©צוות קורס "תורת המספרים האלגוריתמית" סמסטר א תש"פ: בר אלון, מיכאל פרי, שמואל שמעוני, איברהים שאהין, דורון מור, חיה קלר, אלעד אייגנר-חורב. נכתב ע"י דורון מור

חבורות

הגדרה 1 (חבורה): חבורה היא זוג $(G,*)$ של קבוצה G ופעולה בינארית $*$ המקבלת זוג איברים ומחזירה איבר יחיד $G * G \to G$, המקיימת:

א. סגירות (G סגורה תחת $*$, כלומר, $\forall a,b \in G: a * b \in G$)

ב. $*$ אסוציאטיבית: לכל $a,b,c \in G$ מתקיים $(a * b) * c = a * (b * c)$.

ג. קיים איבר ניטרלי e: $e \in G$ כך שלכל $a \in G$ מתקיים $ea = ae = a$.

ד. קיום הופכי: לכל $a \in G$ קיים איבר ב-G שנסמנו a^{-1}, כך ש $a * a^{-1} = a^{-1} * a = e$.

דוגמה 2: $(Z,+)$

בדיקה:

א. סגירות- לכל $a,b \in Z$ אכן $a + b \in Z$.

ב. אסוציאטיביות: לכל $a,b,c \in Z$ מתקיים $(a + b) + c = a + (b + c)$.

ג. קיום ניטרלי: $0 \in Z$ מקיים לכל $a \in Z$, $a + 0 = 0 + a = a$.

ד. קיום הופכי: $a \in Z$ ההופכי שלו בחבורה הוא $-a$, שכן $a + (-a) = (-a) + a = 0$.

שאלות:

1. האם $(N,+)$ היא חבורה? לא, כי אין ניטרלי והופכי.
2. האם $(Z,\cdot)$ היא חבורה? לא, כי אמנם יש ניטרלי אבל אין הופכי.
3. האם $(Q,\cdot)$ היא חבורה? לא, כי לאיבר 0 אין הופכי.
4. האם $(Q \setminus \{0\},\cdot)$ היא חבורה? כן (ניטרלי 1, לכל $\frac{a}{b} \in Q \setminus \{0\}$ קיים ב-$Q \setminus \{0\}$ האיבר $\frac{b}{a}$ ומתקיים $\frac{a}{b} \cdot \frac{b}{a} = 1$.
5. תנו דוגמה נוספת לחבורה.

טענה 3: לכל $n \in N$ מתקיים $(S_n,\circ)$ היא חבורה.

הוכחה:

א. סגירות: ראינו כי לכל $\sigma,\tau \in S_n$ מתקיים $\sigma \circ \tau \in S_n$. (הרכבת פונקציות חח"ע ועל היא פונקציה חח"ע ועל)

©צוות קורס "תורת המספרים האלגוריתמית" סמסטר א תש"פ: בר אלון, מיכאל פרי, שמואל שמעוני, איברהים שאהין, דורון מור, חיה קלר, אלעד אייגנר-חורב. נכתב ע"י דורון מור

ב. אסוציאטיביות: לכל $\sigma, \tau, \alpha \in S_n$ מתקיים

$$(\sigma \circ \tau) \circ \alpha = \sigma \circ (\tau \circ \alpha)$$

כי לכל $1 \leq i \leq n$

$$(\sigma \circ \tau) \circ \alpha(i) = (\sigma \circ \tau)\big(\alpha(i)\big) = \sigma\Big(\tau\big(\alpha(i)\big)\Big)$$

$$\sigma \circ (\tau \circ \alpha)(i) = \sigma\big((\tau \circ \alpha)(i)\big) = \sigma\Big(\tau\big(\alpha(i)\big)\Big)$$

ג. קיום ניטרלי: ראינו כי לכל $\sigma \in S_n$ מתקיים כי הפרמוטציה $e = 1_{S_n} \in S_n$ מקיימת $1_{S_n} \circ \sigma = \sigma \circ 1_{S_n} = \sigma$

ד. קיום הופכי: ראינו כי לכל $\sigma \in S_n$ קיימת $\sigma^{-1} \in S_n$ כך ש $\sigma \circ \sigma^{-1} = \sigma^{-1}\sigma = 1_{S_n}$.

<u>הגדרה 4</u>: נאמר כי השלמים מתחלקים למחלקות שקילות מודולו n ונסמן

$$Z_n = \{[0]_n, [1]_n \dots [n-1]_n\}$$

כעת נראה שתי דוגמות חשובות במיוחד לחבורות הקשורות לחשבון המודולורי:

1. החבורה החיבורית $(Z_n, +)$.

2. החבורה הכפלית $(Z_n^*, \cdot)$.

1. קל לראות את קיום הגדרת החבורה (איבר ניטרלי $[0]_n$, לכל $[k]_n$ ההופכי הוא $[n-k]_n$).

מדוע זה ההופכי? כי $k + (n-k) = n \equiv 0 \ (mod\ n)$.

יש לשים לב כי בחבורה חיבורית ההופכי הוא הנגדי, ולפעמים נסמנו $[-k]_n$.

<u>דיון</u>: האם $(Z_n, \cdot)$ חבורה? אמנם יש ניטרלי $[1]_n$ אך מה לגבי הופכי? לדוגמה, עבור $[2]_6$ אין אף איבר שבו נכפיל ונקבל את $[1]_n$! למדנו שלשקילות $a \cdot x \equiv 1 \ (mod\ n)$ קיים פתרון $\leftrightarrow$ $(a, m) = 1$. זוהי המוטיבציה להגדרת החבורה הכפלית $(Z_n^*, \cdot)$.

2. החבורה הכפלית $(Z_n^*, \cdot)$ כאשר $Z_n^* = \{[a]_n \in Z_n \mid (a, n) = 1\}$

לדוגמה:

$$Z_6^* = \{[1]_6, [5]_6\}$$

שכן שאר האיברים 0,2,3,4 אינם מקיימים $(a, 6) = 1$.

מיהו האיבר הניטרלי? $[1]_6$. מיהו האיבר ההופכי?

$$1 \cdot 1 = 1, \qquad 5 \cdot 5 = 25 = 24 + 1 \equiv [1]_6$$

ולכן כל איבר הוא ההופכי של עצמו.

©צוות קורס "תורת המספרים האלגוריתמית" סמסטר א תש"פ: בר אלון, מיכאל פרי, שמואל שמעוני, איברהים שאהין, דורון מור, חיה קלר, אלעד אייגנר-חורב. נכתב ע"י דורון מור

נוודא שזוהי חבורה:

א. סגירות: אם $[a],[b] \in Z_n^*$ אזי $(a,n) = (b,n) = 1$, ולכן גם $(ab,n) = 1$, ולכן $[ab]_n \in Z_n^*$.

ב. אסוציאטיביות: נובע מאסוציאטיביות של כפל מודולרי.

ג. קיום ניטרלי: $[1]_n \in Z_n^*$ איבר ניטרלי.

ד. קיום הופכי: לכל $[a] \in Z_n^*$ מתקיים $(a,n) = 1$, ולכן (כפי שלמדנו בהרצאת "הופכי מודולרי") ל-a יש איבר הופכי a' מודולו n כך ש $a \cdot a' \equiv 1 \ (mod\ n)$, ובנוסף $(a',n) = 1$, ולכן $[a']_n \in Z_n^*$, ומתקיים $[a][a']_n = [1]_n = [a'][a]_n$.

<u>תרגיל 5</u>: נגדיר $*: NXN \to N$ ע"י $n * m = n^m$. האם $(N,*)$ חבורה?

<u>פתרון</u>: נבדוק לפי ההגדרות.

א. סגירות: עבור $a,b \in N$, המספר $a^b \in N$.

ב. אסוציאטיביות: יהיו $2,3,2 \in N$. האם $(2 * 3) * 2 =^? 2 * (3 * 2)$

$$(2^3)^2 = 8^2 = 64, \quad 2^{(3^2)} = 2^9 = 512$$

מצאנו דוגמה נגדית ולכן $(N,*)$ אינה מקיימת אסוציאטיביות. לכן $(N,*)$ לא חבורה.