K being complete is equivalent to every sequence $\sum_{n=0}^{\infty} a_n \pi^n$ converging. One direction is trivial the other is an exercise.

Proposition 3.1.13.

$$\mathbf{Q}_p^*/(\mathbf{Q}_p^*)^2 \cong \begin{cases} (\mathbf{Z}/2\mathbf{Z})^2 & \textit{if } p \neq 2, \\ (\mathbf{Z}/2\mathbf{Z})^3 & \textit{if } p = 2. \end{cases}$$

Proof.

1. Assume $p \neq 2$. For $b \in \mathbf{Z}_p^*$ we have $b \in (\mathbf{Z}_p^*)^2 \iff \bar{b} \in (\mathbf{F}_p^*)^2$ (applying Hensel's lemma to $f(x) = x^2 - b$). Therefore $\mathbf{Z}_p^*/(\mathbf{Z}_p^*)^2 \xrightarrow{\sim} \mathbf{F}_p^*/(\mathbf{F}_p^*)^2 \cong \mathbf{Z}/2\mathbf{Z}$. But $\mathbf{Q}_p^* \cong \mathbf{Z}_p^* \times \mathbf{Z}$ via the map $up^r \mapsto (u, r)$. Therefore $\mathbf{Q}_p^*/(\mathbf{Q}_p^*)^2 \cong \mathbf{Z}_p^*/(\mathbf{Z}_p^*)^2 \times \mathbf{Z}/2\mathbf{Z} \cong (\mathbf{Z}/2\mathbf{Z})^2$. We have coset reps $1, p, u, pu$ where u is a non-square mod p.

2. Let $p = 2$. Take $b \in \mathbf{Z}_2^*$ with $b \equiv 1 \pmod{8}$, let $f(x) = x^2 - b$. Then $|f(1)| \leq 2^{-3} < 2^{-2} = |f'(1)|^2$. Hensel's lemma now gives us that f has a root in $\mathbf{Z}_2$. So $\mathbf{Z}_2^* \to (\mathbf{Z}/8\mathbf{Z})^* \cong (\mathbf{Z}/2\mathbf{Z})^2$. Clearly $(\mathbf{Z}_2^*) \subset \ker$. We just checked that $\ker \subset (\mathbf{Z}_2^*)^2$. Therefore $\mathbf{Z}_2^*/(\mathbf{Z}_2^*)^2 \cong (\mathbf{Z}/2\mathbf{Z})^2$. Hence $\mathbf{Q}_2^*/(\mathbf{Q}_2^*)^2 \cong (\mathbf{Z}/2\mathbf{Z})^3$. We have coset reps $2^a(-1)^b 5^c$ where $a, b, c \in \{0, 1\}$.

□

Corollary 3.1.14. $\mathbf{Q}_p$ *(for $p \neq 2$) has exactly 3 quadratic extensions.* $\mathbf{Q}_2$ *has exactly 7.*

3.2 Examples of DVR's continued

Example 3.2.1. Let k be any field, $K = k(t)$, $v_0(t^n p(t)/q(t)) = n$, where $p, q \in k[t]$ and $p(0), q(0) \neq 0$. Then $\mathcal{O} = \{f(t) = p(t)/q(t) : f(0) \text{ is defined i.e. } q(0) \neq 0\}$. And $\mathcal{O}^* = \{f(t) = p(t)/q(t) : f(0) \text{ is defined and non-zero}\}$. $m = \{f(t) : f(0) = 0\}$. $\mathcal{O}/m \cong k$ via the map $f \mapsto f(0)$. Likewise for other $a \in k$, $v_a((t-a)^n p(t)/q(t)) = n$, where $p, q \in k[t]$ and $p(a), q(a) \neq 0$, this is the order of zero/pole at $t = a$. We also have $v_\infty(p(t)/q(t)) = v_0(p(1/\epsilon)/q(1/\epsilon)) = \deg(q) - \deg(p)$.

Remark 3.2.2.

1. If $k = \bar{k}$ then these are the only valuations on $K = k(t)$ with $v(k^*) = 0$.
2. $K = k(t)$ is the function field of $\mathbf{P}^1$. Similar examples arise for any smooth point of an algebraic curve/Riemann surface.

Example 3.2.3. $K = k((t))$ = the field of Laurent power series

$$= \left\{ \sum_{n \geq n_0} a_n t^n : a_n \in k \right\}.$$

We have $v(\sum a_n t^n) = \min\{n : a_n \neq 0\}$. Then $\mathcal{O} = k[[t]]$ = ring of power series in t. We get $m = \{f \in k[[t]] : f(0) = 0\}$ and we have $\mathcal{O}/m = k$.

Lemma 3.2.4.

1. *$k[[t]]^* = \{\sum_{n=0}^\infty a_n t^n : a_0 \neq 0\}$.*
2. *$k((t))$ is a field and v extends to v_0 on $k(t)$.*
3. *$k[[t]]$ is the completion of $k[t]$ w.r.t. v_0.*
4. *$k((t))$ is the completion of $k(t)$ w.r.t. v_0.*

Proof.

1. Let $\sum_{n=0}^\infty a_n t^n \in k[[t]]$ with $a_0 \neq 0$. We solve for b_n such that

$$\left(\sum_{n=0}^\infty a_n t^n\right)\left(\sum_{n=0}^\infty b_n t^n\right) = 1.$$

2. By (i) we have $k((t)) = \operatorname{Frac} k[[t]]$. In particular $k((t))$ is a field containing $k[t]$ so $k(t) \subset k((t))$. If $f(t) = t^n p(t)/q(t)$ with $p, q \in k[t]$ and $p(o), q(o) \neq 0$ then by (i) $p, , q \in k[[t]]^*$ so $v(f) = n = v_0(f)$.
3. Let $f_1, f_2, \dots$ be a Cauchy sequence in $k[[t]]$. Then given r there exists N s.t. for all $m, n \geq N$ we have $f_m \equiv f_n \pmod{t^{n+1}}$. Let c_r = coefficient of t^r in f^N. Then $f_n \to g$ where $g = \sum_{r=0}^\infty c_r t^r$ and therefore $k[[t]]$ is complete. But $k[t] \subset k[[t]]$ is a dense subset, therefore $k[[t]]$ is the completion of $k[t]$.
4. Likewise.

□

3.3 The Teichmuller map

Definition 3.3.1 (Teichmuller representatives)**.** Let k be complete w.r.t. a discrete valuation v. Suppose that the residue field k is finite, say $|k| = q$. Let $f(x) = x^q - x \in \mathcal{O}[X]$. Each $\alpha \in k$ is a simple root of $\bar{f} \in k[x]$. Hensel's lemma implies that there is a unique $a \in \mathcal{O}$ s.t. $a^q = a$ and $a \equiv \alpha \pmod{\pi}$. The $a \in \mathcal{O}$ constructed here is the **Teichmuller representative** for $\alpha \in k$.

Lemma 3.3.2. *The map $[\cdot]\colon k \to \mathcal{O}$ given by $\alpha \mapsto a$ is multiplicative.*

Proof. Let $\alpha, \beta \in k$ we have $([\alpha][\beta])^q = [\alpha]^q[\beta]^q = [\alpha][\beta]$ and $[\alpha][\beta] \equiv \alpha\beta \pmod{\pi}$ giving $[\alpha\beta] = [\alpha][\beta]$. $\square$

Example 3.3.3. $\mu_{p-1} \subset \mathbf{Z}_p^*$.

Theorem 3.3.4. *Let K be field complete w.r.t. a discrete valuation v. If* $\operatorname{char} K > 0$ *and k is finite then $K \cong k((t))$.*

Proof. $\operatorname{char}(K) = \operatorname{char}(k) = p$ and $|k| = q = p^l$. Let $\alpha, \beta \in k$ so we have $([\alpha] + [\beta])^q = [\alpha]^q + [\beta]^q = [\alpha] + [\beta]$ and hence $[\alpha + \beta] = [\alpha] + [\beta]$. Therefore the Teichmuller map $k \hookrightarrow K$ is a field embedding. By lemma 2.3

$$K = \left\{ \sum_{n \geq n_0}^{\infty} a_n \pi^n : a_n \in k \right\} \xrightarrow{\sim} k((t))$$

via the map $\pi \mapsto t$. $\square$

Chapter 4

Dedekind domains

4.1 Dedekind domains

Definition 4.1.1 (Dedekind domains)**.** A **Dedekind domain** is a ring R that is

1. an integral domain,
2. Noetherian,
3. integrally closed,
4. has all non-zero prime ideals maximal (Krull dimension ≤ 1).

Example 4.1.2. Any PID is a Dedekind domain.
The ring of integers of a number field is a Dedekind domain.

Theorem 4.1.3. *Let R be a Dedekind domain. Then every non-zero ideal $I \subset R$ can be written uniquely as a product of prime ideals $I = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.*

Proof. Omitted. □

Remark 4.1.4. If R is a PID then the above theorem follows from PID implying UFD.

Theorem 4.1.5. *R is a DVR if and only if it is a Dedekind domain with exactly one non-zero prime.*

Proof. $\Longrightarrow$ is clear since being a PID implies being Dedekind.
□

4.2 Localisation

Let R be an integral domain and $p \subset R$ a prime ideal. Let $S = R \setminus p$ and $S^{-1}R = \{\frac{r}{s} : r \in R, s \in S\} \subset \operatorname{Frac} R$. This is a local ring with maximal ideal $S^{-1}p$. R being Dedekind implies $S^{-1}R$ is, and hence $S^{-1}R$ is a DVR by the above theorem

Theorem 4.2.1. *Let $\mathcal{O}_K$ be a Dedekind domain, $K = \operatorname{Frac} \mathcal{O}_K$ and L/K a finite field extension. Then take $\mathcal{O}_L$ to be the integral closure of $\mathcal{O}_K$ in L, then $\mathcal{O}_L$ is a Dedekind domain.*

Proof. That $\mathcal{O}_L$ is a domain is clear.
It is also clear that it is integrally closed.
To see it is Noetherian we suppose that L/K is a separable and write $n = [L : K]$. There are n distinct embeddings $\sigma_1, \ldots, \sigma_n : L \to \bar{K}$. The trace form $L \times L \to K$ given by $(x, y) \mapsto \operatorname{tr} xy$ is a non-degenerate K-bilinear form. (Using primitive element and expressing as a Vandermonde determinant) Let $x_1, \ldots, x_n$ be a basis for L as K-vector space. Clearing denominators allows us to take $x_i \in \mathcal{O}_L$. Let $y_1, \ldots, y_n$ be the dual basis w.r.t. the trace form. Let $z \in \mathcal{O}_L$ then $z = \sum_{j=1}^{n} \lambda_j y_j$ for some $\lambda_i \in K$, giving that $\lambda_i = \operatorname{tr}_{L/K}(x_i z) \in \mathcal{O}_K$. So $\mathcal{O}_L \subset y_1\mathcal{O}_K + \cdots + y_n\mathcal{O}_K$. $\mathcal{O}_K$ being noetherian gives that $\mathcal{O}_L$ is a f.g. $\mathcal{O}_K$-module and so $a\mathcal{O}_L$ is noetherian too.
Now to see that all non-zero primes are maximal we fix P a non-zero prime of $\mathcal{O}_L$. Then taking $p = P \cap \mathcal{O}_K$ we have a prime of $\mathcal{O}_K$. We can find $x \in p \setminus 0$ so that $0 \neq N_{L/K}(x) \in P \cap \mathcal{O}_K = p$. $\mathcal{O}_K$ being Dedekind gives p maximal and so $k = \mathcal{O}_K/p \hookrightarrow \mathcal{O}_L/P$ gives that $\mathcal{O}_L/P$ is a f.d. k-algebra. But $\mathcal{O}_L/P$ is an integral domain and so applying rank-nullity to $\cdot x$ gives $\mathcal{O}_L/P$ is a field. □

Lemma 4.2.2. *If R is a Dedekind domain and $K = \operatorname{Frac} R$ with an absolute value $|\cdot|$ on K with $|x| \leq 1$ for all $x \in R$ then $|\cdot| \sim |\cdot|_p$ for some prime p of R.*

Proof. Lemma 1.1 implies $|\cdot|$ is non-archimidean. Let $p = \{x \in R : |x| < 1\}$, this is a prime ideal. Localising at $R \setminus p$ gives a DVR by Theorem 3.2 this has valuation v_p. Take $\pi \in p \setminus p^2$ so we can write $x \in K^*$ as $x = u\pi^r$ where $|u|_p = 1$ and $r \in \mathbf{Z}$. To prove $|\cdot| \sim |\cdot|_p$ we need to show that $|\pi| < 1$ (which is true as $\pi \in p$) and also that $|u| = 1$. We have $|u|_p \leq 1$ which gives $u \in S^{-1}R$ so $u = r/s$ for $r \in R, s \in R$ we know $|r| \leq 1$ and $|s| = 1$ so $|u| \leq 1$. We can do the same for u^{-1} to get $|u| = 1$. □

Theorem 4.2.3. *$\mathcal{O}_K$ is a Dedekind domain, $K = \operatorname{Frac} \mathcal{O}_K$, L/K finite field extension, $\mathcal{O}_L$ integral closure of $\mathcal{O}_K$ in L. Let $p \subset \mathcal{O}_K$ be a prime ideal, then $p\mathcal{O}_L = P_1^{e_1} \cdots P_r^{e_r}$ for distinct primes P_i. Then the absolute values on L extending $|\cdot|_p$ on K are (up to equivalence) $|\cdot|_{P_1}, \ldots, |\cdot|_{P_r}$.*

Proof. $\mathcal{O}_L$ is Dedekind . Take $x \in K^*$ we have $v_{P_i}(x) = e_i v_p(x)$ so $|\cdot|_{P_i}$ is equivalent to an absolute value extending $|\cdot|_p$. Now let $|\cdot|$ be any such absolute value on L, it will be non-archimidean by . $\mathcal{O}_K \subset \{x \in L : |x \ \leq 1\}$ so taking integral closures in L we get $\mathcal{O}_L \subset \{x \in L : |x| \leq 1\}$. Lemma 3.4 gives that $|\cdot| \sim |\cdot|_P$ for some prime $P \subset \mathcal{O}_L$. But $|\cdot|$ extends $|\cdot|_p$ so $P \cap \mathcal{O}_K = p$ giving $P = P_i$ for some i. □

Corollary 4.2.4. *The non-archimidean places of a number field K are $|\cdot|_p$ for p a prime of $\mathcal{O}_K$.*

Chapter 5

Relative extensions

Definition 5.0.1 (Norms)**.** Let V be a vector space over$K$. A **norm** on v is a map $\|\cdot\|: V \to \mathbf{R}$ s.t.

1. $\|v\| \geq 0$ with equality iff $v = 0$.

2. $\|\lambda v\| = |\lambda|\|v\|$

3. $\|v + w\| \leq \|v\| + \|w\|$.

Theorem 5.0.2. *Let K be complete $|\cdot|$ on K. If $\dim_K V < \infty$ then any two norms on V are equivalent and V is complete (w.r.t. any one of them).*

Proof. WLOG $V = K^d$ and we will show every norm is equivalent to $\|\cdot\|_{\sup}$, the proof is via induction on d. For $d = 1 \|v\| = c\|v\|_{\sup}$ for some $c > 0$ and the result is clear.
For generl d we let $e_1, \ldots, e_d$ be the standard basis, so

$$\|x\| = \left\|\sum_{i=1}^{d} x_i e_i\right\| \leq \left(\sum_{i=1}^{d} \|e_i\|\right) \max_{1 \leq i \leq d} |x_i|.$$

Let $S = \{v \in V | \|v\|_{\sup} = 1\}$ (the equation implies that $\|\cdot\|: S \to \mathbf{R}_{\geq 0}$ is continuous w.r.t. $\|\cdot\|_{\sup}$ but we don't know S is compact).
We now claim that there exists $\epsilon > 0$ s.t. $\|x\| > \epsilon$ for all $x \in S$. To see this suppose otherwise, i.e. that there exists a sequence $(x^{(n)})$ in$S$ with $\|x^(n)\| \to 0$ as $n \to \infty$. For at least one $1 \leq i \leq d \|x^{(n)}\|_{\sup} = |x_i^{(n}|$ for infinitely many n. WLOG this is $i = d$ and we may pass to a subsequence and multiply through by $\lambda \in K$ with $|\lambda| = 1$ to ensure $x_d^{(n)} = 1$ i.e. $x^{(n)} = y^{(n)} + e_d$ for some $y^{(n)} \in \langle e_1, \ldots, e_{d-1}\rangle$. But as $x^{(n)} \to 0$ w.r.t. $\|\cdot\|$ we have that $x^{(n)}$ is Cauchy and hence so is $y^{(n)}$ w.r.t. $\|\cdot\|$. This implies that $y^{(n)} \to y$ w.r.t. $\|\cdot\|$ (since K^{d-1} is complete by the induction hypothesis) for some $y \in \langle e_1, \ldots, e_{d-1}\rangle$ but $y^{(n)} = x^{(n)} - e_d \to -e_d$ w.r.t. $\|\cdot\|$ therefore $y = -e_d \notin \langle e_1, \ldots, e_{d-1}\rangle$ a contradiction, proving the claim.
Now let $x \in Vx \neq 0$ and $\|\cdot\|_{\sup} = |x_i|$ for some $1 \leq i \leq d$. $x/x_i \in S$ son $\|x/x_i\| > \epsilon$ implying $\|x\| > \epsilon|x_i| = \epsilon\|x\|_{\sup}$. This together with the above equation give that $\|\cdot\|$ and $\|\cdot\|_{\sup}$ are equivalent, K complete implies that V is complete w.r.t. $\|\cdot\|_{\sup}$. $\square$

Theorem 5.0.3. $(K, |\cdot|)$ *complete L/K finite extension. If $|\cdot|_1, |\cdot|_2$ absolute values on L extending ab on K then $|\cdot|_1 = |\cdot|_2$ and L is complete w.r.t. $|\cdot|_1$.*