

## אלגברה ב' 1 - הרצאה 5 - 12.9.12

למה: נניח ש- $G$  פועלת על  $X$ . מתקיים:

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

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

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

IV. יש התאמה חח"ל  $R \rightarrow X'$ , כאשר  $X'$  הוא המסלול המתאים ל- $x$  ו- $R$  זו מערכת

$$G = \bigcup_{g \in R} g G_x, \quad g \mapsto g * x \text{ על ידי } G \text{-ב-} G_x$$

הוכחה:

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.

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

III. נגדיר העתקה  $\xi: G/G_x \rightarrow X'$  על ידי:  $\xi(gG_x) = g * x$ . נראה ש- $\xi$  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- $\xi$  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,  $[G : G_x] = |G/G_x| = |X'|$ .

IV. ההעתקה  $\xi$  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  $\xi(g_i G_x) = g_i * x$ , שזו העתקה

הפיכה. לכן, קל לראות שהטענה מתקיימת.

למת האיפיון לתת-חבורות של חבורות ציקליות: תהי  $G = \langle a \rangle$  חבורה ציקלית מסדר  $n$ . לכל

מחלק  $d$  של  $n$  קיימת חבורה חלקית אחת ויחידה מסדר  $d$ , והיא  $\langle a^{\frac{n}{d}} \rangle$ .

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

תהא  $H \leq G$  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  $|H| \mid \text{ord}(h)$ , כלומר  $d \mid \frac{n}{\text{gcd}(m,n)}$ . לפיכך  $\frac{n}{d} \mid \text{gcd}(m,n)$ , כלומר:

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

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

תרגיל: 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  $\{x, g * x, \dots, g^{d-1} * x\}$  הם כל איבריו השונים של מסלול- $G$  של  $x$ .

הוכחה: המסלול של  $x$  הוא  $\{g^k * x \mid 0 \leq k \leq n-1\}$ . נראה  $g^i * x \neq g^j * x$  לכל  $0 \leq i < j \leq n-1$ .

$$g^i * x = g^j * x \Leftrightarrow g^{i-j} \in G_x$$

$$d \cdot |G_x| = [G : G_x] \cdot |G_x| = |G| = n \Rightarrow |G_x| = \frac{n}{d}$$

$$\Rightarrow G_x = \left\langle g^{\frac{n}{d}} \right\rangle = \langle g^d \rangle$$

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  $i \equiv j \pmod{d}$ , אך שיוויון זה לא ייתכן, ולכן  $g^i * x \neq g^j * x$ .

מסקנה: אם  $G$  פועלת על קבוצה סופית  $X$  ואם  $\{x_i\}_{i \in I}$  היא מערכת מייצגים למסלולי  $G$ , אז

$$|X| = \sum_{i \in I} [G : G_{x_i}]$$

$$1, \text{ אזי } |X| = \sum_{i \in I'} [G : G_{x_i}] + \{x \in X \mid \forall g \in G : g * x = x\}$$

הגדרה: 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 המרכז של  $a$  ב- $G$ . בפרט  $C_G(a) \leq G$ .

אם  $H \leq G$  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,  $N_G(H) \leq G$ .

מסקנה: 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:

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

משוואה זו נקראת משוואת המחלקים.

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

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

מסקנה: נניח  $H \leq G$  ונניח  $n = [G : H] < \infty$ . תהא  $K = \bigcap_{g \in G} gHg^{-1}$ , אזי מתקיים  $K \triangleleft G$ ,

$G/K$ , איזומורפית לתת חבורה של  $S_n$ . בפרט, אם  $G$  סופית ו- $n!$  אינו מתחלק ב- $|G|$ , אז  $K \neq \{e\}$ .

הוכחה: יהיו  $g \in G, a \in K$ . נראה  $gag^{-1} \in \bigcap_{b \in G} bHb^{-1}$ .

יהי  $b \in G$ .  $a \in g^{-1}bH(g^{-1}b)^{-1} \Leftrightarrow gag^{-1} \in bHb^{-1}$ .  
 $a \in K$

החבורה  $G$  פועלת על הקבוצה  $G/H$  על ידי כפל משמאל:  $\sigma^*(gH) = (\sigma g)H$ . פעולה זו מגדירה הומומורפיזם  $\varphi : G \rightarrow S(X)$ . 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  $K \triangleleft G$  ולפי משפט האיזומורפיזם הראשון,  $G/K \cong \text{Im } \varphi \leq S(X) \cong S_n$ . בפרט, אם  $|G| \nmid n!$ , אז הגרעין אינו טריוויאלי. אם הגרעין היה טריוויאלי, אז  $G \leq S(X) \cong S_n$ , ולפי משפט

לגראנוי  $|G| \mid |S_n|$ , בסתירה ל- $|G| \nmid n!$ .

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

מסקנה: אם  $G$  חבורה, ויש ל- $G$  תת-חבורה  $H$  כך ש- $[G : H]!$  אינו מתחלק ב- $|G|$ , אזי  $G$  אינה פשוטה.

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

למה:  $A_n$  נוצרת על ידי המחזורים מאורך 3 ב- $S_n$ .

**הוכחה:** 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:

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

**תרגיל:** תהא  $G$  חבורה מסדר 36 ונניח של- $G$  תת חבורה  $H$  מסדר 9. הוכח ש- $G$  אינה פשוטה. **פתרון:**  $24 \nmid 36$ ,  $4! = 24$ ,  $[G:H] = 4$ ,  $|G| = 36$ . לכן, לפי המסקנה, ב- $H$  מוכלת תת חבורה נורמלית לא-טריוויאלית של  $G$ .

**תרגיל:** תהא  $G$  חבורה מסדר 99, ונניח ש- $H$  תת-חבורה מסדר 11. הוכח ש- $H \triangleleft G$ .

**פתרון:**  $|G| = 99$ ,  $[G:H] = 9$ ,  $11 \nmid 9!$ ,  $9! \nmid 99$ . 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. ראשוני, לכן  $|K| = 11$ , כלומר  $K = H$ , ולכן  $H \triangleleft G$ .

**משפט:** לכל  $n \geq 5$  סופי,  $A_n$  פשוטה. (הערה: זאת הסיבה שלמשוואות ממעלה  $\leq 5$  אין נוסחת שורשים).

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

**טענה:** אם  $N \triangleleft A_n$  מכילה מחזור מאורך 3 אז  $N = A_n$ .

**הוכחה:** 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  $\sigma$  אי-זוגית, נבחר  $g, h$  שונים מ- $a, b, c$  (אפשר, כי  $n \geq 5$ ), ואז  $\tau := \sigma(gh) \in A_n$  (כלומר, "נרמה" ונבנה תמורה זוגית המתנהגת באופן דומה, ונשתמש בחלק הקודם), ומתקיים  $\tau(abc)\tau^{-1} = (def)$ , ולכן  $(def) \in N$ .

**טענה:** אם  $N \triangleleft A_n$ ,  $N \neq \{e\}$ , אז יש מחזור מאורך 3 ב- $N$ .

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

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

$$\begin{aligned} \varphi \sigma \varphi^{-1} &= \varphi \pi_1 \varphi^{-1} \pi_2 \dots \pi_r = \varphi \pi_1 \varphi^{-1} \pi_1^{-1} \sigma = \\ &= (1 2 3)(1 2 3 \dots k)(1 3 2)(r \dots 3 2 1) \sigma = (1 2 4) \sigma \end{aligned}$$

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

II. לכל  $i, \pi_i$  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  $\varphi = (1 2 4)$ .

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

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

III. קיים  $i$  יחיד עבורו  $\pi_i$  מאורך 3, ועבור כל  $i$  אחר  $\pi_i$  מאורך 2. בלי הגבלת הכלליות,

נסמן  $\pi_1 = (1 2 3)$ . כל שאר המחזורים ב- $\sigma$  הם חילופים, ולכן

$$(1 3 2) = \pi_1^2 = \sigma^2 \in N$$

IV.  $\sigma$  היא מכפלה של חילופים. לפיכך,  $\sigma$  היא מכפלה של לפחות שני חילופים, לכן נסמן

בהי"כ  $\pi_2 = (3 4), \pi_1 = (1 2)$ . נסמן  $\varphi = (1 2 3)$ . מתקיים:

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

כלומר מתקיים  $(1 3)(2 4) = \varphi\sigma\varphi^{-1}\sigma^{-1} \in N$ . 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- $\tau$  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.<sup>1</sup>

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

הוכחה: נרשום  $G = \{g_1, g_2, \dots, g_n\}$ . נגדיר פעולה של  $G$  על עצמה על ידי  $\sigma * g = \sigma \cdot g$ , כאשר

$\sigma, g \in G$ . פעולה זו מגדירה הומומורפיזם  $\varphi: G \rightarrow S(G)$  על ידי  $\varphi(\sigma)(g) = \sigma * g = \sigma g$ .

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

<sup>1</sup> ישנן עוד הרבה הוכחות למשפט זה. למתעניינים (הוכחה המוצגת כאן היא הרביעית):

<http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/Ansimple.pdf>

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

הגדרה: יהיו  $G_1, G_2, \dots, G_n$  חבורות. אזי:

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

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

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

הערות:

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

II.  $G_i \triangleleft G$  לכל  $i$ .

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

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

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

משפט: תהא  $G$  חבורה ו- $G_1, G_2, \dots, G_n \leq G$ . התנאים הבאים שקולים:

I. א.  $G = \langle G_1, \dots, G_n \rangle$ .

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

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

II. א.  $G = \langle G_1, \dots, G_n \rangle$ .

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

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

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

הוכחה: III  $\Leftrightarrow$  I ברור.

I  $\Leftrightarrow$  II: נראה את ד'. לפי ב',  $(x_i^{-1} y_j^{-1} x_i) y_j \in G_j$ , אך גם  $x_i^{-1} (y_j^{-1} x_i y_j) \in G_i$ , ולכן לפי ג'

$x_i x_j = x_j x_i$  כלומר  $x_i^{-1} y_j^{-1} x_i y_j \in G_i \cap G_j = \{e\}$ .

נראה את ה': נניח  $x_1 \cdot x_2 \cdot \dots \cdot x_n = y_1 \cdot y_2 \cdot \dots \cdot y_n$  כאשר  $x_i, y_i \in G_i$ . לפי ד',

$x_1 y_1^{-1} \in G_1 \cap \langle G_2, \dots, G_n \rangle = \{e\}$  ולכן  $x_1 y_1^{-1} \in \langle G_2, \dots, G_n \rangle$  כלומר  $x_1 y_1^{-1} = x_2^{-1} y_2 \cdot \dots \cdot x_n^{-1} y_n$

לפי ג', כלומר  $x_1 = y_1$ , ובאופן דומה עבור שאר ה- $i$ .

III  $\Leftarrow$  II : נגדיר העתקה  $\theta: G_1 \times G_2 \times \dots \times G_n \rightarrow G$  על ידי  $\theta(g_1, g_2, \dots, g_n) = g_1 \cdot g_2 \cdot \dots \cdot g_n$ .  
 נראה ש- $\theta$  הומומורפיזם :

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

מד' נובע :

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

נראה ש- $\theta$  על: לפי א' וד', כל איבר ב- $G$  ניתן לכתוב כ- $g_1 \cdot g_2 \cdot \dots \cdot g_n$ , כלומר כ- $\theta(g_1, \dots, g_n)$ .

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

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

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

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

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

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

פתרון: מהו  $O(1,1)$ ?

$$(k, k) = (0, 0) \Leftrightarrow k \cdot (1, 1) = (0, 0) \Leftrightarrow m | k, n | k \Leftrightarrow mn | k$$

$\gcd(m, n) = 1$

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  $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ .

טענה: תהא  $G$  סופית,  $G_1, G_2, \dots, G_n \triangleleft G$ , ונניח שהסדרים  $|G_1|, |G_2|, \dots, |G_n|$  זרים בזוגות, וגם

$$|G| = \prod_{i=1}^n |G_i|$$

ניח ש- $G$  זו המכפלה הישרה של  $G_1, G_2, \dots, G_n$ .

הוכחה:

הערה: אם  $A, B \leq H$  מסדרים זרים, אזי  $A \cap B = \{e\}$ , לפי לגראנז'. יתר על כן, אם גם  $A \triangleleft H$

אזי  $AB \leq H$ , והסדר שלה  $|AB| = |A||B|$ .

לכן, באינדוקציה על  $k$  :

$$I. |G_1| \cdot |G_2| \cdot \dots \cdot |G_k| \text{ מסדר } G_1, G_2, \dots, G_k \leq G$$

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

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

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

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

פתרון: נגדיר העתקה  $\varphi: G \rightarrow G_1/N_1 \times G_2/N_2 \times \dots \times G_n/N_n$  על ידי

$$\varphi(g_1, g_2, \dots, g_n) = (g_1 N, g_2 N, \dots, g_n N)$$

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

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

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

הערה: אם עסקינן בחבורות חיבוריות, לעיתים נסמן  $\oplus$  במקום  $\times$ .