

תרגיל: תהי G חבורה כלשהי, ונסמן ב- H את אוסף האיברים ב- G מסדר סופי. כלומר:

$$H = \{g \in G : \exists n \in \mathbb{N} : g^n = e\}$$

הוכיחו/ הפריכו: H היא תת חבורה.

פתרון:

בסוף התרגול הקודם הוכחנו שלכל $g \in G$, $o(g) = o(g^{-1})$. ולכן אם $g \in H$ גם $g^{-1} \in H$. כלומר, יש סגירות להופכי.

סגירות למכפלה: יהיו $a, b \in H$. נסמן $o(a) = n$, $o(b) = m$.

$$(ab)^{nm} = a^{n-1}(ab)(ab)(ab) \dots (ab)b^{m-1}$$

לא ניתן להוכיח בחבורה כללית!

הפרכה: נחפש הפרכה בחבורה לא אבלית מסדר אינסופי (כי בחבורה סופית כל איבר הוא מסדר סופי)- מטריצות

$$G = GL_2(\mathbb{R})$$

$$a = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

$$a^2 = b^2 = I$$

$$ab = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}$$

$$p_{ab} = (x-2)(x-1) - 1 = x^2 - 3x + 1$$

אם היה קיים n כך ש

$$(ab)^n = I$$

אז זה היה מאפס את הפולינום

$$x^n - 1$$

ולכן

$$m_{ab} | (x^n - 1)$$

אבל זאת מטריצה לא סקלית מדרגה 2, אז $m_{ab} = p_{ab}$

וניתן לראות ש

$$x^2 - 3x + 1 \nmid x^n - 1$$

כי אפשר לפרק אותם לגורמים מדרגה 1 מעל המרוכבים.
דוגמא נוספת:

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

$$a^2 = -I, a^4 = I$$

$$b^3 = I$$

$$ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq I$$

ניתן להוכיח באנדוקציה.

עבור $n = 1$ נתון.

עבור $n = k + 1$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}$$

שאלה: אם a ו b מסדר סופי, לא מתחלפות. האם המכפלה היא בהכרח מסדר לא סופי?
כמובן שלא. למשל, תקחו חבורה סופית לא אבלית. כל האיברים מסדר.

תרגיל: תהי G חבורה אבלית, הוכיחו שאוסף האיברים מסדר סופי הוא תת חבורה.

הוכחה: סגירות להופכי-ראינו.

איבר יחידה- ברור, כי $e = 1$.

סגירות לכפל: יהיו $a, b \in H$. נסמן $o(a) = n, o(b) = m$.

$$(ab)^{nm} = (ab)(ab)(ab) \cdots (ab) = a^{nm} b^{nm} = (a^n)^m (b^m)^n = e^m e^n = e$$

הגדרה: תהי G חבורה. נאמר ש G ציקלית, אם קיים $g \in G$ כך ש $G = \langle g \rangle$.

לדוגמא: $\mathbb{Z} = \langle 1 \rangle$

$\mathbb{Z}_n = \langle 1 \rangle$

משפט: תהי G חבורה סופית. G ציקלית אם קיים איבר $g \in G$, $o(g) = |G|$.

דוגמא: $G = U_{12}$. האם היא ציקלית?

$$G = \{1, 5, 7, 11\}$$

$|G| = 4$ האם קיים איבר מסדר 4?

$$5^2 = 25 \pmod{12} = 1$$

$$7^2 = 49 \pmod{12} = 1$$

$$11^2 = 1$$

אין איבר מסדר 4, לכן החבורה לא ציקלית.
תרגיל: $G = \mathbb{Z}_3 \times \mathbb{Z}_4$. האם היא ציקלית?

$$o(1, 1) = \text{lcm}(o(1), o(1)) = \text{lcm}(3, 4) = 12 = |G|$$

תרגיל: $G = \mathbb{Z}_n \times \mathbb{Z}_n$. האם היא ציקלית?
אם יש יוצר, הוא מהצורה (a, b) והסדר שלו הוא n^2 . לכל איבר ב- \mathbb{Z}_n , הסדר שלו הוא לכל היותר n .

$$o(a, b) = \text{lcm}(o(a), o(b)) \leq o(a)o(b) \leq n^2$$

המכפלה שווה ל- n^2 רק כאשר שניהם שווים ל- n . ואז lcm שווה ל- n .
החבורה לא ציקלית כי יש בה n^2 איברים, אבל אין איבר מסדר n^2 .
שאלה: האם יש ב- $\mathbb{Z}_n \times \mathbb{Z}_n$ קיים איבר מסדר גדול מ- n ?
תשובה: לא. כי כל איבר בחזקת n שווה ל-0.

$$(a, b)^n = (a^n, b^n) = (na \pmod n, nb \pmod n) = (0, 0)$$

ולכן הסדר של כל איבר קטן שווה ל- n .

$$o(g^d) = \frac{n}{(d, n)} \text{ או } o(g) = n \text{ הוכתם שאם } o(g) = n$$

מסקנה: תהי G חבורה ציקלית סופית. $\langle g \rangle = \{g, g^2, g^3, \dots, g^n = e\}$ לא צריך
חזקות שליליות, כי $g^{-1} = g^{n-1}$. אמרנו שאיבר הוא יוצר, אם הסדר שלו שווה למספר האיברים
בחבורה.

$$o(g^d) = n \text{ לכן יהיה יוצר אם } o(g^d) = n$$

$$o(g^d) = \frac{n}{(n, d)}$$

לכן g^d הוא יוצר אם $(g, d) = 1$. כלומר, מספר היוצרים שווה למספר המספרים שזרים ל- n .
זוה $\varphi(n)$.

דוגמא: בחבורה $G = \mathbb{Z}_3 \times \mathbb{Z}_4$ יש 4 יוצרים. מי היוצרים?

$$(1, 1), (1, 1)^5 = (2, 1), (1, 1)^7 = (1, 3), (1, 1)^{11} = (2, 3)$$

דוגמא נוספת: U_7 מי היוצרים?

$$U_7 = \{1, 2, 3, 4, 5, 6\}$$

יש 6 איברים, אז מספר היוצרים הוא $\varphi(6) = 2$.

$$2, 4, 1 \rightarrow o(2) = 3$$

$$3, 2, 6, 4, 5, 1$$

3 הוא היוצר.

היוצר השני הוא 3^5 . שזה 5.

כלומר, היוצרים הם 3, 5.

משפט מההרצאה: תהי G חבורה סופית. לכל $G, g \in G$, $o(g) \mid |G|$.

תרגיל: תהי G חבורה לא אבלית מסדר 8. הוכיחו שיש ב- G איבר מסדר 4.

פתרון: הסדרים האפשריים הם 1, 2, 4, 8.

8 לא יכול להיות, כי אם יש איבר מסדר 8 החבורה ציקלית ולכן בהכרח אבלית.

e הוא היחיד מסדר 1.

אם כל שאר האיברים מסדר 2, זה אומר שלכל $a \in G$, $a^2 = e$, ואז נובע שהחבורה אבלית

(מתרגיל שעשינו בתרגול הראשון).

כלומר, קיים איבר מסדר 4.

תרגיל: תהי G חבורה סופית. הוכיחו שיש ב- G איבר מסדר 2 אם $|G|$ זוגי.

הוכחה: \Leftarrow : אם יש ב- G איבר מסדר 2, אז הסדר שלו מחלק את $|G|$, ולכן $|G|$ חייב להיות

זוגי.

\Rightarrow אם $|G|$ זוגי, אז ראיתם ב"ב שיש ב- G איבר מסדר 2.

הסבר: אפשר לחלק את האיברים ב- G לזוגות של איבר וההופכי שלו.

$$\{g_1, g_1^{-1}\}, \{g_2, g_2^{-1}\}, \dots, \{g_n, g_n^{-1}\}$$

אחד מהאיברים ב- G הוא e , והוא ההופכי של עצמו. כלומר, יש "זוג" שיש בו רק איבר אחד.

בגלל שמספר האיברים ב- G זוגי, חייב להיות זוג נוסף שיש בו רק איבר אחד. זה אומר שהאיבר

הזה הוא ההופכי של עצמו, כלומר, הוא מסדר 2.

ניתן לראות באותו אופן שמספר האיברים מסדר 2 הוא אי זוגי.

מסקנה: (משפט אוילר) אם $(x, n) = 1$ אז $x^{\varphi(n)} \equiv 1 \pmod{n}$.

תרגיל: חשבו את שתי הספרות האחרונות של

$$88211^{4039}$$

פתרון: לחשב 2 ספרות זה בעצם מודולו 100.

$$88211^{4039} \pmod{100} \equiv 11^{4039} \pmod{100}$$

$$11^{\varphi(100)} \equiv 1 \pmod{100} \text{ ולכן } (11, 100) = 1$$

$$\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$$

$$11^{4039} \pmod{100} = 11^{4000} \pmod{100} \cdot 11^{39} \pmod{100} =$$

$$(11^{40})^{100} \pmod{100} \cdot 11^{39} \pmod{100} =$$

$$(11^{40} \pmod{100})^{100} \cdot 11^{39} \pmod{100} =$$

$$11^{39} \pmod{100}$$

מכיוון שאנחנו יודעים ש $11^{40} \equiv 1 \pmod{100}$, אז $11^{39} = 11^{-1} \pmod{100}$.
 כלומר, אנחנו רוצים לחשב את ההופכי את ההופכי של 11 ב U_{100} .

$$1 = 100 - 9 \cdot 11$$

כלומר, ההופכי של 11 הוא $91 \equiv -9$.

שתי הספרות האחרונות הן 91.

הגדרה: לכל n ניתן להגדיר את אוסף שורשי היחידה מסדר n ב $(\mathbb{C} \setminus \{0\}, \cdot)$.

$$\Omega_n = \{x \in \mathbb{C} : x^n = 1\} = \left\{ cis\left(\frac{2\pi k}{n}\right) \right\}$$

חבורת שורשי היחידה:

$$\Omega_\infty = \bigcup \Omega_n$$

זה אכן תת חבורה, כי זה בדיוק האוסף של כל האיברים מסדר סופי בחבורה אבלית.
 זאת חבורה אינסופית, שכל האיברים בה מסדר סופי. ויותר מזה- מכל סדר קיים איבר.
 דומגא לחבורה אינסופית שכל האיברים בה מסדר 2:

$$\prod_{\mathbb{N}} \mathbb{Z}_2$$

וקטורים אינסופיים של 0, 1 עם פעולת חיבור מודולו 2.

שאלה: האם קיימת חבורה אינסופית שכל האיברים בה מסדר 4?

תשובה: ברור שלא!!!! כי אם x הוא איבר מסדר 4, אז x^2 הוא איבר מסדר 2.

הגדרה: תהי G חבורה, ו $x_1, \dots, x_n \in G$. התת חבורה שנוצרת ע"י האיברים היא:

$$\langle x_1, \dots, x_n \rangle = \bigcap_{\{x_1, \dots, x_n\} \subseteq H \leq G} H$$

באופן קונקרטי: החבורה שנוצרת ע"י x_1, \dots, x_n מורכבת מכל האיברים שאפשר ליצור עם x_1, \dots, x_n וההופכיים שלהם.

G נקראת נוצרת סופית, אם יש קבוצה סופית G $x_1, \dots, x_n \in G$, כך ש

$$G = \langle x_1, \dots, x_n \rangle$$

דוגמא Ω_∞ לא נוצרת סופית.

הוכחה: נניח בשלילה ש Ω_∞ נוצרת ע"י x_1, \dots, x_n כלשהם. נסמן ב m את הכפולה של כל הסדרים. כל אחד מהאיברים וההופכיים שלהם, וכפולות של איברים כאלה, בגלל שהחבורה אבלית, יהפוך ל e כשנעלה אותו בחזקת m .

ואנחנו יודעים שב Ω_∞ יש איברים מכל סדר, ובפרט מסדר גדול מ m .
דוגמא לחבורה אינסופית נוצרת סופית:

$$\mathbb{Z} \times \mathbb{Z}$$

היא לא ציקלית. אבל היא נוצרת סופית ע"י $(0, 1), (1, 0)$.