פתרון תרגיל בית 7 בתורת החבורות
88-218 סמסטר א' תשפ"ב

שאלה 1 (חימום)**.** הכינו דגם מנייר של החבורה הדיהדרלית D_4.

שאלה 2. אפשר להעזר בדגם של D_n לבדיקות.

א. מצאו את כל תת־החבורות הלא טריוויאליות של D_4, והוכיחו שכולן אבליות. האם כולן ציקליות?

ב. הוכיחו לכל $m > 1$ כי $Z(D_{2m-1}) = \{\mathrm{id}\}$ ו-$Z(D_{2m}) = \langle\sigma^m\rangle$. רמז: איך נראה איבר כללי בחבורה דיהדרלית?

ג. כתבו את משוואת המחלקות של D_5 מבלי להתאמץ. כלומר חשבו את הגודל של כל מחלקות הצמידות ללא צורך בחישוב ישיר לכל איבר. רמז: הסעיף הקודם עם כך שגודל מחלקת צמידות מחלק את סדר החבורה.

פתרון.

א. נציג את החבורה בצורה הרגילה, כחבורה הנוצרת על ידי האיברים σ, סיבוב ב-$90°$ ו-τ, שיקוף לגבי ציר כלשהו של הריבוע. כלומר בייצוג עם יוצרים ויחסים:

$$D_4 = \left\langle \sigma, \tau \,\middle|\, \sigma^4 = \tau^2 = \mathrm{id}, \sigma\tau = \tau\sigma^{-1} \right\rangle$$

ידוע לנו כי $|D_4| = 8$. לפי משפט לגראנז' הסדרים האפשריים היחידים של תת־חבורות הם $\{1, 2, 4, 8\}$. הסדרים 1 ו-8 מתקבלים עבור תת־החבורות הטריוויאליות. המספר 2 הוא ראשוני, ולכן כל תת־חבורה מסדר זה חייבת להיות ציקלית, ונוצרת על ידי איבר מסדר 2. מסתבר שיש חמש תת־חבורות מסדר 2 והן

$$\left\langle \sigma^2 \right\rangle, \langle \tau \rangle, \langle \tau\sigma \rangle, \left\langle \tau\sigma^2 \right\rangle, \left\langle \tau\sigma^3 \right\rangle$$

יש גם שלוש תת־חבורות מסדר 4 שאותן מגלים על ידי בדיקה של זוגות של איברים מסדר 2 או 4 כקבוצות יוצרים. תת־החבורות הן

$$\langle \sigma \rangle, \left\langle \sigma^2, \tau \right\rangle = \left\{ \mathrm{id}, \sigma^2, \tau, \tau\sigma^2 \right\}, \left\langle \sigma^2, \tau\sigma^3 \right\rangle = \left\{ \mathrm{id}, \sigma^2, \tau\sigma^3, \tau\sigma \right\}$$

קל לראות שכל תת־החבורות הציקליות הן אבליות. לגבי תת־החבורות $\left\langle \sigma^2, \tau \right\rangle$ ו-$\left\langle \sigma^2, \tau\sigma^3 \right\rangle$ בדיקה ישירה תראה שהן אבליות (למשל על ידי טבלת כפל), אבל הן לא ציקליות כי אין בהן איבר מסדר 4.

ב. נתחיל בכך שנשים לב שכל איבר של D_n יכול להכתב בצורה $\tau^i\sigma^j$ כאשר $i \in \{0,1\}$ ו-$j \in \{0,1,\ldots,n-1\}$. מהיחס $\sigma\tau = \tau\sigma^{-1}$ אפשר בקלות לקבל את היחסים $\sigma^k\tau = \tau\sigma^{-k}$ לכל $k \in \mathbb{Z}$. כמו כן, מפני שהקבוצה $\{\sigma,\tau\}$ יוצרת את D_n, אז איבר $\alpha \in D_n$ נמצא במרכז אם ורק אם הוא מתחלף עם קבוצת היוצרים (ודאו שאתם מבינים למה זה נכון גם לחבורות אחרות!).
נניח $\alpha = \tau^i\sigma^j \in Z(D_n)$ בהצגה לעיל. דרשנו כי $\alpha\sigma = \sigma\alpha$, או במפורש $\tau^i\sigma^j\sigma = \sigma\tau^i\sigma^j$. אחרי כפל מימין ב-$\sigma^{-j}$ נקבל

$$\tau^i\sigma = \sigma\tau^i$$

וזה יתכן אם $i = 0$. אך זה לא ייתכן אם i אי זוגי, שהרי נקבל $\tau\sigma = \sigma\tau$ וידוע לנו שהם לא מתחלפים (עבור $n \geq 3$). כלומר האיברים שאנחנו מחפשים הם מן הצורה $\alpha = \sigma^j$. כעת נבדוק התחלפות עם τ, כלומר מתי $\alpha\tau = \tau\alpha$. זה יקרה אם $\sigma^j\tau = \tau\sigma^j$ ולפי היחסים שקיבלנו לעיל, זה שקול ל-$\tau\sigma^{-j} = \tau\sigma^j$, כלומר מתי $\sigma^{2j} = \mathrm{id}$. ידוע לנו כי $o(\sigma) = n$, אז התשובה היא רק כאשר $j = 0$ או $j = \frac{n}{2}$. זה בדיוק הפיצול לפי הזוגיות בשאלה.
קיבלנו שבמקרה ו-$n = 2m-1$ אי זוגי, אז $Z(D_{2m-1}) = \{\mathrm{id}\}$ ואם $n = 2m$ זוגי, אז $Z(D_{2m}) = \{\mathrm{id}, \sigma^m\}$. להשלמת התמונה, נשים לב כי החבורות D_1 ו-D_2 הן אבליות, ולכן המרכז שלהן הוא כל החבורה.

ג. הסכום במשוואת המחלקות הוא $|D_5| = 10$. הגודל של כל מחלקת צמידות מחלק את 10, ולפי הסעיף הקודם האיבר היחיד שמחלקת הצמידות שלו היא בגודל 1 הוא איבר היחידה (כי רק הוא ב-$Z(D_5)$). לכן בהכרח הגדלים של מחלקות הצמידות הם $1,2,2,5$, כי זו הדרך היחידה להציג את 10 כסכום של איברים מ-$\{1,2,5,10\}$ שמופיעה בה בדיוק פעם אחת 1.

שאלה 3. יהי p ראשוני, ותהי G חבורה מסדר p^3.

א. הוכיחו שניתן ליצור את G עם תת־קבוצה בת שלושה איברים $a,b,c \in G$ (כלומר $G = \langle a,b,c\rangle$). רמז: משפט לגראנז' כמה וכמה פעמים.

ב. בחרו p. תנו דוגמה מפורשת לחבורה G אבלית מסדר p^3 שאפשר ליצור עם שני איברים $a,b \in G$, אבל לא עם איבר אחד.

ג. רשות: הראו שישנה חבורה לא אבלית מסדר p^3 שאפשר ליצור עם שני איברים לפי ההדרכה הבאה: התבוננו בקבוצה (שכבר פגשנו מעל $\mathbb{R}$)

$$H(\mathbb{Z}_p) = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \middle| x,y,z \in \mathbb{Z}_p \right\}$$

ועל האיברים $a = \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), b = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. הראו כי $\left|\left\langle a, aba^{-1}b^{-1}\right\rangle\right| = p^2$, והסיקו מזה ש-$H(\mathbb{Z}_p) = \langle a,b\rangle$.

פתרון.

א. כמסקנה ממשפט לגראנז' אנחנו יודעים שהסדרים האפשריים של איברים ב-G הם $\{1,p,p^2,p^3\}$. אם קיים איבר $a \in G$ מסדר p^3, אז G ציקלית ומתקיים $G = \langle a\rangle$. לכן נוכל לבחור **כל** זוג איברים אחרים $b,c \in G$, ויתקיים

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

כלומר $G=\langle a,b,c\rangle$.
אם לא קיים איבר מסדר p^3, אבל קיים איבר $a\in G$ מסדר p^2, אבל תת־החבורה $\langle a\rangle$ מכילה p^2 איברים. לכן קיים איבר $e\neq b\in G\setminus\langle a\rangle$ והסדר שלו הוא לפחות p. לכן

$$|\langle a,b\rangle|\geq|\langle a\rangle\cup\{b\}|>|\langle a\rangle|=p^2$$

כי $b\notin\langle a\rangle$. אבל הסדר של $\langle a,b\rangle$ חייב לחלק את p^3, ולכן הוא בדיוק p^3. כך נוכל לבחור כל איבר נוסף $c\in G$ ונקבל

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

ושוב נקבל $G=\langle a,b,c\rangle$.
אם לא קיימים איברים מסדר p^3 או p^2, אז הסדר של כל האיברים הוא p, פרט לאיבר היחידה. יהי $a\in G$ איבר מסדר p. אז $|\langle a\rangle|=p$. נבחר $e\neq b\in G\setminus\langle a\rangle$ מסדר p (ודאו שברור לכם למה קיים b כזה). אז לפי לגראנז' הסדר של תת־החבורה $\langle a,b\rangle$ מחלק את $|G|=p^3$, ובנוסף הוא חייב להיות גדול מ-p, כי $|\langle a\rangle\cup\{b\}|=p+1$. לכן $|\langle a,b\rangle|\geq p^2$. אם $|\langle a,b\rangle|=p^3$, נסיים כמו מקודם. אחרת, $|\langle a,b\rangle|=p^2$ ונוכל לבחור $e\neq c\in G\setminus\langle a,b\rangle$ מסדר p ומטיעון דומה נסיק $G=\langle a,b,c\rangle$.

ב. עד כדי איזומורפיזם, אפשר לבחור רק את $\mathbb{Z}_{p^2}\times\mathbb{Z}_p$. למשל עבור $p=2$ נבחר את $G=\mathbb{Z}_4\times\mathbb{Z}_2$, ואת האיברים $a=(1,0)$, $b=(1,1)$. זה מתאים למקרה השני של הסעיף הקודם, שבו אין איבר מסדר p^3, אבל $o(a)=p^2$ ובחרנו את $b\neq(0,0)$ כך ש-$b\notin\langle a\rangle$.

ג. ברור שחבורה לא אבלית לא ניתן ליצור עם איבר אחד. לפי ההדרכה נחשב כי $aba^{-1}b^{-1}=\left(\begin{smallmatrix}1&0&1\\0&1&0\\0&0&1\end{smallmatrix}\right)$ (הוא גם איבר מסדר p). הכפל בחבורה מקיים

$$\begin{pmatrix}1&x&z\\0&1&y\\0&0&1\end{pmatrix}\begin{pmatrix}1&x'&z'\\0&1&y'\\0&0&1\end{pmatrix}=\begin{pmatrix}1&x+x'&xy'+z+z'\\0&1&y+y'\\0&0&1\end{pmatrix}$$

בתת־החבורה $\left\langle a,aba^{-1}b^{-1}\right\rangle$ ליוצרים יש במיקום $(2,3)$ רכיב 0, ולכן באינדוציה לכל איבר בתת־החבורה יש 0 במיקום $(2,3)$ (הראו שתת־החבורה איזומורפית ל-$\mathbb{Z}_p\times\mathbb{Z}_p$). אזי $b\notin\left\langle a,aba^{-1}b^{-1}\right\rangle$ ולפי הסעיף הראשון נסיק שהיא מסדר p^3. אבל $\left\langle a,aba^{-1}b^{-1}\right\rangle\subseteq\langle a,b\rangle$ ולכן a,b יוצרים את $H(\mathbb{Z}_p)$.

שאלה 4. תהי G חבורה ותהי $S\subseteq G$ תת־קבוצה לא ריקה. נגדיר את המְרַכֵּז של S ב-G להיות

$$C_G(S)=\{g\in G\,|\,\forall s\in S,gs=sg\}$$

זו הכללה למושג מְרַכֵּז של איבר $s\in G$ שבכיתה סימנו $C_G(s)$.

א. הוכיחו שאם $S\subseteq T\subseteq G$ תת־קבוצות, אז $C_G(T)\subseteq C_G(S)$.

ב. הוכיחו

$$C_G(S)=\bigcap_{s\in S}C_G(s)=\bigcap_{s\in\langle S\rangle}C_G(s)=C_G(\langle S\rangle)$$

והסיקו כי $C_G(S)\leq G$.

ג. תנו דוגמה לחבורה G ותת־קבוצה S כך ש-$|S| \geq 2$ וגם $S \subsetneqq C_G(S) \subsetneqq G$. רמז: אפשר להסתפק ב-$G = S_3$ (אבל לא חייבים!)

ד. תנו דוגמה לחבורה G ותת־קבוצה S כך ש-$|S| \geq 2$ וגם $C_G(S) \subsetneqq S \subsetneqq G$. רמז: אפשר להסתפק ב-$G = S_3$ (אבל לא חייבים!)

פתרון.

א. יהי $g \in C_G(T)$. אזי לכל $t \in T$ מתקיים $gt = tg$. מפני ש-$S \subseteq T$, אז בפרט לכל $t \in S$ מתקיים $gs = sg$. כלומר $g \in C_G(S)$, ולכן $C_G(T) \subseteq C_G(S)$.

ב. נתחיל בהוכחת $C_G(S) = \bigcap_{s\in S} C_G(s)$:

$$g \in C_G(S) \Leftrightarrow \forall s \in S, gs = sg \Leftrightarrow \forall s \in S, g \in C_G(s) \Leftrightarrow g \in \bigcap_{s\in S} C_G(s)$$

ראינו בכיתה כי $C_G(s)$ הוא תת־חבורה, והוכחתם שחיתוך תת־חבורות הוא תת־חבורה. לכן $C_G(S) \leq G$.
הוכחת $\bigcap_{s\in\langle S\rangle} C_G(s) = C_G(\langle S\rangle)$ נובעת ישירות מהחישוב הקודם כאשר מחליפים את S ב-$\langle S\rangle$ (שהרי גם $\langle S\rangle$ היא תת־קבוצה לא ריקה של G). מפני ש-$S \subseteq \langle S\rangle$, אז לפי הסעיף הקודם $C_G(\langle S\rangle) \subseteq C_G(S)$ ונותר לנו להוכיח את ההכלה בכיוון השני. יהי $g \in C_G(S)$, אזי הוא מתחלף עם כל איברי S. מכאן ש-g גם מתחלף עם כל חזקה של איברי S, כולל חזקות שליליות. יהי $s_1^{\pm1}\dots s_n^{\pm1} \in \langle S\rangle$ איבר כלשהו כאשר $s_1, \dots, s_n \in S$. אזי

$$gs_1^{\pm1}s_2^{\pm1}\dots s_n^{\pm1} = s_1^{\pm1}gs_2^{\pm1}\dots s_n^{\pm1} = \dots = s_1^{\pm1}\dots s_n^{\pm1}g$$

כי g מתחלף עם כל s_i או s_i^{-1}. לכן $g \in C_G(\langle S\rangle)$ וקיבלנו $C_G(S) = C_G(\langle S\rangle)$.

ג. יש אינסוף תשובות אפשרויות כאן. כדי להבטיח $S \subsetneqq C_G(S)$ צריך לדאוג שכל איברי S מתחלפים עם כל איברי S (אם S הייתה תת־חבורה היינו אומרים כי S אבלית). נבחר $G = S_3$. אז אפשר לבחור $S = \{(123), (132)\}$. נשים לב כי $\langle S\rangle = \langle(123)\rangle$, וחישוב קצר יראה כי $C_G(S) = \langle(123)\rangle \neq S_3$. לכן $S \subsetneqq C_G(S) \subsetneqq G$.

ד. גם כאן נבחר $G = S_3$. אפשר לבחור $S = \{(123), (12)\}$ או $S = S_3 \backslash \{\mathrm{id}\}$. במקרה זה $\langle S\rangle = G$. אז ראינו כי $C_G(S) = Z(G) = \{\mathrm{id}\}$. לכן $C_G(S) \subsetneqq S \subsetneqq G$.

שאלה 5. נאמר שפעולה של חבורה G על קבוצה X, כך ש-$|X| > 2$, היא 2-טרנזיטיבית אם לכל רביעיית איברים $x_1 \neq x_2 \in X$ ו-$y_1 \neq y_2 \in X$ קיים $g \in G$ כך ש-$g * x_1 = y_1$ וגם $g * x_2 = y_2$.
הערה: השאלה נראית יותר מפחידה ממה שהיא. בעיקר צריך להבין את ההגדרה.

א. הוכיחו שאם G פועלת 2-טרנזיטיבית על X אז היא גם פועלת טרנזיטיבית.

ב. הוכיחו כי G פועלת 2-טרנזיטיבית אם ורק אם G פועלת טרנזיטיבית על הקבוצה $X \times X \setminus \Delta$, כאשר $\Delta = \{(x, x) \,|\, x \in X\}$ והפעולה היא רכיב-רכיב.

ג. הוכיחו כי S_4 פועלת 2-טרנזיטיבית על הקבוצה $\{1, 2, 3, 4\}$.

ד. יהי F שדה, ונניח $|F| > 2$. הוכיחו שהחבורה $GL_2(F)$ פועלת טרנזיטיבית על $F^2 \setminus \{\binom{0}{0}\}$, אבל לא פועלת 2-טרנזיטיבית עליה.

פתרון.

א. לכל שני איברים $x,y \in X$ ניקח איבר $x \neq z \in X$ (קיים כזה לפי הדרישה על הגודל של X).
נתבונן בזוגות $x \neq y$ ו-$x \neq z$. מכיוון שהפעולה היא 2-טרנזיטיבית יש $g \in G$ כך ש-$g * x = y$ (וגם $g * z = x$ אבל זה לא חשוב).

ב. יהיו $(x_1, x_2), (y_1, y_2) \in X \times X \setminus \Delta$ כלומר $x_1 \neq x_2$ ו-$y_1 \neq y_2$. אם הפעולה של G היא 2-טרנזיטיבית, אז קיים $g \in G$ כך ש-$g * x_1 = y_1$ ו-$g * x_2 = y_2$. לכן

$$g * (x_1, x_2) = (g * x_1, g * x_2) = (y_1, y_2)$$

בכיוון השני, אם $x_1 \neq x_2$ ו-$y_1 \neq y_2$, אז $(x_1, x_2), (y_1, y_2) \in X \times X \setminus \Delta$ וקיים $g \in G$ כך ש-$g * (x_1, x_2) = (y_1, y_2)$. כלומר $g * x_i = y_i$.

ג. נסמן $X = \{1,2,3,4\}$. תהי $\sigma \in S_4$. הפעולה של σ על $i \in X$ היא $\sigma * i = \sigma(i)$.
לכל $(i,j), (k,l) \in X \times X \setminus \Delta$ אם $|\{i,j,k,l\}| = 4$ (כלומר כולם שונים), נבחר $\sigma = (ik)(jl) \in S_4$ ואז

$$\sigma * (i,j) = (\sigma(i), \sigma(j)) = (k,l)$$

אם $|\{i,j,k,l\}| = 3$ (כלומר יש בזוגות $(i,j), (k,l)$ איבר משותף אחד), אז בלי הגבלת הכלליות $i = k$ או $i = l$ וקיים $m \notin \{i,j,k,l\}$. אם $i = k$, נבחר את $\sigma = (jlm)$, ואם $i = l$ נבחר את $\sigma = (ikm)$.
לסיום, אם $|\{i,j,k,l\}| = 2$, אז יש שתי אפשרויות: או ש-$i = k, j = l$, ונבחר את $\sigma = \mathrm{id}$, או ש-$i = l, j = k$ ונבחר את $\sigma = (ij)(mm')$ עבור $m, m' \notin \{i,j,k,l\}$.
שימו לב שלכל $n \geq 4$ ניתן להרחיב הוכחה זו לכך ש-A_n פועלת 2-טרנזיטיבית על $\{1,2,\ldots,n\}$, ולא רק S_n.

ד. בשביל טרנזיטיביות, מספיק להראות שיש וקטור שהמסלול שלו הוא כל $F^2 \setminus \{\left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)\}$.
נראה זאת עבור הוקטור $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$. יהי $v \in F^2 \setminus \{\left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)\}$ וקטור כלשהו, ונשלים אותו לבסיס (אפשר, כי הוא לא אפסי) $\{v, w\}$.
ידוע ממשפט ההגדרה (מאלגברה לינארית) שקיימת העתקה לינארית שמעבירה את $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ ל-v ואת $\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ ל-w. מכיוון ש-$\{v, w\}$ הוא בסיס אז ההעתקה הזו היא הפיכה, ולכן המטריצה המייצגת שלה תהיה מ-$GL_2(F)$.
אגב, אפשר להראות שאפילו $SL_2(F)$ פועלת טרנזיטיבית על $F^2 \setminus \{\left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)\}$. נסו למצוא מטריצות מפורשות.
הפעולה היא לא 2-טרנזיטיבית, כי אי אפשר לשלוח שני וקטורים תלויים לינארית לשני וקטורים שאינם תלויים לינארית. למשל עבור $\alpha \neq 0,1$ (קיים α כזה כי $|F| > 2$), נבחר את $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) \neq \left(\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right)$ ואת $\left(\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right) \neq \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$. אז אין מטריצה A כך ש-$A\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) = \left(\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right)$ וגם $A\left(\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ שכן

$$A\left(\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right) = \alpha \cdot A\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) = \left(\begin{smallmatrix}\alpha^2\\0\end{smallmatrix}\right) \neq \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$$

שאלה 6. עבור כל אחת מן ההעתקות הבאות קבעו והוכיחו האם היא הומומורפיזם, מונומורפיזם, אפימורפיזם או איזומורפיזם.

א. $f\colon \mathbb{C}^* \to \mathbb{C}^*$ המוגדרת לפי $f(x) = x^{-3}$.

ב. $f\colon \mathbb{Q}^* \to \mathbb{Q}^*$ המוגדרת לפי $f(x) = x^2$.

ג. $f\colon \mathbb{R}^* \to \mathbb{R}^+$ המוגדרת לפי $f(x) = x^4$ כאשר $\mathbb{R}^+$ זו חבורת המספרים הממשיים החיוביים עם כפל רגיל.

ד. $f\colon S_7 \to \mathbb{Z}$ המוגדרת לפי $f(\sigma) = \sigma(1)$.

ה. $f_x\colon G \to G$ המוגדרת לפי $f_x(g) = xgx^{-1}$ כאשר G חבורה ו-$x \in G$ איבר.

ו. $f\colon \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_n$ המוגדרת לפי $f(k) = ([k], [k])$.

ז. $f\colon \mathbb{Z} \to \mathbb{Z}_3 \times \mathbb{Z}_6$ המוגדרת לפי $f(n) = (n \bmod 3,\, n \bmod 6)$.

פתרון. ההוכחות כאן לא מלאות!

א. הפונקציה היא אפימורפיזם, אבל לא מונומורפיזם. למשל $f(1) = f(e^{\frac{2\pi i}{3}}) = 1$.

ב. הפונקציה f היא הומומורפיזם. אבל היא לא מונומורפיזם כי למשל $f(1) = f(-1) = 1$. היא גם לא אפימורפיזם, כי למשל $-1 \notin \operatorname{im} f$, שהרי לכל $x \in \mathbb{Q}^*$ מתקיים $x^2 > 0$.

ג. הפונקציה f היא הומומורפיזם, באופן דומה לסעיף הקודם. אבל היא לא מונומורפיזם, שוב, כי למשל $f(1) = f(-1) = 1$. הפעם היא כן אפימורפיזם, כי לכל $x \in \mathbb{R}^+$ קיים שורש רביעי $\sqrt[4]{x} \in \mathbb{R}^*$ שהוא ממשי שאינו אפס, ואז $f(\sqrt[4]{x}) = x$.

ד. הפונקציה הזו היא לא הומומורפיזם. למשל

$$f(\mathrm{id} \cdot \mathrm{id}) = 1 \neq 1 + 1 = f(\mathrm{id}) + f(\mathrm{id})$$

ה. הפונקציה הזו היא איזומורפיזם. סוג כזה של איזומורפיזם נקרא אוטומורפיזם פנימי. נראה שאכן מדובר בהומומורפיזם:

$$f_x(gh) = xghx^{-1} = xgx^{-1}xhx^{-1} = f_x(g)f_x(h)$$

נוכיח שהגרעין טריוויאלי בכדי לראות ש-f_x הוא חח"ע. אם $xgx^{-1} = e$, אז $g = x^{-1}ex$ ולכן $g = e$. כלומר $\ker f_x = \{e\}$. כדי להראות ש-f_x הוא על, לכל $h \in G$ נתבונן באיבר $x^{-1}hx$, שהוא אכן מקור עבורו כי $f_x(x^{-1}hx) = h$.

ו. פונקציה זו היא אכן הומומורפיזם. עם זאת, היא לא אפימורפיזם (אלא אם $n = 1$ ואז זה ברור. לאיבר $([0], [1])$ למשל אין מקור) ולא מונומורפיזם (למשל $f(k) = f(k+n)$).

ז. הפונקציה היא הומומורפיזם, כשההוכחה מסתמכת על כך שחיבור מודולו n מוגדר היטב. היא לא מונומורפיזם, כי הסדר של המקור גדול ממש מסדר התמונה, או למשל כי $f(0) = f(6) = ([0], [0])$. היא לא אפימורפיזם, כי $\mathbb{Z}$ ציקלית ואילו $\mathbb{Z}_3 \times \mathbb{Z}_6$ לא ציקלית, וכל התמונות של חבורה ציקלית הן ציקליות. אפשר גם להוכיח ישירות כי למשל $(1, 3) \notin \operatorname{im} f$: אם n נשלח ל-$(1, 3)$, אז לפי הרכיב השני $n \equiv 3 \pmod 6$, ונסיק $n \equiv 0 \pmod 3$. לא יתכן שבאותו הזמן גם $n \equiv 1 \pmod 3$.

שאלה 7. הוכיחו שאם G חבורה נוצרת סופית ויש הומומורפיזם $f : G \to H$ אז $\operatorname{im}(f)$ נוצרת סופית.

פתרון. נניח ש-G נוצרת על ידי $\{g_1, ..., g_n\}$. זה אומר שכל איבר ב-G הוא מהצורה $\prod_i g_i^{k_i}$ כאשר ה-g_i-ים לא בהכרח שונים (למשל, יש איבר $g_1^3 g_2^{-1} g_1$). נוכיח ש-$\mathrm{im}(f)$ נוצרת על ידי $\{f(g_1), ..., f(g_n)\}$: אכן, לכל $h \in \mathrm{im}(f)$,

$$h = f(g) = f\big(\prod_i g_i^{k_i}\big) = \prod_i f(g_i)^{k_i}$$

כשהמעבר האחרון מסתמך על כך ש-f הומומורפיזם (ואינדוקציה).

שאלה 8. תהי G חבורה. נגדיר $f\colon G \to G$ לפי $f(g) = g^2$.

א. הוכיחו שהפונקציה f היא הומומורפיזם אם ורק אם G אבלית.

ב. נניח שהחבורה G אבלית וסופית. הוכיחו שהפונקציה f היא איזומורפיזם אם ורק אם הסדר של G הוא אי-זוגי.

פתרון.

א. הוכחתם את הטענה הזו בשפה אחרת בתרגיל הבית השני! לכיוון הראשון, נניח שהחבורה G אבלית. יהיו $g, h \in G$. לכן

$$f(gh) = (gh)^2 = ghgh \underbrace{=}_{\text{אבליות}} gghh = g^2h^2 = f(g)f(h)$$

ולכן f הומומורפיזם. לכיוון השני, נניח ש-f הומומורפיזם. לכל $g, h \in G$ מתקיים $f(gh) = (gh)^2 = ghgh$ וגם $f(gh) = f(g)f(h) = g^2h^2$, כלומר $g^2h^2 = ghgh$. נצמצם ונקבל: $gh = hg$, כלומר G אבלית.

ב. לכיוון הראשון, נניח שהחבורה מסדר אי-זוגי. מכיוון שהפונקציה היא הומומורפיזם (לפי הסעיף הראשון) והחבורה סופית, מספיק להראות שהפונקציה חח"ע. לשם כך יש להסביר מדוע הגרעין הוא טריוויאלי. נניח בשלילה שקיים $g \in \ker f$ המקיים $g \neq e_G$. מהגדרת הפונקציה, $e_G = f(g) = g^2$, ולכן הסדר של g הוא 2. הסדר של g מחלק את הסדר של החבורה ולכן הסדר של החבורה הוא זוגי בסתירה להנחה. בכיוון השני, נניח כי f היא איזומורפיזם. נניח בשלילה שהסדר של החבורה הוא זוגי, לכן יש איבר מסדר 2 (כפי שראינו בתרגול) ולכן f אינה חח"ע, כי האיבר הזה ואיבר היחידה שניהם בגרעין, שזו סתירה.

שאלות רשות

את שאלות הרשות אין חובה לפתור, אבל אם פתרתם אותן, בבקשה שלחו לנו את הפתרון שלהן.

שאלה 9. כהמשך לתוכנה שמקבלת כקלט רשימת מספרים המייצגת תמורה, הוסיפו לה פונקציה המחשבת את גודל מחלקת הצמידות של תמורה ב-S_n, ופונקציה המחשבת את סדר המְרַכֵּז שלה.

שאלה 10. יהי $\Psi\colon \mathcal{L} \to \mathcal{L}$ אופרטור מקבוצה סדורה חלקית $(\mathcal{L}, \leq)$ לעצמה.

א. הוכיחו שאם Ψ מקיים את שני התנאים:

- לכל $A, B \in \mathcal{L}$, אם $A \le B$ אז $\Psi(B) \le \Psi(A)$.
- לכל $A \in \mathcal{L}$ מתקיים $A \le \Psi^2(A)$.

אז $\Psi^3 = \Psi$. כלומר שלכל $A \in \mathcal{L}$ מתקיים $\Psi(\Psi(\Psi(A))) = \Psi(A)$.

ב. הסיקו שלכל תת־חבורה $H \le G$ מתקיים $C_G(C_G(C_G(H))) = C_G(H)$.

בהצלחה!