

תרגיל מספר 8 מבנים אלגבריים

11 בדצמבר 2017

1. יהיו R_1, R_2 שני חוגים. נגדיר את חוג המכפלה להיות הקבוצה $R_1 \times R_2$ עם חיבור וכפל רכיב כלומר

$$\forall (a, b), (x, y) \in R_1 \times R_2 : (a, b) + (x, y) = (a + x, b + y)$$

$$\forall (a, b), (x, y) \in R_1 \times R_2 : (a, b) (x, y) = (ax, by)$$

כאשר $a + x$ זהו חיבור של R_1 , $b + y$ זהו חיבור של R_2 . באופן דומה הכפלים המצוינים בשאלה מתייחסים לכפלים של R_1, R_2 לפי ההקשר. עובדה: זה אכן חוג. הוכיחו או הפריכו:

(א) אם R_1, R_2 חוגים עם חילוק אז גם $R_1 \times R_2$ **פתרון**: לא למשל $R_1 = R_2 = \mathbb{Q}$ חוג עם חילוק אבל $\mathbb{Q} \times \mathbb{Q}$ אינו חוג עם חילוק כי ל $(1, 0) \in \mathbb{Q} \times \mathbb{Q}$ אין הופכי. הוכחה, אחרת קיים (a, b) המקיים

$$(a, b) (1, 0) = (1, 1)$$

בפרט $b0 = 1$ שלא יתכן

(ב) אם R_1, R_2 חוגים עם יחידה אז גם $R_1 \times R_2$ **פתרון**: נסמן $1_{R_1}, 1_{R_2}$ ונראה כי $(1_{R_1}, 1_{R_2})$ הוא היחידה ב $R_1 \times R_2$. אכן לכל $(a, b) \in R_1 \times R_2$ מתקיים

$$(a, b) (1_{R_1}, 1_{R_2}) = (a1_{R_1}, b1_{R_2}) = (a, b)$$

וגם

$$(1_{R_1}, 1_{R_2}) (a, b) = (1_{R_1}a, 1_{R_2}b) = (a, b)$$

לפי הגדרת היחידות ב R_1 וב R_2

2. הוכיחו כי הבאים הם חוגים. קבעו האם אלו חוגים חילופיים, האם אלו חוגים עם יחידה והאם חוגים אלו עם חילוק.

(א) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ עם חיבור וכפל של מספרים ממשיים (שימו לב שהקבוצה שהגדרנו היא תת קבוצה של המספרים הממשיים \mathbb{R}) **פתרון**: נתחיל עם הטענה כי $\mathbb{Z}[\sqrt{2}]$ ביחס לחיבור היא חבורה כיוון שהיא

תת קבוצה של הממשיים זה שקול להוכיח כי היא תת חבורה שלהם. נשתמש בקריטריון הקצר:

לכל מתקיים $a + b\sqrt{2}, x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$

$$(a + b\sqrt{2}) - (x + y\sqrt{2}) = (a - x) + (b - y)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

בנוסף $0 \in \mathbb{Z}[\sqrt{2}]$.

טענה הכפל ב $\mathbb{Z}[\sqrt{2}]$ מוגדר וקיבוצי:

מוגדר: לכל $a + b\sqrt{2}, x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ מתקיים

$$(a + b\sqrt{2})(x + y\sqrt{2}) = (ax + 2by) + (ay + bx)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

קיבוציות: נובע מקיבוציות של מספרים ממשיים פילוג/חילופיות גם נובע מפילוג/חילופיות של מספרים ממשיים.

בחוג $\mathbb{Z}[\sqrt{2}]$ היחידה היא $1 \in \mathbb{Z}[\sqrt{2}]$

החוג $\mathbb{Z}[\sqrt{2}]$ אינו עם חילוק כי ל 2 אין הופכי. למה?

נניח בשלילה כי קיים $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ כך ש $2(a + b\sqrt{2}) = 1$ זה גורר כי $2a - 1 = b\sqrt{2}$ בצד ימין יש מספר שלם. ולכן גם המספר בצד משאל שלם. זה קורה אמ"מ $b = 0$. זה גורר $2a - 1 = 0$ כלומר $a = \frac{1}{2}$ סתירה לכך ש $a \in \mathbb{Z}$

(ב) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ עם חיבור וכפל של מספרים ממשיים (שימו לב

שהקבוצה שהגדרנו היא תת קבוצה של המספרים הממשיים \mathbb{R})

פתרון: פתרון דומה לסעיף הקודם של $\mathbb{Z}[\sqrt{2}]$. ההבדל הוא ש $\mathbb{Q}[\sqrt{2}]$ הינו חוג עם חילוק (ובעצם שדה).

הוכחה: יהא $(a + b\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$ $0 \neq$ צריך למצוא לו הופכי כלומר $c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ המקיים

$$(a + b\sqrt{2})(c + d\sqrt{2}) = 1$$

זה שני משוואות בשני נעלמים c, d

$$\begin{aligned} ac + 2bd &= 1 \\ (ad + bc)\sqrt{2} &= 0\sqrt{2} \end{aligned}$$

זה מתרגם למערכת המשוואות:

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

יש לה פתרון אמ"מ $\det\left(\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\right) = a^2 - 2b^2 \neq 0$ וזה אכן המצב.

הוכחה: נניח בשלילה כי $a^2 - 2b^2 = 0$ זה גורר כי $\left(\frac{a}{b}\right)^2 = 2$ או $b = 0$

אם $\left(\frac{a}{b}\right)^2 = 2$ אז $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ סתירה.

אם $b = 0$ אז $a = 0$ גם כן ואז נקבל סתירה לכך ש $0 \neq (a + b\sqrt{2})$

(ג) הקבוצה $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ עם כפל וחיבור מטריצות.

פתרון: נתחיל עם הטענה כי R ביחס לחיבור היא חבורה כיוון שהיא תת קבוצה של המטריצות זה שקול להוכיח כי היא תת חבורה שלהם. נשתמש בקריטריון הקצר:

לכל $\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} \in R$ מתקיים כי

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & 0 \end{pmatrix} \in R$$

בנוסף $0 \in R$

טענה הכפל ב R מוגדר וקיבוצי:

מוגדר: לכל $\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} \in R$ מתקיים כי

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 \\ 0 & 0 \end{pmatrix} \in R$$

קיבוציות: נובע מקיבוציות של מטריצות פילוג גם נובע מפילוג של מטריצות.

R אינו חילופי כי =

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

בחוג R אין יחידה

הוכחה: אחרת נסמן אותה ב $\begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix}$. צריך להתקיים לכל $\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}$

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}$$

אבל

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 \\ 0 & 0 \end{pmatrix}$$

ולכן

$$\begin{pmatrix} a_1 a_2 & a_1 b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}$$

שזה לא אפשרי (אם נבחר את $a_1 = 1$ זה גורר כי $b_2 = b_1$ אבל b_1 יכול להיות כמה אפשריות)

כיוון ש R ללא יחידה אז הוא אינו חוג עם חילוק.

משפט השאריות הסיני

נצטט ונדגים מקרה פרטי של משפט השאריות הסיני:
משפט: יהיו p_1, p_2, p_3 שלושה מספרים ראשוניים שונים. יהיו n_1, n_2, n_3 מספרים טבעיים.
יהיו c_1, c_2, c_3 מספרים שלמים קבועים.
אזי למערכת המשוואות

$$\begin{aligned}x &\equiv c_1 \pmod{p_1^{n_1}} \\x &\equiv c_2 \pmod{p_2^{n_2}} \\x &\equiv c_3 \pmod{p_3^{n_3}}\end{aligned}$$

קיים פתרון (יחיד עד כדי כפולות של $(p_1^{n_1} p_2^{n_2} p_3^{n_3})$)
נמחיש זאת באמצעות התרגיל הבא:
מצא x שלם המקיים

$$\begin{aligned}x &\equiv 2 \pmod{2^3} \\x &\equiv 5 \pmod{3^2} \\x &\equiv 20 \pmod{5^2}\end{aligned}$$

לפי משפט הקודם מובטח כי קיים כזאת x .

1. כיוון ש 2^3 זר ל $3^2 5^2$ (כלומר $\gcd(3^2 5^2, 2^3) = 1$) ניתן למצוא c, d שלמים כך ש

$$c \cdot 2^3 + d \cdot 3^2 5^2 = 1 = \gcd(3^2 5^2, 2^3)$$

ולכן

$$1 - c \cdot 2^3 = d \cdot 3^2 5^2$$

נסמן $e_1 = 1 - c \cdot 2^3 = d \cdot 3^2 5^2$ (השתכנעו!)

$$\begin{aligned}e_1 &= 1 \pmod{2^3} \\e_1 &= 0 \pmod{3^2 5^2}\end{aligned}$$

מצאו את e_1
פתרון: נחשב

$$3^2 5^2 = 2^3 \cdot 28 + 1$$

$$e_1 = 2^3 \cdot 28 + 1 = 225$$

(א) באותו אופן מצאו e_2 שלם המקיים

$$\begin{aligned}e_2 &= 1 \pmod{3^2} \\e_2 &= 0 \pmod{2^3 5^2}\end{aligned}$$

ו e_3 שלם המקיים

$$\begin{aligned}e_3 &= 1 \pmod{5^2} \\e_3 &= 0 \pmod{2^3 3^2}\end{aligned}$$

פתרון : נחשב

$$\begin{aligned}2^3 5^2 &= 3^2 \cdot 22 + 2 \\ 3^2 &= 2 \cdot 4 + 1\end{aligned}$$

ולכן

$$1 = 3^2 - 2 \cdot 4 = 3^2 - (2^3 5^2 - 3^2 \cdot 22) \cdot 4 = 89 \cdot 3^2 - 4 \cdot 2^3 5^2$$

$$e_2 = 1 - 89 \cdot 3^2 = -800 \quad \text{לכן נחשב}$$

$$\begin{aligned}2^3 3^2 &= 5^2 \cdot 2 + 22 \\ 5^2 &= 22 \cdot 1 + 3 \\ 22 &= 3 \cdot 7 + 1\end{aligned}$$

ולכן

$$\begin{aligned}1 &= 22 - 3 \cdot 7 = 22 - (5^2 - 22 \cdot 1) \cdot 7 = 8 \cdot 22 - 7 \cdot 5^2 \\ &= 8 \cdot (2^3 3^2 - 5^2 \cdot 2) - 7 \cdot 5^2 = -23 \cdot 5^2 + 8 \cdot 2^3 3^2\end{aligned}$$

$$e_3 = 1 + 23 \cdot 5^2 = 576 \quad \text{לכן}$$

(ב) כעת הגדירו את $x = 2e_1 + 5e_2 + 20e_3$ ובידקו כי הוא פתרון למערכת שבשאלה.
פתרון : נחשב

$$x = 2e_1 + 5e_2 + 20e_3 = 2 \cdot 225 + 5 \cdot (-800) + 20 \cdot 576 = 7970 \equiv 770 \pmod{2^3 3^2 5^2}$$

ואכן

$$\begin{aligned}770 &\equiv 2 \pmod{2^3} \\ 770 &\equiv 5 \pmod{3^2} \\ 770 &\equiv 20 \pmod{5^2}\end{aligned}$$