

89-214 מבנים אלגבריים – מועד א' – 05/01/23

משך המבחן – שלוש שעות. חומר עזר אסור - השימוש במחשבון מותר. מרצה – דר' ארז שיינר

מתרגלים: מר תומר באואר ומר דניאל עומר כל שאלה שווה 28 נקודות. כל ציון מעל 100 יעוגל ל-100.

1. תהי חבורה G ותהי תת חבורה $H < G$.

(אין קשר בין הסעיפים.)

א. נניח כי לכל $a \in G$ קיים $b \in aH$ עבורו $bH = Hb$. הוכיחו או הפריכו: H תת חבורה נורמלית של G .

ב. נניח H אבלית. הוכיחו או הפריכו: H תת חבורה נורמלית של G .

ג. נניח H תת חבורה נורמלית של G . הוכיחו או הפריכו: קיים הומומורפיזם $f: G \rightarrow G/H$ כך ש $\ker(f) = H$.

2. נביט בחבורת התמורות S_n ובחבורה $\mathbb{Z}_n$ עם חיבור מודולו n .

א. מצאו תת חבורה של S_6 האיזומורפית לחבורה $\mathbb{Z}_2 \times \mathbb{Z}_3$, באמצעות משפט קיילי.

ב. האם קיימת תת חבורה של S_3 האיזומורפית לחבורה $\mathbb{Z}_2 \times \mathbb{Z}_3$? הוכיחו תשובתכם.

ג. האם קיימת תת חבורה של $\mathbb{Z}_2 \times \mathbb{Z}_3$ האיזומורפית ל S_2 ? הוכיחו תשובתכם.

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

אליס בחרה בשני המספרים הראשוניים $p = 1741$ ו $q = 1609$.

אליס פרסמה את $n = pq$ ואת $e = 1117$.

א. חשבו את $d = e^{-1} \in U_m$.

ב. בוב רצה לשלוח לאליס את המידע $x = 2$. חשבו את המספר המוצפן שהוא העביר לאליס.

4. נביט בקוד הפולינומי הנוצר על ידי הפולינום $g(x) = x^4 + x + 1$

א. קודדו את המידע 10000.

ב. האם מדובר בקוד ציקלי, בהנחה שאורך המידע הוא 5? הוכיחו תשובתכם.

ג. האם מדובר בקוד ציקלי, בהנחה שאורך המידע הוא 11? הוכיחו תשובתכם.