15/5/2019

$\boxed{\text{הרצאה 9}}$

תכונה: אם יש לנו טור דיריכלה $f(s)=\sum_{n=1}^{\infty} a_n n^{-s}$
~~מתכנס~~ אם $\sum_{n<x} a_n \ll x^b$, פרט, אז יש התכנסות
ב- $\mathrm{Re}(s)>b$.

ראינו ש- $\zeta(s)=\sum n^{-s}$ - אנליטית ב- $\mathbb{C}$ פרט לקוטב פשוט ב- $s=1$.

הגדרנו $\zeta_K(s)=\sum_{\mathfrak{a}}(N\mathfrak{a})^{-s}$, כש- $\mathfrak{a}$ רץ על אידיאלים שונים מ-0 ב- $\mathcal{O}_K$. חבורת מחלקות הקרן היתה $C_K^{\mathfrak{m}}=I^{\mathfrak{m}}/K_{\mathfrak{m},1}$. לכל $H\in C_K^{\mathfrak{m}}$ הגדרנו את $\zeta_K(s,H)=\sum_{\mathfrak{a}\in H}(N\mathfrak{a})^{-s}$. ע"י אינטגרציה ראינו ש-

$$S(n,H)=\#\{\mathfrak{a}\in H \mid N\mathfrak{a}\le n\}\sim g_{\mathfrak{m}}\cdot n$$

$$g_{\mathfrak{m}}=\frac{2^{r+s}\, reg_{\mathfrak{m}}\cdot \pi^{s}}{N_{\mathfrak{m}}\, |\Delta_K|^{1/2}\, w_{\mathfrak{m}}}$$

$$N_{\mathfrak{m}} = 2^{r_0}\cdot 2_{\mathfrak{m}_0}$$

מסקנה: פונקציית כאלו $\zeta_H(K,s)$ אנליטית ב- $\mathrm{Re}(s)>1$ וכן $g_{\mathfrak{m}}=\lim_{s\to 1^+}(s-1)\zeta_H(s,K)$.

בפרט הקוטב לא תלוי ב- $H\in C_K^{\mathfrak{m}}$. נזכיר את הקבועים:

* $r=$ # שיכונים ב- $\mathbb{R}$
* $s=\frac{1}{2}\cdot$ # שיכונים מרוכבים
* $reg_{\mathfrak{m}}=$ נפח של $\ell(\mathcal{O}_K^{*}\cap K_{\mathfrak{m},1})$
* $w_{\mathfrak{m}}$ מס' שורשי היחידה ב- $K_{\mathfrak{m},1}$
* $\Delta_K$ - דיסקרימיננטת השדה

מסקנה: $\zeta_K(s)=\sum_{H\in C_K}\zeta_K(s,H)$ (לוקחים מודולוס $\mathfrak{m}=1$) אנליטית ב- $\mathrm{Re}(s)>1$,
$\lim_{s\to 1^+}(s-1)\zeta_K(s)=g_K\cdot h_K$. (כאן $g_K=g_{\mathfrak{m}}$ ל- $\mathfrak{m}=1$)

מסקנה: תהי $L/K$ הרחבה סופית של שדות מספרים. אז יש $\infty$ ראשוניים
$\mathfrak{p}\in P_f(K)$ שמתפצלים לחלוטין ב- $L$.

בה"כ ההרחבה שלה גלואה (עובר לסגור גלואה, ומתפצל לחלוטין בגלואה $\Leftrightarrow$ מתפצל בהרחבה)

דוגמה: יש $\infty$ ראשוניים שהם $p\equiv 1 \pmod{n}$. כי $p\equiv 1 \pmod{n} \Leftrightarrow \left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p}\right)=1\in(\mathbb{Z}/n\mathbb{Z})^{*} \Leftrightarrow$
p מתפצל לחלוטין.

$\Downarrow$
$e=f=1$

הוכחה: לכל $\mathfrak{P}\in P_f(L)$ נסמן $f_{\mathfrak{P}}$ - הדרגה היחסית מעל $K$.

$$\sum_{\mathfrak{P}\in P_f(L)} N\mathfrak{P}^{-s}-\sum_{\mathfrak{P},\, f_{\mathfrak{P}}=1} N\mathfrak{P}^{-s}=\sum_{\substack{\mathfrak{P}\in P(L)\\ f_{\mathfrak{P}}\ge 2}} N\mathfrak{P}^{-s}=\sum_{p\in P_f(\mathbb{Q})}\sum_{\substack{\mathfrak{P}\mid p\\ f_{\mathfrak{P}}\ge 2}} p^{-f_{\mathfrak{P}|\mathbb{Q}}s}\le$$

$$\le [L:\mathbb{Q}]\sum_{p\in P_f(\mathbb{Q})} p^{-2s}\le [L:\mathbb{Q}]\sum\frac{1}{n^2}=O(1)$$

(נשאר להוכיח ש- $\sum_{P\in P_k(L)} NP^{-s} \xrightarrow[s\to 1]{} \infty$. ואכן

$$\sum_{P\in P_k(L)} NP^{-s} = -\log(s-1)+O(1) \xrightarrow[s\to 1]{} \infty$$

(כי ל-$\zeta_L(s)$ יש קוטב ב-$s=1$,

$$-\log \sum Na^{-s} = \sum \log(1-NP^{-s}) = \sum NP^{-s}+O(1)$$ ) □

<u>משפט</u>: ל-$\zeta_K(s,H)$ יש המשכה אנליטית ל-$Re(s)>1-\frac{1}{d}$, $d=[K:\mathbb{Q}]$, פרט לקוטב פשוט ב-$s=1$.

<u>הוכחה</u>: ראינו

$$S(n,H)\sim ?\frac{a}{g_m}\cdot n$$

וזה נותן ל-$Re(s)>1$. אם נותן הערכה

$$(*)\quad S(n,H)\sim ?\frac{a}{g_m}\cdot n+O(n^{1-1/d})$$

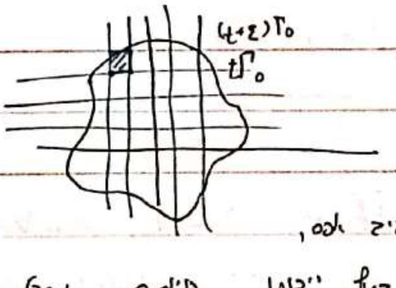
זה יתן המשכה ל-$Re(s)>1-1/d$, כי זה היה ראשית

$$\zeta_H(s,H)-a\cdot\zeta_K(s)=\sum_{n=1}^{\infty} b_n\cdot n^{-s}\quad,\sum_{n\le x} b_n=(S(n,H)-an)$$
$$\left|\sum_{n\le x} b_n\right|\le O(n^{1-1/d})$$

ולכן, ממשפט שהיה לנו, $\zeta_K(s,H)-a\zeta_K(s)$ - אנליטית ב-$Re(s)>1-\frac{1}{d}$, $\zeta_K(s)$ - אנליטית בכל $\mathbb{C}$ פרט לקוטב ב-$s=1$ כלומר, ואז $\zeta_K(s,H)$ אנליטית ב-$Re(s)>1-\frac{1}{d}$ עד קוטב פשוט ב-$s=1$. נוכיח את הערכה (*)

איך חישבנו את $S(n,H)$? כיסינו את ברשת

עבור $t^d=nN_m$, $\mu(t)=\omega_m S(n,K)=$ מס׳ נקודות סריג של $L$ ב-$t\Gamma_0$




אינטואיטיבית - השגיאה מסדר גודל של השפה. נוכיח את זה פורמלית

שם קיבלנו $M(t)\approx t^d\frac{Vol(\Gamma_0)}{Vol(L)}$

אם נוסיף $\varepsilon$,

$$M(t)\le (t+\varepsilon)^d\frac{Vol(\Gamma_0)}{Vol(L)}$$

בגלל ש-$\varepsilon\Gamma_0$ יכיל את המקבילון סביב שפה, ואז כל המקבילונים ש-$\frac{1}{2}$ בפנים $t\Gamma_0$ ייכנסו פנימה. נקבל

$$(t-\varepsilon)^d\frac{Vol(\Gamma_0)}{Vol(L)}\le M(t)\le (t+\varepsilon)^d\frac{Vol(\Gamma_0)}{Vol(L)}$$

$$\Leftarrow \mu(t)=t^d\frac{Vol(\Gamma_0)}{Vol(L)}+O(t^{d-1})$$

□

<u>פונקציות L</u>

<u>רקע: קרקטרים של חבורות אבליות סופיות</u>

$G$ - חבורה אבלית סופית, נזכיר

$$\hat{G}=\{\chi: G\xrightarrow{\text{הומו׳}}\mathbb{C}^*\}$$ - אבלית

נסמן $\hat{G}$ = הקרקטרים הכרכים: (הפעולה - כפל נקודתי)

<u>משפט</u>: $\hat{G}\cong G$. [לא קנוני, $\chi(G)\subseteq\mu_{|G|}$]

הוכחה: נניח תחילה ש- $G$ ציקלית, $G=\langle g\rangle$, $n=|G|$. ניקח $\zeta\in\mu_n$ שורש יחידה פרימיטיבי ונגדיר $\chi(g^i)=\zeta^i$. מסדר שווה ל- $\hat{G}$ ההוגדר, ולכן $n=|\chi|$, $\mathrm{ord}(\chi)=n$, ולכן $\hat{G}\cong G$.

אם $G=G_1\times G_2$ אז ברור ש- $\hat{G}=\hat{G}_1\times\hat{G}_2$ וסיימנו. □

יש העתקה טבעית:

$$G\longrightarrow\hat{\hat{G}}$$
$$g\longmapsto(\chi\mapsto\chi(g))$$

חח"ע ולכן על. ולכן $G\cong\hat{\hat{G}}$ באופן טבעי.

משפט: (יחסי האורתוגונליות הקלאסיים)

(1) $\frac{1}{\#G}\sum_{g\in G}\chi_1(g)\chi_2(g)=\begin{cases}0, & \chi_1\neq\chi_2^{-1}\\ 1, & \text{אחרת}\end{cases}$ ובפרט $\frac{1}{\#G}\sum_{g\in G}\chi(G)=\begin{cases}1, & \chi=\chi_0\\ 0, & \text{אחרת}\end{cases}$ ⊛

(2) $\frac{1}{\#G}\sum_{\chi\in\hat{G}}\chi(g)\chi(h)=\begin{cases}0, & g\neq h^{-1}\\ 1, & \text{אחרת}\end{cases}$ ובפרט $\frac{1}{\#G}\sum_{\chi\in\hat{G}}\chi(g)=\begin{cases}1, & g=1\\ 0, & \text{אחרת}\end{cases}$

הוכחה: די להוכיח אחד מהם כי $G=\hat{\hat{G}}$. נוכיח את ⊛:

$$\sum_{g\in G}\chi(g)=\chi(h)^{-1}\cdot\chi(h)\sum_{g\in G}\chi(g)=\chi(h^{-1})\sum_{g\in G}\chi(hg)=\chi(h)^{-1}\sum_{g\in G}\chi(g)$$

אם $\chi=\chi_0$ - ברור

⇐ יוצא 0

אם נניח $\chi\neq\chi_0$ וניקח $h$ כך ש- $\chi(h)\neq 1$. □

משפט: יהי $u$ משתנה, $G$ אבלית, $g\in G$ מסדר $f$. אז

$$(1-u^f)^{|G|/f}=\prod_{\chi\in\hat{G}}(1-\chi(g)u)$$

הוכחה: נתבונן במרחב

$$V=L^2(G)=\{f:G\longrightarrow\mathbb{C}\},\ \dim V=|G|$$

$G$ פועל על $L^2(G)$ ע"י הזזה -

$$f^g(h)=f(gh)$$

נסמן ב- $\rho_g$ את האופרטור שמתאים ל- $g$ ב- $V$. יש בסיס ~~...~~ אלכסוני, $\{\chi_1,\dots,\chi_{|G|}\}=\hat{G}$.

$$\chi_i^g(h)=\chi_i(gh)=\chi_i(g)\chi_i(h)$$

כלומר זה בסיס של ו"ע, ע"ע $\chi_i(g)$. ולכן מכפלת אחד הפולינומים האופייניים ל- $(1-u\rho_{g^{-1}})$:

$$\det(1-u\rho_{g^{-1}})=\det\begin{pmatrix}1-\chi_1(g) & & \\ & \ddots & \\ & & 1-\chi_{|G|}(g)\end{pmatrix}=\prod_{\chi\in\hat{G}}(1-\chi(g)u)$$

הפולינום המינימלי הוא $1-u^f$ שכן $g$ מסדר $f$, ולו $g$ מופיע
אותו מספר פעמים, כי זה החוג ולכן הוסף $k$ לכל ערך עצמי
מאותו גודל. □

יהא $K$ שדה מספרים, $\mathfrak{m}$ מודולוס, $C_K^{\mathfrak{m}}$ חבורת מחלקות הרי,
$\chi: C_K^{\mathfrak{m}} \to \mathbb{C}^*$ קרקטר. נרחיב את $\chi$ אל $I_{\mathfrak{m}}$ ע"י
$$\chi(\mathfrak{a}) := \chi(\mathfrak{a}\cdot i(K_{\mathfrak{m},1}))$$

נגדיר:
$$L(s,\chi) = \sum_{\mathfrak{a}\in I^{\mathfrak{m}}} \chi(\mathfrak{a}) N(\mathfrak{a})^{-s} =$$
$$= \sum_{\alpha\in C_K^{\mathfrak{m}}} \chi(\alpha) \sum_{\mathfrak{a}\in\alpha} N(\mathfrak{a})^{-s} =$$
$$= \sum_{\alpha\in C_K^{\mathfrak{m}}} \chi(\alpha)\zeta_K(s,\alpha)$$

**מסקנה:** ① אם $\chi\neq\chi_0$ אז $L(s,\chi)$ אנליטית ב-$Re(s)>1-\frac{1}{d}$ (אין קוטב ב-$s=1$)
② אם $\chi=\chi_0$ אז $L(s,\chi)$ אנליטית ב-$Re(s)>1-\frac{1}{d}$ פרט לקוטב
פשוט ב-$s=1$ עם שארית $h_{\mathfrak{m}}\cdot g_{\mathfrak{m}}$ כאשר $h_{\mathfrak{m}}=|C_K^{\mathfrak{m}}|$.

**הוכחה:** $\zeta_K(s,\alpha)$ - כולן אנליטיות ב-$Re(s)>1-\frac{1}{d}$ פרט ל-$s=1$. ב-$s=1$,
$$\lim_{s\to 1^+}(s-1)L(s,\chi) = \lim_{s\to 1}\sum_{\alpha\in C_K^{\mathfrak{m}}}\chi(\alpha)(s-1)\zeta_K(s,\alpha) =$$
$$= \sum_{\alpha\in C_K^{\mathfrak{m}}}\chi(\alpha)g_{\mathfrak{m}} = \begin{cases} 0, & \chi\neq\chi_0 \\ g_{\mathfrak{m}}h_{\mathfrak{m}}, & \chi=\chi_0\end{cases}$$
□

## מכפלת אוילר

**משפט:** עבור $Re(s)>1$,
$$L(s,\chi) = \prod_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ \text{ראשוני}}}\left(1-\chi(\mathfrak{p})N_{\mathfrak{p}}^{-s}\right)^{-1}$$
בפרט, אם $\mathfrak{m}=1$, $\chi=\chi_0$,
$$\zeta_K(s) = \prod_{\mathfrak{p}\ \text{ראשוני}}\left(1-\chi(\mathfrak{p})N_{\mathfrak{p}}^{-s}\right)^{-1}$$

**הוכחה:** תרגיל. □

## הרחבות ציקלוטומיות

נאמר שהרחבה $L/K$ ציקלוטומית אם $L\subseteq K(\xi)$ עבור $\xi$ שורש יחידה.

**תזכורת:** (העתקת ארטין)

$L/K$ אבלית, $G=Gal(L/K)$, יהי $\mathfrak{m}_0$ מודולוס ב-$O_K$, $\mathfrak{p}$ כך ש-$\mathfrak{p}\nmid\mathfrak{m}_0 \Rightarrow$
$\mathfrak{p}$ לא מסועף. (כלומר איננו מחלק דיסקרימיננטה)

ו.ל הגדרנו

$$\phi_{L/K} : I^{\mathfrak{m}} \longrightarrow G$$

$$\phi_{L/K}\left(\prod \mathfrak{p}_i^{e_i}\right) = \prod \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}$$

($G$ אבלית)

$$\operatorname{im} \phi_{L/K} = ? , \quad \ker \phi_{L/K} = ?$$

**טענה:** תהי $L/K$ הרחבה ציקלוטומית כך ש- $L \subseteq K(\xi)$, $\xi$ שורש יחידה מסדר $k$, ו- $\mathfrak{m}$ מודולוס שמחלק ~~~~ $k\mathfrak{m}$. אזי $\ker \phi_{L/K} \supseteq \iota(K_{\mathfrak{m},1})$. בפרט ניתן להגדיר $\phi_{L/K}$ כ- $C\ell^{\mathfrak{m}} \to G$.

<u>הוכחה:</u> הראשוניים המסתעפים ב- $L$ מחלקים ~~~~ את $k$.

$$\begin{array}{ccc} K & — & L \\ | & & | \\ \mathbb{Q} & — & \mathbb{Q}(\xi) \end{array}$$

~~לכן $\mathfrak{m}$ ...~~

ואם לא $\mathfrak{p}$ מחלק את $\mathfrak{m}$. ~~אז~~ בה"כ

ניתן להניח $L = K(\xi)$ (כי ניתן לצמצם את העתקה ... 1.1 מסתעף $\Leftarrow$ לא מסתעף ב- $L/K$

$\phi$). ואז $Gal(L/K) \le (\mathbb{Z}/k\mathbb{Z})^*$, דרך הזיהוי:

$$\sigma \mapsto i \iff \sigma(\xi) = \xi^i$$

ראינו שהצמצום של העתקת ארטין מוביל לנורמה, כלומר

$N_{K/\mathbb{Q}}(\mathfrak{a}) \equiv 1 \pmod k$ עבור $\mathfrak{a} \in I^{\mathfrak{m}}$, אז $\phi_{L/K}(\mathfrak{a}) = 1$.

(של העתקת ארטין ב- $\mathbb{Q}(\xi)/\mathbb{Q}$)

ניקח $x \in K_{\mathfrak{m},1}$. יודעים ש- $x \equiv^* 1 \pmod{\mathfrak{m}}$. כיוון ש- $k \mid \mathfrak{m}$, $x = 1 + ky$, $y \in K$.

אז,

$$N_{K/\mathbb{Q}}(x) = \prod_{\sigma : K \to \mathbb{C}} \sigma(1+ky) = \prod_{\sigma} (1 + k\sigma(y)) = 1 + k\underset{\text{מספר שלם ב-}K}{\underbrace{*}} \equiv 1 \pmod k$$

ולכן $x \in \ker \phi_{L/K}$.

(וזו ההטענה עבור).

**טענה:** $\phi_{L/K}$ היא על אם $L/K$ ציקלוטומית. באופן כללי, אם $L = K(\xi)$, $\operatorname{ord}(\xi) = k$, $k \mid \mathfrak{m}$, אז $\phi_{L/K}$ על ולכל $x \in Gal(L/K)$ לא טריוויאלי,

$$L_{\mathfrak{m}}\left(1, x \circ \left(\frac{L/K}{\cdot}\right)\right) \neq 0$$