תזכורת:

הגדרנו חוגי הערכה, חוגי הערכה בדידה

דוגמאות: $F[[x]]$, $\mathbb{Z}_p$ חוגי הערכה בדידה

$0\neq x\in\mathbb{Z}_p \Leftarrow x=p^n u$ $n\in\mathbb{Z}$, $u\in\mathbb{Z}_p^* \Leftarrow V(x)=n$, $V(0)=\infty$ זו הערכה בדידה

$\mathbb{Z}_p=\{x\in\mathbb{Q}_p : V(x)\geq 0\}$

כמו כן, $0\neq y\in \operatorname{Frac} F[[x]]$. אזי $y$ הוא טור לורן $y=x^n\underbrace{(a_0+a_1x+\dots)}_{\text{הפיך}}$

$V(y)=n$. זו הערכה בדידה על השדה של טורי לורן $F((x))$, החוג $F[[x]]$

הוא חוג הערכה

הגענו לחוגים הולכה דרך השלמה. חוג $R$, אידאל מקסימלי $I\trianglelefteq R$, $\bigcap_{n=1}^{\infty} I^n=(0)$ $\Leftarrow$ השלמה $\hat{R}$

טענה:

אם $R$ נתרי, אזי $\hat{R}$ גם נתרי. אם $I$ ראשי, אזי $\hat{R}$ תמיד חוג הערכה בדידה

שאלה:

לכל $I,R$ כנ"ל אפשר להגדיר, לכל $0\neq x\in\hat{R}$, $V(x)=\max\{n : x\in\hat{I}^n\}$

נוכל להרחיב את זה באופן טבעי ל-$\operatorname{Frac}\hat{R}$. האם תמיד $V(xy)=V(x)+V(y)$?

---

דוגמא: (חוג הערכה שאינו חוג הערכה בדידה)

יהי $F$ שדה. נתבונן בשרשרת של חוגי פולינומים:

$$F[x]\subseteq F[x^{1/2}]\underset{y=x^{1/2}}{\cong} F[y] \longrightarrow F[y^2]\subseteq F[y]$$

$$F[x]\subseteq F[x^{1/2}]\subseteq F[x^{1/4}]\subseteq F[x^{1/8}]\subseteq\dots$$

כל אחד הו חוג פולינומים, נשלים את כולם באידיאל המקסימלי $x^{1/2^n}$

שדות השברים: $F[[x]]\subseteq F[[x^{1/2}]]\subseteq F[[x^{1/4}]]\subseteq\dots$

יהי $R=\bigcup_{n=0}^{\infty} F[[x^{1/2^n}]]$, $F=\operatorname{Frac}R=\bigcup_{n=0}^{\infty} F((x^{1/2^n}))$

אנחנו יודעים שכל $F[[x^{1/2^n}]]$ הוא חוג הערכה בדידה. לכן $R$ הוא חוג הערכה

אכן, $x\in F \Leftarrow x\in F((x^{1/2^n}))$ עבור $n$ מספיק גדול $\Leftarrow$ $x$ או $x^{-1}$ מוכל ב-$F[[x^{1/2^n}]]$

⇐ $x\in R$ או $\frac{1}{x}\in R$

אבל $R$ לא נתרי, כי יש שרשרת עולה של אידאלים $(x)\subsetneq(x^{1/2})\subsetneq(x^{1/4})\subsetneq\dots$

לכן $R$ לא חוג הערכה בדידה

---

דוגמא של שימוש במספרים p-אדיים כדי להוכיח משפט בתורת המספרים האלמנטרית:

מקדמים בינומיאליים: $\binom{n}{k}=\frac{n!}{k!(n-k)!}\in\mathbb{Z}$ אם $n,k\in\mathbb{N}$. אפשר להכליל את ההגדרה הבאה:

לכל $\alpha\in R$ נגדיר $\binom{\alpha}{k}=\frac{\alpha(\alpha-1)\cdot\ldots\cdot(\alpha-(k-1))}{k!}$ $(k\in\mathbb{N})$

אם $\alpha\in\mathbb{Q}$, אזי ברור כי $\binom{\alpha}{k}\in\mathbb{Q}$. אפשר להגיד יותר מזה:

טענה:

יהי $\alpha=\frac{m}{n}$. אזי לכל $k$ $\binom{\alpha}{k}\in\mathbb{Z}[\frac{1}{n}]=\{\frac{a}{b}\in\mathbb{Q}\mid b=n^{\ell},\ell\in\mathbb{N}\}$

הוכחה:

לכל $p$ ראשוני, נסמן $\mathbb{Z}_{(p)}=S^{-1}\mathbb{Z}$ כאשר $S=\mathbb{Z}\setminus p\mathbb{Z}$. נשים לב כי $\mathbb{Z}_{(p)}\subseteq\mathbb{Z}_p$

$$\underset{(p\nmid n)}{\mathbb{Z}_{(p)}\ni\frac{m}{n}}\longmapsto\Big(\underbrace{(m+p\mathbb{Z}_p)(n+p\mathbb{Z}_p)^{-1}}_{\in\mathbb{Z}/p\mathbb{Z}},\underbrace{(m+p^2\mathbb{Z}_p)(n+p^2\mathbb{Z}_p)^{-1}}_{\in\mathbb{Z}/p^2\mathbb{Z}},\dots\Big)\in\mathbb{Z}_p$$

נשים לב כי: $\mathbb{Z}[\frac{1}{n}]=\bigcap_{p\nmid n}\mathbb{Z}_{(p)}$

לכן מספיק להוכיח כי $\binom{m/n}{k}\in\mathbb{Z}_p$ לכל $p\nmid n$. (בנוסף, נשים לב כי $\mathbb{Z}_{(p)}=\mathbb{Z}_p\cap\mathbb{Q}$. ברור כי $\binom{m/n}{k}\in\mathbb{Q}$, לכן מספיק כי $\binom{m/n}{k}\in\mathbb{Z}_p$ לכל $p\nmid n$)

נגדיר פונקציה $f:\mathbb{Q}_p\to\mathbb{Q}_p$, $f(x)=\frac{x(x-1)\cdot\ldots\cdot(x-(k-1))}{k!}$ ונוכיח כי $f$ רציפה (בטופולוגיה של $\mathbb{Q}_p$ הנגזרת מן ההערכה $v_p$, בסיס של קבוצות פתוחות כי $\{y\in\mathbb{Q}_p : v(x-y)\geq n\}$ $(n\in\mathbb{N}, x\in\mathbb{Q}_p)$. ידוע לנו כי $f(\mathbb{Z})\subseteq\mathbb{Z}$. אך $\mathbb{Z}_p$ הוא הסגור של $\mathbb{Z}$ בטופולוגיה הנ"ל.

לכן הרציפות של $f$ גוררת $f(\mathbb{Z}_p)\subseteq\mathbb{Z}_p$. אך $p\nmid n$, לכן $\frac{m}{n}\in\mathbb{Z}_{(p)}\subseteq\mathbb{Z}_p$. לכן $\binom{m/n}{k}=f(\frac{m}{n})\in\mathbb{Z}_p$

וסיימנו.

---

## מספר נושאים על חילוקיים:

הגדרה: חוג עם חילוק הוא חוג $R$ כך שלכל $0\neq a\in R$ קיים איבר $b\in R$ כך ש- $ab=ba=1$

חוג חילופי עם חילוק = שדה

### משפט (המשפט הקטן של Wedderburn)

יהי $R$ חוג עם חילוק סופי, אזי $R$ חילופי, כלומר $R$ שדה

### דוגמא (הקווטרניונים של המילטון (1843))

$\mathbb{H}$ הוא מרחב וקטורי 4-מימדי מעל $\mathbb{R}$ עם בסיס $1,i,j,k$, ועם כפל $\mathbb{R}$ ליניארי

בנוסף מהיחסים הבאים $ki=-ik=j$, $jk=-kj=i$, $ij=-ji=k$, $i^2=j^2=k^2=-1$

לכל $\alpha=a+bi+cj+dk\in\mathbb{H}$ נגדיר הצמדה $\alpha^*=a-bi-cj-dk$

$$N(\alpha)=\alpha\alpha^*=a^2-b^2i^2-c^2j^2-d^2k^2=a^2+b^2+c^2+d^2\in\mathbb{R}$$

ברור כי $N(\alpha)=0\iff\alpha=0$. לכן לכל $0\neq\alpha\in\mathbb{H}$, $\beta=\frac{1}{N(\alpha)}\alpha^*$ מקיים $\alpha\beta=\beta\alpha=1$. כלומר,

$\mathbb{H}$ הוא חוג עם חילוק שאינו שדה.

הגדרה: חוג $R$ (לא בהכרח חילופי) נקרא פשוט אם אין לו אידאלים דו-צדדיים מלבד $R, (0)$

דוגמא: כל חוג עם חילוק הוא פשוט.

הוכחה: יהי $R$ חוג עם חילוק. יהי $I$ אידאל שמאלי (בהתאמה, ימני). יהי $0\neq a\in I$. אז

קיים $b\in R$ כך ש $ab=ba=1$. לכן $1=ba\in Ra\subseteq I$ (בהתאמה $1=ab\in aR\subseteq I$)

אז ל-$R$ אין אידאלים חד צדדיים מלבד $R,(0)$, כל שכן אידאלים דו-צדדיים.

הגדרה: יהי $R$ חוג, $I\subseteq R$ אידאל שמאלי/ימני. נגדיר $M_n(I)=\left\{\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\\ a_{n1}&\cdots&a_{nn}\end{pmatrix}\in M_n(R)\mid a_{ij}\in I\right\}$

$M_n(I)$ הוא אידאל שמאלי/ימני של $M_n(R)$ (לכן אם $I\trianglelefteq R$ דו-צדדי $\Leftarrow M_n(I)\trianglelefteq M_n(R)$ דו-צדדי.

בשיעורי בית: יהי $J\trianglelefteq M_n(R)$ אידאל דו-צדדי. אזי קיים $I\trianglelefteq R$ כך ש- $J=M_n(I)$.

מסקנה:

יהי $R$ חוג עם חילוק. אזי $M_n(R)$ הוא חוג פשוט לכל $n$.

הגדרה: יהי $R$ חוג. אידאל שמאלי/ימני $I$ נקרא מינימלי אם $I\neq(0)$ ולא קיים $(0)\subsetneq J\subsetneq I$

($J$ שמאלי/ימני)

דוגמאות:

1) לחוג $\mathbb{Z}$ אין אידאלים מינימליים

2) יהי $R$ חוג ארטיני משמאל/מימין (אין שרשראות יורדות $(I_1\supsetneq I_2\supsetneq I_3\supsetneq\ldots$

אזי ל-$R$ יש אידאלים מינימליים משמאל/מימין

משפט (Wedderburn (1908±5)):

יהי $R$ חוג פשוט. נניח שיש ל-$R$ אידאל מינימלי שמאלי או ימני. אזי קיים חוג עם חילוק $D$ ומספר $n\in\mathbb{N}$

כך ש $R\cong M_n(D)$

כדי להוכיח את זה נשתמש בטענה הבאה:

טענה (Brauer, 1942):

יהי $R$ חוג ויהי $I$ אידאל שמאלי מינימלי כך ש $I^2\neq(0)$. אזי קיים $e\in R$ כך ש:

1) $e$ הוא אידמפוטנט: $e^2=e$

2) $I=Re$

3) החוג $eRe$ הוא חוג עם חילוק

מה הכוונה? $eRe=\{eae:a\in R\}\subseteq R$, $eae+ebe=e(a+b)e$, $eae\cdot ebe=e(aeb)e$

נשים לב כי $e=e1e\in eRe$, $e\cdot eae=e^2ae=eae$, $eae\cdot e=eae^2=eae$

לכן $e$ הוא יחידה בכפל של החוג $eRe$, לכן $eRe$ הוא חוג.

אבל, אם $I$ אידאל אמיתי, אזי $e\neq1$, לכן החוג $eRe$ אינו תת חוג של $R$.

הוכחה:

כנתון כי $I^2\neq(0)$, לכן קיימים $x,y\in I$ כך ש $Ix=\{yx:y\in I\}\neq0 \Leftarrow yx\neq0$

מצד שני, $Ix$ הוא אידאל שמאלי של $R$. $Ix\subseteq Rx\subseteq I \Leftarrow x\in I$.

לפי המינימליות של $I$ מקבלים $Ix=I$. בפרט, קיים $e\in I$ כך ש- $ex=x$. בפרט, $e^2x=ex=x$

$(e^2-e)x=0$. אבל גם $e^2-e\in I$. נשים לב כי $e^2-e\in \underbrace{I\cap Ann_R(x)}_{\text{אידאל שמאלי של } R}=J$ $\quad(Ann_R(x)=\{r\in R:rx=0\})$

וגם $I\neq J \Leftarrow e\notin J \Leftarrow ex=x\neq0$. וגם $J\subseteq I$, ולפי המינימליות של $I$ מקבלים $J=(0)$. לכן

$e^2=e \Leftarrow e^2-e=0$. כלומר, $e$ אידמפוטנט.

בנוסף, $e\neq 0$ (כי $ex=x\neq 0$), לכן $(0)\neq Re\subseteq I$, לכן $Re=I$ לפי המינימליות של $I$.