

אלגברה מופשטת 1 – הרצאה 2

נחיד כמה נושאים מהרצאה קודמת.

דוגמה: לפתור משוואה $6x \equiv 7 \pmod{35}$ (כאשר x שלם).

פתרון: ניתן לרשום $[6]x = [7]$ במונואיד (\mathbb{Z}_{35}, \cdot) . למדנו בשיעור קודם כי עבור $ax=b$ (בכל מונואיד (X, \cdot)) ולכל הפיך $a \in Gr(X)$ קיים $x = a^{-1}b$. במקרה שלנו, $[6]_{35}^{-1} = [6]_{35}$.

לכן, קיבלנו שהפתרון למשוואה הוא: $x = [6]^{-1}[7] = [6][7] = [42]_{35} = [7] = \{35k + 7 | k \in \mathbb{Z}\}$.

מה קורה כשהמספרים גדולים? ננסה לפתור את $14x \equiv 10 \pmod{29}$. מצאנו כי $[14]_{29}^{-1} = [-2]$. ומכאן ניתן לפתור בקלות.

תרגיל שיהיה יותר קשר לנחש את ההופכי: שוב, לפתור בשלמים את $365x \equiv 2 \pmod{1876}$. בגלל שקשה לנו לנחש, היה עלינו לפתח שיטה. נשתמש בשיטה המבוססת על אחד מהטריקים מתורת המספרים.

נסתכל על המשוואה שלנו באופן כללי: $ax = b \pmod{n}$. ואם $(a, n) = 1$ נוכיח בהמשך את משפט אוילר שאומר סימון: $U_n = \{[a] | (a, n) = 1\} = Gr(\mathbb{Z}_n, \cdot)$ וזה ייקרא חבורת אוילר. ז"א, חבורת הפיכים של \mathbb{Z}_n . השאלה כעת הומרה למציאת $[a]_n^{-1}$ כאשר $(a, n) = 1$.

משפט: שמבוסס על שיטת אוקלידס: $(a, n) = 1$ או"א קיימים u, v מספרים שלמים כך שצירוף לינארי של $ua + vn = 1$. הוכחה: הכיוון שמאלה הוא טריוויאלי. על הכיוון השני, ימינה, נדבר בהמשך.

משפט: נניח $(a, n) = 1$ אז $[a]$ הפיך ב \mathbb{Z}_n ו $[a]^{-1} = [u]$ כאשר $ua + vn = 1$.

הוכחה: אנחנו מתבסס על ההנחה ש $vn = 0$. וקיבלנו ש $ua \equiv 1$ לכן $[a]^{-1} = [u]$.

סיכום: לגבי \mathbb{Z}_n עבור n טבעי קיבלנו $\mathbb{Z}_n = \left\{ \overline{[0]}, \overline{[1]}, \overline{[2]}, \dots, \overline{[n-1]} \right\}$. כדי שמחלוקות שקילות יהיו שוות,

$$[k_1] = [k_2], \text{ צריך שההפרש יהיה אפס מודולו } n. \text{ ז"א } n | k_1 - k_2.$$

נוכיח כי אין תלות בנציגים בחיבור וכפל של מחלקות שקילות: $[x] \cdot [y] = [x \cdot y]$, $[x] \oplus [y] = [x + y]$. כל זאת בגלל $x_1 \equiv y_1 \pmod{n}, x_2 \equiv y_2 \pmod{n} \rightarrow x_1 + x_2 \equiv (y_1 + y_2) \pmod{n}, x_1 x_2 \equiv y_1 y_2 \pmod{n}$.

משפט: (\mathbb{Z}_n, \oplus) חבורה ציקלית.

משפט: כל חבורה ציקלית היא אבלית.

הוכחה: $G = \langle a \rangle = \{a^k | k \in \mathbb{Z}\}$ לכל x, y ששייכים ל G מתקיים $yx = xy$ $a^{k_1} a^{k_2} = a^{k_1+k_2} = a^{k_2+k_1} = a^{k_2} a^{k_1} = xy$ ולכן תמיד $xy = yx$ ומכאן שמדובר בחבורה אבלית. מ.ש.ל. ■

הערה: קיבלנו עוד נוסחה לחזקות $a^{k_1} a^{k_2} = a^{k_1+k_2}$ באגודה (X, \cdot) : $\forall k_1, k_2 \in N$

בנוסף: $k_1 a + k_2 a = (k_1 + k_2) a$: בכל אגודה \mathbb{Z} : $\forall k_1, k_2 \in \mathbb{Z}$

דוגמה: של חבורה אבלית ושאינה ציקלית... $(\mathbb{Q}^n, +), (\mathbb{R}^n, +)$.

דוגמה טיפה יותר מיוחדת לחבורה שהיא אבלית ושאינה ציקלית היא למשל $\mathbb{Z}_2^2 = \{([0], [0]), ([0], [1]), ([1], [0]), ([1], [1])\}$.

נגדיר את הפעולה שלנו (שהיא מין הרחבה של החיבור) בטבלה:

דביר חדד

+	([0], [0])	([0], [1])	([1], [0])	([1], [1])
([0], [0])	([0], [0])	([0], [1])	([1], [0])	([1], [1])
([0], [1])	([0], [1])	([0], [0])	([1], [1])	([1], [0])
([1], [0])	([1], [0])	([1], [1])	([0], [0])	([0], [1])
([1], [1])	([1], [1])	([1], [0])	([0], [1])	([0], [0])

אז היא אינה ציקלית, בוודאות, ביחס לפעולה זו, אבל היא אבלית באופן וודאי.
יותר מזה, נקבל משפט:

משפט: לכל G_1, G_2 חבורות אבליות גם $G_1 \times G_2$ אבלית (לגבי הפעולה הטבעית).

משפט: (Z_n, \cdot) מונואיד קומוטטיבי.

הסבר: אסוציאטיביות נובעת מהאסוציאטיביות של כפל בז.

משפט: (Z_n, \oplus, \cdot) חוג קומוטטיבי.

הגדרה: מבנה $(X, +, \cdot)$ עם 2 פעולות ייקרא חוג (Ring) אם מתקיים:

1. $(X, +)$ חבורה אבלית
2. (X, \cdot) מונואיד
3. דיסטריבוטיביות (וזה הקשר שבין 1 ו 2):

במשפט הקודם שימו לב ש $(Z, +, \cdot)$ חוג. ומכאן נובע ש (Z_n, \oplus, \cdot) חוג.

הגדרה: חוג קומוטטיבי $(X, +, \cdot)$ שבו כל איבר $x \in x^* := x \setminus \{0\}$ הפיך נקרא שדה וגם $|x| \geq 2$ נקרא שדה (Field).

דוגמה: Q, R, C, Z_2 .

משפט: (Z_n, \oplus, \cdot) שדה אוי"א $n=prime$ (ראשוני)

הוכחה: כיוון אחד, ימינה, הוא פשוט. הכיוון השני פחות טריוויאלי.

משפט: לכל n טבעי $Z_n \xrightarrow{f_n} Z$ נגדיר $x \rightarrow [x]_n$. מתקיים כי $f_n(x+y) = f_n(x) \oplus f_n(y)$ וגם $f_n(xy) = f_n(x)f_n(y)$.
ז"א אפימורפיזם של חבורות.

דוגמה: $f_{10}: Z \rightarrow Z_{10}$. במקרה שלנו, נחפש את הספרה האחרונה (ספרת היחידות) כי כל דבר אחר ניתן לחלוקה בעשר

באופן שלם. נניח כעת שמדובר ב $x = 1959^{1999}$. נמצא את ערכו לאחר הפעלת הפונקציה, לכן: $f_n(x) =$

$$f_{10}(1959^{1999}) = f_{10}(1959)^{1999} = 9^{1999} = f_{10}(-1)^{1999} = -1 \text{ mod } 10 = 9$$

למצוא בבית את שתי הספרות האחרונות של $x = 1959^{1999}$. רמז: להשתמש ב f_{100} .

תזכורת: (X^X, \circ) מונואיד עם נייטרלי id . מספר האיברים (או העוצמה) של המונואיד הוא $|X^X| = |X|^{|X|}$. אם $|X|=n$ אז $|X^X| = n^n$.

דוגמה (1): כמה מבנים אלגבריים בינאריים קיימים מעל קבוצה X בת n איברים?

$$\{X \times X \rightarrow X\} = |X^{X^2}| = n^{n^2}$$

דוגמה (2): כמה מבנים קומוטטיביים קיימים מעל קבוצה X בת n איברים?

תשובה: להשלים בבית. רמז: בטבלה של הפעולה, צריכה להיות סימטריות מעל ומתחת לאלכסון.

דוגמה (3): (N^n, \circ) מונואיד. יש איברים שלא הפיכים אבל הפיכים רק מצד אחד. ניקח כדוגמה את הפונקציה $f(n)=n+1$ ונגדיר $g_t(n) = \begin{cases} n-1, & n > 1 \\ t, & n = 1 \end{cases}$. בעצם לא קיים הופכי מצד אחד, כי יש אינסוף אפשרויות לצד השני.

תזכורת: $S_x := Gr(X^X, \circ)$ (Symmetric Group).

בהמשך נוכיח שכל חבורה סופית G עם n איברים איזומורפית איזומורפית לתת חבורה של $S_n = S_{\{1,2,\dots,n\}}$ "חבורת התמורות".

$n=1$: $S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} = e \right\}$ חבורה טריוויאלית עם איבר 1.

$n=2$: $S_2 = \left\{ \begin{pmatrix} 1,2 \\ 1,2 \end{pmatrix} = e, \begin{pmatrix} 1,2 \\ 2,1 \end{pmatrix} = \sigma \right\}$ עם 2 איברים.

הגדרה: תהי (G, \cdot) חבורה ו $a \in G$. נגדיר $r_a: G \rightarrow G, x \rightarrow xa$, $l_a: G \rightarrow G, x \rightarrow ax$.

משפט: לכל a שייך ל G ולכל חבורה G l_a, r_a חחייע ועל.

הוכחה: במקרה של l_a . לכל b שייך ל G יש פתרון למשוואה $ax=b$. ומכאן נובע ש $l_a(x) = b$ ז"א הוכחנו ש l_a היא על.

קל לבדוק שהיא גם חחייע. נניח ש $x_1 \neq x_2$. לכן $l_a(x_1) \neq l_a(x_2)$ $ax_1 \neq ax_2$ ומ.ש.ל. ■ עבור r_a ההוכחה דומה.

תוצאה: בשורה של a שמתמאיה ל a בטבלת Cayley מקבלים איברים $\{ax\}_{x \in G}$. לכן נקבל אותם איברים (אולי בסדר אחר פשוט). אותה תוצאה לגבי הטור שמתאים ל.

תרגיל: הוכח שכל חבורה מ $2/3$ איברים היא ציקלית. נוכיח זאת בתרגול

נביט בתמורות שוב. $n=3$. $S_3 = \left\{ \begin{pmatrix} 1,2,3 \\ 1,2,3 \end{pmatrix} = e, \begin{pmatrix} 1,2,3 \\ 2,1,3 \end{pmatrix} = \sigma, \begin{pmatrix} 1,2,3 \\ 2,3,1 \end{pmatrix} = a, a^2, \sigma^\circ a, \sigma^\circ a^2 \right\}$. $a^\circ \sigma \neq \sigma^\circ a$

הערה: בהמשך נלמד חבורת סימטריות של D_3 של משולש שווה צלעות וגם שם יש 6 איברים. בעצם $D_3 \cong S_3$.

הערה: נוכיח שחבורה ציקלית אינסופית $(Z, +) \simeq (Z_n, \oplus) \simeq (\Omega_n, \cdot)$ וכל חבורה ציקלית סופית עם n איברים

הגדרה: נניח (G, \cdot) חבורה ו a שייך ל G . $O(a) = Ord(a) = |a| := \begin{cases} \min\{k \in N \mid a^k = e\} \\ \infty; \text{ אם אין } k \text{ כזה} \end{cases}$

דוגמה: $O(7) = \infty$ ב (R^*, \cdot) ולכן $O(cis38) = 12$