תרגול 9 חוגים

25 במאי 2021

1 הכרות עם חוגים

תרגילים:

1. האם $\mathbb{Z}_n$ חוג? כמובן עם חיבור וכפל מודולו n?
פתרון: $(\mathbb{Z}_n,+)$ חבורה חילופית. פעולת כפל מודולו n היא קיבוצית, ולכן זהו חוג. האם הוא חילופי? כן. האם יש יחידה? 1 הוא איבר היחידה. (הערה: כשאומרים בחוג יחידה, מתכוונים לאיבר היחידה הכפלה. איבר היחידה החיבורי נקרא 0). האם הוא חוג עם חילוק? אם n לא ראשוני, אז יש $0<a\le b<n$ כך ש־ $ab=n\equiv 0(\mod n)$, ולכן a,b לא הפיכים: נוכיח עבור a: נניח בשלילה שקיים c כך ש־ $ca=1$. נכפיל ב־b מימין, ונקבל:
$$0=c0=cab=1b=b$$
בסתירה לבחירת $0<b<n$ ולכן $b\not\equiv 0(\mod n)$.
הערה: עבור p ראשוני נקבל $\mathbb{Z}_p$ הוא שדה.

2. ראיתם בהרצאה את חוג הפולינומים מעל שדה. ניתן להגדיר את החוג גם מעל חוג. למשל נתבונן בחוג הפולינומים $\mathbb{Z}_4[x]$. פולינומים עם מקדמים מ־$\mathbb{Z}_4$. למשל:
$$x+3x^5-2x^7\equiv x+3x^5+2x^7$$
למשל:
$$(x+1)(2x+3x^2)=2x^2+2x+3x^3+3x^2\equiv 2x+x^2+3x^3$$
זהו לא חוג עם חילוק, למשל: 2 מחלק אפס ולכן לא הפיך. כמו כן $2x$ וכד'.
האם יש איברים הפיכים? למשל 3 הופכי של עצמו: $3\cdot 3=9\equiv 1(\mod 4)$. דוג' נוספת:
$$(1+2x)(1+2x)=1+4x+4x^2\equiv 1(\mod 4)$$

בסה"כ: זהו חוג עם יחידה חילופי.

3. יהי R חוג עם יחידה המקיים:

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

הוכיחו: R חוג חילופי.

פתרון: יהיו $a, b \in R$ צריך להוכיח $ab = ba$. נתבונן ב: $(a+b)^2$:

$$a^2 + b^2 = a + b = (a+b)^2 = (a+b)\cdot(a+b) \underset{*}{=} a^2 + ab + ba + b^2$$

כאשר שיוויון $*$ נובע מחוקי הפילוג. ולכן

$$ab + ba = 0$$

$$ab = -ba$$

כעת נשים לב:

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

4. הגדרה: איבר x בחוג R נקרא נלפוטנטי אם קיים $n \in \mathbb{N}$ כך ש־ $x^n = 0$.

דוגמאות: המטריצה $\mathbb{R}^{3\times 3} \ni A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$. מקיימת:

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

דוגמא נוספת: $2 \in \mathbb{Z}_4$ כי $2^2 = 4 \equiv (0 \mod 4)$.

הערה: נילפוטנטי גורר מחלק אפס, אך לא להיפך.

הוכיחו: אם ab ניל' אז ba ניל'.

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

$$(ab)^n = ababab\cdots ab$$

כמו שרואים:

$$(ab)^n = a(ba)^{n-1}b$$

ולכן ניקח את החזקה $n+1$:

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

2 תתי חוגים

יהי R חוג. קבוצה $S \subset R$ נקראת תת־חוג אם היא חוג בפנ"ע. מספיק לבדוק:

1. תנאי תת־חבורה על פעולת החיבור.
2. סגירות לכפל.

סימון של תת־חוג: $S \leq R$.

תרגילים:

1. האם $GL_n(\mathbb{R}) \leq \mathbb{R}^{n\times n}$. ראשית מטריצת האפס לא נמצאת, ולכן לא תת־חבורה חיבורית (הערה: גם אם נוסיף את מטריצת האפס, קל למצוא 2 מטריצות הפיכות שסכומן מטריצה לא הפיכה שונה מאפס).

2. $S = \left\{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} : a, b \in \mathbb{R} \right\} \leq \mathbb{R}^{2\times 2}$?

   פתרון: זוהי תת־חבורה חיבורית. נראה סגירות לכפל:

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix} \begin{pmatrix} c & c \\ d & d \end{pmatrix} = \begin{pmatrix} a(c+d) & a(c+d) \\ b(c+d) & b(c+d) \end{pmatrix} \in S$$

   אין איבר יחידה

3. הוכיחו: יהי R חוג עם יחידה. אם $S \leq R$ ו־$1_R \in S$ אז 1_R איבר היחידה הכפלי של S.

   פתרון: לכל $s \in S$ מתקיים, כירושה מיחידה ב־R:

$$1_R \cdot s = s \cdot 1_R = s$$

4. $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\} \leq \mathbb{R}^{2\times 2}$. קל לראות שזוהי תת־חבורה חיבורית. ראינו בתרגול הראשון ש־S חבורה כפלית, ולכן קיבלנו ש־S תת־חוג עם יחידה.

   הערה: שימו לב ש$1_S \neq 1_R$, וזה לא סותר את התרגיל הקודם, כי $1_R \notin S$.