Part III Local Fields

Based on lectures by Dr C. Johansson

Michaelmas 2016
University of Cambridge

Contents

1 Basic Theory

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

Definition (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 (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 1. *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 2. *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. *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 3. *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 4. *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. *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. *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 5. *The set of all I-adically open sets form a topology on R, called the* ***I-adic topology****.*

Definition. *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*

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

Proposition 6. *The inverse limit topology is a ring topology.*

Definition. *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****.*

2 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. *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 7. *$\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$.*

Proposition 8. *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 9. *$\mathbb{Z}_p$ is a PID with a unique prime element p (up to units).*

Proposition 10. *The topology on $\mathbb{Z}$ induced by $|\cdot|_p$ is the p-adic topology.*

Proposition 11. *$\mathbb{Z}_p$ is p-adically complete and is (isomorphic to) the p-adic completion of $\mathbb{Z}$.*

Corollary 12. *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

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

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

3 Valued Fields

Definition. *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. *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 13 (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 14. *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 15. *$F \in \mathcal{O}[x]$ 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 16. *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*

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

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

Corollary 17. *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 18. *In the setting of Theorem 16, if $\sigma \in \mathrm{Aut}(L/K)$ then $|\sigma(\alpha)|_L = |\alpha|_L\ \forall \alpha \in L$*

Definition. *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 19. *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 20. *Let* K *be a valued field. Then* $\mathcal{O}_K$ *is integrally closed in* K.