

### הגדרה

סדר של איבר:

$$o(a) = \min \left\{ n \mid \begin{array}{l} n > 0 \\ a^n = 1 \end{array} \right\}$$

### למה

תהי  $G$  חבורה,  $a \in G$ . אזי:

$$o(a) \mid m \Leftrightarrow a^m = 1$$

### משפט

כל חבורה ציקלית איזומורפית ל- $\mathbb{Z}$  או  $\mathbb{Z}_n$  עבור  $n \geq 1$ .

### הגדרה

עבור חבורה  $G$ ,  $\emptyset \neq H \subseteq G$  נקראת **תת חבורה** אם  $H$  חבורה ביחס לפעולה המושרית מ- $G$  (תת חבורה אם ורק אם  $H$  סגורה לכפל ולהופכי).

### דוגמא

$G = (\mathbb{Z}_6, +)$ . תת החבורות הן:

$$\{0\} = \langle 0 \rangle, \{0, 2, 4\} = \langle 2 \rangle = \langle 4 \rangle, \{0, 3\} = \langle 3 \rangle$$

$$\{0, 1\} \not\subseteq G$$

### דוגמא נוספת

$$GL_n(F) = \{A \in M_n(\mathbb{F}) \mid \det(A) \neq 0\} = U(M_n(F), \cdot)$$

תתי חבורות:

$$\{I\} \leq \left\{ \begin{array}{l} \text{מטריצות} \\ \text{אלכסוניות} \end{array} \right\} \leq \left\{ \begin{array}{l} \text{מטריצות} \\ \text{משולשות} \\ \text{עליונות} \end{array} \right\} \leq GL_n(\mathbb{F})$$

$$\leq \left\{ \begin{array}{l} \text{משולשות} \\ \text{עליונות} \\ \text{אלכסון עם} \\ \text{אחד} \end{array} \right\}$$

### הערה

$G$  חבורה,  $\emptyset \neq H \subseteq G$  סופית, סגורה לכפל אז  $H$  תת חבורה.

### הוכחה

ניקח  $a \in H$  מכיוון שכל החזקות  $a^i \in H$ ,  $o(a) < \infty$  ו-  $1 = a^{o(a)} \in H$ . לפי ההנחה  $H$  מונויד, עם צמצום (נורש מ-  $G$ ). לפי המשפט מהרצאה (1),  $H$  חבורה.

### משימה

למצוא את כל תת החבורות של חבורה ציקלית נתונה  $\mathbb{Z}_n$

### תזכורת

$G$  חבורה,  $S \subseteq G$  קבוצה.

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H$$

תיאור נוסף:

$$\langle S \rangle = \left\{ \begin{array}{l} \text{מכפלות של איברי } S \\ \text{וההפכים שלהם} \end{array} \right\}$$

### טענה

תהי  $G$  חבורה. יהי  $g \in G$ . אז לכל  $m, m'$  מתקיים:

$$\langle g^m, g^{m'} \rangle \subseteq \langle g^{(m, m')} \rangle$$

### הוכחה

נסמן  $d := (m, m')$

קיימים סקלרים  $\alpha, \alpha' \in \mathbb{Z}$  כך ש-  $d = \alpha m + \alpha' m'$ .

- $\subseteq$  מספיק להוכיח  $g^m, g^{m'} \in \langle g^d \rangle$ , אבל  $g^m = (g^\alpha)^\alpha$
- $\supseteq$   $g^d = (g^m)^\alpha \cdot (g^{m'})^{\alpha'}$  וכנ"ל.

### טענה

כל תת חבורה של  $\mathbb{Z}_n$  היא ציקלית.

### הוכחה

תהי  $H \leq \mathbb{Z}_n$

נבחר קבוצת יוצרים סופית של  $H$ . סיימנו לפי הטענה הקודמת באינדוקציה עם מספר היוצרים.

### טענה

הסדר של  $m$  בחבורה  $\mathbb{Z}_n$  הוא:  $\frac{n}{(n,m)}$ .

### הוכחה

$$\frac{n}{(n,m)} \cdot m = n \cdot \frac{m}{(n,m)} \equiv 0 \pmod{n}$$

מצד שני, אם  $k \cdot m \equiv 0$  אז  $k \cdot \frac{m}{(n,m)} \leftarrow n \mid km$  אבל  $\frac{n}{(n,m)} \mid k \cdot \frac{m}{(n,m)}$  אבל  $\left(\frac{n}{(n,m)}, \frac{m}{(n,m)}\right) = 1$ .

לכן, לפי הלמה היסודית:  $\frac{n}{(n,m)} \mid k$ .

כלומר:

$$o(m) = \frac{n}{(n,m)}$$

### משפט

תת החבורות של  $\mathbb{Z}_n$  הן החבורות  $\langle d \rangle$  כאשר  $d \mid n$ . לפי הטענה האחרונה,  $|\langle d \rangle| = \frac{n}{d}$ .

### הוכחה

תהי  $H \leq G = \mathbb{Z}_n$ . הוכחנו ש- $H$  ציקלית, כלומר  $H = \langle m \rangle$  כאשר  $m \in \mathbb{Z}$ . אבל:

$$\langle m \rangle = \langle m, n \rangle = \langle (m, n) \rangle$$

### דוגמא

עבור  $\mathbb{Z}_{40}$ :

$$\langle 15 \rangle = \langle 15, 40 \rangle = \langle 5 \rangle$$

### סיכום

לחבורה ציקלית מסדר  $n$  יש תת חבורה יחידה מכל סדר המחלק את  $n$ .

### הערה

את מספר המחלקים של  $n$  מסמנים ב- $\sigma_0(n)$ .

### הגדרה

נתונה חבורה  $G$  עם תת חבורה  $H$ .

קבוצה מהצורה:  $Ha = \{xa \mid x \in H\}$  נקראת קוסט שמאלי של  $H$ .

### הערה

$$|Ha| = |H|$$

### הוכחה

נבנה  $f: H \rightarrow Ha$  על ידי  $f(x) = xa$ . זה איזומופיזם של קבוצות.

### הגדרה

נסמן ב-  $[G: H]$  את מספר הקוסטים של  $H$  ב-  $G$ .

### טענה

קוסטים הם זרים או שווים.

### הוכחה

נוכיח שאם  $b \in Ha$  אז  $Hb = Ha$ . אכן, אם  $b = xa$ ,  $x \in H$ ,

לכל  $h \in H$ ,  $h \cdot b = h \cdot xa = (hx) \in Ha$ ,  $h \cdot a = (hx^{-1})(xa) = (hx^{-1})b \in Hb$

$$h \cdot a = (hx^{-1})(xa) = (hx^{-1})b \in Hb$$

כעת, נניח  $c \in Ha \cap Hb$  אז  $Ha = Hc = Hb$ .

### משפט

משפט לגרנז':

$$|G| = [G: H] \cdot |H| \text{ אזי } H \leq G$$

### הוכחה

נסמן ב-  $H_1, \dots, H_m$  את הקוסטים השונים של  $H$  ב-  $G$ .

לכל  $a \in G$ ,  $a \in Ha$ , נמצא ברשימה, ולכן:

$$\bigcup H_i = G$$

□

### מסקנה

לכל  $H \leq G$ ,  $|H| \mid |G|$ .

### מסקנה

לכל  $g \in G$ :  $o(g) = |\langle g \rangle| \mid |G|$

### מסקנה

$$g^{|G|} = 1, g \in G \text{ לכל}$$

### מסקנה

משפט פרמה:

יהי  $p$  ראשוני. לכל  $a$  כך  $p \nmid a$ ,

$$a^{p-1} \equiv 1 \pmod{p}$$

### הוכחה

נתבונן בחבורת אוילר  $U_p = U(\mathbb{Z}_p, \cdot) = \{1 \leq a \leq p-1\}$

$$|U_p| = p-1 \Rightarrow \forall a: a^{p-1} \equiv 1 \pmod{p}$$

### משפט

משפט אוילר:

נסמן:  $\phi(n) = |U_n|$ .

לכל  $a$  זר ל- $n$ ,  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

### הוכחה

כניל עבור  $G = U_n$ .

### דוגמא

$$U_8 = \{1, 3, 5, 7\}$$

$$3^4 = 81 \equiv 1$$

$$5^4 = 625 \equiv 1$$

$$7^4 = 2401 \equiv 1$$