פתרון תרגיל בית 9 באלגברה מופשטת
88-211 סמסטר א' תשע"ו

שאלה 1. אם $f:G\to H$ היא אפימורפיזם, אז H נקראת תמונה אפימורפית של G.
מצאו את כל התמונות האפימורפיות של D_4 עד כדי איזומורפיזם. רמז: משפט האיזומורפיזם הראשון.

פתרון. לפי משפט האיזומורפיזם הראשון, כל תמונה אפימורפית של D_4 איזומורפית למנה D_4/H, עבור $H\lhd D_4$. לכן מספיק לדעת מי הן כל תת־החבורות הנורמליות של D_4.

קודם כל, יש לנו את תת־החבורות הטריוויאליות $D_4\lhd D_4,\{\mathrm{id}\}$. לכן, קיבלנו את התמונות האפימורפיות $D_4/\{\mathrm{id}\}\cong D_4$ ו-$D_4/D_4\cong\{\mathrm{id}\}$.

כעת, אנו יודעים כי $Z(D_4)=\langle\sigma^2\rangle\lhd D_4$. ננסה להבין מיהי $D_4/\langle\sigma^2\rangle$. רעיון לניחוש: אנחנו יודעים, לפי לגראנז', כי זו חבורה מסדר 4. כמו כן, אפשר לבדוק שכל איבר $x\in D_4/\langle\sigma^2\rangle$ מקיים $x^2=e$. לכן ננחש שזו $\mathbb{Z}_2\times\mathbb{Z}_2$ (בהמשך הקורס נדע להגיד זאת בלי למצוא איזומורפיזם ממש). נגדיר $f:D_4\to\mathbb{Z}_2\times\mathbb{Z}_2$ לפי $f(\tau^i\sigma^j)=(i,j)$. קל לבדוק שזהו אפימורפיזם עם גרעין $\langle\sigma^2\rangle$, ולכן, לפי משפט האיזומורפיזם הראשון,

$$D_4/\langle\sigma^2\rangle\cong\mathbb{Z}_2\times\mathbb{Z}_2$$

נשים לב כי $\langle\sigma\rangle\lhd D_4$, כי זו תת־חבורה מאינדקס 2. גם $\langle\sigma^2,\tau\rangle,\langle\sigma^2,\tau\sigma\rangle\lhd D_4$ מאותו נימוק. אנחנו גם יודעים שכל החבורות מסדר 2 איזומורפיות זו לזו, ולכן

$$D_4/\langle\sigma\rangle\cong D_4/\langle\sigma^2,\tau\rangle\cong D_4/\langle\sigma^2,\tau\sigma\rangle\cong\mathbb{Z}_2$$

צריך לבדוק האם יש עוד תת־חבורות נורמליות. נזכור שבתרגיל הבית מצאתם את כל תת־החבורות של D_4. לפי הרשימה שהכנתם, קל לראות שכתבנו את כל תת־החבורות מסדר 4, ואת $\langle\sigma^2\rangle$. תת־החבורות היחידות שעוד לא הזכרנו הן מהצורה $\langle\tau\sigma^i\rangle=\{\mathrm{id},\tau\sigma^i\}$. כדי שהיא תהיה נורמלית, צריך להתקיים

$$H\ni\tau\left(\tau\sigma^i\right)\tau^{-1}=\sigma^i\tau=\tau\sigma^{4-i}$$

לכן בהכרח $i=2$. אבל אז

$$\sigma\left(\tau\sigma^2\right)\sigma^{-1}=(\sigma\tau)\,\sigma=\tau\sigma^{-1}\sigma=\tau\notin H$$

ולכן $H\ntriangleleft D_4$. מכאן שכתבנו את כל תת־החבורות הנורמליות של D_4, ולכן כל התמונות האפימורפיות של D_4 הן $D_4,\mathbb{Z}_2\times\mathbb{Z}_2,\mathbb{Z}_2,\{\mathrm{id}\}$.

שאלה 2. תהי G חבורה סופית מסדר אי זוגי. הוכיחו שלכל איבר $e\neq x\in G$ מתקיים $x^{-1}\notin\mathrm{conj}(x)$.

פתרון. נניח בשלילה כי $x^{-1}\in\mathrm{conj}(x)$. כלומר x צמוד להופכי שלו, ולכן קיים $g\in G$ כך ש-$gxg^{-1}=x^{-1}$. נצמיד את המשוואה האחרונה שוב ב-g ונקבל

$$g^2xg^{-2}=gx^{-1}g^{-1}=\left(gxg^{-1}\right)^{-1}=x$$

ולכן $g^2x = xg^2$. החבורה G היא סופית מסדר אי זוגי, ולכן הסדר של g הוא אי זוגי, נניח $o(g) = 2m+1$. לכן $e = g^{2m+1} = g\left(g^2\right)^m$, וקיבלנו כי $g^{-1} = \left(g^2\right)^m$. נציב זאת במשוואה $gxg^{-1} = x^{-1}$ ונקבל

$$x = g\left(g^2\right)^m x = gx\left(g^2\right)^m = x^{-1}$$

ולכן $x = x^{-1}$, שזו סתירה כי x אינו איבר היחידה ואין בחבורה איברים מסדר 2.

שאלה 3. מצאו את $|\mathrm{conj}(\sigma)|$ כאשר $\sigma = (2573) \in S_{14}$.

פתרון. אנו נדרשים למצוא את מספר התמורות שצמודות ל-σ. ידוע לנו שהתמורות היחידות שצמודות למחזור מאורך 4 הן מחזורים מאורך 4. מספר המחזורים האלו הוא

$$|\mathrm{conj}(\sigma)| = \binom{14}{4}(4-1)! = 6006$$

שאלה 4. יהיו הומומורפיזמים $f : G \to H$ ו-$g : H \to G$ כך ש-$f \circ g = \mathrm{id}_H$.

א. הוכיחו כי g חח"ע ו-f על.

ב. הוכיחו כי $G = \ker(f) \rtimes \mathrm{im}(g)$.

פתרון. א. לפי טענה מהקורס במתמטיקה בדידה.

ב. נסמן $K = \ker(f)$ ו-$Q = \mathrm{im}(g)$. ידוע לנו כי $K \lhd G$ ו-$Q \leq G$. נוכיח את הדרישות ממכפלה ישרה למחצה (פנימית). נראה כי $K \cap Q = \{e_G\}$. יהי $x \in K \cap Q$, אז קיים $h \in H$ עבור $x = g(h)$. מפני ש-$x \in K$ מתקיים $f(g(h)) = h$ וגם $f(g(h)) = e_H$. לכן $h = e_H$, ולכן $x = e_G$.
נותר להראות כי $G = KQ$. יהי $x \in G$. נשתמש בכך ש-$x^{-1}x = e_G$. נפעיל את f ונקבל

$$e_H = f(e_G) = f(x^{-1})f(x)$$

על המשוואה הזאת נפעיל את g ונקבל

$$e_G = g(e_H) = g(f(e_G)) = g(f(x^{-1}))g(f(x))$$

נסמן $q = g(f(x))$ ו-$k = x \cdot g(f(x^{-1}))$. ברור כי $q \in Q$ וכי $x = kq = x \cdot e_G$. כדי להראות ש-$k \in K$ נבדוק שהתמונה שלו תחת f היא e_H. אכן

$$f(x \cdot g(f(x^{-1}))) = f(x)f(g(f(x^{-1}))) = f(x)f(x^{-1}) = f(e_G) = e_G$$

וקיבלנו את הדרוש $x = kq \in KQ$.

שאלה 5. תהי G חבורה סופית, ותהי H תת־חבורה מאינדקס 2. הוכיחו שאם $f : G \to H$ אפימורפיזם ושהגרעין $\ker(f)$ לא מוכל ב-H, אז $G \cong H \times \mathbb{Z}_2$. רמז: השאלה הקודמת.

פתרון. נסמן $K = \ker(f)$. ברור כי $K, H \lhd G$. לפי משפט האיזומורפיזם הראשון $G/K \cong H$. בפרט $|K| = [G : H] = 2$. לכן $K \cong \mathbb{Z}_2$. כדי להוכיח ש-$G \cong H \times \mathbb{Z}_2$ מספיק להראות כי G היא מכפלה ישרה של H ושל K. כבר ראינו ששתיהן נורמליות, ונשאר להראות $H \cap K = \{e\}$ ו-$G = KH$.
מפני ש-$K = \{e, k\}$ לא מוכלת ב-H, אז בהכרח $k \notin H$ (האיבר k הוא האיבר שאינו איבר היחידה ב-K). לכן $H \cap K = \{e\}$. כמו כן $H \neq kH$, שוב מפני ש-$k \notin H$. לכן $G = H \cup kH = KH$, וקיבלנו את הדרוש.

שאלה 6. נתונות החבורות הבאות מסדר 24: S_4, $\mathbb{Z}_{24}$, $\mathbb{Z}_4 \times \mathbb{Z}_6$, $\mathbb{Z}_4 \times S_3$, $\mathbb{Z}_3 \times D_4$, $\mathbb{Z}_3 \times Q_8$, $\mathbb{Z}_2 \times A_4$, D_{12} ו-$SL_2(\mathbb{Z}_3)$ (מטריצות 2×2 עם דטרמיננטה 1 מעל השדה בן שלושה איברים). בחרו לפחות ארבע מהן והוכיחו שאף אחת מהן לא איזומורפית לאחרות שבחרתן. רמז: סדר של איברים.

אגב, ישנן 15 חבורות מסדר 24 עד כדי איזומורפיזם. האם אתם יכולים להוסיף עוד כמה לרשימה?

פתרון. החבורות $\mathbb{Z}_{24}$ ו-$\mathbb{Z}_4 \times \mathbb{Z}_6$, הן אבליות, ולכן לא איזומורפיות לחבורות האחרות. הן לא איזומורפיות כי $\mathbb{Z}_{24}$ היא ציקלית ואילו $\mathbb{Z}_4 \times \mathbb{Z}_6$ לא ציקלית (הסדר הכי גדול של איבר בחבורה זו הוא 12).

עבור שאר החבורות נמצא שרק בחבורות $\mathbb{Z}_4 \times S_3$, $\mathbb{Z}_3 \times D_4$, $\mathbb{Z}_3 \times Q_8$ ו-D_{12} יש איברים מסדר 12, ולכן הן לא איזומורפיות לאחרות. בחבורה D_{12} יש 4 איברים מסדר 12 והם σ^i עבור $i \in U_{12}$. מספר האיברים מסדר 12 בחבורות שהן מכפלות מגיעות רק מאיבר מן הצורה (x, y) כאשר $[o(x), o(y)] = 12$. כך נוכל לחשב שבחבורה $\mathbb{Z}_3 \times Q_8$ יש 12 איברים מסדר 12, כי יש שישה איברים מסדר 4 ב-Q_8 ושני איברים מסדר 3 ב-$\mathbb{Z}_3$, ואילו בשאר החבורות יש רק 4 איברים מסדר 12. לכן $\mathbb{Z}_3 \times Q_8$ לא איזומורפית לאחרות. כהערת אגב, כפי שמראים ש-D_4 לא איזומורפית ל-Q_8, כך אפשר להראות כי $\mathbb{Z}_3 \times D_4$ ו-$\mathbb{Z}_3 \times Q_8$ הן לא איזומורפיות (זה לא תמיד נכון שאם A ו-B לא איזומורפיות, אז גם $C \times A$ ו-$C \times B$ הן לא איזומורפיות. האם תוכלו למצוא דוגמה למקרה שכזה?).

בחבורה $\mathbb{Z}_3 \times D_4$ שבה יש עשרה איברים מסדר 6 (מספיק להראות שיש יותר משניים), ולכן היא לא איזומורפית לחבורות $\mathbb{Z}_4 \times S_3$ ו-D_{12} שבהן יש רק שני איברים מסדר 6 (הם $(2, (123))$ ו-$(2, (132))$ ב-$\mathbb{Z}_4 \times S_3$ וב-D_{12} הם σ^2 ו-σ^{10}). בחבורה D_{12} יש שני איברים מסדר 4, שהם σ^3 ו-σ^9. לכן החבורה D_{12} לא איזומורפית ל-$\mathbb{Z}_4 \times S_3$, שבה יש בה 8 איברים מסדר 4 (שוב, מספיק להראות שיש יותר משניים).

נשאר לנו להוכיח שהחבורות S_4, $\mathbb{Z}_2 \times A_4$ ו-$SL_2(\mathbb{Z}_3)$ לא איזומורפיות אחת לשניה. בחבורה S_4 ראינו בכיתה שהסדרים האפשריים של האיברים הם רק $1, 2, 3, 4$. בחבורות האחרות יש גם איברים מסדר 6, כמו למשל האיבר $(1, (123)) \in \mathbb{Z}_2 \times A_4$ והאיבר $\left(\begin{smallmatrix} 2 & 2 \\ 0 & 2 \end{smallmatrix}\right) \in SL_2(\mathbb{Z}_3)$. בחבורה $SL_2(\mathbb{Z}_3)$ יש איברים מסדר 4 כמו $\left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$, ולכן היא לא איזומורפית לחבורה $\mathbb{Z}_2 \times A_4$ שבה הסדרים של האיברים הם רק $1, 2, 3, 6$.

שאלה 7. חבורה G תקרא פשוטה אם אין לה תת־חבורות נורמליות לא טריוויאלית. כלומר G פשוטה אם תת־החבורות הנורמליות היחידות שלה הן $\{e\}$ ו-G.

נתונה שרשרת עולה של חבורות פשוטות $G_1 \subseteq G_2 \subseteq G_3 \subseteq \ldots$. הוכיחו שהאיחוד $G = \bigcup_{i=1}^{\infty} G_i$ הוא גם חבורה פשוטה.

פתרון. ודאו שאתם מבינים מדוע G היא חבורה. למשל אם $a, b \in G$, זה אומר שקיים n_1 כך ש-$a \in G_{n_1}$ וקיים n_2 כך ש-$b \in G_{n_2}$. עבור $n = \max\{n_1, n_2\}$ יתקיים כי $ab \in G_n \subseteq G$. באופן דומה מוכיחים את שאר התכונות של חבורה.

תהי $N \lhd G$. נרצה להראות כי N תת־חבורה טריוויאלית. נשים לב שלכל i מתקיים $N \cap G_i \lhd G_i$. מפני ש-G_i הן חבורות פשוטות, אז לכל i יתקיים ש-$N \cap G_i = G_i$ או $N \cap G_i = \{e\}$.

אם $N \cap G_i = \{e\}$ לכל i, אז נחשב

$$N = N \cap G = N \cap \left(\bigcup_{i=1}^{\infty} G_i \right) = \bigcup_{i=1}^{\infty} (N \cap G_i) = \bigcup_{i=1}^{\infty} \{e\} = \{e\}$$

ולכן $N = \{e\}$. אחרת, יהי n המספר המינימלי עבורו $N \cap G_n = G_n$. לכן לכל $i \geq n$ מתקיים $N = G_i$ כי $\{e\} \neq N \leq G_n \leq G_i$ ולכל $i < n$ מתקיים $N \cap G_i = \{e\}$. כעת נחשב

$$N = \bigcup_{i=1}^{\infty} (N \cap G_i) = \bigcup_{i=1}^{n-1} (N \cap G_i) \cup \bigcup_{i=n}^{\infty} (N \cap G_i) = \{e\} \cup \bigcup_{i=n}^{\infty} (G_i) = G$$

ולכן $N = G$.

שאלה 8. כעת נראה שקיים זוג של חבורות לא איזומורפיות המשוכנות אחת בתוך השנייה. נזכיר כי חבורה A משוכנת בחבורה B אם קיים שיכון $f : A \to B$.
נסמן $G = \bigcup_{n\geq 5} S_n$ איחוד כל חבורות הסימטריה S_n עבור $n \geq 5$, ונסמן $H = \bigcup_{n\geq 5} A_n$ איחוד כל חבורות החילופין A_n עבור $n \geq 5$.

הערה. 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 $\hat{\sigma}(n+1) = n+1$. להמשך התרגיל נשתמש בנקודת מבט זו כשנדון בחבורות G ו-H.

א. הראו כי לכל $n \in \mathbb{N}$ קיימים שיכונים $A_n \hookrightarrow S_n \hookrightarrow A_{n+2}$. רמז: השיכון הראשון הוא ברור לפי הכלה. לשיכון השני הגדירו העתקה

$$\phi_n : S_n \to A_{n+2}$$
$$\sigma(i) \mapsto \begin{cases} \sigma(i-2)+2 & 3 \leq i \leq n+2 \\ 1 & i = 1 \wedge \operatorname{sign}(\sigma) = 1 \\ 2 & i = 2 \wedge \operatorname{sign}(\sigma) = 1 \\ 2 & i = 1 \wedge \operatorname{sign}(\sigma) = -1 \\ 1 & i = 2 \wedge \operatorname{sign}(\sigma) = -1 \end{cases}$$

כלומר אם $3 \leq i \leq n+2$ אז $\phi_n(\sigma)(i) = \sigma(i-2)+2$; אם σ היא תמורה זוגית, אז נשלח אותה "להזזה" שלה בשני מקומות בתוך A_{n+2}, ואם σ תמורה אי־זוגית אז היא תשלח לאותה "הזזה" כפול החילוף $(1\,2)$. הראו מהבנייה כי תמונת ϕ_n מוכלת ב-A_{n+2} ושהיא הומומורפיזם מוגדר היטב. אתגר: חשבו למה אי אפשר לשכן את S_n בתוך A_{n+1} עבור $n \geq 2$.

ב. הראו כי G משוכנת בתוך H.
הדרכה: בדרך אחת ניתן לשים לב כי החבורה G היא חבורת התמורות של $\mathbb{N}$ עם תומך סופי (התומך של תמורה הוא המספרים שהיא מזיזה. ב-S_n כל התמורות הן עם תומך סופי), והחבורה H היא חבורת התמורות הזוגיות של $\mathbb{N}$ עם תומך סופי. כעת אפשר להגדיר שיכון $\varphi : G \to H$ לפי $\varphi(\sigma) = (12)^{(\operatorname{sign}(\sigma)-1)/2}\rho\sigma\rho^{-1}$ כאשר $\rho(i) = i+2$.
בדרך אחרת יש להראות כי השיכונים בסעיף הקודם תואמים, כלומר $\phi_{n+1}(\sigma) = \phi_n(\sigma)$ לכל $n \geq 5$ ולכל $\sigma \in S_n$, וכך לבנות שיכון $\varphi : G \to H$.

ג. הראו כי H משוכנת בתוך G.

ד. הוכיחו כי החבורות G ו-H אינן איזומורפיות. רמז: אחת פשוטה והשנייה לא.

פתרון. א. החבורה A_n היא תת־חבורה של S_n לכל n. לכן ודאי יש שיכון $A_n \hookrightarrow S_n$. לשיכון $S_n \hookrightarrow A_{n+2}$ נשתמש בהעתקות מהרמז. אפשר להוכיח כי ההעתקות ϕ_n הן שיכונים לכל $n \geq 5$ לפי הגדרה. נשים לב כי התמונה של תמורה σ היא תמיד ב-A_{n+2}. הרי אם σ היא זוגית, היא עוברת לתמורה זוגית, ואם היא אי־זוגית, אז היא נשלחת לתמורה אי־זוגית כפול חילוף (שהוא תמורה אי־זוגית), ולכן התמונה היא שוב תמורה זוגית
ההעתקות הן חח"ע כי התמורה היחידה שנשלחת ל-id היא id (תמונת כל תמורה אחרת היא לא הזהות עבור איזשהו $3 \leq i \leq n+2$). כדי להראות שההעתקות הן הומומורפיזמים צריך להראות כי לכל $\sigma, \tau \in S_n$ מתקיים $\phi_n(\sigma\tau) = \phi_n(\sigma)\phi_n(\tau)$.
אפשר לשים לב כי בתמונה עבור $3 \leq i \leq n+2$ זו פשוט מכפלת אותן התמורות

"בהזזה", ועבור $1 \leq i \leq 2$ התמונה היא או הזהות או החילוף $(1\,2)$ שזר לשאר המחזורים בתמונות של σ ו-τ עבור $3 \leq i \leq n+2$.
בנוגע לשאלת האתגר: נשים לב שנדרש כי הסדר של S_n יחלק את הסדר של A_{n+1}, לפי לגראנז'. אבל $\frac{|A_{n+1}|}{|S_n|} = \frac{n+1}{2}$, ולכן לא ייתכן כי n זוגי. אם n אי־זוגי, נסמן $m = \frac{n+1}{2}$ שהוא האינדקס של S_n בתוך A_{n+1}. אם S_n איזומורפית לתת־חבורה של A_{n+1}, אזי ישנו הומומורפיזם $f : A_{n+1} \to S_m$ שמושרה מ-m המחלקות של S_n. עבור $n \geq 5$ מתקיים כי $m! < |A_{n+1}| = \frac{(n+1)!}{2}$, ולכן לא ייתכן כי ההומומורפיזם f הוא חח"ע. ידוע כי הגרעין של f הוא תת־חבורה נורמלית של A_{n+1}, וזו סתירה כי A_{n+1} פשוטה עבור $n \geq 5$. עבור $n = 3$ ראינו בכיתה כי אין ל-A_4 תת־חבורה מסדר $|S_3| = 6$, ולכן אין שיכון $S_3 \hookrightarrow A_4$.

ב. השיכון $\varphi : G \hookrightarrow H$ יוגדר לפי איחוד ההעתקות ϕ_n עבור $n \geq 5$. בשביל זה יש להראות כי ההעתקות הנ"ל תואמות, כלומר $\phi_{n+k}(\sigma) = \phi_n(\sigma)$ לכל $k \geq 0$, $n \geq 5$ ולכל $\sigma \in S_n$. מספיק להראות כי $\phi_{n+1}(\sigma) = \phi_n(\sigma)$ לכל $n \geq 5$. נניח בשלילה שההעתקות לא תואמות, ולכן קיימת תמורה $\tau \in S_n$ כך שמתקיים $\phi_{n+1}(\hat{\tau}) \neq \phi_n(\tau)$ (כאשר $\hat{\tau}$ מוגדר לפי ההערה לעיל). לכן קיים $3 \leq i \leq n+2$ כך ש-$\tau(i)+2 \neq \hat{\tau}(i)+2$ וזו סתירה.

ג. השיכון הוא פשוט לפי הכלה.

ד. החבורה A_n היא פשוטה עבור $n \geq 5$. הראינו בשאלה הקודמת כי איחוד **שרשרת** של חבורות פשוטות הוא חבורה פשוטה, ולכן H היא חבורה פשוטה.
החבורה G אינה פשוטה, כי יש לה תת־חבורה נורמלית לא טריוויאלית, שהיא H. הדרך הקצרה להוכיח זאת הוא לשים לב כי H היא הגרעין של העתקת הסימן $\mathrm{sign} : G \to \{\pm 1\}$. דרך אחרת היא לשים לב כי H מוכלת ממש בתוך G, למשל $(1\,2) \in G$ אבל $(1\,2) \notin H$. כדי להוכיח נורמליות נסתכל על תמורה $\pi \in H$. כלומר קיים m כך ש-$\pi \in A_m$. יהי $\tau \in G$, אזי קיים k כך ש-$\tau \in S_k$. נבחר $l \geq m, k$, למשל $l = \max(m,k)$. נשים לב כי $\mathrm{sign}(\tau\pi\tau^{-1}) = 1$ ולכן $\tau\pi\tau^{-1} \in A_l \subset H$, ולכן $H \lhd G$. קיבלנו כי G ו-H אינן איזומורפיות.

שאלה 9 (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 $s \in S = se = e,$. 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!