הגדרה

חוג הוא שלשה הכוללת קבוצה ושתי פעולות בינאריות - "חיבור" וכפל" - $(R,+,\cdot)$

הערה שדה הוא דוגמה פרטית לחוג.

תכונות של חבורה:

1. $(R,+)$ חבורה אבלית. איבר היחידה מסומן ב0.
2. $(R^*,\cdot)$ חבורה למחצה, כאשר $R^*=R\setminus\{0\}$.
3. מתקיים חוק הפילוג - $\begin{array}{l}(a+b)\,c=ac+bc\\ a\,)b+c(\,=ab+ac\end{array}$

חוגים מיוחדים

- חוג קומוטטיבי - אם $(R^*,\cdot)$ הוא חבורה אבלית
- חוג עם יחידה - אם $(R^*,\cdot)$ כולל את איבר היחידה זה מונואיד
- חוג עם חילוק - אם $(R^*,\cdot)$היא חבורה. במקרה זה, ההפכי של a לפעולת הכפל מסומן בa^{-1}.
- שדה - אם $(R^*,\cdot)$ היא חבורה אבלית.

תזכורת

$$A\cdot\operatorname{adj}(A)=\operatorname{adj}(A)\cdot A=\det(A)\cdot I$$

תרגיל

יהי R חוג קומוטטיבי עם יחידה. הוכח כי $A\in M_n(R)$ הפיכה אם ורק אם $\det A$ הפיכה.

דוגמה

$$A\in M_2(\mathbb{Z})$$

$$A=\begin{pmatrix}2&3\\-1&-2\end{pmatrix}=-1$$

מכיוון ש-1 הפיך ב$\mathbb{Z}$, נקבל שA מטריצה הפיכה.

פתרון התרגיל

$\Leftarrow$ נתון $A \in M_n(R)$ מטריצה הפיכה.

$$A \cdot B = B \cdot A = I$$

$$1_R = \det(I) = \det(A \cdot B) = \det(A) \cdot \det(B)$$

R חוג קומוטטיבי, ולכן $\det(B) \cdot \det(A) = 1$, ולכן $\det(a)$ הפיך בR.

$\Rightarrow$ $A \cdot \operatorname{adj}(A) = \det A \cdot I$. נתון ש$\det A$ הפיך בR. ז"א קיים $x \in R$ כך ש$x \cdot \det A = 1_R$, לכן:

$$xA \cdot \operatorname{adj}(A) = (x \cdot \det A) \cdot I$$

R חוג קומוטטיבי, לכן

$$A(x \cdot \operatorname{adj}(A)) = I$$

באותו אופן, ניתן להראות ש$x(\operatorname{adj} A)A = I$.

תזכורת

$\{\mathbb{Q}[\sqrt{2}] = a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ שדה

תרגיל

$\mathbb{Z}[\sqrt{2}]$ חוג קומוטטיבי עם יחידה. הוכיחו שישנם אינסוף מספרים הפיכים ב$\mathbb{Z}(\sqrt{2})$.

פתרון

$$\left(3 + 2\sqrt{2}\right)\left(3 - 2\sqrt{2}\right) = 1$$

$3 + 2\sqrt{2} > 1$ ולכן קבוצת החזקות השלמות שלו היא אינסופית. כלומר $\left(3 + 2\sqrt{2}\right)^n$ איבר הפיך:

$$\left(3 + 2\sqrt{2}\right)^n \left(3 - 2\sqrt{n}\right)^n = \left[\left(3 + 2\sqrt{2}\right)\left(3 - 2\sqrt{2}\right)\right]^n = 1^n = 1$$

הערה

$\mathbb{Z}[i]$ הוא חוג קומוטטיבי עם יחידה, שהאיברים ההפיכים היחידים הם $\pm 1, \pm i$.

הערה

איבר a נקרא הפיך משמאל אם קיים b כך ש$ba = 1$
קיימים חוגים שבהם יש איבר הפיך משמאל ולא מימין, ולהפך.

הגדרה

1. $a \neq 0$ נקרא "מחלק אפס" שמאלי(ימני) אם קיים $b \neq 0$ כך $ab = 0$($ba = 0$)
2. חוג ללא מחלקי אפס נקרא "תחום". תחום קומוטטיבי נקרא "תחום שלמות".

דוגמאות

- $\mathbb{Z}$ תחום שלמות שהוא לא שדה.[1]
- $\mathbb{Z}_6$ אינו תחום, כי $2 \cdot 3 = 0$
- לכל חוג קומוטטיבי עם יחידה R, $n > 1$, $M_n(R)$ איננו תחום.
- חוג עם חילוק הוא תמיד תחום.

הגדרה

בהינתן חוג קומוטטיבי עם יחידה R, נסמן את חוג הפולינומים ב$R[x]$.

- $R[x]$ חוג קומוטטיבי עם יחידה.
- אם R תחום שלמות אז גם $R[x]$ תחום שלמות.
- אם R שדה - $R[x]$ **לא** שדה.
- נגדיר $R[[x]]$ להיות חוג טורי טיילור. $1-x$ הפיך, כי $\frac{1}{1-x} = 1 + x + x^2 ...$

הערה לא מחשבים את הטור עצמו, אלא מכפילים אותו בתור טור טיילור, בלי להציב ערך בx:

$$(1-x)\left(1 + x + x^2 + ...\right) = 1$$

תרגיל

הוכח כי $1 + 2x$ הפיך ב$\mathbb{Z}_4[x]$

פתרון

$$(1+2x)(1+2x) = 1$$

[1] למשל 2 לא הפיך ב$\mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Q}$ שדה, הופכי של 2 ב$\mathbb{Q}$ הוא $\frac{1}{2}$.

הגדרה

תת חוג $S \subseteq R$ הוא תת קבוצה שמהווה חוג ביחס לפעולות המקוריות.

משפט

$S \subseteq \emptyset$ תת חוג של R אם ורק אם לכל $a, b \in S$ מתקיים $a \cdot b \in S, a - b \in S$

דוגמאות

1. $n \in \mathbb{N}$, $n\mathbb{Z}$ הוא תת חוג של $\mathbb{Z}$:

   $a \cdot b \in n\mathbb{Z}$ ז"א קיימים $x, y \in \mathbb{Z}$ כך ש $\begin{matrix} a = nx \\ b = ny \end{matrix}$

$$a \cdot b = nx \cdot ny = n \cdot \underbrace{(x \cdot ny)}_{\in \mathbb{Z}} \in n\mathbb{Z}$$

$$a - b = nx - ny = n \underbrace{(x - y)}_{\in \mathbb{Z}} \in n\mathbb{Z}$$

2. אם S תת חוג של R, אז $M_n(S)$ תת חוג של $M_n(R)$.
3. אם $k|n$ אז $k\mathbb{Z}_n$ הוא תת חוג של $\mathbb{Z}_n$.

תרגיל

1. יהי חוג R ויהי $0 \neq q \in R$. הוכח כי qRq תת חוג של R.
2. נניח ש$q^2 = q$. הוכי כי q הוא היחידה בqRq.

פתרון

$$qRq = \{qaq | a \in R\}$$

1. נניח ש$a, b \in qRq$, צ"ל $a - b \in qRq$, $ab \in qRq$.
   - $a \in qRq$ ז"א קיים $x \in R$ כך ש$a = qxq$
   - $b \in qRq$ ז"א קיים $y \in R$ כך ש$b = qyq$

$$a \cdot b = qxq \cdot qyq = q\left(xq^2y\right)q \in qRq$$

$$a + b = qxq + qyq = (qx + qy)\,q = (q\,(x + y))\,q = q\,(x + y)\,q \in qRq$$

2. צריך להוכיח שלכל $a \in qRq$, $a \cdot q = q \cdot a = a$. $a \in qRq \Leftarrow$ קיים $x \in R$ כך ש$a = qxq$

$$x \cdot q = qxq^2 = qxq$$