

פתרון תרגיל 2 – אלגברה מופשטת

1. יהי M מונואיד. נגדיר את קבוצת ההפיכים $U(M) = \{a \in M : \text{הופכי } a\}$. הוכיחו כי $U(M)$ היא חבורה ביחס לפעולה של M . חבורה זו נקראת חבורת ההפיכים.

הוכחה:

איבר היחידה של המונואיד הפיך לכן $e \in U(M)$ ו- $U(M) \neq \emptyset$.
סגירות הפעולה: יהיו $a, b \in U(M)$ אזי a, b הפיכים. אבל $(ab)^{-1} = b^{-1}a^{-1}$ ובפרט ab הפיך. לכן $ab \in U(M)$.
איבר היחידה של $U(M)$ הוא איבר היחידה של M .
הפיך: יהי $a \in U(M)$. ההופכי שלו ב M , a^{-1} מקיים $a^{-1} \in U(M)$ (שכן גם הוא הפיך ב M) וברור כי a^{-1} הופכי ל a ב $U(M)$.

2. ענו על הסעיפים הבאים.

2.1 מצאו את המחלק המשותף המקסימלי $(5614, 1260)$.
פתרון: נשתמש באלגוריתם אוקלידס:

$$(5614, 1260) \underset{5614=4 \cdot 1260+574}{=} (1260, 574) \underset{1260=2 \cdot 574+112}{=} (574, 112) \underset{574=5 \cdot 112+14}{=} (112, 14) \underset{112=8 \cdot 14+0}{=} (14, 0) = 14$$

2.2 מצאו $\alpha, \beta \in \mathbb{Z}$ כך ש- $1525\alpha + 927\beta = 1$.

פתרון: נשתמש באלגוריתם אוקלידס:

$$(1525, 927) \underset{1525=1 \cdot 927+598}{=} (927, 598) \underset{927=1 \cdot 598+329}{=} (598, 329) \underset{598=1 \cdot 329+269}{=} (329, 269) \underset{329=1 \cdot 269+60}{=} (269, 60) \\ \underset{269=4 \cdot 60+29}{=} (60, 29) \underset{60=2 \cdot 29+2}{=} (29, 2) \underset{29=14 \cdot 2+1}{=} (2, 1) \underset{2=2 \cdot 1+0}{=} (1, 0) = 1$$

כעת, נחזור אחורה:

$$\begin{aligned}
1 &= 29 - 14 \cdot 2 \\
&= 29 - 14 \cdot (60 - 2 \cdot 29) \\
&= 29 - 14 \cdot 60 + 28 \cdot 29 \\
&= -14 \cdot 60 + 29 \cdot 29 \\
&= -14 \cdot 60 + 29 \cdot (269 - 4 \cdot 60) \\
&= -14 \cdot 60 + 29 \cdot 269 - 116 \cdot 60 \\
&= -130 \cdot 60 + 29 \cdot 269 \\
&= -130 \cdot (329 - 1 \cdot 269) + 29 \cdot 269 \\
&= -130 \cdot 329 + 130 \cdot 269 + 29 \cdot 269 \\
&= -130 \cdot 329 + 159 \cdot 269 \\
&= -130 \cdot 329 + 159 \cdot (598 - 1 \cdot 329) \\
&= -130 \cdot 329 + 159 \cdot 598 - 159 \cdot 329 \\
&= -289 \cdot 329 + 159 \cdot 598 \\
&= -289 \cdot (927 - 1 \cdot 598) + 159 \cdot 598 \\
&= -289 \cdot 927 + 289 \cdot 598 + 159 \cdot 598 \\
&= -289 \cdot 927 + 448 \cdot 598 \\
&= -289 \cdot 927 + 448 \cdot (1525 - 1 \cdot 927) \\
&= -289 \cdot 927 + 448 \cdot 1525 - 448 \cdot 927 \\
&= 448 \cdot 1525 - 737 \cdot 927
\end{aligned}$$

לכן, $\alpha = 448$, $\beta = -737$ מקיימים את הדרוס.

2.3 קבעו אם $[927]$ הפיך במונואיד $(Z_{1525}, \cdot, \text{mod } 1525)$. אם כן, מצאו את ההופכי שלו.

פתרון: לפי הסעיף הקודם, $(1525, 927) = 1$ לכן $[927]$ הפיך במונואיד $(Z_{1525}, \cdot, \text{mod } 1525)$. מהשוויון $448 \cdot 1525 - 737 \cdot 927 = 1$ שהתקבל בסעיף הקודם נובע כי $-737 \cdot 927 \equiv 1 \pmod{1525}$ לכן ההופכי של $[927]$ הפיך במונואיד $(Z_{1525}, \cdot, \text{mod } 1525)$ הוא $[-737] = [788]$.

2.4 יהיו $m, n \in Z$ ו $d = (m, n)$ המחלק המשותף המקסימלי שלהם. יהי $k \in Z$ כך ש $k | m \wedge k | n$. הוכיחו כי $k | d$.

פתרון: לפי משפט מההרצאה, מכיוון ש $d = (m, n)$ קיימים מקדמים $s, t \in Z$ כך ש $sm + tn = d$. מכיוון ש $k | m \wedge k | n$, k מחלק כל צירוף לינארי שלהם. בפרט, $k | d$.

3. תהי G חבורה ויהיו $a, b \in G$. הוכיחו את הטענות הבאות.

$$3.1 \quad \text{אם } o(a) = n \text{ ומתקיים } a^m = e \text{ אז } n | m.$$

רמז: חלקו את m ב n חילוק עם שארית והראו כי השארית היא בהכרח אפס.

פתרון: נשתמש בחילוק עם שארית. קיימים $q, r \in \mathbb{Z}$ כך ש $m = qn + r$ ו $0 \leq r < n$. נראה כי $r = 0$ ונקבל כי $n | m$.

נניח בשלילה כי $r > 0$.

מהנתון $a^m = e$ נובע $a^{qn+r} = (a^n)^q a^r = e$. מכיוון ש $o(a) = n$, נציב בשוויון

$a^r = e$ ונקבל כי $a^r = e$ בסתירה לכך ש n הוא המעריך הטבעי המינימלי עבור $a^n = e$. לכן $r = 0$.

$$3.2 \quad o(ab) = o(ba)$$

הוכחה: נחלק למקרים.

א. הסדר של ab סופי.

ב. הסדר של ab אינסופי.

במקרה א': נסמן $o(ab) = n$ ונראה כי $o(ba) \leq n$.

אכן, $(ba)^{n+1} = (ba)(ba) \cdots (ba) = b(ab)^n a = b e a = ba$, נכפול את המשוואה ב $(ba)^{-1}$

משמאל ונקבל: $(ba)^n = e$. לכן $o(ba) \leq n = o(ab)$.

בפרט, הסדר של ba סופי.

באופן סימטרי נקבל כי $o(ab) \leq o(ba)$ (אותו הטיעון יעבוד כי ידוע כבר ש הסדר של ba סופי).

בסה"כ נקבל כי $o(ab) = o(ba)$.

במקרה ב': מ"ל כי גם הסדר של ba אינסופי. אבל, אם הסדר של ba סופי, כמו בסעיף הקודם, נובע כי גם הסדר של ab בסתירה להנחה. לכן $o(ba) = \infty = o(ab)$.

$$3.3 \quad \text{נניח כי } o(a) = n \text{ אזי } a^m = a^k \text{ עבור } m, k \in \mathbb{Z} \text{ אם ורק אם } m \equiv k \pmod{n}.$$

הוכחה: (\Leftarrow) נתון כי $a^m = a^k$. נכפול ב a^{-k} מימין ונקבל $a^{m-k} = e$. לפי סעיף 1, $n | m - k$ לכן $m \equiv k \pmod{n}$.

(\Rightarrow) נתון כי $m \equiv k \pmod{n}$ לכן, קיים $t \in \mathbb{Z}$ כך ש $m = k + tn$. מכיוון ש $a^n = e$ נקבל $a^m = a^{k+tn} = a^k (a^n)^t = a^k e^t = a^k$.

4. ענו על הסעיפים הבאים.

4.1 תהי $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_3 \right\}$ הוכיחו כי G חבורה ביחס לפעולת

כפל מטריצות, מצאו את הסדר של G ואת הסדר של כל איבר ב- G .

פתרון: G מוכלת ב- $GL_3(\mathbb{Z}_3)$ (חבורת המטריצות ההפיכות מסדר 3×3 מעל \mathbb{Z}_3). על מנת לראות שהיא ת"ח שלה (ובפרט חבורה) נשתמש בקריטריון המקוצר. ברור כי G לא ריקה. בדקו כי G סגורה לכפל ולהופכי.

הסדר של G הוא $3 \cdot 3 \cdot 3 = 27$ (כי יש שלוש אפשרויות לבחור את a , שלוש אפשרויות לבחור את b ושלוש – את c).

יהי $x = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in G$ מתקיים $x^3 = \begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix} \stackrel{a,b,c \in \mathbb{Z}_3}{=} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ לכן, לפי

תרגיל 3.1, $o(x) \mid 3$, לכן, $o(x) \in \{1, 3\}$.

לכן, הסדר של כל איבר ב G , למעט הזהות, הוא שלוש.

4.2 תהי G חבורה. אם לכל $a, b \in G$ מתקיים $(ab)^3 = a^3 b^3$ האם G אבלית?

לא. החבורה מסעיף א' מהווה דוגמה נגדית, שכן לכל $a, b \in G$ מתקיים $(ab)^3 = a^3 b^3 = e$ אך החבורה אינה אבלית.

5. קבעו אילו מהחבורות הבאות הן ציקליות? עבור החבורות הציקליות מצאו יוצר, אחרת הסבירו מדוע החבורה אינה ציקלית.

5.1 $\mathbb{Z}_{10} \times \mathbb{Z}_{15}$

5.2 $\mathbb{Z}_5 \times \mathbb{Z}_2$

5.3 U_{20}

פתרון:

1. אינה ציקלית כי אין איבר מסדר 150. אכן, לכל $(a, b) \in \mathbb{Z}_{10} \times \mathbb{Z}_{15}$ מתקיים:

$30(a, b) = (0, 0)$

2. החבורה ציקלית ונוצרת על ידי (1,1).
3. $U_{20} = \{1,3,7,9,11,13,17,19\}$ ולכן $|U_{20}| = 8$. החבורה אינה ציקלית שכן אין בה איבר מסדר 8 (בדקו!).

6. ענו על הסעיפים הבאים.

6.1 תהיינה H, G_1, G_2 תת-חבורות של G . הוכיחו: אם $H \subseteq G_1 \cup G_2$ אזי $H \subseteq G_1$ או $H \subseteq G_2$.

פתרון: תהי $H \subseteq G_1 \cup G_2$. נניח בשלילה שקיימים $t \in H \setminus G_1, h \in H \setminus G_2$ (מה שבפרט אומר $t \in G_1, h \in G_2$). מכיוון ש- $t, h \in H$ מתקיים $th \in H$ ולכן $th \in G_1 \vee th \in G_2$. נניח ש- $th \in G_1$, מכיון ש- $t \in G_1$ גם $t^{-1} \in G_1$ ולכן $t^{-1}(th) = (t^{-1}t)h = 1h = h \in G_1$ לסתירה במקרה בו $th \in G_2$.

6.2 מצאו דוגמה לחבורה G ולתת חבורות $H, G_1, G_2, G_3 \leq G$ כך ש- $H \subseteq G_1 \cup G_2 \cup G_3$ אבל H אינה מוכלת בשום איחוד מהצורה $G_i \cup G_j$.

פתרון: נתבונן ב- $G = Z_2 \times Z_2 \times Z_2$, ובתת החבורות

$$G_1 = \{0\} \times \square_2 \times \square_2 = \{(0,0,0), (0,1,0), (0,0,1), (0,1,1)\}$$

$$G_2 = \square_2 \times \{0\} \times \square_2 = \{(0,0,0), (1,0,0), (0,0,1), (1,0,1)\}$$

$$G_3 = \square_2 \times \square_2 \times \{0\} = \{(0,0,0), (1,0,0), (0,1,0), (1,1,0)\}$$

נגדיר: $H = \{(0,0,0), (0,1,1), (1,1,0), (1,0,1)\}$. קל לראות שזו אכן תת חבורה. מתקיים $H \subseteq G_1 \cup G_2 \cup G_3$, ושימו לב שהיא לב שהיא אכן אינה מוכלת באף איחוד של שניים.

7. תהי G חבורה. הוכיחו: אם לכל $x \in G$ מתקיים $x^2 = 1$ אזי G היא חבורה אבלית.

הוכחה: ידוע מהנתון שמתקיים: $(ab)^2 = a^2 = b^2 = 1$. אזי:

$$(ab)^2 = 1 = 1 \cdot 1 = a^2 \cdot b^2 \rightarrow abab = aabb$$

ונכפיל מימין בהופכי של b ונקבל: $ba = ab$. זה מתקיים לכל שני איברים בחבורה, ולכן החבורה היא אבלית.

8. תהי G חבורה. נסמן $m_2(G) = |\{x \in G : x^2 = 1\}|$, כלומר $m_2(G)$ הוא מספר הפתרונות של המשוואה $x^2 = 1$ בחבורה G .

8.1 הראו שבכל חבורה סופית G מתקיים $m_2(G) \equiv |G| \pmod{2}$;

8.2 הראו שבכל חבורה עם מספר זוגי של איברים קיים איבר מסדר 2.

רמז לסעיף א': הגדירו על G את יחס השקילות הבא:
 $(x = y \vee xy = 1) \Leftrightarrow x \equiv y$, ושימו לב שהאיברים שריבועם אינו 1 שייכים למחלקות שקילות בגודל 2.
 הערה: הרמז מציע דרך פתרון אלגנטית. כדאי שלפני זה תנסו להגיע לאיזשהו פתרון אינטואיטיבי על סמך הרעיונות שכבר ראינו בכיתה.

פתרון:

1. נגדיר את היחס המוצע ברמז. זהו אכן יחס שקילות (בדקו!). מה הן מחלקות השקילות? אם $a \in G$ מקיים $a^2 = 1$ אזי הוא הופכי לעצמו, כלומר, $a = a^{-1}$, ולכן $[a] = \{a\}$. אכן, אם היה איבר נוסף במחלקת שקילות זו, נניח

$$x \in [a], a \neq x \text{ אזי היה מתקיים } xa = 1 \text{ ואז } x = a^{-1} = a.$$

מחלקת השקילות של איבר היחידה היא מגודל 1: $[1] = \{1\}$.

מה לגבי שאר האיברים? אם $b \in G, b \neq 1$ אינו מסדר 2, אזי $[b] = \{b, b^{-1}\}$ (מדוע אין שם עוד איברים? כי ההופכי הינו יחיד).

כעת, האיחוד של כל מחלקות השקילות נותן את החבורה כולה, לכן

$$G = \{1\} \cup \left(\bigcup_{o(a)=2} [a] \right) \cup \left(\bigcup_{\substack{o(b) \neq 2 \\ b \neq 1}} [b] \right)$$

(שימו לב שזה איחוד זר!). נשים לב ש-

$$|G| = \left| \{1\} \cup \left(\bigcup_{o(a)=2} [a] \right) \cup \left(\bigcup_{\substack{o(b) \neq 2 \\ b \neq 1}} [b] \right) \right| = m_2(G) + 2k, \text{ ולכן } m_2(G) = \left| \{1\} \cup \left(\bigcup_{o(a)=2} [a] \right) \right|$$

כאשר k זה מספר מחלקות השקילות באיחוד $\bigcup_{\substack{o(b) \neq 2 \\ b \neq 1}} [b]$. מכיוון ש-

$$|G| = m_2(G) + 2k \text{ נקבל ש-} |G| \equiv m_2(G) \pmod{2}, \text{ כנדרש.}$$

2. תהא G חבורה עם מספר זוגי של איברים, נניח $2k$. נניח בשלילה שאין איבר מסדר 2, ולכן $m_2(G) = 1$. לפי הסעיף הקודם נקבל $1 \equiv 2k \pmod{2}$,

וזאת כמובן סתירה. לכן קיים ב- G איבר מסדר 2.

בהצלחה! 😊