תבניות ריבועיות ומספרים P-אדיים

2 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

1 תבניות בילינאריות 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־$\pi : \mathbb{F}^\times \to {\mathbb{F}^\times}/{(\mathbb{F}^\times)^2}$ 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 $\pi|_R : R \to {\mathbb{F}^\times}/{(\mathbb{F}^\times)^2}$ 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 $\left|{\mathbb{C}^\times}/{(\mathbb{C}^\times)^2}\right| = 1$ וניתן לבחור $R = \{1\}$
2. $\mathbb{F} = \mathbb{R}$ אז $(\mathbb{C}^\times)^2 = \{x \in \mathbb{R}^\times \mid x > 0\}$ ומתקיים $\left|{\mathbb{R}^\times}/{(\mathbb{R}^\times)^2}\right| = 2$ וניתן לבחור $R = \{-1, 1\}$

טענה 1.3

יהי p ראשוני ו־$p \neq 2$ אז $\left|{\mathbb{F}_p^\times}/{(\mathbb{F}_p^\times)^2}\right| = 2$.
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 $Im(s) \cong {\mathbb{F}_p^\times}/{\ker s}$ 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

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

$\square$

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

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

□

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 $k,\ell\in\mathbb{Z},n\in\mathbb{N}$ 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

$$\dim(U\cap W)=\dim U+\dim W-\dim(U+W)\ge\ell+(n-k)-n=\ell-k\ge1$$

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. □

דוגמה

יהי $p\ne2$ 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־$\left[g_{q_2}\right] = \left(\begin{smallmatrix} I_{n-1} & 0 \\ 0 & r \end{smallmatrix}\right)$ 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 $q\left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) = -x_1^2 - x_2^2$.
מהמשפט קיים בסיס $\mathcal{B}$ של $\mathbb{F}_7^2$ כך שמתקיים $\left[g_q\right]_{\mathcal{B}} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right)$.

סוף הרצאה 5 – 12/05

1.4 איזוטרפיות

מוטיבציה: נסתכל על התבנית הריבועית $q : \mathbb{F}^2 \to \mathbb{F}$ הנתונה על־ידי $q\left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) = x_1^2 - x_2^2$ והמרחב הריבועי עם התבנית הזאת הוא לא מנוון (המטריצה המייצגת הפיכה) אבל נניח הוקטור $q\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) = 0$ 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 חפיפת 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 □

סוף הרצאה 6 – 19/05

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 $q_{1,1}\binom{x_1}{x_2}=x_1^2+x_2^2$

      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 $q_{1,r}\binom{x_1}{x_2}=x_1^2+rx_2^2$

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 $g'\binom{x_1}{x_2}=a_1x_1^2+a_2x_2^2$ ולכן

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

ולכן $(\mathbb{F}_p^2,q')$ לא מנוון ולכן קיים $(x)1,x_2)\in\mathbb{F}_p^2$ כך ש־$a_1x_1^2+a_2x_2^2=g'\binom{x_1}{x_2}=-a_3$.
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־$\|a+b\|^n \le \sqrt[n]{n+1}\|a\|$ ומאחר ש־$\lim_{n\to\infty} \sqrt[n]{n+1} = 1$, נסיק כי $\|a+b\| \le \|a\| = \max(\|a\|, \|b\|)$.
$\Longrightarrow$ לכל $n \in \mathbb{N}$ מתקיים $\|n\| = \left\|\sum_{i=1}^{n} 1\right\| \le \max(\|1\|, ..., \|1\|) = 1$ 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

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

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

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

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

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

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 $\|x\|, \|y\| \le 1$ ומכאן $\|xy\| = \|x\|\|y\| \le 1$ ואי־שיוויון המשולש האולטרה מטרי מניב לנו $\|x+y\| \le \max(\|x\|, \|y\|) \le 1$.
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 $\|x\| \le 1$. אז

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

3. יהיו $x, y \in \mathcal{M}_{\|\cdot\|}$. אז $\|x\|, \|y\| < 1$ ולכן מאי־שיוויון האולטרה מטרי $\|x+y\| \le \max(\|x\|, \|y\|) < 1$ 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 $\|x\| < 1$, $\|y\| \le 1$. 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

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

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 $s = v_p(a), t = v_p(b)$. 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 $z' - z \in p\mathbb{Z}_{(p)}$ וגם $z' - z \in \mathbb{Z}$ 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