10/4/19

הרצאה 7

תזכורת: $K_m = \{\frac{x}{y} \in K^* \mid x,y \in \mathcal{O}_K, \gcd(xy, m_0)=1\}$, $K_{m,1} = \{x \in K^* \mid x \equiv^* 1 \mod m\}$.

בדומה גם הגדרנו את חבורת מחלקות הקרן,

$$G_K^m = I^m / \iota(K_{m,1})$$

כאשר -

I^m = אידאלים שברים זרים ל-m_0

$\iota : K^* \to I^m$

$\iota(\alpha) = \alpha \mathcal{O}_K$

כדי לראות שיש העתקה $K_m / K_{m,1} \twoheadrightarrow G_K^m$. (רצינו לחשב את גודל ההעתקה ואת התמונה שלה). נוכיח משפט קירוב -

משפט: תהיינה $|\cdot|_i$, $i=1,\dots,n$, ערכים מוחלטים לא שקולים על K (לא טריוויאליים). יהיו $x_1,\dots,x_n \in K$ ויהי $\varepsilon>0$. אז קיים $x \in K$ כך ש-

$|x-x_i|_i < \varepsilon$, $\forall i$

הוכחה: נמצא איברים $y_1,\dots,y_n$ כך ש-

$|y_i|_i > 1$

$|y_i|_j < 1$, $i \neq j$

באינדוקציה. $n=1$ - טריוויאלי. $n=2$ - מכך שהע"מ לא שקולים,

$\exists w.$ $|w|_1 > 1$, $|w|_2 \leq 1$

$\exists z.$ $|z|_1 \leq 1$, $|z|_2 > 1$

עבור - $y_1 = w/z$, $y_2 = z/w$

$|y_1|_1 = |w|_1 \cdot \frac{1}{|z|_1} > 1$

$|y_1|_2 < 1$

והאי שוויונים ההפוכים מתקיימים ל-y_2, כי $y_2 = 1/y_1$.

נניח שיש לנו y כך ש-

$|y|_1 > 1$, $|y|_j < 1$, $j = 2,\dots,n-1$

נמצא גם w כך ש- $|w|_1 > 1$, $|w|_j < 1$ עבור $j \geq 2$.

נבחר t כך ש- $|t|_n < 1, |t|_1 > 1$ (מהמקרה $n=2$).

~~אם~~ נגדיר עכשיו -

$$y_1 = \begin{cases} y, & |y|_n < 1 \\ y^r t, & |y|_n = 1 \\ \frac{y^r t}{1+y^r}, & |y|_n > 1 \end{cases}$$

כאשר r יבחר בקרוב

במקרה הראשון נבחר ש- y_1 טוב, במקרה השני השלישי,

$$y_1 \xrightarrow[r\to\infty]{\|\cdot\|_j} 0 \quad , \quad j=2,\dots,n-1$$

וכן,

$$y_1 \xrightarrow[r\to\infty]{\|\cdot\|_n} \begin{cases} t, & |y|_n=1 \\ t, & |y|_n>1 \end{cases}$$

ולכן אם $r\gg1$ מקבלים את הדרוש. ניקח -

$$x=\sum_{i=1}^{n}\frac{y_i^r}{1+y_i^r}\cdot x_i$$

אזי,

$$\lim_{r\to\infty,\ \|\cdot\|_i} x = x_i$$

לכן עבור $r\gg1$ נוכל לקבל $|x-x_i|<\varepsilon$. $\square$

טענה: יהיו $\mathfrak{m}_1,\dots,\mathfrak{m}_n$ מודולוסים זרים בזוגות. אזי, אם $\mathfrak{m}=\prod\mathfrak{m}_i$, ~~העתק~~
הצמצום -

$$K_\mathfrak{m}\longrightarrow\prod K_{\mathfrak{m}_i}$$

משרה איזומורפיזם,

$$K_\mathfrak{m}/K_{\mathfrak{m},1}\cong\prod K_{\mathfrak{m}_i}/K_{\mathfrak{m}_i,1}$$

הוכחה: נסמן -

$$f: K_\mathfrak{m}\longrightarrow\prod_i K_{\mathfrak{m}_i}/K_{\mathfrak{m}_i,1}$$

$$x\longmapsto (x \bmod K_{\mathfrak{m}_i,1})_{i=1}^{n}$$

נחשב גרעין ותמונה.

אם $f(\alpha)=1 \iff \alpha\equiv^* 1 \bmod \mathfrak{m}_i$ לכל $i \iff \alpha\equiv^* 1 \bmod \mathfrak{m}$. לכן $\ker f=K_{\mathfrak{m},1}$.

שים לב להראות ש- f על - ניקח: $x_i\in K_{\mathfrak{m}_i}$, $i=1,\dots,n$. ניקח, לפי משפט הקירוב, $x\in K^*$ כך ש- x קרוב ε אל x_i במובן $\|\cdot\|_\mathfrak{p}$ לכל $\mathfrak{p}|\mathfrak{m}$.
ε קטן מספיק $\Rightarrow x\equiv^* x_i \bmod \mathfrak{m}_i$ לכל i. בפרט,

$$\gcd(x,\mathfrak{m})=1\Rightarrow x\in K_\mathfrak{m}$$

$$f(x)=(x_1K_{\mathfrak{m}_1},\dots,x_nK_{\mathfrak{m}_n})$$

$\square$

מסקנה: החבורה $K_\mathfrak{m}/K_{\mathfrak{m},1}$ - סופית.

הוכחה: די להוכיח לחלקים פשוטים. אם $\mathfrak{m}=\mathfrak{p}$, $\mathfrak{p}$ ממשי,

$K_\mathfrak{p}/K_{\mathfrak{p},1}\cong\mathbb{Z}/2\mathbb{Z}$ - בפרט סופי.

אם $\mathfrak{m}=\mathfrak{p}^n$, סופי, $\mathfrak{p}$ סופי,

$K_\mathfrak{m}/K_{\mathfrak{m},1}\cong(\mathcal{O}_K/\mathfrak{p}^n)^*=q^{n-1}(q-1)$ - ולכן סופי

כאשר $q=N\mathfrak{p}$.

$\square$

לסיכום,

$$[K_{\mathfrak m} : K_{\mathfrak m,1}] = 2^{\overset{\#P_\infty}{r}} \cdot N\mathfrak m_0 \cdot \prod_{\mathfrak p | \mathfrak m_0} (1-N\mathfrak p^{-1})$$

טענה 1: לכל קוסט Σ של $K_{\mathfrak m,1}$ ב-$K_{\mathfrak m}$ ולכל אידאל שלם $\mathfrak a$, יש $a\in\Sigma$ זר ל-$\mathfrak a$.

הוכחה: נכתוב $\mathfrak a = \mathfrak a_1 \cdot \mathfrak a_2$, כאשר $\mathfrak a_1 | \mathfrak m$, $\gcd(\mathfrak a_2, \mathfrak m_0)=1$. כל $a\in K_{\mathfrak m}$ זר ל-$\mathfrak a_1$, ולכן די למצוא $a\in\Sigma$ זר ל-$\mathfrak a_2$. בה"כ, נניח אז כי $\gcd(\mathfrak a, \mathfrak m)=1$.

ניקח $\beta K_{\mathfrak m,1}$ קוסט. לפי המשפט שהוכחנו, יש $\gamma\in K_{\mathfrak m}$ כך ש-$\gamma \equiv^* 1 \pmod{\mathfrak a}$, וגם $\gamma \equiv^* \beta \pmod{\mathfrak m}$. אז, $\gamma\in\beta K_{\mathfrak m,1}$, וכן $\gcd(\gamma, \mathfrak a)=1$. □

טענה: לכל קבוצה סופית S של ראשוניים, יש איזומורפיזם,

$$C_K \cong I^S / I^S \cap \iota(K^*)$$

בפרט לכל $\mathfrak m$ מודולוס, אזי $\iota(K_{\mathfrak m}) = I^{\mathfrak m} \cap \iota(K^*)$ ולכן

$$C_K \cong I^{\mathfrak m} / \iota(K_{\mathfrak m})$$

הוכחה: יש לנו העתקה $I^S \to I$ משרה העתקה -

$$I^S / I^S \cap \iota(K^*) \hookrightarrow C_K$$

די להראות שהיא על, או לחילופין ש-$I^S \to C_K$ על. ניקח $\mathfrak b$ אידאל, נפרק -

$$\mathfrak b = \mathfrak b_1 \mathfrak b_2,\ \gcd(\mathfrak b_1, S)=1,\ \underbrace{S \supseteq \mathfrak b_2}_{\text{(החלק ה-S-י של } \mathfrak b)} \text{ כאשר}$$

נרצה להיפטר מ-$\mathfrak b_2$. לכל $\mathfrak p$ ראשוני, ניקח $\pi_{\mathfrak p}$ מאחיד, כך ש-$\pi_{\mathfrak p} \equiv 1 \pmod{\mathfrak q}$ לכל $\mathfrak p \neq \mathfrak q \in S$. נסמן $\alpha = \prod_{\mathfrak p\in S} \pi_{\mathfrak p}^{v_{\mathfrak p}(\mathfrak b)}$. אז, החלק ה-S-י של α שווה ל-$\mathfrak b_2$, ואז,

$$\gcd(\mathfrak b \cdot \alpha^{-1}, S) = 1$$

ולכן $\mathfrak b \alpha^{-1} \in I_S$. וסיימנו. □

מסקנה: לכל מודולוס $\mathfrak m$, חבורת מחלקות הקרן $C_K^{\mathfrak m}$ היא סופית (ובמפורש,
$h_{\mathfrak m} = h_K \cdot 2^r \cdot N\mathfrak m_0 \cdot \prod_{\mathfrak p | \mathfrak m_0} (1-N\mathfrak p^{-1})$, כאשר $r = \#P_\infty \cap \mathfrak m$.

הוכחה: כי,

$$\iota(K_{\mathfrak m,1}) \subseteq \iota(K_{\mathfrak m}) \subseteq I^{\mathfrak m}$$

ניקח מנה, ונקבל -

$$|C_K^{\mathfrak{m}}| = [I^{\mathfrak{m}} : L(K_{\mathfrak{m},1})] = [I^{\mathfrak{m}} : L(K_{\mathfrak{m}})] \cdot$$

$$\cdot [K_{\mathfrak{m}} : K_{\mathfrak{m},1}] = |C_K| \cdot 2^r N_{\mathfrak{m}_0} \prod_{\mathfrak{p} | \mathfrak{m}_0} (1 - N_{\mathfrak{p}}^{-1})$$ $\square$

הנוסחה - יהי L/K אבלית, $C \subseteq G = Gal(L/K)$ - מחלקת שקילות, אזי,

<u>משפט צ'בוטרב</u> -

$$\boxed{Pr\left[\left(\frac{L/K}{\mathfrak{p}}\right) = C\right] = \frac{|C|}{|G|} + Err}$$

<u>טורי דיריכלה</u>

<u>טור דיריכלה</u> - זו פונקציה -

$$f(s) = \sum_{n=1}^{\infty} a(n) n^{-s}$$

כאשר $a(n)$ סדרה מרוכבת, $s = \sigma + it, \sigma, t \in \mathbb{R}$.

f פונקציה יוצרת -

$$\left(\sum_{n=1}^{\infty} a_n z^n\right)\left(\sum_{n=1}^{\infty} b_n z^n\right) = \sum_{k=1}^{\infty} \left(\sum a_k b_{n-k}\right) z^k$$ השקלול יפה כמו בפולינומים

בפונקציות זטה דיריכלה, הם משקלים את סדר עבור $\sum_{kl=n}$ במקום $\sum_{k+l=n}$:

$$\left(\sum_{n=1}^{\infty} a_n n^{-s}\right)\left(\sum_{n=1}^{\infty} b_n n^{-s}\right) = \sum_{n=1}^{\infty} n^{-s} \left(\sum_{dr=n} a_d b_r\right)$$

<u>מקרה פרטי:</u> (הכי חשוב)

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}, \quad Re(s) > 1$$

<u>משפט:</u> ~~[illegible]~~ -

תזכורת -

$$\Gamma(s) = \int_0^{\infty} x^{s-1} e^{-x} dx$$

$$\Gamma(s) = \frac{\Gamma(s+1)}{s}$$ ⟶ המשך אנל' -
זה המשך
עם קטבים

תכונות אנליטיות של $\zeta(s)$ -

1) ל-$\zeta(s)$ יש המשכה אנליטית - ל-$\mathbb{C}$ מלבד קוטב פשוט ב-$s=1$ עם $\operatorname{Res}_{s=1} \zeta(s)=1$.

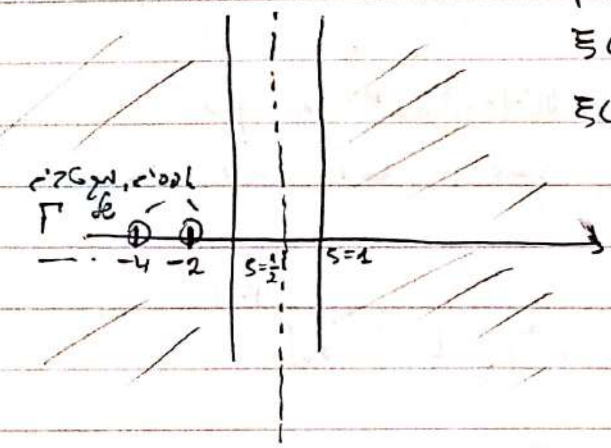
2) $\zeta(s)\neq 0$ לכל $\operatorname{Re}(s)\geq 1$.

3) ζ מקיימת משוואה פונקציונלית, אם נסמן -

$$\xi(s) = \frac{1}{2}\cdot \pi^{-s/2}\cdot \Gamma\left(\frac{s}{2}\right)\cdot s(s-1)\,\zeta(s)$$

אז,

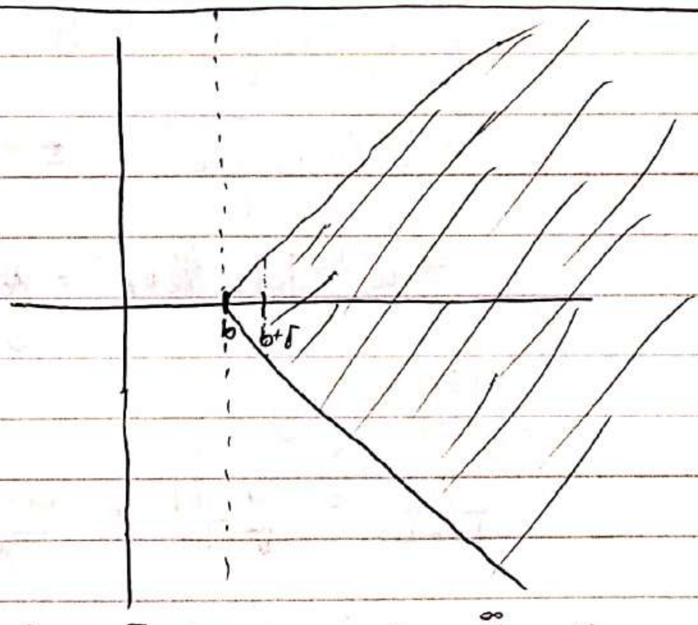
$$\xi(s) = \xi(-(s-1))$$



עבור $b\in\mathbb{R}$, $\delta,\varepsilon>0$,

נגדיר:

$$\boxed{D(b,\delta,\varepsilon)=\{s\in\mathbb{C} \mid \sigma > b+\delta,\ |\arg(s-b)|\leq \tfrac{\pi}{2}-\varepsilon\}}$$



משפט: יהי - $f(s)=\sum_{n=1}^{\infty} a(n)n^{-s}$ ונסמן $S(x)=\sum_{n\leq x} a(n)$. נניח $S(x)\ll x^b$ כש- $x\to\infty$ עבור איזה $b\in\mathbb{R}$. ($f\ll g$ אם קיים C כך ש- $|f(x)|<C\cdot|g(x)|$ כש- $x\to\infty$)

אז -

① $f(s)$ מתכנס במ"ש ב- $D(b,\delta,\varepsilon)$ לכל $\delta,\varepsilon>0$.

② $f(s)$ מתכנס לפונקציה אנליטית - ב- $\operatorname{Re}(s)>b$.

③ אם $\lim_{x\to\infty}\frac{S(x)}{x}=a(\neq 0)$ אז $\lim_{\substack{s\to 1\\ s\in D(0,1,\varepsilon)}}(s-1)f(s)=a$.

הוכחה: נשים לב ש-

$$a(n) = S(n) - S(n-1)$$

לכל $v > u+1$,

$$\left|\sum_{n=u}^{v} a(n)n^{-s}\right| = \ldots = \left|\sum_{n=u}^{v} S(n)n^{-s} - \sum_{n=u+1}^{v+1} S(n)(n+1)^{-s}\right| \le$$

$$\le \underbrace{\sum_{u}^{v-1} |S(n)| \cdot |n^{-s} - (n+1)^{-s}|}_{(**)} + \underbrace{|S(v)v^{-s}| + |S(u-1)u^{-s}|}_{(*)}$$

כיוון ש- $|n^{s}| = n^{\sigma} \ge n^{b+\delta}$ וכיוון ש- $S(x) \ll x^{b}$ נקבל ש- $(*) \ll u^{-\delta}$.

לגבי $(**)$, נשתמש בכך ש-

$$n^{s} - (n+1)^{-s} = s\int_{n}^{n+1} t^{-s-1}\,dt$$

ולכן,

$$\left|\sum_{n=u}^{v} a(n)n^{-s}\right| \ll \cancel{u}^{-\delta} + \sum |s| \cdot n^{b} \left|\int_{n}^{n-1} t^{-s-1}\,dt\right| \le$$

$$\le u^{-\delta} + \sum |s| n^{b} \int^{n+1} t^{-\sigma-1}\,dt \le$$

$$\le u^{-\delta} + \sum |s| \int_{n}^{n+1} t^{b-\sigma-1}\,dt \le$$

$$\le u^{-\delta} + |s| \int_{u}^{v-1} t^{b-\sigma-1}\,dt \le$$

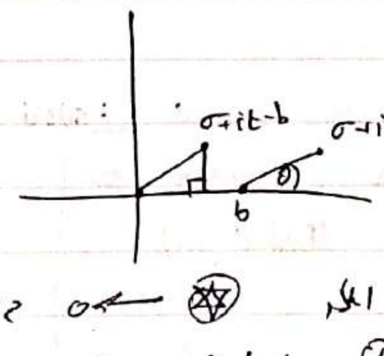
$$\le u^{-\delta} + |s| \int_{u}^{\infty} t^{b-\sigma-1} \le$$

$$= u^{-\delta} + |s| \cdot u^{b-\sigma}(\sigma - b)^{-1} = (*)$$

נשים לב ש-

$$\cancel{\frac{|s|}{|\sigma-b|} \le \arg}$$

$$\frac{|s|}{|\sigma-b|} = \frac{|\sigma+it|}{\sigma-b} \le \frac{|\sigma-b+it|+b}{\sigma-b} =$$



$$= \frac{1}{\cos\theta} + \frac{b}{\sigma-b}$$

כיוון ש- $|\theta| < \frac{\pi}{2} - \varepsilon$ נקבל ש- $\frac{|s|}{|\sigma-b|} = O(1)$. ולכן $(*) \to 0$ כנדרש.

כך שהוכחת ה- (1). (2) נובע מ- (1) + נקבל ש-

$$\{Re(s) > b\} = \bigcup_{\delta,\varepsilon>0} D(b,\delta,\varepsilon)$$

③ - נניח ש- ① נרצה להשתמש בהגבלה אבל צריך (ואז נרצה
בתרגיל בית. נסמן -

$$\varepsilon(n) = \frac{S(n) - na}{n}, \quad \varepsilon(n) \to 0$$

~~לכן~~ נעריך את -

$$|f(s) - a\zeta(s)| = \left|\sum_{n=1}^{\infty} (a(n) - a) n^{-s}\right| =$$

$$a(n) - a = S(n) - na - (S(n-1) - (n-1)a)$$

$$= \left|\sum_{n=1}^{\infty} (S(n) - na)(n^{-s} - (n+1)^{-s})\right| \leq$$

$$\leq \left|\sum_{n=1}^{\infty} n\varepsilon(n) s \int_n^{n+1} x^{-s-1} dx\right| \leq$$

$$\leq \sum_{n=1}^{\infty} n|\varepsilon(n)| \int_n^{n+1} t^{-\sigma-1} dx \cdot |s| \leq$$

$$\leq \sum_{n=1}^{\infty} |\varepsilon(n)| \cdot |s| \int_n^{n+1} x^{-\sigma} dx$$

מכיוון ש- n בגבול כמו קודם

נבחר $N_0>0$ כך ש- $|\varepsilon(n)| \leq \varepsilon_0$ לכל $n \geq N_0$. נחלק את ה- $\varepsilon(n)$ לשני סכומים, נקבל -

$$(s-1)|f(s) - a\zeta(s)| \ll |s-1| \cdot |s| \int_1^N t^{-\sigma} dt +$$

$$+ |s(s-1)| \cdot \varepsilon_0 \cdot \underbrace{\int_N^{\infty} t^{-\sigma} dt}_{N^{-\sigma+1}/\sigma-1}$$

כשניקח $s \to 1$ בתחום $D(1, \theta, \varepsilon)$ נקבל -

$$|s-1| \cdot |f(s) - a\zeta(s)| \ll \frac{|s(s-1)|\varepsilon_0}{\sigma-1} N^{-\sigma+1}$$

ואם הערכים בתחום זוויתי -

$$\frac{|s-1|}{\sigma-1} \ll \frac{1}{\cos\theta} \ll 1$$

ולכן אם קטן, נקבל -

$$|s-1| |f(s) - a\zeta(s)| \ll \varepsilon \to 0$$

ובכלליות אינטגרלית $\mathfrak{S}$ בגבול N. לכן לא נקח N כך ε_1 ... $C\varepsilon_1$ - N כל, נקבל, שה הביטוי לכל $<\varepsilon_1$ ואז נקח $\varepsilon_1 \to 0$. □

יהי K שדה מספרים, N - הנורמה המוחלטת. נגדיר את
פונקציית זטא של דדקינד,

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a} - \text{אידיאל} \\ \text{שלם}}} N(\mathfrak{a})^{-s} = \sum_{n=1}^{\infty} a_K(n) \cdot n^{-s}$$

כאשר $a_K(n)$ - # אידיאלים בנורמה n. אם $K=\mathbb{Q}$ נקבל זטא של
פונקציית זטא של רימן, $\zeta(s)=\zeta_{\mathbb{Q}}(s)$.

כי להחלט שמספר בתוך מישור, דבוקים לכל הצורה על-

$$\sum_{n\le x} a_K(n) = \#\{\mathfrak{a} \mid N\mathfrak{a} \le x\}$$

$$N_{\mathfrak{p}} = p^f \,, \quad \text{לכל } p \text{ כזה יש } [K:\mathbb{Q}] \text{ מעליו כמעט שונים}$$

לכן (?) $\sum_{n\le x} a_K(n) \ll x^{[K:\mathbb{Q}]}$. ולא נכון $\sum a_K(n) \sim \alpha x$.