5. PREDAVANJE

p-ADSKI BROJEVI

$\mathbb{Z}_p$ – p-ADSKI CIJELI BROJEVI

$= \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \{(a_1, \dots, a_n, \dots) : a_i \in \mathbb{Z}/p^i\mathbb{Z},\ a_k \equiv a_i \pmod{p^i} \text{ za } i<k, \forall i,k\}$

REFERENCA: MOJA SKRIPTA "ARITMETIČKA GEOMETRIJA"

Prop. (AG, Prop 4, str 8).
Element $x \in \mathbb{Z}_p$ je invertibilan $\Leftrightarrow x \notin p\mathbb{Z}_p$. $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

Dokaz $x=(a_n)_n$ $\quad x \in \mathbb{Z}_p^\times \Leftrightarrow \exists y \in \mathbb{Z}_p$ t.d. $x\cdot y = 1 = (1,1,\dots,1,\dots)$, $y=(b_n)_n$.

$\Rightarrow$
$x \in p\mathbb{Z}_p \Leftrightarrow a_1 = 0 \Rightarrow$ nije rješivo do $a_1 \cdot b_1 = 1$ ⇒⇐

$\Leftarrow$
$x \notin p\mathbb{Z}_p \Rightarrow a_n \not\equiv 0 + p^n\mathbb{Z}$. Zato postoji $a_n \in \mathbb{Z}$: tj. $a_n \notin p\mathbb{Z}$.

$\Rightarrow \forall a_n$ imaju inverz modulo p^n $(u\ \mathbb{Z}/p^n\mathbb{Z})$
$\Rightarrow \exists b_n \in \mathbb{Z}/p^n\mathbb{Z}$ t.d. $a_n \cdot b_n = 1 \pmod{p^n}\ \forall n$.
$k<n$. $a_k \cdot b_k = 1 \pmod{p^k}$
$\Rightarrow b_n \equiv b_k \pmod{p^k}$
$\Rightarrow y = (b_n) \in \mathbb{Z}_p$ i $x\cdot y = 1$ ✓

Prop (AG, Prop 5, str 8)
$\forall x \in \mathbb{Z}_p$ se može zapisati $0 \neq x = p^n \cdot u$ gdje je $u \in \mathbb{Z}_p^\times$ $n \in \mathbb{N}_0$.

Korolar (AG, korolar 6, str 8). $\mathbb{Z}_p$ je integralna domena.

Dokaz $x = p^n u_1$, $y = p^m u_2 \Rightarrow x\cdot y = p^{(n+m)} u_1 u_2 \neq 0$ ⇒.

Def. Neka je $a=(a_n)\in\mathbb{Z}_p$, $a_n\in[0,p^{n+1}-1]$.

Niz $(b_0,b_1,\ldots,b_n,\ldots)$ def. $\Rightarrow$ $b_0=a_1$ i $b_n=\frac{a_{n+1}-a_n}{p^n}$

se zove <u>p-adska ekspanzija</u> od a.

$p=5$

$$(2,\ 7,\ 7,\ 257,\ \ldots\ )$$

(moduli: 5, 25, 125, 625)

$$2,\ 2+b_1\cdot 5,\ 2+b_1\cdot 5+b_2\cdot 25,\ \ldots$$

$b_1\in[0,4]$, $b_2\in[0,4]$

Onda se a može zapisati kao formalni red $\boxed{a=\sum_{i=0}^{\infty} b_i\cdot p^i}$

Prop. (AG, Prop 7) $\exists!$ p-adska ekspanzija $\forall x\in\mathbb{Z}_p$.

Def. Za $\forall\, 0\neq a\in\mathbb{Z}_p$ p-adska valuacija od a, $V_p(a)$ je najveći cijeli broj m za koji je $a\in p^m\mathbb{Z}_p$.

Ekvivalentno, $V_p(a)$ je za $a=\sum_{i=0}^{\infty} b_i p^i$ najmanji m t.d. $b_m\neq 0$, i ekvivalentno $a=p^m\cdot u$, $u\in\mathbb{Z}_p^{\times}\Rightarrow V_p(a)=m$.

Prop (AG, Prop 8) Svaki ne-nul ideal u $\mathbb{Z}_p$ je oblika (p^m) za neki $m\in\mathbb{N}$.

Korolar (AG, Korolar 9) $\mathbb{Z}_p$ je DGI s jedinstvenim prostim idealom (p).

Prop (AG, Prop 10) $v_p(0) := +\infty$

Uz konvenciju da je $n+\infty = \infty$ $\forall n \in \mathbb{Z}$, p-adska valuacija zadovoljava:

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

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

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

Def Neka je R komutativni prsten. DISKRETNA VALUACIJA (na R) je funkcija $v: R \to \mathbb{Z} \cup \{\infty\}$ koja zadovoljava svojstva iz prethodne propozicije.

Def PRSTEN DISKRETNE VALUACIJE (DVR) je DGI koja sadrži ! maksimalni ideal a nije polje.

Nap. Na svakom DVR se može definirati diskretna valuacija.

POLJE p-ADSKIH BROJEVA

Def Polje p-adskih brojeva $\mathbb{Q}_p$ je polje razlomaka od $\mathbb{Z}_p$.

Nap $a \in \mathbb{Q}_p$, $a = \frac{b}{c}$, $b, c \in \mathbb{Z}_p \Rightarrow b = p^{n_1} \cdot u_1$, $c = p^{n_2} \cdot u_2$

$\Rightarrow a = p^{n_1 - n_2} \cdot (u_1 \cdot u_2^{-1}) = p^m \cdot u$, $m \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times$

$\Rightarrow a \in \mathbb{Q}_p$ def $v_p(a) = m \in \mathbb{Z} \cup \{\infty\}$.

$a = p^m u$

Uvijek $x \in \mathbb{Q}_p \Rightarrow x \in \mathbb{Z}_p$ ili $x^{-1} \in \mathbb{Z}_p$

APSOLUTNE VRIJEDNOSTI

Def Neka je k polje; APSOLUTNA VRIJEDNOST na k je funkcija $\|\cdot\| : k \to \mathbb{R}_{\geq 0}$ sa sljedećim svojstvima:

(1) $\|x\| = 0 \Leftrightarrow x = 0$

(2) $\|x \cdot y\| = \|x\| \cdot \|y\|$

(3) $\|x + y\| \leq \|x\| + \|y\|$.

Neke nama imaju jače svojstvo od (3): NUK

(3') $\|x + y\| \leq \max\{\|x\|, \|y\|\}$.

One koje zadovoljavaju (3') se zovu NEARHIMEDSKE, a one koje ne zadovoljavaju se zovu ARHIMEDSKE.

Def Definiramo p-adsku apsolutnu vrijednost $|\cdot|_p$ na $\mathbb{Q}_p$ s

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

Sjetimo se $\mathbb{Q} \subseteq \mathbb{Q}_p$ pa dobivamo AV na $\mathbb{Q}$.

VRIJEDI: $\mathbb{Q}_p$ je upotpunjenje od $\mathbb{Q}$ s obzirom na $|\cdot|_p$.

~~Napomena za def~~ Vrijedi $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.

Nap! Vrijedi da $\mathbb{Z}_p$ nije algebarsko zatvorenje od $\mathbb{Z}$ u $\mathbb{Q}_p$.

Vrijedi da je $\mathbb{Z}_p$ integralno zatvoren u $\mathbb{Q}_p$.

po $|\ |_p$ nešto je "mali" ako je djeljiv s "velikom" potencijom od p.

KRATKO PONAVLJANJE ATB

Neka je K PAB, L/K konačno Galoisovo proširenje.
$[L:K] = n$.

$\mathfrak{p}$ fiksan prosti ideal u K (u O_K).

$$\mathfrak{p} O_L = (\mathfrak{p}_1 \cdot \mathfrak{p}_2 \quad \mathfrak{p}_r)^e$$

, gdje su $\mathfrak{p}_i$ drugog

cisti stupanj inercije f. $O_L/\mathfrak{p}_i = \mathbb{F}_{p^f}$.

Vrijedi $\boxed{r \cdot e \cdot f = n}$.

$Gal(L/K)$ djeluje tranzitivno na $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

Def DEKOMPOZICIJSKA GRUPA $D(\mathfrak{p}_i/\mathfrak{p})$ od $\mathfrak{p}_i$.

$$D(\mathfrak{p}_i/\mathfrak{p}) = \{\sigma \in Gal(L/K) \mid \sigma(\mathfrak{p}_i) = \mathfrak{p}_i\} \leq Gal(L/K).$$

= Stabilizator od $\mathfrak{p}_i$.

Nap. $D(\mathfrak{p}_j/\mathfrak{p}) = \sigma D(\mathfrak{p}_i/\mathfrak{p}) \sigma^{-1}$, gdje je $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$.

$$TOS \Rightarrow \boxed{\# D(\mathfrak{p}_i/\mathfrak{p}) = \frac{n}{r} = e \cdot f}$$

Primjer $Gal(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) \simeq (\mathbb{Z}/\varphi(15)\mathbb{Z})^\times \simeq \mathbb{Z}/8\mathbb{Z}$.

$$= \{\sigma_a : a \in (\mathbb{Z}/15\mathbb{Z})^\times\} \qquad \sigma_a(\zeta_{15}) = \zeta_{15}^a.$$

$O_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. $f(\zeta_{15}) = 0$ $\quad \bar{f}$ je min polinom

faktor $\bar{f}$ u $\mathbb{F}_p[X]$

~~$\mathbb{Z}/\mathbb{Z}[\zeta_{15}]$~~ $\rightarrow \mathbb{F}$

$\mathfrak{p}_2 = (2, \zeta_{15}^4 + \zeta_{15} + 1)$ ← $f \bmod \mathbb{F}_2[x] = (x^4+x+1)(\dots)$

$\mathfrak{p}_3 = (3, \zeta_{15}^4 + \zeta_{15}^3 + \zeta_{15}^2 + \zeta_{15} + 1)$

$\mathfrak{p}_5 = (5, \zeta_{15}^2 + \zeta_{15} + 1)$

$\mathfrak{p}_{31} = (31, \zeta_{15} + 1)$

	n	e	f
$\mathfrak{p}_2$	2	1	4
$\mathfrak{p}_3$	1	2	4
$\mathfrak{p}_5$	1	4	2
$\mathfrak{p}_{31}$	8	1	1

$D(\mathfrak{p}_3 | 3) = D(\mathfrak{p}_5 | 5) = \mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$

$D(\mathfrak{p}_{31} | 31) = \{\mathrm{id}\}.$

$D(\mathfrak{p}_2 | 2) = ? = \{\mathrm{id}, \sigma_2, \sigma_4, \sigma_8\}.$

$G_4(\zeta_{15}) = \zeta_{15}^4$

$\sigma_2^2(\zeta_{15}) = \zeta_{15}^{16} = \zeta_{15}.$

Dalje o p-adskim brojevima:

Tm (AG, Tm 20, str 15)

(1) $\mathbb{Z}_p^\times \cong (\mathbb{Z}/p-1\mathbb{Z}) \times \mathbb{Z}_p$ za $p \neq 2$, i $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ za $p=2$.

(2) $\mathbb{Q}_p^\times \cong \mathbb{Z} \times (\mathbb{Z}/p-1\mathbb{Z}) \times \mathbb{Z}_p$ za $p \neq 2$, i $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ za $p=2$.

Prop (AG, Prop 21) Za $p \neq 2$ i prirodan broj m $\exists$ m-ti korijen od 1 u $\mathbb{Q}_p^\times$ (tj element reda m) $\Leftrightarrow m \mid p-1$,

za $p=2$ -1 i 1 su jedini korijeni od 1.

KVADRATI U $\mathbb{Q}_p^\times$

TM (AO, TM 23) $p \neq 2$.

1) $x = p^n u \in \mathbb{Q}_p^\times$ je kvadrat $\iff$ n je paran i u mod p je kvadrat u $(\mathbb{Z}/p\mathbb{Z})^\times$.

2) $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$

3) Neka je $c \in \mathbb{Z}_p^\times$, c mod p nije kvadrat. Tada slike od $\underline{p}$ i $\underline{c}$ generiraju $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$.

Nap

$$\mathbb{Q}_p(\sqrt{a}) = \mathbb{Q}_p(\sqrt{b}) \iff a = b \cdot y^2 \iff a (\mathbb{Q}_p^\times)^2 = b (\mathbb{Q}_p^\times)^2$$

$\Rightarrow$ $\exists$ 3 KVADRATNA PROŠIRENJA OD $\mathbb{Q}_p$.

Vratimo se na $D(p_i/p)$ ($\leq L$, $\leq K$). Neka je $\sigma \in D(p_i/p)$

$\Rightarrow \sigma(p_i) = p_i \Rightarrow \sigma$ inducira automorfizam od

$$D(p_i/p) \curvearrowright O_L/p_i \ni (x + p_i)^\sigma = x^\sigma + p_i$$

($\subseteq O_L/p_i$)

$\Rightarrow$ dobivamo homomorfizam

$$D(p_i/p) \to Gal((O_L/p_i)/(O_K/p))$$

(σ fiksira O_K

Def INERCIJSKA GRUPA $I(\mathfrak{P}_i/\mathfrak{p})$ je jezgra ovog homomorfizma.

Ekvivalentno $I(\mathfrak{P}_i/\mathfrak{p}) = \{ \sigma \in D(\mathfrak{P}_i/\mathfrak{p}) \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}_i} \}$

$$D(\mathfrak{P}_i/\mathfrak{p}) / I(\mathfrak{P}_i/\mathfrak{p}) \simeq Gal\left((O_L/\mathfrak{P}_i) / (O_K/\mathfrak{p}) \right).$$

(annotations: $e \cdot f$ above $D(\mathfrak{P}_i/\mathfrak{p})$, f above the Galois group)

$\Rightarrow \#I(\mathfrak{P}_i/\mathfrak{p}) = e$