לינארית 1

שחר פרץ

6 בנובמבר 2024

ABOUT . . . (1)

בן 29, בוגר ארזים. סטודנט לפסיגולוגיה. מייל: kligman@mail.tau.ac.il. עדיף לפנות למתרגל לשאלות.

INTRO . . . (2)

הקורס מתעסק במשוואות ליניאריות, כמו שהוצגו בשיעור הקודם. משוואות ליניאריות הן כמעט המשוואות היחידות שכבני אדם נוכל לפתור באופן פשוט.

יש מגוון אובייקטים שניתנים לתיאור באמצעות אלגברה ליניארית. לדוגמה, מישור בטוך מרחב תלת ממדי. דדוקציה משאלות כאלו למשוואות ליניאריות היא כלי חזק.

ניתן לתאר מערכת משוואות ליניאריות באמצעות מטרציות (מעין טבלה). אפילו תיאור נגזרות של פונקציה ממרחב גבוהה מתוארות באמצעות אלגברה ליניארית.

תיאור כללי של הקורס:

1. שדות (בערך שליש מהקרוס)
2. מרחב וקטורי
3. העתקות ליניאריות (בהרחבה)
4. מטרציות, בהקשר למבנים שראינו קודם
5. בקורסים מתדמים נראה אובייקטים נוספים

LINEAR EUQTIONS SYSTEMS . . . (3)

נתבונן במשוואה הבאה:

$$a_1x_1 + a_2x_2 = d_1$$

שימו לב: בתורת הקבוצות a_1, a_2 שייכים לקבוצה כלשהי. נבחר $a_1, a_2 \in A$. יהיה גם צורך להגדיר פעולת כפל בין x_1 ל־a_1. הוא יהיה פונקציה $f(a_1, x_2) \mapsto ?$. נצטרך פעולת חיבור גם. לאוסף הפעולות האלא נקרא שדה.

הרבה מהקושי הוא הפורמליות והדקדקנות. בניית דברים מאקסיומות יכולה להיות מתעתעת. זה רלוונטי בלמידה, בש"ב ובמבחנים. לפעמים, השאלה צריכה להיות שאלת פרמול בעקרה. לכן, מומלץ לפתור דברים באופן פורמלי – זה יעזור להצלחה בקורס, ועוד יותר יעזור בעתיד.

FIELDS . . . (4)

4.1 הגדרה

נגדיר באופן פרמלי מה זה שדה.

הגדרה. F קבוצה, וקיימת $a\colon F \times F \to F$ פונקציה הקרויה חיבור, וקיימת $m\colon F \times F \to F$ פונקציה הקרויה כפל, נאמר ש־F עם a, m שדה אם:

סימון. $a(x, y) = x + y,\ m(x, y) = x \cdot y$

1. איבר ניטרלי לחיבור: $\exists x \in F. \forall y \in F. y + x = y$

   סימון. האיבר ב־0 או 0_F. נקרא לו איבר האפס.
2. אסוציאטיביות: $\forall x, y, z \in F : (x + y) + z = x + (y + z)$
3. חילופיות של חיבור: $\forall x, \in F : x + y = y + x$
4. קיום איבר נגדי: $\forall x \in F : \exists y \in F. x + y = y + x = 0_F$

   סימון. איבר נגדי של x הוא $(-x)$.

5. ניטרלי לכפל: $\exists x \in F : \forall y \in F : xy = yx = y$
6. אסוציאטיביות של כפל: $\forall x, y, z \in F : (xy) \cdot z = x \cdot (yz)$
7. קיום הופכי: $\forall 0 \neq x \in F \exists y \in F : .xy = yx = 1$
סימון. הופכי של x יהיה x^{-1}. נסמן גם עם חילוק (כלומר $\frac{1}{x}$).
8. חילופיות כפל. $\forall x, y \in F : xy = yx$.
9. דיסטרביוטיביות: $\forall x, y, z \in F : x(y + z) = xy + xz$
10. $1_F \neq 0_F$

סימון. איבר בשדה יקרא סקלר.

4.2 דוגמאות

4.2.1 הרציונליים

נבתונן ב־$\mathbb{Q}$. הרציונלים, הם שדה. קבוצתם היא בערך:

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \neq 0 \in \mathbb{Z} \right\}$$

טענה. $\mathbb{Q}$ הוא השדה המינימלי המכיל את $\mathbb{Z}$. משהו בסגנון, ניקח $a \in \mathbb{Q}$, נסמנו $\frac{x}{y}$ ובהתאם השדה שלנו יעיל את $\frac{x}{y}$ כי ניקח את $x \in \mathbb{Z}$, $0 \neq y \in \mathbb{Z}$, ונייצר $x \cdot y^{-1}$. שדה מינימלי לא הוגדר פורמלית בקורס הזה.

שימו לב – ב־$\mathbb{Q}$ ההצגה היא לא יחידה (ומשפיע על חוסר הפורמליות בנתון לעיל). הרי $\frac{4}{6} = \frac{2}{3}$.

4.2.2 הממשיים

גם $\mathbb{R}$ הם שדה. גם בשדה הזה הסימון לא יחיד. $1 = 0.99999...$ (כי ככה מגדירים באנליזה). בנייה פורמלית בלי אקסיומת החסם העליון – ען=ם ארז.

4.2.3 המרוכבים

גם $\mathbb{C}$ הם שדה. הם סגורים אלגברית, כלומר לכל משוואה יש פתרון. נזהה את $\mathbb{R}^2 = \mathbb{C}^2$. נסמן את $(1, 0)$ אם איבר היחידה, ונגדיר:

$$(x, y) + (z, w) = (z + x, y + w),\ (x, z) \cdot (z, w) = (xz - yw, xw + yz)$$

נסמן $(x, y) = x + yi,\ (0, 1) = i$. נקבל $i^2 = -1$, ואם נסמן $\bar{z} = x - iy$ וגם נסמן $|z| = \sqrt{z \cdot \bar{z}}$ נקבל ש־$z^{-1} = |z| = \frac{z}{|z|^2} - \frac{x - iy}{x^2 + y^2}$. למעשה, דרך להראות ש־$\mathbb{C}$ הוא שדה, בפרט נרצה למצוא את ההופכי.

משפט. המשפט היסודי של האלגברה (ראה עברי) – בהינתן פולינום מרוכב עם מקדמים מרוכבים, נסמן $f(x) = a_n x^n \dots a_0$, אז $\exists z \in \mathbb{C} : f(z) = 0$.

4.2.4 תתי קבוצות של המרוכבים

מתברר, ש־$\mathbb{Q} \cup \{i\}$ הוא גם שדה. אם זאת $\mathbb{R}_{>0}$ הוא אינו שדה. ניקח קבוצה $F = \{a, b\}$ ונגדיר טבלת כפל וחיבור:

$\cdot$	a	b
a	a	a
b	a	b

$+$	a	b
a	a	b
b	b	a

ונגדיר $0_F = a, q_F = b$ אז $\mathbb{F} = \{0, 1\}$ שדה.

4.3 טענות על שדות

משפטים.

- ניטרלי לחיבור הוא יחיד.
- $\forall a \in F . 0 \cdot a = 0$
- ניטרלי לכפל הוא יחיד.
- לכל $a \in F$ האיבר הנגדי יחיד וגם $-a = (-1) \cdot a$.
- לכל $0 \neq a \in F$ הופכי יחיד.

הוכחה (1). נניח בשלילה $x, y \in F$ כך ששניהם ניטרליים לחיבור, ונראה $x = y$. אז:

$$x = x + y = y$$

כי y ניטרלי לחיבור, וכי x ניטרלי לחיבור. סתירה. ■

הוכחה (2). יהי $a \in F$, נראה $0 \cdot a = 0$. ואכן:

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$$

נוסיף $-(0a)$ לשני הצדדים. ומכאן, $0 = 0a$. (חוקי מח"ע) ■

הוכחה (3). יהי $a \in F$ וניקח $b, c \in F$.

$$b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c$$

■

הוכחה (4). נראה כי $(-1) \cdot a$ הוא נגדי ל־a, ולכן $-a = (-1) \cdot a$, כי זה הסימון.

$$a + (-1) \cdot a = a \cdot (1 + (-1)) = a \cdot 0 = 0$$

■

הוכחה (5). יהי $0 \neq a \in F$, וניקח $b, c \in F$ הופכיים.

$$b = b \cdot (a \cdot c) = (b \cdot a) \cdot c = c$$

■

4.4 טענות נוספות

יהיו $a, b, c, d \in F$ כאשר F שדה.

1. $ab = 0 \iff (b = 0 \lor a = 0)$
2. $a + b = a + c \iff b = c$
3. אם $a \neq 0$ אז $ab = ac \iff b = c$

הוכחה (1).

$\Longrightarrow$ הוכחנו מקודם.

$\Longleftarrow$ $ab = 0$. אם $a = 0$, סיימנו. אחרת, $a \neq 0$, נראה כי $b = 0$:

$$b = 1 \cdot b = (a^{-1} \cdot a)b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$$

■

הוכחה (2). $\Longrightarrow$ אם $b = c$ אז נוסיף a לשני האגפים ונקבל $a + b = a + c$.

$\Longleftarrow$ $a + b = c + d$, נוסיף $(-a)$ לשני האגפים, נקבל: $-a + a + b = -a + a + c$ ולכן $b = c$.

דרך אחרת לעשות זאת, היא:

$$b = 0 + b = (-a + a) + b = -a + (a + b) = -a + (a + c) = c$$

■

הוכחה (3). $\Longrightarrow$ $b = c$ אז $a - b = a - c$

$\Longleftarrow$ באופן דומה:

$$b = 1 \cdot b = (a^{-1}a)b = a^{-1} \cdot (ab) = a^{-1} \cdot (ac) = (a^{-1} \cdot a)c = 1 \cdot c = c$$

■

FINITE FILEDS .... (5)

5.1 חשבון מודולרי

המטרה: לראות איך חשבון מודולרי מייצג שדות סופיים.

הגדרה. אם $n \geq 1$ טבעי, אז נגדיר יחס על זוגות שלמים $x, y \in \mathbb{Z}$ הוא:

$$x \equiv y \bmod n \iff \exists k \in \mathbb{N}. x - y = nk$$

זהו יחס שקילות, שיוגדר באמצעות $\equiv_n = \{\langle x, y\rangle \in \mathbb{Z}^2 \mid \exists k \in \mathbb{Z}. x - y = nk\}$.

למה. אם $n \geq 1$, אז $x \equiv y \mod n$ הוא שקילות (רפלקסיבי, סימטרי, טרנזיטיבי). הוכחנו עם נטלי.

הגדרה. $\mathbb{Z} \ni n \geq 1$, $x \in \mathbb{Z}$. נגדיר $[x]_n = \{y \in \mathbb{Z} \mid x \equiv y \mod n\}$ – מחלקת השקילות של x.

טענה. $[x]_n = \{x + nk \mid k \in \mathbb{Z}\}$. לעת עתה לא נוכיח.

5.1.1 דוגמאות

יהי $\mathbb{N} \ni n \geq 1$, אז:

$$[0]_n = \{\dots, -2n, n, 0, n, 2n \cdots \mid\mid n \in \mathbb{N}_+\} \tag{1}$$
$$[1]_n = \{\dots, 1 - n, 1, 1 + n \dots\} \tag{2}$$
$$[n]_1 = [0] \tag{3}$$
$$[n + 1] = [1]_n \tag{4}$$

5.2 טענות נוספות

- כל שתי מחלקות שקילו תשוות או זרות
- בכל מחלקת שקילות יש בדיוק אחד מבין $\{0, \dots n - 1\}$.

הוכחה (1). יהיו $[a], [b]$ מחלקות שקילות. אם $[a] \cap [b] = \varnothing$ סיימנו. אחרת, קיים $c \in [a] \cap [b]$. נראה ש־$[a] \subseteq [b]$ ומסימטריה נקבל שוויון. יהי $x \in [a]$, נראה $x \in [b]$ ע"י $x \equiv b \bmod n$. ע"י $x = c \bmod n$, $c \equiv a \bmod n$, $x \equiv a \bmod n$ והחיתוך $c \equiv b \bmod n$ (רעיון $x = a = b = c$) ולכן $x = b \bmod n$ ומרטנזיטיביות. ■

הוכחה (2). יהי $[a]_n$, $a \in \mathbb{Z}$. צ.ל. קיום $i \in \{0, \dots, n - 1\}$ כך ש־$i \in [a]_n$. נסתכל על $c = a - \left\lfloor \frac{a}{m} \right\rfloor \cdot n$. נראה ש־$c \in \{0, \dots, n - 1\}$. נשים לב ש־$\frac{a}{n} - 1 > \left\lfloor \frac{a}{n} \right\rfloor \leq \frac{a}{n}$. אזי:

$$0 = a - \frac{a}{n} \leq c = a - \left\lfloor \frac{a}{n} \right\rfloor n < a - \left(\frac{a}{n} - 1\right) n = n$$

כדרוש. נראה יחידות. יהיו $r_1, r_2 \in \{0, \dots n - 1\}$ וגם $r_1, r_2 \in [a]_n$. נראה $r_1 = r_2$. מהשייכות ל־$[a]_n$ נקבל:

$$r_1 \equiv a \equiv r_2 \mod n \implies r_1 - r_2$$

בה"כ $r_1 > r_2$, אי־שוויון וניצחנו. ולכן $0 \leq r_1 - r_2 < n$ ואם שונים אז סתירה. ■

5.3 חידה

תהי הקבוצה $F = \{[0], \dots, [n - 1]\}$ והפעולות מודולו, צ.ל. ששדה $\iff$ n ראשוני.