

תרגול 2 - מבנים אלגבריים תשע"ג

יובל חצ'טריאן וחיים שרגא רוזנר

28 בנובמבר 2012

1 חבורות למחצה

נתחיל בדוגמא ראשונה למבנה אלגברי.

הגדרה 1.1 חבורה למחצה היא קבוצה $A \neq \emptyset$ יחד עם פעולה בינארית $*$ המקיימת:

1. $A \times A \rightarrow A : *$ כמעט תמיד במקום לרשום (a, b) , $*$ אנו נרשום $a * b$.

2. אסוציאטיביות: $a * (b * c) = (a * b) * c$.

דוגמאות:

1. כל המספרים הזוגיים יחד עם פעולת כפל מהווים חבורה למחצה.

2. תהי A קבוצה לא ריקה כלשהי. לכל $a, b \in A$ נגדיר $a * b = b$.

3. תהי G קבוצה. אנו נסמן ב- G^G את אוסף כל הפונקציות מ- G אל עצמה. אזי יחד עם פעולת ההרכבת פונקציות, (\circ) , (G^G, \circ) , זו חבורה למחצה. זאת דוגמא חשובה וכדאי ליזכור אותה.

4. $(\mathbb{Z}, -)$ אינה חבורה למחצה, מפני שפעולת $(-)$ אינה אסוציאטיבית.

5. (\mathbb{Q}, \div) אינו חברה למחצה, מפני שהחילוק אונו פעולה אסוציאטיבית.

תרגיל קבע האם \mathbb{R} יחד עם הפעולה $*$ המוגדרת על ידי $a * b := \frac{1}{2}(a^2 + b^2)$ היא חבורה למחצה.

פתרון לא, ניקח $a = 1, b = 2, c = 3$ על מנת לקבל דוגמא נגדית. ■

תרגיל נניח שבחבורה למחצה A אפשר לקרוא את הגורמים מהמכפלה, כלמר מתקיים: $ab = cd \implies a = c \wedge b = d$. הוכח: $|A| = 1$.

פתרון אנו צריכים להראות למעשה שלכל $a, b \in A$, $a = b$. (זאת אומרת, בקוצה לא קיימים שני איברים שונים זה מזה, על כן, יש בה איבר יחיד). מאסוציאטיביות, נובע $(ab)(ab) = a(b(ab)) = ((ab)a)b$. מהנתון, (מתכונת הצמצום) מתקיים ■ $ab = a, ab = b \implies a = b$

2 איבר יחידה

הגדרה 2.1 איבר e בחבורה למחצה G נקרא איבר יחידה אם לכל $g \in G$, מתקיים $g = ge = eg$.

תרגיל: הוכח, אם G קיים איבר יחידה אזי הוא יחיד

פתרון: נניח ש $e, f \in G$ הם איברי יחידה. אזי מתקיים $e = fe = f$. ■

תרגיל: הראה ש $M := \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$, יחד עם כפל מטריצות רגיל, היא חבורה למחצה. האם יש לה איבר יחידה?

פתרון: $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}$. כלמר יש סגירות ביחס לכפל. אסוציאטיביות

נובעת מאסוציאטיביות של כפל מטריצות (הוכחתם כבר בקורס בלינארית שכפל מטריצות אסוציאטיבי). נראה שלא קיים איבר יחידה. מהכפל של מטריצות נובע

ש אם $\begin{pmatrix} e & f \\ 0 & 0 \end{pmatrix}$ הינו איבר יחידה, אזי $e = 1$. מצד שני $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} e & f \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & f \\ 0 & 0 \end{pmatrix}$

לכן $f = 1$. לכן $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ מוכרח להיות איבר יחידה (אם קיים כזה).

אבל $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, ולכן $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ אינו

איבר יחידה. לכן לא קיים איבר יחידה. ■

הערה 2.2 לכל איבר במקום לרשום $\underbrace{aa \dots a}_{n \text{ times}}$ או נרשום a^n

3 מונואידים

הגדרה 3.1 חבורה למחצה M בעלת איבר יחידה e נקראת מונואיד.

דוגמא: תהי A קבוצה. אזי $A^A := \{f : A \mapsto A\}$, יחד עם הרכבת פונקציות (\circ) היא מונואיד, ואיבר יחידה הוא פונקציית הזהות המוגדרת על ידי $\forall a \in A : f(a) = a$.

דוגמא: אוסף כל המספרים הטבעיים יחד עם פעולת הכפל הינה מונואיד.

דוגמא: אוסף $M_n(\mathbb{F})$ של מטריצות מעל שדה \mathbb{F} יחד עם פעולה כפל מטריצות הינו מונואיד.

דוגמא: אוסף פונ' רציפות $\mathbb{R} \rightarrow [0, 1]$ הינה מונואיד, יחד עם פעולת כפל הרגיל $(f * g)(t) = f(t)g(t)$.

4 איברים הפיכים

הגדרה 4.1 יהי M מונואיד עם איבר יחידה 1. איבר $a \in M$ נקרא הפיך משמאל אם קיים $b \in M$ כך ש $ba = 1$. במקרה הזה, b יקרה הופכי שמאלי של a .

איבר $a \in M$ נקרא הפיך מימין אם קיים $b \in M$ כך ש $ab = 1$. במקרה הזה b יקרה הופכי ימני של a .

איבר $a \in M$ נקרא הפיך, אם הוא הפיך מימין וגם משמאל.

תרגיל: תן דוגמא למונואיד בעל איבר הפיך משמאל שאינו הפיך.

פתרון: נתבונן ב $M = (\mathbb{N}^{\mathbb{N}}, \circ)$. ניקח $f := n \mapsto 2n$. הפונ' חח"ע לכן הפיכה מימין. למשל, כך $g := n \mapsto \lfloor \frac{n}{2} \rfloor$. אזי $g \circ f = id$, כאשר id היא פונ' הזהות.

תרגיל: יהי M מונואיד עם 1 איבר יחידה. יהי $a \in M$ הפיך, b ו c כך ש $ab = ca = 1$. הוכח: $b = c$.

פתרון: $c = c \cdot 1 = c(ab) = (ca)b = 1 \cdot b = b$ (להצדיק כל מעבר!) ■

מהתרגיל נובע, שעבור איבר הפיך, הפכי ימני והשמאלי שווים. לכן אנו יכולים לדבר פשוט על הופכי. אנו נארמ ש b הוא ההופכי של a ונסמן $a^{-1} = b$.

טענה 4.2 יהי M מונואיד יחד עם איבר יחידה 1, ונניח $a \in M$ הפיך, אזו ההופכי שלו יחיד.

הוכחה: אם לא הוכח בהרצאה - ייתן כתרגיל בית קל. ■

תרגיל: אם במונואיד M קיימים a, b כך שמתקיים $aba = a$ ו $ab^2a = 1$, אזי $a = b^{-1}$.

פתרון: $ab = ab \cdot 1 = ab(ab^2a) = (ab^2a)ba = ab^2(aba) = ab^2a = 1$.
■ $(ab)(ab^2a) = (aba)b^2a = ab^2a = 1$

5 חבורות

הגדרה 5.1 מונואיד G שבו כל איבר הפיך נקרא חבורה.

הערה 5.2 על מנת להראות שהאובייקט (קבוצה G ופעולה $*$) שקיבלנו הוא חבורה, עלינו להראות שקיימות 4 האקסיומות: סגירות (הפעולה $G \times G \rightarrow G : *$ היא פונקציה), אסוציאטיביות $(a * b) * c = a * (b * c)$, קיים איבר יחידה $1_G \in G$, ולכל איבר קיים הפיך.

הגדרה 5.3 תהי (G, \cdot) חבורה. אם לכל $a, b \in G$ מתקיים $ab = ba$, אנו נאמר שהכפל הוא קומוטטיבי, ו G אבלי.

נביא כמה דוגמאות של חבורות.

דוגמא: קבוצה בעלת איבר יחיד היא חבורה. חבורה זו תקרא החבורה הטריוויאלית.

דוגמא: קבוצת המספרים השלמים \mathbb{Z} , יחד עם פעולת (+) היא חבורה אבלי. (לבדוק שהקסיומות מתקיימות).

דוגמא: מרחב וקטורי V יחד עם פעולת חיבור הרגילה הוא חבורה אבלי.

דוגמא: יהי \mathbb{F} שדה. אם נתעלם מהכפל, $(\mathbb{F}, +)$ הוא חבורה אבלי.

דוגמא: תהי G קבוצה כלשהי. תהי S קבוצת כל הפונקציות ההפיכות (כלמר חח"ע ועל) מ G אל עצמה יחד עם פעולת ההרכבה. אזי S היא חבורה. אם $G = \{1, \dots, n\}$ היא קבוצה סופית, הסימון המקובל הוא S_n . למעת מקרי קצה חבורה זו לא תהיה אבלי.

דוגמא: יהי \mathbb{F} שדה, $n \in \mathbb{N}$. נסמן ב $GL_n(\mathbb{F})$ אוסף כל המטריצות ההפיכות מגודל $n \times n$, יחד עם פעולת כפל מטריצות. אזי, $GL_n(\mathbb{F})$ חבורה. (בד"כ לא אבלית).

דוגמא: המספרים הטבעיים $(\mathbb{N}, +)$ אינו חבורה למחצה, מפני שפרט ל 0 אין איברים הפיכים. (מי הוא ההפיך של 0)?

דוגמא: יהי \mathbb{F} שדה כלשהו. אזי, (\mathbb{F}, \cdot) אינו חבורה, מפני ש 0 אינו הפיך.

הגדרה 5.4 אנו נאמר שמונואיד M יש תכונת צמצום משמאל אם $b = c \Leftarrow ab = ac$.

משפט 5.5 מונואיד סופי M בעל צמצום משמאל הוא חבורה.

הוכחה: אנו רוצים להוכיח שלכל איבר ב M קיים איבר הפיך. יהי $a \in M$. נתבונן בקבוצה של כל החזקות של a , דהיינו

$\{g : \exists n \in \mathbb{N} : g = a^n\}$. קבוצה הזו סופית מכיוון שהיא תת קבוצה של מונואיד סופי M . לכן קיים $n \in \mathbb{N}$ מינימלי כך שקיים $m < n$ כך ש $a^m = a^n$. מתקיים: $a^{n-m}a^m = a^m$. מתכונת צמצום משמאל - $a^m = 1_M$. מתקיים:

$a^{m-1}a = aa^{m-1} = 1_M$. כלומר - $a^{m-1} = a^{-1}$ על פי ההגדרה של הופכי. ■

הגדרה 5.6 תהי G חבורה. העוצמה של G נקראת סדר של חבורה.

תרגיל: מהו סדר של S_n ?

פתרון: יש לנו $n!$ תמורות על $\{1, \dots, n\}$ וזהו הסדר של S_n .

6 דוגמאות נוספות

6.1 חבורות ציקליות

הגדרה 6.1 חבורה G נקראת ציקלית אם היא נוצרת על ידי איבר יחיד, כלומר: קיים $a \in G$ כך שלכל $g \in G$, קיים $n \in \mathbb{Z}$ כך ש $g = a^n$. במקרה זה a נקרא איבר יוצר.

הערה 6.2 חוץ מ- \mathbb{Z}_2 , בכל חבורה ציקלית אחרת היוצר איננו יחיד. אם g יוצר, אז גם g^{-1} יוצר.

דוגמא: \mathbb{Z} היא חבורה ציקלית והיוצר שלה הוא 1.

תזכורת: $n \mid a - b \Leftrightarrow a \equiv b \pmod{n}$. בנוסף, אם $a \equiv a' \pmod{n}$ ו $b \equiv b' \pmod{n}$, אזי $a + b \equiv a' + b' \pmod{n}$. זה מאפשר לנו חבורה חדשה.

הגדרה 6.3 $(\mathbb{Z}_n, +)$ היא חבורה אשר האיברים בה הן מחלקות שקילות המושרות מיחס מודולו n , וחיבור מוגדר להיות $[a + b] = [a] + [b]$. כלומר בוחרים נציג של $[a]$, נציג של $[b]$ ומסתכלים על מחלקת שקילות $[a + b]$. כפי שצויין התוצאה אינה תלויה בבחירת הנציגים לכן הפעולה מודרת היטב.

תרגיל: האם $(\mathbb{Z}_n, +)$ חבורה? אם כן - אבלית או לא? מה הסדר שלה? האם ציקלית?

פתרון: נענה בכמה שלבים:

1. נבדוק שכל האקסיומות מתקיימות

- (א) סגירות: ישנה סגירות מעצם ההגדרה של הפעולה.
 (ב) אסוציאטיביות: $([a] + [b]) + [c] = [a + b] + [c] = [a + b + c] = [a] + [b + c]$
 $[b + c] = [a] + ([b] + [c])$
 (ג) איבר יחידה: $[0]$ הינו איבר יחידה. לכל $m \in \mathbb{N}$ מתקיים $[m] + [0] = [m]$
 $[0] + [m] = [m + 0] = [m]$
 (ד) איבר הופכי: יהא $m \in \mathbb{N}$. יהי d שארית חילוק של m ב n . אזי $[m] = [d]$ מתקיים $[n - d] + [d] = [n] = [0]$. לכן לכל איבר יש הופכי.
2. נראה $(\mathbb{Z}_n, +)$ הינה חבורה אבלית. $[a] + [b] = [a + b] = [b + a] = [b] + [a]$.
3. הסדר של \mathbb{Z}_n הינו n . לכל $m \in \mathbb{Z}$ קיים $0 \leq d \leq n - 1$ כך ש $[d] = [m]$. מכיוון שיש לנו בדיוק n מספרים כאלה, מספר נציגי שקילות הינו לכל היותר n . מצד שני, לכל $0 \leq a, b \leq n - 1$, $a = b \Leftrightarrow (a - b) \equiv 0 \pmod{n}$. לכן לכל $0 \leq a \neq b \leq n - 1$, $[a] \neq [b]$. לכן קיימות לנו לפחות n מחלקות שקילות. לכן, מספר מחלקות שקילות הוא n .
4. נראה כי \mathbb{Z}_n ציקלית. יהי $m \in \mathbb{Z}$. קיים $0 \leq d \leq n - 1$ כך ש $[d] = [m]$. מתקיים $[d] = \underbrace{[1] + \dots + [1]}_{n \text{ times}}$. מכאן, \mathbb{Z}_n נוצרת על ידי $[1]$ ולכן ציקלית.

6.2 חבורת אוילר

בדומה לחיבור על מחלקות שקילות המושרת מיחס "שקול מודולו n ", כפל $[a] \cdot [b] = [a \cdot b]$ אף הוא מוגדר היטב.

שאלה: האם (\mathbb{Z}_n, \cdot) חבורה?

תשובה: לא, כי $[0]$ אינו הפיך.

הגדרה 6.4 לכל $n \in \mathbb{N}$ נגדיר U_n להיות קבוצת האיברים ההפיכים ביחס לכפל ב \mathbb{Z}_n .

תרגיל: הראה ש U_n חבורה.

פתרון: קל לבדוק ש \mathbb{Z}_n הינו מונואיד. אנו נוכיח את הטענה הכללית יותר:

טענה 6.5 עבור מונואיד M , אוסף איברים ההפיכים שלו, $U(M)$ יחד עם הכפל של M הוא חבורה. **הוכחה:** אסוציאטיביות ואיבר יחידה נובעים מהתכונות האלה ב M . אנו נוכיח סגירות וקיום הופכי

- סגירות: יהיו $a, b \in U(M)$. נראה כי ab אף הוא הפיך. $(b^{-1}a^{-1})ab = 1_M$ לכן ab הפיך.
- קיום הופכי: אם a הפיך, אזי a^{-1} הפיך.

■

ננסה לאפיין את כל האיברים ב U_n .

טענה 6.6 יהי $m \in \mathbb{Z}$ אזי $[m] \in U_n \Leftrightarrow (m, n) = 1$.

הוכחה: \Rightarrow נניח ש $(m, n) = 1$. אזי קיימים $x, y \in \mathbb{Z}$ כך ש $xm + yn = 1$. זאת אומרת, $[x][m] = [1] \Leftrightarrow xm \equiv 1 \pmod{n} \Leftrightarrow n \mid 1 - xm$.
 \Leftarrow נניח ש $[m] \in U_n$. אזי קיים $x \in \mathbb{Z}$ כך ש $[xm] = [m][x] = 1$. אז $xm \equiv 1 \pmod{n}$. מכאן $n \mid 1 - xm$. וזה אומר: $\exists y : yn = 1 - xm$. נעביר אנף ונקבל $1 = xm + yn$. ■

6.3 חבורה הסימטרית

S_n כבר הגדרנו בתחילת השיעור. נחזור לחקור כמה מן התכונות שלה. כל תמורה $\sigma \in S_n$ ניתן לרשום כמטריצת שורות באופן הבא:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

הגדרה 6.7 יהיו $1 \leq r_1, \dots, r_t \leq n$. תמורה המעבירה $r_1 \mapsto r_2 \mapsto \dots \mapsto r_t \mapsto r_1$ נקראת מחזור, ודרך כלל מסמנים אותה על ידי (r_1, r_2, \dots, r_t) . הקבוצה $\{r_1, \dots, r_t\}$ נקראת תומך של מחזור. מחזורים נקראים זרים אם התומכים שלהם זרים.

משפט 6.8 כל תמורה ניתן להציג כמכלה של מחזורים זרים.