

שיעורי בית 4

24 בדצמבר 2015

1. כמה כמה יוצרים יש ל $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$ (עם פעולת מדולו 6 או כפי שלמדנו עם פעולה $[a] + [b] = [a + b]$)?
פתרון: ברור כי $[1]$ יוצר. לפי 3 גם $[5] = [-1]$ יוצר. בנוסף כל השאר אינם יוצרים כי $[0] = [4] = [3] = 2 * [3] = 3 * [2] = 3 * [2] = 0$ ולכן הסדרים שלהם קטנים מ-6. כמובן ש $[0]$ אינו יוצר כי הסדר שלו הוא 1.
2. יהיו G_1, G_2 חבורות הוכח/הפרך:

- (א) אם $G_1 \times G_2$ ציקלית אז גם G_2 וגם G_1 ציקלית.
פתרון: נניח (g_1, g_2) יוצר. אזי - טענה: g_i יוצר של G_i . נוכיח עבור g_1 :
יהא $a \in G_1$ אזי קיים n כך ש $(a, e) = (g_1, g_2)^n = (g_1^n, g_2^n) = (g_1^n, a)$ אזי $g_1^n = a$.
- (ב) אם G_1 וגם G_2 ציקליות אז $G_1 \times G_2$ ציקלית.
פתרון: לא נכון. $\mathbb{Z}_n \times \mathbb{Z}_n$ ציקלית (1 יוצר) אבל ראינו כי $\mathbb{Z}_n \times \mathbb{Z}_n$ אינה ציקלית

3. תהא G חבורה סופית. יהיו $a, b \in G$. הוכח/הפרך

- (א) אם a, b מתחלפים אז $o(ab) = o(a) \cdot o(b)$
פתרון: לא נכון. ניקח $a = b = 2 \in \mathbb{Z}_4$ אזי $o(ab) = o(0) = 1$ אבל $o(a)o(b) = 2 \cdot 2$
- (ב) $\langle a \rangle = \langle a^3 \rangle$
פתרון: לא נכון. ניקח $a = 1 \in \mathbb{Z}_3$ אזי $o(3a) = o(0) = 1$ אבל $o(1) = 3$
- (ג) אם $b = a^4$ אזי $\langle ab \rangle \subseteq \langle a \rangle$
פתרון: נכון. יהא $\langle ab \rangle = \langle a^4 \rangle$ אזי $x = (a^4)^n = a^{4n}$ עבור n שלם כלשהו. אזי בפרט x הוא חזקה של a ולכן שייך ל $\langle a \rangle$
- (ד) $\langle a \rangle = \langle a^{-1} \rangle$
פתרון: נכון. נראה הכלה בכיוון אחד (הכיוון השני דומה). יהא $x \in \langle a \rangle$ אזי $x = a^n$ עבור n שלם כלשהו. אזי $x = (a^{-1})^{-n}$ ולכן הוא חזקה של a^{-1} ובפרט שייך לחבורה הנוצרת על ידו.

4. הוכח כי החבורות הבאות אינן ציקליות

(א) $\mathbb{Z} \times \mathbb{Z}$

פתרון: נניח כשהיא ציקלית אזי קיים $\langle (a, b) \rangle \in \mathbb{Z} \times \mathbb{Z}$ כך ש $\langle (a, b) \rangle = \mathbb{Z} \times \mathbb{Z}$ אזי קיים n שלם כך ש $(na, nb) = n(a, b) = (1, 0)$ ולכן $n = a = \pm 1$ ומנימוק דומה $b = \pm 1$ ולכן לכל n שלם מתקיים

$$n(a, b) = (\pm n, \pm n) \neq (2, 3)$$

(ב) \mathbb{Q}

פתרון: נניח שציקלית. אזי $\mathbb{Q} = \langle \frac{a}{b} \rangle$ עבור a, b שלמים. יהא p ראשוני שאינו מחלק את b אזי $\frac{1}{p} \notin \langle \frac{a}{b} \rangle$. הוכחה: אחרת קיים n כך ש $\frac{1}{p} = n \frac{a}{b} = \frac{na}{b}$ ולכן $b = nap$ ומכאן p מחלק את b . סתירה.

5. תהא G חבורה. $g \in G$. נניח כי $g^k = e$. הוכח כי

$$o(g) | k$$

כלומר הסדר של g מחלק את k .

הדרכה: בצע חילוק עם שארית של k ב $o(g)$

פתרון: נסמן $o(g) = a$ אזי לפי חילוק עם שארית קיימים q, r כך ש $k = qa + r$ ו $0 \leq r < a$ אזי

$$e = g^k = g^{qa+r} = (g^a)^q \cdot g^r = e^q \cdot g^r = g^r$$

כיון ש a הוא הסדר של g ו $r < a$ נקבל כי $r = 0$. לכן $k = qa$

6. תהא G חבורה חילופית. יהיו $a, b \in G$ בעלי סדרים זרים. כלומר, נסמן $o(a) = m$ ו $o(b) = n$, אזי $\gcd(n, m) = 1$ (ל n, m אין מחלק משותף פרט ל-1). הוכח כי

$$o(ab) = m \cdot n$$

היעזר בתרגיל מספר 5

פתרון: מצד אחד $e^m e^n = e$ $(ab)^{mn} = a^{mn} b^{mn} = (a^n)^m (b^m)^n = e^m e^n = e$. כעת אם $e = (a^k b^k)^n = a^{kn} b^{kn}$. נעלה את שני האגפים בחזקת n ונקבל $e = (a^k b^k)^n = a^{kn} b^{kn}$. לפי תרגיל 5 $km | kn$ ו $km | kn$ אזי $m | k$ ו $n | k$ באופן דומה נקבל כי $m | k$. שוב, כיוון שאלו מספר זרים נקבל כי $mn | k$ ובפרט $mn \leq k$