אלגברה מופשטת 2 – תרגיל כיתה 3

מתרגלים: ד"ר אפי כהן ואדם צ'פמן.

תרגיל

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

פתרון

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 $I \subseteq R$.

הערה

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 $I = R$.

הגדרה

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

מסקנה

בחוג עם חילוק אין אידיאלים לא טריוויאלים.

תרגיל

יהיו $m, n \in \mathbb{N}$. $n|m \leftrightarrow m\mathbb{Z} \subseteq n\mathbb{Z}$.

פתרון

$\Leftarrow$

נתון ש $n|m$, ז"א קיים $a \in \mathbb{Z}$ כך ש $na = m$. יהי $b \in m\mathbb{Z}$ ז"א קיים $k \in \mathbb{Z}$ כך ש $b = mk = (na)k = n(ak) \in n\mathbb{Z}$.

$\Rightarrow$

נתון ש $m\mathbb{Z} \subseteq n\mathbb{Z}$ ובפרט $m \in n\mathbb{Z}$, ז"א קיים $a \in \mathbb{Z}$ כך ש $na = m$.

<u>טענה</u>

אם I,J אידיאלים אז $I\cap J$ אידיאל.

<u>הוכחה</u>

יהי $r\in R$ ויהי $k\in I\cap J$. מכיוון ש $k\in I$ אז $k\cdot r\in I$ ו מכיוון ש $k\in J$ אז $k\cdot r\in J$ ז"א $k\cdot r\in I\cap J$.

<u>הגדרה</u>

יהיו I,J אידיאלים נגדיר $I+J:=\left\{i+j \middle| i\in I, j\in J\right\}$.

נשים לב ש $I+J$ אידיאל.

<u>דוגמא</u>

$m\mathbb{Z}\cap n\mathbb{Z}=L.c.d\left(m,n\right)\mathbb{Z}, m\mathbb{Z}+n\mathbb{Z}=g.c.d\left(m,n\right)\mathbb{Z}$.

<u>הגדרה</u>

יהי R חוג עם יחידה, $x\in R$ אז הקבוצה $\left\langle x\right\rangle=\left\{\sum_{i=1}^{n}\alpha_i x\beta_i \middle| \alpha_i,\beta_i\in R, n\in\mathbb{N}\right\}$

היא אידיאל ונקראת האידיאל הנוצר ע"י x, וזהו האידיאל המינימאלי שמכיל את x.

אם ניקח קבוצת איברים $\left\{x_i\right\}_{i=1}^{r}$, $x_i\in R$ אז נגדיר- $\left\langle x_1,\dots,x_r\right\rangle=\left\langle x_1\right\rangle+\dots+\left\langle x_r\right\rangle$.

- $\left\langle x\right\rangle$ הוא אכן אידיאל: אם $r\in R$ אז

$$r\cdot\left(\sum_{i=1}^{n}\alpha_i x\beta_i\right)=\sum_{i=1}^{n}\left(r\alpha_i\right)x\beta_i\in\left\langle x\right\rangle,\left(\sum_{i=1}^{n}\alpha_i x\beta_i\right)\cdot r=\sum_{i=1}^{n}\alpha_i x\left(\beta_i\cdot r\right)\in\left\langle x\right\rangle$$

- $\left\langle x\right\rangle$ הוא אידיאל מינימאלי: ז"א אם $I\lhd R$, $x\in I$ אז $\left\langle x\right\rangle\subseteq I$.

אם $\sum_{i=1}^{n}\alpha_i x\beta_i\in\left\langle x\right\rangle$ אז לכל $1\le i\le n$ $\alpha_i x\in I$ ולכן $\left(\alpha_i x\right)\beta_i\in I$ מכיוון ש I

סגור לחיבור נקבל ש $\sum_{i=1}^{n}\alpha_i x\beta_i\in I$

הערה

בחוג קומוטטיבי מתקיים $\langle x\rangle = xR = Rx$.

שימו לב שהשוויון מתקיים גם אם החוג לא קומוטטיבי אבל $x \in Z(R)$.

דוגמא

עבו $\mathbb{Z}[x]$ מתקיים: $\langle 2,x\rangle = \left\{2f(x)+xg(x) \middle| f(x),g(x)\in\mathbb{Z}[x]\right\}$

תרגיל

מצאו חוג לא קומוטטיבי R כך ש $Rx \neq \langle x\rangle$.

הגדרה

יהיו I,J אידיאלים נגדיר $IJ = \left\{\sum i_n j_n \middle| i_n \in I, j_n \in I\right\}$. (הסכום סופי, הראו בהרצאה ש IJ אידיאל)

הערה

שימו לב שאם I,J אידיאלים לא בהכרח שהקבוצה $\left\{i\cdot j \middle| i\in I, j\in J\right\}$ אידיאל.

למשל: יהיו $I=\langle 2,x\rangle, J=\langle 3,x\rangle$ בחוג $\mathbb{Z}[x]$.

נוכיח שהקבוצה $S=\left\{f\cdot g \middle| f\in I, g\in J\right\}$ אינה אידיאל.

$f=2f_1+f_2, g=3g_1+g_2$ כך ש $f_1,f_2,g_1,g_2\in\mathbb{Z}[x]$.

עבור $f=2, g=3$ נקבל ש $6\in S$. $f=g=x$ נקבל ש $x^2\in S$. נוכיח ש $S \not\ni 6+x^2$. נניח בשלילה ש $6+x^2\in S$ ז"א קיימים $f_1,f_2,g_1,g_2\in\mathbb{Z}[x]$ כך ש

$$(2f_1+xf_2)(3g_1+xg_2)=6+x^2 \rightarrow 6f_1g_1+(2f_1g_2+3f_2g_1)x+f_2g_2x^2=6+x^2$$

לכן
$$\begin{array}{l} f_1g_1=1, f_2g_2=1, 2f_1g_2+3f_2g_1=0 \\ f_1g_1=1 \rightarrow f_1=g_1=\pm1 \\ f_2g_2=1 \rightarrow f_2=g_2=\pm1 \end{array}$$
ולכן לא ייתכן $2f_1g_2+3f_2g_1=0$

הגדרה

יהי R חוג עם יחידה, $I,J \lhd R$. נאמר ש I,J קו – מקסימאליים אם $I+J=R$.

טענה

1. $IJ \subseteq I \cap J$.
2. אם R חוג קומוטטיבי עם יחידה, I,J אידיאלים קו מקסימאליים אז $IJ = I \cap J$.

הוכחה

1. מיידי.
2. מכיוון ש $I+J=R$ קיימים $i \in I, j \in J$ כך ש $i+j=1_R$ יהי $a \in I \cap J$.

$a = a \cdot 1 = a(i+j) = a \cdot i + a \cdot j = i \cdot a + a \cdot j \in IJ$.

דוגמא

עבור $2\mathbb{Z}, 3\mathbb{Z} \lhd 6\mathbb{Z}$ נקבל ש

$$1 = 3 \cdot 1 + 2 \cdot (-1) \to 1 \in 2\mathbb{Z} + 3\mathbb{Z} \to 2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$$
$$2\mathbb{Z} \cap 3\mathbb{Z} = 2\mathbb{Z} \cdot 3\mathbb{Z} = 6\mathbb{Z}$$.

תרגיל

הוכיחו ש $\langle 2x-1 \rangle, \langle x-1 \rangle$ הם קו-מקסימאליים ב $\mathbb{Z}[x]$.

הגדרה

I נקרא אידיאל ראשי אם קיים $x \in R$ כך ש $I = \langle x \rangle$.

R הוא חוג ראשי אם כל אידיאל ב R הוא ראשי.

תרגיל

הוכיחו כי $\mathbb{Z}[x]$ אינו חוג ראשי.

פתרון

נסתכל על האידיאל $\langle 2,x \rangle \lhd \mathbb{Z}[x]$. $h(x) = 2f(x) + xg(x) \in \mathbb{Z}[x]$ ולכן

$h(0) \in 2\mathbb{Z}$ ז"א $1 \notin \langle 2,x \rangle$ ולכן $\langle 2,x \rangle \subset \mathbb{Z}[x]$.

נניח שקיים $q\in\mathbb{Z}[x]$ כך ש $\langle q\rangle=\langle 2,x\rangle$ אז $2\in\langle q\rangle, x\in\langle q\rangle$ ז"א קיימים שני

פולינומים n,m כך ש $x=qn, 2=qm$ ז"א q הוא מחלק משותף ב $\mathbb{Z}[x]$ של 2 ו x.

קיבלנו ש $q=\pm 1$ ז"א $\langle q\rangle=\mathbb{Z}[x]$ וקיבלנו סתירה.

<u>הערה</u>

שימו לב ש $\langle 2,x\rangle$ ב $\mathbb{Q}[x]$ הוא כן ראשי, כי

$$\langle 2,x\rangle=\langle 2\rangle+\langle x\rangle=\mathbb{Q}[x]+\langle x\rangle=\mathbb{Q}[x]=\langle 1\rangle$$

<u>תרגיל בית</u>

הוכיחו שבחוג $\mathbb{Q}[x,y]$, האידיאל $\langle x,y\rangle$ אינו ראשי.

<u>דוגמאות</u>

1. $\mathbb{Z}_n$ הוא חוג ראשי – האידיאל מהצורה $m\mathbb{Z}_n$ $m|n$.
2. $\mathbb{Z}$ הוא חוג ראשי – האידיאל מהצורה $m\mathbb{Z}$.
3. אם D חוג אם חילוק אז $D[[x]]$ הוא חוג ראשי. כל אידיאל הוא מהצורה $\langle x^n\rangle$ או $\{0\}$.
4. $H[[x]]$ הוא חוג ראשי שאינו קומוטטיבי.

<u>הגדרה</u>

R יקרא חוג פשוט אם אין לו אידיאלים פרט ל R ול $\{0\}$.

<u>הערה</u>

- חוג עם חילוק הוא חוג פשוט.
- חוג קומוטטיבי עם יחידה ופשוט הוא שדה. מכיוון שאם $0\neq x\in R\to Rx=R$ ואז לכל איבר בחוג יש הופכי. (Rx הוא אידיאל מכיוון שהחוג קומוטטיבי, מכיוון שהחוג פשוט $Rx=R$ מכיוון שהחוג עם יחידה $1_R\in Rx$ ז"א קיים $y\in R$ כך ש $yx=1_R$ ומהקומוטטיביות נקבל ש $xy=1_R$.

<u>תזכורת</u>

אם D חוג עם חילוק אז $Z(D)$ שדה.

<u>טענה</u>

אם R חוג פשוט עם יחידה אז $Z(R)$ שדה.

<u>הוכחה</u>

ראינו ש $Z(R)$ תת חוג קומוטטיבי. יהי $0 \neq x \in Z(R)$. מכיוון ש R חוג פשוט נקבל ש $R = Rx = xR = \langle x \rangle$. R חוג פשוט ולכן הפיך נשאר להוכיח ש $x^{-1} \in Z(R)$.

עבור $r \in R$ מתקיים

$$xr = rx \to x^{-1}xr = x^{-1}rx \to r = x^{-1}rx \to rx^{-1} = x^{-1}r \to x^{-1} \in Z(R)$$

<u>משפט</u>

יהי $I \lhd R$ אז $M_n(I) \lhd M_n(R)$ וכל אידיאל של $M_n(R)$ הוא מהצורה הזו.

<u>דוגמא</u>

$$M_n(2\mathbb{Z}) \lhd M_n(\mathbb{Z})$$

אם R הוא חוג עם חילוק, למשל:הממשיים, הרציונלים, אז ל R אין אידיאלים ולכן $M_n(R)$ הוא חוג פשוט עם יחידה ולכן $Z(M_n(R))$ הוא שדה שאיזומורפי ל $Z(R)$.

<u>הערה</u>

יהי $A \subseteq M_n(R)$ תת חוג, $I \lhd A$. האם בהכרח קיים $J \lhd R$ כך ש $I = A \cap M_n(J)$? לא.

A – מטריצות משולשיות עליונות ב $M_n(\mathbb{Z})$. I מטריצות ב A עם אלכסון שווה לאפס.

אז לא קיים J כך ש $J \lhd R$ ו $I = A \cap M_n(J)$ מכיוון ש $I = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}$ ואילו אידיאל של $M_2(\mathbb{Z})$ הוא $M_2(n\mathbb{Z})$.

<u>תרגיל</u>

יהי D חוג עם חילוק שאינו שדה כך ש $Z\left(D\right)=F\neq D$ (F שדה) צ"ל שלכל $x\in D\setminus F$ מתקיים $\left\langle x-d\right\rangle =D\left[x\right]$.

<u>פתרון</u>

נוכיח שהאידיאל $\left\langle x-d\right\rangle$ מכיל איבר הפיך. יהי $e\in D$ כך ש $ed\neq de$. אז $f(x)=-e\left(x-d\right)+\left(x-d\right)e\in\left\langle x-d\right\rangle$ בנוסף $f(x)=ed-de\in D$ D חוג עם חילוק ולכן ל $f(x)$ יש הופכי. ז"א $\left\langle x-d\right\rangle =D\left[x\right]$.

<u>הערה</u>

שימו לב שאם F שדה אז לכל $a\in F$ $\left\langle x-a\right\rangle \neq F\left[x\right]$.

<u>חוג מנה</u>

יהי R חוג, $I\lhd R$. אז על $R/I=\left\{ a+I\middle|a\in R\right\}$ נגדיר חיבור וכפל באופן הבא:

- $\left(a+I\right)\left(b+I\right)=ab+I$
- $\left(a+I\right)+\left(b+I\right)=\left(a+b\right)+I$

אז $\left(R/I,+,\cdot\right)$ הוא חוג, איבר האפס הוא I ואיבר היחידה הוא $1_{R}+I$.

<u>הערה</u>

אם $I\lhd R$ ו $a\in I$ אז המחלקות I ו $\pm a+I$ הן אותו איבר ב R/I.

<u>דוגמאות</u>

1. $R=3\mathbb{Z},I=18\mathbb{Z}$. אז

$R/I=\left\{ \underbrace{18\mathbb{Z}}_{0},\underbrace{3+18\mathbb{Z}}_{3},\underbrace{6+18\mathbb{Z}}_{6},\underbrace{9+18\mathbb{Z}}_{9},\underbrace{12+18\mathbb{Z}}_{12},\underbrace{15+18\mathbb{Z}}_{15}\right\}$.

בתור חבורה חיבורית $R/I \cong \mathbb{Z}_6$. נבנה את לוח הכפל ונראה שבתור חוגים R/I לא איזומורפי ל $\mathbb{Z}_6$, נשים לב שב R/I אין יחידה וב $\mathbb{Z}_6$ יש.

$\bullet$	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

2. $\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\} \cong \mathbb{Z}_5$.

3. $I = \langle x^2+1 \rangle = \{f(x)(x^2+1) \mid f(x) \in \mathbb{R}[x]\}$, נסמן $R = \mathbb{R}[x]$.

נסמן $\bar{a} = a + I \in R/I$. מתקיים: $x^2 + I = x^2 - (x^2+1) + I = -1 + I$, ולכן $\overline{x^2} = \overline{-1}$ ב R/I באותו אופן ניתן לראות ש $\overline{x^3} = \overline{-x}, \overline{x^4} = \bar{1}, \overline{x^5} = \bar{x}, \ldots$

לכן $R/I = \{\alpha + \beta\bar{x} \mid \alpha, \beta \in \mathbb{R}\}$ כי כל חזקה $\overline{x^n}$ $n > 1$ היא $\overline{\pm x}$ או $\overline{\pm 1}$, כשמתקיים $\bar{x} \cdot \bar{x} = -1$.

תרגיל : $R/I \cong \mathbb{C}$

1. יהי $R = \mathbb{Z}_3[x]$, $I = \langle x^2+1 \rangle$. כמה איברים יש ב R/I? כמו בדוגמא הקודמת גם פה $\overline{x^2} = \overline{-1}$ ב R/I ולכן $R/I = \{\alpha + \beta\bar{x} \mid \alpha, \beta \in \mathbb{Z}_3\}$ ז"א שב R/I יש 9 איברים.

תרגיל

איבר x בחוג R הוא נילפוטנט אם קיים $n \in \mathbb{N}$ כך ש $x^n = 0$. יהי R חוג קומוטטיבי ויהי N קבוצת האיברים הנילפוטנטים ב R.

1. הוכיחו כי N אידיאל ב R.
2. הוכיחו כי ב R/N אין איברים נילפוטנטים שונים מאפס.
3. תנו דוגמא לחוג לא קומוטטיבי כך ש N לא אידיאל.

__פתרון__

1. N שונה מקבוצה ריקה מכיוון ש $0 \in N$. יהיו $a,b \in N$ ז"א קיים l כך ש $b^l = 0$ וקיים j כך ש $a^j = 0$. נשים לב שהבינום של ניוטון נכון גם עבור חוגים לא קומוטטיבים. $(a-b)^{j+l} = \sum_{k=0}^{j+l} (-1)^k \binom{j+l}{k} a^k b^{j+l-k}$.
   - אם $k \geq j$ אז $a^k = 0$.
   - אם $k < j$ אז $l < l + j - k$ ואז $b^{j+l-k} = 0$.
2. נניח בשלילה שיש איברים נילפוטנטים שונים מאפס ב R/N. יהי $\overline{0} \neq \overline{x} = x + N \in R/N$ כך שקיים $k \in \mathbb{N}$ כך ש $\overline{x}^k = \overline{0}$. אז $N = \overline{0} = \overline{x^k} = (x+N)^k = x^k + N$ ז"א $x^k \in N$, ולכן x^k נילפוטנט ז"א קיים $l \in \mathbb{N}$ כך ש $(x^k)^l = 0$ ולכן $x^{kl} = 0$ ז"א $x \in N$ (מכיוון ש x נילפוטנט) ז"א $\overline{x} = \overline{0}$ בסתירה להנחה ש $\overline{x} \neq \overline{0}$.

3. יהי $R=M_2\left(\mathbb{Q}\right)$, $e_{21}=\begin{pmatrix}0&0\\1&0\end{pmatrix}, e_{12}=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ $e_{12}^2=e_{21}^2=0$ ולכן הם

איברים נילפוטנטים, אבל $\left(e_{12}+e_{21}\right)^n=\begin{cases}I\\ \begin{pmatrix}0&1\\1&0\end{pmatrix}\end{cases}$ (I כאשר n זוגי, ל

$\begin{pmatrix}0&1\\1&0\end{pmatrix}$ כאשר n אי זוגי)

סה"כ קיבלנו ש $\left(e_{12}+e_{21}\right)^n\neq 0$ לכל $n\in\mathbb{N}$.

ולכן N אינו סגור לחיבור ו N אינו אידיאל.

<u>משפט האיזומורפיזם הראשון</u>

יהי $f:R\to S$ הומומורפיזם, אז $R/\ker f\cong \operatorname{Im} f$.

<u>דוגמא</u>

עבור $f:\mathbb{Z}\to\mathbb{Z}_n$ כך ש $f\left(a\right)=a\left(\bmod n\right)$ נקבל ש $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$.