20/3/19

$\boxed{\text{הרצאה 4}}$

הרחבות של שדות שלמים ביחס להערכה בדידה

(K,v) - שדה עם הערכה בדידה. L/K - הרחבה סופית וספרבילית.
ניקח $\mathcal{O}=\{x\in K\mid v(x)\geq 0\}$ חוג הערכה של v, $\mathfrak{p}=\{x\in K\mid v(x)>0\}$ האידיאל המקסימלי. ניקח $\mathcal{Q}=ic_L(\mathcal{O})$. [נורמל את v כך שחבורת ההערכה $=\mathbb{Z}$]
נפרק את $\mathfrak{p}$ ב-L - $\mathfrak{p}\mathcal{O}_L=\beta_1^{e_1}\cdots\beta_g^{e_g}$
נסמן ב-ω_i את ההערכה ה-β_i-אדית. מקיים - לכל $x\in\mathcal{O}$, $\omega_i(x)=e_i\cdot v(x)$.
לכן ω_i מרחיב (הערכה שקולה) ל-v. לכן $\omega_1,\dots,\omega_g$ הערכות מעל v
(במובן שמרחיבות הערכה שקולה). לפי CRT יש $x\in\beta_i$ כך ש-$x\notin\beta_j$
הן אינן שקולות.
ההיפך גם נכון - אם ω הערכה של L שמרחיבה את v, קיים i
כך ש-$\omega=\omega_i$. נסמן - $\mathcal{O}_L\subseteq\mathcal{O}_\omega$ (אחרת הערכה לא סופית על שלמים עד מספרים עד הערכה חיובית). נסמן -
$$\mathfrak{p}_\omega=\{x\in L\mid\omega(x)>0\}$$
נסמן - $\mathfrak{P}=\mathfrak{p}_\omega\cap\mathcal{O}_L=\{x\in\mathcal{Q}\mid\omega(x)>0\}$
$\Leftarrow\mathfrak{P}$ אידיאל ראשוני של $\mathcal{Q}$, המכיל את $\mathfrak{p}$. לכן $\mathfrak{P}=\beta_i$, $\omega\equiv\omega_i$

משפט: יהי (K,v) שדה עם הערכה בדידה, $\mathcal{O}=\mathcal{O}_v$, $\mathfrak{p}=\mathfrak{p}_v$. תהא L/K
הרחבה ספרבילית סופית, $\mathcal{O}_L$ - הסגור השלם של $\mathcal{O}$ ב-L. נסמן:
$\omega_1,\dots,\omega_g$ ההערכות ה-β_i-אדיות על L, כאשר $\mathfrak{p}\mathcal{O}_L=\beta_1^{e_1}\cdots\beta_g^{e_g}$.
אלו הרחבות של v ל-L והן מהוות מערכת נציגים לכל ההרחבות
של v ל-L. יתר על כן, $\omega_i|_K=e_i\cdot v$.

מסקנה: אם K שדה מספרים, אזי $P_f(K)=\{\mathcal{Q}_\beta\}^{\text{ראשוניים}}$.

הרמת אידמפוטנטים באלגברות מעל DVR שלמים

אם A אלגברה אז $e\in A$ יקרא אידמפוטנט אם $e^2=e$.
נותן פירוקים של מודולים: אם M הוא A-מודול,
$$M=eM\oplus(1-e)M$$
[אין סכום - ברור, והחיתוך ריק כי $em_1=(1-e)m_2\Rightarrow e^2m_1=(e-e^2)m_2=0\Rightarrow em_1=e^2m_1=0$]
תהי A-אלגברה מעל DVR שלם $\mathcal{O}$. יהי π מאחד של $\mathcal{O}$. נאמר שסדרה
$\{a_n\}\subseteq A$ קושי אם $a_n-a_m\in\pi^{N(n,m)}A$, $\lim_{n,m\to\infty}N(n,m)\to\infty$. נאמר שסדרה
$a_n\xrightarrow{A}a$ אם $a_n-a\in\pi^{N(n)}A$, וגם $\lim_{n\to\infty}N(n)\to\infty$.
ונאמר ש-A שלמה אם -
1) $\bigcap_{n=1}^{\infty}\pi^nA=0$ (הטופולוגיה היא האוסדורף)
2) כל קושי (ו) מתכנסת

שימו לב: אם A היא $\mathcal{O}$-מודול נ"ס, לא ברור שצריך שלמות.

משפט: תהא A, $\mathcal{O}$-אלגברה שלמה. ($\mathcal{O}$ הוא DVR שלם עם מקסימלי π.)
לכל $e\in A/\pi A$ אידמפוטנט, קיים $E\in A$ אידמפוטנט כך ש $E\equiv e \pmod{\pi}$. יתר
על כן, אם $e_1,e_2\in A/\pi A$ אידמפוטנטים כך ש $e_1e_2=e_2e_1=0$, יש: הרמה ל-
$E_1,E_2\in A$ אידמפוטנטים כך ש $E_1E_2=E_2E_1=0$, $E_i\equiv e_i \pmod{\pi}$.

הוכחה: נעבוד - (כפל פורמלי בחוג פולינומים $\mathbb{Z}[x]$)

$$1=(x+(1-x))^{2n}=\sum_{j=0}^{2n}\binom{2n}{j}x^{2n-j}(1-x)^j$$

נסמן -

$$f_n(x)=\sum_{j=0}^{n}\binom{2n}{j}x^{2n-j}(1-x)^j\in\mathbb{Z}[x]$$

$$1-f_n(x)=\sum_{j=n+1}^{2n}\binom{2n}{j}x^{2n-j}(1-x)^j$$

ושמים,

$$f_n(x)\equiv 0 \pmod{x^n}$$

$$f_n(x)\equiv 0 \pmod{(1-x)^n}$$

לכן, $f_n^2\equiv f_n \mod x^n(1-x)^n$ (*)

מקיים: $f_{n+1}\equiv f_n \mod x^n(1-x)^n$. (**)

ניקח עכשיו $e\in A/\pi A$ אידמפוטנט, וניקח a הרמה כלשהי של e. בפרט,
$a^2-a\in\pi A$. לכן, $a^n(1-a)^n\in\pi^nA$. (נגדיר -

$$a_n=f_n(a)$$

מ-(**) נקבל ש- $a_{n+1}\equiv a_n \pmod{\pi^nA}$. לכן הגבול קיים. וכן, $a_n\equiv a_1\equiv e \pmod{\pi}$.

($f_1(x)=x^2+2x(1-x)$, $f_1(a)\equiv e^2=e \pmod{\pi}$)

ניקח:

$$E=\lim_{n\to\infty}a_n$$

$$E\equiv e \pmod{\pi}$$

וכן, $E^2\equiv E \pmod{\pi^nA}$ לכל n

$$\Downarrow$$

ברציפות - $E^2=\lim a_n^2=\lim a_n=E$

חלק השני. ניקח $e_1,e_2\in A/\pi A$ אידמפוטנטים אורתוגונליים. $\Leftarrow$ $e_1+e_2=e$ אידמפוטנט.
נרים את e, לאחר E אידמפוטנט ב-A. נשים לב ש- e_1 נרים לכלשהי לאידמפוטנט
a. כיוון ש- $ee_1e=e_1 \pmod{\pi A}$ (אורתוגונליות)
נקבל - $EaE\equiv e_1 \pmod{\pi A}$. לכן בה"כ ניתן להחליף את a

ב- EaE כדי להניח בה"כ $aE=Ea=a$. (כי אם נשנה ל- $b=EaE$
שאז E אידמפוטנט).
ניקח $E_1=\lim_{n\to\infty} e_n(a)$, אז E_1 אידמפוטנט המתאים ל- e_1, וכן $EE_1=E_1E=E_1$.
נגדיר $E_2=E-E_1$ -מש"ל. □

<u>מסקנה:</u> יהי (K,v) שדה עם הערכה שלמה, L הרחבה פרידה סופית,
O_K - חוג הערכה של v, O_L הסגור השלם של O_K ב-L.
אזי O_L חוג הערכה בדידה שלם. בפרט ל-v יש הרחבה
יחידה להערכה ω של L.

<u>הוכחה:</u> O_L מודול נ"ס מעל O_K ולכן שלם. נסמן $pO_L=\beta_1^{e_1}\cdots\beta_g^{e_g}$
ובשלילה נניח $g\geq 2$. נקבל כי -
$$O_L/pO_L = A_1\times\dots\times A_g,\quad A_i=O_L/\beta_i^{e_i}$$
נרים את האידמפוטנטים - $(1,0,\dots,0),(0,1,0,\dots,0)$ ל- $E_1,E_2\neq 0$ ב- O_L, כך
ש- $E_1E_2=0$ - סתירה. □

<u>מסקנה:</u> יהי (K,v) שדה שלם תחת הערכה בדידה, L/K פרידה.
נסמן $n=[L:K]$. ניקח ω שמרחיבה את v במובן ש- $\omega|_K=v$.
אזי, $\omega(y)=\frac{1}{n}v(N_{L/K}(y))$.

בפרט אם v מנורמל - כך ש- $v(K^*)=\mathbb{Z}$, אזי $\omega(L^*)=\frac{1}{e}\mathbb{Z}$ כאשר
$e=e(\omega|v)=e(P_\omega|P_v)$.

<u>הוכחה:</u> בה"כ נניח v מנורמלת, ויהי π מחולל, כלומר $\pi\in K$ עם
$v(\pi)=1$, ויהי $\tau\in L$ מחולל של ω. (כלומר, $\omega(\tau)=\min\{\omega(x)|\omega(x)>0\}$). אזי,
$\pi O_\omega=\tau^e O_\omega$ - e אינדקס הסיעוף
ניקח ~~$\in O_\omega$~~ $y\in L^*$. נכתוב -
$$y=\tau^r\cdot u,\quad r\in\mathbb{Z},\ u\in O_\omega^*$$
אזי,
$$Norm_{L/K}(y)=Norm_{L/K}(\tau)^r\cdot\underbrace{Norm_{L/K}(u)}_{\in O_v^*}=\dots=\pi^{fr}\cdot\alpha,\quad \alpha\in O_K^*$$
(כי $Norm_{L/K}(\tau O_\omega)=\pi^f O_v$)
לכן,
$$v(Norm_{L/K}(y))=fr$$
מצד שני,
$$\omega(\tau^r u)=r\,\omega(\tau)$$
די להראות ש- $\omega(\tau)=\frac{f}{n}=\frac{1}{e}$. ואכן $1=v(\pi)=\omega(\pi)=\omega(\tau^e)+0=e\,\omega(\tau)$ □

הלמה של הנזל

משפט: יהי $\mathcal{O}$ - DVR של k, עם שדה שאריות $\bar{k}=\mathcal{O}/\pi\mathcal{O}$ (π-מחולל). יהי $f\in\mathcal{O}[x]$ מתוקן, נסמן $\bar f\in\bar k[x]$ הפולינום שמקדמיו בלקיחת מודולו למקדמים.
נניח ש- $\bar f(x)=g_0(x)h_0(x)$, עם $g_0,h_0\in\bar k[x]$ זרים. אזי יש הרמה $g,h\in\mathcal{O}[x]$ [כלומר כך ש- $\bar g=g_0,\bar h=h_0$] עם $\deg g=\deg g_0, \deg h=\deg h_0$, וכן $f=gh$. אם g_0 מתוקן ניתן לקחת את g להיות מתוקן.

הוכחה: ניקח $A=\mathcal{O}[x]/\langle f(x)\rangle$. A נ"ס כ- $\mathcal{O}$ מודול ולכן A - שלם.

$$A/\pi A\cong \mathcal{O}/\pi\mathcal{O}[x]/\langle\bar f\rangle \cong \bar k[x]/\langle g_0h_0\rangle \cong$$

$$\underset{CRT}{\cong} \bar k[x]/\langle g_0\rangle\times\bar k[x]/\langle h_0\rangle$$

נרים את $e_1=(1,0), e_2=(0,1)$ לאידמפוטנטים G,H ב- A, כך ש- $GH=0$.

$$\Rightarrow \boxed{A=A\cdot G\times A\cdot H}$$

כך ש- $AG/\pi AG\cong\bar k[x]/\langle g_0\rangle$

$AH/\pi AH\cong\bar k[x]/\langle h_0\rangle$

נסמן - $\mathcal{X}=x+\langle f(x)\rangle\in A$, אזי,

$f(x)=char(a\mapsto xa)$

נסמן g,h הפולינומים האופייניים של הכפלה ב- $\mathcal{X}$ על המרחבים AG,AH בהתאמה. מאלגברה ליניארית, $f=gh$.
כיוון ש- g_0 - הפולינום האופייני של הכפלה ב- $\mathcal{X}$ מודולו π במרחב $AG/\pi AG$, נקבל ש- $g\equiv g_0 \pmod\pi$, עד כדי מכפלה סקלר, כלומר $g=\bar a\cdot g_0 \pmod \pi$, $\bar a\in \bar k^* \Leftarrow a\in\mathcal{O}^*$. $\deg(g)=\deg(g_0)=\dim(\dots)$. אם כך:

$$f=(ag)\cdot(a^{-1}\cdot f)$$

עם הפירוק הדרוש. אם g_0 היה מתוקן, היינו לוקחים $\bar a=1^{-1}=1$. □

מסקנה: אם ל- $f\in\mathcal{O}[x]$ יש שורש פשוט מודולו π, $\alpha\in\bar k$, אזי יש הרמה יחידה של α ל- $a\in\mathcal{O}$ כך ש- $f(a)=0$. [ניסוח שקול: $f(a)\equiv0 \bmod\pi$, $f'(a)\not\equiv 0\bmod \pi$, אזי קיים b יחיד כך ש- $a\equiv b\bmod\pi$, $f(b)=0$]

הוכחה: ניתן לכתוב $\bar f=(x-\alpha)h(x)$ כך ש- $h(\alpha)\neq0$ כי α שורש פשוט.
נרים ל- $\mathcal{O}$, נקבל $f(x)=(x-a)\tilde h(x)$ $\Leftarrow$ יש שורש, a, הרמה של α, וכן, יחידה
כי אם $b\equiv\alpha \pmod\pi$, $f(b)=0$ אז $\tilde h(b)\not\equiv_{\bmod \pi}0 \Rightarrow \tilde h(b)\neq0 \Rightarrow a=b$ □

מסקנה: $\mu_{p-1} \subseteq \mathbb{Q}_p$.

הוכחה: (נתון) על הפולינום - $f(x)=x^{p-1}-1$. ל-f יש $p-1$ שורשים פשוטים מודולו p (משפט פרמה הקטן). מהנזל הם מורמים ל-$p-1$ שורשים שונים ב-$\mathbb{Q}_p$. □

~~מיון הרחבות שלמות~~

מיון בהשלמה

משפט: יהי K שדה עם הערכה בדידה וחוג הערכה $(\mathcal{O},\mathfrak{p})$. תהי $L|K$ פרידה, $\omega_1,\dots,\omega_g$ ההרחבות של v ל-L. נסמן $(K_v,\hat{v})$, $(L_i,\hat{\omega}_i)$ ההשלמה של השדה ביחס להערכה.

1) אז, $e(\hat{\omega}_i|\hat{v})=e(\omega_i|v)$, $f(\hat{\omega}_i|\hat{v})=f(\omega_i|v)$

2) $L\otimes_K K_v=\prod_{i=1}^{g} L_{\omega_i}$

הוכחה: לכל i יש שיכון $\rho_i: K_v \hookrightarrow L_{\omega_i}$ של ההשלמה, ויש גם $\psi_i: L\to L_{\omega_i}$. כך מגדיר העתקה:

$$\varphi_i=\psi_i\otimes\rho_i : L\otimes_K K_v \longrightarrow L_{\omega_i}$$
$$\ell\otimes x \mapsto \psi_i(\ell)\rho_i(x)$$

והיא על, ~~[illegible]~~ כי $L\subseteq L_{\omega_i}$ צפוף, $L\otimes_K K_v$ שלם, לכן $\varphi_i(L\otimes K_v)$ סגורה ומכילה את L ולכן $\varphi_i(\ )=L_{\omega_i}$.

כך מגדיר -

$$\varphi: L\otimes_K K_v \longrightarrow \prod_{i=1}^{g} L_{\omega_i}$$

כך גם על: מספיק משפט השאריות הסיני: $L_{\omega_i}=\varprojlim \mathcal{O}/\mathfrak{P}_i^n$, $\mathfrak{P}_i$ הראשוני של ω_i. ולכל קירוב n-י ל-x, $a\equiv x \pmod{\mathfrak{P}_i^n}$, ויש CRT $\Leftarrow$ התמונה של L צפופה במכפלה! לפי (1) המימדים שווים ($n=\sum e_i f_i$, מעל K_v). לכן φ איזו.

(1) - צריך כי אם $x\in K_v$, יש סדרה $x_n\to x$, $x_n\in K$, $v(x_n)$ קבועה.

~~[illegible] $\omega_i(x_n)=e_i v(x_n)$~~

$$\Rightarrow \omega_i(\tau^{e_i})=\omega_i(\pi)=v_i(\pi)=1 \Rightarrow \omega_i(\tau)=1/e_i$$

לכן e_i ... [illegible] v של [illegible] ω_i

□