תזכורת:

חבורה סדורה (לצרכינו) היא חבורה אבלית G עם סדר מלא שמקיים:

$a\le b \Rightarrow a+c\le b+c$ לכל $a,b,c\in G$ (למשל $\mathbb{Z}$ עם הסדר הרגיל)

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

כאשר G חבורה סדורה ($\infty>g$ לכל $g\in G$, $\infty+g=\infty$ לכל $g\in G$)

כך ש:

1) $x=0 \Leftrightarrow v(x)=\infty$

2) $v(xy)=v(x)+v(y)$ לכל $x,y\in\mathbb{F}$.

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

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

נגדיר את ההערכה ה-p-אדית $v_p:\mathbb{Q}\to\mathbb{Z}\cup\{\infty\}$, $v_p(x)=\begin{cases} c & x\ne0\\ \infty & x=0\end{cases}$

דוגמא: לכל שדה $\mathbb{F}$ יש הערכה טריוויאלית $v:\mathbb{F}\to G\cup\{\infty\}$, $v(x)=\begin{cases}\infty & x=0\\ e_G & x\ne0\end{cases}$

טענה:

יהי R תחום שלמות (שאינו שדה), $\mathbb{F}=\mathrm{Frac}\,R$ שדה השברים. התנאים הבאים שקולים:

א) לכל $x\in\mathbb{F}$, מתקיים $x\in R$ או $x^{-1}\in R$ ($\mathbb{Z}$ לא מקיים את זה $\frac{2}{3},\frac{3}{2}\in\mathbb{Q}\setminus\mathbb{Z}$)

ב) הקבוצה של האידאלים של R מסודרת מלאו תחת הכלה. כלומר, לכל שני אידאלים $I,J\trianglelefteq R$.

מתקיים $I\subseteq J$ או $J\subseteq I$.

ג) לכל שני אידאלים ראשוניים $I,J\trianglelefteq R$ מתקיים $I\subseteq J$ או $J\subseteq I$

ד) קיימת הערכה $v:\mathbb{F}\to G\cup\{\infty\}$ (לא טריוויאלית) כך ש- $R=\{x\in\mathbb{F}:v(x)\ge e_G\}$

הגדרה: חוג R שמקיים את אחד מהתנאים הנ"ל (ולכן את כולם) נקרא חוג הערכה (Valuation ring)

הערה: כל חוג הערכה הוא מקומי. ניתן לראות את זה בתנאי (ב) כי יש רק אידאל מקסימלי אחד.

הוכחה:

(א) ⇐ (ב): נניח כי $x\in R$ או $x^{-1}\in R$ לכל $x\in\mathbb{F}$. יהיו $I,J\trianglelefteq R$ שני אידיאלים.

אם $I\subseteq J$ אז סיימנו. נניח כי $I\nsubseteq J$, 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 $\frac{x}{y}\notin R$ ולכן (לפי (א)) $\frac{y}{x}\in R$, ולכן $y=\underbrace{x}_{\in I}\cdot\underbrace{\frac{y}{x}}_{\in R}\in I$.

והוכחנו כי $J\subseteq I$

(ב) ⇐ (ג): ברור

(ג) ⇐ (א): תהי $v:\mathbb{F}\to G\cup\{\infty\}$ הערכה כך ש- $R=\{x\in\mathbb{F}:v(x)\geq e_G\}$. נשים לב שלכל $x\in\mathbb{F}$,

$v(x)=v(x\cdot 1)=v(x)+v(1_F)$ ולכן $v(1_F)=e_G$. ברור כי $0\in R$. לכל $0\neq x\in\mathbb{F}$, $x\cdot x^{-1}=1_F$

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

(ג) ⇐ (ד): נניח שלכל שני אידאלים ראשיים $I,J\trianglelefteq R$ מתקיים $I\subseteq J$ או $J\subseteq I$

נגדיר $R^*=\{x\in R: x \text{ הפיך}\}$, זו חבורה לכפל. היא תת-חבורה נורמלית של

$\mathbb{F}^*=\mathbb{F}\setminus\{0\}$. תהי $G=\mathbb{F}^*/R^*$. נגדיר סדר על G: נאמר כי $xR^*\geq yR^*$ אם קיים

$r\in R$ כך ש: $xr,yr\in R$ וגם $(xr)\subseteq(yr)$.

תרגיל: הסדר מוגדר היטב ומלא

נגדיר הערכה $v:\mathbb{F}\to G\cup\{\infty\}$ $v(x)=\begin{cases}\infty & x=0\\ xR^* & x\neq 0\end{cases}$. נבדוק שזו הערכה:

האקסיומה היחידה שאינה ברורה היא: $v(x+y)\geq\min\{v(x),v(y)\}$

אכן, נניח בלי הגבלת הכלליות כי $\min\{v(x),v(y)\}=v(x)$. זה אומר כי $xR^*\leq yR^*$

קיים $r\in R$ כך ש $xr,yr\in R$ וגם $(yr)\subseteq(xr)$ אבל $(x+y)r=\underbrace{xr}_{\in(xr)}+\underbrace{yr}_{\in(xr)}\in(xr)$ ולכן

$((x+y)r)\subseteq(xr)\Rightarrow v(x+y)\geq v(x)=\min\{v(x),v(y)\}$.

נגדיר סוג עדין יותר של חוגי הערכה

טענה:

יהי R חוג הערכה (בפרט, R אינו שדה), יהי $\mathbb{F}=\mathrm{Frac}R$ שדה השברים. התנאים הבאים שקולים:

א) R תחום ראשי

ב) R נותרי

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

הגדרה: הערכה כמו בתנאי (ג) נקראות הערכה בדידה. חוג R שמקיים את התנאים הנ"ל נקרא חוג הערכה בדידה (DVR - discrete valuation ring)

הוכחה

(א)$\Rightarrow$(ב): נכון לכל תחום ראשי (הוכחנו שכל תחום ראשי הוא נותרי)

(ג)$\Rightarrow$(א): יהי $I\trianglelefteq R$. אם $I=(0)$ ברור שהוא ראשי, אז נניח $I\neq(0)$. יהי $n=\min\{v(x):x\in I\}\geq 0$

יהי $y\in I$ כך ש $v(y)=n$. נראה ש $I=(y)$. ברור כי $y\in I\Rightarrow (y)\subseteq I$.

מצד שני, לכל $x\in I$ $\quad v(\frac{x}{y})=v(x)-v(y)\geq 0 \Rightarrow \frac{x}{y}\in R \Rightarrow x=y\cdot\frac{x}{y}\in(y)$ לכן

$I=(y)$ ראשי

(ב)$\Rightarrow$(ג): נניח כי R חוג הערכה נותרי. תהי $v:\mathbb{F}\to G\cup\{\infty\}$ ההערכה מההוכחה הקודמת

עבור החבורה הסדורה $G=\mathbb{F}^*/R^*$

המטרה: להוכיח כי $v(\mathbb{F}^*)$ היא תת חבורה ציקלית של G.

תת-טענה:

המינימום $g=\min\{h\in G \mid h\in v(\mathbb{F}^*), h>e_G\}$ קיים

הוכחה:

אכן, אם הוא לא קיים, אז יש סדרה של איברים $r_1,r_2,\ldots\in R$ כך ש:

$v(r_1)>v(r_2)>\ldots>e_G$

לפי הגדרת v, נקבל שרשרת של אידיאלים ראשיים $(r_1)\subsetneq(r_2)\subsetneq\ldots$ בסתירה

לנותריות.

יהי $g=\min\{h\in G : h\in V(\mathbb{F}^*), h>e_G\}$. יהי $r\in R$ כך ש- $V(r)=g$.

רוצים להוכיח כי $V(\mathbb{F}^*)=\langle g\rangle\le G$.

תרגיל: לבדוק כי $V(F^*)$ תת חבורה של G.

ברור כי $V(r^n)=g^n$ לכל $n\in\mathbb{Z}$, לכן $\langle g\rangle\le V(F^*)$.

יהי $h\in V(F^*)$. נניח בשלילה $h\notin\langle g\rangle$. אם 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 $n\in\mathbb{Z}$. יהי $y\in R$ כך ש $V(y)=h$. בפרט, $V(y)>V(r^n)$ $\Leftarrow$ $(y)\subsetneq(r^n)$ $\Leftarrow$ לכל $n\in\mathbb{N}$ קיים $s_n\in R$ כך ש- $y=r^ns_n$. בפרט $r^ns_n=r^{n+1}s_{n+1}$ $\Leftarrow$ $s_n=rs_{n+1}$. $V(r)>e_G$ $\Leftarrow$ s_n,s_{n+1} לא חברים וקיבלנו שרשרת $\dots\subsetneq(s_2)\subsetneq(s_1)$ בסתירה לנותריות

הוכחנו כי $V(\mathbb{F}^*)=\langle g\rangle$. ברור כי $\mathbb{Z}\cong\langle g\rangle$ הוא איזו' של חבורות $n\mapsto g^n$

ששומר סדר.

אם נרכיב את V עם האיזו' הזה, נקבל $V:\mathbb{F}\to\mathbb{Z}\cup\{\infty\}$ על

תוצאה:

יהי R חוג הערכה בדידה. יהי $I\trianglelefteq R$ אידיאל, $M\trianglelefteq R$ האידיאל המקסימלי. אם $I\neq(0)$, אזי $I=M^n$ עבור $n\in\mathbb{N}$

הוכחה:

תהי $V:F\to\mathbb{Z}\cup\{\infty\}$ הערכה על (ואומרים גם מנורמלת) כך ש $R=\{x\in\mathbb{F}:V(x)\ge 0\}$.

ידוע לנו שהאידיאל המקסימלי הוא:

$$M=\{x\in F : V(x)>0\}=\{x\in F : V(x)\ge 1\}$$

יהי $\pi\in R$ איבר כך ש $V(\pi)=1$. הוא קיים כי V מנורמלת. אזי $M=(\pi)$ לפי

ההוכחה של (ג) $\Leftarrow$ (א).

יהי $I\trianglelefteq R$ אידיאל כלשהו. יהי $n=\min\{V(x):x\in I\}$. יהי $y\in I$ כך ש $V(y)=n$. אזי $I=(y)$

לפי (ג) $\Leftarrow$ (א). אבל $V(\pi^n)=n=V(y)$ $\Leftarrow$ $V(\frac{y}{\pi^n})=0$ $\Leftarrow$ $\frac{y}{\pi^n}\in R^*$ $\Leftarrow$ $I=(y)=(\pi^n)$ $\Leftarrow$

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