הרצאה 6

הגדרה יהי R חוג חילופי (בעל-יחידה). אידיאל (אמיתי) $P \triangleleft R$ נקרא ראשוני אם
לכל $a,b\in R$, $ab\in P \Leftarrow a\in P$ או $b\in P$.

דוגמא יהי $I \triangleleft \mathbb{Z}$ אידיאל. אזי I ראשוני $\Leftrightarrow$ $I=(0)$ או
$I=p\mathbb{Z}$ כאשר p מספר ראשוני.

הוכחה ($\Rightarrow$) (0) ראשוני כי $\mathbb{Z}$ תחום שלמות.
אם p ראשוני, $a,b\in\mathbb{Z}$, אזי $ab\in p\mathbb{Z} \Leftarrow$
$p|ab \Leftarrow p|a$ או $p|b$ כי p ראשוני $\Leftarrow$
$a\in p\mathbb{Z}$ או $b\in p\mathbb{Z}$.

($\Leftarrow$) כבר מיינו את האידיאלים של $\mathbb{Z}$. יהי $P\triangleleft\mathbb{Z}$
אידיאל ראשוני. נניח בשלילה כי $P\neq(0)$,
$P\neq p\mathbb{Z}$. אזי $P=n\mathbb{Z}$ כאשר $n>1$ לא ראשוני.
אזי $n=ab$ כאשר $1<a,b<n$. ברור
כי $a,b\notin n\mathbb{Z}$ אך $ab=n\in n\mathbb{Z}$ בסתירה
לראשוניות של $P=n\mathbb{Z}$.

טענה יהי R חוג חילופי, $I \triangleleft R$ אידיאל. התנאים הבאים

שקולים: א) I אידיאל ראשוני.

ב) לכל שני אידיאלים $J_1, J_2 \triangleleft R$, אם

$J_1 J_2 \subseteq I$ אז $J_1 \subseteq I$ או $J_2 \subseteq I$.

ג) המנה R/I הינה תחום שלמות.

הוכחה **א) $\Leftarrow$ ב)** נניח שלא, אז יהי $I \triangleleft R$ ראשוני, ויהיו

$J_1, J_2 \triangleleft R$ כך ש- $J_1 J_2 \subseteq I$ אך $J_1 \not\subseteq I$, $J_2 \not\subseteq I$.

אז קיימים $a \in J_1 \setminus I$, $b \in J_2 \setminus I$. אך $ab \in J_1 J_2 \subseteq I$,

קיבלנו $ab \in I$, $a \notin I$, $b \notin I$ בסתירה לראשוניות.

ב) $\Leftarrow$ א) יהי I אידיאל שמקיים את ב) נניח בשלילה

שהוא לא ראשוני. אז קיימים $a, b \in R$ כך ש-

$ab \in I$, $a \notin I$, $b \notin I$. ויהיו $J_1 = (a) = Ra$, $J_2 = (b)$, $J_1 J_2 = (ab)$,

בסתירה ל-ב), כי $J_1 J_2 \subseteq I$

$J_1, J_2 \not\subseteq I$.

__א ⟺ ב__

I ראשוני ⟺ לכל $a,b\in R$ אם $ab\in I$, אזי $a\in I$ או $b\in I$ ⟺

לכל $a+I, b+I\in R/I$, אם $(a+I)(b+I)=ab+I=0_{R/I}$

$ab+I=0+I \iff ab\in I$

אזי בהכרח $a+I=0_{R/I}$ או $b+I=0_{R/I}$

⟺ בחוג R/I אין מחלקי אפס ⟺ R/I תחום שלמות.

__מסקנה__ יהי R חוג חילופי. כל אידיאל מקסימלי של R ראשוני.

__הוכחה__ יהי $I\triangleleft R$ מקסימלי! אזי R/I שדה ⟸ הראשוני.

R/I תחום שלמות ⟸ I ראשוני.

__תכונה__ בשדה F אין מחלקי אפס, אכן, יהיו $a,b\in F$ ו-$ab=0$. אם $a\neq 0$, $a^{-1}ab=a^{-1}0=0$

$b=0$.

הגדרה יהי R חוג בלי יחידה. אידיאל I שמאלי/ימני נקרא ראשי אם הוא נוצר על ידי איבר אחד, כלומר קיים $a\in R$ כך ש- $I=Ra$ / $I=aR$.

הגדרה יהי R חוג חילופי. איברים $a,b\in R$ נקראים חברים אם קיים איבר הפיך $u\in R$ כך ש- $a=ub$.

הערה חברות הינה יחס שקילות. אכן, $a=1a$.

$a=ub \Leftarrow$ קיים v כך ש- $uv=vu=1$ $\Leftarrow$ $va=vub=b$. לכן אם a,b חברים אזי b,a גם חברים.

טרנזיטיביות: $a=ub$, $b=vc$ כאשר u,v הפיכים, $\Leftarrow$ $a=uvc$. אך מכפלה של איברים הפיכים הינה הפיכה: $u'u=uu'=1$, $v'v=vv'=1$ $\Leftarrow$ $uvv'u'=v'u'uv=1$.

הגדרה יהי R חוג, הקבוצה של איברים הפיכים הינה חבורה תחת פעולת הכפל, מסומנים אותה R^*.

דוגמאות F שדה.

$$\left.\begin{aligned} F^* &= F\setminus\{0\} \\ \mathbb{Z}^* &= \{\pm 1\} \\ (\mathbb{Z}/n\mathbb{Z})^* &= U_n \end{aligned}\right\} \text{חבורות לכפל}$$

תרגילים

$$(R[x])^* = R^*$$

$$(R[[x]])^* = \left\{ \sum_{n=0}^{\infty} a_n x^n \;\middle|\; a_0 \in R^* \right\}$$

לדוגמא, בחוג $\mathbb{Z}[[x]]$,

האיבר $1-x$ הפיך, וההפכי הינו

$1+x+x^2+x^3+\dots$.

$a_0 \in R^*$

$$(a_0+a_1x+\dots)(b_0+b_1x+\dots) = 1+0x+0x^2+\dots$$

$a_0b_0=1$, יש פתרון כי a_0 הפיך.

אם $b_0,\dots,b_{n-1}$ כבר נבנו, אז
נסתכל על המקדם של x^n במכפלה:

$$a_0b_n + a_1b_{n-1} + \dots + a_nb_0 = 0$$

צריך למצוא b_n כך ש-

$$a_0b_n = \underbrace{-a_1b_{n-1} - \dots - a_nb_0}_{\text{נתון}}$$

אפשר למצוא b_n כזה כי a_0 הפיך.

<u>טענה</u> יהי R תחום שלמות. יהיו $a,b\in R$ שני איברים.
אז $(a)=(b)$ אם ורק אם a,b חברים.

<u>הוכחה</u> $(\Leftarrow)$ נכון בכל חוג חילופי! אם $a=ub$,
יהי v ההפכי של u, $uv=vu=1$. אז

$$(a)=(b) \Leftarrow \begin{cases} (a)\subseteq(b) \Leftarrow a\in(b) \Leftarrow a=ub \\ (b)\subseteq(a) \Leftarrow b\in(a) \Leftarrow b=va \quad \text{וגם} \end{cases}$$

$\Leftarrow)$ יהי R תחום שלמות. נניח כי $(a)=(b)$.

בפרט, $a\in(b) \Leftarrow$ קיים $r\in R$ כך ש- $a=rb$.

$b\in(a) \Leftarrow$ קיים $s\in R$ כך ש- $b=sa$.

מקבלים: $a=rb=rsa$

$$a-rsa=0$$

$$(1-rs)a=0$$

אם $a=0$, הטענה נכונה.

אם $a\neq 0$, אזי בהכרח $1-rs=0$ כי ב-R אין מחלקי אפס $\Leftarrow rs=sr=1 \Leftarrow r,s$ הפיכים, לכן a,b חברים.

<u>הערה</u> אם R הוא לא תחום שלמות, יכול להיות כי $(a)=(b)$ אך a,b לא חברים.

<u>קצת מוטיבציה</u> יהי F שדה. קבוצה $V\subseteq F^n$ נקראת יריעה אלגברית אם קיימת קבוצה

$S \subseteq F[x_1,\dots,x_n]$ כך ש-

$$V = \{(a_1,\dots,a_n) \in F^n : f(a_1,\dots,a_n) = 0 \quad \forall f \in S\}$$

<u>עובדה</u> אם V יריעה אלגברית, אזי ניתן להגדיר אותה על ידי מספר סופי של פולינומים,

כלומר קיימים $f_1,\dots,f_m \in F[x_1,\dots,x_n]$ כך ש-

$$V = \{\underline{a} = (a_1,\dots,a_n) \in F^n : f_1(\underline{a}) = \dots = f_m(\underline{a}) = 0\}$$

<u>הגדרה</u> בהינתן יריעה אלגברית V, יהי

$$I(V) = \{f \in F[x_1,\dots,x_n] : f(a_1,\dots,a_n) = 0 \quad \forall \underline{a} \in V\}$$

<u>תרגיל</u> $I(V) \trianglelefteq F[x_1,\dots,x_n]$ אידיאל.

כמו כן, אם $I \trianglelefteq F[x_1,\dots,x_n]$ אידיאל, נגדיר יריעה

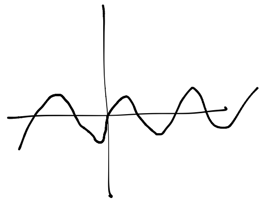
$$V(I) = \{\underline{a} \in F^n : f(\underline{a}) = 0 \quad \forall f \in I\}$$

דוגמאות

$F=\mathbb{R}$

$n=2$

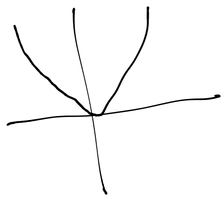
$F[x_1,x_2]=F[x,y]$



$y=\sin x$

$y-\sin x=0$

לא יריעה

$V=$ 

$y=x^2$

$y-x^2=0$

יריעה

$I(V)=(y-x^2)$

אידיאל

$I(V)=(y)$

ציר ה-x-ים

 $=V$

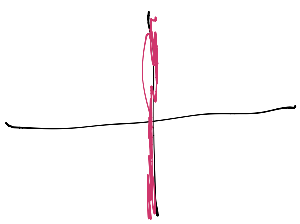
אם $f\notin(y)$, אזי $f=\underbrace{g(x)}_{\neq 0}+yh(x,y)$

קיים $x_0\in\mathbb{R}$ כך ש- $g(x_0)\neq 0$ $\therefore$ $f(x_0,0)\neq 0$

לכן $f\notin I(V)$

קיבלנו $I(V)\subseteq(y)$

ברור $(y)\subseteq I(V)$.



$I(V)=x$

$V=$ איחוד של שני הצירים

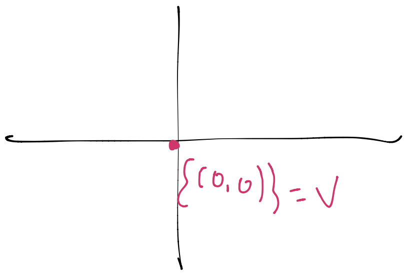
$I(V)=(x)\cap(y)=(xy)$

V לא אי-פריק

$V=\{$ציר $x\}\cup\{$ציר ה-y-ים$\}$

הערה אם V_1,V_2 וריעות, אזי

$$I(V_1\cup V_2)=I(V_1)\cap I(V_2)$$



$I(V)=(x,y)=\{$ פולינומים ללא איבר חופשי $\}$

הגדרה תהי $V\subseteq F^n$ וריעה אלגברית. חוג הקואורדינטות של V הינו

$$A(V)=F[x_1,\dots,x_n]/I(V)$$

"החוג של כל הפונקציות הפולינומיאליות על V"

פילוסופיה תכונות גיאומטריות רבות של V שקולות לתכונות אלגבריות של החוג $A(V)$.

הגדרה וריעה V נקראת אי-פריקה אם

$V=V_1\cup V_2 \Rightarrow V=V_1$ או $V=V_2$

(V_1,V_2 גם וריעות)

משפט תהי $V\subseteq F^n$ יריעה. אזי V אי-פריקה

$\iff$ $I(V)$ הינו אידיאל ראשוני.

דוגמה $V=\{$ציר x-ים$\}$ הוכחנו כי $I(V)=(y)$.

$$F[x,y]/(y) \simeq \underbrace{F[x]}_{\text{תחום שלמות}}$$

לכן $I(V)$ ראשוני $\Longrightarrow$ V אי-פריק.

הוכחת המשפט $\Leftarrow$) נניח כי V אי-פריקה.

נניח בשלילה כי $I(V)$ לא ראשוני. אזי

קיימים $f,g\in F[x_1,\dots,x_n]$, $fg\in I(V)$ $f,g\notin I(V)$

לכן קיימת נקודה $f(\underline{a})\neq 0$ $(a_1,\dots,a_n)\in V$

בהכרח $g(\underline{a})=0$

נאמר כן, יש $\underline{b}\in V$ $f(\underline{b})=0$

$g(\underline{b})\neq 0$

אזי

$$V = \underbrace{\left(V\cap\{\underline{a} : f(\underline{a})=0\}\right)}_{\neq V} \cup \underbrace{\left(V\cap\{\underline{b} : g(\underline{b})=0\}\right)}_{\neq V}$$

בסתירה לאי-פריקות של V.

<u>שאלה</u> איך רואים את המימד של V

בתוך $A(V)$?