Lecture 2

1 P-adic absolute value

Recall $\mathbb{Z} \subseteq \mathbb{Z}_p \subseteq \mathbb{Q}_p$
$\qquad\qquad\qquad\qquad\qquad \cup\!\!|$
$\qquad\qquad\qquad\qquad\qquad \mathbb{Q}$

$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$

$\mathbb{Q}_p =$ its field of fractions

And $\mathbb{Z}_p = \{ \sum_{n \geq 0} a_n p^n \}$
$a_n \in \{0, \dots p-1\}$

|Algebra|

2 Today a bit of analysis. Fix p = prime.

Pick $q \in \mathbb{Q}$. Suppose $q \neq 0$. Then $q = p^m \frac{a}{b}$.

Def: $|q|_p = \frac{1}{p^m}$.

$$\left.\begin{array}{l} (a,b)=1 \\ (a,p)=1 \\ (b,p)=1 \end{array}\right\}$$

If $q=0$, put $|q|_p = 0$.

This gives: $|\ |_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ s.t.

norm axioms
$$\begin{cases} 1)\ |a|_p = 0 \iff a = 0 \\ 2)\ |ab|_p = |a|_p |b|_p \\ 3)\ |a+b|_p \leq \max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p \end{cases}$$

Remark: We will see later (Ostrowski Th) that $|a|_p^s$ & $|\ |^s$ $s \in (0,1]$ are all norms

(2) Th (EASY) Let q be a RATIONAL $\neq 0$ number

Then $|q| \cdot \prod_p |q|_p = 1$. ☆

Usually we also put $|q| = |q|_\infty$.

Link to geometry: $\mathbb{Z}, \mathbb{C}[t]$

"$[1:0] = \infty$"

$\mathbb{C} \subseteq \mathbb{P}^1 = 2$ copies of $\mathbb{C}$ glued by $\mathbb{C}^*$

$\mathbb{C}[t], \mathbb{C}[t^{-1}]$

$\mathbb{C}[t]$

$\cap$

$\mathbb{C}(t)$

$\mathbb{P}^1 = \{[a:b] \mid a, b \in \mathbb{C}, (a,b) \neq 0\}$

$t = \frac{a}{b}$, $t^{-1} = \frac{b}{a}$ $\quad [a:b] = [\lambda a : \lambda b]$, $\lambda \in \mathbb{C}^*$

$U_y \quad U_x$

Pick $f \in \mathbb{C}(t)$.

Pick a point (FIX FOR A WHILE) $p \in \mathbb{P}^1$.

We may assume $p \in \mathbb{C}^1$ (usual one)

$f = \frac{a(t)}{b(t)}$ polynomials. $f = (x-p)^m \frac{a(t)}{b(t)}$

bla bla bla.

$|f|_p = \frac{1}{q^m}$ (q = fixed > 0 REAL)

☆ holds

$\hookrightarrow$ we missed one point: $[1:0]$.

$f = a(1/t)/b(1/t) \in \mathbb{C}[t]$ another copy. $|f|_{[10]} = \frac{1}{q^m}$

$m = \deg b - \deg a$.

(3) $q \in \mathbb{Q}$ $\quad q \neq 0$ $\quad q = p^m \frac{a}{b}$ ...

$|q|_p = 1/p^m$.

OR $\boxed{v_p(q) = m}$ and we put $v_p(0) = \infty$.

order of vanishing.

(4) 1) $v_p(q) = \infty \iff q = 0$

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

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

$$\begin{cases} m + \infty = \infty \\ \infty + \infty = \infty \\ \infty > m. \end{cases}$$

$$|q|_p = \frac{1}{p^{v_p(q)}}$$

$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ p-adic (exponential) valuation.

$| \ |_p : \mathbb{Q} \to \mathbb{R}$ p-adic absolute value.

5 Def: A *Cauchy seq* in $\mathbb{Q}$ wrt $|\ |_p$ is a sequence $\{x_n\}$ s.t. $\forall \varepsilon > 0$ $\exists n_0(\varepsilon)$ s.t. $|x_n - x_m|_p < \varepsilon$ $\forall n, m \geq n_0(\varepsilon)$

Ex: $\sum_{n=0}^{\infty} a_n p^n$ $\quad 0 \leq a_n < p$ is Cauchy.

We understand it as $x_m = \sum_{n=0}^{m} a_n p^n$.

Def: A sequence $\{x_n\}$ $x_n \in \mathbb{Q}$ is a *nullsequence* if it is converges to 0.

Ex: $1, p, p^2, -$

$R :=$ Ring of Cauchy sequences.

[Claim: Let I_0 be ideal generated by all nullseqences. Then I is maximal.]

Corollary: $R/I_0 =$ field.

Def: $\mathbb{Q}_p = R/I_0$

(6) $\mathbb{Z} \subset \mathbb{Z}_p \subseteq \mathbb{Q}_p$ constructed backwards.

Put $|x|_p = \lim\limits_{n\to\infty} |x_n|_p \in \mathbb{R}$. $\{x_n\}$ = Cauchy

Claim: $|x|_p$ exists.

$|x|_p = |y|_p$ if $x - y \in I_0$

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

If $\{x_n\}$ = Cauchy and $\{x_n\} \notin I_0$, put

$$v_p(\{x_n\}) = \lim_{n\to\infty} -\log_p |x_n|_p \quad (x_n \neq 0 \text{ (or for } n \gg 0\text{)}).$$

Then $|\{x_n\}|_p = p^{-v_p(\{x_n\})}$.

(7) Theorem: $\mathbb{Q}_p$ is complete wrt $|\ |_p$.

Proof: the same as for $\mathbb{R}$.

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

$$\begin{array}{l} \mathbb{Q} \to |\ |_\infty \to \mathbb{R} \\ \searrow |\ |_2 \to \mathbb{Q}_2 \\ \downarrow |\ |_3 \to \mathbb{Q}_3 \\ \vdots \end{array}$$

Put $\mathbb{Q} \subseteq \mathbb{Q}_p$

$(q, q, q, \dots)$ constant Cauchy s.

(7) $\overline{VI}$

Put $\mathbb{Z}_p = \{ x \in \mathbb{Q}_p \text{ s.t. } |x|_p \leq 1 \}$.

Th. $\mathbb{Z}_p$ is a subring.
.. $\mathbb{Z}_p$ is a closure of $\mathbb{Z}$.

Proof:
• follows from $|x+y|_p \leq \max\{|x|_p, |y|_p\}$
$|xy|_p = |x|_p |y|_p$
$1 \in \mathbb{Z}_p$, $0 \in \mathbb{Z}_p$.

.. $\overline{\mathbb{Z}} \subseteq \mathbb{Z}_p$ obvious.
To see that $\mathbb{Z}_p \subseteq \overline{\mathbb{Z}}$ take
$x = \{x_n\}$ with $|x|_p \leq 1$.
Then $\exists n_0$ s.t. $|x_n|_p \leq 1$ $\forall n \geq n_0$ (Cauchy)
$x_n = \frac{a_n}{b_n}$ b_n is coprime to p.
Solve $y_n \cdot b_n \equiv a_n \mod p^n$. $y_n \in \mathbb{Z}$
$|x_n - y_n|_p \leq 1/p^n$ $\forall n \geq n_0$
$\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n$.

(8) $\mathbb{Z} \subseteq \mathbb{Z}_p \subseteq \mathbb{Q}_p \qquad \overline{\mathbb{Z}} = \mathbb{Z}_p$

$$\begin{array}{c} \mathbb{Q}_p \\ \cup \\ \mathbb{Q} \end{array}$$

Put $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \text{ s.t. } |x|_p = 1\}$

Then $\mathbb{Z}_p^*$ is a group of units of $\mathbb{Z}_p$

Claim: $\forall\, x \in \mathbb{Q}_p^*$ we have $\boxed{x = p^m u}$

$m \in \mathbb{Z}$

$u \in \mathbb{Z}_p^*$

unique way

(9) Th: Let I be an ideal of $\mathbb{Z}_p$.

Then eith $I = 0$ or $I = \mathbb{Z}_p$ or $I = p^n\mathbb{Z}_p$ for some $n \geq 1$.

Note: $p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \text{ s.t. } v_p(x) \geq n\}$

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

Proof: $x = p^m u$, $u \in \mathbb{Z}_p^*$ m = smallest.

$\varphi: \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p \quad a \to a \bmod p^n\mathbb{Z}_p$.

$\operatorname{Ker}\varphi = p^n\mathbb{Z}$. $\operatorname{Im}\varphi = \mathbb{Z}_p/p^n\mathbb{Z}_p$ $\Rightarrow x - a \in p^n\mathbb{Z}_p$

$(\forall x \in \mathbb{Z}_p\ \exists a \in \mathbb{Z} \text{ s.t. } |x-a|_p \leq 1/p^n$

(10) Now we compare 2 defn.

old: $\mathbb{Z}_p = \sum_{m\geq 0} a_m p^m \quad a_m \in \{0, \dots p-1\}$.

$\hookrightarrow S_n = \sum_{m=0}^{n-1} a_m p^m$.

$\begin{cases} \bar{S}_n = S_n \bmod p^n \\ \bar{S}_n \in \mathbb{Z}/p^n\mathbb{Z} \end{cases}$

$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \{(x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z},$

$x_{n+1} \to x_n$

new: $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z} \quad \forall n \geq 1$

$\Downarrow$

$\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z} \to$ bunch of homom

glue them

$\mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$

(11) Th: $\mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is an isomorphism.

Proof.

1) Kernel: $x \to 0 \Rightarrow x \in p^n\mathbb{Z}_p \; \forall n\geq 1 \Rightarrow |x|_p \leq \frac{1}{p^n} \; \forall n \geq 1$

2) Image: $y \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \rightsquigarrow S_n = \sum_{m=0}^{n-1} a_m p^m \quad \forall n \geq 1.$

Cauchy $\quad 0 \leq a_m \leq p-1$

$\mathbb{Z}[[X]]$ Ring of all formal power series with coeff. in $\mathbb{Z}$

Th $\mathbb{Z}_p \cong \mathbb{Z}[[X]]/(X-p)$

Proof: $\varphi : \mathbb{Z}[[X]] \to \mathbb{Z}_p$ surjective

$x \to p$.

$(X-p)\mathbb{Z}[[X]]$ is in kernel.

$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$

$f(p) = 0$ in $\mathbb{Z}_p \Rightarrow a_0 + a_1 p + a_2 p^2 + \cdots a_{n-1} p^{n-1} \equiv 0 \mod p^n$.

Put $b_{n-1} = \frac{-1}{p^n}(a_0 + \cdots + a_{n-1} p^{n-1})$

$$\left.\begin{aligned} a_0 &= -p b_0 \\ a_1 &= b_0 - p b_1 \\ a_2 &= b_1 - p b_2 \end{aligned}\right\}$$

$\cdots$

$(a_0 + a_1 x + a_2 x^2 + \cdots) = (x-p)(b_0 + b_1 x + b_2 x^2 \ldots)$