

הגדרה: תהי G חבורה. המרכז של G

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

למשל, אם G אבלית, אז

$$Z(G) = G$$

תרגיל: חשבו

$$Z(GL_n(\mathbb{F}))$$

פתרון:

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

נוכיח הכלה דו כיוונית: $\{\alpha I : \alpha \in \mathbb{F} \setminus \{0\}\} \subseteq Z(GL_n(\mathbb{F}))$.
אכן, תהי $A \in GL_n(\mathbb{F})$ אז ידוע ש

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

תהי $A \in Z(GL_n(\mathbb{F}))$. $Z(GL_n(\mathbb{F})) \subseteq \{\alpha I : \alpha \in \mathbb{F} \setminus \{0\}\}$.
בשביל להוכיח שמטריצה היא סקלרית צריך להוכיח שלכל i, j :

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

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

A מתחלפת עם כל מטריצה הפיכה, בפרט היא מתחלפת עם המטריצה

$$I + E_{i,j}$$

עבור $i \neq j$

(כלומר, מטריצה שעל האלכסון יש 1, וברכיב ה- i, j יש 1)
היא הפיכה כי היא משולשית (עליונה או תחתונה, תלוי בערכים של i, j) ולכן הדטרמיננטה שלה היא מכפלת איברי האלכסון, כלומר 1. מתקיים:

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

כלומר:

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

לכן

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

עבור מטריצה A כלשהי, $AE_{i,j}$ היא מטריצה שהעמודה ה- j שלה שווה לעמודה ה- i של A , וכל שאר העמודות הן 0.

עבור מטריצה A כלשהי, $E_{i,j}A$ היא מטריצה שהשורה ה- i שלה שווה לשורה ה- j של A , ושאר השורות הן 0.

מכיוון ששתי המטריצות שוות, לכן לכל k, l

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

מכיוון שבמטריצה השמאלית יש רק עמודה אחת שונה מ-0 וכל השאר הן עמודות אפסים, אז

$$\forall l \neq j (E_{i,j}A)_{k,l} = 0$$

ולכן

$$\forall l \neq j (AE_{i,j})_{k,l} = 0$$

כלומר, השורה ה- i של $AE_{i,j}$ שווה ל-0 חוץ ברכיב ה- j (הוא יכול להיות 0, אבל לא בהכרח). אבל זה שווה לשורה ה- j של A . כלומר, השורה ה- j של A שווה כולה ל-0 חוץ מברכיב ה- j שלה. כלומר, קיבלנו ש A אלכסונית. בנוסף,

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

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

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

סה"כ קיבלנו ש

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

זה נכון לכל i, j . לכן כל איברי האלכסון שווים. כלומר, המטריצה סקלרית. הוכיחו/הפריכו:

תהי G חבורה ו $H \leq G$. אזי:

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

פתרון : נוכיח $Z(H) \supseteq Z(G) \cap H$: יהי $g \in Z(G) \cap H$. לכן $g \in Z(G)$. כלומר, לכל $x \in G$,

$$gx = xg$$

בפרט, לכל $x \in H$

$$gx = xg$$

כמו כן, $g \in H$ ולכן

$$g \in Z(H)$$

למה זה תת חבורה : הוכחתם בהרצאה שמרכז של חבורה הוא תת חבורה, לכן $Z(G)$ תת חבורה, וכן H תת חבורה מהנתון. בנוסף, הוכחנו בתרגול הקודם שחיתוך של תת חבורות הוא תת חבורה. לכן $Z(G) \cap H$ הוא תת חבורה של G . אבל הוא מוכל ב- H , אז הוא גם תת חבורה של H .
דוגמא נגדית להכללה השנייה :

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

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

$$Z(H) = H$$

כי ידוע שכל שתי מטריצות אלכסיניות מתחלפות (להכפיל שתי מטריצות אלכסיניות זה פשוט כפל רכיב-רכיב באיברי האלכסון). אז H היא תת חבורה אבלית. אבל

$$H \cap Z(G) = \{\text{matrices scalar}\}$$

חבורת אוילר :
תזכורת : לכל מונואיד M , מוגדרת חבורת ההופכיים. מסמנים $U(M)$.
דוגמא קנונית : (\mathbb{Z}_n, \cdot) זה מונואיד (לא חבורה). לחבורת ההופכיים של המונואיד הנ"ל קוראים חבורת אוילר של n , מסמנים U_n .
בהרצאה הוכחתם שהאיברים ב- U_n הם כל המספרים שזרים ל- n (בין 1 ל- n).
לדוגמא :

$$U_6 = \{1, 5\}$$

$$5 \cdot 5 = 1$$

זכרו שהפעולה היא מודולו n .
 תרגיל: פתרו את המשוואה הבאה:

$$61x \equiv 1 \pmod{234}$$

פתרון: למעשה אנחנו מחפשים את ההופכי של 61 ב- U_{234} .
 איך הוכחתם בהרצאה שהאיברים ההפיכים הם בדיוק האיברים הזרים?
 יהי n כלשהו ו- $0 \leq m \leq n-1$.
 m הפיך אמ"ם קיים x כך ש- $mx \equiv 1 \pmod{n}$. כלומר, $n \mid mx - 1$. כלומר, קיים $k \in \mathbb{Z}$ כך ש- $kn = mx - 1$.
 כלומר, $mx - kn = 1$. זה אומר שה- gcd של m ו- n הוא 1. וזה אומר שהם זרים.
 כלומר, ההופכי של m הוא המקדם של m בצירוף הלינארי של m ו- n שנותן 1.
 לפי אלגוריתם אוקלידס אנחנו יודעים למצוא את המקדם בצירוף הלינארי.

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

$$61 = 51 + 10 \rightarrow 10 = 61 - 51 = 61 - (234 - 3 \cdot 61) = 4 \cdot 61 - 234$$

$$51 = 5 \cdot 10 + 1 \rightarrow 1 = 51 - 5 \cdot 10 = (234 - 3 \cdot 61) - 5(4 \cdot 61 - 234)$$

$$= 6 \cdot 234 - 23 \cdot 61$$

$$6 \cdot 234 - 23 \cdot 61 = 1$$

$$-23 \cdot 61 - 1 = -6 \cdot 234$$

מפה נקבל $x = -23$
 אם רוצים למצוא הופכי ב- U_{234} אז צריך להעביר את התשובה לתחום שבין 0 ל-233.

$$234 - 23 = 211$$

$x = 211$
 תרגיל: פתרו את המשוואה:

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

פתרון: ידוע ש

$$61 \cdot 211 \equiv 1 \pmod{234}$$

ולכן

$$61 \cdot 211 \cdot 18 \equiv 1 \cdot 18 \pmod{234}$$

$$.x = 211 \cdot 18$$

$$x = 3798$$

צריך לחלק עם שארית ב-234.

$$3798 : 234 = 16.23\dots$$

$$234 \times 16 = 3744$$

$$3798 - 3744 = 54$$

אפשר להעביר את x לטווח שבין 0 ל-233. נקבל 54.

פונקציית אוילר:

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

כלומר, מספר האיברים ב- U_n .

בעצם, $\varphi(n)$ = מספר האיברים החיוביים שקטנים מ- n וזרים לו.

בהרצאה הוכחתם את הנוסחה הבאה: אם $n = p_1^{k_1} \dots p_m^{k_m}$

$$\varphi(p^k) = p^k - p^{k-1}$$

הוכחתם שאם n, m זרים אז

$$\varphi(nm) = \varphi(n) \cdot \varphi(m)$$

ולכן

$$\varphi(n) = \varphi(p_1^{k_1} \dots p_m^{k_m}) = \varphi(p_1^{k_1}) \dots \varphi(p_m^{k_m}) = (p_1^{k_1} - p_1^{k_1-1}) \dots (p_m^{k_m} - p_m^{k_m-1}) =$$

$$p_1^{k_1} \dots p_m^{k_m} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_m}\right) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_m}\right)$$

למשל:

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

סדרים של איברים:

הגדרה: תהי G חבורה ו- $a \in G$, הסדר של a , מסומן ב- $O(a)$ זה המספר הטבעי המינימלי n ,

כך ש- $a^n = e$. אם אין כזה אז $O(a) = \infty$.

לדוגמא: $O(2)$ ב- U_7 הוא?

פתרון:

$$2, 4, 1$$

$$.O(2) = 3$$

תרגיל: תהי G חבורת הפונקציות ההפיכות מ \mathbb{N} ל \mathbb{N} , עם פעולת הרכבה. מהם הסדרים האפשריים של איברים בחבורה?

פתרון: איבר מסדר 1- פונקציית הזהות.
איבר מסדר 2- נחלק את \mathbb{N} לזוגות,

1, 2

3, 4

5, 6

וכו'. ובכל זוג נבצע החלפה.

$1 \leftrightarrow 2$

וכו'.

זאת פונקציה מסדר 2.

אפשר לחלק את \mathbb{N} למיות:

$\{1, \dots, n\}, \{n+1, \dots, 2n\}, \dots$

ובכל n יהי לעשות מעגל:

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

זאת פונקציה מסדר n .

פונקציה מסדר אינסוף: נחלק את \mathbb{N} למחזורים מגדלים הולכים וגדלים.

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

ובכל אחד f עושה מעגל כמו בדוגמאות הקודמות.

אז זאת פונקציה הפיכה, שבשום חזקה לא שווה לזהות.

תזכורת: יהיו n, m מספרים טבעיים. $lcm(n, m)$ זה המספר החיובי המינימלי ששניהם

מחלקים.

למשל:

$$lcm(6, 4) = 12$$

תכונה ידועה: אם $n|k \wedge m|k$ אז $lcm(n, m)|k$.
תרגיל: יהיו G, H חבורות. בש"ב נתקלתם בחבורה

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

פעולה רכיב-רכיב.

נניח ש g ו h מסדר סופי. הוכיחו ש $o(g, h) = lcm(o(g), o(h))$
הוכחה: בשביל הנוחות נסמן $o(g) = n, o(h) = m$.
בהרצאה הוכחתם $g^k = e$ אם $o(g) | k$.
נניח

$$(g, h)^k = (e_G, e_H) \rightarrow g^k = e \wedge h^k = e \rightarrow n | k \wedge m | k$$

ולכן

$$lcm(n, m) | k$$

ולכן

$$lcm(n, m) \leq k$$

בנוסף, $n | lcm(n, m) \wedge m | lcm(n, m)$ ולכן

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

ולכן $lcm(n, m)$ הוא החזקה המינימלית שבה (g, h) יוצא היחידה.
ולכן $o(g, h) = lcm(o(g), o(h))$