תבניות ריבועיות ומספרים p־אדיים

30 ביוני 2026

תוכן עניינים

1 תבניות ביליניאריות סימטריות 3
1.1 כותרת כלשהי 3
1.2 פעולות עמודה אלמנטריות 4
1.3 מיון מרחבים ריבועיים 5
1.4 איזוטרפיות 8
2 מספרים p־אדיים 13
2.1 שדות נורמיים 13
2.2 תזכורת על מרחבים מטריים שלמים והשלמה 17
2.3 שדה המספרים ה־p־אדיים 19
3 בחזרה לתבניות ריבועיות 25

1 תבניות ביליניאריות סימטריות

סוף הרצאה 1 – 24/03

תשלימי...

סוף הרצאה 2 – 14/04

תשלימי...

1.1 כותרת כלשהי

תזכורת:

טענה 1.1

יהי V מרחב וקטורי נוצר סופית מעל $\mathbb{F}$ ו־g תבנית בילנארית סימטרית על V.
אז קיים בסיס $\mathcal{B}$ של V כך ש־$[g]_{\mathcal{B}}$ מטריצה אלכסונית.

מסקנה 1.2

לכל $A \in M_n(\mathbb{F})$ סימטרית קיימת מטריצה $D \in M_n(\mathbb{F})$ אלכסונית אשר חופפת ל־A.

– סוף התזכורת –
יהי $\mathbb{F}$ שדה ונסתכל על $(\mathbb{F}^\times)^2 = \{a^2 \mid a \in \mathbb{F}^\times\}$ זו תת־חבורה של $\mathbb{F}^\times$ ביחס לכפל.
נסמן ב־$\pi : \mathbb{F}^\times \to \mathbb{F}^\times\big/_{(\mathbb{F}^\times)^2}$ ההומומורפיזם הקאנוני כלומר $\pi(a) = a(\mathbb{F}^\times)^2$ לכל $a \in \mathbb{F}^\times$.
תת־קבוצה $R \subseteq \mathbb{F}^\times$ תיקרא קבוצת נציגים כאשר $\pi|_R : R \to \mathbb{F}^\times\big/_{(\mathbb{F}^\times)^2}$ הוא חד־חד ערכי ועל.
מעכשיו נקבע קבוצת נציגים R כלשהי ב־$\mathbb{F}$.

עובדה

לכל $a \in \mathbb{F}^\times$ קיים $r \in R$ יחיד ו־$c \in \mathbb{F}^\times$ כך ש־$a = rc^2$.

דוגמה

1. $\mathbb{F} = \mathbb{C}$ אז $(\mathbb{C}^\times)^2 = \mathbb{C}^\times$ ומתקיים $\left|\mathbb{C}^\times\big/_{(\mathbb{C}^\times)^2}\right| = 1$ וניתן לבחור $R = \{1\}$
2. $\mathbb{F} = \mathbb{R}$ אז $(\mathbb{C}^\times)^2 = \{x \in \mathbb{R}^\times \mid x > 0\}$ ומתקיים $\left|\mathbb{R}^\times\big/_{(\mathbb{R}^\times)^2}\right| = 2$ וניתן לבחור $R = \{-1, 1\}$

טענה 1.3

יהי p ראשוני ו־$p \neq 2$ אז $\left|\mathbb{F}_p^\times\big/_{(\mathbb{F}_p^\times)^2}\right| = 2$.
בנוסף, לכל $r \in \mathbb{F}_p^\times \setminus \left(\mathbb{F}_p^\times\right)^2$ ניתן לבחור קבוצת נציגים להיות $R = \{1, r\}$.

הוכחה: נגדיר $s : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ על־ידי $s(a) = a^2$ לכל $a \in \mathbb{F}_p^\times$ והוא כמובן הומומורפיזם (של חבורות) וגם $Im(s) = \left(\mathbb{F}_p^\times\right)^2$.
מתקיים $Im(s) \cong \mathbb{F}_p^\times\big/_{\ker s}$ ובנוסף $x \in \ker s \iff s(x) = 1 \iff x^2 = 1 \iff (x-1)(x+1) = 0 \iff x \in \{-1, 1\}$.
לכן $\ker s = \{1, -1\}$ ומכאן $|\ker s| = 2$.
לסיכום

$$\left|\mathbb{F}_p^\times\big/_{\left(\mathbb{F}_p^\times\right)^2}\right| = \left|\mathbb{F}_p^\times\big/_{Im(s)}\right| = \left|\mathbb{F}_p^\times\right| : |Im(s)| = \left|\mathbb{F}_p^\times\right| : \left(\left|\mathbb{F}_p^\times\right| : |\ker s|\right) = |\ker s| = 2$$

$\square$

טענה 1.4

יהי V מרחב וקטורי נוצר נוספת מעל $\mathbb{F}$, g תבנית בילנארית סימטרית על V. אז קיים בסיס $\mathcal{C}$ של V כך ש־$[g]_{\mathcal{C}}$ אלכסונית ואיברי אלכסונה שייכים ל־$R \cup \{0\}$ (כאשר R הקבוצת נציגים).

הוכחה: יהי $\mathcal{B} = (v_1, ..., v_n)$ בסיס של V כך ש־$[g]_{\mathcal{B}}$ אלכסונית ($\mathcal{B}$ בסיס אורתוגונלי).
נסמן $a_i = g(v_i, v_i) = q(v_i)$ לכל $1 \leq i \leq n$.
אם $a_i \neq 0$ אז קיימים $r_i \in R, c_i \in \mathbb{F}^\times$ כך ש־$a_i = r_i c_i^2$ ואם $a_i = 0$ נגדיר $r_i = 0$ ו־$c_i = 1$.
כעת, נגדיר $\mathcal{C} = \left(\frac{v_1}{c_1}, ..., \frac{v_n}{c_n}\right)$.
מטריצת המעבר בין הבסיסים נראית מהצורה הבאה

$$[\mathrm{Id}]_{\mathcal{B}}^{\mathcal{C}} = \begin{pmatrix} \frac{1}{c_1} & & 0 \\ & \ddots & \vdots \\ 0 & & \frac{1}{c_n} \end{pmatrix}$$

ומכאן

$$[g]_{\mathcal{C}} = \left([\mathrm{Id}]_{\mathcal{B}}^{\mathcal{C}}\right)^t [g]_{\mathcal{B}} [\mathrm{Id}]_{\mathcal{B}}^{\mathcal{C}} = \begin{pmatrix} \frac{1}{c_1} & & 0 \\ & \ddots & \vdots \\ 0 & & \frac{1}{c_n} \end{pmatrix} \begin{pmatrix} a_1 & & 0 \\ & \ddots & \vdots \\ 0 & & a_n \end{pmatrix} \begin{pmatrix} \frac{1}{c_1} & & 0 \\ & \ddots & \vdots \\ 0 & & \frac{1}{c_n} \end{pmatrix} = \begin{pmatrix} \frac{a_1}{c_1^2} & & 0 \\ & \ddots & \vdots \\ 0 & & \frac{a_n}{c_n^2} \end{pmatrix} = \begin{pmatrix} r_1 & & 0 \\ & \ddots & \vdots \\ 0 & & r_n \end{pmatrix}$$

□

מסקנה 1.5

לכל מטריצה $A \in M_n(\mathbb{F})$ סימטרית קיימת $D \in M_n(\mathbb{F})$ אלכסונית כך שאיברי אלכסונה שייכים ל־$R \cup \{0\}$ אשר חופפת ל־A.

1.2 פעולות עמודה אלמנטריות

סימון

תהיי ε פעולת שורה אלמנטרית על מטריצות מ־$M_n(\mathbb{F})$.
נסמן ב־$\overline{\varepsilon}$ את פעולת עמודה אלמנטרית המתאימה, כלומר

1. אם $\varepsilon = R_i \mapsto cR_i$ אז $\overline{\varepsilon} = C_i \mapsto cC_i$
2. אם $\varepsilon = R_i \mapsto R_i + cR_j$ אז $\overline{\varepsilon} = C_i \mapsto C_i + cR_j$
3. אם $\varepsilon = R_i \leftrightarrow R_j$ אז $\overline{\varepsilon} = C_i \leftrightarrow C_j$ (החלפת שורות/עמודות)

עובדה

לכל $A \in M_n(\mathbb{F})$ מתקיים $\overline{\varepsilon}(A) = \left(\varepsilon(A^t)\right)^t$.

טענה 1.6

תהיי ε פעולת שורה אלמנטרית, $A \in M_n(\mathbb{F})$. אז $\overline{\varepsilon}(A) = A\varepsilon(I_n)^t$.
למה זה מעניין? כי באלגברה לינארית רואים ש־$\varepsilon(A) = \varepsilon(I_n)A$.

הוכחה:

$$\overline{\varepsilon}(A) = \left(\varepsilon(A^t)\right)^t = \left(\varepsilon(I_n)A^t\right)^t = A\varepsilon(I_n)^t$$

□

מסקנה 1.7

תהיי ε פעולת שורה אלמנטרית, $A \in M_n(\mathbb{F})$. אז $\varepsilon(\overline{\varepsilon}(A)) = \overline{\varepsilon}(\varepsilon(A)) = \varepsilon(I_n)A\varepsilon(I_n)^t$.

טענה 1.8

תהיי g תבנית בילנארית סימטרית על $\mathbb{F}^n$ ונסמן את $[t]_{\mathcal{E}} = A$ (כאשר $\mathcal{E}$ הוא הבסיס הסטנדרטי).
יהיו $\varepsilon_1, ..., \varepsilon_k$ פעולות שורה אלמנטריות ונסמן $D = \overline{\varepsilon_k}(\varepsilon_k(...(\overline{\varepsilon_1}(\varepsilon_1(A)))))$ ו־$P = \overline{\varepsilon_k}(...(\overline{\varepsilon_1}(I_n)))$.
נסמן ב־$b_1, ..., b_n$ את העמודות של P ו־$\mathcal{B} = (b_1, ..., b_n)$ הוא בסיס של $\mathbb{F}^n$ וגם $[g]_{\mathcal{B}} = D$.

הוכחה: לפי הטענה לעיל מתקיים $P = I_n\varepsilon_1(I_n)^t \cdots I_n\varepsilon_k(I_n)^t = \varepsilon_1(I_n)^t \cdots \varepsilon_k(I_n)^t$ ובנוסף ברור כי $[\mathrm{Id}_V]_{\mathcal{E}}^{\mathcal{B}} = P$ ולכן

$$[g]_{\mathcal{B}} = \left([\mathrm{Id}_V]_{\mathcal{C}}^{\mathcal{B}}\right)^t [g]_{\mathcal{E}} [\mathrm{Id}_V]_{\mathcal{C}}^{\mathcal{B}} = P^t A P = \left(\varepsilon_1(I_n)^t \cdots \varepsilon_k(I_n)^t\right)^t A \varepsilon_1(I_n)^t \cdots \varepsilon_k(I_n)^t$$
$$= \varepsilon_k(I_n) \cdot \cdots \cdot \varepsilon_1(I_n) A \varepsilon_1(I_n)^t \cdot \cdots \cdot \varepsilon_k(I_n)^t = \overline{\varepsilon_k}(\varepsilon_k(...(\overline{\varepsilon_1}(\varepsilon_1)(A)))) = D$$

□

סימון

בהינתן תבנית ריבועית $q : V \to \mathbb{F}$ על מרחב וקטורי V נסמן ב־$g_q : V \times V \to \mathbb{F}$ את התבנית הבילנארית הסימטרית המקיימת

$$q(v) = g_q(v, v)$$

דוגמה

תבנית ריבועית $q:\mathbb{R}^3\to\mathbb{R}$ מוגדרת על־ידי

$$q\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=2x_1^2+8x_1x_2+8x_2^2+2x_2x_3+x_3^2$$

נמצא בסיס $\mathcal{B}$ של $\mathbb{R}^3$ כך ש־$\left[g_q\right]_{\mathcal{B}}$ אלכסונית ואיברי אלכסונה שייכים ל־$\{1,-1,0\}$.
מתקיים

$$g_q\left(\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix},\begin{pmatrix}y_1\\y_2\\y_3\end{pmatrix}\right)=2x_1y_1+4x_1y_2+4x_2y_1+8x_2y_2+x_2y_3+x_3y_2+x_3y_3$$

הצבה פשוטה מראה שמתקיים $g_q\left(\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix},\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\right)=q\left(\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\right)$ ועם (מטריצת גראם־שמידט) מתקיים גם־כן

$$\left[g_q\right]_{\mathcal{E}}=\begin{pmatrix}2&4&0\\4&8&1\\0&1&1\end{pmatrix}$$

וזו גם מטריצה סימטרית, אז (פעולות שורה עושים רק על המטריצה למעלה ועל פעולות עמודה עושים על שניהם)

$$\frac{\begin{pmatrix}2&4&0\\4&8&1\\0&1&1\end{pmatrix}}{\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}}\xrightarrow{R_2\mapsto R_2-2R_1}\frac{\begin{pmatrix}2&4&0\\0&0&1\\0&1&1\end{pmatrix}}{\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}}\xrightarrow{C_2\mapsto C_2-2C_1}\frac{\begin{pmatrix}2&0&0\\0&0&1\\0&1&1\end{pmatrix}}{\begin{pmatrix}1&-2&0\\0&1&0\\0&0&1\end{pmatrix}}\xrightarrow{R_2\leftrightarrow R_3}\frac{\begin{pmatrix}2&0&0\\0&1&1\\0&0&1\end{pmatrix}}{\begin{pmatrix}1&-2&0\\0&1&0\\0&0&1\end{pmatrix}}\xrightarrow{C_2\leftrightarrow C_3}\frac{\begin{pmatrix}2&0&0\\0&1&1\\0&1&0\end{pmatrix}}{\begin{pmatrix}1&0&-2\\0&0&1\\0&1&0\end{pmatrix}}$$

$$\xrightarrow{R_3\mapsto R_3-R_2}\frac{\begin{pmatrix}2&0&0\\0&1&1\\0&0&-1\end{pmatrix}}{\begin{pmatrix}1&0&-2\\0&0&1\\0&1&0\end{pmatrix}}\xrightarrow{C_3\mapsto C_3-C_2}\frac{\begin{pmatrix}2&0&0\\0&1&0\\0&0&-1\end{pmatrix}}{\begin{pmatrix}1&0&-2\\0&0&1\\0&1&-1\end{pmatrix}}\xrightarrow{R_1\mapsto\frac{1}{\sqrt{2}}R_1}\frac{\begin{pmatrix}\sqrt{2}&0&0\\0&1&0\\0&0&-1\end{pmatrix}}{\begin{pmatrix}1&0&-2\\0&0&1\\0&1&-1\end{pmatrix}}\xrightarrow{C_1\mapsto\frac{1}{\sqrt{2}}C_1}\frac{\begin{pmatrix}1&0&0\\0&1&0\\0&0&-1\end{pmatrix}}{\begin{pmatrix}\frac{\sqrt{2}}{2}&0&-2\\0&0&1\\0&1&-1\end{pmatrix}}$$

נגדיר $\mathcal{B}=\left(\begin{pmatrix}\frac{\sqrt{2}}{2}\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\1\end{pmatrix},\begin{pmatrix}-2\\1\\-1\end{pmatrix}\right)$ ואז $\left[g_q\right]_{\mathcal{B}}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&-1\end{pmatrix}$.

דוגמה

תבנית ריבועית $q:\mathbb{R}^2\to\mathbb{R}$ מוגדרת על־ידי $q\begin{pmatrix}x_1\\x_2\end{pmatrix}=x_1x_2$.
מתקיים

$$g_q\left(\begin{pmatrix}x_1\\x_2\end{pmatrix},\begin{pmatrix}y_1\\y_2\end{pmatrix}\right)=\frac{1}{2}x_1y_2+\frac{1}{2}x_2y_1$$

וכן

$$\left[g_q\right]_{\mathcal{E}}=\begin{pmatrix}0&\frac{1}{2}\\\frac{1}{2}&0\end{pmatrix}$$

אז

$$\frac{\begin{pmatrix}0&\frac{1}{2}\\\frac{1}{2}&0\end{pmatrix}}{\begin{pmatrix}1&0\\0&1\end{pmatrix}}\xrightarrow{R_1\mapsto R_1+R_2}\frac{\begin{pmatrix}\frac{1}{2}&\frac{1}{2}\\\frac{1}{2}&0\end{pmatrix}}{\begin{pmatrix}1&0\\0&1\end{pmatrix}}\xrightarrow{C_1\mapsto C_1+C_2}\frac{\begin{pmatrix}1&\frac{1}{2}\\\frac{1}{2}&0\end{pmatrix}}{\begin{pmatrix}1&0\\1&1\end{pmatrix}}\xrightarrow{R_2\mapsto R_2--\frac{1}{2}R_1}\frac{\begin{pmatrix}1&\frac{1}{2}\\0&-\frac{1}{4}\end{pmatrix}}{\begin{pmatrix}1&0\\1&1\end{pmatrix}}\xrightarrow{C_2\mapsto C_2-\frac{1}{2}C_1}\frac{\begin{pmatrix}1&0\\0&-\frac{1}{4}\end{pmatrix}}{\begin{pmatrix}1&-\frac{1}{2}\\1&\frac{1}{2}\end{pmatrix}}$$

סוף הרצאה 3 – 28/04

1.3 מיון מרחבים ריבועיים

תשלימי...

סוף הרצאה 4 – 05/05

דוגמה

1. $\mathbb{F}=\mathbb{C}$ ויהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{C}$, אז קיים בסיס $\mathcal{B}$ של V כך שמתקיים $[g_q]_{\mathcal{B}}=I_n$.
בפרט, אם $(V,q),(V',q')$ מרחבים ריבועיים לא מנוונים מעל $\mathbb{C}$ כך ש־$\dim V=\dim V'$ אז $(V,q)\cong(V',q')$.
2. $\mathbb{F}=\mathbb{R}$ יהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{R}$ כאשר $\dim V=n$ אז קיים בסיס $\mathcal{B}$ של V כך שמתקיים $[g_q]_{\mathcal{B}}=\begin{pmatrix} I_k & 0 \\ 0 & -I_{n-k}\end{pmatrix}$ כאשר $0\le k\le n$.

משפט 1.9 משפט סילבסטר

יהיו $n\in\mathbb{N}, k,\ell\in\mathbb{Z}$ כך ש־$0\le k<\ell\le n$.
נגדיר $q_1,q_2:\mathbb{R}^n\to\mathbb{R}$ על־ידי

$$q_1\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}=x_1^2+\dots+x_k^2-x_{k+1}^2-\dots-x_n^2$$

$$q_2\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}=x_1^2+\dots+x_\ell^2-x_{\ell-1}^2-\dots-x_n^2$$

אז $(\mathbb{R}^n,q_1)\ncong(\mathbb{R}^n,q_2)$.

הוכחה: נניח בשלילה שקיים איזומורפיזם $f:(\mathbb{R}^n,q_1)\to(\mathbb{R}^n,q_2)$.
נסמן ב־$U=\mathrm{Span}(\mathrm{e}_1,\dots,\mathrm{e}_\ell)$, $V=\mathrm{Span}(\mathrm{e}_{k+1},\dots,\mathrm{e}_n)$ ואת $W=f(V)$.
מתקיים ש־$\dim U=\ell$ ומכך ש־f איזומורפיזם $\dim W=\dim V=n-k$.
מכאן נובע

$$\dim(U\cap W)=\dim U+\dim W-\dim(U+W)\ge \ell+(n-k)-n=\ell-k\ge 1$$

לכן קיים $0_V\ne z\in U\cap W$.

מאחר ש־$z\in U$ נובע שקיימים $c_1,\dots,c_\ell\in\mathbb{R}$ כך שלא כולם אפס ומתקיים $z=\begin{pmatrix} c_1\\ \vdots\\ c_\ell\\ 0\\ \vdots\\ 0\end{pmatrix}$ ולכן

$$q_2(z)=c_1^2+\dots+c_\ell^2-0^2+\dots+0^2>0$$

מאחר ש־$z\in W$ נובע שקיים $0_V\ne v\in V$ כך ש־$f(v)=z$ ולכן קיימים $d_{k+1},\dots,d_n\in\mathbb{R}$ לא כולם אפס ומתקיים $v=\begin{pmatrix} 0\\ \vdots\\ 0\\ d_{k+1}\\ \vdots\\ d_n\end{pmatrix}$ ולכן

$$q_2(z)=q_2(f(v))\underset{(\star)}{=}q_1(v)=0^2+\dots+0^2-d_{k+1}^2-\dots-d_n^2<0$$

כאשר $(\star)$ נובע מכך ש־f איזומורפיזם וכמובן שהגענו לסתירה. $\square$

דוגמה

יהי $p\ne 2$ ראשוני, נסמן $\mathbb{F}=\mathbb{F}_p$ ו־$r\in\mathbb{F}_p^\times\setminus\left(\mathbb{F}_p^\times\right)^2$.
יהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{F}_p$ עם $\dim V=n$.
אז קיים בסיס $\mathcal{B}$ של V כך שמתקיים $[g_q]_{\mathcal{B}}=\begin{pmatrix} I_k & 0\\ 0 & rI_{n-k}\end{pmatrix}$ (מטריצת בלוקים).

הגדרה 1.10 תבניית מייצגת

יהי (V,q) מרחב ריבועי מעל $\mathbb{F}$ ו־$a\in\mathbb{F}$. אומרים ש־q מייצגת את a כאשר $a\in q(V\setminus\{0_V\})$.

תרגיל 1.11

יהיו $(V,q),(V',q')$ מרחבים ריבועיים כך ש־$(V,q)\cong(V',q')$. אז $q(V\setminus\{0_V\})=q'(V'\setminus\{0_V\})$.

משפט 1.12

יהי p ראשוני ויהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{F}_p$ עם $\dim V=2$. אז $\mathbb{F}_p^\times\subseteq q(V\setminus\{0\})$.

הוכחה: יהי $\mathcal{B}$ בסיס אורתוגונלי של V אז $[g_q]_{\mathcal{B}} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}$ כאשר $a_1, a_2 \in \mathbb{F}_p^\times$.
נגדיר $q' : \mathbb{F}_p^2 \to \mathbb{F}_p$ על־ידי

$$q'\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = a_1 x_1^2 + a_2 x_2^2$$

ולכן $(V, q) \cong (\mathbb{F}_p^2, q')$ כי הם מיוצגים על־ידי אותה המטריצה.
יהי $b \in \mathbb{F}_p^\times$ ונוכיח כי קיימים $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in \mathbb{F}_p^2$ כך ש־$q'\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = b$.
נסמן

$$A_1 := \{a_1 x^2 \mid x \in \mathbb{F}_p\}$$
$$A_2 := \{a_2 x^2 \mid x \in \mathbb{F}_p\}$$
$$B := \{b - a_2 x^2 \mid x \in \mathbb{F}_p\}$$

נגדיר $f : (\mathbb{F}_p^\times)^2 \cup \{0\} \to A_1$ על־ידי $f(x_1) = a_1 x$ ולכן f היא חד־חד ערכית ועל (ההופכית זה חילוק) ולכן $\left|(\mathbb{F}_p^\times)^2 \cup \{0\}\right| = |A_1| = \frac{p+1}{2}$.
באופן דומה גם $|A_2| = \frac{p+1}{2}$.
נגדיר $g : A_2 \to B$ על־ידי $g(y) = b - y$ וכמובן שגם g היא חד־חד ערכית ועל ולכן $|B| = |A_2| = \frac{p+1}{2}$ ומכאן

$$|A_1 \cap B| = |A_1| + |B| - |A_1 \cup B| \geq \frac{p+1}{2} + \frac{p+1}{2} - p = 1$$

כלומר החיתוך שלהם לא ריק ולכן קיים $c \in A_1 \cap B$ כלומר קיימים $x_1, x_2 \in \mathbb{F}_p$ כך ש־$a_1 x_1^2 = c = b - a_2 x_2^2$ ומכאן $q'\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = a_1 x_1^2 + a_2 x_2^2 = b$.
יתר על־כן, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ כי $b \neq 0$. □

הערה

זה כמובן לא נכון ב־$\mathbb{R}$ כשהדוגמה הקלאסית היא מכפלה פנימית למרות שהיא מגדירה מרחב ריבועי לא מנוון.

מסקנה 1.13

יהי (V, q) מרחב ריבועי לא מנוון מעל $\mathbb{F}_p$ עם $\dim V \geq 2$. אז $\mathbb{F}_p^\times \subseteq q(V \setminus \{0\})$.

הוכחה: נסמן $\dim V = n$ ויהי $\mathcal{B} = (v_1, ..., v_n)$ בסיס אורתוגונלי של V אז קיימים $a_1, ..., a_n \in \mathbb{F}_p^\times$ כך שמתקיים $[g_q]_{\mathcal{B}} = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$.
נסמן $\mathcal{C} = (v_1, v_2)$, $U = \operatorname{Span} \mathcal{C}$ אז $\dim U = 2$ וגם $[g_{q|_U}]_{\mathcal{C}} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}$.
לכן $(U, q|_U)$ מרחב לא מנוון ומתקיים $\mathbb{F}_p^\times \subseteq q|_U\ (U \setminus \{0_V\}) \subseteq q(V \setminus \{0\})$. □

למה 1.14

יהי (V, q) מרחב ריבועי לא מנוון ותהיי $u \in V$ כך ש־$q(u) \neq 0$. נסמן $W = \{u\}^\perp$ אז $(W, q|_W)$ הוא מרחב ריבועי לא מנוון.

הוכחה: יהי $z \in W$ בגרעין של $(W, q|_W)$ כלומר לכל $w \in W$ מתקיים $g_q(z, w) = 0$.
יהי $v \in V$, מאחר ש־$V = \operatorname{Span}(u) \oplus W$ נובע שקיימים $w \in W, c \in \mathbb{F}$ כך ש־$v = cu + w$ ומכאן

$$g_q(z, v) = c q_g(z, u) + g_q(z, w) = 0$$

כאשר $g_q(z, u) = 0$ כי $z \in w$ בגרעין ולכן $z \in V^\perp$.
מאחר ש־(V, q) לא מנוון אנו מקבלים כי $z = 0_V$ ולכן $(W, q|_W)$ לא מנוון. □

משפט 1.15

יהי $p \neq 2$ ראשוני ו־$r \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$ ויהי (V, q) מרחב ריבועי לא מנוון עם $\dim V = n$. אז קיים בסיס $\mathcal{B}$ של V כך ש־$[g_q]_{\mathcal{B}} = I_n$ או $[g_q]_{\mathcal{B}} = \begin{pmatrix} I_{n-1} & 0 \\ 0 & r \end{pmatrix}$.

הוכחה: באינדוקציה על n: עבור $n = 1$ כבר ראינו בדוגמה 1.10 ונניח כי הטענה נכונה למרחב ריבועי ממימד $n - 1$.
מאחר ש־$1 \in \mathbb{F}_p^\times \subseteq q(V \setminus \{0_V\})$ וגם $\dim V \geq 2$ קיים $u \in V$ כך ש־$q(u) = 1$.
נסמן $W = \{u\}^\perp$ אז $\dim W = n - 1$ וגם $(W, q|_W)$ לא מנוון ומהנחת האינדוקציה קיים בסיס $\mathcal{C} = (w_1, ..., w_{n-1})$ של W כך ש־$[g_{q|_W}]_{\mathcal{C}} = I_{n-1}$ או ש־$[g_{q|_W}]_{\mathcal{C}} = \begin{pmatrix} I_{n-2} & 0 \\ 0 & r \end{pmatrix}$.
נגדיר $\mathcal{B} = (u, w_1, ..., w_{n-1})$. מאחר ש־$V = \operatorname{Span}(u) \oplus W$ נובע ש־$\mathcal{B}$ הוא בסיס של V.
כמו־כן, $[g_q]_{\mathcal{B}} = I_n$ או $[g_q]_{\mathcal{B}} = \begin{pmatrix} I_{n-1} & 0 \\ 0 & r \end{pmatrix}$. □

טענה 1.16

יהי $n \in \mathbb{N}$ ונגדיר $q_1, q_2 : \mathbb{F}_p^n \to \mathbb{F}_p$ על־ידי

$$q_1\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1^2 + \cdots + x_n^2$$

$$q_2\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1^2 + \cdots + x_{n-1}^2 + rx_n^2$$

כאשר $r \in \mathbb{F}_p^\times \setminus \left(\mathbb{F}_p^\times\right)^2$ כבטענה הקודמת. אז $\left(\mathbb{F}_p^n, q_1\right) \ncong \left(\mathbb{F}_p^n, q_2\right)$.

הוכחה: נניח בשלילה שהם איזומורפיים ולכן המטריצות $\left[g_{q_1}\right]_{\mathcal{E}} = I_n$ ו־$\left[g_{q_2}\right] = \begin{pmatrix} I_{n-1} & 0 \\ 0 & r \end{pmatrix}$ חופפות כלומר קיימת $P \in M_n(\mathbb{F}_p)$ הפיכה כך שמתקיים

$$\begin{pmatrix} I_{n-1} & 0 \\ 0 & r \end{pmatrix} = P^t I_n P = P^t P$$

נסמן $\det P = c$ ו־$c \neq 0$ כי P הפיכה ונקבל

$$r = \det\begin{pmatrix} I_{n-1} & 0 \\ 0 & r \end{pmatrix} = \det(P^t P) = c^2 \in \left(\mathbb{F}_p^\times\right)^2$$

וזאת סתירה. □

מסקנה 1.17

יהיו $(V, q), (V', q')$ מרחבים ריבועיים לא מנוונים מעל $\mathbb{F}_p$ ויהיו $\mathcal{B}, \mathcal{B}'$ בסיסים של V, V' בהתאמה כך שמתקיים

1. $\dim V = \dim V'$
2. $\det\left[g_q\right]_{\mathcal{B}} \cdot \left(\mathbb{F}_p^\times\right)^2 = \det\left[g_{q'}\right]_{\mathcal{B}'} \cdot \left(\mathbb{F}_p^\times\right)^2$

אז $(V, q) \cong (V', q')$.

דוגמה

עבור $p = 7$ אז $q : \mathbb{F}_7^2 \to \mathbb{F}_7$ אז $r = -1 \notin \left(\mathbb{F}_7^\times\right)^2$ והתבנית $q\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = -x_1^2 - x_2^2$.
מהמשפט קיים בסיס $\mathcal{B}$ של $\mathbb{F}_7^2$ כך שמתקיים $\left[g_q\right]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$.

סוף הרצאה 5 – 12/05

1.4 איזוטרפיות

מוטיבציה: נסתכל על התבנית הריבועית $q : \mathbb{F}^2 \to \mathbb{F}$ הנתונה על־ידי $q\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1^2 - x_2^2$ והמרחב הריבועי עם התבנית הזאת הוא לא מנוון (המטריצה המייצגת הפיכה) אבל נניח הוקטור $q\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 0$ ותופעה כזאת נקראת איזוטרופיה והיא מעניינת.
יהי (V, q) מרחב ריבועי מעל $\mathbb{F}$ ויהי $v \in V$ נגדיר $g_q^v : V \to \mathbb{F}$ על־ידי $g_q^v(w) = g_q(v, w)$ וברור כי $g_q^v \in \mathrm{Hom}(V, \mathbb{F})$.
נגדיר $\hat{g}_q : V \to \mathrm{Hom}(V, \mathbb{F})$ על־ידי $\hat{g}_q = g_q^v$.

טענה 1.18

יהי (V, q) מרחב ריבועי מעל $\mathbb{F}$. אז (V, q) לא מנוון אם ורק אם $\hat{g}_q$ חד־חד ערכית.

הוכחה: (V, q) מנוון אם ורק אם קיים $0_V \neq v \in V^\perp$ אם ורק אם קיים $0_V \neq v \in V$ כך ש־$g_q^v \equiv 0$ אם ורק אם קיים $0_V \neq v \in V$ כך ש־$\hat{g}_q(v) = 0$ אם ורק אם $\ker \hat{g}_q \neq \{0_V\}$ אם ורק אם $\hat{g}_q$ אינה חד־חד ערכית. □

למה 1.19

V מרחב וקטורי נוצר סופית מעל $\mathbb{F}$ ו־U תת־מרחב של V.
נגדיר $\rho_U : \mathrm{Hom}(V, \mathbb{F}) \to \mathrm{Hom}(U, \mathbb{F})$ על־ידי $\rho_U(\ell) = \ell|_U$ לכל $\ell \in \mathrm{Hom}(V, \mathbb{F})$ אז ρ_U העתקה לינארית על.

תרגיל 1.20

הוכיחו את למה 1.19.

טענה 1.21

יהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{F}$ ו־U תת־מרחב של V. אז

$$\dim V = \dim U + \dim U^{\perp}$$

הוכחה: נתבונן בהעתקה הלינארית $\rho_U \circ \hat{g}_q : V \to \mathrm{Hom}(U,\mathbb{F})$ ויהי $v \in V$.
אז $v \in U^{\perp}$ אם ורק אם $g_q^v\ |_U = 0$ אם ורק אם $\varphi_U \circ \hat{g}_q = 0_V$ אם ורק אם $v \in \ker \varphi_U \circ \hat{g}_q$ ולפיכך $U^{\perp} = \ker \rho_U \circ \hat{g}_q$.
מאחר ש־(V,q) לא מנוון נובע ש־$\hat{g}_q$ חד־חד ערכית ולכן $\hat{g}_q$ היא גם על ומכאן (למה?) ש־$\rho_U \circ \hat{g}_q$ על כלומר $Im\, \rho_U \circ \hat{g}_q = \mathrm{Hom}(U,\mathbb{F})$.
לפי משפט המימדים

$$\dim V = \dim Im\, \rho_U \circ \hat{g}_q + \dim \ker \rho_U \circ \hat{g}_q + \dim \mathrm{Hom}(U,\mathbb{F}) + \dim U^{\perp} = \dim U + \dim U^{\perp}$$

□

טענה 1.22

יהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{F}$ ו־U תת־מרחב של V. אז $\left(U^{\perp}\right)^{\perp} = U$.

הוכחה: יהי $u \in U$. לכל $w \in U^{\perp}$ מתקיים ש־$u \perp w$ ולכן $u \in \left(U^{\perp}\right)^{\perp}$ ולפיכך $U \subseteq \left(U^{\perp}\right)^{\perp}$ וזה נכון בכל מרחב ריבועי.
לפי הטענה הקודמת מתקיים

$$\dim \left(U^{\perp}\right)^{\perp} = \dim V - \dim U^{\perp} = \dim V - (\dim V - \dim U) = \dim U$$

□

תרגיל 1.23

מתי ההכלה השנייה שהוכחנו לעיל לא מתקיימת?

טענה 1.24

יהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{F}$ ו־U תת־מרחב של V. אז $(U,q|_U)$ ~~לא~~ מנוון אם ורק אם $(U^{\perp},q|_{U^{\perp}})$ ~~לא~~ מנוון.

הוכחה: $\Longleftarrow$ $(U,q|_U)$ מנוון ולכן קיים $0 \neq v \in U$ כך ש־$v \perp u$ לכל $u \in U$ ולכן $v \in U^{\perp}$.
מאחר ש־$v \in U$ מתקיים ש־$v \perp w$ לכל $w \in U^{\perp}$ וזה אומר כי $(U^{\perp},q|_{U^{\perp}})$ מנוון.
$\Longrightarrow$ מכך ש־$(U^{\perp},q|_{U^{\perp}})$ מנוון נובע כי $\left(\left(U^{\perp}\right)^{\perp},q|_{(U^{\perp})^{\perp}}\right)$ גם מנוון ולפי הטענה הקודמת אנחנו מקבלים כי $(U,q|_U)$ מנוון. □

טענה 1.25

יהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{F}$ ו־U תת־מרחב של V כך ש־$(U,q|_U)$ לא מנוון אז
1. $(U^{\perp},q|_{U^{\perp}})$ לא מנוון
2. $V = U \oplus^{\perp} U$

הוכחה:
1. נובע מהטענה הקודמת
2. יהי $v \in U \cap U^{\perp}$ ונרצה להראות שהוא וקטור האפס: מאחר ש־$v \in U^{\perp}$ מתקיים ש־$v \perp u$ לכל $u \in U$ ובגלל ש־$v \in U$ נובע ש־v בגרעין של $(U,q|_U)$ אבל $(U,q|_U)$ הוא לא מנוון ולכן הגרעין שלו הוא וקטור האפס כלומר $v = 0_V$ ולכן $U \cap U^{\perp} = 0$. לסיום

$$\dim(U+U^{\perp}) = \underbrace{\dim U + \dim U^{\perp}}_{\dim V} - \underbrace{\dim(U \cap U^{\perp})}_{0} = \dim V$$

□

הגדרה 1.26 וקטור איזוטרופי

יהי (V,q) מרחב ריבועי מעל $\mathbb{F}$ ו־$0_V \neq v \in V$ אז v נקרא **איזוטרופי** אם $q(v) = 0$.

הגדרה 1.27 מרחב ריבועי איזוטרופי

מרחב ריבועי (V,q) נקרא **מרחב איזוטרופי** אם קיים $0_V \neq v \in V$ כך ש־v איזוטרופי. כלומר, $0 \in q(V \setminus \{0_V\})$.

מסקנה 1.28

כל מרחב ריבועי מנוון הוא איזוטרופי.

הגדרה 1.29

נגדיר תבנית ריבועית $h:\mathbb{F}^2\to\mathbb{F}$ על־ידי $h\begin{pmatrix}x_1\\x_2\end{pmatrix}=x_1x_2$. מרחב ריבועי $(\mathbb{F}^2,h)$ נקרא **מישור היפרבולי**.

טענה 1.30

1. $[g_h]_{\mathcal{E}}=\begin{pmatrix}0&\frac{1}{2}\\\frac{1}{2}&0\end{pmatrix}$
2. $\det[g_h]_{\mathcal{E}}=-\frac{1}{4}$ ובפרט $(\mathbb{F}^2,h)$ לא מנוון
3. h תבנית איזוטרופית ובפרט $(\mathbb{F}^2,h)$ איזוטרופי
4. $h\left(\mathbb{F}^2\setminus\left\{\begin{pmatrix}0\\0\end{pmatrix}\right\}\right)=\mathbb{F}$
5. נגדיר $q:\mathbb{F}^2\to\mathbb{F}$ על־ידי $q\begin{pmatrix}x_1\\x_2\end{pmatrix}=x_1^2-x_2^2$ אז $(\mathbb{F}^2,h)\cong(\mathbb{F}^2,q)$

הוכחה:

1. נובע מכך ש־$h\begin{pmatrix}x_1\\x_2\end{pmatrix}=x_1x_2=\frac{1}{2}x_1x_2+\frac{1}{2}x_2x_1$
2. הגדרה
3. $h\begin{pmatrix}1\\0\end{pmatrix}=0$
4. לכל $c\in\mathbb{F}$ מתקיים $h\begin{pmatrix}1\\c\end{pmatrix}=c$
5. עם הפיפת מטריצות ישירה

$$\begin{pmatrix}1&1\\-1&1\end{pmatrix}\begin{pmatrix}0&1/2\\1/2&0\end{pmatrix}\begin{pmatrix}1&-1\\1&1\end{pmatrix}=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

□

טענה 1.31

יהי (V,q) מרחב ריבועי לא מנוון ואיזוטרופי מעל $\mathbb{F}$. אז קיים תת־מרחב U של V כך ש־$(U,q|_U)\cong(\mathbb{F}^2,h)$.

הוכחה: מאחר ש־(V,q) איזוטרופי קיים $0_V\neq v\in V$ כך ש־$q(v)=0$ ומאחר ש־(V,q) לא מנוון קיים $w\in V$ כך ש־$g_q(v,w)\neq 0$.
נסמן $b=g_q(v,w)$ ונגדיר $w'=\frac{1}{2b}$ ונקבל $g_q(v,w')=\frac{1}{2b}g_q(v,w)=\frac{1}{2}$.
לכל $c\in\mathbb{F}$ מתקיים

$$q(w'+cv)=g_q(w'+cv,w'+cv)=g_q(w',w')+2g_q(w',cv)=g(w')+2c\underbrace{g_q(w',v)}_{=\frac{1}{2}}=g(w')+c$$

אז נגדיר $c=-g(w')$ ו־$u=w'-q(w')v$ אז $g(u)=0$.
בנוסף מתקיים

$$g_q(v,u)=g_q(v,w'cv)=g_q(v,w')=\frac{1}{2}$$

עכשיו $\mathcal{B}=(v,u)$ היא סדרה בלתי־תלויה לינארית (כי אחרת היינו מקבלים ש־$g_q(v,u)=0$) ונגדיר $U=\mathrm{Span}(U)$.
אז $\mathcal{B}$ בסיס של U ומתקיים

$$[g_q|_U]=\begin{pmatrix}0&1/2\\1/2&0\end{pmatrix}$$

ולכן $(U,q|_U)\cong(\mathbb{F}^2,h)$ □

מסקנה 1.32

יהי (V,q) מרחב ריבועי לא מנוון ואיזוטרופי מעל $\mathbb{F}$ כך ש־$\dim V=2$. אז $(V,q)\cong(\mathbb{F}^2,h)$.

מסקנה 1.33

יהי (V,q) מרחב ריבועי לא מנוון ואיזוטרופי מעל $\mathbb{F}$. אז $q(V\setminus\{0_V\})=\mathbb{F}$.

משפט 1.34

יהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{F}$. אז קיים $m\in\mathbb{N}\cup\{0\}$ ותתי־מרחבים $U_1,...,U_m,W$ של V כך שמתקיים

1. $V=U_1\oplus^{\perp}...\oplus^{\perp}U_m\oplus^{\perp}W$
2. לכל $i\leq m$ מתקיים $\left(U_i,q|_{U_i}\right)\cong(\mathbb{F}^2,h)$ ו־$(W,q|_W)$ אינו איזוטרופי

הוכחה: מתקבלת באינדוקציה על מימד V בשימוש עם הטענה הקודמת ובטענה 1.25 □

הגדרה 1.35 מרחב אנאיזוטרופי

מרחב ריבועי (V,q) שאינו איזוטרופי נקרא אנאיזוטרופי.

הערה

מרחב ריבועי $(\{0_V\},Q)$ היינו אנאיזוטרופי.

טענה 1.36

יהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{F}$ כך ש־$\dim V=1$ אז (V,q) אנאיזוטרופי.

הוכחה: כי אם הוא לא מנוון, יש לו בסיס מוקטור אחד שביחס אליו המטריצה היא מטריצה 1×1 שצריכה להיות הפיכה כלומר יש לה ערך אחד שאינו אפס אז כל וקטור הוא סקלר של וקטור הבסיס ששונה מאפס והטענה נובעת. □

טענה 1.37

יהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{F}$ כך ש־$\dim V=2$ ו־$\mathcal{B}$ הוא בסיס של V. אז (V,q) איזוטרופי אם ורק אם $-\det\left[g_q\right]_{\mathcal{B}}\in(\mathbb{F}^\times)^2$.

הוכחה: $\Longleftarrow$ נניח שהמרחב הוא איזוטרופי ולכן קיים $0_V\neq v\in V$ כך ש־$q(v)=0$.
מאחר ש־(V,q) לא מנוון קיים $w\in V$ כך ש־$g_q(v,w)\neq 0$ ולכן $\mathcal{C}=(v,w)$ בלתי־תלויים לינארית כי אחרת היינו מקבלים ש־$g_q(v,w)=0$.
נסמן $g_q(v,w)=b$ ו־$g_q(w,w)=q(w)=c$ אז

$$\left[g_q\right]_{\mathcal{C}}=\begin{pmatrix}0&b\\b&c\end{pmatrix}$$

מאחר ש־$\left[g_q\right]_{\mathcal{C}}$ ו־$\left[g_q\right]_{\mathcal{B}}$ חופפות קיימת מטריצה P הפיכה עבורה מתקיים

$$\left[g_q\right]_{\mathcal{B}}=P^t\left[g_q\right]_{\mathcal{C}}P$$

ולכן

$$-\det\left[g_q\right]_{\mathcal{B}}=-\det P^t\det\left[g_q\right]_{\mathcal{C}}\det P=-(\det P)^2\det\left[g_q\right]_{\mathcal{C}}=-(\det P^2)(-b^2)=(b\det P)^2\in(\mathbb{F}^\times)^2$$

$\Longrightarrow$ יהי $\mathcal{C}=(v_1,v_2)$ בסיס אורתוגונלי של V אז קיימים $a_1,a_2\in\mathbb{F}^\times$ עבורם

$$\left[g_q\right]_{\mathcal{C}}=\begin{pmatrix}a_1&0\\0&a_2\end{pmatrix}$$

קיימת P הפיכה עבורה מתקיים

$$\left[g_q\right]_{\mathcal{C}}=P^t\left[g_q\right]_{\mathcal{B}}P$$

מאחר ש־$-\det\left[g_q\right]_{\mathcal{B}}\in(\mathbb{F}^\times)^2$ קיים $k\in\mathbb{F}^\times$ כך ש־$\det\left[g_q\right]_{\mathcal{B}}=-k^2$.
אז

$$a_1a_2=\det\begin{pmatrix}a_1&0\\0&a_2\end{pmatrix}=\det\left[g_q\right]_{\mathcal{C}}=\det P^t\det\left[g_q\right]_{\mathcal{B}}\det P=-(k\det P)^2$$

נגדיר $v=k\det Pv_1+a_1v_2$ מאחר ש־$a_1\neq 0$ מתקיים $v\neq 0_V$ ולכן

$$\begin{aligned}q(v)&=q(k\det Pv_1+a_1v_2)\\&=q(k\det Pv_1)+g(a_1v_2)\\&=(k\det P)^2q(v_1)+a_1^2q(v_2)\\&=(k\det P)^2a_1+a_1^2a_2\\&=a_1\left(\underbrace{(k\det P)^2}_{=-a_1a_2}+a_1a_2\right)\\&=0\end{aligned}$$

□

דוגמה

1. $\mathbb{F}=\mathbb{C}$ מעל המרוכבים כל מספר הוא ריבוע כלשהו.
נבחין שאם (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{C}$ עם $\dim V\geq 2$, אז קיים תת־מרחב U של V כך ש־$(U,q|_U)$ לא מנוון וגם $\dim U=2$.
לפיכך, כל מרחב ריבועי אנאיזוטרופי לא טריוויאלי מעל $\mathbb{C}$ איזומורפי ל־$(\mathbb{C},q)$ כאשר $q:\mathbb{C}\to\mathbb{C}$ מוגדר על־ידי $g(x)=x^2$
2. $\mathbb{F}=\mathbb{R}$ כל מרחב ריבועי אנאיזוטרופי לא טריוויאלי מעל $\mathbb{R}$ איזומורפי לאחד מהמרחבים הבאים
   1. $(\mathbb{R}^n,q_1)$ כאשר $q_1\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\sum_{i=1}^n x_i^2$
   2. $(\mathbb{R}^n,q_{-1})$ כאשר $q_{-1}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\sum_{i=1}^n -x_i^2$
3. $\mathbb{F}=\mathbb{F}_p$ כאשר $p\neq 2$ ראשוני
   1. יהי $p\neq 2$ ראשוני כך ש־$-1\notin\left(\mathbb{F}_p^\times\right)^2$. אז כל מרחב אנאיזוטרופי לא טריוויאלי מעל $\mathbb{F}_p$ איזומורפי לאחד מהמרחבים הבאים
      1. $(\mathbb{F}_p,q_1)$ כאשר $q_1:\mathbb{F}_p\to\mathbb{F}_p$ מוגדר על־ידי $q_1(x)=x^2$
      2. $(\mathbb{F}_p,q_{-1})$ כאשר $q_{-1}:\mathbb{F}_p\to\mathbb{F}_p$ מוגדר על־ידי $g_{-1}(x)=-x^2$
      3. $(\mathbb{F}_p^2,q_{1,1})$ כאשר $q_{1,1}:\mathbb{F}_p^2\to\mathbb{F}_p$ מוגדר על־ידי $q_{1,1}\left(\begin{smallmatrix}x_1\\ x_2\end{smallmatrix}\right)=x_1^2+x_2^2$

      כאשר השניים הראשונים ממימד 1 והאחרון ממימד 2.
   2. יהי $p\neq 2$ ראשוני כך ש־$-1\in\left(\mathbb{F}_p^\times\right)^2$ ויהי $r\in\mathbb{F}_p^\times\setminus\left(\mathbb{F}_p^\times\right)^2$.
   אז כל מרחב אנאיזוטרופי לא טריוויאלי מעל $\mathbb{F}_p$ איזומורפי לאחד מהמרחבים הבאים
      1. $(\mathbb{F}_p,q_1)$ כמקודם $q_1(x)=x^2$
      2. $(\mathbb{F}_p,q_r)$ כאשר $q_r:\mathbb{F}_p\to\mathbb{F}_p$ מוגדרת על־ידי $q_r(x)=rx^2$
      3. $(\mathbb{F}_p,q_{1,r})$ כאשר $q_{1,r}:\mathbb{F}_p^2\to\mathbb{F}_p$ מוגדרת על־ידי $q_{1,r}\left(\begin{smallmatrix}x_1\\ x_2\end{smallmatrix}\right)=x_1^2+rx_2^2$

טענה 1.38

יהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{F}_p$ כך ש־$\dim V\geq 3$. אז (V,q) איזוטרופי.

הוכחה: קיים בסיס אורתוגונלי $\mathcal{B}=(v_1,...,v_n)$ של V כלומר קיימים $a_1,...,a_n\in\mathbb{F}_p^\times$ כך שמתקיים

$$[g_q]_{\mathcal{B}}=\begin{pmatrix}a_1 & & 0\\ & \ddots & \\ 0 & & a_n\end{pmatrix}$$

נגדיר תבנית ריבועית $g':\mathbb{F}_p^2\to\mathbb{F}_p$ על־ידי $g'\left(\begin{smallmatrix}x_1\\ x_2\end{smallmatrix}\right)=a_1x_1^2+a_2x_2^2$ ולכן

$$[g_{q'}]_{\mathcal{E}}=\begin{pmatrix}a_1 & 0\\ 0 & a_2\end{pmatrix}$$

ולכן $\left(\mathbb{F}_p^2,q'\right)$ לא מנוון ולכן קיים $(x)1,x_2)\in\mathbb{F}_p^2$ כך ש־$a_1x_1^2+a_2x_2^2=g'\left(\begin{smallmatrix}x_1\\ x_2\end{smallmatrix}\right)=-a_3$.
נגדיר $v=x_1v_1+x_2v_2+v_3$ וברור ש־$v\neq 0$. בנוסף

$$q(v)=q(x_1v_1)+q(x_2v_2)+q(v_3)=x_1^2q(v_1)+x_2^2q(v_2)+q(v_3)=a_1x_1^2+a_2x_2^2+a_3=-a_3+a_3=0$$

$\square$

2 מספרים p־אדיים

2.1 שדות נורמיים

הגדרה 2.1 נורמה

יהי F שדה ממציין כלשהו. פונקציה $\|\cdot\| : \mathbb{F} \to \mathbb{R}^+ = \{x \in \mathbb{R} \mid x \geq 0\}$ נקראת **נורמה** כאשר

1. $\|a\| = 0$ אם ורק אם $a = 0$
2. $\|ab\| = \|a\|\|b\|$ לכל $a, b \in \mathbb{F}$
3. $\|a + b\| \leq \|a\| + \|b\|$ לכל $a, b \in \mathbb{F}$

טענה 2.2 תכונות הנורמה

תהיי $\|\cdot\| : \mathbb{F} \to \mathbb{R}^+$ נורמה אז

1. $\|1\| = \|-1\| = 1$
2. $\|a^n\| = \|a\|^n$ לכל $a \in \mathbb{F}$
3. $\left\|\frac{a}{b}\right\| = \frac{\|a\|}{\|b\|}$ לכל $a, b \in \mathbb{F}$ עם $b \neq 0$
4. $\|a - b\| \geq \|a\| - \|b\|$
5. $\|n\| \leq n$ לכל $n \in \mathbb{N}$

הוכחה: כולן נובעות ישירות מהגדרה (תרגיל). □

דוגמה

1. $\mathbb{F}$ שדה ו־$\|\cdot\| : \mathbb{F} \to \mathbb{R}^+$ מוגדרת על־ידי $\|0\| = 0, \|a\| = 1$ לכל $a \in \mathbb{F}^\times$
2. $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ו־$\|\cdot\| : \mathbb{F} \to \mathbb{R}^+$ המוגדרת על־ידי $\|a\| = |a|$ לכל $a \in \mathbb{F}$

הגדרה 2.3 שדה נורמי

לזוג $(\mathbb{F}, \|\cdot\|)$ כאשר $\mathbb{F}$ שדה ו־$\|\cdot\|$ נורמה קוראים **שדה נורמי**.

הגדרה 2.4 מטריקה

יהי $(\mathbb{F}, \|\cdot\|)$ שדה נורמי. נגדיר $d : \mathbb{F} \times \mathbb{F} \to \mathbb{R}$ על־ידי $d(a, b) = \|a - b\|$ ו־d היא פונקציית מרחק על $\mathbb{F}$ כלומר $(\mathbb{F}, d)$ הוא מרחב מטרי.

הגדרה 2.5 שדה ארכימדי

שדה נורמי $(\mathbb{F}, \|\cdot\|)$ נקרא **ארכימדי** כאשר לכל $a \in \mathbb{F}$ קיים $n \in \mathbb{N}$ כך ש־$\|n\| > \|a\|$.

טענה 2.6

יהי $(\mathbb{F}, \|\cdot\|)$ שדה נורמי. אז $(\mathbb{F}, \|\cdot\|)$ ארכימדי אם ורק אם קיים $n \in \mathbb{N}$ כך ש־$\|n\| > 1$.

הוכחה: $\Longleftarrow$ עבור $a = 1$ קיים $n \in \mathbb{N}$ כך ש־$\|n\| > \|1\| = 1$.
$\Longrightarrow$ יהי $a \in \mathbb{F}$ מאחר ש־$\|n\| > 1$ נובע שקיים $N \in \mathbb{N}$ כך ש־$\|n\|^N > \|a\|$ (לדוגמה $N = \left\lfloor \log_{\|n\|}(\|a\|) \right\rfloor + 1$). אז $\left\|n^N\right\| = \|n\|^N > \|a\|$. □

דוגמה

בהמשך לדוגמה 2.3, הנורמה הראשונה לא ארכימדית בעוד הנורמה השנייה כן ארכימדית.

טענה 2.7

יהי $(\mathbb{F}, \|\cdot\|)$ שדה נורמי. אז $(\mathbb{F}, \|\cdot\|)$ לא ארכימדי אם ורק אם לכל $a, b \in \mathbb{F}$ מתקיים $\|a + b\| \leq \max(\|a\|, \|b\|)$ (אי־שיוויון האולטרה מטרי).

הוכחה: $\Longleftarrow$ נניח שהוא לא ארכימדי ויהיו $a, b \in \mathbb{F}$ ובלי הגבלת הכלליות נניח $\|a\| \geq \|b\|$. מתקיים

$$\|a + b\|^n = \|(a + b)^n\| = \left\|\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right\| \leq \sum_{k=0}^{n} \left\|\binom{n}{k} a^k b^{n-k}\right\| = \sum_{k=0}^{n} \left\|\binom{n}{k}\right\| \|a\|^k \|b\|^{n-k} \underset{(\star)}{\leq} \sum_{k=0}^{n} \|a\|^k \|b\|^{n-k} \leq \sum_{k=0}^{n} \|a\|^k \|a\|^{n-k}$$
$$= \sum_{k=0}^{n} \|a\|^n = (n + 1)\|a\|^n$$

כאשר $(\star)$ נובע מהיות השדה לא ארכימדי ועם טענה 2.6.
מכאן ש־$\|a\|\|a+b\|^n \leq \sqrt[n]{n+1}\|a+b\|^n$ ומאחר ש־$\lim_{n\to\infty} \sqrt[n]{n+1} = 1$, נסיק כי $\|a+b\| \leq \|a\| = \max(\|a\|, \|b\|)$.
$\Longrightarrow$ לכל $n \in \mathbb{N}$ מתקיים $\|n\| = \left\|\sum_{i=1}^{n} 1\right\| \leq \max(\|1\|, ..., \|1\|) = 1$ ולכן $(\mathbb{F}, \|\cdot\|)$ לא ארכימדי. □

טענה 2.8

יהי $(\mathbb{F}, \|\cdot\|)$ שדה נורמי לא ארכימדי ויהיו $a, b \in \mathbb{F}$ כך ש־$\|a\| \neq \|b\|$ אז $\|a+b\| = \max(\|a\|, \|b\|)$.

הוכחה: בלי הגבלת הכלליות $\|b\| < \|a\|$ ונניח בשלילה כי $\|a+b\| < \max(\|a\|, \|b\|) = \|a\|$ ולכן

$$\|a\| > \max(\|a+b\|, \|b\|) = \max(\|a+b\|, \|-b\|) \underset{\text{אי־שיוויון האולטרה מטרי}}{\geq} \max(\|a+b\| + (-b)) = \|a\|$$

וזאת סתירה ולכן $\|a+b\| = \max(\|a\|, \|b\|)$. □

טענה 2.9

יהי $(\mathbb{F}, \|\cdot\|)$ שדה נורמי לא ארכימדי ויהיו $a, b, c \in \mathbb{F}$. אז בין המספרים $\|a-b\|, \|b-c\|, \|a-c\|$ יש שניים ששווים זה לזה.

הוכחה: בלי הגבלת הכלליות $\max(\|a-b\|, \|b-c\|, \|a-c\|) = \|a-c\|$ ונניח בשלילה כי הם כולם שונים זה מזה ומהנחת השלילה נקבל

$$\|a-c\| = \|(a-b)+(b-c)\| \underset{\text{אי־שיוויון האולטרה מטרי}}{\leq} \max(\|a-b\|, \|b-c\|) < \|a-c\|$$

וזאת סתירה ולכן מתוכם יש שניים ששווים זה לזה (ובעצם הוא יהיה שווה למקסימום). □

סוף הרצאה 7 – 26/05

טענה 2.10

יהי $(\mathbb{F}, \|\cdot\|)$ לא ארכימדי ונגדיר

$$\mathcal{O}_{\|\cdot\|} := \{x \in \mathbb{F} \mid \|x\| \leq 1\}$$
$$\mathcal{M}_{\|\cdot\|} := \{x \in \mathbb{F} \mid \|x\| < 1\}$$
$$\mathcal{O} \setminus \mathcal{M} = \mathcal{U}_{\|\cdot\|} := \{x \in \mathbb{F} \mid \|x\| = 1\}$$

אז
1. $\mathcal{O}_{\|\cdot\|}$ הוא חוג קומוטטיבי עם יחידה
2. $\mathcal{O}_{\|\cdot\|}^{\times} = \mathcal{U}_{\|\cdot\|}$
3. $\mathcal{M}_{\|\cdot\|}$ אידיאל מקסימלי יחיד ב־$\mathcal{O}_{\|\cdot\|}$

הוכחה:
1. נוכיח כי $\mathcal{O}_{\|\cdot\|}$ סגורה ביחס לחיבור וכפל וכי $-1, 1 \in \mathcal{O}_{\|\cdot\|}$.
יהיו $x, y \in \mathcal{O}_{\|\cdot\|}$ ולכן $\|x\|, \|y\| \leq 1$ ומכאן $\|xy\| = \|x\|\|y\| \leq 1$ ואי־שיוויון המשולש האולטרה מטרי מניב לנו $\|x+y\| \leq \max(\|x\|, \|y\|) \leq 1$.
לכן קיבלנו סגירות לכפל ולחיבור ונשים לב ש־$\|-1\| = \|1\| = 1$ ולכן גם $-1, 1 \in \mathcal{O}_{\|\cdot\|}$.
2. יהי $x \in \mathcal{O}_{\|\cdot\|}$ כלומר $\|x\| \leq 1$. אז

$$x \in \mathcal{O}_{\|\cdot\|}^{\times} \iff \frac{1}{x} \in \mathcal{O}_{\|\cdot\|}^{\times} \iff \left\|\frac{1}{x}\right\| \leq 1 \iff \frac{1}{\|x\|} \leq 1 \iff 1 \leq \|x\| \iff \|x\| = 1 \iff x \in \mathcal{U}_{\|\cdot\|}$$

3. יהיו $x, y \in \mathcal{M}_{\|\cdot\|}$. אז $\|x\|, \|y\| < 1$ ולכן מאי־שיוויון האולטרה מטרי $\|x+y\| \leq \max(\|x\|, \|y\|) < 1$ ומכאן $x+y \in \mathcal{M}_{\|\cdot\|}$, כלומר $\mathcal{M}_{\|\cdot\|}$ סגור לחיבור.
יהיו $x \in \mathcal{M}_{\|\cdot\|}, y \in \mathcal{O}_{\|\cdot\|}$ אז $\|x\| < 1$, $\|y\| \leq 1$. מכאן ש־$\|xy\| = \|x\|\|y\| < 1$ ומכאן $xy \in \mathcal{M}_{\|\cdot\|}$ וזה בידיוק אומר ש־$\mathcal{M}_{\|\cdot\|}$ אידיאל.
יהי I אידיאל ב־$\mathcal{O}_{\|\cdot\|}$ כך ש־$\mathcal{M} \subseteq I$ ו־$I \neq \mathcal{M}$. אז קיים $x \in I \setminus \mathcal{M}_{\|\cdot\|} \subseteq \mathcal{O}_{\|\cdot\|} \setminus \mathcal{M}_{\|\cdot\|} = \mathcal{U}_{\|\cdot\|} \in \mathcal{O}_{\|\cdot\|}^{\times}$.
אז $\frac{1}{x} \in \mathcal{O}_{\|\cdot\|}$ ולכן $1 = \frac{1}{x} \cdot x \in I$ וזאת סתירה, לכן $\mathcal{M}_{\|\cdot\|}$ אידיאל מקסימלי.
נוכיח כי כל אידיאל של $\mathcal{O}_{\|\cdot\|}$ מוכל ב־$\mathcal{M}_{\|\cdot\|}$: יהי I אידיאל ב־$\mathcal{O}_{\|\cdot\|}$ ונניח בשלילה ש־$I \not\subseteq \mathcal{M}$ כלומר קיים $x \in I \setminus \mathcal{M}_{\|\cdot\|} \subseteq \mathcal{O}_{\|\cdot\|}^{\times}$ ולכן $\frac{1}{x} \in \mathcal{O}_{\|\cdot\|}$ ולכן $1 = \frac{1}{x} \cdot x \in I$ וזאת סתירה ולכן $I \subseteq \mathcal{M}_{\|\cdot\|}$ וקיבלנו ש־$\mathcal{M}_{\|\cdot\|}$ הוא אידיאל מקסימלי יחיד.

□

הערה

$\mathcal{U}_{\|\cdot\|}$ זה כל האיברים ההפיכים.

הגדרה 2.11 שדה שאריות

יהי $(\mathbb{F}, \|\cdot\|)$ שדה נורמי לא ארכימדי. השדה $\overline{\mathbb{F}}_{\|\cdot\|}$ נקרא **שדה השאריות** של $(\mathbb{F}, \|\cdot\|)$.

הגדרה 2.12 **הערכה p־אדית**

יהי p ראשוני, נגדיר $v_p : \mathbb{Z} \to \mathbb{N} \cup \{0\} \cup \{\infty\}$ על־ידי

$$v_p(a) = \max\{k \in \mathbb{N} \cup \{0\} \cup \{\infty\} \mid p^k \mid a\}$$

טענה 2.13 **תכונות ההערכה ה־p־אדית**

1. $v_p(a) = \infty$ אם ורק אם $a = 0$
2. $v_p(ab) = v_p(a) + v_p(b)$ לכל $a, b \in \mathbb{Z}$
3. $v_p(a+b) \geq \min\big(v_p(a), v_p(b)\big)$

הערה

יהיו $a \in \mathbb{Z} \setminus \{0\}$, $s \in \mathbb{N} \cup \{0\}$. אז $v_p(a) = s$ אם ורק אם קיים $u \in \mathbb{Z} \setminus \{0\}$ כך ש־$a = p^s u$ וגם $p \nmid u$.

הוכחה של טענה 2.13:

1. ישירות מהגדרה
2. אם $a = 0$ או $b = 0$ השיוויון ברור. אחרת, נסמן $t = v_p(b)$ ו־$s = v_p(a)$ ולכן קיימים $u, v \in \mathbb{Z} \setminus \{0\}$ כך ש־$p \nmid u, p \nmid v$ ואז $a = p^s u$ ו־$b = p^t v$. מכאן
$$ab = p^s u \cdot p^t v = p^{s+t} uv$$
אבל $p \nmid u$ וגם $p \nmid v$ ולכן גם $p \nmid uv$. מכאן $v_p(ab) = s + t = v_p(a) + v_p(b)$
3. אם $a = 0$ או $b = 0$ האי־שיוויון ברור.
אחרת, נסמן $t = v_p(b), s = v_p(a)$. אז קיימים $u, v \in \mathbb{Z}$ כך ש־$p \nmid u, p \nmid v$ וגם $a = p^s u, b = p^t v$.
בלי הגבלת הכלליות, $v_p(a) \leq v_p(b)$ כלומר $s \leq t$. אז
$$a + b = p^s u + p^t v = p^s(u + p^{t-s} v)$$
מכאן נובע ש־$p^s \mid a + b$ ולכן $v_p(a+b) \geq s = \min(s,t) = \min\big(v_p(a), v_p(b)\big)$.

□

הגדרה 2.14 **הרחבת ההערכה ה־p־אדית לרציונליים**

נגדיר $\tilde{v}_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ עבור $m \in \mathbb{Z}, n \in \mathbb{N}$ על־ידי

$$\tilde{v}_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n)$$

הערה

$\tilde{v}_p$ מוגדרת היטב ולא תלוי בהצגה של $q \in \mathbb{Q}$ כשבר: אם $m, m' \in \mathbb{Z}, n, n' \in \mathbb{N}$ כך ש־$\frac{m}{n} = \frac{m'}{n'}$ אז $m'n = n'm$ ולכן
$$v_p(m') + v_p(n) = v_p(m'n) = v_p(n'm) = v_p(n') + v_p(m)$$
ולכן $v_p(m') - v_p(n') = v_p(m) - v_p(n)$.

טענה 2.15 **תכונות של $\tilde{v}_p$**

1. $\tilde{v}_p(x) = \infty$ אם ורק אם $x = 0$
2. $\tilde{v}_p(xy) = \tilde{v}_p(x) + \tilde{v}_p(y)$ לכל $x, y \in \mathbb{Q}$
3. $\tilde{v}_p(x+y) \geq \min\big(\tilde{v}_p(x), \tilde{v}_p(y)\big)$ לכל $x, y \in \mathbb{Q}$

הוכחה: תרגיל. □

הגדרה 2.16 **נורמה p־אדית**

יהי $\alpha \in \mathbb{R}$ כך ש־$0 < \alpha < 1$. נגדיר $|\cdot|_{p,\alpha} : \mathbb{Q} \to \mathbb{R}^+$ על־ידי

$$|x|_{p,\alpha} = \alpha^{\tilde{v}_p(x)}$$

טענה 2.17

$\big(\mathbb{Q}, |\cdot|_{p,\alpha}\big)$ הוא שדה נורמי לא ארכימדי.

הוכחה:

1. $|x|_{p,\alpha} = 0$ אם ורק אם $\tilde{v}_p(x) = \infty$ וזה קורה אם ורק אם $x = 0$
2. $|xy|_{p,\alpha} = \alpha^{\tilde{v}_p(xy)} = \alpha^{\tilde{v}_p(x)}\alpha^{\tilde{v}_p(y)} = |x|_{p,\alpha}|y|_{p,\alpha}$
3. $|x+y|_{p,\alpha} = \alpha^{\tilde{v}_p(x+y)} \leq \alpha^{\min(\tilde{v}_p(x),\tilde{v}_p(y))} = \max\left(\alpha^{\tilde{v}_p(x)}, \alpha^{\tilde{v}_p(y)}\right) = \max\left(|x|_{p,\alpha}, |y|_{p,\alpha}\right)$

□

הגדרה 2.18

$$\mathcal{O}_{|\cdot|_{p,\alpha}} := \left\{x \in \mathbb{Q} \mid |x|_{p,\alpha} \leq 1\right\} = \left\{x \in \mathbb{Q} \mid \tilde{v}_p(x) \geq 0\right\} = \left\{\frac{m}{n} \in \mathbb{Q} \mid m \in \mathbb{Z}, n \in \mathbb{N}, p \nmid n\right\}$$

בפרט $\mathcal{O}_{|\cdot|_{p,\alpha}}$ לא תלוי ב־α ונסמן $\mathbb{Z}_{(p)} = \mathcal{O}_{|\cdot|_{p,\alpha}}$.

טענה 2.19

ב־$\left(\mathbb{Q}, |\cdot|_{p,\alpha}\right)$ מתקיים ש־$\overline{\mathbb{Z}} = \mathbb{Z}_{(p)}$.

הוכחה:

$\overline{\mathbb{Z}} \subseteq \mathbb{Z}_{(p)}$: נובע מההגדרה של $\mathbb{Z}_{(p)}$ ש־$\mathbb{Z}_{(p)}$ קבוצה סגורה (כי זה כדור סגור) ו־$\mathbb{Z} \subseteq \mathbb{Z}_{(p)}$ כי כל מספר שלם אפשר לכתוב כמספר רציונלי עם מכנה 1 ולפיכך $\overline{\mathbb{Z}} \subseteq \mathbb{Z}_{(p)}$.
$\overline{\mathbb{Z}} \supseteq \mathbb{Z}_{(p)}$: יהי $x \in \mathbb{Z}_{(p)}$ כלומר $z = \frac{m}{n} \in \mathbb{Q}$ כך ש־$m \in \mathbb{Z}, n \in \mathbb{N}$ ו־$p \nmid n$.
יהי $\varepsilon > 0$ ונוכיח כי קיים $z \in \mathbb{Z}$ כך ש־$|z - x|_{p,\alpha} < \varepsilon$.
קיים $N \in \mathbb{N}$ כך ש־$\alpha^N < \varepsilon$ (לדוגמה $N = \lfloor \log_\alpha(\varepsilon) \rfloor + 1$).
מאחר ש־$\gcd(n, p^N) = 1$ נובע שקיימים $s, t \in \mathbb{Z}$ כך ש־$sp^N + tn = 1$ (מאלגוריתם אוקלידס).
מכאן $msp^N + mtn = m$ ולכאן $msp^N = m - mtn$ אבל $p^N \mid msp^N$ נגדיר $z = mt$ ונראה שהוא מקיים את הנדרש:

$$N \leq v_p(m - mtn) = v_p(m - zn)$$

לכן

$$N \leq \tilde{v}_p(m - zn) - \underbrace{\tilde{v}_p(n)}_{=0} = \tilde{v}_p\left(\frac{m - zn}{n}\right) = \tilde{v}_p(x - z)$$

ומכאן

$$\varepsilon > \alpha^N \geq \alpha^{\tilde{v}_p(x-z)} = |x - z|_{p,\alpha} = |z - x|_{p,\alpha}$$

לפיכך $x \in \overline{\mathbb{Z}}$ כלומר $\mathbb{Z}_{(p)} \subseteq \overline{\mathbb{Z}}$. □

הגדרה 2.20

$$\mathcal{M}_{|\cdot|_{p,\alpha}} = \left\{x \in \mathbb{Q} \mid |x|_{p,\alpha} < 1\right\} = \left\{x \in \mathbb{Q} \mid \tilde{v}_p(x) > 0\right\} = \left\{\frac{m}{n} \in \mathbb{Q} \mid m \in \mathbb{Z}, n \in \mathbb{N}, p \mid m, p \nmid n\right\}$$

טענה 2.21

1. $\mathcal{M}_{|\cdot|_{p,\alpha}} = p\mathbb{Z}_{(p)}$
2. $\mathcal{M}_{|\cdot|_{p,\alpha}} \cap \mathbb{Z} = p\mathbb{Z}_{(p)} \cap \mathbb{Z} = p\mathbb{Z}$

הוכחה: תרגיל. □

טענה 2.22

$$\overline{\mathbb{F}}_{|\cdot|_{p,\alpha}} = \mathcal{O}_{|\cdot|_{p,\alpha}} / \mathcal{M}_{|\cdot|_{p,\alpha}} = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{F}_p$$

הוכחה: לכל $x \in \mathbb{Z}_{(p)}$ קיים $z \in \mathbb{Z}$ כך ש־$|x - z|_{p,\alpha} < 1$ כלומר $x - z \in \mathcal{M}_{|\cdot|_{p,\alpha}}$.
נגדיר $\pi : \mathbb{Z}_{(p)} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ על־ידי $\pi(x) = z + p\mathbb{Z}$.
אם $z' \in \mathbb{Z}$ כך ש־$|x - z'|_{p,\alpha} < 1$ אז $x - z' \in p\mathbb{Z}_{(p)}$ ולכן $z' - z \in \mathbb{Z}$ וגם $z' - z \in p\mathbb{Z}_{(p)}$ ולכן $z' - z = p\mathbb{Z}$ כלומר $\pi(x)$ לא תלוי בבחירה של z.
קל לוודא כי π הוא הומומורפיזם של חוגים שהוא על וגם ש־$\ker \pi = p^{\mathbb{Z}_{(p)}}$ ולפיכך $\mathbb{Z}_p/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}_p = \mathbb{F}_p$ ממשפטי האיזומורפיזם. □

סוף הרצאה 8 – 02/06

משפט 2.23 משפט אוסטרובסקי

תהיי $\|\cdot\| : \mathbb{Q} \to \mathbb{R}_+$ נורמה לא ארכימדית ולא טריוויאלית. אז קיימים p ראשוני ו־$\alpha \in \mathbb{R}$ כך ש־$0 < \alpha < 1$ כך ש־$\|\cdot\| = |\cdot|_{p,\alpha}$.

הוכחה: מאחר ש־$\|\cdot\|$ לא ארכימדית, לכל $n \in \mathbb{N}$ מתקיים $\|n\| \leq 1$. מאחר ש־$\|\cdot\|$ לא טריוויאלית, קיים $n \in \mathbb{N}$ כך ש־$\|n\| < 1$.
נגדיר $p := \min\{n \in \mathbb{N} \mid |n| < 1\}$ ונראה ש־p ראשוני (ברור שהוא לא 1). נניח בשלילה כי p פריק ולכן קיימים $a, b \in \mathbb{N}$ כך ש־$a, b < p$ ו־$p = ab$.
מאחר ש־$a, b < p$ מתקיים ש־$\|a\| = \|b\| = 1$ ולכן מכפליות הנורמה $\|p\| = \|ab\| = \|a\|\|b\| = 1$ וזו סתירה לכך ש־$\|p\| < 1$ ולפיכך p ראשוני.
יהי $u \in \mathbb{N}$ כך ש־$p \nmid u$ אז קיימים $q \in \mathbb{N} \cup \{0\}, r \in \mathbb{N}$ כך ש־$u = qp + r$ ו־$r < p$.
מתקיים ש־$\|r\| = 1$ וכמו כן $\|q\| \leq 1$ ולכן $\|qp\| = \|q\|\|p\| < 1$. מאחר ש־$\|pq\| \neq \|r\|$ מתקיים ש־$\|u\| = \|qp + r\| = \max(\|qp\|, \|r\|) = \|r\| = 1$.
יהי $v \in \mathbb{Z}$ _ (כלומר $v \in \mathbb{Z}, v < 0$) ו־$p \nmid v$ אז $-v \in \mathbb{N}$ ו־$p \nmid -v$ ולכן $\|v\| = \|-v\| = 1$.
נגדיר $\alpha = \|p\|$ ויהי $0 \neq q \in \mathbb{Q}$ אז קיימים $0 \neq m \in \mathbb{Z}, n \in \mathbb{N}$ כך ש־$q = \frac{m}{n}$. קיימים $s \in \mathbb{Z}, t \in \mathbb{N}$ כך ש־$p \nmid s, p \nmid t$ ו־$m = p^{v_p(m)}s, n = p^{v_p(n)}t$. אז

$$q = \frac{p^{v_p(m)}s}{p^{v_p(n)}t} = p^{\tilde{v}_p(q)}\frac{s}{t} \Longrightarrow \|q\| = \left\|p^{\tilde{v}_p(q)}\frac{s}{t}\right\| = \|p\|^{\tilde{v}_p(q)}\frac{\|s\|}{\|t\|} = \alpha^{\widetilde{v_p}(q)}\frac{1}{1} = \alpha^{\widetilde{v_p}(q)} = |q|_{p,\alpha}$$

□

הערה

1. יהי p ראשוני, $\gamma, \alpha \in \mathbb{R}$ כך ש־$0 < \alpha < 1$ וגם $0 < \gamma$. אז לכל $q \in \mathbb{Q}$

$$|q|_{p,\alpha}^{\gamma} = \left(\alpha^{\tilde{v}_p(q)}\right)^{\alpha} = (\alpha^{\gamma})^{\tilde{v}_p(q)} = |q|_{p,\alpha^{\gamma}}$$

2. יהי p ראשוני, $\alpha, \beta \in \mathbb{R}$ כך ש־$0 < \alpha, \beta < 1$. אז לכל $q \in \mathbb{Q}$ $|q|_{p,\beta} = |q|_{p,\alpha}$ כאשר $\gamma = \log_{\alpha}(\beta)$.

טענה 2.24

יהיו p ראשוני, $\alpha, \beta \in \mathbb{R}$ כך ש־$0 < \alpha, \beta < 1$ ו־$S \subseteq \mathbb{Q}$. אז S פתוחה ב־$(\mathbb{Q}, |\cdot|_{p,\alpha})$ אם ורק אם S פתוחה ב־$(\mathbb{Q}, |\cdot|_{p,\beta})$.

הוכחה: נניח כי S פתוחה ב־$(\mathbb{Q}, |\cdot|_{p,\beta})$. אז לכל $x \in S$ קיים $r > 0$ כך שלכל $y \in \mathbb{Q}$, $|y - x|_{p,\beta} < 1$ גורר ש־$y \in S$.
אז לכל $y \in \mathbb{Q}$ כך ש־$|y - x|_{p,\alpha} < r^{\log_{\beta}(\alpha)}$ מתקיים

$$|y - x|_{p,\beta} = |y - x|_{p,\alpha}^{\log_{\alpha}(\beta)} < \left(r^{\log_{\beta}(\alpha)}\right)^{\log_{\alpha}(\beta)} = r$$

לפיכך S פתוח ב־$(\mathbb{Q}, |\cdot|_{p,\alpha})$ והכיוון ההפוך סימטרי. □

טענה 2.25

יהיו p ראשוני, $\alpha, \beta \in \mathbb{R}$ כך ש־$0 < \alpha, \beta < 1$ ו־$(a_n)_{n=1}^{\infty}$ היא סדרת מספרים רציונליים. אז $(a_n)_{n=1}^{\infty}$ היא סדרת קושי ב־$(\mathbb{Q}, |\cdot|_{p,\alpha})$ אם ורק אם $(a_n)_{n=1}^{\infty}$ היא סדרת קושי ב־$(\mathbb{Q}, |\cdot|_{p,\beta})$

הוכחה: נניח כי $(a_n)_{n=1}^{\infty}$ היא סדרת קושי ב־$(\mathbb{Q}, |\cdot|_{p,\alpha})$ ויהי $0 < \varepsilon$ ולכן $0 < \varepsilon^{\log_{\beta}(\alpha)}$ ולכן קיים $N \in \mathbb{N}$ כך שלכל $k, l \in \mathbb{N}$ המקיימים $k, l > N$ מתקיים

$$|a_k - a_l|_{p,\alpha} < \varepsilon^{\log_{\beta}(\alpha)}$$

מכאן מתקיים

$$|a_k - a_l|_{p,\beta} = |a_k - a_l|_{p,\alpha}^{\log_{\beta}(\alpha)} < \varepsilon^{(\log_{\beta}(\alpha))^{\log_{\alpha}(\beta)}} = \varepsilon$$

ולכן $(a_n)_{n=1}^{\infty}$ היא סדרת קושי ב־$(\mathbb{Q}, |\cdot|_{p,\beta})$ □

סימון

יהי p ראשוני. אז מסמנים $|\cdot|_p = |\cdot|_{p,\frac{1}{p}}$.

2.2 תזכורת על מרחבים מטריים שלמים והשלמה

הגדרה 2.26 מרחב מטרי שלם

מרחב מטרי (M, d) נקרא שלם כאשר כל סדרת קושי בו מתכנסת.

משפט 2.27

יהי (M, d) מרחב מטרי (לאו דווקא שלם). אז קיים מרחב מטרי שלם $(\widehat{M}, \hat{d})$ כך ש־$M \subseteq \widehat{M}$, $\hat{d}|_M = d$ ו־$\overline{M} = \widehat{M}$ וההשלמה יחידה (זה לא קריטי לנו).
<u>בניית $\widehat{M}$:</u> נסמן ב־$CS(M)$ את הקבוצה של כל סדרות קושי ב־M. נגדיר יחס $\sim$ על $CS(M)$ באופן הבא: $(x_n) \sim (y_n)$ אם ורק אם $\lim_{n\to\infty} d(x_n, y_n) = 0$.
אז $\widehat{M}$ היא קבוצת מחלקות השקילות $\hat{d}([(x_n)], [(y_n)]) = \lim_{n\to\infty} d(x_n, y_n)$.
לכל $x \in M$ נתאים סדרה (x_n) כאשר $x_n = x$ לכל $n \in \mathbb{N}$. אז $M \subseteq \widehat{M}$.

הגדרה 2.28 **שדה נורמי שלם**

יהי $(\mathbb{F},\|\cdot\|)$ שדה נורמי. $(\mathbb{F},\|\cdot\|)$ נקרא שלם כאשר מרחב מטרי $(\mathbb{F},d)$ שלם עבור $d(x,y)=\|x-y\|$ לכל $x,y\in\mathbb{F}$ ונסמן ב־$\left(\hat{\mathbb{F}},\hat{d}\right)$ את ההשלמה של $(\mathbb{F},d)$.
נגדיר $+,\cdot,\|\cdot\|$ על $\hat{\mathbb{F}}$ על־ידי

$$[(x_n)]+[(y_n)]=[(x_n+y_n)]$$
$$[(x_n)]\cdot[(y_n)]=[(x_n\cdot y_n)]$$
$$\|[(x_n)]\|=\hat{d}([(x_n)],[(0)])$$

טענה 2.29

1. $+,\cdot$ ב־$\hat{\mathbb{F}}$ מוגדרים היטב ומקיימים את אקסיומת השדה
2. $\|\cdot\|$ היא נורמה ב־$\hat{\mathbb{F}}$ וגם $\left(\hat{\mathbb{F}},\hat{d}\right)$ שדה נורמי שלם
3. $\left(\hat{\mathbb{F}},\|\cdot\|\right)$ ארכימדי אם ורק אם $(\mathbb{F},\|\cdot\|)$ ארכימדי

הוכחה: תרגיל. □

הערה

ההשלמה של $(\mathbb{Q},|\cdot|)$ היא $(\mathbb{R},|\cdot|)$.

למה 2.30

יהי $(\mathbb{F},\|\cdot\|)$ שדה נורמי לא ארכימדי ו־$(a_n)_{n=1}^{\infty}$ סדרת קושי ב־$\mathbb{F}$ שאינה שואפת ל־0. אז קיים $N\in\mathbb{N}$ כך שלכל $n\geq N$ מתקיים כי $\|a_n\|=\|a_N\|$ (כלומר החל ממקום מסויים היא קבועה).

הוכחה: מאחר ש־$(a_n)_{n=1}^{\infty}$ אינה שואפת ל־0, קיים $0<\varepsilon$ כך שלכל $m\in\mathbb{N}$ קיים $n>m$ כך ש־$\varepsilon<\|a_n\|$.
מאחר ש־$(a_n)_{n=1}^{\infty}$ סדרת קושי, קיים M כך שלכל $k,l\in\mathbb{N}$ עבורם $k,l>M$ מתקיים $\|a_k-a_l\|<\varepsilon$.
אז קיים $M<N$ כך ש־$\varepsilon<\|a_N\|$ ואז לכל $N<n$ מתקיים

$$\|a_n\|=\|(a_n-a_N)+a_N\|=\max(\|a_n-a_N\|,\|a_N\|)=\|a_N\|$$

□

טענה 2.31

יהי $(\mathbb{F},\|\cdot\|)$ שדה נורמי לא ארכימדי. נסמן את חוג השלמים והאידיאל המקסימלי של $\left(\hat{\mathbb{F}},\|\cdot\|\right)$ ב־$\widehat{M}_{\|\cdot\|}$ ו־$\hat{O}_{\|\cdot\|}$ בהתאמה. אז

1. $\hat{O}_{\|\cdot\|}=\overline{O_{\|\cdot\|}}$
2. $\widehat{M}_{\|\cdot\|}=\overline{M_{\|\cdot\|}}$
3. נסמן ב־$\overline{\mathbb{F}_{\|\cdot\|}}$ את שדה השאריות. אז $\overline{\hat{\mathbb{F}}_{\|\cdot\|}}\cong\overline{\mathbb{F}_{\|\cdot\|}}$
4. $\left\{\|a\|\mid a\in\hat{\mathbb{F}}\right\}=\{\|a\|\mid a\in\mathbb{F}\}$

הוכחה:

1. מאחר ש־$O_{\|\cdot\|}\subseteq\hat{O}_{\|\cdot\|}$ וגם $\hat{O}_{\|\cdot\|}$ סגור מתקיים ש־$\overline{O}_{\|\cdot\|}\subseteq\hat{O}_{\|\cdot\|}$. בכיוון השני, יהי $0\neq a\in\hat{O}_{\|\cdot\|}$. אז קיימת סדרת קושי $(a_n)_{n=1}^{\infty}\subseteq\mathbb{F}$ כך ש־$\lim_{n\to\infty}a_n=a$ אז $\lim_{n\to\infty}\|a_n\|=\|a\|$. לפי הלמה, קיים $N\in\mathbb{N}$ כך שלכל $N<n$ מתקיים ש־$\|a_n\|=\|a_N\|=\|a\|$ אבל $\|a\|<1$ ומכאן $a_n\in O_{\|\cdot\|}$. ולכן $a\in\overline{O}_{\|\cdot\|}$ כגבול של סדרה.
2. זהה
3. נגדיר $\varphi:\overline{\mathbb{F}}\to\overline{\hat{\mathbb{F}}}$ על־ידי $\varphi\left(a+M_{\|\cdot\|}\right)=a+\widehat{M}_{\|\cdot\|}$ לכל $a\in O_{\|\cdot\|}$.
קל לראות שזה מוגדר היטב וזה הומומורפיזם של חוגים. מאחר ש־$\overline{\mathbb{F}}$ שדה אז $\ker\varphi=\{0\}$ ולכן φ חד־חד ערכית.
לא טריוויאלי שהוא על (מה עם ההרחבה גדולה יותר?). יהי $a\in\hat{O}_{\|\cdot\|}$ ולכן קיימת סדרת קושי $(a_n)_{n=1}^{\infty}\subseteq O_{\|\cdot\|}$ כך ש־$\lim_{n\to\infty}a_n=a$.
אז קיים $N\in\mathbb{N}$ כך שלכל $N<n$ מתקיים $\|a_n-a\|<1$ כלומר $a_n-a\in\widehat{M}_{\|\cdot\|}$. מכאן ש־$\varphi(a_n)=a_n+\widehat{M}_{\|\cdot\|}=a+\widehat{M}_{\|\cdot\|}$ ולכן φ על ו־φ איזומורפיזם.

סוף הרצאה 9 – 09/06

4. ברור כי $\{\|x\|\mid x\in\mathbb{F}\}\supseteq\left\{\|x\|\mid x\in\hat{\mathbb{F}}\right\}$. בכיוון השני, יהי $0\neq a\in\hat{\mathbb{F}}$. אז קיימת סדרה (a_n) של איברים מ־$\mathbb{F}$ כך ש־$\lim_{n\to\infty}a$. מהלמה קיים $N\in\mathbb{N}$ כך שלכל $N\leq n$ מתקיים $\|a_n\|=\|a_N\|$ ומאחר ש־$\lim_{n\to\infty}\|a_n\|=\|a\|$ לכל $N\leq n$ מתקיים $\|a_n\|=\|a\|$ ולכן $\|a\|=\|a_n\|\in\{\|x\|\mid x\in\mathbb{F}\}$

□

2.3 שדה המספרים ה־p־אדיים

סימון

נסמן את ההשלמה של $(\mathbb{Q}, |\cdot|_p)$ ב־$\mathbb{Q}_p$ ונקרא לו שדה המספרים ה־p־אדיים.
בנוסף, נסמן

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

טענה 2.32

1. $\mathbb{Z}_p = \overline{\mathbb{Z}_{(p)}} = \overline{\mathbb{Z}}$
2. האידיאל המקסימלי ב־$(\mathbb{Q}_p, |\cdot|_p)$ הוא $\overline{p\mathbb{Z}_{(p)}} = p\mathbb{Z}_p$
3. שדה השאריות של $(\mathbb{Q}_p, |\cdot|)$ הוא $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p$
4. $\{|x|_p \mid x \in \mathbb{Q}_p\} = \{|x|_p \mid x \in \mathbb{Q}\} = \left\{\frac{1}{p^s} \mid s \in \mathbb{Z} \cup \{\infty\}\right\}$

הוכחה: אנלוגי לטענה הקודמת. □

למה 2.33

יהי $(\mathbb{F}, \|\cdot\|)$ שדה נורמי לא ארכימדי שלם ותהיי (a_n) סדרה ב־$\mathbb{F}$ ששואפת ל־0. אזי $\sum_{n=0}^{\infty} a_n = \lim_{n\to\infty} a_i$ מתכנס.

הוכחה: יהי $\varepsilon > 0$, קיים $N \in \mathbb{N}$ כך שלכל $N \leq n$ מתקיים $\|a_n\| < \varepsilon$. מכאן, לכל $N \leftarrow m < n$ מתקיים כי

$$\|b_n - b_m\| = \left\| \sum_{i=1m+}^{n} a_i \right\| \leq \max_{m+1 \leq i \leq n} \|a_i\| < \varepsilon$$

לכן (b_n) היא סדרת קושי ומאחר ש־$(\mathbb{F}, \|\cdot\|)$ שלם היא מתכנסת. □

סימון

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.
מעתה והלאה הנורמה המדוברת היא הנורמה ה־p־אדית אלא אם נאמר אחרת (לפעמים נרשם $\|\cdot\|$ או $|\cdot|$ אבל הכוונה לנורמה ה־p־אדית).

טענה 2.34

תהיי $(a_n)_{n=1}^{\infty}$ סדרה ב־$\mathbb{Z}$ כך ש־$0 \leq a_n \leq p-1$ עבור $n \in \mathbb{N}_0$.
ב־$\mathbb{Q}_p$ קיים הגבול $\sum_{n=0}^{\infty} a_n p^n = a$ וגם $a \in \mathbb{Z}_p$ ויתר על־כן, $a \in p\mathbb{Z}_p \iff a_0 = 0$.

הוכחה: מאחר ש־$\|a_n\| \in \{0, 1\}$ לכל $n \in \mathbb{N}_0$ מתקיים $\|a_n p^n\| \in \left\{0, \frac{1}{p^n}\right\}$ ולכן $\lim_{n\to\infty} a_n p^n = 0$ ומהלמה הקודמת הסכום $\sum_{n=0}^{\infty} a_n p^n$ מתכנס ל־a.
מאחר ש־$\left|\sum_{i=1}^{n} a_i p^i\right|_p < 1$ (מלמה 2.30) מתקיים $\left|\sum_{i=1}^{\infty} a_i p^i\right|_p < 1$ ולכן אם $a_0 = 0$ אז $|a|_p = \left|\sum_{i=1}^{\infty} a_i p^i\right|_p$.
אם $a_0 \neq 0$ אז $|a_0|_p = 1$ ולכן $|a|_p = \max\left(|a_0|_p, \left|\sum_{i=1}^{\infty} a_i p^i\right|_p\right) = 1$. □

טענה 2.35

תהיינה $(a_n)_{n=0}^{\infty}, (b_n)_{n=0}^{\infty}$ סדרות ב־$\mathbb{Z}$ כך ש־$0 \leq a_n, b_n \leq p-1$ לכל $n \in \mathbb{N}_0$ וגם $\sum_{i=0}^{\infty} a_n p^n = \sum_{i=0}^{\infty} b_n p^n$ אז $a_n = b_n$ לכל $n \in \mathbb{N}_0$.

הוכחה: נניח בשלילה שקיים $n \in \mathbb{N}_0$ כך ש־$a_n \neq b_n$ ולכן נגדיר $m = \min\{n \in \mathbb{N}_0 \mid a_n \neq b_n\}$.
אזי $\sum_{i=0}^{m-1} a_i p^i = \sum_{i=0}^{m-1} b_i p^i$ ולכן גם $\sum_{i=m}^{\infty} a_i p^i = \sum_{i=m}^{\infty} b_i p^i$ (זנב) ומכאן

$$a_m + \sum_{i=m+1}^{\infty} a_i p^{i-m} = \sum_{i=m}^{\infty} a_i p^{i-m} = \sum_{i=m}^{\infty} b_i p^{i-m} = b_m + \sum_{i=m+1}^{\infty} b_i p^{i-m}$$

לכן

$$a_m - b_m = \sum_{i=m+1}^{\infty} b_i p^{i-m} - \sum_{i=m+1}^{\infty} a_i p^{i-m}$$

כמו בהוכחה הקודמת,

$$\left| \sum_{i=m+1}^{\infty} b_i p^{i-m} - \sum_{i=m+1}^{\infty} a_i p^{i-m} \right|_p < 1$$

אבל $a_m \neq b_m$ ולכן $|a_m - b_m|_p = 1$ וזאת סתירה. □

טענה 2.36

לכל $x \in \mathbb{Z}_p$ ולכל $k \in \mathbb{N}_0$ קיים $r \in \mathbb{Z}$ יחיד כך ש־$0 \le r \le p^x - 1$ כך ש־$|x-r|_p \le \frac{1}{p^k}$.

הוכחה: מאחר ש־$\overline{\mathbb{Z}} = \mathbb{Z}_p$ נובע שקיים $z \in \mathbb{Z}$ כך ש־$|x-z|_p \le \frac{1}{p^k}$.
נחלק את z ב־p^k עם שארית ונקבל $q, r \in \mathbb{Z}$ כך ש־$z = qp^k + r$ ו־$0 \le r \le p^k - 1$ ומתקיים

$$|x-r|_p = |(x-z)+(z-r)|_p = \left|x - z + qp^k\right| \le \max\left(|x-z|_p, \left|qp^k\right|_p\right) \le \frac{1}{p^k}$$

נשאר להראות יחידות - יהיו $0 \le r_1, r_2 \le p-1$ כך ש־$|x-r_1|_p, |x-r_2|_p \le \frac{1}{p^k}$ מכאן

$$|r_1 - r_2|_p = |(x-r_1)-(x-r_2)|_p \le \max\left(|x-r_1|_p, |x-r_2|_p\right) \le \frac{1}{p^k}$$

מאחר ש־$-\left(p^k - 1\right) \le |r_1 - r_2| \le p^k - 1$ אנו מסיקים ש־$r_2 - r_1 = 0$. □

מסקנה 2.37

לכל $x \in \mathbb{Z}_p$ קיימת סדרה יחידה $(r_n)_{n=1}^{\infty} \subseteq \mathbb{Z}$ כך שמתקיים

1. $0 \le r_k \le p^k - 1$
2. $|x - r_k|_p \le \frac{1}{p^k}$
3. $p^k \mid r_{k+1} - r_k$

הוכחה: נשים לב ש־1 ו־2 נובעים מהטענה הקודמת. עבור 3,

$$\left|r_{k+1} - r_k\right|_p = \left|(x-r_k)-(x-r_{k+1})\right| \le \max\left(|x-r_k|_p, |x-r_{k+1}|_p\right) \underset{(2)}{\le} \frac{1}{p^k}$$

□

טענה 2.38

יהי $x \in \mathbb{Z}_p$ קיימת סדרה $(a_n)_{n=0}^{\infty} \subseteq \mathbb{Z}$ כך ש־$0 \le a_n \le p-1$ לכל $n \in \mathbb{N}_0$ וגם $\lim_{n\to\infty} \sum_{i=0}^{n} a_i p^i = \sum_{n=0}^{\infty} a_n p^n = x$.

הוכחה: נגדיר

$$a_0 = r_1, \quad a_1 = \frac{r_2 - r_1}{p}, \quad a_2 = \frac{r_3 - r_2}{p^2}, \quad a_i = \frac{(r_{i+1} - r_i)}{p^i}$$

מהמסקנה $a_i \in \mathbb{Z}$ ומאחר ש־$0 \le r_{i+1} \le p^{i+1} - 1$ ו־$0 \le r_i \le p^i - 1$ מתקיים $-\left(p^i - 1\right) \le r_{i+1} - r_i \le p^{i+1} - 1$.
מאחר ש־$p^i \mid r^{i+1} - r^i$ מתקיים $0 \le r_{i+1} - r_i \le p^{i+1} - p^i$ ולכן $0 \le a_i \le p-1$ ולסיום

$$r_n = r_{n-1} + a_{n-1}p^{n-1} = r_{n-2} + a_{n-2}p^{n-2} + a_{n-1}p^{n-1} = \dots = \sum_{i=0}^{n-1} a_i p^i$$

ולכן $\lim_{n\to\infty} \sum_{i=0}^{n} a_i p^i = \lim_{n\to\infty} r_{n+1} = x$. □

טענה 2.39

לכל $x \in \mathbb{Q}_p^{\times}$ קיים $s \in \mathbb{Z}$ וסדרה $(a_n)_{n=s}^{\infty} \subseteq \mathbb{Z}$ כך ש־$0 \le a_n \le p-1$ לכל $n \in \mathbb{Z}$ עם $n \ge s$ ובנוסף $a_s \ne 0$ ו־$\sum_{n=s}^{\infty} a_n p^n = x$.

הוכחה: קיים $s \in \mathbb{Z}$ כך ש־$|x|_p = \frac{1}{p^s}$ ולכן נגדיר $x' = \frac{x}{p^s}$ ואז $|x'|_p = \frac{|x|_p}{\left|\frac{1}{p^s}\right|_p} = 1$ ולכן קיימת סדרה $(a'_n)_{n=0}^{\infty} \subseteq \mathbb{Z}$ כך ש־$0 \le a'_n \le p-1$ וגם $\sum_{n=0}^{\infty} a'_n p^n$ ומאחר ש־$|x'| = 1$ מתקיים $a'_0 \ne 0$ ולכן נגדיר $a_n = a'_{n-s}$ לכל $n \in \mathbb{N}$ ו־$s \le n$ ונקבל $\sum_{n=s}^{\infty} a_n p^n = \sum_{n=0}^{\infty} a_{n+s} p^{n+s} = \sum_{n=0}^{\infty} a'_n p^n p^s = x' p^s = x$. □

סוף הרצאה 10 – 16/06

סימון

1. אם $(a_i)_{i=0}^{\infty} \subseteq \mathbb{Z}$ כאשר $0 \le a_i \le p-1$ רושמים $(\dots a_2 a_1 a_0)_p = \sum_{i=0}^{\infty} a_i p^i$
2. אם $s \in \mathbb{Z}_$ ו־$(a_i)_{i=s}^{\infty} \subseteq \mathbb{Z}$ עם $0 \le a_i \le p-1$ ו־$a_s \ne 0$ רושמים $(\dots a_1 a_0 . a_{-1} \dots a_{s+1} a_s)_p = \sum_{i=s}^{\infty} a_i p$

מסקנה 2.40

$\overline{\mathbb{N}_0} = \mathbb{Z}_p$.

דוגמה

$x=-1$ ואז

$$-1=\lim_{n\to\infty}(p^n-1)=\lim_{n\to\infty}(p-1)(1+p+1+\cdots+p^{n-1})=\lim_{n\to\infty}\sum_{i=0}^{n-1}(p-1)p^i=\sum_{i=0}^{\infty}(p-1)p^i$$

כלומר $(\ldots(p-1)(p-1))=-1$

טענה 2.41

יהיו $s,t\in\mathbb{Z}$, $d\in\mathbb{N}$ ו־$(a_i)_{i=s}^{\infty}\subseteq\mathbb{Z}$ כך ש־$0\le a_i\le p-1$ לכל $n\in\mathbb{Z}$, $s\le n$ עם $a_s\neq 0$, $s\le t$ ולכל $t\le i$ מתקיים $a_{i+d}=a_i$.
אזי $\sum_{i=s}^{\infty}a_ip^i\in\mathbb{Q}$.

הערה

s המיקום של הספרה הראשונה, d אורך המחזור ו־t כמה ספרות יש עד שזה הופך להיות למחזורי (המיקום של ההתחלה של המחזור הראשון).

הוכחה: נסמן

$$x=\sum_{i=s}^{\infty}a_ip^i,\qquad r=\sum_{i=s}^{t-1}a_ip^i,\qquad q=\sum_{s=t}^{t+d-1}a_ip^i$$

אז

$$x-r-q=\sum_{i=t+d}^{\infty}a_ip^i\underset{a_{i+d}=a_i}{=}p^d\sum_{i=t+d}^{\infty}a_{i-d}p^{i-d}=p^d\sum_{j=t}^{\infty}a_jp^j=p^d(x-r)$$

מכאן $(x-r)(1-p^d)=q$ ולכן $x=r+\frac{q}{1-p^d}\in\mathbb{Q}$. □

טענה 2.42

יהיו $s\in\mathbb{Z}$, $(a_i)_{i=s}^{\infty}\subseteq S$ כך ש־$0\le a_i\le p-1$ לכל $s\le i$, $a_s\neq 0$ וגם $\sum_{i=s}^{\infty}a_ip^i\in\mathbb{Q}$. אז קיימים $t\in\mathbb{Z}$, $s\le t$ ו־$d\in\mathbb{N}$ כך ש־$a_{i+d}=a_i$ לכל $t\le i$.

הוכחה: קיימים $m,n\in\mathbb{Z}$ כך ש־$p\nmid m,p\nmid n$ וגם $\sum_{i=s}^{\infty}a_ip^i=p^s\frac{m}{n}$ כאשר כמובן $n\neq 0$.
לכל $i\in\mathbb{N}_0$ נגדיר $c_i=a_{i+s}$ ואז

$$\frac{m}{n}=\sum_{i=s}^{\infty}a_ip^{i-s}=\sum_{j=0}^{\infty}a_{j+s}p^j=\sum_{j=0}^{\infty}c_jp^j$$

מכאן $m=n\sum_{j=0}^{\infty}c_jp^j$.
לכל $k\in\mathbb{N}$ נסמן

$$r_k:=\frac{n\sum_{j=k}^{\infty}c_jp^j}{p^k}=\frac{m-n\sum_{j=0}^{k-1}c_jp^j}{p^k}$$

אז $r_k\in\mathbb{Q}$, $|r_k|_p\le 1$ וגם $r_k\in\mathbb{Z}$. יתר על־כן מתקיים

$$\frac{m+n}{p^k}-n=\frac{m-n(p^k-1)}{p^k}\le\frac{m-n\sum_{j=0}^{k-1}(p-1)p^j}{p^k}\frac{m-n\sum_{j=0}^{k-1}c_jp^j}{p^k}\le\frac{m}{p^k}$$

קיים $N\in\mathbb{N}$ כך שלכל $N\le k$ מתקיים ש־$\left|\frac{m}{p^k}\right|<1$ וגם $\left|\frac{m+n}{p^k}\right|<1$ ולכן עבור $N\le k$ מתקיים $-n-1<r_k<1$ ולכן קיימים $N\le k<l$ כך ש־$r_k=r_l$.
מאחר שמתקיים כי $r_k\equiv nc_k\bmod p$ אנו מסיקים כי $nc_k\equiv nc_l\bmod p$ ומכאן $c_k\equiv c_l\bmod p$ אבל מכך ש־$0\le a_i\le p-1$ נובע כי $c_k=c_l$.
בנוסף, מתקיים ש־

$$r_{k+1}=\frac{r_k-nc_k}{p}=\frac{r_l-nc_l}{p}=r_{l+1}$$

אז לכל $i\in\mathbb{N}_0$ מתקיים כי $c_{k+1}=c_{l+1}$, נגדיר $t=k+s$, $d=l-k$ ואז לכל $t\le i$ מתקיים $0\le i-k-s$ ולכן

$$a_{i+d}=c_{i+d-s}=c_{l+(i-k-s)}=c_{k+i-k-s}=c_{i-s}=a_i$$

□

דוגמה

נמצא הצגה 5־אדית של $\frac{1}{3}$ ולכן נסמן $\frac{1}{3} = \sum_{i=0}^{\infty} a_i p^i$ כאן $s = 0$, $m = 1$, $n = 3$, $r_0 = m = 1$ ו־$0 \le a_i = c_i \le p-1 = 4$.
מתקיים $3a_0 \underset{\mathrm{mod}\,5}{\equiv} 1$ ולכן $a_0 = 2$ אז $r_1 = \frac{r_0 - na_0}{p} = \frac{1-3\cdot 2}{5} = \frac{-5}{5} = -1$.
כעת ניתן לחשב גם $3 \cdot a_1 \underset{\mathrm{mod}\,5}{\equiv} -1$ ולכן $a_1 = 3$ ואז באופן דומה $r_2 = \frac{r_1 - na_1}{5} = \frac{-1-3\cdot 3}{5} = \frac{-10}{5} = -2$.
ניקח $3 \cdot a_2 \underset{\mathrm{mod}\,5}{\equiv} -2$ ולכן $a_2 = 1$ ושוב $r_3 = \frac{r_2 - na_2}{5} = \frac{-2-3\cdot 1}{5} = \frac{-5}{5} = -1$.
מתקיים ש־$r_3 = r_1$ ובעצם התחלנו את המחזור ולכן לכל $1 \le i$ מתקיים כי $a_{i+2} = a_i$ ולסיכום $\frac{1}{3} = (...13132)_5$.

טענה 2.43

כל אידיאל ב־$\mathbb{Z}_p$ הוא מהצורה $p^n\mathbb{Z}_p$ עבור $n \in \mathbb{N}$.

הוכחה: יהי I אידיאל ב־$\mathbb{Z}_p$ ולכן מתקיים $I \subseteq p\mathbb{Z}_p$ ו־$\left\{|x|_p \mid x \in p\mathbb{Z}_p\right\} = \left\{\frac{1}{p^i} \mid i \in \mathbb{N}\right\}$.
לכן קיים $h = \max\left\{|x|_p \mid x \in I\right\}$ וגם קיים $a \in I$ כך ש־$|a|_p = h$. בנוסף, קיים $n \in \mathbb{N}$ כך ש־$h = \frac{1}{p^n}$, נוכיח כי $I = p^n\mathbb{Z}_p$.
מתקיים כי $|p^n|_p = h$ ומכאן $\left|\frac{p^n}{a}\right|_p = 1$ ולכן $\frac{p^n}{a} \in \mathbb{Z}_p$ ומכאן $p^n \in a\mathbb{Z}_p \subseteq I$ לפיכך $p^n\mathbb{Z}_p \subseteq I$.
להכלה השנייה, יהי $b \in I$ ואז $|b|_p \le |a|_p = h$ ומכאן $\left|\frac{b}{p^n}\right|_p \le 1$ ולכן $\frac{b}{p^n} \in \mathbb{Z}_p$ וכמקודם $b \in p^n\mathbb{Z}_p$ ולפיכך $I \subseteq p^n\mathbb{Z}_p$. □

מסקנה 2.44

$\mathbb{Z}_p$ הוא חוג ראשי (תחום שלמות שכל אידיאל שלו הוא ראשי).

סימון

1. עבור $a, b \in \mathbb{Z}_p$ נרשום $a \underset{\mathrm{mod}\,p^n}{\equiv} b$ כאשר $a - b \in p^n\mathbb{Z}$
2. לכל $a \in \mathbb{Z}_p$ נסמן $\overline{a} = a + p\mathbb{Z}_p \in \mathbb{Z}_p/p\mathbb{Z}_p$ (הרדוקציה)

למה 2.45 הלמה של הנזל

יהיו $f \in \mathbb{Z}_p[x]$ ו־$w_0 \in \mathbb{Z}_p$ כך ש־$\overline{f(w_0)} = 0$ וגם $\overline{f'(w_0)} \neq 0$. אז קיים $w \in \mathbb{Z}_p$ יחיד כך ש־$\overline{w} = \overline{w_0}$ וגם $f(w) = 0$.

הערה

עבור $f = c_n x^n + \cdots + c_1 x + c_0$ הנגזרת היא $f' = nc_n x^{n-1} + \cdots + c_1$.

דוגמה

עבור $p \neq 2$ ראשוני, נבחר $a \in \mathbb{Z}_p$ כך ש־$\overline{a} \neq 0$ (לא מתחלק ב־p) ונגדיר $f = x^2 - a$.
מתקיים $d' = 2x$ ומהלמה של הנזל נובע כי אם קיים $w_0 \in \mathbb{Z}_p$ כך ש־$w_0^2 \underset{\mathrm{mod}\,p}{\equiv} a$ אז מאחר ש־$a \underset{\mathrm{mod}\,p}{\not\equiv} 0$ מתקיים $f'(w_0) = 2w_0 \underset{\mathrm{mod}\,p}{\not\equiv} 0$ ולכן קיים $w \in \mathbb{Z}_p$ כך ש־$w^2 = a$ כלומר קיים שורש!

הערה

כאשר $p = 2$ הדוגמה לעיל לא נכונה כי עבור $a = 3$ נסתכל על הפולינום $f = x^2 - 3 = x^2 - 1$ ועבור $w_0 = 1$ מתקיים ש־$1^2 \underset{\mathrm{mod}\,2}{\equiv} 3$ אבל ב־$\mathbb{Z}_2$ אין שום מספר שהריבוע שלו ייתן לנו שלוש בידיוק כי זה או אפס או אחד.

סוף הרצאה 11 – 23/06

הוכחה של למה 2.45: נבנה סדרה $(r_k)_{k=1}^{\infty}$ כך ש־$r_k \in \mathbb{Z}$, $0 \le r_k \le p^k - 1$, $\overline{r_k} = \overline{w_0}$, $p^k \mid r_{k+1} - r_k$, $f(r_k) \in p^k\mathbb{Z}_p$ לכל $k \in \mathbb{N}$ באופן רקורסיבי.
קיים $r_1 \in \mathbb{Z}$ יחיד כך ש־$0 \le r_1 \le p-1$ ו־$\overline{r_1} = \overline{w_0}$ ונניח כי $r_1, ..., r_k$ כבר הוגדרו ומקיימים את התנאים הנדרשים.
נגדיר $r_{k+1} = r_k + dp^k$ כאשר $0 \le d \le p-1$ יוגדר באופן הבא: נניח כי קיים $0 \le d \le p-1$ יחיד כך ש־$f(r_{k+1}) \in p^{k+1}\mathbb{Z}_p$.
נסמן $f = c_0 + c_1 x + \cdots + c_n x^n$ ואז לכל $d \in \mathbb{Z}$, $0 \le d \le p-1$ מתקיים

$$\begin{aligned}
f(r_{k+1}) &= f(r_k + dp^k) = c_0 + c_1(r_k + dp^k) + c_2(r_k + dp^k)^2 + \cdots + c_n(r_k + dp^k)^n \\
&= c_0 + c_1(r_k + dp^k) + c_2(r_k^2 + 2r_k dp^k + d^2p^{2k}) + \cdots + c_n\left(r_k^n + nr_k^{n-1}dp^k + \binom{n}{2}r_k^{n-2}d^2p^{2k}\right) + \cdots + \binom{n}{n}d^n p^{nk} \\
&\underset{\mathrm{mod}\,p^{k+1}}{\equiv} c_0 + c_1(r_k + dp^k) + c_2(r_k^2 + 2r_k dp^k) + c_3(r_k^3 + 3r_k^2 dp^k) + \cdots + c_n(r_k^n + nr_k^{n-1}dp^k) \\
&= \left(c_0 + c_1 r_k + c_2 r_k^2 + c_3 r_k^3 + \cdots + c_n r_k^n\right) + \left(c_1 + 2c_2 r_k + 3c_3 r_k^2 + \cdots + nc_n r_k^{n-1}\right)dp^k \\
&= f(r_k) + f'(r_k)dp^k \bmod p^{k+1}
\end{aligned}$$

מאחר ש־$f(r_k) \in p^k\mathbb{Z}_p$, קיים $z \in \mathbb{Z}_p$ כך ש־$f(r_k) = zp^k$.
מאחר ש־$f'(r_k) = f'(w_0) \neq 0$, קיים ויחיד $d \in \mathbb{Z}$ עבורו $0 \leq d \leq p-1$ כך ש־$f'(r_k)d \underset{\mod p}{\equiv} -z$ ואז $p \mid z + f'(r_k)d$.
מכאן

$$f(r_k) = f(r_k) + f'(r_k)dp^k = (z + f'(r_k)d)p^k \in p^{k+1}\mathbb{Z}$$

בנוסף $0 \leq r_{k+1} \leq p^k - 1 + (p-1)p^k = p^{k+1} - 1$ וגם $\overline{r_{k+1}} = \overline{r_k} = \overline{w_0}$ ו־$p^k \mid dp^k = r_{k+1} - r_k$.
לפיכך $r_1, \ldots, r_{k+1}$ מקיימים את כל התנאים הנדרשים ולכן הסדרה $(r_k)_{k=1}^{\infty}$ היא סדרת קושי ולכן קיים $w = \lim_{k\to\infty} r_k$.
יתר על־כן, מתקיים

$$f(w) = f\left(\lim_{k\to\infty} r_k\right) = \lim_{k\to\infty} f(r_k) = 0$$

□

מסקנה 2.46

אם $p \neq 2$ וגם $a \in \mathbb{Z}_p$ כך ש־$\overline{a} \neq 0$ ו־$w_0 \in \mathbb{Z}_p$ כך ש־$\overline{w_0^2} = \overline{a}$. אז קיים $w \in \mathbb{Z}_p$ כך ש־$w^2 = a$ וגם $\overline{w} = \overline{w_0}$.

הוכחה: נגדיר $f = x^2 - a$ ואז מכך ש־$\overline{w_0^2} = \overline{a}$ נקבל

$$\overline{f(w_0)} = \overline{w_0^2} - \overline{a} = 0$$
$$\overline{f'(w_0)} = \overline{2w_0} = \overline{2}\,\overline{w_0} \neq 0$$

לכן קיים $w \in \mathbb{Z}_p$ כך ש־$f(w) = 0$ כלומר $w^2 = a$. □

הערה

1. התנאי $p \neq 2$ הכרחי. דוגמה נגדית קלאסית היא $a = 3 \in \mathbb{Z}_2 = \mathbb{Z}_p$.
2. התנאי $\overline{a} \neq 0$ הכרחי. דוגמה נגדית קלאסית היא $a = p \in \mathbb{Z}_p$.

מסקנה 2.47

אם $p \neq 2$ וגם $a \in \mathbb{Z}_p$ כך ש־$\overline{a} = 1$ אז קיים $w \in \mathbb{Z}_p$ כך ש־$w^2 = a$ וגם $\overline{w} = 1$.

טענה 2.48

יהי $p \neq 2$ ראשוני. אז

$$\mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2 \cong \mathbb{F}_p^\times / \left(\mathbb{F}_p^\times\right)^2 \cong \mathbb{Z}/2\mathbb{Z}$$

הוכחה: נגדיר $pr : \mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ על־ידי $pr(a) = a + p\mathbb{Z}_p$.
אז pr הוא הומומורפיזם של חוגים ולכן $pr|_{\mathbb{Z}_p^\times} : \mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ הוא הומומורפיזם של חבורות שהוא על.
נסמן $\pi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times / \left(\mathbb{F}_p^\times\right)^2$ על־ידי $\pi(x) = x \cdot \left(\mathbb{F}_p^\times\right)^2$ ולכן גם π הוא הומומורפיזם של חבורות שהוא על.
נרכיב ונקבל $\pi \circ pr|_{\mathbb{Z}_p^\times} : \mathbb{Z}_p^\times \to \mathbb{F}_p^\times / \left(\mathbb{F}_p^\times\right)^2$.
אם $x \in \left(\mathbb{Z}_p^\times\right)^2$ אזי $pr|_{z_p^\times}(x) \in \left(\mathbb{F}_p^\times\right)^2$ ולכן $\pi \circ pr|_{\mathbb{Z}_p^\times}(x) = 1$ ולכן $\left(\mathbb{Z}_p^\times\right)^2 \subseteq \ker\left(\pi \circ pr|_{\mathbb{Z}_p^\times}\right)$.
יהי $a \in \ker\left(\pi \circ pr|_{\mathbb{Z}_p^\times}\right)$ אז $pr|_{\mathbb{Z}_p^\times}(a) = \ker \pi = \left(\mathbb{F}_p^\times\right)^2$ מכאן קיים $w_0 \in \mathbb{Z}_p$ כך ש־$\overline{a} = \overline{w_0^2}$ ומהמסקנה שראינו קיים $w \in \mathbb{Z}_p$ כך ש־$a = w^2$ ולכן $a \in \left(\mathbb{Z}_p^\times\right)^2$
ולפיכך $\ker\left(\pi \circ pr|_{\mathbb{Z}_p^\times}\right) \subseteq \left(\mathbb{Z}_p^\times\right)^2$.
אז לפי משפט ההומומורפיזם מתקיים $\mathbb{Z}_p^\times / \left(\mathbb{Z}_p^\times\right)^2 \cong \mathbb{F}_p^\times / \left(\mathbb{F}_p^\times\right)^2$. □

טענה 2.49

יהי p ראשוני. אזי $\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}$.

הוכחה: נגדיר $f : \mathbb{Z}_p^\times \times \mathbb{Z} \to \mathbb{Q}_p^\times$ על־ידי $f(u, s) = up^s$.
קל לראות ש־f הומומורפיזם, חד־חד ערכית ועל כלומר איזומורפיזם. □

מסקנה 2.50

יהי $p \neq 2$ ראשוני. אז $\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
בנוסף, אם $r \in \mathbb{Z}_p^\times$ כך ש־$\overline{r} \in \mathbb{F}_p^\times / \left(\mathbb{F}_p^\times\right)^2$ אז

$$\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2 = \left\{\left(\mathbb{Q}_p^\times\right)^2, r\left(\mathbb{Q}_p^\times\right)^2, p\left(\mathbb{Q}_p^\times\right)^2, rp\left(\mathbb{Q}_p^\times\right)^2\right\}$$

הערה

ניקח כעובדה את המקרה של $p=2$

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$$
$$(\mathbb{Q}_2^\times)/(\mathbb{Q}_2^\times)^2 = \left\{(\mathbb{Q}_2^\times)^2, -(\mathbb{Q}_2^\times)^2, 2(\mathbb{Q}_2^\times)^2, -2(\mathbb{Q}_2^\times)^2, 5(\mathbb{Q}_2^\times)^2, -5(\mathbb{Q}_2^\times)^2, 10(\mathbb{Q}_2^\times)^2, -10(\mathbb{Q}_2^\times)^2\right\}$$

3 בחזרה לתבניות ריבועיות

טענה 3.1

יהי (V,q) מרחב ריבועי לא מנוון מעל $\mathbb{Q}_p$ עבור $p \neq 2$.
אז קיים בסיס $\mathcal{B}$ של V כך שמתקיים

$$[g_q]_{\mathcal{B}} = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$$

כאשר $a_i \in \{1, r, p, pr\}$ לכל $1 \leq i \leq n$.

סוף הרצאה 12 – 30/06