פתרון תרגיל בית 6 במבנים אלגבריים
89-214 סמסטר א' תשע"ט

שאלה 1 (חזרה)**.** נסתכל על $G = U_{14} \times \mathbb{Z}_4$.

א. מהו הסדר של $(3,2)$ ב-G? נמקו.

ב. האם G אבלית? נמקו.

ג. האם G ציקלית? נמקו.

פתרון.

א. אפשר להתחיל לחשב (לא מומלץ), אבל אפשר להיעזר בטענה שראינו בכיתה. לפי השאלה הזו, מספיק לחשב את הסדר של 3 ב-U_{14} ואת הסדר של 2 ב-$\mathbb{Z}_4$. על ידי חישוב ישיר, הסדר של 3 ב-U_{14} הוא 6, והסדר של 2 ב-$\mathbb{Z}_4$ הוא 2. לכן,

$$o\left((3,2)\right) = [6,2] = 6$$

ב. אנחנו יודעים ש-U_{14} ו-$\mathbb{Z}_4$ אבליות, ולכן גם $U_{14} \times \mathbb{Z}_4$ אבלית לפי תרגיל בית שפתרתם.

ג. נשים לב כי $|U_{14} \times \mathbb{Z}_4| = \varphi\left(14\right) \cdot 4 = 6 \cdot 4 = 24$. כלומר, כדי לבדוק אם $U_{14} \times \mathbb{Z}_4$ ציקלית, מספיק לבדוק אם יש בה איבר מסדר 24.
לפי שאלה 4, כדי שהסדר של (g,h) יהיה 24, צריך שיתקיים $24 = [o\left(g\right), o\left(h\right)]$.
הסדרים של האיברים ב-$\mathbb{Z}_4$ הם $1,2,4$, ואילו הסדרים של האיברים ב-U_{14} הם $1,2,3,6$ (על ידי בדיקה ישירה, או על ידי שימוש בלגראנז' שלמדנו יותר מאוחר).
לכן, אין דרך שבה ה-lcm ייצא 24 - גם אם $o\left(g\right) = 6$ ו-$o\left(h\right) = 4$, יתקיים

$$o\left((g,h)\right) = [o\left(g\right), o\left(h\right)] = [6,4] = 12$$

לכן זו לא חבורה ציקלית.

שאלה 2. מצאו את האינדקסים הבאים. משפט לגראנז' הוא שימושי.

א. $[U_{14} : \langle 11 \rangle]$

ב. $[\mathbb{Z}_8 \times \mathbb{Z}_8 : \langle (2,2) \rangle]$

ג. $[\mathbb{Z} \times \mathbb{Z} : \langle (2,2) \rangle]$ רמז: קודם תארו את המחלקות השמאליות.

ד. $[2\mathbb{Z} \times S_3 : 6\mathbb{Z} \times \langle \mathrm{id} \rangle]$

פתרון.

א. איברי U_{14} הם הטבעיים שקטנים וזרים ל-14. כלומר $U_{14} = \{1,3,5,9,11,13\}$. חישוב קצר יראה כי $\langle 11 \rangle = \{1,9,11\}$, ואז לפי משפט לגרנז' נקבל שיש בדיוק שתי מחלקות שמאליות. כלומר $[U_{14} : \langle 11 \rangle] = 2$.

ב. הסדר של החבורה $\mathbb{Z}_8 \times \mathbb{Z}_8$ הוא $8 \cdot 8 = 64$, והסדר של תת־החבורה $\langle (2,2) \rangle$ הוא כסדר של האיבר $(2,2)$, שהוא 4. לכן לפי משפט לגראנז' $[\mathbb{Z}_8 \times \mathbb{Z}_8 : \langle (2,2) \rangle] = 64/4 = 16$.

ג. נוכיח כי $[\mathbb{Z} \times \mathbb{Z} : \langle (2,2) \rangle] = \infty$ לפי זה שנראה ש-$\{(0,n) + \mathbb{Z} \times \mathbb{Z}\}$ היא קבוצה אינסופית של מחלקות שמאליות שונות (אלו לא כל המחלקות). אם $(0,n) + \mathbb{Z} \times \mathbb{Z} = (0,m) + \mathbb{Z} \times \mathbb{Z}$ זה אומר

$$(0,n) - (0,m) \in \langle (2,2) \rangle$$

כלומר ש-$(2k,2k) = (0, n-m)$ לאיזשהו $k \in \mathbb{Z}$. לכן $n - m = 0$, ולכן $n = m$. כלומר יש אינסוף מחלקות שמאליות שונות.

ד. אינדקס של תת־חבורות הוא כפלי (הוכיחו!). כלומר אם $K \leq H \leq G$, אז

$$[G : K] = [G : H] \, [H : K]$$

בפרט נקבל

$$[2\mathbb{Z} \times S_3 : 6\mathbb{Z} \times \langle \mathrm{id} \rangle] = [2\mathbb{Z} \times S_3 : 6\mathbb{Z} \times S_3] \, [6\mathbb{Z} \times S_3 : 6\mathbb{Z} \times \langle \mathrm{id} \rangle]$$

ולכן נוכל לחשב בנפרד. המחלקות השמאליות של $6\mathbb{Z} \times S_3$ בחבורה $2\mathbb{Z} \times S_3$ הן

$$\{(0, \mathrm{id}) \, (6\mathbb{Z} \times S_3) \, , (2, \mathrm{id}) \, (6\mathbb{Z} \times S_3) \, , (4, \mathrm{id}) \, (6\mathbb{Z} \times S_3)\}$$

וכמובן שיש העתקה חח"ע ועל למחלקות השמאליות של $6\mathbb{Z}$ ב-$2\mathbb{Z}$. באופן דומה, את האינדקס של $6\mathbb{Z} \times \langle \mathrm{id} \rangle$ ב-$6\mathbb{Z} \times S_3$ אפשר לחשב לפי האינדקס של $\langle \mathrm{id} \rangle$ ב-S_3, שהוא 6. לכן האינדקס המבוקש הוא $3 \cdot 6 = 18$.

שאלה 3. תהי G חבורה ותהינה $H, K \leq G$ תת־חבורות סופיות שלה.

א. הוכיחו שאם $(|H|, |K|) = 1$, אז $H \cap K = \{e\}$.

ב. יהי p מספר ראשוני. הוכיחו שאם $|H| = |K| = p$ וגם $H \neq K$, אז $H \cap K = \{e\}$.

פתרון.

א. ידוע לנו כי $H \cap K$ היא תת־חבורה של H ושל K. לכן לפי משפט לגראנז' מתקיים כי $|H \cap K|$ מחלק את $|H|$ ואת $|K|$. אך לפי הנתון הממ"מ של $|H|$ ו-$|K|$ הוא 1. לכן $|H \cap K| \leq 1$. אבל תמיד $|H \cap K| \geq 1$ כי איבר היחידה שייך אליו, ולכן קיבלנו כי $H \cap K = \{e\}$.

ב. יהי $x \in H \cap K$ איבר כלשהו. נניח בשלילה כי $x \neq e$. לכן $o(x) > 1$. אנחנו יודעים כי $o(x)$ מחלק את $|H|$ ואת $|K|$, ולכן בהכרח $o(x) = p$. כלומר $|\langle x \rangle| = p$ ומפני ש-H, K הן חבורות אז הן סגורה לפעולה ונסיק $\langle x \rangle \subseteq H, K$. מהנתון $|H| = |K| = p$ נקבל $\langle x \rangle = H = K$ כי ב-$\langle x \rangle$ יש בדיוק p איברים שונים. אך זו סתירה לנתון, ונסיק כי $x = e$.

שאלה 4. נסתכל על $G = GL_2(\mathbb{Z}_2)$, חבורת המטריצות ההפיכות מגודל 2×2 מעל $\mathbb{Z}_2$.

א. כתבו את כל איברי G (הזכרו בהבדל בין $GL_2(\mathbb{Z}_2)$ ל-$M_2(\mathbb{Z}_2)$).

ב. תהי $A = \langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle \leq G$ תת־חבורה של G. מצאו את $[G : A]$.

ג. תהי $B = \langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \rangle \leq G$ תת־חבורה של G. מצאו את $[G : B]$.

ד. מצאו איזומורפיזם $\varphi\colon G \to S_3$ מפורש (כתבו לאן נשלח כל איבר).
את הבדיקה שאכן מדובר באיזומורפיזם אפשר (וכדאי) לממש בעזרת תוכנה, שהרי אפשר לממש את החבורות האלו במחשב ואנחנו יודעים איך לכפול את האיברים שלהן. אפשר להעזר במערכת מתמטית כמו SageMath לצורך הפתרון.

פתרון.

א. נרשום את כל המטריצות ההפיכות (כלומר הדטרמיננטה שונה מאפס) מגודל 2×2 מעל $\mathbb{Z}_2$:

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

ב. האינדקס של A ב-G שווה על פי לגראנז' למנה $[G:A] = \frac{|G|}{|A|}$. את סדר החבורה G חישבנו בסעיף הקודם, וקיבלנו $|G| = 6$. נותר לחשב את $|A|$: $A = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\}$, כלומר $|A| = 2$. לכן $[G:A] = \frac{|G|}{|A|} = \frac{6}{2} = 3$.

ג. כמו בסעיף הקודם, נחשב $B = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)\}$, ולכן $|B| = 3$. לפי לגראנז' נקבל $[G:B] = \frac{|G|}{|B|} = \frac{6}{3} = 2$.

ד. נתאים את האיברים הבאים (יש אפשרויות אחרות):

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto \mathrm{id} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \mapsto (1\ 2\ 3) \qquad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \mapsto (1\ 3\ 2)$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mapsto (1\ 2) \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \mapsto (1\ 3) \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto (2\ 3)$$

ההוכחה שזהו איזומורפיזם נשארת לכם, והחלק היחיד שנשאר זה רק להוכיח שזה הומומורפיזם.

תרגיל 5. תהי G חבורה מסדר 8.

א. הוכיחו שאם G ציקלית, אז יש לה תת־חבורה מסדר 4 (למה ברור כי תת־החבורה כאן היא ציקלית?).

ב. הוכיחו שאם G לא אבלית, אז יש לה תת־חבורה ציקלית מסדר 4 (כאן הציקליות של תת־החבורה לא ברורה מיידית).

ג. מצאו דוגמה נגדית לסעיף הקודם אם G אבלית.

ד. (רשות) נכליל למקרה שבו G היא חבורה לא אבלית מסדר 2^t עבור $t > 2$. הוכיחו שיש לה תת־חבורה ציקלית מסדר 4.

פתרון.

א. נניח $G = \langle g \rangle$ ציקלית מסדר 8 עם יוצר g. אזי קיימת תת־החבורה הציקלית שנוצרת על ידי $\left\langle g^2 \right\rangle = \left\{ e, g^2, g^4, g^6 \right\}$.

ב. תהא G חבורה לא אבלית. לפי משפט לגראנז', הסדר של כל איבר בחבורה סופית מחלק את סדר החבורה. לכן הסדרים האפשריים היחידים בחבורה מסדר 8 הם 1, 2, 4 או 8 (לא בהכרח כל הסדרים משתתפים).
יש רק איבר אחד מסדר 1 והוא איבר היחידה. לא ייתכן כי כל שאר האיברים הם מסדר 2, שכן לפי תרגיל שראינו נקבל כי G אבלית. אין בחבורה איבר מסדר 8, שכן אז היא תהיה ציקלית, וכל חבורה ציקלית היא אבלית. מכאן קיים איבר, נאמר $a \in G$, שהוא מסדר 4. הסדר של איבר הוא הסדר של תת־החבורה הציקלית $\{e, a, a^2, a^3\}$ שהוא יוצר.

ג. במקרה זה G לא יכולה להיות ציקלית. נבחר את $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. אפשר לבדוק שהסדר של כל איבר בחבורה זו הוא 2, פרט לאיבר היחידה. לכן אין לה תת־חבורה ציקלית מסדר 4.

ד. באופן דומה לשאלה האחרונה, הסדרים האפשריים היחידים בחבורה מסדר 2^t (כאשר $t > 2$) הם רק מן הצורה 2^k עבור $k \in \{0, 1, 2, \ldots, t\}$. ישנו רק איבר אחד מסדר 1. הסדר של כל שאר האיברים לא יכול להיות 2, כי אז G אבלית. אין איבר מסדר 2^t, שכן אז החבורה ציקלית ולכן אבלית. לכן קיים איבר, נאמר $a \in G$, כך ש-$o(a) = 2^k > 2$.
נתבונן בתת־החבורה $\langle a \rangle$ ונבחר את האיבר a^{k-2}. מתקיים

$$o(a^{2^{k-2}}) = \frac{2^k}{(2^k, 2^{k-2})} = 4$$

וקיבלנו שזהו האיבר שיוצר את תת־החבורה הציקלית הדרושה מסדר 4.

שאלה 6 (רשות). נקרא למטריצה M מטריצת תמורה אם היא מטריצה שכל האיברים בה הם אפסים ואחדות, ושבכל שורה ובכל עמודה יש בדיוק פעם אחת 1. למשל

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

היא מטריצת תמורה בגודל 4×4. הוכיחו שאוסף מטריצות התמורה בגודל $n \times n$ הוא חבורה עם הפעולה של כפל מטריצות. התאימו לכל איבר $\sigma \in S_n$ מטריצת תמורה M_σ כך שיתקבל איזומורפיזם, והוכיחו שהסימן של σ הוא הדטרמיננטה של M_σ.

בהצלחה!