

תרגיל 2 - מונויד

הערה

אם לאיבר במונויד קיים הפכי משמאל b והפכי מימין c אזי $b = c$.

תזכורת

1. חבורה למחצה זו חבורה שסגורה לאיזושהי פעולה בינארית אסוציאטיבית.

2. מונויד זו חבורה למחצה עם איבר יחידה.

דוגמה למונויד: $(\mathbb{Z} \setminus \{0\}, \cdot)$

פתרון ("הוכחה") להערה

e איבר היחידה

$$ba = e$$

$$ac = e$$

$$b = be = b(ac) = (ba)c = ec = c$$

מסקנה

אם a הפיך אזי קיים הופכי יחיד a .

תרגיל

יהיו איברים a, b הפיכים. הוכח כי ab הפיך.

פתרון

$$abb^{-1}a^{-1} = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

$$b^{-1}a^{-1}ab = b^{-1}eb = b^{-1}b = e$$

הגדרה

תהי חבורה (G, \otimes) . נגדיר חזקה n של איבר $x \in G$ להיות $x^n = \underbrace{x \otimes x \otimes x \otimes \dots \otimes x}_{n \text{ times}}$

$$x^0 = e$$

הערה

$$\begin{aligned}x^{m+n} &= x^m \otimes x^n \\(x^m)^n &= x^{mn} \\x^{-n} &= (x^{-1})^n \text{ (בחבורה ולא במונויד)}\end{aligned}$$

כתיב חיבורי וכתיב כפלי

הערה: בחבורה שבה הפעולה היא פעולת חיבור זה פחות נוח לרשום x^n , אז משתמשים בסימון $n \cdot x$.

כתיב חיבורי	כתיב כפלי	
$a \cdot b$	$a \cdot b$	פעולה
0	1 או e	יחידה
$-a$	a^{-1}	הפכי
$n \cdot a$	a^n	חזקה
$a - b$	$a \cdot b^{-1}$	כפל בהפכי

הגדרה

נאמר כי שני איברים a, b מתחלפים אם $a \cdot b = b \cdot a$.

טענה

G היא חבורה אבלית אם כל שני איברים בה מתחלפים.

תרגיל

$(G, *)$ חבורה. הוכח כי אם לכל $x \in G$, $x^2 = e$ אזי G אבלית.

הוכחה

$$x, y \in G \Rightarrow x * y \in G$$

$$(x * y)^2 = (x * y) (x * y) = e$$

$$xyxy = e$$

$$yxy = x$$

$$xy = yx$$

תרגיל

$(G, *)$ חבורה. הוכח שלמשוואה $axx = b$ יש פתרון אם ורק אם ab הוא ריבוע(כלומר קיים $t \in G$ כך ש $t^2 = ab$).

פתרון

(\Leftarrow) נתון שיש פתרון $cac = b$. נכפיל את שני הצדדים ב a משמאל: $acac = ab$
 $t = ac$

(\Rightarrow) נתון $ab = t^2$. נבדוק $c = a^{-1}t$: $cac = a^{-1}taa^{-1}t = a^{-1}t^2 = a^{-1}ab = b$
 $axx = b \Leftarrow$

הגדרה

מונויד M הוא בעל צמצום משמאל אם $\forall a,b,c \in M ab = ac \Rightarrow b = c$. (באופן דומה מגדירים צמצום מימין)

דוגמה למונויד עם צמצום

$$(\mathbb{Z} \setminus \{0\}, \cdot)$$

$$5a = 5b \Rightarrow a = b$$

דוגמה למונויד בלי צמצום

$$(\mathbb{R}, \cdot)$$

$$0 \cdot 5 = 0 \cdot 3$$

$$5 \neq 3$$

טענה

מונויד סופי עם צמצום משמאל הוא חבורה.

הוכחה

צ"ל כי לכל איבר קיים איבר הפכי. עבור $a \in M$ נגדיר $l_a(x) = ax$. הפונקציה הזאת היא חח"ע: $l_a(x) = l_a(y) \Leftrightarrow ax = ay \Leftrightarrow x = y$. מכיוון ש l_a חח"ע מ M ל M אזי l_a היא על, ולכן קיים b כך ש $l_a(b) = e$. זה אומר כי כל איבר ב M הוא הפיך מימין ולפי תרגיל בית זה אומר ש M חבורה.

תרגיל

1. אם A חבורה למחצה סופית אזי קיים $a \in A$ כך ש $a^2 = a$.

2. הראו שזה לאו דווקא נכון אם A אינסופית.

3. אם A חבורה אזי $a^2 = a \Rightarrow a = e$.

פתרון

1. נביט בסדרת החזקות a, a^2, a^3, \dots . סדרת החזקות אינה יכולה לתת אינסוף ערכים שונים ולכן קיימים $j \neq k$ כך ש $a^j = a^k$. אם $j = 2k$ אז גמרנו - $a^k a^k = a^k$. אם $j > 2k$ אזי

$$j = d + 2k$$

$$a^{d+2k} = a^k$$

$$a^d a^{d+2k} = a^d a^k$$

$$(a^{d+k})^2 = a^{2d+2k} = a^{d+k}$$

נראה כי אפשר להניח כי $j > 2k$: לכל $t \geq 0$ מתקיים

$$a^{j+t(j-k)} = a^j a^{t(j-k)} = a^k a^{(j-k)} a^{(t-1)(j-k)} = a^j a^{(t-1)(j-1)} = a^j a^{(t-1)(j-k)} = a^{j+(t-1)(j-k)}$$

באינדוקציה אפשר להראות כך ש $a^{j+t(j-k)} = a^j$. לכן לכל t ניתן להחליף את j ב $j + t(j - k)$ ולכן ניתן להניח ש $j > 2k$.

2. לדוגמה: $(\mathbb{N}, +)$

טענה

קבוצת האיברים ההפיכים $U(m)$ במונויד היא חבורה.

פתרון

תרגיל בית. סגירות. $a, b \in U(M)$ צ"ל $ab \in U(M)$.

חבורת אוילר

$(\mathbb{Z}_n, \cdot, 1)$ לא חבורה, כן מונויד.
 $U(\mathbb{Z}_n) = U_n = Euler(n)$ זו כן חבורה.

דוגמאות

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

נבדוק אילו איברים הם הפיכים:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$$U_6 = \{1, 5\}$$

טענה

$a \in \mathbb{Z}_n$ הפיך (כפלית) אם ורק אם $\gcd(a, n) = 1$

הוכחה

$$\gcd(a, b) = 1 \Leftrightarrow \exists_{u,v} av + nu = 1$$

\Downarrow

$$\exists_v av = 1 \pmod{4}$$

$a \in \mathbb{Z}_n$ הפיך \Leftrightarrow

מסקנה

$$U_n = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$$

דוגמאות

$$U_{14} = \{1, 3, 5, 9, 11, 13\}$$

הגדרה

פונקציית אוילר

$$\varphi(n) = |U_n|$$

$$\varphi(6) = 2, \varphi(14) = 6, \varphi(p) = p - 1 \quad \text{לדוגמה:}$$

נוסחה

$$\varphi\left(\prod p_k^{d_k}\right) = \prod (p_k - 1) p_k^{d_k - 1}$$