תזכורת

R חוג.

$M \lhd R$ מקסימלי - $M \neq R$ ולא קיים $M \subset M' \lhd R$.

בחוג פשוט, 0 מקסימלי.

M מקסימלי $\Leftrightarrow$ R/M פשוט

R קומוטטיבי $\Leftrightarrow$ R/M שדה

אם $I_1, ...I_n \lhd R$:

$R \to R/I_1 \times ... \times R/I_n$

$x \mapsto (x + I_1, x + I_2, ...x + I_n)$

$R/I_1 \cap ... \cap I_n \hookrightarrow R/I_1 \times ... \times R/I_n$

$R, J \lhd R$ קומקסימליים אם $I + J = R$. למשל אם I מקסימלי ו$J \not\subseteq I$.

בפרט כל שני אידאלים מקסימליים הם קומקסימליים.

הוכחנו שאם $I + J = R$ אז גם $I^n + J^n = R$ לכל n, m.

תזכורת

$$R = \mathbb{Z} \qquad I = a\mathbb{Z} \qquad J = b\mathbb{Z}$$

$$a\mathbb{Z} \cdot b\mathbb{Z} = ab\mathbb{Z}$$

$$a\mathbb{Z} + b\mathbb{Z} = (a, b)\,\mathbb{Z}$$

$$a\mathbb{Z} \cap b\mathbb{Z} = [a, b]\,\mathbb{Z}$$

בפרט, $a\mathbb{Z}, b\mathbb{Z}$ קומקסימליים $\Leftrightarrow$ $(a, b) = 1$

משפט השארית הסיני

יהי R חוג כלשהו עם אידאלים $I_1, ...I_n$ קומקסימליים בזוגות.

אז

$$R/I_1 \cap ... \cap I_n \cong R/I_1 \times ... \times R/I_n$$

בפרט, אם I_1, I_2 קומקסימליים,

$$R/I_1 \cap I_2 \cong R/I_1 \times R/I_2$$

דוגמה

נניח ש$(a, b) = 1$.

$$\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

$$x + ab\mathbb{Z} \mapsto (x + a\mathbb{Z}, x + b\mathbb{Z})$$

מסקנה

אם a, b זרים, אזי

$$\forall \alpha, \beta \exists x$$

$$x \equiv \alpha \pmod a \qquad x \equiv \beta \pmod b$$

כלומר x אחד פותר את שתי המשוואות.

הוכחת המשפט

נקבע $1 \le i \le n$. לכל $j \neq i$, $1 \in R = I_i + I_j$. לכן קיימים, לכל j, $a_j \in I_I, b_j \in I_j$ כך ש$1 = a_j + b_j$. נכפיל:

$$1 = 1 \cdot 1 \cdots 1 = (a_1 + b_1) \cdots (a_{i-1} + b_{i-1})(a_{i+1} + b_{i+1}) \cdots (a_n + b_n) =$$

$$= \underbrace{\left(\text{sum of all other } 2^{n-1} \text{ monoms}\right)}_{\in I_i} + \underbrace{b_1 b_2 \cdots b_{i-1} b_{i+1} \cdots b_n}_{e_i}$$

לכל $j \neq i$, $e_i = \cdots b_j \cdots \in I_j$, ולפי חישוב המונומים, $1 \in e_i + I_i$, כלומר

$$e_i \mapsto (0, 0, ..., 0, 0)$$

(כאשר ה1 במקום הi)

כעת, לכל $\alpha_1, ...\alpha_n$,

$$x = \sum \alpha_i e_i \mapsto (x_1, ...x_n)$$

דוגמה

תנו נוסחה לפתרון המשוואה

$$x \equiv \alpha \pmod{11}$$
$$x \equiv \beta \pmod{35}$$

פתרון

צריך להציג $1 \in 11\mathbb{Z} + 35\mathbb{Z}$:

$$1 = \underbrace{11 \cdot 16}_{a} + \underbrace{35\,(-5)}_{b}$$

$$e = 35 \cdot (-5) \mapsto (1, 0)$$

$$\mathbb{Z} \to \mathbb{Z}/_{11\mathbb{Z}} \times \mathbb{Z}/_{35\mathbb{Z}}$$

$$x \mapsto (x, x)$$

סיכום

$$\mathbb{Z}/385\mathbb{Z} \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z}$$

לפי $x \mapsto (x,x)$, וההפכי הוא $(\alpha,\beta) \mapsto (166\beta k 167\alpha u)$

תרגיל

נניח ש$I_1, ...I_n$ קומקסימליים בזוגות. אזי

$$I_1 \cap ... \cap I_n = \sum_{\sigma \in S_n} I_{\sigma_1} \cdots I_{\sigma_n}$$

בפרט, כאשר R קומוטטיבי

$$I_1 \cap ... \cap I_n = I_1 \cdots I_n$$

עבור $I_1, I_2, ...I_n \lhd R$ מקסימליים שונים.
לכל $m_1, ...m_n$, גם $I_1^{m_1}, ...I_n^{m_n}$ מקסימליים שונים, ולכן

$$R/\cap I_i^{m_i} \cong \prod R/I_i^{m_i}$$

דוגמה

שוב נניח $R = \mathbb{Z}$, ויהי $k \in \mathbb{Z}$ כלשהו. אפשר לפרק

$$k = p_1^{m_1} \cdots p_n^{m_n}$$

כל $p_i\mathbb{Z}$ מקסימלי; כל ה$p_i^{m_i}\mathbb{Z}$ קומקסימליים; $\mathbb{Z}/\prod p_i^{m_i}\mathbb{Z}$

נתבונן מקרוב בחוגים מהצורה $\mathbb{Z}/p^m\mathbb{Z}$, p ראשוני. לדוגמה:

$$\begin{tikzcd}
\mathbb{Z}/81\mathbb{Z} \arrow[d, dash] \\
3\mathbb{Z}/81\mathbb{Z} \arrow[d, dash] \\
9\mathbb{Z}/81\mathbb{Z} \arrow[d, dash] \\
27\mathbb{Z}/81\mathbb{Z} \arrow[d, dash] \\
0
\end{tikzcd}$$

הגדרה

חוג(קומוטטיבי) נקרא <u>מקומי</u> אם יש לו אידיאל מקסימלי יחיד.

טענה

נניח שR חוג קומוטטיבי, $M \lhd R$ מקסימלי. אזי, לכל n, R/M^n מקומי.

הוכחה

נראה שM/M^nהוא האידאל המקסימלי היחיד:

אידיאלים של חוג מנה R/M^n הם מהצורה I/M^n, כאשר $M^n \subseteq I \lhd R$. נניח ש$I \not\subseteq M$, אז כיוון שM מקסימלי, I, M קו־מקסימליים, ולכן גם I, M^n קו־מקסימליים. לכן $I + M^n = R$, וכיוון ש$M^n \subseteq I$, נקבל ש$I = R$ וסתירה! לכן $M \supseteq I$.

לכן $I/M^n \subseteq M/M^n$

לכן M/M^n מקסימלי ויחיד, ולכן R/M^n מקומי.

טענה

יהי R חוג קומוטטיבי. איבר של אידאל אמיתי אינו יכול להיות הפיך. אם a לא הפיך באידאל אמיתי Ra, ו$u(R)$ קבוצת ההפיכים בR,

$$\Downarrow$$

$$u(R) = R \setminus \bigcup_{\substack{I \lhd R \\ I \text{ proper ideal}}} I$$

$$\Downarrow$$

$$u(R) = R \setminus \bigcup_{\substack{M \lhd R \\ \text{max ideal}}} M$$

מסקנה

אם R (קומוטטיבי) מקומי עם אידאל מקסימלי M, אזי:

$$u(R) = R \setminus M$$

משפט

עבור חוג קומוטטיבי R, התנאים הבאים שקולים:

1. החוג מקומי
2. אם $x+y=1$, אז x או y הפיך, או שניהם הפיכים
3. אוסף האיברים הלא־הפיכים סגור לחיבור

הוכחה

$(1) \Leftarrow (2)$ נסמן בM את האידאל המקסימלי. נניח ש$x+y=1$ ושx וy לא הפיכים. לכן $x,y \in M$. לכן $1 \in M \Leftarrow 1 = x+y \in M$ ו1 הפיך וסתירה, לכן x או y הפיך.

$(2) \Leftarrow (3)$ יהי a,b לא הפיכים, ונניח בשלילה ש$a+b$ הפיך. לכן קיים u כך ש$ua+ub=u(a+b)=1$. לפי (2), או שua הפיך או ub הפיך או שניהם, לכן a או b או שניהם הפיכים וסתירה! שכן $a+b$ לא הפיך $\Leftarrow$ אוסף האיברים הלא הפיכים סגור לחיבור.

$(3) \Leftarrow (1)$ נסמן $M = R \backslash u(R)$ אוסף הלא הפיכים. M, לפי ההנחה, סגור לחיבור. אם $x \in R$ ו$a \in M$, אז xa לא הפיך, ונקבל שM אידאל מקסימלי יחיד, ולכן R מקומי.

תזכורת

יהי $\mathbb{F}$ שדה.

$$\mathbb{F}((x)) \supseteq \mathbb{F}[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n \middle| a_0, a_1, ... \in \mathbb{F} \right\} = R$$

הוכחנו שכל איבר עם מקדם חופשי$\neq 0$ הוא הפיך.

$\Leftarrow$ $R/u(R) = \{\sum a_n x^n | a_0 = 0\} = Rx$

$\Leftarrow$ $\mathbb{F}[[x]]$ חוג מקומי עם האידאל המקסימלי $Rx = \langle x \rangle$.

לדוגמה

נסמן את חוג השלמים הp־אדיים

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \middle| 0 \leq a_i \leq p^{i-1} \right\}$$

למשל אם $p=3$ אז $7 = 1 + 2 \cdot 3$.

כל מספר p־אדי שאינו שקול ל0 ב$\mathrm{mod}\ p$ הוא הפיך. כלומר:

$$u(\mathbb{Z}_p) = \mathbb{Z}_p \backslash p\mathbb{Z}_p$$

תרגיל

הוכח ש$\sqrt{11} \in \mathbb{Z}_p$