

פתרון תרגיל בית 6 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 ג' כסלו ה'תשע"ז, 2017.01.01.

שאלה 1. תהי D_4 החבורה הדיהדרלית מסדר 8. תארו את כל תת החבורות הלא טריוויאליות של D_4 . הוכיחו כי כולן אבליות. האם כולן ציקליות?
פתרון.

נציג את החבורה D_4 כחבורה הנוצרת על ידי האיברים $\langle \sigma, \tau \rangle$ כאשר מתקיימים היחסים $\sigma^4 = \tau^2 = e, \sigma\tau = \tau\sigma^3$.

האיברים ב D_4 (בסה"כ 8 איברים) הם: $\{e, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \sigma, \sigma^2, \sigma^3\}$. לפי משפט לגרנז' עבור $H \leq D_4$ מתקיים $|H| \mid |D_4|$, כלומר $|H| \in \{1, 2, 4, 8\}$. תת החבורות הטריוויאליות מתקבלות במקרים $|H| \in \{1, 8\}$.

אחרת, סדר תת החבורה הוא 2 או 4. נוח להתחיל עם תת החבורות הציקליות. כלומר לבדוק עבור כל אחד מאיברי D_4 , מהי תת החבורה הציקלית הנוצרת על ידו. נקבל:

תת החבורות הציקליות מסדר 2
 $\langle \tau \rangle = \{e, \tau\}, \langle \tau\sigma \rangle = \{e, \tau\sigma\}, \langle \tau\sigma^2 \rangle = \{e, \tau\sigma^2\}, \langle \tau\sigma^3 \rangle = \{e, \tau\sigma^3\}, \langle \sigma^2 \rangle = \{e, \sigma^2\}$

תת החבורות הציקליות מסדר 4
 $\langle \sigma \rangle = \langle \sigma^3 \rangle = \{e, \sigma, \sigma^2, \sigma^3\}$

כעת נבנה תת חבורות בעזרת שני יוצרים מסדר 2, לקבלת תת חבורות לא ציקליות מסדר 4. נקבל:

$\langle \tau, \sigma^2 \rangle = \{e, \tau, \sigma^2, \tau\sigma^2\}, \langle \tau\sigma, \sigma^2 \rangle = \{e, \tau\sigma, \sigma^2, \tau\sigma^3\}$
 עבור כל יתר הצירופים של שני יוצרים מסדר 2 נקבל את אחת משתי תת חבורות אלו או את כל החבורה D_4 .

כמוכן שלא כל תת החבורות ציקליות כפי שניתן לראות מתאור תת החבורות. יחד עם זאת כולן אבליות.

הסבר: כל תת החבורות הציקליות הן בהכרח אבליות. ולגבי תת החבורות שאינן ציקליות - כל איבריהן מסדר 2 והוכחנו שחבורה שכל איבריה מסדר 2 היא בהכרח אבלית.

שאלה 2. זכרו שהמרכז של חבורה G הוא הקבוצה

$$Z(G) = \{g \in G : \forall h \in G, gh = hg\}$$

דהיינו אוסף כל איברי G שמתחלפים עם כל איברי G .

1. מצאו את $Z(D_3 \times \mathbb{Z}_4)$.

2. הוכיחו $Z(D_{2n+1}) = \{e\}$ וכי $Z(D_{2n}) = \langle \sigma^n \rangle$ עבור $n > 1$. רמז: איך נראה איבר כללי בחבורה הדיהדרלית?

פתרון.

1. לגבי $Z(D_3 \times \mathbb{Z}_4)$, נבחן את חבורת המכפלה $D_3 \times \mathbb{Z}_4$. החבורה \mathbb{Z}_4 אבליית ולכן כל איבריה במרכז. לעומת זאת $Z(D_3) = e$. קל לוודא שאיבר של חבורת המכפלה נמצא במרכז אם כל אחד מהאיברים במכפלה נמצא במרכז של החבורה אליה הוא משתייך. לכן נקבל: $Z(D_3 \times \mathbb{Z}_4) = \{(e, 0), (e, 1), (e, 2), (e, 3)\}$.

2. נוכיח את שני המקרים יחד. נסמן את החבורה הדיהדרלית ע"י D_{2n} , ונראה שעבור n זוגי $Z(D_{2n}) = \langle \sigma^n \rangle$, ועבור n אי זוגי $Z(D_{2n+1}) = \{e\}$. איבר כללי בחבורה הדיהדרלית הינו מהצורה: $\tau^i \sigma^j : i \in \{0, 1\}, j \in \{0, 1, \dots, n-1\}$. מתקיימים היחסים: $\sigma \tau = \tau \sigma^{-1}$. אם נכפול ב σ משמאל את שני האגפים, נקבל: $\sigma^2 \tau = \sigma \tau \sigma^{-1} = \tau \sigma^{-2}$. באופן כללי נכתוב:

$$\sigma^r \tau = \tau \sigma^{-r} \quad (1)$$

כעת, מכיוון ש σ ו τ יוצרים יחד את D_{2n} , איבר כלשהו בחבורה זו מוכל במרכז אא"ם האיבר מתחלף אם כל אחד מהיוצרים. כלומר: $x \in Z(D_{2n}) \iff x = \tau^i \sigma^j$ אא"ם $x \tau = \tau x$ וגם $x \sigma = \sigma x$. מהתנאי $x \sigma = \sigma x$ נקבל $\sigma \tau^i \sigma^j = \tau^i \sigma^{j+1}$. ותנאי זה שקול ל:

$$\tau^i \sigma = \sigma \tau^i \quad (2)$$

ניתן לראות שתנאי זה מתקיים עבור $i = 0$, אך האם תנאי זה מתקיים עבור $i = 1$? התשובה היא לא מכיוון שאם $i = 1$ אזי נקבל מנוסחה (2) ש: $\tau \sigma = \sigma \tau$, ועל פי נוסחה (1) מתקיים: $\sigma \tau = \tau \sigma^{-1}$. אבל אז נקבל: $\sigma^2 = 1$, בסתירה לסדר של σ . לכן בהכרח $i = 0$ ו $x = \sigma^j$. נעבור לתנאי השני לפיו $x \tau = \tau x$. נציב את x ונקבל: $\sigma^j \tau = \tau \sigma^j$. וכן מתקיים:

$$\sigma^{2j} = 1 \quad (3)$$

לכן, מכיוון ש $o(\sigma) = n$, נקבל מנוסחה (3) ש: $n | 2j$. לכן מתקיים אחד מהשניים: $j = 0$ או $2j = n$ מכיוון ש: $0 \leq j \leq n-1$. אם $j = 0$ אז: $x = \sigma^j = 1$ ואם $2j = n$, אז n בהכרח זוגי ו $\sigma^{\frac{n}{2}} = \sigma^j = x$. לכן לסיכום $Z(D_{2n}) = \langle \sigma^n \rangle$ ו $Z(D_{2n+1}) = \{e\}$.

שאלה 3. חשבו בשיטה של חישוב חזקה בעזרת ריבועים את הביטויים הבאים. מותר להשתמש במחשבון (כולל בפונקציית המודולו) לחישובי הביניים, שאותם תפרטו:

א. $2790^{2753} \in \mathbb{Z}_{3233}$. רמז: בתרגול ראיתם שהתוצאה הסופית היא ההודעה שבוב רצה לשלוח לאליס.

ב. $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{12} \in GL_2(\mathbb{Z}_{10000})$.

פתרון. א. נחשב ש- $101011000001_2 = 2753$. לכן נשתמש באותו תהליך שראינו בכיתה,

כשכל המשוואות הן מודולו 3233:

$$\begin{aligned}
 2790^1 &= 2790 \\
 2790^2 &= 2269 \\
 2790^4 &= 1425 \\
 2790^5 &= 2393 \\
 2790^{10} &= 806 \\
 2790^{20} &= 3036 \\
 2790^{21} &= 3213 \\
 2790^{42} &= 400 \\
 2790^{43} &= 615 \\
 2790^{86} &= 3197 \\
 2790^{172} &= 1296 \\
 2790^{344} &= 1689 \\
 2790^{688} &= 1215 \\
 2790^{1376} &= 1977 \\
 2790^{2752} &= 3065 \\
 2790^{2753} &= 65
 \end{aligned}$$

וזה פענוח ההודעה $m = 65$ שבו שלח לאליס.

ב. נסמן $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. נחשב ש- $12 = 1100_2$, ולכן עלינו לחשב למעשה את

$$A^{12} = \left((A^2)^2 \cdot \left(\left((A^2)^2 \right)^2 \right)^2 \right)$$

ובחישוב מלא, כשכל המשוואות הן מודולו 10000:

$$\begin{aligned}
 \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^1 &= \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \\
 \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^2 &= \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix} \\
 \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^4 &= \begin{pmatrix} 199 & 290 \\ 435 & 634 \end{pmatrix} \\
 \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^8 &= \begin{pmatrix} 5751 & 1570 \\ 2355 & 8106 \end{pmatrix} \\
 \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{12} &= \begin{pmatrix} 7339 & 3170 \\ 4755 & 2154 \end{pmatrix}
 \end{aligned}$$

שאלה 4. עבור כל אחת מן ההעקות הבאות קבעו והוכיחו האם היא הומומורפיזם, מונומורפיזם, אפימורפיזם או איזומורפיזם.

א. $f : \mathbb{C}^* \rightarrow \mathbb{C}^*$ המוגדרת לפי $f(x) = x^{-3}$.

ב. $f : S_7 \rightarrow \mathbb{Z}$ המוגדרת לפי $f(\sigma) = \sigma(1)$.

ג. $f_x : G \rightarrow G$ המוגדרת לפי $f_x(g) = xgx^{-1}$ כאשר G חבורה ו- $x \in G$ איבר.

ד. $f : \mathbb{Z} \rightarrow \mathbb{Z}_n \times \mathbb{Z}_n$ המוגדרת לפי $f(k) = ([k], [k])$.

פתרון. א. הפונקציה היא אפימורפיזם, אבל לא מונומורפיזם. למשל $f(1) = f(e^{\frac{2\pi i}{3}}) =$

1.

ב. הפונקציה הזו היא לא הומומורפיזם. למשל

$$f(\text{id} \cdot \text{id}) = 1 \neq 1 + 1 = f(\text{id}) + f(\text{id})$$

ג. הפונקציה הזו היא איזומורפיזם. סוג כזה של איזומורפיזם נקרא אוטומורפיזם פנימי. נראה שאכן מדובר בהומומורפיזם:

$$f_x(gh) = xghx^{-1} = xgx^{-1}xhx^{-1} = f_x(g)f_x(h)$$

כדי לראות ש- f_x הוא חח"ע נשים לב שאם $xgx^{-1} = e$, אז $g = x^{-1}ex$ ולכן $g = e$. כדי להראות ש- f_x הוא על, יהי $h \in G$. נבחר בתור המקור שלו את $x^{-1}hx$, ואכן $f_x(x^{-1}hx) = h$.

ד. פונקציה זו היא אכן הומומורפיזם. עם זאת, היא לא אפימורפיזם (אלא אם $n = 1$ ואז זה דבילי. לזוג $([0], [1])$ למשל אין מקור) ולא מונומורפיזם (למשל $f(k) = f(k + n)$).

שאלה 5. יהי $f : G \rightarrow H$ הומומורפיזם.

א. הוכיחו שאם G אבלית, אז $\text{im } f$ תת-חבורה אבלית.

ב. הסיקו מהסעיף הקודם שאם $G \cong H$, אז G אבלית אם ורק אם H אבלית.

ג. הוכיחו או הפריכו: קיים מונומורפיזם $\varphi : U_{37} \rightarrow D_{18}$.

פתרון. א. אנחנו יודעים כי $\text{im } f \leq H$. נותר להראות שהיא אבלית. יהיו $h_1, h_2 \in \text{im } f$ אז ישנם איברים g_1, g_2 כך שמתקיים $f(g_1) = h_1, f(g_2) = h_2$. מפני שנתון ש- G אבלית יתקיים גם

$$h_1h_2 = f(g_1)f(g_2) = f(g_1g_2) = f(g_2g_1) = f(g_2)f(g_1) = h_2h_1$$

ולכן כל זוג איברים ב- $\text{im } f$ מתחלף.

ב. אם חבורות הן איזומורפיות, אז יש ביניהן איזומורפיזם. נניח $\phi : G \rightarrow H$ הוא איזומורפיזם. לכן ϕ הוא על, כלומר $\text{im } \phi = H$. אם G היא אבלית, אז גם H היא אבלית לפי הסעיף הקודם. באופן דומה יש איזומורפיזם $\phi^{-1} : H \rightarrow G$ ולכן אם H אבלית, אז גם G אבלית.

ג. שתי החבורות הן מסדר 36. לכן אם קיימת פונקציה על בינהן, אז היא גם חח"ע. כלומר אילו קיים φ אפימורפיזם כזה, אז זה איזומורפיזם. אבל D_{18} לא אבלית ואילו U_{37} היא אבלית ולפי הסעיף הקודם נגיע לסתירה.

שאלה 6. תהיינה G, H חבורות ויהי $f : G \rightarrow H$ הומומורפיזם. הוכיחו: f חח"ע אם ורק אם $\ker f = \{e_G\}$.

פתרון. לכיוון הראשון, נניח שההומומורפיזם f חח"ע. f הומומורפיזם ולכן $f(e_G) = e_H$.
 f חח"ע ולכן e_G היחיד שהולך לאיבר e_H , ולכן $\ker f = \{e_G\}$.
 לכיוון השני, נניח שמתקיים: $\ker f = \{e_G\}$. נניח שעבור g_1, g_2 מתקיים $f(g_1) = f(g_2)$, ונרצה להראות שגם $g_1 = g_2$. אם כן, $f(g_1) f(g_2)^{-1} = e_H$ ומכיוון שזהו הומומורפיזם מתקיים: $f(g_1 g_2^{-1}) = e_H$. לכן $g_1 g_2^{-1} \in \ker f$ ומהנתון נקבל: $g_1 g_2^{-1} = e_G$, ולכן $g_1 = g_2$. לכן f אכן חח"ע.

שאלה 7. תהי G חבורה. נגדיר $f : G \rightarrow G$ ע"י: $f(g) = g^2$.

1. הוכיחו שהפונקציה f היא הומומורפיזם אם ורק אם G אבליה.
2. נניח שהחבורה G אבליה וסופית. הוכיחו שהפונקציה f היא איזומורפיזם אם ורק אם הסדר של G הוא אי-זוגי.

פתרון. ב. לכיוון הראשון, נניח שהחבורה אבליה. יהיו $g, h \in G$. כעת: $f(gh) = (gh)^2 = ghgh = g^2 h^2 = f(g) f(h)$.
 נניח ש: f הומומורפיזם. יהיו $g, h \in G$. כעת: $f(gh) = (gh)^2 = ghgh$. כלומר $f(gh) = f(g) f(h) = g^2 h^2$. נצמצם ונקבל: $gh = hg$ כלומר G אבליה.

ב. לכיוון הראשון, נניח שהחבורה מסדר אי-זוגי. מכיוון שהפונקציה היא הומומורפיזם (לפי הסעיף הראשון) והחבורה סופית, מספיק להראות שהפונקציה חח"ע. לשם כך יש להסביר מדוע הגרעין הוא טריוויאלי. נניח בשלילה שקיים $g \in \ker f$ המקיים $g \neq e_G$. מהגדרת הפונקציה, $e_G = f(g) = g^2$, ולכן הסדר של g הוא 2. הסדר של g מחלק את הסדר של החבורה ולכן הסדר של החבורה הוא זוגי וסתירה.

לכיוון השני, נניח שהפונקציה היא איזומורפיזם. נניח בשלילה שהסדר של החבורה הוא זוגי, לכן יש איבר מסדר 2 (ראינו בתרגול) ולכן f לא חח"ע (האיבר הזה ואיבר היחידה שניהם בגרעין) וסתירה.

שאלות רשות

שאלה 8. חשבו האם ניתן לממש את אלגוריתם RSA באמצעות חבורה לא אבליה (כמו S_n , למשל)? מה משתבש?

שאלה 9. הראו שכאשר $n = pq$ והראשוניים p, q "קרובים יחסית", אפשר לתקוף די בקלות את RSA .

שימו לב שמתקיים: $n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$, ואז $\frac{p+q}{2}$ יחסית קרוב למספר \sqrt{n} . סמנו: $t = \frac{p+q}{2}$, $s = \frac{p-q}{2}$ והסבירו למה במצב כזה יחסית קל למצוא את t, s (ובאמצעותם את p, q בהינתן n).
 הדגימו זאת על $n = 23360947609$.