הרצאה 24

הגדרה חבורה סדורה (לצרכים שלנו)
היינו חבורה אבלית G עם סדר
מלא שמקיים $a\le b \implies a+c\le b+c$
לכל $a,b,c\in G$.

דוגמא $\mathbb{Z}$ עם הסדר הרגיל.

הגדרה יהי F שדה. הערכה (הערכה
חיבורית, הערכה של קרול) היינו
פונקציה $v: F \longrightarrow G\cup\{\infty\}$

כאשר G חבורה סדורה ו- $g<\infty$ לכל $g\in G$
כך ש- $\infty+g=\infty$ לכל $g\in G$

1) $x=0 \iff v(x)=\infty$.

2) $v(xy)=v(x)+v(y)$ לכל $x,y\in F$.

3) $v(x+y)\ge \min\{v(x),v(y)\}$

הדוגמא: $F=\mathbb{Q}$, p ראשוני. לכל $0\neq x\in\mathbb{Q}$ ניתן
לרשום $x=p^c\cdot\frac{m'}{n'}$ כאשר $p\nmid m'$
$p\nmid n'$.

נזכיר את הערכה ה-p-אדית

$$v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

$$v_p(x) = \begin{cases} c, & x \neq 0 \\ \infty, & x = 0 \end{cases}.$$

$v : F \to G \cup \{\infty\}$

$v(x) = \begin{cases} \infty, & x = 0 \\ e_G, & x \neq 0 \end{cases}$

<u>דוגמא</u>: לכל F יש הערכה טריוויאלית

<u>טענה</u>: יהי R תחום שלמות שאינו שדה ו-$F = \mathrm{Frac}\, R$ שדה השברים. התנאים הבאים שקולים:

א) לכל $x \in F$, מתקיים $x \in R$ או $x^{-1} \in R$.

($\mathbb{Z}$ לא מקיים את זה כי $\frac{2}{3}, \frac{3}{2} \in \mathbb{Q} \setminus \mathbb{Z}$).

ב) הקבוצה של האידיאלים של R מסודרת מלאה תחת הכלה. כלומר, לכל שני אידיאלים $I, J \trianglelefteq R$, מתקיים $I \subseteq J$ או $J \subseteq I$.

ג) לכל שני אידיאלים ראשיים $I, J \trianglelefteq R$ מתקיים $I \subseteq J$ או $J \subseteq I$.

ד) קיימת הערכה $v : F \to G \cup \{\infty\}$ לא טריוויאלית כך ש-:

$$R = \{x \in F : v(x) \geq e_G\}$$

<u>הגדרה</u> חוג R שמקיים אחד מן התנאים הנ"ל (ולכן את כולם) נקרא חוג הערכה.
valuation ring

<u>הערה</u> כל חוג הערכה הינו מקומי, רואים את זה מן התנאי ב) כי יש רק אידאל מקסימלי אחד.

<u>הוכחה</u> א)⇐ב) נניח כי $x\in R$ או $x^{-1}\in R$ לכל $x\in F$. יהיו $I,J\trianglelefteq R$ שני אידאלים.

אם $I\subseteq J$ אין סימני. נניח כי $I\not\subseteq J$, לכן קיים $x\in I$ כך ש- $x\notin J$, בפרט $x\neq 0$. יהי $y\in J$, צריך להוכיח כי $y\in I$. אם $y=0$ זה ברור, אז נניח $y\neq 0$. אם $\frac{x}{y}\in R$, אזי $x=\underbrace{y}_{\in J}\cdot\underbrace{\frac{x}{y}}_{\in R}\in J$ בסתירה.

להנחה. לכן $\frac{x}{y}\notin R$ ובהגדרה, לפי א),

לכן $\frac{y}{x} \in R$, ולכן $y = \underbrace{x}_{\in I} \cdot \underbrace{\frac{y}{x}}_{\in R} \in I$. הוכחנו

כי $J \subseteq I$.

ב) ⇐ ג) ברור.

ג) ⇐ א) תהי $v: F \to G \cup \{\infty\}$ הערכה.

כך ש- $R = \{x \in F : v(x) \geq e_G\}$. נשים

לב שלכל $x \in F$: $v(x) = v(x \cdot 1) = v(x) + v(1_F)$

ולכן $v(1_F) = e_G$. ברור כי $0 \in R$.

לכל $0 \neq x \in F$, $x \cdot x^{-1} = 1_F$ לכן

$$v(x) + v(x^{-1}) = v(xx^{-1}) = v(1) = e_G$$

אם $v(x), v(x^{-1}) < e_G$, אזי

$$v(x) + v(x^{-1}) < e_G + e_G = e_G$$

בסתירה. לכן $\underset{x \in R}{v(x) \geq e_G}$ או $\underset{x^{-1} \in R}{v(x^{-1}) \geq e_G}$.

$(1)\Rightarrow(2)$ נניח שלכל שני אידאלים ראשיים

$I,J \trianglelefteq R$ מתקיים $J\subseteq I$ או $I\subseteq J$

נגדיר $R^*=\{x\in R: \text{הפיך } x\}$.

זו חבורה לכפל. היא תת״ח (נורמלית)

של $F^*=F\setminus\{0\}$. יהי $G=F^*/R^*$.

נגדיר סדר על G: נגדיר כי

$xR^*\ge yR^*$ אם קיים $r\in R$ כך ש-

$xr, yr\in R$ וגם $(xr)\subseteq(yr)$.

<u>תרגיל</u> הסדר מוגדר היטב ומלא.

נגדיר הערכה:

$$v: F \longrightarrow G\cup\{\infty\}$$

$$v(x)=\begin{cases}\infty, & x=0\\ xR^*, & x\neq 0\end{cases}$$

נבדוק שזו הערכה. ההומומורפיות היא מיידית. אולם

לא ברורה היא השלישית: $v(x+y)\ge\min\{v(x),v(y)\}$.

אם $x=0$ או $y=0$ זה ברור. נניח $x,y\neq 0$.

אז, נניח בלי הגבלת הכלליות כי

$\min\{v(x),v(y)\}=v(x)$. זה אומר כי $yR^* \subseteq xR^* \Leftarrow$

קיים $r\in R$ כך ש- $xr, yr\in R$ ולכן $(yr)\subseteq(xr)$

אבל $(x+y)r = \underbrace{xr}_{\in(xr)}+\underbrace{yr}_{\in(xr)} \in (xr)$ ולכן

$$\Leftarrow ((x+y)r) \subseteq (xr)$$

$$v(x+y) \geq v(x) = \min\{v(x),v(y)\}.$$

עכשיו נגדיר סוג עוד יותר עדין של חוגי הערכה.

(בפרט, R אינו שדה)

<u>טענה</u> יהי R חוג הערכה, ויהי $F=\mathrm{Frac}\,R$ שדה השברים. התנאים הבאים שקולים:

א) R תחום ראשי.

ב) R נותרי.

לא טריוויאלית

ג) קיימת הערכה $v: F \to \mathbb{Z}\cup\{\infty\}$ כך ש- $R=\{x\in F : v(x)\geq 0\}$.

הערה הערכה כמו בתנאי ג) נקראת הערכה בדידה. חוג R שמקיים את התנאים הנ"ל נקרא חוג הערכה בדידה =

discrete valuation ring = DVR.

הוכחה א)$\Leftarrow$ב) נכון לכל תחום ראשי. (הוכחנו שכל תחום ראשי הוא נתרי).

ג)$\Leftarrow$א) יהי $I \trianglelefteq R$. אם $I=(0)$ ברור שהוא ראשי, אך נניח $I \neq (0)$.

יהי $n = \min\{v(x) : x \in I\} \geq 0$. יהי $y \in I$ כך ש- $v(y)=n$ $(y \neq 0)$. אני טוען כי $I=(y)$.

אכן, ברור כי $y \in I \Rightarrow (y) \subseteq I$.

מצד שני, לכל $x \in I$, $v\left(\frac{x}{y}\right) = v(x) - v(y) \geq 0$ $\Leftarrow$ $\frac{x}{y} \in R$ $\Leftarrow$ $x = y \cdot \frac{x}{y} \in (y)$. לכן $I=(y)$ ראשי!

<u>ב) ⇐</u> נניח כי R חוג הערכה נתרי.

יהי $v: F \to G \cup \{\infty\}$ ההערכה מן ההוכחה הקודמת, עבור החבורה הסדורה $G = F^*/R^*$ שעלולה להיות מפלצת. המטרה: להוכיח כי $v(F^*)$ היא תת-חבורה ציקלית של G.

<u>תת-טענה</u> המינימום $g=\min\left\{h\in G \;\middle|\; \begin{matrix} h\in v(F^*) \\ h>e_G \end{matrix}\right\}$ קיים. אכן, אם הוא לא קיים, אזי יש סדרה של איברים $r_1, r_2, r_3, \dots \in R$ כך ש-

$$v(r_1) > v(r_2) > v(r_3) > \dots > e_G.$$

לפי הגדרת v, נקבל שרשרת של אידאלים ראשיים $(r_1) \subsetneq (r_2) \subsetneq (r_3) \subsetneq \dots$ בסתירה לנתריות.

אז יהי $g=\min\left\{h\in G: \begin{matrix} h\in v(F^*) \\ h>e_G \end{matrix}\right\}$. ויהי $r\in R$ כך ש- $v(r)=g$.

רוצים להוכיח כי $v(F^*) = \langle g \rangle \le G$.

ברור כי $v(r^n) = g^n$ לכל $n \in \mathbb{Z}$,

<u>תרגיל</u> לבדוק כי $v(F^*)$ תת-חבורה של G.

לכן $\langle g \rangle \le v(F^*)$. מאידך, יהי $h \in v(F^*)$.

נניח בשלילה כי $h \in \langle g \rangle$. אזי

קיים $n \in \mathbb{N}$ כך ש- $g^n < h < g^{n+1}$,

אזי $e_G < hg^{-n} < g$ בסתירה למינימליות

של G. לכן, h (נחליף h ב- h^{-1} אם

צריך) מקיים $h > g^n$ לכל $n \in \mathbb{Z}$.

אזי יהי $y \in R$ כך ש- $v(y) = h$.

בפרט, $v(y) > v(r^n) \Leftarrow (y) \subseteq (r^n) \Leftarrow$

לכל $n \in \mathbb{N}$ קיים $s_n \in R$ כך ש- $y = r^n s_n$.

בפרט,

$$r^n s_n = r^{n+1} s_{n+1}$$

$$s_n = r s_{n+1}.$$

ש$v(r) < n$ $\Leftarrow$ s_n, s_{n+1} לא חברים, ונקבל

שרשרת

$$(s_1) \subsetneq (s_2) \subsetneq (s_3) \subsetneq \cdots$$

שוב בסתירה לנתריות.

הוכחנו כי $v(F^\times) = \langle g \rangle$.

ברור כי
$$\langle g \rangle \simeq \mathbb{Z}$$
$$g^n \longmapsto n$$

הינו איזו' של חבורות ששומר סדר.

אם נרכיב את v עם האיזו' הנ"ל,

נקבל $v : F \to \mathbb{Z} \cup \{\infty\}$ על.

<u>דוגמה</u> יהי R חוג הערכה בדידה.

יהי $I \trianglelefteq R$ אידיאל, $M \lhd R$

האידיאל המקסימלי. אם $I \neq (0)$, אזי

$I = M^n$ עבור $n \in \mathbb{N}$.

<u>הוכחה</u> תהי $v: F \to \mathbb{Z}\cup\{\infty\}$

הערכה על (מנורמלת) כך ש-

$R=\{x\in F : v(x)\geq 0\}$. יוצא לנו שהאידאל

המקסימלי הינו

$M=\{x\in F : v(x)>0\}=\{x\in F : v(x)\geq 1\}$.

יהי $\pi\in R$ איבר כך ש- $v(\pi)=1$.

הוא קיים כי v מנורמלת. אזי

$M=(\pi)$ לפי ההוכחה של (ב⇐א).

עכשיו יהי $I\lhd R$ אידאל כלשהו.

יהי $n=\min\{v(x) : x\in I\}$. יהי $y\in I$

כך ש- $v(y)=n$. אזי $I=(y)$ לפי

(ב⇐א). אבל $v(\pi^n)=n=v(y) \Leftarrow$

$$I=(y)=(\pi^n) \Leftarrow \frac{y}{\pi^n}\in R^* \Leftarrow v\left(\frac{y}{\pi^n}\right)=0$$

$$I=M^n \Leftarrow I=(\pi)^n \Leftarrow$$