Part III Local Fields

Based on lectures by Dr C. Johansson

Michaelmas 2016
University of Cambridge

Contents

1 Basic Theory

Definition 1 (Absolute value)**.** *Let K be a field. An **absolute value** on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ s.t.*

i. $|x| = 0 \iff x = 0$

ii. $|xy| = |x|\,|y| \quad \forall x, y \in K$

iii. $|x + y| \leq |x| + |y|$

Definition 2 (Valued field)**.** *A **valued field** is a field with an absolute value.*

Definition 3 (Equivalence of absolute values)**.** *Let K be a field and let $|\cdot|$, $|\cdot|'$ be absolute values on K. We say that $|\cdot|$ and $|\cdot|'$ are **equivalent** if the associated metrics induce the same topology.*

Definition 4 (Non-archimedean absolute value)**.** *An absolute value $|\cdot|$ on a field K is called **non-archimedean** if $|x + y| \leq \max(|x|, |y|)$ (the **strong triangle inequality**).*

*Metrics s.t. $d(x, z) \leq \max(d(x, y), d(y, z))$ are called **ultrametrics**.*

Assumption: unless otherwise mentioned, all absolute values will be non-archimedean. These metrics are weird!

Proposition 5. *Let K be a valued field. Then $\mathcal{O} = \{x \mid |x| \leq 1\}$ is an open subring of K, called the* ***valuation ring*** *of K. $\forall r \in (0,1]$, $\{x \mid x < r\}$ and $\{x \mid x \leq r\}$ are open ideals of $\mathcal{O}$.*

Moreover, $\mathcal{O}^x = \{x \mid |x| = 1\}$.

Proposition 6. *Let K be a valued field.*

i. Let (x_n) be a sequence in K. If $x_n - x_{n+1} \to 0$ then (x_n) is Cauchy

Assume that K is complete

ii. Let (x_n) be a sequence in K. If $x_n - x_{n+1} \to 0$ then (x_n) converges

iii. Let $\sum_{n=0}^{\infty} y_n$ be a series in K. If $y_n \to 0$, then $\sum_{n=0}^{\infty} y_n$ converges

Definition 7. *Let $R \subseteq S$ be rings. Then $s \in S$ is* ***integral over R*** *if $\exists$ monic $f(x) \in R[x]$ s.t. $f(s) = 0$.*

Proposition 8. *Let $R \subseteq S$ be rings. Then $s_1, \ldots, s_n \in S$ are all integral over $R \iff R[s_1, \ldots, s_n] \subseteq S$ is a finitely generated R-module.*

Corollary 9. *let $R \subseteq S$ be rings. If $s_1, s_2 \in S$ are integral over R, then $s_1 + s_2$ and $s_1 s_2$ are integral over R. In particular, the set $\tilde{R} \subseteq S$ of all elements in S integral over R is a ring, called the* ***integral closure*** *of R in S.*

Definition 10. *Let R be a ring. A topology on R is called a* ***ring topology*** *on R if addition and multiplication are continuous maps $R \times R \to R$. A ring with a ring topology is called a* ***topological ring****.*

Definition 11. *Let R be a ring, $I \subseteq R$ an ideal. A subset $U \subseteq R$ is called* ***I-adically open*** *if $\forall x \in U$ $\exists n \geq 1$ s.t. $x + I^n \subseteq U$.*

Proposition 12. *The set of all I-adically open sets form a topology on R, called the* ***I-adic topology****.*

Definition 13. *Let $R_1, R_2, \ldots$ be topological rings with continuous homomorphisms $f_n : R_{n+1} \to R_n$ $\forall n \geq 1$. The* ***inverse limit*** *of the R_i is the ring*

$$\begin{aligned} \varprojlim_n R_n &= \left\{ (x_n) \in \prod_n R_n \mid f_n(x_{n+1}) = x_n \forall n \geq 1 \right\} \\ &\subseteq \prod_n R_n \end{aligned}$$

Proposition 14. *The inverse limit topology is a ring topology.*

Definition 15. *Let R be a ring, I an ideal. The **I-adic completion** of R is the topological ring $\varprojlim_n R/I^n$ (R/I^n has the discrete topology, and $R/I^{n+1} \to R/I^n$ is the natural map).*

*There exists a map $\nu : R \to \varprojlim R/I^n$, $r \mapsto (r \mod I^n)_n$ This map is a continuous ring homomorphism when R is given the I-adic topology. We say that R is **I-adically complete** if ν is a bijection.*

*If $I = xR$ then we often call the I-adic topology the **x-adic topology**.*

1.1 The p-adic Numbers

Let p be a prime number throughout.

If $x \in \mathbb{Q}\backslash\{0\}$ then $\exists!$ representation $x = p^n \frac{a}{b}$, where $n \in \mathbb{Z}$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}_{>0}$ and $(a, p) = (b, p) = (a, b) = 1$.

We define the **p-adic absolute value** on $\mathbb{Q}$ to be the function $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ given by

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

Then $|\cdot|_p$ is an absolute value.

Definition 16. *The **p-adic numbers** $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$.*

*The valuation ring $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ is called the **p-adic integers**.*

Proposition 17. *$\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$.*

Proposition 18. *The non-zero ideals of $\mathbb{Z}_p$ are $p_n\mathbb{Z}_p$ for $n \geq 0$. Moreover, $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$*

Corollary 19. *$\mathbb{Z}_p$ is a PID with a unique prime element p (up to units).*

Proposition 20. *The topology on $\mathbb{Z}$ induced by $|\cdot|_p$ is the p-adic topology.*

Proposition 21. *$\mathbb{Z}_p$ is p-adically complete and is (isomorphic to) the p-adic completion of $\mathbb{Z}$.*

Corollary 22. *Every $a \in \mathbb{Z}_p$ has a unique expansion*

$$a = \sum_{i=0}^{\infty} a_i p^i$$

with $a_i \in \{0, 1, \ldots, p-1\}$

Every $a \in \mathbb{Q}_p^\times$ has a unique expansion

$$a = \sum_{i=n} \infty a_i p^i$$

$n \in \mathbb{Z}$, $n = -\log_p |a|_p$, $a_n \neq 0$.

1.2 Valued Fields

Definition 23. *Let K be a field. A **valuation** on K is a function $v : K \to \mathbb{R} \cup \{\infty\}$ s.t.*

i. $v(x) = \infty \iff x = 0$

ii. $v(xy) = v(x) + v(y)$

iii. $v(x + y) \geq \min(v(x), v(y))$

$\forall x, y \in K$.

Here we use the conventions $r + \infty = \infty$, $r \leq \infty \; \forall r \in \mathbb{R} \cup \{\infty\}$. v a valuation $\implies$ if $|x| = c^{-v(x)}$, $c \in \mathbb{R}_{>1}$, then $|\cdot|$ is an absolute value. Conversely, if $|\cdot|$ is an absolute value then $v(x) = -\log_c |x|$.

Let K be a valued field.

- $\mathcal{O} = \mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$ is the **valuation ring**
- $\mathfrak{m} = \mathfrak{m}_K = \{x \in K \mid |x| < 1\}$ is the **maximal ideal**
- $k = k_K = \mathcal{O}/\mathfrak{m}$ is the **residue field**

Definition 24. *If K is a valued field and $F(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ is a polynomial, we say that F is **primitive** if $\max_i |a_i| = 1$ ($\implies F \in \mathcal{O}[x]$).*

Theorem 25 (Hensel's Lemma)**.** *Assume that K is complete and that $F \in K[x]$ is primitive. Put $f = F \mod \mathfrak{m} \in k[x]$. If $\exists$ factorisation $f(x) = g(x)h(x)$ with $(g, h) = 1$, then $\exists$ factorisation $F(x) = G(x)H(x)$ in $\mathcal{O}[x]$ with $g \equiv G$, $h \equiv H \mod \mathfrak{m}$ and $\deg g = \deg G$.*

Proof. Put $d = \deg F$, $m = \deg g$, so $\deg h \leq d - m$. Pick lifts $G_0, H_0 \in \mathcal{O}[x]$ of g, h with $\deg G_0 = \deg g$, $\deg H_0 \leq d - m$.

$(g, h) = 1 \implies \exists A, B \in \mathcal{O}[x]$ s.t. $AG_0 + BH_0 \equiv 1 \mod \mathfrak{m}$.

Pick $\pi \in \mathfrak{m}$ s.t. $F - G_0 H_0 \equiv AG_0 + BH_0 - 1 \mod \pi$.

Want to find $G = G_0 + \pi P_1 + \pi^2 P_2 + \ldots$, $H = H_0 + \pi Q_1 + \pi^2 Q_2 + \cdots \in \mathcal{O}[x]$ with $P_i, Q_i \in \mathcal{O}[x]$, $\deg P_i < m$, $\deg Q_i \leq d - m$.

Define

$$G_{n-1} = G_0 + \pi P_1 + \cdots + \pi^{n-1} P_{n-1}$$
$$H_{n-1} = H_0 + \pi Q_1 + \cdots + \pi^{n-1} Q_{n-1}$$

We want $F \equiv G_{n-1} H_{n-1} \mod \pi^n$, then take the limit.

Induction on n: $n = 1$ ✓

Assume we have G_{n-1}, H_{n-1}, $G_n = G_{n-1} + \pi^n P_n, H_n = H_{n-1} + \pi^n Q_n$. Expanding $F - H_n G_n$, we want

$$F - G_{n-1}H_{n-1} \equiv \pi^n (G_{n-1}Q_n + H_{n-1}P_n) \mod \pi^{n+1}$$

and divide by π^n

$$G_{n-1}Q_n + H_{n-1}P_n = \frac{1}{\pi^n}(F - G_{n-1}H_{n-1}) \mod \pi$$

Let $F_n := F - G_{n-1}H_{n-1}$. $AG_o + BH_0 \equiv 1 \mod \pi \implies F_n \equiv AG_0F_n + BH_0F_n \mod \pi$.

Write $BF_n = QG_0 + P_n$ with $\deg P_n < \deg G_0$, $P_n \in \mathcal{O}[x]$

$$\implies G_0(AF_n + H_0Q) + H_0P_n \equiv F_n \mod \pi$$

Now omit all coefficients from $AF_n + H_0Q$ divisible by π to get Q_n. □

Corollary 26. *Let $F(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$, K complete, $a_0a_n \neq 0$. If F is irreducible, then $|a_i| \leq \max(|a_0|, |a_n|)$ $\forall i$.*

Corollary 27. *$F \in \mathcal{O}[x]$ monic, K complete. If $F \mod \mathfrak{m}$ has a simple root $\bar{\alpha} \in k$, then F has a (unique) simple root $\alpha \in \mathcal{O}$ lifting $\bar{\alpha}$.*

Useful fact: let K be a valued field, $x, y \in K$. $|x| > |y| \implies |x + y| = |x|$. More generally, if we have a convergent series $\sum_{i=0}^{\infty} x_i$ and the non-zero $|x_i|$ are distinct, then $|x| = \max |x_i|$.

Theorem 28. *Let K be a complete valued field and let L/K be a finite extension. Then the absolute value $|\cdot|$ on K has a unique extension to an absolute value $|\cdot|_L$ on L, given by*

$$|\alpha|_L = \sqrt[n]{\left|N_{L/K}(\alpha)\right|},\ n = [L : K]$$

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

Corollary 29. *Let K be a complete valued field. If M/K is an algebraic extension of K, then $|\cdot|$ extends uniquely to an absolute value on M.*

Corollary 30. *In the setting of Theorem 16, if $\sigma \in \mathrm{Aut}(L/K)$ then $|\sigma(\alpha)|_L = |\alpha|_L$ $\forall \alpha \in L$*

Definition 31. *Let K be a valued field and V a vector space over K. A **norm** on V is a function $||\cdot|| : V \to \mathbb{R}_{\geq 0}$ such that*

i. $||x|| = 0 \iff x = 0$

ii. $||\lambda x|| = |\lambda|\,||x|| \;\; \forall \lambda \in K, x \in V$

iii. $||x+y|| \leq \max(||x||, ||y||) \; \forall x, y, \in V$

Two norms $||\cdot||, ||\cdot||'$ *are* ***equivalent*** *if they induce the same topology on* V $\iff \exists C, D > 0$ *s.t.* $C\,||x|| \leq ||x||' \leq D\,||x|| \;\; \forall x \in V$.

Proposition 32. *Let* K *be a complete valued field and* V *a finite dimensional* K*-vector sapce. Let* $x_1, \ldots, x_n$ *be a basis of* V*, then if* $x = \sum a_i x_i \in V$*,*

$$||x||_{\max} = \max_i |a_i|$$

defines a norm on V*, and* V *is complete w.r.t* $||\cdot||_{\max}$*.*

Moreover, if $||\cdot||$ *is any norm on* V*, then* $||\cdot||$ *is equivalent to* $||\cdot||_{\max}$ *and hence* V *is complete w.r.t* $||\cdot||$*.*

Lemma 33. *Let* K *be a valued field. Then* $\mathcal{O}_K$ *is integrally closed in* K*.*

Corollary 34. *Let* K *be a complete valued field,* L/K *finite. Equip* L *with* $|\cdot|_L$ *extending* $|\cdot|$ *on* K*. Then* $\mathcal{O}_L$ *is the integral closure of* $\mathcal{O}_K$ *inside* L*.*

1.3 Newton Polygons

Definition 35. $S \subset \mathbb{R}^2$ *is* ***lower convex*** *if*

i. $(x, y) \in S \implies (x, z) \in S \; \forall z \geq y$

ii. S *is convex*

Given any $T \subset \mathbb{R}^2$, there exists a minimal lower convex $LCH(T) \supseteq T$ ($LCH(T) = \bigcap_{T \subset S', S' \text{lower convex}} S'$).

Definition 36. *Let* $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ *where* K *is a valued field,* v *a valuation on* K*.*

Define the ***Newton polygon*** *of* f *as* $LCH\left(\left\{(i, v(a_i)) \;\middle|\; \begin{array}{c} i = 0, 1, \ldots, n \\ a_i \neq 0 \end{array}\right\}\right)$.

Definition 37. *The horizontal length of a line segment is called the* ***multiplicity****. Line segments have a* ***slope****.*

Theorem 38. *Let* K *be a complete valued field,* v *a valuation on* K*,* $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$*. Let* L *be the splitting field of* f *over* K*, equipped with the unique extension* w *of* v*.*

If $(r, v(a_r)) \to (s, v(a_s))$ *is a line segment of the Newton polygon of* f *with slope* $-m \in \mathbb{R}$*, then* f *has precisely* $s - r$ *roots of valuation* m*.*

Proof. Dividing by a_n only shifts the NP vertically, so wlog $a_n = 1$.

Number the roots of f s.t.

$$\begin{array}{ccccccc} v(\alpha_1) & = & \dots & = & v(\alpha_{s_1}) & = & m_1 \\ v(\alpha_{s_1+1}) & = & \dots & = & v(\alpha_{s_2}) & = & m_2 \\ \vdots & & & & \vdots & & \vdots \\ v(\alpha_{s_t+1}) & = & \dots & = & v(\alpha_{s_1}) & = & m_{t+1} \end{array}$$

where $m_1 < m_2 < \cdots < m_{t+1}$, and the α_i are the roots of f with multiplicity.

$v(a_n) = v(1) = 0$

$v(a_{n-1}) = v(\sum_i a_i) \geq \min_i v(\alpha_i) = m_1$

$v(a_{n-2}) \geq \min_{i \neq j} v(\alpha_i \alpha_j) = 2m_1$

$v(a_{n-s_1}) = v(\sum_{i_1, \dots i_{s_1} \text{ distinct}} \alpha_{i_1} \dots \alpha_{i_{s_1}}) = s_1 m_1$

$v(a_{n-s_1-1}) \geq \min v(\alpha_{i_1} \dots \alpha_{i_{s_1+1}}) = s_1 m_1 + m_2$

$\vdots$

$v(a_{n-s_2}) = \min v(\alpha_{i_1} \dots \alpha_{i_{s_2}}) = s_1 m_1 + (s_2 - s_1) m_2$

etc. Drawing the lines between the points $(n, 0)$, $(n - s_1, s_1 m_1)$, $\dots$ gives the NP of f.

The first line segment has length $n-(n-s_1) = s_1$ and slope $\frac{0 - s_1 m_1}{n-(n-s_1)} = -m_1$. For $k \geq 2$, the kth line segment has length $(n - s_{k-1}) - (n - s_k) = s_k - s_{k-1}$ and slope

$$\frac{(s_1 m_1 + \sum_{i=1}^{k-2} (s_{i+1} - s_i) m_{i+1}) - (s_1 m_1 + \sum_{i=1}^{k-1} (s_{i+1} - s_i) m_{i+1})}{(n - s_{k-1}) - (n - s_k)}$$

$$= \frac{-(s_k - s_{k-1}) m_k}{s_k - s_{k-1}} = -m_k$$

□

Corollary 39. *If f is irreducible, then the NP has a single line segment.*

Proof. we need to show that all roots have the same valuation. Let α, β be roots in the splitting field L. Then $\exists \sigma \in \mathrm{Aut}(L/K)$ s.t. $\sigma(\alpha) = \beta$. So $v(\alpha) = v(\sigma(\alpha)) = v(\beta)$ by Corollary 30. □

Definition 40. *Let K be a valued field with valuation v. K is a **discretely valued field** (DVF) if $v(K^\times) \subset \mathbb{R}$ is a discrete subgroup of $\mathbb{R}$ ($\iff$ $v(K^\times)$ is infinite cyclic).*

Definition 41. *A complete DVF with finite residue field is called a **local field**.*

Let K be a DVF. $\pi \in K$ is called a **uniformiser** if $v(\pi) > 0$ and $v(\pi)$ generates $v(K^\times)$ ($\iff$ $v(\pi)$ has minimal positive valuation).

Proposition 42. *Let K be a DVF, uniformiser π. Let $S \subset \mathcal{O}_K$ be a set of coset representatives of $\mathcal{O}_k/\mathfrak{m}_K = k_K$ containing 0. Then*

1. *The non-zero ideals of $\mathcal{O}_K$ are $\pi^n\mathcal{O}_K$, $n \geq 0$*
2. *$\mathcal{O}_K$ is a PID with unique prime π (up to units), $\mathfrak{m}_K = \pi\mathcal{O}_K$*
3. *The topology on $\mathcal{O}_K$ induced by $|\cdot|$ is the π-adic topology*
4. *If K is complete, then $\mathcal{O}_K$ is π-adically complete*
5. *If K is complete, then any $x \in K$ can be written uniquely as*

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

with $a_n \in S$ and $|x| = |pi|^{-\inf\{n \,|\, a_n \neq 0\}}$

6. *The completion $\hat{K}$ of K is a DVF, π is a uniformiser and*

$$\mathcal{O}_K/\pi^n\mathcal{O}_K \xrightarrow{\sim} \mathcal{O}_{\hat{K}}/\pi^n\mathcal{O}_{\hat{K}}$$

via the natural map.

Proof. The same as for $\mathbb{Q}_p$ and $\mathbb{Z}_p$ (use π instead of p). Note that $\left|\hat{K}\right| = |K|$ by Ex 9, sheet 1 ($\implies$ $\hat{K}$ is a DVF). □

Proposition 43. *Let K be a DVF. Then K is a local field $\iff$ $\mathcal{O}_K$ is compact*

Proof. $\mathcal{O}_K$ compact $\implies$ $\pi^{-n}\mathcal{O}_K$ is compact $\forall n \geq 0$ (π uniformiser).

$\mathcal{O}_K \cong \pi^{-n}\mathcal{O}_K \implies K = \bigcup_{n\geq 0}^{\infty} \pi^{-n}\mathcal{O}_K$ is complete.

Also $\mathcal{O}_K \twoheadrightarrow k_K$ and this map is continuous when k_K is given the discrete topology. So k_K is compact and discrete $\implies$ k_K finite.

Conversely, we seek to prove that K local $\implies$ $\mathcal{O}_K$ is sequentially compact ($\iff$ compact). Note that $\mathcal{O}_K/\pi^n\mathcal{O}_K$ is finite $\forall n \geq 0$ (induction and $\pi^{n-1}\mathcal{O}_K/\pi^n\mathcal{O}_K \cong \mathcal{O}_K/\pi\mathcal{O}_K$).

Let (x_i) be a sequence in $\mathcal{O}_K$. $\exists$ a subsequence (x_{1i}) which is constant modulo π. Keep going: choose a subsequence $(x_{n+1,i})$ of (x_{ni}) s.t. $(x_{n+1,i})$ is constant mod π^{n+1}.

Then $(x_{ii})_{i=1}^{\infty}$ converges: it's Cauchy since $|x_{ii} - x_{jj}| \leq |\pi|^j \ \ \forall j \leq i$, and K is complete. □

Definition 44. *A ring R is called a **discrete valuation ring** (DVR) if it is a PID with a unique prime element (up to units).*

Proposition 45. *R is a DVR $\iff$ $R \cong \mathcal{O}_K$ for some DVF K.*

Proof. The reverse implication is contained in Proposition 42.

Suppose R is a DVR, π prime. $\forall x \in R\backslash\{0\}$, $\exists! u \in R^\times$, $n \in \mathbb{Z}_{\geq 0}$ such that $x = \pi^n u$ by uniqueness of prime factorisation.

Define $v(x) = \begin{cases} n & \text{if } x \neq 0 \\ \infty & \text{if } x = 0 \end{cases} \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$.

v defines a discrete valuation of $R \implies v$ extends uniquely to $K = \mathrm{Frac}(R)$. It remains to show that $R = \mathcal{O}_K$. First, note that $K = R[\frac{1}{\pi}]$. Any non-zero element looks like $\pi^n u$, $u \in R^\times$, $n \in \mathbb{Z}$, so it is invertible.

Then $v(\pi^n u) = n \in \mathbb{Z}_{\geq 0} \iff \pi^n u \in R$

$\therefore R = \mathcal{O}_K$. □

Definition 46. *Let K be a valued field with residue field k_K. K has **equal characteristic** if $\mathrm{char}\, K = \mathrm{char}\, k_K$, **mixed characteristic** otherwise ($\implies \mathrm{char}\, K = 0, \mathrm{char}\, k_K > 0$).*

Definition 47. *Let R be a ring of characteristic p. R is **perfect** if the Frobenius map $x \mapsto x^p$ is an automorphism of R.*

Theorem 48. *Let K be a complete DVF of equal characteristic p and assume that k_K is perfect. Then $K \cong k_K[[T]]$ (as DVFs).*

Corollary 49. *Let K be a local field of equal characteristic p. Have $k_K \cong \mathbb{F}_q$ for some q a power of p, and $K \cong \mathbb{F}_q((T))$.*

Definition 50. *Let K be a DVF. The **normalised valuation** v_K on K is the unique valuation on K in the given equivalence class s.t. $v_K(\pi) = 1$ for any uniformiser π.*

Lemma 51. *Let R be a ring and let $x \in R$. Assume that R is x-adically complete and that R/xR is perfect of characteristic p.*

Then $\exists!$ map $[-] : R/xR \to R$ such that

$$[a] \equiv a \mod x$$
$$[ab] = [a][b]\ \forall a, b \in R/xR$$

Moreover if R has characteristic p, then $[-]$ is a ring homomorphism.

Proof. Let $a \in R/xR$. $\exists!$ $a^{p^{-n}} \in R/xR\ \forall n \geq 0$ since R/xR is perfect. Now lift arbitrarily: take $\alpha_n \in R$ such that $\alpha_n \equiv a^{p^{-n}} \mod x$.

Put $\beta_n = \alpha_n^{p^n}$.

Claim: $\lim_{n\to\infty} \beta_n$ exists and is independent of choices. Call this $[a]$.

Note that if the limit exists no matter how the α_n are chosen, then it is independent of the choices.

Want to prove $\beta_{n+1} - \beta_n \to 0$ x-adically.

$$\beta_{n+1} - \beta_n = (\alpha_{n+1}^p)^{p^n} - (\alpha_n)^{p^n}$$

$$\alpha_{n+1}^p \equiv (a^{p^{-n-1}})^p \equiv a^{p^{-n}} \equiv \alpha_n \mod x$$

The binomial theorem, R/xR characteristic p and induction $\implies$

$$(\alpha_{n+1}^p)^{p^n} \equiv \alpha_n^{p^n} \mod x^{n+1}$$

i.e. $\beta_{n+1} - \beta_n \equiv 0 \mod x^{n+1}$ so $\lim_{n\to\infty} \beta_n$ exists.

Multiplicativity: if $b \in R/xR$, with $\gamma_n \in R$ lifting $b^{p^{-n}}$ $\forall n \geq 0$, then $\alpha_n\gamma_n$ lifts $(ab)^{p^{-n}} = a^{p^{-n}}b^{p^{-n}}$

$$\implies [ab] = \lim_{n\to\infty} \alpha_n^{p^n} \lim_{n\to\infty} \gamma_n^{p^n} = [a][b]$$

$[a] \equiv a \mod x$:

$$\lim_{n\to\infty} \alpha_n^{p^n} \equiv \lim_{n\to\infty} (a^{p^{-n}})^{p^n} \equiv \lim_{n\to\infty} a \equiv a \mod x$$

Uniqueness: let $\phi : R/xR \to R$ be another map with these properties.

$$[a] = \lim_{n\to\infty} \phi(a^{p^{-n}})^{p^n} = \lim_{n\to\infty} \phi(a) = \phi(a)$$

since $\phi(a^{p^{-n}}) \equiv a^{p^{-n}} \mod x$ and ϕ is multiplicative.

Finally, if R has characteristic p, then $\alpha_n + \gamma_n$ lifts $a^{p^{-n}} + b^{p^{-n}} - (a+b)p^{-n}$, so

$$[a+b] = \lim_{n\to\infty} (\alpha_n + \gamma_n)^{p^n} = \lim_{n\to\infty} \alpha_n^{p^n} + \gamma_n^{p^n} = [a] + [b]$$

So $[-]$ is additive and multiplicative and (check!) $[1] = 1$, so it's a homomorphism. □

Definition 52. *$[-] : R/xR \to R$ is called the **Teichmüller map/lift** and $[x]$ is called the **Teichmüller lift/representative** of x.*

Proof of Theorem 48. K is a complete DVF. We want to prove that $\mathcal{O}_K \cong k_K[[T]]$.

$\mathcal{O}_K$ char $p \implies [-] : k_K \hookrightarrow \mathcal{O}_K$ is an injective ring homomorphism.

Choose a uniformiser $\pi \in \mathcal{O}_K$. Then $k_K = \mathcal{O}/\pi\mathcal{O}_K$, $\mathcal{O}_K$ π-adically complete. Now define

$$k_K[[T]] \to \mathcal{O}_K$$
$$\sum_{n=0}^{\infty} a_n T^n \mapsto \sum_{n=0}^{\infty} [a_n]\pi^n$$

It's a bijection by one of the basic properties of complete DVFs, check it's a homomorphism. □

Fact: let F be a field of characteristic p. Then F is perfect $\iff$ every finite extension of F is separable.

$\mathbb{F}_q$ is perfect for every $q = p^n$.