12/6/19

הרצאה 12

משפט אי-הפריקות של הילברט

יהי $f(x,y)\in\mathbb{Q}[x,y]$ כך ש- $\deg_y f\ge 1$ וכן f אי פריק. אז:
קיימים אינסוף $a\in\mathbb{Q}$ כך ש- $f(a,y)\in\mathbb{Q}[y]$ אי פריק.

תוצאות כמותיות יותר -

* - קבוצת ה-a-ים הרעים קטנה, כלומר

$$\#\{1\le \underset{\text{שלם}}{a}\le N \mid \underset{\text{פריק}}{f(a,y)}\} \ll N^{1-\delta} \text{, באופן גס}$$

$$\ll N^{1/2}$$

$$\ll N^{1/d},\quad d<\deg_y f$$

$$\ll 1 \quad - \text{"genus}(f(x,y)=0)\ge 2\text{"}$$

* $\{1\le a\le N \mid \underset{\text{פריק}}{f(a,y)}\}$ מכילה סדרה חשבונית.

לשדה המקיים את המשפט קוראים <u>שדה הילברטי</u>: שדות מספרים ושדות פונקציות הם דוגמאות. גם $\mathbb{Q}(\zeta_n \mid n=1,2,\ldots)$.
השדה $\mathbb{Q}^{sol}=\{$מספרים עם גלואה פתיר$\}$ לא הילברטי. אם G: הרחבה סופית של
אז גם כן (Weissauer)

<u>שדות סופיים</u>: $\mathbb{F}_q$ שדה סופי ונסתכל על $\mathbb{F}_q[T]\le\mathbb{F}_q(T)$. זה אנלוגי ל-
$\mathbb{Z}\le\mathbb{Q}$ ונרצה להגדיר

$$\zeta_{\mathbb{F}_q[T]}(s)=\sum_{f \text{ מתוקן}}|f|^{-s}=\sum_{f \text{ מתוקן}}q^{-s\cdot\deg f}=(*)$$

כאשר $|f|=\#\left(\mathbb{F}_q[T]/\langle f\rangle\right)$.

$$(*)=\sum_{d=0}^{\infty}q^{-ds}\cdot q^{d}=\frac{1}{1-q^{1-s}}$$

ואז $\#\{P:\deg P=d\}=\frac{q^d}{d}+O(q^{d/2})$,

נגדיר <u>מחלק בשדה</u> של $\mathbb{F}_q(T)$ להיות הערכה בדידה (עד כדי שקילות).
<u>מחלק</u> מוכלל להיות סכום פורמלי של מחלקים בדידים מעל $\mathbb{Z}$,

$$v=\sum a_i\cdot v_i,\quad v_i-\text{מחלק},\quad a_i\in\mathbb{Z}$$

נגדיר מחלק <u>אפקטיבי</u> (אי שלילי), ונסמן $D\ge 0$, אם כל $a_i\ge 0$. נגדיר:

$$\zeta_{\mathbb{F}_q(T)}(s)=\sum_{D\ge 0}\underset{\text{אפקטיבי}}{|D|^{-s}}=\zeta_{\mathbb{F}_q[T]}(s)\cdot(1-q^{-s})^{-1}$$

כאשר $|v_i|=\#\mathcal{O}_i/v_i$, $|D|=\prod|v_i|^{a_i}$.

$$\Rightarrow \zeta_{\mathbb{F}_q(T)}(s)=\frac{1}{(1-q^{-s})(1-q^{1-s})}$$

K שדה פונקציות של משתנה אחד מעל $\mathbb{F}_q$ - הרחבה סופית של $\mathbb{F}_q(T)$.
~~כאמור~~ אם כן יש מחלקים וכו' ויש פונקציית זטא

$$\zeta_K(s) = \sum_{D \geq 0} |D|^{-s} = \prod_{v \text{ ראשוני}} (1-|v|^{-s})^{-1} = \frac{P(s)}{(1-q^{-s})(1-q^{1-s})}$$

כאן P פולינום ממעלה $(2g)$. השאלה היכן - האפסים?

ע"פ $\mathrm{Re}(s) = 1/2$, $g = \mathrm{genus}(K)$. זה אם $g=0$ ($K=\mathbb{F}_q(T)$) זה קל

$g=1$ (עקום אליפטי) הוכיח Hasse

4?

עם ?? מה השאלה דמיון-וייל הוכיח

מיוחס ל- Deligne. פא-זה? (קוהומולוגיה אטלית של ...)

ניקח עקום C מעל שדה סופי, נאמר $C = Z(f(x,y))$, $f \in \mathbb{F}_q[x,y]$.

ונסתכל על $\mathbb{F}_q$, $\mathbb{F}_{q^N}$, אפשר לחשב את

$$C(\mathbb{F}_{q^N}) = \{(a,b) \in \mathbb{F}_{q^N}^2 \mid f(a,b) = 0\}$$

נסמן $d = \deg(f(x,y))$. השערת רימן לעקומים שקולה לכך שאם C אי פריק

q, עם החסם $\#C(\mathbb{F}_q) = q + O_d(\sqrt{q})$

<u>מסקנה מהשערת רימן:</u> תהי $L/\mathbb{F}_q(T)$ הרחבה גלואה עם $d = \deg(f)$, $L \cap \bar{\mathbb{F}}_q = \mathbb{F}_q$,

נסמן $G = \mathrm{Gal}(L/\mathbb{F}_q(T))$ (ההרחבה סופית). יהי C מחלקת צמידות,

$$\#\{a \in \mathbb{F}_q \mid \left(\frac{L/\mathbb{F}_q(T)}{T-a}\right) = C\} = \frac{|C|}{|G|} q \left(1 + O_d(1/\sqrt{q})\right)$$

תזכורת <u>למשפט אי-הפריקות של הילברט:</u>

$f(x,y) \in \mathbb{Q}[x,y]$, $\deg_y(f) \geq 1$, ונניח f אי פריק ב-$\mathbb{Q}$. N - סגור גלואה

ניקח משתנה x קבוע, y כך ש- $f(x,y) = 0$

$$\mathbb{Q}(x,y) \quad | \quad \mathbb{Q}(x)$$

N סגור גלואה: שדה פיצול של $f(x,y)$ מעל $\mathbb{Q}(x)$.

ניקח יוצר של הסגור גלואה, $z \in N$, $N = \mathbb{Q}(x,z)$, ניקח g - הפולינום המינימלי של z מעל $\mathbb{Q}(x)$. מה"כ g משתנה y-z, ושורש של ... ההרחבה אותה.

להשלמה: מה ש-$\mathbb{Q}$ סגור הילברטי צריך...

אם $a \in \mathbb{Q}$ כך ש- $g(a,y)$ א"פ אז גם $f(a,y)$ א"פ.

כי $g(a,y)$ אי פריק $\Rightarrow$ דרגה החלוקה ב-N ולכן ב-$\mathbb{Q}(x,y)$.

משפיטרין קיום $f(a,y)$ א"פ.

ה"כ $f = ...$ כלומר נשים לב ש... מאפשר

$$\begin{tikzcd} N \arrow[r, dash] \arrow[d, dash] & N\bar{\mathbb{Q}} \arrow[d, dash] \\ \mathbb{Q}(x) \arrow[d, dash] & \bar{\mathbb{Q}}(x) \arrow[d, dash] \\ \mathbb{Q} \arrow[r, dash] & \bar{\mathbb{Q}} \end{tikzcd}$$

נשים לב שאיזון ש- $N\cap\bar{\mathbb{Q}}=\mathbb{Q}$, כי מוגדרים לינארית. לכן,

$$[N\bar{\mathbb{Q}} : \bar{\mathbb{Q}}(x)] = [N:\mathbb{Q}(x)] = \deg_y f$$

$\Rightarrow f\in\bar{\mathbb{Q}}[x,y]$ א' פריק מעל $\bar{\mathbb{Q}}$.

<u>משפט:</u> (קרונקר)

$f\in\mathbb{Z}[x,y]$ כך ש- f א' פריק ב- $\bar{\mathbb{Q}}[x,y]$ אזי לכל p פרט למספר סופי, $f_{\bmod p}$ ב- $\mathbb{F}_p[x,y]$ א"פ מעל $\bar{\mathbb{F}}_p$.

<u>משפט:</u> (ז'ורדן)

נניח $G=\bigcup_{\sigma\in G} H^\sigma$ כאשר $H\le G$. אז $H=G$. (G,H סופיות)

(במילים אחרות: אם $H\cap C\neq\emptyset$ לכל מחלקת צמידות C אז $H=G$)

<u>הוכחה:</u> יש לקחת $[G:N_G(H)]$ איברים σ. אבל -

$[G:H] \geq [G:N_G(H)]$

לכן אם $H\neq G$ ונחשב אז ש-

$|G| \le \frac{|G|}{|H|}\cdot|H| - 1 = |G|-1$ - סתירה ∎

$G\ni C$ לכל

~~הוכחת טענה:~~

נניח שעבור $a\in\mathbb{Z}$ הנ"ל תנאי $\sqrt{}$ (נגזר אחרת) על a כך ש
שמקבלת הפירוק ב- $x=a$ תואם את C. התנאים יהיו שמספר
סופי של p שונים ולבחור a שיכיל את כולם. ואז $D_a=G$
לפי צ'בוטרב, וכך $f(a,Y)$ יהיה א"פ (כי G_a ה-a יהיו לא טרנזיטיבי)
ניקח C מחלקת צמידות. נבחר ראשוני $p=p_C$ מספיק גדול
כך ש-

1) $f \bmod p =: f_p\in\mathbb{F}_p[x,y]$ א' פריק מעל $\bar{\mathbb{F}}_p$.

2) גם $p-c_g\sqrt{p}>0$ (g הקבוע מהמשפט רימן)

נבחר את הראשוני p שיהיו שונים לכל C.

$$\begin{tikzcd} N_p \arrow[r, dash] \arrow[d, dash, "G"'] & N_p\bar{\mathbb{F}}_p \arrow[d, dash] \\ \mathbb{F}_p(x) \arrow[d, dash] & \bar{\mathbb{F}}_p(x) \arrow[d, dash] \\ \mathbb{F}_p \arrow[r, dash] & \bar{\mathbb{F}}_p \end{tikzcd}$$

N_p - שדה הפיצול של $f_p(x,y)$ מעל $\mathbb{F}_p(x)$.

נזכיר ש-

$$[N_p:\mathbb{F}_p(x)] = [N:\mathbb{Q}(x)] = \deg_y f$$

מצד שני,

$$G = |Gal(N_p/\mathbb{F}_p(x))| = |D/I| \le G$$

$\Rightarrow |D|=|G|$, $|I|=1$, $D=G$.

משפט צ'בוטרב:

$$\#\{a_p\in\mathbb{F}_p \mid \left(\frac{N_p/\mathbb{F}_p(x)}{x-a_p}\right)=C\} \ge p-g\sqrt{p} > 0 \quad \text{כי}$$

$\Leftarrow$ יש $a_p\in\mathbb{F}_p$ כך ש- $\left(\frac{N_p/\mathbb{F}_p(x)}{x-a_p}\right)=C$

עבור כל $a\in\mathbb{Z}$ שמקיים $a\equiv a \pmod p$, נקח

$\bar N|\mathbb{Q}$ זהו שדה הפיצול של $f(a,y)$ מעל $\mathbb{Q}$,

ונקח מודולו p.

$$D_a - \begin{array}{c}\bar N\\ |\\ \mathbb{Q}\end{array} \qquad D_{a,p}\cong D_{a_p}$$

לכן $D_a\cap C\neq\emptyset$ כי $D_{a,p}\cap C\neq\emptyset$.

לכן אם נקח את הקבוצה החשבונית

$\{a \mid \forall C\in G \mid a\equiv a_{p_C} \pmod{p_C}\}$

ע"פ ג', בצירוף משפט דירכלה. $\square$

הערה 1: אם $N\cap\bar{\mathbb{Q}}=E$,

$$\begin{array}{ccc} & & N \\ & & |\ G_0 \\ \mathbb{Q}(x) & - & E(x) \\ | & & | \\ \mathbb{Q} & - & E \end{array}$$

הדיון הפולינומי עושים אותו דבר - f הוא פולינום של N מעל $E(x)$.

עם: $p=p_C$ שמתפצל לגמרי ב-E.

אז מודולו p היינו מקבלים:

$$\begin{array}{c} \text{אותו דבר} \\ | \\ \mathbb{F}_p - \bar E_p=\mathbb{F}_p \end{array}$$

הערה 2: התכונה עובדת גם לשדה מספרים.

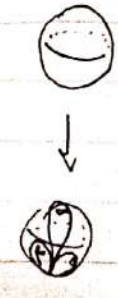
הערה 3: $K=K_0(x)$ הילברטי. K_0 סופי - אותה הוכחה. אם K_0 לשדה - ...

$\boxed{\text{שימושים לחבר גלואה}}$

התשובה בפולינום $N - \mathbb{Q}[x,y]\ni f = y^n - y^{n-1} - x$

התשובה של f היא ...

$$\begin{array}{ccc} \mathbb{Q}(y) & - & \mathbb{C}(y) \\ | & & | \\ \mathbb{Q}(x) & - & \mathbb{C} \end{array}$$



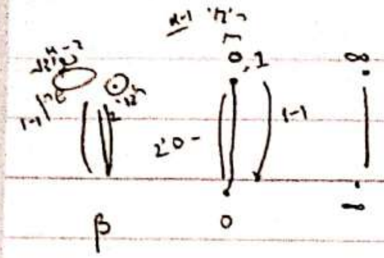
$y\mapsto -y^n,\ y^{n-1}$

$\mathbb{C}[y]\cup\mathbb{C}[y^{-1}]$

$\downarrow$

$\mathbb{C}[x]\cup\mathbb{C}[x^{-1}]$ ...

נבחר α כך ש- נוגע עם הציר האופקי.



$$0 = (y^n - y^{n-1})' = ny^{n-1} - (n-1)y^{n-2}$$
$$\Rightarrow y = 0,\ \frac{n-1}{n} = \alpha$$

מעל $x = 0$: $f(y,0) = y^{n-1}(y-1)$.

מעל $x = \beta = \alpha^n - \alpha^{n-1}$:

$$y^n - y^{n-1} = x = \alpha^n - \alpha^{n-1}$$
$$f(y,\beta) = (y-\alpha)^2 \cdot (y-\alpha_1)\cdots(y-\alpha_{n-2}) \qquad \alpha_i \neq \alpha_j$$

לכן

$$\begin{cases} I_\infty = \langle n\text{-cycle} \rangle \\ I_0 = \langle n-1 \text{ cycle} \rangle \\ I_\beta = \langle 2\text{-cycle} \rangle \end{cases} \Rightarrow Gal\left(f(x,y)/\mathbb{C}(x)\right) = S_n$$

$$\Downarrow$$

(כי השדות של [illegible]) $Gal\left(f(x,y)/\mathbb{Q}(x)\right) = S_n$

$$\Downarrow$$

$$Gal\left(y^n - y^{n-1} - a / \mathbb{Q}\right) = S_n$$

ה כללי:

כאשר $G \leq G$ n (דרגת המעבר [illegible])

$$\begin{array}{ccc} & N & \\ S_n & | & \diagdown^{A_n} \\ & & E = \mathbb{C}(z) \\ & & \diagup \\ & \mathbb{C}(x) & \end{array}$$

$0, \beta, \infty$

מעל ∞ [illegible] 2 - ו

ומסועפים $N/E - 2$

β – מסועף

o_1, o_2 מסועפים

יש סיעוף ב- o_1, o_2 – ~~[illegible]~~ – ∞_1, ∞_2

הגודל סיעוף –

$[\frac{n}{2}, \frac{n}{2}]$ $[\frac{n}{2}, \frac{n}{2}]$

$[n-1]$ $[n-1]$

יש לנו נוסחה רמן הורביץ [illegible].

$$g_E = 0 \Leftarrow 2g_E - 2 = 2(2 - 2g_{\mathbb{C}(x)}) + \Sigma(\deg p^e - 1)$$

$\Leftarrow E \cong \mathbb{C}(z)$.

$\Leftarrow$ לא נקח פולינום א' פריק $f(z,y)$ ו- N מעל E הוא יהיה עם חבורת גלואה A_n.

7.7 – משפט 38 של Galois