

פתרון תרגיל בית 3 בקורס 89-214 סמסטר א' תשע"ד

נהלים בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך ההגשה הוא בשבוע המתחיל ב-10.11.2013 לידי המתרגל.

תזכורת תהא G חבורה. הגדרנו את הסדר של איבר $a \in G$ להיות המספר הטבעי המינימלי n כך שמתקיים $a^n = e$ וסימנו $|a| = n$. הגדרנו את חבורת אוילר להיות החבורה של כל האיברים ההפיכים במונואיד (\mathbb{Z}_n, \cdot) , וסימנו $U_n = U(\mathbb{Z}_n)$.

שאלה 1. עבור כל אחת מן החבורות U_9, U_{12} ו- $(\mathbb{Z}_8, +)$ מצאו את כל האיברים וענו:

1. מה הסדר של כל איבר?

2. אם החבורה ציקלית, כמה יוצרים שונים יש לה?

פתרון. בכל חבורה הסדר של איבר היחידה הוא 1. בכל חבורה הסדר של איבר היחידה הוא 1. הסדר של 8 הוא 2 כי איברי החבורה U_9 הם $\{1, 2, 4, 5, 7, 8\}$, כאשר 1 הוא איבר היחידה. הסדר של 8 הוא 2 כי

$$8^2 = 8 \cdot 8 = 64 \equiv 1 \pmod{9}$$

בדיקה ישירה תראה כי הסדר של 4, 7 הוא 3. הסדר של 2, 5 הוא 6. לכן U_9 היא חבורה ציקלית, שכל אחד מן האיברים 2, 5 הוא יוצר שלה. איברי החבורה U_{12} הם $\{1, 5, 7, 11\}$, כאשר 1 הוא איבר היחידה. הסדר של כל האיברים האחרים הוא 2:

$$5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$$

בדיקה ישירה לפי ההגדרה יכולה להראות כי U_{12} לא ציקלית, אבל אפשר להשתמש בטיעון יותר מוצלח: בחבורה לא קיים איבר מסדר 4 שהוא סדר החבורה, ולכן היא לא ציקלית. איברי החבורה \mathbb{Z}_8 הם $\{0, 1, 2, 3, 4, 5, 6, 7\}$, כאשר 0 הוא איבר היחידה. הסדר של 4 הוא 2, הסדר של 2, 6 הוא 4 והסדר של 1, 3, 5, 7 (שימו לב כי הם זרים ל-8) הוא 8. חבורה זו היא ציקלית, וכל אחד מארבעת האיברים שזר ל-8 יוצר אותה.

שאלה 2. תהי G חבורה ויהי איבר $a \in G$ מסדר אינסופי. הוכיחו כי אם $m \neq n$, אז $a^m \neq a^n$.

פתרון. יהי איבר $a \in G$ מסדר אינסופי. נניח בשלילה כי מתקיים $a^m = a^n$ עבור $m < n$. נקבל $a^{n-m} = a^m \cdot a^{-m} = e$, כלומר יש מספר טבעי $n - m \in \mathbb{N}$ כך ש- $a^{n-m} = e$, וזו סתירה לכך שהאיבר a הוא מסדר אינסופי.

שאלה 3. הוכיחו בעזרת טבלאות כפל כי כל חבורה מסדר 2 וכל חבורה מסדר 3 היא ציקלית. מצאו כמה יוצרים יש בכל מקרה. רמז: אם מניחים בשלילה שחבורה לא ציקלית, מה לומדים על סדר האיברים?

פתרון. נניח כי $(S, *)$ היא חבורה מסדר 2. כלומר יש בה איבר יחידה e , שהוא יחיד, ועוד איבר אחר שנסמן אותו a . סך הכל $S = \{e, a\}$. נוכל למלא את טבלת הכפל של $(S, *)$ באופן יחיד:

*	e	a
e	e	a
a	a	e

מה שיש למלא בשורה ובטור של e הוא ברור. מה שנשאר הוא המשבצת של $a * a$ שחייבת להיות e כי לכל איבר בחבורה ישנו איבר הופכי, לפי הגדרה. נשים לב כי חזקות של האיבר a הן כל האיברים של $(S, *)$, ולכן היא ציקלית. האיבר a הוא היוצר היחיד. כעת נניח כי $(T, *)$ היא חבורה מסדר 3. נסמן את האיברים השונים באופן דומה $T = \{e, a, b\}$. נוכל למלא חלקית את טבלת הכפל:

*	e	a	b
e	e	a	b
a	a		
b	b		

נתבונן בחזקות של האיבר a . בכל מקרה החזקות של איבר זה תמיד כוללות את $a^1 = a$ ואת $a^0 = e$. באופן דומה החזקות של b תמיד כוללות את b ואת e . נניח בשלילה כי T אינה ציקלית, אז אין חזקה שבה $a^k = b$. בפרט, במשבצת $a * a$ לא נוכל למלא b . גם לא נוכל למלא $a * a = a$, שכן אחרי כפל ב- a^{-1} נגיע לסתירה בשיוויון $a = e$ של איברים שונים. לכן נשאר למלא $a * a = e$, שמשמעותו $a^{-1} = a$. משיקולים סימטריים נצטרך למלא $b * b = e$, שמשמעותו $b^{-1} = b$. מפני שאיבר הופכי בחבורה הוא יחיד, במשבצת $a * b$ לא נוכל למלא e . אם $a * b = a$, מגיעים לסתירה $b = e$, ואם $a * b = b$, מגיעים לסתירה $a = e$. מכאן שההנחה המקורית שלנו לא נכונה, ואכן קיימת חזקה של a כך שמתקיים $a^k = b$, שבמקרה זה אומר כי $a * a = b$. בשורה ובטור של a חייב להופיע e פעם אחת, עבור האיבר ההופכי של a , ולכן $a * b = e$ וגם $b * a = e$. לבסוף נקבל כי טבלת הכפל האפשרית היחידה היא

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

שמראה כי $(T, *)$ היא חבורה ציקלית, שיש לה שני יוצרים שונים $\langle a \rangle = \langle b \rangle$. אגב, טבלאות הכפל גם מראות כי בשני המקרים מדובר בחבורות אבליות. נזכיר כי כל החבורות הציקליות מסדר 2 הן בעצם \mathbb{Z}_2 עד כדי "שינוי שמות" (מבלי שהגדרנו זאת באופן מדויק), וגם כי כל החבורות הציקליות מסדר 3 הן בעצם \mathbb{Z}_3 עד כדי "שינוי שמות".

שאלה 4. תהא קבוצה X כלשהי (אם זה עוזר, אפשר להניח שהיא סופית) ומגדירים את קבוצת החזקה $P(X)$ להיות קבוצת כל תת הקבוצות של X . נגדיר על $P(X)$ את פעולת ההפרש הסימטרי המוגדר לכל $A, B \in P(X)$ לפי $A \Delta B = (A \cup B) \setminus (A \cap B)$. ענו עבור $(P(X), \Delta)$ האם הוא אגודה? האם הוא מונואיד? האם הוא חבורה? האם הפעולה היא חילופית?

פתרון. המבנה $(P(X), \Delta)$ הוא חבורה. סגירות הפעולה נובעת מכך שאם $A, B \in P(X)$, אז גם $A \Delta B$ היא תת קבוצה של X . קיבוציות הפעולה ידועה ממתמטיקה בדידה. איבר היחידה הוא הקבוצה הריקה. קל לבדוק שכל איבר הוא ההופכי של עצמו. הפעולה (כפי ששמה רומז) היא חילופית. אגב, אפשר להראות כי החבורה הזו חילופית גם לפי התרגיל שבו נדרש להוכיח שאם בחבורה מתקיים $a^2 = e$ לכל איבר $a \in G$, אז G חילופית.

שאלה 5. יהיו $a, b \in \mathbb{Z}$. הוכיחו את הטענות הבאות:

1. $a\mathbb{Z} \subseteq b\mathbb{Z}$ אם ורק אם $b | a$.
2. נגדיר קבוצה $a\mathbb{Z} + b\mathbb{Z} = \{au + bv : u, v \in \mathbb{Z}\}$. הוכיחו $a\mathbb{Z} + b\mathbb{Z} = (a, b) \cdot \mathbb{Z}$.
3. $a\mathbb{Z} \cap b\mathbb{Z} = [a, b] \cdot \mathbb{Z}$.

פתרון.

1. מצד אחד, אם $a\mathbb{Z} \subseteq b\mathbb{Z}$, אזי בפרט $a \in b\mathbb{Z}$. לכן קיים $n \in \mathbb{Z}$ כך שמתקיים $a = bn$. כלומר $b | a$. מצד שני, אם $b | a$, אז קיים $n \in \mathbb{Z}$ כך שמתקיים $a = bn$. לכן אם $x \in a\mathbb{Z}$, קיים $m \in \mathbb{Z}$ כך ש- $x = am$ ולכן $x = bnm$, כלומר $x \in b\mathbb{Z}$.

2. נוכיח בהכלה דו-כיוונית. נתחיל עם \subseteq : ידוע כי ניתן להציג את (a, b) כצירוף לינארי של a, b . כלומר קיימים $u, v \in \mathbb{Z}$ כך שמתקיים $(a, b) = au + bv$. יהי $x \in a\mathbb{Z} + b\mathbb{Z}$, ולכן קיימים $n_a, n_b \in \mathbb{Z}$ כך ש- $x = an_a + bn_b$. אנו צריכים למצוא $m \in \mathbb{Z}$ שיתקיים $(a, b)m = an_a + bn_b$. אפשר לבחור את $m = \frac{a}{(a,b)}n_a + \frac{b}{(a,b)}n_b$. הכיוון השני \supseteq הוא יותר קל כי ידוע לנו שניתן להציג את (a, b) כצירוף לינארי של a, b , ולכן גם כל כפולה שלו.

3. הוכחה (בסימונים מתמטיים) שנעזרת בהגדרה של כפולה משותפת מינימלית:

$$x \in [a, b] \cdot \mathbb{Z} \iff \exists m \in \mathbb{Z} : x = [a, b]m \iff [a, b] | x \iff a | x \wedge b | x \iff x \in a\mathbb{Z} \cap b\mathbb{Z}$$

שאלה 6. תנו דוגמה נגדית לכל אחת מן הטענות השגויות הבאות:

1. תהא G חבורה מסדר זוגי. אם $x^3 = y^3$, אז $x = y$.
2. תהא G חבורה אבלית מסדר n . ודאי קיים איבר מסדר n בחבורה G .
3. כל חבורה מסדר 8 היא אבלית. רמז: למשל חבורה המוגדרת באופן דומה לחבורת מטריצות מתרגיל הבית הקודם.

פתרון.

1. אפשר לבחור למשל את $G = (\mathbb{Z}/6\mathbb{Z}, +)$. נסתכל על $3 \in G$. 1, 3 מתקיים

$$"1^3" = 1 + 1 + 1 \equiv 3 \equiv 3 + 3 + 3 = "3^3" \pmod{6}$$

אבל $1 \neq 3$ בחבורה G .

2. אפשר לבחור את $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (עם חיבור מודולו 3 רכיב-רכיב) שהיא חבורה מסדר 9, אבל הסדר הגבוה ביותר של איבר בה הוא 3. ליתר דיוק, בדיקה ידנית תראה כי כל איבר פרט לאיבר היחידה $(0, 0)$ שהוא מסדר 1, הם מסדר 3.

3. בדומה לשאלה מתרגיל בית קודם, נגדיר חבורה H להיות אוסף המטריצות

$$H = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}/2\mathbb{Z} \right\}$$

עם הפעולה של כפל מטריצות. עבור כל אחד מן $a, b, c \in \mathbb{Z}/2\mathbb{Z}$ יש שתי אפשרויות, ולכן החבורה H היא מסדר $2^3 = 8$. החבורה הזו לא אבליית כי למשל:

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

בהצלחה!