פתרון שיעורי בית 6

1. תהא G חבורה ו $H_1, H_2 \leq G$ תתי חבורות שלה. הוכיחו:

   (א) אם $|G| = 210, |H_1| = 21, |H_2| = 30$ אז $H_1 \cap H_2$ ציקלית.

   פתרון:

   נסמן $|H_1 \cap H_2| = n$. כיון ש־ $H_1 \cap H_2 \leq H_1, H_2$ נקבל ש־ $n|21 \wedge n|30$ ולכן $n|\gcd(21,30) = 3$, ולכן $n \in \{1,3\}$. חבורה עם איבר אחד או עם שלושה איברים היא תמיד ציקלית.

   (ב) אם $|G| = 84, |H_1| = 28, |H_2| = 12$ אז $H_1 \cap H_2$ אבלית.

   פתרון:

   נסמן $|H_1 \cap H_2| = n$. כיון ש־ $H_1 \cap H_2 \leq H_1, H_2$ נקבל ש־ $n|28 \wedge n|12$ ולכן $n|\gcd(28,12) = 4$, ולכן $n \in \{1,2,4\}$. חבורה עם איבר אחד או שניים היא תמיד ציקלית ולכן אבלית, חבורה עם ארבעה איברים היא תמיד אבלית כפי שראינו בכיתה.

2. תהי G חבורה, $H_1, H_2 \leq G$ תתי חבורות. יהי p מספר ראשוני. הוכיחו שאם $|H_1| = |H_2| = p$ וגם $H_1 \neq H_2$ אז $H_1 \cap H_2 = \{e\}$.

   פתרון:

   נסמן $|H_1 \cap H_2| = n$. כיון ש־ $H_1 \neq H_2$ נקבל ש־ $n < p$, כיון ש־ $n|p$ ו־p ראשוני נובע $n = 1$, ולכן $H_1 \cap H_2 = \{e\}$.

3. תהי G חבורה מסדר 8 (סדר של חבורה הכוונה מס' האיברים שבה).

   (א) הוכיחו שאם G ציקלית אז קיימת תת חבורה ציקלית $H \leq G$ מסדר 4.

   (ב) הוכיחו שאם G לא אבלית אז קיימת תת חבורה ציקלית $H \leq G$ מסדר 4.

   (ג) הוכיחו או הפריכו: לכל חבורה G מסדר 8 יש תת חבורה ציקלית $H \leq G$ מסדר 4.

   פתרון:

   א. G ציקלית ולכן יש יוצר כלומר, קיים $g \in G$ כך ש־ $G = \langle g \rangle$. לכן נקבל $o(g) = 8 \Rightarrow o(g^2) = 4$, ותת החבורה $H = \langle g^2 \rangle$ היא מסדר 4.

   ב. נראה שיש איבר מסדר 4, ואז תת החבורה הנוצרת על ידו היא מסדר 4: לפי לגראנז', לכל $e \neq g \in G$ מתקיים $o(g) \in \{2,4,8\}$. G לא אבלית ולכן גם לא ציקלית, ולכן אין איבר מסדר 8, ולכן לכל $e \neq g \in G$ מתקיים $o(g) \in \{2,4\}$. רוצים להראות שקיים איבר מסדר 4. נניח בשלילה שכל האיברים (חוץ מהיחידה) מסדר 2, אז לפי תרגיל בית נקבל ש־G אבלית, בסתירה. לכן יש איבר מסדר 4.

ג. הפרכה: לפי סעיפים א־ב ההפרכה חייבת להיות חבורה אבלית שאיננה ציקלית. ניקח את החבורה $G = (\mathbb{Z}_2)^3$. היא מסדר 8, וכל איבריה (למעט היחידה) מסדר 2, לכן אין איבר מסדר 4, ואין תת־חבורה מסדר 4.

4. יהי $g \in D_5$ (חבורת השיקופים והסיבובים). מה האפשרויות ל־$o(g)$? מצאו איבר מתאים לכל אפשרות כזו.

פתרון:

$|D_5| = 10$, ולכן לפי לגראנז' לכל $g \in D_5$ נקבל $o(g) \in \{1,2,5,10\}$. ידוע שהחבורה לא אבלית ולכן לא ציקלית, ולכן אין איבר מסדר 10. נמצא איברים משאר הסדרים: איבר היחידה הוא מסדר 1, איבר השיקוף שסימנו אותו ב־τ הוא מסדר 2, ואיבר הסיבוב שסימנו אותו ב־σ הוא מסדר 5.

5. הציגו את החבורות הבאות כ־ $\mathbb{Z}_n$ או $\mathbb{Z}_n \times \mathbb{Z}_m$:

(א) U_{11}

(ב) U_{12}

(ג) U_{13}

(ד) U_{14}

פתרון:

א. כיון ש־11 ראשוני, נקבל ש־ $U_{11} \cong \mathbb{Z}_{10}$, כפי שאמרנו בכיתה.

ב. $U_{12} = \{1,5,7,11\}$. נבדוק את סדרי האיברים:

$5^2 = 25 \equiv 1(\mod 12) \Rightarrow o(5) = 2$

$7^2 = 49 \equiv 1(\mod 12) \Rightarrow o(7) = 2$

$11^2 = 121 \equiv 1(\mod 12) \Rightarrow o(11) = 2$.

כל האיברים (למעט היחידה) מסדר 2, ולכן $U_{12} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

ג. כיון ש־13 ראשוני, נקבל ש־ $U_{13} \cong \mathbb{Z}_{12}$, כפי שאמרנו בכיתה.

ד. $U_{14} = \{1,3,5,9,11,13\}$. גם כאן נבדוק לפי סדרי האיברים:

$3^2 = 9, 3^3 = 27 \equiv 13(\mod 14)$, לכן $o(3) > 3$, אבל כיון שסדר של איבר צריך לחלק את גודל החבורה נקבל שמתחייב $o(3) = 6$. לכן יש איבר מסדר 6, ולכן החבורה איזומורפית לחבורה הציקלית $\mathbb{Z}_6$.

6. חשבו:

(א) $21^{91}(\mod 31)$.

(ב) מהן שלושת הספרות האחרונות של 7^{4003}.

(ג) $17^{17}(\mod 20)$.

פתרון:

א. 31 הוא מספר ראשוני, ולכן לפי פרמה $21^{30} \equiv 1(\mod 31)$, ולכן

$$21^{91} = \left(21^{30}\right)^3 \cdot 21 \equiv 21(\mod 31)$$

ב. בדומה לחישוב שעשינו בכיתה עבור $\phi(100)$, נקבל ש־ $\phi(1000) = 400$ (מכל עשירייה יש ארבעה זרים ל־1000, אלה שעם ספרת אחדות מ־$\{1, 3, 7, 9\}$). לכן לפי אוילר (7 זר ל1000) $7^{400} \equiv 1(\mod 1000)$, ולכן ($7^3 = 343$)

$$7^{4003} = \left(7^{400}\right)^{10} \cdot 7^3 \equiv 343(\mod 1000)$$

ג. הזרים ל־20 הם: $\{1, 3, 7, 9, 11, 13, 17, 19\}$ ולכן $\phi(20) = 8$. לפי אוילר (17 זר ל־20) נקבל $17^8 \equiv 1(\mod 20)$ ולכן

$$17^{17} = \left(17^8\right)^2 \cdot 17 \equiv 17(\mod 20)$$