פתרון מבחן מועד א' בתורת החבורות
88-218 סמסטר א' תשפ"ב

שאלה 1. הוכיחו או הפריכו את הטענות הבאות:

א. יהי $n \geq 3$. הפעולה הטבעית של A_n על הקבוצה $\{1, 2, \ldots, n\}$ הינה טרנזיטיבית.

ב. תהי G חבורה, ותהי $H \lhd G$ תת־חבורה נורמלית. אזי קיים מונומורפיזם $f\colon G/H \to G$.

פתרון.

א. <u>הוכחה.</u> כדי להוכיח שהפעולה טרנזיטיבית, ניקח $i, j \in \{1, 2, \ldots, n\}$. צ"ל שקיימת תמורה $\sigma \in A_n$ כך ש-$\sigma(i) = \sigma * i = j$. נחלק לשני מקרים:

- אם $i = j$, אפשר כמובן לקחת $\sigma = \mathrm{id}$.
- נניח $i \neq j$. כיוון ש-$n \geq 3$, אפשר לבחור $k \in \{1, 2, \ldots, n\}$ כך ש-$k \neq i, j$. אז נבחר $\sigma = (i\ j\ k) \in A_n$ תמורה זוגית (כי היא מחזור מאורך אי־זוגי), ואכן $\sigma(i) = j$ כנדרש.

ב. <u>הפרכה.</u> ניקח $G = \mathbb{Z}$ ו-$H = 2\mathbb{Z}$. כפי שראינו, $G/H \cong \mathbb{Z}_2$. מצד שני, אין אף מונומורפיזם $f\colon \mathbb{Z}_2 \to \mathbb{Z}$; אכן, אילו היה מונומורפיזם f כזה, היינו מקבלים $0 = f(0) = f(1+1) = f(1) + f(1) = 2f(1)$, כלומר $f(1) = 0$, בסתירה לכך ש-f חח"ע.

טעות נפוצה הייתה להגדיר $f\colon G/H \to G$ על ידי $f(gH) = g$. הבעיה היא שההגדרה הזו לא מוגדרת היטב, שהרי לכל מחלקה gH יש כמה אפשרויות ל-g. גם אם נבחר מראש לכל מחלקה נציג מסוים, הפונקציה f לא תהיה בהכרח הומומורפיזם.

שאלה 2. תהי G חבורה בעלת סדר $616 = 2^3 \cdot 7 \cdot 11$. הוכיחו שהיא לא פשוטה.

פתרון. נניח בשלילה ש-G פשוטה. ניעזר במשפטי סילו על מנת לספור כמה איברים של G יש מכל סדר, ומכאן נגיע לסתירה.

נספור את כמות תת־החבורות 11-סילו. לפי משפט סילו השלישי, $n_{11} \mid 2^3 \cdot 7 = 56$ ו-$n_{11} \equiv 1 \pmod{11}$. מהאילוץ הראשון נקבל $n_{11} \in \{1, 2, 4, 8, 7, 14, 28, 56\}$, אך כיוון ש-$n_{11} \equiv 1 \pmod{11}$ נישאר עם שתי האפשרויות $n_{11} \in \{1, 56\}$. מאחר שהנחנו ש-G פשוטה, $n_{11} \neq 1$ (אחרת תת־חבורת 11-סילו תהיה נורמלית), ולכן בהכרח $n_{11} = 56$.

כיוון ש-G מסדר שמתחלק ב-11 אך לא ב-11^2, כל תת־חבורת 11-סילו היא מסדר 11. לכן כל שתי תת־חבורות 11-סילו שונות נחתכות רק באיבר היחידה $\{e_G\}$ (לפי לגראנז', הסדר של החיתוך שלהן צריך לחלק את הסדרים שלהן, כלומר את 11, אבל צריך להיות קטן יותר כי הן שונות). כמו כן, כל איבר מסדר 11 נמצא באיזושהי תת־חבורת 11-סילו, ולכן כמות האיברים מסדר 11 ב-G היא $560 = (11-1) \cdot 56$.

נותרנו עם $616 - 560 = 56$ איברים. נספור את כמות תת־החבורות 7-סילו. לפי משפט סילו השלישי, $n_7 \mid 2^3 \cdot 11 = 88$ ו-$n_7 \equiv 1 \pmod{7}$. מהאילוץ הראשון נקבל $n_7 \in \{1, 2, 4, 8, 11, 22, 44, 88\}$, וביחד עם האילוץ השני בהכרח $n_7 \in \{1, 8, 22\}$. גם במקרה זה $n_7 \neq 1$ כי G פשוטה, ולכן $n_7 \in \{8, 22\}$.

מנימוק דומה למקרה הקודם, כל שתי תת־חבורות 7-סילו שונות נחתכות רק באיבר היחידה, וכל איבר מסדר 7 נמצא באיזושהי תת־חבורת 7-סילו. לכן נקבל $n_7 \cdot (7-1) = 6n_7$ איברים מסדר 7 ב-G. לכן גם האפשרות $n_7 = 22$ נפסלת (שהרי נותרו רק 56 איברים ב-G שאינם מסדר 11), ונשארנו רק עם האפשרות $n_7 = 8$, כלומר ב-G יש 48 איברים מסדר 7.

עד כה ספרנו כבר $48 + 560 = 608$ איברים ב-G מסדרים 7 ו-11. אך לפי משפט סילו הראשון, ל-G יש לפחות תת־חבורת 2-סילו אחת. כל תת־חבורת 2-סילו של G מכילה 8 איברים, וכיוון שנותרו לנו רק 8 איברים שאינם מסדר 7 או 11 – הם בדיוק מרכיבים תת־חבורת 2-סילו של G, והיא יחידה כי ספרנו את כל האיברים של G. לכן $n_2 = 1$, ומכאן שתת־חבורת 2-סילו של G נורמלית בה, ובפרט G אינה פשוטה, בסתירה.

אם מסתכלים על ההוכחה, אנחנו רואים שלמעשה היה מספיק לספור כמה איברים יש מסדרים ראשוניים (11 ו-7), ולא היינו צריכים לספור את כמות האיברים מסדרים לא ראשוניים.

שאלה 3. יהי p ראשוני, ותהי G חבורה בעלת סדר p^{5782}. נניח כי G פועלת על הקבוצה A.

א. הוכיחו שאם $|A| < p$ אזי הפעולה הזאת הינה בהכרח הפעולה הטריוויאלית, כלומר $g * a = a$ לכל $g \in G$ ולכל $a \in A$.

ב. הביאו דוגמה לכך שאם $|G| = p^{5782}$ ואילו $|A| = p$, אזי הפעולה לא בהכרח טריוויאלית.

פתרון.

א. עבור איבר $a \in A$ נסמן ב-$\mathrm{orb}(a)$ את המסלול שלו תחת הפעולה של G. כמסקנה ממשפט מסלול-מייצב, לכל $a \in A$ מתקיים $|\mathrm{orb}(a)| \mid |G| = p^{5782}$, כלומר $|\mathrm{orb}(a)|$ הוא חזקת p. מצד שני, כמובן $|\mathrm{orb}(a)| \leq |A| < p$, ולכן בהכרח $|\mathrm{orb}(a)| = 1$, כלומר $\mathrm{orb}(a) = \{a\}$. זה מראה שלכל $g \in G$, $g * a = a$, כנדרש.
פתרון נוסף: אם G פועלת על A, הפעולה מגדירה הומומורפיזם $G \to S_{|A|}$. לפי משפט קושי, ב-G יש איבר מסדר p; אך ב-$S_{|A|}$ אין איבר מסדר p, כי p ראשוני ו-$|A| < p$, ולכן ההומומורפיזם הזה חייב להיות טריוויאלי, כלומר הפעולה היא הפעולה הטריוויאלית.

ב. אפשר לתת כאן מספר דוגמאות. אחת מהן היא למשל $G = \mathbb{Z}_p \times \mathbb{Z}_{p^{5781}}$ שפועלת על $A = \mathbb{Z}_p$ לפי $(m, n) * a = m + a$. זו בעצם הפעולה של $\mathbb{Z}_p$ על עצמה על ידי הפעולה של החבורה, כשהוספנו את $\mathbb{Z}_{p^{5781}}$ שפועלת טריוויאלית על $\mathbb{Z}_p$. קל לראות שזו אכן פעולה, והיא אינה טריוויאלית כי למשל $(1,1) * 0 = 1$.

שאלה 4.

א. כמה הומומורפיזמים $f\colon \mathbb{Z}_{24} \to S_5$ יש?

ב. תהי G חבורה ותהיינה $H, K \lhd G$ תת־חבורות נורמליות כך ש-$H \cap K = \{e\}$. הוכיחו כי G איזומורפית לתת־חבורה של $G/H \times G/K$.

פתרון.

א. הומומורפיזם $f\colon \mathbb{Z}_{24} \to S_5$ נקבע על ידי $f(1)$. אכן, אם נבחר $a = f(1)$, כדי ש-f תהיה הומומורפיזם נהיה חייבים להגדיר

$$f(n) = f(1 + \cdots + 1) = f(1) \cdots f(1) = a^n$$

וזה יגדיר את f על כל $\mathbb{Z}_{24}$. כדי שההגדרה הזו תהיה מוגדרת היטב, חייבים ש-$f(n) = f(n+24)$, כלומר $a^n = a^{n+24}$, ומכאן נסיק ש-$a^{24} = \mathrm{id}$, כלומר $o(a) \mid 24$. מצד שני, אם אכן $o(a) \mid 24$, אז f אכן מגדירה הומומורפיזם, כי אז

$$f(m+n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n).$$

לכן נותר לספור לכמה איברים ב-S_5 יש סדר שמחלק את 24. ראינו בתרגול שהסדרים של איברים ב-S_5 הם $1, 2, 3, 4, 5, 6$ (על פי מבנה המחזורים של התמורה), ולכן אפשר לבחור את a להיות כל איבר ב-S_5 שאינו מסדר 5. נספור את כמות האיברים ב-S_5 מסדר 5: כל איבר כזה הוא בהכרח מחזור מאורך 5, וכמות המחזורים באורך 5 ב-S_5 היא כמות הדרכים לסדר 5 מספרים במעגל, כלומר $(5-1)! = 24$.
בסך הכל, לכל אחד מ-$96 = 120 - 24 = 5! - 4!$ האיברים האחרים ב-S_5 אפשר להגדיר הומומורפיזם כנ"ל, ובסך הכל נקבל שיש 96 הומומורפיזמים שונים $f\colon \mathbb{Z}_{24} \to S_5$.

ב. השאלה הזו הופיעה בתרגילי הבית (שאלה 3 בתרגיל בית 9).

נגדיר פונקציה $f\colon G \to G/H \times G/K$ לפי $f(g) = (gH, gK)$. נרצה להוכיח כי f היא מונומורפיזם, ואז נקבל ש-G איזומורפית לתמונה של f, שהיא תת־חבורה של $G/H \times G/K$.

f הומומורפיזם: אכן, לכל $g_1, g_2 \in G$,

$$f(g_1g_2) = (g_1g_2H, g_1g_2K) \overset{(\star)}{=} (g_1H, g_1K)(g_2H, g_2K) = f(g_1)f(g_2).$$

המעבר $(\star)$ הסתמך על כך ש-$H, K \lhd G$, ולכן $g_1g_2H = (g_1H)(g_2H)$ (וכנ"ל ל-K).

f חח"ע: נניח ש-$g \in \ker f$. נזכור כי איבר היחידה ב-$G/H \times G/K$ הוא (H, K); לכן $(gH, gK) = f(g) = (H, K)$. מכאן נקבל ש-$g \in H$ וגם $g \in K$, כלומר $g \in H \cap K$. אך נתון ש-$H \cap K = \{e\}$, ולכן בהכרח $g = e$. הוכחנו ש-$\ker f = \{e\}$, ולכן f חח"ע.