

אלגברה מופשטת 2 – תרגיל כיתה 2

מתרגלים: ד"ר אפי כהן ואדם צ'פמן.

טענה

המרכז של חוג עם חילוק D הוא שדה.

הוכחה

D הוא חוג עם חילוק, ולכן קיים ב D איבר יחידה שנסמנו ב 1_D . לכל $x \in D$ מתקיים

$$1_D \in Z(D) \text{ ז"א } x = 1_D \cdot x = x \cdot 1_D$$

מכיוון ש $Z(D)$ חוג קומוטטיבי מספיק להראות שלכל $0 \neq x \in Z(D)$ קיים $x^{-1} \in Z(D)$.

מכיוון ש D חוג עם חילוק נקבל שאם $0 \neq x \in Z(D) \subseteq D$ קיים $x^{-1} \in D$.

יהי $d \in D$

$$x^{-1} \in Z(D) \text{ ז"א } x^{-1}d = (d^{-1}x)^{-1} = (xd^{-1})^{-1} = dx^{-1}$$

• השוויון הראשון D - חוג עם חילוק ולכן קיים ל $d \in D$ איבר הופכי $d^{-1} \in D$.

$$\text{ובנוסף } (x^{-1}d)(d^{-1}x) = 1_D$$

• השוויון השני - $x \in Z(D)$ ולכן לכל $y \in D$ מתקיים $yx = xy$ ובפרט $d^{-1}x = xd^{-1}$.

• השוויון השלישי – דומה מאוד להוכחה עבור השוויון הראשון.

דוגמאות

1. הקבוצה $H = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{C} \right\}$ היא תת חוג של $M_2(\mathbb{C})$. החוג H הוא חוג עם

חילוק שאינו קומוטטיבי.

• חוג עם חילוק - $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$ ובנוסף $\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a\bar{a} + b\bar{b} = 0 \Leftrightarrow a = b = 0$

• אינו קומוטטיבי - $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$

חוג זה נקרא חוג הקוטרניונים. שימו לב שמתקיים:

• אם נסמן $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ אז

$Z(H) = \text{span}_{\mathbb{R}}\{1\} \cong \mathbb{R}$ ומתקיים $H = \text{span}_{\mathbb{R}}\{1, i, j, k\}$

• $i^2 = j^2 = k^2 = -1, i \cdot j = -j \cdot i$

2. יהי F שדה כך ש $\text{char}(F) \neq 2$, $a \in F$ כך ש $a \notin (F^*)^2$.

נסמן $K = F[\sqrt{a}] = \{\alpha + \beta\sqrt{a} \mid \alpha, \beta \in F\}$ אז ניתן לבדוק ש K שדה.

נניח עתה שקיים $b \in F^*$ כך ש $b \neq u^2 - av^2$ לכל $u, v \in F$.

(למשל $F = \mathbb{Q}, a = -2, b = -5$.)

נסמן עבור $x = \alpha + \beta\sqrt{a}$, $\bar{x} = \alpha - \beta\sqrt{a}$ יהי $A = \left\{ \begin{pmatrix} x & y \\ b\bar{y} & \bar{x} \end{pmatrix} \mid x, y \in K \right\} \subset M_2(K)$

טענה

A חוג עם חילוק לא קומוטטיבי.

הוכחה

נוכיח ש A תת חוג של $M_2(K)$. סגור להפרש – מייד.

נראה סגירות עבור מכפלה:

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

נראה ש A לא קומוטטיבית: $\begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} \cdot \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \neq \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}$

נוכיח שלכל איבר ב A יש הופכי. מספיק להראות שלכל $0 \neq T \in A$ מתקיים $\det(T) \neq 0$.

נניח ש $\det(T) = 0$ ונוכיח ש $T = 0$.

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

אם $y = 0$ אז $x\bar{x} = 0 \leftrightarrow \alpha^2 - \beta^2 a = 0 \leftrightarrow \alpha = \beta = 0$ ולכן נקבל את מטריצת האפס.

אם $y \neq 0$ אז $b = \frac{xy}{y}$ נסמן $\frac{x}{y} = u + v\sqrt{a}$ כך ש $u, v \in F$ ואז $\frac{\bar{x}}{y} = u - v\sqrt{a}$ (חישבו למה)

ז"א $b = u^2 - v^2a$ בסתירה להנחה ש $b \neq u^2 - v^2a$.

הגדרה

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

- $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$
- $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$
- אם במוסף מתקיים $\varphi(1_R) = 1_S$ נאמר שההומומורפיזם יוניטרי.

דוגמאות

1. הומומורפיזם האפס: $\varphi(x) = 0$ לכל $x \in R$.
2. $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ כך שלכל $m \in \mathbb{Z}$ $\varphi(m) = m \pmod{n}$ וזאת דוגמא להומומורפיזם על.
3. יהי A תת חוג המטריצות האלכסוניות ב $M_2(R)$ ונגדיר $\varphi: A \rightarrow A$ ע"י

$$\varphi \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

אזי φ הומומורפיזם:

$$\varphi \left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \right) = \varphi \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & 0 \end{pmatrix}$$

$$\varphi \left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right) \cdot \varphi \left(\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \right) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & 0 \\ 0 & 0 \end{pmatrix}$$

$$\varphi \left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \right) = \varphi \left(\begin{pmatrix} a+c & 0 \\ 0 & b+d \end{pmatrix} \right) = \begin{pmatrix} a+c & 0 \\ 0 & 0 \end{pmatrix}$$

$$\varphi \left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right) + \varphi \left(\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \right) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} c & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+c & 0 \\ 0 & 0 \end{pmatrix}$$

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

אבל עבור ההומומורפיזם $\varphi: A \rightarrow \text{Im } \varphi$ כאשר $\varphi \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ מתקיים

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

4. $\varphi: C \rightarrow C$ המוגדר ע"י $\varphi(z) = \bar{z}$ הוא הומומורפיזם חח"ע ועל.

5. $\varphi: H \rightarrow H$ המוגדר ע"י $\varphi(a + bi + cj + dk) = a - bi - cj - dk$ הוא אנטי

הומומורפיזם כי לכל $x, y \in H$ מתקיים $\varphi(x + y) = \varphi(x) + \varphi(y)$ ו

$$\varphi(x \cdot y) = \varphi(y) \cdot \varphi(x)$$

הגדרה

הומומורפיזם על נקרא אפימורפיזם.

הומומורפיזם חח"ע ועל נקרא איזומורפיזם.

טענה

יהיו S, R חוגים עם יחידה ותהיי $\varphi: R \rightarrow S$ אפימורפיזם. אזי $\varphi(1_R) = 1_S$.

הוכחה

φ על ולכן לכל $a \in S$ קיים $b \in R$ כך ש $\varphi(b) = a$.

$$a = a \cdot \varphi(1_R) \quad a \in S \quad \text{קיבלנו שלכל } a = \varphi(b) = \varphi(b \cdot 1_R) = \varphi(b) \cdot \varphi(1_R) = a \cdot \varphi(1_R)$$

$$\varphi(1_R) = 1_S$$

תרגיל

יהי $\varphi: \mathbb{Q} \rightarrow \mathbb{Q}$ הומומורפיזם כך ש $\varphi(1) = 1$ אזי $\varphi := id$.

הוכחה

$$\varphi(n) = \varphi(\underbrace{1 + \dots + 1}_{n\text{-times}}) = \underbrace{\varphi(1) + \dots + \varphi(1)}_{n\text{-times}} = 1 + \dots + 1 = n \quad n \in \mathbb{N}$$

לכל הומומורפיזם מתקיים $\varphi(0) = 0$. ניתן להוכיח באופן הבא:

$$0 = \varphi(1 + (-1)) = \varphi(1) + \varphi(-1) = 1 + \varphi(-1) \rightarrow -1 = \varphi(-1)$$

ולכן לכל $n \in \mathbb{N}$ עבור $m \in \mathbb{N}$ נקבל

$$1 = \varphi(1) = \varphi\left(m \cdot \frac{1}{m}\right) = \varphi(m) \cdot \varphi\left(\frac{1}{m}\right) = m \cdot \varphi\left(\frac{1}{m}\right) \rightarrow \frac{1}{m} = \varphi\left(\frac{1}{m}\right)$$

$$\varphi\left(\frac{n}{m}\right) = \varphi(n) \cdot \varphi\left(\frac{1}{m}\right) = n \cdot \frac{1}{m} = \frac{n}{m}$$

הערה

התרגיל הנ"ל אינו בהכרח נכון עבור שדות אחרים. למשל: $\varphi: \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{2}]$ כך ש $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$ הוא איזומורפיזם כך ש $\varphi(1) = 1$ אבל $\varphi \neq id$.

תרגיל

יהי R חוג עם יחידה. הוכיחו ש $M_n(R[x]) \cong M_n(R)[x]$.

פתרון

תרגיל בית.

הגדרה

יהי $\varphi: R \rightarrow S$ הומומורפיזם.

נסמן את התמונה של φ ע"י $\text{Im } \varphi = \{\varphi(x) : x \in R\} \subset S$ תת חוג של S .

נסמן את הגרעין של φ ע"י $\text{Ker } \varphi = \{x \in R : \varphi(x) = 0\} \subset R$.

נשים לב שאם $\varphi \neq 0$ אז $1_R \notin \text{Ker } \varphi$ (אם קיים 1_R) מכיוון שעבור $\varphi: R \rightarrow \text{Im } \varphi$ נקבל ש

$$\varphi(1_R) = 1_S$$

$\text{Ker } \varphi$ הוא תת מרחב חיבורית:

אם $a, b \in \text{Ker } \varphi$ אז

$$\varphi(a) = \varphi(b) = 0 \rightarrow \varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0 \rightarrow a - b \in \text{Ker } \varphi$$

$$\text{אם } a \in \text{Ker } \varphi, r \in R \text{ אז } \varphi(r \cdot a) = \varphi(r) \cdot \varphi(a) = 0 \text{ ולכן } r \cdot a, a \cdot r \in \text{Ker } \varphi$$

הגדרה

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

1. I תת חבורה חיבורית.

2. לכל $i \in I, r \in R$ מתקיים $i \cdot r, r \cdot i \in I$.

נסמן $I \triangleleft R$.

I הוא אידיאל ימני אם:

1. I תת חבורה חיבורית.

2. לכל $i \in I, r \in R$ מתקיים $i \cdot r \in I$.

I הוא אידיאל ימני אם:

1. I תת חבורה חיבורית.

2. לכל $i \in I, r \in R$ מתקיים $r \cdot i \in I$.

הערה

בחוג קומוטטיבי נקבל שאידיאל ימני שווה לאידיאל שמאלי שווה לאידיאל דו צדדי.

דוגמאות

1. לכל הומומורפיזם $\varphi: R \rightarrow S$, $\text{Ker } \varphi$ הוא אידיאל של R .

2. האידיאלים היחידים של \mathbb{Z} הם מהצורה $n\mathbb{Z}$ מכיוון שאלו תת-החבורות החיבוריות

וגם לכל $m \in \mathbb{Z}, a \in n\mathbb{Z}$ קיים $b \in \mathbb{Z}$ כך ש $a = nb$ ואז $m \cdot a = m \cdot (nb) = n \cdot (mb) \in n\mathbb{Z}$.

3. יהי $x \in R$ אז הקבוצה $Rx = \{r \cdot x : r \in R\}$ היא אידיאל שמאלי. אם $a \in Rx$ אז קיים

$r \in R$ כך ש $a = r \cdot x$. יהי $s \in R$ $s \cdot a = s \cdot (r \cdot x) = (s \cdot r) \cdot x \in Rx$.

דוגמה לסעיף 3

יהי $R = M_2(\mathbb{Q})$, אז $e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

$I = \text{Re}_{12} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} : a, c \in \mathbb{Q} \right\}$ זהו אידיאל שמאלי

שאינו ימני מכיוון ש $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin I$

ובאותו אופן $I = \left\{ \begin{pmatrix} c & a \\ 0 & 0 \end{pmatrix} : a, c \in \mathbb{Q} \right\}$ הוא אידיאל ימני שאינו שמאלי של $M_2(\mathbb{Q})$.

4. יהי $R = \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$. אז $I := \{a + b\sqrt{5} : a \in 5\mathbb{Z}, b \in \mathbb{Z}\}$.

הוכחה לסעיף 4

I תת חבורה חיבורית (חישבו למה)

$$(c + d\sqrt{5})(5n + m\sqrt{5}) = 5nc + 5md + 5nd\sqrt{5} + mc\sqrt{5} = 5(nc + md) + (5nd + mc)\sqrt{5} \in I$$

מכיוון ש R קומוטטיבי נקבל ש $I \triangleleft R$.

5. יהי $A \subset M_n(R)$ ($n > 1$) קבוצת המטריצות המשולשיות עליונות, אז A הוא חוג עם

יחידה $I \subset A$ תהיי I קבוצת המטריצות המשולשיות עליונות עם

$$\begin{pmatrix} 1 & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 1 \end{pmatrix}$$

אפסים באלכסון – ז"א אם $(\alpha_{ij}) \in I$ אז לכל $1 \leq i \leq n$ $\alpha_{ii} = 0$. אז $I \triangleleft A$ (תרגיל

בית)

תרגיל

יהי $e_{22} \in A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. הוכיחו $e_{22}A$ הוא אידיאל ימני שאינו אידיאל שמאלי.

פתרון

תרגיל בית.