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.

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

   (הסימון A^t הוא שחלוף המטריצה.)

2.

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

   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 $g \circ f \in H$.

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}?

   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.

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

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

   ב. קודדו את וקטור המידע $f(x) = x^n$.