

מבנים דיסקרטיים - תרגול 5

תרגיל:

תהי G חבורה ויהיו $a, b \in G$. אם a, b מסדר סופי, האם גם ab מסדר סופי?

פתרון:

תלוי בחבורה. נסמן $o(a) = n, o(b) = m$ ונתבונן בשני מקרים:

א. G אבלית: מתקיים

$$(ab)^{mn} = ab \cdot ab \cdot \dots \cdot ab = a \cdot a \cdot \dots \cdot a \cdot b \cdot b \cdot \dots \cdot b = a^{mn} \cdot b^{mn} = (a^n)^m (b^m)^n = e$$

לכן $o(ab) \leq mn$ ובפרט סופי.

ב. G אינה אבלית: נמצא דוגמה נגדית. תהי $G = (GL_n(\mathbb{R}), \cdot)$ ונתבונן בשני אברים:

$$ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad a^4 = b^3 = I \quad \text{עם זאת} \quad a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

$$\text{אינו מסדר סופי, שכן מתקיים } (ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \text{ מש"ל}$$

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 לו הופכי ונשאר שהוא הופכי לעצמו כלומר $a^2 = e$ ולכן $o(a) = 2$ □

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 $r = 0$.

הגדרה: בהנתן שני מספרים $a, b \in \mathbb{Z}$ שאינם שניהם 0, נגדיר את **הכפולה המשותפת**

הקטנה ביותר (הכמק"ב) שלהם להיות המספר **הטבעי** הקטן ביותר שמתחלק בשניהם.

נסמן ע"י $lcm(a, b)$. $lcm = \text{least common multiple}$.

דוגמא: $\gcd(6,4) = 2, \gcd(6,12) = 6, \text{lcm}(2,3) = 6, \text{lcm}(2,4) = 4$

תרגיל: הראו שאם $a, b \in G$ בחבורה כלשהיא מתחלפים ($ab = ba$) אזי

$$o(ab) \mid \text{lcm}(o(a), o(b))$$

פתרון: נסמן $m = \text{lcm}(o(a), o(b))$. אזי $(ab)^m = a^m b^m$ (שייוון זה נכון במקרה שהאיברים

מתחלפים). כעת לפי הגדרת הכפולה המשותפת המינימלית, מתקיים $o(a) \mid m$ וגם

$o(b) \mid m$ ולכן קיימים k_1, k_2 שלמים כך ש $m = o(a)k_1, m = o(b)k_2$. לכן

$$a^m = a^{o(a)k_1} = (a^{o(a)})^{k_1} = e^{k_1} = e$$

$$b^m = b^{o(b)k_2} = (b^{o(b)})^{k_2} = e^{k_2} = e$$

לכן $(ab)^m = a^m b^m = ee = e$. לפי תרגיל קודם נקבל $o(ab) \mid \text{lcm}(o(a), o(b))$.

תרגיל: מצאו מצב כנ"ל בו $o(ab) < \text{lcm}(o(a), o(b))$.

פתרון: יהי איבר $a \in G$ בחבורה כלשהיא כך ש $a \neq e$. אזי $o(a) > 1$. האיברים a, a^{-1}

מתחלפים. בנוסף מתקיים $o(a^{-1}) = o(a)$ כיוון ש $a^{-n} = e \Leftrightarrow a^n = e$. לכן

$$\text{lcm}(o(a), o(a^{-1})) = o(a) \text{ אבל מתקיים } o(aa^{-1}) = o(e) = 1 < o(a)$$

סדר של איברים בחבורת התמורות:

טענה: הסדר של מחזור (כאיבר בחבורה) הוא אורכו, כלומר מס' האיברים שבמחזור.

במילים אחרות: מחזור באורך k הוא מסדר k . לדוגמא (3 4) מחזור מסדר 2 המכונה

חילוף. מדוע הטענה הנ"ל נכונה? נראה בעזרת דוגמא שקל להכלילה:

$$\text{כלומר } [(12\dots k)^k](i) = (i+k) \pmod k$$

$$(12\dots k)(1) = 2$$

$$(12\dots k)(2) = 3 \Rightarrow (12\dots k)^2(1) = 3$$

...

$$(12\dots k)(k-1) = k \Rightarrow (12\dots k)^{k-1}(1) = k$$

$$(12\dots k)(k) = 1 = (k+1) \pmod k \Rightarrow (12\dots k)^k(1) = 1$$

משפט: איך מוצאים את הסדר של תמורה? תחילה מפרקים למחזורים **זרים**: $\pi = \sigma_1 \cdots \sigma_k$

$$\text{אזי } o(\pi) = \text{lcm}(o(\sigma_1), \dots, o(\sigma_k))$$

דוגמא: $o((123)(45)) = \text{lcm}(o((123)), o((45))) = \text{lcm}(3, 2) = 6$. **שימו לב:** אם המחזורים אינם

זרים הטענה **אינה נכונה**. $o((123)(34)) = o((1234)) = 4$. אם נתונה לכם מכפלה של

מחזורים שאינם זרים, פשוט פרקו אותה למכפלת מחזורים זרים וחשבו את הסדר.