14/11/18

הרצאה 4

הערה: הוכחנו בעבר שאם $B \subseteq S$ הרחבה שלמה, אז ההעתקה $i^*: \operatorname{spec} S \to \operatorname{spec} B$ היא על, כלומר, לכל β ראשוני של B קיים $\mathfrak{P}$ ראשוני של S כך ש- $\mathfrak{P} \cap B = \beta$. היום נציג הוכחה נוספת ונשלים אותה.

הוכחה: יהי β ראשוני של B. נמקם את S, B בקבוצה הכפלית $B-\beta$. אז $\tilde{B} \subseteq \tilde{S}$ גם הרחבה שלמה והמיקום שומר על שוויון הראשוניים שזרים לה מול $B-\beta$. נוכל אז להניח ש- $B \subseteq S$ וכן $\tilde{B} \subseteq \tilde{S}$ כך ש- β מקסימלי. ניקח אידאל מקסימלי $\mathfrak{P}$ של S. אז $q = B \cap \mathfrak{P} \subseteq \beta$ (כי β מקסימלי מקומי), וכן, $B/q \subseteq S/\mathfrak{P}$ הרחבה שלמה. וכן, $S/\mathfrak{P}$ שדה! אם נראה ש- B/q שדה, אז q מקסימלי ולכן $q = \beta$.

ואכן, ניקח $0 \neq x \in B/q$. אז $x^{-1} \in S/\mathfrak{P}$ $\Leftarrow$ $x^{-m} = -\sum_{i=0}^{m-1} a_i x^{-i}$ עם $a_i \in B/q$. נכפול ב- x^{m-1}, ונקבל –

$$x^{-1} = -\sum_{i=0}^{m-1} a_i x^{m-1-i} \in B/q$$

כנדרש. □

בפעם הקודמת, דיברנו על העתק העקבה – $Tr_{L/k}(x) = Tr(m_x)$, $m_x : L \to L$, $y \mapsto xy$. ראינו כי אם L/k ספרבילי אז –

$$Tr_{L/k}(x) = \sum_{\substack{\sigma : L \to \bar{k} \\ \sigma|_k = id}} \sigma(x)$$

בדומה, דיברנו על העתק הנורמה והיא נתונה ע"י $Norm_{L/k}(x) = \prod_{\substack{\sigma : L \to \bar{k} \\ \sigma|_k = id}} \sigma(x)$.
ודיברנו גם על פולינום אופייני.

3.2 – פירוק (המשך)

משפט: יהי B חוג, $Q_1, \dots, Q_k$ - קבוצת אידאלים זרים בזוגות, כלומר $Q_i + Q_j = B$. אז, ההעתקה הטבעית –

$$B / \bigcap_{i=1}^{k} Q_i \longrightarrow \prod_{i=1}^{k} B/Q_i$$

המוגדרת ע"י $b + \bigcap_{i=1}^{k} Q_i \mapsto (b + Q_1, \dots, b + Q_k)$ היא איזומורפיזם.

הוכחה: בדיוק כמו משפט השאריות הסיני. □

(אבחנה)
מסקנה: $\bigcap Q_i = \prod Q_i$ אם Q_i, Q_j זרים בזוגות:

הוכחה: תמיד $\prod Q_i \subseteq \bigcap Q_i$. את ההכלה השנייה נוכיח באינדוקציה על k. נתחיל עם $k=2$. מהזרות, יש $q_i \in Q_i$ כך ש- $q_1 + q_2 = 1$. ואז, ניקח $q \in \bigcap Q_i$. נראה:

$$q = 1 \cdot q = (q_1+q_2)q = q_1 q + q_2 q \in Q_1 Q_2$$

לכן יש שוויון. באופן כללי, נסמן -

$$J = \bigcap_{i=1}^{k-1} Q_i = \prod_{i=1}^{k-1} Q_i$$

די להוכיח ש- J, Q_k זרים. ואכן,

$$B = B^{k-1} = \prod_{i=1}^{k-1} (Q_i + Q_k) \subseteq J + Q_k \subseteq B$$

ולכן,

$$J \cap Q_k = J Q_k = \prod_{i=1}^{k} Q_i \qquad \square$$

משפט השאריות הסיני למודולים: תחת התנאים והסימונים הקודמים, יהי:

M B-מודול, $I = \bigcap_{i=1}^{k} Q_i$. ההעתקה -

$$m \in M \longrightarrow (m+Q_i)_{i=1}^{k}$$

משרה איזומורפיזם -

$$M/IM \cong \bigoplus M/Q_iM$$

הוכחה: בה״כ $IM=0$ (אחרת נחליף את M ב- M/IM ואת M/Q_iM ב- $\frac{M/IM}{M/IM\, Q_i}$)

לפי משפט השאריות הסיני, יש איברים $u_1, \dots, u_k \in B$ כך ש-

$$u_i \equiv \begin{cases} 1, & i=j \\ 0, & i \neq j \end{cases} \pmod{Q_j} \quad (= \delta_{ij})$$

זה דומה לרעיון בהוכחה - פרוק יחידה

נגדיר הומומורפיזם $f_i : M \to u_i M$, $f_i(m) = u_i m$, אז -

$$\ker f_i = Q_i M$$

(אם $u_i m = 0$ אז $m = (1-u_i)m$ ואז $1-u_i \in Q_i$ ולכן $(1-u_i)m \in Q_iM$. לכן $\ker f_i \subseteq Q_iM$. עבור הכיוון השני, $u_i Q_i M \subseteq IM = 0$ ($I = \prod Q_j$) $\Leftarrow$ $Q_iM \subseteq \ker f_i$ כי)

לכן $u_iM \cong M/Q_iM$. נשאר להראות - $M=\bigoplus u_iM$.

נראה ישירות ש- $f_1+\dots+f_k : M \longrightarrow M$ היא הזהות.

ביתר פירוט -

$$1 \equiv u_1+\dots+u_k \pmod{I}$$

לכן לכל $m\in M$,

$$m = u_1m+\dots+u_km$$

וכיוון ש- $IM=0$ זו הצגה יחידה - כי אם יש פירוק נוסף,

$$m=u_1m_1+\dots+u_km_k$$

אז -

$$\cancel{u_i^2 m} = u_im = \underset{\substack{\downarrow \\ u_i^2=1 \bmod Q_i \text{ כי}}}{u_i^2 m_i = u_im_i}$$

$\square$

(וידוא - $(u_i^2-u_i)m_i = 0 \pmod{Q_i}$ וגם 0 מודולו כל ראשוני אחר.)

$\boxed{\text{3.3 - חבורות פירוק ואינרציה}}$

נקבע סימונים - יהי B תחום סגור בשלמות עם שדה מנות K.
ניקח L/K הרחבת גלואה סופית, ויהי S' הסגור השלם של B ב- L.

נשים לב, כי $\operatorname{Frac} S' = L$. אכן,

$$\begin{array}{ccc} L & \supseteq & S' \\ | & & | \\ K & \supseteq & B \end{array}$$

יהי $\alpha\in L$ ויהי $f(x)\in K[x]$ הפולינום המינימלי של α. (טווח - שוויון)

$$\alpha^n + \frac{a_1}{b_1}\alpha^{n-1}+\dots+\frac{a_n}{b_n}=0 \quad (B\ni a_i,b_i)$$

נכפיל במכנה משותף - נסמן $b_1\cdots b_n =: b$

$$b\alpha^n + a_1'\alpha^{n-1}+\dots+a_n' = 0 \;/\; b^{n-1}$$

$$(b\alpha)^n + a_1'(b\alpha)^{n-1}+\dots+b^{n-1}a_n'=0$$

ולכן $b\alpha$ שלם מעל B; לכן $b\alpha\in S' \Leftarrow \alpha\in\operatorname{Frac}(S')$.

למעשה, $\underline{b\in B}$.

ש. מה הקשר בין "הראשוניים" של B לראשוניים של S'?

לראשוני $\beta \in Spec(S)$ נסמן $p=\beta \cap B$ ראשוני של B. נסמן $S(\beta)=Frac(S/\beta)$ - שדה השארית ב-β. בדומה, נסמן -

$$k(p)=B(p)=Frac(B/p)$$

השיכון $B \hookrightarrow S$ משרה שיכון $K(\beta)\hookrightarrow L(\beta)$.

טענה: אם p מקסימלי ב-B, אז β מקסימלי ב-S.

[הראשוניים ״תלויים״ רק בשדה, לא שכן באיזו]

הוכחה: יודעים ש-S/β הרחבה שלמה של B/p. כמו כן B/p שדה. אז G יוצר ב-$Frac(S/\beta)$ הגיוני מה דורכה -

$$x=\frac{\bar{s}}{\bar{r}}$$

$$\bar{s}\in S/\beta\ ,\quad \bar{r}\in B/p \Rightarrow r^{-1}\in B/p$$

□

למה: (למה שעשינו קודם) $\beta \subseteq Q$ אידיאלים ראשוניים של S, המצומצמים מעל ראשוני β של B. אז $\beta=Q$.

תרגיל

הוכחה: נמקם ב-$B-p$, ונחליף את B ב-B_{B-p}. ואת S ב-S_{B-p}. וזה יכול להניח בה״כ ש-p מקסימלי ואז β מקסימלי $\Leftarrow Q$ מקסימלי.

עובדה נפוצה: לוקליזציה משמרת שרשרת אידיאלים סגורים ב-p

□

מסקנה: ראשוניים שונים מעל אותו ראשוני הם בלתי ניתנים להשוואה (אף אחד לא מוכל ממש בשני).

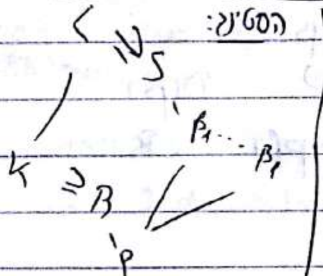
למה: (משפט השארית הסיני) יהיו $\beta_1,\dots,\beta_k\in Spec(S)$ שונים, הנמצאים מעל $p\in Spec(B)$ מקסימלי, ויהי $x_i\in S'$, $i=1,\dots,k$. אז קיים $x\in S'$ כך ש-$x=x_i \pmod{\beta_i}$ לכל i. בפרט קיים $x\in\beta_1$ אבל לא שייך ל-β_j עבור $j\neq 1$.

הוכחה: נסתכל על המכפלה ~~...~~ $U=B/p$ חיסור... נמקם ב-B/p. אז p יהיה מקסימלי; כיוון ש-$S'/_pS' \subseteq B/p$, אז יוצר ב-U ניתן לצמצם בראשוניים. נניח $x\in S_U$ כך ש-$X\equiv X_1 \pmod{\beta_1 S_U}$.

הוכחה: לפי טענה קודמת, β_i שונים ומקסימליים. לפי CRT קיים
יש כזה x.
$\square$

מעכשיו ועד ז'ימן עולם נניח כי $L(\beta)/K(p)$ ספרבילי. כי -
① זה נורמה יותר קל
② בכל השימושים זה מתקיים! למשל $B=\mathbb{Z}$, $B(p)=\mathbb{Z}/p\mathbb{Z}$.

הסטינג:



משפט: יהי $p\in \operatorname{Spec}B$ מקסימלי. אז $G=\mathrm{Gal}(L/K)$ פועל טרנזיטיבית על $\{\beta\in\operatorname{Spec}S : \beta\cap B=p\}$. דהיינו כל קבוצה סופית כי G סופי.

הוכחה: לא קשה כשלמד. יש לציין את הפעולה המוגדרת שלו ואז [illegible] ל-B. לכן זה סופי G, גם [illegible]. לכן G פועל על [illegible] B.

אין נחש - ההוכחה על כשמוני הראשוני e כיוון בשדה של השלמה

אם $\sigma\in G$, $\beta\in\operatorname{Spec}S'$, אז גם $\sigma(\beta)$ מקסימלי. (כי σ איזומורפיזם!)
וכיוון ש-$\sigma|_K=id$ $\sigma(\beta)\cap B=\sigma(\beta\cap B)=\beta\cap B=p$, $\Leftarrow$ G פועל על $\{\beta_i\}$!

מה דרוש? יותר קל
אפשר מוכן - נניח להניח בה"כ ש-p מקסימלי.
למה? שמים ב-B_p זה הופך את p למקסימלי
ועל משפט - קבוצת $\{\beta \mid \beta\cap B=p\}$ - באופן מוכן?
נניח בשלילה שהפעולה לא טרנזיטיבית. כלומר יש Q
שאינו באותו מסלול תחת פעולת G.
נסמן -

$$\Omega_1=\{\beta_1,\dots,\beta_r\}=\text{המסלול של }\beta_1\text{ תחת פעולת }G$$

אזי:

$$Q\notin\Omega_1$$

בפרט, $Q\neq\sigma(\beta)$ לכל $\sigma\in G$. ניקח $a\in Q$,
$a\notin\bigcup_{i=1}^{r}\beta_i$. נתבונן ב-

$$R\ni x=\mathrm{Norm}_{L/K}(a)=a\cdot\prod_{id\neq\sigma\in G}\sigma(a)\in Q\cap B=p$$

כלומר, $x\in\beta$.

x הוא מכפלה של איברים שאינם ב-β_1. לכן, $x\notin\beta_1\Rightarrow x\notin p$ סתירה!
$\square$

למה?
$\sigma(a)\in\beta_1\Rightarrow a\in\mathrm{Orb}(\beta_1)$
$a\in\sigma^{-1}(\beta_1)$ והוא לא שם.

הגדרה: חבורת הפירוק של β/p היא –

$$D(\beta/p) = D(\beta) = \{\sigma\in G \mid \sigma(\beta)=\beta\}$$

כלומר המייצב של β תחת הפעולה.

מסקנה: $[G:D(\beta)] = \#\{\beta \mid \beta\cap B = p\}$.

מסקנה – G פועלת על S, $D(\beta)$ מייצב את β ⇐ $D(\beta)$ פועלת על S/β, ולכן $D(\beta)$ פועלת גם על $L(\beta)$. וכרגיל – על B, ולכן על B/p ולכן על $B(p)$. ולכן על $K(p)$.

$$D(\beta) \longrightarrow Aut(L(\beta)/K(p))$$

(נסמן את התמונה של $x\in S$ ב-S/β ע"י $\bar{x}$ ואת התמונה של $\sigma\in D(\beta)$ ב-$\bar\sigma$. ואז,

$$\bar\sigma\bar x = \overline{\sigma x}$$

ולאחר מכן ב-$L(\beta)$ –

$$\bar\sigma \frac{\bar x}{\bar y} = \overline{\sigma x}\,(\overline{\sigma y})^{-1}$$

הגדרה: נגדיר $I(p) = I(\beta/p) = \{\sigma\in D(\beta) \mid \bar\sigma = 1\}$. כלומר, אלו ה-~~σ~~ $D(\beta)$ כך ש- $\sigma x - x\in\beta$. כלומר הגרעין של $D(\beta)\to Aut(L(\beta)/K(\beta))$.

הערה – אם $\sigma\in G$ כך ש- $\sigma x - x\in\beta$ לכל $x\in S$, בפרט $\sigma\beta=\beta$.

$$I(\beta) = \{\sigma\in G \mid \sigma x - x\in\beta,\ \forall x\in S\}$$

משפט: תהא ההנחה ש- $L(\beta)/K(\beta)$ פרידה, ההרחבה $L(\beta)/K(\beta)$ היא נורמלית, וההעתקה שהגדרנו משרה סדרה מדויקת קצרה.

$$1 \longrightarrow I(\beta) \longrightarrow D(\beta) \longrightarrow Gal(L(\beta)/K(\beta)) \longrightarrow 1$$

דוגמאות: נתבונן ב- $\mathbb{Z}$,

$$\mathbb{Z} — \mathbb{Z}[i]$$

$$Gal(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \quad , \quad = \langle \text{הצמדה מרוכבת} \rangle$$

נתבונן בשלושה מקרים - י' פרק - כי $L(p) = \mathbb{Z}[i]/_{1+i} = \mathbb{Z}/2\mathbb{Z}$

① $p=2$ - $2=(1+i)(1-i)$, $2=-i(1+i)^2$. $K(p) = \mathbb{Z}/2\mathbb{Z}$

לכן $Gal(L(p)/K(p)) = id$ - טריוויאלי. מה חבורת הפירוק ב-

$\mathfrak{p} = \langle 1+i \rangle = \langle 1-i \rangle$! לכן, $D(\beta) = \mathbb{Z}/2\mathbb{Z}$. ולכן $I(\beta)=D(\beta)$. מסיכום - $2\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i]$

② $p=3$ - $\mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$, $\mathbb{Z}[i]/3\mathbb{Z}[i] \cong \mathbb{F}_3[x]/_{x^2+1} = \mathbb{F}_9$.

והרחבה הגלואה - ציקלית. מכיוון $D(\beta)=\mathbb{Z}/2\mathbb{Z}$, והרחבה $I(\beta)=1$! אין מצב שהסדרה מפוצלת $\Leftarrow$ 3 ראשוני

③ $p=5$ - $\mathbb{Z}[i]/5\mathbb{Z}[i] = \mathbb{F}_5[x]/\langle x^2+1 \rangle \cong \mathbb{F}_5 \times \mathbb{F}_5 \to \mathbb{F}_5 =$ דומה

CRT $\quad \mathbb{F}_5 \cong \mathbb{F}_5[x]/_{x-2}$, $\mathbb{F}_5[x]/_{x+2}$

והם ראשוניים - $\mathfrak{P}_1, \mathfrak{P}_2 = \ker(\mathbb{Z}[i]/5\mathbb{Z}[i] \to \mathbb{F}_5)$

$$\Rightarrow \mathfrak{P}_1 = \langle 5, i-2 \rangle = \langle 1+2i \rangle$$

$$\mathfrak{P}_2 = \langle 5, i+2 \rangle = \langle 1-2i \rangle$$

$$\mathfrak{P}_1 = \mathfrak{P}_2 \Rightarrow D(\beta) = 1 \quad , \quad I(p) = 1$$

כי מוכל ב- $D(\beta)$. וזה משום ש- $5=(1+2i)(1-2i)$

~~הוכחת המשפט: נשים לב - p, כמו להניח שה- p~~

~~מקסימלי. ניקח $\bar{x} \in L(\beta) \Leftarrow$ מקיים משוואה מתוקנת,~~

~~$\bar{f}(x) = 0$~~

~~עם מקדמים ב- $K(\beta)$. נניח ש- $\bar{f}$ כמו~~

~~שורשים לא כל B. נסמן את הפולינום המינימלי~~

~~ב- f. כיוון ש- L/K נורמלית,~~

$$f = \prod (x-\alpha_i) , \alpha_i \in S$$

$$\bar{f} = \prod (x-\bar{\alpha}_i)$$

הוכחת המשפט: ניקח $\bar{x} \in L(\beta)$. ניקח $x \in S$ תמונה העתק של $\bar{x}$. $f \in B[x]$ פולינום מינימלי של x

אז צריך $\Leftarrow$ $\bar{f}$ מקיים $\bar{f}(\bar{x})=0$. צריך של p כל f

א' ערך - לכן L/K נורמלית $\Leftarrow$ $f = \prod (x-\alpha_i)$.

ולכן, $\bar{f} = \prod (x-\bar{\alpha}_i)$ מתפצל ב-$\bar{L}$. לכן, G משמר $\bar{x}$ (נובע
ב-$L(\beta)$ ולכן נקבל $L(\beta)/K(\beta)$ נורמלית.