

10.5.2010

2.8.12

$$U = Z^*$$

$$U_n = 1 + p^n Z_p$$

$$\beta(uU_n) = \varepsilon_1(u)$$

$$\ker(\beta) = U_1/U_n$$

$$1 \longrightarrow \mathcal{U}_L / \mathcal{U}_n \xrightarrow{\alpha} \mathcal{U} / \mathcal{U}_n \xrightarrow{\beta} (\mathbb{Z} / p\mathbb{Z})^* \longrightarrow 1$$

$$V_n = \{u \in U_n \mid (u \cup u_n)^{p-1} = u_n\}$$

$$\text{rad } n \quad \int \int u/u_n = u_1/u_n \times V_n$$

$$V = \{u \in U \mid u^{p-1} = 1\} \quad \text{max : } \underline{\text{Cen}}$$

שני גורמים λ שרשי הריבוע מסדר $p-1$ ב- $\mathbb{Q}_p$.
 נחלקי: V היא מרחב $\mathbb{F}_3$ מסדר $p-1$; λ ו- μ
 גורמים הריבוע μ ו- λ שרשי מילויים $\mathbb{F}_3$.

[illegible][illegible]

כ"ב שמי' ה'תרי"ג עשר לך חת מה חבוב סומט Q_p^*
 וספן ס' ו"א ח"ט מה חבוב סומט, חספס חבוב חספס

$p=2$ 330 ~ $\sqrt{3}$ V $p=1$ $\sqrt{3}$ 42, $p=2$ 330
 $p=1$ 330 $p=2$ 330 ($\sqrt{3}$) 330 $R \subseteq U$

$$R = V \quad \text{so} \quad R \subseteq V \quad \text{for } \Omega, \quad r \in R \quad \Omega^r$$

Sei $\gamma \in \Gamma$, $y_n \in U_1$, $x_n \in U_2$ e, per ogni n s.f., $u \in U$ si

$$u \equiv x_n y_n \pmod{U_n} \quad \text{p.s.} \quad y_n^{p-1} \in U_n$$

ב"מ, ע-א וסודות, ע' מן המצב $\{x_n\}$ ל- $\{x_n\}_{n=1}^\infty$

$$x_{ng_n} \xrightarrow{h_{ng_n}} a \quad \text{! / } \Rightarrow \text{ w. } a \in U_1 \quad \text{direct reason}$$
$$n \int \int x_n y_n u^{-2} \epsilon u_n \quad (3)$$

$$(x_n y_n u^{-1} \xrightarrow{n \rightarrow \infty} 1 \quad \text{für } |x_n y_n u^{-1} - 1| \leq \rho^{-n} \xrightarrow{n \rightarrow \infty} 0$$

נגדל מנסה $\{y_n\}_{n \geq 1}$ כן יום. $x_n y_n \xrightarrow{n \rightarrow \infty} u$
 $\downarrow$
 u

$$y_n^{p-1} \xrightarrow{n \rightarrow \infty} 1 \quad ; \text{כי} \quad y_n^{p-1} \in U_n = 1 + p^n \mathbb{Z}_p, \quad y \in U$$

$$\downarrow$$

$$y^{p-1} \Rightarrow y^{p-1} = 1 \Rightarrow y \in V.$$

$U \cap V = \{1\}$ נגדל מנסה, $U = U_1 \cdot V$: נגדל מנסה

$(x \in \mathbb{Z}_p) \quad 1 + px \in U_1$: נגדל מנסה

$(1+px)^{p-1} = 1$

$$\Rightarrow 1 + \sum_{k=1}^{p-1} \binom{p-1}{k} p^k x^k = 1$$

$$px \left((p-1) + \underbrace{\binom{p-1}{2} p x + \dots + \binom{p-1}{p-2} p^{p-3} x^{p-3} + p^{p-2} x^{p-2}}_{\in p \mathbb{Z}_p} \right) = 0$$

נגדל מנסה : נגדל מנסה $p \geq 3$ נגדל מנסה $x \neq 0$ נגדל מנסה

$1+px=1$ נגדל מנסה, $x=0$ נגדל מנסה, $1 \notin p \mathbb{Z}_p$ נגדל מנסה $1+px \in 1+p \mathbb{Z}_p$ נגדל מנסה

$1+px = (1+px)^{p-1} = 1 \quad ; \quad p=2$ נגדל מנסה

נגדל מנסה

$$U_1 \cong \varprojlim U_1/U_n$$

$$U_1/U_n \subseteq U/U_n \cong (\mathbb{Z}/p^n \mathbb{Z})^*$$

$(p \geq 3 \Rightarrow \text{נגדל מנסה}) \quad \phi(p^n) \xrightarrow{\sim} \mathbb{Z}/p^n \mathbb{Z}$

$(p^{n+1} \text{ נגדל מנסה}) \quad \mathbb{Z}/p^{n+1} \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p^n \mathbb{Z}$

$\alpha = 1+p$ נגדל מנסה, $\alpha \in U_1 \setminus U_2$ נגדל מנסה

$\alpha \in U_1 \setminus U_2$ נגדל מנסה $\alpha \in U_n$ נגדל מנסה : נגדל מנסה

נגדל מנסה $\alpha \in U_n \setminus U_{n+1}$ נגדל מנסה $\alpha \in U_{n+1}$ נגדל מנסה

$\forall n \quad \alpha^p \in U_{n+1} \setminus U_{n+2}$

$V \in \mathbb{Z}_p^*$ נגדל מנסה, $\gamma = 1 + p^n V$ נגדל מנסה

$$\gamma^p = (1 + p^n V)^p = \sum_{k=0}^p \binom{p}{k} p^{nk} V^k =$$

$$= 1 + p^{n+1} V + \sum_{k=2}^{p-1} \binom{p}{k} p^{nk} V^k + p^{np} V^p$$

$k \geq 2 \Rightarrow p^{nk+1} \Rightarrow p^{n+1} \binom{p}{k} p^{nk}, \quad nk+1 \geq 2n+1 \geq n+2$

$(p \geq 3) \quad np \geq 3n \geq n+2$

נגדל מנסה, $\gamma^p \in U_{n+2}$ נגדל מנסה, $\gamma^p \in 1 + p^{n+2} \mathbb{Z}_p = U_{n+1}$ נגדל מנסה

$p^{n+1} V \in p^{n+2} \mathbb{Z}_p \Rightarrow V \in p \mathbb{Z}_p \quad V \in \mathbb{Z}_p^*$ נגדל מנסה

$$\alpha \in U_1 \setminus U_2 \Rightarrow \alpha^p \in U_2 \setminus U_3 \Rightarrow \alpha^{p^2} \in U_3 \setminus U_4 \Rightarrow \dots$$

$$\Rightarrow (\alpha U_n)^{p^{n-2}} \neq 1 \cdot U_n$$

~~אם~~ $\alpha \in U_n$ אז $\alpha^{p^{n-2}} = 1$ כי U_n היא קרן של $\mathbb{F}_p$ וכל $x \in U_n$ מקיים $x^{p^n} = 1$.

נניח $p=2$ ונראה ש $U_2 \cong \mathbb{Z}_2$ ו $U_3 \cong \mathbb{Z}_4$.

$$(\alpha \equiv 5 \pmod{8}) \quad \alpha \in U_2 \setminus U_3 \quad \text{אז } \alpha^2 \equiv 1 \pmod{8}$$

$$(\alpha^{p^{n-2}})^{p^2} = \alpha^{p^n} = 1 \quad \text{אם } \alpha \in U_n$$

$$U_1 \cong \mathbb{Z}_p, \quad p \neq 2 \quad \text{אם } \alpha \in U_1 \setminus U_2$$

$$U_2 = \{\pm 1\} \times U_1, \quad p=2 \quad \text{אם } \alpha \in U_2 \setminus U_1$$

$$U_2 \cong \mathbb{Z}_p = \mathbb{Z}_2$$

$$\alpha \in U_1 \setminus U_2 \quad \text{אז } \alpha^2 \equiv 1 \pmod{p^2}$$

$$f: U_1 \rightarrow \mathbb{Z}_p$$

$$f(u) = \{i_n + p^{n-1} \mathbb{Z}\}_{n=2}^\infty$$

$$|U_1/U_n| = p^{n-1} \quad \text{אם } \alpha \in U_1 \setminus U_2 \quad \text{אז } \alpha^{p^{n-1}} \equiv 1 \pmod{p^n}$$

$$i_{n+1} \equiv i_n \pmod{p^{n-1}} \quad \text{אם } \alpha \in U_1 \setminus U_2$$

$$U^{p^{n-1}} \alpha^{i_n} \in U_n \quad \text{אם } \alpha \in U_1 \setminus U_2$$

$$U^{p^{n-1}} \alpha^{i_{n-1}} \in U_{n+1} \subseteq U_n \quad \text{אם } \alpha \in U_1 \setminus U_2$$

$$u U_n = \alpha^{i_n} U_n = \alpha^{i_{n+1}} U_n \quad \text{אם } \alpha \in U_1 \setminus U_2$$

$$(u U_n)^{p^{n-1}} = (\alpha U_n)^{p^{n-1}} \quad \text{אם } \alpha \in U_1 \setminus U_2$$

$$i_n \equiv i_{n+1} \pmod{p^{n-1}}$$

$$f(uv) = f(u) + f(v) \quad \text{אם } \alpha \in U_1 \setminus U_2$$

$$2 \leq n \quad \text{אם } i_n \in p^{n-1} \mathbb{Z} \quad \text{אז } u \in \ker f$$

$$u U_n = U_n \quad \text{אם } \alpha \in U_1 \setminus U_2 \quad \text{אז } \alpha^{p^{n-1}} \equiv 1 \pmod{p^n}$$

$$u=1 \quad \text{אם } \forall n \quad |u-1| \leq p^{n-1} \rightarrow 0 \quad \text{אם } \alpha \in U_1 \setminus U_2$$

$$\mathbb{Z}_p \ni \{i_n + p^{n-1} \mathbb{Z}\}_{n=2}^\infty \quad \text{אם } \alpha \in U_1 \setminus U_2$$

$$\alpha^{i_{n+1}} U_n = \alpha^{i_n} U_n \quad \text{אם } \alpha \in U_1 \setminus U_2 \quad \text{אז } i_n \equiv i_{n+1} \pmod{p^{n-1}}$$

$$\alpha^{i_{n+1}-i_n} \in U_n \quad \text{אם } \alpha \in U_1 \setminus U_2 \quad \text{אז } i_n \equiv i_{n+1} \pmod{p^{n-1}}$$

$$1 = |\alpha^{i_n}| \rightarrow \text{אם } \alpha \in U_1 \setminus U_2 \quad \text{אז } |\alpha^{i_{n+1}-i_n} - 1| \leq p^{-n}$$

$$|\alpha^{i_{n+1}} - \alpha^{i_n}| \leq p^{-n} \quad \text{אם } \alpha \in U_1 \setminus U_2$$

$u \in U_2$ לכל מספר n יהיה
 $|\alpha^{i_{n+2}} - \alpha^{i_n}| = |(\alpha^{i_{n+2}} - \alpha^{i_{n+1}}) + (\alpha^{i_{n+1}} - \alpha^{i_n})| \leq$
 $\leq \max\{p^{-(n+1)}, p^{-n}\} = p^{-n}$
 $|\alpha^{i_{n+2}} - \alpha^{i_n}| \leq \max\{p^{-(n+j)}\}_{j=0}^n = p^{-n}$: כלומר
 $2 \leq n$ לכל $|u - \alpha^{i_n}| \leq p^{-n}$: ולכן $u \in U_n$

$u - \alpha^{i_n} \in p^n Z_p$
 $u \in \alpha^{i_n} + p^n Z_p = \alpha^{i_n} (1 + p^n Z_p)$ ($\alpha^{i_n} \in Z_p^*$)
 $u \in \alpha^{i_n} U_n$
 $f(u) = \{i_n + p^{n-2} \mathbb{Z}\}_{n \geq 2}$, וכל $u U_n = \alpha^{i_n} U_n$

$f: U_2 \rightarrow \mathbb{Z}_p$, נשים $\alpha \in U_2 \setminus U_3$, נגד: $p=2$
 $f(u) = \{i_n + p^{n-2} \mathbb{Z}\}_{n \geq 3}$ ($p=2$)
 $p^{n-2} = |U_2/U_n|$
 , f מונוטונית - נגד

$U_2 \rightarrow U_2/U_2 \cong \mathbb{Z}/2\mathbb{Z}$: $p=2$, כלומר
 $\varphi: 1+2x \mapsto (1+2x)U_2 \mapsto \varepsilon_2(x)$
 $\varphi: U_2 \rightarrow \mathbb{Z}/2\mathbb{Z}$: מונומורפיזם
 $\varphi(1+2x) = \varepsilon_2(x)$

$\{\pm 1\}$: 2 מספרים φ מונומורפיזם
 $\varphi(1) = \varphi(1+2 \cdot 0) = \varepsilon_2(0) = 0 \pmod{2}$
 $\varphi(-1) = \varphi(1+2(-1)) = \varepsilon_2(-1) = 1 \pmod{2}$
 $\mathbb{Z}/2\mathbb{Z}$: כל $u \in U_2$, $\varphi|_{\{\pm 1\}}$, כל
 $\varepsilon \in \{\pm 1\}$, $u \in U_2$, כל
 $\varphi(u) = \varphi(\varepsilon)$

$u \varepsilon^{-1} \in \ker \varphi = U_2$, כלומר
 $U = \varepsilon \cdot U_2$, כל $u \in \varepsilon U_2 \subseteq \varepsilon \cdot U_2$
 $\therefore -1 \in U_2$, כלומר , $\{\pm 1\} \cap U_2 = \{\pm 1\}$, כל
 $-1 \in 1 + 4\mathbb{Z}_2 \Rightarrow 2 \in 4\mathbb{Z}_2 \Rightarrow 1 \in 2\mathbb{Z}_2$, כל

: צד 1

: צד 2 $p \neq 2$ $\Rightarrow$ $\mathbb{Z}_p^* \cong \mathbb{Z} \times \mathbb{Z}_{p-1}$

: צד 3 $p=2$ $\Rightarrow$ $\mathbb{Z}_2^* \cong \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}_2$

: צד 4 $\mathbb{Q}_p^*$ $\cong$ $\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}_p$

$$(\mathbb{Q}_p^*)^2 = \{x^2 \mid x \in \mathbb{Q}_p^*\}$$

: צד 5 $p \neq 2$ $\Rightarrow$ $\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}_p$

$x = p^n u$ $u \in \mathbb{Z}_p^*$ $x \in \mathbb{Q}_p^*$ $\Rightarrow$ $x^2 = p^{2n} u^2$

$u \in \mathbb{Z}_p^* \Rightarrow u \equiv a \pmod{p}$ $a \in \mathbb{Z}_p^*$ $\Rightarrow$ $u^2 \equiv a^2 \pmod{p}$

$u \mapsto u \pmod{p} \mapsto (u \pmod{p})^2 \in (\mathbb{Z}_p^*)^2$

$u \mapsto u \pmod{p} \mapsto \varepsilon_2(u)$

$\left(\left(\frac{\varepsilon_2(u)}{p}\right) = 1 \pmod{p}\right)$ $\Rightarrow$ $\varepsilon_2(u) \in (\mathbb{Z}_p^*)^2$

$\left(\frac{u}{p}\right) = \left(\frac{\varepsilon_2(u)}{p}\right)$: צד 6

$(x = p^n u \mapsto (n, u))$ $\mathbb{Q}_p^* \cong \mathbb{Z} \times \mathbb{U}$: צד 7

$\mathbb{U} = \mathbb{Z}_p^* \Rightarrow u \in \mathbb{U} \Leftrightarrow u \in \mathbb{Z}_p^*$

$\mathbb{U} = \mathbb{U}_2 \times V \cong \mathbb{Z}_p \times V$

$\mathbb{U}^2 = \mathbb{U}_2^2 \times V^2 \cong 2\mathbb{Z}_p \times V^2$

$\mathbb{U}_2 \in \mathbb{Z}_p^*$ $\Rightarrow$ $\mathbb{U}_2^2 \in \mathbb{Z}_p^*$ $\Rightarrow$ $\mathbb{U}_2^2 \in \mathbb{Z}_p^*$

$u = u_2 \cdot v$ $v \in V$ $u_2 \in \mathbb{U}_2$ $\Rightarrow$ $u^2 = u_2^2 \cdot v^2$

$V \Rightarrow$ $v \in V \Leftrightarrow v \in \mathbb{U}_2$ $\Rightarrow$ $v \in \mathbb{U}_2$

$\varepsilon_2(u) = \varepsilon_2(u_2) \varepsilon_2(v) = \varepsilon_2(v) \in (\mathbb{Z}_p^*)^2$

$\varepsilon_2|_V : V \rightarrow (\mathbb{Z}_p^*)^2$ $\Rightarrow$ $\varepsilon_2|_V$ $\Rightarrow$ $\varepsilon_2(u) \in (\mathbb{Z}_p^*)^2$

$\varepsilon_2(u) \in (\mathbb{Z}_p^*)^2 \Leftrightarrow \varepsilon_2(v) \in (\mathbb{Z}_p^*)^2$

: צד 8 $p=2$ $\Rightarrow$ $\mathbb{Q}_2^* \cong \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}_2$

$x = 2^n u$ $u \in \mathbb{Z}_2^*$ $x \in \mathbb{Q}_2^*$ $\Rightarrow$ $x^2 = 2^{2n} u^2$

$u \in \mathbb{Z}_2^* \Rightarrow u \equiv 1 \pmod{2}$ $\Rightarrow$ $u^2 \equiv 1 \pmod{2}$

$u \equiv 1 \pmod{2} \Rightarrow u \in 1 + 2\mathbb{Z}_2$ $\Rightarrow$ $u^2 \equiv 1 \pmod{2}$

$$\mathbb{Q}_p^* / (\mathbb{Q}_p^*)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
$$\mathbb{Q}_2^* / (\mathbb{Q}_2^*)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$(Q_2^* \cong \mathbb{Z} \times \{\pm 1\} \times (U_2 \cong \mathbb{Z}_2)) \quad \text{is not}$$

$$(\mathbb{Q}_3^*)^2 \cong 2\mathbb{Z} \times \{1\} \times 2\mathbb{Z}_2$$

$$Q_p^* \rightarrow \text{analog } (Q_p^*)^2 : \text{analog}$$

$p \neq 2$ rows, $\text{len} \sqrt{}$

$$(Q_p^*)^2 = \bigcup_{h \in \mathbb{Z}} p^{2h} U^2 = \bigcup_n p^{2n} U_1^2 \cdot V^2 = \bigcup_n p^{2n} U_1 \cdot \overset{\uparrow}{V^2} =$$

$$= \bigcup_{a \in V^2} \bigcup_{n \in \mathbb{Z}} \underbrace{(p^{2n} a U)}_{\text{orbit}} = \text{orbit of } p^{2n} a U$$

minimale ρ mit $U_{2^{2n}} U_3$ $\mathcal{L}_{2^p}$ $p=2$ es

פירק 3 - הסדר הלימוד

מסמך: כרמל ריבלין 20

$\bar{K} \rightarrow \pi^0 \ell^+ \ell^-$ vs $\gamma \pi^0 \ell^+ \ell^-$ $K \rightarrow \pi^0 \ell^+ \ell^-$

 $x^2 - 3x = 0$ nullen, $3 \notin (k^*)^2$ neu. $3 \in k^*$ / neu

$\pm \sqrt{50}$ → unvollst., $k \rightarrow$ wie oft je c

שורש $\sqrt{a}$ הוא מספר חיובי x כזה ש- $x^2 = a$.

$$k(\sqrt{5}) \quad \text{Lille } p=0$$

$$\{x + y\sqrt{b} \mid x, y \in k\} \subseteq k(\sqrt{b})$$

Answer: Since $\sin \theta$ is odd

$(y \neq 0 \Rightarrow \sqrt{y} = \frac{x}{y} \in K) \quad x=y=0 \quad (\Leftrightarrow x+y\sqrt{y}=0 \quad \hookrightarrow \text{OK})$

13 June 1950, Gila Wood, Santa Fe

$$\frac{1}{x+y\sqrt{5}} = \frac{x-y\sqrt{5}}{x^2-y^2 \cdot 5} = \frac{x}{x^2-y^2 \cdot 5} + \frac{-y}{x^2-y^2 \cdot 5} \sqrt{5}$$

הומומורפיזם

$k(\sqrt{b})$ הומומורפיזם $\overline{(x+y\sqrt{b})} = x-y\sqrt{b}$

$z \in k(\sqrt{b})$ הערות: $tr(z) = z + \bar{z} (= 2x)$
 $(k(\sqrt{b}) \rightarrow k)$ k הערות $\sqrt{b}$

$N_{k(\sqrt{b})/k}(z) = z \cdot \bar{z} = (x+y\sqrt{b})(x-y\sqrt{b}) = x^2 - y^2b$ הערות: $x^2 - y^2b$

k^* הערות N $k(\sqrt{b})^*$ $\sqrt{b}$

$(a,b) = 1$ הערות: $a, b \in k^*$
 $z^2 - ax^2 - by^2 = 0$ הערות: $(0,0,0) \neq$ $(a,b) = -1$

$(ar^2, bs^2) = (a, b) \quad \forall r, s \in k^*$ הערות:

$\frac{k^*}{(k^*)^2} \times \frac{k^*}{(k^*)^2} \rightarrow \{\pm 1\}$ הערות: $(a,b) = 1$

$a \in N(k(\sqrt{b})) \Leftrightarrow (a,b) = 1$

$(a, c^2) = 1$ הערות: $c \in k^*$ $b = c^2$

$z = 1, x = 0, y = \frac{1}{c}$ הערות: $1^2 - a \cdot 0^2 - b \cdot \frac{1}{c^2} = 1 - \frac{c^2}{c^2} = 0$

$\sqrt{b} = \sqrt{c^2} \in k \Rightarrow k(\sqrt{b}) = k$

$N(x) = x$ הערות: N k

$(z,y) = (0,0) \Rightarrow z^2 = by^2$ הערות: $z \neq 0$ $ax^2 = z^2 - by^2$

$a = (\frac{z}{x})^2 - b(\frac{y}{x})^2 = N(\frac{z}{x} + \frac{y}{x}\sqrt{b}) \in N(k(\sqrt{b}))$

$a = z_0^2 - by_0^2$ הערות: $a \in N(k(\sqrt{b}))$ $(1, y_0, z_0)$

צד 1: $p \neq 2$, $u, v \in \mathbb{Z}_p^*$, $(u, v) = 1$

$$z^2 - ux^2 - vy^2 = 0 \quad \text{! מכנה}$$

מכנה p : $z^2 - ux^2 - vy^2 \equiv 0 \pmod{p}$ - משוואה הומוגנית בשלוש משתנים מעלה שני ב $\mathbb{Z}_p$

משוואה הומוגנית מעלה שני, כל משוואה הומוגנית מעלה שני (או מעלה זוגית) מעלה שני, כל משוואה הומוגנית מעלה שני מעלה שני, כל משוואה הומוגנית מעלה שני מעלה שני.

$$(x, y, z) \begin{pmatrix} -u & -v \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

$$z^2 - ux^2 - vy^2 = 0$$

אם $z \neq 0$, אז $x, y \in \mathbb{Z}_p$ הם פתרונות למשוואה $z^2 - ux^2 - vy^2 = 0$.