

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?

שאלה 2. זכרו שהמֶרְכֶז 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?

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

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 $x \in G$ חבורה ו- x איבר.

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

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 $\varphi : U_{37} \rightarrow D_{18}$.

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

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 אבלית.

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

שאלות רשות

שאלה 8. חשבו האם ניתן לממש את אלגוריתם RSA באמצעות חבורה לא אבלית (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 $n = 23360947609$.