אלגברה ב' 1 - הרצאה 7 - 19.9.12

<u>תרגיל</u>: כמה חבורות 5–סילוב יש ב- S_5? לפי משפטי סילוב מתקיים:

$$|S_5| = 120 = 5 \cdot 24$$

$$\begin{cases} n_5 \equiv 1 (\mathrm{mod}\, 5) \\ n_5 \mid 24 \Rightarrow n_5 \in \{1,2,3,4,6,8,12,24\} \end{cases}$$

$$\Downarrow$$

$$n_5 \in \{1,6\}$$

אם $n_5 = 1$, אז יש ב- S_5 בדיוק חבורה אחת H מסדר 5, וכל איבר שהסדר שלו הוא 5 שייך לחבורה H. בחבורה H יש בדיוק $5-1=4$ איברים מסדר 5, ולכן ב- S_5 יש בדיוק 4 איברים מסדר 5. אולם, ב- S_5 כל מעגל מאורך 5 הוא מסדר 5, ויש $(5-1)! = 24$ מעגלים כאלו, וזו סתירה לגודל H, לכן $n_5 = 6$.

<u>תרגיל</u>: כמה חבורות 3-סילוב יש ב- S_4?

$$|S_4| = 24 = 3 \cdot 8$$

$$\begin{cases} n_3 \equiv 1 (\mathrm{mod}\, 3) \\ n_3 \mid 8 \Rightarrow n_3 \in \{1,2,4,8\} \end{cases}$$

$$\Downarrow$$

$$n_3 \in \{1,4\}$$

נניח $n_3 = 4$, אזי יש 4 חבורות מסדר 3 ב- S_4, וכל חבורה כזו תורמת 3 איברים מסדר 3 (כל שתי חבורות כאלו או שוות או בעלות חיתוך טריוויאלי). לפיכך, ב- S_4 יש לפחות 9 איברים מסדר 3. אולם, מספר האיברים מסדר 3 ב- S_4 זהו מספר המעגלים מגודל 3, שהוא $\binom{4}{3} \cdot (3-1)! = 8$, סתירה. לכן $n_3 = 1$.

<u>למה</u>: תהא G חבורה סופית, $N \lhd G$, P חבורת $p-$סילוב. אזי:

I. $P \cap N$ היא חבורת $p-$סילוב ב- N.

II. PN/N היא $p-$סילוב ב- G/N.

<u>הוכחה</u>: מתקיים $P \le PN \le G$. לפי משפט לגראנז' $[G:P] = [G:PN][PN:P]$. $[G:P]$ זר ל- p, ולכן $[G:PN],[PN:P]$ זרים ל- p. לפי משפט האיזומורפיזם השני, $PN/N \cong P/P \cap N$, ובפרט $\frac{|P|}{|P \cap N|} = \frac{|PN|}{|N|}$. בנוסף, $P \cap N \le P$, לכן $P \cap N$ זו חבורת- p. מתקיים:

$$[N:P\cap N]=\frac{|N|}{|P\cap N|}=\frac{|PN|}{|P|}=[PN:P]$$

ולכן $[N:P\cap N]$ זר ל- p, ולכן $P\cap N$ זו תת-חבורת $p-$סילוב של N.
$P/P\cap N$ זו מנה של חבורת- p, ולכן היא חבורת- p, ולכן גם PN/N זו חבורת- p. לפי משפט האיזומורפיזם השלישי $[G/N:PN/N]=[G:PN]$, ולכן גם $[G/N:PN/N]$ זר ל- p, כלומר PN/N זו תת-חבורה $p-$סילוב של G/N. ▨

<u>תרגיל</u>: תהא G חבורה מסדר pq, כאשר $q<p$ ראשוניים. אזי:
א. G פתירה.
ב. אם $q\nmid p-1$, G ציקלית.

<u>הוכחה</u>: א. $n_p\in\{1,q\}\Leftarrow n_p\mid q,\ n_p\equiv 1(\mathrm{mod}\ p)$. אם $n_p=q$ אזי $q-1\equiv 0(p)$, כלומר $p\mid q-1$, אבל $p>q$, סתירה. לכן $n_p=1$. מכאן, יש תת-חבורה יחידה P מסדר p, ולכן $P\lhd G$. $|P|=p$ מסדר ראשוני, לכן ציקלית, בפרט אבלית, ובפרט פתירה. G/P מסדר q, ולכן גם היא ציקלית $\leftarrow$ אבלית $\leftarrow$ פתירה. הוכחנו שאם P ו- G/P פתירות אז גם G פתירה, ולכן סיימנו.
ב. $n_q\in\{1,p\},\ n_q\equiv 1(q)$. אם $n_q=p$, אזי $p-1\equiv 0(q)$, כלומר $q\mid p-1$ בסתירה להנחה. לכן $n_q=1$, כלומר קיימת תת-חבורה יחידה $Q\lhd G$ מסדר q. מתקיים $P\cap Q=\{e\}$, $|P||Q|=|G|$, $P,Q\lhd G$, ולפיכך $G\cong P\times Q\cong\mathbb{Z}_p\times\mathbb{Z}_q=\mathbb{Z}_{pq}$, ולכן G ציקלית. ▨

<u>תרגיל</u>: כל חבורה מסדר 90 אינה פשוטה.

<u>פתרון</u>: $90=2\cdot 3^2\cdot 5$.

$$n_5\in\{1,6\}\Leftarrow n_5\in\{1,2,3,6,9,18\},\ n_5\equiv 1(5)$$
$$n_3\in\{1,10\}\Leftarrow n_3\in\{1,2,5,10\},\ n_3\equiv 1(3)$$
$$n_2\in\{1,3,5,9,15,45\},\ n_2\equiv 1(2)$$

נניח בשלילה שקיימת חבורה פשוטה G מסדר 90. אם $n_5=1$ או $n_3=1$, אזי בהכרח קיימת תת-חבורה נורמלית ל- G. לכן נניח $n_3=10,\ n_5=6$. יש 6 חבורות מסדר 5, בכל אחת מהן יש בדיוק 4 איברים מסדר 5, וכל שתי חבורות כאלו הן או שוות או בעלות חיתוך טריוויאלי. לפיכך, בחבורה יש בסה"כ $6\cdot 4=24$ איברים מסדר 5. בנוסף, לחבורה הנתונה ישנן 10 תת-חבורות מסדר 9. נניח שחיתוך כל זוג מתוך חבורות אלו טריוויאלי, ואז היו בחבורות אלו $10\cdot 8=80$ איברים מסדר 3 או 9, כלומר בחבורה יש לכל הפחות $1+24+80=105$ איברים, בסתירה לכך שהחבורה מסדר 90. לפיכך, קיימות 2 תת-חבורות 3-סילוב P_1,P_2 כך ש- $|P_1\cap P_2|=3$. P_1,P_2 הן חבורות מסדר $9=3^2$, והראנו שכל חבורה מסדר ריבוע של ראשוני היא אבלית, לכן הן אבליות, כלומר מתקיים $P_1\cap P_2\lhd P_1,P_2$. מהגדרת הנורמליות מתקיים $P_1\cap P_2\lhd\langle P_1,P_2\rangle$. מתקיים $9\mid\langle P_1,P_2\rangle$, ולכן $[G:\langle P_1,P_2\rangle]\in\{1,2,5,10\}$.

אם $[G:\langle P_1,P_2\rangle]=1$, אזי $G=\langle P_1,P_2\rangle$ וסיימנו. אם $[G:\langle P_1,P_2\rangle]=10$, אזי $|\langle P_1,P_2\rangle|=9$, ולכן $P_1=\langle P_1,P_2\rangle=P_2$, סתירה. אם $[G:\langle P_1,P_2\rangle]=2$ אז סיימנו, כי תת-חבורה מאינדקס 2 היא תת-חבורה נורמלית. אם $[G:\langle P_1,P_2\rangle]=5$ אז $90\nmid 5! \Leftarrow \langle P_1,P_2\rangle$ מכילה תת-חבורה נורמלית לא טריוויאלית של החבורה G.

רשימת טריקים:

I. משפטי סילוב – לספור חבורות $p-$סילוב. אם $n_p=1$ אז יש תת-חבורה נורמלית.

II. לספור איברים – שיקולים קומבינטורים.

III. עבור חבורות שהן מכפלה של מס׳ קטן של ראשוניים:
א. חבורה מסדר p היא ציקלית.
ב. חבורה מסדר p^2 היא אבלית.
ג. חבורה מסדר pq כאשר $q>p,\ p\nmid q-1$ היא ציקלית.
(בד״כ נפעיל אינפורמציה זו על חבורות מנה).

IV. תת-חבורת הקומוטטור: אם $N\lhd G$ אזי G/N אבלית $\Leftrightarrow G'\leq N$.

V. לזהות איזושהי פעולה (למשל, אם $[G:H]=m$, $|G|=n\nmid m!$ אזי H מכילה תת-חבורה לא טריוויאלית של G).

VI. כל מיני טענות ספורדיות:
א. חבורה מאינדקס 2 היא נורמלית.
ב. כל חבורת-p בעלת מרכז לא-טריוויאלי.

<u>תרגיל</u>: הוכח שחבורה מסדר 255 היא אבלית.

<u>פתרון</u>: תהא G חבורה מסדר $255=3\cdot5\cdot17$.

$$n_{17}\in\{1,3,5,15\},\ n_{17}\equiv1(17)\Rightarrow n_{17}=1$$
$$n_5\in\{1,3,17,51\},\ n_5\equiv1(5)\Rightarrow n_5\in\{1,51\}$$
$$n_3\in\{1,5,17,85\},\ n_3\equiv1(3)\Rightarrow n_3\in\{1,85\}$$

לכן יש ל- G יש תת-חבורה נורמלית מסדר 17, נסמנה P_{17}. נניח $n_5=51,\ n_3=85$. כל תת-חבורה מסדר 5 תורמת 4 איברים מסדר 5, וכל חבורה מסדר 3 תורמת 2 איברים מסדר 3. לפיכך ב- G יש לכל הפחות $51\cdot4+85\cdot2=374$ איברים, בסתירה לסדר של G. לכן, או $n_3=1$ או $n_5=1$. לכן, או שקיימת תת-חבורה נורמלית מסדר 3, ונסמנה P_3, או תת-חבורה נורמלית מסדר 5, נסמנה P_5.

בהנחת קיום P_3,P_5:

$$|G/P_{17}|=15=3\cdot5,\ |G/P_5|=51=3\cdot17,\ |G/P_3|=85=5\cdot17$$

ולכן G/P_5, G/P_3, G/P_{17} ציקליות, ובפרט אבליות.

G/P_{17} אבלית, ולכן $G' \le P_{17}$. אם P_3 קיימת, אזי G/P_3 אבלית ולכן $G' \le P_3$. אחרת, P_5 קיימת, G/P_5 אבלית ולכן $G' \le P_5$. לפיכך, $G' \le P_5 \cap P_{17}$ או $G' \le P_3 \cap P_{17}$, ובכל אחד מהמקרים החיתוך טריוויאלי, לכן $G' = \{e\}$, כלומר G אבלית.

<u>תרגיל</u>: הוכח כי כל חבורה מסדר 255 היא ציקלית, כלומר איזומורפית לחבורה $\mathbb{Z}_{255}$.

<u>פתרון</u>: תהא G חבורה מסדר 255. יהיו P_3, P_5, P_{17} חבורות 3-סילוב, 5-סילוב ו-17-סילוב של G בהתאמה. G מסדר 255, ולכן היא אבלית (התרגיל הקודם). לפיכך, $P_5, P_3, P_{17} \lhd G$. חיתוך כל שתיים מתוך חבורות אלו טריוויאלי, ומכפלת הסדרים שלהם היא 255. לפיכך,

$G \cong P_3 \times P_5 \times P_{17} \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \cong \mathbb{Z}_{255}$.

<u>תרגיל</u>: תהי G מסדר 1225. הוכח ש-G אבלית.

<u>פתרון</u>:

$$|G| = 5^2 \cdot 7^2$$
$$n_7 \in \{1,5,25\},\ n_7 \equiv 1(7) \Rightarrow n_7 = 1$$
$$n_5 \in \{1,7,49\},\ n_5 \equiv 1(5) \Rightarrow n_5 = 1$$

יש חבורות נורמליות P,Q מסדרים 25 ו-49 בהתאמה. מכיוון שסדרים אלו הם ריבועי ראשוניים, P,Q אבליות, ומתקיים:

I. $P,Q \lhd G$

II. $P \cap Q = \{e\}$

III. $|P||Q| = |G|$

ולכן G זו המכפלה הישרה של P,Q, ומשום שהן אבליות, גם G אבלית.

<u>תרגיל</u>: כל חבורה מסדר 12 פתירה.

<u>פתרון</u>: תהא G חבורה מסדר $12 = 2^2 \cdot 3$.

$$n_3 \in \{1,2,4\},\ n_3 \equiv 1(3) \Rightarrow n_3 \in \{1,4\}$$
$$n_2 \in \{1,3\}$$

אם $n_3 = 4,\ n_2 = 3$ אז יש ב-G 8 איברים מסדר 3 ו9 איברים מסדר 2 או 4, כלומר ב-G יש לפחות 17 איברים, בסתירה לסדר G. לכן, או שקיימת $P \lhd G$ מסדר 3, או שקיימת $Q \lhd G$ מסדר 4.

במקרה הראשון, $|G/P| = 4$, לכן G/P אבלית, ולכן פתירה, ומכיוון ש-P מסדר 3 (ולכן גם היא אבלית ופתירה), גם G פתירה.

במקרה השני, Q פתירה (כי סדרה 4, לכן היא אבלית ובפרט פתירה), $|G/Q| = 3$, ולכן G/Q ציקלית ובפרט פתירה, ולכן G פתירה.

תרגיל: הוכח שכל חבורה מסדר $2^m \cdot 3$ פתירה, לכל $m \ge 0$.

פתרון: תהא חבורה G מסדר $2^m \cdot 3$. עבור $m=0$ זו חבורה ציקלית, ולכן בפרט פתירה. עבור $m=1$ זו חבורה מסדר 6, וההוכחה שחבורה זו פתירה דומה לתרגיל הקודם (ספירת איברים). גם עבור $m=2$ הוכחנו כבר. נוכיח באינדוקציה על $m \ge 3$.

תהא P חבורה 2-סילוב של G, $|P| = 2^m$. $[G:P]=3$, אבל $2^m \nmid 3!$ ($m>2$), לכן P מכילה תת-חבורה $N \lhd G$. נסמן: $|N| = 2^k, 1 \le k \le m$. N חבורת-2, ולכן היא פתירה.

$[G:N] = 2^{m-k} \cdot 3$, ולפי הנחת האינדוקציה גם G/N פתירה, ולפיכך G פתירה.

תרגיל: הוכח שכל חבורה מסדר $2^m \cdot 3^k$ פתירה, לכל $m,k \ge 0$.

פתרון: יש בעייתיות בפתרון שראינו בכיתה. אולי אוסיף פתרון לתרגיל זה מאוחר יותר (הערה: הטענה נכונה לכל p,q ראשוניים, ולא רק ל-2,3. תוצאה זו ידועה בתור משפט ברנסייד, אבל ההוכחה למשפט דורשת ידע בתורת ההצגות שחורג ממסגרת קורס זה).

תרגיל: תהי G חבורה, $P \le G$ תת-חבורה $p-$סילוב. הוכח: $N(N(P)) = N(P)$.

הוכחה: מהגדרת הנורמליזטור מתקיים $N(P) \le N(N(P))$. נראה את הכיוון השני.
יהי $g \in N(N(P))$, ולכן $gN(P)g^{-1} = N(P)$. מספיק להראות $gPg^{-1} = P$. $P \le N(P)$, לכן $gPg^{-1} \le gN(P)g^{-1} = N(P)$. P חבורת $p-$סילוב ב-G, ולכן היא חבורת $p-$סילוב גם ב-$N(P)$, ולכן גם gPg^{-1} חבורת $p-$סילוב ב-$N(P)$. לפי המשפט השני של סילוב, תת-חבורות $p-$סילוב של אותה חבורה צמודות זו לזו, ולכן קיים $h \in N(P)$ עבורו $gPg^{-1} = hPh^{-1}$. אולם, $P \lhd N(P)$, ולכן $hPh^{-1} = P$, כלומר $gPg^{-1} = P$, ולכן $g \in N(P)$.