מבנים דיסקרטיים - תרגול 11

תחומים אוקלידיים, אידאלים

תרגיל: יהי R חוג קומוטטיבי. נניח ש $a|b$ כלומר קיים $c\in R$ כך ש $b=ac$.
הראו שאם $u\in R$ הפיך (כפלית) אזי $(au)|b$.

הערה: 0 אינו מחלק של אף מספר חוץ מאפס, כל מספר מחלק את 0.

תרגיל: יהי R תחום שלמות. אם $a|b$ וגם $b|a$ אזי $a=ub$ עבור איבר הפיך $u\in R$.

הגדרה: יהי R תחום שלמות. נאמר ש $a,b\in R$ חברים ונסמן $a\sim b$ אם מתקיים $a|b$ וגם $b|a$.

הגדרה לא פורמלית: תחום אוקלידי הוא תחום שלמות (חוג קומוטטיבי ללא מחלקי אפס) שבו יש חלוקה עם שארית.

אנחנו מכירים שני חוגים עיקריים בהם זה מתקיים:

1. חוג המספרים השלמים: $\mathbb{Z}$

לפי **משפט אוקלידס**, לכל שני מספרים $a,b\in\mathbb{Z}$ וגם $b\neq 0$ קיימות מנה q ושארית r כך ש $a=bq+r$, ומתקיים $|r|<|b|$. ניתן לדרוש דרישה חזקה יותר $0<r<|b|$, ואז נקבל שהשארית והמנה נקבעות ביחידות.

דוגמאות: $7=3\times 2+1$ (מנה 3, שארית 1). $7=(-3)\times(-2)+1$ (מנה -3 שארית 1).

2. חוג פולינומים $F[x]$ מעל שדה F:

לכל שני פולינומים $f,g\in F[x]$ כך ש $g\neq 0$ קיימות מנה $q\in F[x]$ ושארית $r\in F[x]$ כך ש $f=qg+r$ ומתקיים $\deg(r)<\deg(b)$.

דוגמה:

$$
\begin{array}{r|l}
 & x^3+x^2\quad -1 \\
\hline
x^3+x+1 & x^6+x^5+x^4+x^3+x^2+x+1 \\
 & -x^6\quad -x^4-x^3 \\
\hline
 & x^5\quad +x^2 \\
 & -x^5\quad -x^3-x^2 \\
\hline
 & -x^3\quad +x+1 \\
 & x^3\quad +x+1 \\
\hline
 & 2x+2
\end{array}
$$

הגדרה: בחוג קומוטטיבי R **מחלק משותף מקסימלי** gcd של שני איברים $a,b\in R$ (כך שלפחות אחד שונה מאפס) הוא איבר $d\in R$ המקיים $d\mid a$ וגם $d\mid b$ (כלומר d **מחלק משותף** של a,b) ואם קיים מחלק משותף אחר $d'\in R$ המקיים $d'\mid a$ וגם $d'\mid b$ אזי אזי $d'\mid d$. כפולה משותפת מינימלית.

הערה: מחלק משותף מקסימלי נקבע עד כדי כפל באיבר הפיך בחוג. לדוגמה המחלקים המשותפים המקסימליים של $2,6$ ב $\mathbb{Z}$ הם ± 2 . בחוג השלמים $\mathbb{Z}$ ניתן "לשפר" את ההגדרה ולקבל יחידות gcd (פשוט דורשים שהוא יהיה אי-שלילי).

דוגמא:

$$\gcd(6,4)=2,\ \gcd(6,12)=6,\ lcm(2,3)=6,\ lcm(2,4)=4$$

תרגיל: אם d הוא gcd של a,b אזי d הוא gcd של b,r.

דוגמה:

$$x^3-2x^2+1=(x^2-x-3)\cdot(x-1)+(2x-2)$$
$$x^2-x-3=\quad(2x-2)\quad\cdot\quad\tfrac{1}{2}x\quad+-3$$
$$2x-2=\quad-3\quad\cdot\quad(-\tfrac{2}{3}x+\tfrac{2}{3})\quad+0$$

דוגמא: נפעיל את אלגוריתם הבניה עבור הדוגמא: gcd(234,61)=1.

$$234=61\times3+51$$

$$61=51\times1+10$$

$$51=10\times5+1$$

$$10=1\times10$$

ואז נקבל:

$$\gcd(234,61)=\gcd(61,51)=\gcd(51,10)=\gcd(5,1)=1.$$

את הצירוף הלינארי המתאים נקבל כמו בהוכחה ע"י הצגת כל שארית כצירוף אלגברי מתאים של השאריות הקודמות:

$$1=51-10\times5$$
$$10=61-51\times1$$
$$51=234-61\times3$$
$$\Rightarrow$$
$$1=51-10\times5=(234-61\times3)-(61-51\times1)\times5=(234-61\times3)-(61-(234-61\times3)\times1)\times5=$$
$$=6\times234+(-23)\times61$$

<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>

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 $R=M_2(\mathbb{Q})$, 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 $M_2(\mathbb{Q})$.

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 $I\lhd R$.

הוכחה לסעיף 3

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 $I\lhd R$.

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 $\left(\alpha_{ij}\right)\in I$ אז לכל $1\le i\le n$ $\alpha_{ii}=0$. אז $I\lhd A$ (**תרגיל בית**)