Part III — Local Fields

Based on lectures by C. Johansson
Summary created by Kaimyn Chapman-Brown
Framework created by Dexter Chua

Michaelmas 2016

A brief summary of important ideas and results in the course

0 Introduction

Lecture 1

If we look at $f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$, what are the ways we can look for solutions $\mathbf{a} \in \mathbb{Z}^n$?

One way would be to look over $\mathbb{R}$, but the point of this course is to package all of the information modulo $p^n \forall n \geq 0$ together.

Notation. Throughout this course, all rings will be commutative with a 1, unless otherwise stated.

1 Basic Theory

1.1 Some Generalities

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) $|xy| = |x| \cdot |y| \quad \forall x, y \in K$

(iii) $|x + y| \leq |x| + |y| \quad \forall x, y \in K$

Example. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $|z| = \sqrt{z\bar{z}}$

Note that $||x| - |y|| \leq |x - y| \; \forall x, y$. Also, an absolute value defines a metric $d(x, y) = |x - y|$ on K

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

Definition 3 (Equivalent)**.** If K is a field, then two absolute values $|\cdot|, |\cdot|'$ are **equivalent** if they induce the same topology.

Exercise 4. Using notation as in Definition 3, prove that TFAE

(i) $|\cdot|$ and $|\cdot|'$ are equivalent

(ii) $\forall x \in \quad |x| < 1 \Rightarrow |x|' < 1$

(iii) $\exists s \in \mathbb{R}_{>0}$ s.t. $|x|^s = |x|' \quad x \in K$

Exercise 5. Let K be a valued field. Then the completion $\hat{K}$ of K is independent of $|\cdot|$ up to equivalence, and it is a valued field with an absolute value extending $|\cdot|$.

Definition 6 (Archimedean)**.** An absolute value $|\cdot|$ on a field K is called **non-Archimedean** if it satisfies the strong triangle inequality, i.e.

$$|x + y| \leq \max(|x|, |y|)$$

Otherwise, the absolute value is **Archimedean**.

Unless otherwise mentioned, **all absolute values will be non-Archimedean**. Also, all **absolute values are assumed to be non-trivial**.

Definition. If K is a valued field, then the **valuation ring** of K is $\mathcal{O} = \{x \; : \; |x| \leq 1\}$.

Proposition 7. (i) $\mathcal{O}$ is an open subring of K

(ii) $\forall r \in (0, 1]$, $\{x \; : \; |x| < r\}$ and $\{x \; : \; |x| \leq r\}$ are open ideals of $\mathcal{O}$

(iii) $\mathcal{O}^\times = \{x \; : \; |x| = 1\}$

Proof. Fairly trivial - obvious proof for each section works. □

Proposition 8. Let K be a valued field. For parts (ii) and (iii), assume that K is complete.

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

(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.

Proof. The first follows from the Archimedean assumption - use epsilons and that:

$$|x_m - x_n| = |x_m - x_{m-1} + x_{m-1} - \cdots - x_n| \leq \max(|x_m - x_{m-1}|, \cdots, |x_{n+1} - x_n|)$$

The other two follow easily from the first. □

Lecture 2

Definition 9 (Integral Over a Ring)**.** Let $R \subseteq S$ be rings, then $s \in S$ is **integral over** R if there exists a monic $f(x) \in R[x]$ s.t. $f(s) = 0$.

Proposition 10. Let $R \subseteq S$ be rings. Then, $s_1, \cdots, s_n \in S$ are integral over $R \iff R[s_1, \cdots, s_n] \subseteq S$ is a finitely generated R-module.

Proof. We do the $\Rightarrow$ direction first.
By induction, it suffices to prove the case $n = 1$. Pick a monic poly with $f(s) = 0$, and construct any other polynomial using this and the division algorithm, so that $1, s, \cdots, s^{\deg f - 1}$ is a basis of $R[s]$.
For the $\Leftarrow$ direction, pick R-module generators and an element from $b \in R[s_1, \cdots, s_n]$. Write bt_i in terms of the t_j to make a matrix, then use its determinant and an "inverse" (adjoint) to get a polynomial from the determinant. $\square$

Corollary 11. Let $R \subseteq S$ be rings. If s_1, s_2 are integral over R, then $s_1 + s_2$ and $s_1 s_2$ are integral over R.
Moreover, the set $\widetilde{R} \subseteq S$ of all elements of S integral over R is a ring.

Definition (Integral Closure)**.** $\widetilde{R}$ is called the **integral closure** of R in S. If $R = \widetilde{R}$, then we say R is integrally closed in S.

Proof. $s_1 s_2$ integral over R, so $R[s_1, s_2]$ finite over R and hence any $b \in R[s_1, s_2]$ is integral over R. $\square$

Definition 12 (Ring Topology)**.** Let R be a ring. A topology on R is called a **ring topology** on R if addition and multiplication are a continuous map $R \times R \to R$, where $R \times R$ is given the product topology.
A ring with a ring topology is called a **topological ring**.

Exercise. Let K be a valued field. Then K is a topological ring.

Definition 13 (I-adically Open)**.** 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 14. The set of all I-adically open sets form a topology on R, call the I-adic topology.

Proof. ϕ, R are I-adically open by definition, as are arbitrary unions of I-adically open sets. Also, if U, V are I-adically open and $x \in U \cap V$ with $x + I^m \subseteq U$ and $x + I^n \subseteq V$, then $x + I^{\max(m,n)} \subseteq U \cap V$ $\square$

Exercise. The I-adic topology is a ring topology of R.

Definition 15 (Inverse Limit)**.** Let $R_1, R_2, \cdots$ be topological rings with continuous homomorphisms $f_n : R_{n+1} \to R_n$ $\forall n \geq 1$. Then, the **inverse limit** or **projective limit** of the R_i is the ring:

$$\underset{\mathrm{n}}{\overset{\lim}{\longleftarrow}} = \left\{ (x_n) \in \prod_n R_n \ : \ f_n\left(x_{n+1}\right) = x_n \ \forall n \geq 1 \right\} \subseteq \prod_n R_n$$

with coordinate-wise addition/multiplication, together with the subspace topology[1] induced by the product topology on $\prod_n R_n$.

Proposition 16. The inverse limit topology is a ring topology.

[1] called the inverse limit topology

Proof. Use that $\prod R_n \times \prod R_n \to \prod R_n$ is continuous, with the map being coordinate-wise addition/multiplication, as well as containment of the inverse limit inside $\prod R_n$ and the projection map. Also, use the map $\left(\varprojlim_{n} R_n\right) \times \left(\varprojlim_{n} R_n\right) \to \prod R_n \times \prod R_n$ □

Definition 17 (I-adic completion)**.** R a ring, I an ideal. The ***I*-adic completion** of R is the topological ring:

$$\varprojlim_{n} R/I^n$$

Where R/I^n has the discrete topology and $R/I^{n+1} \to R/I^n$ is the natural map.

$$\mathscr{A} \subset X^{\lfloor n/2 \rfloor} \cup X^{\lceil n/2 \rceil}$$

Lecture 3

Definition (I-adically Complete)**.** R a ring, $I \subseteq R$ an ideal. Then $\exists$ a map

$$\begin{aligned} \nu : R &\to \left(\varprojlim_{n} R/I^n\right) \\ r &\mapsto (r \bmod I^n)_n \end{aligned}$$

This map is a cts ring homomorphism when R is given the I-adic topology. We say that R is ***I*-adically complete** if ν is a bijection.

Exercise. If ν is a bijection, then ν is a homeomorphism

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

2 The p-adic numbers

From now on in this course, p will be taken to mean a prime number.
If $x \in \mathbb{Q} \setminus \{0\}$, then there is a unique representation $p^n \frac{a}{b}$, where $a, n \in \mathbb{Z},\ b \in \mathbb{Z}_{\geq 0}$ and $(a,p) = (b,p) = (a,b) = 1$

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

$$|x|_p = \begin{cases} 0, & \text{if } x = 0 \\ p^{-n}, & \text{if } x = p^n \frac{a}{b} \quad \text{(i.e. } x \neq 0) \end{cases}$$

That $|\cdot|$ is a (non-Archimedean) absolute value is clear.

Fact. $x \in \mathbb{Z}_{\neq 0} \implies |x|_p = p^{-n} \iff p^n \| x$

Definition 18 (p-adic Numbers/Integers)**.** The **p-adic numbers**, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$
The valuation ring $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ :\ |x|_p \leq 1\}$ is called the **p-adic integers**.

Proposition 19. $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$.

Proof. Consider that $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \ :\ |x|_p \leq 1\}$ is dense in $\mathbb{Z}_{(p)}$ and that $\mathbb{Z} \subseteq \mathbb{Z}_{(p)}$. Show that $\mathbb{Z}$ is dense in $\mathbb{Z}_{(p)}$. ☐

Proposition 20. The non-zero ideals of $\mathbb{Z}_p$ are $p^n\mathbb{Z}_p$ for $p \geq 0$. Moreover,

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

Proof. Pick an ideal I and a maximal element $x \neq 0$ from it. Show that $I = xR$ and $p^n\mathbb{Z}_p = x\mathbb{Z}_p$ to get the first part.
For the second part, look at $f_n \ :\ \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ and its kernel (which is $p^n\mathbb{Z}$), showing that it induces an isomorphism. ☐

Corollary 21. $\mathbb{Z}_p$ is a PID with a unique prime element p (up to units).

Proposition 22. The topology on $\mathbb{Z}$ induced by $|\cdot|_p$ is the p-adic topology

Proof. Straightforward - pick $U \subseteq \mathbb{Z}$ and show it directly. ☐

Proposition 23. $\mathbb{Z}_p$ is p-adically complete and is isomorphic to the p-adic completion of $\mathbb{Z}$.

Proof. The second part follows from the first by the proof of Proposition 20 via

$$\mathbb{Z}_p \xleftarrow{\nu} \left(\underset{\text{n}}{\overset{\text{lim}}{\longleftarrow}} \mathbb{Z}_p/p^n\mathbb{Z}_p\right) \xrightarrow{\nu} \lim \mathbb{Z}/p^n\mathbb{Z}$$

To prove the first part, we get injectivity by looking at $x \in \ker(\nu) \iff x \in p^n\mathbb{Z}_p\ \forall n \iff x = 0$.
We get surjectivity by picking $(z_n) \in \underset{\text{n}}{\overset{\text{lim}}{\longleftarrow}} \mathbb{Z}_p/p^n\mathbb{Z}_p$ with the unique representative of z_n in $\{0, 1, \cdots, p^n - 1\}$ as $x_n = \sum_{i=0}^{n-1} a_i p_i$, then considering $x = \sum_{i=0}^{\infty} a_i p^i$. ☐

Lecture 4

Corollary 24. Every $a \in \mathbb{Z}_p$ has a unique expansion $a = \sum_{i=0}^{\infty} a_i p^i$ with $a_i \in \{0, 1, \cdots, p-1\}$
Also, every $a \in \mathbb{Q}_p^\times$ has a unique expansion $a = \sum_{i=n}^{\infty} a_i p^i$ with $n \in \mathbb{Z}, \quad n = -\log_p |a|_p$ and $a_n \neq 0$.

3 Valued Fields

Definition 25 (Valuation)**.** Let K be a valued field. A **valuation** on K is a function $V : K \to \mathbb{R} \cup \{\infty\}$ s.t., $\forall x, y \in K$:

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

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

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

Here we use the conventions $r + \infty = \infty,\ r \leq \infty \quad \forall r \in \mathbb{R} \cup \{\infty\}$

Remarks. If V is a valuation, and $|x| = c^{-V(x)}$ for some $c \in \mathbb{R}_{>1}$, then $|\cdot|$ is an absolute value.
Conversely, $|\cdot|$ an absolute value implies that $V(x) = -\log_c |x|$.

Definition (Field of Formal Laurent Series')**.** If K a field, then the **field of formal Laurent series' over** K is

$$K((T)) = \left\{ \sum_{i \gg -\infty}^{\infty} a_i T^i \ : \ a_i \in K \right\}$$

Exercise. Show that $v\left(\sum a_i T^i\right) = \min\{i \ : \ a_i \neq 0\}$ is a valuation of $K((T))$

Notation. The **valuation ring**: $\mathscr{O} = \mathscr{O}_k = \{x \in K \ : \ |x| \leq 1\}$
The **maximal ideal**: $\mathfrak{m} = \mathfrak{m}_k = \{x \in K \ : \ |x| < 1\}$
The **residue field**: $k = k_K = \mathscr{O}/\mathfrak{m}$

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

Theorem 26 (Hensel's Lemma)**.** Assume that K is complete and that $F \in K[x]$ is primitive. Put $f = F \bmod \mathfrak{m} \in \mathfrak{k}[x]$. Then, if there's a factorisation $f(x) = g(x)h(x)$ with $(g, h) = 1$, then there's a factorisation $F(x) = G(x)H(x)$ in $\mathscr{O}[x]$ with $g \equiv G,\ h \equiv H \bmod \mathfrak{m}$ and $\deg g = \deg G$.

Proof. Put $d = \deg F, m = \deg g$, giving $\deg h \leq d - m$. Pick lifts $G_0, H_0 \in \mathscr{O}[x]$ of g, h with $\deg G_0 = \deg g$ and $\deg H_0 \leq d - m$.
So, $(g, h) = 1 \implies \exists A, B \in \mathscr{O}[x]$ s.t. $AG_0 + BH_0 \equiv 1 \mod \mathfrak{m}$
Pick $\pi \in \mathfrak{m}$ s.t. $F = G_0 H_0 \equiv AG_0 + BH_0 - 1 \equiv 0 \mod \pi$. Then, we want to find:

$$\left.\begin{aligned} G &= G_0 + \pi P_1 + \pi^2 P_2 + \cdots \\ H &= H_0 + \pi Q_1 + \pi^2 Q_2 + \cdots \end{aligned}\right\} \in \mathscr{O}[x]$$

with $P_i, Q_i \in \mathscr{O}[x]$, $\deg P_i < m$ and $\deg Q_i \leq d - m$. By the definition of $\mathfrak{m}$, this would converge, so doing this suffices.
We want $F \equiv G_{n-1} H_{n-1} \mod \pi^n$ then to take the limit, which we'll find by induction. The base case is trivial, so we assume we have G_{n-1}, H_{n-1}. We want to find $G_n = G_{n-1} + \pi^n P_n$ and $H_n = H_{n-1} + \pi^n Q_n$.
Expanding $F - G_n H_n$, it is equivalent to find

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

Divide by π^n to get:

$$G_0 Q_n + H_0 P_n \equiv G_{n-1} Q_n + H_{n-1} P_n \equiv \frac{1}{\pi^n} \left(F - G_{n-1} H_{n-1}\right) \mod \pi$$

But $AG_0 + BH_0 \equiv 1 \mod \pi \implies F_n \equiv AG_0 F_n + BH_0 F_n \mod \pi$. Now, write $BF_n = SG_0 + P_n$, with $\deg P_n < \deg G_0, P_n \in \mathscr{O}[x]$ and S is some quotient. Then,

$$G_0 \left(AF_n + H_0 Q\right) + H_0 P_n \equiv F_n \mod \pi$$

Omit all coefficients from $AF_n + H_0 Q$ divisible by π to get Q_n. $\square$

Corollary 27. Let $F(x) = a_0 + a_1 x + \cdots + a_n x^n \in k[x]$, k complete and $a_0 a_n \neq 0$. If F is irreducible, then $|a_i| \leq \max(|a_0|, |a_n|)$ $\forall i$

Proof. WLOG F is primitive (scale). Pick the minimal r s.t. $|a_r| = 1$ and look at F modulo $\mathfrak{m}$. If $\max(|a_0|, |a_n|) \neq 1$, then F lifts to a non-trivial factorisation via Hensel's Lemma. $\square$

Corollary 28. $F \in \mathscr{O}[x]$, k complete. If F mod $\mathfrak{m}$ has a simple root $\bar{\alpha} \in k$, then F has a unique simple root $\alpha \in \mathscr{O}$ lifting $\bar{\alpha}$

Index