

תרגול 4: סדר של איברים, ת"ח נוצרת, הומומורפיזמים

הגדרה: סדר של איבר מוגדר כסדר התת חבורה הציקלית הנוצרת על ידו, והסימון הוא $o(g) := |\langle g \rangle|$, נסמן פעמים רבות גם $|g|$.

משפט: $o(g) = \min(n > 0 \mid g^n = e)$ אם קיים n כזה או $o(g) = \infty$ אם לא קיים n המקיים את הנ"ל.

תרגיל: תהי $GL_2(\mathbb{R})$ - חבורת המטריצות ההפיכות מגודל 2×2 עם ערכים ב \mathbb{R} . מצאו את הסדר של

$$B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \quad (B \in GL_2(\mathbb{R}) \text{ ולכן } \det(B) = 1)$$

$$B^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

$$B^3 = B^2 B = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

$$\Rightarrow o(B) = 3$$

תרגיל: תהי $G = \mathbb{Z}_{12}$. מהו הסדר של 3, 8, 5?

פתרון: $\langle 3 \rangle = \{3, 6, 9, 0\}$ ולכן $|3| = 4$.

$\langle 8 \rangle = \langle 8, 4, 0 \rangle$ ולכן $|8| = 3$.

$\langle 5 \rangle = \langle 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0 \rangle$ ולכן $|5| = 12$.

תרגיל: הראו שעבור $x \in \mathbb{Z}_n$ מתקיים $|x| = \frac{n}{\gcd(n, x)}$.

פתרון: אם $d = \gcd(x, n)$ אזי $o(x) \leq \frac{n}{d}$ כיוון ש: $x \cdot \frac{n}{d} \equiv \frac{x}{d} \cdot n \equiv 0 \pmod{n}$. אם $o(x) = m$ אזי

$mx \equiv 0 \pmod{n}$ כלומר $n \mid mx$ ולכן $\frac{n}{d} \mid m \frac{x}{d}$, וכיוון ש $\gcd(\frac{n}{d}, \frac{x}{d}) = 1$ נקבל ש $\frac{n}{d} \mid m$ ולכן $\frac{n}{d} \leq m$.

הערה: בפרט מתקיים $|x| = \frac{n}{x}$ לכל $x \in \mathbb{Z}_n$ המקיים $x \mid n$.

תרגיל: הראו ש $\mathbb{Z}_n \times \mathbb{Z}_n$ אינה חבורה ציקלית.

פתרון: הסדר של החבורה $\mathbb{Z}_n \times \mathbb{Z}_n$ הוא $|\mathbb{Z}_n \times \mathbb{Z}_n| = n^2$. לכל $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n$ מתקיים $n(a, b) = (na, nb) = (0, 0) \pmod{n}$ (אנחנו מתייחסים כאן ל $\mathbb{Z}_n \times \mathbb{Z}_n$ כחבורה חיבורית, והסימונים בהתאם). לכן $|(a, b)| \leq n$. נקבל שאין אף איבר מסדר n^2 ולכן $\mathbb{Z}_n \times \mathbb{Z}_n$ אינה חבורה ציקלית.

תרגיל: אם $g^n = e$ אזי $o(g) | n$.

הוכחה: ברור ש $o(g) \leq n$. נבצע חלוקה עם שארית $n = o(g)q + r$ כאשר $0 \leq r < o(g)$, ונקבל $e = g^n = g^{o(g)q+r} = (g^{o(g)})^q g^r = g^r$. הדרך היחידה שזה יכול לקרות היא אם $r = 0$.

המשפט היסודי של חבורות ציקליות:

1. כל ת"ח של חבורה ציקלית היא ציקלית.
2. הסדר של כל ת"ח של חבורה ציקלית מסדר n הוא מחלק של n (למעשה בהמשך נוכיח שזה נכון לכל חבורה).
3. אם G חבורה ציקלית מסדר n אזי לכל מחלק k של n קיימת ת"ח יחידה מסדר k .

מסקנה: הת"ח היחידות של \mathbb{Z}_n הן מהצורה $k\mathbb{Z}_n$ כך ש $k | n$.

תרגיל בית: הראו שהסדר של כל איבר $a' \in G$ השייך לחבורה ציקלית מסדר n , הוא $\frac{n}{\gcd(n, t)}$.

תרגיל: הוכיחו או הפריכו: אם $a, b \in G$ מסדר סופי בחבורה, אזי ab הוא מסדר סופי.

פתרון: הטענה נכונה בחבורה אבליות, אבל לא בכל חבורה. אם $|a|=n, |b|=m$, אזי בחבורה אבלית מתקיים $(ab)^{mn} = a^{mn}b^{mn} = (a^n)^m (b^m)^n = ee = e$, ולכן $|ab| \leq mn < \infty$. נראה חבורה בה הטענה לא מתקיימת: ניקח

את $GL_2(\mathbb{R})$, ואת האיברים $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. ראינו ש $|B|=3$, ובדקו שמתקיים $|A|=4$,

כלומר שניהם איברים מסדר סופי. כעת $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ומתקיים:

$$(AB)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, (AB)^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \dots, (AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

לכן לא קיים $n \in \mathbb{N}$ כך ש $(AB)^n = I$, כלומר $|AB| = \infty$.

תרגיל: תהי G חבורה מסדר זוגי. הוכיחו שקיים איבר מסדר 2 ב G .

הוכחה: נבחר צמדים ב G כל צמד יהיה מורכב מאיבר והופכי שלו (לכל איבר ב G קיים הופכי והוא יחיד) מכיוון שסדר החבורה זוגי ול e אין הופכי אז ישאר איבר בודד (לפחות 1) שלו לא יהיה זוג ($a \in G$) כלומר אין לו הופכי בכל שאר אברי החבורה, אבל מכיוון שהוא בחבורה קיים לא הופכי ונשאר שהוא הופכי לעצמו כלומר $a^2 = e$ ולכן $O(a) = 2$ \square

תרגיל: תהי G חבורה כלשהי, ויהיו $g, h \in G$ איברים מתחלפים ($gh = hg$) כך ש- $|g|=n, |h|=k$ כך ש

$$gcd(k, n) = 1. \text{ הראו ש- } |gh| = |g| \cdot |h|$$

פתרון: נסמן $m := |gh|$. אזי:

$$(gh)^{nk} = g^{nk}h^{nk} = (g^n)^k (h^k)^n = e$$

ולכן $nk | m$. כיוון ש $gcd(n, k) = 1$ אזי $n | m$. בצורה דומה נקבל ש

$$k | m, \text{ ולכן } lcm(n, k) | m \text{ אבל } lcm(n, k) = \frac{nk}{gcd(n, k)} \text{ ולכן } nk | m$$

קיבלנו $m | nk$ וגם $nk | m$ ולכן $m = nk$.

ת"ח הנוצרת ע"י קבוצת איברים:

הגדרה: תהי G חבורה ותהי $A \subseteq G$ תת קבוצה של איברים ב- G (כך ש) $A \neq \emptyset$

A אינה בהכרח תת חבורה של G . נגדיר **תת חבורה הנוצרת ע"י** להיות התת-חבורה המינימלית המכילה את A ונסמנה $\langle A \rangle$.

אם $G = \langle A \rangle$ אזי נאמר ש G נוצרת ע"י A .

עבור קבוצה סופית של איברים, נכתוב בקיצור $\langle x_1, \dots, x_k \rangle$ במקום $\langle \{x_1, \dots, x_k\} \rangle$.

משפט:

$$\text{א. } \langle A \rangle = \bigcap_{\substack{H_i \leq G \\ A \subseteq H_i}} H_i$$

$$\text{ב. } \langle A \rangle = \{x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} \mid x_1, \dots, x_k \in A, n_1, \dots, n_k \in \mathbb{Z}, k \in \mathbb{Z}\}$$

הערה:

בחבורה אבלית ניתן לדרוש בסעיף ב. שכל ה x_i ים במכפלה שונים זה מזה, כיוון שניתן לקבץ אותם יחד.

הערה: אם החבורה חיבורית, סעיף ב. במשפט מקבל את הצורה:

$$\langle A \rangle = \{n_1 x_1 + n_2 x_2 + \cdots + n_k x_k \mid x_1, \dots, x_k \in A, n_1, \dots, n_k \in \mathbb{Z}, k \in \mathbb{Z}\}$$

דוגמאות:

א. אם ניקח $\{2, 3\} \subseteq \mathbb{Z}$ אזי $\langle 2, 3 \rangle = \mathbb{Z}$ (כיוון ש $1 \in H \Rightarrow (-2) + 3 = 1 \in H \Rightarrow -2 \in H \Rightarrow 2 \in H$. נקבל ש $\mathbb{Z} = \langle 1 \rangle \subseteq H$).

ב. אם ניקח $\{4, 6\} \subseteq \mathbb{Z}$ אזי לפי המשפט (סעיף ב.) נקבל $\langle 4, 6 \rangle = \{4n + 6m \mid m, n \in \mathbb{Z}\}$. נטען ש $\langle 4, 6 \rangle = \gcd(4, 6)\mathbb{Z} = 2\mathbb{Z}$, מדוע? ברור ש $2 \mid 4m + 6n$ ולכן $\langle 4, 6 \rangle \subseteq 2\mathbb{Z}$. יהי $2k \in 2\mathbb{Z}$ אזי $2k = 4(-k) + 6k \in \langle 4, 6 \rangle$, ולכן $2\mathbb{Z} \subseteq \langle 4, 6 \rangle$. באופן דומה מראים עבור $a, b \in \mathbb{Z}$ ש $\langle a, b \rangle = \gcd(a, b)\mathbb{Z}$.

הומומורפיזמים

הגדרה: תהיינה $(G, *_G, e_G)$ ו $(H, *_H, e_H)$ חבורות.

פונקציה $\varphi: G \rightarrow H$ תקרא **הומומורפיזם**. אם היא **כפלית**, כלומר אם מתקיים:

$$\forall a, b \in G \quad \varphi(a *_G b) = \varphi(a) *_H \varphi(b) \quad (\text{הכפל מימין ומשמאל הוא שונה!})$$

תכונות של הומומורפיזמים:

1. $\varphi(e_G) = e_H$ יחידה עוברת ליחידה

2. $\varphi(x^{-1}) = \varphi(x)^{-1}$ הפכי עובר להפכי

3. $\varphi(x^n) = \varphi(x)^n$ חזקה עוברת לחזקה (הוכחה באינדוקציה)

4. $\varphi(x^{-n}) = \varphi(x)^{-n}$

תרגיל: $f: G \rightarrow H$ היא אפימורפיזם (הומומורפיזם על), הראו שאם G אבלית אז H אבלית.

הוכחה: יהיו $c, d \in H$ וכיוון ש f על קיימים $a, b \in G$ כך ש $c = f(a), d = f(b)$ אזי

$$. ab = ba \Rightarrow f(ab) = f(ba) \Rightarrow f(a)f(b) \Rightarrow f(b)f(a) \Rightarrow cd = dc$$

תרגיל בית: הראו שאם $f: G \rightarrow H$ היא איזומורפיזם אזי G ציקלית אם ורק אם H ציקלית.

תרגיל: $f: G \rightarrow H$ היא הומומורפיזם, הראו ש $o(f(a)) \mid o(a)$ (הסדר של התמונה מחלק את סדר המקור).

הוכחה: $f(a)^{o(a)} = f(a^{o(a)}) = f(e) = e$. ראינו בתחילת התרגול שאם $g^n = e$ אזי $o(g) \mid n$.