

למבוא אל תורת הרשתות - תרגיל 2

הצדקה:

יהי R חוג. המרכז (center) $Z(R)$ הוא $Z(R) = \{a \in R \mid \forall r \in R: ar = ra\}$

המרכז של תת-קבוצה $S \subseteq R$ (centralizer) הוא $C_R(S) = \{a \in R \mid \forall r \in S: ar = ra\}$

באגמא:

א. $C_R(S) = R, S \subseteq R$ $\Leftrightarrow Z(R) = R \Leftrightarrow R$ חילופי

ב. $Z(M_n(R)) = Z(R) \cdot I_n$

ג. $Z(H) = \mathbb{R}$

טענה:

יהי R חוג ו- $S \subseteq R$

א. $Z(R)$ תת-חוג חילופי של R

ב. $C_R(T) = R, T \subseteq R$ $\Leftrightarrow Z(R) = R \Leftrightarrow R$ חילופי

ג. $C_R(S)$ תת-חוג של R

ד. $S \subseteq C_R(C_R(S))$

ה. $C_R(C_R(C_R(S))) = C_R(S)$

ו. $C_R(Z(R)) = R, C_R(R) = Z(R)$

הומומורפיזמים

הצדקה:

יהיו R, S חוגים. פונקציה $\varphi: R \rightarrow S$ תיקרא הומומורפיזם של חוגים (homomorphism) אם

א. $\varphi(x+y) = \varphi(x) + \varphi(y)$

ב. $\varphi(xy) = \varphi(x)\varphi(y)$

ג. $\varphi(1_R) = 1_S$ (אם התכונה הישנה לא מתקיימת, נאמר ש- φ הוא

הומומורפיזם של חוגים בלי יחידה).

קואמורפס:

היו R, S שני חוגים ו $\varphi: R \rightarrow S$ שמוקדו $\varphi(r) = 0_S$ כל החומורפיזם של חוגים בלי יחידה

הגדרה:

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

א. אם φ חתוף, אומרים ש- φ חומורפיזם או איזומורפיזם.

ב. אם φ חתוף, אומרים ש- φ אפימורפיזם או הטלה.

ג. אם φ חתוף ו φ איזומורפיזם, אז $R \cong S$.

דוגמאות:

א. $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ המוקדו $\varphi(m) = m \pmod n$ הוא איזומורפיזם.

ב. $\varphi: \mathbb{C} \rightarrow \mathbb{C}$ המוקדו $\varphi(z) = \bar{z}$ הוא איזומורפיזם.

ג. נסמן A את אוסף המטריצות (הארכיוניות) ב- $M_2(\mathbb{R})$.

$$\varphi: A \rightarrow A, \quad \varphi \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

היא חומורפיזם של חוגים בלי יחידה. נלקח φ מבקרת נכשלת:

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

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

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

אם היינו מצמצמים את הטווה ל- $\left\{ \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix} \right\}$, כה היה חומורפיזם (ואפילו איזומורפיזם) (צריך לבדוק ש- φ גם מבקרת חיבור)

תרגיל:

יהיו R, S חוגים, והי $\varphi: R \rightarrow S$ אפימורפיזם של חוגים בלי יחידה. הוכיחו ש- φ אפימורפיזם של חוגים.

הוכחה:

φ אפימורפיזם, לכן קיים $a \in R$ כך ש- $\varphi(a) = 1_S$.

$$1_S = \varphi(a) = \varphi(a \cdot 1_R) \underset{\uparrow}{=} \varphi(a) \cdot \varphi(1_R) = 1_S \cdot \varphi(1_R) = \varphi(1_R)$$

φ מבקרת נכשלת

□

תרגיל:

יהי $\varphi: \mathbb{Q} \rightarrow \mathbb{Q}$ הומומורפיזם של חוגים. הוכיחו כי $\varphi = Id_{\mathbb{Q}}$.

הוכחה:

כיוון ש- φ הומומורפיזם של חוגים, לכל $n \in \mathbb{Z}$, $\varphi(n) = n$.
כן $\varphi(1) = 1$ וכן $\varphi(-1) = -1$.

יהי $\frac{m}{n} \in \mathbb{Q}$.

$$n \cdot \varphi\left(\frac{m}{n}\right) = \underbrace{\varphi\left(\frac{m}{n}\right) + \dots + \varphi\left(\frac{m}{n}\right)}_{n \text{ פעמים}} = \varphi\left(\underbrace{\frac{m}{n} + \dots + \frac{m}{n}}_{n \text{ פעמים}}\right) = \varphi(m) = m$$
$$\Downarrow$$
$$\varphi\left(\frac{m}{n}\right) = \frac{m}{n}$$

□

שאלה:

רשמו את האחרים שהם לא נכונים! האינו אף $\varphi \neq Id_{\mathbb{C}}$, $\varphi: \mathbb{C} \rightarrow \mathbb{C}$
 $z \mapsto \bar{z}$

זכרו $\mathbb{Q}[\sqrt{2}]$ קומוטטיבי, $\varphi: \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{2}]$ איזומורפיזם (הקטן!)
 $a + b\sqrt{2} \mapsto a - b\sqrt{2}$

הצגה:

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

א. $Im \varphi = \{\varphi(x) \mid x \in R\}$ תת-חוג של S .

ב. $ker \varphi = \{x \in R \mid \varphi(x) = 0\}$ תת-חוג בתו יחידה של R .

ג. אם $R = S$, נקרא φ אנדומורפיזם. אם $R = S$ ו- φ איזומורפיזם, נאמר ש- φ איזומורפיזם.

$ker \varphi$ חלקים בתת-חוגה: אם $a \in ker \varphi$ ו- $r \in R$, אז $ra \in ker \varphi$.

הצגה:

יהי R חוג, ותהי $I \subseteq R$ תת-חבורה חיבורית.

א. I איזאל שטתו של R , נסמן $I \leq R$ או לפעמים $I \leq R$, אם

לכל $r \in R$ ו- $a \in I$, $ra \in I$.

$a \in I \Rightarrow \exists r \in R, a \in I$ \Leftrightarrow $a \in I$ \Leftrightarrow $\exists r \in R, a = r$ \Leftrightarrow $a \in R$.
 \Rightarrow $I = R$ \Leftrightarrow $a \in I \Rightarrow a \in R$.

החוג חילופי \Leftrightarrow ההגדרה האלו מתקבלת.

דוגמה:

א. $\{0\} \triangleleft R$ \Leftrightarrow $\{0\}$ חוג R . (האיזום הטריוויאלי)

$R \triangleleft R$

ב. $I \triangleleft R, I \subsetneq R$ \Leftrightarrow I איזום נכון/אמיתי (proper).

$\varphi: R \rightarrow S$ \Leftrightarrow $\ker \varphi \triangleleft R$.

$\varphi: R \rightarrow R/I$ \Leftrightarrow $\ker \varphi = I$.

ג. האיזום היתר $\mathbb{Z} \rightarrow \mathbb{Z}$ \Leftrightarrow \mathbb{Z} .

ד. $a \in R$ \Leftrightarrow a חוג R .

$a \in R \Leftrightarrow Ra = aR$ \Leftrightarrow a איזום ראשוני a .

$a \in R \Leftrightarrow aR = Ra$ \Leftrightarrow a איזום ראשוני a .

(הגדרה):
 איזום ראשוני $a \in R$ \Leftrightarrow a ראשוני (principal), $a \neq 0$.
 $I = RaR = \left\{ \sum_{i=1}^n r_i a s_i \mid r_i, s_i \in R \right\}$

דוגמה:

$R = M_2(\mathbb{Q})$ \Leftrightarrow R איזום ראשוני e_{12} .

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

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

e_{12} איזום ראשוני? \Leftrightarrow $e_{12} \notin Re_{12}$.

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin Re_{12}$$

\uparrow \uparrow
 R R

תרגיל: (הקדמה)

החוג $\mathbb{Z}[\sqrt{5}]$ איננו שדה אבל \mathbb{Z} הוא חבורה תחת הכפל.

תרגיל:

$I \triangleleft R$ הוא $I = \{a+b\sqrt{5} \mid a \in 5\mathbb{Z}, b \in \mathbb{Z}\}$, $R = \mathbb{Z}[\sqrt{5}] = \{a+b\sqrt{5} \mid a, b \in \mathbb{Z}\}$
הוכחה:

$I \subseteq R$ תת-חבורה תחת חיבור $(a+b\sqrt{5}) + (c+d\sqrt{5}) = (a+c) + (b+d)\sqrt{5} \in I$

(נראה בקלות מימין (חספוק, כי R חילופי). יהי $a+b\sqrt{5} \in R$, $5c+d\sqrt{5} \in I$

$$(5c+d\sqrt{5})(a+b\sqrt{5}) = \underbrace{(5ac+5bd)}_{5\mathbb{Z}} + \underbrace{(5bc+ad)}_{\mathbb{Z}}\sqrt{5} \in I$$

כיוון R -חילופי, נובע $I \triangleleft R$.

תרגיל:

יהיו $a, b \in \mathbb{N}$. הוכיחו $b\mathbb{Z} \subseteq a\mathbb{Z} \iff a|b$

הוכחה:

\Leftarrow אם $a|b$ אז $b=na$ לכל $n \in \mathbb{N}$. יהי $bme \in b\mathbb{Z}$.

$b\mathbb{Z} \subseteq a\mathbb{Z}$ מכיון $bm = a(nm) \in a\mathbb{Z}$.

\Rightarrow אם $b\mathbb{Z} \subseteq a\mathbb{Z}$, בפרט $ba \in a\mathbb{Z}$, מכאן $ba = an$ ל- $n \in \mathbb{N}$ קיים $a|b$.

תרגיל:

יהי R חוג, ויהי $I \triangleleft R$. הוכיחו שאם $1 \in I$, אז $I=R$.

הוכחה:

אם איננו מניחים ש- $1 \in I$ אז איבדנו דבר.

הוכחה:

החוג \mathbb{Z} חילופי ש- $1 \in \mathbb{Z}$ הוא טריוויאלי.

חוג נ/ה

הגדרה:

יהי R חוג ויהי $I \triangleleft R$ אידיאל. חוג החניה הוא הקבוצה

$$R/I = \{a + I \mid a \in R\}$$

על הפעולות

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

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

$$0_{R/I} = 0 + I$$

$$1_{R/I} = 1 + I$$

דוגמה:

$$I = 18\mathbb{Z}, R = 3\mathbb{Z}$$

$$R/I = \{0+18\mathbb{Z}, 3+18\mathbb{Z}, 6+18\mathbb{Z}, 9+18\mathbb{Z}, 12+18\mathbb{Z}, 15+18\mathbb{Z}\}$$

החבורה החיבורית של $R/I \cong \mathbb{Z}_6$.

האם זה נכון גם לחבורה של החוג? אולי לא!

.	0	3	6	9	12	15
0	0	0	0	0	0	0
3	0	9	0	9	0	9
6	0	0	0	0	0	0
9	0	9	0	9	0	9
12	0	0	0	0	0	0
15	0	9	0	9	0	9

עם זאת איננו חבורה \mathbb{Z}_6 !

אזכור! במקום \mathbb{Z}_n לכתוב $\mathbb{Z}/n\mathbb{Z}$!

דוגמה:

לכל p ראשוני $\mathbb{Z}/p\mathbb{Z} = \{p\mathbb{Z}, 1+p\mathbb{Z}, \dots, (p-1)+p\mathbb{Z}\} \cong \mathbb{F}_p$

הוכחה

$$I = \langle x^2 + 1 \rangle = \left\{ f(x) \cdot (x^2 + 1) \mid f(x) \in \mathbb{R}[x] \right\}, \quad R = \mathbb{R}[x]$$

$R \cdot (x^2 + 1) \cdot R$

$$\bar{a} = a + I \in R/I \quad \forall a \in \mathbb{R}$$

$$x^2 + I = x^2 - (x^2 + 1) + I = -1 + I$$

$$\bar{x}^2 = \bar{x}^2 = \bar{-1} \quad \leftarrow$$

$$\dots \bar{x}^4 = \bar{1}, \quad \bar{x}^3 = -\bar{x}$$

$$R/I = \{ \bar{a} + \bar{b}\bar{x} \mid a, b \in \mathbb{R} \} \cong \mathbb{C}$$

$$\bar{a}_n = a_n + I$$

$$a_0 + a_1 x + \dots + a_n x^n = \bar{a}_0 + \bar{a}_1 \bar{x} + \dots + \bar{a}_n \bar{x}^n \quad \bar{x}^2 = -1$$

הוכחה

$$\mathbb{R}[x] / \langle x^2 + 1 \rangle \cong \mathbb{R}$$

$$\bar{x}^2 = \bar{1}, \quad \bar{x} = \bar{-1}$$

$$x^2 + \langle x^2 + 1 \rangle = (x + \langle x^2 + 1 \rangle)^2 = (-1 + \langle x^2 + 1 \rangle)^2 = 1 + \langle x^2 + 1 \rangle$$

תוצאה

האם R/I היא תחום? $I = \langle x^2 + 1 \rangle, R = \mathbb{Z}/3\mathbb{Z}[x]$

פתרון

$$|R/I| = 9 \quad \text{כאשר} \quad R/I = \{ a + b\bar{x} \mid a, b \in \mathbb{Z}/3\mathbb{Z} \}$$