אלגברה לינארית 1א׳ - שיעור 3

09 בינואר, 2024

יונתן מגר

דוגמאות לשדות

ראינו סוג מסוים של שדות: לדוגמה, $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

תזכורת (מהשיעור עם ענת):

נגדיר יחס על $\mathbb{Z}$ בהינתן $n \geq 1$ קבוע: $a \equiv b \bmod n \Leftrightarrow n|a-b$, כלומר קיים c שלם כך ש-$a-b=cn$. הוכחנו כי היחס **רקלפסיבי**: $a \equiv a \bmod n$, **סימטרי וטרנזיטיבי**. (אשלים בהמשך).

נגדיר את מחלקות השקילות $[x]_n = \{y \in \mathbb{Z} \mid y \equiv x \bmod n\} = \{x, x \pm n, x \pm 2n...\}$.

למה:

(1) כל שתי מחלקות שקילות שוות או זרות.
(2) כל איבר שלם נמצא באחת ממחלקות השקילות.
(3) זה מגדיר חלוקה של $\mathbb{Z}$: כלומר, $\mathbb{Z} = [0]_n \uplus ... \uplus [n-1]_n$ (זה אומר ש-$\mathbb{Z}$ איחוד של מחלקות השקילות $[0]$ עד $[n-1]$ ואין חפיפה).

הוכחה:

(1) יהיו $[a]_n, [b]_n$ מחלקות שקילות.
- במקרה א׳, $[a] \cap [b] = \emptyset$. ניצחנו (מחלקות השקילות זרות).
- במקרה ב׳, $\exists c \in [a] \cap [b]$. כלומר, $c \equiv a \bmod n \vee c \equiv b \bmod n$. צ״ל $[a]=[b]$.

נוכיח ש-$[b] \subseteq [a]$ (משיקולי סימטריה, ייובע גם ש-$[a] \subseteq [b]$): יהי $x \in [a]$. כלומר, $x \equiv a \bmod n$, וגם ראינו קודם ש-$c \equiv a \bmod n$. משיקולי סימטריות וטרנזיטיביות, נגרר ש-$x \equiv c \bmod n$. נזכיר ש-$c \equiv b \bmod n$, ומטרנזיטיביות $x \equiv b \bmod n$, כרצוי.

■

(2) ברור כי לכל $a \in \mathbb{Z}$ מתקיים $a \in [a]$ מרפלקסיביות.

■

(3) קודם נוכיח ש-$\mathbb{Z} = \bigcup_{i=0}^{n-1} [i]_n$. הכיוון $\supseteq$ ברור. עבור הכיוון $\subseteq$, נוכיח: יהי $x \in \mathbb{Z}$ צריך למצוא $0 \leq i \leq n-1$, כך ש-$x \in [i]$. נזכיר כי השלמים $\mathbb{Z}$ באים עם חילוק עם שארית, כלומר נוכל לבטא את x בתור $an+r$, כך ש-$x \leq r \leq n-1$. אז, $x-r=an$ ולכן $x \equiv r \bmod n$ ומכך $x \in [r]$ (■ חלק ראשון).

חלק שני: לכל $0 \leq j \leq i \leq n-1$ מתקיים ש-$[i] \cap [j] = \emptyset$. לפי (1) די להראות ש-$[i] \neq [j]$. נראה ש-$i \notin [j]$ למרות ש-$i \in [i]$, ואכן $0 \leq i-j \leq n$. לכן $i-j \neq an$ ולכן $i \neq j \bmod n$ כלומר $i \notin [j]$.

■

הגדרה - $\mathbb{Z}/n\mathbb{Z}$

נסמן ב-$\mathbb{Z}/n\mathbb{Z}$ את קבוצת מחלקות השקילות, כלומר $\mathbb{Z}/n\mathbb{Z} = \left\{[0]_n, [1]_n ..., [n-1]_n\right\}$ קבוצה בגודל n.

נגדיר: $[x]+[y] := [x+y]$, $[x] \cdot [y] := [x \cdot y]$. צריך להראות שהפעולות מוגדרות היטב, כלומר אינן תלויות בבחירת הנציגים.

טענה - החיבור והכפל ב-$\mathbb{Z}/n\mathbb{Z}$ מוגדרים היטב

נוכיח: $x_1, x_2 \in \mathbb{Z}$ כך ש-$[x_1]=[x_2]$ ו-$y_1, y_2 \in \mathbb{Z}$ כך ש-$[y_1]=[y_2]$. צ״ל $[x_1+y_1]=[x_2+y_2]$ וגם $[x_1 \cdot y_1] = [x_2 \cdot y_2]$. לפי הלמה הקודמת, די להראות ש-$[x_1+y_1] \cap [x_2+y_2] \neq \emptyset$. די להראות ש-$x_1+y_1 \equiv x_2+y_2 \bmod n$ (ואותו דבר עבור כפל).

ואכן, קיימים $x_1 - x_2 = x_3 n$ ו-$y_1 - y_2 = y_3 n$. ואז,

$$x_1 + y_1 - (x_2 + y_2) = x_1 - x_2 + y_1 - y_2 = n(x_3 + y_3)$$

ולכן הם שקולים. באופן דומה עבור כפל,

$$x_1 y_1 - x_2 y_2 = (x_2 + x_3 n)(y_2 + y_3 n) - x_2 y_2 = n[x_3 y_2 + x_2 y_3 + x_3 y_3 n]$$

■

טענה - $\mathbb{Z}/n\mathbb{Z}$ הוא שדה

$\mathbb{Z}/n\mathbb{Z}$ עם החיבור והכפל שהגדרנו ועם $[0]$ כאיבר האפס ו-$[1]$ כאיבר היחידה מקיים את כל התכונות של שדה, פרט אולי לקיום הופכי. נוכיח (חלקית): נגיד ש-$[0]$ הוא באמת איבר האפס: $[x] + [0] = [x + 0] = [x]$ כרצוי. כך הלאה עבור איבר היחידה ושאר תכונות השדה. הטענה לכן נובעת מקיום התכונות בשלמים.

■

דוגמאות

(1) $n = 2$. $\mathbb{Z}/2\mathbb{Z} = \{\text{זוגיים, אי-זוגיים}\} = \{[0], [1]\} = \{[8], [-3]\}$. זה שדה המזדהה עם $\mathbb{F}_2$.
(2) $n = 3$. $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\} = \{[0], [1], [-1]\}$. זהו שדה (ניתן לזהותו בתור $\mathbb{F}_3$).
(3) $n = 4$. $\mathbb{Z}/4\mathbb{Z} = \left\{[0]_4, [1]_4, [2]_4, [3]_4\right\}$. ל-2 אין הופכי, כי $[2] \cdot [x] = [2x]$ וכל האיברים ב-$2x$ זוגיים ולכן לא נקבל את $[1]$. דרך אחרת: $[0] = [2] \cdot [2]$ ובשדה זה לא יכול להתקיים. כלומר, זהו לא שדה.
(4) $n = 5$. $\mathbb{Z}/5\mathbb{Z}$ שדה, $2 \cdot 3 \equiv 1 \bmod 5$.
(5) $n = 6$. $\mathbb{Z}/6\mathbb{Z}$ לא שדה כי $2 \cdot 3 \equiv 0 \bmod 6$.

קל להכליל בתור משפט: **$\mathbb{Z}/n\mathbb{Z}$ הוא שדה אמ"מ n ראשוני.** (נדלג על ההוכחה).

מציין של שדה

ב-$\mathbb{Q}$, $1 + 1 + 1 + 1 ... + 1 \neq 0$. אך ב-$F = \mathbb{Z}/p\mathbb{Z}$, מתקיים $1_F + ... + 1_F$ (p פעמים) שווה ל-0. נגדיר באינדוקציה $n \cdot 1_F := 1_F + ... + 1_F$ (n פעמים), ו-$-n \cdot 1_F = -(n \cdot 1_F)$.

נגדיר את המציין של השדה כך:

$$\mathrm{char}(F) := \begin{cases} 0 \text{ if } n \cdot 1_F \neq 0 \forall n \in \mathbb{N} \\ \text{else} \min\{n \in \mathbb{N} \mid n \cdot 1_F = 0\} \end{cases}$$

מערכות משוואות מעל שדות

יהי F שדה כלשהו, ונסמן $1 = 1_F$ ו-$0 = 0_F$.

הגדרות

(1) משוואה לינארית ב-n נעלמים מעל F עם מקדמים $a_1 ... a_n, b \in F$ היא משוואה מהצורה $a_1 x_1 + ... + a_n x_n = b$.
(2) מערכת משוואות של m משוואות ב-n נעלמים מעל F היא אוסף של m משוואות כמו ב-(1). נרשום:

$$\begin{pmatrix} a_{1n} x_1 + ... & a_{1n} x_n & = b_1 \\ \vdots & \vdots & \vdots \\ a_{m1} x_1 + ... & a_{mn} x_n & = b_m \end{pmatrix}$$

כאשר $a_{ij} \in F$, $1 \leq i \leq m$ נקראים המקדמים. (להשלים)

(3) פתרון של מערכת המשוואות זה $(x_1, ... x_n) \in F^n$ הוא n-יה של איברים ב-F כך שאם נציב את x_i ב-X_i במערכת המשוואות כל המשוואות יתקיימו.
(4) קבוצת הפתרונות היא $\{(x_1, ..., x_n) \in F^n \mid (x_1, ..., x_n) \text{ הוא פתרון של מערכת המשוואות}\}$.

דוגמה: $X+Y=0$.

פתרונות לדוגמה, $(0,0)$, $(1,-1)$. קבוצת הפתרונות היא $\{(\alpha,-\alpha) \mid \alpha \in F\}$.