מבוא לחוגים ומודולים - תרגול 5

תרגיל:

מיהם האידאלים הראשוניים של $\mathbb{Z}[x]$ שמכילים את x?

פתרון:

יהי $P \trianglelefteq \mathbb{Z}[x]$ אידאל ראשוני. $x \in P \iff \langle x \rangle \subseteq P$, לכן לפי משפט ההתאמה יש התאמה חח"ע ועל בין אידאלים ראשוניים של $\mathbb{Z}[x]$ שמכילים את x לאידאלים ראשוניים של חוג המנה $\mathbb{Z}[x]/\langle x \rangle$.

ממשפט האיזומורפיזם הראשון, $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$ (לפי הומומורפיזם ההצבה).

האידאלים הראשוניים של $\mathbb{Z}$ הם 0 והאידאלים מהצורה $p\mathbb{Z}$ ל-p ראשוני.

לכן האידאלים הראשוניים של $\mathbb{Z}[x]$ שמכילים את x הם $\langle x,p \rangle$ לכל p ראשוני או $\langle x \rangle$.

תרגיל:

יהי R חוג חילופי ו-$I \trianglelefteq R$ אידאל אמיתי. הוכיחו כי I ראשוני $\iff R \setminus I$ סגורה לכפל.

הוכחה:

$\boxed{\Leftarrow}$ נניח כי I ראשוני, ויהיו $a,b \in R \setminus I$. נניח בשלילה $ab \notin R \setminus I \Leftarrow ab \in I$. אבל I ראשוני, לכן $a \in I$ או $b \in I$, בסתירה. לכן $R \setminus I$ סגורה לכפל.

$\boxed{\Rightarrow}$ נניח כי $R \setminus I$ סגורה לכפל, ויהיו $a,b \in R$ כך ש-$ab \in I$.

נניח בשלילה ש-$a,b \notin I \Leftarrow a,b \in R \setminus I \xLeftarrow[\text{סגורה לכפל } R\setminus I]{} ab \in R \setminus I$, בסתירה.

לכן I ראשוני. □

תרגיל:

יהי R חוג חילופי שבו כל האידאלים ראשוניים. אזי R הוא שדה.

הוכחה:

$\{0\}$ ראשוני $\Leftarrow$ R תחום שלמות.

יהי $0\neq x\in R$. נתבונן באידאל $I=\langle x^2\rangle$. לפי ההנחה, I ראשוני.

$x\cdot x=x^2\in I$ $\Leftarrow$ $x\in I$ $\Leftarrow$ קיים $r\in R$ כך ש- $x=r\cdot x^2$ $\Leftarrow$ $x(rx-1)=0$

R תחום שלמות, $x\neq 0$ $\Leftarrow$ $rx-1=0$ $\Leftarrow$ $rx=1$. אבל R חילופי, לכן גם $xr=1$, ולכן x הפיך.

$\square$

הערה:

חיתוך של אידאלים ראשוניים הוא לא בהכרח ראשוני.

I,J ראשוניים, $ab\in I\cap J$ $\Leftarrow$ $ab\in I$, $ab\in J$ $\Leftarrow$ $a\in I$ או $b\in I$, $b\in J$ או $a\in J$

למשל ניקח $R=\mathbb{Z}$, $I=2\mathbb{Z}$, $J=3\mathbb{Z}$. $I\cap J=6\mathbb{Z}$ לא אידאל ראשוני.

טענה:

בכל חוג R, כל אידאל מקסימלי הוא ראשוני.

הוכחה:

יהי $M\triangleleft R$ אידאל מקסימלי, ונניח בשלילה שהוא לא ראשוני. ז"א קיימים $I,J\triangleleft R$ כך ש- $IJ\subseteq M$ אבל $I,J\not\subseteq M$.

$$(*)\quad (I+M)(J+M)=\underset{\substack{\cap\\ M}}{IJ}+\underset{\substack{\cap\\ M}}{IM}+\underset{\substack{\cap\\ M}}{MJ}+\underset{\substack{\cap\\ M}}{M^2}\subseteq M$$

מצד שני, כיוון ש- M מקסימלי, $I+M=J+M=R$. ובכן $(*)$ הוא $R=R^2\subseteq M$, בסתירה.

$\square$

תרגיל:

יהי R חוג חילופי שבו לכל $x\in R$ קיים $1<n\in\mathbb{N}$ כך ש- $x^n=x$. הוכיחו שב-R כל אידאל ראשוני הוא מקסימלי.

הוכחה:

יהי $P\lhd R$ אידאל ראשוני. נסתכל על חוג המנה R/P שהוא תחום שלמות.

יהי $0+P\neq x+P\in R/P$, ונראה ש- $x+P$ הפיך ב- R/P.

לפי ההנחה, קיים $1<n\in\mathbb{N}$ כך ש- $x^n=x$. לכן גם

$$(x+P)^n = x^n+P = x+P$$
$$\Downarrow$$
$$(x+P)^n-(x+P)=0$$
$$\Downarrow$$
$$(x+P)\left((x+P)^{n-1}-(1+P)\right)=0$$
$$\Downarrow \text{ תחום שלמות } R/P$$
$$(x+P)^{n-1}=1+P$$

לכן $(x+P)^{n-2}$ הוא ההופכי של $x+P$, זה מראה ש- R/P שדה, ולכן P אידאל מקסימלי.

למה: (למת ההתחמקות מראשוניים) (Prime avoidance lemma)

יהי R חוג חילופי, ויהיו $P_1,\dots,P_n\lhd R$ אידאלים ראשוניים. נניח ש- $I\lhd R$ מוכל באיחוד $\bigcup_{i=1}^n P_i$. אז קיים $1\le j\le n$ כך ש- $I\subseteq P_j$.

הוכחה:

נוכיח גרסה שקולה: אם $I\nsubseteq P_j$ לכל $1\le j\le n$, אז $I\nsubseteq\bigcup_{i=1}^n P_i$.

נוכיח באינדוקציה על n.

$\boxed{n=2}$ לפי ההנחה קיימים $a_1\in I\setminus P_1$ ו- $a_2\in I\setminus P_2$. אם $a_1\notin P_2$ או $a_2\notin P_1$ אז סיימנו.

לכן נניח $a_1\in P_2$ ו- $a_2\in P_1$, ונתבונן ב- $a_1+a_2\in I$.

$a_1\in P_2$, $a_2\notin P_2 \Rightarrow a_1+a_2\notin P_2$, ובדומה $a_1+a_2\notin P_1$. לכן $I\not\subseteq P_1\cup P_2$.

$\boxed{\text{n כללי}}$ נניח שהטענה נכונה עבור $n-1$, ויהי $I\lhd R$ כך ש- $I\not\subseteq P_1,\dots,P_n$.

לפי הנחת האינדוקציה, I אינו מוכל באיחוד של כל $n-1$ מתוך האידיאלים $P_1,\dots,P_n$. לכל $1\le i\le n$ נבחר

$$a_i\in I\setminus\Big(\bigcup_{j\ne i}P_j\Big).$$

כמו מקודם נוכל להניח $a_i\in P_i$.

ניקח את האיבר $x=a_1\cdots a_{n-1}+a_n\in I$. נטען ש- $x\notin\bigcup_{i=1}^{n}P_i$.

מדוע?

אילו $x\in P_n$, אז $\overset{x-a_n}{\overset{\shortparallel}{a_1\cdots a_{n-1}}}\in P_n \xRightarrow{P_n \text{ ראשוני}}$ איזשהו $\underset{1\le i\le n-1}{a_i\in P_n}$ - בסתירה.

אילו $x\in P_i$ עבור $i\le n-1$, אז $a_n\in P_i$ - בסתירה.

זה מראה ש- $I\not\subseteq\bigcup_{j=1}^{n}P_j$. $\square$

חוגים ראשוניים

הגדרה:

אומרים שחוג R הוא ראשוני (prime) אם לכל $A,B\lhd R$ המקיימים $AB=0$, בהכרח $A=0$ או $B=0$.

משפט:

R ראשוני $\iff$ לכל $0\ne a,b\in R$ קיים $r\in R$ כך ש- $arb\ne 0$.

מסקנה:

כל תחום הוא ראשוני.

משפט:

חוג ראשוני חילופי הוא תחום שלמות

דוגמה:

$M_n(F)$ הם חוגים ראשוניים (F שדה).

תרגיל:

יהי R חוג ראשוני. אז המרכז של $Z(R)$ הוא תחום שלמות.

הוכחה:

נראה ש- $Z(R)$ חוג ראשוני. יהיו $A,B \triangleleft Z(R)$. לכן $AR, BR \triangleleft R$.

אם $AB=0$, אז $(AR)(BR) \underset{B\subset Z(R)}{=} ABR = 0 \xRightarrow{R \text{ ראשוני}} AR=0$ או $BR=0$

$\Downarrow$

$A=0$ או $B=0$.

לכן $Z(R)$ חוג ראשוני חילופי, ולכן תחום שלמות.

חוגי טורים פורמליים

הגדרה:

יהי R חוג. חוג טורי החזקות הפורמליים מעל R, המסומן $R[[x]]$, הוא אוסף כל הסכומים $\sum_{n=0}^{\infty} a_n x^n$ כאשר $a_n \in R$, והפעולות הן בדומה לחוג הפולינומים.

דוגמה:

ב- $R[[x]]$, $1-x$ הפיך. ההופכי של הוא $1+x+x^2+\dots$.

לעומת זאת, $R[[x]]$ אינו שדה, כי x אינו הפיך.

הערה:

$R[[x]]$ חילופי $\Leftrightarrow$ R חילופי.

תרגיל:

יהי R חוג. הוכיחו ש- $R[[x]]$ תחום אם ורק אם R תחום.

הוכחה:

$\boxed{\Leftarrow}$ R תת-חוג של $R[[x]]$, לכן אם $R[[x]]$ תחום אז גם R תחום.

$\boxed{\Rightarrow}$ נניח ש-R תחום, ויהיו $0 \neq \sum_{n=0}^{\infty} a_n x^n, \sum_{n=0}^{\infty} b_n x^n \in R[[x]]$. יהיו

$$n_1 = \min\{n \mid a_n \neq 0\}, \qquad n_2 = \min\{n \mid b_n \neq 0\}$$

$$\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k b_{n-k}\right)x^n$$

המקדם הראשון שאינו 0 הוא המקדם של $x^{n_1+n_2} = a_{n_1} b_{n_2} \neq 0$.

כי R תחום

לכן גם המכפלה שונה מאפס.

□

משפט:

נניח ש-R חילופי. $f(x) \in R[[x]]$ הפיך $\iff$ המקדם החופשי של הפיך ב-R.

הוכחה:

נסמן $f(x) = \sum_{n=0}^{\infty} a_n x^n$.

$\boxed{\Leftarrow}$ אם $f(x)$ הפיך, יהי $g(x) = \sum_{n=0}^{\infty} b_n x^n$ ההופכי שלו.

$$f(x)g(x) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k b_{n-k}\right)x^n = 1$$

בפרט אם נשווה את המקדמים החופשיים נקבל $a_0 b_0 = 1 \Rightarrow$ R חילופי a_0 הפיך.

$\boxed{\Rightarrow}$ נניח ש-a_0 הפיך. נגדיר $g(x) = \sum_{n=0}^{\infty} b_n x^n$ באופן הרקורסיבי:

$$b_0 = a_0^{-1}$$

$$\forall n \geq 1: \quad b_n = -a_0^{-1}(a_1 b_{n-1} + a_2 b_{n-2} + \dots + a_n b_0)$$

ומפה אפשר לבדוק שבאמת $f(x)g(x) = 1$.

□

מסקנה:

נניח ש-F שדה. אז האידאל המקסימלי היחיד של $F[[x]]$ הוא $\langle x\rangle$.

הוכחה:

ראשית נוכיח ש-$\langle x\rangle$ מקסימלי. נראה כי $F[[x]]/\langle x\rangle \cong F$. מדוע?

אם נגדיר $\varphi\left(\sum_{n=0}^{\infty} a_n x^n\right) = a_0$ אז φ אפימורפיזם ו-$\ker\varphi = \langle x\rangle$.

$F[[x]]/\langle x\rangle$ שדה $\Leftarrow$ $\langle x\rangle$ אידאל מקסימלי.

מדוע אין עוד אידאלים מקסימליים? יהי M אידאל מקסימלי של $F[[x]]$,

ונניח בשלילה $M \neq \langle x\rangle$. לכן $M \not\subseteq \langle x\rangle$ $\Leftarrow$ קיים $f(x) \in M \setminus \langle x\rangle = \sum_{n=0}^{\infty} a_n x^n$.

אבל אז $a_0 \neq 0$ $\Leftarrow$ $f(x)$ הפיך $\Leftarrow$ $M = F[[x]]$, סתירה. $\square$

הגדרה:

יהי R חוג. חוג טורי לורן הפורמליים (Laurent)

$$R((x)) = \left\{ \sum_{i=-n}^{\infty} a_i x^i \;\middle|\; n \in \mathbb{N},\ a_i \in R \right\}.$$

$$R \subsetneq R[x] \subsetneq R[[x]] \subsetneq R((x))$$

הגדרה:

על $R((x))$ ניתן להגדיר הערכה $v : R((x)) \longrightarrow \mathbb{Z} \cup \{\infty\}$

$$v\left(\sum_{i=-n}^{\infty} a_i x^i\right) = \min\{ i \mid a_i \neq 0 \}, \quad v(0) = \infty$$

טענה:

א. $v(f+g) \geq \min\{v(f), v(g)\}$

ב. $v(f \cdot g) \geq v(f) + v(g)$

ג. אם R תחום, יש שוויון ב-ב.

טענה:

אם R תחום, $R((x))$ תחום. אם F שדה, אז $F((x))$ שדה.

הוכחה של החלק השני:

יהי $\sum_{i=-n}^{\infty} a_i x^i \in F((x))$, $0 \neq$. נניח $a_{-n} \neq 0$. אז

$$\sum_{i=-n}^{\infty} a_i x^i = x^{-n} \sum_{i=-n}^{\infty} a_i x^{i+n} = \underbrace{\underbrace{x^{-n}}_{\text{הפיך ב-}F((x))} \underbrace{\sum_{i=0}^{\infty} a_{i-n} x^i}_{\substack{\text{הפיך ב-}F[[x]] \\ \Downarrow \\ \text{הפיך ב-}F((x))}}}_{\text{הפיך.}}$$

$\square$

$$F[x][y] = F[x,y] = F[y][x]$$

$$F[x,y] \subsetneq F[[x]][y] \subsetneq F[y][[x]] \subsetneq F[[x]][[y]] \subsetneq F[[y]]((x)) \subsetneq F((x))[[y]] \subsetneq F((x))((y))$$