אלגברה מופשטת – פתרון תרגיל 3

<u>שאלה 1</u>

א. מצאו את שתי הספרות האחרונות של 1249^{602}.

ב. מצאו את $5774^{862}+2014 \pmod{95}$.

<u>פתרון</u>

א. יש לחשב את הביטוי $1249^{602} \pmod{100}$ ששווה לביטוי $49^{602} \pmod{100}$. אנחנו יודעים כי סדר כל איבר a מחלק את סדר החבורה U_n, שהוא $\varphi(n)$, ולכן מתקיים $a^{\varphi(n)} \equiv 1 \pmod n$. מכאן $49^{40} \equiv 1 \pmod{100}$, לכן $49^{602} \equiv (49^{40})^{15} \cdot 49^2 \equiv 1 \cdot 49^2 \pmod{100}$. בחישוב ישיר אפשר למצוא כי $49^2 \equiv 1 \pmod{100}$. לכן התשובה היא 01.

ב. נשים לב כי $2014 = 21 \cdot 95 + 19 \equiv 18 \pmod{95}$ וגם כי $5774 = 60 \cdot 95 + 74 \equiv 74 \pmod{95}$. לכן צריך לחשב את הביטוי $74^{862} + 19 \pmod{95}$. לפי משפט אוילר 2 נקבל כי מפני ש- $\varphi(95) = 72$, אז $74^{72} \equiv 1 \pmod{95}$. לכן $74^{862} = 74^{11 \cdot 72 + 70} = 74^{70} \pmod{95}$. לכן מפני ש- $74^{70} = 74^{72} \cdot 74^{-2} = 74^{-2} \pmod{95}$, נרצה למצוא הופכי של 74. ישנו פתרון למשוואה $74x \equiv 1 \pmod{95}$ אם ורק אם קיים $k \in \mathbb{Z}$ כך ש- $95k + 74x = 1$. נשתמש באלגוריתם אוקלידס כדי למצוא את x, כלומר למצוא ביטוי של $\gcd(95,72)$ כצירוף לינארי של 74 ושל 95:

$$(95,74) \underset{95=1\cdot 74+21}{=} (74,21) \underset{74=3\cdot 21+11}{=} (21,11) \underset{21=1\cdot 11+10}{=} (11,10) \underset{11=1\cdot 10+1}{=} (10,1) = 1$$ מהצבה לאחור

נקבל כי $1 = 11 - 1 \cdot 10 = -1 \cdot 21 + 2 \cdot 11 = 2 \cdot 74 - 7 \cdot 21 = -7 \cdot 95 + 9 \cdot 74$, כלומר $x = 9$. נחשב $74^{-2} \equiv 9^2 \equiv 81 \pmod{95}$. ולכן $5774^{862} + 2014 \equiv 81 + 19 \equiv 5 \pmod{95}$.

<u>שאלה 2</u>

א. תהי D_7 החבורה הדיהדרלית מסדר 14. תארו שלוש תת־חבורות לא טריוויאליות שלה. הוכיחו כי כולן חבורות אבליות.

ב. מצאו תת־חבורה נורמלית לא טריוויאלית של D_7. האם יש יותר מאחת?

<u>פתרון</u>

א. נציג את החבורה בצורה הרגילה, כחבורה הנוצרת על ידי האיברים $\langle\sigma,\tau\rangle$ כאשר מתקיימים היחסים $\sigma^7=\tau^2=e,\tau\sigma\tau^{-1}=\sigma^{-1}$. לפי משפט לגראנז' עבור $H\le D_7$ מתקיים כי $|H|\,\big|\,|D_7|=14$, כלומר $|H|\in\{1,2,7,14\}$. תת־החבורות הטריוויאליות מתקבלות במקרים ש-$|H|\in\{1,14\}$. אחרת, הסדר H הוא ראשוני, ולכן H ציקלית, ולכן היא חבורה אבלית.
כעת אפשר לבנות תת־חבורות מחזקות של איבר אחד של D_5. בדיקה "ידנית" תראה שהרשימה היא $\{e,\sigma,\sigma^2,\sigma^3,\sigma^4,\sigma^5,\sigma^6\}$, $\{e,\tau\}$, $\{e,\tau\sigma\}$, $\{e,\tau\sigma^2\}$, $\{e,\tau\sigma^3\}$, $\{e,\tau\sigma^4\}$, $\{e,\tau\sigma^5\}$, $\{e,\tau\sigma^6\}$. האם אתם יכולים להציג כל תת־חבורה כאשר D_7 מוצגת כחבורת תמורות?

ב. תת־החבורה הנוצרת על ידי σ היא תת־החבורה הנורמלית הלא טריוויאלית היחידה של D_7. אפשר להוכיח זאת למשל לפי זה שהיא מאינדקס 2. אפשר לראות שאם H היא תת־חבורה לא טריוויאלית אחרת, אז $\sigma H\ne H\sigma$.

<u>שאלה 3</u>

יהיו $H,K\le G$ תת־חבורות. הגדרנו מכפלת תת־חבורות $HK=\{hk:h\in H,\mathrm{k}\in K\}$.

א. הוכיחו כי HK תת־חבורה אם ורק אם $HK=KH$.

ב. הסיקו מהסעיף הקודם כי אם $N\lhd G$ תת־חבורה נורמלית, אז $HN\le G$ תת־חבורה.

ג. הוכיחו כי אם $N_1,N_2\lhd G$ תת־חבורות נורמליות, אז $N_1\cap N_2\lhd G$ וגם $N_1N_2\lhd G$ תת־חבורות נורמליות.

<u>פתרון</u>

א. $(\Rightarrow)$ נניח כי $HK=KH$. שימו לב כי הנתון $HK=KH$ **לא אומר** שלכל $h\in H,k\in K$ מתקיים $hk=kh$. מן הנתון נדע שאם $hk\in HK$, אז קיימים $h'\in H,k'\in K$ כך שמתקיים $hk=k'h'$.
נראה כי HK היא תת־חבורה בעזרת הקריטריון המקוצר. יש להראות כי $\varnothing\ne HK\subseteq G$. ההכלה מתקיימת מסגירות הפעולה של G. כמו כן HK לא ריקה כי היא מכילה את איבר היחידה, שכן $e\in H$ וגם $e\in K$, ולכן $e\cdot e=e\in HK$. כעת נשאר להראות שלכל $a,b\in HK$ מתקיים $ab^{-1}\in HK$.
נרצה להראות שאם $h_1k_1,h_2k_2\in HK$ אז $h_1k_1(h_2k_2)^{-1}\in HK$. מתקיים כי $h_1k_1(h_2k_2)^{-1}=h_1k_1k_2^{-1}h_2^{-1}$, ונסמן $k_3=k_1k_2^{-1}\in K,h_3=h_2^{-1}$. כעת לפי הנתון עבור

k_3h_3 קיימים $h_3'\in H, k_3'\in K$ כך שמתקיים $h_3'k_3'=k_3h_3$. לכן
$h_1k_1k_2^{-1}h_2^{-1}=h_1k_3h_3=h_1h_3'k_3'$. מפני ש- $h_1h_3'\in H, k_3'\in K$ קיבלנו כי
$h_1k_1(h_2k_2)^{-1}\in HK$, ולכן $HK\le G$.
דרך אחרת להוכחת סגירות להופכי ולפעולה היא שנשים לב שעבור חבורה X מתקיים $X=X^{-1}=\left\{a^{-1}:a\in X\right\}$. בנוסף $\left(hk\right)^{-1}=k^{-1}h^{-1}$ לכל זוג איברים, ולכן $\left(HK\right)^{-1}=K^{-1}H^{-1}=KH=HK$, כלומר סגירות להופכי. סגירות לפעולה היא לפי $HK\cdot HK=HHKK=HK$ כי לכל חבורה X מתקיים $X\cdot X=X$ (הוכחה לפי הכלה דו צדדית).
$\left(\Leftarrow\right)$ אם $HK\le G$, אז $HK=(HK)^{-1}=K^{-1}H^{-1}=KH$ שכן גם $H^{-1}\le G,\mathrm{K}^{-1}\le G$ הן תת־חבורות.

ב. אם $N\lhd G$ תת־חבורה נורמלית, אזי מתקיים $HN=NH$. זהו בדיוק התנאי מהסעיף הקודם שדרוש כדי להוכיח כי HN תת־חבורה.

ג. נתון כי $N_1,N_2\lhd G$, ולכן $N_1\cap N_2\le G$ כי חיתוך תת־חבורות הוא תת־חבורה. נשאר להראות כי $N_1\cap N_2\lhd G$. יהיו $h\in N_1\cap N_2$, $g\in G$. צריך להראות כי $ghg^{-1}\in N_1\cap N_2$. מפני ש- $h\in N_1\lhd G$, אז $ghg^{-1}\in N_1$ כי N_1 תת־חבורה נורמלית. באופן דומה $ghg^{-1}\in N_2$, ולכן $ghg^{-1}\in N_1\cap N_2$.
נראה כי $N_1N_2\lhd G$. לפי הסעיף הקודם ידוע לנו כי N_1N_2 תת־חבורה, ונשאר להראות שהיא נורמלית. יהיו $h\in N_1N_2$, $g\in G$. צריך להראות כי $ghg^{-1}\in N_1N_2$. כיוון ש- $h\in N_1N_2$ קיימים $h_1\in N_1,h_2\in N_2$ כך ש- $h=h_1h_2$. כיוון ש- N_1 נורמלית נקבל $gh_1g^{-1}\in N_1$ וכיוון ש- N_2 נורמלית נקבל $gh_2g^{-1}\in N_2$.
לכן $(gh_1g^{-1})(gh_2g^{-1})=gh_1h_2g^{-1}=h\in N_1N_2$ כפי שרצינו להראות.

<u>שאלה 4</u>

תארו את המחלקות השמאליות של תת־החבורה H בחבורה G:

א. $H=12\mathbb{Z},G=3\mathbb{Z}$.

ב. תהינה G_1,G_2 חבורות. $H=G_1\times\left\{e_2\right\},G=G_1\times G_2$ כאשר e_2 הוא איבר היחידה של G_2.

ג. $G=U_{36},H=\left\langle 13\right\rangle$.

פתרון

א. המחלקות הן $\{12\mathbb{Z}, 3+12\mathbb{Z}, 6+12\mathbb{Z}, 9+12\mathbb{Z}\}$. שימו לב כי G אבלית, ולכן H תת־חבורה נורמלית. מכאן שכל מחלקה שמאלית $a+H$ שווה למחלקה ימנית $H+a$.

ב. המחלקות הן מהצורה $(g_1, g_2)\cdot\left(G_1\times\{e_2\}\right)$. נראה כי קבוצת המחלקות איזומורפית ל-G_2: $\left\{(g_1, g_2)\cdot\left(G_1\times\{e_2\}\right): g_1\in G_1, g_2\in G_2\right\}$ היא בעצם $\left\{\left(g_1G_1\times\{g_2\}\right): g_1\in G_1, g_2\in G_2\right\}=\left\{\left(G_1\times\{g_2\}\right): g_2\in G_2\right\}\cong G_2$.

ג. ידוע לנו כי $|U_{36}|=\varphi(36)=12$, ואפשר לחשב כי $U_{36}=\{1,5,7,11,13,17,19,23,25,29,31,35\}$. תת־החבורה H היא $\langle 13\rangle=\{1,13,25\}$. לפי משפט לגראנז' נקבל כי יש ארבע מחלקות: $\langle 13\rangle=\{1,13,25\}$, $5\langle 13\rangle=\{5,29,17\}$, $7\langle 13\rangle=\{7,19,31\}$, $11\langle 13\rangle=\{11,35,23\}$.

שאלה 5

תהי G חבורה. ראינו כי ישנה התאמה חח"ע ועל בין מחלקות שמאליות ולבין מחלקות ימניות לפי ההעתקה $\varphi: gH\mapsto Hg^{-1}$ כאשר $g\in G$ ו-$H\le G$ תת־חבורה.

הוכיחו או הפריכו: ההעתקה $\psi: gH\mapsto Hg$ היא חח"ע ועל.

פתרון

נפריך על ידי דוגמה נגדית. נבחר $G=D_3$ החבורה הדיהדרלית מסדר 6 הנוצרת על ידי σ,τ באופן הסטנדרטי ותת־החבורה $H=\langle\tau\rangle=\{e,\tau\}$. נרצה למצוא $g_1, g_2\in G$ כך שמתקיים $g_1H=g_2H$, אבל $Hg_1\neq Hg_2$. כלומר למצוא $g_2^{-1}g_1\in H$ כך ש-$g_1g_2^{-1}\notin H$. נבחר $g_1=\sigma^{-1}\tau, g_2=\sigma^{-1}$ ואכן $g_2^{-1}g_1=\sigma\cdot\sigma^{-1}\tau=\tau\in H$ אבל $g_1g_2^{-1}=\sigma^{-1}\tau\cdot\sigma\notin H$. בעצם הראנו כי ψ אינה מוגדרת היטב במקרה זה.

שאלה 6

א. כתבו בכתיב מחזורים איברים מסדר 4 בחבורה S_6. מצאו כמה כאלו יש.

ב. הוכיחו כי החבורות S_4 ו-D_{12} הן לא איזומורפיות, למרות ששתיהן חבורות לא אבליות מסדר 24.

<u>פתרון</u>

א. האיברים היחידים מסדר 4 בחבורה S_6 הם רק המחזורים מאורך 4 ומכפלה של מחזור מאורך 4 עם חילוף (שזר לו). אלו הם איברים מן הצורה (i_1,i_2,i_3,i_4) או $(i_1,i_2,i_3,i_4)(j_1,j_2)$.

אפשר לבדוק ששאר האיברים בכתיב מחזורים זרים הם: איבר היחידה (סדר 1), תמורה המורכבת ממחזור אחד מאורך שתיים (סדר 2), תמורה המורכבת משניים או שלושה מחזורים מאורך שתיים (סדר 2), תמורה המורכבת ממחזור אחד או שניים מאורך שלוש (סדר 3), תמורה המורכבת ממחזור אחד מאורך חמש (סדר 5) ותמורה המורכבת ממחזור אחד מאורך שש (סדר 6).

בתרגול נראה כי מספר המחזורים מאורך $2\le r\le n$ בחבורה S_n הוא $\binom{n}{r}(r-1)!$. לכן מספר המחזורים מאורך 4 הוא $\binom{6}{4}(4-1)!=15\cdot 6=90$.

כלומר רשימת האיברים היא $(1,2,3,4)$, $(1,2,4,3)$, $(1,3,4,2)$, $(1,3,2,4)$, $(1,4,3,2)$, $(1,4,2,3)$. מספר המכפלות של מחזור מאורך 4 וחילוף שזר לו הם גם בדיוק 90, שכן הבחירה לחילוף מוגבלת לאפשרות אחת. סה"כ ישנם 180 איברים מסדר 4 בחבורה S_6.

ב. בחבורה D_{12} יש איבר מסדר 12, אבל אין איבר מסדר זה בחבורה S_4.

<u>שאלה 7</u>

עבור כל אחת מן הפונקציות הבאות הוכיחו כי היא הומומורפיזם. בדקו עבור כל פונקציה האם היא מונומורפיזם, האם היא אפימורפיזם והאם היא איזומורפיזם.

א. $f:(\mathbb{C}^*,\cdot)\to(\mathbb{C}^*,\cdot)$ המוגדרת על ידי $f(x)=x^3$.

ב. $f:(\mathbb{Q}^*,\cdot)\to(\mathbb{Q}^*,\cdot)$ המוגדרת על ידי $f(x)=x^3$.

ג. $f:G_1\times G_2\to G_2\times G_1$ כאשר $g_1\in G_1, g_2\in G_2$ איברי חבורות אבליות G_1,G_2 בהתאמה והפונקציה מוגדרת על ידי $f(g_1,g_2)=(g_2^{-1},g_1)$.

ד. $f:(\mathbb{R},+)\to(\mathbb{R}^+,\cdot)$ המוגדרת על ידי $f(x)=e^x$. הפונקציה הזו נקראת $\exp$.

<u>פתרון</u>

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

ב. הפונקציה היא מונומורפיזם, אבל לא אפימורפיזם. למשל $\frac{1}{2}$ לא בתמונה.

ג. הפונקציה היא איזומורפיזם. אפשר לראות כי $f^4=id$. שימו לב כי התנאי שהחבורה G_2 היא אבלית הוא הכרחי. אחרת לא בטוח כי f מוגדרת היטב.

ד. הפונקציה היא איזומורפיזם. האיזומורפיזם ההופכי הוא $\log$.

שאלה 8

א. מצאו אפימורפיזם $\varphi:(M_5(\mathbb{Q}),+)\to(\mathbb{Q}^5,+)$ כאשר $\mathbb{Q}^5$ היא מכפלה קרטזית של חמישה עותקים של $\mathbb{Q}$.

ב. מצאו איזומורפיזם $\varphi:G\to\mathbb{C}^*$ כאשר $G=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}: a,b\in\mathbb{R}, a^2+b^2>0\right\}$ שהוכחתם בתרגיל 1 שהיא חבורה.

פתרון

א. נשים לב כי $(M_5(\mathbb{Q}),+)\cong(\mathbb{Q}^{25},+)$ לפי איזומורפיזם שמסדר כל אחד מאיברי מטריצה ששייכת ל- $M_5(\mathbb{Q})$ בשורה מאורך 25, כלומר וקטור ב-$\mathbb{Q}^{25}$. הוכיחו כי העתקה של מכפלה קרטזית $G_1\times\ldots\times G_n$ למכפלה קרטזית $G_1\times\ldots\times G_k$ עבור $k\le n$ כשברכיב i היא העתקת הזהות של G_i היא הומומורפיזם על. כלומר יש להגדיר את ההעתקה $f(a_1,a_2,\ldots,a_{25})=(a_1,a_2,a_3,a_4,a_5)$ ולבדוק שהיא אכן אפימורפיזם.

ב. נגדיר את האיזומורפיזם $\varphi:G\to\mathbb{C}^*$ לפי $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\mapsto a+bi$. ברור כי זו פונקציה חח"ע ועל. נשאר להראות כי זהו הומומורפיזם: יהיו $M_1,M_2\in G$ ונרצה להראות כי $\varphi(M_1M_2)=\varphi(M_1)\varphi(M_2)$. נניח כי $M_1=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, M_2=\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$, אז נקבל כי

$$\varphi(M_1M_2)=\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right)=\varphi\left(\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}\right)=$$
$$ac-bd+(ad+bc)i=(a+bi)(c+di)=\varphi(M_1)\varphi(M_2).$$

שאלת אתגר

יהיו תמורות $\sigma,\tau\in S_n$ כך שמתקיים $\sigma=\tau^2$, אז נקרא ל- τ **שורש** של σ. מצאו תנאי מספיק והכרחי שקובע האם לתמורה נתונה $\sigma\in S_n$ קיים שורש. אם קיים שורש לתמורה, איך אפשר למצוא אותו?

פתרון

(מבוסס על התשובה http://math.stackexchange.com/a/266605)

כל תמורה היא מכפלה של מחזורים זרים $\tau = c_1c_2\dots c_k$. מפני שמחזורים זרים מתחלפים נקבל כי $\tau^2 = c_1c_2\dots c_kc_1c_2\dots c_k = c_1^2c_2^2\dots c_k^2$. מכאן, שלתמורה יהיה שורש אם היא מכפלה של מחזורים ריבועיים זרים (כמו c_i^2).

כעת צריך לבדוק מתי מחזור יהיה ריבועי. נניח כי אורך המחזור $c = (i_1\, i_2 \dots i_m)$ הוא m. בדקו שאם m הוא אי זוגי, אז גם c^2 הוא מאורך m. העזרו בכך ש-$(m,2)=1$.
אם m זוגי, אז נקבל כי $c^2 = (i_1\, i_3 \dots i_{m-1})(i_2\, i_4 \dots i_m)$, מכפלה של שני מחזורים זרים מאורך $m/2$.

סך הכל התנאי הוא שלתמורה יש שורש אם ורק אם בהצגה של התמורה למחזורים זרים, לכל m זוגי מספר המחזורים מאורך m הוא זוגי. במקרה ולתמורה σ יש שורש, נוכל לפי הקריטריון הנ"ל למצוא שורש: נציג את σ כמכפלת מחזורים זרים $d_1d_2\dots d_k$. לכל מחזור d_i מאורך m אי זוגי נוכל למצוא את השורש שלו $\sqrt{d_i} = (i_1\, i_{(m+1)/2}\, i_2\, i_{(m+3)/2} \dots i_m\, i_{(m-1)/2})$. לכל מחזור $d_i = (i_1\, i_2 \dots i_m)$ מאורך m זוגי, יהיה עוד מחזור $d_i' = (j_1\, j_2 \dots j_m)$ מאורך m בהצגה של σ ונוכל לבנות את השורש $\sqrt{d_id_i'} = (i_1\, j_1\, i_2\, j_2 \dots i_m\, j_m)$.

<u>שאלת אתגר</u>

הוכחתם בהרצאה את המסקנה הבאה ממשפט לגראנז': תהי G חבורה <u>סופית</u>, ויהיו $K \le H \le G$ תת־חבורות, אזי $[G:K]=[G:H][H:K]$.
כעת הוכיחו את אותה תוצאה כאשר מניחים רק ש-K תת חבורה מאינדקס סופי ב-G. כלומר, מבלי להניח ש-G סופית, ומבלי להניח סופיות של H.

<u>פתרון</u>

ראשית יש להראות כי אם $[G:K]$ סופי, אז גם $[G:H]$ ו-$[H:K]$ סופיים. אחרי שמוכיחים זאת, אפשר להניח כי $G = \bigcup_{i=1}^n g_iH$ איחוד זר של מחלקות וגם $H = \bigcup_{j=1}^m h_jK$ איחוד זר של מחלקות כי מניחים $[G:H]=n, [H:K]=m$. כדי להוכיח את הדרוש מספיק להראות ש-$G = \bigcup_{i=1}^n \bigcup_{j=1}^m g_ih_jK$ ושזהו איחוד זר, שכן אז נקבל כי $[G:K]=mn$. נוכיח תחילה את השיוויון. ברור שאגף ימין מוכל באגף שמאל G, ולכן נראה רק את ההכלה בכיוון ההפוך.

יהי $g \in G$, אזי מהשוויון $G=\bigcup_{i=1}^{n} g_i H$ נקבל שקיים $1 \le i \le n$ וקיים $h \in H$ כך ש- $g = g_i h$. כעת מפני ש- $h \in H$ ומהשוויון $H=\bigcup_{j=1}^{m} h_j K$, קיים $1 \le j \le m$ כך ש- $h = h_j K$. כך נקבל כי $g = g_i h \in g_i h_j K$ וסיימנו להוכיח את ההכלה הדו־צדדית.

כעת יש להוכיח כי האיחוד זר (זה החלק היותר קשה). כזכור, כל שתי מחלקות או שמתלכדות או שהן זרות. נניח $g_{i_1} h_{j_1} K = g_{i_2} h_{j_2} K$ ונראה בהכרח $g_{i_1} = g_{i_2}, h_{j_1} = h_{j_2}$.

מהשוויון $g_{i_1} h_{j_1} K = g_{i_2} h_{j_2} K$ נקבל כי $h_{j_1}^{-1} g_{i_1}^{-1} g_{i_2} h_{j_2} = \left(g_{i_1} h_{j_1}\right)^{-1} g_{i_2} h_{j_2} \in K$. כיוון ש- $K \le H$ נקבל כי $h_{j_1}^{-1} g_{i_1}^{-1} g_{i_2} h_{j_2} \in H$ שכן $h_{j_1}, h_{j_2} \in H$, ומכאן נסיק (הראו איך) כי $g_{i_1}^{-1} g_{i_2} \in H$. מכאן נובע כי $g_{i_2} \in g_{i_1} H$, ולכן בהכרח $g_{i_1} = g_{i_2}$ שכן עבור $i_1 \ne i_2$ מתקיים כי g_{i_1}, g_{i_2} שייכים למחלקות שונות, שהן זרות. כעת מפני ש- $h_{j_1}^{-1} g_{i_1}^{-1} g_{i_2} h_{j_2} = \left(g_{i_1} h_{j_1}\right)^{-1} g_{i_2} h_{j_2} \in K$, ומן השלב האחרון קיבלנו כי $g_{i_1}^{-1} g_{i_2} = e$ (עבור e איבר היחידה), נקבל כי $h_{j_1}^{-1} g_{i_1}^{-1} g_{i_2} h_{j_2} = h_{j_1}^{-1} h_{j_2} \in K$ וטיעון דומה עבור H נקבל כי $h_{j_2} \in h_{j_1} K$. מפני ש- $H=\bigcup_{j=1}^{m} h_j K$ הוא איחוד זר, נקבל כי $h_{j_1} = h_{j_2}$ כדרוש.

בהצלחה!