הרצאה 5

מחלקות של תת-חבורה ומשפט לגראנז'

הגדרה 1. מספר האיברים בחבורה נקרא סדר החבורה.

הגדרה 2. תהי H תת-חבורה כלשהי של חבורה G. תת-קבוצה של G מהצורה $g*H := \{g*h \mid h \in H\}$ נקראת מחלקה שמלית (או קוסט שמאלי) של H.
תת-קבוצה של G מהצורה $H*g := \{h*g \mid h \in H\}$ נקראת מחלקה ימנית (או קוסט ימני) של H.

אם G חבורה אבלית, אז אין הבדל בין מחלקות ימניות ומחלקות שמאליות.
אם H תת-חבורה טריביאלית, אז כל מחלקה ימנית(שמאלית) מכילה איבר אחד בלבד.

דוגמה 1.
אם $G = \mathbf{Z}_{12}, H = \{0,3,6,9\}$ אז המחלקות של H הן:

$$0+H = H;\ 1+H = \{1,4,7,10\};\ 2+H = \{2,5,8,11\};$$
$$3+H = \{0,3,6,9\};\ 4+H = \{1,4,7,10\};\ 5+H = \{2,5,8,11\};$$
$$6+H = \{0,3,6,9\};\ 7+H = \{1,4,7,10\};\ 8+H = \{2,5,8,11\};$$
$$9+H = \{0,3,6,9\};\ 10+H = \{1,4,7,10\};\ 11+H = \{2,5,8,11\}.$$

דוגמה 2.
אם $G = S_3, H = \left\{id, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right\}$ אז המחלקות השמאליות של H הן:

$$id \cdot H = H; \qquad \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \cdot H = H;$$
$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \cdot H = \left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}; \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \cdot H = \left\{\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\};$$
$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \cdot H = \left\{\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\}; \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \cdot H = \left\{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\};$$

המחלקות הימניות של H הן:

$$H \cdot id = H; \qquad H \cdot \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = H;$$
$$H \cdot \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\}; H \cdot \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \left\{\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\};$$
$$H \cdot \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \left\{\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}; H \cdot \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \left\{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\};$$

טענה 1. תהי H תת-חבורה כלשהי של חבורה G. אז:
1. $\forall g \quad g \in g*H$
2. $g_1 \in g_2*H \Leftrightarrow g_1*H = g_2*H$.
3. $\forall g_1\ \forall g_2 \quad (g_1*H = g_2*H) \vee (g_1*H \cap g_2*H) = \varnothing$.
4. $\forall g \mid g*H \mid = \mid H \mid$.

הוכחה.
1. $g = g*e \in g*H$.

2. מפני ש- $g_1 \in g_1*H$, כיוון $\Leftarrow$ טריביאלי. נניח ש- $g_1 \in g_2*H$ ונוכיח ש- $g_1*H = g_2*H$. מהשייכות $g_1 \in g_2*H$ נובע שקיים $h \in H$ כך ש- $g_1 = g_2*h$.
מהגרירות הבאות נובע ש- $g_1*H = g_2*H$.

$$x \in g_1 * H \Rightarrow \exists h_1 \in H \;\; x = g_1 * h_1 = g_2 * h * h_1 \Rightarrow x \in g_2 * H$$
$$x \in g_2 * H \Rightarrow \exists h_2 \in H \;\; x = g_2 * h_2 = g_1 * h^{-1} * h_1 \Rightarrow x \in g_1 * H .$$

3. אם $g_1 * H \cap g_2 * H = \varnothing$, אז אין מה להוכיח. נניח שקיים $g \in g_1 * H \cap g_2 * H$ אז, לפי סעיף 2, $g_1 * H = g * H$ ו $g_2 * H = g * H$.

4. נביט בפונקציה $f_g : H \to g * H$ המוגדרת ע"י הנוסחה $f_g(h) = g * h$. מספיק להוכיח ש- f_g הפיכה.

f_g שלמה לפי הגדרתה. f_g חד-חד-ערכית, מפני ש:

$$f_g(h_1) = f_g(h_2) \Rightarrow g * h_1 = g * h_2 \Rightarrow g^{-1} * g * h_1 = g^{-1} * g * h_2 \Rightarrow h_1 = h_2 .$$

f_g פונקצית על, כי לכל $y \in g * H$ קיים $h \in H$ כך ש- $y = g * h$.

מ.ש.ל.

<u>**הערה.**</u> אותן תכונות תיתן להוכיח גם למחלקות הימניות של H.

<u>**הגדרה 2.**</u> מספר המחלקות השמאליות של תת-חבורה $H \leq G$ נקרא <u>האינדקס</u> של H ב- G ומסומן כ- $[G : H]$.

<u>**משפט 2. (משפט לגראנז'):**</u>

תהי H תת-חבורה כלשהי של חבורה סופית G. אז $[G : H] = \frac{|G|}{|H|}$.

<u>**הוכחה.**</u>

נגדיר את סידרת איברים $g_k \in G$ באופן אינדוקטיבי:

א. $g_1 = e$.

ב. אם $G \setminus (g_1 * H \cup ... g_{k-1} * H) \neq \varnothing$ אז נבחר איבר $g_k \in G \setminus (g_1 * H \cup ... g_{k-1} * H)$ באופן אקראי.

מפני ש- G חבורה סופית אנו נקבל קבוצה סופית של איברים: $g_1,..., g_m$. מבניית הסידרה וטענה 1, חלק 3, נובע שהמחלקות $g_i * H, i = 1,..., m$ זרות זו מזו. מבניית הקבוצה $g_1,..., g_m$ גם נובע ש- $g_1 * H \cup ... \cup g_m * H = G$. לכן $|G| = |g_1 * H| + ... + |g_m * H|$. מטענה 1, חלק 4, נובע ש- $|g_i * H| = |H|$ לכל $i = 1,...,m$. מכאן נובע ש- $m|H| = |G|$. המחלקות $g_1H,..., g_mH$ שונות זו מזו. נביט במחלקה כלשהי $g * H, g \in G$. מהשוויון $g_1 * H \cup ... \cup g_m * H = G$ נובע שקיים $i \in \{1,...,m\}$ כך ש- $g \in g_i * H$. מסעיף 2 של טענה 1 נובע ש- $g * H = g_i * H$. לכן כל מחלקה ימנית של H שווה לאחת מהמחלקות: $g_1 * H,..., g_m * H$ ולכן $m = [G : H]$.

מ.ש.ל.

<u>**הערה.**</u> באופן דומה ניתן להראות שמספר המחלקות הימניות גם שווה ל- $\frac{|G|}{|H|}$.

לכן מספר המחלקות הימניות שווה למספר המחלקות השמאליות ושווה ל- $\frac{|G|}{|H|}$.

מפני שהאינדקס $[G : H]$ תמיד מספר טבעי, אנו מקבלים

<u>מסקנה 3.</u> אם $H \le G$ ו G חבורה סופית, אז $|H|$ מחלק את $|G|$.

<u>בעיה 1.</u> תהי $H \le G$ תת-חבורה כלשהי של חבורה G. נגדיר יחס בינארי מעל G :

$$x \sim y \Leftrightarrow x * y^{-1} \in H \quad .$$

הוכח שיחס הנ"ל הוא יחס שקילות והמחלקות השקילות שלו שוות למחלקות השמאליות של H .

<u>בעיה 2.</u> תהי $H \le G$ תת-חבורה כלשהי של חבורה G. הוכח שתת-קבוצה $S \subseteq G$ תהיה מחלקה ימנית של H אם ורק אם הקבוצה $S^{-1} = \{s^{-1} \mid s \in S\}$ היא מחלקה שמאלית של H.