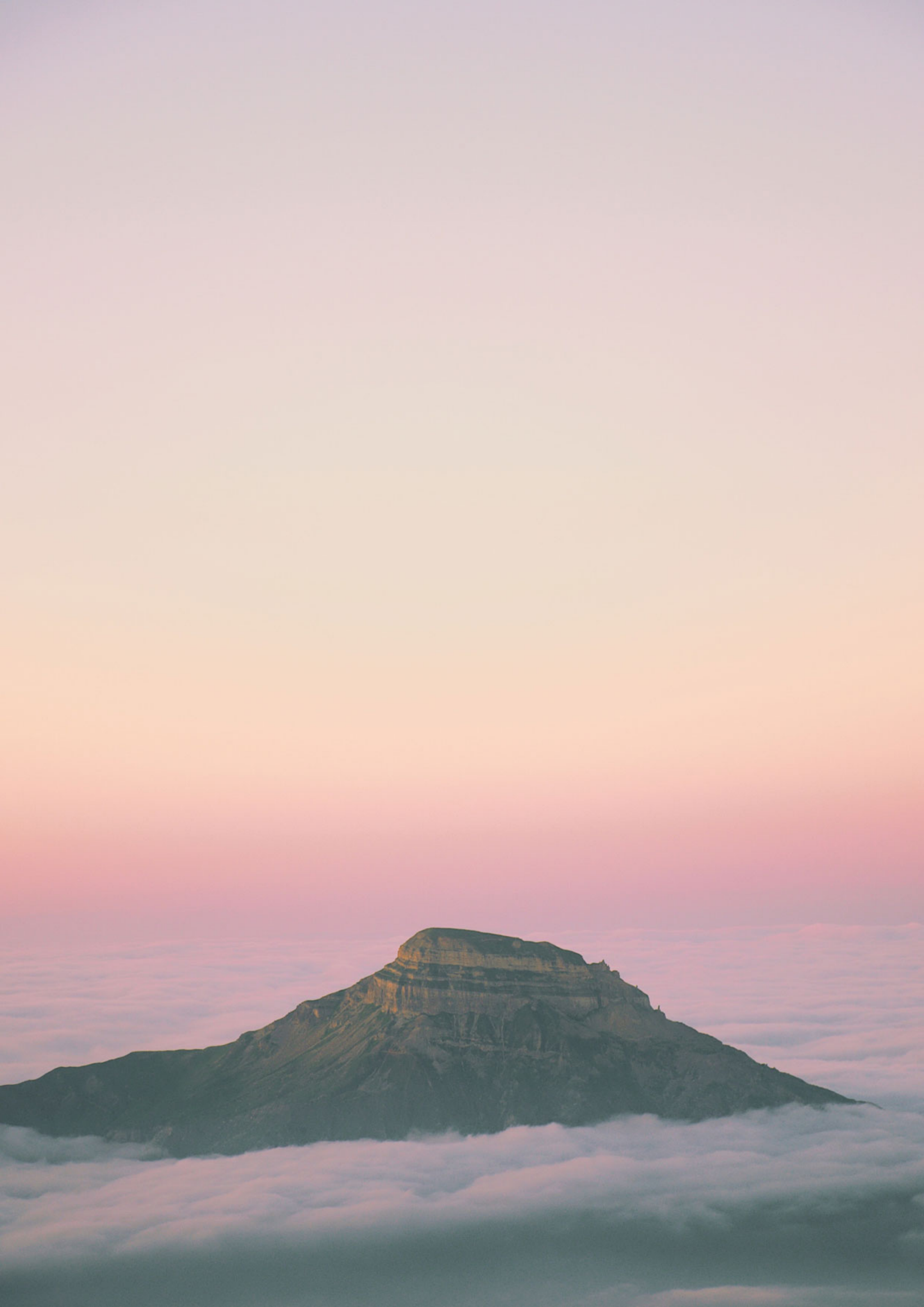

p-adic field

1. p-adic 整数
2. 构造 p-adic 域
3. p进方程
4. 二次扩张

Q: $x^2 \equiv 2 \pmod{7^n}$ $\pm\sqrt{2} =$

$n=1$ $x^2 \equiv 2 \pmod 7$ $x \equiv 3 \pmod 7$ $x \equiv 4 \pmod 7$

$n=2$ $(7a_1+3)^2 \equiv 2 \pmod{49}$ $(7a_2+4)^2 \equiv 2 \pmod{49}$

$a_1 \equiv 1 \pmod 7$ $a_2 \equiv -2 \pmod 7$.

$x = 3 + 7\times 1 = 10$ $4 + 7\times(-2) = -10 = 39$

3 — 10 — 108 — 2166 — ...

4 — 39 — 235 — 235 — ...

$\mathbb{Q}$.

$x = a_0 + a_1 \times 7 + a_2 \times 7^2 + \cdots$ $\mathbb{Z}$

$x^2 \equiv 25 \pmod{3^n}$

2 — 5 — 5 — 5 — ...

1 — 11 — 211 — 2211 ...

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

$$:= \left\{ (a_1, a_2, \cdots) \in \prod_{i=1}^{\infty} \mathbb{Z}/p^i \;\middle|\; a_{m+1} \equiv a_m \pmod{p^m} \right\}$$

拓扑群： Group $\mu: G\times G \to G$

$\nu: G \to G$

$(\mathbb{R}, +)$. $|x-y|$

拓扑群必是"齐性空间"： X, $a, b \in X$.

$\varphi(a) = b$.

定义 I $\mathcal{C}$ $\{A_i\}$. $i \leq j$

$f_{ji}: A_j \to A_i$

(1) $i=j$ $f_{ii} = id$

(2) $i \leq j \leq k$ $f_{ji} f_{kj} = f_{ki}$

$\{A_i, f_{ji}\}$. 反向系统

$$\begin{tikzcd}
& A \arrow[dl, "\sigma_j"'] \arrow[dr, "\sigma_i"] & \\
A_j \arrow[rr, "f_{ji}"'] & & A_i
\end{tikzcd}$$

锥

反向极限： $A := \varprojlim A_i$ 在锥中、唯一性

p进整数：

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

$$|x|_p = p^{-v_p(x)}$$

其中 $v_p : \mathbb{Z} - \{0\} \to \mathbb{R}$

$0 \mapsto +\infty.$ $\qquad n = p^{v_p(n)} \cdot n' \qquad p \nmid n'$

$6 = 2 \times 3 \qquad v_3(6) = 1 \qquad |6|_3 = 3^{-1} = \frac{1}{3}$

度量： i) $|x| = 0 \Leftrightarrow x = 0.$

ii) $|xy| = |x||y|$

iii) $|x+y| \le |x| + |y|$

$x, y \in \mathbb{R}. \qquad |nx| > |y|.$

非阿： $\left| \, |x+y| \le \max\{|x|, |y|\}. \right.$ $\qquad v(a+b) \geq \min\{v(a), v(b)\}.$

$$\boxed{p^a \mid x, \quad p^b \mid y \qquad \begin{matrix} a > b. \\ p^b \mid x+y \end{matrix}}$$

$$|x|_p = p^{-v_p(x)}.$$

$$|7|_3 = |1 + 2 \times 3^1| = 3^0 = 1.$$

Q. 上去：
$$x = p^{-v_p(x)} \frac{a}{b} \quad 其中 \quad p \nmid a, b.$$

Example $\quad \left|\frac{1}{4}\right| = 1. \qquad \left|\frac{1}{3}\right| = \left|3^{-1} \cdot \frac{1}{1}\right| = 3^1 = 3.$

$| \; |_p \; , \quad | \; |_\infty .$

Topology: $d(x,y) \le \max\{d(x,z), d(z,y)\}$.

$B(a,r) := \{x \in \mathbb{Q} : |x-a| \le r\}$.

proposition: Every point in $B(a,r)$ is the centre of ball.

$x \in B(a,r)$, $|x-a|_p \le r$

$\forall y \in B(a,r)$.

$|y-x|_p = |y-a+a-x|_p \le \max\{\underbrace{|y-a|_p}_{\le r}, \underbrace{|a-x|_p}_{\le r}\}$

$\le r$.

Corollary 1: $B(a,r)$ is both open and closed.

Corollary 2: $\forall$ 两个 B_1, B_2

要么 $B_1 \cap B_2 \ne \phi$.

要么, $B_1 \subset B_2$ 或 $B_2 \subset B_1$

Corollary 3: $\forall$ 紧空间 $U \subset \mathbb{Q}$. p-adic norm.

fixed r. $U = \bigcup_{i=1}^{n} B_i$ B_i 有限不交.

特别地对 $\mathbb{Z}$

$v_p \ge 0$. $|\mathbb{Z}| \le p^0 = 1$.

$\mathbb{Z}$ 在 p-adic 域 $[0,1]$. (子集)

$\mathbb{Z} = \bigcup_{i=1}^{N} B_i = \bigcup_{i=1}^{q^N} B(x_i, q^{-N})$.

$\mathbb{Q} \swarrow$ p-adic norm

Cauchy sequence. $\{x_n\}$ $\lim |x_{n+1} - x_n| \to 0.$

$C(\mathbb{Q})$: Cauchy sequence in $\mathbb{Q}$. p-adic norm.

$N := \{ (x_n) : |x_n|_p \to 0 \}.$

$\mathbb{Q}_p = C(\mathbb{Q}) / N.$

$\mathbb{Q}_p$ 就是完备的. p-adic 域.

$\mathbb{Z}_p := \{ x \in \mathbb{Q}_p \mid |x|_p \le 1 \}.$ $\mathbb{Z}$ 10.

Example:

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

p^2 p^{-1}

$$\frac{1}{12} = 3^{-1} \cdot \frac{1}{4}$$

$$= 3^{-1} \cdot \frac{1}{1+3} = 3^{-1}(1 - 3 + 3^2 - 3^3 + \cdots).$$

$$= 3^{-1} + 2\times 1 + 3 + 2\times 3^2 + \cdots$$

$x = p^r \cdot x'$. $a_0 + a_1 p$

$v_p(x') = 1.$

Theorem Ostrowski

$\mathbb{Q}$ 上的非平凡绝对值只有两种. (等价意义下).

$\boxed{|\ |_p}$ $|\ |_\infty$

$|x| = p^{-v_p(x)}$. $q^2, pq < 1.$

$e^{-v_p(x)}$.

Product Formula

$$\prod_{p \le \infty} |x|_p = 1.$$

$$|x|_\infty = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

$$|x|_{p_i} = p_i^{-a_i}$$

$$|x|_q = 1$$

p-adic field.

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(h)}{h}$$

$$|h| \to \cancel{0}.$$

$$h = a_0 + a_1 p + \cdots + a_n p^n + \cdots$$

$$p^{n+1}$$

≪ p-adic numbers an introduction. ≫

Fernando Q. Gouvêa.

≪ P-adic analysis and mathematical physics ≫

V.S. Vladimirov

$$f(b) - f(a) = f'(\xi)(b-a).$$

$$\xi = at + b(1-t).$$

$$|t| \le 1.$$

$$\mathbb{Z}_q.$$

$$f(x) = x^p \qquad f(0) = 0, \quad f(1) = 1.$$

$$\boxed{f'(\xi) = 1.} \qquad f'(x) = p x^{p-1}$$

$|\xi| = |at + b(1-t)| \in \mathbb{Z}_q$. $\quad |\xi| \le q^0 = 1$.

$$|f'(\xi)| \le p^{-1} = \frac{1}{p}.$$

« Le théorème des accroissements finis p-adiques ».

$$r_p \le |p|^{\frac{1}{p-1}} = \boxed{p^{-\frac{1}{p-1}}} \quad \mathbb{R}$$

$(x+\Delta x)$ $\quad |\Delta x| \le p^{-1}$

$$|e^x| = p^{\frac{1}{p-1}}.$$

$f(x) = \sum_{n \geq 0} a_n x^n$ $\quad D$ where it convergent.

$f'(x) = \sum n a_n x^{n-1}$ $\quad D$.

§ p-adic equations.

Lemma: Let $\cdots \to D_n \xrightarrow{\varphi_n} \boxed{D_{n-1}} \to \cdots \to D_1$ be a projective system and Let $D = \varprojlim D_n$

If D_n are finite and nonempty, D is nonempty.

$\boxed{1}$ 承认 $D_n \to D_{n-1}$ 满射. D 非空的.

② $\underline{D_{n,p}}$ $\quad \underline{\boxed{D_{n+p}}} \longrightarrow D_n$. stationary.

E_n $\quad \lim D_{n,p}$. $\quad E_n$ 不变的 $\subset D_n$.

$E \xleftarrow{} \cdots \to E_n \to E_{n-1} \to \cdots$

$E \subset D$.

$f \in \mathbb{Z}_p[X_1, \cdots, X_m]$.

Proposition 5.

$f^{(i)} \in \mathbb{Z}_p[X_1, \cdots, X_m]$.

i). $f^{(i)}$ 有共同零点 在 $(\mathbb{Z}_p)^m$ 中.

ii) For all $n \geq 1$, $f_n^{(i)}$ 在 $\underline{(\mathbb{Z}/p^n\mathbb{Z})^m}$ 上一个

公共零点.

$(\mathbb{Z}_p)^m = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^m$.

Definition:

称 $x = (x_1, \cdots, x_m)$ of $(\mathbb{Z}_p)^m$ 是 primitive if

x_i 中有一个可逆. (不可被 p 整除) $(A_n)^m$.

$A_n = \mathbb{Z}/p^n\mathbb{Z}$

Proposition 6. $f^{(i)}$ 齐次多项式 TFAE:

a) $f^{(i)}$ 在 $(\mathbb{Q}_p)^m$ 上有非平凡的公共零点.

b) $f^{(i)}$ 在 $(\mathbb{Z}_p)^m$ 上公共的 primitive zero.

c). $f^{(i)}$ 在 $(A_n)^m$ 上有公共的 primitive zero.

Lemma:

$f \in \mathbb{Z}_p[x]$ and f'. Let $x \in \mathbb{Z}_p$, $n, k \in \mathbb{Z}$

s.t. $0 \leq 2k < n$, $f(x) \equiv 0 \pmod{p^n}$ $v_p(f'(x)) = k$.

there exist $y \in \mathbb{Z}_p$ s.t:

$\boxed{f(y) \equiv 0 \pmod{p^{n+1}}}$, $\boxed{v_p(f'(y)) = k}$,

$\boxed{y \equiv x \pmod{p^{n-k}}}$.

令 $y = x + p^{\boxed{n-k}} z$.

$$f(y) = \underset{\underset{p^n \underline{b}}{\|}}{f(x)} + p^{n-k} z \underset{\underset{p^k \boxed{c}}{\|}}{f'(x)} + p^{2n-2k} \underline{a}. \qquad a \in \mathbb{Z}_p.$$

$$b + zc \equiv 0 \pmod p.$$

$$f(y) = p^n (b + zc) + p^{2n-2k} a \equiv 0 \pmod{p^{n+1}}.$$

$$f'(y) = f'(x + p^{n-k} z) \equiv p^k c \pmod{p^{n-k}}.$$

$2k < n$. $\quad n-k > k \qquad v_p(f'(y)) = k$.

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

Corollary 1:

Every simple zero of the reduction modulo p of a polynomial f lifts to a zero of f with coefficients in $\mathbb{Z}_p$.

simple. $\qquad v_p(f'(x)) = 0$.

$\mathbb{Q}$上的二次扩张: $\qquad (\mathbb{Q}_p)$.

$$x^2 = a. = p^{r(a)} (a_0 + a_1 p + a_2 p^2 + \cdots) \qquad 0 \le a_j \le p-1.$$

has a solution $\Leftrightarrow$.

1). $r(a)$ is even

2). $\left(\frac{a_0}{p}\right) = 1$ if $p \ne 2$.

$a_1 = a_2 = 0$. $\qquad p = 2$.

"Necessity":

$$x = p^{r(x)}(x_0 + x_1 p + \cdots)$$

$$x^2 = p^{2r(x)}(x_0 + x_1 p + \cdots)^2 = p^{r(a)}(a_0 + a_1 p + \cdots)$$

$r(a)$ is even.

$x_0^2 = a_0$

$\left(\frac{a_0}{p}\right) = 1.$ $\quad p \neq 2$ 时.

$$\left(\frac{x_1 + x_1^2}{2} + x_2\right) 2^3 = \qquad a_1 = a_2 = 0.$$

充分:

$$2x_0 x_j \equiv a_j + N_j \pmod p.$$

N_j about $(x_0, x_1, \cdots, x_{j-1})$

$p=2$.

$$x_j \equiv a_{j+1} + N_j \pmod 2.$$

Corollaries.

1. $p \neq 2$ 时. 所有非平方数只有3种.

$k_i = \eta. \quad p\eta, \quad p.$ $\quad$ 其中 η 可逆的 $\left(\frac{\eta}{p}\right) \neq 1.$

$i=1,2,3.$

$a_0 + a_1 p + \cdots \qquad a_1 p + a_2 p^1 \qquad p.$

$\varepsilon^2, \quad \varepsilon^2\eta. \quad \varepsilon^2 p\eta \quad \varepsilon^2 p.$

$\mathbb{Q}_p$ 上面存在三种不同构的二次扩张.

$\mathbb{Q}_p(\sqrt{k_i})$.

$p=2$ 时.

$$k_2=3, \quad k_3=5, \quad k_4=7.$$

$$k_5=2, \quad k_6=6, \quad k_7=10. \quad k_8=14.$$

$$(\pm 1, \pm 2, \pm 3. \pm 6.).$$

$\mathbb{Q}_2^* \backslash \mathbb{Q}_2^{*2}$ 8 种元素.

$\mathbb{Q}_p^* \backslash \mathbb{Q}_p^{*2}$ 4 种元素.

Discrete Valuation Rings.

K. field.

$$v: K \to \mathbb{Z} \cup \infty$$

discrete valuation.

(i) v 是满同态 $K^* \to \mathbb{Z}$
$0 \mapsto \infty$.

(ii) $v(x+y) \geq \inf\{v(x), v(y)\}$.

$R_v = \{x \in K \mid v(x) \geq 0\}$. 整环.

$P_v = \{x \in K \mid v(x) > 0\} = (\pi). \mapsto p.$

Claim. R_v 中.

$a = \pi^n \underline{u}$. $v(\pi)=1$. u. 可逆的.

$I = (P_v)^n.$

R_v 一个"分式理想" $I \subset K$. R_v $\exists$ a.

$aI \subset R_v$.

$p^{-n}(a_0 + a_1 p + \cdots)$. p^n.

$I = (p_v)^n$.

$v(I) = \inf_{x \in I} v(x)$.

$I = aJ$ $a \in K^*$

$v(I) = v(J) + v(a)$.

choose $b \in I$. $v(b) = v(I)$.

$\underline{\pi^{v(b)} R_v} = b R_v \underline{\subset I}$.

$I \subset \{ x \in K \mid v(x) \geq v(I) \}$.

$\underline{I \subset} \pi^{v(I)} R_v = \underline{\pi^{v(b)} R_v}$

$I = (\pi R_v)^{v(I)}$

$I = (p_v)^{v(I)}$ $I \subset R_v$.

$v(I) \geq 0$.

Discrete valuation Ring.

① PID ② 有且只有一个素理想.

"$\Leftarrow$" d.v ring R. 是 $R_v = \{ x \in K \mid v(x) \geq 0 \}$.

其中 K 是 R 的分式域

$p = \pi R$

$x = \pi^{n} u$. u 是 unit.

$$\boxed{v(x) = n}$$

d.v. ring R $\quad \mathfrak{p}$ $\quad \boxed{k = R/\mathfrak{p}}$

$$\boxed{\mathfrak{p}^n / \mathfrak{p}^{n+1} \cong k}$$

$$\boxed{\bigcap \mathfrak{p}^n = 0}$$

$$0 \to U \to K^* \to \mathbb{Z} \to 0$$

$n \geq 1$ $\qquad U_n := \boxed{1 + \mathfrak{p}^n}$

$$U / U_1 \cong k^*$$

$$U_1 = 1 + \mathfrak{p}$$

$$U - \{0\} / U_1 \cong k^*$$

$$U_n / U_{n+1} \cong \mathfrak{p}^n / \mathfrak{p}^{n+1} \cong k$$

$$e(x) = \exp(2\pi i \{x\}_p)$$

$$x = p^{v(x)}(x_0 + x_1 + \cdots) \in \mathbb{Z}_q$$

$$v(x) \geq 0$$

1. $\mathbb{Q}_p$ 上的加性特征

$$\chi_p(\xi x) = \exp(2\pi i \{\xi x\}_p)$$

$$\pi(x) = |x|_p^{\alpha-1} \pi_0(|x|_p, x).$$

$$|\pi_0(x')|_p = 1.$$

Q_q. 拓扑群. Haar measure.

$$\int_{|x|_p \leq 1} dx = 1.$$

$a \in Q_p^*$

$$d(xa) = |a|_p \, dx.$$

$$f, g \in L^1 \cap L^2.$$

$$\int f \hat{g} = \int \hat{f} g.$$

$|Q_q| \geq \infty$.

数论问题

Z_q 上做积分 $[0,1]$.