אלגברה מופשטת 1 – תרגול 5

החבורה הדיהדרלית

D_n- חבורת הסיבובים והשיקופים של מצולע משוכלל בעל n צלעות.

למשל: החבורה D_3 היא חבורה הנוצרת מסיבוב (σ) בזווית 120 מעלות, ושיקוף (ז).

מתקיימים היחסים: $\tau\sigma\tau = \sigma^{-1}, \sigma^2 = \tau^2 = id$.

איברי החבורה הם: $D_3 = \{id, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. האם $\sigma\tau \in D_3$?

מתקיים:

$$\tau\sigma\tau = \sigma^{-1} \;/\; \tau$$
$$\sigma\tau = \tau\sigma^{-1} \;/\; \sigma^3$$
$$\sigma\tau\sigma^3 = \tau\sigma^2$$
$$\sigma\tau = \tau\sigma^2$$

מכאן רואים שלכל $n \geq 3$ החבורה D_n אינה אבלית, שכן (למשל) $\tau\sigma \neq \sigma\tau$.

באופן דומה D_n נוצרת על ידי σ, τ (באשר σ הוא סיבוב של $\frac{360^\circ}{n}$) כאשר $\tau\sigma\tau = \sigma^{-1}, \sigma^n = \tau^2 = id$.

איברי $D_n = \left\{id, \sigma, \sigma^2, ..., \sigma^{n-1}, \tau, \tau\sigma, ..., \tau\sigma^{n-1}\right\}$.

מתקיים $|D_n| = 2n$.

תרגיל: תהי G חבורה סופית ויהיו $a, b \in G$ האם יכול להיות ש$o(a)o(b) > o(ab)$?

פתרון: כן. D_3. נבחר $a = \tau, b = \tau\sigma$. כעת $o(\tau) = 2, o(\tau\sigma) = 2$. אבל מה הסדר של $ab = \tau\tau\sigma$? הוא בדיוק זה של σ, ולכן זה שלוש. קיבלנו דוגמה שמקיימת $o(a)o(b) > o(ab)$.

מחלקות / קוסטים (*cosets*) בחבורה

הגדרה: תהי G חבורה ו$H \leq G$ תת חבורה. עבור $a \in G$:

1. המחלקה השמאלית של a בH היא $aH = \{ah | h \in H\}$
2. המחלקה הימנית של a בH היא $Ha = \{ha | h \in H\}$

הערה: אם החבורה אבלית אזי $Ha = aH$.

דוגמאות:

1. קוסטים של $3\mathbb{Z}$ כתת חבורה של $\mathbb{Z}$: $3\mathbb{Z} + 2 = 2 + 3\mathbb{Z} = 3\mathbb{Z} + 8$.

2. כעת נביט ב$G = S_3 = \{id, (12), (13), (23), (123), (132)\}$. ונתבונן בקוסטים השמאליים של תת החבורה $H = \langle (12) \rangle = \{id, (12)\}$.

$$idH = \{(12), id\} = H$$
$$(123)H = \{(13), (123)\}, (132)H = \{(23), (132)\},$$
$$(23)H = \{(132), (13)\}, (13)H = \{(123), (13)\}, (12)H = \{id, (12)\}.$$

<u>תזכורת</u>:

הקוסטים הם מחלקות שקילות. למשל, או ששתי מחלקות זרות או שהן שוות. וגם מתקיים שהחבורה היא איחוד זר של מחלקות השקילות הללו. בדוגמה שלנו: $S_3 = H \cup (13)H \cup (132)H$

3. $G = GL_2(\mathbb{Q})$. נגדיר $H = \left\{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z}\right\}$ ותבדקו בבית ש$H \leq G$. עבור איבר $g = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} \in G$ הקוסטים הם $gH = \left\{\begin{pmatrix} 5 & 5n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z}\right\}$. $Hg = \left\{\begin{pmatrix} 5 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z}\right\}$. מתקיים כי $Hg \neq gH$.

<u>הערות</u>:

1. לכל תת חבורה $H \leq G$ מתקיים כי *H* היא מחלקה שמאלית וגם מחלקה ימנית $eH = He = H$
2. קיימת התאמה חח"ע ועל בין המחלקות הימניות למחלקות השמאליות $Hg \mapsto g^{-1}H$.

הגדרה: תהי *G* חבורה, $H \leq G$ תת חבורה. נסמן את האינדקס של *H* ב*G* כך: *[G:H]* וזהו מספר המחלקות השמאליות (ימניות) של *H* ב*G*.

למשל: מתקיים $[G:H] = 3 : H =< (12) >, G = S_3$.

תרגיל: מצאו חבורה *G* ות"ח $H \leq G$ כך ש-

1. $[G:H] = \aleph_0$
2. $[G:H] = \aleph$

פתרון:

1. $G = \mathbb{Z} \times \mathbb{Z}$. $H = \mathbb{Z} \times \{0\}$. ולכן *[G:H]*=$\aleph_0$. כל הקוסטים הם $\{Z \times \{x\}\}_{x \in \mathbb{Z}}$.
2. $[GL_2(\mathbb{R}), GL_2(\mathbb{Q})] = \aleph$. דוגמה הרבה יותר אלגנטית $G = \mathbb{R} \times \mathbb{R}, H = \mathbb{R} \times \{0\}$.

<u>משפט לגרנג' ומסקנותיו:</u>

תהי G חבורה סופית ו$H \leq G$ תת חבורה. אזי $|G| = [G:H] \cdot |H|$.

מסקנה: מתקיים כי $|H|$ מחלק את $|G|$ כלומר, הסדר של תת חבורה מחלק את סדר החבורה. בפרט, סדר של כל איבר בחבורה מחלק את סדר החבורה. כי $\forall a \in G : o(a) = |< a >|$.

נשים לב: הסדר של איבר הוא סדר של ת"ח הציקלית שהוא יוצר. וראינו שסדר של הת"ח מחלק את סדר החבורה.

מסקנה: G סופית, $K \leq H \leq G$ מתקיים $[G:K] = [G:H][H:K]$.

הערה: $a^{|G|} = e$ לכל $a \in G$.

תרגיל: תהא G חבורה מסדר 8. הוכיחו שקיימת ב-G תת חבורה ציקלית מסדר 4.

פתרון: יש רק איבר אחד מסדר 1 (היחידה) . לא יתכן שכל שאר האיברים (חוץ מהנייטרלי) הם מסדר 2, כי אז היא אבלית (הוכחנו את הטענה: אם בחבורה כל איבר (חוץ מהנייטרלי) הוא מסדר 2, אזי החבורה אבלית).

אין איבר מסדר 8 , כי אם היה G הייתה ציקלית ולכן אבלית. מכאן שקיים איבר מסדר 4 שיוצר את תת החבורה הדרושה. מ.ש.ל. ■

טענה (הכללה של התרגיל): תהא G חבורה לא אבלית מסדר 2^t $(t > 2)$ אזי קיימת בG תת חבורה ציקלית מסדר 4.

הוכחה: לפי לגרנג' הסדרים האפשריים של אברים ב-G הם: 2^k , $k = \{0,1,2, \dots, t\}$.

- יש רק איבר 1 מסדר 1
- לא כולם מסדר 2 כי אז G אבלית
- אין איבר מסדר 2^t כי אז G ציקלית ולכן אבלית.

לכן, קיים איבר a בG כך ש $o(a) = 2^k, 2 \le k < t$.

אנו יודעים כי $|< a >| = 2^k$. אנחנו טוענים שבתת חבורה הזו ניתן לייצר איבר מסדר 4.

להזכירם: $|G| = n$, $o\,(g^t) = \frac{n}{(n,t)}$, $G =< g >$. וכעת נבחר $a^j \in < a >$ כך ש $o(a^j) = \frac{2^k}{(2^k,j)} = 4$.
נבחר $j = 2^{k-2}$. כלומר, בתוך <a> נבחר את האיבר $a^{2^{k-2}} \in < a >$ וקל לראות $o\left(a^{2^{k-2}}\right) = 4$. ולכן $a^{2^{k-2}}$ יוצר את תת החבורה הציקלית הדרושה. מ.ש.ל. ■

תרגיל: הוכיחו : תהא G חבורה סופית אזי G מסדר זוגי או"א קיים ב-G איבר מסדר 2.

פתרון: $\rightarrow$: כיוון פשוט, ע"פ לגרנג' הסדר של על איבר מחלק את סדר החבורה, ולכן סדר החבורה הוא זוגי.

$\leftarrow$: שימו לב: איבר מסדר 2 הוא איבר שהופכי לעצמו. נניח שבשלילה שאין אף איבר בG שהוא ההופכי של עצמו. (חוץ מהיחידה , e, כמובן). ניתן להצמיד כל איבר להפכי שלו (שהוא איבר שונה ממנו). ביחד עם איבר היחידה, נקבל מספר אי-זוגי. מ.ש.ל■

<u>הערה</u>: לחבורה מסדר זוגי יש מספר אי זוגי של איברים מסדר 2. (המשפט של ארד ☺).

<u>משפט אוילר 2</u>:

לכל $a \in U_n$ מתקיים $a^{\varphi(n)} \equiv 1(mod(n))$.

מסקנה:

זהו למעשה זהו משפט פרמה הקטן שאומר: אם $a \in U_p$ כאשר p ראשוני אזי $a^{p-1} \equiv 1(modp)$.

תרגיל: חשבו את שתי הספרות אחרונות של $8073767^{1999}+2013$.

פתרון: נפעיל mod100 ונקבל:

$67^{1999}+13=67^{50\cdot 40-1}+13\equiv (67^{\varphi(100)})^{50}67^{-1}+13\equiv 67^{-1}+13$ נשתמש באלגוריתם למציאת הופכי, שתרגלנו בשיעורים הקודמים, ונקבל $67^{-1}=3$. ולכן שתי הספרות האחרונות הן 16=13+3.

תזכורת לאלגוריתם למציאת ההופכי:

אנו יודעים שיש הופכי ל-67 בחבורה $\mathbb{Z}_{100}$ כי הם זרים. כלומר ישנו פתרון למשוואה $67x\equiv 1(\mathrm{mod}100)$ אם ורק אם קיים $k\in\mathbb{Z}$ כך ש- $100k+67x=1$. נשתמש באלגוריתם אוקלידס כדי למצוא את x, כלומר למצוא ביטוי של $\gcd(100,67)$ כצירוף לינארי של 67 ושל 100: $(100,67)\underset{100=1\cdot 67+33}{=}(67,33)\underset{67=2\cdot 33+1}{=}(33,1)=1$

ומהצבה לאחור נקבל $1=67-2\cdot 33=-2\cdot 100+3\cdot 67$ ולכן $x=3$.

מ.ש.ל. ■

<u>אתגר</u>:

ידוע כי עבור $H_1,H_2\le G$ ועבור $H\le G$ מתקיים ש$H_1\cup H_2$ לא בהכרח תת חבורה.

הוכיחו תחילה את הטענה הבאה: אם $H\subseteq H_1\cup H_2$ אזי $H\subseteq H_1$ או $H\subseteq H_2$.

לעומת זאת, כשמדובר בשלוש תת חבורות באיחוד, המצב משתנה.

יהיו $H,H_1,H_2,H_3\le G$ (כולן תתי חבורות) מצאו דוגמה שבה מתקיים:

א. $H\subseteq H_1\cup H_2\cup H_3$;

ב. H לא מוכלת באף H_i ובאף איחוד של שתיים $H_i\cup H_j$.