# מופשטת 1 תרגיל בית 11

1. עבור $H \leq G$ נגדיר את המנרמל של $H$ ב $G$ להיות $N_G(H) = \{x \in G | xH = Hx\}$.
הוכיחו:
א. $N_G(H) \leq G$, ו $(H \trianglelefteq G) \iff N_G(H) = G$.
ב. $H \trianglelefteq N_G(H)$.
ג. אם $H \trianglelefteq K \subseteq G$ אז $K \subseteq N_G(H)$.
ד. נניח $K \subseteq H \leq G$ ו $K \trianglelefteq G$, אזי $N_{G/K}(H/K) = N_G(H)/K$.
פתרון:
א. סגירות לכפל: יהיו $a, b \in N_G(H)$. כלומר, $aH = Ha$ ו $bH = Hb$. צ"ל: $abH = Hab$.
ובכן, $abH = aHb = Hab$.
סגירות להופכי: יהי $a \in N_G(H)$. אזי $aH = Ha$. נכפיל ב$a^{-1}$ מימין ומשמאל לקבל: $Ha^{-1} = a^{-1}H$.
בנוסף, $1 \in N_G(H)$ כי $1H = H = H1$.
לגבי החלק השני: $H \trianglelefteq G \iff \forall g \in G, gH = Hg \iff N_G(H) = G$.
ב. מהגדרה, $\forall g \in N_G(H), gH = Hg$.
ג. יהי $k \in K$. מאחר ו$H \trianglelefteq K$, מתקיים $kH = Hk$. לכן $k \in N_G(H)$.
ד. קל לראות שתמיד $H \subseteq N_G(H)$, ולכן $K \subseteq N_G(H)$.
נסמן את פו' ההטלה הטבעית $G \to G/K$ ב $\varphi$. צריך להוכיח:

$$N_{G/K}(\varphi(H)) = \varphi(N_G(H))$$

.

ובכן, יהי $x \in N_G(H)$. כלומר, $xH = Hx$. אזי,

$$\varphi(x)\varphi(H) = \varphi(xH) = \varphi(Hx) = \varphi(H)\varphi(x)$$

. כלומר,

$$\varphi(x) \in N_{G/K}(\varphi(H))$$

.

מצד שני, יהי $x$ כך ש $\varphi(x) \in N_{G/K}(\varphi(H))$. כלומר,

$$xHx^{-1}H^{-1} \subseteq \ker\varphi \Longleftarrow \varphi(xHx^{-1}H^{-1}) = e \Longleftarrow \varphi(xH) = \varphi(Hx) \Longleftarrow \varphi(x)\varphi(H) = \varphi(H)\varphi(x)$$

.

אבל $\ker\varphi = K$. כלומר, $xHx^{-1}H^{-1} \subseteq K$.
נובע: $xHx^{-1} \subseteq KH$.

אבל $K \subseteq H$ ולכן $KH = H$.
כלומר, נקבל ש $xHx^{-1} \subseteq H$. וזה בדיוק אומר ש $x \in N_G(H)$.
מש"ל.

2. הוכיחו:
א. לכל חבורת־ $p$ $G$, ו $H < G$, $H < N_G(H)$ (כלומר, $H$ תת חבורה אמיתית של המנרמל שלה).
רמז: אינדוקציה על הסדר של $G$.
ב. הסיקו מהסעיף הקודם שכל תת חבורה מאינדקס $p$ של חבורת־ $p$ היא נורמלית.
פתרון:
א. תהי $G$ חבורה מסדר $p^k$. נוכיח את הטענה באינדוקציה על $k$.
נניח שלכל $k < n$ הטענה נכונה, ונסתכל על $G$ מגודל $p^n$.
כזכור, לכל חבורת $p$ יש מרכז לא טריוויאלי.
תהי $H < G$.
אם קיים $g \in Z(G) \setminus H$, אז כמובן ש $g \in N_G(H)$, ולכן $H$ מוכלת ממש במנרמל שלה.
אחרת, $Z(G) \subseteq H$.
לפי שאלה 1 סעיף ד' $N_{G/Z(G)}(H/Z(G)) = N_G(H)/Z(G)$.
מכיוון ש$Z(G)$ לא טריוויאלית, בהכרח $|G/Z(G)| < |G|$. כמו כן, הסדר של $G/Z(G)$ מח<לק את הסדר של $G$, ולכן $|G/Z(G)| = P^k$ עבור $k < n$. מהנחת האינדוקציה, $H/Z(G) < N_{G/Z(G)}(H/Z(G))$.
אם $H = N_G(H)$ אז $H/Z(G) = N_G(H)/Z(G) \Longleftarrow H/Z(G) = N_{G/Z(G)}(H/Z(G))$. סתירה.
ב. תהי $H \leq G$ תת חבורה מאינדקס $p$. מסעיף א' ראינו ש $H < N_G(H)$.
$N_G(H) \leq G$ ולכן $[G:H] = p$ $[N_G(H):H]|$. אבל $[N_G(H):H] \neq 1$ כי $H$ היא תת חבורה אמיתית של $N_G(H)$. לכן בהכרח $[N_G(H):H] = p$. נקבל ש $N_G(H) = G$.
כלומר, $H$ נורמלית ב$G$.

3. נתבונן ב$S_6$ ובתת חבורה $H = \{\sigma \in S_6 | \sigma(2) = 2, \sigma(4) = 4, \sigma(6) = 6\}$.
הוכחתם ש$H$ אכן תת חבורה. הראו כי ב$N_{S_6}(H)$ יש שתי תת חבורות $K, L$ כך ששתיהן איזומורפיות ל$S_3$, ו $L \cap K = \{e\}$.
פתרון: ראשית, ראינו שלכל תת חבורה $H$, $H \subseteq N_G(H)$. הוכחתם בעבר ש $H \cong S_3$, אז נקח $L = H$.
נסתכל על התת חבורה הבאה: $K = \{\sigma \in S_6 | \sigma(1) = 1, \sigma(3) = 3, \sigma(5) = 5\}$. קל לראות שהיא איזומורפית ל$H$ (ע"י החלפה של 1 ב2, 3 ב4, ו5 ב6) ולכן איזומורפית ל$S_3$.
לכל $k \in K$, $h \in H$ מתקיים $kh = hk$ כי הם פועלים על קבוצות זרות, ולכן $K \subseteq N_G(H)$.
בנוסף, אם $\sigma \in H \cap K$ אז $\sigma(1) = 1, \sigma(3) = 3, \sigma(5) = 5$ וגם $\sigma(2) = 2, \sigma(4) = 4, \sigma(6) = 6$. כלומר, $\sigma = id$.

4. רשמו את שוויון המחלקות עבור החבורות $S_5, S_4, D_4$. כלומר, הביעו את הסדר של כל אחת מהן באמצעות סכום הגדלים של מחלקות הצמידות. שימו לב כמה איברים יש במרכז.
פתרון:
$D_4$: נשים לב ש $|D_4| = 2^3$. הוכחנו בכיתה שלכל חבורה מסדר $p^3$ המרכז הוא מגודל $p$, ולכל איבר שלא במרכז גודל מחלקת הצמידות שלו הוא $p$. לכן יש שני איברים במרכז ו3 מחלקות צמידות מגודל 2. כלומר: $8 = 2 + 2 + 2 + 2$.

$S_4$ : כזכור לכל $S_n, n>2$ המרכז הוא טריוויאלי.

מחלקות הצמידות הן כל האיברים מאותו מבנה מחזורים. צריך לספור כמה איברים יש מכל מבנה מחזורים.

$()()()()$ - זה היחידה, ויש רק 1.

$(-,-)$ יש 6 איברים.

$(-,-),(-,-)$ יש 3 איברים.

$(-,-,-)$ יש 8 איברים.

$(-,-,-,-)$ יש 6 איברים.

לכן משוואת המחלקות היא: $24 = 1+6+3+8+6$.

$S_5$: כמו קודם, המרכז טריוויאלי. צריך לספור כמה איברים יש מכל מבנה מחזורים.

גודל מחלקת הצמידות $(-,-)$ הוא $10 = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$.

גודל מחלקת הצמידות $(-,-,-)$ הוא $20 = 2! \begin{pmatrix} 5 \\ 3 \end{pmatrix}$.

גודל מחלקת הצמידות $(-,-,-,--)$ הוא $30 = 3! \begin{pmatrix} 5 \\ 4 \end{pmatrix}$.

גודל מחלקת הצמידות $(-,-)(-,-)$ הוא $15 = \dfrac{\begin{pmatrix} 5 \\ 2 \end{pmatrix}\begin{pmatrix} 3 \\ 2 \end{pmatrix}}{2}$.

גודל מחלקת הצמידות $(-,-,-)(-,-)$ הוא $20 = 2! \begin{pmatrix} 5 \\ 3 \end{pmatrix}$.

לכן משוואת המחלקות היא: $120 = 1+10+20+30+15+20$.

5. א. תהי $H \leq G$. ו-$P$ תת חבורת $p$- סילו של $H$, הוכיחו שקיימת $P'$ תת חבורת $p$- סילו של $G$ כך ש $P = P' \cap H$.

ב.תהי $H \trianglelefteq G$, ו-$P$ תת חבורת $p$- סילו של $G$, הוכיחו ש $P \cap H$ היא תת חבורת $p$- סילו של $H$.

פתרון:

א. נניח $|G| = p^n t$ כך ש $(p,t)=1$ ו $|H| = p^k s$ כך ש: $k \leq n, s|t$.

אם $P$ תת חבורת $p$- סילו של $H$ אז $|P| = p^k$. בפרט, $P$ היא תת חבורת $p$ של $G$ ולכן ממשפט סילו 2 קיימת $P'$ חבורת $p$- סילו של $G$ כך ש: $P \subseteq P'$.

ברור ש $P \subseteq P' \cap H$.

מצד שני, $P' \cap H$ היא תת חבורה של $H$, והיא גם תת חבורה של $P'$ ולכן סידרה הוא חזקה של $p$ שמחלקת את הגודל של $H$.

כלומר, $p^k = |P| \leq |P' \cap H| = p^m | p^k s$. נובע מכאן ש $|P' \cap H| = p^k$. אבל הוא מכיל את $P$ שהיא מסדר $p^k$. כלומר, $P = P' \cap H$.

ב. נניח כמו קודם ש $|G| = p^n t$ כך ש $(p,t)=1$ ו $|H| = p^k s$ כך ש: $k \leq n, s|t$.

$|P| = p^n$. $P \cap H$ היא תת חבורה של של $P$ ולכן הסדר שלו הוא $p^m$ לאיזשהו $m \leq n$.

כמו כן, היא תת חבורה של $H$ ולכן בהכרח $m \leq k$. המטרה היא להראות ש $m = k$.

ובכן, ממשפט האיזומורפיזם השני: $P/P \cap H \cong PH/H \Longleftarrow |P/P \cap H| = |PH/H| \Longleftarrow |P|/|P \cap H| = |PH|/|H| \Longleftarrow |PH|/|P| = |H|/|P \cap H| \Longleftarrow [HP:P] = [H : P \cap H]$.

$HP \leq G$ ולכן $[HP:P] | [G:P]$. אבל $[G:P] = |G|/|P| = t$ זר ל-$p$. לכן $[H : P \cap H] = |H|/|P \cap H|$ זר ל-$p$. $\Longleftarrow |P \cap H| = p^k$. כלומר, $P \cap H$ הית תת חבורת $p$- סילו של $H$.

6. נתבונן בחבורת הסימטריה $S_p$ עבור מספר ראשוני $p$.
א. כמה איברים מסדר $p$ יש בחבורה?
ב. חשבו בעזרת סעיף א' את מספר תת החבורות מסדר $p$ ב $S_p$.
ג. העזרו בסעיף ב' ובמשפט סילו 3 כדי להוכיח: לכל ראשוני $p$,

$$(p-1)! \equiv (p-1) \mod p$$

פתרון:
א.האיברים מסדר $p$ הם בדיוק המחזורים מאורך $p$. יש $(p-1)!$ כאלה.
ב. תת חבורה מסדר $p$ ב $S_p$ היא למעשה תת חבורת־ $p$ סילו.
ידוע שתת חבורות שונות מסדר $p$ נחתכות באופן טריוויאלי. כל חבורה כזאת מוסיפה $(p-1)$ איברים מסדר $p$, ולכן יש $(p-2)!$ חבורות כאלה.
ג. $n_p = (p-2)!$.
ממשפט סילו 3 ידוע: $(p-2)! \equiv 1 \mod p$. נכפיל את שני האגפים ב$p-1$ לקבל:

$$(p-1)! \equiv (p-1) \mod p$$

7. א. תהי $G$ חבורה מסדר $pq$ כאשר $p > q$ ראשוניים ו $p \neq 1 \mod q$, הוכיחו כי $G$ ציקלית.
הדרכה: חשבו את $n_p$ ו $n_q$, והסיקו כמה איברים מכל סדר אפשרי קיימים בחבורה.
ב. תהי $G$ חבורה מסדר 55 כך שיש בה יותר מ4 איברים מסדר 5, אזי $G$ אינה אבלית.
פתרון:
א. $n_p|q$ וכן $n_p \equiv 1 \mod p$. מכיוון ש $p > q$ זה אומר שבהכרח $n_p = 1$.
כמו כן, $n_q|p$ וכן $n_q \equiv 1 \mod q$. מכיוון שנתון ש $p \neq 1 \mod q$ נקבל $n_q = p$.
הסדרים האפשריים של איברים בחבורה הם: $1, p, q, pq$. כל איבר מסדר $p$ מוכל בחבורת $p$־ סילו. מכיוון שיש רק אחת כזו, יש רק $p-1$ איברים מסדר $p$.
באופן דומה יש $q-1$ איברים מסדר $q$.
ביחד עם איבר היחידה נקבל שספרנו עד כה $1+p-1+q-1 = p+q-1 < p+q \leq pq$.
כלומר, יש עוד איברים שלא ספרנו, והסדר שלהם הוא בהכרח $pq$.
קיים איבר מסדר $pq \Longleftarrow$ החבורה ציקלית.
ב. כל איבר מסדר 5 מוכח בחבורת 5 ־ סילו. במקרה שלנו חבורת 5 סילו היא מגודל 5, ולכן מכילה בדיוק 4 איברים מגודל 5 (+איבר היחידה). נתון שיש יותר מ4 איברים מסדר 5, לכן בהכרח יש יותר מחבורת 5 ־ סילו אחת $\Longleftarrow$ חבורת 5 ־ סילו היא לא נורמלית.
אם $G$ הייתה אבלית, אז כל תת חבורה שלה הייתה נורמלית. לכן חייב להתקיים ש $G$ לא אבלית.

8. תהי $G$ חבורה מסדר 12 ויהיו $n_2$ ו $n_3$ מספר חבורות ה־2 סילו וה3־ סילו בהתאמה.
א. מהם ערכי$n_2$ האפשריים? (הביאו דוגמאות לכך שכל ערכי $n_2$ המדוברים אכן אפשריים)
ב. מהם ערכי $n_3$ האפשריים? (הביאו דוגמאות לכך שכל ערכי $n_3$ המדוברים אכן אפשריים)
ג. האם יתכן ש $n_2 = 3$ ו $n_3 = 4$?
פתרון:

א. $n_2|3$ וכן $n_2 \equiv 1 \mod 2$. לכן $n_2 \in \{1,3\}$.
נראה כי שני הערכים אפשריים:

עבור $G=\mathbb{Z}_{12}$ יש רק חבורת 2 סילו אחת, כי $G$ אבלית ולכן כל תת חבורה שלה נורמלית.

עבור $G=D_6$ יש יותר מחבורת 2 - סילו אחת, כי כל איבר מסדר 2 שייך לחבורת 2 - סילו. חבורת 2 - סילו ב $G$ היא מגודל 4, ולכן היא מכילה לכל היותר 3 איברים מסדר 2. אולם ב$D_6$ יש יותר מ3 איברים מסדר 2. (לכל $0 \le i \le 5$, $\tau\sigma^i$ הוא מסדר 2).

ב. $n_3|4$ וכן $n_3 \equiv 1 \mod 3$. לכן $n_3 \in \{1,4\}$.
נראה כי שני הערכים אפשריים:

עבור $G=\mathbb{Z}_{12}$ יש רק חבורת 3 סילו אחת, כי $G$ אבלית ולכן כל תת חבורה שלה נורמלית.

עבור $G=A_4$ יש יותר מחבורת 3 - סילו אחת, כי כל איבר מסדר 3 שייך לחבורת 3 סילו. הגודל של חבורת 3 סילו ב $G$ הוא 3, ולכן היא מכילה שני איברים מסדר 3. אולם ב$A_4$ יש יותר מ2 איברים מסדר 3 - כל המחזורים מאורך 3 הם מסדר 3.

ג. לא. הוכחה:

נניח $n_3=4$. חבורות 3 סילו הן מגודל 3 ולכן החיתוך של כל שתיים שונות הוא טריוויאלי. כל חבורה תורת 2 איברים שונים מסדר 3. לכן סה"כ יש 8 איברים מסדר 3. ביחד עם איבר היחידה ספרנו עד כה 9 איברים. נשארו 3 איברים. עם 3 איברים אי אפשר לבנות יותר מחבורת 2 סילו אחת, כי הגודל של חבורות 2 סילו ב $G$ הוא 4. לכן בהכרח $n_2=1$.