

## אלגברה ב' 1 - הרצאה 9 - 24.9.12

משפט המבנה לחבורות אבליות נוצרות סופית: ראינו גרסה אחת, לפיה אם  $G$  חבורה אבלית

נוצרת סופית אזי  $G \cong \mathbb{Z}_{\varepsilon_1} \times \mathbb{Z}_{\varepsilon_2} \times \dots \times \mathbb{Z}_{\varepsilon_k} \times \overbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}^r$ ,  $\varepsilon_i \in \mathbb{N}$ ,  $\varepsilon_1 | \varepsilon_2 | \dots | \varepsilon_k$ ,  $k, r \geq 0$ . גרסה

נוספת של המשפט טוענת  $G \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \dots \times \mathbb{Z}_{p_k^{e_k}} \times \overbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}^r$ , כך ש- $p_1, \dots, p_k$  ראשוניים,

לאו דווקא שונים,  $e_1, \dots, e_k \geq 1$ ,  $k, r \geq 0$ . הצגה זו יחידה, עד כדי סדר.

לא הוכחנו את השקילות בין הגרסה הראשונה (שראינו את הוכחת נכונותה בהרצאה הקודמת) לבין הגרסה השנייה. אביא כאן הוכחה פשוטה, בעזרת שימוש במשפט השאריות הסיני (מי שמתעניין בהוכחתו מוזמן להסתכל בסיכום המופיע באתר, של הקורס "תורת המספרים").

משפט השאריות הסיני: יהיו  $j \cdot k = m$ ,  $\gcd(j, k) = 1$ ,  $j, k, m \in \mathbb{N}$ . אזי  $\mathbb{Z}_m \cong \mathbb{Z}_j \oplus \mathbb{Z}_k$ .

הוכחת משפט המבנה: לפי הגרסה הראשונה,  $G \cong \mathbb{Z}_{\varepsilon_1} \times \mathbb{Z}_{\varepsilon_2} \times \dots \times \mathbb{Z}_{\varepsilon_k} \times \overbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}^r$ , באופן יחיד.

עבור כל  $i$  נפרק את  $\varepsilon_i$  לראשוניים  $p_{1_i}^{e_{1_i}} \cdot \dots \cdot p_{k_i}^{e_{k_i}}$ , ונקבל  $\mathbb{Z}_{\varepsilon_i} \cong \mathbb{Z}_{p_{1_i}^{e_{1_i}}} \oplus \dots \oplus \mathbb{Z}_{p_{k_i}^{e_{k_i}}}$ . מיחידות

פירוק הטבעיים לראשוניים, סיימנו.  $\square$

דוגמה:  $\mathbb{Z}_2 \times \mathbb{Z}_7^2 \times \mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_{5^2} \times \mathbb{Z}_{19} \times \mathbb{Z}_{2^4} \cong \mathbb{Z}_2 \times \mathbb{Z}_{7^2 \cdot 5 \cdot 2^3} \times \mathbb{Z}_{7^3 \cdot 5^2 \cdot 19 \cdot 2^4}$

תרגיל: כמה חבורות אבליות יש מסדר 9800 (עד כדי איזומורפיזם)?

פתרון:  $9800 = 7^2 \cdot 5^2 \cdot 2^3$ . כל חבורה אבלית סופית איזומורפית, לפי משפט המבנה, ל-

עד כדי איזומורפיזם. לכן, נרצה לחשב את מספר האפשרויות של המספר 9800 כהצגה כמכפלה של

חזקות של ראשוניים (לאו דווקא שונים). 7 יכול להופיע או כפעמיים 7 או כפעם אחת 49, כנ"ל 5 – פעמיים 5 או פעם 25, ו-2 יכול להופיע כשלוש פעמים 2, 2 ו-4 או 8. נכפול את האפשרויות, ונקבל  $2 \cdot 2 \cdot 3 = 12$ .

תרגיל: כמה חבורות אבליות יש מסדר  $7^2 \cdot 3^5$  (עד כדי איזומורפיזם)?

פתרון: ל-5 יש 7 חלוקות, ול-2 יש 2 חלוקות, לכן יש  $2 \cdot 7 = 14$  חבורות אפשריות.

## חבורות נילפוטנטיות

תהא  $G$  חבורה סופית, נסמן  $|G| = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$  פירוק לראשוניים של הסדר של  $G$ . אנחנו אוהבים שעבור  $p$  ראשוני המקיים  $p \mid |G|$  מתקיים  $n_p = 1$ , שכן במקרה זה קיימת חבורה יחידה  $p$ -סילוב ל- $G$ , ולכן חבורה זו נורמלית. הכי הכי כף זה שלכל  $p$  המחלק את הסדר של  $G$  מתקיים  $n_p = 1$ , כי אז לכל  $p_i$  קיימת תת-חבורה יחידה  $P_i \triangleleft G$  מסדר  $p_i^{e_i}$ . קיבלנו:

$$P_i \triangleleft G \quad \text{I}$$

$$\forall i \neq j: P_i \cap P_j = \{e\} \quad \text{II}$$

$$|G| = |P_1| \cdot |P_2| \cdot \dots \cdot |P_k| \quad \text{III}$$

ולכן  $G$  היא המכפלה הישרה של תת-החבורות  $p$ -סילוב שלה. לחבורה מסוג זה נקרא חבורה סבבה (*Sababa*).

הגדרה: עבור  $H, K \leq G$  מסמנים:  $[H, K] := \{[h, k] \mid h \in H, k \in K\}$  (בפרט,  $[G, G] = G'$ ).  
אנו נתעניין רק במקרה  $[H, G]$ . קל להראות שזו חבורה.

טענה: תהא  $G$  חבורה,  $H, K \leq G$ . מתקיים:

$$\text{I. אם } K \leq H, \text{ אזי } [K, G] \leq [H, G]$$

$$\text{II. } [H, G] \leq H \Leftrightarrow H \triangleleft G$$

$$\text{III. אם } K \triangleleft G, K \leq H \leq G, \text{ אזי } [H, G] \leq K \Leftrightarrow H/K \leq Z(G/K)$$

הוכחה: I ברור. נוכיח את II, III.

II.  $\Rightarrow$ :  $[H, G] \leq H$ , לפיכך, לכל  $h \in H, g \in G$  מתקיים  $ghg^{-1}g^{-1} \in H$ , לכן לכל  $h \in H, g \in G$  מתקיים  $gh^{-1}g^{-1} \in H$ , ולכן לכל  $h \in H, g \in G$  מתקיים  $gh \in Hg$ , כלומר לכל  $g \in G$  מתקיים  $gH = Hg$ , ולכן  $H \triangleleft G$ .  
 $\Leftarrow$ :  $H \triangleleft G$ , לכן לכל  $h \in H, g \in G$  מתקיים  $gh^{-1}g^{-1} \in H$ . לכן,  $[H, G] \leq H$ , ולכן  $ghg^{-1}g^{-1} \in hH = H$ . כלומר  $[H, G] \leq H$ .  
 III. לכל  $h \in H, g \in G$  מתקיים  $(gK)(hK) = (hgK)$ . כלומר  $ghg^{-1}h^{-1} \in K$ , ולכן  $ghK = hgK$ . כלומר  $[H, G] \leq K$ .  
 $\square$

הגדרה: תהא  $G$  חבורה, נגדיר אינדוקטיבית סדרת תת-חבורות  $\{\Phi_i(G)\}_{i=1}^{\infty}$  על ידי  $\Phi_1(G) = G$  ו-  
 $\Phi_{i+1}(G) = [\Phi_i(G), G] \leq \Phi_i(G)$ . לעיתים נסמן  $\Phi_i$ , כאשר ברור על איזו חבורה מדובר. סדרה זו נקראת הסדרה המרכזית היורדת של  $G$ .

למה:  $\Phi_{i+1} \triangleleft \Phi_i$ .

הוכחה: נוכיח אינדוקטיבית על  $i$ . עבור  $i=1$  נראה  $\Phi_2 \triangleleft \Phi_1$ . ואכן,  $\Phi_2 = [G, G] = G' \triangleleft G = \Phi_1$ . כעת, מהנחת האינדוקציה מתקיים  $\Phi_i \triangleleft \Phi_{i-1}$ , ולכן לפי התרגיל הקודם מתקיים  $\Phi_{i+1} = [\Phi_i, G] \leq [\Phi_{i-1}, G] = \Phi_i$ . מאותם שיקולים, מתקיים  $[\Phi_{i+1}, G] \leq G$ , ולכן לפי התרגיל  $\Phi_{i+1} \triangleleft G$ , ובפרט  $\Phi_{i+1} \triangleleft \Phi_i$ .  $\square$

למה:  $\Phi_i / \Phi_{i+1} \leq Z(G / \Phi_{i+1})$ .

הוכחה: נתבונן בתרגיל בעמוד הקודם. נבחר  $H = \Phi_i$ ,  $K = \Phi_{i+1}$ , וסיימנו.  $\square$

הגדרה: תהא חבורה  $G$ . נאמר ש- $G$  נילפוטנטית אם קיים  $i$  עבורו  $\Phi_i(G) = \{e\}$ .

הגדרה: הסדרה המרכזית העולה של חבורה  $G$  תסומן  $Z_i(G)$ , ותקיים:

$$Z_0(G) = \{e\}, Z_1(G) = Z(G), Z_i(G) / Z_{i-1}(G) = Z(G / Z_{i-1}(G))$$

הסבר: יש התאמה חחול בין תת-חבורות של  $G / Z_i$  לבין תת-חבורות של  $G$  המכילות את  $Z_i$  (משפט האיזומורפיזם השלישי), ולכן נגדיר את  $Z_i$  להיות החבורה המתאימה ל- $Z(G / Z_{i-1})$ . בנוסף, מתקיים  $Z_i(G) / Z_{i-1}(G) \triangleleft G / Z_{i-1}(G)$  לכל  $i$ , ולכן לפי משפט האיזומורפיזם השלישי  $Z_i \triangleleft G$ .

משפט:  $Z_m = G \Leftrightarrow \Phi_{m+1} = \{e\}$ . יתרה מכך, אם  $Z_m = G$  אזי  $\Phi_{i+1} \leq Z_{m-i}$  לכל  $0 \leq i \leq m$ .

הוכחה: נניח  $Z_m = G$ , ונוכיח את הטענה באינדוקציה על  $i$  (ועבור  $i=m$  נקבל  $\Phi_{m+1} \leq Z_0 = \{e\}$ ). עבור  $i=0$  מתקיים  $\Phi_1 = G = Z_m$ . נניח  $\Phi_{i+1} \leq Z_{m-i}$ , אזי:

$$\Phi_{i+2} = [\Phi_{i+1}, G] \leq [Z_{m-i}, G] \leq Z_{m-i-1}$$

כאשר המעברים נכונים לפי התרגיל בתחילת ההרצאה.

נראה את הכיוון השני, שוב אינדוקטיבית. נניח  $\Phi_{m+1} = \{e\}$ , ונראה  $\Phi_{m-j+1} \leq Z_j$  לכל  $0 \leq j \leq m$  (שקול לטענה אותה רצינו להוכיח). עבור  $j=0$  מתקיים  $\Phi_{m+1} = Z_0 = G$ . נניח  $\Phi_{m-j+1} \leq Z_j$ , ונתבונן באפימורפיזם הקנוני  $\pi: G \rightarrow G / Z_j$ , הנתון על ידי  $\pi(g) = gZ_j$ . אפימורפיזם זה משרה את האפימורפיזם  $\pi': G / \Phi_{m-j+1} \rightarrow G / Z_j$  המוגדר על ידי  $\pi'(g\Phi_{m-j+1}) = \pi(g)$ . לפי הלמה האחרונה, מתקיים  $\Phi_{m-j} / \Phi_{m-j+1} \leq Z(G / \Phi_{m-j+1})$ , ולכן:

$$\pi(\Phi_{m-j}) = \pi'(\Phi_{m-j} / \Phi_{m-j+1}) \leq \pi'(Z(G / \Phi_{m-j+1}))$$

$\pi'$  הוא אפימורפיזם, לכן תמונתו של כל איבר השייך למרכז של התחום נמצאת במרכז של  $\text{Im } \pi'$ .

הסבר: יהיו  $a \in G/\Phi_{m-j+1}$ ,  $z \in Z(G/\Phi_{m-j+1})$ .  
 $\pi'(z) \in Z(G/Z_j)$  ולכן  $\pi'(a) \cdot \pi'(z) = \pi'(az) = \pi'(za) = \pi'(z) \cdot \pi'(a)$  ומתקיים  
 $\pi'(Z(G/\Phi_{m-j+1})) \leq Z(G/Z_j)$ . לפיכך,  $\pi(\Phi_{m-j}) \leq Z(G/Z_j)$ , כלומר  
 $\Phi_{m-j}/Z_j \leq Z(G/Z_j) = Z_{j+1}/Z_j$ . ולכן (משפט האיזומורפיזם השלישי),  $\Phi_{m-j} \leq Z_{j+1}$ .  $\square$

הגדרה: לפי המשפט, אנו יכולים לקבוע הגדרה שקולה לחבורה נילפוטנטית:  $G$  נילפוטנטית אם קיים  $m \in \mathbb{N}$  עבורו  $Z_m(G) = G$ .

דוגמה: כל חבורה אבלית היא נילפוטנטית (כי  $Z_1(G) = Z(G) = G$ ).

דוגמה: כל חבורת- $p$  סופית היא נילפוטנטית.

הוכחה: נתבונן בסדרה המרכזית העולה של  $G$ . עבור אינדקס  $i$  מתקיים  $Z_{i+1}/Z_i = Z(G/Z_i)$ . אם  $G = Z_i$  סיימנו. אחרת,  $G$  חבורת- $p$  ולכן  $G/Z_i$  חבורת- $p$  (שאינה טריוויאלית), ולכן מרכזיה אינו טריוויאלי. לפיכך  $|Z_{i+1}/Z_i| > 1$ , כלומר  $Z_{i+1} > Z_i$ .  $G$  סופית, לכן הסדרה  $\{Z_i\}$  זו סדרה מונוטונית עולה וחסומה (על ידי  $|G|$ ) של טבעיים, ולכן בהכרח קיים ערך  $i$  עבורו  $Z_i = G$ , כלומר  $G$  נילפוטנטית.  $\square$

טענה: מכפלה ישרה של חבורות נילפוטנטיות היא חבורה נילפוטנטית.

הוכחה: יהיו  $G_1, G_2$  חבורות נילפוטנטיות, מספיק להראות ש- $G = G_1 \times G_2$  נילפוטנטית. נראה שמתקיים  $\Phi_i(G) = \Phi_i(G_1) \times \Phi_i(G_2)$ , ואז אורך הסדרה המרכזית היורדת של  $G$  יהיה הערך המקסימלי מבין אורכי הסדרות המרכזיות היורדות של  $G_1, G_2$ . נוכיח זאת באינדוקציה על  $i$ . עבור  $i = 1$  מדובר בהגדרת  $G$ . נניח נכונות ל- $i$ .

$$\begin{aligned} \Phi_{i+1}(G) &= [\Phi_i(G), G] = [\Phi_i(G_1) \times \Phi_i(G_2), G_1 \times G_2] = \\ &= [\Phi_i(G_1), G_1] \times [\Phi_i(G_2), G_2] = \Phi_{i+1}(G_1) \times \Phi_{i+1}(G_2) \end{aligned}$$

$\square$

קיבלנו בפרט שכל חבורה סבבה היא נילפוטנטית. נראה שכל חבורה נילפוטנטית היא סבבה.

למה: אם  $G$  נילפוטנטית ו- $H < G$ , אז  $H < N_G(H)$ .

הוכחה: יהי  $i$  הטבעי הראשון כך ש- $\Phi_{i+1} \leq H$  (קיים מנילפוטנטיות). קיים  $a \in G$  כך ש- $a \in \Phi_i \setminus H$ . לכל  $h \in H$  מתקיים:  $ah^{-1}a^{-1}h = [a, h^{-1}] \in [\Phi_i, G] = \Phi_{i+1} \leq H$ , ולכן  $aha^{-1} \in H$ , ולכן  $a \in N_G(H) \setminus H$ , כלומר  $H$  תת-חבורה ממש של  $N_G(H)$ .  $\square$

למה (הארגומנט של פראטיני - Frattini): תהא  $G$  חבורה סופית,  $K \triangleleft G$ ,  $P$  תת-חבורה  $p$ -סילוב של  $K$ , אזי  $G = K \cdot N_G(P)$ .

הוכחה: יהי  $g \in G$ , אזי  $gPg^{-1} = K$ , ולכן  $gPg^{-1} \leq K$  היא תת-חבורה  $p$ -סילוב של  $K$ , ולפי המשפט השני של סילוב  $P$ ,  $gPg^{-1} \leq P$ , כלומר קיים  $k \in K$  כך ש:

$$gPg^{-1} = kPk^{-1} \Rightarrow g^{-1}kPk^{-1}g = P \Rightarrow k^{-1}g \in N_G(P) \Rightarrow g = k \cdot k^{-1}g \in K \cdot N_G(P)$$

$\in K \quad \in N_G(P)$

ולכן  $G = K \cdot N_G(P)$  , כלומר  $G \geq K \cdot N_G(P)$  , וברור ש-  $G \leq K \cdot N_G(P)$  .

למה: תהא  $P$  חבורת  $p$ -סילוב של חבורה סופית  $G$  . אם  $N_G(P) \leq H \leq G$  , אזי  $N_G(H) = H$  .

הוכחה: מתקיים  $P \triangleleft N_G(P) \leq H \triangleleft N_G(H) \leq G$  . מוכלת ב-  $H$  ולכן היא תת-חבורה  $p$ -סילוב של  $H$  . לפי הלמה של פראטיני  $G = H \cdot N_{N_G(H)}(P)$  , אבל  $N_{N_G(H)}(P) \leq N_G(P) \leq H$  , ולכן  $N_G(H) \leq H \cdot N_{N_G(H)}(P) \leq H \cdot H = H \leq N_G(H)$  , ולכן  $N_G(H) = H$  .

משפט: חבורה היא סבבה אם"ם היא נילפוטנטית.

הוכחה: נניח ש-  $G$  נילפוטנטית ונראה שהיא סבבה (את הכיוון השני כבר הראנו). תהא  $P$  חבורת  $p$ -סילוב שלה, ויהי  $H = N_G(P)$  . לפי הלמה האחרונה,  $H = N_G(H)$  . לפי למה קודמת, אם  $G$  נילפוטנטית ו-  $H$  תת-חבורה ממש שלה, אזי  $H$  תת-חבורה ממש של  $N_G(H)$  . זו סתירה, ולכן  $H = G$  , כלומר  $P \triangleleft G \triangleleft N_G(P) = G$  . קיבלנו אם כך שכל החבורות  $p$ -סילוב של  $G$  נורמליות ב-  $G$  , כלומר  $G$  סבבה.  $\square$

תרגיל: תהא  $G$  חבורה ותהא  $A$  תת-חבורה נורמלית ב-  $G$  . הוכח כי התנאים הבאים שקולים:

I. קיימת תת-חבורה  $B \leq G$  כך ש-  $G = A \times B$  .

II. קיים אפימורפיזם מ-  $G$  על  $A$  שצמצומו על  $A$  זו העתקת הזהות.

פתרון: נניח I:  $G = A \cdot B$  ,  $A, B \triangleleft G$  ,  $A \cap B = \emptyset$  . נגדיר העתקה  $\varphi: G \rightarrow A$  על ידי  $\varphi(ab) = a$  . העתקה זו מוגדרת היטב בגלל ש-  $G$  המכפלה הישרה של  $A$  ו-  $B$  .

$$\varphi(a_1 b_1 a_2 b_2) = \varphi(a_1 a_2 b_1 b_2) = a_1 a_2 = \varphi(a_1 b_1) \varphi(a_2 b_2)$$

לכן  $\varphi$  הומומורפיזם. לכל  $a \in A$  ,  $\varphi(a \cdot e) = a$  , ולכן  $\varphi$  אפימורפיזם. צמצום  $\varphi$  ל-  $A$  זו העתקת הזהות.

נניח II: יהי  $\varphi$  הומומורפיזם כזה. נסמן  $B = \ker \varphi$  . יהי  $g \in G$  , אזי  $\varphi(g) \in A$  .

$$g = \varphi(g) \cdot (\varphi(g))^{-1} \cdot g$$

$$. b = (\varphi(g))^{-1} \cdot g \text{ נסמן}$$

$$\varphi(b) = \varphi((\varphi(g))^{-1} \cdot g) = \underbrace{\varphi((\varphi(g))^{-1})}_{\in A} \cdot \varphi(g) = (\varphi(g))^{-1} \cdot \varphi(g) = e$$

$\varphi_A = Id$

לכן  $b \in \ker \varphi$  , ולכן  $G = A \cdot B$  .

$B = \ker \varphi \triangleleft G$  ,  $A \triangleleft G$  נתון.

נניח  $g \in A \cap B$ , אזי  $\varphi(g) = e \Leftrightarrow g \in B = \ker \varphi$ ,  $\varphi(g) = g \Leftrightarrow g \in A$ ,  $\varphi|_A = Id$ . לכן בהכרח  $A \cap B = \{e\}$ . קיבלנו  $G = A \times B$ , כלומר  $g = e$ .

תרגיל: תהא חבורה  $G$  כך ש- $|G| = p^n q^2$ ,  $p > q \geq 3$ , ראשוניים. הוכח:  $G'$  חבורת- $p$ .

פתרון:  $n_p \equiv 1(p)$ ,  $n_p \in \{1, q, q^2\}$ . נניח  $n_p = q^2$ , אזי  $p \mid q^2 - 1$ . ראשוני, לכן נניח  $p \mid q + 1$  (אם  $p \mid q - 1$  אזי  $q > p$ , סתירה). לפיכך  $q < p \leq q + 1$ , כלומר  $p = q + 1$ , ומראשוניות  $q, p$  נסיק  $q = 2, p = 3$ , סתירה. נניח  $n_p = q$ , ולכן  $p \mid q - 1$ , שכאמור מביא לסתירה.

לפיכך,  $n_p = 1$ , לכן קיימת תת-חבורה  $p$ -סילוב יחידה, נסמנה  $P$ . מתקיים  $P \triangleleft G$ . לפי טענה שהוכחנו בהרצאות קודמות, מתקיים  $G/P \leq P$ , ולכן גם  $|G/P| = q^2$ , לכן  $G/P$  אבלית. לפי טענה שהוכחנו בהרצאות קודמות, מתקיים  $G' \leq P$ , ולכן גם  $G'$  זו חבורת- $p$ .

תרגיל: באותם נתונים של התרגיל הקודם, הוכח שאם  $x, y \in G$  כך ש- $[x, y]^q = e$ , אזי  $[x, y] = e$ .

פתרון:  $[x, y] \in G'$ , לכן לפי משפט לגראנז'  $o([x, y])$  הוא חזקה של  $p$ . מצד שני,  $[x, y]^q = e$ , ולכן  $q \mid o([x, y])$ . לכן  $o([x, y]) = 1$ , כלומר  $[x, y] = e$ .

תרגיל: תהא חבורה סופית  $G$ , נניח ש- $r$  הראשוני הקטן ביותר המחלק את סדרה. תהא חבורה  $H$  ב- $G$  מאינדקס  $r$ . הוכח:  $H \triangleleft G$ .

פתרון:  $|G| \nmid [G : H]!$ , כי נבחר ראשוני  $|G|$ ,  $r < p \mid |G|$ , ואז  $p$  לא מחלק את  $r!$ . אם  $|G| = r^l$ ,  $l > 1$  אזי  $r! \nmid r^2$ , ואם  $l = 1$  אזי  $H = \{e\}$  והטענה טריוויאלית. לפי טענה שהוכחנו בהרצאה קודמת (5), קיימת תת-חבורה  $K \triangleleft G$ ,  $K \leq H$ , שאינה טריוויאלית, ו- $G/K$  איזומורפית לתת-חבורה של  $S_r$ .  $|G/K| \mid |G|$ , לכן  $|G/K|$  מכפלה של גורמים ראשוניים של  $|G|$ . אולם,  $|S_r| = r!$ , ולכן כל ראשוני שמחלק את  $|G|$  מחלק את  $|G/K|$ . רק אם הוא מחלק את  $r!$ . כאמור,  $p > r \Rightarrow p \nmid r!$ , וממינימליות  $r$  נקבל ש- $G/K$  זו חבורת- $r$ . יותר מכך, משום ש- $r! \nmid r^2$ , נקבל  $|G/K| = r$ . לכן  $|G/K| = |G/H| = r$ , ולכן  $|K| = |H|$ . מהכלה נקבל  $H = K \triangleleft G$ .

**תרגיל:** תהא  $G$  חבורה המקיימת  $|G| = p^3 \cdot q^2 \cdot r$  כאשר  $p > q > r \geq 3$  ראשוניים וגם  $p > q^3 - 1$ . הוכח:  $G$  מכילה חבורת  $p$ -סילוב נורמלית  $P$ , ואם  $Q$  חבורת  $q$ -סילוב, אזי  $PQ \triangleleft G$ .

**פתרון:**  $n_p \equiv 1 \pmod{p}$ ,  $n_p \in \{1, q, r, qr, q^2, q^2r\}$ . לכן  $p > q > r$  לכן  $n_p \neq q, r$ . בדומה לתרגיל הקודם,  $n_p \neq q^2$  ( $p, q > 3$ ). נניח  $n_p = qr$ , אזי  $qr - 1 \mid p$ . לכן  $p \leq qr - 1 < q(qr - 1) < (q^2r - 1) < q^3 - 1$ , ולכן  $p \leq q^2r - 1 < q^3 - 1$ . סתירה. קיבלנו  $n_p = 1$ . לפיכך, קיימת תת-חבורה  $p$ -סילוב יחידה ל- $G$  ונסמנה  $P$ . מתקיים  $P \triangleleft G$ . תהא  $Q$  חבורת  $q$ -סילוב,  $P$  נורמלית ולכן  $PQ$  חבורה. מתקיים  $|PQ| = p^3q^2$ , ולכן  $[G : PQ] = r$ . כלומר, זוהי תת-חבורה מאינדקס ראשוני מינימלי, ולפי התרגיל הקודם היא נורמלית ב- $G$ .