

אלגברה ב' 1 - הרצאה 2 - 28.8.12

הגדרה: תהא G חבורה, $H \subseteq G$. נאמר ש- H תת חבורה של G , ונסמן $H \leq G$, אם H חבורה ביחס לפעולה של G . אם H תת חבורה ממש של G , נסמן $H < G$.

טענה: תהא G חבורה, $H \subseteq G$. $H \leq G$ אם ורק אם:

I. $H \neq \emptyset$ (שקול ל- $e \in H$).

II. $\forall a, b \in H. ab \in H$

III. $\forall a \in H. a^{-1} \in H$

למה: אם $H \leq G$, אזי $e_G = e_H$.

הוכחה:

$$\left. \begin{array}{l} e_H \cdot e_G = e_H \\ e_H \cdot e_H = e_H \end{array} \right\} \Rightarrow e_H \cdot e_H = e_H \cdot e_G \Rightarrow e_H = e_G$$

הוכחת הטענה:

\Leftarrow : I, II ברורים, שכן אם H חבורה אזי בוודאי יש בה איבר יחידה, וכן היא סגורה לפעולה. ניקח $a \in H$, אזי קיים לו הפכי ב- H , $b \in H$, $ba = ab = e$. ל- a גם קיים הפכי ב- G , $c \in G$, המקיים $ac = ca = e$.

$$\Rightarrow ba = ca \Rightarrow b = c \Rightarrow a^{-1} = c \in H$$

\Rightarrow נראה ש- H חבורה עם הפעולה של G . סגירות נובעת מ-II, אסוציאטיביות מושרת מהיות איברי H ב- G . לכל איבר ב- H קיים הפכי ב- H מתכונה 3.

איבר יחידה: ניקח $a \in H$, לפי III $a^{-1} \in H$, ומסגירות $a \cdot a^{-1} = e \in H$.

דוגמה: אם G חבורה, אזי $\{e\} \leq G$.

דוגמה: תהא $G = S_3$. נסמן: $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. מתקיים $\langle \sigma \rangle < G$, אך $\langle \sigma \rangle \neq G$.

תרגיל: נניח $G_1, G_2 \leq G$. צ"ל: $G_1 \cup G_2 \leq G \Leftrightarrow G_1 \leq G_2$ או $G_2 \leq G_1$.

פתרון: \Rightarrow ברור.

\Leftarrow : נניח בשלילה שקיימים $g_1 \in G_1 \setminus G_2$, $g_2 \in G_2 \setminus G_1$ כך ש- $g_1 \cdot g_2 \in G_1 \cup G_2$. נניח בלי הגבלת הכלליות $g_1 g_2 \in G_1$. מתקיים:

$$g_2 = (g_1^{-1} \cdot g_1) \cdot g_2 = g_1^{-1} \cdot (g_1 \cdot g_2) \in G_1$$

בסתירה להנחה.

טענה: אם G_1, G_2 חבורות, $\varphi: G_1 \rightarrow G_2$ הומומורפיזם, אזי $\text{Im } \varphi = \varphi(G_1) \leq G_2$.

הוכחה:

$$I. \varphi(e_{G_1}) = e_{G_2}$$

$$II. \varphi(g_1) \cdot \varphi(g_1') = \varphi(g_1 \cdot g_1') \in \text{Im } \varphi, \forall g_1, g_1' \in G_1. \varphi(g_1), \varphi(g_1') \in \text{Im } \varphi$$

III. נניח ש- $\varphi(g_1) \in \text{Im } \varphi$. אזי:

$$(\varphi(g_1))^{-1} = \varphi(g_1^{-1}) \in \text{Im } \varphi$$

$$\Rightarrow \text{Im } \varphi = \varphi(G_1) \leq G_2$$

הערה: אם $\varphi: G_1 \rightarrow G_2$ מונומורפיזם, אזי הצמצום $\varphi: G_1 \rightarrow \text{Im } \varphi$ הוא איזומורפיזם.

סימונים: יהיו חבורה $G, g \in G, A, B \subseteq G$ תתי-קבוצות. נסמן:

$$Ag = \{ag \mid a \in A\} \bullet$$

$$gA = \{ga \mid a \in A\} \bullet$$

$$AB = \{ab \mid a \in A, b \in B\} \bullet$$

$$A^{-1} = \{a^{-1} \mid a \in A\} \bullet$$

תרגיל: (נובע מההגדרות)

$$(AB)C = A(BC) \bullet$$

$$A = B \Leftrightarrow Ag = Bg \bullet$$

$$eA = Ae = A \bullet$$

$$(AB)^{-1} = B^{-1}A^{-1} \bullet$$

תרגיל: יהיו G, H חבורות.

$$I. \forall h \in H : hH = Hh = H, H^{-1} = H, H \cdot H = H \text{ אזי } H \leq G$$

$$II. \text{ אם } H \leq G \text{ אזי } \forall g \in G : gHg^{-1} \leq G \text{ (פעולה זו נקראת הצמדה).}$$

פתרון:

$$I. \text{ כל } h \in H \text{ נוכל לכתוב כך: } h = h \cdot e \in H \cdot H \text{ לכן } H \subseteq H \cdot H \text{ . אולם,}$$

$$H \cdot H \subseteq H \text{ , לכן } H = H \cdot H$$

ברור ש- $H = H^{-1}$, שכן בחבורה יש סגירות להפכי.

$$hH \subseteq H \text{ אם } h \in H \text{ או } h = h(h^{-1}h) \in hH \text{ , ולכן } hH = Hh = H$$

$$II. gHg^{-1} = \{ghg^{-1} \mid h \in H\} \text{ . נראה שזו תת-חבורה.}$$

$$\text{יחידה: } e = g \cdot e \cdot g^{-1} \in gHg^{-1}$$

$$\text{סגירות: } (gh_1g^{-1}) \cdot (gh_2g^{-1}) = gh_1h_2g^{-1} \in gHg^{-1}$$

$$\text{הפכי: } (ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$$

לעיתים נסמן את פעולת ההצמדה באופן הבא: $h^g := ghg^{-1}$.

למה: יהיו $H \leq G$, $g_1, g_2 \in G$. התנאים הבאים שקולים:

$$I. \quad g_1H = g_2H$$

$$II. \quad g_1H \subseteq g_2H$$

$$III. \quad g_1H \cap g_2H \neq \emptyset$$

$$IV. \quad g_1 \in g_2H$$

$$V. \quad g_2^{-1}g_1 \in H$$

לקבוצה מהצורה gH קוראים מחלקה (Coset) שמאלית של H ב- G .

הוכחה: $I \Leftrightarrow II \Leftrightarrow III$ ברור.

$IV \Leftrightarrow III$: נניח ש- $g_1h_1 = g_2h_2$ שייך לחיתוך.

$$\Rightarrow g_1 = g_2(h_2h_1^{-1}) \in g_2H$$

$V \Leftrightarrow IV$: קיים h כך ש:

$$g_1 = g_2h \Rightarrow g_2^{-1}g_1 = h \in H$$

$I \Leftrightarrow V$: ניקח איבר $g_1h \in g_1H$:

$$g_1h = g_2 \overbrace{((g_2^{-1}g_1) \cdot h)}^{\in H} \in g_2H$$

ולכן $g_1H \subseteq g_2H$, ומשיקולי סימטריה $g_1H = g_2H$. \square

הגדרה/סימון: את אוסף המחלקות השמאליות של H ב- G נסמן $G/H = \{hG \mid h \in H\}$. יש מקומות בהם מסמנים את אוסף המחלקות הימניות כ- $G \setminus H$, אך בסיכום זה נשתמש בסימון זה כסימון המקובל בתורת הקבוצות למשלים. את העצמה של G/H מסמנים $[G:H]$ - האינדקס של H ב- G .

דוגמה:

$$H = 4\mathbb{Z}, \quad G = \mathbb{Z}$$

$$G/H = \mathbb{Z}/4\mathbb{Z} = \{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$$

$$\Rightarrow [\mathbb{Z}:4\mathbb{Z}] = 4 = |\mathbb{Z}/4\mathbb{Z}|$$

משפט (לגראנז'): אם $H \leq G$ סופית, אזי $|G| = |H| \cdot [G:H]$.

הוכחה: לפי הלמה, ניתן לכתוב את G כאיחוד זר של מחלקות, כלומר $G \doteq \bigcup_{A \in G/H} A$.

כל מחלקה ניתן להציג בדרכים רבות, לכן: $G = \bigcup_{i \in I} g_iH$, כאשר $\{g_i \mid i \in I\}$ מערכת נציגים של

H ב- G . כל נציג מקיים $|g_iH| = |H|$, לכן $|G| = |G/H| \cdot |H| = [G:H] \cdot |H|$. \square

מסקנה: $|G| = [G:H] \cdot |H|$.

מסקנה: סדר של איבר בחבורה מחלק את סדר החבורה.

הוכחה: $o(g) = |\langle g \rangle|$, תת-חבורה של G . \square

מסקנה: כל חבורה מסדר ראשוני היא ציקלית.

הוכחה: נניח $|G| = p$ ראשוני. נבחר $e \neq g \in G$. לפיכך:

$$\begin{aligned} & \{e\} \neq \langle g \rangle \\ \Rightarrow & 1 \neq |\langle g \rangle| \mid p \\ \Rightarrow & |\langle g \rangle| = p \\ \Rightarrow & \langle g \rangle = G \quad \square \end{aligned}$$

מסקנה: כל חבורה מסדר ראשוני p איזומורפית ל- \mathbb{Z}_p .

הוכחה: נניח $|G| = p$ ונניח ש- $\{1, g, g^2, \dots, g^{p-1}\} = G = \langle g \rangle$.

נגדיר העתקה $\varphi: G \rightarrow \mathbb{Z}_p$ ע"י $\varphi(g^i) = i$. קל לבדוק שההעתקה היא איזומורפיזם המוגדר היטב. \square

טענה: אם G ציקלית מסדר אינסופי, אזי $G \cong \mathbb{Z}$.

הוכחה: מגדירים איזומורפיזם בדומה למסקנה האחרונה.

תרגיל: G חבורה, $g \in G$, אזי $g^m = e$ אם ורק אם $m \mid o(g)$. (ראינו כבר).

מסקנה: כל החבורות מסדר 4 הן \mathbb{Z}_4 וחבורת קליין (עד כדי איזומורפיזם).

הוכחה: אם G ציקלית, אז $G \cong \mathbb{Z}_4$. לכן נניח ש- G אינה ציקלית. לפי משפט לגרנו' הסדר של

כל האיברים פרט לאיבר היחידה הוא 2. נסמן $G = \{a, b, c, e\}$, ואז $a^2 = b^2 = c^2 = e$, ואין

ברירה ומתקיים $ab = c, ac = b, bc = a$ - וזו חבורת קליין. \square

תת חבורות נורמליות

היו $H \leq G$ חבורות, נתבונן באוסף המחלקות $G/H = \{gH \mid g \in G\}$. ננסה להגדיר ממנה

$$(g_1H) \cdot (g_2H) := g_1g_2H$$

נבדוק: אסוציאטיביות: קל.

$$H \cdot g_1H = g_1H : H \text{ איבר יחידה}$$

$$(gH)^{-1} = g^{-1}H \in G/H : \text{איבר הפכי}$$

לכן נדמה שזו חבורה.

בעיה: האם הכפל מוגדר היטב בין מחלקות (כלומר, לא תלוי בנציג שנבחר מן המחלקה).

תשובה: לא תמיד. לכן נעבור להגדרה הבאה.

הגדרה: תת חבורה $H \leq G$ נקראת נורמלית, אם מתקיים $gH = Hg$ לכל $g \in G$. נסמן

$$H \triangleleft G \text{ - נורמלית ב- } G.$$

למה: התנאים הבאים שקולים:

$$I. N \triangleleft G$$

$$II. \forall g \in G: gNg^{-1} = N$$

$$III. \forall g \in G: gNg^{-1} \subseteq N$$

הוכחה: $I \Rightarrow III$: N נורמלית ב- G , כלומר לכל $g \in G$ מתקיים $gN = Ng$. נכפול משמאל ב-

$$g^{-1} \text{ ונקבל } gNg^{-1} = N$$

$III \Rightarrow II$: יהי $g \in G$, עבורו מתקיים $gNg^{-1} \subseteq N$. תנאי III מתקיים לכל איברי G , ולכן גם

$$gNg^{-1} = N \Leftarrow N \subseteq gNg^{-1} \Leftarrow g^{-1}Ng \subseteq N : \text{לכן}$$

$$II \Rightarrow I : gNg^{-1} = N : \text{לכן, } gN = gN(g^{-1}g) = (gNg^{-1})g = Ng \quad \square$$

טענה: אם $N \triangleleft G$ אזי הפעולה $(g_1N) \cdot (g_2N) := g_1g_2N$ מוגדרת היטב, כלומר אינה תלויה

בנציגים.

הוכחה: נניח $g_1N = g_1'N$, $g_2N = g_2'N$. נראה $g_1g_2 = g_1'g_2'$.

$$g_1g_2N = g_1'(g_1')^{-1}g_1g_2N = g_1' \underbrace{(g_1')^{-1}g_1}_{\in N} Ng_2 = g_1'Ng_2 = g_1'g_2'(g_2')^{-1}Ng_2$$

$$= g_1'g_2' \underbrace{(g_2')^{-1}g_2}_{\in N} N = g_1'g_2'N \quad \square$$

מסקנה: אם $N \triangleleft G$ אז G/N עם הפעולה שהגדרנו זו חבורה. חבורה זו נקראת חבורת המנה

של N ב- G .

טענה: אם H תת-חבורה של חבורה אבלית G , אזי $H \triangleleft G$.

הוכחה: אם $g \in G$, אזי $gh = hg$, $\forall h \in H$, ולכן $gH = Hg$. \square

הגדרה: תהי G חבורה, $\varphi: G \rightarrow K$ הומומורפיזם לחבורה אחרת K . הגרעין של φ מוגדר להיות:

$$\ker \varphi = \{g \in G \mid \varphi(g) = e\}$$

טענה: $\ker \varphi \triangleleft G$.

הוכחה: ניתן לבדוק שזו תת-חבורה ישירות מההגדרה. נראה שהיא נורמלית.

יהיו $g \in G, n \in \ker \varphi$. מספיק להוכיח $gng^{-1} \in \ker \varphi$.

$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g^{-1}) = \varphi(g) \cdot e \cdot \varphi(g^{-1}) = \varphi(g \cdot g^{-1}) = \varphi(e) = e$$

ואכן $gng^{-1} \in \ker \varphi$. \square

טענה: הומומורפיזם $\varphi: G \rightarrow K$ הוא מונומורפיזם אם ורק אם $\ker \varphi = \{e\}$. (הוכחה – בדומה לאיך מוכיחים עבור העתקות לינאריות ופונקציות).

דוגמה: $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_2$, $\varphi(2a+b) = b$, $b \in \{0,1\}$. קל להוכיח שזהו הומומורפיזם. מתקיים:

$$\ker \varphi = \{a \in \mathbb{Z} \mid \varphi(a) = 0\} = 2\mathbb{Z}$$