מבוא לחוגים ומודולים - תרגול 4

תרגיל:

הוכיחו שהחוגים

$$R = \mathbb{C}[x,y]/\langle xy-1\rangle \quad , \quad S = \mathbb{C}[x,y]/\langle y-x^2\rangle$$

אינם איזומורפיים.

פתרון:

נראה ש- $S \cong \mathbb{C}[t]$ ע"י ההומומורפיזם

$$\varphi: \mathbb{C}[x,y] \longrightarrow \mathbb{C}[t]$$
$$x \longmapsto t$$
$$y \longmapsto t^2$$
$$f(x,y) \longmapsto f(t,t^2)$$

זה אפימורפיזם.

נבדוק כי $\ker\varphi = \langle y-x^2\rangle$.

$\boxed{\supseteq}$ אם $f(x,y)\in\langle y-x^2\rangle$, אז $f(x,y)=g(x,y)(y-x^2)$. לכן

$$\varphi(f) = \varphi(g(x,y)(y-x^2)) = \varphi(g(x,y))\cdot\varphi(y-x^2) = \varphi(g(x,y))\cdot(t^2-t^2)=0$$

$\boxed{\subseteq}$ יהי $f(x,y)\in\ker\varphi$.

כיוון ש- $y-x^2$ מתוקן ב-y, אפשר לכתוב

$$f(x,y) = g(x,y)(y-x^2)+r(x)$$

$$xy^3 - xy^2 = (y-x^2)(xy^2+(x^3-x)y+(x^5-x^3)) + x^2(x^5-x^3)$$

$$\mathbb{C}[x,y] = (\mathbb{C}[x])[y]$$

$$\varphi(f(x,y)) = \varphi(g(x,y)(y-x^2)+r(x)) = r(t) = 0$$

לכן $r(x)=0$. לכן $f\in\langle y-x^2\rangle$.

הראינו ש-φ אפימורפיזם עם גרעין $\langle y-x^2\rangle$, לכן $S = \mathbb{C}[x,y]/\langle y-x^2\rangle \cong \mathbb{C}[t]$.

לגבי R:

$$R = \mathbb{C}[x,y]/\langle xy-1\rangle \cong \mathbb{C}[t,t^{-1}]$$

$$\begin{aligned} \mathbb{C}[x,y] &\longrightarrow \mathbb{C}[t,t^{-1}] \\ x &\longmapsto t \\ y &\longmapsto t^{-1} \end{aligned}$$

ניתן להוכיח $\mathbb{C}[t]\not\cong\mathbb{C}[t,t^{-1}]$. מדוע?

ראינו בתרגול בית $(\mathbb{C}[t])^\times = \mathbb{C}^\times$. לכן $(\mathbb{C}[t])^\times \cup\{0\} = \mathbb{C}$ קבוצה סגורה לחיבור. מצד שני, ב-$\mathbb{C}[t,t^{-1}]$ הקבוצה $(\mathbb{C}[t,t^{-1}])^\times\cup\{0\}$ לא סגורה לחיבור, כי $1,t\in(\mathbb{C}[t,t^{-1}])^\times\cup\{0\}$ אבל סכומם אינו הפיך ב-$\mathbb{C}[t,t^{-1}]$.

<u>הגדרה:</u>

אידאל מהצורה $\langle x\rangle$ נקרא <u>אידאל ראשי</u> (principal ideal).
חוג שבו כל אידאל הוא ראשי, נקרא <u>חוג ראשי</u>, תחום שלמות ראשי נקרא גם <u>תחום ראשי</u> (principal ideal domain, PID).

<u>דוגמה:</u>

$\mathbb{Z}$ הוא תחום ראשי.

<u>תרגיל:</u>

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

<u>פתרון:</u>

$h(0)=2f(0)$

נסתכל על $I=\langle 2,x\rangle \lhd \mathbb{Z}[x]$. יהי $h(x)=2f(x)+xg(x)\in\langle 2,x\rangle$. $2=q\cdot g_1$

בפרט $h(0)\in 2\mathbb{Z}$, לכן $1\notin\langle 2,x\rangle$. לכן זה אידאל אמיתי. $x=q\cdot g_2$

מצד שני, נניח בשלילה $\langle 2,x\rangle=\langle q\rangle$. אז $2\in\langle q\rangle$ ו-$x\in\langle q\rangle$.

לכן q מחלק משותף של 2 ושל x, לכן $q=\pm1$, בסתירה לכך ש-$\langle 2,x\rangle$ הוא אידאל אמיתי.

הערה:

ב- $\mathbb{Q}[x]$, האידיאל $\langle 2,x\rangle$ לא היה ראשי, כי

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

תרגיל:

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

טענה:

מנה של חוג ראשי היא חוג ראשי. לכן גם $\mathbb{Z}/n\mathbb{Z}$ חוג ראשי.

חוגים פשוטים

הגדרה:

חוג R נקרא פשוט (simple) אם אין לו אידאלים פרט ל-$\{0\}$ ו-R.

דוגמה:

כל חוג עם חילוק הוא פשוט.

תרגיל:

חוג חילופי ופשוט הוא שדה.

הוכחה:

יהי $0\neq x\in R$. כיוון ש-R פשוט וחילופי, $Rx=R \Leftarrow 1\in Rx \Leftarrow$ קיים $y\in R$

שעבורו $yx=1 \overset{R\text{ חילופי}}{\Longleftarrow} xy=1 \Leftarrow x$ הפיך. לכן R שדה. $\square$

תרגיל:

המרכז של חוג פשוט הוא שדה.

הוכחה: יהי R פשוט.

ידוע ש- $Z(R)$ תת-חוג חילופי. יהי $0\neq x\in Z(R)$. R פשוט, לכן $Rx=R$

$\Leftarrow$ בדומה לתרגיל הקודם, x הפיך.

ניתן להראות ש-$x^{-1}\in Z(R)$. יהי $r\in R$.

$$rx=xr \Rightarrow x^{-1}rx = x^{-1}xr = r \Rightarrow x^{-1}r = rx^{-1}$$

כנדרש. לכן $Z(R)$ שדה. $\square$

<u>תרגיל:</u>

יהי D חוג עם חילוק שאינו שדה. נסמן $F=Z(D)$. הוכיחו שלכל $d\in D\setminus F$, $\langle x-d\rangle = D[x]$.

<u>הוכחה:</u>

$d\in D\setminus F \Leftarrow$ קיים $e\in D$ כך ש-$de\neq ed$.

$$\langle x-d\rangle \ni -e\underbrace{(x-d)}_{\in\langle x-d\rangle} + \underbrace{(x-d)}_{\in\langle x-d\rangle}e = -\cancel{ex}+ed+\cancel{ex}-de = \underset{\in D}{ed-de}\neq 0$$

אבל $ed-de$ איבר הפיך ב-$\langle x-d\rangle$, לכן $\langle x-d\rangle = D[x]$. $\square$

<u>משפט:</u>

כל אידיאל של $M_n(R)$ הוא מהצורה $M_n(I)$ עבור $I\lhd R$.

בפרט, אם R פשוט, גם $M_n(R)$ פשוט.

<u>תרגיל:</u>

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

<u>פתרון:</u>

לא!

$$A=\begin{pmatrix} * & * & \cdots & * \\ & * & & \vdots \\ & 0 & \ddots & \\ & & & * \end{pmatrix} \rhd I = \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix}$$

אידאלים מקסימליים

הגדרה:

אידאל אמיתי $I \lhd R$ הוא <u>מקסימלי</u> אם לא קיים אידאל אמיתי שמכיל אותו ממש.

דוגמה:

ב- $\mathbb{Z}/_{32\mathbb{Z}}$ יש אידאל מקסימלי (יחיד) שהוא $2 \cdot \mathbb{Z}/_{32\mathbb{Z}} \; \left(= (2+32\mathbb{Z}) \cdot \mathbb{Z}/_{32\mathbb{Z}}\right)$

ב- $\mathbb{Z}/_{45\mathbb{Z}}$ יש שני אידאלים מקסימליים - $3\mathbb{Z}/_{45\mathbb{Z}}$, $5\mathbb{Z}/_{45\mathbb{Z}}$.

דוגמה:

ב- $\mathbb{Z}$, האידאלים המקסימליים הם $p\mathbb{Z}$ עבור p ראשוני.

דוגמה:

עבור R חילופי, $\langle x \rangle \lhd R[x,y]$ לא מקסימלי, כי $\langle x \rangle \subsetneq \underbrace{\{f \in R[x,y] \mid f(0,0)=0\}}_{=\langle x,y \rangle}$.

תרגיל:

יהי $f: R \longrightarrow S$ אפימורפיזם, ויהי $I \lhd R$ אידאל אמיתי המכיל את $\ker f$.
הוכיחו ש- $f(I) \lhd S$ אידאל אמיתי.

הוכחה:

$f(I)$ אידאל של S כי f אפימורפיזם.

נניח בשלילה ש- $I \lhd R$ אידאל אמיתי אבל $\underline{f(I)=S}$. נבחר $x \in R \setminus I$,
קיים איבר $y \in I$ כך ש- $f(y)=f(x)$. לכן $f(y-x)=0$,
כלומר $y-x \in \ker f \subseteq I$ $\Leftarrow$ $x = y-(y-x) \in I$, בסתירה. $\square$

מסקנה:

אם $f: R \longrightarrow S$ אפימורפיזם ו- $J \lhd S$ מקסימלי, אז $f^{-1}(J) \lhd R$ מקסימלי.

מה היה קורה אילו לא היינו דורשים אפימורפיזם? הטענה לא הייתה נכונה.

ההכלה $\varphi:\mathbb{Z}\hookrightarrow\mathbb{Q}$

$\{0\}$ מקסימלי $\quad$ $\{0\}$ לא מקסימלי

הוכחת המסקנה:

נניח בשלילה ש- $f^{-1}(J)$ לא אידאל מקסימלי. כלומר קיים $f^{-1}(J)\subsetneq I\triangleleft_{\neq} R$.

מכיוון $\ker f\subseteq f^{-1}(J)\subsetneq I$ $\overset{\text{תרגיל}}{\Rightarrow}$ $f(I)$ אידאל אמיתי של S.

$J\subseteq f(I)\triangleleft_{\neq} S$ $\overset{J\text{ מקסימלי}}{\Rightarrow}$ $f(I)=J$ $\Rightarrow$ $I\subseteq f^{-1}(J)$, בסתירה.

□

משפט:

יהי R חוג, אידאל אמיתי $I\triangleleft R$ הוא מקסימלי $\iff$ R/I פשוט.

אם R חילופי, $I\triangleleft R$ מקסימלי $\iff$ R/I שדה.

דוגמה:

$\langle p,x\rangle\triangleleft\mathbb{Z}[x]$ אידאל מקסימלי, כי $\mathbb{Z}[x]/\langle p,x\rangle\cong\mathbb{Z}/p\mathbb{Z}$ שדה.

אידאלים ראשוניים

הגדרה:

אידאל $I\triangleleft R$ ייקרא ראשוני (prime) אם לכל $A,B\triangleleft R$ כך ש- $AB\subseteq I$, מתקיים $A\subseteq I$ או $B\subseteq I$.

אם R חילופי, הגדרה שקולה: אם $a\cdot b\in I$ אז $a\in I$ או $b\in I$.

דוגמה:

מחוץ לא חילופי, ההגדרות יכולות להיות שונות. ניקח $R=M_2(F)$. $\{0\}$ אידאל ראשוני, אבל מתקיים $\begin{pmatrix}1&0\\0&0\end{pmatrix}\cdot\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$.

בחוג פשוט, $\{0\}$ אידאל ראשוני:

תרגיל:

יהי $C(\mathbb{R})$ חוג הפונקציות הממשיות הרציפות. הוכיחו כי
$$I=\{f\in C(\mathbb{R}) \mid f(0)=0\}$$
הוא אידאל ראשוני.

הוכחה:

ראיתם $I\lhd C(\mathbb{R})$. כדי לוודא שהוא ראשוני, נניח $f(x)g(x)\in I$.
$$f(0)g(0)=0$$
ולכן $f(0)=0$ או $g(0)=0$ $\Leftarrow$ $f\in I$ או $g\in I$.

משפט:

יהי R חוג חילופי. $I\lhd R$ ראשוני $\Longleftrightarrow$ R/I תחום שלמות.

מסקנה:

אם R חילופי, אז R הוא תחום שלמות $\Longleftrightarrow$ $\{0\}$ ראשוני.

דוגמה:

$\langle x\rangle \lhd \mathbb{Z}[x]$ אידאל ראשוני, כי $\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}$ תחום שלמות.

$\langle x\rangle \lhd (\mathbb{Z}/4\mathbb{Z})[x]$ לא אידאל ראשוני, כי $(\mathbb{Z}/4\mathbb{Z})[x]/\langle x\rangle \cong \mathbb{Z}/4\mathbb{Z}$ אינו תחום שלמות.