אלגברה ב' 1 - הרצאה 5 - 12.9.12

<u>למה</u>: נניח ש- G פועלת על X. מתקיים:

I. $G_x=\{g\in G \mid g*x=x\}$ זו תת-חבורה, הנקראת תת-חבורת המיצב של x.

II. $g_2^{-1}g_1\in G_x \Leftrightarrow g_1*x=g_2*x$

III. אורך המסלול (עוצמת מחלקת השקילות המתאימה) של x הוא $[G:G_x]$.

IV. יש התאמה חח"ע $R\to X'$, כאשר X' הוא המסלול המתאים ל- x ו- R זו מערכת מייצגים של המחלקות השמאליות של G_x ב- G, על ידי $g\mapsto g*x$, $G=\biguplus_{g\in R} gG_x$.

<u>הוכחה</u>:

I. יהיו $g,h\in G_x$. מתקיים:

$$(gh)*x=g*(h*x)=g*x=x\Rightarrow gh\in G_x$$
$$g^{-1}*x=g^{-1}*(g*x)=(g^{-1}g)*x=e*x=x\Rightarrow g^{-1}\in G_x$$

ולכן זו תת-חבורה.

II. $g_2^{-1}g_1\in G_x \Leftrightarrow g_2^{-1}g_1*x=x \Leftrightarrow g_2^{-1}*(g_1*x)=g_2^{-1}*(g_2*x) \Leftrightarrow g_1*x=g_2*x$.

III. נגדיר העתקה $\xi: G/G_x\to X'$ על ידי: $\xi(gG_x)=g*x$. נראה ש- ξ מוגדרת היטב:

יהיו $g,h\in G$ כך ש- $gG_x=hG_x$. לפיכך, $h^{-1}g\in G_x$, ולפי סעיף II מתקיים

$g*x=h*x$

נראה ש- ξ חח"ע (ברור שהיא על). אם $\xi(gG_x)=\xi(hG_x)$, אזי:

$$g*x=h*x\Rightarrow h^{-1}g\in G_x\Rightarrow hG_x=gG_x$$

כלומר ההעתקה חח"ע. לפיכך, $[G:G_x]=\left|G/G_x\right|=\left|X'\right|$.

IV. ההעתקה ξ בסעיף ג' הגדירה נציג לכל מחלקה של G_x. נסמן ב- $R=\{g_i \mid i\in I\}$ את קבוצת הנציגים הנ"ל. מתקיים $|R|=[G:G_x]$, וכמו כן $\xi(g_iG_x)=g_i*x$, שזו העתקה הפיכה. לכן, קל לראות שהטענה מתקיימת.

<u>למת האיפיון לתת-חבורות של חבורות ציקליות</u>: תהי $G=\langle a\rangle$ חבורה ציקלית מסדר n. לכל מחלקל d של n קיימת חבורה חלקית אחת ויחידה מסדר d, והיא $\left\langle a^{\frac{n}{d}}\right\rangle$.

<u>הוכחה</u>: $\left\langle a^{\frac{n}{d}} \right\rangle$ זו תת-חבורה של G מסדר d, ולכן קיימת חבורה כזו. נראה שחבורה זו יחידה.

תהא $H \le G$ מסדר d. יהי $h \in H$. קיים $m \in \mathbb{Z}$ כך ש- $a^m = h$. סדר של איבר בחבורה מחלק את סדר החבורה, לכן $ord(h) \mid |H|$, כלומר $\frac{n}{\gcd(m,n)} \mid d$. לפיכך $\frac{n}{d} \mid \gcd(m,n)$, כלומר:

$$h = a^m \in \{(a^{\frac{n}{d}})^k \mid k \in \mathbb{Z}\}$$

לכן $\left\langle a^{\frac{n}{d}} \right\rangle \supseteq H$, ומשוויון סדרים נקבל $H = \left\langle a^{\frac{n}{d}} \right\rangle$.

<u>תרגיל</u>: נניח ש- $G = \langle g \rangle$ ציקלית מסדר n, פועלת על קבוצה X. יהי $x \in X$, ונניח ש- $[G:G_x] = d$. הראה כי $\{x, g*x, ..., g^{d-1}*x\}$ הם כל איבריו השונים של מסלול- G של x.

<u>הוכחה</u>: המסלול של x הוא $\{g^k * x \mid 0 \le k \le n-1\}$. נראה $g^i * x \ne g^j * x$ לכל $0 \le i < j \le n-1$.

$$g^i * x = g^j * x \Leftrightarrow g^{i-j} \in G_x$$
$$d \cdot |G_x| = [G:G_x] \cdot |G_x| = |G| = n \Rightarrow |G_x| = \frac{n}{d}$$
$$\Rightarrow G_x = \left\langle g^{\frac{n}{\frac{n}{d}}} \right\rangle = \left\langle g^d \right\rangle$$

לפי למת האיפיון לתת חבורות של חבורות ציקליות.

לכן, $g^i * x = g^j * x \Leftrightarrow g^{i-j} \in G_x \Leftrightarrow d \mid i-j$, כלומר $i \equiv j (\bmod d)$, אך שיוויון זה לא ייתכן, ולכן $g^i * x \ne g^j * x$.

<u>מסקנה</u>: אם G פועלת על קבוצה סופית X ואם $\{x_i\}_{i \in I}$ היא מערכת מייצגים למסלולי G, אז $|X| = \sum_{i \in I} [G:G_{x_i}]$. אם $\{x_i \mid i \in I'\}$ היא מערכת מייצגים של מחלקות השקילות שגודלן גדול מ1, אזי $|X| = \sum_{i \in I'} [G:G_{x_i}] + \{x \in X \mid \forall g \in G : g*x = x\}$.

<u>הגדרה</u>: נתבונן בפעולת ההצמדה של חבורה G על עצמה.

אם $a \in G$ אז $C_G(a) = \{g \in G \mid aga^{-1} = g\} = \{g \in G \mid ga = ag\}$ נקרא המְרַכֵּז של a ב- G.

בפרט $C_G(a) \le G$.

אם $H \le G$ אז $N_G(H) = \{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid gH = Hg\}$ נקרא המשמר (נורמליזטור) של H ב- G. בפרט, $N_G(H) \le G$.

<u>מסקנה</u>: תהי G חבורה סופית. למסלולים של פעולת ההצמדה של G על עצמה קוראים מחלקות צמידות. אם נסמן ב- $\{x_i \mid i \in I'\}$ מערכת מייצגים של מחלקות הצמידות בעלות יותר מאיבר אחד, יתקיים:

$$|G| = \sum_{i\in I'}[G:C_G(x_i)] + \left|\{x \in G \mid \forall g \in G : gxg^{-1} = x\}\right| = \sum_{i \in I'}[G:C_G(x_i)] + |Z(G)|$$

משוואה זו נקראת משוואת המחלקים.

<u>טענה</u>: נניח שחבורה G פועלת על קבוצה X, ונסמן את הפעולה ב- π. הפעולה π מגדירה הומומורפיזם $\varphi : G \to S(X)$ על ידי: $\varphi(g)(x) = \pi(g,x)$.

<u>הוכחה</u>: $\varphi(gh)(x) = \pi(gh,x) = \pi(g,\pi(h,x)) = \varphi(g)\cdot\pi(h,x) = (\varphi(g)\circ\varphi(h))(x)$.

<u>מסקנה</u>: נניח G $H \le G$ ונניח $n = [G:H] < \infty$. תהא $K = \bigcap_{g\in G} gHg^{-1}$, אזי מתקיים $K \lhd G$, $K \le H$, G/K איזומורפית לתת חבורה של S_n. בפרט, אם G סופית ו-$|G| \nmid n!$, אז $K \ne \{e\}$.

<u>הוכחה</u>: יהיו $a \in K$, $g \in G$. נראה $gag^{-1} \in \bigcap_{b\in G} bHb^{-1}$.
יהי $b \in G$. $gag^{-1} \in bHb^{-1} \Leftrightarrow a \in g^{-1}bH(g^{-1}b)^{-1}$, והתנאי בצד שמאל אכן מתקיים כי $a \in K$.
החבורה G פועלת על הקבוצה G/H על ידי כפל משמאל: $\sigma * (gH) = (\sigma g)H$. פעולה זו מגדירה הומומורפיזם $\varphi : G \to S(X)$. אולם, $|G/H| = n$, ולכן $S(X) \cong S_n$.

$$\begin{aligned}\ker\varphi &= \{\sigma \in G \mid \forall g \in G : \sigma * (gH) = gH\} = \{\sigma \in G \mid \forall g \in G : \sigma gH = gH\} \\ &= \{\sigma \in G \mid \forall g \in G : g\sigma g^{-1}H = H\} = \{\sigma \in G \mid \forall g \in G : \sigma H = gHg^{-1}\} \\ &= \{\sigma \in G \mid \sigma \in \bigcap_{g\in G} gHg^{-1}\} = K\end{aligned}$$

לכן $K \lhd G$ ולפי משפט האיזומורפיזם הראשון, $G/K \cong \operatorname{Im}\varphi \le S(X) \cong S_n$. בפרט, אם $|G| \nmid n!$, אז הגרעין אינו טריוויאלי. אם הגרעין היה טריוויאלי, אז $G \le S(X) \cong S_n$, ולפי משפט לגראנז' $|G|\,\big|\,|S_n|$, בסתירה ל-$|G| \nmid n!$.

<u>הגדרה</u>: חבורה G נקראת פשוטה אם אין לה תת-חבורות נורמליות פרט ל- G ו- $\{e\}$.

<u>מסקנה</u>: אם G חבורה, ויש ל- G תת-חבורה H כך ש-$|G| \nmid [G:H]!$, אזי G אינה פשוטה.

<u>דוגמה</u>: $\mathbb{Z}_p$ לכל p ראשוני, היא פשוטה.

<u>למה</u>: A_n נוצרת על ידי המחזורים מאורך 3 ב- S_n.

<u>הוכחה</u>: תחילה, נשים לב שכל מחזור מאורך 3 הוא זוגי, ולכן נמצא ב- A_n. כל איבר ב- A_n הוא מכפלה של מספר זוגי של חילופים, לכן מספיק להראות שמכפלה של שני חילופים ניתנת להצגה כמכפלה של מחזורים מאורך 3. ואכן, יהיו i, j, k, l שונים זה מזה, מתקיים:

$$(kl)(ij) = (kl)(kj)(jk)(ij) = (jlk)(ikj) \ \ ,(ik)(ij) = (ijk) \ \ ,(ij)(ij) = (e)$$

<u>תרגיל</u>: תהא G חבורה מסדר 36 ונניח של- G תת חבורה H מסדר 9. הוכח ש- G אינה פשוטה.

<u>פתרון</u>: $36 \nmid 24$, $4! = 24$, $[G:H] = 4$, $|G| = 36$. לכן, לפי המסקנה, ב- H מוכלת תת חבורה נורמלית לא-טריוויאלית של G.

<u>תרגיל</u>: תהא G חבורה מסדר 99, ונניח ש- H תת-חבורה מסדר 11. הוכח ש- $H \lhd G$.

<u>פתרון</u>: $|G| = 99$, $[G:H] = 9$, $9!$, $11 \nmid 9! \Leftarrow |G| = 99 \nmid 9!$. לכן, לפי המסקנה, ב- H מוכלת תת-חבורה נורמלית לא-טריוויאלית של G , K. הסדר של K גדול מ-1, ולפי משפט לגראנז' מחלק את הסדר של H, כלומר את 11. 11 ראשוני, לכן $|K| = 11$, כלומר $K = H$, ולכן $H \lhd G$.

<u>משפט</u>: לכל $n \geq 5$ סופי, A_n פשוטה. (הערה: זאת הסיבה שלמשוואות ממעלה ≤ 5 אין נוסחת שורשים).

על מנת להוכיח משפט זה, נוכיח מספר טענות עזר, בהן נניח ש- $n \geq 5$.

<u>טענה</u>: אם $N \lhd A_n$ מכילה מחזור מאורך 3 אז $N = A_n$.

<u>הוכחה</u>: נניח $(abc) \in N$. לפי הלמה מספיק להראות ש- N מכילה כל מחזור (def) מאורך 3. נבחר $\sigma \in S_n$ כך ש- $\sigma(a) = d, \sigma(b) = e, \sigma(c) = f$. מתקיים $\sigma(abc)\sigma^{-1} = (def)$. לכן, אם $\sigma \in A_n$ אז $(def) \in N$ [נורמליות]. אם σ אי-זוגית, נבחר g, h שונים מ- a, b, c (אפשר, כי $n \geq 5$), ואז $\tau := \sigma(gh) \in A_n$ (כלומר, "נרמהי" ונבנה תמורה זוגית המתנהגת באופן דומה, ונשתמש בחלק הקודם), ומתקיים $\tau(abc)\tau^{-1} = (def)$, ולכן $(def) \in N$.

<u>טענה</u>: אם $N \lhd A_n$, $N \neq \{e\}$, אז יש מחזור מאורך 3 ב- N.

<u>הוכחה</u>: יהי $e \neq \sigma \in N$. נציג את π כמכפלת מחזורים זרים $\sigma = \pi_1 \pi_2 \cdot \ldots \cdot \pi_r$. נניח שכל מחזור זר הוא מגודל $2 \leq$. נחלק למקרים את הבעיה, ונראה שבכל מקרה יש ב- N מחזור מאורך 3:

I. קיים i עבורו π_i מגודל לפחות 4. נבצע החלפת שמות לשם נוחות ("כלל אלפא") ונקבל $\pi_1 = (1\,2 \ldots k)$, כאשר $k \geq 4$. יהי $\varphi = (1\,2\,3)$. מנורמליות N מתקיים $\varphi\sigma\varphi^{-1} \in N$, ומזרות המחזורים מתקיים:

$$\varphi\sigma\varphi^{-1} = \varphi\pi_1\varphi^{-1}\pi_2 \cdot \ldots \cdot \pi_r = \varphi\pi_1\varphi^{-1}\pi_1^{-1}\sigma =$$
$$= (1\,2\,3)(1\,2\,3 \ldots k)(1\,3\,2)(r \ldots 3\,2\,1)\sigma = (1\,2\,4)\sigma$$

ולכן $(1\,2\,4) = \varphi\sigma\varphi^{-1}\sigma^{-1} \in N$.

II. לכל i, π_i מגודל לכל היותר 3, וקיימים לפחות שני מחזורים מאורך 3 (כלומר, $n \geq 6$).

בלי הגבלת הכלליות נסמן $\pi_2 = (4\,5\,6)$, $\pi_1 = (1\,2\,3)$. יהי $\varphi = (1\,2\,4)$.

$$\begin{aligned}\varphi\sigma\varphi^{-1} &= \varphi\pi_1\pi_2\varphi^{-1}\pi_3\cdot\ldots\cdot\pi_r = \varphi\pi_1\pi_2\varphi^{-1}{\pi_2}^{-1}{\pi_1}^{-1}\sigma = \\ &= (1\,2\,4)(1\,2\,3)(4\,5\,6)(1\,4\,2)(4\,6\,5)(1\,3\,2)\sigma = \\ &= (1\,2\,5\,3\,4)\sigma\end{aligned}$$

כלומר $N \ni \varphi\sigma\varphi^{-1}\sigma^{-1} = (1\,2\,5\,3\,4)$. כעת, ניתן להמשיך עם מקרה I עבור המחזור מאורך 5 שמצאנו.

III. קיים i יחיד עבורו π_i מאורך 3, ועבור כל i אחר π_i מאורך 2. בלי הגבלת הכלליות, נסמן $\pi_1 = (1\,2\,3)$. כל שאר המחזורים ב- σ הם חילופים, ולכן $N \ni \sigma^2 = {\pi_1}^2 = (1\,3\,2)$, כלומר יש מחזור מאורך 3 ב- N.

IV. σ היא מכפלה של חילופים. לפיכך, σ היא מכפלה של לפחות שני חילופים, לכן נסמן בה״כ $\pi_2 = (3\,4)$, $\pi_1 = (1\,2)$. נסמן $\varphi = (1\,2\,3)$. מתקיים:

$$\begin{aligned}\varphi\sigma\varphi^{-1} &= \varphi\pi_1\pi_2\varphi^{-1}\pi_3\cdot\ldots\cdot\pi_k = \varphi\pi_1\pi_2\varphi^{-1}{\pi_2}^{-1}{\pi_1}^{-1}\sigma = \\ &= (1\,2\,3)(1\,2)(3\,4)(1\,3\,2)(3\,4)(1\,2)\sigma = (1\,3)(2\,4)\sigma\end{aligned}$$

כלומר מתקיים $N \ni \varphi\sigma\varphi^{-1}\sigma^{-1} = (1\,3)(2\,4) =: \tau$. כעת, נבחר $\psi = (1\,3\,5)$. נצמיד:

$$\psi\tau\psi^{-1} = (1\,3\,5)(1\,3)(2\,4)(1\,5\,3) = (1\,5)(2\,4)(1\,5\,3) = (3\,5)(2\,4) \in N$$

נכפול ב- τ את שני האגפים:

$$\tau\psi\tau\psi^{-1} = (1\,3)(2\,4)(3\,5)(2\,4) = (1\,3\,5) \in N$$

והשייכות נובעת מן הסגירות לפעולה, כלומר יש מחזור מאורך 3 ב- N.

קיבלנו שעבור $n \geq 5$, כל תת-חבורה נורמלית (שאינה $\{e\}$) של A_n מכילה מחזור מגודל 3, וכל תת-חבורה נורמלית של A_n המכילה מחזור מגודל 3 היא בהכרח A_n עצמה. לפיכך, ל- A_n, עבור $n \geq 5$, אין תת-חבורות נורמליות לא-טריוויאליות, כלומר A_n פשוטה.[1]

<u>משפט</u> ($Cayley$): תהא G חבורה סופית מסדר n, אזי G איזומורפית לתת-חבורה של S_n.

<u>הוכחה</u>: נרשום $G = \{g_1, g_2, \ldots, g_n\}$. נגדיר פעולה של G על עצמה על ידי $\sigma * g = \sigma \cdot g$, כאשר $\sigma, g \in G$. פעולה זו מגדירה הומומורפיזם $\varphi : G \to S(G)$ על ידי $\varphi(\sigma)(g) = \sigma * g = \sigma g$.

$$\ker\varphi = \{\sigma \in G \mid \forall g \in G : \varphi(\sigma)(g) = g\} = \{\sigma \in G \mid \forall g \in G : \sigma g = g\} = \{e\}$$

---

[1] ישנן עוד הרבה הוכחות למשפט זה. למתעניינים (הוכחה המוצגת כאן היא הרביעית):
http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/Ansimple.pdf

כלומר φ מונומורפיזם, ולפיכך כל חבורה סופית היא חבורת תמורות, כלומר איזומורפית לתת-חבורה של S_n.

<u>הגדרה</u>: יהיו $G_1,G_2,...,G_n$ חבורות. אזי:

$$G=G_1\times G_2\times ...\times G_n=\{(g_1,g_2,...,g_n)\mid g_i\in G_i\}$$

זו חבורה, הנקראת המכפלה הישרה (החיצונית) של $G_1,G_2,...,G_n$. הפעולה בחבורה זו מתבצעת איבר איבר, לפי הפעולות של $G_1,G_2,...,G_n$.

<u>אבחנה</u>: קיים מונומורפיזם $\varphi_i:G_i\to G$ הנתון על ידי: $\varphi_i(g_i)=(e_1,e_2,...,e_{i-1},g_i,e_{i+1},...e_n)$, ולכן תמונתו איזומורפית ל-G_i. מעתה, נחשוב על G_i כעל תת-חבורה של $G_1\times G_2\times ...\times G_n$ בעזרת השיכון φ_i.

<u>הערות</u>:

I. $G=\langle G_1,G_2,...,G_n\rangle$ (ואפילו $G=G_1\cdot G_2\cdot ...\cdot G_n$).

II. $G_i\lhd G$ לכל i.

III. $G_i\cap\langle G_j\mid j\neq i\rangle=\{e\}$.

IV. $x_j\in G_j$, $x_i\in G_i$, $i\neq j$, אזי $x_ix_j=x_jx_i$.

V. אם $x_1\cdot x_2\cdot ...\cdot x_n=y_1\cdot y_2\cdot ...\cdot y_n$ כאשר $x_i,y_i\in G_i$, אזי $x_i=y_i$.

<u>משפט</u>: תהא G חבורה ו-$G_1,G_2,...,G_n\leq G$. התנאים הבאים שקולים:

I. א. $G=\langle G_1,...,G_n\rangle$

ב. $\forall i\in\{1,...,n\}:G_i\lhd G$

ג. $\forall i\in\{1,...,n\}:G_i\cap\langle G_j\mid j\neq i\rangle=\{e\}$

II. א. $G=\langle G_1,...,G_n\rangle$

ד. לכל $x_j\in G_j$, $x_i\in G_i$, $i\neq j$, מתקיים $x_ix_j=x_jx_i$.

ה. אם $x_1\cdot x_2\cdot ...\cdot x_n=y_1\cdot y_2\cdot ...\cdot y_n$ כאשר $x_i,y_i\in G_i$, אזי $x_i=y_i$.

III. G איזומורפית ל-$G_1\times G_2\times ...\times G_n$.

<u>הוכחה</u>: $\mathrm{III}\Rightarrow\mathrm{I}$ ברור.

$\mathrm{I}\Rightarrow\mathrm{II}$: נראה את ד'. לפי ב', $(x_i^{-1}y_j^{-1}x_i)y_j\in G_j$, אך גם $x_i^{-1}(y_j^{-1}x_iy_j)\in G_i$, ולכן לפי ג' $x_i^{-1}y_j^{-1}x_iy_j\in G_i\cap G_j=\{e\}$, כלומר $x_ix_j=x_jx_i$.

נראה את ה': נניח $x_1\cdot x_2\cdot ...\cdot x_n=y_1\cdot y_2\cdot ...\cdot y_n$ כאשר $x_i,y_i\in G_i$. לפי ד',
$x_1y_1^{-1}=x_2^{-1}y_2\cdot ...\cdot x_n^{-1}y_n$, כלומר $x_1y_1^{-1}\in\langle G_2,...,G_n\rangle$, ולכן $x_1y_1^{-1}\in G_1\cap\langle G_2,...,G_n\rangle=\{e\}$
לפי ג', כלומר $x_1=y_1$, ובאופן דומה עבור שאר ה-i.

II $\Leftarrow$ III: נגדיר העתקה $\theta: G_1 \times G_2 \times ... \times G_n \to G$ על ידי $\theta(g_1, g_2, ..., g_n) = g_1 \cdot g_2 \cdot ... \cdot g_n$.

נראה ש- θ הומומורפיזם:

$$\theta((g_1, g_2, ..., g_n)(h_1, h_2, ..., h_n)) = \theta(g_1 h_1, g_2 h_2, ..., g_n h_n) = g_1 h_1 g_2 h_2 \cdot ... \cdot g_n h_n$$

מד' נובע:

$$\theta((g_1, g_2, ..., g_n)(h_1, h_2, ..., h_n)) = g_1 g_2 \cdot ... \cdot g_n h_1 h_2 \cdot ... \cdot h_n = \theta(g_1, g_2, ..., g_n)\theta(h_1, h_2, ..., h_n)$$

נראה ש- θ על: לפי א' וד', כל איבר ב- G ניתן לכתוב כ- $\underset{\in G_1}{g_1} \cdot \underset{\in G_2}{g_2} \cdot ... \cdot \underset{\in G_n}{g_n}$, כלומר כ- $\theta(g_1, ..., g_n)$.

נראה ש- θ חח"ע: יהי $(g_1, ..., g_n) \in \ker\theta$.

$$\Rightarrow g_1 g_2 \cdot ... \cdot g_n = e$$

מ-ה' נובע ש- $\forall 1 \le i \le n: g_i = 1$, ולכן $\ker\theta = \{e\}$.

קיבלנו ש- θ איזומורפיזם, כלומר $G_1 \times G_2 \times ... \times G_n \cong G$.

<u>הגדרה</u>: אם G חבורה, $G_1, G_2, ..., G_n$ תת חבורות שלה, ומתקיימים התנאים א'-ג' או א',ד',ה', אז נאמר ש- G זו המכפלה הישרה (הפנימית) של $G_1, G_2, ..., G_n$. (הראנו שהגדרת המכפלה הישרה החיצונית והפנימית שקולות).

<u>תרגיל</u>: $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ אם m,n זרים.

<u>פתרון</u>: מהו $O(1,1)$?

$$(k,k) = (0,0) \Leftrightarrow k \cdot (1,1) = (0,0) \Leftrightarrow m \mid k, n \mid k \underset{\gcd(m,n)=1}{\Leftrightarrow} mn \mid k$$

לכן $O(1,1) = mn$.

$$|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = mn$$

ולכן $(1,1)$ יוצר את $\mathbb{Z}_m \times \mathbb{Z}_n$, כלומר $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

<u>טענה</u>: תהא G סופית, $G_1, G_2, ..., G_n \lhd G$, ונניח שהסדרים $|G_1|, |G_2|, ..., |G_n|$ זרים בזוגות, וגם נניח ש- $|G| = \prod_{i=1}^{n} |G_i|$, אזי G זו המכפלה הישרה של $G_1, G_2, ..., G_n$.

<u>הוכחה</u>:

הערה: אם $A, B \le H$ מסדרים זרים, אזי $A \cap B = \{e\}$, לפי לגראנז'. יתר על כן, אם גם $A \lhd H$ אזי $AB \le H$, והסדר שלה $|AB| = |A||B|$.

לכן, באינדוקציה על k :

I. $G_1,G_2,...,G_k \le G$ מסדר $|G_1|\cdot|G_2|\cdot...\cdot|G_k|$.

II. לכל j , $\prod_{\substack{i=1\\i\neq j}}^{k} G_i$ מסדר $\prod_{\substack{i=1\\i\neq j}}^{k} |G_i|$.

לכן, עבור $k=n$, $G_1\cdot G_2\cdot...\cdot G_n=G$ וגם $G_j\cap\langle G_i \mid i\neq j\rangle=\{e\}$. לפיכך, לפי התנאים שהיו לנו במשפט שאפיין מכפלות ישרות נסיק ש- G אכן המכפלה הישרה של $G_1,G_2,...,G_n$.

<u>מסקנה</u> : יהי m טבעי, $m=p_1^{n_1}p_2^{n_2}p_3^{n_3}\cdot...\cdot p_k^{n_k}$ הצגתו כמכפלה של חזקות של ראשוניים. אזי מתקיים : $\mathbb{Z}_m=\mathbb{Z}_{p_1^{n_1}}\cdot\mathbb{Z}_{p_2^{n_2}}\cdot...\cdot\mathbb{Z}_{p_k^{n_k}}$ (החבורות נורמליות כי הכפל אבלי).

<u>תרגיל</u> : $G=G_1\times G_2\times...\times G_n$ ולכל i תהי $N_i\lhd G_i$. נגדיר $N=N_1\times N_2\times...\times N_n$. הוכח כי $N\lhd G$ ומתקיים $G/N\cong G_1/N_1\times G_2/N_2\times...\times G_n/N_n$.

<u>פתרון</u> : נגדיר העתקה $\varphi:G\to G_1/N_1\times G_2/N_2\times...\times G_n/N_n$ על ידי

$$\varphi(g_1,g_2,...,g_n)=(g_1N,g_2N,...,g_nN)$$

קל להראות שהעתקה זו היא אפימורפיזם. נראה חח"ע :

$$\ker\varphi=\{(g_1,...,g_n)\in G \mid (g_1N,g_2N,...,g_nN)=(N,...,N)\}=$$
$$\{(g_1,...,g_n)\in G \mid g_1\in N,g_2\in N,...,g_n\in N\}=N_1\times N_2\times...\times N_n=N$$

לכן, לפי משפט האיזומורפיזם הראשון, $G/N\cong G_1/N_1\times G_2/N_2\times...\times G_n/N_n$.

<u>הערה</u> : אם עסקינן בחבורות חיבוריות, לעיתים נסמן $\oplus$ במקום $\times$.