הגדרות

יהי חוג R. המרכז של החוג R מסומן ב$Z\left(R\right)$

$$Z\left(R\right)=\left\{y\in R|\forall_{x\in R}xy=yx\right\}$$

המרכז של תת קבוצה $S\subseteq R$ הוא

$$C_{R}\left(S\right)=\left\{y\in R|\forall_{x\in S}xy=yx\right\}$$

תכונות

1. $Z\left(R\right)$ תת חוג קומוטטיבי של R.
2. R קומוטטיבי אם ורק אם $R=Z\left(R\right)$
3. $C_{R}\left(S\right)$ תת חוג של R.

טענה

המרכז של חוג עם חילוק D הוא שדה.

הוכחה

נתון שD חוג עם חילוק. צריך להוכיח ש$Z\left(D\right)$ שדה.
$Z\left(D\right)$ הוא תת חוג של D:

1. אם $a,b\in Z\left(D\right)$ אז $ab\in Z\left(D\right)$
2. $a-b\in Z\left(D\right)$

הוכחה: 1. נניח ש$a,b\in Z\left(D\right)$, ז"א לכל $x\in R$ $ax=xa$, $bx=xb$.
יהי $x\in R$.

$$\left(a\cdot b\right)\cdot x=a\cdot\left(b\cdot x\right)=a\cdot\left(x\cdot b\right)=\left(a\cdot x\right)\cdot b=\left(x\cdot a\right)\cdot b=x\cdot\left(a\cdot b\right)\Rightarrow a\cdot b\in Z\left(D\right)$$

2. קל מאוד להוכיח.

$Z\left(D\right)$ חוג קומוטטיבי - נובע ישירות מההגדרה. אם $x,y\in Z\left(D\right)$, בפרט $x\in D$ ולכן $xy=yx$.
נוכיח ש$Z\left(D\right)$ חוג עם חילוק. מכיוון שD חוג עם חילוק אז קיים לו איבר יחידה. נסמן $1_{D}\in D$. לכל $x\in D$ מתקיים $1_{D}\cdot x=x=x\cdot1_{D}$ ולכן $1_{D}\in Z\left(D\right)$.
נוכיח שלכל $a\in Z\left(D\right)$ קיים איבר $a^{-1}\in Z\left(D\right)$. צ"ל שלכל $x\in D$, $a^{-1}x=xa^{-1}$:

$$x\cdot a^{-1}=\left(\left(x\cdot a^{-1}\right)^{-1}\right)^{-1}=\left(a\cdot x^{-1}\right)^{-1}=\left(x^{-1}\cdot a\right)^{-1}=a^{-1}\cdot x\Rightarrow a^{-1}\in Z\left(D\right)$$

דוגמאות

1. הקבוצה $H=\left\{\begin{pmatrix} a & b \\ -\bar{b} & \bar{a}\end{pmatrix}\middle| a,b\in\mathbb{C}\right\}$ היא תת חוג של $M_2\left[\mathbb{C}\right]$. החוג $M_2\left[\mathbb{C}\right]$ הוא חוג עם חילוק שאינו קומוטטיבי.

   • החוג H הוא חוג עם חילוק:

$$\det\begin{pmatrix} a & b \\ -\bar{b} & \bar{a}\end{pmatrix}=a\bar{a}-\left(-\bar{b}\right)b=|a|^2+|b|^2=0\Leftrightarrow a=b=0$$

ז"א לכל מטריצה $0\neq A\in H$, $\det\left(A\right)\neq 0$, ולכן הפיכה.

   • אינו קומוטטיבי:

$$\begin{pmatrix} i & 0 \\ 0 & -i\end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0\end{pmatrix}\neq\begin{pmatrix} 0 & i \\ i & 0\end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i\end{pmatrix}$$

חוג זה נקרא חוג הקווטרניונים.

2. יהי $\mathbb{F}$ שדה, כך $\mathrm{char}\mathbb{F}\neq 2$. $a\in\mathbb{F}$ כך ש$a\notin\left(\mathbb{F}^*\right)^2$.[1]
נסמן $K=\mathbb{F}\left[\sqrt{a}\right]=\left\{\alpha+\beta\sqrt{a}|\alpha,\beta\in\mathbb{F}\right\}$ שדה.
נניח שקיים $b\in\mathbb{F}^*$ כך ש$b\neq u^2-av^2$ לכל $u,v\in\mathbb{F}$.
נסמן: $A=\left\{\begin{pmatrix} x & y \\ b\bar{y} & \bar{x}\end{pmatrix}\middle| x,y\in K\right\}\subseteq M_2\left(K\right)$.
עבור $x=\alpha+\beta\sqrt{a}$ נסמן $\bar{x}=\alpha-\beta\sqrt{a}$

טענה: A חוג עם חילוק לא קומוטטיבי.

הוכחה: נראה שA תת חוג של $M_2\left(K\right)$. נתבונן ב $\begin{pmatrix} z & w \\ b\bar{w} & \bar{z}\end{pmatrix}$, $\begin{pmatrix} x & y \\ b\bar{y} & \bar{x}\end{pmatrix}$.

$$\begin{pmatrix} x & y \\ b\bar{y} & \bar{x}\end{pmatrix}-\begin{pmatrix} z & w \\ b\bar{w} & \bar{z}\end{pmatrix}=\begin{pmatrix} x-z & y-w \\ b\left(\overline{y-w}\right) & \overline{x-z}\end{pmatrix}\in A$$

$$\begin{pmatrix} x & y \\ b\bar{y} & \bar{x}\end{pmatrix}\begin{pmatrix} z & w \\ b\bar{w} & \bar{z}\end{pmatrix}=\begin{pmatrix} xz+by\bar{w} & xw+y\bar{z} \\ b\bar{y}z+b\bar{x}\bar{w} & b\bar{y}w+\bar{x}\bar{z}\end{pmatrix}$$

נראה שA לא קומוטטיבי.

$$\begin{pmatrix} 0 & 1 \\ b & 0\end{pmatrix}\begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a}\end{pmatrix}\neq\begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a}\end{pmatrix}\begin{pmatrix} 0 & 1 \\ b & 0\end{pmatrix}$$

נוכיח שלכל איבר בA יש הופכי. מספיק להראות שלכל $0\neq T\in A$, $\det\left(T\right)\neq 0$.
נניח בשלילה ש$\det\left(T\right)=0$ ונוכיח ש$T=0$.

$$\det\begin{pmatrix} x & y \\ b\bar{y} & \bar{x}\end{pmatrix}=x\bar{x}-by\bar{y}=0\Leftrightarrow x\bar{x}=by\bar{y}$$

[1] $\mathbb{F}^*$ זה $\mathbb{F}$ ללא איבר ה0

אם $y=0$ אז $x=\bar{x}=y=\bar{y}=0$, וקיבלנו את מטריצת האפס.(בהנחה שהוכחנו שK שדה)

אם $y\neq 0$ אז $\frac{x}{y}\cdot\frac{\bar{x}}{\bar{y}}=\frac{x\bar{x}}{y\bar{y}}=b$. נסמן $\frac{x}{y}=u+v\sqrt{a}$, ואז $\frac{\bar{x}}{\bar{y}}=u-v\sqrt{a}$.(ניתן להראות ש $\overline{\left(\frac{x}{y}\right)}=\frac{\bar{x}}{\bar{y}}$).

$$b=\left(u+v\sqrt{a}\right)\left(u-v\sqrt{a}\right)=u^2-v^2a$$

בסתירה לכך ש$b\neq u^2-v^2a$.

הגדרה

יהיו S,R חוגים.
נאמר כי $\varphi:R\to S$ הומומורפיזם של חוגים אם מתקיים

$$\varphi\left(r_1\cdot r_2\right)=\varphi\left(r_1\right)\cdot\varphi\left(r_2\right)$$

$$\varphi\left(r_1+r_2\right)=\varphi\left(r_1\right)+\varphi\left(r_2\right)$$

אם בנוסף מתקיים $\varphi\left(1_R\right)=r_S$ נאמר שההומומורפיזם יוניטרי.

דוגמאות

1. $\varphi:\mathbb{Z}\to\mathbb{Z}_n$ כך שלכל $m\in\mathbb{Z}$, $\varphi\left(m\right)=m\left(\bmod n\right)$.
φ הוא אפימורפיזם(הומומורפיזם על)

2. A תת חוג המטריצות האלכסוניות ב$M_2\left(R\right)$, ונגדיר $\varphi\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}=\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}$.
הוכחת ההומומורפיזם ־ מיידי.

$$\varphi\left(1_A\right)=\varphi\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$$

כלומר החוג מעביר גם יחידה ליחידה(למרות שזו לא אותה יחידה), לכן זהו הומומורפיזם יוניטרי.

טענה

יהי S,R חוגים עם יחידה. $\varphi:R\to S$ אפימורפיזם.
אזי $\varphi\left(1_R\right)=1_S$

הוכחה

φ על. ז"א לכל $a \in S$ קיים $b \in R$ כך ש$\varphi(b) = a$. יהי $a \in S$.

$$a = \varphi(b) = \varphi(b) \cdot \varphi(1_R) = a \cdot \varphi(1_R)$$

הערה

1. אם $\varphi : \mathbb{Q} \to \mathbb{Q}$ הומומורפיזם כך ש$\varphi(1) = 1$ אז $\varphi := \mathrm{Id}$
2. הערה 1 לא מתקיימת לכל שדה.
$\varphi : \mathbb{Q}\left[\sqrt{2}\right] \to \mathbb{Q}\left[\sqrt{2}\right]$ כך ש$\varphi\left(a + b\sqrt{2}\right) = a - b\sqrt{2}$ לא מתקיים $\varphi := \mathrm{Id}$

הגדרה

יהי $\varphi : R \to S$ הומומורפיזם.

- נסמן את התמונה של φ ע"י $\mathrm{Im}\varphi = \{\varphi(x) | x \in R\}$(תת חוג של S)
- נסמן את הגרעין של φ ע"י $\ker\varphi = \{x \in R | \varphi(x) = 0\}$

נשים לב שאם $\varphi \neq 0$ אז $1_R \notin \ker\varphi$

הגדרה

יהי R חוג, $I \subset R$ תת קבוצה.
נאמר שI אידיאל או אידיאל דו צדדי אם:

1. I תת חבורה חיבורית.
2. לכל $r \in R, i \in I$ מתקיים $i \cdot 1, 1 \cdot i \in I$

מסמנים $I \lhd R$

דוגמאות

1. לכל הומומורפיזם $\varphi : R \to S$, $\ker\varphi$ הוא אידיאל של R.
2. האידיאלים היחידים של $\mathbb{Z}$ הם מהצורה $n\mathbb{Z}$($n > 1$).
3. יהי $x \in R$, אז הקבוצה $Rx = \{r \cdot x | r \in R\}$ היא אידאל שמאלי.
$R = M_2(D)$, $e_{12} \in R$

$$I = Re_{12} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} \middle| a, c \in \mathbb{Q} \right\}$$

4. יהי $R = Z\left[\sqrt{5}\right] = \left\{a + b\sqrt{5} \middle| a, b \in \mathbb{Z}\right\}$
אז $I = \left\{a + b\sqrt{5} \middle| a \in 5\mathbb{Z}, b \in \mathbb{Z}\right\}$ אז $I \lhd R$.

הוכחה:

$$\overbrace{\left(c + d\sqrt{5}\right)}^{\in R}\overbrace{\left(5n + m\sqrt{5}\right)}^{\in I} = 5cn + 5dn + cm\sqrt{5} + 5dn\sqrt{5} = 5\left(cn + dm\right) + \left(cm + 5dn\right)\sqrt{5}$$