7/11/18

הרצאה 3

תזכורת - הרחבות שלמות: יש לנו חוג B שמוכל ב-S. אמרנו ש-$s\in S$ שלם מעל B אם הוא מקיים משוואה מתוקנת $s^n+r_1s^{n-1}+\dots+r_n=0$, עם מקדמים $r_i\in B$.

תנאים שקולים -

* $B[s]$ מודול נוצר סופית מעל B
* $s\in M\subseteq S$, M B-מודול נ"ס, M חוג.
* ק"מ $B[s]$-מודול M, נ"ס כ-B-מודול, וכן $\mathrm{Ann}_{B[s]}(M)=0$.

מהתנאים השקולים נקבל -

מסקנה: יהי $B\subseteq B'$ הרחבה חח"ע, וניקח $x_1,\dots,x_n\in B'$ שלמים מעל B. אז **החוג** $B[x_1,\dots,x_n]$ הוא B-מודול נ"ס. בפרט, אם x,y שלמים אז גם $x+y$, xy.

הוכחה: באינדוקציה על n. בושר $n=1$ - זוהי הטענה הקודמת. נניח נכונות ל-$n-1$ ונסמן -

$$B''=B[x_1,\dots,x_{n-1}]$$

לפי הנחת האינדוקציה, B'' הוא B-מודול נ"ס. כמו כן, מהמשפט הקודם, $B''[x_n]$ הוא B''-מודול נ"ס.

לכן, יש יוצרים -

$y_1,\dots,y_t\in B''$ - של B'' כ-B-מודול

$z_1,\dots,z_s\in B''[x_n]$ - של $B''[x_n]$ כ-B''-מודול

לכן, הקבוצה $\{y_iz_j\}_{i=1,\dots,t}^{j=1,\dots,s}$ - היא קבוצת יוצרים ל-$B''[x_n]$ כ-B-מודול.

(ניקח $z\in B''[x_n]$ ונכתוב - $z=\sum a_jz_j$, $a_j\in B''$ ונכתוב - $a_j=\sum b_{ij}y_i$, $b_{ij}\in B$ $\Leftarrow$ $z=\sum b_{ij}y_iz_j$.) □

הערה: (חישוב לא חשוב)

כדי למצוא תלות לינארית נרצה לעשות איכשהו את היוצרים שלנו כאופרטורים לינאריים.

דוגמה - איך מוצאים תלות לינארית של x_1+x_2?

דוגמה ספציפית - $x_1=\sqrt2$, $x_1^2-2=0$ תלות שלמה ל-x_1.

$x_2=\sqrt{3}$, $x_2^2-3=0$ – תלוי שלמה ע-ו x_2.

ונחפש את התלות השלמה של $z=\sqrt{2}+\sqrt{3}$. נחשוב על

z כאופרטור לינארי על המרחב $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

בסיס למרחב – $1,\sqrt{2},\sqrt{3},\sqrt{6}$. איך פועל כל דבר על המרחב?

(לפי כפל) $\sqrt{2}: \begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ $\sqrt{3}: \begin{pmatrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

$$\Rightarrow \sqrt{2}+\sqrt{3}: \begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

$$\Rightarrow \text{char poly} = x^4-10x^2+1$$

מקיימי המילטון, $f(\sqrt{2}+\sqrt{3})=0$: תמיד יש תלות שלמה! כי עשינו את החישוב למטריצה מעל $\mathbb{Z}$-מודול. אז הדט' רמינימלי תהיה שלמה (של הפולינום האופייני) ובפרט תלות שלמה. כי הפולינום המינימלי תמיד מחלק.

דרך נוספת –

$$(z-\sqrt{2})^2-3=0$$
$$\Downarrow$$
$$z^2-2\sqrt{2}-1=0$$

בצמוד – $z^2+2\sqrt{2}-1=0$

הכפלה בינהם נותן כפולות מתוקן ה 4 שלמים ל- z ⇐ מתחלק בה מאפסים ושלם.

דרך נוספת –

$$z^0=1$$
$$z=\sqrt{2}+\sqrt{3}$$
$$z^2=5+2\sqrt{6}$$
$$\vdots$$
$$z^4=25+24+20\sqrt{6}$$
$$\Rightarrow z^4-10z^2+1=0$$

<u>הגדרה:</u> יהי $B \hookrightarrow A$ הרחבת חוגים. <u>הסגור השלם</u> של B ב-A הוא $\{s\in A \mid s \text{ שלם מעל } B\}$ – וזה חוג מהאמור לעיל. נאמר ש-B <u>סגור בשלמות ב-A</u> אם B הסגור השלם של עצמו ב-A. נאמר ש-B <u>סגור בשלמות</u> אם B סגור בשלמות ב- $\mathrm{Frac}(B)$.

טענה: אם $B \xrightarrow{\varphi} B' \xrightarrow{\varphi'} B''$ אז φ,φ' שלמים $\Leftrightarrow$ $\varphi'\circ\varphi$ שלמה.

הכיוון $\Leftarrow$ ברור. $\boxed{\text{לתזכורת}}$

הוכחה: בדומה לטיעונים שבגיאו, ניקח $b\in B''$. — יש לנו משוואה:

$$b^n + r_1' b^{n-1} + \dots + r_n' = 0 \quad , r_i' \in B'$$

ולכן,

$$\underset{\substack{B\text{-מודול נ"ס שכן}\\ r_i' \text{ הם שלמים, ומהטענה}}}{B \subseteq B[r_1',\dots,r_n']} \subseteq \underset{\substack{\text{מודול נ"ס}\\ \text{כי } b \text{ שלם}}}{B[r_1',\dots,r_n'][b]}$$

$\Rightarrow$ $B[r_1',\dots,r_n',b]$ שלם מעל B [כי B-מודול נ"ס שהוא] גם הוא) $\square$

הערה: אפשר לנסח סגירה כאן — עם פעולות אלגבר'. ולכן בעצם הכל נובע מהתנאים השקולים שניתנו שגורר שלמה.

דוגמאות לסגירות בשלמות:

① כל UFD הוא סגור בשלמות — ניקח B חוג UFD. ניקח $\frac{x}{y}\in Frac(B)$ עם $gcd(x,y)=1$. נניח -

$$\left(\frac{x}{y}\right)^n + r_1\left(\frac{x}{y}\right)^{n-1} + \dots + r_n = 0 \quad , r_i\in B$$

$$\Rightarrow x^n = \underbrace{-r_1 y x^{n-1} - \dots - r_n y^n}_{\text{מתחלק ב-}y}$$

$$\Rightarrow y \mid x^n$$

אבל y זר ל-x; לכן y יחידה $\Leftarrow$ $\frac{x}{y}\in B$.

② בפרט, כל PID הוא סגור בשלמות. בפרט, $\mathbb{Z}, k[x]$ סגורים בשלמות.

③ אי-דוגמה — $\mathbb{Z}[\sqrt5]$ לא סגור בשלמות שכן $\frac{1+\sqrt5}{2}$ שלם מעל $\mathbb{Z}$. אבל $\mathbb{Z}[\frac{\sqrt5+1}{2}]$ הסגור השלם של $\mathbb{Z}$ ב-$\mathbb{Q}(\sqrt5)$ — שכן $\mathbb{Z}[\sqrt5]\subseteq\mathbb{Z}[\frac{1+\sqrt5}{2}]$ כן סגור בשלמות. נראה כך:

נסמן ב-$\mathcal{O}$ את הסגור השלם. $\mathbb{Z}[\frac{\sqrt5+1}{2}]\subseteq\mathcal{O}$. ניקח $\frac{a}{b}+\frac{c}{d}\sqrt5\in\mathcal{O}$, $c\neq0$, $gcd(a,b)=gcd(c,d)=1$.

כיוון ש-z שלם כך גם $\bar{z}$. לכן,

כי שלם רציונלי הוא שלם!

לכן, $z+\bar{z} = \frac{2a}{b} \in \mathcal{O}\cap\mathbb{Q} = \mathbb{Z}$ - שלם

⇐ $b|2a$. אך b זר ל-a לכן $b\in\{\pm1,\pm2\}$.

מצד שני,

$z\cdot\bar{z} = \frac{a^2}{b^2} - 5\frac{c^2}{d^2} \in \mathcal{O}\cap\mathbb{Q} = \mathbb{Z}$ - שלם

לחזור לזה.

אם $b^2=1$, נקבל ש- $d=\pm1$.

אם $b^2=4$, נקבל ש- $d=\pm2$.

לכן, במקרה הראשון - $z\in\mathbb{Z}[\sqrt{5}]$

במקרה השני - (נקבל) - $z=\frac{a}{2}+\frac{c}{2}\sqrt{5}$ (כיון זוגיות ל- a,c ו- הסימן)

⇓

$(a,c\in\mathbb{Z}$ עם$)$

$\frac{2k+1}{2}+\frac{(2l+1)\sqrt{5}}{2} = k+l\sqrt{5}+\frac{1+\sqrt{5}}{2}\in\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$

[הערה: הסגור השלם סגור בשלמות - כורח ממש שלמות]

[באותו מסלול - מסיק ש- $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ הוא הסגור השלם של $\mathbb{Z}$. הסגור השלם סגור בשלמות ⇐ הוא סגור בשלמות]

טענה: יהי B תחום עם שדה מנות K. תהי L/K הרחבת שדות, ויהי $x\in L$, עם פולינום מינימלי מעל K,

$K[x]\ni f(x)=x^n+a_1x^{n-1}+\_\_\_+a_0$, $a_i\in K$

אם x שלם מעל B, אז מקדמי $f(x)\in\bar{B}[x]$, כאשר $\bar{B}$ - הסגור השלם של B ב-K. בפרט, אם B סגור בשלמות, אז $f\in B[x]$.

הוכחה: ניקח g שמאפס x, כלומר $g(x)\in B[x]$ מתוקן כך ש- $g(x)=0$. כיון ש-f מינימלי, $f|g$ ב-$K[x]$: בפרט שורשי f שלמים, ומהנוסחאות וייטה, מקדמי f שלמים!

אם B סגור בשלמות, מקדמי f הם ב-$K\cap\bar{B}=B$ כנדרש. □

משפט: תהי $B\subseteq S$ הרחבה שלמה של חוגים, כלומר כל $s\in S$ שלם מעל B. אזי ההעתקה המושרית $i^*:\operatorname{spec}S\to\operatorname{spec}B$ היא על.

לשני המשפטים, דוגמה, תשובה -

יהי B חוג סגור בשלמות, $M\subseteq B$ קבוצה כפלית. אז B_M סגור בשלמות. (הוכחה: משפט השורש הרציונלי - להשלים).
כלומר - לוקליזציות שומרות על תכונת הסגירות בשלמות.

הוכחת המשפט: מהלמה של צורן ניתן להניח בה"כ כי $S=B[b]$. [ואז להעלות את הראשוני כל פעם]
ניקח $\beta\in \operatorname{Spec}B$. נחליף את B ב- B/β כדי להניח ש- $\beta=0$ ראשוני (ואת S' ב- $S/\beta S$).
נמקם בקבוצה הכפלית $B-\beta=B\setminus\{0\}$, כדי להניח ש- β מקסימלי - כלומר B שדה. בסדר כי אם נמצא ראשוני של $S_{B-\{0\}}$ מעל 0, הוא יתאים לראשוני של S' מעל 0.
אנחנו במצב:

$b\in S'$ $\quad B$ - שדה

b - אלגברי מעל B. ניקח את f הפולינום המינימלי של b מעל B. אז:

$$B[b]\cong B[x]/\langle f(x)\rangle$$

וניקח f_0 שהוא אי פריק של $f(x)$. יש לנו העתקה:

$$B[b]\cong B[x]/\langle f(x)\rangle \xrightarrow{\varphi} \underbrace{B[x]/\langle f_0(x)\rangle}_{\text{שדה}}$$

$\ker\varphi$ - אידיאל מקסימלי, שחיתוכו עם B - חייב להיות 0. [כי הוא אידיאל של השדה]
□

הערה: התנאי שההרחבה שלמה לא ניתן לביטול: למשל, $\mathbb{Z}\to\mathbb{Q}$ הרחבה לא שלמה של חוגים, ולכן ראשוני $\neq 0$ ב- $\mathbb{Z}$ לא ניתן להרים לראשוני ב- $\mathbb{Q}$.

4. ראשוניים בהרחבות

4.1 - נורמה ועקבה

יהי E/K הרחבת שדות, ונניח שזו הרחבה סופית ממימד $[E:K]=n$.

לכל $x\in E$ נגדיר אופרטור לינארי מעל K, $m_x: E\to E$,
המוגדר ע"י $m_x(y)=xy$.
העקבה של x מוגדרת להיות -

$$T_{E/K}(x) := Tr(m_x)$$

והנורמה של x מוגדרת להיות -

$$Norm_{E/K}(x) := N_{E/K}(x) := \det(m_x)$$

כדי לקבל נוסחה - נבחר בסיס $e_1,\dots,e_n$ של E/K.
המטריצה המייצגת $M=(a_{ij})$ של m_x מוגדרת ע"י ש-

$$xe_i = \sum a_{ij} e_j$$

ואז,

$$T_{E/K}(x)=\sum a_{ii},\quad N_{E/K}(x)=\det M$$

תכונות בסיסיות של עקבה ונורמה -

יהיו $x,y\in E$ ויהי $\alpha\in K$. (אפשר לקחת ל-K...)

① תכונה - העקבה $T_{E/K}: E\to E$ היא העתקה K-לינארית.
כלומר, $T_{E/K}(\alpha x)=\alpha T_{E/K}(x)$, $T_{E/K}(x+y)=T_{E/K}(x)+T_{E/K}(y)$.

② הנורמה $N_{E/K}: E^*\to K^*$ היא הומומורפיזם של חבורות כפליות -
כלומר, מתקיים - $N_{E/K}(xy)=N_{E/K}(x)N_{E/K}(y)$, $N_{E/K}(1)=1$

③ אם $[E:K]=n$ אזי -

$$N_{E/K}(\alpha)=\alpha^n,\quad Tr_{E/K}(\alpha)=n\cdot\alpha,\quad \forall\alpha\in K$$

④ טרנזיטיביות של עקבה ונורמה - אם $K/F/E$ הרחבה שלה,

$$T_{E/K}=T_{F/K}\circ T_{E/F},\quad N_{E/K}=N_{F/K}\circ N_{E/F}$$

(יש גרסה כללית עם ח"ג שההרחבה E/K ספרבילית -
(בגרסה שלי))

①+②+③ - מיידים.

④: ניקח בסיסים $e_1,\dots,e_n$ של E/F, $f_1,\dots,f_m$ של F/K
וניקח $\{e_if_j\}$ בסיס של E/K. ניקח איבר x, ניתן לכתוב אותו
ע"י -

$$x\in E,\quad e_i x=\sum a_{ij}(x)e_j,\quad a_{ij}(x)\in F$$

$$a\in F,\quad a f_\ell = \sum_{k} b_{\ell m}(a) f_m$$

$$\Rightarrow Tr_{F/K}(Tr_{E/F}(x)) = Tr_{F/K}(\sum a_{ij}(x)) = \sum Tr_{F/K}(a_{ij}(x)) \sum_i \sum_l b_{ll}\, a_{ii}(x)$$

מתקיים:

$$x(e_i f_j) = \sum a_{ij}(x)\, e_j f_l = \circledast$$

(... – כי אלו חישובים כפליים)

$$\circledast = \sum e_j (a_{ij}(x) f_l) = \sum e_j\, b_{lm}(a_{ij}(x)) f_m \Rightarrow$$

$$\Rightarrow Tr_{E/K}(x) = \sum b_{ll}(a_{ii}(x))$$

כנדרש. $\square$

⑤: לעומת ה אלגברה לינארית, קשר עם תורת גלואה – אם E/K פרידה, ניקח L/K סגור נורמלי סופי – שמכיל את E, וניקח $G=Gal(L/K)$:

$$\begin{array}{l} L \\ \big|\ Gal(L/E) \\ E \\ \big|\ F \\ K \end{array} \quad G$$

(סמן ב- $\Sigma_{E/K} := $ "$G/Gal(L/E)$" – קבוצת נציגי קוסטים. $\Sigma_{E/K}$ – מתאים באופן טבעי לשיכונים של E בתוך L. ~~הנוסחה~~ המוכרת –

$$\boxed{\begin{aligned} T_{E/K}(x) &= \sum_{\sigma \in \Sigma_{E/K}} \sigma(x) \\ N_{E/K}(x) &= \prod_{\sigma \in \Sigma_{E/K}} \sigma(x) \end{aligned}}$$

(הוכחה – לבד)

ועל נעבור לטרנזיטיביות – ~~כל איבר ב $\Sigma_{F/K} = \Sigma$ ...~~

~~הוא הצמדה ...~~

(סוכם על נציגים, $\Sigma_{F/K}$. הם נציגי קוסטים שונים של $Gal(L/F)$. בפרט קוסטים שונים של $Gal(L/E)$.

ניתן לבחור נציגים של $\Sigma_{E/K}$ שמכילים את הנציגים שבחרנו ל- $\Sigma_{F/K}$. לכל $\tau \in \Sigma_{F/K}$, נסמן ב-

$$S_\tau = \{\sigma \in \Sigma_{F/K} : \sigma|_F = \tau|_F\}$$

לכן,

$$\Sigma_{E/K} = \biguplus_{\tau \in \Sigma_{F/K}} S_\tau$$

$$Norm_{E/K}(x) = \prod_{\sigma \in \Sigma_{E/K}} \sigma(x) = \prod_{\tau \in \Sigma_{F/K}} \prod_{\sigma \in S_\tau} \sigma(x) =$$

$$= \prod_{\tau \in \Sigma_{F/K}} \tau \Big(\underbrace{\prod_{\sigma \in S_\tau} \tau^{-1}\sigma}_{\text{פועל טריוויאלית על } F} (x) \Big) = \circledast$$

נשים לב ש- $\{\tau^{-1}\sigma \mid \sigma \in S_\tau\}$ היא קבוצת נציגים מסוג $\Sigma_{E/F}$. לכן,

$$\circledast = \prod_{\tau \in \Sigma_{F/K}} \tau(N_{E/F}(x)) = N_{F/K}(N_{E/F}(x))$$

כנדרש. □

הגדרה: נגדיר פולינום אופייני של $x \in E$ להיות הפולינום האופייני של ההעתקה m_x, כלומר הפולינום $\det(XI - m_x)$. ממשפט קיילי-המילטון, $f(x) = 0$. כמו כן, $f(0) = (-1)^n N(x)$ (כאן $[E:k]=n$) וכן המקדם ה-$n-1$ של f הוא $-T(x)$.