אלגברה מופשטת 3 - הרצאה מס' 4.

תזכורת:

$$\begin{array}{ccc} F_1 & & \\ | & \searrow & \\ F & \hookrightarrow & E \end{array}$$

$n_{F\hookrightarrow E}^{F_1}$ = מספר ההמשכות של השיכון

$F_1=F[a]$ ⇐ (נסמן) ב- f את הפול' המינימלי של a;

$n^{F_1}_{F \hookrightarrow E}$ = מספר השורשים של $\varphi(f)$ ב- F

דוגמה:

$$4\left\{\begin{array}{ccc} \mathbb{Q}[\sqrt[4]{2}] & & \\ 2| & & \\ \mathbb{Q}[\sqrt{2}] & \hookrightarrow & \mathbb{R} \\ 2| & & \| \\ \mathbb{Q} & \hookrightarrow & \mathbb{R} \end{array}\right.$$

$n_{\mathbb{Q}[\sqrt{2}]\subseteq\mathbb{R}}^{\mathbb{Q}[\sqrt[4]{2}]}=2$

$n_{\mathbb{Q}\subseteq\mathbb{R}}^{\mathbb{Q}[\sqrt{2}]}=2$

$n_{\mathbb{Q}[\sqrt{2}]\hookrightarrow\mathbb{R}}^{\mathbb{Q}[\sqrt[4]{2}]}\overset{⊛}{=}0$

$n_{\mathbb{Q}\subseteq\mathbb{R}}^{\mathbb{Q}[\sqrt[4]{2}]}=2$

⊛ לפולינום $x^2-\alpha$ → $x^2-\sqrt{2}$ ← יש לו 2 שורשים ב-$\mathbb{R}$

↘ $x^2+\sqrt{2}$ ↑ אין שורשים בכלל ב-$\mathbb{R}$

מהמשפט (משיעור שעבר) - אם $F_1=F[a_1,\dots,a_t]$ כאשר a_i שורשים של פולינום f המתפצל ב- E, ו- f ספרבילי, אז $n^{F_1}_{F\hookrightarrow E}=[F_1:F]\overset{?}{=}t$

הגדרה: יהי f פולינום מעל שדה F.

f ספרבילי אם יש לו $n=\deg f$ שורשים שונים בשדה הפיצול.

הערה: נניח $f=f_1\cdot\ldots\cdot f_k$ פירוק לגורמים אי-פריקים.

אם f ספרבילי ⇐ ה- f_i שונים וספרביליים.

אבל הכיוון ההפוך נכון, אם: $\alpha\in E$ / F אז יש ל- α פול' מינימלי מעל F, g,

⇓

f ספרבילי ⇔ ה- f_i שונים וספרביליים. ואם מתקיים $f_1(\alpha)=f_2(\alpha)=0$

אז $g\mid f_1,f_2$

$\Rightarrow g=f_1=f_2$

דוגמה: p ראשוני.

$$F = \mathbb{F}_p(t) = \left\{ \frac{a(t)}{b(t)} \,\middle|\, a,b \in \mathbb{F}_p[x] \right\}$$

נתבונן בפולינום $x^p - t$, (הוא אי-פריק מבחן אייזנשטיין מעל $\mathbb{F}_p[t]$).

(סימון) $E = F[\alpha \mid \alpha^p = t]$

נחשב מעל E: $(x-\alpha)^p = x^p - \alpha^p = x^p - t$

$x-\alpha$ אי-פריק כי הוא פול ממעלה 1.

נניח ש- $x^p - t = f(\,)g(\,)$ מעל F

$\Leftarrow$ $f(x) = (x-\alpha)^i$, $g(x) = (x-\alpha)^{p-i}$ $\Leftarrow$ $(-\alpha)^i = f(0) \in F$ $\Leftarrow$ $i=0$ או $i=p$

בשדה ממאפיין p, לכל a,b:
$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p$$

$\Leftarrow$ קיבלנו פירוק טריוויאלי.

גם כן סיבה לכך ש- $x^p - t$ אי-פריק.

השורש היחיד של (השדה הפיצול) הוא α.

בשדה ממאפיין p, אם למשהו יש שורש p אז הוא יחיד:

$a^p = b^p$

$0 = a^p - b^p = (a-b)^p$

$a-b=0 \Rightarrow a=b$

הגדרה: (נגזרת פורמלית)

אם $f = \sum a_i x^i$ אז נגדיר:

$f' = \sum i a_i x^{i-1}$.

קל להוכיח: $(f+g)' = f' + g'$

$(fg)' = fg' + f'g$.

טענה: f פול אי-פריק מעל שדה F. (נניח שבשדה הפיצול E, יש $\underset{E}{\alpha}$ כך ש-

$(x-\alpha)^2 \mid f$ (מעל E)

$\Leftarrow$ $f = (x-\alpha)^2 \cdot g(x) \in E[x]$

$f' = (x-\alpha)^2 \cdot g' + 2(x-\alpha)\cdot g = (x-\alpha)\cdot[$

בגלל ש-α הוא שורש כפול, α שורש של הפולינום של הנגזרת.

$f' \in F[x]$

אבל f אי-פריק מעל F, $\Leftarrow$ $f'(\alpha)=0$ $\Leftarrow$ $f \mid f'$ $\Leftarrow$ $f' = 0$

$\deg = n$, $\deg < n$

f הוא הפולינום המינימלי של α

07/11/13 יום ה' ד' כסלו תשע"ד

סימון: אם f אי-פריק ולא ספרבילי אז $f'=0$.

נניח $f=\sum a_i x^i$ ו- $0=f'=\sum i a_i x^{i-1}$

← לכל i, $ia_i=0$

← אם $a_i\neq 0$ אז $i=0$ בשדה

לכן $f'=0 \Leftarrow 0<p=\mathrm{char}F$

$$\Downarrow$$

$$f=\sum_{p\mid i} a_i x^i = \sum a_j x^{pj} = g(x^p)$$

כאשר $g(x)=\sum a_j x^j$

טענה: $f'=0$ (לכל פולי f) $\Leftrightarrow$ $\mathrm{char}F=p$ ו- $f=g(x^p)$ לפולינום g.

הוכחה: $\boxed{\Leftarrow}$ הוכחנו

$\boxed{\Rightarrow}$ אם $f(x)=g(x^p)$ $(*)$

$$f'(x)=g'(x^p)\cdot(px^{p-1})=0$$

מסקנה: f אי-פריק. f לא ספרבילי $\Leftrightarrow$ קיים g כך ש- $f=g(x^p)$ כאשר $p=\mathrm{char}F$.

הוכחה: $\boxed{\Leftarrow}$ הוכחנו

$\boxed{\Rightarrow}$ השורשים של f הם מהצורה $\sqrt[p]{\alpha}$ כאשר α שורש של g

לכן יש ל- f ול- g אותו מספר שורשים.

דוגמה: $F=\mathbb{F}_2(t)$

$g(t)=x^2+x+t$ (אי פריק)

$f(x)=x^4+x^2+t=g(x^2)$

$E=F[\alpha]$ שדה הפיצול של g

$2\mid$

F

$x^2-\alpha$

$E_2'=E[\sqrt{\alpha}]$ שדה הפיצול של f:

$=(x-\sqrt{\alpha})^2(x-(\sqrt{\alpha}+1))^2$

$$g(x)=(x-\alpha)(x-(\alpha+1))$$

$$\alpha^2+\alpha+t=0$$

$$\shortparallel$$

$$(\alpha+1)^2+(\alpha+1)+t$$

הגדרה: יהי F שדה ממאפיין p.

אז הפונקציה $a\mapsto a^p$, $F\to F$ מהווה שיכון.

(העתקה מחבק p שומרת על חיבור וכפל; $a^p=b^p\to a=b$

$$Im\varphi = \{a^p \mid a\in F\} = F^p$$

$$\ldots \subset F^{p^3} \subset F^{p^2} \subset F^p \underset{\neq}{\subset} F$$

לדוגמה אם $F=\mathbb{F}_p(t)$, $F^p=\mathbb{F}_p(t^p)$, ..., $F^{p^n}=\mathbb{F}_p(t^{p^n})$.

(סדרה יורדת של תת-שדות איזומורפיים)

אוטומורפיזמים

הגדרה: אוטומורפיזם של הרחבה K/F הוא איזומורפיזם של שדות, $K\xrightarrow{\sigma}K$ כך ש- $\sigma(a)=a$ לכל $a\in F$.

דוגמאות:

(1) הזהות תמיד אוטו'

(2) נתבונן בהרחבה $\mathbb{C}/\mathbb{R}$. הצמוד המרוכב מהווה אוטו'.
נמצא את כל האוטו' של ההרחבה הזו:

$$\sigma(a+bi) = \sigma(a)+\sigma(b)\sigma(i) = a+b\sigma(i)$$

σ שומרת חיבור וכפל

σ שומרת על הסקלרים מ- $\mathbb{R}$

מכיוון ש- $i^2+1=0$ נפעיל σ על שני האגפים: $\sigma(i)^2+1=0$

$\Leftarrow$ $\sigma(i)=\pm i$ (אם נשלח את i ל- i נקבל את הזהות ואם ל- $-i$ אז זה הצמוד המרוכב).

הגדרה: $Gal(K/F)=\{\sigma \mid$ σ אוטו' של ההרחבה $\}$, ביחס להרכבה.

קרי: חבורת גלואה של ההרחבה

נניח שההרכבה מהווה פעולה, כלומר שאם σ,σ' אוטו' אז גם $\sigma\circ\sigma'$ כזה.

✓ חח"ע ועל, שומרת חיבור וכפל וסקלרים

$$\sigma(\sigma'(a+b)) = \sigma(\sigma'(a)+\sigma'(b)) = \sigma(\sigma'(a))+\sigma(\sigma'(b))$$

$$\sigma(\sigma'(\alpha)) = \sigma(\alpha)=\alpha$$

נשאר להראות שאם σ אוטו' אז גם σ' אוטו'.

$$\sigma^{-1}(a+b) = \sigma^{-1}(a)+\sigma^{-1}(b)$$

$$\sigma^{-1}(ab) = \sigma^{-1}(a)\cdot\sigma^{-1}(b)$$

$$\alpha\in F \quad \sigma^{-1}(\alpha)=\alpha$$

23/11/13 כד

הכלל ד' כפלו משעה

להעשרה:

$$\mathrm{Gal}(F(t)/F) \cong PGL_2(F) = GL_2(F)/\left\{\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}\right\}$$

$$t \mapsto \frac{at+b}{ct+d}$$

$\Leftarrow$ $\mathrm{Gal}(K/F)$ חבורה.

לדוגמה, $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}_2$.

איך מגדירים אותו?

נניח $K = F[a_1, \dots, a_t]$.

(1) אם אותו σ, σ' מסכימים על כל a_i, אז הם שווים.

(2) $\sigma \in \mathrm{Gal}(K/F)$, $a \in K$.

והי f הפולינום המינימלי של a מעל F.

$$f = \sum \alpha_i x^i, \quad \alpha_i \in F$$

$$f(\sigma(a)) = \sum \alpha_i \sigma(a)^i = \sum \sigma(\alpha_i)\sigma(a^i) =$$

$$= \sum \sigma(\alpha_i a^i) = \sigma\left(\sum \alpha_i a^i\right) = \sigma(0) = 0$$

$\Leftarrow$ התמונה של איבר a תחת אוטומורפיזם σ הוא שורש של הפולינום המינימלי של a. (*)