shira.gilat@live.biu.ac.il

בס"ד

תרגול 1
29/02/16

דוגמא: אם G חבורה חילופית (אבלית)
$End(G)=\{f:G\to G \text{ הומו}\}$

זהו חוג ביחס לחיבור והרכבה.

תזכורת:

· איבר הפיך מימין $x\square=1$, הפיך משמאל $\square x=1$ והפיך.

· חוג שבו כל איבר הוא הפיך נקרא חוג עם חילוק.

דוגמא: נניח V מ"ו ממימד אינסופי $\aleph_0$ ונסתכל על החוג $End(V)$ ונגדיר

$$T(a_1,\dots a_\dots)=(0,a_1,\dots)$$
$$S(a_1,a_2,\dots)=(a_2,\dots)$$

$S\circ T=1$ T הפיך משמאל, S הפיך מימין.

אך T ו-S לא הפיכים.

תרגיל: יהי R חוג $a\in R$ הפיך מימין ולא הפיך משמאל הראה של-a יש ∞ הופכים מימין.

פתרון:

a הפיך מימין ולכן קיים $b\in R$ כך ש $ab=1$ ונגדיר לכל: $i\in\mathbb{N}$
$b_i=(1-ba)a^i+b$

נראה ש-b_i הופכי מימין ל-a:

$$ab_i=a[(1-ba)a^i+b]=a^{i+1}-aba^{i+1}+ab=ab=1$$

נראה ש-b_i שונים אחד מהשני: נניח בשלילה שיהיו $i<j$ כך ש $b_i=b_j$

$$(1-ba)a^i+\cancel{b}=(1-ba)a^j+\cancel{b}$$
$$(1-ba)a^i=(1-ba)a^j \quad /\cdot b^j \text{ מימין}$$
$$(1-ba)\underbrace{a^ib^j}_{1}=(1-ba)=a^{j-i}$$

$$1=((1-b)a^{j-i-1}+b)a$$

לכן a הפיך משמאל - סתירה!

מסקנה: אם R חוג סופי אז כל איבר הפיך מימין הוא הפיך.

דוגמא: $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$
הוא שדה (כלומר חוג + חילוק קומוטטיבית)

הוכחה: חוג ✓
קומוטטיבי ✓.
הופכיים: ניקח איבר $a+b\sqrt{2}\neq 0$ ונמצא לו איבר הופכי:

$$\frac{1}{a+b\sqrt{2}}\cdot\frac{a-b\sqrt{2}}{a-b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}$$

נשים לב ש- $a^2-2b^2\neq 0$ כי $a+b\sqrt{2}\neq 0$

$$\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$$

דוגמא: זה חוג, לא שדה אך ישנן איברים הפיכים?

הוכחה: כמו לא שדה & כלומר 3 לו הפך. מתי איבר ב- $\mathbb{Z}[\sqrt{2}]$ הוא הפיך?
נובע מהנוסחה שמצאנו שעבור $\mathbb{Z}[\sqrt{2}]\subset\mathbb{Q}(\sqrt{2})$ צריך ש- $a^2-2b^2=\pm 1$

כך ההופכי בצורה ב- $\mathbb{Z}[\sqrt{2}]$
דוגמא: $a=3,\ b=2$ אז - $x=3+2\sqrt{2}$ הוא הפיך ונקבל ש- x^k $k\in\mathbb{N}$

דוגמא: חוג עם חילוק לא קומוטטיבי - קווטרניונים

$$\mathbb{H}=\left\{\begin{pmatrix}a&b\\ \bar{b}&\bar{a}\end{pmatrix}\mid a,b\in\mathbb{C}\right\}\subseteq M_2(\mathbb{C})$$

זה חוג
כל איבר $\neq 0$ הוא הפיך (וההופכי שלו גם ב- H)
נסמן $1=\begin{pmatrix}1&\\&1\end{pmatrix}$ $i=\begin{pmatrix}i&\\&-i\end{pmatrix}$
$\mathbb{H}=\mathrm{span}\{1,i,j,k\}$ אז $j=\begin{pmatrix}&-1\\1&\end{pmatrix}$ $k=\begin{pmatrix}&-i\\-i&\end{pmatrix}$

וגם $ij=-ji=k$
סימון: יהי חוג R נסמן ב- $R^\times$ את כל ההפיכים ב- R. זה לא חוג!
$1-1\in R^\times$ אבל כן סגור תחת הכפלה (x,y הפיכים $\Rightarrow$ xy הפיך)

דקה:

תרגיל: אם R קומוטטיבי $xy\in R$ ו-xy הפיך אז גם x,y הפיכים

פתרון: $x^{-1}=y(xy)^{-1}$

$y^{-1}=(xy)^{-1}x$

דוגמא נגדית למקרה הלא קומוטטיבי: V ממימד ∞ $T,S\in End(V)$

ההרכבה TS = הפיכה אבל T,S לא הפיכות.

תרגיל: יהי R חוג ונניח שכל איבר $0\neq a\in R$ הפיך משמאל. הוכח כי R חוג עם חילוק

פתרון: ניקח $a\neq 0$ לפי ההנחה ישנו הופכי משמאל $\exists x\in R$ $xa=1$

גם לו קיים הופכי משמאל $\exists y\in R$ $yx=1$

אז $y(xa)=y\cdot 1$ ⇐ $yxa=y$ ⇐ $a=y$ כלומר $ax=1$ ⇐ $x=a^{-1}$

הגדרה- יהי R חוג. אז איברים $0\neq a,b\in R$ המקיימים $ab=0$ אז

a נקרא מחלק אפס משמאל

b נקרא מחלק אפס מימין.

הגדרה- חוג שאין בו מחלקי אפס נקרא תחום.

תחום קומוטטיבי נקרא תחום שלמות.

דוגמאות: תחום- $\mathbb{Z}$, $2\mathbb{Z}$, שדה.

לא תחום- $M_n(F)$ $\mathbb{Z}_6 - 2\cdot 3=0$.

הערה:

איבר הפיך (מימין/משמאל) הוא אף פעם לא מחלק אפס לכן כל חוג עם חילוק הוא תחום.

תרגיל:

תחום סופי כל איבר $\neq 0$ הוא או הפיך או מחלק אפס.

פתרון: נניח $0\neq a\in R$ ונניח שהוא לא הפיך.

נסתכל על $ab_1, ab_2, ..., ab_n$ כאשר ... אומר כחוק.

$ab_i\neq 1$ לכל i לפי ההנחה.

רמז

ולכן לפי שובך היונים יש $i \neq j$ המקיימים $a(b_i - b_j) = 0$

$ab_i = ab_j$

לכן a_3 מחלק אפס.

מסקנה: תחום סופי הוא חוג עם חילוק.
תחום שלמות סופי הוא שדה.

תת חוג -

הגדרה - $S \subseteq R$ תת-חוג אם הוא חוג (אופציונלי $1_R \in S$)

דוגמאות: $\phi \subset n\mathbb{Z} \subseteq \mathbb{Z}$ $n\mathbb{Z}$ תת חוג בלי יחידה של ϕ.

קריטריון: $S \subseteq R$ תת חוג אם:

- $S \neq \phi$
- סגירות לחיסור $a, b \in S \to a - b \in S$
- סגירות לכפל
- $1_R \in S$

הגדרה - יהי R חוג. המרכז של R הוא:

$$Z(R) = \{x \in R \mid \forall y \in R;\ xy = yx\}$$

המרכז של R הוא:

$$C_R(S) = \{x \in R \mid \forall s \in S: xs = sx\}$$

טענה: $C_R(S)$ הוא תת חוג.

טענות:

(1) אם R קומוטטיבי $C_R(S) = R$.

(2) R קומוטטיבי $\leftrightarrow$ $Z(R) = R$

(3) אם $A \subseteq B$ אז $C_R(A) \supseteq C_R(B)$.

(4) $S \subseteq C_R(C_R(S))$

הוכחה:

יהי $s \in S$ וניקח $x \in C_R(S)$ ונרצה להוכיח $xs = sx$ וזה הגיוני.

(5) $C_R(S) = C_R(C_R(C_R(S)))$

מינימליות (ב) נסמן $X=C_R(S)$ אזי $X\subseteq C_R(C_R(X))$ לפי (4)

(ג) לפי (3)+(4)

תכונות עולה/יורדת מתת חוג

$S\subseteq R$

	יורד	עולה
קומוטטיביות	כן	לא
איבר הפיך	לא $\mathbb{Z}\subseteq\mathbb{R}$ 2 הפיך למעלה אך לא מטה	כן
להיות חוג עם חילוק	לא	לא $\mathbb{H}\subseteq M_2(\mathbb{C})$
איבר מחלק 0	לא $\begin{pmatrix}x&x\\0&0\end{pmatrix}\in M_2(\mathbb{R})$	כן
תחום	כן	לא $\begin{pmatrix}x&0\\0&0\end{pmatrix}\in M_2(\mathbb{R})$

דוג'

דוגמא 2) $R_1\times R_2 \subseteq \prod R_i$ $\quad M_n(R)$

מת-חוגים

הגדרה-

יהי R חוג ותת חוג $S\subseteq R$ ות"ק $X\subseteq R$ את החוג הנוצר ע"י X מעל S נסמן $S[X]=S[a_1 \dots a_n]$ את החוג המינימלי

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

שמכיל את S ואת X.

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

דוגמה:

אם R חוג קומוטטיבי ו-a איך נראה אותו:

$$R[a]=\{r_0+r_1a+r_2a^2+\dots+r_na^n \mid n\in\mathbb{N},\ r_i\in R\}$$

$$(r_0+r_1a)+(r_1'a+r_2a^2)=r_0+(r_1+r_1')a+r_2a^2$$

הגדרה-

יהי R חוג. חוג הפולינומים במשתנה X מעל R הוא $R[x]=\{r_0+r_1x+\dots+r_nx^n\}$

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- $p(x)q(x)=0$ נניח ש-q מדרגה מינימלית. (נסמן-

$$p(x)=a_0+a_1x+\dots+a_nx^n$$
$$q(x)=b_0+b_1x+\dots+b_mx^m$$

$pq=0$ ולכן המקדם העליון $a_nb_m=0$ ולכן $a_nq(x)$ מדרגה קטנה מ-m

$(a_nq)p=0$ כלומר הוא פולינום מדרגה $< m$ "מאפס" את p

ולכן $a_nq=0$ כעת נשים לב- $(a_0+a_1x+\dots+a_{n-1}x^{n-1})q(x)$

טענה: $R[x]^\times=R^\times$

הערה: $x\in Z(R[x])$

הומומורפיזמים

הגדרה - פונקציה $\varphi: R_1 \to R_2$ נקראת הומומורפיזם (של חוגים) אם:

(1) היא הומומורפיזם של חבורות $(R,+)$.

(2) שומרת כפל

דוגמאות:

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

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

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

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

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

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

הוכחה:

- עבור $n \in \mathbb{N}$ $\quad \varphi(n) = \varphi(1+\dots+1) = \varphi(1) + \dots + \varphi(1) = n$
- מכאן $\varphi(0)=0$ אזי $0 = \varphi(1-1) \quad \varphi(1)-\varphi(1) \Rightarrow \varphi(-1)=-1$

ולכן $\varphi(-n) = -n$

- עבור $0 \neq m \in \mathbb{Z}$
$1 = \varphi(1) = \varphi(\frac{m}{n}) = \varphi(m) \cdot \varphi(\frac{1}{n}) = m \cdot \varphi(\frac{1}{m}) \Rightarrow \varphi(\frac{1}{m}) = \frac{1}{m}$

יחידות ההופכי.

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

דף:

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

פתרון: הוכחנו $1\to1$ ולכן ברור מה עושים על איברי $\mathbb{Z}$ ( )

השאלה היחידה על התמונה של $\sqrt{2}$ והיא יש- $\varphi(\sqrt{2})^2=\varphi(2)=2$

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

ולכן יש 2 הומו $\sqrt{2}\to3$

$\sqrt{2}\to4$

הגדרה- יהי $\varphi:R_1\to R_2$ הומו'

התמונה של φ היא $\operatorname{Im}\varphi$ ותת חוג של R_2

הגרעין של φ הוא $\ker\varphi$ והוא תת חוג של R_1 עם תכונה נוספת:

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

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

אידיאלים

הגדרה- יהי R חוג.

$L\subseteq R$ נקרא אידיאל שמאלי אם הוא תת חבורה חיבורית ו- $RL\subseteq L$ (כלומר 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) $\{0\}$ זהו האידיאל הטריוויאלי.

(2) R הוא לעצמו אידיאל.

(3) $\ker\varphi$ כש- φ הומו'.

(4) $I\trianglelefteq\mathbb{Z}[\sqrt{2}]$ $I=\{a+b\sqrt{2} \mid a\in2\mathbb{Z}, b\in\mathbb{Z}\}$

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

סגור לכפל: $\underbrace{(a'+b'\sqrt{2})}_{\in R}\underbrace{(2a+b\sqrt{2})}_{\in I}=\underbrace{2aa'+2bb'}_{\in 2\mathbb{Z}}+(a'b+2b'a)\sqrt{2}$

דוגמ'

(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) $R[x] \rhd \langle x\rangle =: (R[x])x(R[x]) = x(R[x])$

$$\downarrow$$

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

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

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

יהי $p(x)\in\ker\varphi_0$ אזי $\varphi_0(p(x))=p(0)=0$ אם נרשום

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

$a_0=0 \Leftarrow p(0)=0$

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: $m\mathbb{Z}\subseteq n\mathbb{Z} \iff n|m$ (מתמטיקה 1)

טענה: אידאל $I\lhd R$ הוא אמיתי $(I\neq R) \iff 1\notin I \iff$ אין איברים הפיכים ב-I

מסקנה:
אם R חוג עם חילוק אז האידיאלים שלו הם רק 0 ו-R.

סכום וחיתוך וכפל אידאלים!

הגדרה:

$I_1, I_2 \lhd R$

$I_1\cap I_2\lhd R$ האידאל המקסימלי שמוכל ב- I_1 וב- I_2.

$I_1+I_2\lhd R$ האידאל המינימלי שמכיל את I_1 ו- I_2.

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

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

$\Leftarrow$ יש שריג אידיאלים (כמו לסבר ההרצאה)

Scanned by CamScanner

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

לפני

טענה:
האידיאלים המקסימליים ב- $R[[x]]$ הם מהצורה-
$R^x - xR[[x]] = R^x(1-xR[[x]])$

הוכחה:
נתחיל מהראיה, ש- $1-xp(x)$ הפיך -
$$\frac{1}{1-xp(x)} = \sum_{n=0}^{\infty}(xp(x))^n$$
מספיק 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- $xp(x)$.
$\vdots$
הטיעון הזה שהמקדם של x^n מספיק לסכום מקדמים
$p(x)+xp(x)+\dots+x^n p(x)$

תרגיל:
הוכיחו כי כל אידיאל של $F[[x]]$ (כאשר F שדה) הוא מהצורה $\langle x^k\rangle$
כאשר k טבעי.

הוכחה:
יהי $I \trianglelefteq F[[x]]$ 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-
$$p(x) = a_k x^k + a_{k+1}x^{k+1} + \dots = x^k\underbrace{(a_k + a_{k+1}x + \dots)}_{\text{הפיך (לפי תרגיל קודם)}} \in \langle x^k\rangle$$

ולכן $\langle x^k\rangle = I$

רצא

אלג' 3

<u>פולינומים, טורים</u>

$R[x] \subset R$

טענה: אם R תחום $R[x]^\times = R^\times$

טענה: אם R קומוטטיבי $p(x)=a_0+a_1x+\dots+a_nx^n\in R[x]$ הוא הפיך

$(\Leftrightarrow)$ a_0 הפיך ו- a_i לכל $1\le i\le n$ נילפוטנטי.

דוגמה

נניח: בתוך קומוטטיבי אם 4 הוא הפיך ו-x נילפוטנטי אז $4+x$ הפיך.

$$\left(4\left(1-\frac{x}{4}\right)\right)^{-1} = 4^{-1}\left(1+\left(\frac{-x}{n}\right)+\left(\frac{-x}{4}\right)^2+\dots+0\right)$$

הוכחה:

$(\Leftarrow)$ a_i נילפוטנטי ($i\neq 0$) ולכן כל a_ix^i נילפוטנטי (קומוטטיביות)

וסכום נילפוטנטים הוא נילפוטנטים ולכן נקבל

$p(x)=a_0+y(a_1x+\dots a_nx^n)$

כאשר x נילפוטנטי. ונקבל ש- a_0 הפיך ולפי הלמה $p(x)$ הפיך.

$(\Rightarrow)$ נניח $p(x)$ הפיך $p(x)\cdot q(x)=1$

$p(x)=\sum^n a_ix^i$

$q(x)=\sum^m b_ix^i$

$a_0b_0=1 \Rightarrow a_0$ הפיך.

$a_nb_m=0$

$a_{n-1}b_m+a_nb_{m-1}=0 \xrightarrow{\cdot a_n} a_n^2b_{m-1}=0$ $\qquad a_n^k\cdot b_{m-k+1}=0.$

$a_{n-2}b_m+a_{n-1}b_{m-1}+a_nb_{m-2}= \xrightarrow{a_n^2} a_n^3b_{m-2}=0$

$\vdots$

$\dots + a_{n-1}b_1+a_nb_0=0 \xrightarrow{a_n^m} a_n^{m+1}\cdot b_0=0.$

$\Downarrow$

אבל b_0 הפיך ולכן קיבלנו $a_n^{m+1}=0 \Rightarrow a_n$

חוזרים על אותו תהליך על פולינום $\underbrace{p(x)}_{\text{הפיך}}-\underbrace{a_nx^n}_{\text{נילפוטנטי}}$ שהוא הפיך נילפוטנטי.

לפי הלמה.

Scanned by CamScanner

דגש:

וכן הלאה, קיבלנו שכל המשתנים נילפוטנטים

$\square$.

חוג חזקות פורמליים

$$R[[X]] = \{ \sum a_n x^n \mid a_i \in R \}$$

<u>טענה:</u> $1+X\cdot P(X)$ הוא איבר הפיך שמה.

$P(X) \in R[[X]]$

$$\frac{1}{1-X\cdot P(X)} = \sum_{n=0}^{\infty} (XP(X))^n \in R[[X]]$$

<u>טענה:</u> איבר $f(x) \in R[[X]]$ הפיך $\Leftrightarrow$ המקדם החופשי הוא הפיך.

כי:

$$f(x) = a_0 + a_1 X + \dots = a_0(1 + a_0^{-1}a_1 X + a_0^{-1}a_2 X^2 + \dots)$$

$$= \underbrace{a_0}_{\text{הפיך לפי הנתון}} \underbrace{(1 + X(\underbrace{a_0^{-1}a_1 + a_0^{-1}a_2 X + \dots}_{p(x)}))}_{\text{הפיך}}$$

<u>משל</u>.

חוג טורי לורן

$$R((X)) = \left\{ \sum_{i=-n}^{\infty} a_i x^i \;\middle|\; \begin{array}{c} a_i \in R \\ n \in \mathbb{N} \end{array} \right\}$$

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

לאיבר של $R((X))$ $(R[[X]])$ אין דרגה / מעלה מוגדרת, אך במקום זה מגדירים-

<u>הערכה</u>: $v: R((X)) \to \mathbb{Z} \cup \{\infty\}$

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

$$v(0) = \infty$$

287

למה: $v(f+g) \ge \min\{v(f), v(g)\}$

$v(f\cdot g) \ge v(f)+v(g)$ זה תחום ועל להוכיח שאתם לבד

אם R תחום אז זה שוויון

טענה: אם R תחום אז גם $R[[x]]$ הוא תחום.

טענה: אם F שדה $F((x))$ (טורי לורן מעל השדה) הוא גם שדה.

הוכחה:

$$f(x)=\sum_{-n}^{\infty} a_i x^i = x^{-n}\underbrace{\left(a_{-n}+a_{-n+1}x+\dots\right)}_{g(x)\ \in\ F[[x]]}$$

$\ne 0$, $-n = v(f(x))$

המקדם החופשי של $g(x)$ הוא $0 \ne a_n \in F$ (זה הקצינה אין להוכיח $\ne 0$)

ולכן הפיך.

ו-x^{-n} בוודאי הפיך ולכן $f(x)$ הפיך.

$\blacksquare$

את כל הדברים שלמדנו אפשר לעשות שוב ושוב... $(R[[x]](y))[z]$ - פולינום ב-z שהמקדמים שלו

הם טורי לורן ב-y שהמקדמים שלהם הם חזקות פורמליות.

הערה: חוקי חילוף:

$$R[x_1,x_2,\dots,x_n]=R[x_1][x_2]\dots[x_n]$$

$$R[x][y]=R[y][x]$$

$$\sum_{k=0} (p_k(x))\, y^k = \sum_{k=0}^{n} q_k(y)\, x^k$$

תרגיל: בחוג חזקות הכללית נסה?

$$F((x))(y) \underset{\ne}{\subset} F[y][(x)] \underset{\ne}{\subset} F[[x]]((y))$$

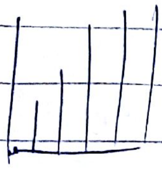
$$\left\{ \sum\left(\sum_{i=0}^{k} a_{i,k} x^i\right) y^k \right\}$$

לפי

דוגמא להכלה ממשית:

$F[[x]][y] \subsetneq F[y][[x]]$

$\sum_{k=1}^{\infty}\left(\sum_{i=1}^{k} y^i\right) x^k$



הערה: $F((x))((y)) \neq F((x,y))$

משל: $\sum_{n=1}^{\infty}(x^{-n})\,y^n \notin F((x,y))$

להסתכל בסוף ההגדרה של הנושא הזה.

אידיאלים

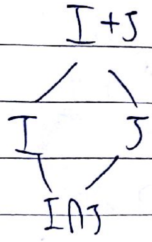
$I \triangleleft R$ אם $RIR \subseteq I$

אידיאל ראשי - $\langle x\rangle = \left\{\sum_{\text{סופי}} r_i x r_j\right\}$

$I/+$

בחוג קומוטטיבי -

$\langle x\rangle = Rx = xR$



$IJ = \left\{\sum_{\text{סופי}} a_i b_i \;\middle|\; a_i \in I,\ b_i \in J\right\}$

הערה: אי אפשר להגדיר - $IJ = \left\{ab \;\middle|\; a\in I,\ b\in J\right\}$ כי לא סגור לחיבור.

~~משל~~

$\cancel{\langle x\rangle, \langle y\rangle \triangleleft F(x,y)}$

$\cancel{\langle x\rangle * \langle y\rangle = \{x\cdot p(x), y\,q(x,y)\}}$

תרגיל: הוכיחו כי האידיאל $I=\langle 2,x\rangle \triangleleft \mathbb{Z}[x]$ אינו ראשי

$\Downarrow$

$\langle 2\rangle + \langle x\rangle$

הוכחה: איבר כללי באידיאל - $H(x) = 2\cdot f(x) + x\cdot g(x)$

כאשר $f,g \in \mathbb{Z}[x]$ קל לראות ש $1 \notin I$. מאחר ולא להגיד 0 כי $\mathbb{Z}[x]$ הוא קומוטטיבי.

לכן

נשים לב כי $2\in 2\mathbb{Z}$ $(h(0)\in 2\mathbb{Z})$ ולכן $I \subsetneq \mathbb{Z}(x)$ (אידאל אמיתי - מוכל ממש).

שימו לב - ש- $\mathbb{Z}[x]$ הוא ראשי: $(\mathbb{Z}(x) = \langle 1\rangle)$

הראנו שהוא לא ראשי:

נניח בשלילה שקיים $q(x)$ כך ש- $\langle q(x)\rangle = \langle 2,x\rangle = I$

לפיכך - $2,x\in\langle q\rangle$ ולכן $2=q(x)\cdot a(x)$
$x=q(x)\cdot b(x)$

כאשר $a(x),b(x)\in\mathbb{Z}[x]$

אבל אין אף פולינום שמחלק גם את 2 וגם את x. חוץ מ- $q=1$

אבל אם $q=1$ אז $I=\langle q\rangle=\mathbb{Z}[x]$ בסתירה לכך שראינו קודם שהוא אידאל אמיתי.

חוג מנה

$I \triangleleft R$ אז- $R/I = \{r+I \mid r\in R\}$ חוג מנה.

$(r_1+I)+(r_2+I) = r_1+r_2+I$

$(r_1+I)(r_2+I) = r_1\cdot r_2+I$

$0_{R/I} = 0+I = I$

$1_{R/I} = 1+I$

דוגמאות

(1) $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ כחוגים!

(2) $3\mathbb{Z}/18\mathbb{Z} = \{0+18\mathbb{Z}, 3+18\mathbb{Z}, 6+18\mathbb{Z}, 9+18\mathbb{Z}, 12+18\mathbb{Z}, 15+18\mathbb{Z}\}$

כמבנה חבורה חיבורית - $3\mathbb{Z}/18\mathbb{Z} \cong \mathbb{Z}_6$

כמבנה חוגים - (טבלת כפל) -

	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\bar{12}$	$\bar{15}$
$\bar{0}$	0	0	0	0	0	0
$\bar{3}$	0	9	0	9	0	9
$\bar{6}$	0	0	0	0	0	0
$\bar{9}$	0	9	0	9	0	9
$\bar{12}$	0	0	0	0	0	
$\bar{15}$	0	9	0	9	0	9

הוכח ש- $3\mathbb{Z}/18\mathbb{Z} \cong \mathbb{Z}_6$ כאיזו חוגים

(3) $I = \langle x^2+1 \rangle \triangleleft \mathbb{R}[x]$

תאר את המנה $\mathbb{R}[x]/\langle x^2+1 \rangle$

$\boxed{p(x)+I = \overline{p(x)} \quad \text{:סימון}}$

$\bar{1}$

$\bar{x}$ -

$\overline{x^2} = x^2 + \langle x^2+1 \rangle = x^2 - (x^2+1) + \langle x^2+1 \rangle = -1 + I = \overline{-1}$

$\overline{x^3} = \overline{x^2} \cdot \bar{x} = -\bar{x}$

$\overline{x^4} = \bar{1}$

$\mathbb{R}[x]/\langle x^2+1 \rangle = \{ p(x)+I \mid p(x) \in \mathbb{R}[x] \}$ - כל המחלקות הן

$= \{ \overline{a_0 + a_1 x + \dots + a_n x^n} \mid ? \} = \{ a_0 \cdot \bar{1} + a_1 \bar{x}^2 + \dots + a_n \bar{x}^n \mid ? \}$

$= \{ b_0 \cdot \bar{1} + b_1 \bar{x} \mid b_0, b_1 \in \mathbb{R} \} \cong \mathbb{C}$

$\bar{x}^2 = -1 \qquad \bar{x} \to i$

$\bar{1} \to 1$

$\bar{1} =$ (4) $\langle x^2-3 \rangle \triangleleft \mathbb{Q}[x]$

$\bar{x} =$

$\overline{x^2} = x^2 + \langle x^2-3 \rangle = x^2 - (x^2-3) + \langle x^2-3 \rangle = 3 + \langle x^2-3 \rangle = \bar{3}$

$\overline{x^3} = \overline{x^2} \cdot \bar{x} = \bar{3}\bar{x}$

$\vdots$

$\mathbb{Q}/\langle x^2-3 \rangle = \{ p(x) + \langle x^2-3 \rangle \mid p \in \mathbb{Q}[x] \} = \{ \overline{a_0} + a_1 \bar{x} + \dots + a_n \bar{x}^n \mid ? \}$

$= \{ \bar{b_0} + b_1 \bar{x} \mid b_0, b_1 \in \mathbb{Q},\ \bar{x}^2 = 3 \} \cong \mathbb{Q}[\sqrt{3}]$.

17.7

<u>תרגיל:</u> הוכיחו כי $R_2 = \mathbb{C}[x,y]/(y-x^2) \ncong R_1 = \mathbb{C}[x,y]/(xy-1)$

<u>פתרון:</u> נפרש את שני החוגים <u>מצד אחד:</u> $R_2 \xrightarrow[\substack{x \to t \\ y \to t^2}]{\sim} \mathbb{C}[t]$

<u>מצד שני:</u> $R_1 \xrightarrow[\substack{x \to t \\ y \to t^{-1}}]{\sim} \mathbb{C}[t,t^{-1}]$

עכשיו נשאר להוכיח ש- $\mathbb{C}[t] \ncong \mathbb{C}[t,t^{-1}]$

נסתכל על האיברים <u>ההפיכים</u> ב- $\mathbb{C}[t]^\times = \mathbb{C}^\times = \mathbb{C}-\{0\}$

נשים לב- $\mathbb{C}[x]^\times \cup \{0\}$ מקבלים קבוצה סגורה לחיבור

(למעשה זה מיוחד לחוגים).

<u>ואילו</u> אם נסתכל על - $\mathbb{C}[t,t^{-1}]^\times \cup \{0\}$ הוא לא סגור לחיבור.

<u>נימוק:</u> $t+1$ הוא לא הפיך.

בס"ד

תרגול 4
21/03/16

תזכורות

משפט ההתאמה:

$I \triangleleft R$

כל אידיאל של R/I הוא J/I . $I \subseteq J$. $J \triangleleft R$

משפט האיזומורפיזם הראשון: $\varphi: R \to S$ $\operatorname{Im}\varphi \cong R/\ker\varphi$ ואם על

על: $R/\ker\varphi \cong S$

דוגמא: אפימורפיזם ההצבה $\varphi_0: \mathbb{R}[x] \to \mathbb{R}$, $x \to 0$ ולכן $\mathbb{R}[x]/\langle x\rangle \cong \mathbb{R}$

נוכיח ש- $\ker\varphi_0 = \langle x\rangle$

$$\ker\varphi_0 = \{p(x) \in \mathbb{R}[x] \mid \varphi_0(p) = p(0) = 0\}$$

מהשוויון

$$= \{a_0 + a_1x + \dots a_nx^n \mid a_0 = 0\} = \{a_1x + \dots a_nx^n \mid \ \}$$

$$= \{(a_1 + \dots a_nx^{n-1})x \mid \ \} = \langle x\rangle$$

הכללה: $c \in Z(R)$: $\varphi_c: R[x] \to R$, $x \to c$ $\ker\varphi_c = \langle x - c\rangle$

דוגמא: $\varphi_0: R[x,y] \to R[y]$

$$R[x,y]/\langle x\rangle \cong R[y]$$

דוגמא: $R \subseteq S$ תת-חוג ו- $a \in C_R(S)$

קבוצת האיברים ב-R שמתחלפים עם איברי S

$S[x] \to S[a]$, $x \to a$

~~$S[x]/\langle x-a\rangle$~~

תרגיל: $\mathbb{Q}[x]/\langle x^2-3\rangle \cong \mathbb{Q}[\sqrt{3}]$

הערות: לגבי קומוטטיבי - $\langle x\rangle = RxR = xR$

משפטי האיזומורפיזם ה-II וה-III:

II $S\subset R$ תת-חוג, $I\lhd R$ אידיאל

$$S+I/I = S/S\cap I$$

III $A,B\lhd R$, $A\subseteq B$

$$\frac{R/B}{A/B}\cong R/A$$

תרגיל

$\frac{\gcd(n,m)\mathbb{Z}}{n\mathbb{Z}}$ - אידיאל שנוצר ע"י $\gcd(n,m)$

$$\gcd(n,m)\mathbb{Z}/n\mathbb{Z} \cong n\mathbb{Z}+m\mathbb{Z}/n\mathbb{Z} \overset{II}{\cong} m\mathbb{Z}/n\mathbb{Z}\cap m\mathbb{Z} \cong m\mathbb{Z}/\mathrm{lcm}(n,m)\mathbb{Z}$$

נשווה עוצמות

$$\gcd\cdot\mathrm{lcm}=n\cdot m$$

תרגיל

$$\mathbb{Z}/n\mathbb{Z}+m\mathbb{Z} \cong \frac{\mathbb{Z}/m\mathbb{Z}}{m\mathbb{Z}+n\mathbb{Z}/n\mathbb{Z}} \cong \frac{\mathbb{Z}/m\mathbb{Z}}{n(\mathbb{Z}/m\mathbb{Z})}$$

תרגיל

$$\mathbb{Z}[x]/\langle 7,x^2-2\rangle \overset{III}{\cong} \frac{\mathbb{Z}[x]/\langle 7\rangle}{\langle 7,x^2-2\rangle/\langle 7\rangle} \cong \mathbb{Z}_7[x]/\langle x^2-2\rangle \underset{\bar{x}\to 4}{\cong} \mathbb{Z}/7\mathbb{Z}$$

אידיאלים מקסימליים

הגדרה: אידיאל $M\lhd R$ מקסימלי אם הוא מקסימלי

(1) $M\neq R$ (אמיתי).

(2) $M\subseteq J\underset{\neq}{\lhd} R$ אז $M=J$

דוגמאות:

(1) ב- $\mathbb{Z}$: $p\mathbb{Z}$ כש- p מספר ראשוני.

(2) ב- $\mathbb{Z}/45\mathbb{Z}$ האידיאלים הם (לפי משפט ההתאמה) מהצורה - $k\mathbb{Z}/45\mathbb{Z}$

כאשר $k|45$

ולכן המקסימליים $5\mathbb{Z}/45\mathbb{Z}$, $3\mathbb{Z}/45\mathbb{Z}$.

(3) יהי R ~~תחום שלמות~~ $\langle x\rangle \triangleleft R[x,y]$

והוא לא מקסימלי

$\langle x\rangle \subsetneq J = \{f(x,y) \mid f(0,0)=0\} \to$ זה גרעין של ההומומורפיזם $x \to 0$, $y \to 0$

$J \underset{\neq}{\triangleleft} R[x,y]$

הפונקציה הקבועה לא נמצאת באידיאל J ולכן זה מוכל ממש.

(4) ב- $F[[x]]$ (F שדה) (אין שם) אידיאל שם הוא מהצורה $\langle x^t\rangle$

ולכן היחיד שהוא מקסימלי הוא $\langle x\rangle$.

תרגיל: יהי $\varphi: R\to S$ אפימורפיזם ויהי $M \triangleleft S$ אידיאל מקסימלי. הוכיחו כי $\varphi^{-1}(M)$ הם אידיאל מקסימלי.

תזכורת: דבר להשתמש להוכחת טענות הבאות:

- אם $\varphi: R\to S$ הומומורפיזם, $J \triangleleft S$ אז $\varphi^{-1}(J) \triangleleft R$.
- אם $\varphi: R\to S$ אפימורפיזם $I \triangleleft R$ אז $\varphi(I) \triangleleft S$.

נניח בשלילה ש $\varphi^{-1}(M) \subsetneq J \underset{\neq}{\triangleleft} R$ נפעיל את φ ונקבל-

$M \subset \varphi(J) \triangleleft S$

φ אפימורפיזם

אבל M מקסימלי ולכן-

$\varphi(J) = S = \varphi(R)$

ולכן לכל $r \in R$ יש $j \in R$ כך ש $\varphi(r) = \varphi(j)$

$\varphi(r-j) = 0 \in M$.

$r-j \in \varphi^{-1}(M) \subset J$

ולכן - $r=(r-j)+j \in J$

קיבלנו $R=J$ סתירה!

מש"ל.

• מה לגבי תמונה של אידאל מקסימלי? (באפימורפיזם)

דוגמה: $f:\mathbb{Z}\to\mathbb{Z}/_{2\mathbb{Z}}$ הטלה.

$3\mathbb{Z}$ הוא אידאל מקסימלי ב- $\mathbb{Z}$ אבל התמונה שלו -
$f(3\mathbb{Z})=\mathbb{Z}/_{2\mathbb{Z}}$

טענה: יהי $\varphi: R\to S$ אפימורפיזם ו-$M\lhd R$ מקסימלי

(+) $\ker\varphi \subseteq M$

אזי: $\varphi(M)$ מקסימלי.

הוכחה: ~~נניח בשלילה ש~~ $\cancel{\varphi(M)\subsetneq J\lhd S}$

לפי משפט האיזומורפיזם ה-I: $S\cong R/_{\ker\varphi}$

ולכן אפשר להחליף את φ בהטלה $\varphi: R\to R/_{\ker\varphi}$

$r\to r+\ker\varphi$

נניח בשלילה ש- $M/_{\ker\varphi}=\varphi(M)\underset{\neq}{\subset} J \underset{\neq}{\lhd} R/_{\ker\varphi}$.

לפי משפט ההתאמה $J={J'}/_{\ker\varphi}$ עבור $\ker\varphi\subseteq J'\lhd R$.

אז ישנו $M/_{\ker\varphi}\subseteq {J'}/_{\ker\varphi}$ וכן שמשפט ההתאמה

שומר על הכלה ואי הכלה ממש. ולכן - $M\subsetneq J'\subsetneq R$

סתירה

$\left(J: R/_{\ker\varphi}\to S\right)$

הסתירה לכך ש-M מקסימלי!

מש"ל.

22

משפט: R חוג $M \triangleleft R$
M אידיאל מקסימלי $\iff$ R/M פשוט.

אם: R קומוטטיבי
M מקסימלי $\iff$ R/M שדה.

דוגמאות:

(1) $p\mathbb{Z}$ כי $\mathbb{Z}/p\mathbb{Z}$ שדה.

(2) $\langle x-a\rangle \triangleleft F[x]$ מקסימלי כי $F[x]/\langle x-a\rangle \cong \underset{\text{שדה}}{F}$

(3) $\mathbb{R}[x]/\langle x^2+1\rangle = \mathbb{C}$ ולכן $\langle x^2+1\rangle \triangleleft \mathbb{R}[x]$ מקסימלי.

(4) $\langle x\rangle \triangleleft \mathbb{Z}[x]$ $\qquad \mathbb{Z}[x]/\langle x\rangle \cong \underset{\text{לא שדה!}}{\mathbb{Z}}$

(5) $C(\mathbb{R})$ חוג כל הפונקציות הרציפות
חוג ביחס לחיבור וכפל פונקציות. - $M=\{f\in C(\mathbb{R}) \mid f(0)=0\} \triangleleft C(\mathbb{R})$ (לבדוק!)

(שכה איבר אפס)
(פונקציה קבועה 1 איבר יחידה)

נראה שהוא מקסימלי (החוג קומוטטיבי): נראה ש- $C(\mathbb{R})/M$ הוא שדה.
ניקח $0 \neq f(x)+M \in C/M$
$f(x)\notin M \Rightarrow f(0)\neq 0$.
נתבונן בפונקציה - $g(x)=f(x)-f(0) \in M$.

$$f(x)+M = \underset{\text{פונקציה קבועה.}}{f(0)}+M$$

- $f(0)+M$ הפיך (כי $f(0)\neq 0$ ולכן $\frac{1}{f(0)}+M$ הוא ההופכי)

ולכן הוכחנו שכל איבר $\neq 0$ הפיך
(במנה מי שנמצא מחוץ ל-M הפיך)

משל.

אידמפוטנט - תזכר
2 הבלגנים

לקט

חוגים מקומיים – קומוטטיבי + אידאל מקסימלי יחיד

משפט: התנאים שקולים עבור חוג R קומוטטיבי:

(1) R מקומי

(2) $a+b=1$ ⇐ a הפיך או b הפיך

(3) אוסף כל האיברים שאינם הפיכים הוא אידאל

מסקנה: (2) אם R מקומי, לכל $x\in R$ x הפיך או $1-x$ הפיך.

מסקנה: בחוג מקומי אין אידמפוטנטים

כי $e=e^2$ ⇐ $e(1-e)=0$ ⇐ e ו-$1-e$ לא הפיכים (מחלק אפס)

דוגמה: $F[x]/\langle x^t\rangle$ חוג מקומי. $\langle \bar{x}\rangle$ האידאל שנוצר ע"י x בחוג. הוא אידאל מקסימלי.

$\bar{x}$ לא הפיך כי הוא מחלק אפס ($0=\bar{x}\cdot\bar{x}^{t-1}$) ולכן לפי המסקנה $\bar{x}-1$ הפיך. $\frac{1}{1-x}=1+\bar{x}+\dots+\bar{x}^{t-1}$ סכום של סדרה הנדסית

כי $\bar{x}$ נילפוטנטי כי $\bar{x}^t=0$.

תרגיל: יהי $M\triangleleft R$ מקסימלי אזי לכל n R/M^n מקומי. R קומוטטיבי.

הוכחה: נחשוב כמו M/M^n האידאל המקסימלי היחיד. נראה שכל איבר מחוץ לו הוא הפיך ונוכיח שזה גורר האידאל המקסימלי היחיד.

$\bar{x}\notin M/M^n$ ⇐ $x\notin M$ ולכן

$x+M^n$

$M\subsetneq M+\langle x\rangle$

M מקסימלי ולכן $R=M+\langle x\rangle$ כלומר $1=m+rx$ כאשר $m\in M$, $r\in R$

$$1=1^n=(m+rx)^n=m^n+(\underbrace{n\,m^{n-1}r+\dots+r^n x^{n-1}}_{\in R})x$$

ולכן (בשדה) $\bar{1} = \overline{m^n} + \bar{r}\bar{x}$

⇐ x הפיך

מש"ל.

תרגיל: יהי R חוג קומוטטיבי שבו איברים הם או מחלקי אפס (כולל אפס) או הפיכים. הוכיחו כי R מקומי.

הוכחה: $N = \{$מחלקי אפס (כולל אפס)$\}$ נראה שהוא אידיאל.

ברור $0 \in N$.

$x, a \in N$ ⇐ $xy = ab = 0$ $\exists y, b$

$(x+a)yb = xyb + ayb = 0$

ולכן $x + a \in N$.

בנוסף: $r \in R$, $a \in N$ ⇐ $ab = 0$ $\exists b$

$ra \in N$ כי $rab = 0 = (ra)b = 0$

מצאנו שאוסף האיברים הלא הפיכים (מחלקי האפס) הוא אידיאל.
ולכן החוג מקומי.

הרצאה 5
13/03/22

תזכורת
משפט השאריות הסיני:

אם $I_1, \dots, I_k \trianglelefteq R$ יש הומומורפיזם $R \to R/I_1 \times R/I_2 \times \dots \times R/I_k$
$a \to (\underbrace{a+I_1}_{a \bmod I_1}, \dots, a+I_k)$

מה הגרעין? $I_1 \cap \dots \cap I_k$

$\left(\underset{a \in I}{\underset{\Updownarrow}{a+I=I}}=0+I \right)$

ולכן יש לנו שיכון $R/_{I_1 \cap \dots \cap I_k} \hookrightarrow R/I_1 \times \dots \times R/I_k$
מתי זה על?

הגדרה - אידיאלים $I_1 \dots I_k$ נקראים קו מקסימליים אם $I_i+I_j=R$ $i \neq j$

למשל: אם M מקסימלי ו-I אידיאל שלא מוכל בו אז I, M קומקסימלים
(כי $M \subsetneq M+I=R$)

הערה: אם J, I קו מקסימליים $JI+IJ=I \cap J$.

משפט: (CRT) שאריות הסיני:
אם $I_1 \dots I_k$ קו מקסימלים אז ההשיכון $R/_{I_1 \cap \dots \cap I_k} \hookrightarrow R/I_1 \times \dots \times R/I_k$
הוא איזומורפיזם.

דוגמה ל-$\mathbb{Z}$: אם $P_1 \dots P_k$ ראשוניים שונים אז ($P_1\mathbb{Z}, \dots, P_k\mathbb{Z}$ קו מקס)
תזכורת גוד $P_i\mathbb{Z}+P_j\mathbb{Z}=\gcd(\mathbb{Z})$

דוגמה ל-$\mathbb{Z}$: אם $P_1 \dots P_k$ ראשוניים שונים אז ($P_1\mathbb{Z}, \dots, P_k\mathbb{Z}$ קו מקס)
$P_i\mathbb{Z}+P_j\mathbb{Z}=\gcd \cdot \mathbb{Z}$

לכל מערכת משוואות
$$\left\{ \begin{array}{l} x=a_1 \bmod p_1 \\ \vdots \\ x=a_k \bmod p_k \end{array} \right.$$
יש פתרון ב-$\mathbb{Z}$

והוא יחיד עד כדי $P_1\mathbb{Z} \cap \dots \cap P_k\mathbb{Z} = P_1 \cdot \dots \cdot P_k\mathbb{Z}$

דוגמא: מצאו מספר $x\in\mathbb{Z}$ המקיים
$x = 2 \mod 3$
$x = 2 \mod 4$
$x = 1 \mod 5$

פתרון:
$$x = \underbrace{4\cdot5\cdot n_1}_{\mod 3} + \underbrace{3\cdot5\cdot n_2}_{\mod 4} + \underbrace{3\cdot4\cdot n_3}_{\mod 5}$$

במקרה של מודולו 3- $x \equiv 20n_1 = 2n_1 \mod 3$
אז ניקח $n_1=1$.
במקרה של מודולו 4- $x = 15n_2 = 3n_2 = 2$

$n_2 = \underset{\mathbb{Z}_4}{3^{-1}}\cdot 2 = 3\cdot 2 = 6 = 2$

במקרה של מודולו 5-
$x = 12n_3 = 2n_3$
$n_3 = \underset{\mathbb{Z}_5}{2^{-1}} = 3$

ולכן- $x = 20\cdot1 + 15\cdot2 + 12\cdot3 = 86 = 26$ מודולו $3\cdot4\cdot5$

תרגיל: הוכח שיש רצף מספרים טבעיים מכל גודל כך שאף אחד מהם הוא לא "חזק" Powerful.

הגדרה- מספר טבעי חזק אם לכל ראשוני שמחלק אותו מחלק גם $p^2 | n$

הוכחה: ניקח רצף מאורך k ניקח k ראשוניים שונים $p_1 \ldots p_k$
הרעיון שאנו יוצרים קונגרואנציות לפי CRT קיים $x\in\mathbb{N}$ כך ש
$x \equiv -1 \mod p_1^2$
אז הרצף $x+1, x+2, \ldots, x+k$ הוא רצף של מספרים לא חזקים

לכן?
למה?
$x \equiv 1 \mod p_1^2$

$x+1 \equiv 0 \mod p_1^2$

$\Leftarrow p_1^2 | x+1$. $x+1$ לא מחלק וזו הסתירה.

תרגיל: $\mathbb{R}[x]/\langle x^2-5x+6\rangle \cong \mathbb{R}\times\mathbb{R}$

פתרון: $x^2-5x+6=(x-3)(x-2)$ ולכן $\cancel{x^2-5x+6}$

$\langle x^2-5x+6\rangle = \langle x-3\rangle\langle x-2\rangle$

(מהיות קומוטטיבי: $\langle a\rangle\cdot\langle b\rangle=\langle ab\rangle$)

ונראה ש- $\langle x-2\rangle$ ו- $\langle x-3\rangle$ קומקסימליים:

$1=(x-2)-(x-3)\in\langle x-2\rangle+\langle x-3\rangle$

ולכן:

$\langle x-2\rangle\langle x-3\rangle = \langle x-2\rangle\cap\langle x-3\rangle$

ומשפט הסיני:

$\mathbb{R}[x]/\langle x^2-5x+6\rangle = \mathbb{R}[x]/\langle x-2\rangle\cap\langle x-3\rangle \overset{\text{סיני}}{\cong} \mathbb{R}[x]/\langle x-2\rangle \times \mathbb{R}[x]/\langle x-3\rangle$

$\cong \mathbb{R}\times\mathbb{R}$

(ההומומורפיזם ההצבה הינו באופן כללי - $\mathbb{R}[x]/\langle x-c\rangle \cong \mathbb{R}$, $x\to c$)

אידיאל ראשוני

הגדרה: יהי R חוג. אידיאל אמיתי $P \triangleleft R$ נקרא ראשוני אם לכל שני אידיאלים $A,B\triangleleft R$ כך ש- $AB\subseteq P$ מתקיים $A\subseteq P$ או $B\subseteq P$

דוגמאות:

① ב-$\mathbb{Z}$ האידיאלים הראשוניים $p\mathbb{Z}$ כאשר p ראשוני, $\{0\}$.

$nm\mathbb{Z}=n\mathbb{Z}\cdot m\mathbb{Z}\subseteq p\mathbb{Z}$ $\Leftarrow$ $p|mn$ $\Leftarrow$ $p|n$ או $|m$

$\Leftarrow$ $n\mathbb{Z}\subseteq p\mathbb{Z}$ או $m\mathbb{Z}\subseteq p\mathbb{Z}$

הערה

(2) אם R חוג פשוט (=אין אידיאלים חוץ מ-0 ו-R) אז $\{0\}$ אידיאל ראשוני.
כי אם $AB\subseteq\{0\}$, A,B אידיאלים של R ולכן הם או $\{0\}$ או R. המכפלה שלהם היא $\{0\}$ ולכן אחד מהם חייב להיות 0.

טענה: אם R חוג קומוטטיבי אז $P\triangleleft R$ ראשוני $\Leftrightarrow$ הוא מקיים את התנאי של האיברים
$ab\in P \Rightarrow a\in P$ או $b\in P$.

דוגמאות:

(1) $\langle x\rangle\triangleleft F[x]$ ראשוני.
נניח ש-$f(x)\cdot g(x)\in\langle x\rangle \Leftarrow$ ל-$f(x)\cdot g(x)$ אין איבר חופשי
$\Downarrow$
אז ל-f או ל-g אין איבר חופשי.
ולכן שייך לאידיאל.

(2) $I=\langle x^2-1\rangle\triangleleft \mathbb{R}[x]$
לא ראשוני - כי $(x-1)(x+1)=x^2-1\in I$ אך אף אחד מהם לא ב-I.

(3) אם R תחום $\{0\}$ הוא ראשוני
מכיוון $ab\in\{0\} \Rightarrow ab=0 \Rightarrow a=0$ או $b=0$.

הערה: במקרה הלא קומוטטיבי, התנאי של האיברים חזק יותר מראשוניות.

למשל: אם F שדה אז $M_n(F)$ $(n>1)$ חוג פשוט.
יש התאמה
$\{$אידיאלים של $R\}\longleftrightarrow\{$אידיאלים של $M_n(R)\}$

(כלומר בהתאמה שכל אידיאל של $M_n(R)$ הוא מהצורה $M_n(I)$ עבור $I\triangleleft R$)

דמי

ולכן $\{0\}$ אידיאל ראשוני אבל לא מקיים את התנאי של האיברים:

$e_{11}\cdot e_{22}=0\in\{0\}$

אבל $e_{11},e_{22}\notin\{0\}$

"דיון"

נניח R קומוטטיבי $P\triangleleft R$ ראשוני $\boxed{ab\in P \Rightarrow a\in P \text{ או } b\in P}$

שקול ל-

$$\boxed{a,b\notin P \Rightarrow ab\notin P}$$

מסקנה: R קומוטטיבי אזי $P\triangleleft R$ ראשוני אמ"מ $R\setminus P$ סגור לכפל.

טענה: יהי R חוג קומוטטיבי $S\subseteq R$, $0\notin S$ סגורה לכפל (לפי הלמה של צורן) קיים אידיאל I מקסימלי ביחס לתכונה ש- $I\cap S=\emptyset$. אידיאל זה הוא ראשוני.

הוכחה: נניח I הוא מקסימלי ביחס לתכונה זו. (זר ל-S)

נראה שהוא ראשוני.

יהיו $a,b\notin I$ נניח בשלילה ש- $ab\in I$ נתבונן באידיאלים $I+Ra$

$I\subsetneq I+Ra$

$I\subsetneq I+Rb$

ולכן לפי מקסימליות של I

$i+r_1a \in (I+Ra)\cap S\neq\emptyset$

$j+r_2b \in (I+Rb)\cap S\neq\emptyset$

$(i,j\in I,\ r_1,r_2\in R)$

נכפול את האיברים $=(i+r_1a)(j+r_2b)\in S$

$$=\underbrace{ij+ir_2b+jr_1a}_{\in I}+\underbrace{r_1r_2ab}_{\in I}\in I$$

קיבלנו איבר ב- $I\cap S$ סתירה!

רקע

למה: (לא המתמטיקה מאושיינים)

יהי R חוג קומוטטיבי ו- $P_1,\ldots,P_n$ אידיאלים ראשוניים אזי אם אידיאל $I \triangleleft R$ מקיים $I \subseteq \bigcup P_i$ אז $I \subseteq P_i$ לאיזשהו i.

הוכחה: נוכיח עבור $n=2$: נניח $I \not\subseteq P_1, P_2$ רוצים להוכיח ש- $I \not\subseteq P_1 \cup P_2$.
לפי ההנחה אפשר למצוא איברים a_1,a_2 ש"ע $a_1 \notin P_1$ ו $a_2 \notin P_2$.

אם $a_1 \notin P_2$ או $a_2 \notin P_1$ – סיימנו. ולכן נוכל להניח $a_1 \in P_2 \setminus P_1$, $a_2 \in P_1 \setminus P_2$.

אני רוצה להסתכל על $x = a_1 + a_2 \in I$ (סגור לחיבור איברים ב- I)

$x \notin P_1$ כי אחרת $\underset{P_1}{a_1} = \underset{P_1}{x} - a_2 \in P_1$

באותו אופן $x \notin P_2$. ולכן $x \notin P_1 \cup P_2$.

נוכיח באינדוקציה עבור $n-1$ אידיאלים ונוכיח עבור n

~~$a_i \in I \setminus P_i$ ולכן יש איבר $I \not\subseteq P_i$~~

לפי הנחת האינדוקציה $I \not\subseteq \bigcup_{i \neq j} P_i$ לכל j ולכן לכל j יש איבר $a_j \in I \setminus \bigcup_{i \neq j} P_i$

כמו קודם נוכל להניח שכל $a_j \in P_j$ (אחרת – סיימנו.)
נסמן איבר: $x = a_1 \ldots a_{n-1} + a_n \in I$; x לא שייך לאף אחד.
אם $x \in P_n$, $a_1 \ldots a_n \in x - a_n \in P_n$
$\Rightarrow$ $a_i \in P_n$ לאיזשהו i (כי P_n ראשוני.)
סתירה.

ואם $x \in P_j$ עבור $j \neq n$ אזי ~~$a_n \in x$~~
$a_n = x - \underbrace{a_1 \ldots a_{n-1}}_{\in P_j} \in P_j$ סתירה.

מש"ל.

דף

<u>מקסימלי אמ"ר ראשוני.</u>

<u>הערה:</u> חיתוך של ראשוניים הוא בדרך כלל לא ראשוני.

$2\mathbb{Z}\cap 3\mathbb{Z}=6\mathbb{Z}$

<u>טענה:</u> (בחוג קומוטטיבי) חיתוך של אידיאלים מקסימליים שונים הוא אף פעם לא ראשוני.

<u>הוכחה:</u> נניח I,J מקסימליים שונים אז אף אחד מהם לא מכיל את השני ולכן אפשר למצוא איברים $a\in I\setminus J$
$b\in J\setminus I$

<u>אזי</u> - $ab\in IJ\subseteq I\cap J$

נימוק =

אם ה- חיתוך היה ראשוני אז: $a\in I\cap J$ או $b\in I\cap J$
אבל לפי הבחירה שלנו $a\notin J$ ו- $b\notin I$

<u>סתירה.</u>

$\Leftarrow$ $\boxed{I\cap J \text{ ראשוני אז } I\subseteq J \text{ או } J\subseteq I}$

<u>מש"ל.</u>

תרגול 6
אלגברה
04/04

אידיאל ראשוני (דו-צד): $AB\subseteq P \Rightarrow A\subseteq P$ או $B\subseteq P$.

טענה: יהי $I\lhd R$ אזי האידיאלים הראשוניים של R/I הם P/I עבור $I\subseteq P\lhd R$ (ראשוני).

תרגיל: יהי R חוג בוליאני (= כל האיברים אידמפוטנטים $e^2=e$) אזי כל אידיאל שווה לחיתוך של האידיאלים הראשוניים שמכילים אותו.

הוכחה: $I\lhd R$ מספיק להראות שמנה R/I (גם חוג בוליאני). $\bigcap P = I$ ($I\subseteq P$ ראשוניים).
הטענה שקולה (מוכיח של-R/I חיתוך האידיאלים הראשוניים הוא 0 (למה?))
יהי $1,0\neq x\in R/I$ ($x+I$) מתאים.
החוג בוליאני ולכן $\bar{x}^2=\bar{x}$ $\quad \bar{x}(\bar{x}-\bar{1})=0$
$\Rightarrow$ $\bar{x}-1$ מחלק אפס $\Rightarrow$ לא הפיך ולכן הוא מוכל באידיאל
הראינו שאם אידיאל מקסימלי $\Rightarrow$ ראשוני.
וכמו כן x באידיאל מקס $\Rightarrow$ ראשוני,
אבל לא יכול שהם מוכלים יחד באידיאל ראשוני. אמיתי. ■

משפט: יהי R חוג $I\lhd R$. I ראשוני $\Leftrightarrow$ R/I חוג ראשוני.
$\Downarrow$
($AB=0 \Rightarrow A=0$ או $B=0$)

אם R קומוטטיבי: I ראשוני $\Leftrightarrow$ תחום.

מסקנה: מקסימלי $\Rightarrow$ ראשוני. (בחוגים עם יחידה $2\mathbb{Z}\subseteq\mathbb{Z}$).

דוגמאות:

(1) $\mathbb{Z}/4\mathbb{Z}[x] \rhd \langle x\rangle$ $\qquad \frac{\mathbb{Z}/4\mathbb{Z}[x]}{\langle x\rangle}\cong \mathbb{Z}/4\mathbb{Z}$
$\Downarrow$
לא תחום ולכן האידיאל לא ראשוני.

דוג' (2)

$\mathbb{Q}[x] \triangleleft x^2-1$ לא ראשוני.

$\mathbb{Q}[x]/\langle x^2-1\rangle =$

$(\overline{x-1})(\overline{x+1}) = \overline{x^2-1} = \overline{0}$

כיוון שיש מחלק אפס זה לא תחום שלמות ולכן האידיאל לא יכול להיות ראשוני.

תרגיל: הוכיחו כי $\langle 3\rangle \triangleleft \mathbb{Z}[i]$ ראשוני.

$\{a+bi \mid a,b\in\mathbb{Z}\}$

(למה $\langle 5\rangle \triangleleft \mathbb{Z}[i]$ לא ראשוני?) $(1-2i)(1+2i)=5$

הוכחה: נשתמש באיזומורפיזם - התמונה של $\langle 3\rangle$ בחוג המנה

$\mathbb{Z}[x]/\langle x^2+1\rangle = \mathbb{Z}[i]$

$\langle 3,x^2+1\rangle / \langle x^2+1\rangle$

$$\frac{\mathbb{Z}[x]/\langle x^2+1\rangle}{\langle 3,x^2+1\rangle/\langle x^2+1\rangle} \cong \mathbb{Z}_3[x]/\langle x^2+1\rangle$$

$\Downarrow$

זו תחום שלמות

תזכורת: $S\subseteq R$ את קבוצה סגורה לכפל ו־0 אפס אין, האידיאל ב־R המקסימלי ביחס לתכונה ש־$P\cap S=\emptyset$ הוא ראשוני.

מיקום

תזכורת: $S\subseteq R$ את קבוצה סגורה לכפל איברים רגולרים = לא מחלקי אפס.
$S\subseteq Z(R)$ (תת מרכזית), $(1\in S)$, $(0\notin S)$.

הרעיון: חוג מינימלי המכיל את R ש־איברי S יהיו הפיכים.
$R\subseteq S^{-1}R$

רפ'

״להפוך״: את איברי S.

<u>בנייה</u>

$$S^{-1}R = S\times R/\sim \qquad (s,r) \longleftrightarrow \frac{r}{s}$$

יחס שקילות של שברים.

$$\frac{r}{s}=\frac{r'}{s'} \iff rs'=sr'$$

<u>תכונה אוניברסלית</u> ($? \to S^{-1}R$) – איך קיים הומומורפיזם ל-

אם יש הומומ' $f: R\to T$ כך ש- $f(S)\subseteq T^{\times}$ אז קיים הומומורפיזם <u>יחיד</u> $\hat f: S^{-1}R\to T$ כך ש- $f=\hat f\circ i$

$$\begin{tikzcd} R \arrow[r] \arrow[d, "i"'] & T \\ S^{-1}R \arrow[ur] & \end{tikzcd}$$

<u>התאמה של אידיאלים:</u>

$$I\lhd R \rightleftarrows S^{-1}R\lhd R \qquad \left\{\frac{a}{s} \,\middle|\, \begin{matrix} a\in I \\ s\in S\end{matrix}\right\}$$

א היחס שקול

באופן זה יש התאמה של אידיאלים ראשוניים (עבור אידיאלים ראשוניים)
וההתאמה שומרת על הכלה.

<u>דוגמאות חשובות!</u>

(1) מיקוד באידיאל ראשוני: $P\lhd R$ $\quad S=R\setminus P$

$$S^{-1}R = R_P = \left\{\frac{a}{b} \,\middle|\, \begin{matrix} a\in R \\ b\notin P\end{matrix}\right\}$$

זהו חוג מקומי עם אידיאל מקסימלי $\left\{\frac{a}{b} \,\middle|\, \begin{matrix} a\in P \\ b\notin P\end{matrix}\right\}=P_P$

ושאר האידיאלים $I_P = \left\{\frac{a}{b} \,\middle|\, \begin{matrix} a\in I \\ b\notin P\end{matrix}\right\}$ כאשר $I\subseteq P$

דוגמה
(2) **שדה השברים?**

נניח R תחום שלמות $S=R-\{0\}$

המקרה כזה: $S^{-1}R=\{\frac{a}{b} \mid b,a\in R,\ b\neq 0\}$ הוא שדה.מיני:
הוא יחיד (עד כדי איזומורפיזם) ונקרא **שדה השברים** $q(R)$ $\underline{\quad}$ (q

זה השדה המינימלי שמכיל את R.

דוגמאות:

(1) $\mathbb{Z}$ $\quad S=\{5^i\}_{i\in\mathbb{N}}$

$$S^{-1}\mathbb{Z}=\left\{\frac{a}{b} \;\middle|\; \begin{matrix} a\in\mathbb{Z} \\ b\in S\end{matrix}\right\}=$$

$$=\left\{\frac{a}{5^i} \;\middle|\; i\right\}\cong \mathbb{Z}[\tfrac{1}{5}]$$

וזהו שינוי של $\frac{1}{5}$
פולינומים שהצבנו במקום x
המישור.

(2) $\mathbb{Z}$, $\quad P=5\mathbb{Z} \quad S=\mathbb{Z}-5\mathbb{Z} \quad S\notin\{\mathbb{Z}\setminus 5\mathbb{Z}\}$

$$\mathbb{Z}_{(5)}=\left\{\frac{a}{b} \;\middle|\; \begin{matrix} a\in\mathbb{Z} \\ b\in \underset{\mathbb{Z}-5\mathbb{Z}}{\underset{\parallel}{S}}\end{matrix}\right\}=\left\{\frac{a}{b} \;\middle|\; \begin{matrix} b,a\in\mathbb{Z} \\ b\in 5\mathbb{Z}\end{matrix}\right\}=$$

$$=\left\{\frac{a}{b} \;\middle|\; \begin{matrix} a,b\in\mathbb{Z} \\ b\notin 5\mathbb{Z}\end{matrix}\right\}=\left\{\frac{a}{b} \;\middle|\; \begin{matrix} a,b\in\mathbb{Z} \\ 5\nmid b\end{matrix}\right\}.$$

$$5\mathbb{Z}_{(5)}=\left\{\frac{a}{b} \;\middle|\; \begin{matrix} a\in 5\mathbb{Z} \\ b\notin 5\mathbb{Z}\end{matrix}\right\}=\left\{\frac{5a}{b} \;\middle|\; \begin{matrix} a,b\in\mathbb{Z} \\ 5\nmid b\end{matrix}\right\}$$ זו האידיאל המקסימלי.

[illegible]-

$$25\mathbb{Z}_{(5)}=\left\{\frac{25a}{b} \;\middle|\; \begin{matrix} a,b\in\mathbb{Z} \\ 5\nmid b\end{matrix}\right\}.$$

$\mathbb{Z}$ $\quad 5$

[illegible]

(ג) $S=\{6^i\}\subseteq\mathbb{Z}$

$$S^{-1}\mathbb{Z}=\left\{\frac{a}{b}\ \middle|\ \begin{matrix}a\in\mathbb{Z}\\ b=6^i\end{matrix}\right\}\cong\mathbb{Z}\left[\tfrac{1}{6}\right]$$

האם 2 הפיך? כן! $\frac{2}{1}\cdot\frac{3}{6}=\frac{1}{1}$ וכך 3 הפיך

מסקנה: $\mathbb{Z}\left[\frac{1}{6}\right]=\mathbb{Z}\left[\frac{1}{2},\frac{1}{3}\right]$

(ד) דוגמא לשדה שברים $R=\mathbb{Z}$ $S=\mathbb{Z}-\{0\}$

$$q(\mathbb{Z})=S^{-1}R=\left\{\frac{a}{b}\ \middle|\ \begin{matrix}a,b\in\mathbb{Z}\\ b\neq0\end{matrix}\right\}=\mathbb{Q}$$

ולכן $\mathbb{Q}$ הוא השדה המינימלי שמכיל את $\mathbb{Z}$.

(5) $R=F_x$ פולינומים מעל שדה F, $S=F[x]-\{0\}$

$$q(F[x])=\left\{\frac{p(x)}{q(x)}\ \middle|\ \begin{matrix}p(x),q(x)\in F[x]\\ q\neq0\end{matrix}\right\}=F(x)$$

$\Downarrow$ שדה הפונקציות הרציונליות.

תרגיל: יהי $a\in R$ חוגי ומכפלי א"כ $S=\{a^i\}$ סגור לכפל וכו'

הוכיחו כי $S^{-1}R\cong R[x]/\langle ax-1\rangle$

הוכחה: (ניתן לשיכון $R\to R[x]/\langle ax-1\rangle$ אחת שיכון בה כל איברי S הפיכים ($\bar{a}^i\cdot\bar{x}^i=\bar{1}$)

ולכן יש הומומורפיזם $S^{-1}R\to R[x]/\langle ax-1\rangle$ ונשאר לנו לוודא שזה על.

$$\begin{tikzcd} R \arrow[r, hook, "r\mapsto\bar{r}"] \arrow[d] & R[x]/\langle ax-1\rangle \\ S^{-1}R \arrow[ur, dashed, "\exists!"] \arrow[ur, bend right] & \end{tikzcd}$$

$=\bar{x}=\bar{a}^{-1}$

$\bar{r}\bar{x}^i$

$r\cdot\frac{1}{s=a^i}=\frac{r}{s=a^i}$

$S^{-1}R\to R[x]/\langle ax-1\rangle$

$\frac{r}{a^i}\to\bar{r}\bar{x}^i$

ברור שזה על כי לכל $\bar{r}$ יש מקור (r) והמקור של $\bar{x}$ הוא $\frac{1}{a}$

מש"ל.

תרגיל: ~~יהי R תחום~~ תהי F לא

דוג'

תרגיל: יהי R תחום ויהי F שדה השברים שלו (נסמן $R-\{0\}$ ב-S) $(F=S^{-1}R)$ הוכיחו $S^{-1}(R[x])=F[x]$.

הוכחה:
קיים שיכון $R[x]\to F[x]$ כל האיברים ב-S הפיכים ולכן יש שיכון
$S^{-1}(R[x])$-ל

$S^{-1}(R[x])\subseteq F(x)$

ניקח איבר $\frac{a_0}{b_0}+\frac{a_1}{b_1}x+\frac{a_2}{b_2}x^2+\dots+\frac{a_n}{b_n}x^n\in F(x)$ $(a_i,b_i\in R)$

נעשה מכנה משותף ונקבל $p=\frac{c_0+c_1x+\dots+c_nx^n}{d}$ $c_i,d\in R$

וברור ש- $p\in S^{-1}(R[x])$

מש"ל.

תרגיל: ניקח (P אידיאל ב-R) $P\triangleleft R$ ראשוני מינימלי. הוכח כי $P_P\triangleleft R_P$ הראשוני היחיד.

ראשוני ב-R
מוכלה $P \not\subseteq$

הוכחה: ניקח אידיאל ראשוני אמיתי של R_P הוא מהצורה I_P כאשר I אידיאל ראשוני של R המקיים $I\cap S=\emptyset$ ז"א הגדל ש- $I\subseteq P$.

$I\cap(R-P)$

אבל מינימליות P נקבל $I=P$

מש"ל.

דני

תחומי שלמות -

משמעות תכונת

הערה: תחום סופי ⟸ שדה
תת חוג של תחום הוא תחום.
R תחום ⟸ $R[x]$ תחום

מסקנה - ~~[illegible]~~ לא תחום שלמות $(0,1)\cdot(1,0)=(0,0)$

שונה / ~~[illegible]~~

שונה - לא תחום $\mathbb{Z}/4\mathbb{Z}$ $F[x,y]/\langle xy\rangle$ $(\bar{x}\bar{y}=0)$

תכונה: לתחום שלמות חיתוך סופי של אידיאלים $\neq 0$ תמיד שונה מ-0.

הוכחה: מספיק להוכיח עבור 2 $A,B \lhd R$ $0\neq$ תמיד $AB\subseteq A\cap B$
ניקח $0\neq a\in A$ ו-$0\neq b\in B$ $0\neq ab\in AB\subseteq A\cap B$ כי נתון תחום.

משל

דוגמא חשובה: חוגי השלמים הריבועיים.
$d\in\mathbb{Z}$ חופשי מריבועים

$$\mathcal{O}_d=\begin{cases}\mathbb{Z}[\sqrt{d}] & d\not\equiv 1 \bmod 4\\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d\equiv 1 \bmod 4\end{cases}$$

$$\| \quad \left\{\begin{matrix} a+b\sqrt{d} \\ \frac{a}{2}+\frac{b}{2}\sqrt{d}\end{matrix}\right\}$$

$$a+b\left(\frac{1+\sqrt{d}}{2}\right)$$

$$\boxed{\frac{2a+b}{2}+\frac{b}{2}\sqrt{d}}.$$

תרגיל: R תחום שלמות.

תכונה הקלה - הוכיחו כי הפונקציה $N:R\to\mathbb{N}\cup\{\infty\}$

$$N(a)=\left|R/Ra\right|$$

היא כפלית -

הוכחה: לפי צריך להוכיח -

$$\left|R/Rab\right|=\left|R/Ra\right|\left|R/Rb\right|$$

$$Rab=RaRb\subseteq Ra\cap Rb.$$

לפי משפט האיזומורפיזם ה-3:

$$\frac{R/Rab}{Ra/Rab} \cong R/Ra$$

לכן: $\left|R/Rab\right| = \left|R/Ra\right| \cdot \left|Ra/Rab\right|$

נשאר להראות $\left|Ra/Rab\right| = \left|R/Rb\right|$

נגדיר פונקציה: $R \to Ra/Rab$ (לא מהכיוון האיזומורפיזם)

$r \mapsto ra+Rab$.

חיבורי – ✓ ~~(הומומורפיזם)~~

כפלי – $\times$

קיבלנו הומומורפיזם של חבורות חיבוריות

קל לראות שזה על.

הגרעין:

$$\ker = \{r\in R \mid r\bar{a}=\bar{0}\}$$

$$\Updownarrow$$

$$ra\in Rab$$

$$= \{r\in R \mid \underset{Rb}{ra = r'ab}\} = Rb.$$

לפי משפט איזו' ראשון של חבורות יש איזו' ומתקיים: $Ra/Rab \cong R/Rb$

לסיום:

והפונקציה היא כפלית. מש"ל.

הגדרה: ל-O_d יש נורמה

$N(x) = x\cdot\underset{\text{צמוד}}{\bar{x}}$

אם $x=a+b\sqrt{d}$ אז $\bar{x}=a-b\sqrt{d}$.

רמז

ויש עקבה- $tr(x)=x+\bar{x}$

תכונות:

(1) נורמה היא כפלית.

(2) tr היא חיבורית.

(3) $x\in O_d$ הפיך $\iff$ $N(x)=\pm 1$.

תרגיל: מצאו את כל ההפיכים ב- O_{-3}.

פתרון: נקח איבר כללי $O_{-3}=\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ ניקח איבר כללי -

$$\alpha = a+b\left(\frac{1+\sqrt{-3}}{2}\right) = \frac{2a+b}{2}+\frac{b}{2}\sqrt{-3}$$

נחשב את הנורמה:

$$N(\alpha)=\left(\frac{2a+b}{2}+\frac{b}{2}\sqrt{-3}\right)\left(\frac{2a+b}{2}-\frac{b}{2}\sqrt{-3}\right)$$

$$=a^2+ab+b^2$$

ב- O_{-3} הנורמה חיובית ולכן נשאר לחפש מתי $N(\alpha)=1$.

$$a^2+ab+b^2=1$$

פתרונות ברורים: $a=0$, $b=\pm 1$

$a=\pm 1$, $b=0$

$a=\pm 1, b=\mp 1$

אין עוד פתרונות כי אם $|a|,|b|\geq 2$ ולכן $a^2+b^2\geq 8$ -

$a^2+ab+b^2\neq 1$.

תרגיל: פתרו את המשוואה $(3+2\sqrt{2})^n-\sqrt{2}(\sqrt{2}+1)^n+\sqrt{2}=0$ כאשר n טבעי.

פתרון: $\underbrace{(3+2\sqrt{2})}_{a}{}^n=\sqrt{2}\left(\underbrace{(\sqrt{2}+1)}_{b}{}^n-1\right)$

Scanned by CamScanner

המשך: נסתכל על המשוואה. תזכור $\mathbb{Z}[\sqrt{2}] = \mathcal{O}_2$

$N(a) = 9-8 = 1$

$N(b) = -1$

אנחנו רוצים - $a^4 = \sqrt{2}(b^4-1)$

נפעיל נורמה

$N(a^4) = 1 = \underbrace{N(\sqrt{2})}_{-2} \cdot \underbrace{N(b^4-1)}_{\in \mathbb{Z}}$

ולכן יכול להיות לזה פתרון.

תרגיל: ① עבור $\alpha \in \mathcal{O}_d$ אם ורק אם $\alpha | n$ עבור $n \in \mathbb{Z}$ גם $n | N(\alpha)$

② הסיקו $R_\alpha \cap \mathbb{Z} = \mathbb{Z} \cdot N(\alpha)$

פתרון:

(1) נחשב $n = \alpha \cdot \beta =$

$= (a+b\sqrt{d})(x+y\sqrt{d})$

ומזה נקבל משוואות-

$$\begin{cases} n = ax+byd \\ 0 = ay+bx \end{cases}$$

$N(\alpha) = a^2-b^2d$

~~נכפול את המשוואה השנייה ב-a~~:

$bn = \cancel{bax} + b^2yd$

$0 = aby + b^2x$

נכפול את המשוואה הראשונה ב-b:

$$\begin{cases} nb = abx + b^2yd \\ 0 = ay + bx \end{cases}$$

כמו

$$\begin{cases} nb = -a^2y + b^2yd = -N(\alpha)y \\ 0 = ay + bx \end{cases}$$

מ- $N(\alpha)|nb$ אז ש- $N(\alpha)\nmid b$ וגם $N(\alpha)|n$ (סיימנו) אז

ש- $N(\alpha)|b$ = a^2+b^2d

$\Downarrow$

$N(\alpha)|a$

$\Downarrow$

$\alpha | N(\alpha) | \alpha$.

$\Downarrow$

α נוצר ע"י דבר שהוא קבוע.

(2) לפי סעיף קודם $N(\alpha) \in \langle\alpha\rangle$

$\langle\alpha\rangle \cap \mathbb{Z} = \mathbb{Z}N(\alpha)$

ולכן ברור $\mathbb{Z}N(\alpha) \subseteq \langle\alpha\rangle \cap \mathbb{Z}$

מצד שני $n \in \langle\alpha\rangle \cap \mathbb{Z}$ אז $\alpha|n$ ולפי הסעיף הקודם

$N(\alpha)|n$ ולכן $n \in \mathbb{Z}\cdot N(\alpha)$

מש"ל

~~דוגמא:~~

מסקנות:

• כל אידיאל ב- $\mathcal{O}_d$ מכיל מס. ולכן כל מנה של $\mathcal{O}_d$ סופית.

~~$\mathcal{O}_d/I = \{a+b\sqrt{d}\}$~~

$$\exists N \in I \quad \mathcal{O}_d/I = \{a+b\sqrt{d}+I\} = \underbrace{\{\overline{a+b\sqrt{d}} \mid a,b \in \{0,\dots,N-1\}\}}_{\text{קבוצה סופית}}$$

• ב- $\mathcal{O}_d$ כל אידיאל ראשוני הוא מקסימלי. $\Leftarrow$

תזכר

אבחנה: יהי $\alpha \in O_d = R$ $= a+b\sqrt{d}$ כך ש- $(a,b)=1$, אזי -

$$|N(\alpha)| = |R/R\alpha|$$

הוכחה:

נסמן $N = N(\alpha)$. לפי משפט המיון ה-II

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}+R\alpha/R\alpha$$

לפי איזומ' הקודם.

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}+R\alpha/R\alpha \longrightarrow R/R\alpha$$

אפשר לא על

שים לב!

ולכן $N \le |R/R\alpha|$

נשאר הכיוון השני - צריך להוכיח את המנה. (רוצים N נציגים)

לפי הנתון -

$$(b,N) = (b, a^2-b^2d) = (a,b) = 1$$

(a,N)

[illegible] המספרים

מחלק משותף 1.

ולכן -

$$\cancel{a^2-b^2d = N}$$

$\boxed{!}$ → תזכירו לנו אחר-כך!

מסקנה: הנורמה של O_d מתלכדת עם הפונקציה הכפלית שהגדרנו!

$$\alpha = a+b\sqrt{d} = c\cdot\underbrace{(a'+b'\sqrt{d})}_{\alpha'} \qquad (a',b')=1$$

$$N(\alpha) = N(c)\cdot N(\alpha') \underset{\text{איך}}{=} c^2\cdot|R/R\alpha'| = |R/Rc|\cdot|R/R\alpha'| = |R/R\alpha|$$

דפי

יחס החלוקה (תחומי-שלמות).

$a|b \Rightarrow \exists c: b=a\cdot c$

זה לא יחס סדר! (רפלקסיבי, טרנזיטיבי ולא אנטי סימטרי).

למשל ב-$\mathbb{Q}$ $2|3 \Rightarrow 2\cdot\frac{3}{2}=3$

יחס שקילות - $a\sim b$ a **חבר** של b אם $a=b\cdot u$ עבור u הפיך.

יחס החלוקה הוא יחס סדר על חברי החוג.

אזי: $a\sim b \iff \langle a\rangle=\langle b\rangle$ אפשר לתרגם את יחס החלוקה ליחס סדר על אידאלים:

$a|b \iff \langle b\rangle\subseteq\langle a\rangle$.

הגדרה - איבר $a\in R$ נקרא אי-פריק אם $a=bc$ כאשר a לא הפיך $\Rightarrow$ אז b או c הפיך (פירוק טריוויאלי).

דוגמאות:

(1) ב-$\mathbb{Z}$ האיברים האי-פריקים הם המספרים הראשוניים.

(2) $x\in F[x]$ הוא אי-פריק $x=f(x)\cdot g(x)$ $\deg x=1$ $=\deg f(x)+\deg(g(x))$

ולכן $\deg f=0$ או $\deg(g)=0$

$\downarrow$ $\downarrow$

f הפיך g הפיך.

(3) $x^2+1\in\mathbb{R}[x]$ אי-פריק.

$x^2+1\in\mathbb{Q}[x]$ כן פריק.

(4) $2\in\mathbb{Z}[i]$ הוא פריק כי - $2=(1+i)(1-i)$ (כדאי שהוא נורמה)

זה לא פירוק טריוויאלי כי $2=N(1+i)\neq 2$ (הוא גם פירוק)

ולכן הם לא הפיכים.

דפי

תרגיל: $a\sim b$ ו-a אי פריק אז גם b.

הוכחה: $a\sim b$ חברים ולכן $a=by$ כאשר y הפיך. אם b היה הפיך אז by הפיך אז גם a הפיך בסתירה.

אם $b=x\cdot y$ (x ו-y לא הפיכים) $a=by=x\cdot y\cdot y$

a אי פריק ולכן $\Leftarrow$ x הפיך.

$\Leftarrow$ yy הפיך $\Leftarrow$ y הפיך.

טענה: ב-O_d אם $N(\alpha)$ היא אי-פריקה (ב-$\mathbb{Z}$) אז α הוא אי פריק (ב-O_d).

ההפך לא נכון!

דוגמה: נראה כי $4\pm\sqrt{10}, 2, 3 \in O_{10}$ הם אי פריקים אבל הנורמה שלהם לא מספר ראשוני.

ניקח פירוק $4+\sqrt{10}=xy$ ~~$4+\sqrt{10}=x\cdot y$~~

ונניח בשלילה ש-x,y לא הפיכים $N(x)\neq\pm1$

$$N(4+\sqrt{10})=6=N(x)\cdot N(y)$$

$\Leftarrow$ $N(x)=\pm2,\pm3$.

נרשום $x=a+b\sqrt{10}$

$$N(x)=a^2-10b^2\equiv a^2 \pmod{10}$$

אבל $\pm2,\pm3$ הם לא ריבועים מודולו 10, המשמעות שאין איבר לא הפיך שהנורמה שלו היא $\pm2\ \pm3$ ולכן זה יוצר סתירה להנחת השלילה.

~~ולכן לא יכול להיות~~

אין איבר עם נורמה כזאת ולכן לא יכול להיות פירוק.

הגדרה - איבר $a \in R$ נקרא ראשוני/איבר ראשוני אם הוא לא הפיך ו- $a|bc \Rightarrow a|b$ או $a|c$.

טענה: איבר ראשוני $\Rightarrow$ אי פריק.

הערה: a איבר ראשוני $\Leftrightarrow$ $\langle a \rangle$ אידאל ראשוני. $\Leftrightarrow$ $R/\langle a \rangle$ תחום שלמות