מבנים דיסקרטיים – תרגול 10

תרגיל: מצאו איבר הפיך (כפלית), ואיבר לא הפיך (כפלית) השונה מ 0 ב $\mathbb{Z}_4[x]$.

פיתרון:

נראה כי $1+2x$ הוא הפיך: $(1+2x)(1-2x)=1-4x^2=1$.

2 אינו איבר הפיך ב $\mathbb{Z}_4[x]$ כי נניח שקיים איבר הפכי ל 2, אזי $2a=1$. נכפיל את שני האגפים ב 2, ונקבל $0=4a=2$, סתירה כי $0\neq 2$.

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

הערה: מספיק להוכיח ש S תת-חבורה חיבורית ותת-אגודה כפלית של R.

תרגיל:

1. יהי חוג R (לאו דוקא עם יחידה) ויהי $0\neq q\in R$. הוכח כי qRq תת-חוג של R.
2. נניח ש $q^2=q$ [איבר כזה נקרא **אידמפוטנט**]. הוכח כי q הוא איבר היחידה ב qRq.

פתרון:

1. בוודאי ש qRq הוא תת-קבוצה. צריך להוכיח ש qRq תת-חבורה חיבורית של R: qRq אינה ריקה, כי $0=q0q\in qRq$. בנוסף $qaq-qbq=q(aq-bq)=q(a-b)q\in qRq$. תת-אגודה: $(qaq)(qbq)=q(aq^2b)q\in qRq$.
2. קודם כל $q=q^2=qq=qq^2=qqq\in qRq$. בנוסף, מתקיים $q(qaq)=q^2aq=qaq$ ובצורה דומה מראים ש q יחידה מימין.

דוגמאות:

ייתכן שלחוג עם יחידה יש תת-חוג ללא יחידה (לדוגמה $2\mathbb{Z}$ הוא תת-חוג של $\mathbb{Z}$ אך ללא יחידה).

ייתכן שלחוג עם יחידה יש תת-חוג עם יחידה אחרת. לדוגמה

$\left\{\begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix}\right\}$ הוא תת-חוג של $M_2(\mathbb{C})$ והיחידה שלו היא $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

הגדרות:

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

דוגמאות:

1. $\mathbb{Z}$ הוא תחום שלמות.
2. $\mathbb{Z}_6$ איננו תחום משום שהוא מכיל מחלקי אפס 2 ו3.
3. חוג עם חילוק הוא תמיד תחום: אם $a, b \neq 0$ אזי $ab = 0 \Rightarrow a^{-1}ab = 0 \Rightarrow b = 0$, סתירה.

תרגיל:

הראו שלכל חוג קומוטטיבי עם יחידה R ו$n > 1$, $M_n(R)$ איננו תחום.

פתרון:

מספיק להראות ש $M_2(R)$ אינו תחום, כי אם יש מחלק אפס A ב $M_2(R)$ אזי ניתן לבנות מחלק 0 ב $M_n(R)$ ע"י מטריצת בלוקים $\begin{pmatrix} A & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$.

ב $M_2(R)$ תמיד מתקיים $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = 0$.

תרגיל: הראו שאם R שדה, אזי $A \in M_n(R)$ מחלקת 0 אם ורק אם $|A| = 0$. האם הדבר נכון עבור חוג קומוטטיבי R כללי?

פתרון: <= אם $|A| \neq 0$ אזי A הפיכה ואזי A אינה מחלקת 0 (נכון בכל חוג).

<= אם A אינה מחלקת 0, אזי $|A|\cdot I = A\cdot Adj(A)\neq 0$ ומכאן נקבל ש $|A|\neq 0$.

בחוג כללי הטענה אינה נכונה, ניקח לדוגמה $R=\mathbb{Z}_8$, ואת $M_2(R)$.

אזי $\left|\begin{pmatrix}2&0\\0&2\end{pmatrix}\right| = 4\neq 0$ אבל $\begin{pmatrix}0&0\\0&0\end{pmatrix} = \begin{pmatrix}8&0\\0&8\end{pmatrix} = \begin{pmatrix}2&0\\0&2\end{pmatrix}^3$ ולכן $\begin{pmatrix}2&0\\0&2\end{pmatrix}$ מחלק 0.

<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 $I\triangleleft R$.

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 $r\cdot i\in I$.

<u>הערה</u>

1. בחוג קומוטטיבי נקבל שאידיאל ימני שווה לאידיאל שמאלי שווה לאידיאל דו צדדי.
2. כל אידאל הוא תת-חוג (ללא יחידה).

<u>דוגמאות</u>

1. 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 $m\cdot a = m\cdot(nb) = n\cdot(mb)\in n\mathbb{Z}$.

2. 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 2

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

$I=\mathrm{Re}_{12}=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\cdot\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&a\\0&c\end{pmatrix}\right\}=\left\{\begin{pmatrix}0&a\\0&c\end{pmatrix}: a,c\in\mathbb{Q}\right\}$ 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 $M_2(\mathbb{Q})$.

3. 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 $I\triangleleft R$.

הוכחה לסעיף 3

I תת חבורה חיבורית (חישבו למה)

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

4. יהי $A\subset M_n(R)$ $(n>1)$ 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 $(\alpha_{ij})\in I$ אז לכל $1\le i\le n$ $\alpha_{ii}=0$. אז $I\triangleleft A$ (**תרגיל בית**)