תרגול 9 חוגים

25 במאי 2021

1 הכרות עם חוגים

תרגילים:

1. האם $\mathbb{Z}_4$ עם פעולות חיבור וכפל מודולו 4 הוא חוג?
צריך לבדוק ש־ $(\mathbb{Z}_4,+)$ זו חבורה אבלית ־ וזה אכן כך. וכן ש־ $(\mathbb{Z}_4,\cdot)$ אגודה ־ וזה גם נכון. לכן זה חוג. בנוסף, פעולת הכפל חילופית, ולכן זהו חוג חילופי. כמו כן, יש לנו יחידה כפלית ־ 1. ולכן זהו חוג חילופי עם יחידה. האם זהו חוג עם חילוק? בעצם השאלה היא האם $(\mathbb{Z}_4^{\times},\cdot)$ היא חבורה ־ לא. 2 לא הפיך. יותר מזה, 2 הוא "מחלק אפס" כי : $2\cdot 2=4\equiv 0(\mod 4)$.

2. הראו שאם n לא ראשוני אז $\mathbb{Z}_n$ הוא חוג שאיננו חוג עם חילוק.
פתרון: n לא ראשוני, ולכן ישנם $0<a\leq b<n$ כך ש־ $ab=n\equiv 0(\mod n)$.
ולכן a,b לא הפיכים. נראה למשל על b: נב"ש b הפיך, כלומר שיש c כך ש־ $bc=1$.
נכפיל ב־a משמאל, ונקבל:
$$0=0c=\underbrace{a\cdot b}_{\equiv 0}c=a\cdot 1=a$$
בסתירה לכך ש־ $0<a<n$ ולכן $a\not\equiv 0(\mod n)$.

3. ראיתם בהרצאה את חוג הפולינומים מעל שדה. מתקיים: ניתן לקחת חוג פולינומים גם מעל חוג. למשל: $\mathbb{Z}_4[x]$. האם חוג עם יחידה? כן ־ הפולינום 1 הוא איבר היחידה.
דוגמאות לאיברים בחוג:
$$0,1$$
$$x^5+3x^7-2x^{15}=x^5+3x^7+2x^{15}$$
$$(x^2+1)(2x^3+2x)=2x^5+2x^3+2x^3+2x\equiv 2x^5+2x(\mod 4)$$

החוג לא עם חילוק: למשל 2 לא הפיך, וכל פולינום מהצורה $2x^k$ לא הפיך כי הוא מחלק אפס:

$$2 \cdot 2x^k \equiv 0$$

יש איברים הפיכים. למשל:

$$3 \cdot 3 = 9 \equiv 1 (\mod 4)$$

כלומר, 3 הופכי של עצמו. כמו כן:

$$(2x+1)^2 = 4x^2 + 4x + 1 \equiv 1$$

ולכן $2x+1$ גם הופכי של עצמו.

4. יהי R חוג יחידה המקיים:

$$\forall x \in R : x^2 = x$$

הוכיחו: זהו חוג קומוטטיבי.
פתרון: יהיו $a, b \in R$. נשים לב:

$$a^2 + b^2 = a + b = (a+b)^2 = a^2 + ab + ba + b^2$$

ולכן

$$ab + ba = 0 \iff ab = -ba$$

וכעת:

$$ab = (ab)^2 = (-ba)^2 \underset{H.W.}{=} (ba)^2 = ba$$

5. הגדרה: איבר x בחוג R ייקרא נילפטנטי, אם קיים $n \in \mathbb{N}$ כך ש־ $x^n = 0$. דוג': $2 \in \mathbb{Z}_4$ כי $2^2 \equiv 0$.
$\mathbb{R}^{3\times 3} \ni A = \begin{pmatrix} & 1 & \\ & & 1 \\ & & \end{pmatrix}$. ומתקיים:

$$A^2 = \begin{pmatrix} & & 1 \\ & & \\ & & \end{pmatrix}, A^3 = 0$$

הוכיחו: אם ab ניל' אז גם ba ניל'.

פתרון: נתום שיש n כך ש־ $(ab)^n = 0$. נשים לב:

$$(ba)^k = \underbrace{ba \cdot ba \cdots ba}_{k \text{ times}} = b(ab)^{k-1}a$$

ולכן, אם ניקח $k = n+1$ נקבל:

$$(ba)^{n+1} = b(ab)^n a = b \cdot 0 \cdot a = 0$$

2 תתי־חוגים

יהי R חוג, $S \subseteq R$. S ייקרא תת־חוג אם הוא חוג. צריך לבדוק:

1. תנאי תת־חבורה ביחס לפעולת חיבור.
2. סגירות ביחס לכפל.

תרגילים:

1. $GL_n(\mathbb{R}) \leq \mathbb{R}^{n\times n}$?

פתרון: לא, $0 \notin GL_n(\mathbb{R})$ ולכן זוהי לא תת־חבורה חיבורית. גם קל למצוא 2 מטריצות הפיכות שסכומן לא הפיכה.

2. טענה: אם R חג עם יחידה, ו־S תת־חוג כך ש־ $1_R \in S$. אז S הוא חוג עם יחידה והיחידה היא 1_R.

הוכחה: יהי $s \in S$, אז בירושה מהחוג R נקבל: $1_R \cdot s = s \cdot 1_R = s$. מיחידות היחידה נקבל $1_R = 1_S$.

3. $\mathbb{R}^{2\times 2} \geq \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, a \in \mathbb{R} \right\} = S$. ראינו ש־ $\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, a \in \mathbb{R} \right\}$ חבורה ביחס לפעולת חיבור (קל להוכיח בכל מקרה), וכמו כן, ללא מטריצת האפס זוהי חבורה גם כפלית.

נשים לב שאמנם איבר היחידה הכפלי של $\mathbb{R}^{2\times 2}$ הוא I. אבל כיון ש־ $I \notin S$ אז תרגיל קודם לא רלוונטי כאן, ולכן ל־S אולי אין יחידה ואולי יש יחידה אחרת. במקרה שלנו יש לו יחידה אחרת:

$$1_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$