מבנים דיסקרטיים – תרגול 12

חוגים, הומומורפיזמים, אידאלים

תרגיל:

הראו שאם $a\in\mathbb{Z}_n$ כך ש $\gcd(a,n)\neq 1$ אזי a אינו הפיך.

פתרון:

אם $\gcd(a,n)=d\neq 1$ אזי $a=da'$, כך ש $\gcd(a',n)=1$. נכפול את שני האגפים ב $\frac{n}{d}$ ונקבל $\frac{n}{d}a=na'\equiv 0 \pmod n$. נשים לב שבהכרח $\frac{n}{d}\not\equiv 0 \pmod n$, כי $\frac{n}{d}<n$, ולכן a מחלק 0 ב $\mathbb{Z}_n$ ולכן אינו הפיך.

הגדרה

יהיו R,S חוגים נאמר כי $\varphi:R\to S$ הומומורפיזים 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 שההומומופיזים יוניטרי.

דוגמאות

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

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

אזי φ הומומורפיזם:

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

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

אבל עבור ההומורפיזים $\varphi:A\to\operatorname{Im}\varphi$ כאשר $\varphi\begin{pmatrix}a&0\\0&b\end{pmatrix}=\begin{pmatrix}a&0\\0&0\end{pmatrix}$ מתקיים

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

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

<u>תרגיל</u>

יהיו S,R חוגים עם יחידה ויהי $\varphi:R\to S$ הומ' על. הראו שמתקיים $\varphi(1_R)=1_S$. כלומר φ יוניטרי.

<u>פתרון</u>

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

$a=\varphi(b)=\varphi(b\cdot 1_R)=\varphi(b)\cdot\varphi(1_R)=a\cdot\varphi(1_R)$ קיבלנו שלכל $a\in S$ $a=a\cdot\varphi(1_R)$ ז"א $\varphi(1_R)=1_S$.

<u>תרגיל</u>

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

<u>פתרון</u>

יהי $n\in\mathbb{N}$. $\varphi(n)=\varphi\left(\overset{n-times}{1+...+1}\right)=\overset{n-times}{\varphi(1)+...+\varphi(1)}=\overset{n-times}{1+...+1}=n$.

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

לכן $0=\varphi(1+(-1))=\varphi(1)+\varphi(-1)=1+\varphi(-1)\to -1=\varphi(-1)$

ולכן $\varphi(-n)=-n$ לכל $n\in\mathbb{N}$. עבור $m\in\mathbb{N}$ נקבל

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

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

<u>הערה</u>

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

<u>הגדרה</u>

יהי $\varphi:R\to S$ הומומורפיזם.

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

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

<u>הגדרה</u>

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 $I\lhd R$.

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 $r\cdot i\in I$.

<u>הערה</u>

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

<u>דוגמאות</u>

1. לכל הומומורפיזם $\varphi: R\to S$, $Ker\varphi$ 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 $e_{12}=\begin{pmatrix}0&1\\0&0\end{pmatrix}$

$I=\mathrm{Re}_{12}=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\cdot\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&a\\0&c\end{pmatrix}\right\}=\left\{\begin{pmatrix}0&a\\0&c\end{pmatrix}: a,c\in\mathbb{Q}\right\}$ 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 $R=\mathbb{Z}\left[\sqrt{5}\right]=\left\{a+b\sqrt{5}: a,b\in\mathbb{Z}\right\}$. $I:=\left\{a+b\sqrt{5}: a\in 5\mathbb{Z}, b\in\mathbb{Z}\right\}$ אז $I\lhd R$.

הוכחה לסעיף 4

I תת חבורה חיבורית (חישבו למה)

$\left(c+d\sqrt{5}\right)\left(5n+m\sqrt{5}\right)=5nc+5md+5nd\sqrt{5}+mc\sqrt{5}=5\left(nc+md\right)+\left(5nd+mc\right)\sqrt{5}\in I$ מכיוון ש R קומוטטיבי נקבל ש $I\lhd R$.

5. יהי $A\subset M_n\left(R\right)$ $(n>1)$ קבוצת המטריצות המשולשיות עליונות, אז A הוא חוג עם יחידה $\begin{pmatrix}1 & . & . & . & 0\\ & . & . & & .\\ & . & & . & .\\ & . & & . & .\\ 0 & . & . & . & 1\end{pmatrix}$. תהיי $I\subset A$ קבוצת המטריצות המשולשיות עליונות עם אפסים באלכסון – ז"א אם $\left(\alpha_{ij}\right)\in I$ אז לכל $1\le i\le n$ $\alpha_{ii}=0$. אז $I\lhd A$ (**תרגיל בית)**

<u>תרגיל</u>

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

<u>פתרון</u>

תרגיל בית.

<u>תרגיל</u>

יהי R חוג עם יחידה, $I\lhd R$. אם $1_R\in I$ אז $I=R$.

<u>פתרון</u>

על פי הגדרת אידיאל לכל $r\in R,i\in I$ $r\cdot i\in I$. יהי $r\in R$, מכיוון ש $1_R\in I$ אז $r=r\cdot 1_R\in I$, ולכן $R\subseteq I$ ועל פי הגדרת אידיאל $I\subseteq R$.

<u>הערה</u>

אם יש ב I איבר הפיך אז $I=R$. אם $i\in I$ הפיך אז $1_R=i\cdot i^{-1}\in I$ ומהתרגיל נקבל ש $I=R$.

<u>הגדרה</u>

יהי R אם $I=\{0\}\vee R$ נאמר ש I אידיאל טריוויאלי