

## אלגברה ב'1 – מבוא לתורת החבורות

- מבוסס על הרצאות של ד"ר אלעד פארן ועל הרשימות של פרופ' דן הרן.

### הרצאה 1 – 29.7.12

הגדרה: חבורה היא קבוצה  $G$  ופעולה  $*$  (לעיתים תסומן גם על ידי  $\cdot$ ), המקיימת את התנאים הבאים:

- I. סגירות:  $\forall a, b \in G: a * b \in G$
- II. קיבוציות/אסוציאטיביות:  $\forall a, b, c \in G: a * (b * c) = (a * b) * c$
- III. קיום איבר נייטרלי (הנקרא איבר היחידה):  $\exists e \in G. \forall a \in G: a * e = e * a = a$
- IV. קיום הפכי:  $\forall a \in G. \exists a^{-1} \in G: a * a^{-1} = a^{-1} * a = e$

קבוצות המקיימות את אקסיומות 1 ו-2 נקראות אגודה (*Semi-Group*), ואגודה בעלת איבר יחידה נקראת מונואיד (*Monoid*).

הערות:

- I. איבר היחידה הוא יחיד. הוכחה: נניח בשלילה ש- $e, e'$  הם איברי יחידה שונים בחבורה  $G$ . מתקיים:

$$e = e * e' = e'$$

- II. בחבורה מתקיימת אסוציאטיביות מוחלטת, כלומר בביטוי

$$a_1 * a_2 * \dots * a_k$$

אין זה משנה היכן נמקם סוגריים.

- III. האיבר ההופכי לאיבר נתון  $a \in G$  הוא יחיד. הוכחה: נניח שגם  $b \in G$  וגם  $c \in G$  הופכיים ל- $a$ . לכן:

$$ab = ba = 1 = ac = ca$$

$$\Rightarrow b * 1 = b * (ac) = (ba) * c = c$$

$$\Rightarrow b = c$$

- IV. לכל  $a \in G$  ו- $n \in \mathbb{Z}$  נגדיר את סימון החזקה באופן הבא:

$$a^n := \begin{cases} a * a^{n-1}, & n > 0 \\ 1, & n = 1 \\ a^{-1} * a^{n-1}, & n < 0 \end{cases}$$

וסימון זה מקיים את חוקי חזקות הזכורים לנו מן הממשיים:

$$(a^n)^k = a^{nk}, a^{n+k} = a^n * a^k$$

## דוגמאות:

- $\mathbb{Z}$  - ביחס לפעולת החיבור  $+$ , מהווה חבורה. האיבר הניטרלי בחבורה הוא 0.
- $\mathbb{Z}$  - ביחס לפעולת הכפל מהווה מונואיד, משום שלאיבר 0 אין הפכי.
- $\mathbb{Z}_2$  - ביחס לפעולת החיבור מודולו 2, מהווה חבורה.  $G = \{-1, 1\}$  ביחס לפעולת הכפל, חבורה.
- אם  $F$  שדה, אזי  $F$  ביחס לחיבור זו חבורה.
- עבור שדה  $F$ , קבוצת כל ההפיכים בשדה, המסומנת על ידי  $F^\times$ , מהווה חבורה ביחס לכפל.
- הקבוצה  $\mathbb{Z}$  ביחס לפעולת החיסור אינה חבורה, שכן פעולת החיסור אינה אסוציאטיבית.

הגדרה: חבורה  $G$  נקראת קומוטטיבית/חילופית/אבלית אם  $\forall a, b \in G: a \cdot b = b \cdot a$ .  
כל החבורות לעיל הינן חבורות אבליות.

דוגמה: נניח ש- $F$  שדה, ונסמן ב- $M_n(F)$  את אוסף המטריצות הריבועיות מסדר  $n \times n$  מעל  $F$ , אזי  $M_n(F)$  עם פעולת כפל מטריצות הינו מונואיד (ל- $O_n$  אין הפכי).  
נסמן ב- $GL_n(F)$  את אוסף המטריצות ההפיכות ב- $M_n(F)$ . זוהי חבורה ביחס לכפל מטריצות, אך היא אינה קומוטטיבית – כי כפל מטריצות אינו קומוטטיבי.

דוגמה: אם  $X$  קבוצה, נסמן ב- $S(X)$  את אוסף הפונקציות ההפיכות (חיייע ועל) מן  $X$  אל עצמה. זוהי חבורה ביחס לפעולת ההרכבה, בשל העובדות הבאות:

- הרכבה של פונקציות חיייע ועל היא גם חעייל.
- $Id$  הוא איבר היחידה ב- $S(X)$ .
- האיבר ההפכי של  $f$  הוא  $f^{-1}$ , לפי ההגדרה.

במקרה ש- $X = \{1, 2, \dots, n\}$ , נסמן ב- $S_n$  את  $S(X)$ . לאיברי  $S_n$  נקרא תמורות (פרמוטציות).

טענה:  $S_n$  חבורה, שאינה קומוטטיבית עבור  $n > 2$  (קל להוכיח זאת).

הגדרה: הסדר של חבורה סופית  $G$  הוא מספר האיברים בה. נסמנו  $|G| = o(G)$ .

דוגמה:  $|S_n| = n!$ .

הגדרה: חבורת קליין ( $Klein$ ) היא החבורה  $G = \{e, a, b, c\}$ , המוגדרת על ידי טבלת הפעולות הבאה:

|         |     |     |     |     |
|---------|-----|-----|-----|-----|
| $\cdot$ | $e$ | $a$ | $b$ | $c$ |
| $e$     | $e$ | $a$ | $b$ | $c$ |
| $a$     | $a$ | $e$ | $c$ | $b$ |
| $b$     | $b$ | $c$ | $e$ | $a$ |
| $c$     | $c$ | $b$ | $a$ | $e$ |

ניתן לבדוק שזו חבורה קומוטטיבית.

הגדרה: יהיו  $(G, \cdot)$ ,  $(H, *)$  חבורות. המכפלה הקרטזית  $G \times H = \{(g, h) \mid g \in G, h \in H\}$  מהווה חבורה עם הפעולה:  $(g_1, h_1) \cdot (g_2, h_2) := (g_1 g_2, h_1 h_2) \in G \times H$ . ואכן, קל לראות שמתקיימת תכונת האסוציאטיביות, איבר היחידה בחבורה הינו  $(e_G, e_H)$ , וההפכי של  $(g, h)$  הינו  $(g^{-1}, h^{-1})$ .

הערה: בסיכום זה, מעתה והלאה נסמן את כל הפעולות ב- $\cdot$ , ואת כל איברי היחידה ב- $e$ . בנוסף, אם אנו עוסקים בחבורה חיבורית, נסמן את הפעולה ב- $+$ .

דוגמה:  $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ . ניתן לראות שחבורה זו מסדר 4, ומקיימת את הטבלה של חבורת קליין בעמוד הקודם, לכן "למעשה" זו חבורת קליין.

תרגיל (חוק הצמצום): אם  $G$  חבורה,  $g, h, k \in G$  ומתקיים  $gh = gk$ , אזי  $h = k$ .

פתרון: נכפיל ב- $g^{-1}$  את שני אגפי המשוואה.

הגדרה: תהי  $G$  חבורה. נאמר ש- $G$  היא ציקלית/מעגלית אם קיים איבר  $g \in G$  כך ש:

$$G = \{g^n \mid n \in \mathbb{Z}\}$$

במקרה זה נאמר ש- $g$  יוצר של  $G$ , ונסמן  $G = \langle g \rangle$ .

דוגמה:  $(\mathbb{Z}, +)$  מקיימת  $\langle 1 \rangle = \langle -1 \rangle$ .

דוגמה:  $2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle$ .

דוגמה:  $\mathbb{Z}_2 = \langle 1 \rangle$ .

טענה + סימון:  $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$  עם חיבור מודולו  $n$  היא חבורה (קל להוכיח).

הערה: אם  $G$  חבורה ו- $g \in G$ , נסמן ב- $\langle g \rangle$  את אוסף החזקות של  $g$ .

טענה:  $\langle g \rangle$  היא תת חבורה של  $G$ , כלומר תת קבוצה שהיא עצמה חבורה ביחס לאותה פעולה.

הוכחה: חוקי חזקות.

טענה:  $\mathbb{Z}_n$  ציקלית.

הוכחה:  $\langle 1 \rangle \subseteq \mathbb{Z}_n$ . ניקח  $k \in \mathbb{Z}_n$ .

$$k = \overbrace{1+1+\dots+1}^k = 1^k \in \langle 1 \rangle$$

$$\Rightarrow \mathbb{Z}_n \subseteq \langle 1 \rangle \Rightarrow \mathbb{Z}_n = \langle 1 \rangle$$

דוגמה: חבורת קליין אינה ציקלית.

הוכחה:  $\langle e \rangle = \{e\}, \langle a \rangle = \{a, e\}, \langle b \rangle = \{b, e\}, \langle c \rangle = \{c, e\}$ .

הגדרה: אם  $g \in G$ , אזי הסדר של  $g$ , המסומן ב- $o(g)$ , הוא המספר הטבעי הקטן ביותר כך ש- $g^n = e$  (אם קיים כזה). אחרת, נאמר ש- $g$  מסדר אינסופי ונסמן  $o(g) = \infty$ , או  $o(g) = \aleph_0$ .

טענה: אם  $g \in G$ , אזי  $o(g) = |\langle g \rangle|$ .

הוכחה: נניח ש- $g$  מסדר אינסופי, אזי לכל  $i \neq j \in \mathbb{Z}$  מתקיים  $g^i \neq g^j$ , אחרת  $g^{i-j} = e$ . בסתירה להנחה. כלומר, הקבוצה  $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$  מכילה  $\aleph_0$  איברים שונים, כלומר אינסופית.

נניח ש- $o(g) = n$  סופי, נסמן  $\{e, g, g^2, \dots, g^{n-1}\}$  איברי הקבוצה. אחרת  $g^i = g^j, 1 < i < j < n$ , ואז  $g^{i-j} = e$ , אבל  $i-j < n$ , בסתירה למינימליות הסדר. לפיכך,  $\langle g \rangle$  מכילה לפחות  $n$  איברים שונים. כעת נראה להיפך, כלומר  $\langle g \rangle \subseteq \{e, g, g^2, \dots, g^{n-1}\}$ . נבחר איבר שרירותי  $g^k \in \langle g \rangle, k \in \mathbb{Z}$ , ונחלק עם שארית את  $k$  ב- $n$ :

$$\begin{aligned} k &= qn + r, \quad 0 \leq r \leq n-1 \\ g^k &= g^{qn+r} = (g^n)^q \cdot g^r = e^q \cdot g^r = g^r \in \{1, g, \dots, g^{n-1}\} \\ &\Rightarrow \langle g \rangle \subseteq \{1, g, g^2, \dots, g^{n-1}\} \\ &\Rightarrow o(g) = |\langle g \rangle| = n \end{aligned}$$

תרגיל: נתבונן ב- $\mathbb{Z}_4$ .

$$\begin{cases} o(0) = 1 \\ o(1) = 4 \\ o(2) = 2 \\ o(3) = 4 \end{cases} \Rightarrow \mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle$$

הערת אגב:  $\mathbb{Z}_4$  ציקלית, חבורת קליין לא. לכן הן לא איזומורפיות (ראה הגדרה הבאה).

הגדרה: יהיו  $G, H$  חבורות, ותהא  $\varphi: G \rightarrow H$  המקיימת  $\varphi(xy) = \varphi(x) \cdot \varphi(y)$ .

- נאמר ש- $\varphi$  הומומורפיזם.
- אם  $\varphi$  חח"ע נאמר ש- $\varphi$  מונומורפיזם (שיכון). נסמן:  $\hookrightarrow$ .
- אם  $\varphi$  על נאמר ש- $\varphi$  אפימורפיזם.
- אם  $\varphi$  חחעל נאמר ש- $\varphi$  איזומורפיזם.
- אם הומומורפיזם כך ש- $G = H$  נאמר ש- $\varphi$  אוטומורפיזם.

## הערות:

- I. אם קיים איזומורפיזם מ- $G$  ל- $H$ , נאמר ש- $G$  איזומורפית ל- $H$  ונסמן  $G \cong H$ .
  - II. כל חבורה איזומורפית לעצמה (הוכחה: איזומורפיזם הזהות).
  - III. אם  $G$  איזומורפית ל- $H$ , אזי  $H$  איזומורפית ל- $G$  (הוכחה: קיים לאיזומורפיזם הפכי).
  - IV. אם  $G$  איזומורפית ל- $H$ , ו- $H$  איזומורפית ל- $K$ , אזי  $G \cong K$  (הוכחה: הרכבת איזומורפיזמים).
- כלומר, יחס האיזומורפיה הינו יחס שקילות על חבורות.

דוגמה:  $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong$  חבורת קליין (ראינו זאת).

טענה:  $\mathbb{Z} \cong 2\mathbb{Z}$ .

הוכחה: אם  $n \in \mathbb{Z}$ , נגדיר  $\varphi(n) := 2n$ . ברור ש- $\varphi: \mathbb{Z} \rightarrow 2\mathbb{Z}$  היא חחעל. מתקיים

$$\varphi(n+k) = 2(n+k) = 2n + 2k = \varphi(n) + \varphi(k)$$

לכן  $\varphi$  איזומורפיזם.

טענה: אם  $H \cong G$  אז  $G$  ציקלית  $\Leftrightarrow H$  ציקלית.

הוכחה: נניח ש- $G$  ציקלית,  $G = \langle g \rangle$ , ונסמן  $h = \varphi(g)$ . יהי  $a \in H$ , לכן  $\varphi^{-1}(a) \in G$ , ולכן קיימת חזקה  $k \in \mathbb{Z}$  כך ש- $\varphi^{-1}(a) = g^k$ .

$$\Rightarrow a = \varphi(\varphi^{-1}(a)) = \varphi(g^k) = \varphi(g)^k = h^k$$

כלומר  $H = \langle h \rangle$ .

דוגמה: תהא  $(G, \cdot)$  חבורה ותהא  $G^{op}$  החבורה שאיבריה הם איברי  $G$  והפעולה \* מוגדרת

כך:  $g * h = h \cdot g$ . נראה ש- $G^{op}$  חבורה:

I. סגירות – ברור.

II. אסוציאטיביות:

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

III. איבר היחידה הוא אותו איבר יחידה.

IV. ההפכי ל- $g \in G^{op}$  הוא עדיין  $g^{-1}$ .

טענה:  $G \cong G^{op}$ .

הוכחה: נגדיר העתקה  $\varphi: G \rightarrow G^{op}$  עי"י  $\varphi(g) = g^{-1}$ . חחעל.

$$\varphi(g \cdot h) = h^{-1} \cdot g^{-1} = g^{-1} * h^{-1} = \varphi(g) * \varphi(h)$$

דוגמה:  $G = (\mathbb{C}, +)$ , אז פעולת ההצמדה היא אוטומורפיזם.

טענה: אם  $\varphi: G \rightarrow H$  הומומורפיזם, אזי :

$$\varphi(e) = e \quad .I$$

$$\forall g \in G. \varphi(g^{-1}) = \varphi(g)^{-1} \quad .II$$

הוכחה:

$$\varphi(e) = e \text{ מתקיים , ולפי חוק הצמצום } \varphi(e) \cdot \varphi(e) = \varphi(e) = \varphi(e) \cdot e \quad .I$$

$$\varphi(g) \cdot \varphi(g^{-1}) = \varphi(g \cdot g^{-1}) = \varphi(e) = e \quad .II$$

$$\Rightarrow \varphi(g^{-1}) = [\varphi(g)]^{-1}$$