הרצאה 11

5/6/19

תזכורת: L/K גלואה עם חבורת גלואה G, $C \subseteq G$ מחלקת צמידות.

מניחים שאם L/K ציקלוטומית, אז

$$\circledast \quad \#\{\mathfrak{p} \in \mathcal{P}(K) \mid N\mathfrak{p} \le x,\ (\tfrac{L/K}{\mathfrak{p}}) = C\} \underset{x\to\infty}{\sim} \frac{|C|}{|G|} \cdot \frac{x}{\log x}$$

מטרה: להוכיח ל-G כלשהי. (L/K לאו דווקא ציקלוטומית) ראינו

← (נובע מכך שיש f — [illegible] בדיוק [illegible] ראשוניים מעל $\mathfrak{p}$)

$$\#\{\mathfrak{p} \mid (\tfrac{L/K}{\mathfrak{p}}) = C,\ N\mathfrak{p} \le x\} = \frac{f}{|G|} \cdot |C| \cdot \#\{\mathfrak{P} \in \mathcal{P}(L) \mid N\mathfrak{P} \le x^f,\ (\tfrac{L/K}{\mathfrak{P}}) = \sigma\}$$

כאשר $\sigma \in C$, $f = \mathrm{ord}(\sigma)$. לכן, $\circledast \iff \#\{\mathfrak{P} \in \mathcal{P}(L) \mid N\mathfrak{P} \le Y,\ (\tfrac{L/K}{\mathfrak{P}}) = \sigma\} \underset{Y\to\infty}{\sim} \frac{Y^{1/f}}{\log Y}$.

אמרנו שדי להוכיח

$$\#\{\mathfrak{P} \in \mathcal{P}(L) \mid N\mathfrak{P} \le Y,\ (\tfrac{L/K}{\mathfrak{P}}) = \sigma\} \ge \frac{Y^{1/f}}{\log Y}(1 + o(1))$$

[illegible]

נבחר שלם ראשוני ℓ, ו-η כך ש- $\mathrm{ord}(\eta) = \ell$ כאשר:

(1) $f = \mathrm{ord}(\sigma) \mid \ell - 1$

(2) $\ell \nmid \mathrm{disc}(L/\mathbb{Q}) \Leftarrow$ מטעמי מספור, $L \cap \mathbb{Q}(\eta) = \mathbb{Q}$.

$$\begin{array}{ccc}
L & \xrightarrow{\ \mathbb{Z}/(\ell-1)\mathbb{Z}\ } & L(\eta) = N \\
 & & | \\
\sigma \in G \ | & D := L(\eta)^{\Delta},\ \Delta = \langle\sigma,\tau\rangle & \\
 & & | \\
k & \xrightarrow{\ \mathbb{Z}/(\ell-1)\mathbb{Z}\ } & K(\eta) \\
| & & | \\
\mathbb{Q} & \text{———} & \mathbb{Q}(\eta)
\end{array}$$

נבחר $\tau \in \mathbb{Z}/(\ell-1)\mathbb{Z} \cong (\mathbb{Z}/\ell\mathbb{Z})^* \cong \mathrm{Gal}(L(\eta)/L)$, כך ש- $f \mid t := \mathrm{ord}(\tau)$. נסמן

$$\Delta = \langle(\sigma,\tau)\rangle = \langle\rho\rangle \quad (\rho := (\sigma,\tau))$$

נסמן ב- D שדה השבת - $D = L(\eta)^{\Delta}$.

נשים לב ש- $\Delta \cap G\times\{1\} = 1$

$\Leftarrow \langle(\sigma^i,\tau^i)\rangle \ni \dots \Leftarrow \tau^i = 1,\ f \mid \mathrm{ord}(\tau) \mid i \Leftarrow \sigma^i = 1$

מכאן,

$$D \cdot K(\eta) = N$$

לכן, N/D - ציקלוטומית (נוצרת ע"י שורש היחידה η).

כמו כן: $\Delta \cap (\{1\} \times \mathbb{Z}/(\ell-1)\mathbb{Z}) = \langle\rho^f\rangle = \langle(1,\tau^f)\rangle \cong \mathbb{Z}/(\tfrac{t}{f})\mathbb{Z}$ - כי f הוא הסדר של σ.

נסמן $\frac{t}{f} = f'$.

נסמן

$$\Omega_{N,\tau} = \{\mathfrak{P} \in \mathcal{P}(N) \mid (\tfrac{N/K}{\mathfrak{P}}) = \rho\}$$

מכיוון ש- N/D ציקלוטומית,

$$\#\{\mathfrak{P}\in\mathcal{P}(N) \mid \underset{N\mathfrak{P}\le Y}{\left(\tfrac{N/D}{\mathfrak{P}}\right)=\rho}\} \overset{*}{\sim} \frac{Y^{1/t}}{\log Y}$$

לכל $\mathfrak{P}\in\mathcal{P}(N)$ שאינו מסועף מעל K מקיים

[נובע ממטופקטוריאליות סמל הסוחק]

$$\left(\tfrac{N/K}{\mathfrak{P}}\right)=\rho \iff \left(\tfrac{N/D}{\mathfrak{P}}\right)=\rho,\ f(\mathfrak{P}_D/\mathfrak{P}_K)=1$$ אם״ם

$\mathfrak{P}_K=\mathfrak{P}\cap K,\ \mathfrak{P}_D=\mathfrak{P}\cap D$. כאן

לכן:

$$\#\{\mathfrak{P}\in\mathcal{P}(N) \mid N\mathfrak{P}\le Y,\ \left(\tfrac{N/K}{\mathfrak{P}}\right)=\rho\} = O(1)+\frac{Y^{1/t}}{\log Y}+$$

למה מסופק שאנו עושים פה? לא הבנתי?

הרחבה — המוספים בהרחבה מעל ℓ-ב — חסום ״ונפוחו״

צריך לספור רק פעם אחד! (לבדוק) (כי ה במובן L/K שונה פה)

$$=\#\{\mathfrak{P}\in\mathcal{P}(N) \mid \underset{f(\mathfrak{P}_D/\mathfrak{P}_K)=1}{\underset{\left(\tfrac{N/D}{\mathfrak{P}}\right)=\rho}{N\mathfrak{P}\le Y}}\}=$$

השגיאה של * כמו שם שופכי

$$= O(1)+\frac{Y^{1/t}}{\log Y}+O(Y^{1/2t}) \underset{Y\to\infty}{\sim} \frac{Y^{1/t}}{\log Y}$$

עכשיו ניתן לחסום את σ-

$$\#\{\mathfrak{P}\in\mathcal{P}(L) \mid \left(\tfrac{L/K}{\mathfrak{P}}\right)=\sigma\} =: \Omega_L$$

ע״י נוסחה הסומה.

יהי $\mathfrak{P}\in N_{N,\tau}$ נקח

עבור $\tau\in\mathbb{Z}/(\ell-1)\mathbb{Z}$ ונשים ש... ב-L, אז החבורה הפירוק של הבשוני מעל L היא

$$\mathbb{Z}/f'\mathbb{Z}\cong\langle 1,\tau^f\rangle=\Delta\cap Gal(N/L)$$

ולכן,

$$N P_L^{f'}=N\mathfrak{P}$$

לכן.

$$N\mathfrak{P}\le Z^{f'}\iff N\mathfrak{P}_L\le Z$$

יתר על כן,

$$\left(\tfrac{L/K}{\mathfrak{P}_L}\right)=res_L\left(\tfrac{N/K}{\mathfrak{P}}\right)=\sigma$$

בגלל k של קונגרואנציה הבשוני

ההרחבה לא חסומה לנו לחשב במדויק כמה ראשונים יש מעל Δ - $\mathfrak{P}_L$ ~~...~~ לכל היותר

$$\frac{\ell-1}{f'}=\frac{(\ell-1)f}{t}$$ ראשונים מעל $\Omega_{N,\tau}$ ->

ולכן אם כמו כן ...

$$\#\{P\in\Omega_L \mid p=\mathfrak{P}_L,\ \mathfrak{P}_L\in\Omega_{N,\tau}\}\ge$$

$$\ge\frac{t}{(\ell-1)f}\cdot\frac{Z^{f'/t}}{\log Z^{f'}(1+o(1))}=\frac{Z^{1/f}}{\log Z}\cdot\frac{t}{(\ell-1)f}\cdot\frac{1}{f'(1+o(1))}=$$

$$=\frac{Z^{1/f}}{\log Z}\cdot\frac{1}{\ell-1}(1+o(1))$$

תזכורת:

$$\cancel{\#\{P\in \mathbb{Z}(\zeta) \mid N_P \le Z, \ldots\}}$$

$$\#\{P\in\Omega_{N,\tau} \mid N_P \le Y\} \sim \frac{Y^{1/\mathrm{ord}(\tau)}}{\log Y}$$

שים תרגילים ל-Ω_l -

$$\frac{1}{l-1}\cdot\frac{Z^{1/f}}{\log Z} \sim \#\{P\in\Omega_l \mid P = P_N,\ N_P \le Z\}$$

אם $\tau_1 \neq \tau_2 \in \mathbb{Z}/(l-1)\mathbb{Z}$, $f \mid \mathrm{ord}\,\tau_i$, $i=1,2$ - אז

$$\Omega_{N,\tau_1} \cap \Omega_{N,\tau_2} = \emptyset$$

(זה ברור כי ההתאמה משאירה לפולינום מ"מ)

לכן,

$$\#\{P\in\Omega_l \mid N_P \le Z\} \underset{\Downarrow}{\gtrsim} \#\left\{\frac{\tau\in\mathbb{Z}/(l-1)\mathbb{Z}}{f\mid\mathrm{ord}\,\tau}\right\}\cdot\frac{Z^{1/f}}{\log Z}$$

$$f \gtrsim g \Leftrightarrow f \ge g(1+o(1))$$

דוגמאות: ניקח $f=2$.

$$l-1 = 2\cdot k, \quad k \text{ אי-זוגי}$$

$$\#\{2 \mid \mathrm{ord}\,\tau\} = \cancel{\ldots} = \#\{1\le\tau\le 2k \mid \tau \text{ אי-זוגי}\} = \frac{2k}{2} = k$$

$$i\in\mathbb{Z}/n\mathbb{Z},\quad \mathrm{ord}_n(i) = \frac{n}{\gcd(i,n)}$$

$$\Downarrow$$

$$l-1 = 2^{\alpha}\cdot k, \quad k \text{ אי-זוגי}$$

$$\frac{\#\{i\in\mathbb{Z}/2^{\alpha}\mathbb{Z} \mid \text{סדר זוגי}\}}{2^{\alpha}} = 1-\frac{1}{2^{\alpha}} \xrightarrow[\alpha\to\infty]{} 1$$

באופן כללי, אם $f = p_1^{a_1}\cdots p_r^{a_r}$, ניקח $b_1,\dots,b_r$ מאוד גדולים ($a_i \le b_i$) וניקח l כך ש-

$$p_1^{b_1}\cdot\ldots\cdot p_r^{b_r} \mid l-1$$

אז $\frac{1}{l-1}\#\{\tau\in\mathbb{Z}/(l-1)\mathbb{Z} \mid f \mid \mathrm{ord}\,\tau\} \ge \prod_{i=1}^{r}(1-p^{a_i-b_i}) \xrightarrow[b_i\to\infty]{} 1$ (*) .

$$\Rightarrow \#\{P\in\Omega_l \mid N_P \le Z\} \gtrsim \frac{Z^{1/f}}{\log Z}(1-\varepsilon)$$

לכל ε.

$\Leftarrow$ (סיימנו את ההוכחה) משפט צ'בוטרב. (**) $\square$

(*) נניח שוות,

$$\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$\hat{a} \mapsfrom a$$

אם φ ש- $f \nmid \mathrm{ord}(a)$ ⇐ אז $\hat{a}$ φ -ש $\hat{a} \nmid \mathrm{ord}(m)$, אז $f \nmid \mathrm{ord}(\hat{a})$

והעובדה שיש ל' סוגים בגודל שווה ⇐

לכן

$$\Pr\left[\begin{array}{c} a\in \mathbb{Z}/m\mathbb{Z} \\ f \nmid \mathrm{ord}(a)\end{array}\right] \geq \Pr\left[\begin{array}{c} a\in \mathbb{Z}/n\mathbb{Z} \\ f\nmid \mathrm{ord}(\bar{a})\end{array}\right] = \prod_{i=1}^{r}\left(1-\frac{p^{a_i}}{p^{b_i}}\right)$$

מכפלי

מהורדת כפי אם בושני דביוק של $n=p_1^{b_1}\cdots p_r^{b_r}$

(**) אם $\varepsilon>0$, יש z_0 ש- $z>z_0$ אז,

$$\frac{\#\{\mathfrak{p}\in\Omega_L \mid N_{\mathfrak{p}}\leq z\}-1}{z^{1/f}/\log z} \geq -\varepsilon$$

⇐ $\underline{\lim}_{z}(\ldots)\geq 0$

מסקנה: (*) לשארית מדויקת אם $\mathrm{Gal}(\cdots)=S_n$:

$G\leq S_n$ עבור חבורת תמורות מדרגה n. (כבר פולט – נתון אם קיים רצון) בעיה ההפוכה – האם לכל חבורה סופית ניתן למצוא הרחבת גלואה $G\simeq \mathrm{Gal}(L/\mathbb{Q})$?

בעיה כללית: כמה פולינומים $f=x^n+a_1x^{n-1}+\dots+a_0$ יש חבורת גלואה S_n.

אם $\mathrm{Gal}(L/\mathbb{Q})=S_n$, אז מחלקות צמידות

$$\underbrace{(2,1,\ldots,1)}_{\text{חילוף}},\ \underbrace{(n-1,1)}_{n-1\ \text{מחזור}},\ \underbrace{(n)}_{n\ \text{מחזור}}$$ (יוצר את S_n?)

אז שבכל אחת מספיק מהסוג הזה משפט המונים.

בעיית גלואה ההפוכה - בהינתן חבורה סופית האם יש הרחבה גלואה של ידועים
על Q ...

מה כן ידוע?

① S_n, A_n

② ציקליות (משפט דיריכלה)

③ חבורות פתירות - משפט שפרביץ' (שפרביץ')

משפט Scholtz-Reichardt - חבורות p אי־זוגי

* בעיה פתוחה לסופר־פתירות (בעיה אנלוגית)

④ חבורות מטריצות $PSL_n(\mathbb{F}_q)$, $O_n^{\pm}(\mathbb{F}_q)$, $Sp_n(\mathbb{F}_q)$

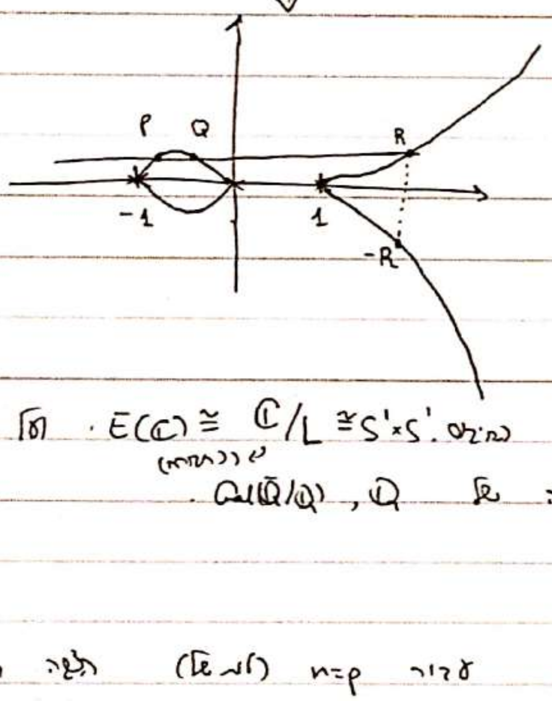
$$G \left[\begin{array}{l} N \\ \mid \; \big] G \cong H \\ E \\ \mid \; \big] G/H \\ \mathbb{Q} \end{array}\right.$$

פתירות
|
סופר פתירות
|
נילפוטנטי — חבורת p
|
אבלית
|
ציקלית

שיטה: הרבה שונה. למשל - $E = \{y^2 = x^3 - x\}$

$E(\mathbb{R}) = \{(x,y) \in \mathbb{R}^2 \mid y^2 = x^3 - x\}$

$E(\mathbb{C}) = \{\cdots \; \mathbb{C}^2 \; \cdots\}$



$P+Q+R=0$

אם $E(\mathbb{Q})$ הרבה יותר קשה לתאר. $E(\mathbb{C}) \cong \mathbb{C}/L \cong S^1 \times S^1$ (טורוס) נראה
$E(\bar{\mathbb{Q}})$ יש פעולה של חבורת גלואה של $\mathbb{Q}$, $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.
ויש $E[n] = \{p \in E(\mathbb{C}) \mid np = 0\} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
$\subseteq E(\bar{\mathbb{Q}})$

לכן, $G_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \circlearrowright E[n]$. קיבלנו עבור $n=p$ (ראשוני) הצגה מודולו
p של $G_{\mathbb{Q}}$, כי $E[p]$ מרחב וקטורי ממימד 2. כלומר E משרה

$$\rho_p : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_p)$$

משפט: שדה של הגרעין, L_p, יש חבורת גלואה $Gal(L_p/\mathbb{Q}) = im\,\rho \leq GL_2(\mathbb{F}_p)$.

(הפילוסופיה - חבורת גלואה היא הכי בדרך כלל. לכן מעניין)

תוצאות $\subset SL_n$

D. Zywina (2022)

$PSL_2(\mathbb{F}_p)$ חבורת גלואה לכל p.

(5) משפט אי-הפריקות של הילברט – רעיון: במקום לפתור את הבעיה מעל $\mathbb{Q}$, לפתור מעל $\mathbb{Q}(t)$.

משפט אי הפריקות של הילברט – אם $f(x,t)\in\mathbb{Q}[x,t]$ אי פריק, ואם $\deg_x f\geq 1$, אז יש אינסוף t-ים ב-$\mathbb{Q}$ כך ש-$f(x,t)\in\mathbb{Q}[x]$ אי פריק.

דוגמה: הבעיה של G ריבועי – תרגיל – אם $f(x)$ פולינום, $f(n)=\square$ לכל ה-n-ים >0, אז $f(x)=g(x)^2$.

מסקנה: אם G חבורת גלואה מעל $\mathbb{Q}(t)$, אז גם מעל $\mathbb{Q}$.

הרחבות של $\mathbb{Q}(t)$ מתאימות לכיסויים של $\mathbb{P}^1_{\mathbb{Q}}$, וגיאומטריה נכנסת למשחק.