הגדרה: חוג R נקרא פשוט אם אין לו אידאלים מלבד R, (0)

משפט: (Wedderburn)

יהי R חוג פשוט, נניח שאין שרשרת יורדת אינסופית של אידאלים שמאליים
$I_1 \supsetneq I_2 \supsetneq I_3 \supsetneq \dots$

(ב- $\mathbb{Z}$ יש שרשראות יורדות אינסופיות $2\mathbb{Z} \supsetneq 4\mathbb{Z} \supsetneq 8\mathbb{Z} \supsetneq \dots$)

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

הגדרה: יהי R חוג חילופי, אידאל $P \lhd R$ נקרא ראשוני אם לכל $a,b \in R$ מתקיים
$ab \in P \Rightarrow a \in P$ או $b \in P$

דוגמאות:

$R = \mathbb{Z}$, אזי $I \lhd \mathbb{Z}$ ראשוני $\Leftrightarrow I = (0)$ או $I = p\mathbb{Z}$ כאשר p ראשוני

הוכחה:

$(\Rightarrow)$ (0) ראשוני - ברור. $I = p\mathbb{Z}$, $ab \in I$ אזי $p|ab \Rightarrow p|a$ או $p|b \Rightarrow$ $a \in I$ או $b \in I$

$(\Leftarrow)$ $I = \mathbb{Z}$ לא ראשוני (כי לא אמיתי). כל אידאל אחר שעדיין לא טיפלנו בו הוא מהצורה $n\mathbb{Z}$, n מספר פריק. $n = ab$. $1 < a,b < n$. אזי $ab = n \in n\mathbb{Z}$ ו- $a,b \notin n\mathbb{Z}$. אזי $n\mathbb{Z}$ לא ראשוני

המשפט היסודי של האריתמטיקה (בניסוח הנכון):

יהי $(0) \neq I \lhd \mathbb{Z}$. אזי ניתן לפרק את I כמכפלה של אידאלים ראשוניים $I = P_1 \dots P_r$. המכפלה הנ"ל יחידה עד כדי החלפת סדר הגורמים.

הערה: עבור $I = \mathbb{Z}$ המשפט עדיין נכון $I = (\text{מכפלה ריקה})$ $(I \cdot R = I)$

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

הגדרה: R חוג, איבר $0 \neq a \in R$ נקרא רגולרי שמאלי (ימני) אם הוא לא מחלק אפס שמאלי (ימני)

טענה:

יהי a רגולרי משמאל (ימין). אזי $b=c \Leftarrow ab=ac$ $\quad (b=c \Leftarrow ba=ca)$

הוכחה:

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

$b=c \Leftarrow b-c=0 \Leftarrow ab'=0$

הגדרה: חוג חילופי נקרא תחום שלמות אם אין בו מחלקי אפס

טענה:

יהי R תחום שלמות. יהיו $a,b\in R$ אזי $\underset{Ra}{\underset{\|}{(a)}}=\underset{Rb}{\underset{\|}{(b)}} \Leftrightarrow$ קיים $u\in R$ הפיך כך ש- $b=au$

הוכחה:

$(\Rightarrow)$ נכון לכל חוג. $Rb\subseteq Ra,\ b\in Ra \Leftarrow b=au$

יהי $v\in R$ כך ש $uv=1 \Leftarrow bv=auv=a \Leftarrow Ra\subseteq Rb$

ובסה"כ $Ra=Rb$

$(\Leftarrow)$ נניח $(a)=(b)$. אזי $a\in(b) \Leftarrow$ קיים $r\in R$ כך ש $a=rb$

כמו כן, קיים $s\in R$ כך ש $b=sa=srb \Leftarrow (1-sr)b=0$

(אם $(a)=(b)=(0)$ אזי $a=b=0$. לכן נניח $a,b\neq 0$)

R תחום, לכן b לא מחלק אפס, $b\neq 0 \Leftarrow 1-sr=0 \Leftarrow rs=sr=1$

לכן r,s הפיכים

טענה:

יהי R חוג חילופי, $I\triangleleft R$. אזי I ראשוני $\Leftrightarrow R/I$ תחום שלמות

הוכחה:

$(\Leftarrow)$ נניח בשלילה ש R/I לא תחום שלמות. לכן יש בו מחלקי אפס. כלומר,

יש מחלקות $a+I, b+I\in R/I$ כך ש $0_R+I=0_{R/I}\neq a+I,\ b+I$

לכן $a,b\notin I$. אבל $(a+I)(b+I)=ab+I=0_{R/I}$, כלומר $ab\in I$

לכן I לא ראשוני. בסתירה

$(\Longrightarrow)$ כל צעד בהוכחה הקודמת בכיוון ההפוך

תוצאה:

כל אידיאל מקסימלי של חוג חילופי הוא ראשוני

הוכחה:

I מקסי' $\Leftarrow$ 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

ולכן I ראשוני

טענה:

R חוג חילופי. אזי R תחום שלמות $\Longleftrightarrow$ (0) אידיאל ראשוני

הגדרה: תחום שלמות R נקרא תחום ראשי אם כל אידיאל $I\trianglelefteq R$ הוא ראשי

תזכורת: אידיאל ראשי הוא אידיאל שנוצר על ידי איבר אחד

דוגמא: $\mathbb{Z}$ הוא תחום ראשי

טענה:

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

הוכחה:

לפי משפט מהשיעור הקודם קיים אידיאל מקסימלי $M\trianglelefteq R$ כך ש $P\le M$.

לפי ההנחה ש-R תחום ראשי, קיים $m\in R$ כך ש $M=(m)$, כמו כן $P=(p)$

עבור $p\in R$ מתאים. בפרט $p\in P\le M$ $\Leftarrow$ $p=mr$ עבור $r\in R$ מתאים

P ראשוני $\Leftarrow$ $m\in P$ או $r\in P$. אם $m\in P$ אזי $M=(m)\le P$ $\Leftarrow$ $P=M$ וסיימנו

אם $r\in P$ $\Leftarrow$ $r=sp$ $\Leftarrow$ $p=mr=msp$. R הוא תחום שלמות, $p\neq 0$ כי $P\neq(0)$

אזי p רגולרי $\Leftarrow$ $ms=1$ $\Leftarrow$ m הפיך $\Leftarrow$ $(m)=R$ בסתירה למקסימליות של M

$mm^{-1}=1$

לכן p מקסימלי

טענה:

יהי R תחום שלמות סופי. אזי R שדה.

הוכחה:

יהי $0\neq a\in R$ אזי a רגולרי, $ab=ac \Rightarrow b=c$

נתבונן בהעתקה $\mu_a:R\to R$ $\mu_a(x)=ax$ (זה לא בהכרח הומ' של חוגים)

לפי האבחנה הנ"ל, μ_a חח"ע. R סופי $\Leftarrow$ μ_a גם על

בפרט קיים $b\in R$ כך ש $ba=ab=\mu_a(b)=1$

משפט: (Wedderburn)

יהי R חוג סופי עם חילוק. אזי R חילופי, כלומר R שדה. - לא נוכיח

דוגמאות של אידאלים ראשוניים ולא ראשוניים:

1) $R=\mathbb{Z}[x]$ ניקח את האידאל $I=(x)$.

$I=\left(\text{פולינומים ללא מקדם חופשי}\right)$

$(a_0+a_1x+\ldots)(b_0+b_1x+\ldots)=a_0b_0+\left(\text{מונומים מדרגה } \geq 1\right)$

(הוכחנו שאם R תחום שלמות $\Longleftrightarrow$ (x) ראשוני בחוג $R[x]$)

אפשר להוכיח ישירות מההגדרה כמו למעלה. $R[x]/(x)\cong R$

2) R חוג חילופי. $R[x]$, $I=(x^2)$

I לא ראשוני $\Leftarrow$ $x\notin I$, $x\cdot x=x^2\in I$

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

$I=\left\{\left(\text{פולינום עם מקדמים זוגיים}\right)+\left(\text{פולינום עם מקדם חופשי } 0\right)\right\}=\{f=a_0+\ldots+a_nx^n:\ a_0 \text{ זוגי}\}$

I ראשוני כי

$(a_0+a_1x+\dots)(b_0+b_1x+\dots)\in I \Rightarrow a_0b_0$ זוגי $\Rightarrow a_0$ או b_0 זוגי $\Rightarrow (a_0+a_1x+\dots)$ או $(b_0+b_1x+\dots)$ שייך ל- I

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

שניהם ראשוניים

לפי טענה קודמת, $\mathbb{Z}[x]$ לא תחום ראשי: נוכיח בפעם הבאה כי $(2,x)$ לא ראשי

הגדרה: יהי F שדה. תהי $X\subseteq F^n$. כל פולינום $g(x_1,\dots,x_n)\in F[x_1,\dots,x_n]$

הינו פונקציה $F^n\to F$

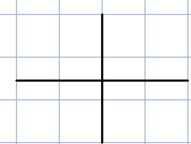
$(a_1,\dots,a_n)\mapsto g(a_1,\dots,a_n)$

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

טענה:

$I \trianglelefteq F[x_1,\dots,x_n]$

דוגמאות:

1) $X\subseteq\mathbb{R}^2$, $X=$  , $I(X)=(xy)\subseteq\mathbb{R}[x,y]$

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

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

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