12/6/19 $\boxed{\text{הרצאה 12}}$

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 דלילה, כלומר

$$\#\{1\le \underset{\text{שלמים}}{a}\le N \mid \underset{\text{פריק}}{f(a,y)}\}\ll N^{1-\delta}\text{, משנות ה-50}$$
$$\ll N^{1/2}$$
$$\ll N^{1/d},\quad d<\deg_y f$$
$$\ll 1 \quad - \text{"genus}(f(x,y)=0)\ge 2\text{"}$$

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

לשדה המקיים את המשפט קוראים שדה הילברטי: שדה מספרים ושדה פונקציות הם דוגמאות. גם $\mathbb{Q}(\zeta_n \mid n=1,2,\dots)$.
השדה $\mathbb{Q}^{\text{sol}}=\{\text{מספרים עם נוסחה סגורה}\}$ לא הילברטי. אם G הרחבה סופית של ... אז כן (Weissauer)

שדות פונקציות: $\mathbb{F}_q$ שדה סופי ונסתכל על $\mathbb{F}_q[T]\subseteq\mathbb{F}_q(T)$. זה נעשה אנלוגיה של $\mathbb{Z}\subseteq\mathbb{Q}$ ואז נגדיר

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

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 מחלק בשדה של $\mathbb{F}_q(T)$ להיות הערכה בדידה (עד כדי שקילות).
מחלק מוכלל להיות סכום פורמלי של מחלקים ראשוניים מעל $\mathbb{Z}$,

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

נגדיר מחלק אפקטיבי (אי שלילי), ומסמנים $v\ge 0$, אם $a_i\ge 0$ לכל i. נגדיר:

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

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 $\mathbb{F}_q(T)$.
~~כעת~~ גם כאן יש מחלקים וכו' ויש פונקצית זטא

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

כאן P פולינום ממעלה $(2g)$. השערת רימן - האפסים

על $Re(s) = 1/2$, $g = genus(K)$. אם $g=0$ למשל $K=\mathbb{F}_q(T)$ אין אפסים כלל

$g=1$ (עקום אליפטי) הוכיח Hasse

4? עבור g כללי הוכיח השערת רימן-וייל

מימד כללי - Deligne. (קוהומולוגיה אטלית)

ניקח עקום C שאינו סגור, למשל $C=Z(f(x,y))$, $f\in \mathbb{F}_q[x,y]$.

ונביט בנקודות של C ב- $\mathbb{F}_q$, $\mathbb{F}_{q^n}$

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

נסמן $d = \deg(f(x,y))$. השערת רימן גוררת שעבור C כזה

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

$d = tot\deg(f)$, L אי פריק

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

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

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

חזרה <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 קטן, y קבוע ש-

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

$f(x,y)=0$

$\mathbb{Q}(x)$

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 מעל $z-y$, ושורש של יוצר הרחבה אחרת.

ומשפט - יש ש- $\mathbb{Q}$ סגור ... אינסוף a.

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

כי $g(a,y)$ אי פריק $\Leftarrow$ ... יוצר הרחבה ל- N ולכן ל- $\mathbb{Q}(x,y)$.

משפט ... $f(a,y)$ אי"פ.

מספיק ... $f=$ ... ...

נשים לב שאיזון ש- $N\cap\bar{\mathbb{Q}}=\mathbb{Q}$, (כי מופרדים ליניארית) לכן,

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

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

$\Leftarrow f\in\bar{\mathbb{Q}}[x,y]$ אי פריק מעל $\bar{\mathbb{Q}}$.

<u>משפט:</u> (קרסטן)

$f\in\mathbb{Z}[x,y]$ כך ש- f אי 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 לא ש- $H=G$ ונקבל אז ש-

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

לכל $G_a\in C$

~~הוכחה שנייה:~~

לכסין נבחר $a\in\mathbb{Z}$ היטב תנאי $\sqrt{}$ (נגדיר אחר) על a כך שמחלקות הפיצול ב- $x-a$ תהיינה את C. התנאים יהיו שעבור לכל $\wp$ שעולה למעלה a שייכים את כולם. ואז $D_a=G$ לפי צ'בוטרב, ורק $f(a,y)$ יהיה א"פ (כי G ה- a יהיו לא מסועפים)

ניקח C מחלקת צמידות. נבחר ראשוני $p=p_C$ מספיק גדול כך ש-

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

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

נבחר את הראשוני $\wp$ שמעליו שייך ל- C.

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

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

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

מצד שני,

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

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

ממשפט צ'בוטרב:

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

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

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

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

ונקח מודולו p.

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

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

לכן אם ניקח את הקבוצה החיתוכית

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

סה"כ, בעזרת משפט הסיני. $\square$

<u>הערה 1:</u> אם $N\cap\bar{Q}=E$,

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

היינו הפולינום עושים אותו אפשר לפרק ל-f מעל $E(x)$.

עם: 1

1) $p=p_C$ שמפצל לגמרי בשדה E.

ואז מודולו p היינו שגליל:

$$\begin{array}{c} \\ | \\ \mathbb{F}_p - \bar{E}_p=\mathbb{F}_p \end{array}$$

<u>הערה 2:</u> התוספת עובדת לכל שדה מספרים.

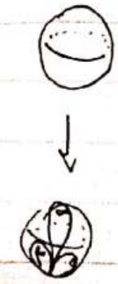
<u>הערה 3:</u> $K=K_0(x)$ הילברטי. K_0 סופי - אלגברי. אם K_0 לשלוט - הילברטי.

$\boxed{\text{שימושים לתורת גלואה}}$

התמונה הפולינום $f=y^n-y^{n-1}-t$

$$\begin{array}{ccc} N & - & \mathbb{Q}[x,y]\ni f \\ | & & \\ Q(y) & - & \mathbb{C}(y) \\ | & & | \\ Q(x) & - & \mathbb{C} \end{array}$$

חבורת גלואה של f



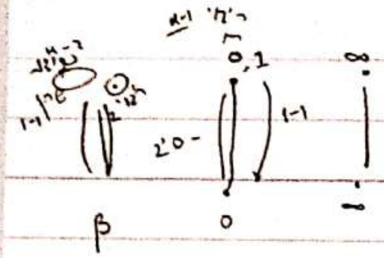
$y\mapsto -y^n,\ y^{n-1}$

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

$\downarrow$

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

נבחר פולי' נוסף עם הגלואה הנשמרת.



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

$f(y,0)=y^{n-1}(y-1)$. מעל $\underline{x=0}$

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

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

אז

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

$\Downarrow$

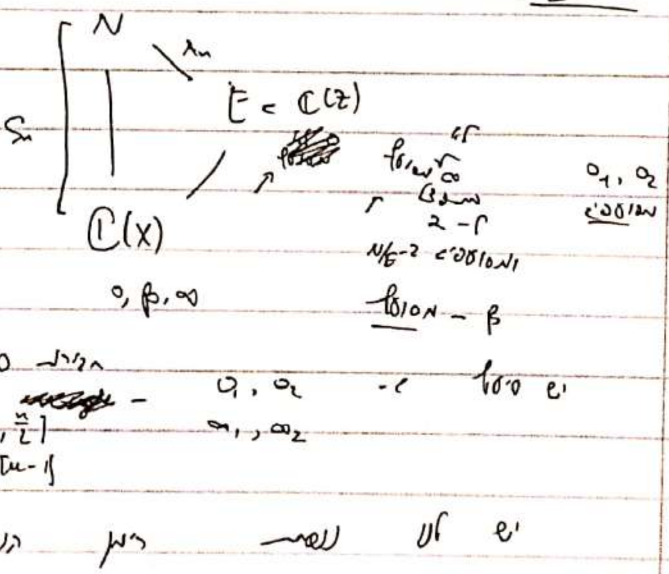
(כי תמורות פ"ג נקבעות מנוסחה) $Gal\left(f(x,y)/\mathbb{Q}(x)\right)=S_n$

$\Downarrow$

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

כמו G על n (דוגמה המשפט סופי הפרק פי הילברט)

ה בלגן:



$0,\beta,\infty$

יש סוף ב- $0_1, 0_2$ ~~[illegible]~~ - הגדרת סוף -

∞_1,∞_2

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

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

יש לנו נשאר רק השבירה לבנות.

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

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

$\Leftarrow$ אם נעה פולינום $f(z,y)$ ה- N מעל E הוא יהיה עם חבורת גלואה A_n.

7.7 – משפט מעל שדה סופי