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.

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

2.

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

3.

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

4.

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

כפל

1.

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

2.

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

.3

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

פילוג

.1

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

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

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

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

זוהי חבורה אבלית.

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

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

הגדרה 0.3 $\emptyset \neq I \subseteq R$ נקרא <u>אידאל</u> אם הוא סגור לחיבור, וכן לכפל בכל איברי R. כלומר,

$$\forall a,b \in I \ \ a+b \in I$$
$$\forall a \in I, r \in R \ \ ar \in I$$

הגדרה 0.4 $A \subseteq \mathbb{R}$ נקרא <u>תת חוג</u> 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:

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

דוגמא לאידאל:

$$2\mathbb{Z} \subseteq \mathbb{Z}$$
$$\mathbb{C}\left[x\right] \backslash \mathbb{C}\left[x\right]^* = \{x \cdot f\left(x\right) \mid f\left(x\right) \in \mathbb{C}\left[x\right]\} = x \cdot \mathbb{C}\left[x\right] \subseteq \mathbb{C}\left[x\right]$$

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

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.

$$\mathbb{Z}/2\mathbb{Z}\cong\mathbb{F}_2$$
$$\mathbb{C}[x]/x\mathbb{C}[x]\cong\mathbb{C}$$
$$\mathbb{F}_2[x,y]/(xy-1)\mathbb{F}_2[x,y]\cong\mathbb{F}_2\left[x,x^{-1}\right]$$

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 $\varphi : A \to B$ 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

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

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 $\varphi_i : \prod A_n \to A_i$. ההטלות הללו הן כמובן הומומורפיזמים.
חשוב לשים לב שהחוגים A, B <u>לאו דווקא</u> תתי חוגים של $A \times B$.
נחזור לדוגמא בא $A_n = \mathbb{Z}/p^n\mathbb{Z}$. נגדיר העתקות

$$\lambda_{i+1,i} : \mathbb{Z}/p^{i+1}\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$$
$$\lambda_{i+1,i}(x) = x \mod p^i$$

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

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

זהו חוג שנקרא <u>חוג השלמים הp־אדיים</u>. בנוסף, זהו תחום שלמות:

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

חוג זה אינו בן מניה, ונסמן $\mathbb{Q}_p$ את שדה המנות של $\mathbb{Z}_p$. שדה זה נקרא <u>שדה המספרים הp־אדיים</u>.