

פתרון תרגיל בית 3 במבנים אלגבריים

89-214 סמסטר א' תשע"ז

הוראות בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך הגשת התרגיל הוא לתרגול בשבוע המתחיל בתאריך י"א כסלו ה'תשע"ז, 11.12.2016.

שאלות חימום

שאלה 1. הוכיחו שהקבוצה S_n עם פעולת ההרכבה בין פונקציות היא אכן חבורה.
שאלה 2. תהי $\sigma \in S_n$ המקיימת: $\sigma = \tau_1 \tau_2$, כאשר τ_1, τ_2 הם מחזורים זרים. הוכיחו כי $o(\sigma) = [o(\tau_1), o(\tau_2)]$.

שאלות להגשה

שאלה 3. תהי G חבורה אבלית. נסמן ב- T את אוסף האיברים מסדר סופי ב- G . הוכיחו כי $T \leq G$.

הוכחה. נוכיח זאת לפי הקריטריון הפחות מקוצר, כלומר נוכיח:

א. $e \in T$.

ב. אם $g_1, g_2 \in T$ אזי $g_1 g_2 \in T$.

ג. אם $g \in T$ אזי $g^{-1} \in T$.

אכן,

א. $e \in T$ כי $o(e) = 1 < \infty$.

ב. נניח ש- $g_1, g_2 \in T$. לכן $n = o(g_2) < \infty$, $m = o(g_1)$. כיוון שהחבורה G אבלית,

$$(g_1 g_2)^{mn} = g_1^{mn} g_2^{mn} = (g_1^m)^n (g_2^n)^m = e^n e^m = e$$

הוכחנו שקיים $k = mn < \infty$ שעבורו $(g_1 g_2)^k = e$; לכן, $o(g_1 g_2) \leq k < \infty$, כלומר $g_1 g_2 \in T$.

ג. הוכחנו בתרגול ש- $o(g^{-1}) = o(g)$ לכל $g \in G$. בפרט, אם $g \in T$ אזי $o(g) < \infty$, ולכן גם $o(g^{-1}) = o(g) < \infty$.

□ בסך הכל, לפי הקריטריון המקוצר, $T \leq G$.

שאלה 4. לכל תמורה σ מהתמורות הבאות, כתבו את σ כמכפלת מחזורים זרים, וחשבו את $o(\sigma^2)$.

א. S_9 -ב $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 9 & 7 & 1 & 6 & 4 & 3 & 8 \end{pmatrix}$.

ב. S_5 -ב $(1\ 2)(2\ 5\ 4)(3\ 1\ 4)(1\ 5)$.

פתרון.

א. נסמן את התמורה הנתונה σ . מפרקים לפי הדרך שראינו בתרגול. מקבלים כי יש את המעגלים הבאים:

$$1 \mapsto 5 \mapsto 1, 3 \mapsto 9 \mapsto 8 \mapsto 3, 4 \mapsto 7 \mapsto 4$$

לכן $\sigma = (1\ 5)(3\ 9\ 8)(4\ 7)$ (2 ו-6 נשלחים כל אחד לעצמו).
נחשב את σ^2 כיוון שמחזורים זרים מתחלפים זה עם זה, נקבל:

$$\sigma^2 = (1\ 5)^2 (3\ 9\ 8)^2 (4\ 7)^2 = (3\ 8\ 9)$$

ב. נסמן את התמורה הנתונה σ . פה התמורה בכלל לא נתונה בצורה נוחה; נכתוב אותה בצורה כמו של מטריצה:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix}$$

לכן קל לראות שיש פה מעגל אחד, כלומר $\sigma = (1\ 4\ 3\ 2\ 5)$. נחשב את σ^2 :

$$\sigma^2 = (1\ 4\ 3\ 2\ 5)^2 = (1\ 3\ 5\ 4\ 2)$$

שאלה 5. בכל סעיף נתונה חבורה G ותת-חבורה $H \leq G$. כתבו את כל המחלקות השמאליות של H ב- G :

א. $H = \langle 9 \rangle, G = (U_{14}, \cdot)$.

ב. $H = 5\mathbb{Z}_{15}, G = (\mathbb{Z}_{15}, +)$.

ג. $H = \{e\}$, חבורה כלשהי, G .

פתרון.

א. מכיוון ש- $G = (U_{14}, \cdot) = \{1, 3, 5, 9, 11, 13\}$ ו- $H = \langle 9 \rangle = \{1, 9, 11\}$ נצפה לקבל על פי משפט לגרנז' בדיוק שתי מחלקות שמאליות. אכן מתקיים:

$$1 \cdot H = H$$

$$3 \cdot H = \{3, 5, 13\}$$

$$5 \cdot H = \{3, 5, 13\}$$

$$9 \cdot H = H$$

$$11 \cdot H = H$$

$$13 \cdot H = \{3, 5, 13\}$$

בסה"כ:

$$G/H = \{H, 3H\}$$

ב. נשים לב ש- $H = 5\mathbb{Z}_{15} = \{0, 5, 10\}$ לכן, עפ"י לגרנז' נצפה לקבל בסה"כ 5 מחלקות שמאליות של H ב- G . חישוב פשוט מראה

$$0 + H = 5 + H = 10 + H = H = \{0, 5, 10\}$$

$$1 + H = 6 + H = 11 + H = \{1, 6, 11\}$$

$$2 + H = 7 + H = 12 + H = \{2, 7, 12\}$$

$$3 + H = 8 + H = 13 + H = \{3, 8, 13\}$$

$$4 + H = 9 + H = 14 + H = \{4, 9, 14\}$$

בסה"כ:

$$G/H = \{H, 1 + H, 2 + H, 3 + H, 4 + H\}$$

ג. מכיוון שתת החבורה H הינה החבורה הטריטוראלית (הכוללת רק איבר אחד - האיבר הניטרלי), המחלקות השמאליות הם פשוט איברי G ובסה"כ נקבל מספר מחלקות כמספר האיברים ב- G .

שאלה 6. נסתכל על $G = (GL_2(\mathbb{Z}_2), \cdot)$, חבורת המטריצות ההפיכות מגודל 2×2 מעל \mathbb{Z}_2

א. רשום את כל איברי הקבוצה G (הזכר בהבדל בין $GL_2(\mathbb{Z}_2)$ ל- $M_2(\mathbb{Z}_2)$ בעת הכנת רשימת האיברים).

ב. תהי תת חבורה של G : $A = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$. מהו האינדקס של A ב- G ?

ג. תהי תת חבורה של G : $B = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle$. מהו האינדקס של B ב- G ?

פתרון.

א. נרשום את כל המטריצות ההפיכות ($\det \neq 0$) מגודל 2×2 מעל \mathbb{Z}_2 :

$$\left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

ב. האינדקס של A ב- G , המסומן $[G : A]$, שווה על פי לגרנז' למנה $\frac{|G|}{|A|}$. את גודל החבורה G חישבנו למעשה בסעיף א', וקיבלנו $|G| = 6$. נותר לחשב את $|A|$:

$$[G : A] = \frac{|G|}{|A|} = \frac{6}{2} = 3 \text{ לכן } |A| = 2, \text{ כלומר } A = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

ג. נחשב את $|B|$: $B = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. כלומר $|B| = 3$. לכן $[G : B] = \frac{|G|}{|B|} = \frac{6}{3} = 2$

ד. תת החבורה C נוצרת על ידי שני יוצרים - היוצר של תת-החבורה A והיוצר של תת-החבורה B . בתת-החבורה B יש 3 איברים ותת-החבורה A אינה מוכלת ב- B , לכן בהכרח ב- C יש לפחות 4 איברים. כעת, מכיוון שסדר של תת-חבורה חייב לחלק את סדר החבורה, בהכרח $|C| = 6$, כלומר $C = G$. לכן $[G : C] = [G : G] = 1$.

שאלה 7. תהא G חבורה לא אבלית מסדר 8. הוכח שקיימת ב- G תת חבורה מסדר 4. (הדרכה: הראה שקיים בהכרח איבר מסדר 4 היוצר את תת החבורה המבוקשת).

פתרון.

ב- G בסה"כ 8 איברים. נראה שבהכרח קיים איבר מסדר 8. הסדרים האפשריים הם אלו המחלקים את 8, כלומר 1, 2, 4, 8. אין איבר מסדר 8 כי אם היה איבר כזה, הייתה זו חבורה ציקלית ולכן אבלית, בסתירה לנתון.

יש רק איבר אחד בכל חבורה מסדר 1. זהו איבר היחידה. כעת נניח שכל אברי G מלבד איבר היחידה הם מסדר 2. על פי טענת עזר שנוכיח בסוף הפתרון, הנחה זו גוררת בהכרח שהחבורה אבלית, שוב בסתירה לנתון. לכן בהכרח קיים איבר אחד לפחות מסדר 4 ב- G ותת החבורה הציקלית שאיבר זה יוצר היא מסדר 4. סיימנו. כעת נוכיח את טענת העזר.

כלומר נוכיח שאם בחבורה כלשהי כל האיברים (מלבד איבר היחידה), הם מסדר 2, אזי בהכרח החבורה אבלית.

לכל $x, y \in G$, מתקיים $x^2 = 1$ ו $y^2 = 1$, אבל גם המכפלה xy הינה איבר ב- G ואיבר זה אינו איבר היחידה (כי כל איבר בחבורה זו הופכי לעצמו), לכן מתקיים גם $(xy)^2 = 1$. ולכן

$1 = (xy)^2 = xyxy$ אבל גם: $1 = (x)^2(y)^2 = xxyy$. נשווה בין הביטויים ונקבל $xyxy = xxyy$ ואם נכפול את שני האגפים משמאל ב- x ומימין ב- y , נקבל $yx = xy$, כלומר החבורה אבלית.

שאלות רשות

הגדרה. תהינה $(G, *)$ ו- (H, \bullet) חבורות. נזכור ממתטיקה בדידה את המכפלה הקרטזית

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

נגדיר פעולה על $G \times H$ רכיב-רכיב,

$$(g_1, h_1) \odot (g_2, h_2) = (g_1 * g_2, h_1 \bullet h_2)$$

שיחד איתה הופכת את $G \times H$ לחבורה. מי הוא איבר היחידה?

שאלה 8. תהינה G, H חבורות. הוכיחו: $G \times H$ היא אבלית אם ורק אם G ו- H אבליות.

הוכחה. נוכיח כל גרירה בנפרד.

☞ נניח ש- $G \times H$ אבלית. צ"ל ש- G ו- H אבליות. נוכיח ש- G אבלית (ההוכחה עבור H באופן סימטרי).

יהיו $g_1, g_2 \in G$. רוצים להוכיח כי $g_1 g_2 = g_2 g_1$. נשים לב כי

$$(g_1 g_2, e_H) = (g_1, e_H) (g_2, e_H) = (g_2, e_H) (g_1, e_H) = (g_2 g_1, e_H)$$

כאשר במעבר השני השתמשנו בנתון ש- $G \times H$ אבלית. כיוון שקיבלנו שוויון של זוגות סדורים, הרכיב הראשון שווה - לכן $g_1 g_2 = g_2 g_1$, ובסך הכל G אבלית.

☞ נניח ש- G ו- H אבליות. צ"ל ש- $G \times H$ אבלית.

יהיו $(g_1, h_1), (g_2, h_2) \in G \times H$. לכן

$$(g_1, h_1) (g_2, h_2) = (g_1 g_2, h_1 h_2) = (g_2 g_1, h_2 h_1) = (g_2, h_2) (g_1, h_1)$$

☐ כאשר במעבר השני השתמשנו בנתון ש- G ו- H אבליות. לכן $G \times H$ אבלית.

הערה. את הכיוון ☞ היה אפשר להוכיח גם בדרך אחרת, עם הכלים של הומומורפיזמים (שלא למדנו באותו הזמן). יש לנו אפימורפיזם $\pi_1 : G \times H \rightarrow G$ המוגדר על ידי $\pi_1(g, h) = g$ (ודאו שזהו אפימורפיזם). אם $G \times H$ אבלית, גם $G = \text{Im} \pi_1$ אבלית (לפי שאלה מתרגיל 7). באופן דומה עבור H .

שאלה 9. תהינה G, H חבורות, ויהיו $g \in G, h \in H$ איברים מסדר סופי. נסתכל על האיבר $(g, h) \in G \times H$. הוכיחו: $o((g, h)) = [o(g), o(h)]$ (כלומר: הסדר של (g, h) הוא הכפולה המשותפת המינימלית של $o(g)$ ושל $o(h)$).

הוכחה. נסמן $m = o(g), n = o(h), k = [m, n]$. צריך להראות שני דברים:

א. $(g, h)^k = (e_G, e_H)$.

ב. אם $(g, h)^\ell = (e_G, e_H)$, אזי $k \leq \ell$ (אפשר גם להראות כי $k \mid \ell$, שזה לרוב יותר נוח).

אכן,

א. כיוון ש- $k = [m, n]$, אנחנו יודעים שמתקיים $k \mid m$ ו- $k \mid n$. כלומר $\frac{k}{m}, \frac{k}{n} \in \mathbb{Z}$. לכן

$$(g, h)^k = (g^k, h^k) = \left((g^m)^{\frac{k}{m}}, (h^n)^{\frac{k}{n}} \right) = (e_G, e_H)$$

ב. נניח כי $(g, h)^\ell = (e_G, e_H)$. לכן, בפרט $g^\ell = e_G, h^\ell = e_H$. לפי משפט מההרצאה, נובע כי $\ell \mid m = o(g)$ וגם $\ell \mid n = o(h)$. הוכחנו ש- $\ell \mid m$ וגם $\ell \mid n$, ולכן $\ell \mid [m, n] = k$. כדרוש.

□

שאלה 10. נסתכל על $G = U_{14} \times \mathbb{Z}_4$.

א. מהו הסדר של $(3, 2)$ ב- G ? נמקו.

ב. האם G אבלית? נמקו.

ג. האם G ציקלית? נמקו.

פתרון.

א. אפשר להתחיל לחשב (לא מומלץ), אבל אפשר להיעזר בשאלה 3. לפי השאלה הזו, מספיק לחשב את הסדר של 3 ב- U_{14} ואת הסדר של 2 ב- \mathbb{Z}_4 . על ידי חישוב ישיר, הסדר של 3 ב- U_{14} הוא 6, והסדר של 2 ב- \mathbb{Z}_4 הוא 2. לכן,

$$o((3, 2)) = [6, 2] = 6$$

ב. אנחנו יודעים ש- U_{14} ו- \mathbb{Z}_4 אבליות, ולכן גם $U_{14} \times \mathbb{Z}_4$ אבלית (לפי שאלה 2).

ג. נשים לב כי $|U_{14} \times \mathbb{Z}_4| = \varphi(14) \cdot 4 = 6 \cdot 4 = 24$. כלומר, כדי לבדוק אם $U_{14} \times \mathbb{Z}_4$ ציקלית, מספיק לבדוק אם יש בה איבר מסדר 24.

לפי שאלה 4, כדי שהסדר של (g, h) יהיה 24, צריך שיתקיים $[o(g), o(h)] = 24$. הסדרים של האיברים ב- \mathbb{Z}_4 הם 1, 2, 4, ואילו הסדרים של האיברים ב- U_{14} הם 1, 2, 3, 6 (על ידי בדיקה ישירה, או על ידי שימוש בלגראנז' שלמדנו יותר מאוחר). לכן, אין דרך שבה ה-lcm ייצא 24 - גם אם $o(g) = 6$ ו- $o(h) = 4$, יתקיים

$$o((g, h)) = [o(g), o(h)] = [6, 4] = 12$$

לכן זו לא חבורה ציקלית.

שאלה 11. תהינה G, H חבורות. האם כל תת-חבורה K של $G \times H$ היא בהכרח מהצורה $K_1 \times K_2$, כאשר K_1 תת-חבורה של G ו- K_2 תת-חבורה של H ? הוכיחו או תנו דוגמה נגדית.

פתרון. התשובה היא **לא!**

ניקח $G = H = \mathbb{Z}_2$ (אפשר לקחת כל חבורה לא טריוויאלית). כלומר $G \times H = \mathbb{Z}_2 \times \mathbb{Z}_2$. נסתכל על

$$K = \langle (1, 1) \rangle = \{(0, 0), (1, 1)\}$$

מהגדרת K (כתת-החבורה הנוצרת על ידי $(1, 1)$), $K \leq \mathbb{Z}_2 \times \mathbb{Z}_2$. אבל אי אפשר להציג את K כמכפלה של תתי-חבורות $K_1 \times K_2$ כנ"ל (כי אז $0, 1 \in K_1$ וגם $0, 1 \in K_2$, ומקבלים $K_1 \times K_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \neq K$).
 כעת נציג את **ההוכחה השגויה** הנפוצה. ההוכחה הולכת ככה:
 תהי $K \leq G \times H$ תת-חבורה. נגדיר

$$K_1 = \{g \in G \mid \exists h \in H : (g, h) \in K\}$$

$$K_2 = \{h \in H \mid \exists g \in G : (g, h) \in K\}$$

אז קל לבדוק ש- $K_1 \leq G$ ו- $K_2 \leq H$ (הקריטריון המקוצר, למשל). **ברור ש- $K = K_1 \times K_2$** , ולכן סיימנו.

הבעיה, כמו שניחשתם, היא בזה שמה שכתוב באדום לא ברור. למעשה, הוא לא נכון. בדוגמה הנגדית להלן, מקבלים ש- $K_1 = K_2 = \mathbb{Z}_2$, ואז $K_1 \times K_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \neq K$.

שאלה 12. כתבו תוכנה שמקבלת כקלט רשימת מספרים המייצגת תמורה, כלומר מקבלת את השורה השנייה בהצגת תמורה כמטריצה בגודל $2 \times n$. התוכנה תדפיס כפלט את התמורה כמכפלת מחזורים זרים. הרחיבו את התוכנה כך שתקבל כמה תמורות, ותדפיס את מכפלתן כמכפלת מחזורים זרים.