שאלה 1

לכבוד ל"ח בעומר, שלושים ושמונת האיברים של החבורה הדיהדרלית D_{19} מארגנים חגיגה. כל תת־חבורה לקחה על עצמה לארגן חלק מן האירוע.

א. כמה תת־חבורות יש בחבורה D_{19}?

ב. איזה איברים שייכים ליותר מתת־חבורה אמתית אחת? תזכורת: תת־חבורה H של חבורה G נקראת אמתית אם $H \neq G$.

תשובה:

א. לפי משפט לגרנז, הסדר של כל חבורה של D_{19} מחלק את $|D_{19}| = 38$. לכן הסדרים האפשריים של תת־חבורות של D_{19} הם $1, 2, 19, 38$.

יש תת־חבורה אחת מסדר 1. זאת התת־חבורה $\{e\}$.

יש גם תת־חבורה אחת מסדר 38. זאת D_{19} כולה.

לפי משפט סילו השלישי, $n_{19}|2$ וגם $n_{19} \equiv 1 \bmod 19$, ולכן $n_{19} = 1$. כיוון שכל תת־חבורה מסדר 19 הינה תת־חבורה 19־סילו, זה אומר שיש רק תת־חבורה אחת מסדר 19.

שוב לפי משפט סילו השלישי, $n_2|19$ וגם $n_2 \equiv 1 \bmod 2$. התנאי השני לא מוסיף שום מידע במקרה הזה, ומקבלים $n_2 \in \{1, 19\}$. אך לכל $0 \leq i \leq 18$ מתקיים $(\tau\sigma^i)^2 = \tau\sigma^i\tau\sigma^i = \tau\sigma^i\sigma^{-i}\tau = \tau^2 = e$. האיבר $\tau\sigma^i$ לא טריוויאלי, לכן הסדר שלו הוא 2. לכל $0 \leq i \leq 18$, מסיקים כי $\langle\tau\sigma^i\rangle = \{e, \tau\sigma^i\}$ הינה תת־חבורה של D_{19} מסדר 2. אז מצאנו כבר 19 תת־חבורות שונות מסדר 2. לחילופין, היינו יכולים לספור את האיברים מכל סדר אפשרי ולמצוא שאם $n_2 = 1$ אז אין ב־ D_{19} מספיק איברים. לא אתן כאן את כל הפרטים של השיטה הזאת. אופציה אחרת זה לשים לב שאם $n_2 = 1$, אזי כל תת־חבורה p־סילו של D_{19} הינה נורמלית, ואז מוכיחים כי D_{19} אבלית בדיוק כמו בפתרון לשאלה השלישית במבחן הזה. אך ידוע כי D_{19} לא אבלית, וקיבלנו סתירה. בכל אופן, מוכיחים כי $n_2 = 19$. לכן, סך הכל ב־ D_{19} יש $1 + 1 + 19 + 1 = 22$ תת־חבורות.

ב. הסדר של התת־חבורה $\langle\sigma\rangle = \{e, \sigma, \sigma^2, \ldots, \sigma^{18}\}$ הינו 19, והוכחנו בסעיף הקודם שזו התת־חבורה היחידה עם סדר 19. בנוסף, הוכחנו בסעיף הקודם כי 19 התת־חבורות עם סדר 2 הן בדיוק $\{e, \tau\sigma^i\}$ לכל $0 \leq i \leq 18$. התת־חבורה האמתית היחידה שלא הזכרנו עדיין היא $\{e\}$. כיוון ש־

$$D_{19} = \{e, \sigma, \sigma^2, \ldots, \sigma^{18}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{18}\}$$

ברור שהאיבר היחיד שמשתתף ביותר מתת־חבורה אמתית אחת הוא האיבר הטריוויאלי e.

שאלה 2

נתונה פעולה של חבורה G על קבוצה A. נגדיר

$$\mathrm{Aut}_G(A) = \{f \in S_A : \forall g \in G, \forall a \in A,\ f(g * a) = g * f(a)\}.$$

א. הוכח כי $\mathrm{Aut}_G(A)$ הינה תת־חבורה של S_A.

ב. יהי $\varphi : G \to S_A$ ההומומורפיזם הנובע מן הפעולה: $(\varphi(g))(a) = g * a$ לכל $g \in G, a \in A$. הוכח כי

$$\mathrm{Aut}_G(A) = \bigcap_{g \in G} C_{S_A}(\varphi(g)).$$

תשובה:

ברור מן ההגדרה שתמורת הזהות $e \in S_A$ שייכת ל־ $\mathrm{Aut}_G(A)$, ולכן $\mathrm{Aut}_G(A) \neq \varnothing$.
יהיו $f_1, f_2 \in \mathrm{Aut}_G(A)$. אזי לכל $g \in G$ ולכן $a \in A$ מתקיים

$$f_1 f_2(g * a) = f_1(f_2(g * a)) = f_1(g * f_2(a)) = g * f_1(f_2(a)) = g * f_1 f_2(a),$$

ולכן $f_1 f_2 \in \mathrm{Aut}_G(A)$. זה אומר כי $\mathrm{Aut}_G(A)$ סגורה לכפל.
כדי להוכיח סגירות להפכים, נראה שלכל $f \in \mathrm{Aut}_G(A)$ ולכל $g \in G$ ולכל $a \in A$ מתקיים

$$f^{-1}(g * f(a)) = f^{-1}(f(g * a)) = g * a = g * f^{-1}(f(a)).$$

אך f על, ולכן כל איבר של A שייך לתמונתו. זה אומר כי

$$f^{-1}(g * a) = g * f^{-1}(a)$$

לכל $g \in G$ ולכל $a \in A$. במילים אחרות, $f^{-1} \in \mathrm{Aut}_G(A)$ והוכחנו כי $\mathrm{Aut}_G(A) \leq S_A$ תת־חבורה.
כדי להוכיח את הסעיף השני, יהי $f \in S_A$. אזי $f \in \bigcap_{g \in G} C_{S_A}(\varphi(g))$ אם ורק אם
$f \in C_{S_A}(\varphi(g))$ **לכל $g \in G$ אם ורק אם**
$f \circ \varphi(g) = \varphi(g) \circ f$ **לכל $g \in G$ אם ורק אם**
$f((\varphi(g))(a)) = (\varphi(g))(f(a))$ **לכל $g \in G$ ולכל $a \in A$ אם ורק אם**
$f(g * a) = g * f(a)$ **לכל $g \in G$ ולכל $a \in A$ לפי ההגדרה של $\varphi(g)$. אבל זה נכון אם רק אם $f \in \mathrm{Aut}_G(A)$. הוכחנו כי $\mathrm{Aut}_G(A) = \bigcap_{g \in G} C_{S_A}(\varphi(g))$.**

שאלה 3

תהי G חבורה בעלת סדר $665 = 5 \cdot 7 \cdot 19$. הוכח כי G אבלית.

תשובה:

נעזרים במשפט סילו השלישי. הוא אומר כי $n_5 | 7 \cdot 19$, כלומר $n_5 \in \{1, 7, 19, 133\}$. אך גם $n_5 \equiv 1 \bmod 5$, וזה אומר כי $n_5 = 1$.

כמו כן, $n_7 | 5 \cdot 19$, מה שאומר כי $n_7 \in \{1, 5, 19, 95\}$. אך $n_7 \equiv 1 \bmod 7$, ולכן $n_7 = 1$.

כמו כן, $n_{19} | 5 \cdot 7$, כלומר $n_{19} \in \{1, 5, 7, 35\}$. אך $n_{19} \equiv 1 \bmod 19$, ומסיקים כי $n_{19} = 1$.

לפי משפט סילו השני, זה אומר שכל התת־חבורות p־סילו של G הינן נורמליות. לפי משפט מן השיעור, זה אומר כי G נילפוטנטית, ולכן כי G איזומורפית למכפלה הישרה של תת־חבורות p־סילו שלה. אך כל התת־חבורות האלה מסדר ראשוני, לכן ציקליות, לכן אבליות. לכן G איזומורפית למכפלה ישרה של חבורות אבליות, מה שאומר שהיא עצמה אבלית.

שאלה 4

יהי s הסכום של ארבע הספרות האחרונות של מספר תעודת הזהות שלך. רשום את המספר s. לא ייעשה שימוש בו כדי לזהות אותך בעת בדיקת המבחן. איזו טענה מן הטענות הבאות נכונה? נמק את תשובתך.

1. כל חבורה מסדר $105(4s-2)^2$ הינה פתירה.
2. יש חבורות פתירות וגם חבורות לא פתירות מסדר $105(4s-2)^2$.
3. אף חבורה מסדר $105(4s-2)^2$ אינה פתירה.

תשובה:

נשים לב כי $15|105$ ואילו $4|(4s-2)^2$. לכן, המספר $n=105(4s-2)^2$ מתחלק ב־ 60 לכל s.

החבורה $\mathbb{Z}_n$ הינה חבורה אבלית, ולכן פתירה, מסדר n. דוגמא אחרת של חבורה פתירה מסדר n היא החבורה הדיהדרלית $D_{\frac{n}{2}}$. מצד שני, החבורה $G=A_5\times\mathbb{Z}_{\frac{n}{60}}$ הינה מסדר n, ויש לה תת־חבורה $A_5\times\{e\}\simeq A_5$ שאינה פתירה, שהרי הוכחנו בשיעור כי A_5 לא פתירה. גם הוכחנו שכל תת־חבורה של חבורה פתירה הינה פתירה, ולכן G אינה פתירה. זה אומר שהטענה השניה היא הנכונה.

שאלה 5

תהי G חבורה, $H \leq G$ תת־חבורה, ו־$N \trianglelefteq G$ תת־חבורה נורמלית. נניח שהסדר $|H|$ והאינדקס $[G:N]$ סופיים וכי $\gcd(|H|,[G:N])=1$. הוכח כי $H \leq N$.

תשובה:

כיוון ש־ $|H|$ סופי, יש לנו שוויון של מספרים טבעיים: $|H| = |H \cap N| \cdot [H : H \cap N]$. בפרט $[H : H \cap N] \,|\, |H|$. בנוסף, משפט האיזומורפיזם השני אומר לנו כי $HN/N \simeq H/(H \cap N)$, וכיוון שהאינדקס $[G:N]$ סופי, כפליות האינדקסים אומרת לנו כי $[G:N] = [G:HN][HN:N] = [G:HN][H:H\cap N]$.

לכן, $[H : H \cap N]$ הינו מחלק משותף של $|H|$ ושל $[G:N]$. אבל הנחנו שהמספרים האלה זרים. לכן $[H : H \cap N] = 1$. מכאן מסיקים כי $H = H \cap N$, ולכן $H \leq N$.

פתרון אחר, אך בעצם שקול, זה להתבונן בהומומורפיזם $f : H \to G/N$ המוגדר על ידי $f(h) = hN$. זה הצמצום ל־ H של ההטלה הטבעית $G \to G/N$.

התמונה של כל הומומורפיזם הינה תת־חבורה, ואז לפי לגרנז $|f(H)|$ מחלק את $[G:N] = |G/N|$. מצד שני, לפי משפט האיזומורפיזם הראשון, $f(H) \simeq H/\ker f$, וכיוון ש־ $|H|$ סופי זה אומר כי $|f(H)| = \frac{|H|}{|\ker f|}$ ולכן כי $|f(H)| \,|\, |H|$. אך שוב המספרים $|H|, [G:N]$ זרים ואילו $|f(H)|$ הינו מחלק משותף. לכן $|f(H)| = 1$. יש רק תת־חבורה אחת של G/N מסדר 1, שהיא התת־חבורה הטריוויאלית. לכן ההומומורפיזם f הינו טריוויאלי. לכן, לכל $h \in H$, מקבלים $f(h) = hN = eN = e_{G/N}$. אבל זה אומר כי $h \in N$ לכל $h \in H$, כלומר $H \leq N$.