Topics in ANT

Lecture 3.

Last Week: Completions of valued fields (K, φ)

Field F is complete if every Cauchy sequence $(a_i)_{i=1}^{\infty}$ (i.e $\forall\, \varepsilon > 0$, $\varphi(a_i - a_j) < \varepsilon$ if i, j large enough) has a limit in F.

Theorem: There exists field extension $K \subset K_\varphi$ s.t.

① φ extends to a valuation on K_φ

② K_φ is complete

③ K is dense in K_φ

Remark: K_φ is the "universal" complete extension, i.e. if $F \supset K$ is complete wrt valuation extending φ then $\exists!$ continuous K-hom h:

$$\begin{tikzcd} K \arrow[r, hook] \arrow[dr] & K_\varphi \arrow[d, dashed, "h"] \\ & F \end{tikzcd}$$

Will study completions when

φ is archimedean "familiar and unsurprising"

φ is non-archimedean "exotic and exciting"

Peter showed (using Ostrowski's identity) that

Thm: A complete archimedean field is topologically isomorphic to either $\mathbb{R}$ or $\mathbb{C}$.

§1. Non-archimedean completions.

Assume (K, φ) non-archimedean, then have

$$A := \{ x \in K : \varphi(x) \leq 1 \}$$ Valuation ring

$$\mathfrak{m} := \{ x \in K : \varphi(x) < 1 \}$$ Max ideal

$$k := A/\mathfrak{m}$$ residue class field

Lemma: Let K_φ be completion of (K, φ), with residue class field k_φ, then

$$\varphi(K^\times) = \varphi(K_\varphi^\times), \qquad k = k_\varphi$$

Suppose henceforth that φ is non-trivial and discrete (i.e $\varphi(K^\times)$ is discrete in $\mathbb{R}_{>0}$).

then $\varphi(K^\times)$ is infinite cyclic group, generated by

$\varphi(\pi)$ largest value in $(0,1)$

π "uniformiser" unique up to

$A^\times = \{ x \in K : \varphi(x) = 1 \}$.

Therefore any $x \in K^\times$ can be written as

$$x = u \cdot \pi^{\mathrm{ord}_m(x)}$$

where $u \in A^\times$

$\mathrm{ord}_m(x) \in \mathbb{Z}$.

Theorem: Suppose (K, φ) is complete. Let $S \subset A$ be set of representatives for elements of residue field $k = A/m$, containing 0.

Then we have

$$A = \left\{ \sum_{i=0}^{\infty} a_i \pi^i \; : \; a_i \in S \right\}$$

Every $x \in K$ has unique expansion

$$x = \sum_{i \geq \mathrm{ord}_m(x)} a_i \pi^i, \qquad a_i \in S.$$

Proof: Exercise, use (crucially) the property that K is complete non-archimedean, so

$$\sum_{k \geq 0} b_k \text{ converges} \iff \varphi(b_k) \to 0 \text{ as } k \to \infty$$

Example: p-Adic numbers $\mathbb{Q}_p \supset \mathbb{Q}$

completion with respect to p-adic absolute value

$$|\cdot|_p : \quad |0|_p = 0$$
$$|a/b|_p = p^{\mathrm{ord}_p(b) - \mathrm{ord}_p(a)}$$

Valuation ring: $\mathbb{Z}_p = \{ x \in \mathbb{Q}_p : |x|_p \leq 1 \}$.

Uniformiser: Can choose $\pi = p$

Residue field: $k = \mathbb{Z}_p / p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$

By the above theorem, may think in terms of concrete p-adic expansions

e.g.: $S = \{0, 1, \dots, p-1\}$ reps for $k = \mathbb{F}_p$ in $A = \mathbb{Z}_p$.

In $\mathbb{Q}_3$ have

$$13 = 1 + 1\cdot 3 + 1 \cdot 3^2$$

$$13/3 = 1 \cdot 3^{-1} + 1 \cdot 3^{0} + 1 \cdot 3^{1}$$

$$\begin{aligned} 3/13 = 3 &+ 2 \cdot \underline{3}^{2} + 2 \cdot 3^{3} + 0 \cdot 3^{4} \\ &+ 2 \cdot 3^{5} + 2 \cdot 3^{6} + 0 \cdot 3^{7} \\ &+ 2 \cdot 3^{8} + 2 \cdot 3^{9} + 0 \cdot 3^{10} \\ &+ 2 \cdot 3^{11} + 2 \cdot 3^{12} + 0 \cdot 3^{13} \\ &+ \cdots \end{aligned}$$

$$= 3 + 2 \cdot \frac{3^{2}}{1-3^{3}} + 2 \cdot \frac{3^{3}}{1-3^{3}}$$

Def: A valued field (K, φ) with φ non-trivial is called a <u>local field</u> if topology induced by φ is locally compact (i.e every element has a compact neighbourhood)

Thm: Let K be a local field, then

1. K is complete
2. either

    K is archimedean (top. iso. to $\mathbb{R}$ or $\mathbb{C}$)

    K is non-archimedean, with discrete valuation and finite residue class field.

§2. Hensel's lemma.

Very important result! Allows us to 'lift'

$\begin{cases} \text{roots of polynomials} \\ \text{factorisations of polynomials } f = g \cdot h \end{cases}$

from $k = A/m$ to K !

<u>Lemma</u>: Let K be complete non-arch field.

Suppose $f \in A[x]$ factors over k as

$$\bar{f} = \bar{g} \cdot \bar{h} \quad \in k[x]$$

s.t. $\bar{g}, \bar{h}$ are coprime.

Then there exists factorisation

$$f = g \cdot h \quad \in A[x]$$

s.t. $\deg(g) = \deg(\bar{g})$

$g \bmod m = \bar{g}$

$h \bmod m = \bar{h}$.

Proof: Iterative and constructive procedure

i.e construct $g = $ limit of $g_1, g_2, \ldots$

$h = $ limit of $h_1, h_2, \ldots$

Define $g_1, h_1 \in A[x]$ such that

$$\begin{cases} g_1 \equiv \bar{g} \mod m[x] & (+\text{ same degree}) \\ h_1 \equiv \bar{h} \mod m[x] \end{cases}$$

Then for each $i \geq 1$ construct $g_{i+1}, h_{i+1} \in A[x]$

s.t $\begin{cases} g_{i+1} = g_i + \delta \\ h_{i+1} = h_i + \varepsilon \end{cases}$ $\quad \delta, \varepsilon \in m^i[x]$

and $f \equiv g_{i+1} \cdot h_{i+1} \mod m^{i+1}[x]$

① Find α, β s.t $1 = \alpha g_i + \beta h_i \mod m[x]$

② Find γ, ε s.t $\Delta\alpha = \gamma h_i + \varepsilon$ (Euclid)

where

$$\Delta = f - g_i h_i \in m^i[x]$$

③ Find $\delta = \gamma g_i + \Delta\beta \in m^i[x]$

and show $f = (g_i + \delta)(h_i + \varepsilon) \mod m^{i+1}[x]$

Then show the convergence of $(g_i)_i$ and $(h_i)_i$ to polynomials g and h, and show $f = g \cdot h$. $\square$

The most useful case is the following:

Corollary: Let $f \in A[x]$.

Then every simple zero of $\bar{f} \in k[x]$ can be uniquely lifted to zero of $f \in A[x]$.

Example 1: Note that proof of Hensel's lemma is iterative and constructive, so can use it in practice

$$f = x^2 - 7 \quad \text{over} \quad \mathbb{Q}_3$$

Then f mod 3 has 2 simple roots

$$\bar{\alpha} = 1$$
$$\bar{\beta} = 2.$$

which lift to simple roots

$$\alpha \quad (= \text{"}\sqrt{7}\text{"}) = 1 + 1\cdot 3 + 1\cdot 3^2 + 0\cdot 3^3 + 2\cdot 3^4 + \dots$$

$$\beta \quad (= \text{"}-\sqrt{7}\text{"}) = 2 + 1\cdot 3 + 1\cdot 3^2 + 2\cdot 3^3 + 0\cdot 3^4 + \dots$$

Example 2: (Teichmüller representatives)

The polymial $f = x^{p-1} - 1 \in \mathbb{Z}_p[x]$

$$\equiv \prod_{i=1}^{p-1} (x - i) \in \mathbb{F}_p[x]$$

has $(p-1)$ simple roots over $\mathbb{F}_p$, all of which can be lifted to $\mathbb{Z}_p$, have natural bijection

$$\mathbb{F}_p^\times \longrightarrow \{ \alpha \in \mathbb{Z}_p^\times : \alpha^{p-1} = 1 \}$$

$$i \longmapsto \alpha_i \equiv i \pmod p$$

Say α_i is the Teichmüller representative of i.