

תזכורת: תהי G חבורה, המרכז של G

$$Z(G) = \{g \in G : \forall x \in G, gx = xg\}$$

לדוגמה: $Z(G) = G$ אבלית אמ"ם
תרגיל: חשבו את $Z(GL_n(\mathbb{F}))$
פתרון:

$$Z(GL_n(\mathbb{F})) = \{\alpha I : \alpha \neq 0\}$$

במילים: אוסף המטריצות הסקלריות חוץ מ-0.
נוכיח עם הכלה דו כיוונית.
 $\{\alpha I : \alpha \neq 0\} \subseteq Z(GL_n(\mathbb{F}))$
צריך להוכיח שלכל $\alpha \neq 0$ ולכל $A \in GL_n(\mathbb{F})$:

$$\alpha IA = A(\alpha I)$$

אבל שתיהן שוות ל

$$\alpha A$$

ולכן הן שוות.
 $\{\alpha I : \alpha \neq 0\} \supseteq Z(GL_n(\mathbb{F}))$
תהי $A \in Z(GL_n(\mathbb{F}))$. בשביל להוכיח ש A סקלרית, צריך להוכיח שלכל $i \neq j$

$$A_{i,j} = 0$$

ולכל i, j

$$A_{i,i} = A_{j,j}$$

כלומר, האיברים מחוץ לאלכסון הם 0, ואיברי האלכסון שווים זה לזה.
נסמן $E_{i,j}$ להיות המטריצה שבמקום i, j יש 1 ובכל השאר 0.
לכל $i \neq j$, נסתכל על המטריצה $I + E_{i,j}$.
 $I + E_{i,j} \in GL_n(\mathbb{F})$ כי היא מטריצה משולשית שאיברי האלכסון הם 1, אז הדטרמיננטה שלה שווה ל-1.
לכן

$$A(I + E_{i,j}) = (I + E_{i,j})A$$

$$A + AE_{i,j} = A + E_{i,j}A$$

$$AE_{i,j} = E_{i,j}A$$

$AE_{i,j}$ - נחשב למה שווה כל עמודה. ידוע שזה שווה ל A כפול העמודה המתאימה. חוץ מהעמודה j כל העמודות הן עמודות אפסים. לכן במטריצה $AE_{i,j}$ כל העמודות שוות ל 0 חוץ מהעמודה j , שהיא שווה לעמודה i של A . (כי זה בעצם (Ae_i)). באופן דומה, $E_{i,j}A$ שווה למטריצה שכל השורות שלה אפסים חוץ מהשורה i ששווה לשורה j של A . המטריצות הנ"ל שוות, ולכן שוות בכל רכיב. יש רק רכיב אחד שבשתי המטריצות הוא לא בהכרח מתאפס. זה האיבר במקום i, j של שתי המטריצות.

$$(AE_{i,j})_{i,j} =$$

זה שווה לרכיב i בעמודה j . אבל העמודה j שווה לעמודה i של A . זה שווה ל $A_{i,i}$.

$$(E_{i,j}A) =$$

זה שווה לרכיב j בשורה i של $(E_{i,j}A)$, אבל השורה i שווה לשורה j של A . כלומר, זה שווה ל $A_{j,j}$ ש"ח קיבלנו ש

$$A_{i,i} = A_{j,j}$$

אפשר להפעיל זאת לכל i, j ולכן נקבל שכל איברי האלכסון שווים. כעת, נסתכל על

$$(AE_{i,j})_{k,j}$$

כאשר $k \neq i$. זה שווה ל

$$(E_{i,j}A)_{k,j}$$

זה לא בשורה i ולכן שווה ל 0. אבל

$$E_{i,j}(A)_{k,j} = A_{k,i}$$

כלומר, ש"ח קיבלנו שכל האיברים בעמודה i של A , חוץ מ $A_{i,i}$ שווים ל 0. ניתן לעשות זאת לכל i ולכל j , ולכן קיבלנו שבכל עמודה, כל איברי העמודה חוץ מהאיבר שבאלכסון שווים ל 0.

תרגיל: תהי $G \leq H$, הוכיחו/הפריכו:

$$Z(H) = Z(G) \cap H$$

במידה ולא, קבעו האם יש הכלה נכונה.
 פתרון:
 \supseteq : יהי $H \cap Z(G) = \{h\}$. זה נכון בגלל שהוא מתחלף עם כל האיברים ב G כי הוא שייך ל $Z(G)$.
 דוגמא נגדית בכיוון השני:

$$G = GL_n(\mathbb{F})$$

$$H = \text{matrices diagonal}$$

H אבליית, ולכן

$$Z(H) = H$$

חבורת אוילר:
 בהרצאה הוכחתם שלכל מונואיד M , יש את חבורת ההפיכים $U(M)$.
 מונואיד ספציפי שמעניין אותנו הוא (\mathbb{Z}_n, \cdot) . לחבורת ההפיכים קוראים U_n .
 בהרצאה הוכחתם ש U_n שווה לאיברים שזרים ל n .
 נחזור על ההוכחה:
 יהי $m \in \text{lcm}_n$ שזר ל n . זה אומר שקיים צירוף לינארי ששווה 1. כלומר,

$$\alpha m + \beta n = 1$$

$$\alpha m \equiv 1 \pmod n$$

לכן m הפיך וההופכי שלו הוא α . אבל ההופכי צריך להיות בתחום של $\{0, \dots, n-1\}$. נקח $\alpha \pmod n$.
 תרגיל: מצאו את ההופכי של 61 ב U_{234} .
 פתרון: אנחנו צריכים למצוא את הצירוף הלינארי של 61 ו 234 שיוצא 1, ולקחת את המקדם של 61.

$$234 = 3 \cdot 61 + 51 \rightarrow 51 = 234 - 3 \cdot 61$$

$$61 = 51 + 10 \rightarrow 10 = 61 - 51 = 4 \cdot 61 - 234$$

$$51 = 5 \cdot 10 + 1 \rightarrow 1 = 51 - 5 \cdot 10 = 6 \cdot 234 - 23 \cdot 61$$

אז ההופכי של 61 הוא $-23 \pmod{234}$ שזה 211.

הערה: אם נרצה לפתור משוואה, למשל:

$$61x \equiv 18 \pmod{234}$$

פשוט נכפיל בהופכי של 61. $x = 211 \cdot 18 \pmod{234} = 54$.
 הגדרה: פונקציית אוילר

$$\varphi(n) = |U_n|$$

ראיתם בהרצאה נוסחא לחישוב פונקציית אוילר:

$$n = p_1^{m_1} \cdot \dots \cdot p_k^{m_k}$$

אז

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)$$

(הערה: אם n, m זרים אז $\varphi(nm) = \varphi(n)\varphi(m)$)

$$U_{mn} \rightarrow U_m \times U_n$$

$$\text{lcm}_{mn} \rightarrow \text{lcm}_m \times \text{lcm}_n$$

$$x \rightarrow (x \pmod m, x \pmod n)$$

$$\alpha m + \beta n = 1$$

הפונקציה $\text{lcm}_{mn} \rightarrow \text{lcm}_m \times \text{lcm}_n$ היא חח"ע ועל. בנוסף, אם $x \in U_{mn}$ אז $x \pmod m \in U_m$ וזה נובע מהצירוף הלינארי שיוצא 1. $\alpha x + \beta mn = 1$.
 ולכן $U_{mn} \rightarrow U_m \times U_n$. בנוסף, אם $x \in \text{lcm}_{mn} \setminus U_{mn}$ אז יש ראשוני $p|x$ וגם $p|mn$.
 הוכחנו בתרגול הראשון שאם ראשוני מחלק כפולה אז הוא מחלק אחד מהם. ולכן לא זר ל m או n .
 ש x לא זר ל n .

לכן לכן איבר ב $U_m \times U_n$ יש מקור ב lcm_{mn} , והמקור הזה חייב להיות ב U_{mn} .
 וצמצום של פו' חח"ע הוא חח"ע.
 לכן $U_{mn} \rightarrow U_m \times U_n$ היא חח"ע ועל, ולכן הגדלים שווים. כלומר,

$$\varphi(mn) = |U_{mn}| = |U_m \times U_n| = |U_m| |U_n| = \varphi(m)\varphi(n)$$

הגדרה: תהי G חבורה ו $g \in G$ חבורה $\{g^n = e\}$. אם הקבוצה ריקה אז הסדר הוא אינסוף.

דוגמא: מה הסדר של 3 ב U_{11} .

$$3, 9, 5, 4, 1$$

הסדר הוא 5.

תרגיל: נסתכל על חבורת הפונקציות ההפיכות lcm ל lcm . זאת חבורה עם פעולת הרכבה. מה הסדרים האפשריים של איברי החבורה?
פתרון: 1- פונקציית הזהות.
-2

$$f(1) = 2$$

$$f(2) = 1$$

$$f(n) = n$$

לכל n , נקח

$$1 \rightarrow 2 \rightarrow 3 \rightarrow \dots \rightarrow n \rightarrow 1$$

וכל שאר האיברים הולכים לעצמם. הפונקציה הזאת מסדר n .
פונקציה מסדר אינסוף: נפרק את lcm למחזורים הולכים וגדלים.

$$\{1, 2\}, \{3, 4, 5\}, \{6, 7, 8, 9\}$$

ובתוך כל קבוצה עושים מחזור מעגלי. זה פונקציה מסדר אינסוף.
תכונה של סדר:

אם $o(a) = n$, אז $a^d = e$ אם $n|d$.
תרגיל: יהיו G ו H חבורות, ונסתכל על $G \times H$ (כפל רכיב-רכיב). הוכיחו ש

$$o(g, h) = lcm(o(g), o(h))$$

הוכחה:

$$o(g, h) \leq lcm(o(g), o(h))$$

$$(g, h)^{lcm(o(g), o(h))} = (g^{lcm(o(g), o(h))}, h^{lcm(o(g), o(h))}) = (e, e)$$

כי מהגדרה, lcm של שני מספרים הוא כפולה של כל אחד מהמספרים, אז משתמשים בתכונה שכתבנו.

$$o(g, h) \geq lcm(o(g), o(h))$$

$$(e, e) = (g, h)^{o(g, h)} = (g^{o(g, h)}, h^{o(g, h)})$$

לכן מהתכונה שכתבנו $o(g) | o(h) \wedge o(h) | o(g, h)$
 לכן מתכונה של lcm (שהוכחתם בש"ב) $lcm(o(g), o(h)) | o(g, h)$ ובפרט $lcm(o(g), o(h)) \leq o(g, h)$

תרגיל: הוכיחו שלכל $a \in G$, $o(a) = o(a^{-1})$
 הוכחה:
 אם הסדר של a סופי:

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

$$(a^{-1})^{o(a)} = (a^{o(a)})^{-1} = e^{-1} = e$$

(ההופכי של מכפלה הוא מכפלת ההופכיים)

$$o(a^{-1}) | o(a)$$

באופן סימטרי נקבל $o(a) | o(a^{-1})$

$$o(a) = o(a^{-1})$$

אם הסדר של a הוא אינסופי, אז גם הסדר של a^{-1} הוא אינסופי, אחרת, יש n כך ש $(a^{-1})^n = e$
 ואז נקבל ש $a^n = e$, וזאת סתירה.