הרצאה 5 — 25.3.2020

הגדרה חוג R נקרא פשוט אם אין לו אידיאלים מלבד $R, (0)$.

משפט (Wedderburn) יהי R חוג פשוט, נניח שאין שרשרת יורדת אינסופית של אידיאלים שמאליים

$$I_1 \supsetneq I_2 \supsetneq I_3 \supsetneq \dots$$

(ב-$\mathbb{Z}$ יש שרשראות יורדות אינסופיות

$$(2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq 8\mathbb{Z} \supsetneq 16\mathbb{Z} \supsetneq \dots$$

אזי $R \simeq M_n(D)$ כאשר D חוג עם חילוק.

הגדרה יהי R חוג חילופי, אידיאל $P \triangleleft R$ אמיתי נקרא ראשוני אם לכל $a,b \in R$ מקיימים

$ab \in P \Leftarrow$ $a \in P$ או $b \in P$.

דוגמא $R=\mathbb{Z}$, אזי $I \triangleleft \mathbb{Z}$ ראשוני $\Leftrightarrow I=(0)$

או $I = p\mathbb{Z}$ כאשר p ראשוני.

הוכחה $\Leftarrow$ (0) ראשוני, ברור. $I=p\mathbb{Z}$, $ab \in I$

אזי $p|ab \Leftarrow p|a$ או $p|b \Leftarrow$ $a\in I$, $b \in I$.

$\Rightarrow$) $I \neq \mathbb{Z}$ כי ראשוני לפי הגדרה אמיתי. כל אידיאל אחר שעדיין לא טיפלנו בו הינו

מן הצורה $n\mathbb{Z}$, n מספר פריק,

$n=ab$ $\;1<a,b<n$. אזי

$ab=n\in n\mathbb{Z}$, $a,b\notin n\mathbb{Z}$. אזי $n\mathbb{Z}$ לא ראשוני.

המשפט היסודי של אריתמטיקה בניסוח הנ״ל:

יהי $\mathbb{Z} \trianglerighteq I \neq (0)$. אזי ניתן לרשום את I כמכפלה של אידיאלים ראשוניים $I=P_1P_2\cdots P_r$, המכפלה הנ״ל יחידה עד כדי החלפת סדר הגורמים.

הערה $I=\mathbb{Z}=1\mathbb{Z}$ המשפט עדיין נכון:

$I=$ (מכפלה ריקה)

$(I\cdot R=I)$

הגדרה) R חוג, איבר $0\neq a\in R$ נקרא מחלק אפס שמאלי (ימני) אם קיים $0\neq b\in R$ כך ש- $ab=0$ $(ba=0)$.

2) איבר $0\neq a\in R$ נקרא רגולרי שמאלי (ימני) אם הוא לא מחלק אפס שמאלי (ימני).

טענה יהי a רגולרי שמאלי (ימני). אזי

$ab=ac \Rightarrow b=c$ $\;(ba=ca \Rightarrow b=c)$.

__הוכחה__ $ab=ac \Leftarrow a(b-c)=ab-ac=0$.

a רגולרי משמאל $\Leftarrow$ לא קיים $b'\neq 0$ כך ש- $ab'=0 \Leftarrow b-c=0 \Leftarrow b=c$.

__הגדרה__ חוג חילופי רגיל נקרא תחום שלמות (תחום) אם אין בו מחלקי אפס.

__טענה__ יהי R תחום שלמות. ויהיו $a,b\in R$.

אזי $\underset{\overset{\shortparallel}{Ra}}{(a)}=\underset{\overset{\shortparallel}{Rb}}{(b)} \iff$ קיים $u\in R$ הפיך כך ש- $b=au$.

__הוכחה__ $\Rightarrow$) נכון לכל חוג. $b\in Ra \Leftarrow b=au$
$Rb\subset Ra \Leftarrow$.

יהי $uv=1$, אזי $Ra\subseteq Rb \Leftarrow bv=auv=a$
לכן $Ra=Rb$.

$\Leftarrow$) נניח $(a)=(b)$. אזי $a\in(b) \Leftarrow$
קיים $r\in R$ כך ש- $a=rb$.
כמו כן קיים $s\in R$ כך ש- $b=sa$.

אבל $(a)=(b)=(0)$, אז $a=b=0$

והטענה נכונה. אז נניח $a,b\neq 0$.

$$a=rb$$

$$b=sa=srb$$

$$b(1-sr)=0.$$

R תחום, לכן b לא מחלק אפס, אבל

$b\neq 0 \Rightarrow 1-sr=0 \Rightarrow 1=sr=rs$,

לכן s,r הפיכים.

<u>טענה</u> יהי R חוג חילופי, $I\triangleleft R$.

אז I ראשוני $\iff R/I$ תחום שלמות

<u>הוכחה</u> ($\Leftarrow$) נניח בשלילה R/I

לא תחום שלמות, אזי יש בו

מחלקי אפס. כלומר יש מחלקים

$a+I,\ b+I \in R/I$ כך ש-

$$0_R+I = 0_{R/I} \neq a+I,\ b+I$$

אבל $(a,\ b \notin I)$

$$(a+I)(b+I) = ab+I = 0_{R/I}$$

כלומר $ab \in I$.

לכן I לא ראשוני.

($\Rightarrow$) כל צעד בהוכחה הקודמת

היה הפך.

מסקנה כל אידאל מקסימלי של חוג חילופי הינו ראשוני.

הוכחה I מקס' $\Leftarrow$ R/I שדה.

בשדה אין מחלקי אפס.

נניח R שדה

$ab=0$) , אם $b=0$ סיימנו, אחרת $a=0b^{-1}=0$, לכן R/I תחום שלמות

לכן I ראשוני.

טענה R חוג חילופי. אזי

R תחום שלמות $\Leftrightarrow$ (0) אידאל ראשוני.

הגדרה חוג שלמות R נקרא חוג ראשי אם כל אידיאל $I \trianglelefteq R$ הינו ראשי. לזכור: אידיאל ראשי הינו אידיאל שנוצר ע״י איבר אחד.

דוגמא $\mathbb{Z}$ חוג ראשי.

טענה יהי R חוג ראשי. יהי $P \trianglelefteq R \neq (0)$ אידיאל ראשוני. אזי P מקסימלי.

הוכחה לפי משפט מן השיעור הקודם, קיים אידיאל מקסימלי $M \trianglelefteq R$

כך ש- $P \le M$. לפי הקחה, ש-

R תחום ראשי, קיים $m \in R$

כך ש- $M=(m)$, כמו כן $P=(p)$

עבור $p \in R$ מתאימים. בפרט,

$p \in P \le M \Rightarrow p = mr$ עבור

$r \in R$ מתאימים.

P ראשוני $\Rightarrow$ $m \in P$ או $r \in P$. אם $m \in P$

אזי $M=(m) \subseteq P \Rightarrow P=M$

וסיימנו.

אם $r \in P \Rightarrow r = ps \Rightarrow$

$p = mr = msp$, R תחום שלמות, $p \neq 0$

כי $P\neq(0)$, אזי P רגולרי $\Leftarrow$

$1=ms=sm$ $\Leftarrow$ m הפיך $\Leftarrow$

$R=(m)$, בסתירה למקסימליות של M.

קיבלנו $P=M$, כלומר P מקסימלי!

<u>טענה</u> יהי R תחום שלמות סופי. אזי R שדה.

<u>הוכחה</u> יהי $0\neq a\in R$.

אזי a רגולרי, $ab=ac \Rightarrow b=c$.

נגדיר העתקה $\mu_a : R \to R$
$\mu_a(x) = ax$.

(לא בהכרח הומ' של חוגים).

לפי ההבחנה הנ"ל, μ_a חד-חד-ערכי.

R סופי $\Leftarrow$ μ_a גם על.

בפרט קיים $b \in R$ כך ש-

$ba = ab = \mu_a(b) = 1$.

<u>משפט</u> (Wedderburn) יהי R חוג סופי עם חילוק. אזי R חילופי, כלומר R שדה.

לא נוכיח את זה.

דוגמאות של אידאלים ראשוניים ולא

1. $R=\mathbb{Z}[x]$.

ניקח את האידאל $I=(x)$.

$I = $ (פולינומים ללא מקדם חפשי)

$(a_0+a_1x+\cdots)(b_0+b_1x+\cdots) = a_0b_0 + $ (מונומים מדרגה ≥ 1)

(הוכחנו שאם R תחום שלמות אם ורק אם (x) ראשוני בתוך $R[x]$)

אפשר להוכיח ישירות מן ההגדרה כמו למעלה.

$R[x]/(x) \cong R$.

2. $R[x]$, R חילופי.

$I=(x^2)$.

$I=\{f=a_0+a_1x+\cdots+a_nx^n : a_0=a_1=0\}$

$x\cdot x = x^2 \in I$

$x\notin I \Leftarrow I$ לא ראשוני.

3. $R=\mathbb{Z}[x]$, $I=(2,x) = 2R+xR$.

$I = \{$ (פולינומים שכל המקדמים זוגיים) $+$ (פולינום עם מקדם חופשי 0) $\} =$

$\{f=a_0+\cdots+a_nx^n : a_0$ זוגי $\}$

I ראשוני $\Leftarrow (a_0+\dots)(b_0+b_1x+\dots)\in I$

a_0b_0 זוגי $\Leftarrow$ a_0 או b_0 זוגי $\Leftarrow$

$(a_0+a_1x+\dots)$ או $(b_0+b_1x+\dots)$ שייך ל-I.

$$(0)\neq(x)\subsetneq(2,x)$$

שניהם ראשוניים.

לפי הטענה הקודמת (לפני), $\mathbb{Z}[x]$ לא תחום ראשי.

נוכיח בשבוע הבא כי $(2,x)$ לא ראשי.

<u>הגדרה</u> יהי F שדה, יהי $X\subseteq F^n$.

כל פולינום $g(x_1,\dots,x_n)\in F[x_1,\dots,x_n]$

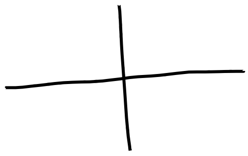
הינו פונקציה $F^n\to F$ הומ' של חוגים

$(a_1,\dots,a_n)\mapsto g(a_1,\dots,a_n)$

$$I(X)=\{g\in F[x_1,\dots,x_n] \mid g(a_1,\dots,a_n)=0 \text{ לכל } (a_1,\dots,a_n)\in X\}$$

שים לב כי $I\trianglelefteq F[x_1,\dots,x_n]$

<u>דוגמא</u> 1) $X\subseteq\mathbb{R}^2$

$X=$ 

$(0,a_2)$

$(a_1,0)$

$I(X)=(xy)\subseteq\mathbb{R}[x,y]$

$X=\{(0,0)\}$ $\quad I(X)=(x,y)$

$X=\{(\pi,\pi)\}$ $\quad I(X)=(0)$

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

חוג הקואורדינטות של X.