Fix prime p.

Chapter 2 of "Algebraic NT" by Neukirch

p-adic integers defn:

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

$\forall i,\ a_i \in \{0, \ldots, p-1\}$.

$\mathbb{Z}_p = \{\text{all } p\text{-adic integers}\}$.

$\Downarrow$ extends

$\mathbb{Q}_p = \{p\text{-adic numbers}\}$

$$a_{-m} p^{-m} + \cdots + a_{-1} p^{-1} + a_0 + a_1 p + \cdots$$

Any $f \in \mathbb{Q}$, $f = \frac{g}{h} p^{-m}$, g, h no factors of p

We can take a p-adic expansion of just $\frac{g}{h}$: $a_0 + a_1 p + a_2 p^2 \cdots$ and

mult. by p^{-m} to get:

$$f = a_0 p^{-m} + a_1 p^{1-m} + \cdots \in \mathbb{Q}_p.$$

Note: $\mathbb{Q} \to \mathbb{Q}_p$. injective.

If a, b same p-adic expansion,

then $a - b = \sum_{n \in \mathbb{N}} 0 \cdot p^n$

$p^n \mid (a-b) \quad \forall\, n \in \mathbb{N}, \Rightarrow a - b = 0.$

$\mathbb{Z} \neq \mathbb{Z}_p$

$\mathbb{Z} \subset \mathbb{Z}_p$

$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$

$= \dfrac{(p-1)}{1-p} = -1$

$\dfrac{1}{1-p} = 1 + p + p^2 + \cdots$

$\in \mathbb{Z}_p$

$\in \mathbb{Z}_p$.

Define + and × of p-adic #s.

Simple way: view p-adic numbers as sequences of residue classes mod

$$\mathbb{Z}/p^n\mathbb{Z}, \quad n \in \mathbb{N}$$

Absolute value: $|\cdot|_p$

Consider $a = \frac{b}{c}$, $b, c \in \mathbb{Z}$, $b, c \neq 0$.

$$a = p^m \frac{b'}{c'}, \quad (b', p) = (c', p) = 1.$$

Denote $|a|_p = \frac{1}{p^m}$.

$|3|_3 = \frac{1}{3}$. $|9|_3 = \frac{1}{9}$ $|2|_3 = 1$.

$|0|_p = 0$

$a_0 + a_1 p + a_2 p^2 + \cdots$ = sequence of summands converges to 0 with respect to $|\ |_p$.

m be denoted $v_p(a)$. (define $v_p(0) = \infty$)

v_p = p-adic valuation

$$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

1) $v_p(a) = \infty \iff a = 0$

2) $v_p(ab) = v_p(a) + v_p(b)$

3) $v_p(a+b) \geq \min\{m_p(a), v_p(b)\}$.

$x + \infty = \infty$, $\infty + \infty = \infty$, $\infty > x \quad \forall x$.

"p-adic exponential valuation of $\mathbb{Q}$":

"p-adic absolute value" derived as

$$|\ |_p : \mathbb{Q} \to \mathbb{R}, \quad a \mapsto |a|_p = p^{-v_p(a)}$$

Norm on $\mathbb{Q}$

- Zero norm iff zero value
- $|ab|_p = |a|_p |b|_p$
- $|a+b|_p \leq \max\{|a|_p, |b|_p\}$.

  $\leq |a|_p + |b|_p$.

2 "senses" of abs. value:

$|\ |$, $|\ |_p$.

↑ ↑

Notation: ~~Ordinary~~ $|\ |$ is denoted by $|\ |_\infty$.

New def'n of field of p-adic nums:

Cauchy sequence w.r.t. $|\ |_p$ is a sequence $\{x_n\}$ of rationals s.t. $\forall\ \varepsilon > 0$,

$\exists\ n_0 \in \mathbb{N}$ s.t. $|x_n - x_m|_p < \varepsilon$

for all $n, m \geq n_0$.

Ex: every formal series

$$\sum_{\nu=0}^{\infty} a_\nu p^\nu, \quad 0 \leq a_\nu < p.$$

$\Downarrow$

partial sums = Cauchy sequence.

Nullsequence: abs. values converge to 0.

p-adically, $1, p, p^2, p^3, \ldots$

Consider set of all Cauchy sequences over $\mathbb{Q}$ w.r.t. $|\,|_p$.

$\Downarrow$

forms a ring R, nullsequences

form an ideal m that is maximal.

Define $\mathbb{Q}_p := R/m$

$a \in \mathbb{Q} \longmapsto (a, a, a, \ldots) \in \mathbb{Q}_p$.

Proposition: $\mathbb{Q}_p$ is complete w.r.t. $|\ |_p$.

(Explanation: every Cauchy sequence in $\mathbb{Q}_p$ converges wrt to $|\ |_p$).

Prop: $\mathbb{Z}_p := \{ x \in \mathbb{Q}_p \mid |x|_p \leq 1 \}$ is a subring of $\mathbb{Q}_p$.

$\mathbb{Z}_p = \overline{\mathbb{Z}}$ wrt. $\mathbb{Q}_p$.

$$\mathbb{Z}_p \cong \frac{\mathbb{Z}[[X]]}{X - p}.$$

$|\ |$, $|\ |_p$. generalized to arbitrary fields.

Defn: A valuation, given a field K, is a function $|\ | : K \to \mathbb{R}$.

1) $|x| \geq 0$ for all x, $|x| = 0 \iff x = 0$.

2) $|xy| = |x||y|$

B) $|x+y| \leq |x| + |y|$

Explicitly exclude trivial valuation

$|x| = 1 \quad \forall \; x \neq 0.$

Given any valuation, $\underline{K}$ becomes a metric space.

define $d(x,y) = |x-y|$.

$\Downarrow$

gives us a topological space by defining open balls based on

$d(x, \text{center}) < \text{radius}$.

Defn: two valuations defining the same topology on K

$\Updownarrow$

equivalent valuations

Prop: $|\ |_1$, $|\ |_2$ valuations are equivalent on K iff

$\exists\ s > 0 \in \mathbb{R}$ such that

$$|x|_1 = |x|_2^s, \quad \text{for all } x \in K.$$

given any valuation $|\ |$ on K,

$|x| < 1 \iff \{x^n\}_{n \in \mathbb{N}}$ converges

to zero.

If $|\ |_1$ and $|\ |_2$ are equivalent then we must have $|x|_1 < 1$ for x.

$$\Updownarrow$$

$$|x|_2 < 1$$

Approximation Theorem:

Any number (n) of pairwise-inequivalent valuations on K, and $a_1 \dots a_n \in K$.

For all $\varepsilon > 0$, $\exists\ x \in K$ s.t.

$$|x - a_i|_i < \varepsilon \quad \text{for all } i = 1 \dots n.$$

(proof: page 118 of the book)

Archimedean vs. nonarchimedean valuations

- $|n|$ bounded $\forall n \in \mathbb{N}$, nonarchimedean.
- unbounded $\iff$ archimedean.

Prop: $|\ |$ is nonarchimedean iff satisfies the strong Δ inequality

$$|x+y| \leq \max\{|x|, |y|\}.$$

Pf: If we know strong Δ ineq holds:

$$|n| = |1 + \cdots + 1| \leq 1.$$

Other direction: $|n| \leq N$, $x, y \in K$ s.t. $|x| \geq |y|$,

$$|x|^v |y|^{n-1} \leq |x|^n \quad \text{for all } v \geq 0.$$

$$|x+y|^n \leq \sum_{v=0}^{n} \binom{n}{v} |x|^v |y|^{n-v}$$

$$\leq (n+1) N |x^n|$$

$$\vdots$$

$$|x+y| \leq N^{1/n} (1+n)^{1/n} \boxed{|x|} \qquad \max(|x|, |y|)$$

$$\Rightarrow \quad |x+y| \leq \max(|x|, |y|).$$

$$n \to \infty.$$

$$|x| \neq |y| \Rightarrow \quad |x+y| = \max\{|x|, |y|\}.$$

Theorem: Every valuation of $\mathbb{Q}$ is equivalent to either $|\ |_\infty$ or $|\ |_p$.

- any archimedean valuation on $\mathbb{Q}$ equiv. to $|\ |_\infty$
- any non-archimedean " equiv. to some $|\ |_p$.

All p-adic valuations $|\ |_p$ are inequivalent for different p.

Nonarchimedean val on K (III)

Consider a function $v: K \to \mathbb{R} \cup \{\infty\}$

$$\begin{cases} v(x) \mapsto -\log |x|, & x \neq 0 \\ v(x) \mapsto \infty, & x = 0. \end{cases}$$

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

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

3) $v(x+y) \geq \min\{v(x), v(y)\}$.

v is called an exponential valuation of K.

2 exp. valuations are equiv. if one is a product of another, thus a positive real constant.

Proposition:

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\} \quad \text{is a ring}$$
$$= \{x \in K \mid |x| \leq 1\}$$

$\mathcal{O}$ has a group of units:

$$\mathcal{O}^* = \{x \in K \mid v(x) = 0\}$$
$$= \{x \in K \mid |x| = 1\}$$

$\mathcal{O}$ has a unique maximal ideal:

$$\mathfrak{p} = \{x \in K \mid v(x) > 0\}$$
$$= \{x \in K \mid |x| < 1\}.$$

- $\mathcal{O}$ is an integral domain w/ field of fractions K.

- $\forall\, x \in K$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.

(Valuation Ring)

- only maximal ideal $= \{x \in \mathcal{O} \mid x^{-1} \notin \mathcal{O}\}$.

- Discrete exponential valuation if $\mathcal{O}$ has a smallest positive value.

Completions

- Consider K, $|\ |$ (valued field)

- complete iff every Cauchy seq. $\{a_n\}_{n \in \mathbb{N}}$ converges to an element a in K.

$(K, |\,|)$ gets <u>completed</u> $(\hat{K}, |\,|)$.

Let R = ring of all Cauchy seq.s of $(K, |\,|)$, m = maximal ideal of all nullsequences:

$$\hat{K} = R/m.$$

<u>Ostrowski's Theorem:</u> $\mathbb{R}$ and $\mathbb{C}$ are only complete fields w.r.t. archimedean valuation.

$\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\,|_p$.

Prop $\mathcal{O} \subseteq K$

$\hat{\mathcal{O}} \subseteq \hat{K}$

$\hat{v}, v \to$ valuation

$\hat{\mathfrak{p}}, \mathfrak{p} \to$ maximal ideal

$$\hat{\mathcal{O}}/\hat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}.$$

If v is discrete,

$$\hat{\mathcal{O}}/\hat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n \quad \forall\ n \geq 1.$$

Hensel's Lemma: If $f(x) \in \mathcal{O}[x]$ is a primitive poly and

$$f(x) \equiv \bar{g}(x)\,\bar{h}(x) \mod \mathfrak{p},$$ where

$\bar{g}, \bar{h} \in k[x]$ relatively prime

$(k = \mathcal{O}/\mathfrak{p})$, then we can factorize

$$f(x) = g(x)\,h(x),$$

$g, h \in \mathcal{O}[x]$ s.t. $\deg(g) = \deg(\bar{g})$

and

$g(x) \equiv \bar{g}(x)$, $h(x) \equiv \bar{h}(x) \mod \mathfrak{p}$.

$$X^{p-1} - 1 \in \mathbb{Z}_p[x]$$

$$\mathbb{Z}_p / p\mathbb{Z}_p = \mathbb{F}_p$$

$$\Downarrow$$

$(p-1)^{th}$ roots of unity are in $\mathbb{Q}_p$.

Theorem: K complete wrt. $|\ |$.

Then, $|\ |$ extended in a unique way to a valuation of any given L/K algebraic extension.

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

L/K has finite degree n.

L is complete.