

אלגברה ב2

© ארזים

14 במרץ 2017

הגדרה 0.1 חוג (קומוטטיבי עם יחידה) R הוא קבוצה עם שתי פעולות בינאריות, כפל וחיבור, שמקיימות:

חיבור

.1

$$\forall a, b \quad a + b = b + a$$

.2

$$\forall a, b, c \quad a + (b + c) = (a + b) + c$$

.3

$$\exists 0 \forall a \quad a + 0 = 0 + a = a$$

.4

$$\forall a \exists b \quad a + b = b + a = 0$$

כפל

.1

$$\forall a, b \quad ab = ba$$

.2

$$\forall a, b, c \quad a(bc) = (ab)c$$

3.

$$\exists 1 \forall a \quad a \cdot 1 = 1 \cdot a = a$$

פילוג

1.

$$\forall a, b, c \quad a(b + c) = ab + ac$$

דוגמאות $\mathbb{F}_2[x, y], \mathbb{Z}, \mathbb{C}$

הגדרה 0.2 נסמן בתור R^* את קבוצת ההפיכים ביחס לכפל בחוג R :

$$R^* = \{x \in R \mid \exists y \in R \quad xy = 1\}$$

זוהי חבורה אבלית.

דוגמאות בחוג $\mathbb{Z}$, ההפיכים הם $\{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$. כמו כן,

$$\mathbb{Q}[x]^* = \mathbb{Q}^*$$

הגדרה 0.3 $\emptyset \neq I \subseteq R$ נקרא אידיאל אם הוא סגור לחיבור, וכן לכפל בכל איברי R . כלומר,

$$\forall a, b \in I \quad a + b \in I$$

$$\forall a \in I, r \in R \quad ar \in I$$

הגדרה 0.4 $A \subseteq \mathbb{R}$ נקרא תת חוג אם הוא חוג ביחס לפעולות של R . באופן שקול, מספיק לבדוק כי $0, 1 \in A$, וכן כי A סגור לחיבור ולכפל.

דוגמא לתת חוג:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

דוגמא לאידיאל:

$$2\mathbb{Z} \subseteq \mathbb{Z}$$

$$\mathbb{C}[x] \setminus \mathbb{C}[x]^* = \{x \cdot f(x) \mid f(x) \in \mathbb{C}[x]\} = x \cdot \mathbb{C}[x] \subseteq \mathbb{C}[x]$$

הדוגמא השנייה היא של אוסף כל הפולינומים המרוכבים בעלי מקדם חופשי 0 (או אלה שמתחלקים בפולינום x - שקול). דוגמא נוספת - כל הפולינומים בחוג $\mathbb{F}_2[x, y]$ שמתחלקים בפולינום $xy - 1$. מסמנים אותו $(xy - 1)\mathbb{F}_2[x, y]$.

הגדרה 0.5 עבור $I \subseteq R$ אידאל נגדיר מבנה של חוג על R/I :

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I)(b + I) = ab + I$$

דוגמאות נלך לפי הדוגמאות שלעיל לאידאלים.

$$\mathbb{Z}/2\mathbb{Z} \cong \mathbb{F}_2$$

$$\mathbb{C}[x]/x\mathbb{C}[x] \cong \mathbb{C}$$

$$\mathbb{F}_2[x, y]/(xy - 1)\mathbb{F}_2[x, y] \cong \mathbb{F}_2[x, x^{-1}]$$

לגבי הדוגמה האחרונה - לקחת מנה מודולו פולינום מסויים זה כמו להחליט שהוא שווה לאפס, כלומר במקרה הזה

$$xy - 1 = 0$$

$$xy = 1$$

$$y = x^{-1}$$

הסימון של איזומורפיזם יוסבר מיד.

הגדרה 0.6 העתקה $\varphi : A \rightarrow B$ בין חוגים תקרא הומומורפיזם אם מתקיים:

1.

$$\varphi(0) = 0, \varphi(1) = 1$$

2.

$$\varphi(ab) = \varphi(a)\varphi(b)$$

3.

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

הגדרה 0.7 הומומורפיזם φ שהוא חד־חד־ערכי ועל נקרא איזומורפיזם.

כמו בחבורות, אם נגדיר

$$\ker \varphi = \{a \in A \mid \varphi(a) = 0\}$$

נקבל אידאל של A , ונקבל

$$A/\ker \varphi \cong \operatorname{Im} \varphi$$

בהינתן A, B חוגים, נוכל לתת מבנה של חוג על $A \times B$ (לפי קואורדינטות). באופן כללי יותר, אם $\{A_n\}_{n=1}^\infty$ אז יש מבנה של חוג על

$$\prod_{n=1}^\infty A_n$$

למשל, ניקח $A_n = \mathbb{Z}/p^n\mathbb{Z}$, עבור p ראשוני כלשהו. ישנן הטלות $\varphi_i : \prod A_n \rightarrow A_i$. ההטלות הללו הן כמובן הומומורפיזמים. חשוב לשים לב שהחוגים A, B לאו דווקא תתי חוגים של $A \times B$. נחזור לדוגמא בא $A_n = \mathbb{Z}/p^n\mathbb{Z}$. נגדיר העתקות

$$\begin{aligned} \lambda_{i+1,i} : \mathbb{Z}/p^{i+1}\mathbb{Z} &\rightarrow \mathbb{Z}/p^i\mathbb{Z} \\ \lambda_{i+1,i}(x) &= x \pmod{p^i} \end{aligned}$$

זהו הומומורפיזם של חוגים. נגדיר תת חוג של $\prod \mathbb{Z}/p^n\mathbb{Z}$ על ידי

$$\mathbb{Z}_p := \left\{ v \in \prod_{n=1}^\infty \mathbb{Z}/p^n\mathbb{Z} \mid \forall i \in \mathbb{N} \quad \lambda_{i+1,i} \varphi_{i+1}(v) = \varphi_i(v) \right\}$$

זהו חוג שנקרא חוג השלמים ה־p־אדיים. בנוסף, זהו תחום שלמות:

$$\forall a \neq 0, b \neq 0 \quad ab \neq 0$$

חוג זה אינו בן מניה, ונסמן $\mathbb{Q}_p$ את שדה המנות של $\mathbb{Z}_p$. שדה זה נקרא שדה המספרים ה־p־אדיים.