הרצאה 25

בפעם שעברה הגדרנו חוגי הערכה, חוגי הערכה בדידה.

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

$0 \neq x \in \mathbb{Q}_p = \mathrm{Frac}\,\mathbb{Z}_p \Leftarrow x = p^n u$ $n \in \mathbb{Z}$, $u \in \mathbb{Z}_p^*$

$$v(x) = n$$

$$v(0) = \infty$$

כי הערכה בדידה

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

כמו כן $0 \neq y \in \mathrm{Frac}\, F[[x]]$

אזי x הינו טור לורן

$$y = x^n \underbrace{(a_0 + a_1 x + \dots)}_{\text{הפיך}} \qquad a_0 \neq 0$$

$$v(y) = n$$

כי הערכה בדידה על השדה של טורי לורן $F((x))$, החוג $F[[x]]$ הוא חוג ההערכה.

הענין לחוגים הולך דרך השלמה.

חוג R, אידיאל מקסימלי $I \triangleleft R$, $\bigcap_{n=1}^{\infty} I^n = (0)$ $\Leftarrow$ השלמה $\hat{R}$.

<u>טענה</u> אם R נתרי, אזי $\hat{R}$ גם נתרי.

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

<u>הוכחה</u> לכל R, I 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 של חוג הערכה שאינו חוג הערכה בדידה.

יהי F שדה. נתבונן בשרשרת של חוגי פולינומים:

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

$$F[y^2] \subseteq F[y] \qquad y = x^{1/2}$$

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

כל אחד הוא חוג פולינומים, נשלים

אך כולם באידיאל המקסימלי $(x^{1/2^n})$.

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

שדות השברים

$$F((x)) \subseteq F((x^{1/2})) \subseteq F((x^{1/4})) \subseteq \dots$$

יהי

$$R = \bigcup_{n=0}^{\infty} F[[x^{\frac{1}{2^n}}]]$$

$$F = \text{Frac } R = \bigcup_{n=0}^{\infty} F((x^{1/2^n})).$$

וידוע לנו כבר ש $F[[x^{\frac{1}{2^n}}]]$ הינו חוג

הערכה בדידה. לכן R 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- $F[[x^{1/2^n}]] \Leftarrow$

$x \in R$ או $\frac{1}{x} \in R$.

אבל R לא נתרי, כי יש שרשרת עולה של אידאלים

$$(x) \subsetneq (x^{1/2}) \subsetneq (x^{1/4}) \subsetneq (x^{1/8}) \subsetneq \dots$$

לכן R לא חוג הערכה בדידה..

דוגמא אחת של שימוש במספרים ק-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: לכל $\alpha\in\mathbb{R}$ נגדיר
$k\in\mathbb{N}$

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-(k-1))}{k!}$$

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

<u>טענה</u> יהי $\alpha=\frac{m}{n}$. אזי לכל k

$$\binom{\alpha}{k}\in\mathbb{Z}\left[\frac{1}{n}\right] = \left\{\frac{a}{b}\in\mathbb{Q} \,\middle|\, b=n^\ell,\ \ell\in\mathbb{N}\right\}$$

<u>הוכחה:</u> לכל p ראשוני נסמן

$$\mathbb{Z}_{(p)} = S^{-1}\mathbb{Z}$$

כאשר $S = \mathbb{Z} \setminus p\mathbb{Z}$.

נשים לב כי $\mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p$

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

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

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 להוכיח כי

$\binom{m/n}{k} \in \mathbb{Z}_p$ לכל $p \nmid n$.

נגדיר פונקציה $f : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$

$$f(x) = \frac{x(x-1)\cdots(x-(k-1))}{k!}$$

ונוכיח כי f רציפה (בטופולוגיה) של $\mathbb{Q}_p$ הנוצרת מן הנורמה v_p, בסיס של קבוצות פתוחות כי

$$\{y \in \mathbb{Q}_p : v(x-y) \geq n\} \quad x \in \mathbb{Q}_p \quad n \in \mathbb{N}$$

ידוע לנו כי $f(\mathbb{Z}) \subseteq \mathbb{Z}$. אך $\mathbb{Z}_p$ הינו הסגור של $\mathbb{Z}$ בטופולוגיה הנ"ל. לכן הרציפות של f גוררת $f(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$. אך מצד, לכן $\frac{m}{n} \in \mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p$. לכן $\binom{m/n}{k} = f\left(\frac{m}{n}\right) \in \mathbb{Z}_p$.

וסיימנו

כמה נושאים לא חילופיים

<u>הגדרה</u> חוג עם חילוק הינו חוג R כך שלכל $0 \neq a \in R$ קיים איבר $b \in R$ כך ש- $ab = ba = 1$.

חוג עם חילוק חילופי = שדה.

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

<u>הדוגמא</u> הקנונית של המילטון (1843)

$\mathbb{H}$ הינו מרחב וקטורי 4-מימדי מעל $\mathbb{R}$ עם בסיס $1, i, j, k$, ועם כפל $\mathbb{R}$-לינארי מוגדר מן היחסים הבאים:

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

$$i^2 = j^2 = k^2 = -1.$$

מדוע זה חוג עם חילוק?

לכל $a, b, c, d \in \mathbb{R}$

$$\alpha = a + bi + cj + dk \in \mathbb{H}$$

נגדיר הצמוד,

$$\alpha^* = a - bi - cj - dk$$

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

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

<u>הגדרה</u> חוג R (לאו בהכרח חילופי) נקרא פשוט אם אין לו אידיאלים דו-צדדיים מלבד (0), R.

<u>דוגמא</u> כל חוג עם חילוק הינו פשוט.

<u>הוכחה</u> יהי R חוג עם חילוק. יהי I אידיאל שמאלי (בהתאמה, ימני). יהי $0\neq a\in I$. אזי קיים $b\in R$ כך ש- $ab=ba=1$. לכן $1=ba\in Ra\subseteq I$ (בהתאמה, $1=ab\in aR\subseteq I$).

לכן $I\neq(0) \Rightarrow I=R$. אז ל-R אין אידיאלים חד-צדדיים מלבד R, (0), כל שכן אידיאלים דו-צדדיים.

הגדרה יהי R חוג, $I\subseteq R$ אידיאל שמאלי/ימני.

אזי $M_n(I)=\left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in M_n(R) \;\middle|\; a_{ij}\in I \right\}$ לכל.

$M_n(I)$ הינו אידיאל שמאלי/ימני של $M_n(R)$.

לכן $I\triangleleft R$ דו-צדדי $\Longleftarrow$ $M_n(I)\triangleleft M_n(R)$ דו-צדדי!

שיעורי בית יהי $J\triangleleft M_n(R)$ אידיאל דו-צדדי.

אזי קיים $I\triangleleft R$ כך ש- $J=M_n(I)$.

מסקנה יהי R חוג עם חילוק, אזי $M_n(R)$ הינו חוג פשוט לכל n.

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

דוגמאות לחוג $\mathbb{Z}$ אין אידיאלים מינימליים.

2) יהי R חוג ארטיני שמאלי/ימני (כלומר שרשראות יורדות $I_1\supsetneq I_2\supsetneq I_3\supsetneq\ldots$ סופיות)

אזי ל-R יש אידיאלים מינימליים שמאלי/ימני.

משפט (Wedderburn) 1908 ± 5 יהי R חוג פשוט.

נניח שיש ל-R אידיאל מינימלי שמאלי או ימני. אזי קיים חוג עם חילוק D ומספר $n\in\mathbb{N}$ כך ש- $R\simeq M_n(D)$.

כדי להוכיח את זה נשתמש בטענה הבאה.

טענה (Brauer, 1942) יהי R חוג, יהי I אידיאל שמאלי מינימלי כך ש- $I^2\neq0$. אזי קיים $e\in R$ כך ש-

1) e הינו אידמפוטנט: $e^2=e$

2) $I=Re$

3) החוג eRe הינו חוג עם חילוק

מה הכוונה?

$$eRe=\{eae : a\in R\}\subseteq R$$

$$eae+ebe=e(a+b)e$$

$$eae\cdot ebe=e(aeb)e \qquad (e^2=e)$$

נשים לב כי $e = e1e \in eRe$

$$e \cdot eae = e^2ae = eae$$

$$eae \cdot e = eae^2 = eae$$

לכן e הינו יחידה כפלית של החוג eRe,

לכן eRe הינו חוג

אבל, אם I אידיאל אמיתי, אזי $e \neq 1$, לכן

החוג eRe אינו תת-חוג של R.

הוכחה הנחנו כי $I^2 \neq (0)$, לכן קיימים

$y, x \in I$ כך ש- $yx \neq 0$ $\Leftarrow$

$$Ix = \{yx : y \in I\} \neq (0).$$

מכאן ש- Ix הינו אידיאל שמאלי של R.

$x \in I$ $\Leftarrow$ $Ix \subseteq Rx \subseteq I$. לפי המינימליות של

I, מקבלים $Ix = I$. בפרט, קיים $e \in I$

כך ש- $ex = x$. בפרט,

$$e^2x = ex = x$$

$(e^2 - e)x = 0$, אך גם $e^2 - e \in I$

שים לב כי $e^2 - e \in \underbrace{I \cap Ann_R(x)}_{R \text{ אידיאל מינימלי של}} = J$.

$$Ann_R(x) = \{r \in R : rx = 0\}$$

אך $I \neq J \Leftarrow e \notin J \Leftarrow ex = x \neq 0$.

אך $J \subseteq I$, 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

$(0) \neq Re \subseteq I$ $(e \in I)$ לכן

$Re = I$ לפי המינימליות של I.