לינארית 1א 2

שחר פרץ

13 בנובמבר 2024

(1) REMINDERS

שייעור שעבר דיברנו על שגות, ועל מחלקת השקילות mod.

(2) MODULAR FIELD

הגדרה. $\mathbb{Z}/_{n\mathbb{Z}} = \{[x]_n \mid x \in \mathbb{Z}\}$ ("מודולו $\mathrm{z}n$")
נגדיר פעולות להיות:

$$[x]_n + [y]_n = [x+y]_n$$
$$[x]_n \cdot [y]_n = [x \cdot y]_n$$

בשביל ח"ע, נדרוש שבפרט:

$$\mathbb{Z}_5 \implies [1]_5 = [6]_5 = [11]_5,\ [1]_5 + [2]_5 = [3]_5 \stackrel{!}{=} [8]_5 = [6]_5 + [2]_5$$

למה. חיבור וכפל ב־$\mathbb{Z}/_{n\mathbb{Z}}$ מוגדרים היטב ואינם תלויים בבחירת הנציגים.

הוכחה. יהי $A, B \in \mathbb{Z}$ מחלקות שקילות. יהיו $a_1, a_2, a \in A, b_1.b_2, b \in B$. כלומר $[b_1] + [b_2] = B$, $[a_1] + [a_2] = A$. נראה כי $[a_1 + b_1] = [a_2 + b_2]$ וגם $[a_1 \cdot b_1] = [a_2 \cdot b_2]$. ואכן:

$$a_2 = a_1 + na,\ b_2 = b_1 + nb$$

אזי

$$a_2 + b_2 = a_1 + b_1 + b(a+b) \equiv a_1 + b_1 \mod n$$

ובעבור כפל:

$$a_2 b_2 = (a_1 + na)(b + nb) = \cdots = a_1 b_1 \mod n$$

■

נרצה לחקור מתי הדבר הזה הוא שדה, ומתי הוא לא.

טענה. לכל $n > 1$ הקבוצה $\mathbb{Z}/_{n\mathbb{Z}}$ עם $[0]$ בתור איבר ה־0 ו־$[1]$ בתור איבר היחידה, מקיימת את כל התכונות של שדה פרט להופכי.

2.1 דוגמאות

(1) $$\mathbb{Z}_2 = \{0, 1\},\ 1 \cdot 1 \equiv 1 \mod 2$$
(2) $$\mathbb{Z}_3 = \{1, 2, 3\},\ 1 \cdot 1 \equiv \mod 3,\ 2 \cdot 2 = 4 \equiv 1 \mod 3$$
(3) $$\mathbb{Z}_4 = \{1, 2, 3, 4\},\ 2 \cdot 2 \equiv 4 \equiv 0$$
(4) $$\mathbb{Z}_5,\ 2 \cdot 3 = 6 \equiv 0 \mod 6$$

השניים האחרונים סתירה כי לא ייתכנו שני איברים שכפלם הוא 0.

טענה. $\mathbb{Z}/_{n\mathbb{Z}}$ שדה אמ"מ n ראשוני. **תכונה של ראשוניים.** p ראשוני וגם $p \mid n = ab$ ו־$a, b \in \mathbb{Z}$, אז $p \mid a \vee p \mid b$.

הוכחה. $\Longleftarrow$ אם n לא ראשוני, אז $\exists a, b \in \mathbb{N}. 1 \le ab < n,\ n = ab$. אזי $ab \not\equiv 0 \mod n$. אבל $ab \equiv - \mod n$, ולכן $\mathbb{Z}_n$ לא שדה.

$\implies$ נניח p ראשוני. יהיה $x \in \mathbb{Z}_{n\mathbb{Z}}$ כך ש־$x \not\equiv 0 \mod p$. נראה כי $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ כאשר $f([y]) = [x][y]$ היא הפיכה. נראה שהיא חח"ע. יהיו $y_1, y_2 \in \mathbb{Z}_n$ נבקש $f(y_1) = f(y)2$ כלומר $xy_1 \equiv xy_2 \mod n$ וסה"כ $n \mid x(y_1 - y_2)$. אזי n (p שלכם) ראשוני ולכן: $p \mid x \vee p \mid (y_1 - y_2)$. לא ייתכן $p \mid x$ כי $x \equiv 0 \mod n$. סה"כ $p \mid (y_1 - y_2)[y_1] = [y_2]$. ולכן f חחע. וכם על מקור ותמונה סופית וזהים בגודלם, ולכן f על ולכן $\exists y \in \mathbb{Z}_n . f(y) = xy = 1$. ל־$x$ יש הופכי.

■

IDK THE NAME IN ENGLISH . . . . (3)

הגדרה. יהי F שדה, $a \in F, \mathbb{Z} \ni n \geq 0$. נגדיר:

$$n \cdot a := \underbrace{a + \cdots + a}_{\times n} \tag{5}$$

$$(-n) \cdot a := -(na) \tag{6}$$

נאמר שהמציין של השדה הוא אפס אם $\forall n > 0 . n \times 1_f \neq 0$. אחרת, המקדם של השדה יהיה:

$$\mathrm{char}(F) = \min\{n \in \mathbb{N} \mid n \cdot 1_f = 0\}$$

משפט. F שדה. יהי $p \geq 0$ מציין של F. נגרר:

1. $p = 0 \vee p$ ראשוני

הוכחה. אם $p = 0$ אז F מכיל עותק של 2. אחרת, F מכיל עותק שלם של $\mathbb{Z}$. אם אכן $n \in \mathbb{N}$ נבקש $n \cdot 1_F = 0$ כלומר $\mathrm{char}(F) = 0$.

נזהה עם $\mathbb{Q}$. לכל $n \in \mathbb{N}$ נזהה את $n \cdot 1_F$ עם n ולכן F "מכיל" את הטבעיים. נזהה את $-(n \cdot 1_F)$ עם $-n$ כלומר F "מכיל" את $\mathbb{Z}$. עכשיו לכל $m, n \in \mathbb{Z}$ מזהה את $m \cdot n^{-1}$ עם $\frac{n}{m} \in \mathbb{Q}$. ולכן קיבלנו "עותק" של $\mathbb{Q}$ (למעשה, צריך פורמלית להראות קיסו איזומורפיזם).

במקרה השני, נניח $n \cdot 1_F = 0$. יהיה p הטבעי המינימלי שמקיים $p = \mathrm{char(F0)}$. נניח בשלילה ש־p לא ראשוני, אזי $a \leq a, b, < p$ עבורם $p = ab$ קיימים. מכיוון ש־p מינימלי עבור $p \cdot 1 = 0$. לכן:

$$b \cdot 1 \neq 0,\ a \cdot 1 \neq 0,\ (ab) \cdot 1 = 0 \implies (a \cdot 1_F) \cdot (b \cdot 1_F) = 0 \tag{7}$$

בסתירה כי מצאנו $a, b \neq 0$ כך ש־$ab = 0$ וגם $a, b \in F$.

יהי $a \in \mathbb{Z}_p$. נזהה עם a עם $1_F \cdot a$. נשים לב ש־$a = b + kp \iff a \equiv \mathrm{mod} \mathbb{R}$. לכן:

$$a \cdot 1_F = (b + pk) \cdot 1 = b \cdot 1_F + k(pk) = b1_F$$

■

2. המציין של שדה סופי הוא חיובי.

הוכחה. יש אינסוף טבעיים, אך $|F|$ סופית. לכן $n \cdot 1_F = m \cdot 1_F$ (שובך היונים). בה"כ $m > n$. לכן:

$$m \cdot 1_F - n \cdot 1_F = (m - n) \cdot 1_F = 0$$

ובפרט $(m - n) \in \mathbb{N}$. משהו לגבי מינימום שלא הספקתי כי התעסקתי עם השלט של השם. ■

THE MATRIX . . . . (4)

הפאנץ': בהינתן מערכת משוואות כמו:

$$\begin{cases} 3x + y = 7 \\ 8 = 2x - y \end{cases} \sim \begin{pmatrix} 3 & 1 \\ 2 & -1 \end{pmatrix} \begin{matrix} 7 \\ 8 \end{matrix}$$

נוכל לעשות משחקים על המטריצות כמו על משוואות רגילות, כמו לחלק ולחסר אגפים.

4.1 מערכת משוואות ליניאריות

הגדרה. משוואה ליניארית מעל שדה F ב־n נעלמים $x_1, \ldots, x_n$ עם $a_1, \ldots a_n$ מקדמים היא משוואה מהצורה:

$$a_1 x_1 + \cdots + a_n x_n = b$$

(זהו הייצוג הסטנדטי) לדוגמה $3x - 7 = 0$ ליניארי אך לא סטנדרטי, בעוד $y^2 + 7 = x$ כלל לא ליניארי.

הגדרה. מערכת של m משוואות ב־n נעלמים מעל שדה F הוא אוסף של m משוואות מעל F ב־n נעלמים. צורת ריסום סטנדרטית:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n} = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n} = b_2 \\ \vdots \\ a_{n1}x_{n1} + \cdots + a_{nn} = b_n \end{cases}$$

ל־$\in \mathrm{F} b_1, \dots b_n$ נקרא מקדמים חופשיים. לדוגמה:

$$\begin{cases} x_1 + 3x_2 = 2 \\ 7x_1 - 6x_2 = 1 \end{cases}$$

יתקיים $a_{12} = 3, b_1 = 1$ וכו'.

הגדרה. $a_{ij} \in F$ מקדמים $i \in \{1, \dots m\},\ j \in \{1, \dots, n\}$.

הגדרה. A קבוצה לא ריקה, $n \in \mathbb{N}$. יהיו $a_1, \dots a_n$. נסמן את ה־n־יה שאיבריה לפי הסדר בתור $(a_1, \dots a_n) \in A^n$. "שתי n־יות שוות אם שוות בכל n-מקום" (פרמול בבדידה).

הגדרה. פתרון למערכת משוואות זה $(x_1 \dots x_n) \in F^n$ כך שכל המשוואות מתקיימת לאחר הצבה.

הגדרה. שתי מערכות משוואות נקראות שקולות אם יש להן את אותה קבוצת הפתרונות.

חידה. בהינתן שדה $F = \mathbb{Z}_{17}$. הוכיחו, שאין מערכת משוואות עם בדיוק 16 פתרונות.

דוגמה: בעבור $x + y = 0$, קבוצת הפתרונות היא $\{(\alpha, -\alpha) \mid \alpha \in \mathbb{F}\}$. ל־$x \in \mathbb{F}^n$ נקרא וקטור. $c \in \mathbb{F}$ יקרא סקלר. בעבור מערכת משוואות, נוכל לחסר משהו מהמשוואות, להפכיל אותן, וכו', ולשמר את קבוצת הפתרונות.

הגדרה. תהי מערכת משוואות. פעולה אלמנטרית היא אחת מבין:

1. החלפת מיקום של שתי משוואות.
2. הכפלה של משוואה אחת בסקלר שונה מ־0.
3. הוספה לאחת המשוואות משוואה אחרת מוכפלת בסקלר.

משפט. פעולה אלמנטרית אל מערכת משוואות מעבירה למערכת שקולה.

הוכחה.

החלפת סדר לא משפיע על האם $x \in \mathbb{F}^n$ הוא פתרון.

נסתכל על מרעכת משוואות **מוכפלת בסקלר** $\lambda \neq 0$.

$$\begin{cases} \sum_{i=0}^{n} a_{1i}x_i = b_1 \\ \vdots \\ \lambda \sum_{i=0}^{n} a_{ti}x_i = \lambda b_t \\ \vdots \\ \sum_{i=0}^{n} a_{ni}x_i = b_n \end{cases}$$

יהי $(\alpha_1, \dots ag_n) \in \mathbb{F}^n$ שפותר את המערכת המקורית. נראה שגם פותר את החדשה:

$$\lambda \underbrace{\sum x_{tj}x_j}_{bt} = \lambda b_t$$

כדרוש. נראה כיוון הפוך (כדי להראות שלא הוספנו פתרונות). יהי $\alpha \in F^n$ פתרון של החדשה. נסתכל על מערכת משוואות חדשה מאוד, מוכפלת ב־$\frac{1}{\lambda}$. מההוכחה שלנו, α פתרון שלה, וזו בדיוק המקורית.

הכפלה בסקלר וחיסור. יהי $\alpha \in F^n$ פתרון של המקורית. נראה שהוא של החדשה. לא פורמלי, תוכלו לפרמל בעצמכם. הפעולה שעשינו היא על שורה t. חיבור $c \cdot \binom{\text{שורה}}{p}$. נקבל:

$$\underbrace{\sum x_j a_{tj}}_{bt} + \underbrace{\sum x_j a_{pj}}_{bp} = b_t + cb_p$$

כיוון הפוך אפשר לעשות באופן דומה ע"י יצירת משוואה חדשה מאוד. סוף קטע לא פורמלי.

■

4.2 Blue Pill, Red Pill

יהיו $m,n \in \mathbb{N}$. **מטריצה** מסדר $m \times n$ אוסף mn סקלרים מסוגרים במבלן a_{ij}. יתקיים:

$$i \in \{1 \dots m\},\ j \in \{1 \dots n\} \tag{8}$$

$$A = (a_{ij})_{\substack{i=1\dots m \\ j=1\dots n}} = \begin{pmatrix} a_{11} & a_{12} & \dots & a1n \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \tag{9}$$

כאשר $R_i := (a_{1i}, \dots, a_{in}) \in \mathbb{F}^1$ יקרא וקטור השורה.

$c_j := (a_1k, \dots, a_{mj}) \in \mathbb{F}^1$ יקרא וקטור עמודה/

$$A = \begin{pmatrix} R_1 \\ R_2 \\ \vdots \\ R_n \end{pmatrix} = \begin{pmatrix} C_1 \dots C_n \end{pmatrix}$$

$M_{mn}(F) :=$ כל המטרציות מסדר $m \times n$ מעל שדה $\mathbb{F}$.

$M_n(F) :=$ כל המטריצות מסדר $n \times n$ מעל שדה $\mathbb{F}$ (מטריצות ריבועיות).

לדוגמה:

$$(4) \in M_1(F),\ (1\ 2\ 3) \in M_{1\times3}(F),\ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \in M_{3\times1},\ \begin{pmatrix} 4 & -1 & 7 \\ 7 & -2 & 4 \end{pmatrix} \in M_{2\times3}(F)$$

מטריצה של מערכת משוואות:

$$A = \begin{pmatrix} a_{11} & \dots & a_n & b_1 \\ \vdots & & & \vdots \\ a_{m1} & \dots & a_{mn} & b_n \end{pmatrix}$$

מטריצה מצומצמת היא מטריצה בלי העמודה ה־$m+1$.

הגדרה. פעולות אלמנטריות על מטריצה:

1. החלפת מיקום שורות $R_i \longleftrightarrow R_j$
2. הכפלה של שורה בסקלר שונה מאפס: $R_i \to \lambda R_i$
3. הוספה לשורה אחרת מוכפלת בסקלר: $R_i \to R_i + C \cdot R_j,\ \neq 0c \in \mathbb{F}$

דוגמה:

$$\begin{cases} x+y+z=1 \\ x+2y+3z=4 \\ 2x+0+z=-1 \end{cases} \implies \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 2 & 0 & 1 & -1 \end{array}\right) \overset{R_2 \to R_2 - R_1}{\to} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & -1 \end{array}\right) \overset{R_3 \to R_3 - 2R_1}{\to} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & -2 & -1 & -3 \end{array}\right)$$

$$\overset{R_1 \to R_1 - R_2, R_3 \to R_3 + 2R_2}{\to} \left(\begin{array}{ccc|c} 1 & 0 & -1 & -2 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 3 & 3 \end{array}\right) \overset{J}{\to} \left(\begin{array}{ccc|c} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

כאשר J אומר $R_3 \to 1/3R_3$ וגם $R_1 \to R_1 + R - 3,\ R_2 \to R_2 - 2R_3$.

הגדרה. $A, B \in M_{n,m}$ מטריצות. נאמר ש־A, B שקולות אם ניתן לקבל מ־B את A ע"י מספר סופי של פעולות אלמנטריות. נסמן $A \sim B$.

טענה. יחס זה הוא שקילות.

הוכחה.
- $A \sim A$: ברור, כי 0 פעולות.
- $A \sim B,\ B \sim C$: נסמן בתור E את רצף הפעולות מ־A ל־B וב־E' את רצף הפעולות מ־B ל־C. בהתאם, E, E' יהיה מ־A ל־C.
- $A \sim B$ ונראה $B \sim A$. נסמן את $E_1, \dots E_b$ שדה של פעולות עלמנטריות מ־A ל־B ונמצא E^{-1} כך שסדרה מ־B ל־A.

■