

# תורת החבורות 88-218-01 תשפ"א

## הערות הרצאה 13

שלום!

**תזכורת 0.1.** תהי  $G$  חבורה. אמרנו ש- $G$  פתירה אם קיימת לה סדרה תת-נורמלית שבה כל המנות אבליות. באופן שקול, זה אומר שסדרת הנגזרות שלה היא טריוויאלית אחרי מספר סופי של צעדים. כלומר קיים  $n \in \mathbb{N}$  עבורו  $G^{(n)} = \{e\}$ , כאשר

$$G^{(n)} = \begin{cases} G & n = 0 \\ [G^{(n-1)}, G^{(n-1)}] & n > 0 \end{cases}$$

אפילו ראינו שאם  $N \triangleleft G$  נורמלית, אז  $G$  פתירה אם ורק אם  $N$  וגם  $G/N$  פתירות. אמרנו כי  $G$  נילפוטנטית אם הסדרה המרכזית היורדת שלה היא טריוויאלית אחרי מספר סופי של צעדים. כלומר קיים  $n \in \mathbb{N}$  עבורו  $\gamma_n(G) = \{e\}$ , כאשר

$$\gamma_n(G) = \begin{cases} G & n = 1 \\ [G, \gamma_{n-1}(G)] & n > 1 \end{cases}$$

אם  $G$  נילפוטנטית, אז כל תת-חבורה שלה וכל חבורת מנה הן נילפוטנטיות. הכיוון ההפוך לא בהכרח נכון, למשל  $G = S_3$  אינה נילפוטנטית אבל יש לה תת-חבורה נורמלית  $A_3 \triangleleft S_3$  שהיא נילפוטנטית וגם המנה  $S_3/A_3$  נילפוטנטית.

### 0.1 מכפלות ישרות

ראינו שבהנתן חבורות  $H_1, H_2$  אפשר לבנות חבורה "גדולה" יותר  $H_1 \times H_2$  הנקראת המכפלה הישרה (החיצונית) של  $H_1$  ו- $H_2$ .

**0.2 הגדרה.** חבורה  $G$  היא מכפלה ישרה (פנימית) של תת-חבורות  $K_1, K_2 \leq G$  אם שלושת התנאים הבאים מתקיימים:

$$K_1, K_2 \triangleleft G \bullet$$

$$K_1 \cap K_2 = \{e\} \bullet$$

$$G = K_1 K_2 \bullet$$

סענה 0.3. תהי  $G$  שהיא מכפלה ישרה פנימית של  $K_1, K_2 \leq G$ . אז

$$G \cong K_1 \times K_2$$

$$g = k_1 k_2 \mapsto (k_1, k_2)$$

למשל

$$K_1 \ni (k'_1)^{-1} k_1 = k'_2 k_2^{-1} \in K_2$$

סענה 0.4. עם מעט אינדוקציה נקבל שחבורה  $G$  היא מכפלה ישרה (פנימית) של תת-חבורות  $H_1, \dots, H_n \leq G$  אם ורק אם שלושת התנאים הבאים מתקיימים:

$$H_1, \dots, H_n \triangleleft G \bullet$$

$$H_i \cap \prod_{j \neq i} H_j = \{e\} \text{ כלומר } i \in [n] \text{ לכל } H_i \cap (H_1 \dots H_{i-1} H_{i+1} \dots H_n) = \{e\} \bullet$$

$$G = H_1 \dots H_n \bullet$$

דוגמה 0.5. למשל

$$G = \mathbb{Z}_5 \times \mathbb{Z}_{20} \times \mathbb{Z}_{12} = \langle (1, 0, 0) \rangle \langle (0, 1, 0) \rangle \langle (0, 0, 1) \rangle$$

משפט 0.6. תהי  $G$  חבורה סופית. התנאים הבאים שקולים:

1. החבורה  $G$  נילפוטנטית.

2. לכל תת-חבורה נאותה  $H \leq G$  (כלומר  $H \neq G$ ) מתקיים  $H \subsetneq N_G(H)$ .

3. כל תת-חבורה מקסימלית של  $G$  היא נורמלית. ( $M \leq G$  היא מקסימלית אם  $M \neq G$  וגם אם  $M \leq H \leq G$ , אז  $H = M$  או  $H = G$ ).

4. כל תת-חבורת סילו של  $G$  היא נורמלית.

5. החבורה  $G$  היא מכפלה ישרה של תת-חבורות סילו שלה. (כלומר יהיו  $p_1, \dots, p_r$  הראשוניים שפחלקים את  $|G|$ , ותהינה  $P_1, \dots, P_r$  תת-חבורות  $p_i$ -סילו, בהתאמה. אז  $G \cong P_1 \times \dots \times P_r$ )

הוכחת 1. גורר 2. נניח כי  $G$  נילפוטנטית. לכן הסדרה המרכזית היורדת שלה

$$\{e\} = \gamma_n(G) \triangleleft \gamma_{n-1}(G) \triangleleft \dots \triangleleft \gamma_1(G) = G$$

מגיעה ל- $\{e\}$  אחרי מספר סופי של צעדים. לא נסתמך על כך ש- $G$  סופית. תמיד מתקיים  $H \leq N_G(H)$  בנוסף אם  $H \leq G = \gamma_1(G)$  וגם  $\{e\} = \gamma_n(G)$ , אז קיים  $1 \leq k < n$  מקסימלי עבורו  $\gamma_{k+1}(G) \leq H$  וגם  $\gamma_k(G) \not\leq H$ . אנחנו נראה כי  $\gamma_k(G) \leq N_G(H)$ .

יהי  $g \in \gamma_k(G)$  ו- $h \in H \leq G$  אז

$$[h, g] \in [G, \gamma_k(G)] = \gamma_{k+1}(G) \leq H$$

לכן  $[h, g] = hgh^{-1}g^{-1} \in H$  מפני ש- $h \in H$ , אז  $h^{-1} \in H$  ולכן

$$gh^{-1}g^{-1} = h^{-1}hgh^{-1}g^{-1} \in H$$

ולכן  $g \in N_G(H)$ . אבל  $\gamma_k(G)$  מכיל איברים שאינם ב- $H$ , ולכן  $H \subsetneq N_G(H)$ . □

הערה 0.7 (ב. פלוטקין, 1954). תהי  $G$  חבורה. אם לכל תת-חבורה נאותה  $H \leq G$  מתקיים  $H \subsetneq N_G(H)$ , אז  $G$  היא נילפוטנטית מקומית (כלומר כל תת-חבורה נוצרת סופית שלה היא נילפוטנטית).

בפרט, אם  $G$  נוצרת סופית, ולכל תת-חבורה נאותה  $H \leq G$  מתקיים  $H \subsetneq N_G(H)$ , אז  $G$  נילפוטנטית.

הוכחת 2. גורר 3. נניח לכל תת-חבורה נאותה  $H \leq G$  מתקיים  $H \subsetneq N_G(H)$ . תהי  $M \leq G$  מקסימלית. אז

$$M \subsetneq N_G(M) \leq G$$

ולכן  $N_G(M) = G$ . כלומר  $M \triangleleft G$ . □

הוכחת 3. גורר 4. נניח שכל תת-חבורה מקסימלית של  $G$  היא נורמלית. תהי  $P \leq G$  תת-חבורת  $p$ -סילו, ונניח בשלילה שהיא לא נורמלית. כלומר

$$N_G(P) \neq G$$

אז יש תת-חבורה מקסימלית  $M \leq G$  המכילה את  $N_G(P)$ . אנחנו נראה כי  $N_G(M) = M$ , וזו סתירה להנחה  $N_G(M) = G$ . יהי  $g \in N_G(M)$ , אז

$$gPg^{-1} \subseteq gN_G(P)g^{-1} \subseteq gMg^{-1} = M$$

ולכן  $gPg^{-1}$  היא תת-חבורת  $p$ -סילו של  $M$  (כי הסדר של  $M$  מחלק את הסדר של  $G$ ). אז קיים  $m \in M$  כך ש- $gPg^{-1} = mPm^{-1}$  (לפי משפט סילו 2). לכן

$$P = m^{-1}gPg^{-1}m = (m^{-1}g)P(m^{-1}g)^{-1}$$

אז קיבלנו כי  $m^{-1}g \in N_G(P)$  אז  $g \in mN_G(P) \subseteq M$  לכן  $N_G(M) = M \neq G$ . □ וזו הסתירה שרצינו.

הוכחת 4. גורר 5. נניח כי כל תת-חבורת סילו של  $G$  היא נורמלית. נרצה להוכיח שאם  $p_1, \dots, p_r$  הם הראשוניים שמחלקים את  $|G|$ , ותהינה  $P_1, \dots, P_r$  תת-חבורות  $p_i$ -סילו, בהתאמה, אז  $G \cong P_1 \times \dots \times P_r$ .

אם  $r = 1$ , אז  $G = P_1$  היא מכפלה ישרה של "כל" תת-חבורות  $p_1$ -סילו שלה.

עבור  $r > 1$ , נעזרים באינדוקציה. צריך לבדוק שכל התנאים למכפלה ישרה (פנימית) מתקיימים. ברור לפי ההנחה כי  $P_i \triangleleft G$  לכל  $1 \leq i \leq r$ . מפני שהסדרים זרים (בזוגות), אז אפשר להוכיח כי

$$P_i \cap (P_1 \dots P_{i-1} P_{i+1} \dots P_r) = \{e\}$$

אם מניחים את נכונות הטענה עבור חבורות עם  $r - 1$  ראשוניים שמחלקים אותו, אז

$$(P_1 \dots P_{r-1})P_r/P_r \cong P_r/(P_1 \dots P_{r-1} \cap P_r) \cong P_r$$

□ לפי משפט האיזומורפיזמים השני.

הוכחה 5. גורר 1. נניח כי  $G$  היא מכפלה ישרה (סופית) של תת-חבורות סילו שלה. בהרצאה הקודמת ראינו שכל חבורת- $p$  היא נילפוטנטית. אם  $H, K$  הן חבורות נילפוטנטיות ממעלת נילפוטנטיות  $c$  לכל היותר, אז

$$\begin{aligned} \gamma_{c+1}(H) &= \{e_H\} \\ \gamma_{c+1}(K) &= \{e_K\} \\ \gamma_{c+1}(H \times K) &= \gamma_{c+1}(H) \times \gamma_{c+1}(K) = \{e_H\} \times \{e_K\} = \{e_{H \times K}\} \end{aligned}$$

ובאינדוקציה על מספר הראשוניים שמחלקים את  $|G|$ , נקבל כי  $G$  נילפוטנטית בתור מכפלה ישרה של חבורות נילפוטנטיות. □

**מסקנה 0.8.** תהי  $G$  חבורה נילפוטנטית סופית. אם  $m$  מחלק את הסדר של  $G$ , אז קיימת ל- $G$  תת-חבורה מסדר  $m$ .

$$m = p_1^{c_1} \dots p_r^{c_r} |p_1^{a_1} \dots p_r^{a_r}| = |G|$$

הערה 0.9. לחבורות פתירות סופית יש משהו דומה. אם  $m$  זר ל- $|G|/m$ , אז קיימת ל- $G$  תת-חבורה מסדר  $m$  (והאינדקס שלה זר לה). נשים לב שההפך לא נכון: למשל ל- $S_3$  שאינה נילפוטנטית יש תת-חבורה מכל סדר שמחלק אותה.

## 0.2 חבורות אבליות נוצרות סופית

**תזכורת 0.10.** חבורה  $G$  נקראת נוצרת סופית אם קיימים מספר סופי של איברים  $g_1, \dots, g_n$  כך ש- $G = \langle g_1, \dots, g_n \rangle$ . אם בנוסף  $G$  אבלית, אז כל איבר  $g \in G$  ניתן להציג

$$g = g_1^{a_1} g_2^{a_2} \dots g_n^{a_n}$$

עבור  $a_1, \dots, a_n \in \mathbb{Z}$ .

**דוגמה 0.11.** הוכחתם מתישהו כי  $\mathbb{Q}$  וגם  $\mathbb{Q}^*$  אינן נוצרות סופית. החבורה  $\mathbb{R}$  לא נוצרת סופית משיקולי עוצמה, כי כל חבורה נוצרת סופית היא מעוצמה  $\aleph_0$  לכל היותר.

**משפט 0.12** (משפט המיון לחבורות אבליות נוצרות סופית). תהי  $G$  חבורה אבלית נ"ס. אז  $G$  איזומורפית למכפלה הישרה

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$$

כאשר  $r$  נקרא הדרגה של  $G$  (בפרט  $r = 0$  אם ורק אם  $G$  סופית) ו- $n_i \in \mathbb{N}$  לכל  $1 \leq i \leq s$ . אם זורשים ש- $n_i | n_{i+1}$  לכל  $1 \leq i < s$ , אז זאת נקראת הצורה הקנונית של  $G$ . היא קיימת ויחידה. למספרים  $n_1, \dots, n_s$  במקרה הזה קוראים המחלקים האלמנטריים של  $G$ .

**הערה 0.13**. אם  $G$  אבלית סופית, בצורה הקנונית המספר  $n_s$  הוא המעריך  $\exp(G)$  של  $G$  (זהו המספר המינימלי עבורו  $g^{\exp(G)} = e$  לכל  $g \in G$ ). מספר היוצרים המינימלי של  $G$  הוא  $s$ .

מפני שכל חבורה אבלית היא נילפוטנטית, אז  $G$  היא מכפלה ישרה של תת-חבורות סילו שלה.

**הגדרה 0.14**. תהי  $G$  חבורה אבלית סופית מסדר  $n = p_1^{a_1} \cdots p_r^{a_r}$ . אז

$$G \cong P_1 \times \cdots \times P_r$$

כאשר  $P_i$  היא תת-חבורת  $p_i$ -סילו לכל  $i$  מסדר  $p_i^{a_i}$ . זהו הפירוק הפרימרי של  $G$ . כל חבורת- $p$  אבלית סופית מסדר  $a$  אפשר להציג בדרך הבאה:

$$P \cong \mathbb{Z}_{p^{b_1}} \times \cdots \times \mathbb{Z}_{p^{b_m}}$$

כאשר  $b_1 + \cdots + b_m = a$ . באופן דומה

$$P_i \cong \mathbb{Z}_{p^{b_{i,1}}} \times \cdots \times \mathbb{Z}_{p^{b_{i,m_i}}}$$

האיברים ברב-הקבוצה  $\left\{ \left\{ p_1^{b_{1,1}}, \dots, p_1^{b_{1,m_1}}, p_2^{b_{2,1}}, \dots, p_2^{b_{2,m_2}}, \dots, p_r^{b_{r,1}}, \dots, p_r^{b_{r,m_r}} \right\} \right\}$  נקראים הגורמים הפרימריים של  $G$ , ורב-הקבוצה הזו קובעת את  $G$  עד כדי איזומורפיזם.

**דוגמה 0.15**. החבורה  $\mathbb{Z}_3 \times \mathbb{Z}_8$  לא איזומורפית לחבורה  $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ , למרות ששתיהן מסדר 24.

**הערה 0.16**. כדי לעבור בין הצורה הקנונית של  $G$  (עם המחלקים האלמנטריים) לבין הפירוק הפרימרי (עם החזקות של הראשוניים), משתמשים כמה וכמה פעמים במשפט השאריות הסיני:

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$$

אם ורק אם  $(n, m) = 1$ .

**דוגמה 0.17.** נמייך את כל החבורות האבליות מסדר  $72 = 2^3 \cdot 3^2$ . יש 3 חלוקות של 3 והן

$$1 + 1 + 1 = 2 + 1 = 3$$

ויש 2 חלוקות של 2 שהן  $1 + 1 = 2$ . לכן החבורות האבליות מסדר 72 עד כדי איזומורפיזם הן

$$\begin{aligned} \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 &\cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6 \\ \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 &\cong \mathbb{Z}_6 \times \mathbb{Z}_{12} \\ \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 &\cong \mathbb{Z}_3 \times \mathbb{Z}_{24} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{18} \\ \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 &\cong \mathbb{Z}_2 \times \mathbb{Z}_{36} \\ \mathbb{Z}_8 \times \mathbb{Z}_9 &\cong \mathbb{Z}_{72} \end{aligned}$$

**טענה 0.18.** אפשר להסיק שמספר החבורות האבליות מסדר  $p_1^{a_1} \dots p_r^{a_r}$  הוא  $\rho(a_1) \dots \rho(a_r)$  כאשר  $\rho(k)$  הוא מספר החלוקות של המספר הטבעי  $k$ . בפרט, חבורה אבלית מסדר חופשי מריבועים היא ציקלית. עכשיו אפשר לגשת להוכחת המיון לפחות עבור חבורות אבליות סופיות.

$$\begin{aligned} T \leq G &\Rightarrow T \triangleleft G \\ G &\cong (G/T) \times T \end{aligned}$$

**טענה 0.19.** תהי  $G$  חבורה אבלית נ"ס עם קבוצת יוצרים  $g_1, \dots, g_k$ . לכל  $c_1, \dots, c_k \in \mathbb{Z}$  עבורם  $\gcd(c_1, \dots, c_k) = 1$  קיימת קבוצת יוצרים  $h_1, \dots, h_k$  של  $G$  עבורם  $h_1 = g_1^{c_1} \dots g_k^{c_k}$ .

הוכחה. על ידי החלפת  $g_i$  ב- $g_i^{-1}$  במידת הצורך, אפשר להניח בלי הגבלת הכלליות כי  $c_i \geq 0$ . נוכיח את הטענה עם אינדוקציה על  $C = c_1 + \dots + c_k \geq 1$ . אם  $C = 1$ , אז מספיק לבצע תמורה על קבוצת היוצרים המקורית (כי אז  $c_i = 0$  לכל  $i$  פרט למקום אחד שבו  $c_i = 1$ ). אם  $C > 1$ , אז מפני ש- $\gcd(c_1, \dots, c_k) = 1$ , אז בהכרח קיימים  $i \neq j$  כך ש- $c_i$  ו- $c_j$  שונים מאפס. נניח  $c_1 \geq c_2 > 0$ . נשים לב שגם  $g_1, g_1 g_2, g_3, \dots, g_k$  היא קבוצת יוצרים של  $G$  בגודל  $k$ . בנוסף

$$1 = \gcd(c_1, c_2, \dots, c_k) = \gcd(c_1 - c_2, c_2, \dots, c_k)$$

וכן

$$(c_1 - c_2) + c_2 + \dots + c_k = c_1 + c_3 + \dots + c_k < C$$

לכן לפי הנחת האינדוקציה קיימת קבוצת יוצרים  $h_1, \dots, h_k$  עבורה

$$h_1 = g_1^{c_1 - c_2} (g_1 g_2)^{c_2} g_3^{c_3} \dots g_k^{c_k} = g_1^{c_1} \dots g_k^{c_k}$$

□ כאשר השתמשנו באבליות של  $G$ , וקיבלנו את קבוצת היוצרים הרצויה.

לפני הוכחת משפט המיזון, נראה מסקנה יפה שלו:

טענה 0.20. תהי  $G$  חבורה אבלית סופית. אם לכל  $n \in \mathbb{N}$  היא מכילה לכל היותר  $n$  איברים מסדר שמחלק את  $n$ , אז היא ציקלית.

הוכחה. נניח  $G \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_s}$  לפי משפט המיזון. אם  $n | n_i, n_j$  עבור  $i \neq j$ , אז יש ב- $G$  יותר מ- $n$  איברים מסדר שמחלק את  $n$ .

$$\mathbb{Z}_{n_i} = \mathbb{Z}_{an}$$

$$\mathbb{Z}_{n_j} = \mathbb{Z}_{bn}$$

אז לפי ההנחה נסיק כי  $n_i$  ו- $n_j$  זרים לכל  $i \neq j$ . לכן בעזרת שימוש חוזר במשפט השאריות הסיני נקבל

$$G \cong \mathbb{Z}_{n_1 \dots n_s}$$

□

והיא ציקלית.

**דוגמה 0.21.** יהי  $F$  שדה. האיברים ב- $F^*$  מסדר שמחלק  $n \in \mathbb{N}$  הם בדיוק השורשים של הפולינום  $x^n - 1 \in F[x]$ . תחת ההנחה שיש פירוק יחיד לפולינומים מעל שדה, אז לפולינום  $x^n - 1$  יש לכל היותר  $n$  שורשים בשדה. לכן כל תת-חבורה סופית של  $F^*$  היא ציקלית. בפרט החבורה  $\mathbb{F}_p^* \cong U_p$  היא ציקלית לכל  $p$  ראשוני.

הוכחת משפט המיזון לחבורות אנליות סופיות. תהי  $G$  חבורה אבלית סופית, ונוכיח באינדוקציה על מספר היוצרים המינימלי  $k$  של  $G$ .

אם  $k = 1$ , אז  $G$  ציקלית, ומשפט המיזון ברור. אחרת, נניח את נכונות המשפט עבור  $k - 1$  ונוכיח אותו עבור  $k$  באינדוקציה. מבין כל קבוצות היוצרים של  $G$  בגודל

$k$  נבחר קבוצת יוצרים  $x_1, \dots, x_k$  כאשר  $x_1$  הוא מסדר מינימלי.

נסמן  $d_i = o(x_i)$  לכל  $i$  וגם  $d = \gcd(d_1, \dots, d_k)$ . אם  $d_i = du_i$ , אז  $\gcd(u_1, \dots, u_k) = 1$ . לפי טענה קודמת קיימת קבוצת יוצרים  $h_1, \dots, h_k$  של  $G$  עבורם  $h_1 = x_1^{u_1} \dots x_k^{u_k}$  ברור כי

$$h_1^d = x_1^{d u_1} \dots x_k^{d u_k} = e$$

וגם  $d | d_1$ . כלומר  $d \leq d_1$  והמינימליות של  $d_1$  נסיק  $d = d_1$ .

נסמן  $H = \langle x_1 \rangle$  ו- $K = \langle x_2, \dots, x_k \rangle$ . נטען כי  $G \cong H \times K$ . מפני ש- $H$  ציקלית ו- $K$  היא מכפלה ישרה של  $k - 1$  חבורות ציקליות לפי הנחת האינדוקציה, אז זה יסיים את הוכחת המשפט.

החבורה  $G$  אבלית, ולכן ברור כי  $H, K \triangleleft G$ . בנוסף הן יוצרות את  $G = HK$  (כי  $HK$  כוללת את  $x_1, \dots, x_k$ ). נותר להוכיח  $H \cap K = \{e\}$ . נניח בשלילה כי קיים איבר  $e \neq g \in H \cap K$ , ולכן קיימים מספרים  $r_1, \dots, r_k \in \mathbb{Z}$  כך ש-

$$H \ni x_1^{r_1} = x_2^{r_2} \dots x_k^{r_k} \in K$$

וגם  $1 \leq r_1 < d_1$ . נסמן  $r = \gcd(r_1, \dots, r_k)$  ולכל  $i$  נניח  $r_i = r v_i$ . אז באופן דומה  $\gcd(-v_1, \dots, v_k) = 1$ . לפי הטענה הקודמת נקבל שיש קבוצת יוצרים  $h_1, \dots, h_k$  עבורה

$$h_1 = x_1^{-v_1} x_2^{v_2} \dots x_k^{v_k}$$

ונחשב כי

$$h_1^r = (x_1^{-v_1} x_2^{v_2} \dots x_k^{v_k})^r = x_1^{-r v_1} x_2^{r v_2} \dots x_k^{r v_k} = e$$

כלומר  $|o(h_1)|r < d_1$ . זו סתירה למינימליות של  $d_1$ , ולכן  $H \cap K = \{e\}$ .  
 קיבלנו שיש איזומורפיזם  $G \cong \mathbb{Z}_d \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$  כאשר  $m_i | m_{i+1}$  לכל  $1 \leq i < k$ .  
 לפי הנחת האינדוקציה. נותר להוכיח כי  $d | m_2$ . לכל  $1 \leq i \leq k$  נבחר איבר

$$y_i = (0, \dots, 1, \dots, 0) \in \mathbb{Z}_d \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$$

שבו יש רק 1 במקום ה- $i$ . הקבוצה  $y_1, \dots, y_k$  יוצרת את  $G$  (בתמונה של האיזומורפיזם),  
 וגם  $y_1$  הוא מסדר  $d = d_1$ . מפני ש- $d_1$  הוא מינימלי ו- $o(y_1) = m_1$  לכל  $2 \leq i \leq k$ .  
 לפי טיעון דומה שהיה בתחילת ההוכחה נקבל  $m_1 = d = \gcd(m_1, \dots, m_k)$ . בפרט  $d | m_2$ , וסיימנו.  $\square$

(לא הספקנו לדבר על מכפלות ישרות למחצה ועל הרחבות של חבורות. יש עוד הרבה מה ללמוד!)  
 תם ולא נשלם.