אלגברה לינארית 1א ~ תרגיל בית 3

שחר פרץ

14 באפריל 2025

.... (1) ....

יהיו $(A \mid a)$ ו־$(B \mid b)$ מערכות משוואות מסדר $m \times n$ מעל $\mathbb{R}$. נוכיח שלא ייתכן שיש בדיוק 10 פתרונות למשוואות.

הוכחה. x פתרון משותף לשני המשוואות אמ"מ $Ax = a \wedge Bx = b$. נסמן ב־$\begin{pmatrix} A \\ B \end{pmatrix}$ את המטריצה מסדר $2m \times n$ שמתחילה ב־A ומתחתיה B (מטריצת הבלוקים). באופן דומה, $\begin{pmatrix} a \\ b \end{pmatrix}$ תהיה המטריצה/וקטור מגודל $2m \times 1$ הכולל פעמיים את איברי x. נבחין כי מתקיימת השקילות $\begin{pmatrix} A \\ B \end{pmatrix} x = \begin{pmatrix} a \\ b \end{pmatrix} \iff (Ax = a \wedge Bx = b)$. ממשפט, למערכת המשוואות הזו יש או פתרון יחיד, או 0 פתרונות, או לפחות $|\mathbb{F}|$ פתרונות. משום ש־$10 \neq 0, 1$, אז $|\mathbb{F}| \geq 10$, אך $\mathbb{F} = \mathbb{R}$ ו־$2^{\aleph_0} \ngeq 10$. לכן לא ייתכן שיש למערכת המשוואות הזו 10 פתרונות עבור x־ים שונים, ומאקסיומת ההקפיות (שוויון קבוצות) $\text{sols}\begin{pmatrix} A \\ B \end{pmatrix} = \{Ax = a \wedge Bx = b \mid x \in \mathbb{R}\}$ וממשפט לשוויון עוצמות $\left|\text{sols}\begin{pmatrix} A \\ B \end{pmatrix}\right| = |\{Ax = a \wedge Bx = b \mid x \in \mathbb{R}\}|$ ובפרט לא שווה ל־10, וסה"כ למערכות המשוואות $(A \mid a), (B \mid b)$ אין 10 פתרונות משותפים. ■

.... (2) ....

תהי $(A \mid 0)$ מערכת משוואות, ו־$\bar{c},\ \bar{d}$ פתרונות. צ.ל. $\bar{c} + \bar{d}$ פתרון.

הוכחה. ידוע $\bar{c}, \bar{d}$ פתרונות אמ"מ $A\bar{c} = A\bar{d} = 0$. נחבר את המשוואות ונקבל $A\bar{c} + A\bar{d} = 0$. מדיסטריבוטיביות כפל מטריצה בוקטור/מטריצה, סה"כ $A(\bar{c} + \bar{d}) = 0$, כלומר $\bar{c} + \bar{d}$ פתרון כדרוש.

הוכחה לדיסטרבוטיביות בה השתמשתי. נסמן ב־C_i^A את העמודה ה־i של המטריצה ה־A.

$$\forall \bar{c}, \bar{d} \in \mathbb{F}^n,\ A \in M_{m\times n}(\mathbb{F})\colon\ A\bar{c} + A\bar{d} = \sum_{i=1}^{n} C_i^A \bar{c}_i + \sum_{i=1}^{n} C_i^A \bar{d}_i = \sum_{i=1}^{n} C_i^A \underbrace{(\bar{c}_i + \bar{d}_i)}_{(\bar{c}+\bar{d})_i} = A(\bar{c} + \bar{d}) \quad \top$$

■

.... (3) ....

נסמן:

$$\mathcal{A} = \left\{ \begin{pmatrix} 3 - 2s \\ 1 - s - t \\ 2t \end{pmatrix} \mid s, t \in \mathbb{R} \right\}$$

(א) נראה כי לא קיימת מערכת משוואות הומוגנית ש־$\mathcal{A}$ קבוצת הפתרונות שלה. לשם כך, נוכיח למה – לכל A מטריצה, $\ker A := \{x \in \mathbb{R}^3 \colon Ax = 0\}$ הוא תמ"ו של $\mathbb{R}^3$.

הוכחה.

- נוכיח קיום איבר 0 – עבור $x = 0$ מתקיים $Ax = A0 = 0$ (מהגדרת כפל מטריצה בוקטור).
- נוכיח סגירות לחיבור – לכל $x, y \in \ker A$ מתקיים $Ax = Ay = 0$ ומשאלה 2 מתקיים $A(x + y) = 0$ כלומר $x + y \in \ker A$ מעקרון ההפרדה.
- נוכיח סגירות לכפל בסקלר – לכל $x \in \ker A,\ \lambda \in \mathbb{R}$ מתקיים $Ax = 0$ ולכן $A(\lambda x) = \lambda(Ax) = \lambda 0 = 0$ וסה"כ $\lambda x \in \ker A$ כדרוש.

■

נחזור לטענה:

הוכחה. נניח בשלילה ש־$\mathcal{A}$ קבוצת הפתרונות של איזושהי מערכת משוואות הומוגנית $(A \mid 0)$. אז מהגדרה $\mathcal{A} = \ker A$. לכן $\mathcal{A}$ מ"ו כלומר $0 \in \mathcal{A}$. נפתור מערכת משוואות:

$$\begin{cases} 3-2s=0 & \implies 3-2\cdot 1 = 3-2 = 1 = 0 \\ 1-s-t=0 & \implies 1-s=0 \implies s=1 \\ 2t=0 & \implies t=0 \end{cases}$$

סה"כ $1=0$ וזו סתירה. ■

(ב) עתה נראה ש־$\mathcal{A}\cup 0_V$ כאשר 0_V וקטור ה־0 ב־$\mathbb{R}^3$, לא קיים בעבורה מערכת משוואות הומוגנית שזו קבוצת הפתרונות שלה.

הוכחה. עבור $s=t=0$, ניכר כי $(3,1,2)\in\mathcal{A}$. מסגירות, $0.5(2,1,3)\in\mathcal{A}$. לכן:

$$\begin{cases} 3-2s=1.5 \implies 3-2\cdot 0 = 3 = 1.5 \\ 1-s-t=0.5 \implies 1-s-0.5=0.5 \implies s=0 \\ 2t=1 \implies t=0.5 \end{cases}$$

סה"כ $3=1.5$ וזו סתירה. ■

. . . . (4) . . . .

כבר בתרגיל הבית הקודם כתבתי את קבוצת הפתרונות המתאימה לכל מערכת משוואות. אעתיק שוב לתרגיל הבית הזה:

$$(4a)\quad \left\{\begin{pmatrix} 15+5x_3+3x_4 \\ -19-7x_3-5x_4 \\ x_3 \\ x_4 \end{pmatrix} \mid x_3,x_4\in\mathbb{R}\right\}$$

$$(4b)\quad \left\{\begin{pmatrix} -\frac{6}{7} \\ \frac{1}{7} \\ \frac{15}{7} \\ 0 \end{pmatrix}\right\}$$

$$(4c)\quad \left\{\begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}\right\}$$

$$(5a)\quad \left\{\begin{pmatrix} -2x_4 \\ 1-2x_3 \\ x_3 \\ x_4 \end{pmatrix} \mid x_3,x_4\in\mathbb{F}_5\right\}$$

$$(5b)\quad \left\{\begin{pmatrix} 0 \\ 1-2x_3-4x_4 \\ x_3 \\ x_4 \end{pmatrix} \mid x_3,x_4\in\mathbb{F}_7\right\}$$

$$(5c)\quad \left\{\begin{pmatrix} 0 \\ 1-x_4-x_5 \\ 1-x_4 \\ x_4 \\ x_5 \end{pmatrix} \mid x_4,x_5\in\{0,1\}\right\}$$

(5)

נפתור את מערכת המשוואות הבאה מעל $\mathbb{Z}_5$:

$$\begin{cases} x+y+z=2 \\ 3x+y+2z=1 \\ x+3z=4 \end{cases} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & 2 \\ 3 & 1 & 2 & 1 \\ 1 & 0 & 3 & 4 \end{pmatrix} \xrightarrow[R_3\to R_3-R_1]{R_2\to R_2-3R_1} \begin{pmatrix} 1 & 1 & 1 & 2 \\ 0 & 3 & 4 & 0 \\ 0 & 4 & 2 & 2 \end{pmatrix}$$

$$\xrightarrow{R_2\to 2R_2} \begin{pmatrix} 1 & 1 & 1 & 2 \\ 0 & 1 & 3 & 0 \\ 0 & 4 & 2 & 2 \end{pmatrix} \xrightarrow{R_3\to R_3-4R_2} \begin{pmatrix} 1 & 1 & 1 & 2 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

מהשורה התחתונה, בהנחה בשלילה שקיים פתרון (x,y,z), נבחין בשוויון $0x+0y+0z=2$. ממשפטים על שדות $0=2$, וזו סתירה. כלומר – לא קיים פתרון למערכת המשוואות. סה"כ קבוצת הפתרונות היא $\varnothing$.

(6)

בעבור p ראשוני כלשהו, נתבונן בשדה $\mathbb{Z}_p$. נתבונן במערכת המשוואות הלינארית הבאה מעל $\mathbb{Z}_p$:

$$\left\{x_1+x_2+\cdots+x_{k+1}=0\right.$$

אזי, מערכת המשוואות לעיל תהיה בעלת קבוצת הפתרונות:

$$(x_1,x_2,\ldots x_{k+1}) \sim \left\{\left(-\sum_{i=1}^{p}\alpha_i,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k\right) \mid \alpha_1\cdots\alpha_p\in\mathbb{Z}_p\right\} =: \mathcal{S}$$

נבחין כי $|\mathcal{S}| = \underbrace{|\mathbb{Z}_p|\cdot|\mathbb{Z}_p|\cdots|\mathbb{Z}_p|}_{k\ \text{times}}$, כלומר למערכת המשוואות יש $p^k=|\mathcal{S}|$ פתרונות.

בפרט, בעבור $p=3,k=4$ מצאנו מערכת משוואות עם 81 פתרונות.

עתה, נראה אי־קיום מערכת משוואות לינארית עם 36 פתרונות. בעבור מערכת משוואות לינארית $(A\mid b)$ כלשהי, מצורתה המדורגת נבחין כי גודל קבוצת הפתרונות של $(A\mid b)$הוא $|\mathbb{F}|^k$ כאשר k מספר האיברים החופשיים. נניח בשלילה כי קיימת מערכת משוואות לינארית עם 36 פתרונות, אזי משום ש־$k=2$ השלם היחידי בעבורו קיים $a\in\mathbb{N}$ כך ש־$a^k=36$, בהכרח $|\mathbb{F}|^2=36$ מהמשפט הקודם. נוציא שורש, נקבל $|\mathbb{F}|=\pm6$. אם $|\mathbb{F}|=-6$ סתירה להגדרת עוצמה, ואם $|\mathbb{F}|=6$ אז $3,2$ מחלקים ראשוניים זרים של 6 ולכן הוא אינו מהצורה p^n בעבור p ראשוני ו־n טבעי, בניגוד למשפט הנתון כחלק מסעיף זה. לכן לא קיים $\mathbb{F}$ מתאים, ונסיק ש

(7)

יהי $\mathbb{F}$ שדה סופי.

(א) נראה קיום $0<m\in\mathbb{N}$ כך ש־$\underbrace{1+1+\cdots+1}_{m\,\text{times}}=0$, נקראו המציין של השדה ונסמנו $\operatorname{char}\mathbb{F}$

הוכחה. יהי סופי. נגדיר את הפונקציה $f\colon\mathbb{N}\to\mathbb{F}$ לפי $f(n)=\underbrace{1+1+\cdots+1}_{n\ \text{times}}$ (במקרה הריק $f(0_\mathbb{N})=0_\mathbb{F}$). נסמן $f(n)=n_\mathbb{F}$.

משום ש־$\mathbb{F}$ סופי אז $|\mathbb{F}|<|\mathbb{N}|$ וממשפטים על עוצמות f איננה חח"ע, ולכן קיימים שני מספרים $n,m\in\mathbb{F}$ שונים כך ש־$n_\mathbb{F}=m_\mathbb{F}$. בה"כ $n>m$, אז $n-m>0$ ולכן $(n-m)_\mathbb{F}\in\mathbb{F}$. קיבלנו $(n-m)_\mathbb{F}=n_\mathbb{F}-m_\mathbb{F}=n_\mathbb{F}-n_\mathbb{F}=0$, משמע:

$$\underbrace{1+1+\cdots+1}_{n-m\,\text{times}}=0_\mathbb{F}$$

ולכן לפי הגדרה $\operatorname{char}\mathbb{F}$ קיים, שכן $n-m=\operatorname{char}\mathbb{F}$ או ש־$0<\operatorname{char}\mathbb{F}<n-m$ מהגדרת מינימליות. ■

(ב) צ.ל. $\operatorname{char}\mathbb{F}$ ראשוני.

הוכחה. יהי $\mathbb{F}$ שדה סופי. נראה ש־$p=:\operatorname{char}\mathbb{F}$ ראשוני. נניח בשלילה שהוא לא ראשוני, אזי הוא פריק מהלמה של אוקלידס, ולכן קיימים n,m טבעיים כך ש־$nm=p$ וכן $n,m\notin\{p,1\}$. בגלל ש־$n,m<p$ ומהיות p המינימלי כך ש־$p_\mathbb{F}=0_\mathbb{F}$ (בסימונים מהסעיף הקודם), אז $n_\mathbb{F},m_\mathbb{F}\neq0_\mathbb{F}$. קל לראות ש־$0_\mathbb{F}=p_\mathbb{F}=(nm)_\mathbb{F}=n_\mathbb{F}m_\mathbb{F}$, וממשפט שראינו $n_\mathbb{F}=0_\mathbb{F}\vee m_\mathbb{F}=0_\mathbb{F}$, בסתירה לכך ש־$n_\mathbb{F},m_\mathbb{F}\neq0_\mathbb{F}$. סה"כ הנחת השלילה נסתרה ולכן p ראשוני כדרוש. ■

(ג) נראה כי־$\mathbb{Z}_2 0$ איננו שדה.

הוכחה. ניעזר בסימון $a_{\mathbb{F}}$ מהסעיף הראשון. נראה כי בעבור $\mathbb{Z}_p$ כלשהו, $\operatorname{char}\mathbb{Z}_p = p$. נתחיל מלהוכיח ש־$p_{\mathbb{F}} = 0$:

$$p_{\mathbb{F}} = (\underbrace{1 + 1 + \cdots + 1}_{p \text{ times}}) \bmod p = p \bmod p = 0$$

נראה מינימליות. נניח בשלילה קיום $0 \neq n < p$ כך ש־$n_{\mathbb{F}} = 0$, אזי $n \bmod p = 0$, ולכן $p \mid n$. סה"כ נסיק $n \in \{kp \mid k \in \mathbb{Z}\}$, ומכיוון ש־$0 < n < p$ נבחין בסתירה שכן לא קיים k מתאים.

סה"כ, $\operatorname{char}\mathbb{Z}_p = p$. בפרט, $\operatorname{char}\mathbb{Z}_{20} = 20$ ומכיוון ש־20 איננו ראשוני, מהסעיף הקודם $\mathbb{Z}_{20}$ איננו שדה – כדרוש. ■

. . . .