

תזכורת

- אידאלים אמיתיים $(R, +)$
- אידאל מקסימלי = אידאל שאינו מוכל באף אידאל אחר
- הלמה של צורן \Leftarrow כל אידאל מוכל באידאל מקסימלי
- $M \triangleleft R \Leftrightarrow R/M$ פשוט (חוג בלי אידאלים)
- חוג קומוטטיבי פשוט = שדה

דוגמאות

1. $R = \mathbb{Z}$. $n\mathbb{Z} \triangleleft \mathbb{Z}$ מקסימלי $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ שדה $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ תחום שלמות $\Leftrightarrow n$ ראשוני ($\mathbb{Z}/n\mathbb{Z}$ שדה)

2. $R = R_1 \times R_2$. לכל אידאל $I \triangleleft R$, נסמן:

$$I_1 = \{a \in R_1 \mid \exists b \in R_2 (a, b) \in I\} \triangleleft R$$

$$I_2 = \{b \in R_2 \mid \exists a \in R_1 (a, b) \in I\} \triangleleft R_2$$

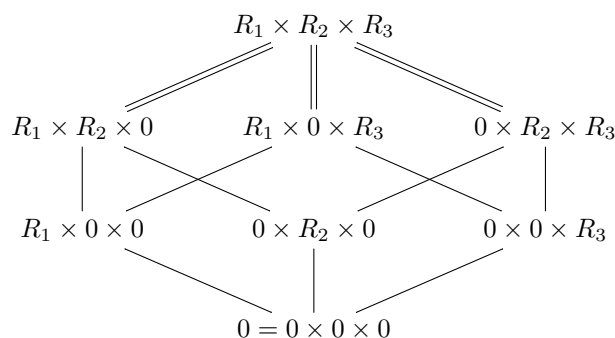
$$\begin{matrix} \subset R & \subset R_1 \times R_2 \\ \underbrace{I} & = \underbrace{I_1 \times I_2} \end{matrix}$$

טענה:

הוכחה: לכל $(a, b) \in I$, $a \in I_1$ ו $b \in I_2$ מצד שני, לכל $a \in I_1$ ו $b \in I_2$ קיימים $a' \in R_1, b' \in R_2$ כך ש $(a', b) = (a, b')$ וכעת

$$I \ni \underbrace{(a, b') \cdot (1, 0)}_{=(a, 0) \in R} + \underbrace{(a', b) \cdot (0, 1)}_{=(0, b) \in R} = (a, b)$$

- למשל, נניח R_1, R_2, R_3 הם חוגים פשוטים. אז סריג האידאלים של $R = R_1 \times R_2 \times R_3$ הוא



- כמכפלה ישרה של חוגים פשוטים, $R_1 \times \dots \times R_n$, האידיאלים המקסימליים הם $R_1 \times \dots \times R_{i-1} \times 0 \times R_{i+1} \times \dots \times R_n$

3. אם R פשוט אז גם $M_n(R)$ חוג פשוט.

נתבונן בחוג $M_n(\mathbb{Z})$. האידיאלים שלו הם $m \cdot M_n(\mathbb{Z})$

$$M_n(\mathbb{Z})/m \cdot M_n(\mathbb{Z}) \cong M_n(\mathbb{Z}/m\mathbb{Z})$$

מסקנה: לכל ראשוני p , $p \cdot M_n(\mathbb{Z})$ אידיאל מקסימלי.

הגדרה

R חוג ראשוני אם $AB = 0 \Leftrightarrow A = 0$ או $B = 0$ לכל $A, B \in R$

\Updownarrow

לכל $a, b \neq 0$ קיים x כך $a \times b \neq 0$

- הוכחנו: כל חוג פשוט הוא ראשוני.

- כל תחום הוא ראשוני.

הגדרה

$S \subseteq R$ תת חוג. R נקרא "הרחבה מרכזית" של S אם $Z(R) \cdot S = R$

דוגמה

$$M_n(\mathbb{Z}) \subseteq M_n(\mathbb{Q})$$

$$\begin{pmatrix} \alpha & & \\ & \ddots & \\ & & \alpha \end{pmatrix} \begin{pmatrix} & \\ & \\ & \end{pmatrix} = \begin{pmatrix} & \\ & \mathbb{Q} \\ & \end{pmatrix}$$

אז $M_n(\mathbb{Q})$ היא הרחבה מרכזית של $M_n(\mathbb{Z})$, למשל:

$$\begin{pmatrix} \frac{1}{24} & \\ & \frac{1}{24} \end{pmatrix} \begin{pmatrix} 4 & 32 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} \frac{1}{6} & \frac{4}{3} \\ \frac{1}{8} & \frac{1}{12} \end{pmatrix}$$

משפט

אם $S \subseteq R$ הרחבה מרכזית כאשר R חוג ראשוני, אז S ראשוני.

מסקנה

$M_n(\mathbb{Z})$ הוא חוג ראשוני

הוכחת המשפט

נסמן $Z = Z(R)$. לפי ההנחה $Z \cdot S = R$. רוצים להוכיח ש S ראשוני. יהיו $A, B \triangleleft S$, $0 \neq A, B$. אז $Z \cdot AB = ZA \cdot ZB = R$ ולכן $ZA, ZB = R$ פשוט, מכיוון ש R פשוט, $AB \neq 0 \Leftrightarrow R \cdot R = R \neq 0$.

הגדרה - חוג ראשוני

חוג ראשוני אם $AB = 0 \Leftrightarrow A = 0$ או $B = 0$ לכל $A, B \triangleleft R$.

הגדרה - אידיאל ראשוני

$P \triangleleft R$ ראשוני אם R/P ראשוני.

טענה

התכונות הבאות שקולות:

1. P ראשוני
2. לכל $A, B \notin P$, $AB \notin P$.
3. אם $A \notin P$ ו $AB \subseteq P$ אז $B \subseteq P$.
4. אם $A, B \subseteq P$ אז $AB \subseteq P$.

הוכחה

לכל $\alpha = A/P$
 $\beta = B/P$
 $\Leftrightarrow \alpha\beta \neq 0$ גם $\alpha, \beta \triangleleft R/P$, $0 \neq \alpha, \beta$ לכל $\alpha, \beta \triangleleft R/P$ \Leftrightarrow ראשוני R/P \Leftrightarrow 1
 $AB \notin P$ גם $P \subset AB + P$ גם $P \subset A, B \triangleleft R$

2 \Leftrightarrow 3: לוגית

2 \Leftrightarrow 4: כמקרה פרטי

2 \Leftrightarrow 4: נניח ש $A, B \notin P$. נסמן $A' = A + P \supseteq P$
 $B' = B + P \supseteq P$

לפי ההנחה

$$AB + P \supseteq AB + PB + AP + P^2 = (A + B)(B + P) = A'B' \not\subseteq P$$

$$AB + P \Rightarrow AB \notin P$$

טענה

כל אידאל מקסימלי M הוא ראשוני.

הוכחה

לפי קריטריון 4: אם $M \subset A, B$ אז $A = B = R$ ואז $AB = R \not\subseteq M$

הוכחה שנייה

M מקסימלי $\Leftrightarrow R/M$ פשוט $\Leftrightarrow R/M$ ראשוני $\Leftrightarrow M$ ראשוני.

תרגיל

יהי $\phi : R \rightarrow S$ הומו' על של חוגים. נניח ש $P \triangleleft S$ מקסימלי/ראשוני. אז $R \triangleleft \phi^{-1}(P)$ והוא מקסימלי בהתאמה.

הוכחה

כדי להוכיח את התכונה המבוקשת של $\phi^{-1}(P)$ נתבונן בחוג המנה

$$R/\phi^{-1}(P) \cong \text{Im}\phi/P \cap \text{Im}\phi \cong \text{Im}\phi + P/P \subseteq S/P$$

כי ϕ על

$$\bar{\phi}(x) = \phi(x) + (P \cap \text{Im}\phi) \text{ על ידי } \bar{\phi} : R \rightarrow \text{Im}\phi/P \cap \text{Im}\phi$$

דוגמה(לאידאל מקסימלי שהמקור שלו אינו ראשוני)

$R = \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}, P = 0, S = M_2(\mathbb{Q})$. לא ראשוני כי $J = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}$ מקיים $J^2 = 0$
(זו דוגמה לתת-חוג לא ראשוני של חוג פשוט)

עוד דוגמה

$S/P \cong M_2(\mathbb{Q})$ פשוט. $P = xS, S = M_2(\mathbb{Q}[x])$ מקסימלי, $\phi : R \rightarrow S$ השיכון, $R = \begin{pmatrix} \mathbb{Q}[x] & \mathbb{Q}[x] \\ 0 & \mathbb{Q}[x] \end{pmatrix} \subseteq S$
 $\phi^{-1}(P) = xR$

$$R/\phi^{-1}(P) \cong \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$$

לא ראשוני $\Leftarrow \phi^{-1}(P)$ לא ראשוני.

2.3. פירוק למכפלה ישרה

הערה

נניח ש $I_1, \dots, I_n \triangleleft R$ אז יש הומו'

$$\varphi : R \rightarrow R/I_1 \times R/I_2 \times \dots \times R/I_n$$

המוגדר לפי ההטלות $x \mapsto (x + I_1, \dots, x + I_n)$.

$$\ker \varphi = I_1 \cap \dots \cap I_n$$

בפרט, אם $I_1 \cap \dots \cap I_n = 0$ אז $R \hookrightarrow R/I_1 \times \dots \times R/I_n$

הערה

אם $\{I_\alpha\}$ משפחה של אידאלים של R , $R/\bigcap I_\alpha \hookrightarrow \prod R/I_\alpha$, לדוגמה, $R = \mathbb{Z}$, ואז מקבלים שיכון

$$\mathbb{Z} \hookrightarrow \prod_{n \neq 0} \mathbb{Z}/n\mathbb{Z}$$

הגדרה

אידאלים I, I' נקראים קו־מקסימלים אם $I + I' = R$

דוגמאות

1. לכל מקסימלי M ו $I \not\subseteq M$, M, I קו־מקסימליים (כי $M \subsetneq I + M$).
בפרט, כל שני אידאלים מקסימליים שונים הם קו־מקסימליים.
2. $\mathbb{Z}, \mathbb{Z}, (n, m)\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z}$.¹ לכן, $n\mathbb{Z}, m\mathbb{Z}$ קו־מקסימליים $\Leftrightarrow n, m$ זרים.
3. נניח ש I, J קו־מקסימליים, וגם I', J קו־מקסימליים. אז I, J קו־מקסימליים

הוכחה: לפי ההנחה קיימים:

- $a + b = 1$ כך $a \in I, b \in I$
- $a' + b' = 1$ כך $a' \in I', b' \in J$

כעת:

$$1 = 1 \cdot 1 = (a + b)(a' + b') = \underbrace{aa'}_{\in II'} + \underbrace{(ab' + a'b + bb')}_{\in J}$$

¹ (n, m) המכנה המשותף המקסימלי של n ו m

מסקנה

אם I, J קומקסימליים לכל $i = 1, \dots, n$, אז $I_1 \cdots I_n, J$ קומקסימליים.

מסקנה

אם I, J קומקסימליים, גם I^n, J קומקסימליים וגם I^n, J^m קומקסימליים.

דוגמה

$2\mathbb{Z}, 3\mathbb{Z} \triangleleft \mathbb{Z}$ קומקסימליים. לכן $2^n\mathbb{Z}, 3^m\mathbb{Z}$ קומקסימליים.

משפט השאריות הסיני

נניח ש $I_1, I_2, \dots, I_n \triangleleft R$ קומקסימליים בזוגות. אז $R/I_1 \cdots I_n \cong R/I_1 \times \dots \times R/I_n$. כלומר: $\forall_i x - a_i \in I_i$ כן קיים x כן $a_1, \dots, a_n \in R$.

$$\begin{aligned} x &\equiv a_1 \pmod{I_1} \\ &\vdots \\ x &\equiv a_n \pmod{I_n} \end{aligned}$$