$R_1 \times R_2 \subset \prod R_i$ $\quad M_n(R)$

תת-חוגים

הגדרה-

יהי R חוג ותת חוג $S \subseteq R$ ותת קבוצה $X \subseteq R$ אז החוג הנוצר ע"י X מעל S נסמן $S[X] = S[a_1 \ldots a_n]$ את החוג המינימלי

$X = \{a_1 \ldots a_n\}$

המכיל את S ואת X.

דוגמאות: $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{2}]$

דוגמא:

אם R חוג קומוטטיבי ו-a איבר כלשהו אזי:

$R[a] = \{r_0 + r_1 a + r_2 a^2 + \ldots + r_n a^n \mid n \in \mathbb{N}, r_i \in R\}$

$(r_0 + r_1 a) + (r_1' a + r_2 a^2) = r_0 + (r_1 + r_1')a + r_2 a^2$

הגדרה-

יהי חוג R. חוג הפולינומים במשתנה X מעל R הוא $R[x] = \{r_0 + r_1 x + \ldots + r_n x^n\}$

משפט:

יהי R חוג קומוטטיבי ונניח $p(x) \in R[x]$ הוא מחלק אפס אז הוכיחו כי קיים איבר $b \in R$ כך ש- $bp(x) = 0$.

הוכחה:

p(x) מחלק אפס ולכן קיים $q(x) \in R[x]$ כך ש- $p(x)q(x) = 0$ ניקח q כזה מדרגה מינימלית. נסמן- $p(x) = a_0 + a_1 x + \ldots + a_n x^n$

$q(x) = b_0 + b_1 x + \ldots + b_m x^m$

$pq = 0$ ולכן המקדם העליון $a_n b_m = 0$ ולכן $a_n q(x)$ מדרגה קטנה מ-m

$(a_n q)p = 0$ כלומר הגם פולינום מדרגה $< m$ "מאפס" את p

ולכן $a_n q = 0$ כעת נשים לב- $(a_0 + a_1 x + \ldots + a_{n-1} x^{n-1})q(x)$

טענה: $R[x]^\times = R^\times$

הערה: $x \in Z(R[x])$

הגדר

הומומורפיזמים

הגדרה - פונקציה $\varphi : R_1 \to R_2$ נקראת **הומומורפיזם** (של חוגים) אם:
(1) היא הומומורפיזם של החבורות $(R_1, +)$.
(2) שומרת כפל

דוגמאות:

(א) $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ הוא הומו.
$a \to a \bmod (n)$

(ב) $\varphi : \mathbb{C} \to \mathbb{C}$, $z \to \bar{z}$ $\varphi(z_1 \cdot z_2) = \overline{z_1 \cdot z_2} = \bar{z_1} \cdot \bar{z_2} = \varphi(z_1) \cdot \varphi(z_2)$

(ג) $\det : M_n(R) \to R$ הוא לא הומו. אם R קומוטטיבי זה כן כפל.

(ד) הומו' הצבה: $\varphi_0 : R[x] \to R$
$x \to 0$
$p(x) \to p(0)$

(ה) הצבה כללית $a \in Z(R)$ אם $\varphi_a : R[x] \to R$
$x \to a$

תרגיל:

יהי $\varphi : \mathbb{Q} \to \mathbb{Q}$ הומו' של חוגים כך ש- $\varphi(1) = 1$ אזי $\varphi = id$.

הוכחה:

- אזי $n \in \mathbb{N}$ $\varphi(n) = \varphi(1 + \dots + 1) = \varphi(1) + \dots + \varphi(1) = n$
- מכיוון $\varphi(0) = 0$ אזי $0 = \varphi(1-1)$ $\varphi(1) - \varphi(1) \Rightarrow \varphi(-1) = -1$
  לכן $\varphi(-n) = -n$
- אזי $0 \neq m \in \mathbb{Z}$

$1 = \varphi(1) = \varphi\left(\frac{m}{m}\right) = \varphi(m) \cdot \varphi\left(\frac{1}{m}\right) = m \cdot \varphi\left(\frac{1}{m}\right) \Rightarrow \varphi\left(\frac{1}{m}\right) = \frac{1}{m}$
יחידות ההופכי.

- סך הכל:
$\varphi\left(\frac{n}{m}\right) = \varphi(n) \cdot \varphi\left(\frac{1}{m}\right) = \frac{n}{m}$.

דסי

תרגיל: מצאו את כל ההומו׳ האפשריים $\varphi: \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_7$

פתרון: ההרכבה $1\to 1$ ולכן ברור מה עושים עם איברי $\mathbb{Z}$ (   )

הבעיה היחידה זו התמונה של $\sqrt{2}$ היא ש- $\varphi(\sqrt{2})^2 = \varphi(2) = 2$

האיברים היחידים ב- $\mathbb{Z}_7$ שמקיימים זאת הם $3,4$.

ולכן יש 2 הומו׳ $\sqrt{2}\to 3$

$\sqrt{2}\to 4$

הגדרה- יהי $\varphi: R_1\to R_2$ **הומו׳**

התמונה של φ היא $Im\varphi$ והיא תת חוג של R_2

הגרעין של φ היא $\ker\varphi$ והוא תת חוג של R_1 עם תכונה נוספת: **בליעה**.

בליעה: לכל $x\in\ker\varphi$ ולכל $r\in R$ $rx, xr\in\ker\varphi$

הוכחה: $\varphi(xr) = 0$ $\quad \varphi(rx) = \varphi(r)\cdot\varphi(x) = \varphi(r)\cdot 0 = 0$

אידיאלים

הגדרה- יהי R חוג.

$L\subseteq R$ נקרא **אידיאל שמאלי** אם הוא תת חבורה חיבורית ו- $RL\subseteq L$ (בליעה משמאל)

$A\subseteq R$ נקרא **אידיאל ימני** אם הוא תת חבורה חיבורית ו- $AR\subseteq A$

$I\subseteq R$ נקרא **אידיאל** (דו-צדדי) אם $RIR\subseteq I$

דוגמאות:

1) $\{0\}$ הוא האידיאל הטריוויאלי.

2) R הוא עצמו אידיאל.

3) $\ker\varphi$ כש- φ הומו׳.

4) $I \trianglelefteq \mathbb{Z}[\sqrt{2}]$ $\quad I = \{a+b\sqrt{2} \mid a\in 2\mathbb{Z},\ b\in\mathbb{Z}\}$

סגור לחיבור: $(2a+b\sqrt{2})+(2a'+b'\sqrt{2})$

בליעה: $\underset{\in R}{(a'+b'\sqrt{2})}\underset{\in I}{(2a+b\sqrt{2})} = \underset{\in 2\mathbb{Z}}{2aa'+2bb'}+(a'b+2b'a)\sqrt{2}$

[illegible]

(5) אם R חוג, $x \in R$ אזי Rx הוא אידיאל שמאלי.
xR הוא אידיאל ימני.
$RxR = \{\sum_{i=1}^{n} r_i x r_i'\}$ הוא אידיאל (דו-צדדי)

(6) האידיאלים היחידים ב- $\mathbb{Z}$ הם $n\mathbb{Z}$.

(7) $R[x] \trianglerighteq \langle x \rangle =: (R[x])x(R[x]) = X(R[x])$

$x \in Z(R[x])$

הוכחה: נראה ש- $\langle x \rangle = \ker\varphi_0$ ברור ש- $\ker\varphi_0 \supseteq \langle x \rangle$

למה? $\varphi_0(xp(x)) = 0 \cdot p(0) = 0$

וניח $p(x) \in \ker\varphi_0$ אזי $\varphi_0(p(x)) = p(0) = 0$ אם נכתוב

$p(x) = a_0 + a_1x + \dots + a_nx^n$ $\Leftarrow$ $p(0)=0$ $\Rightarrow$ $a_0 = 0$

ולכן $p(x) = a_1x + \dots + a_nx^n$ כלומר $p(x) = x(a_1 + a_2x + \dots + a_nx^{n-1})$

ולכן $p(x) \in \langle x \rangle$.

תרגיל: $m\mathbb{Z} \subseteq n\mathbb{Z} \iff n|m$ (מספרים)

טענה:
אידיאל $I \trianglelefteq R$ הוא אמיתי ($I \neq R$) $\iff 1 \notin I \iff$ אין איבר הפיך ב- I

מסקנה:
אם R חוג עם חילוק אין אידיאלים שונים מ- 0 ו- R.

סכום וחיתוך וכפל אידיאלים!

הגדרה:

$I_1, I_2 \trianglelefteq R$

$I_1 \cap I_2 \trianglelefteq R$ האידיאל המקסימלי שמוכל ב- I_1 וב- I_2.

$I_1 + I_2 \trianglelefteq R$ האידיאל המינימלי שמכיל את I_1 ו- I_2.

$I_1 \cdot I_2 \trianglelefteq R$ $\quad I_1 \cap I_2 \supseteq \{\sum a_ib_i \mid a_i \in I_1, b_i \in I_2\}$

$I_1 + I_2$

$I_1 \qquad I_2$

$I_1 \cap I_2$

$I_1 \cdot I_2$

$\Leftarrow$ יש שרשרת אידיאלים (רוחב לסדר ההכלה)

הערה

(5) יהי R חוג, $x\in R$, אזי Rx הוא אידיאל שמאלי,
xR הוא אידיאל ימני,
$RxR=\{\sum_{i=1}^{n} r_i x r_i'\}$ הוא אידיאל (דו-צדדי)

(6) האידיאלים היחידים ב-$\mathbb{Z}$ הם $n\mathbb{Z}$.

(7) $\langle x\rangle \triangleleft R[x]$:$= (R[x])\,x\,(R[x]) = x(R[x])$

$x \in Z(R[x])$

הוכחנו! נראה ש- $\ker\varphi_0=\langle x\rangle$ קודם ש- $\ker\varphi_0\supseteq\langle x\rangle$
למה? $\varphi_0(x\cdot p(x))=0\cdot p(0)=0$
עכשיו $p(x)\in\ker\varphi_0$ אזי $\varphi_0(p(x))=p(0)=0$ אם נרשום
$p(x)=a_0+a_1x+\dots+a_nx^n$ $p(0)=0 \Rightarrow a_0=0$
לכן $p(x)=a_1x+\dots+a_nx^n$ כלומר $p(x)=x(a_1+a_2x+\dots+a_nx^{n-1})$
לכן $p(x)\in\langle x\rangle$

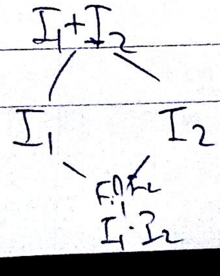
תרגיל! $n\mathbb{Z}\subseteq m\mathbb{Z} \iff m|n$ ([illegible])

טענה!
אידיאל $I\triangleleft R$ הוא **אמיתי** $(I\neq R) \iff 1\notin I \iff$ אין איברים הפיכים ב-I

מסקנה!
אם R חוג עם חילוק אין אידיאלים שאינם רק 0 ו-R.

סכום, חיתוך וכפל אידיאלים!

תזכורת!
$I_1,I_2\triangleleft R$
$I_1\cap I_2\triangleleft R$ האידיאל המקסימלי שמוכל ב-I_1 וב-I_2
$I_1+I_2\triangleleft R$ האידיאל המינימלי שמכיל את I_1 ו-I_2.
$I_1\cdot I_2\triangleleft R$ $I_1\cap I_2 \supseteq \{\sum a_ib_i \mid a_i\in I_1,\ b_i\in I_2\}$



$\Leftarrow$ ויש שרשרת אידיאלים (בדומה לסדר ההכלה)

לפי

טענה:

האידיאלים המקסימליים ב- $R[[x]]$ הם מהצורה-

$$R^x - xR[[x]] = R^x(1 - xR[[x]])$$

$$\begin{tikzcd}[column sep=small] & I_1+I_2 \arrow[dl, dash] \arrow[dr, dash] & \\ I_1 \arrow[dr, dash] & & I_2 \arrow[dl, dash] \\ & I_1 \cap I_2 \arrow[d, dash] & \\ & I_1 \cdot I_2 & \end{tikzcd}$$

הוכחה:

נתחיל מלהראות ש $1-xp(x)$ הפיך -

$$\frac{1}{1-xp(x)} \approx \sum_{n=0}^{\infty}(xp(x))^n$$

מתקיים ש- $\sum(xp(x))^n \in R[[x]]$

$$\sum(x^n p(x)^n) = p(x) + xp(x)$$

המקדם של x^0 = המקדם של x^0 ב- $p(x)$

המקדם של x^1 = המקדם של x^1 ב- $p(x)$ + המקדם של x^0 ב- $xp(x)$.

הרעיון הוא שבסוף המקדם של x^n מסתכם לסכום מקדמים

$$p(x) + xp(x) + \dots + x^n p(x)$$

תרגיל:

הוכיחו כי כל אידיאל של $F[[x]]$ (כאשר F שדה) הוא מהצורה $\langle x^t \rangle$

כאשר t סופי.

הוכחה:

יהי $I \lhd F[[x]]$ ניקח $\sum a_i x^i = p(x) \in I$ כך ש- $\min\{i \mid a_i \neq 0\}$ מינימלי. נסמן את האינדקס הזה ב-k כלומר-

$$p(x) = a_k x^k + a_{k+1}x^{k+1} + \dots = x^k \underbrace{(a_k + a_{k+1}x + \dots)}_{\text{הפיך (כפי ראינו קודם)}} \Rightarrow \langle x^k \rangle$$

ולכן $\langle x^k \rangle = I$