

### תרגול 3: תתי-חבורות, תתי-חבורות ציקליות, סדר של איבר בחבורה

#### תתי חבורות:

תת חבורה: תהי  $(G, *, e)$  חבורה אז תת קבוצה  $H \subseteq G$  תקרא תת חבורה של  $G$  אם  $H$  חבורה ביחס לפעולה  $*$ . מסמנים  $H \leq G$ .

טרמינולוגיה: קוראים לחבורה  $\{e\}$  החבורה הטריטיואלית. כאשר אומרים תתי-החבורות הטריטיואליות של חבורה  $G$ , מתכוונים ל-  $\{e\}, G$ .

#### דוגמאות לת"ח

1.  $(\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0)$

2. האם:  $\mathbb{Z}_3 \leq \mathbb{Z}_6$ ? תשובה: לא!! כי פעולת החבורה היא שונה. למה אנחנו מתכוונים בפעולות שונות? שימו לב ש 2 הוא ההפכי של 1 ב-  $\mathbb{Z}_3$ , אבל ב  $\mathbb{Z}_6$  זה לא נכון. בצורה דומה  $\mathbb{Z}_n \not\leq \mathbb{Z}$ .

3. קבוצת כל החזקות של איבר מסוים בחבורה היא ת"ח. כלומר אם  $G$  חבורה, ו-  $x \in G$  אזי  $\{x^n \mid n \in \mathbb{Z}\} \leq G$ . קבוצת כל החזקות החיוביות היא אגודה, קבוצת כל החזקות הלא-שליליות היא מונואיד.

4. יהי  $\Omega_n$  אוסף הפתרונות של המשוואה  $z^n = 1$  ב  $\mathbb{C}$ . אזי  $\Omega_n \leq \mathbb{C}^*$ . נראה זאת: נניח ש  $a, b \in \Omega_n$ , ז"א  $a^n = b^n = 1$ . אזי  $(ab)^n = a^n b^n = 1$  (בגלל האבליות של  $\mathbb{C}^*$ ). עבור  $a \in \Omega_n$  ניקח את  $a^{-1} \in \mathbb{C}^*$ . אזי  $(a^{-1})^n = (a^n)^{-1} = 1$  ולכן  $a^{-1} \in \Omega_n$ . נשים לב ש  $\Omega_n = \{cis(\frac{2\pi k}{n}) \mid 0 \leq k \leq n-1\}$ , כאשר  $cis(\alpha) = \cos(\alpha) + i \sin(\alpha)$  הוא סימון מקוצר ל

$$(cis(30) = \cos(30) + i \sin(30) = \frac{\sqrt{3}}{2} + \frac{1}{2}i \text{ (לדוגמא:)}.$$

$$\left( cis\left(\frac{2\pi k}{n}\right) \right)^n = cis(2\pi k) = 1 \text{ , ולכן } cis(\alpha)cis(\beta) = cis(\alpha + \beta) \text{ , זאת כיוון ש}$$

ל  $\Omega_n$  קוראים חבורת שורשי- $n$  של היחידה.

## קריטריונים לבדיקה האם תת-קבוצה היא ת"ח:

### משפט קיצור הדרך 1:

תהי  $H$  תת קבוצה לא ריקה של  $G$ . אז  $H \leq G$  אם ורק אם:

$$\forall a, b \in H, ab \in H \quad (1)$$

$$\forall a \in H, a^{-1} \in H \quad (2)$$

### משפט קיצור הדרך 2:

תהי  $H$  תת קבוצה לא ריקה של  $G$ . אז  $H \leq G$  אם ורק אם:

$$\forall a, b \in H, ab^{-1} \in H$$

**תרגיל:** הראו שהתת-חבורות היחידות של  $\mathbb{Z}$  הן מהצורה  $n\mathbb{Z}$ .

**פתרון:** תחילה נראה שמתקיים  $n\mathbb{Z} \leq \mathbb{Z}$ . ע"פ משפט קיצור הדרך מספיק להראות שלכל  $a, b \in n\mathbb{Z}$

מתקיים  $a - b \in n\mathbb{Z}$  (שימו לב לשינוי הקריטריון לכתוב החיבורי). כיוון ש  $a, b \in n\mathbb{Z}$  אזי קיימים

$$a', b' \in \mathbb{Z} \text{ כך ש- } a = na', b = nb'. \text{ לכן } a - b = na' - nb' = n(a' - b') \in n\mathbb{Z} \text{ כנדרש.}$$

כעת, האם יש ל  $\mathbb{Z}$  ת"ח מצורה שונה? תהי  $\{0\} \neq H \leq \mathbb{Z}$ , וניקח את  $0 < n \in H$  המינימלי, ונטען ש

$$H = n\mathbb{Z}. \text{ יהי } k \in H \text{ ונחלק את } n \text{ ב } k \text{ חלוקה עם שארית: } k = nq + r, 0 \leq r < n \text{ ואז נקבל}$$

$$k - nq = r \in H \text{ וזה יכול להיות רק אם } r = 0 \text{ (אחרת סתירה למינימליות נ). בצורה דומה ניתן להראות}$$

$$\text{שכל ת"ח של } n\mathbb{Z} \text{ הם מהצורה } m\mathbb{Z} \text{ כאשר } m | n.$$

**הערה:** אם  $A, B \leq G$  וגם  $A \subseteq B$  אזי בוודאי שגם  $A \leq B$  (אין צורך להוכיח זאת, זה נובע ישירות

מהגדרה, הרבה סטודנטים מנסים להוכיח זאת בעזרת משפטי קיצור הדרך).

**תרגיל:** אם  $G$  חבורה סופית ו- $H$  תת-קבוצה של  $G$  אזי  $H \leq G$  אם ורק אם  $H \neq \emptyset$  וגם

$$x, y \in H \Rightarrow xy \in H$$

**הוכחה:** כיוון  $\leq$  ברור. בכיוון השני, מספיק לפי משפט קיצור הדרך להראות  $\forall a \in H, a^{-1} \in H$ . יהי

$$e \neq a \in H \text{ (אם } H = \{e\} \text{ אזי סיימנו). לפי התנאי, מתקיים } a \in H \Rightarrow a^2 = aa \in H \text{ , ובאינדוקציה רואים}$$

שכל החזקות החיוביות של  $a$  הן ב  $H$ . אבל החבורה היא סופית, ולכן בסדרה  $a, a^2, a^3, \dots, a^n, \dots$

$$\text{קיימים } i < j \text{ כך ש } a^i = a^j \text{ ונקבל } a^{j-i} = e \text{ , ומכאן נקבל ש- } a^{-1} = a^{j-i-1} \Leftarrow aa^{j-i-1} = a^{j-i-1}a = e$$

**משפט:** יהי  $G$  חבורה ו  $H, K \leq G$  אז  $H \cap K \leq G$ .

**משפט:** יהי  $\{H_i\}_{i \in I}$  קבוצה לא בהכרח סופית של תתי חבורות של חבורה  $G$  אז חיתוכן הוא תת חבורה.

### דוגמא:

יהיו  $a\mathbb{Z}, b\mathbb{Z}$  ת"ח של  $\mathbb{Z}$ . אזי  $a\mathbb{Z} \cap b\mathbb{Z} = \text{lcm}(a, b)\mathbb{Z}$  (לדוגמא:  $2\mathbb{Z} \cap 3\mathbb{Z} = \text{lcm}(2, 3)\mathbb{Z} = 6\mathbb{Z}$ ). מדוע?  
אם  $m \in a\mathbb{Z} \cap b\mathbb{Z}$  אזי  $a|m$  וגם  $b|m$  ולכן לפי תכונות של הכפולה המשותפת המינימלית,  $\text{lcm}(a, b) | m$ , ולכן  $m \in \text{lcm}(a, b)\mathbb{Z}$ . אם  $m \in \text{lcm}(a, b)\mathbb{Z}$  אזי  $\text{lcm}(a, b) | m$  ואז לפי טרנזיטיביות חילוק נקבל  $a | m \Rightarrow a | \text{lcm}(a, b)$  ואותו דבר גם עבור  $b$ . לכן  $m \in a\mathbb{Z} \cap b\mathbb{Z}$ .

**תרגיל בית:** אם נסמן  $a\mathbb{Z} + b\mathbb{Z} = \{an + bm | n, m \in \mathbb{Z}\}$  אזי  $a\mathbb{Z} + b\mathbb{Z} = \text{gcd}(a, b)\mathbb{Z}$ .

### ת"ח ציקליות:

הראינו בתרגול הקודם שעבור חבורה  $G$  ואיבר  $a \in G$ , קבוצת כל החזקות של  $a$  היא ת"ח  $\langle a \rangle = \{a^n | n \in \mathbb{Z}\} \leq G$ .

**הגדרה:** נקרא ל  $\{a^n | n \in \mathbb{Z}\} \leq G$  ת"ח הציקלית של  $G$  הנוצרת ע"י  $a$  ונסמן ב  $\langle a \rangle$ .  
חבורה הנוצרת ע"י איבר אחד נקראת חבורה ציקלית ( $\langle a \rangle = G$ ).  
המשמעות של הגדרה זו שאם  $G$  חבורה ציקלית אז קיים איבר  $a \in G$  כך שכל איבר  $g \in G$  מקיים  $g = a^n$ . כלומר כל איבר ב  $G$  הוא חזקה של  $a$ .

**תרגיל:** הראו שבחבורה סופית מתקיים  $\langle a \rangle = \{a^n | n \in \mathbb{N}\}$  (כלומר לא צריך לדרוש ש

$$\langle a \rangle = \{a^n | n \in \mathbb{Z}\} \text{ (כלומר } a^0 = e, a^{-n} \in \langle a \rangle \text{)}$$

**פתרון:** ראינו שכדי להוכיח שתת-קבוצה של חבורה סופית היא תת-חבורה, מספיק שהיא תהיה לא ריקה ושתהיה סגורה לכפל. בוודאי ששני התנאים מתקיימים עבור  $\langle a \rangle$ .

**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  $2 \times 2$  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  $|\langle 3 \rangle| = 4$ .

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

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

**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  $|(a, b)| \leq n$  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 צמדדים 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  $O(a) = 2$  □

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

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

**פתרון:** נסמן  $|gh| = m$ . אזי:

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

לכן  $m | nk$ .

$$g^{mk} = g^{mk} e = g^{mk} (h^k)^m = (gh)^{mk} = e$$

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

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

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