פתרון תרגיל בית 7 במבנים אלגבריים
89-214 סמסטר א' תשע"ו

הוראות בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך הגשת התרגיל הוא לתרגול בשבוע המתחיל בתאריך א' טבת ה'תשע"ו, 13.12.2015.

שאלה 1. חשבו בשיטה של חישוב חזקה בעזרת ריבועים את הביטויים הבאים. מותר להשתמש במחשבון (כולל בפונקציית המודולו) לחישובי הביניים, שאותם תפרטו:

א. $2790^{2753} \in \mathbb{Z}_{3233}$. רמז: בתרגול ראיתם שהתוצאה הסופית היא ההודעה שבוב רצה לשלוח לאליס.

ב. $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^9 \in GL_2(\mathbb{Z}_{1000})$.

פתרון. א. נחשב ש-$2753 = 101011000001_2$. לכן נשתמש באותו תהליך שראינו בכיתה, כשכל המשוואות הן מודולו 3233:

$$\begin{aligned}
2790^1 &= 2790 \\
2790^2 &= 2269 \\
2790^4 &= 1425 \\
2790^5 &= 2393 \\
2790^{10} &= 806 \\
2790^{20} &= 3036 \\
2790^{21} &= 3213 \\
2790^{42} &= 400 \\
2790^{43} &= 615 \\
2790^{86} &= 3197 \\
2790^{172} &= 1296 \\
2790^{344} &= 1689 \\
2790^{688} &= 1215 \\
2790^{1376} &= 1977 \\
2790^{2752} &= 3065 \\
2790^{2753} &= 65
\end{aligned}$$

וזה פענוח ההודעה $m = 65$ שבוב שלח לאליס.

ב. נסמן $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. נחשב ש-$9 = 1001_2$, ולכן עלינו לחשב למעשה את

$$A^9 = A \cdot \left(\left((A)^2 \right)^2 \right)^2$$

ובחישוב מלא, כשכל המשוואות הן מודולו 1000:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^1 = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^2 = \begin{pmatrix} 7 & 10 \\ 15 & 22 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^4 = \begin{pmatrix} 199 & 290 \\ 435 & 634 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^8 = \begin{pmatrix} 751 & 570 \\ 355 & 106 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^9 = \begin{pmatrix} 461 & 782 \\ 673 & 134 \end{pmatrix}$$

שאלה 2. עבור כל אחת מן ההעתקות הבאות קבעו והוכיחו האם היא הומומורפיזם, מונומורפיזם, אפימורפיזם או איזומורפיזם.

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

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

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

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

ב. הפונקציה הזו היא לא הומומורפיזם. למשל

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

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

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

כדי לראות ש-f_x הוא חח"ע נשים לב שאם $xgx^{-1} = e$, אז $g = x^{-1}ex$ ולכן $g = e$. כדי להראות ש-f_x הוא על, יהי $h \in G$. נבחר בתור המקור שלו את $x^{-1}hx$, ואכן $f_x(x^{-1}hx) = h$.

שאלה 3. יהי $f : G \to H$ הומומורפיזם.

א. הוכיחו שאם G אבלית, אז $\mathrm{im}\, f$ תת־חבורה אבלית.

ב. הסיקו מהסעיף הקודם שאם $G \cong H$, אז G אבלית אם ורק אם H אבלית.

ג. הוכיחו או הפריכו: קיים אפימורפיזם $\varphi : D_8 \to U_{17}$.

פתרון. א. אנחנו יודעים כי $\operatorname{im} f \leq H$. נותר להראות שהיא אבלית. יהיו $h_1, h_2 \in \operatorname{im} f$. אז ישנם איברים g_1, g_2 כך שמתקיים $f(g_1) = h_1, f(g_2) = h_2$. מפני שנתון ש-$G$ אבלית יתקיים גם

$$h_1 h_2 = f(g_1)f(g_2) = f(g_1 g_2) = f(g_2 g_1) = f(g_2)f(g_1) = h_2 h_1$$

ולכן כל זוג איברים ב-$\operatorname{im} f$ מתחלף.

ב. אם חבורות הן איזומורפיות, אז יש בינהן איזומורפיזם. נניח $\phi : G \to H$ הוא איזומורפיזם. לכן ϕ הוא על, כלומר $\operatorname{im}\phi = H$. אם G היא אבלית, אז גם H היא אבלית לפי הסעיף הקודם. באופן דומה יש איזומורפיזם $\phi^{-1} : H \to G$ ולכן אם H אבלית, אז גם G אבלית.

ג. שתי החבורות הן מסדר 16. לכן אם קיימת פונקציה על בינהן, אז היא גם חח"ע. כלומר אילו קיים φ אפימורפיזם כזה, אז זה איזומורפיזם. אבל D_8 לא אבלית ואילו U_{17} היא אבלית ולפי הסעיף הקודם נגיע לסתירה.

שאלה 4. בכל סעיף קבעו ונמקו האם החבורות איזומורפיות. רמז כללי: סדרים של איברים.

א. החבורה $\mathbb{C}^*$ והחבורה

$$G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{R}) : a^2 + b^2 > 0 \right\}$$

עם הפעולה של כפל מטריצות (שכבר הראיתם שהיא חבורה).

ב. החבורה $\mathbb{Z}_{60}$ והחבורה $\mathbb{Z}_6 \times \mathbb{Z}_{10}$.

ג. החבורה $\mathbb{Z}_{33}$ והחבורה $\mathbb{Z}_3 \times \mathbb{Z}_{11}$.

ד. החבורה S_4 והחבורה $\mathbb{Z}_2 \times A_4$.

ה. החבורה S_5 והחבורה D_{60}.

פתרון. א. החבורות איזומורפיות. נגדיר את האיזמורפיזם $\varphi : G \to \mathbb{C}^*$ לפי $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \mapsto a + bi$. ברור כי זו העתקה חח"ע ועל (מי היא ההעתקה ההופכית?). נשאר להראות כי זהו הומומורפיזם של חבורות: יהיו איברים $M_1, M_2 \in G$ ונרצה להראות כי $\varphi(M_1 M_2) = \varphi(M_1)\varphi(M_2)$. נניח כי

$$M_1 = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad M_2 = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

ועל ידי חישוב ישיר נקבל את הדרוש:

$$\varphi(M_1 M_2) = \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}\right)$$
$$= ac - bd + (ad+bc)i = (a+bi)(c+di) = \varphi(M_1)\varphi(M_2)$$

ב. החבורות הן לא איזומורפיות. בחבורה $\mathbb{Z}_{60}$ יש איבר מסדר 60, ואילו בחבורה $\mathbb{Z}_6 \times \mathbb{Z}_{10}$ הסדר המירבי של איבר הוא 30.

ג. החבורות איזומורפיות. אפשר לראות ששתיהן ציקליות, למשל $\mathbb{Z}_{33} = \langle 1 \rangle$ ו-$\mathbb{Z}_{11} \times \mathbb{Z}_3 = \langle (1,1) \rangle$, ואנחנו יודעים שמכל סדר יש רק חבורה ציקלית אחת עד כדי איזומורפיזם. בכיתה הראנו איזומורפיזם בין חבורות כאלו, ספציפית

$$f : \mathbb{Z}_{33} \to \mathbb{Z}_{11} \times \mathbb{Z}_3$$
$$x \mapsto (x \,(\mathrm{mod}\, 11), x \,(\mathrm{mod}\, 3))$$

ד. החבורות לא איזומורפיות. ראינו בכיתה שהסדרים האפשריים של איברים ב-S_4 הם $1,2,3,4$. בחבורה $\mathbb{Z}_2 \times A_4$ יש איברים מסדר 6, כמו למשל $((1),(123))$. למי שהחישוב אינו ברור, הזכרו מה הוא הסדר של איבר במכפלה קרטזית.

ה. החבורות לא איזומורפיות. ראינו בכיתה שהסדרים האפשריים של איברים ב-S_5 הם $1,2,\ldots,6$. בחבורה D_{60} יש איברים מסדר 60, כמו למשל σ.

שאלה 5. מצאו העתקות לפי התנאים הנתונים:

א. מצאו שיכון $f : A_4 \to S_6$.

ב. מצאו שיכון $f : S_5 \hookrightarrow S_6$ עבורו $f((1\ 2\ 3\ 4\ 5)) \neq (1\ 2\ 3\ 4\ 5)$.

ג. מצאו הומומורפיזם לא טריוויאלי $f : \mathbb{Z}_8 \to D_4$ (נאמר שהומומורפיזם $\varphi : G \to H$ הוא טריוויאלי אם הוא שולח את כל איברי G אל e_H). למה הוא לא אפימורפיזם?

ד. מצאו אפימורפיזם $f : \mathbb{Z}_{200} \times 2\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_4$.

פתרון. א. אנו יכולים לראות את S_n כתת־חבורה של S_{n+1} לפי השיכון הסטנדרטי, השולח תמורה σ של n איברים לתמורה $\hat{\sigma}$ של $n+1$ איברים לפי $\hat{\sigma}(i) = \sigma(i)$ לכל $1 \leq i \leq n$ ומקבע את האיבר האחרון $\hat{\sigma}(n+1) = n+1$. לפי נקודת מבט זו, פשוט נבחר את השיכון $\sigma \mapsto \sigma$, כאשר המספרים $5,6$ נשלחים לעצמם. קל לראות שזה אכן שיכון (למעשה מצאנו תת־חבורה של S_6 שאיזומורפית ל-A_4).

ב. בדומה לסעיף הקודם, הפעם אפשר לבחור להעביר את $\sigma \in S_5$ לתמורה ב-$S_{\{2,\ldots,6\}}$, וזו חבורה המשוכנת ב-S_6. כלומר נגדיר $f : S_5 \to S_6$ לפי זה ש-σ תעבור לתמורה $f(\sigma)(i) = \sigma(i-1)+1$ עבור $2 \leq i \leq 6$ ועבור $i = 1$, $f(\sigma)(1) = 1$. בפרט $f((1\ 2\ 3\ 4\ 5)) = (2\ 3\ 4\ 5\ 6)$.
באופן יותר כללי אפשר להפעיל אוטומורפיזם של S_5 שלא מקבע את $(1\ 2\ 3\ 4\ 5)$, ואז לשכן את התוצאה ב-S_6. אפשר גם לשכן את S_5 ב-S_6 באופן הטבעי כמו בסעיף הקודם ואז להפעיל אוטומורפיזם של S_6 שלא מקבע את $(1\ 2\ 3\ 4\ 5)$. באיזה מן הדרכים יש לנו יותר אפשרויות?
נעיר שרבים ענו בעזרת שאלה 2. כל מה שצריך זה לשכן את S_5 ב-S_6 באופן טבעי, ואז לבחור $x \in S_6$ שלא מתחלף עם $(1\ 2\ 3\ 4\ 5)$ עבור אוטומורפיזם פנימי.

ג. אנחנו כבר מכירים את תת־החבורות של D_4. התמונה של f חייבת להיות ציקלית, כי $\mathbb{Z}_8$ ציקלית. אפשר לבחור כל תת־חבורה ציקלית של D_4 ולמצוא הומומורפיזם אליה מ-$\mathbb{Z}_8$. למשל $\langle\sigma\rangle = \{\sigma^i : i \in \mathbb{Z}_4\} \leq D_4$. ההומורפיזם שנבחר יהיה

$$\begin{aligned} f : \mathbb{Z}_8 &\to D_4 \\ a &\mapsto \sigma^{a(\bmod 4)} \end{aligned}$$

קל להראות שזה הומומורפיזם לא טריוויאלי. זה לא אפימורפיזם, ולא יתכן שיהיה אפימורפיזם, כי החבורות הן סופיות ומאותו סדר, ולכן יהיה מדובר באיזומורפיזם. אבל $\mathbb{Z}_8$ אבלית ואילו D_4 לא אבלית, וכבר ראינו שזה לא ייתכן.

ד. אפשר למצוא אפימורפיזם $\phi_1 : \mathbb{Z}_{200} \to \mathbb{Z}_4$ ואפימורפיזם $\phi_2 : 2\mathbb{Z} \to \mathbb{Z}$, ובעזרתם למצוא את האפימורפיזם המבוקש:

$$\begin{aligned} f : \mathbb{Z}_{200} \times 2\mathbb{Z} &\to \mathbb{Z} \times \mathbb{Z}_4 \\ (x,y) &\to (y/2, x\,(\mathrm{mod}4)) \end{aligned}$$

שאלה 6 (רשות)**.** תהי G חבורה ויהיו $x, y \in G$ איברים. נתון כי $|G| = 22$, $x \neq e$ וגם ש-y אינו חזקה של x. הוכיחו כי $G = \langle x, y\rangle$. אתגר: הוכיחו כי $G \cong D_{11}$.

פתרון. נסמן $H = \langle x, y \rangle$. לפי משפט לגראנז' מתקיים כי $|H| \,|\, 22$. נפסול את כל הסדרים שקטנים מ-22. ברור כי $|H| \neq 1$ מפני ש-$x \in H$ וגם $x \neq e$. בנוסף $y \in H$ והוא אינו חזקה של x, בפרט $y \neq e = x^0$. כלומר $|H| \neq 2$. נניח בשלילה כי $|H| = 11$. אז נקבל כי $o(x) = 11$, לכן H ציקלית, ולכן y חזקה של x, שזו סתירה לנתון. כלומר $|H| = 22$ ואפשרות היחידה היא $H = G$.

שאלה 7 (אתגר רשות)**.** תהי G חבורה סופית, ויהי α אוטומורפיזם של G השולח יותר משלושת רבעי G להופכי שלהם. כלומר

$$\left|\left\{x : \alpha(x) = x^{-1}\right\}\right| > \frac{3\,|G|}{4}$$

הוכיחו כי $\alpha(x) = x^{-1}$ לכל $x \in G$.

פתרון. נגדיר את הקבוצה $S = \left\{x \in G : \alpha(x) = x^{-1}\right\}$. נראה שהיא סימטרית, כלומר שאם $x \in S$, אז $x^{-1} \in S$, ואכן

$$\alpha(x^{-1}) = \alpha(x)^{-1} = x$$

נבחר $s \in S$ כלשהו (הקבוצה S לא ריקה, למשל $e \in S$) ונגדיר שלוש קבוצות

$$T = \{t \in G | t, st \in S\}, \qquad U_1 = \{t \in G | t \in S\}, \qquad U_2 = \{t \in G | st \in S\}$$

קל לראות כי $T = G \setminus (U_1 \cup U_2)$. לכן

$$|T| = |G| - |U_1| - |U_2| + |U_1 \cap U_2|$$
$$|T| > |G| - \frac{1}{4}\,|G| - \frac{1}{4}\,|G| = \frac{1}{2}\,|G|$$

איבר היחידה $e \in T$ כי $e, se = s \in S$. אם $t \in T$, אז

$$st = \left((st)^{-1}\right)^{-1} = \alpha\left((st)^{-1}\right) = \alpha(t^{-1}s^{-1}) = \alpha(t^{-1})\alpha(s^{-1}) = ts$$

ולכן $t \in C_G(s)$. לכן $T \subseteq C_G(s)$. מפני ש-$C_G(s) \leq G$ וגם $|T| > \frac{1}{2}\,|G|$, נקבל כי $C_G(s) = G$, ולכן $s \in Z(G)$. החישוב נכון לכל $s \in S$, ולכן $|Z(G)| > \frac{3}{4}\,|G|$. בהכרח $Z(G) = G$, כלומר G אבלית.

לכן לכל $s, t \in S$ נקבל כי

$$\alpha(st) = \alpha(s)\alpha(t) = s^{-1}t^{-1} = t^{-1}s^{-1} = (st)^{-1}$$

כלומר S סגורה תחת כפל (וראינו שהיא סגורה להופכי), ולכן היא תת־חבורה של G. מכיוון שגודלה הוא יותר מחצי G, נקבל $S = G$, שזה מה שרצינו להוכיח.

בהצלחה!