

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

שאלה 1 (חימום). מצאו את כל המחלקות השמאליות ב- $\mathbb{Z}_{30}/\langle 3 \rangle$. פתרון. האיבר 3 הוא מסדר 10, ולכן $|\langle 3 \rangle| = 10$. לפי משפט לגראנז' נקבל

$$|\mathbb{Z}_{30}/\langle 3 \rangle| = \frac{|\mathbb{Z}_{30}|}{|\langle 3 \rangle|} = \frac{30}{10} = 3$$

והמחלקות, עד כדי בחירת נציגים, הן $\{\langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle\}$.

שאלה 2 (חימום). מצאו את הסימן של התמורה

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

פתרון. בכתוב של מכפלת מחזורים זרים, התמורה היא המחזור $(1, 2, 3, \dots, 2n)$, והוא מאורך זוגי. לכן הסימן הוא -1 והתמורה אי-זוגית.

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.

פתרון. נחשב $n = 36853$ ואת $\varphi(n) = (p-1)(q-1) = 36448$. נבחר מעריך הצפנה $e = 5$, שזר ל- $\varphi(n)$. נחשב את ההופכי של e בחבורה $U_{\varphi(n)}$ לפי אלגוריתם אוקלידס המורחב (שאתם צריכים להכיר),

$$d \equiv e^{-1} \equiv 21869 \pmod{\varphi(n)}$$

ולכן המפתח הציבורי שלנו הוא הזוג הסדור $(36853, 5)$ והמפתח הפרטי הוא 21869. נניח ורוצים לשלוח לנו את ההודעה $a = 1000$. אז יצפינו את ההודעה בעזרת המפתח הציבורי כמו שראינו בכיתה:

$$c = a^e \equiv 1000^5 \equiv 3795 \pmod{36853}$$

כאשר החישוב נעשה לפי הדרך שראינו לחישוב חזקות מודולריות. לפענוח ההודעה המוצפנת c נעזר במפתח הפרטי שלנו

$$c^d \equiv 3795^{21869} \equiv 1000 \pmod{36853}$$

כפי שציפינו.

שאלה 4 (חזרה על בדידה). תהי G חבורה והיו $A, B \subseteq G$ 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. פתרון. כל סעיף גורר את אלו שתחתיו.

א. $\forall a \in A \forall b \in B : ab = ba$.

ב. $\forall a \in A \forall b \in B \exists b' \in B : ab = b'a$.

ג. $\forall a \in A \forall b \in B \exists b' \in B \exists a' \in A : ab = b'a'$.

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

פתרון. האיברים ב- A_4 הם התמורות הזוגיות ב- S_4 . הסדר של איבר נקבע לפי מבנה המחזורים שלו, ולכן קל למצוא את הסדרים: מסדר 1 יש רק את איבר היחידה id . מסדר 2 יש את האיברים שהם מכפלה של שני חילופים זרים, כלומר מהצורה $(ij)(kl)$ עבור i, j, k, l שונים. מסדר 3 יש את המחזורים מאורך 3, כלומר תמורות מהצורה (ijk) . זה מכסה לנו את כל איברי 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 $f: G \rightarrow H$ 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.

פתרון.

א. למשל $SL_2(\mathbb{R})$ אינה אבלית, אבל היא נורמלית ב- $GL_2(\mathbb{R})$.

ב. למשל $\langle (1\ 2) \rangle$ היא תת-חבורה אבלית של S_3 שאינה נורמלית.

ג. למשל בכל שיכון $f: \langle (1\ 2) \rangle \rightarrow S_3$ התמונה היא לא תת-חבורה נורמלית.

ד. נבחר $G = \mathbb{Z}$ ואת $N = 2\mathbb{Z}$. אז $G/N \cong \mathbb{Z}_2$ מסדר 2, אבל G אינסופית.

ה. נבחר $G = S_3$ ואת $N = A_3$ שראינו בכיתה שהיא נורמלית ב- S_3 . החבורה G/N מסדר 2 (שהוא ראשוני) ולכן ציקלית. אבל G אינה 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-חבורה הקטנה ביותר של G שמכילה את $\mathbb{Z} + \frac{3}{14}$ ו- $\mathbb{Z} + \frac{2}{5}$ (מסמנים זאת האלו). הוכיחו כי H הוא ציקלית ומצאו את האינדקס $[G : H]$. רמז: למעשה רוצים למצוא $\frac{a}{b} \in \mathbb{Q}$ כך ש- $H = \langle \frac{a}{b} + \mathbb{Z} \rangle$, ולוודא הכלה דו-כיוונית.

פתרון.

א. איבר היחידה בחבורה G הוא המחלקה $0 + \mathbb{Z} = \mathbb{Z}$. לכן יש למצוא לכל $x \in G$ מספר טבעי $n \in \mathbb{N}$ כך שנקבל $n \cdot x + \mathbb{Z} = \mathbb{Z}$. שימו לב כי החבורה חיבורית ולכן למציאת הסדר "העלאה בחזקה" היא כפל ב- n .
כל איבר בחבורה אפשר לרשום בצורה $x = \frac{a}{b} + \mathbb{Z}$ עבור $a \in \mathbb{Z}, b \in \mathbb{N}$. נשים לב כי $b \cdot (\frac{a}{b} + \mathbb{Z}) = a + \mathbb{Z} = \mathbb{Z}$. לכן x הוא לכל היותר מסדר מסופי (b נניח כי $\frac{a}{b}$ הוא שבר מצומצם, ולכן הסדר של x במקרה זה הוא בדיוק b). מכאן ברור שבקבוצת האיברים $\{\frac{1}{n} + \mathbb{Z}\}_{n \in \mathbb{N}}$ יש איברים מסדר גדול כרצוננו.

ב. יש להוכיח שקיים $\frac{a}{b} \in \mathbb{Q}$ כך שמתקיים $H = \langle \frac{a}{b} + \mathbb{Z} \rangle$. נראה שאפשר לבחור את $\frac{a}{b} = \frac{1}{70}$. בשביל להראות הכלה דו-כיוונית, מספיק להראות הכלה של היוצרים. נשים לב כי $\frac{1}{70} = 7 \cdot \frac{2}{5} - 13 \cdot \frac{3}{14}$, ולכן $\langle \frac{1}{70} + \mathbb{Z} \rangle \subseteq H$. מצד שני $\frac{2}{5} = 28 \cdot \frac{1}{70}$, $\frac{3}{14} = 15 \cdot \frac{1}{70}$, ולכן $H = \langle \frac{1}{70} + \mathbb{Z} \rangle$.
סדר תת-החבורה H הוא 70 ואילו G היא אינסופית, ולכן האינדקס שלה היא אינסופי לפי משפט לגראנז'. בנוגע לאינדקס, אפשר להראות גם שלכל שני מספרים ראשוניים $p_1 \neq p_2$ שונים שאינם מחלקים את 70 יתקיים כי $p_1 + H \neq p_2 + H$ ולכן ישנן אינסוף מחלקות שמאליות שונות.

בהצלחה!