תרגיל בית 9 במבנים אלגבריים
89-214 סמסטר א' תשע"ט

שאלה 1 (חימום)**.** מצאו את כל המחלקות השמאליות ב-$\mathbb{Z}_{30}/\langle 3\rangle$.

שאלה 2 (חימום)**.** מצאו את הסימן של התמורה

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & 2n-1 & 2n \\ 2 & 3 & 4 & \cdots & 2n & 1 \end{pmatrix} \in S_{2n}$$

שאלה 3. יהיו שני ראשוניים $p = 137, q = 269$. הריצו שליחת הודעה שבחרתם עם אלגוריתם RSA כפי שראינו בכיתה עם $n = pq$. דאגו גם להצפין וגם לפענח את ההודעה.

שאלה 4 (חזרה על בדידה)**.** תהי G חבורה ויהיו $A, B \subseteq G$ תת־קבוצות שלה. לכל סעיף כתבו פסוק לוגי שקול אך ורק עם כמתים (כמו $\forall$ ו-$\exists$) ושיוויונות מן הצורה $xy = zw$ עבור איברים של הקבוצות.

א. $ab = ba$ לכל איבר a של A ואיבר b של B.

ב. $aB = Ba$ לכל איבר a של A.

ג. $AB = BA$ (ההגדרה של הקבוצות האלו היא מכפלה איבר־איבר).

נסו למצוא דוגמאות שמראות שיש הבדל בין הסעיפים השונים ומי גורר את מי.

שאלה 5. מצאו את הסדרים של כל האיברים ב-A_4.

שאלה 6. הפריכו את הטענות השגויות הבאות:

א. כל תת־חבורה נורמלית היא אבלית.

ב. כל תת־חבורה אבלית היא נורמלית.

ג. התמונה של כל הומומורפיזם $f : G \to H$ היא תת־חבורה נורמלית של H.

ד. אם חבורת המנה G/N סופית ולא טריוויאלית, אז G סופית.

ה. אם חבורת המנה G/N ציקלית ולא טריוויאלית, אז G אבלית.

שאלה 7. נתבונן בחבורה $G = \mathbb{Q}/\mathbb{Z}$.

א. הוכיחו שהסדר של כל איבר ב-G הוא סופי, אבל שישנם איברים בחבורה מסדר גדול כרצוננו.

ב. תהי H תת־החבורה הקטנה ביותר של G שמכילה את $\frac{2}{5} + \mathbb{Z}, \frac{3}{14} + \mathbb{Z}$ (מסמנים זאת $H = \left\langle \frac{2}{5} + \mathbb{Z}, \frac{3}{14} + \mathbb{Z} \right\rangle$ ואומרים כי H היא תת־החבורה שנוצרת על ידי האיברים האלו). הוכיחו כי H היא ציקלית ומצאו את האינדקס $[G : H]$.
רמז: למעשה רוצים למצוא $\frac{a}{b} \in \mathbb{Q}$ כך ש-$H = \left\langle \frac{a}{b} + \mathbb{Z} \right\rangle$, ולוודא הכלה דו־כיוונית.

בהצלחה!