הרצאה 1 27/2/19

משפט צ'בוטרב: תהי L/K הרחבת גלואה של שדות מספרים, עם חבורת גלואה G.
אזי, אם $C\subseteq G$ מחלקת צמידות,
$$\delta(\{O_K\text{-ראשוני ב}\ p \mid \left(\tfrac{L/K}{p}\right)=C\}) \sim \frac{|C|}{|G|}$$

(כאן δ מסמן, צפיפות שנגדיר בהמשך, יש שני סוגים והמשפט נכון לכל אחד מהם)

תזכורת: מחלקת הצמידות פרובניוס היא $\left(\frac{L/K}{p}\right)=\left\{\left(\frac{L/K}{\beta/p}\right) \,\middle|\, \substack{\beta\in \operatorname{spec}O_L \\ p \text{ מעל}}\right\}$, כאשר $\left(\frac{L/K}{\beta/p}\right)$ איבר פרובניוס המוגדר כך ש-
$$\left(\frac{L/K}{\beta/p}\right)x \equiv x^{N_p} \pmod{\beta}$$
כאשר $N_p=\#O_K/p$.

נגדיר עכשיו את האפשרויות לצפיפות במשפט צ'בוטרב-

הגדרה: (צפיפות דיריכלה)
אם הגבול קיים נגדיר- עבור $A\subseteq \operatorname{spec}O_K-\{0\}$ -
$$\delta_D(A)=\lim_{s\to 1^+}\frac{\sum_{\beta\in A}|N_\beta|^{-s}}{\sum_{\beta\in \operatorname{spec}O_K-\{0\}}|N_\beta|^{-1}}$$

הגדרה: (צפיפות טבעית)
אם הגבול קיים, נגדיר - שוב, עבור $A\subseteq \operatorname{spec}O_K-\{0\}$ -
$$\delta_N=\lim_{x\to\infty}\frac{\#\{p\in A \mid N_p\le x\}}{\#\{p \mid N_p\le x\}}$$

ניתן להוכיח (נראה בהמשך) שאם הצפיפות הטבעית קיימת, אז גם צפיפות דיריכלה קיימת (והיפך לא נכון). כאמור המשפט נכון לשני סוגי הצפיפויות אבל נוכיח אותו רק לצפיפות דיריכלה.

דוגמה: $K=\mathbb{Q},\ L=\mathbb{Q}(\zeta_n)$. אז $G\cong(\mathbb{Z}/n\mathbb{Z})^\times$, ואז, $\left(\frac{L/\mathbb{Q}}{p}\right)=p \pmod n$. מכאן,
$\{p \mid \left(\frac{L/\mathbb{Q}}{p}\right)=a \pmod n\}=\{p\mid p\equiv a \mod n\},\ \gcd(a,n)=1$ (מחלקת צמידות כי מדובר בחבורה אבלית)
ולכן נסיק מצ'בוטרב שיש אינסוף ראשוניים p כך ש-$p\equiv a \pmod n$, לכל a זר ל-n. (משפט דיריכלה)

עם צפיפות טבעית - $\#\{p\le x \mid p\equiv a \mod n\}=\frac{x}{\log x}\cdot\varphi(n)^{-1}(1+o(1))$

צריכים פונקציית L של דיריכלה כדי להוכיח את המשפט. ניקח $\chi:(\mathbb{Z}/n\mathbb{Z})^\times\to\mathbb{C}^\times$ קרקטר. נרחיב אותו להעתקה.

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C}$$

$$\chi(a) = \begin{cases} \chi(a \bmod n), & \gcd(a,n)=1 \\ 0, & \text{אחרת} \end{cases}$$

ל-χ כזה נקרא קרקטר <u>דיריכלה</u> מודולו n. נגדיר גם <u>פונקציית</u> <u>L של דיריכלה</u> ביחס ל-χ,

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \text{מוגדרת ל-}\mathrm{Re}(s)>1$$

כמו שהיה פירוק אוילר $\zeta(s)=\prod_p (1-p^{-s})^{-1}$, אותה הוכחה נותנת ש-

$$L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s} \underset{\chi(ab)=\chi(a)\chi(b)}{=} \sum_{p_i,e_i} \frac{\prod \chi(p_i)^{e_i}}{\prod p_i^{e_i}} = \prod_p \left(1-\frac{\chi(p)}{p^{s}}\right)^{-1}$$

שים לב של-$L(s,\chi)$ אין אפסים ב-$\mathrm{Re}(s)>1$. איך זה קשור לשוויוני סדרות חשבוניות?

<u>יחסי האורתוגונליות:</u>

$$\frac{1}{\#\{\chi\}} \cdot \sum_{\chi \bmod n} \chi(a) = \begin{cases} 1, & a \equiv 1 \pmod n \\ 0, & \text{אחרת} \end{cases}$$

כי אם a שקול ל-1 זה ברור; אחרת יש קרקטר $\eta(a)\neq 1$ של הדואלי. נקבל-

$$\eta(a)\sum_{\chi}\chi(a) = \sum_{\chi}\eta\chi(a) \underset{\text{הקרקטרים הם חבורה}}{=} \sum_{\chi}\chi(a) \Rightarrow \sum \chi(a)=0 \qquad \square$$

בעזרתם, נחשב-

$$\#\{p\leq x \mid p\equiv a \pmod n\} = \sum_{p\leq x} \mathbb{1}_{\{p\equiv a \pmod n\}} \underset{\text{יחסי האורתוגונליות}}{=} \sum_{p\leq x} \frac{1}{\#\{\chi\}}\sum_{\chi}\chi(p\bar{a}) =$$

$$\bar{a} = a^{-1} \pmod n$$

$$= \frac{1}{\#\{\chi\}}\sum_{\chi}\chi(a)\sum_{p\leq x}\chi(p) = \frac{1}{\varphi(n)}\cdot\#\{p\leq x\} + \sum_{\chi\neq\chi_0}\chi(a)\sum_{p\leq x}\chi(p)$$

$L(s,\chi)$

אם L/K אבלית, אז צריך לפתח תורה "כמו ציקלוטומית", שהיא Ray Class Groups. זה יהיה הנושא השני. בשבוע זה צריך קצת שעה שלמים (זה יהיה הנושא המשולש). ה-Ray Class Group נקבע פונקציות L-של הקה. משפט צ'בוטרב "יוצא" מפונקציות L של ארטין, שיש להן פירוק לוקלי, מהעירה הגלובלי. ויש נמצא גם ההוכחה של העירה הגלובלי.

מקורות:

- Janustz
- Serre, Local Fields
- Fried-Jordan, Field Arithmetic

שדות שלמים (Complete Fields)

הערכה

יהא K שדה כלשהו, Γ חבורה אבלית עם סדר. (יש סדר $<$ כך ש- $\alpha<\beta \Leftrightarrow \alpha+\gamma<\beta+\gamma$ לכל $\alpha,\beta,\gamma\in\Gamma$) למשל - $\Gamma=\mathbb{Z}$ או $\Gamma\subseteq\mathbb{R}$.

הגדרה: הערכה v על K זה העתקה, $v:K\to\Gamma\cup\{\infty\}$, Γ - חבורה עם סדר, כך ש-

① $v(ab)=v(a)+v(b)$

② $v(a+b)\ge\min(v(a),v(b))$

③ $v(a)=\infty \Leftrightarrow a=0$

④ לא טריוויאלית - קיים $a\neq 0$ כך ש- $v(a)\neq 0$.

תכונות בסיסיות:

⑤ $v(-a)=v(a)$, $v(1)=0$ לכל $a\in K$

⑥ אם $v(a)\neq v(b)$ אזי $v(a+b)=\min(v(a),v(b))$

הגדרה: אז, (K,v) - שדה מוערך. $\Gamma_v=v(K^\times)$ - חבורת הערכים. בנוסף, $O_v=\{x\in K\mid v(x)\ge 0\}$ - חוג ההערכה ויש בו אידיאל $m_v=\{x\in K\mid v(x)>0\}$.

נבחין ש- (O_v,m_v) חוג מקומי. ברור ש- $O_v-m_v=O_v^\times$, שכן -

$$v(x)=0 \Rightarrow v(\tfrac{1}{x})=-v(x)=0 \Rightarrow \tfrac{1}{x}\in O_v$$

לכן די להוכיח ש- O_v חוג ו- m_v אידיאל, אך זה ברור מ-1,2.

נסמן ב- $\bar{K}_v=O_v/m_v$ - שדה השאריות.

דוגמה: אם $x=p^a\cdot\frac{r}{s}$, כאשר $p\nmid r,s$ אזי $v_p(x)=a$ (הערכה על $K=\mathbb{Q}$)

דוגמה: אם $K=\mathbb{C}(x)$, $v_\alpha(f)=\underset{x=\alpha}{\mathrm{ord}}(f)=r\in\mathbb{Z}$ כאשר $f=(x-\alpha)^r\cdot\frac{g}{h}$, $\alpha\in\mathbb{C}, g(\alpha),h(\alpha)\neq 0$.

דוגמה: ניקח את השדה, $\mathbb{Q}\subseteq\mathbb{Q}(\sqrt{2})\subseteq\mathbb{Q}(\sqrt[4]{2})\subseteq\dots\subseteq K$, כאשר $K=\bigcup_{i=0}^{\infty}\mathbb{Q}(\sqrt[2^i]{2})$.

$$v_2 \quad \tfrac{1}{2}v_{\sqrt{2}} \quad \tfrac{1}{4}v_{\sqrt[4]{2}} \quad \dots \quad v=\text{"}\lim_{i\to\infty}\tfrac{1}{2^i}v_{\sqrt[2^i]{2}}\text{"}$$

$$\mathbb{Z}\hookrightarrow\tfrac{1}{2}\mathbb{Z}\hookrightarrow\tfrac{1}{4}\mathbb{Z}\ \dots\ \text{"}\lim_{i\to\infty}\text{"}=\mathbb{Z}[1/2]$$

דוגמה: $\mathbb{C}(x,y)$, $\mathbb{C}[x,y]_{(x,y)}$

$v(x)=(1,1)$

$v(y)=(1,0)$

$v(x/y)>0$

הגדרה: נאמר ש- v_1, v_2 שקולות אם יש $f:\Gamma_{v_1} \longrightarrow \Gamma_{v_2}$ איזומורפיזם של חבורות עם סדר כך ש- $f\circ v_1 = v_2$.

הגדרה: תת חוג $\mathcal{O}\subseteq K$ נקרא חוג הערכה אם לכל $0\neq x\in K$, $x\in\mathcal{O}$ או $\frac{1}{x}\in\mathcal{O}$.

טענה: אם v הערכה, אזי $\mathcal{O}_v$ חוג הערכה.

הוכחה: אם $x\in K^*$ אזי $v(x)\geq 0$ או $v(x)<0 \Rightarrow 0<v(x^{-1}) \Rightarrow x^{-1}\in\mathcal{O}_v$. □

חוג הערכה הוא תמיד מקומי עם אידיאל מקסימלי -

$$\mathfrak{m} = \{x\in\mathcal{O} \mid x^{-1}\notin\mathcal{O}\} = \mathcal{O}-\mathcal{O}^\times$$

צריך להוכיח שהוא אידיאל. ברור שיש סגירות לכפל (כפל של משהו עם הפיך אינו הפיך). לגבי סגירות לחיבור, אם $x,y\in\mathfrak{m}$, מהתכונות של $\mathcal{O}$, $x/y\in\mathcal{O}$ או $y/x\in\mathcal{O}$, ובה"כ $x/y\in\mathcal{O}$. ואז,

$$x+y = \underbrace{\left(1+\frac{x}{y}\right)}_{\in\mathcal{O}}\underbrace{y}_{\in\mathfrak{m}} \in\mathfrak{m}$$

טענה: אם $\mathcal{O}\subseteq K$ חוג הערכה, אז קיימת הערכה v על K כך ש- $\mathcal{O}=\mathcal{O}_v$.

הוכחה: נגדיר $\Gamma=K^*/\mathcal{O}^*$, חבורה כפלית. נגדיר עליה סדר,

$$x\mathcal{O}^* \leq y\mathcal{O}^* \iff \frac{y}{x}\in\mathcal{O}^*$$

זה סדר מלא כי $\mathcal{O}$ חוג הערכה. ההעתקה הטבעית $v:K^*\longrightarrow\Gamma$ היא הערכה אחרי שנגדיר $v(0)=\infty$. הערת תרגיל -

$x\mathcal{O}^* \leq y\mathcal{O}^* \iff \frac{y}{x}\in\mathcal{O}^* \Rightarrow 1+\frac{y}{x}\in\mathcal{O}^*$. ואז,

$$x\mathcal{O}^* \leq (x+y)\mathcal{O}^*$$ ∎

מתי שתי הערכות הן שקולות? אמ"מ $\mathcal{O}_{v_1}=\mathcal{O}_{v_2}$, אם נבחר ש- $v_1\equiv v$ כאשר v ההערכה מהטענה. ואכן, נסמן $\mathcal{O}=\mathcal{O}_{v_1}$ ונחשב -

$$\ker v_1 = \{x\in K^* \mid v_1(x)=0\} = \mathcal{O}^* = \ker v$$

מכאן יש f איזומורפיזם כך שהדיאגרמה תתחלף -

$$\begin{tikzcd} K^* \arrow[r, "v_1"] \arrow[dr, "v"'] & \Gamma_{v_1} \arrow[d, dashed, "f"] \\ & \Gamma \end{tikzcd}$$

סדר נשמר כי מחלקות לא שליליות

שכן, $\Gamma_{v_1},\Gamma \cong K^*/\ker v$. (משפט 1 מלמות על סדר) שקול -

מסקנה: v_1,v_2 שקולות $\iff \mathcal{O}_{v_1}=\mathcal{O}_{v_2}$.

מעכשיו נצמצם להערכה ממשית - הערכה השקולה להערכה עם $\Gamma\subseteq\mathbb{R}$.

הערכה v נקראת דיסקרטית (בדידה) אם $\Gamma_v\cong\mathbb{Z}$.

טענה: $\mathcal{O}$ הוא ראשי $\iff \mathcal{O}=\mathcal{O}_v$, v הערכה בדידה.

הוכחה: בלה אחרי שנכיר בהגדרה. [אם $v(x)=100$, $v(\pi)=1$, אזי $v(x\pi^{-100})=0$

ולכן $x\cdot\pi^{-100}$ הפיך $\Rightarrow (x)=(\pi^{100})$ ....] □

ערכים מוחלטים

הגדרה: ערך מוחלט על K זה פונקציה $|\cdot|:K\to\mathbb{R}$ כך ש-

(1) $|xy|=|x|\cdot|y|$

(2) $|x+y|\le|x|+|y|$

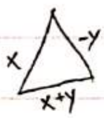
(3) $|x|\ge0$, $|x|=0\iff x=0$

ערך מוחלט נקרא טריוויאלי אם $|x|=1$ לכל $x\neq0$ (והוא משרה כמעט את הטופולוגיה הטריוויאלית).

נאמר ש-$|\cdot|$ הוא לא ארכימדי או אולטרה מטרי אם במקום (2) מתקיים התנאי החזק יותר,

(2') - $|x+y|\le\max\{|x|,|y|\}$

זה אומר שכל משולש הוא שווה שוקיים -



אם $|x|\neq|y|$ אזי $|x+y|=\max\{|x|,|y|\}$.

אם לא לוקחים בחשבון את הע"מ שאינם לא ארכימדיים, דברים פחות טובים קורים.

$\zeta(s)\neq\zeta(1-s)$ כי לא לוקחים בחשבון את הגורמים שלא סופיים. אם מוסיפים את הגורם ב-∞ נקבל $\xi(s)=\xi(1-s)$. לכן צ"ל לקחת בחשבון את הע"מ גם ב-∞ וגם הסופיים.

שני ע"מ שקולים אם הם מגדירים אותה טופולוגיה; וזה קורה אמ"מ לכל $x\in K$, $|x|_1<1\iff|x|_2<1$.

טענה: יהיו $|\cdot|_1,|\cdot|_2$ שני ע"מ שקולים. אז קיים $a\in\mathbb{R}^+$ כך ש- $|x|_1=|x|_2^a$ לכל x.

הוכחה: ניקח $y\in K$ כך ש- $|y|_1>1$ (יש כי $|\cdot|_1$ לא טריוויאלי). נגדיר -

$$a=\log|y|_2/\log|y|_1>0$$

כי הם שקולים - אזי הסימנים שלהם שווים

ניקח $x\in K^*$. יש $b\in\mathbb{R}$ כך ש- $|x|_1=|y|_1^b$. נבחר $b<m_i/n_i$ סדרת רציונליים שמתכנסת ל-b ($n_i>0$, $1=\gcd(m_i,n_i)$, $m_i,n_i\in\mathbb{Z}$). אז כך -

$$|x|_1=|y|_1^b<|y|_1^{m_i/n_i}$$

$$\Rightarrow \left|\frac{x^{n_i}}{y^{m_i}}\right|_1<1$$

ומכאן, משיקולי הערכים המתאימים,

$$\left|\frac{x^{n_i}}{y^{m_i}}\right|_2 < 1$$

ולכן, $|x|_2 < |y|_2^{\frac{m_i}{n_i}}$. נקבל, בלקיחת גבול,

$$|x|_2 \le |y|_2^b$$

בדומה בלקיחת $\frac{m_i}{n_i} < b$ נקבל,

$$|x_2| \ge |y|_2^b$$

לכן $|x|_2 = |y|_2^b$. ואז,

$$|x|_2 = |y|_2^b = |y|_1^{ab} = |x|_1^a \qquad \square$$