# אלגברה לינארית 2

הרצאה מס' 22 – 02/6/2009

## חבורות – המשך

מטרת השיעור הזה היא להוכיח את משפט לגרנז' בחבורות. השיעור הזה כרמית חולה ולכן בועז החליף אותה. היה כיף חיים, תהנו ☺

**הגדרה**: תהי $G$ חבורה, $H$ תת-חבורה (חבורה חלקית) של $G$. עבור איבר $g \in G$ כלשהו, הקבוצה $gH = \{g \cdot h \mid h \in H\}$ קרויה *מחלקה של $H$*.

**דוגמה**:

$G = \mathbb{Z}_5^*$ $H = < 4 > = \{1,4\}$. נחשב את $2H$, $3H$, $4H$, $1H$.

$4H = \{4 \cdot 1, 4 \cdot 4\} = \{4,1\}$
$1H = \{1 \cdot 1, 1 \cdot 4\} = \{1,4\}$

$2H = \{2 \cdot 1, 2 \cdot 4\} = \{2,3\}$
$3H = \{3 \cdot 1, 3 \cdot 4\} = \{3,2\}$

☺ באופן כללי, $H$ היא תמיד אחת המחלקות של $G$ (נקח $g = 1_G$ ואז $1_G H = H$.

**דוגמה**:

עבור $H$ מהדוגמה הקודמת, מהו *אוסף המחלקות של $H$*?

$$\{gH \mid g \in G\} = \{1H, 2H, 3H, 4H\} = \{\{1,4\},\{2,3\},\{2,3\},\{1,4\}\} = \{\{1,4\},\{2,3\}\}$$

**טענה**: תהי $G$ חבורה סופית, ו- $H$ ת"ח (תת-חבורה) של $G$, אזי:

**א.** לכל איבר $g \in G$ מתקיים: $|gH| = |H|$.

**ב.** לכל איבר $h \in H$ מתקיים: $hH = H$.

**הוכחה**

**א.** נסמן $H = \{h_1, \dots, h_m\}$ כאשר $m = |H|$. אז $gH = \{gh_1, \dots, gh_m\}$. בבירור מספר האיברים הוא לכל היותר $m$. יותר מכך, יש בדיוק $m$ איברים, שכן אם $gh_i = gh_j$ אז $g^{-1}gh_i = g^{-1}gh_j$, כלומר $h_i = h_j$.

**ב.** יהי $h \in H$. $H$ חבורה, ולכן מתקיימת סגירות, ומכאן $hH \subseteq H$. נניח עד"ש (על דרך השלילה) כי אין שיוויון, כלומר $hH \subset H$, אך $H$ סופית, ולכן $|hH| < |H|$. בסתירה לסעיף א.

**הערה**: הטענה הזו וגם טענות נוספות נכונות עבור חבורות סופיות ואינסופיות כאחד. אולם בקורס הזה, אנו מתעסקים אך ורק בחבורות סופיות.

**דוגמה**:

$G = \mathbb{Z}_{12}$, $H = <3> = \{0,3,6,9\}$. נחשב את המחלקות $1+H,\ 2+H,\ 3+H,\ 4+H$.

$1+H = \{1+0, 1+3, 1+6, 1+9\} = \{1,4,7,10\}$

$2+H = \{2+0, 2+3, 2+6, 2+9\} = \{2,5,8,1\}$

$3+H = \{3+0, 3+3, 3+6, 3+9\} = \{0,3,6,9\} = H$

$4+H = \{4+0, 4+3, 4+6, 4+9\} = \{4,7,10,1\} = 1+H$

**טענה**: עבור חבורה $G$, ו- $H$ תת-חבורה של $G$ מתקיים שכל שתי מחלקות הן זרות או זהות.

**הוכחה**

אם $g_2H$ ו- $g_1H$ זרות אז סיימנו. נניח אם כן $g_1H \cap g_2H \neq \phi$. מכאן קיימים $h', h'' \in H$ כך ש- $g_1h' = g_2h''$. ומכאן $g_1 = g_2h''(h')^{-1}$ $(*)$.

די להראות כי $g_1H \subseteq g_2H$ (סימטריות). לכן נניח $z \in g_1H$, ונוכיח כי $z \in g_2H$. ובכן, מההנחה קיים $h \in H$ כך ש- $z = g_1h$.

אבל מ- $(*)$ נובע $z = g_2h''(h')^{-1}h$. ואז מסגירות $z \in g_2 + 1$.

מ.ש.ל

**משפט (לגרנז')**: תהי $G$ חבורה סופית, ו- $H$ תת-חבורה של $G$. אזי $|H| \mid |G|$ (קרי: $|H|$ מחלק את $|G|$).

**הוכחה**

יהיו $g_1H, \dots, g_nH$ אוסף כל המחלקות של $H$ ($G = \{g_1, \dots, g_n\}$). מהטענות הקודמות כל שתי מחלקות זרות או שוות, וגודל כל אחת מהן הוא $|H|$.

נסתכל על $k$ המחלקות השונות של $H$ ($k \leq n$) (ללה"כ $g_1H, \dots, g_kH$). נראה כי $G = g_1H \uplus g_2H \uplus \cdots \uplus g_kH$.

ההכלה $\supseteq$ ברורה. נוכיח את ההכלה $\subseteq$. יהי $g \in G$. קיים ש- $g \in gH$ (משום ש- $1_G \in H$, ולכן $gH = \{g \cdot 1_G, \dots\}$). בהכרח קיים $1 \leq i \leq k$ כך ש- $gH = g_iH$, ולכן $g \in g_iH$ מסויים.

כעת, $|G| = |g_1H| + |g_2H| + \cdots + |g_kH|$. אבל כל מחלקה היא בגודל $|H|$, ולכן $|G| = k|H|$. כנדרש.

**הערה**: $\uplus$ = איחוד זר.

**מסקנה**: תהי $G$ חבורה סופית, ו- $g \in G$.

א. $o(g) \mid |G|$.

ב. $g^{|G|} = 1_G$.

**הוכחה**

א. נקח את תת החבורה הנוצרת על-ידי $g$, כלומר את $H = < g >$. קיים ש- $|H| = o(g)$. ($t = o(g)$ הוא החזקה הקטנה ביותר כך ש- $g^t = 1$, ואילו $< g >$ היא אוסף החזקות של $g$).

וממשפט לגרנז' $|H| \mid |G|$, כלומר $o(g) \mid |G|$.

ב. נסמן $t = o(g)$. כעת, $g^{qt} = (g^t)^q = 1_G^q = 1_G$ $\underset{\substack{\downarrow \\ \text{לכן } t \mid |G| \\ \text{יש } q \text{ שלם כך ש} \\ tq=|G|}}{=}$ $g^{|G|}$.

**הערות**:

1) הכיוון ההפוך של משפט לגרנז' אינו נכון. כלומר, אם $H$ תת קבוצה של $G$ (לאו דווקא תת-חבורה, ומתקיים $|H| \mid |G|$, אז לא בהכרח $H$ תת-חבורה.

למשל, $|S_5| = 120$ אבל אין בה תת-חבורה מסדר 40, למרות ש- $40|120$.

2) בחבורה ציקלית מסדר $m$ מתקיים שלכל $n$ המחלק את $m$ יש תת-חבורה אחת ויחידה מסדר $n$ (במילים אחרות, המשפט ההפוך ללגרנז' נכון במקרה של חבורה ציקלית).

**תרגיל**: נסי להוכיח זאת (לא חובה)

**דוגמה**:

$G = \mathbb{Z}_{12}$. זאת חבורה ציקלית מסדר 12, כי למשל $< 1 > = \mathbb{Z}_{12}$. לכל $m \mid 12$ יש תת-חבורה מסדר $m$:

☺ $2 \mid 1 \Leftarrow < 0 > = \{0\}$

☺ $12 \mid 2 \Leftarrow < 6 > = \{0,6\}$

☺ $12 \mid 3 \Leftarrow < 4 > = \{0,4,8\}$

☺ $12 \mid 4 \Leftarrow < 3 > = \{0,3,6,9\}$

☺ $12 \mid 6 \Leftarrow < 2 > = \{0,2,4,6,8,10\}$

☺ $12 \mid 12 \Leftarrow < 1 > = \mathbb{Z}_{12}$.

**הערה**: ניתן להוכיח כי $\mathbb{Z}_p^*$ היא ציקלית כאשר $p$ ראשוני.

**דוגמה**: נמצא יוצר של $\mathbb{Z}_{23}^*$. ניתן היה לחשב עבור על איבר את החבורה שהוא יוצר. אבל זה היה לוקח הרבה זמן והרבה חישובים, שניתן לקצר.

נמצא את הסדר של 2. ממסקנה של משפט לגרנז', $o(2) \mid |\mathbb{Z}_{23}^*| = 22$. לכן $o(2) \in \{1,2,11,22\}$. קל לראות כי $o(2) \neq 1,2$. נוכיח כי $o(2) = 11$ (על-ידי חישובי חזקות):

$$2^1 = 2, \qquad 2^2 = 4, \qquad 2^4 = (2^2)^2 = 4^2 = 16, \qquad 2^8 = (2^4)^2 = 256 \overset{mod\ 23}{=} 3$$

$$2^{11} = 2^8 2^3 = 3 \cdot 8 = 24 = 1$$

$\Leftarrow$ 2 לא יוצר. כך עוברים לשאר:

$$3^1 = 3, \qquad 3^2 = 9, \qquad 3^4 = 81 = 12, \qquad 3^8 = 12^2 = 144 = 6, \qquad 3^{11} = 24 = 1$$

$\Leftarrow o(3) = 11 \Leftarrow$ גם 3 לא יוצר.

**הערה**: בועז חשב ש-2 יהיה הסדר, ותכנן להוכיח ש- $o(2) \neq 11$, ולכן $o(2) = 22$, ולכן הוא היוצר. אבל משהו השתבש בדרך.

## שיעורי בית

מחלק ד': 3) ב,ג; 7) 8) 9) 13)

מסמך זה הגיע אליך מאתר תלמידונת
מסמכים נוספים ניתן למצוא בכתובת http://talmido.net
רשת חברתית לשיתוף תכנים אקדמים