

# תורת החבורות 88-218-01 תשפ"א

## הערות הרצאה 2

שלום!

**תזכורת 0.1.** מה זו חבורה? מה זו תת-חבורה.

טענה 0.2. תהי  $G$  חבורה, ותהי  $H \leq G$  תת-חבורה. אז  $e_G = e_H$ .  
הוכחה. מתקיים  $e_H e_H = e_H$  ב- $H$ . המשוואה הזאת נכונה גם ב- $G$ . נכפיל ב- $e_H^{-1}$  שקיים ב- $G$  ונקבל

$$e_H = e_H e_G = e_H e_H e_H^{-1} = e_H e_H^{-1} = e_G$$

□

וסיימנו.

טענה 0.3 (קריטריון המקוצר לתת-חבורה). תהי  $H \subseteq G$  תת-קבוצה בחבורה. אזי  $H$  תת-חבורה של  $G$  אם ורק אם שני התנאים הבאים מתקיימים:

1.  $H \neq \emptyset$  (בדרך כלל קל להראות  $e \in H$ ).

2. לכל  $h_1, h_2 \in H$ , גם  $h_1 \cdot h_2^{-1} \in H$ .

הוכחה. בכיוון הקל, אם  $H \leq G$ , אז...

בכיוון השני, קיים  $x \in H$  כלשהו לפי התנאי הראשון. לפי התנאי השני  $e_G = e_H$   
 $x \cdot x^{-1} \in H$  לכן ב- $H$  יש את איבר היחידה. קיבוציות הפעולה מגיעה בחינם  
מהפעולה ב- $G$ . נוכיח סגירות להופכי: יהי  $x \in H$  כלשהו, אז לפי התנאי השני  
 $x^{-1} = e \cdot x^{-1} \in H$  נשאר להוכיח סגירות לפעולה: יהיו  $x, y \in H$ . ידוע לנו כי  
□  $y^{-1} \in H$ , ולכן  $x \cdot y = x \cdot (y^{-1})^{-1} \in H$  בסך הכל  $H \leq G$ .

**דוגמה 0.4.** תהי  $X$  קבוצה, ונתבונן בחבורה  $S_X$ . יהי  $a \in X$  ונסמן את המייצג שלו להיות

$$\text{stab}(a) = \{\sigma \in S_X \mid \sigma(a) = a\} \subseteq S_X$$

נשתמש בקריטריון המקוצר לתת-חבורה כדי להראות  $\text{stab}(a) \leq S_X$ . קל לשים לב ש- $\text{id}_X \in \text{stab}(a)$  כי  $\text{id}_X(a) = a$ . לכן מתקיים התנאי הראשון בקריטריון.

נשים לב שאם  $\sigma \in \text{stab}(a)$ , אז  $\sigma(a) = a$  ומפני שב- $S_X$  יש רק פונקציות הפיכות, נסיק  $\sigma^{-1}(a) = a$ . אז לכל  $\tau, \sigma \in \text{stab}(a)$  מתקיים

$$(\tau \circ \sigma^{-1})(a) = \tau(\sigma^{-1}(a)) = \tau(a) = a$$

ולכן  $\tau \circ \sigma^{-1} \in \text{stab}(a)$ . לכן מדובר בתת-חבורה לפי הקריטריון המקוצר. תוספת: תהי  $A \subseteq X$  ונגדיר  $\text{stab}(A) = \bigcap_{a \in A} \text{stab}(a)$ . הראו כי  $\text{stab}(A) \leq S_X$ .

### 0.1 חבורות ציקליות

**הגדרה 0.5.** תהי  $G$  חבורה. אם קיים איבר  $a \in G$  כך ש- $\langle a \rangle = G$ , נאמר כי  $G$  היא ציקלית וכי  $a$  הוא יוצר שלה.

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} \leq G$$

**דוגמה 0.6.** החבורה  $\mathbb{Z}$  (מבלי לרשום שום דבר נוסף הפעולה היא חיבור רגיל) היא ציקלית. למשל

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$$

ואלו כל היוצרים של  $\mathbb{Z}$ .

הערה 0.7. כל חבורה ציקלית היא אבלית, כי חזקות של אותו איבר מתחלפות, והרי כל האיברים בחבורה ציקלית ניתן להציג כחזקות של היוצר.

**מסקנה 0.8.** החבורה  $S_3 = S_{\{1,2,3\}}$  אינה ציקלית, כי אינה אבלית.

**דוגמה 0.9.** ראינו כי  $(\mathbb{Q}, +)$  חבורה אבלית. לא היא אינה ציקלית? נניח בשלילה שיש יוצר  $\frac{a}{b} \in \mathbb{Q}$ . האם ניתן להציג כל מספר רציונלי  $\frac{c}{d} \in \mathbb{Q}$  כחזקה (לגבי פעולת החיבור)?

$$\left(\frac{a}{b}\right)^k = \frac{a}{b} + \frac{a}{b} + \dots + \frac{a}{b} = \frac{ka}{b}$$

ברור שלא, ולכן  $\mathbb{Q}$  אינה ציקלית.

**הגדרה 0.10.** יהיו  $a, b \in \mathbb{Z}$ . נאמר כי  $a$  מחלק את  $b$  אם קיים  $k \in \mathbb{Z}$  כך ש- $b = ka$ . נסמן זאת  $a|b$ . למשל  $3|6$  או  $100|3000$ .

**הגדרה 0.11.** יהי  $n \in \mathbb{N}$ . נאמר כי  $a, b \in \mathbb{Z}$  שקולים מודולו  $n$  אם  $n|a - b$ .

טענה 0.12. שקילות מודולו  $n$  היא יחס שקילות על  $\mathbb{Z}$ . מחלקות השקילות מתאימות לשארית החלוקה ב- $n$ . לכן יש בדיוק  $n$  מחלקות שקילות.

כפל וחיבור מודולו  $n$  מוגדרים היטב. כלומר אם  $a \equiv b, c \equiv d \pmod{n}$ , אז  $ac \equiv bd \pmod{n}$  וגם  $a + c \equiv b + d \pmod{n}$ . הן פעולות חילופיות.

הוכחה. כדי להוכיח יחס שקילות צריך להוכיח רפלקסיביות, סימטריות וטרנזיטיביות. דיברנו על זה...

נניח  $a \equiv b \pmod{n}$  וגם  $c \equiv d \pmod{n}$ . אז קיימים  $k, k' \in \mathbb{Z}$  כך ש-

$$a - b = kn, \quad c - d = k'n$$

נסכום את המשוואות האלו ונקבל

$$(a - b) + (c - d) = (a + c) - (b + d) = (k + k')n$$

ומפני שגם  $k + k' \in \mathbb{Z}$  קיבלנו כי

□  $a + c \equiv b + d \pmod{n}$ . בבית הוכיחו כי הכפל מוגדר היטב.

**דוגמה 0.13.** יש לנו קבוצה

$$\mathbb{Z}_n = \{[a] \mid a \in \mathbb{Z}\} = \{[0], [1], \dots, [n-1]\}$$

כאשר  $[a]$  מסמנת את מחלקת השקילות של  $a$  מודולו  $n$ . לרוב פשוט נכתוב  $a$ . אז  $(\mathbb{Z}_n, +)$  כאשר הפעולה  $+$  היא חיבור מודולו  $n$  היא חבורה. איבר היחידה הוא  $[0]$ , שהרי

$$[a] + [0] = [0] + [a] = [a]$$

ההופכי של  $[a]$  הוא  $[n-a]$ . היא אבלית.

$\mathbb{Z}_2 = \{[0], [1]\}$  והיא ציקלית. יש לה רק יוצר אחד והוא  $[1]$ . החבורה  $\mathbb{Z}_{10}$  גם היא ציקלית, ולה כבר יש ארבעה יוצרים:  $[1], [3], [7], [9]$ .

$$\langle [3] \rangle = \{[0], [3], [6], [9], [2], [5], [8], [1], [4], [7]\} = \mathbb{Z}_{10}$$

**דוגמה 0.14.** יש עוד פעולה לגבי  $\mathbb{Z}_n$  והיא כפל מודולו  $n$ . המבנה האלגברי  $(\mathbb{Z}_n, \cdot)$  אינו חבורה, למשל כי אין הופכי ל- $[0]$ . מה יקרה אם נגדיר  $\widehat{\mathbb{Z}}_n = \mathbb{Z}_n \setminus \{[0]\}$ , האם  $(\widehat{\mathbb{Z}}_n, \cdot)$  חבורה? אם ורק אם  $n$  ראשוני. עבור  $n = 6$  למשל אין אפילו סגירות! לדוגמה  $[2] \cdot [3] = [0] \notin \widehat{\mathbb{Z}}_6$ .

0.15. הערה. החבורה  $(\mathbb{Z}_n, +)$  אינה תת-חבורה של  $(\mathbb{Z}, +)$ . לא מדובר בתת-קבוצה בכלל, והפעולות הן שונות למרות שהסימנים זהים.

## 0.2 סדרים

**0.16. הגדרה.** תהי  $G$  חבורה. הסדר של החבורה  $G$  הוא עוצמתה כקבוצה. במילים פחות פורמליות, כמה איברים יש בה. נסמן את הסדר של  $G$  ב- $|G|$ .

**דוגמה 0.17.** מתקיים  $|\mathbb{Z}_6| = 6, |S_n| = n!, |\mathbb{Z}| = \infty, |U(\mathbb{Z}, \cdot)| = 2$ .

**הגדרה 0.18.** תהי  $(G, \cdot, e)$  חבורה, ויהי  $g \in G$ . הסדר של האיבר  $g$  הוא המספר הטבעי הקטן ביותר  $n$  המקיים  $g^n = e$ , ואם לא קיים כזה נאמר שהסדר אינסופי. נסמן את הסדר של  $g$  ב- $o(g)$ .

$$\min \{n \in \mathbb{N} \mid g^n = e\}$$

טענה 0.19. בחבורה סופית, הסדר של כל איבר הוא סופי.

הוכחה. יהי  $g \in G$  איבר בחבורה סופית. אז הקבוצה של החזקות הטבעיות של  $g$  היא תת-קבוצה של  $G$ :

$$\{g^n \mid n \in \mathbb{N}\} \subseteq G$$

ולכן היא סופית. לכן קיימים  $n \neq m \in \mathbb{N}$  כך ש- $g^n = g^m$ . בלי הגבלת הכלליות  $n > m$ , על ידי צמצום (כלומר כפל ב- $g^{-m}$ ) נקבל

$$g^{n-m} = g^n g^{-m} = g^m g^{-m} = e$$

והרי  $n - m \in \mathbb{N}$ . אז  $o(g) \leq n - m$ .  $\square$

**דוגמה 0.20.** בחבורה  $\mathbb{Z}$  הסדר של 0 הוא 1, והסדר של שאר האיברים הוא  $\infty$ .  
בכל חבורה איבר היחידה הוא מסדר 1, והוא האיבר היחיד מסדר 1.  
בחבורה  $\mathbb{Z}_6$  הסדר של האיברים הוא

$$o(0) = 1$$

$$o(1) = 6$$

$$o(2) = 3$$

$$o(3) = 2$$

$$o(4) = 3$$

$$o(5) = 6$$

**דוגמה 0.21.** בחבורה  $GL_2(\mathbb{R})$  נתבונן באיבר  $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$  ונחשב את הסדר שלו:

$$b^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \neq I_2$$

$$b^3 = b^2 \cdot b = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

ולכן  $o(b) = 3$

**דוגמה 0.22** (סדר של מכפלה). בהנתן  $n, m, r > 1$  שלמים קיימת חבורה  $G$  (אפילו סופית) שבה יש איברים  $a, b \in G$  כך שמתקיים

$$o(a) = n, o(b) = m, o(ab) = r$$

נראה גרסה צנועה יותר של הטענה הזו: יהי  $r \geq 3$  ונתבונן במטריצות

$$A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

אז מתקיים  $o(A) = o(B) = 2$ , אבל  $o(AB) = \infty$  שהרי

$$(AB)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

אם נתבונן בחבורה  $G = GL_2(\mathbb{Z}_r)$ , אז  $A, B \in G$  ואז  $o(AB) = r$

הערה 0.23 (אזהרה נוספת). לרוב  $(ab)^n \neq a^n b^n$ . זה נכון בחבורות אבליות, ורק בחבורות לא אבליות מאוד מסוימות ולרוב לא נכון.

**משפט 0.24** (משפט החילוק, או חלוקה אוקלידית). לכל  $n \in \mathbb{Z}$  ולכל  $d \neq 0$  שלם קיימים  $q, r$  יחידים כך ש- $n = qd + r$  כאשר  $0 \leq r < |d|$ .

הוכחה. באינדוקציה (לביט).  $\square$

0.25. טענה. תהי  $G$  חבורה, ויהי  $g \in G$ . אז  $g^n = e$  אם ורק אם  $o(g) | n$ .

0.26. טענה. תהי  $G$  חבורה, ויהי  $g \in G$ . אם  $g^n = g^m$  אם ורק אם  $o(g) | n - m$ .

הוכחה. נניח בלי הגבלת הכלליות  $n \geq m$ . אז  $g^n = g^m \cdot g^{n-m}$ . לכן בעזרת צמצום הטענה  $g^n = g^m$  שקולה לטענה  $g^{n-m} = e$ .

בכיוון אחד, נניח  $o(g) | n - m$ . אז קיים  $k \in \mathbb{Z}$  כך ש- $n - m = k \cdot o(g)$ . לכן

$$g^{n-m} = g^{k \cdot o(g)} = (g^{o(g)})^k = e^k = e$$

בכיוון השני, נניח  $g^{n-m} = e$ . אם  $n = m$ , הטענה בוודאי נכונה (עבור  $o(g) = \infty$  נכונה באופן ריק). אם  $n \neq m$ , אז בהכרח  $o(g) \neq \infty$ . נשתמש בחלוקה אוקלידית ונחלק את  $n - m$  ב- $o(g)$  עם שארית. כלומר קיימים  $q, r \in \mathbb{Z}$  כך ש-

$$n - m = q \cdot o(g) + r$$

וגם  $0 \leq r < o(g)$ . לכן

$$e = g^{n-m} = g^{q \cdot o(g) + r} = (g^{o(g)})^q g^r = e^q g^r = g^r$$

כלומר  $g^r = e$ . לפי המינימליות של הסדר, נקבל בהכרח כי  $r = 0$  (אחרת  $r$  חיובי וקטן ממש מ- $o(g)$ ...). כלומר  $n - m = q \cdot o(g)$ , או לפי הגדרה  $o(g) | n - m$ .  $\square$

**מסקנה 0.27**. סדרת החזקות הטבעיות של  $g$  מכילה בדיוק  $o(g)$  איברים שונים.

הוכחה. אם  $o(g) = \infty$ , אז כל שתי חזקות של  $g$  הן שונות. הרי אם  $g^n = g^m$ , נקבל  $g^{n-m} = e$ . בסתירה להנחה על הסדר.

אחרת, אם  $o(g)$  סופי, אז האיברים  $g, g^2, g^3, \dots, g^{o(g)}$  הם  $o(g)$  איברים שונים. לעומת זאת עבור חזקה  $g^n$  אחרת, נוכל לחלק את  $n$  ב- $o(g)$  ונמשיך כמו בטענה הקודמת כדי לקבל את שארית החלוקה... □

**מסקנה 0.28.** בחבורה סופית  $G$  מסדר  $n$ , איבר  $g \in G$  הוא יוצר כחבורה ציקלית (ואז  $G$  ציקלית) אם ורק אם  $o(g) = n$ .

**מסקנה 0.29.** בכל חבורה, לכל  $g \in G$  מתקיים  $|\langle g \rangle| = o(g)$ .

**תרגיל 0.30.** תהי  $G$  חבורה, ויהי  $a \in G$ . נניח  $o(a) = n < \infty$ . אז לכל  $d \leq n$  טבעי מתקיים

$$o(a^d) = \frac{n}{\gcd(d, n)} = \frac{n}{(d, n)} = \frac{o(a)}{(d, o(a))}$$

הוכחה. נוכיח היתכנות של הסדר, ואז מינימליות. נשים לב כי

$$(a^d)^{\frac{n}{(d, n)}} = (a^n)^{\frac{d}{(d, n)}} = e^{\frac{d}{(d, n)}} = e$$

כלומר  $o(a^d) \leq \frac{n}{(d, n)}$ .

קעת נניח כי  $(a^d)^t = e$  עבור  $t$  טבעי כלשהו, ונראה כי  $\frac{n}{(d, n)} | t$ . אז  $a^{dt} = e$  ואז לפי טענה קודמת נקבל  $n | dt$  כי  $n = o(a)$ . זה (הכוונה  $n | dt$ ) קורה אם ורק אם  $n | dt$  וגם  $n | nt$ , וזה מתקיים אם ורק אם  $n | (nt, dt)$ , וזה מתקיים אם ורק אם  $n | t(n, d)$ , אם ורק אם  $\frac{n}{(n, d)} | t$ . כלומר  $\frac{n}{(d, n)} \leq o(a^d) \leq \frac{n}{(n, d)}$ , ומכאן מסיימים. □

**מסקנה 0.31.** הסדר של  $a \in \mathbb{Z}_n$  הוא  $o(a) = \frac{n}{(a, n)}$ . כי  $a = "1^a" = 1 + \dots + 1$ , וידוע לנו כי  $o(1) = n$ .

בפרט, לכל  $d$  שמחלק את  $n$ , קיים איבר  $\mathbb{Z}_n$ - מסדר  $d$ , למשל  $[\frac{n}{d}] \in \mathbb{Z}_n$ .

טענה 0.32. תהי  $G$  חבורה ציקלית. אז כל תת-חבורה שלה היא ציקלית.

הוכחה. תהי  $H \leq G$  תת-חבורה. נניח כי  $G = \langle a \rangle$ . בפרט, כל האיברים של  $H$  הם חזקות שלמות של  $a$ .

אם  $H = \{e\}$ , אז  $H = \langle e \rangle = \langle a^0 \rangle$ , וסיימנו. אחרת, נניח כי  $H$  לא טריוויאלית. יהי  $s$  המספר הטבעי הקטן ביותר כך ש- $a^s \in H$ . שימו לב שאם  $a^T \in H$ , אז  $a^{-T} \in H$ .

קעת נרצה להוכיח כי  $H = \langle a^s \rangle$ . בהכלה דו-כיוונית, בכיוון הקל  $\langle a^s \rangle \subseteq H$ , כי  $a^s \in H$  ויש סגירות לפעולה ולהופכי. בכיוון השני, יהי  $a^k \in H$ . לפי חלוקה אוקלידית קיימים  $q, r$  כך ש- $k = qs + r$  וגם  $0 \leq r < s$ . לכן

$$H \ni a^k = a^{qs+r} = (a^s)^q a^r$$

אז  $a^r = a^k (a^s)^{-q} \in H$ . אבל  $a^k, a^s \in H$ , ולכן גם  $a^r \in H$ . מהמינימליות של  $s$ , בהכרח  $r = 0$ , ולכן  $k = qs$ . כלומר  $a^k \in \langle a^s \rangle$ . לכן  $H = \langle a^s \rangle$ . □

**0.33 מסקנה.** תת-החבורות של  $\mathbb{Z}$  הן בדיוק  $(n\mathbb{Z}, +)$  עבור  $n \in \{0\} \cup \mathbb{N}$ .

**0.34 תרגיל (לבית).** תהי  $G$  חבורה. יהיו  $g_1, g_2 \in G$  איברים מסדרים סופיים  $n_1, n_2$ , בהתאמה. הוכיחו שאם  $g_1$  ו- $g_2$  מתחלפים וגם  $(n_1, n_2) = 1$ , אז  $o(g_1 g_2) = n_1 n_2$ .

**0.35 תרגיל (קשה יותר).** יהי  $g \in G$  איבר מסדר סופי  $n$ . נניח כי  $n = k_1 k_2$  כאשר  $(k_1, k_2) = 1$ . אז קיימים איברים  $h_1, h_2 \in G$  מסדרים  $o(h_1) = k_1$  ו- $o(h_2) = k_2$  המקיימים  $g = h_1 h_2 = h_2 h_1$ , והם יחידים עם התכונות האלו.

### 0.3 חבורות אוילר

**0.36 הגדרה.** המונואיד הכפלי  $(\mathbb{Z}_n, \cdot)$  הוא לא חבורה עבור  $n > 1$ . נגדיר את חבורת אוילר (או החבורה הכפלית מודולו  $n$ ) להיות

$$U_n = U(\mathbb{Z}_n, \cdot)$$

בחלק מהספרים רואים את הסימון  $\mathbb{Z}_n^\times$  או  $(\mathbb{Z}/n\mathbb{Z})^\times$ .

טענה 0.37 (איפיון איברי  $U_n$ ). יהי  $m \in \mathbb{Z}$ . אז  $[m] \in U_n$  אם ורק אם  $(n, m) = 1$ .

הוכחה. אם  $(n, m) = 1$ , אז לפי אלגוריתם אוקלידס המורחב קיימים  $s, t \in \mathbb{Z}$  כך ש- $sn + tm = 1$ . לכן  $tm \equiv 1 \pmod{n}$ . כלומר  $[t][m] \equiv [1] \pmod{n}$ . מפני שכפל מודולו  $n$  מוגדר היטב, אזי  $[t]$  הוא ההופכי של  $[m]$  במונואיד  $(\mathbb{Z}_n, \cdot)$ , אזי  $[m] \in U_n$ . בכיוון השני, נניח  $[m] \in U_n$ . אז קיים הופכי  $[b]$  ל- $[m]$ . כלומר

$$[b \cdot m] = [b] \cdot [m] \equiv [1] \pmod{n}$$

כלומר  $n \mid 1 - bm$ . לכן קיים  $k \in \mathbb{Z}$  כך ש- $1 - bm = kn$ , כלומר  $kn + bm = 1$ . הממ"מ הוא הצירוף הלינארי הטבעי המזערי, ולכן  $(n, m) = 1$ .  $\square$

**0.38 הגדרה.** פונקציית אוילר  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  המוגדרת לפי  $\varphi(n) = |U_n|$ .

**0.39 דוגמה.**  $U_8 = \{1, 3, 5, 7\}$ . אזי  $\varphi(8) = 4$ . אם  $p$  ראשוני, אז  $U_p = \{1, 2, \dots, p-1\}$  ולכן  $\varphi(p) = p-1$ .

**0.40 תרגיל.** תהי  $G$  חבורה ציקלית מסדר  $n$ . מצאו כמה יוצרים (לבדם) את  $G$ .

פתרון. נניח כי  $G = \langle a \rangle$ . כלומר  $o(a) = n$ . האיברים היחידים שיוצרים את  $G$  הם האיברים מסדר  $n$ . אז

$$G = \langle a^k \rangle \iff o(a^k) = n \iff \frac{n}{(k, n)} = n \iff (k, n) = 1$$

לכן מספר היוצרים הוא  $|U_n|$ , או במילים אחרות בדיוק  $\varphi(n)$ .

הערה 0.41. אם  $U_n$  היא ציקלית, אז מספר היוצרים שלה הוא  $\varphi(\varphi(n))$ .  
 לרוב  $U_n$  אינה ציקלית. יש איפיון מלא מתי היא כן: אם  $n \in \{1, 2, 4\}$ , או  $n = p^k$  או  $n = 2p^k$  עבור  $p > 2$  ראשוני.

הערה 0.42. יש דרך לחישוב  $\varphi(n)$  באופן קצת יותר מהיר. מתברר שלכל  $(a, b) = 1$  מתקיים  $\varphi(ab) = \varphi(a)\varphi(b)$ .  
 לפי המשפט היסודי של האריתמטיקה, כל מספר שלם ניתן לפרק למכפלה של חזקות של ראשוניים באופן יחיד (עד כדי סדר וסימן). נניח

$$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$$

עבור  $p$  ראשוני, כבר ראינו כי  $\varphi(p) = p - 1$ . עבור  $p^k$  נשים לב שבקבוצה  $\{1, 2, 3, \dots, p^k\}$  מתוך  $p^k$  האיברים בדיוק  $p^{k-1}$  אינם זרים ל- $p^k$  כי הם כפולה של  $p$ . לכן

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1) = p^k \left(1 - \frac{1}{p}\right)$$

לכן עבור מספר טבעי כלשהו  $n$  וההערה לגבי הכפוליות האריתמטית של  $\varphi$  נקבל

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}) \\ &= \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \dots \varphi(p_m^{k_m}) \\ &= p_1^{k_1} \left(1 - \frac{1}{p_1}\right) p_2^{k_2} \left(1 - \frac{1}{p_2}\right) \dots p_m^{k_m} \left(1 - \frac{1}{p_m}\right) \\ &= p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_m}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_m}\right) \end{aligned}$$

**דוגמה 0.43.** כדי לחשב את  $|U_{100}|$  מספיק לחשב  $100 = 2^2 \cdot 5^2$ , ולפי ההערה האחרונה

$$\varphi(100) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40$$

או למשל

$$\varphi(60) = 60 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 16$$

טענה 0.44. יהיו  $p, q$  ראשוניים שונים, ונסמן  $n = pq$ . אז חישוב  $\varphi(n)$  קשה כמו פירוק  $n$  לגורמים ראשוניים.

2619995643649944960380551432982458751688046862741691431671487783  
 = 100000000000000000000000000000000057 · 2619995643649944960380551432833119