89-214 מבנים אלגבריים – מבחן לדוגמא 3

משך המבחן – שלוש שעות. השימוש במחשבון מותר. מרצה – דר' ארז שיינר

כל שאלה שווה 28 נקודות, כל ציון מעל 100 יעוגל ל100.

1. תהי $G \subseteq \mathbb{R}^{2\times 2}$ חבורת המטריצות ההפיכות בגודל 2×2, עם פעולת כפל מטריצות, ותהי $f: G \to G$ פונקציה.

א. הוכיחו/הפריכו: הפונקציה $f(A) = A^t$ היא הומומורפיזם.

הומומורפיזם צריך לקיים $f(AB) = f(A)f(B)$ לכל שתי מטריצות, כלומר $(AB)^t = A^t B^t$.

אבל שחלוף לא עובד ככה, וכל שנותר לנו הוא למצוא דוגמא נגדית.

נבחר $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, שתי מטריצות הפיכות.

$$f(AB) = f\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$f(A)f(B) = f\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} f\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq f(AB)$$

ב. הוכיחו/הפריכו: הפונקציה $f(A) = \left(A^t\right)^{-1}$ היא הומומורפיזם.

(הסימון A^t הוא שחלוף המטריצה.)

תהיינה שתי מטריצות הפיכות $A, B \in G$.

אזי $f(A)f(B) = \left(A^t\right)^{-1}\left(B^t\right)^{-1} = \left(B^t A^t\right)^{-1} = \left((AB)^t\right)^{-1} = f(AB)$ ואכן הוכחנו כי f היא הומומורפיזם.

שימו לב- ניתן למעשה להוכיח כי מדובר באיזומורפיזם – עשו זאת כתרגיל.

.2

א. מצאו תת חבורה של חבורת תמורות המכילה בדיוק 5 איברים.

נמצא את תת חבורת התמורות של S_5 שאיזומורפית ל $\mathbb{Z}_5$ לפי משפט קיילי. כיוון שב $\mathbb{Z}_5$ יש בדיוק 5 איברים, זה יענה על השאלה.

נזכור כי משפט קיילי מראה שכל חבורה איזומורפית לתת חבורה של חבורת תמורות, ע"י כך שהפעלת הפעולה של איבר מהחבורה על שאר האיברים בעצם מהווה תמורה של איברי החבורה.

למשל, עבור $2\in\mathbb{Z}_5$ מתקיים כי: $1+2=0, 2+2=3, 3+2=4, 4+2=1, 0+2=2$ ולכן האיבר 2 מתאים לתמורה $\begin{pmatrix}0&1&2&3&4\\2&3&4&0&1\end{pmatrix}$.

באופן דומה נשלח כל איבר ב $\mathbb{Z}_5$ לתמורה המתאימה ונקבל ש $\mathbb{Z}_5$ איזומורפית לתת החבורה הבאה:

$$\left\{\begin{pmatrix}0&1&2&3&4\\0&1&2&3&4\end{pmatrix},\begin{pmatrix}0&1&2&3&4\\1&2&3&4&0\end{pmatrix},\begin{pmatrix}0&1&2&3&4\\2&3&4&0&1\end{pmatrix},\begin{pmatrix}0&1&2&3&4\\3&1&4&2&0\end{pmatrix},\begin{pmatrix}0&1&2&3&4\\4&3&2&1&0\end{pmatrix}\right\}$$

ב. תהי $H\subseteq S_3$ תת חבורה. הוכיחו/הפריכו: לכל שתי תמורות $f,g\in S_3$ אם $f\circ g\in H$ אזי גם $g\circ f\in H$.

נביט בתת החבורה הציקלית הנוצרת ע"י החילוף $(1\ \ 2)$,

$H=\langle(1\ \ 2)\rangle=\{(1),(1\ \ 2)\}$.

מתקיים כי $(1\ \ 3)(1\ \ 2\ \ 3)=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(1\ \ 2)\in H$

אבל $(1\ \ 2\ \ 3)(1\ \ 3)=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(2\ \ 3)\notin H$

3. אליס ובוב מעוניינים לתאם מפתח משותף באמצעות אלגוריתם דיפי-הלמן.

הם הסכימו על הראשוני הבטוח $p=107=2\cdot 53+1$, ובחרו $g=3$.

א. האם g יוצר של החבורה U_{107} ?

גודל החבורה U_{107} הוא 106. הסדר של כל איבר חייב לחלק את גודל החבורה, ולכן הסדר של g הוא אחד מבין המספרים $2,53,106$ (את 1 פסלנו כיוון ש $g\neq 1$).

g יהיה יוצר של החבורה אם ורק אם הסדר שלו הוא 106 וכך תת החבורה הציקלית שהוא יוצר שווה לחבורה כולה.

נבדוק: $g^2=9\neq 1$, $g^{53}=3^{53}\bmod 107=1$. לכן הסדר של g הוא 53 והוא <u>אינו יוצר</u> של החבורה.

שימו לב: $53=32+16+4+1$ וכך חישבנו את החזקה 3^{53} .

ב. אליס שלחה לבוב את המידע $81=3^a\bmod 107$ ובוב שלח לאליס את המידע $56=3^b\bmod 107$. מצאו את הסוד המשותף של אליס ובוב.

מדוע יכולתם לעשות זאת? הוכיחו.

נשים לב כי $81=3^4$. אמנם <u>לא ניתן להסיק</u> כי $a=4$ אך זה מספיק לנו על מנת לשבור את ההצפנה.

שימו לב כי החולשה היא שאליס בחרה a עבורו 3^a הוא חזקה שלימה של 3 שקטנה יותר מ 107 ובכך הופכת את הלוגריתם הדיסקרטי (קשה לפתור) ללוגריתם רגיל (פתיר בקלות).

ידוע לנו כי אליס שלחה לבוב את $3^a=3^4\bmod 107$. בוב יעלה אותו בחזקת b ויקבל את $3^{ab}=3^{4b}\bmod 107$.

אבל אנחנו יכולים לחשב את $3^{4b}=\left(3^b\right)^4=56^4\bmod 107=19$, וזה הסוד המשותף.

(שימו לב: אנחנו לא יודעים מהם a,b וזה לא משנה. למשל ייתכן כי $a=57,b=37$, בדקו שאכן המפתח המשותף במקרה זה הוא 19.)

4. נתון הפולינום $g(x)=x^n+1$ בעזרתו ניצור קידוד פולינומי.

א. קודדו את וקטור המידע $f(x)$, כאשר נתון כי $\deg\left(f(x)\right)<n$.

כיוון ש $\deg\left(f(x)\right)<n=\deg\left(g(x)\right)$ נובע שהחלוקה עם שארית היא $f(x)=0\cdot g(x)+f(x)$ ולכן המידע המקודד הוא $f(x)\cdot x^n+f(x)=f(x)\left(x^n+1\right)=f(x)g(x)$.

שימו לב – אין חובה בפירוט לעיל, יכלנו לעצור את התשובה בשלב הראשון.

(האם תמיד כאשר $\deg(f)<\deg(g)$ מתקיים כי המידע המקודד הינו $f(x)g(x)$?)

ב. קודדו את וקטור המידע $f(x)=x^n$.

נבצע חלוקה עם שארית: $x^n=x^n+1+1$, ולכן המידע המקודד הינו $f(x)\cdot x^n+1=x^{2n}+1$.