

**אלגברה מופשטת 1 – הרצאה 1**

אין ציוני תרגילים. יש חובת הגשה ובוחרן אמצע. הקורס ינוהל דרך math-wiki.com ולשם יועלו התרגילי בית וסיכומים לסוגיהם. המטרה היא לא רק ללמוד את הקורס, אלא גם ללמוד דברים רלוונטיים אחרים. 90% מהקורס הוא תורת החבורות (English: Group Theory), ו-10% זה נושאים שונים שקשורים לחבורות למחצה (English: Semigroups) וכו'.

המבחן הוא על כל החומר, אבל רמת התרגילים אינם קשים. 80% מהתרגילים יהיו מוכרים- תרגילים שנלקחו מההרצאות ומהתרגילי בית וכיתה. חשוב מאוד להכיר את ההרצאות.

נתחיל מההגדרות הראשוניות שקשורות למבנים הבסיסיים:

**הגדרה:** פעולה בינארית מעל קבוצה  $X$  שאינה קבוצה הריקה היא פונקציה. ז"א  $X \times X \xrightarrow{w} X$  או  $w(x, y) \mapsto (x, y)$ . סימנו מוכרים אחרים ל $w$  הם  $x + y, x \cdot y, x * y, x \cdot y$ . אז הזוג  $(X, w)$  נקרה מבנה אלגברי (או מערכת אלגברית) (English: Algebraic Structure).

דוגמאות: ...  $(\mathbb{R}, \cdot)$ ,  $(\mathbb{Z}, +)$ ,  $(\mathbb{N}, +)$  כל אלה הם מבחנים אלגבריים. מה לא? לדוגמה;  $(\mathbb{N}, -)$  כי הוא לא מוגדר, אין סגירות.

**אקסיומות:**

1. אסוציאטיביות (חוק הקיבוץ הכללי) -  $\forall x, y, z \in X : (x \cdot y) \cdot z = x \cdot (y \cdot z)$  ומכאן, אסוציאטיביות מוכללת- עבור כל  $n$  טבעי החל מ-3 אין משמעות לסוגריים (כאשר מדובר באותה פעולה. אם מדובר בפעולה אחרת בוודאי ובוודאי שיש משמעות לסדר של הסוגריים). ז"א שעבור  $a, b, c, d$  מתקיים  $(ab)(cd) = a(bc)d = a(b(cd))$ .
2. קומוטטיביות-  $\forall x, y \in X : x \cdot y = y \cdot x$

**הגדרה:** מבנה אלגברי  $(X, \cdot)$  נקרא אגודה (או חבורה למחצה) (English: Semigroup) אם הפעולה היא אסוציאטיבית.

3. איבר נייטרלי משמאל- נניח  $(X, \cdot)$  מבנה. אומרים ש  $a \in X$  איבר נייטרלי משמאל (או "יחידה משמאל") אם  $\forall x \in X : ax = x$
4. איבר נייטרלי מימין- באופן דומה למשמאל,  $\forall x \in X : xa = x$

**טענה:** אם קיימים נייטרלי משמאל  $e_1$  ומימין  $e_2$  אזי  $e_1 = e_2$ .

הוכחה: נסתכל כל המכפלה של שתיים פעם מימין ופעם משמאל (המכפלה מוגדרת כי זהו מבנה):  $e_1 e_2 = \begin{matrix} \nearrow e_1 \\ \searrow e_2 \end{matrix}$  ולכן  $e_1 = e_2$ .

**תרגיל:**  $X := \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$  מבנה לגבי כפל מטריצות. צריך להוכיח שיש אינסוף נייטרלים משמאל. ולכן אין נייטרלים מימין (חשוב לשים לב לטענה הקודמת!)

**הגדרה:** חזקה (וכפולה).  $a^n = \underbrace{a \cdot a \cdots a}_n$  לכל  $a \in X$  ולכל  $n$  טבעי כאשר  $(X, \cdot)$  אגודה. והגדרה זו מוגדרת היטב בגלל אסוציאטיביות מוכללת.

דוגמה נגדית להגדרה (א), בהנחה ואין אסוציאטיביות. נביט ב  $(\mathbb{Z}, -)$  שם  $(x - x) - x \neq x - (x - x)$  ולכן אין זה מתקיים. במקרה שלנו החזקה היא עבור הפעולה של החיסור. הנקודה "..." של האגודה שלנו היא -.

דוגמה נגדית נוספת (ב): נגדיר  $(\mathbb{N}, *)$  ואז  $a * b = a^b$  ו  $9^3 = (3 * 3) * 3 \neq 3 * (3 * 3) = 3^9$ .

·	a	b
a	b	b
b	a	a

## דביר חדד

דוגמה (ג): נגדיר מבנה מעל קבוצה בת 2 איברים.  $X = \{a, b\}$ . נרשום את "לוח הכפל" של אותה פעולה משמאל. גם כן

$$a = \underbrace{(a \cdot a)}_{ba} \cdot a \neq a \cdot \underbrace{(a \cdot a)}_{ab} = b$$

תכונות חשובות של החזקה (באגודה):

ב  $(x, \cdot)$  מתקיים  $(x^n)^m = x^{mn}$  ובאופן אנלוגי לחזקה וכפל נקבל את הכפולה לחיבור. ז"א  $na := \underbrace{a + a + \dots + a}_n$

וב  $(x, +)$  מתקיים  $m(nx) = (mn)x$ .

הגדרה: איבר נקרא נייטרלי או יחידה אם הוא נייטרלי משמאל וגם מימין. ז"א (נסמן e)  $\forall x \in X : ex = xe = x$  (הסימון בד"כ הוא אכן 0).

טענה: אם קיים נייטרלי, אז הוא יחיד.

הסבר: נובע מהטענה הקודמת.

הגדרה: אגודה עם נייטרלי נקרא גם מונויד (English: Monoid) או יחידון ©.

הגדרה: נניח  $(x, \cdot)$  מונויד עם e נייטרלי.

- איבר  $a \in X$  נקרא הפיך משמאל אם קיים  $b \in X$  כך  $a \cdot b = e$
- במצב זה ניתן גם לומר ש b הפיך מימין.
- a נקרא הפיך אם הוא הפיך משמאל וגם מימין.

טענה: נניח a הפיך משמאל.  $\exists b' : a \cdot b' = e$  וגם הפיך מימין  $b'' : b'' \cdot a = e$  אזי  $b'' = b'$ .

הוכחה: ■  $b'' = b' \rightarrow b' = b'' \rightarrow eb' = b'' \rightarrow (b''a)b' = b'' \rightarrow b''(ab') = b''e \rightarrow ab' = e$  מ.ש.ל.

מסקנה: אם a הפיך משמאל וימין, אז הפכי מימין שווה להפכי משמאל. נקרא לאיבר זה האיבר ההפכי.

הגדרה: חבורה (Group).

מבנה  $(x, \cdot)$  נקרא חבורה אם הוא מונויד שכל האיברים הפיכים. הגדרה זו שקולה לתנאים הבאים:

- א. אסוציאטיביות
- ב. קיום איבר נייטרלי
- ג. קיום איבר הופכי.  $\forall x \in X \exists y : xy = e$  נסמן  $y := x^{-1}$ . יש יחידות להפיכות ולכן הוא מוגדר באופן חד משמעי.

הגדרה: אם חבורה היא קומוטטיבית אומרים שהיא חבורה אבלית (על שם Abel).

הגדרה: נניח  $(X, \cdot)$  חבורות. פונקציה  $f : X \rightarrow Y$ .

הומומורפיזם  $\forall a, b \in X : f(ab) = f(a) * f(b)$

אפימורפיזם  $Im(f) = Y, f(x) = Y$

מונומורפיזם זה הומומורפיזם חח"ע.

איזומורפיזם = הומומורפיזם (חח"ע ועל). אם קיים איזו' אז מסמנים  $(Y, *) \cong (X, \cdot)$  יש להן אותן תכונות אלגבריות.

לבדוק:

1. הרכבה של הומומורפיזם (מונו, אפי, איזו) גם הומו(...) בהתאמה
2. איזומורפיזם מקיים רפלקסיביות סימטריות וטרנזיטיביות.

תכונות של הפיכים במונויד:

נניח  $(X, \cdot)$  מונויד עם נייטרלי  $e$ . נסמן:  $\{X \text{ הפיכים של } X\} = Gr(X, \cdot)$ .

1.  $e \in Gr(X, \cdot)$  וגם  $e^{-1} = e$  ולכן  $e$  הפיך.
2. אם  $a \in Gr(X, \cdot)$  אזי  $a^{-1} \in Gr(X, \cdot)$ . ההסבר הוא תכונת הסימטריות שהמונויד מקיים.  
 $(a^{-1})^{-1} = a$  1,2 נובע כי
3. אם  $a, b \in Gr(X, \cdot)$  אזי  $ab \in Gr(X, \cdot)$  ומתקיים  $(ab)^{-1} = b^{-1}a^{-1}$ . בדיקה:  $(ab)(b^{-1}a^{-1}) = e$   
 $a(bb^{-1})a^{-1} = a(ea^{-1}) = aa^{-1} = e$

כתוצאה מ-1,2,3 נקבל:

**משפט:** לכל מונויד  $X$  הקבוצה  $Gr(X)$  יחד עם פעולת הצמצום מגדיר חבורה שנקראת חבורת הפיכים של מונויד  $X$ .

דוגמה (1):  $\{מטריצות ריבועיות ממשיות\} = Mat_{n \times n}(R)$  לגבי הכפל מונויד.

$$Gr(Mat_{n \times n}(R)) = \{מטריצות הפיכות\} = \{A \mid \det(A) \neq 0\}$$

דוגמה (2):  $(P(X), \cup)$  מונויד. כאשר  $P(X) = \{A \mid A \subseteq X\}$  (קבוצת החזקה). סגירות, אסוציאטיביות ונייטרלי מתקיים ע"פ ההגדרה. האיבר הנייטרלי לפי הפעולה (איחוד) הוא הקבוצה הריקה, שגם כן שייך ל- $P(X)$ . כעת, מהו  $Gr(x)$  במקרה זה? יש לנו איבר נייטרלי אחד ויחיד, ולכן  $Gr(P(X), \cup) = \{\emptyset\}$ .

דוגמה (3):  $(N \cup \{0\}, +)$  ולכן  $Gr(x) = \{0\}$ .

הערה: אם  $(X, +)$  מבנה נתון, אזי במקום הפיך אומרים נגדי ומסמנים ב- $a^{-1}$  ולא ב- $a^{-1}$ .

דוגמה (4):  $(Mat_{n \times n}(R), +)$   $X = (Mat_{n \times n}(R), +)$   $Gr(X) = X$  ואז  $Gr(X) = X$ .

באופן כללי,  $Gr(X) = X \Leftrightarrow X$  חבורה.

למדנו את התכונות הבאות:

- א.  $e^{-1} = e$
- ב.  $(a^{-1})^{-1} = a$
- ג. בהנחה וקיימים הופכיים  $a, b$ ,  $(ab)^{-1} = b^{-1}a^{-1}$
- ד. לכל  $a$  הפיך במונויד  $(X, \cdot)$  מוגדרת  $a^k = \overbrace{a \cdot a \cdots a}^k$  לכל  $k \in \mathbb{Z}$ . וגם  $a^0 = e$ .  
 אם  $-n = k < 0$  (n טבעי) אז  $a^k = (a^{-1})^{-k} = (a^{-1})^n$ .

**משפט:** ניתן לצמצם בהפיך.

אם  $a$  הפיך במונויד  $(X, \cdot)$  אז  $ax = ay \rightarrow x = y$  וגם  $xa = ya \rightarrow x = y$ .

הוכחה:  $ax = ay \rightarrow a^{-1}(ax) = a^{-1}(ay) \rightarrow (a^{-1}a)x = (a^{-1}a)y \rightarrow ex = ey \rightarrow x = y$  ■

**משפט:** בכל מונויד  $X$  ולכל הפיך  $a \in X$  המשוואה האלמנטרית  $(ax=b)$  פתירה עם פתרון יחיד כאשר  $x = a^{-1}b$ . ובאופן דומה  $xa = b$  בעל פתרון שהוא  $x = a^{-1}b$ .

הוכחה:  $ax = b \rightarrow a^{-1}(ax) = a^{-1}b \rightarrow (a^{-1}a)x = a^{-1}b \rightarrow ex = a^{-1}b \rightarrow x = a^{-1}b$  ■

דביר חדד

**הגדרה:** תת חבורה. נניח  $(X, \cdot)$  חבורה ו $Y$  מוכל ב $X$ . אומרים  $Y$  תת חבורה של  $X$  ונסמן  $Y \leq X$  אם פעולת הצמצום מעל  $Y$  מגדיר חבורה.

אפשרויות לבדיקה:

א.  $Y$  לא ריקה. בד"כ בודקים שהאיבר הנייטרלי של  $X$  שייך ל $Y$ .

ב. סגירות.  $y_1, y_2 \in Y \rightarrow y_1 \cdot y_2 \in Y$

ג. סגירות לגבי הפכיות. ז"א שאם  $y_1 \in Y \rightarrow y_1^{-1} \in Y$ .

דוגמה נגדית: נניח  $X = (\mathbb{Z}, +)$  חבורה ו $Y = \mathbb{N} \cup \{0\}$ . א, ב, מתקיימים, אבל ג לא.

אפשרות אחרת לבדיקה היא:

א.  $Y$  לא ריקה

ב.  $y_1, y_2 \in Y \rightarrow y_1 \cdot y_2^{-1} \in Y$ . לבדוק בבית איך שתי האפשרויות להגדרת תת חבורה שקולות.

דוגמה: ניקח  $(\mathbb{C} \setminus \{0\}, \cdot) = (\mathbb{C}^*, \cdot) \leq (\mathbb{R}^*, \cdot) \leq (\mathbb{Q}, \cdot)$  חבורות אבליות.

באופן כללי, לכל שדה  $(F, +, \cdot)$  ה $(F^*, \cdot)$  היא חבורה אבלית.

דוגמה: {שורשי יחידה}  $\Omega_\infty := \{z \in \mathbb{C} \mid \exists n \in \mathbb{Z} : z^n = 1\}$ . נבדוק ש $(\Omega_\infty, \cdot)$  נעשה זאת ע"פ המקוצרת.

התנאי הראשון מתקיים כי 1 שייך ל $\Omega_\infty$ . עבור התנאי השני ניקח  $z_1, z_2 \in \Omega_\infty$  וצריך להוכיח כי  $z_1 \cdot z_2^{-1} \in \Omega_\infty$ . קיימים

$$z_1, z_2 \in \Omega_\infty \Rightarrow \exists n_1, n_2 \in \mathbb{Z} : z_1^{n_1} = z_2^{n_2} = 1 \text{ ואז } (z_1 \cdot z_2^{-1})^{n_1 n_2} = (z_1^{n_1})^{n_2} (z_2^{n_2})^{-n_1} = 1$$

להוכיח בבית כי {שורשי יחידה מסדר  $n$ }  $\Omega_n \geq \Omega_\infty$  לכל  $n$  טבעי גם כן תת חבורה.

**הגדרה:** חבורה  $(X, \cdot)$  נקראת ציקלית אם קיים איבר  $a \in X$  כך ש $\langle a \rangle := \{a^k \mid k \in \mathbb{Z}\}$  בעצם החזקות של  $a$ . נקרא היוצא של  $X$ .

דוגמה (1):  $\Omega_n = \langle w \rangle$  כאשר  $w = cis \frac{2\pi}{n}$  (יש עוד יוצרים למשועממים שביננו...אופק?)

דוגמה (2):  $(\mathbb{Z}, +)$ : כאשר  $\langle 1 \rangle = \{k \mid k \in \mathbb{Z}\}$  (כפולות).

דוגמה (3) חשובה:  $X$  לא ריקה. נגדיר פונקציות  $Map(X, X) = X^X := \{f: X \rightarrow X\}$  (הרכבה,  $\circ$ ) מונויד עם נייטרל  $id_x$  שהוא פונקציית הזהות. בעצם מדובר בהגדרת הרכבות של פונקציות.

$$\begin{aligned} (f_1 \circ f_2) \circ f_3 &= f_1 \circ (f_2 \circ f_3) \\ e &= id_x \\ 1_x & \end{aligned}$$

ואז נסמן {פונקציות חחע ועל  $X \rightarrow X$ }  $Gr(X^X) = \{f: X \rightarrow X \mid f(x) = x\}$  נקראת חבורה סימטרית.

**תרגיל:** לבנות טבלה של  $S_3$ .

דוגמה גם חשובה מאוד: שאריות מודולו  $n$ .

defined

**הגדרה:** מעל קבוצת השלמים מגדירים את יחס שקילות  $a \equiv b \pmod{n}$  ז"א שקיים מספר שלם  $q$  כך ש $ab = nq$ . שקול ל: יש אותה שארית ל $a, b$  מודולו  $n$ .

מגדירים פעולות מעל  $Z_n := \{[0], [1], \dots, [n-1]\}$  כך שכפל הוא  $[a] \cdot [b] := [a \cdot b]$  וחבור  $[a] \oplus [b] := [a + b]$ . צריך לבדוק שההגדרה לא תלויה בנציגים. ז"א, לבחור  $a_1 \equiv a_2 \pmod{n}, b_1 \equiv b_2 \pmod{n}$

## דביר חדד

ולראות שנגרר  $a_1 b_1 \equiv a_2 b_2$  and  $a_1 + b_1 \equiv a_2 + b_2$ .

**משפט 1:**  $(\mathbb{Z}_n, \oplus)$  חבורה ציקלית ולכן קומוטטיבית יוצר למשל [1] (יש עוד..)

**משפט 2:**  $(\mathbb{Z}_n, \cdot)$  מונויד קומוטטיבי.

לפתור בבית:  $6x \equiv 7 \pmod{35}$