תרגיל מספר 8 מבנים אלגבריים

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

(ב) אם R_1, R_2 חוגים עם יחידה אז גם $R_1 \times R_2$

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

(א) $\mathbb{Z}[\sqrt{2}] = \left\{ a + b\sqrt{2} \,| a, b \in \mathbb{Z} \right\}$ עם חיבור וכפל של מספרים ממשיים (שימו לב שהקבוצה שהגדרנו היא תת קבוצה של המספרים הממשיים $\mathbb{R}$)

(ב) $\mathbb{Q}[\sqrt{2}] = \left\{ a + b\sqrt{2} \,| a, b \in \mathbb{Q} \right\}$ עם חיבור וכפל של מספרים ממשיים (שימו לב שהקבוצה שהגדרנו היא תת קבוצה של המספרים הממשיים $\mathbb{R}$)

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

3. יהא R חוג. הוכיחו את הבאים:

(א) לכל $a \in R$ מתקיים $-(-a) = a$

(ב) לכל $a, b \in R$ מתקיים $-(a+b) = -a - b$

(ג) לכל $a, b \in R$ מתקיים $a(-b) = -(ab) = (-a)b$

(ד) לכל $a, b \in R$ מתקיים $(-a)(-b) = ab$

(ה) לכל $a \in R$ מתקיים $(-a)^2 = a^2$

4. יהא R חוג חילופי עם יחידה. איבר $a \in R$ יקרא מחלק אפס אם קיים $0 \neq b \in R$ כך ש $ab = 0$.

(א) הוכיחו/הפירכו: אם $a \in R$ הפיך אז a אינו מחלק אפס.

(ב) הוכיחו/הפריכו: אם $a \in R$ אינו מחלק אפס אז a הפיך.

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

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

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

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

לפי המשפט הקודם מובטח כי אכן קיים כזה 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 (ע"י אלגוריתם אוקלידס) 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 $e_1 = 1 - c \cdot 2^3 = d \cdot 3^2 5^2$ ואז (השתכנעו!)

$$\begin{aligned} e_1 &\equiv 1 \bmod 2^3 \\ e_1 &\equiv 0 \bmod 3^2 5^2 \end{aligned}$$

(א) מצאו את e_1. (שימו לב כי $e_1 = 0 \bmod 3^2 5^2$ ולכן: $e_1 = 0 \bmod 3^2$ וגם $e_1 = 0 \bmod 5^2$)

(ב) באותו אופן מצאו e_2 שלם (שוב, ע"י העובדה $\gcd(3^2, 2^3 5^2) = 1$ + אלגוריתם אוקלידס) המקיים

$$\begin{aligned} e_2 &\equiv 1 \bmod 3^2 \\ e_2 &\equiv 0 \bmod 2^3 5^2 \end{aligned}$$

ו e_3 שלם המקיים

$$\begin{aligned} e_3 &\equiv 1 \bmod 5^2 \\ e_3 &\equiv 0 \bmod 2^3 3^2 \end{aligned}$$

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