פתרון תרגיל 4 מבוא לתורת החבורות תשע"ט

שאלה 1. הי p ראשוני, ותהי G חבורה מסדר p^2.

א. הוכיחו שניתן ליצור את G עם תת־קבוצה בת שני איברים. רמז: משפט לגראנז' כמה פעמים.

ב. בחרו p. תנו דוגמה מפורשת ל-G לא ציקלית מסדר p^2, ולשני איברים $a, b \in G$ כך ש-$G = \langle a, b \rangle$.

פתרון. א. כמסקנה מלגראנז' אנחנו יודעים שהסדרים האפשריים של איברים ב-G הם $\{1, p, p^2\}$.
אם קיים איבר $a \in G$ מסדר p^2, אז G ציקלית ומתקיים $G = \langle a \rangle$. לכן נוכל לבחור **כל** איבר אחר $b \in G$, ויתקיים

$$G = \langle a \rangle \leq \langle a, b \rangle \leq G$$

כלומר $G = \langle a, b \rangle$. אם לא קיים איבר מסדר p^2, אז הסדר של כל האיברים הוא p, פרט לאיבר היחידה. יהי $c \in G$ איבר מסדר p. אז $p = |\langle c \rangle|$, כי הסדר של תת־החבורה הציקלית שאיבר יוצר הוא הסדר של האיבר. נבחר $d \in G \setminus \langle c \rangle$ מסדר p (ודאו שברור לכם למה קיים d כזה). אז לפי לגראנז' הסדר של תת־החבורה $\langle c, d \rangle$ מחלק את $|G| = p^2$, ובנוסף הוא חייב להיות גדול מ-p, כי $|\langle c \rangle \cup \{d\}| = p + 1$. לכן $|\langle c, d \rangle| = p^2$. כלומר $G = \langle c, d \rangle$, כדרוש.

ב. עד כדי איזומורפיזם, אפשר לבחור רק את $\mathbb{Z}_p \times \mathbb{Z}_p$. למשל אפשר לבחור את $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, ואת האיברים $a = (1, 0)$, $b = (1, 1)$, ששניהם מסדר $p = 2$.

שאלה 2. חשבו את האינדקס של תת־החבורה:
$[\mathbb{Z} \times \mathbb{Z} : \langle (1, 1) \rangle]$. רמז: מצאו קבוצה אינסופית של מחלקות שונות.

פתרון.
נראה ש-$\{(0, n) + \mathbb{Z} \times \mathbb{Z}\}$ היא קבוצה אינסופית של מחלקות שונות. אם

$$(0, n) + \mathbb{Z} \times \mathbb{Z} = (0, m) + \mathbb{Z} \times \mathbb{Z}$$

זה אומר ש-$(0, n) - (0, m) \in \langle (1, 1) \rangle$. כלומר ש-$(0, n - m) = (k, k)$ לאיזשהו $k \in \mathbb{Z}$. לכן $k = 0 = n - m$, ולכן $n = m$. כלומר עבור $n \neq m$ מדובר במחלקות שונות. לכן $[\mathbb{Z} \times \mathbb{Z} : \langle (1, 1) \rangle] = \infty$ (ודאו שאתם יודעים למה לא יתכן שיש יותר מ-$\aleph_0$ מחלקות שונות).

שאלה 3. נסתכל על $G = (GL_2(\mathbb{Z}_2), \cdot)$ – חבורת המטריצות ההפיכות מגודל 2×2 מעל $\mathbb{Z}_2$ (שדה בין שני איברים),

א. רשמו את כל איברי הקבוצה G (זכרו את ההבדל 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 4. תהי G חבורה.

1. הוכיחו שהמרכז של G הוא תת-חבורה נורמלית.
2. נניח שכל תתי-החבורות של G הן נורמליות. האם G אבלית?

פתרון. א. נזכור שהמרכז הוא:

$$Z(G) = \{a \in G | \forall h \in G : \ ah = ha\}$$

קבוצת האיברים שמתחלפים עם כל האיברים, ולכן:

$$gZ(G) = \{ga | \forall h \in G : \ ah = ha\} = \{ag | \forall h \in G : \ ah = ha\} = Z(G)g$$

ב. לא בהכרח. נתבונן בחבורת הקווטרניונים: $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, הפעולה היא כפל ומתקיים:

$$i^2 = j^2 = k^2 = ijk = -1$$

כדאי לכם להוכיח שזו אכן חבורה. היכנסו לערך הויקיפדיה בעברית, הוא מספיק טוב – הסתכלו על לוח הכפל של החבורה. שימו לב שאם הסימונים לא ברורים, אפשר לרשום את החבורה כתת-חבורה של $SL_2(\mathbb{C})$ עם 8 מטריצות, ואז יותר קל להבין איך נראות המכפלות ולמה החבורה לא אבלית.
החבורה אינה אבלית, אך כל תתי-החבורות שלה הן נורמליות. מהן תתי-החבורות שלה?
הסדר של החבורה הוא 8 ולכן הסדרים האפשריים הם $1, 2, 4, 8$.
תתי-החבורות מסדרים $1, 8$ הן תתי-החבורות הטריוויאליות: $Q_8, \{1\}$ וברור שהן נורמליות.
תת-חבורה מסדר 4 היא תת-חבורה מאינדקס 2 ולכן נורמלית.
תת החבורה מסדר 2 היא $\{\pm 1\}$ והיא נורמלית כי היא המרכז של G.