פתרון מטלה 02 — תבניות ריבועיות ומספרים P-אדיים, 80507

15 במאי 2026

שאלה 1

יהיו (V,q) מרחב ריבועי מעל שדה $\mathbb{F}$ ו־$u_1,...,v_k \in V$.
המטריצה $A=\left(a_{ij}\right)_{1\le i,j\le n} \in M_n(\mathbb{F})$ מוגדרת על־ידי $a_{ij}=g_q\left(u_i,u_j\right)$. נוכיח שאם A הפיכה אז הסדרה $(u_1,...,u_k)$ בלתי תלויה לינארית.

הוכחה: להוכיח שהסדרה בלתי תלויה ליניארית מספיק שנשתמש בהגדרת התלות הליניארית ונראה שכל צירוף ליניארי שמתאפס גורר שכל המקדמים הם אפס.
נניח שקיימים $\alpha_1,...,\alpha_k \in \mathbb{F}$ כך שמתקיים $\sum_{j=1}^{k}\alpha_j u_j = 0_V$.
נסמן ב־g_q את התבנית הבילנארית הסימטרית של q.
מהלינאריות של התבנית ברכיב השני נקבל

$$g_q\left(u_i,\sum_{j=1}^{k}\alpha_j u_j\right)=g_q(u_i,0_V)=0$$

מצד שני, מלינאריות התבנית ניתן להוציא החוצה סכום וסקלר

$$\sum_{j=1}^{k}\alpha_j g_q\left(u_i,u_j\right)=0$$

אבל זה בידיוק כפל של שורה במטריצה A בוקטור המקדמים, אז נציב $a_{ij}=g_q\left(u_i,u_j\right)$ ונקבל מערכת של k משוואות

$$\begin{cases}\alpha_1 a_{11}+\alpha_2 a_{12}+...+\alpha_k a_{1k}=0\\ \alpha_1 a_{21}+\alpha_2 a_{22}+...+\alpha_k a_{2k}=0\\ \vdots\\ \alpha_1 a_{k1}+\alpha_2 a_{k2}+...+\alpha_k a_{kk}=0\end{cases}$$

כלומר

$$A\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_k\end{pmatrix}=\begin{pmatrix}0\\0\\ \vdots\\0\end{pmatrix}$$

אבל A היא מטריצה הפיכה ולכן למערכת הומוגנית לעיל קיים רק הפיתרון הטריוויאלי, $\alpha_1=\alpha_2=...=\alpha_k=0$ וכל המקדמים הם אפסים.
ולכן הסדרה $(u_1,...,u_k)$ בלתי־תלויה לינארית. $\square$

שאלה 2

יהיו $(V,q),(V',q')$ מרחבים ריבועיים ו־$f:V\to V'$ איזומטריה.
נוכיח כי אם (V,q) לא מנוון אז f חד־חד ערכית.

הוכחה: f איזומטריה כלומר לכל $v\in V$ מתקיים $q(v)=q'(f(v))$.
נניח ש־(V,q) לא מנוון ולכן $V^{\perp}=\{0_V\}$ כאשר הגדרנו

$$V^{\perp}:=\{w\in V\mid \forall v\in V,\ w\perp v\}$$

מכיוון ש־f העתקה לינארית מספיק שנראה $\ker f=\{0\}$.
נניח בשלילה שקיים $w\neq 0$ כך ש־$f(w)=0_{V'}$.
מנוסחאת הפולריזציה ומכך ש־f איזומטריה נקבל

$$g_{q'}(f(v),f(u))=g_q(v,u)$$

ובמקרה שלנו עם כל $v\in V$ מתקיים

$$g_q(w,v)=g_{q'}(f(w),f(v))=g_{q'}(0_{V'},f(v))=0$$

כלומר קיבלנו ש־$g_q(w,v)=0$ לכל $v\in V$ כלומר $w\in V^{\perp}$ אבל הנחנו ש־$V^{\perp}=\{0\}$ ו־$w\neq 0$ וזאת סתירה. אז f חד־חד ערכית. $\square$

שאלה 3

נביא דוגמה למרחבים ריבועיים $(V,q),(V',q')$ ואיזומטריה $f:V\to V'$ שאיננה חד־חד ערכית.

הוכחה: מהשאלה הקודמת נובע שהדוגמה חייבת להיות על מרחב מנוון.
ניקח $V=\mathbb{R}^2, V'=\mathbb{R}$ עם התבניות

$$q(x,y)=x^2 \qquad q'(x)=x^2$$

ונגדיר את $f:\mathbb{R}^2\to\mathbb{R}$ על־ידי $f(x,y)=x$.
עלינו להראות שהיא איזומטריה אז נבחר $v=(x,y)$, עלינו להראות ש־$q'(f(v))=q(v)$, ואכן

$$q'(f(v))=q'(x)=x^2=q(x,y)$$

וברור ש־f לא חד־חד ערכית שכן

$$\ker f=\{(x,y)\in\mathbb{R}^2 \mid f(x,y)=0\}=\{(0,y)\mid y\in\mathbb{R}\}$$

אז עבור הוקטורים $u=(0,1)$ ו־$w=(0,2)$ הם כמובן וקטורים שונים זה מזה אבל

$$f(0,1)=0=f(0,2)$$

$\square$

שאלה 4

יהיו (V,q) מרחב ריבועי ו־U,W תתי־מרחבים של V כך ש־$V=U\oplus^{\perp}W$. נוכיח כי (V,q) לא מנוון אם ורק אם $(U,q|_U),(W,q|_W)$ לא מנוונים.

הוכחה: תחת תנאי השאלה הגדרנו $V=U\oplus^{\perp}W$ כאשר לכל $u\in U,w\in W$ מתקיים $u\perp w$ $(\star)$.

$\Longleftarrow$ נניח ש־(V,q) לא מנוון ולכן $V^{\perp}=\{0_V\}$ ונראה ש־$(U,q|_U)$ לא מנוון (ההוכחה עבור $(W,q|_W)$ זהה):

יהי $u\in U^{\perp}$ (וקטור ב־U שמאונך לכל איברי U).

מכך ש־$V=U\oplus^{\perp}W$ נובע שכל $v\in V$ ניתן לכתיבה על־ידי $v=u'+w$ כאשר $u'\in U,w\in W$.

נסתכל על g_q התבנית הבילנארית הסימטרית של q ומהלינאריות נקבל

$$g_q(u,v)=g_q(u,u'+w)=g_q(u,u')+g_q(u,w)$$

אבל מכיוון ש־u מאונך לכל וקטור ב־U נקבל ש־$g_q(u,u')=0$ ומ־$(\star)$ נקבל שגם $g_q(u,w)=0$ כלומר $g_q(u,v)=0$ לכל $v\in V$ ולכן $u\in V^{\perp}$.

מהיות V לא מנוון נובע כי בהכרח $u=0$ ולכן $U^{\perp}=\{0\}$ ו־$(U,q|_U)$ מנוון.

$\Longrightarrow$ נניח ש־$(U,q|_U),(W,q|_W)$ לא מנוונים, יהי $v\in V^{\perp}$ ונרצה להראות ש־$v=0$.

מכך ש־$V=U\oplus^{\perp}W$ נובע שקיימים $u\in U,w\in W$ כך ש־$v=u+w$.

מכך ש־$v\in V^{\perp}$ נובע שבפרט לכל $u'\in U$ מתקיים

$$g_q(v,u')=g_q(u+w,u')=g_q(u,u')+g_q(w,u')=0$$

שכן $W\perp U$ ולכן גם המחובר הימני אפס, כלומר $g_q(u,u')=0$ לכל $u\in U$ ובפרט $u\in U^{\perp}$.

אבל הנחנו ש־U לא מנוון ולכן $u=0$.

מתהליך זהה נקבל ש־$w=0$ ולכן $v=u+w=0+0=0$ ו־V לא מנוון. $\square$

שאלה 5

נתונים שדה $\mathbb{F}$ ומטריצות $A, B \in M_n(\mathbb{F})$ החופפות זו לזו, נוכיח כי $\operatorname{rank} A = \operatorname{rank} B$.

הוכחה: מכך ש־A, B חופפות נובע שקיימת $P \in M_n(\mathbb{F})$ הפיכה כך ש־$B = P^t AP$.
בלינארית 1 ראינו שאם A מטריצה מסדר כלשהי נכפלת במטריצה P שהיא הפיכה מאותם סדרים מתקיים $\operatorname{rank}(AP) = \operatorname{rank}(A)$ ולכן מתקיים

$$\operatorname{rank}(B) = \operatorname{rank}(P^t AP) = \operatorname{rank}(AP) = \operatorname{rank}(A)$$

$\square$

שאלה 6

יהיו (V,q) מרחב ריבועי ו־$\mathcal{B}$ בסיס של V. נוכיח $\dim V = \operatorname{rank}\left[g_q\right]_{\mathcal{B}} + \dim V^{\perp}$.

הוכחה: מטענה שראינו בהרצאה נובע ש־(V,q) מנוון אם ורק אם $\left[g_q\right]_{\mathcal{B}}$ אינה הפיכה.
אם (V,q) לא מנוון נובע ש־$V^{\perp} = \{0_V\}$ ולכן $\left[g_q\right]_{\mathcal{B}}$ היא מדרגה מלאה ו־$\dim V^{\perp} = 0$ והטענה נובעת.
אחרת, (V,q) מנוון ולכן $V^{\perp} \neq \{0_V\}$ כלומר $\dim V^{\perp} > 0$ ו־$\left[g_q\right]_{\mathcal{B}}$ אינה הפיכה כלומר $\operatorname{rank}\left(\left[g_q\right]_{\mathcal{B}}\right) < \dim V$.
$w \in V^{\perp}$ אם ורק אם לכל $v \in V$ מתקיים $g(w,v) = 0$, כלומר $w^t\left[g_q\right]_{\mathcal{B}} v = 0$ לכל $v \in V$ וזה קורה אם ורק אם $w^t\left[g_q\right]_{\mathcal{B}} = 0$ ו־$\left[g_q\right]_{\mathcal{B}}$ כמובן סימטרית (כי היא מייצגת תבנית בילינארית סימטרית) ולכן התנאי קורה אם ורק אם $\left[g_q\right]_{\mathcal{B}} w = 0$.
לכן $w \in V^{\perp}$ אם ורק אם וקטור הקורדינאטות שלו נמצא במרחב האפס של המטריצה נסמנו ב־$\operatorname{null}\left(\left[g_q\right]_{\mathcal{B}}\right)$ ולכן $\dim V^{\perp} = \dim \operatorname{null}\left(\left[g_q\right]_{\mathcal{B}}\right)$.
ממשפט הדרגה באלגברה לינארית נקבל

$$\operatorname{rank}\left(\left[g_q\right]_{\mathcal{B}}\right) = n - \dim \operatorname{null}\left(\left[g_q\right]_{\mathcal{B}}\right) \Longrightarrow \operatorname{rank}\left(\left[g_q\right]_{\mathcal{B}}\right) + \dim \operatorname{null}\left(\left[g_q\right]_{\mathcal{B}}\right) = n \Longleftrightarrow \operatorname{rank}\left(\left[g_q\right]_{\mathcal{B}}\right) + \dim V^{\perp} = n$$

$\square$

שאלה 7

נמצא דוגמה למרחב ריבועי לא מנוון (V,q) ולתת־מרחב U של V כך ש־$(U,q|_U)$ מנוון.

הוכחה: כדי שמרחב יהיה לא מנוון המטריצה שלו צריכה להיות הפיכה וכדי שתת־מרחב שלו U יהיה מנוון צריך שיהיה בו ווקטור u שהוא מאונך לכל U.
נסתכל על המרחב $V=\mathbb{R}^2$ עם התבנית $q(x,y)=x^2-y^2$.
המטריצה המייצגת של התבנית בבסיס הסטנדרטי היא

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

וזו מטריצה הפיכה כי $\det(A)=-1$ ולכן (V,q) לא מנוון.
מצד שני, נבחר את הוקטור $u=(1,1)$, מתקיים $q(1,1)=0$ ו־$U=\mathrm{Span}\{(1,1)\}$.
כל וקטור ב־U הוא מהצורה αu עבור α סקלאר ומתקיים $g(u,\alpha u)=\alpha q(u)=0$ מנוסחת הפולריזציה, כלומר כל וקטור ב־U מאונך ל־u וכמובן ש־$u\in U$ ו־$u\neq 0$ ולכן $u\in U^{\perp}$ והמרחב מנוון.

$\square$

שאלה 8

יהיו (V,q) מרחב ריבועי ו־$u,w\in V$ כך ש־$q(u)=q(w)=0$. נסמן $U=\mathrm{Span}(u)$ ו־$W=\mathrm{Span}(u,w)$.

סעיף א'

נוכיח ש־$(U,q|_U)$ בהכרח מנוון.

הוכחה: נשים לב שמהגדרת הספאן נובע שכן $v\in U$ הוא מהצורה αu עבור α סקלר כלשהו ולכן

$$g(\alpha u,\beta u)=\alpha\beta g(u,u)=\alpha\beta q(u)=\alpha\beta 0=0$$

וזה בידיוק אומר שכל וקטור ב־U מאונך לכל וקטור אחר ב־U ולכן $U=U^\perp$ ובפרט $U^\perp\neq\{0_V\}$ (תחת ההנחה ש־$u\neq 0$). □

סעיף ב'

נוכיח ש־$(W,q|_W)$ לא בהכרח מנוון.

הוכחה: נסתכל על $V=\mathbb{R}^2$ עם $q(x,y)=xy$, אז המטריצה המייצגת היא $A=\begin{pmatrix}0&\frac{1}{2}\\\frac{1}{2}&0\end{pmatrix}$ ונבחר את הוקטורים $u=\begin{pmatrix}1\\0\end{pmatrix},v=\begin{pmatrix}0\\1\end{pmatrix}$.
אכן מתקיים $q(u)=0,q(v)=0$ ובפרט u,v פורשים את $\mathbb{R}^2$ אבל A מטריצה הפיכה ולכן משאלה 6 נובע ש־$W^\perp=\{0_V\}$ (כי ההפתרון היחיד למשוואה הוא הפיתרון הטריוויאלי). □

שאלה 9

יהיו V מרחב וקטורי מעל שדה $\mathbb{F}$ ו־$\ell_1, \ell_2 : V \to \mathbb{F}$ העתקות לינאריות.
נגדיר $q : V \to \mathbb{F}$ על־ידי $q(v) = \ell_1(v)\ell_2(v)$.

סעיף א'

נוכיח ש־q היא תבנית ריבועית.

הוכחה: עלינו להראות
1. לכל $v \in V$ ולכל סקלר $\alpha \in \mathbb{F}$ מתקיים $q(\alpha v) = \alpha^2 q(v)$
2. להראות קיום של תבנית בילנארית סימטרית

יהי $v \in V$ ו־$\alpha \in \mathbb{F}$, מתקיים מכך ש־ℓ_1, ℓ_2 העתקות לינאריות

$$q(\alpha v) = \ell_1(\alpha v)\ell_2(\alpha v) = \alpha\ell_1(v)\alpha\ell_2(v) = \alpha^2\ell_1(v)\ell_2(v) = \alpha^2 q(v)$$

נגדיר אם כך

$$g(u,v) = \frac{1}{2}(q(u+v) - q(u) - q(v))$$

היא כמובן סימטרית מכך ש־ℓ_1, ℓ_2 הן העתקות לינאריות ותכונות ההעתקה הלינארית.
נראה לינאריות ברכיב הראשון, גם זה נובע מהיות ℓ_1, ℓ_2 העתקות לינאריות

$$\begin{aligned}
g(\alpha u + w, v) &= \frac{1}{2}(q(\alpha u + w + v) - q(\alpha u + w) - q(v)) \\
&= \frac{1}{2}(\ell_1(\alpha u + w + v)\ell_2(\alpha u + w + v) - \ell_1(\alpha u + w)\ell_2(\alpha u + w) - \ell_1(v)\ell_2(v)) \\
&= \frac{1}{2}((\alpha\ell_1(u) + \ell_1(w) + \ell_1(v))(\alpha\ell_2(u) + \ell_2(w) + \ell_2(v)) - (\alpha\ell_1(u) + \ell_1(w))(\alpha\ell_2(u) + \ell_2(w)) - \ell_1(v)\ell_2(v)) \\
&\underset{(\star)}{=} \frac{1}{2}(\alpha a_1 + b_1 + c_1)(\alpha a_2 + b_2 + c_2) - (\alpha a_1 + b_1)(\alpha a_2 + b_2) - c_1 c_2 \\
&= \frac{1}{2}(\cancel{\alpha^2 a_1 a_2} + \cancel{\alpha a_1 b_2} + \alpha a_1 c_2 + \cancel{b_1 \alpha a_2} + \cancel{b_1 b_2} + b_1 c_2 + c_1 \alpha a_2 + c_1 b_2 + \cancel{c_1 c_2} - \cancel{\alpha^2 a_1 a_2} - \cancel{\alpha a_1 b_2} - \cancel{b_1 \alpha a_2} - \cancel{b_1 b_2} - \cancel{c_1 c_2}) \\
&= \frac{1}{2}(\alpha a_1 c_2 + b_1 c_2 + c_1 \alpha a_2 + c_1 b_2) \\
&= \frac{\alpha}{2}(a_1 c_2 + c_1 a_2) + \frac{1}{2}(b_1 c_2 + c_1 b_2) \\
&= \alpha q(u,v) + g(w,v)
\end{aligned}$$

כאשר $(\star)$ זה כי סימנו $a_i = \ell_i(u)$, $b_i = \ell_i(w)$ ו־$c_i = \ell_i(v)$ לפשטות.

□

סעיף ב'

נוכיח שאם $\dim V \geq 3$ אזי (V, q) מנוון.

הוכחה: נביט בגרעינים של שתי ההעתקות הליניאריות

$$U_1 = \ker(\ell_1) = \{v \in V \mid \ell_1(v) = 0\} \qquad U_2 = \ker(\ell_2) = \{v \in V \mid \ell_2(v) = 0\}$$

ℓ_1, ℓ_2 הן העתקות לינאריות לתוך שדה שמימדו 1 הרי ש־$\dim U_1 \geq \dim V - 1$ ו־$\dim U_2 \geq \dim V - 1$.
ממשפט המימד מתקיים

$$\dim(U_1 \cap U_2) = \dim U_1 + \dim U_2 - \dim(U_1 + U_2)$$

מכיוון ש־$\dim(U_1 + U_2) \leq \dim V$, נקבל

$$\dim(U_1 \cap U_2) \geq (\dim V - 1) + (\dim V - 1) - \dim V = \dim V - 2$$

מההנחה, $\dim V \geq 3$ ולכן $\dim(U_1 \cap U_2) \geq 3 - 2 = 1$.
מכאן שקיים ווקטור $w \neq 0$ כך ש־$w \in U_1 \cap U_2$, כלומר $\ell_1(w) = 0$, $\ell_2(w) = 0$.
נציב $\ell_1(w) = 0 = \ell_2(w)$ בהגדרת $q(w,v)$ לכל $v \in V$ ונקבל

$$g(w,v) = \frac{1}{2}(0 \cdot \ell_2(v) + 0 \cdot \ell_1(v)) = 0$$

קיבלנו ש־$w \neq 0$ ומאונך לכל $v \in V$, לכן $w \in V^\perp$ ולכן $V^\perp - \{0_V\} \neq \emptyset$ ולכן (V, q) מנוון. □

שאלה 10

יהי $\mathbb{F}$ שדה ותהיי תבנית ריבועית $q : \mathbb{F}^2 \to \mathbb{F}$ מוגדרת על־ידי

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

נוכיח כי $0 \in q\left(\mathbb{F}^2 \setminus \left\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right\}\right)$ אם ורק אם $-1 \in \left(\mathbb{F}_p^\times\right)^2$.

הוכחה: כפי שציינו בהרצאה, התנאי $0 \in q(\mathbb{F}^2 \setminus \{0\})$ שקול לקיום פתרון לא טריוויאלי למשוואה

$$x_1^2 + x_2^2 = 0 \Longrightarrow x_1^2 = -x_2^2$$

$\Longleftarrow$ נניח כי $0 \in q(\mathbb{F}^2 \setminus \{0\})$ ולכן קיימים $x_1, x_2 \in \mathbb{F}$ כך ש־ששניהם אינם אפסים כך ש־$x_1^2 + x_2^2 = 0$.
בלי הגבלת הכלליות, ברור כי $x_2 \neq 0$ כי אחרת זה יגרור $x_1^2 = 0$ כלומר $x_1 = 0$ וקיבלנו את וקטור האפס בסתירה להנחה, אז $x_2 \neq 0$.
מכך ש־$x_2 \neq 0$ נובע שקיים לו איבר הופכי, x_2^{-1} אז

$$x_1^2 + x_2^2 = 0 \Longleftrightarrow x_1^2 = -x_2^2 \Longleftrightarrow x_1^2\left(x_2^{-1}\right)^2 = -1 \Longleftrightarrow \left(x_1 x_2^{-1}\right)^2 = -1$$

אז אם נסמן $a = x_1 x_2^{-1}$ קיבלנו $a^2 = -1$ ואם $p \neq 2$ (שזאת לדעתי הנחה די הגיונית) נקבל גם $-1 \neq 0$ ולכן $-1 \in \left(\mathbb{F}_p^\times\right)^2$. $\square$

שאלה 11

תבנית ריבועית $q : \mathbb{F}_{11}^2 \to \mathbb{F}_{11}$ מוגדרת על־ידי

$$q\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 2x_1^2 - 3x_2^2$$

נמצא בסיס $\mathcal{B}$ של $\mathbb{F}_{11}^2$ כך ש־$[g_q]_{\mathcal{B}}$ תהיה בצורה הקנונית כאשר הנציג של $\mathbb{F}_{11}^\times \setminus (\mathbb{F}_{11}^\times)^2$ הוא -1.

פתרון: נפעל באופן דומה למה שמופיע במודל, עבור $\mathbb{F}_7$ הנציגים היו בין -3 ל־3 ולכן במקרה שלנו הם יהיו בין -5 ל־5, כלומר

$$\mathbb{F}_{11} = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$$

במקרה שלנו $2x^2$ האיבר הראשון בתבנית ו־$-3x^2$ האיבר השני בתבנית שכמובן מתקיים $8 \underset{\text{mod } 11}{\equiv} -3$.
נבנה את הטבלה בהתאם

$\boldsymbol{x}$	-5	-4	-3	-2	-1	0	1	2	3	4	5
$\boldsymbol{x^2}$	3	5	-2	4	1	0	1	4	-2	5	3
$\boldsymbol{2x^2}$	-5	-1	-4	-3	2	0	2	-3	-4	-1	-5
$\boldsymbol{-3x^2}$	2	-4	-5	-1	-3	0	-3	-1	-5	-4	2
$\boldsymbol{x^{-1}}$	-2	-3	-4	-6	-1	0	1	6	4	3	2

נשים לב שהשורה השנייה זאת קבוצת הריבועים $\{1, 3, 4, 5, 9\} = \{1, 3, 4, 5, -2\}$ ו־$10 \underset{\text{mod } 11}{\equiv} (-1)$ הוא נציג של הלא ריבועים כי הוא לא בשורה.
עלינו למצוא $(x_1, x_2) \in \mathbb{F}_{11}^2$ כך ש־$2x_1^2 - 3x_2^2 = q(x_1, x_2) = 1$.
ניקח את $x_1 = 1$ ולכן $2x_1 = 2$ ואם נבחר $x_2 = 2$ נקבל $-3x_2 = -1$ ואכן $q(x_1, x_2) = 1$.
אז $\mathcal{C} = ((1, 2), (0, 1))$ מהווים בסיס של $\mathbb{F}_{11}^2$.
מתקיים $q(0, 1) = -3$ ו־$g_q((1, 2), (0, 1)) = -6 \underset{\text{mod } 11}{\equiv} 5$ (מנוסחת הפולריזציה).
לכן

$$[g_q]_{\mathcal{C}} = \begin{pmatrix} 1 & 5 \\ 5 & -3 \end{pmatrix}$$

נמצא בסיס אורתוגונלי של $\mathbb{F}_{11}^2$ המכיל את $(1, 2)$

$$\frac{\begin{pmatrix} 1 & 5 \\ 5 & -3 \end{pmatrix}}{\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}} \xrightarrow{R_2 \mapsto R_2 - 5R_1} \frac{\begin{pmatrix} 1 & 5 \\ 0 & 5 \end{pmatrix}}{\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}} \xrightarrow{C_2 - 5C_1} \frac{\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}}{\begin{pmatrix} 1 & -5 \\ 2 & 2 \end{pmatrix}}$$

ולכן עבור $\mathcal{D} = ((1, 2), (-5, 2))$ מתקיים

$$[g_q]_{\mathcal{D}} = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$$

נמצא בסיס אורתוגונלי של $\mathbb{F}_{11}^2$ שמכיל את $(1, 2)$ כך שהאיבר השני באלכסון של מטריצת גרם ביחס אליו יהיה שייך ל־$\{1, -1\}$.
בטבלה לעיל רואים ש־$4^2 = 5$ ולכן 5 הוא ריבוע וכדי להפוך אותו ל־1 מהשורה הרביעית עלינו לכפול את הווקטור השני ב־4^{-1} ונקבל שצריך לכפול את הוקטור השני ב־3, כלומר

$$3 \cdot (-5, 2) = (-15, 6) \underset{\text{mod } 11}{\equiv} (-4, -5)$$

ולכן $\mathcal{B} = ((1, 2), (-4, -5))$ והמטריצה המייצגת ביחס אליו היא I_2. $\square$

שאלה 12

תבנית ריבועית $q:\mathbb{F}_7^3\to\mathbb{F}_7$ מוגדרת על־ידי

$$q\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}=3x_1^2-2x_2^2-2x_3^2$$

נמצא בסיס $\mathcal{B}$ של $\mathbb{F}_7^3$ כך ש־$\left[g_q\right]_{\mathcal{B}}$ תהיה בצורה הקנונית כאשר הנציג של $\mathbb{F}_7^\times\setminus\left(\mathbb{F}_7^\times\right)^2$ הוא -1.

פתרון: בהתאם למסמך מהמודל $\mathbb{F}_7=\{-3,-2,-1,0,1,2,3\}$, נרחיב את הטבלה משם

$\boldsymbol{x}$	-3	-2	-1	0	1	2	3
$\boldsymbol{x^2}$	2	-3	1	0	1	-3	2
$\boldsymbol{-x^2}$	-2	3	-1	0	-1	3	-2
$\boldsymbol{3x^2}$	-1	-2	3	0	3	-2	-1
$\boldsymbol{-2x^2}$	3	-1	-2	0	-2	-1	3
$\boldsymbol{x^{-1}}$	-1	0	1	6	4	3	2

אז קבוצת הריבועים הפעם היא $\{1,2,4\}=\{1,2,-3\}$ וקבוצת הלא ריבועים היא $\{-1,-2,3\}$ עם הנציג שלנו -1.
אנחנו שוב צריכים למצוא וקטורים שיניבו 1 עם התבנית הריבועית הנתונה: מהשורה הרביעית נקבל $x_1=1$ מניב 3 ואם נבחר $x_2=2$ נקבל

$$q\begin{pmatrix}1\\1\\0\end{pmatrix}=3-2-0=1$$

נקבע את הוקטור $u_1(1,1,0)$ ונשלים לבסיס וניקח $\mathcal{C}=((1,1,0),(0,1,0),(0,0,1))$.
נחשב את המטריצה המייצגת $\left[g_q\right]_{\mathcal{C}}$ לפי הנוסחה $g_q(u,v,w)=3u_1v_1-2u_2v_2-2u_3v_3$ ונקבל

$$\begin{cases}a_{11}=q(1,1,0)=1\\a_{22}=q(0,1,0)=-2=a_{33}=q(0,0,1)\\a_{12}=g_q((1,1,0),(0,1,0))=3\cdot1-2\cdot1=-2\\a_{13}=0=a_{23}\end{cases}$$

ולכן

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

נחפוף

$$\underbrace{\begin{pmatrix}1&-2&0\\-2&-2&0\\0&0&-2\end{pmatrix}}_{\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}}\xrightarrow{R_2\mapsto R_2+2R_1}\underbrace{\begin{pmatrix}1&-2&0\\0&-1&0\\0&0&-2\end{pmatrix}}_{\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}}\xrightarrow{C_2\mapsto C_2+2C_1}\underbrace{\begin{pmatrix}1&0&0\\0&-1&0\\0&0&-2\end{pmatrix}}_{\begin{pmatrix}1&2&0\\1&3&0\\0&0&1\end{pmatrix}}$$

אז קיבלנו מטריצה אלכסונית $\operatorname{diag}(1,1,-2)$ והבסיס האורתוגונלי $\mathcal{D}=((1,1,0),(2,3,0),(0,0,1))$.
נשאר לנרמל ואנחנו רוצים להפוך את ה־-2 ל־±1: מהטבלה לעיל -2 ניתן לראות ש־-2 הוא לא ריבוע ב־$\mathbb{F}_7$, אז נרצה להפוך אותו ל־-1 אנחנו מחפשים α כך שיתקיים

$$-2\alpha^2\underset{\text{mod }7}{\equiv}-1\iff2\alpha^2\underset{\text{mod }7}{\equiv}1$$

מהטבלה לעיל מתקיים $2\cdot2^2=2\cdot4=8\underset{\text{mod }7}{\equiv}1$ ולכן הפעולה על הוקטור ה־3 תהיה לכפול ב־2 כלומר $u_3=2\cdot(0,0,1)=(0,0,2)$.
אז הבסיס הקנוני הוא $\mathcal{B}=((1,1,0),(2,3,0),(0,0,2))$ והמטריצה המייצגת ביחס אליו היא

$$\left[g_q\right]_{\mathcal{B}}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&-1\end{pmatrix}$$

$\square$