5/6/19

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

מניחים שאם L/K ציקלוטומית, אז

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

רוצים להוכיח ל-G כלשהי. (L/K לא בהכרח ציקלוטומית) ראינו

← (נובע מכך שיש [illegible] [illegible] 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

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

[מתקנים טעות בהוכחה משיעור שעבר]

נבחר שורש יחידה ζ, כך ש- $\mathrm{ord}(\zeta) = \ell$ ראשוני.

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

(2) $\ell \nmid \mathrm{disc}(L/\mathbb{Q}) \Leftarrow$ [illegible] $L \cap \mathbb{Q}(\zeta) = \mathbb{Q}$,

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

נבחר $\tau^* \in \mathbb{Z}/(\ell-1)\mathbb{Z} \cong (\mathbb{Z}/\ell\mathbb{Z})^* \cong \mathrm{Gal}(L(\zeta)/L)$, 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 - $D = L(\zeta)^{\Delta}$.

נשים לב ש-

$$\Delta \cap G \times \{1\} = 1$$

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

מכאן,

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

לכן, N/D - ציקלוטומית (נוצר ע"י שורש היחידה ζ).

בנוסף: $\Delta \cap (\{1\} \times \mathbb{Z}/(\ell-1)\mathbb{Z}) = \langle \rho^f \rangle = \langle (1, \tau^f) \rangle \cong \mathbb{Z}/(\tfrac{t}{f})\mathbb{Z}$ - כי צריך לאפס את 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,

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

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

[נובע מפונקטוריאליות של סמל הפרובניוס]

$$\left(\frac{N/K}{\mathfrak{P}}\right) = \rho \iff \left(\frac{N/D}{\mathfrak{P}}\right) = \rho \ , \ f(\mathfrak{P}_D/\mathfrak{P}_K)=1 \text{ וגם}$$

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

לכן:

$$\#\{\mathfrak{P}\in\mathcal{P}(N) \mid N\mathfrak{P}\le Y, \left(\frac{N/K}{\mathfrak{P}}\right)=\rho\} = O(1) + \frac{Y^{1/t}}{\log Y} + \underbrace{\#\{\mathfrak{P}\in\mathcal{P}(N) \mid \underset{f(\mathfrak{P}_D/\mathfrak{P}_K)>1}{\underset{\left(\frac{N/D}{\mathfrak{P}}\right)=\rho}{N\mathfrak{P}\le Y}}\}}_{*} =$$

הגבלה - המוספים בהרחבה מעל - ב-ℓ חסום ונפתרות

לכן יש p אחד! (לבדוק) (עם 6 מעל ...)

* - ה-השגיאה של כמה שגיאה שונים

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

עכשיו ניתן להסיק ש-

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

עם הנכונה הסופה.

יהי $\mathfrak{P}\in N_{N,\tau}$

עבור איזשהו $\tau\in\mathbb{Z}/(l-1)\mathbb{Z}$ מסדר שמחלק L-ב, אז תהיה הפירוק של הראשוני מעל L הוא

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

וגם,

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

לכן.

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

יתר על כן,

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

בגלל הפונקטוריאליות של הפרובניוס

הערה: לא חייב להיות לכל בדיוק כמה ראשונים יש מעל

Δ - $\mathfrak{P}_L$ יש ~~.....~~ לכל היותר

$\frac{l-1}{f'} = \frac{(l-1)f}{t}$ ראשונים שונים מ-$\Omega_{N,\tau}$

ולכן אם נספור נקבל

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

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

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

תזכורת:

$$\cancel{\#\{\mathfrak{P} \in \mathcal{Z}(L) \mid N\mathfrak{p} \le Y,\ (\tfrac{L}{K})\}}$$

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

שים לב: תרגמים ל- Ω_l -

$$\frac{1}{l-1}\cdot\frac{z^{1/f}}{\log z} \sim \#\{\mathfrak{P} \in \Omega_l \mid \mathfrak{p} = \mathfrak{P}_N,\ N\mathfrak{p} \le z\}$$

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

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

(זה ברור כי ההתאמה משאירה לפרוקים ת"ג)

לכן,

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

$$\frac{\quad}{l-1}$$

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

דוגמא: ניקח $f=2$.

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

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

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

$$\Downarrow$$

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

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

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

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

$$\Rightarrow \#\{\mathfrak{p} \in \Omega_l \mid N\mathfrak{p} \le z\} \gtrsim \frac{z^{1/f}}{\log z}(1-\varepsilon)$$

לכל ε.

⇐ סיימנו (לפי הטענה משפט צ'בוטרב). (**) □

(*) ~~...~~ נניח מוח,

$$\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

$$\psi \qquad\qquad \Psi_a$$

φ $f\,|\,\mathrm{ord}(a) \Leftarrow$ אם $\hat{a}$ φ -ש $\hat{a}\cdot\mathrm{ord}(m)$, אז $f\,|\,\mathrm{ord}(\hat{a})$

והעתקה עם ' סגור בגלל שונה $\Leftarrow$ ~~...~~

לכן

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

מכפלי

מוורעה כפי לכן בושוני דבירוך של $n=p_1^{b_1}\cdots p_r^{b_r}$

(**) לכן $\varepsilon>0$, יש z_0 φ שלכל $z>z_0$,

$$\frac{\#\{P\in\Omega_L \mid N_P\le z\}-1}{z^{1/f}/\log z} \geq -\varepsilon$$

$$\Leftarrow \quad \underline{\lim_{z}}(\dots)\geq 0 \quad ~~...~~$$

מסקנה: (*) משתרתם עבדיקה של $\mathrm{Gal}(\dots)=S_n$:

$G\le S_n$ עם חבורה תמורות מדרגה n. (כמו כולם - נושא של דוגמה בעוק n בגם שאלה ההפוכה - האם לכל חבורה סופית נחה משוואה כמו שאלה $G\simeq \mathrm{Gal}(L/\mathbb{Q})$?

דוגמה לגלואה: לרוב הפולינומים $f=x^n+a_1x^{n-1}+\dots+a_0$ יש חבורת גלואה S_n.

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

$$(2,1,\dots,1),\ (n-1,1),\ (n)$$

חילוף, מעגל $n-1$, מעגל n (יוצר את S_n?)

א שבכל אלמנט בסגנון חסוס הלך שמן מסוים.

בעיית גלואה ההפוכה - בעיה פתוחה. כמובן שיש הרבה חבורות שלא יודעים

אם כן / לא

מה כן יודעים?

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

① S_n, A_n

② ציקליות (משפט דיריכלה)

③ חבורות פתירות - משפט שפרביץ' (הפוך)

משפט Scholtz-Reichart - חבורות p אי-זוגי

* הוכחה חדשה לסופר-פתירות (עשה באמצעות [illegible])

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

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

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

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

פתירות

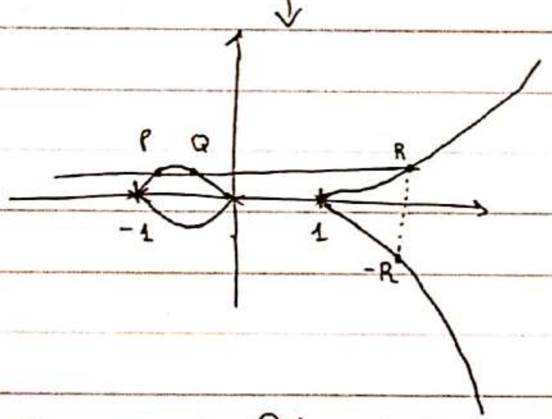
סופר פתירות

נילפוטנטית

חבורת p

אבלית

ציקלית



$P+Q+R=0$

אם $E(\mathbb{Q})$ חבורה צריך לבדוק. כמובן $E(\mathbb{C}) \underset{\text{(כטורוס)}}{\cong} \mathbb{C}/L \cong S^1\times S^1$. נכון

$E(\bar{\mathbb{Q}})$ יש פעולה של חבורת גלואה של $\mathbb{Q}$, $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.

יתרה מזאת $E[n]=\{p\in E(\mathbb{C}) \mid np=0\} \cong \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$.

$\subseteq E(\bar{\mathbb{Q}})$

לכן, $G_{\mathbb{Q}}=Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \curvearrowright E[n]$. קיבלנו עבור $n=p$ (למשל) הצגה מעניינת של $G_{\mathbb{Q}}$, כי $E[p]$ מרחב וקטורי ממימד 2. כלומר E מגדיר

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

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

הפילוסופיה - חבורת גלואה היא הכי דבר מעניין. לכן גם מעניינים

תמונות $\subset GL_n$

D. Zywina (20??)

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

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

משפט י' 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 ריבועית - תזכורת - אם $f(x)$ פולינום, ~~$f(x)=\square$~~ לכל ה-x ≥ 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 לנושא.