פתרון תרגיל בית 5 במבנים אלגבריים
89-214 סמסטר א' תשע"ו

הוראות בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך הגשת התרגיל הוא לתרגול בשבוע המתחיל בתאריך יז' כסלו ה'תשע"ו, 29.11.2015.

שאלה 1. בכל סעיף נתונה חבורה G ותת-חבורה $H \leq G$. כתבו את כל המחלקות השמאליות של H ב-G:

א. $G = (U_{10}, \cdot)$, $H = \langle 9 \rangle$.

ב. $G = (\mathbb{Z}_{12}, +)$, $H = 3\mathbb{Z}_{12}$.

ג. G חבורה כלשהי, $H = \{e\}$.

פתרון.

א. מכיוון ש $G = (U_{10}, \cdot) = \{1, 3, 7, 9\}$ ו $H = \langle 9 \rangle = \{9, 1\}$ נצפה לקבל על פי משפט לגרנז' בדיוק שתי מחלקות שמאליות. אכן מתקיים:

$$1 \cdot H = H$$

$$3 \cdot H = \{7, 3\}$$

$$7 \cdot H = \{3, 7\}$$

$$9 \cdot H = H$$

בסה"כ:

$$G/H = \{H, 3H\}$$

ב. נשים לב ש: $H = 3\mathbb{Z}_{12} = \{0, 3, 6, 9\}$ לכן, עפ"י לגרנז' נצפה לקבל בסה"כ 3 מחלקות שמאליות של H ב G. חישוב פשוט מראה ש:

$$0 + H = 3 + H = 6 + H = 9 + H = H = \{0, 3, 6, 9\}$$

$$1 + H = 4 + H = 7 + H = 10 + H = \{1, 4, 7, 10\}$$

$$2 + H = 5 + H = 8 + H = 11 + H = \{2, 5, 8, 11\}$$

בסה"כ:

$$G/H = \{H, 1 + H, 2 + H\}$$

ג. מכיוון שתת החבורה H הינה החבורה הטריוויאלית (הכוללת רק איבר אחד - האיבר הניטרלי), המחלקות השמאליות הם פשוט איברי G ובסה"כ נקבל מספר מחלקות כמספר האיברים ב G.

שאלה 2. נסתכל על $G = (GL_2(\mathbb{Z}_2), \cdot)$ – חבורת המטריצות ההפיכות מגודל 2×2 מעל $\mathbb{Z}_2$ (שדה בין שני איברים),

א. רשום את כל איברי הקבוצה G (הזכר בהבדל בין $GL_2(\mathbb{Z}_2)$ ל: $M_2(\mathbb{Z}_2)$ בעת הכנת רשימת האיברים) .

ב. תהי תת חבורה של G: $A=<\begin{pmatrix}0&1\\1&0\end{pmatrix}>$. מהו האינדקס של A ב G?

ג. תהי תת חבורה של G: $B=<\begin{pmatrix}0&1\\1&1\end{pmatrix}>$. מהו האינדקס של B ב G?

ד. תהי תת חבורה של G: $C=<\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}>$. מהו האינדקס של C ב G?

פתרון.

א. נרשום את כל המטריצות ההפיכות $(det\neq 0)$ מגודל 2×2 מעל $\mathbb{Z}_2$:

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

ב. האינדקס של A ב G , המסומן $[G:A]$, שווה על פי לגרנז' למנה $\frac{|G|}{|A|}$. את גודל החבורה G חישבנו למעשה בסעיף א', וקיבלנו $|G|=6$. נותר לחשב את $|A|$: $A=\left\{\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}$, כלומר $|A|=2$. לכן $[G:A]=\frac{|G|}{|A|}=\frac{6}{2}=3$.

ג. נחשב את $|B|$: $B=\left\{\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}$, כלומר $|B|=3$. לכן $[G:B]=\frac{|G|}{|B|}=\frac{6}{3}=2$.

ד. תת החבורה C נוצרת ע"י שני יוצרים - היוצר של ת"ח A והיוצר של ת"ח B. בת"ח B יש 3 איברים ות"ח A אינה מוכלת ב B, לכן בהכרח ב C יש לפחות 4 איברים. כעת, מכיוון שסדר ת"ח חייב לחלק את סדר החבורה, בהכרח $|C|=6$, כלומר $C=G$. לכן $[G:C]=[G:G]=1$

שאלה 3. תהא G חבורה לא אבלית מסדר 8. הוכח שקיימת ב G תת חבורה מסדר 4. (הדרכה: הראה שקיים בהכרח איבר מסדר 4 היוצר את תת החבורה המבוקשת).

פתרון.

ב G בסה"כ 8 איברים. נראה שבהכרח קיים איבר מסדר 8.

הסדרים האפשריים הם אלו המחלקים את 8, כלומר $1,2,4,8$.

אין איבר מסדר 8 כי אם היה איבר כזה, הייתה זו חבורה ציקלית ולכן אבלית, בסתירה לנתון.

יש רק איבר אחד בכל חבורה מסדר 1. זהו איבר היחידה.

כעת נניח שכל אברי G מלבד איבר היחידה הם מסדר 2. על פי טענת עזר שנוכיח בסוף הפתרון, הנחה זו גוררת בהכרח שהחבורה אבלית, שוב בסתירה לנתון.

לכן בהכרח קיים איבר אחד לפחות מסדר 4 ב G ותת החבורה הציקלית שאיבר זה יוצר היא מסדר 4. סיימנו.

כעת נוכיח את טענת העזר.

כלומר נוכיח שאם בחבורה כלשהי כל האיברים (מלבד איבר היחידה), הם מסדר 2, אזי בהכרח החבורה אבלית.

לכל $x,y\in G$, מתקיים $x^2=1$ ו $y^2=1$, אבל גם המכפלה xy הינה איבר ב G ואיבר זה אינו איבר היחידה (כי כל איבר בחבורה זו הופכי לעצמו), לכן מתקיים גם $(xy)^2=1$. ולכן

$xyxy = (xy)^2 = 1$ אבל גם: $xxyy = (x)^2 (y)^2 = 1$. נשווה בין הביטויים ונקבל $xyxy = xxyy$ ואם נכפול את שני האגפים משמאל ב x ומימין ב y, נקבל $yx = xy$, כלומר החבורה אבלית.

שאלה 4. תהי G חבורה סופית, $a, b \in G$ כך ש: $ab = ba$ ו $\langle a \rangle \cap \langle b \rangle = 1$.
הוכח ש $o(ab) = lcm(o(a), o(b))$

פתרון.
נסמן $e = o(ab)$ ו $d = lcm(o(a), o(b))$. נוכיח ש $e|d$ וגם $d|e$ ונסיק ש $e = d$.
$d = lcm(o(a), o(b))$ כלומר $o(a)|d$ ולכן $a^d = 1$. באותו אופן, מאחר ש $o(b)|d$, נקבל ש $b^d = 1$.
כעת נשתמש בנתון ש $ab = ba$, על מנת לקבל ש: $(ab)^d = a^d b^d = 1 \cdot 1 = 1 \Rightarrow o(ab)|d$, כלומר $e|d$.
כעת נוכיח שגם $d|e$.על פי הסימון, $e = o(ab)$, כלומר $1 = (ab)^e = a^e b^e \Rightarrow a^e = b^{-e} = (b^e)^{-1}$. כמו כן, $a^e \in \langle a \rangle$, לכן : $a^e \in \langle a \rangle \cap \langle b \rangle = 1$, כלומר $a^e = 1$.
באופן דומה מראים ש: $b^e = 1$. ולכן $o(a)|d$ וגם $o(e)|d \Rightarrow lcm(o(a), o(b))|e$, כלומר $d|e$. לכן בהכרח: $e = d$.

שאלה 5. חשב בעזרת משפט אוילר:

א. 197^{81} מודולו 34

ב. שתי הספרות האחרונות של 1249^{602}

הערה. ניתן להעזר בנוסחה הבאה לחישוב פונצקיית אוילר של מספר שלם כלשהו:

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$

כאשר $p_1, \ldots\ldots, p_k$ המספרים הראשוניים בפירוק של השלם n.

פתרון.

א. על פי הנוסחה לחישוב פונקציית אוילר, נקבל $\varphi(34) = 34 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{17}\right) = 16$.
לכן, תוך שימוש במשפט אוילר לפיו עבור $a \in U_n$, $a^{\varphi(n)} = 1 \pmod{n}$ נקבל:
$197^{81} = \left((197)^{15}\right)^5 \cdot (197)^1 = \left((197)^{\varphi(34)}\right)^5 \cdot (197)^1 \equiv (1)^5 \cdot (197)^1 = 197$.
כלומר 197^{81} שקול ל 197 (mod 34). ו $197 \pmod 3 4 = 27$.

ב. חישוב שתי הספרות האחרונות של 1249^{602} שקול לחישוב $1249^{602} \pmod{100}$. כמו בסעיף א', נחשב תחילה $\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$. נשתמש שוב במשפט אוילר ונקבל: $1249^{602} \equiv 49^{602} = \left((49)^{40}\right)^{15} \cdot (49)^2 = \left((197)^{\varphi(100)}\right)^{15} \cdot (49)^2 \equiv (1)^{15} \cdot (49)^2 = 49^2$.
כלומר 1249^{602} שקול ל 49^2 (mod 100). ו $49^2 = 2401 = 1 \pmod{100}$.

בהצלחה.