פתרון תרגיל בית 4 בתורת החבורות

88-218 סמסטר א' תשע"ט

שאלות חימום

שאלות החימום הן שאלות קלות יותר בדרך כלל, אבל כדאי מאוד לוודא שיודעים איך לפתור אותן, אפילו בעל פה.

1. תארו את כל המחלקות השמאליות ב-$\mathbb{Z}_{30}/\left\langle 3\right\rangle$.

פתרון:

האיבר 3 הוא מסדר 10, ולכן $\left|\left\langle 3\right\rangle\right|=10$. לפי משפט לגראנז' נקבל

$$\left|\mathbb{Z}_{30}/\left\langle 3\right\rangle\right|=\frac{\left|\mathbb{Z}_{30}\right|}{\left|\left\langle 3\right\rangle\right|}=\frac{30}{10}=3$$

והמחלקות, עד כדי בחירת נציגים, הן $\left\{\left\langle 3\right\rangle, 1+\left\langle 3\right\rangle, 2+\left\langle 3\right\rangle\right\}$.

2. מצאו איבר מסדר 6 בחבורה S_5. רמז: מצאו איבר מסדר 2 ב-S_2 ואיבר מסדר 3 ב-S_3.

פתרון: האיברים מסדר 6 בחבורה S_5 הם בדיוק התמורות שניתן לרשום כמכפלה של מחזורים זרים מאורך 2 ומאורך 3. למשל התמורה $(12)(345)$.

שאלות רגילות

1. רמז: הסעיפים הבאים דורשים קצת קומבינטוריקה.

(א) מצאו כמה איברים מסדר 6 יש בחבורה S_6.

(ב) מצאו כמה איברים מסדר 2 יש בחבורה S_6.

פתרון:

(א) כל תמורה ניתן להציג כמכפלת מחזורים זרים, והסדר של התמורה יהיה הכמ"מ (lcm) של אורכי המחזורים בהצגה זו. הסבירו מדוע ב-S_6 ניתן לקבל כמ"מ 6 בשני אופנים בדיוק: מחזורים מאורך 6 $(a_1,\ldots,a_6)$ שישנם $\binom{6}{6}(6-1)!=5!=120$ כאלו; ומכפלה של מחזור מאורך 3 עם חילוף $(a_1,a_2)(a_3,a_4,a_5)$ ויש $\binom{6}{2}\binom{6-2}{3}(3-1)!=120$ כאלו. בסך הכל יש 240 איברים מסדר 6.

ודאו שאתם מבינים את החישובים הקומבינטוריים לעיל ויודעים כיצד להגיע אליהם.

(ב) באופן דומה לסעיף הקודם, כאן יהיו לנו שלושה סוגי איברים מסדר 2: חילופים, מכפלה של שני חילופים ומכפלה של שלושה חילופים. בסך הכל ישנם

$$\binom{6}{2}+\binom{6}{2}\binom{4}{2}\frac{1}{2!}+\binom{6}{2}\binom{4}{2}\binom{2}{2}\frac{1}{3!}=15+45+15=75$$

איברים מסדר 2 בחבורה S_6.

2. לכל תמורה σ מהתמורות הבאות, כתבו את σ כמכפלת מחזורים זרים וחשבו את σ^2, את σ^{20} ואת $o(\sigma)$.

(א) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 2 & 9 & 7 & 1 & 6 & 4 & 3 & 8 \end{pmatrix} \in S_9$.

(ב) $(1\ 2)\,(2\ 5\ 4)\,(3\ 1\ 4)\,(1\ 5) \in S_5$

פתרון:

(א) נסמן את התמורה הנתונה σ. מפרקים לפי הדרך שראינו בתרגול. מקבלים כי יש את המעגלים הבאים:

$$1 \mapsto 5 \mapsto 1,\ 3 \mapsto 9 \mapsto 8 \mapsto 3,\ 4 \mapsto 7 \mapsto 4$$

לכן $\sigma = (1\ 5)\,(3\ 9\ 8)\,(4\ 7)$ (2 ו־6 נשלחים כל אחד לעצמו).

נחשב את σ^2 בעזרת העובדה שמחזורים זרים מתחלפים זה עם זה, ונקבל:

$$\sigma^2 = (1\ 5)^2\,(3\ 9\ 8)^2\,(4\ 7)^2 = (3\ 8\ 9)$$

הסדר של תמורה בהצגה כמכפלת מחזורים זרים היא הכמ"מ של אורכי המחזורים. אצלנו $o(\sigma) = [2,3,2] = 6$. לכן $\sigma^6 = \mathrm{id}$. מכאן קל לחשב

$$\sigma^{20} = \left(\sigma^6\right)^3 \sigma^2 = \mathrm{id}^3 \cdot \sigma^2 = (3\ 8\ 9)$$

(ב) נסמן את התמורה הנתונה σ. נכתוב אותה כמטריצה:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix}$$

לכן קל לראות שיש פה מעגל אחד, כלומר $\sigma = (1\ 4\ 3\ 2\ 5)$. נחשב את σ^2:

$$\sigma^2 = (1\ 4\ 3\ 2\ 5)^2 = (1\ 3\ 5\ 4\ 2)$$

סדר של מחזור הוא אורכו, ולכן $o(\sigma) = 5$. לכן $\sigma^5 = \mathrm{id}$ ונקבל $\sigma^{20} = \left(\sigma^5\right)^4 = \mathrm{id}$.

3. תהי $\sigma \in S_n$ תמורה, ויהי מחזור $a = (a_1, a_2, \ldots, a_k) \in S_n$. הוכיחו כי

$$\sigma a \sigma^{-1} = \sigma\,(a_1, a_2, \ldots, a_k)\,\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))$$

למשל, עבור $\sigma = (1\ 2)\,(4\ 5)$ ו־$a = (2\ 3\ 5\ 6)$ נקבל

$$\sigma\,(2\ 3\ 5\ 6)\,\sigma^{-1} = (1\ 3\ 4\ 6)$$

כאתגר, האם אתם יכולים למצוא נוסחה עבור $\sigma a \sigma^{-1}$ כאשר a היא תמורה כלשהי?

פתרון:

שיוויון בין שתי פונקציות, כמו למשל התמורות בשאלה, אפשר להוכיח על ידי זה שנראה שכל קלט נשלח לאותו פלט בשתי הפונקציות. כלומר נבדוק לאן האיברים ב־$\{1, 2, \ldots, n\}$ מועתקים בשתי התמורות.

ראשית, נניח כי $m = \sigma(a_i)$ עבור איזשהו $1 \le i \le k$. התמורה באגף ימין תשלח את m ל־$\sigma(a_{i+1})$ כאשר האינדקס $i+1$ מחושב מודולו k. נסתכל מה קורה באגף שמאל:

$$\begin{aligned}\left(\sigma\,(a_1, a_2, \ldots, a_k)\,\sigma^{-1}\right)(m) &= \sigma\left((a_1, a_2, \ldots, a_k)\left(\sigma^{-1}(\sigma(a_i))\right)\right) \\ &= \sigma\left((a_1, a_2, \ldots, a_k)(a_i)\right) = \sigma(a_{i+1})\end{aligned}$$

ולכן התמורות פועלות אותו דבר על $\sigma(a_1), \ldots, \sigma(a_k)$. כעת נניח כי m אינו מהצורה $\sigma(a_i)$ לאף $1 \le i \le k$; לכן התמורה באגף ימין תשלח אותו לעצמו. לגבי אגף שמאל: נשים לב כי $\sigma^{-1}(m) \ne a_i$ לכל i, ולכן

$$\left(\sigma\,(a_1, a_2, \ldots, a_k)\,\sigma^{-1}\right)(m) = \sigma\left((a_1, a_2, \ldots, a_k)\left(\sigma^{-1}(m)\right)\right) = \sigma\left(\sigma^{-1}(m)\right) = m$$

מכאן ששתי התמורות האלו שוות.

4. נתבונן ב־S_n עבור $n > 2$.

(א) הוכיחו שלכל מחזור $\mathrm{id} \neq \tau \in S_n$ קיימת תמורה $\sigma \in S_n$ כך ש־$\sigma\tau \neq \tau\sigma$. רמז: העזרו בשאלה הקודמת.

(ב) הוכיחו כי $Z(S_n) = \{\mathrm{id}\}$.

פתרון:

(א) נניח כי $\tau = (a_1, \ldots, a_k)$. נשים לב ש־$\sigma\tau = \tau\sigma$ אם ורק אם $\sigma\tau\sigma^{-1} \neq \tau$. אז בעזרת השאלה הקודמת, נוכל למצוא σ כדרוש.

אם האורך של המחזור $k \geq 3$, אז נבחר $\sigma = (a_1, a_2)$ ונקבל

$$\begin{aligned}(a_1, a_2)(a_1, a_2, a_3, \ldots, a_k)(a_1, a_2)^{-1} &= (\sigma(a_1), \sigma(a_2), \sigma(a_3), \ldots, \sigma(a_k)) \\ &= (a_2, a_1, a_3, \ldots, a_k)\end{aligned}$$

מפני ש־τ שולח את a_1 ל־a_2 ואילו $\sigma\tau\sigma^{-1}$ שולח את a_1 ל־a_3, אז בודאי $\tau \neq \sigma\tau\sigma^{-1}$.

נותרנו עם המקרה שבו $k = 2$. כלומר $\tau = (a_1, a_2)$. מן הנתון $n > 2$, נסיק שקיים $b \in \{1, \ldots, n\} \setminus \{a_1, a_2\}$. נבחר $\sigma = (a_1, b)$ ונחשב

$$(a_1, b)(a_1, a_2)(a_1, b)^{-1} = (\sigma(a_1), \sigma(a_2)) = (b, a_2)$$

מפני ש־τ שולח את a_2 ל־a_1 ואילו $\sigma\tau\sigma^{-1}$ שולח את a_2 ל־$a_1 \neq b$, אז בודאי $\tau \neq \sigma\tau\sigma^{-1}$.

(ב) המרכז הוא תת־חבורה, ולכן תמיד כולל את איבר היחידה. כלומר $id \in Z(S_n)$. נניח בשלילה שקיימת תמורה $\mathrm{id} \neq \sigma \in Z(S_n)$, ויהי $\sigma = \sigma_1 \ldots \sigma_r$ פירוק שלה למכפלת מחזורים זרים.

אם $r = 1$, אז σ היא מחזור, וסיימנו לפי הסעיף הקודם שבו מצאנו תמורה שלא מתחלפת עם σ.

נניח $r > 1$ ושקיים בפירוק למחזורים זרים מחזור מאורך לפחות 3. בלי הגבלת הכלליות נניח σ_1 הוא מחזור מאורך $k \geq 3$ (כי מחזורים זרים מתחלפים, כלומר $\sigma_i\sigma_j = \sigma_j\sigma_i$). נסמן $\sigma_1 = (a_1, \ldots, a_k)$. כמו בסעיף הקודם נבחר $\mu = (a_1, a_2)$, נשים לב כי μ מתחלף עם $\sigma_2, \ldots, \sigma_r$ ונחשב

$$\mu\sigma\mu^{-1} = \mu\sigma_1\sigma_2 \ldots \sigma_r\mu^{-1} = \mu\sigma_1\mu^{-1}\sigma_2 \ldots \sigma_r$$

נניח בשלילה כי $\sigma = \mu\sigma\mu^{-1}$, ונכפיל ב־$(\sigma_2 \ldots \sigma_r)^{-1}$ מימין ונקבל $\sigma_1 = \mu\sigma_1\mu^{-1}$, בסתירה לסעיף הקודם.

נותרנו רק עם המקרה שבו בפירוק של σ למחזורים זרים מופיעים רק חילופים (מחזורים מאורך 2). נניח $\sigma_1 = (a_1, a_2)$ ו־$\sigma_2 =$ עבור a_1, a_2, b_1, b_2 שונים (הבינו למה מקרה זה לא יקרה עבור $n = 3$). נבחר $\mu = (a_1, b_1)$ ונקבל

$$\mu\sigma\mu^{-1} = \mu\sigma_1\sigma_2\sigma_3 \ldots \sigma_r\mu^{-1} = \mu\sigma_1\sigma_2\mu^{-1}\sigma_3 \ldots \sigma_r$$

כי μ מתחלף עם $\sigma_3, \ldots, \sigma_r$. נניח בשלילה כי $\sigma = \mu\sigma\mu^{-1}$, ונכפיל ב־$(\sigma_3 \ldots \sigma_r)^{-1}$ מימין ונקבל $\sigma_1\sigma_2 = \mu\sigma_1\sigma_2\mu^{-1}$, אבל

$$\mu\sigma_1\sigma_2\mu^{-1} = (a_1, b_1)(a_1, a_2)(b_1, b_2)(a_1, b_1) = (a_1, b_2)(a_2, b_1) \neq (a_1, a_2)(b_1, b_2)$$

וזו סתירה. בסך הכל קיבלנו כי $\sigma \notin Z(S_n)$. לכן $Z(S_n) = \{\mathrm{id}\}$.

5. תזכורת:הוכחתם בהרצאה כי ישנה התאמה חח"ע ועל בין מחלקות שמאליות של $H \leq G$, ובין מחלקות ימניות לפי $gH \mapsto Hg^{-1}$. הוכיחו כי ההתאמה $gH \mapsto Hg$ אינה פונקציה.

רמז: השתמשו בדוגמת החישוב של מחלקות שמאליות וימניות של S_3 שהראנו בתרגול, והראו שהפונקציה לא מוגדרת היטב.

פתרון:

עבור $G = S_3$, ו $H = \langle (1\ 2) \rangle$ תת החבורה הנוצרת ע"י החילוף $(1\ 2)$, נחשב את:

$$(1\ 2\ 3)\,H = \{(1\ 2\ 3)\,\mathrm{id}, (1\ 2\ 3)\,(1\ 2) = (1\ 3)\} = (1\ 3)\,H$$

כלומר $g_1 = (1\ 2\ 3)$ ו־$g_2 = (1\ 3)$ הם שניהם נציגים של המחלקה.

נקבל כי מצד אחד ההתאמה שולחת את $H\,(1\ 2\ 3)$ ל $H\,(1\ 2\ 3) = \{(1\ 2\ 3)\,, (2\ 3)\}$, ומצד שני $H\,(1\ 3) = (1\ 2\ 3)\,H$ ואת $H\,(1\ 3)$ההתאמה שולחת ל $H\,(1\ 3) = \{(1\ 3\ 2)\,, (1\ 3)\}$.

קיבלנו שבחירת נציגים שונים של המחלקה משנה את התוצאה, ולכן ההתאמה לא מוגדרת היטב.

6. מצאו את האינדקסים הבאים:

(א) $[U_{14} : \langle 11 \rangle]$ רמז: משפט לגראנז'.

(ב) $[\mathbb{Z}_8 \times \mathbb{Z}_8 : \langle (2,2) \rangle]$ רמז: משפט לגראנז'.

(ג) $[\mathbb{Z} \times \mathbb{Z} : \langle (2,2) \rangle]$ רמז: קודם תארו את המחלקות השמאליות.

פתרון:

(א) איברי U_{14} הם הטבעיים שקטנים וזרים ל־14. כלומר $U_{14} = \{1, 3, 5, 9, 11, 13\}$. חישוב קצר יראה כי $\langle 11 \rangle = \{1, 9, 11\}$, ואז לפי משפט לגרנז' נקבל שיש בדיוק שתי מחלקות שמאליות. כלומר $[U_{14} : \langle 11 \rangle] = 2$.

(ב) הסדר של החבורה $\mathbb{Z}_8 \times \mathbb{Z}_8$ הוא $64 = 8 \cdot 8$, והסדר של תת־החבורה $\langle (2,2) \rangle$ הוא כסדר של האיבר $(2, 2)$, שהוא 4. לכן לפי משפט לגראנז' $[\mathbb{Z}_8 \times \mathbb{Z}_8 : \langle (2,2) \rangle] = 64/4 = 16$.

(ג) נוכיח כי $[\mathbb{Z} \times \mathbb{Z} : \langle (2,2) \rangle] = \infty$ לפי זה שנראה ש־$\{(0,n) + \mathbb{Z} \times \mathbb{Z}\}$ היא קבוצה אינסופית של מחלקות שמאליות שונות (אלו לא כל המחלקות). אם $(0,n) + \mathbb{Z} \times \mathbb{Z} = (0,m) + \mathbb{Z} \times \mathbb{Z}$ זה אומר

$$(0,n) - (0,m) \in \langle (2,2) \rangle$$

כלומר ש־$(0, n-m) = (2k, 2k)$ לאיזשהו $k \in \mathbb{Z}$. לכן $n - m = 0$, ולכן $n = m$. כלומר יש אינסוף מחלקות שמאליות שונות.

7. תהי G חבורה ותהינה $H, K \leq G$ תת־חבורות סופיות שלה

(א) הוכיחו שאם $(|H|\,, |K|) = 1$, אז $H \cap K = \{e\}$.

(ב) יהי p מספר ראשוני. הוכיחו שאם $|H| = |K| = p$ וגם $H \neq K$, אז $H \cap K = \{e\}$.

פתרון:

1. ידוע לנו כי $H \cap K$ היא תת־חבורה של H ושל K. לכן לפי משפט לגראנז' מתקיים כי $|H \cap K|$ מחלק את $|H|$ ואת $|K|$. אך לפי הנתון הממ"מ של $|H|$ ו־$|K|$ הוא 1. לכן $|H \cap K| \leq 1$. אבל תמיד $|H \cap K| \geq 1$ כי איבר היחידה שייך אליו, ולכן קיבלנו כי $H \cap K = \{e\}$.

2. יהי $x \in H \cap K$ איבר כלשהו. נניח בשלילה כי $x \neq e$. לכן $o(x) > 1$. אנחנו יודעים כי $o(x)$ מחלק את $|H|$ ואת $|K|$, ולכן בהכרח $o(x) = p$. כלומר $|\langle x \rangle| = p$ ומפני ש־H, K הן חבורות אז הן סגורה לפעולה ונסיק $\langle x \rangle \subseteq H, K$. מהנתון $|H| = |K| = p$ נקבל $H = K = \langle x \rangle$ כי ב־$\langle x \rangle$ יש בדיוק p איברים שונים. אך זו סתירה לנתון, ונסיק כי $x = e$.

שאלות אתגר

אם פתרתם את שאלות האתגר, ואין לשאלה פתרון, בבקשה שלחו לי את הפתרון שלהן.

1. תהי I קבוצה מכוונת (כלומר I היא קבוצה סדורה חלקית כך שלכל $i, j \in I$ קיים $k \in I$ כך ש־$k > i, j$). מערכת של חבורות $\{G_i\}_{i\in I}$ נקראת רשת עולה אם לכל $i < j$ מתקיים $G_i \subseteq G_j$.
הוכיחו שבמקרה זה $\bigcup_{i\in I} G_i$ היא חבורה. בפרט, אם ישנה שרשרת עולה של חבורות $G_1 \subseteq G_2 \subseteq \ldots$, אז גם איחוד השרשרת הוא חבורה.

בהצלחה!