הרצאה 7

יהי n טבעי. מתבוננים בשדה הציקלוטומי $L_n=\mathbb{Q}(\zeta_n)$ כאשר ζ_n שורש n-י פרימיטיבי של 1. הצמודים של ζ_n הן השורשים ה-n-יים הפרימיטיביים האחרים של 1, כלומר ζ_n^c, $c\in(\mathbb{Z}/n\mathbb{Z})^*$. בפעם שעברה ראינו:

אם $n=p^a$, אזי $p\mathcal{O}_{L_n}=P^{\varphi(n)}$, $P=(1-\zeta_n)\mathcal{O}_{L_n}$

כלומר p מסועף לגמרי

$L_n/\mathbb{Q}$ הרחבת גלואה $\Rightarrow$ $[L_n:\mathbb{Q}]=\varphi(n)=efr$

במקרה הזה: $e=\varphi(n)$

$f=r=1$

מטרות היום: 1) אם $n=p^a$, אזי

$d_{L_n}=$ (חזקה גדולה של p)

2) לכל n טבעי, $\mathcal{O}_{L_n}=\mathbb{Z}[\zeta_n]$

לכן, $1,\zeta_n,\zeta_n^2,\dots,\zeta_n^{\varphi(n)-1}$

הינו בסיס שלם.

<u>טענה</u>: יהי $n=\prod_p p^{a_p}$ (ו-$a_p=0$ עבור "כמעט כל" הראשוני, כלומר כל p חוץ ממספר סופי של הראשוניים)

לכל p, יהי f_p הטבעי המינימלי כך ש: $p^{f_p}\equiv 1 \mod \frac{n}{p^{a_p}}$. ו-$(p,\frac{n}{p^{a_p}})=1$, לכן

אזי: $f_p = o([p])_{U_{\frac{n}{p^{a_p}}}}$ ← סדר של $[p]$ בחבורת אוילר

$$p\mathcal{O}_{L_n} = (P_1P_2\cdots P_r)^{\varphi(p^{a_p})}$$

כלומר $f_p=f$ מעלת ההתמדה.

$$\varphi(p^{a_p})=e$$

לכן: $r=\frac{\varphi(n)}{ef}=\frac{\varphi(n)}{\varphi(p^{a})f_p}$.

<u>משים לב</u>: אם $n=p^a$, אזי הסדר של p ב-$U_1=\{e\}$ - הינו $1 \Leftarrow f_p=1$.

$$e=\varphi(p^a)=\varphi(n)$$

$$r=\frac{\varphi(n)}{ef}=1$$

לכן הטענה מן הפעם הקודמת הינה מקרה פרטי, אך היה צריך להוכיח אותה בנפרד כדי לקבל את ו.ג.נ"ל שימושיו בהוכחה של הטענה שלנו.

הוכחה מקרה 1 נניח מתפצל, כלומר $a_p=0$. ונזכור כי $O_{L_n}=\mathbb{Z}[\zeta_n]$, ניקח $\theta=\zeta_n$, הפולינום המינימלי הינו $\Phi_n(x)$,

$\underbrace{\Phi_n(x)}_{\text{שורשים: שורשים ה-}n\text{-ים פרימיטיביים}} \mid \underbrace{(x^n-1)}_{\text{שורשים: כל השורשים ה-}n\text{-ים של }1}$.

$f(x)=x^n-1$

$f'(x)=nx^{n-1} \longrightarrow$ בגלל שה מאפיין p, $n\neq 0$,

לכן השורש היחיד של f' הינו 0, לכן אין ל-f,f' שורשים משותפים. לכן, אין ל-f שורשים כפולים.

$$f(x)=(x-a_1)(x-a_2)\cdots(x-a_m)$$

$$f'(x)=\sum_{i=1}^{m}(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_m)$$

לכן השדה $l=O_{L_n}/p$, כאשר $P|p$ הראשוני, מכיל n שורשי יחידה n-ים שונים.

לכן, הוא מכיל את המחלקות ζ_n^b+p לכל b, אחרי לפולינום $f(x)=x^n-1$ יש n שורשים ב-l, אין אולי עם ריבוי.

הראינו שהם כולם <u>שונים</u>.

השדה הסופי ממאפיין p הכי קטן שמכיל n שורשים $\mathbb{F}_{p^f}$

n-יים הינו: ה-f הכי קטן כך ש-:

$$n \mid p^f-1 \iff \mathbb{Z}/n\mathbb{Z} \subseteq \mathbb{Z}/(p^f-1) \simeq \mathbb{F}_{p^f}^*$$

שהוא $f=f_p$. בתוך $\mathbb{F}_p[x]$ הפולינום $\bar{\Phi}_n(x)$

מתפרק ל-

$$\bar{\Phi}_n(x) = \prod \left(\text{פולינומים מינימליים של שורשים } n\text{-יים}\right)$$

פרימיטיביים. כולם

מייצרים את $\mathbb{F}_{p^{f_p}}$ מעל $\mathbb{F}_p$.

לכן $\bar{\Phi}_n = \bar{g}_1 \cdot \bar{g}_2 \cdots \bar{g}_r$

כאשר $\bar{g}_i$ פולינומים זרים ממעלה $[\mathbb{F}_{p^{f_p}}:\mathbb{F}_p]=f_p$.

$e=1=\varphi(p^{a_p})$, כמו שרצינו.

<u>מקרה 2</u> המקרה הכללי, נניח. אזי $n=p^{a_p}m$, $p\nmid m$.

אזי $\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_m)\cdot\mathbb{Q}(\zeta_{p^{a_p}})$

השורשים הפרימיטיביים ה-n-יים של 1 הינם

$\zeta_m^{d}\,\zeta_{p^{a_p}}^{d'}$. $(d,m)=1$, $(d',p^{a_p})=1$

מודולו, p (כלומר $\mathbb{F}_p$)

$$(x^{p^{a_p}}-1) = (x-1)^{p^{a_p}}$$

לכן $\zeta_{p^{a_p}} \equiv 1 \mod p$.

לכן, מעל $\mathcal{O}_{L_n}$:

$$\Phi_n(x) = \prod_{c\in U_n}(x-\zeta_n^c) =$$

$$\prod_{d\in U_m}\prod_{d'\in U_{p^{a_p}}}(x-\zeta_m^{d}\zeta_{p^{a_p}}^{d'})$$

ב-$\mathcal{O}_{L_n}/p\mathcal{O}_{L_n}$:
$$\prod_{d\in U_m}\prod_{d'\in U_{p^{a_p}}}(x-\zeta_m^{d}) = \bar\Phi_m^{\varphi(p^{a_p})}$$

לפי המקרה הקודם: ב-$\mathbb{F}_p[x]$,
$$\bar\Phi_m = \bar g_1\cdots\bar g_r$$

כאשר $e=1$

$f=f_p$ המינימלי כך ש- $p^{f_p}\equiv 1 \mod m=\frac{n}{p^{a_p}}$.

$$\bar\Phi_n = (\bar g_1\cdots\bar g_r)^{\varphi(p^{a_p})}\in\mathbb{F}_p[x].$$

מה שמוכיח את כל הטענה.

שדות מקומיים

הגדרה יהי K שדה. הערכה כפלית על K (= ערך מוחלט) הינה פונקציה $|\cdot| : K \to \mathbb{R}_{\geq 0}$ כך ש-:

1) $|x| = 0 \iff x = 0$.

2) $|xy| = |x|\cdot|y|$ לכל $x,y \in K$.

3) אי-שוויון המשולש: $|x+y| \leq |x| + |y|$ לכל $x,y \in K$.

דוגמאות 1) $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ עם הערך המוחלט הרגיל.

2) K שדה כלשהו,

$$|x| = \begin{cases} 0, & x = 0 \\ 1, & x \neq 0 \end{cases}$$

ההערכה הטריוויאלית.

$p \nmid m', n'$

3) $K = \mathbb{Q}$. p ראשוני

$$0 \neq x = \frac{m}{n} = \frac{p^a m'}{p^b n'} = p^{a-b} \cdot \frac{m'}{n'}$$

$$|x|_p = p^{b-a} = \left(\frac{1}{p}\right)^{a-b}$$ ההערכה ה-p-אדית.

4) הכללה: K שדה מספרים. $\mathfrak{p} \triangleleft O_K$ אידיאל ראשוני לא אפס.

לכל $0 \neq x \in K$, נתבונן בפירוק הראשוני של xO_K.

$(x) = \mathfrak{p}^c I \,, \qquad c \in \mathbb{Z}$

כאשר I הינו אידיאל שברי זר ל-$\mathfrak{p}$.

יהי $q = |\mathcal{O}_K/\mathfrak{p}|$, נגדיר $|x|_{\mathfrak{p}} = \frac{1}{q^c}$.

$|0|_{\mathfrak{p}} = 0$

נראה הערכה: 1) ✓

2) ✓

3) יהיו $x,y \in K$.

$(x) = \mathfrak{p}^c I$

$(y) = \mathfrak{p}^d I$

יהי בלי הגבלת הכלליות $c \le d \Longrightarrow \mathfrak{p}^d \subseteq \mathfrak{p}^c$

$x \in \mathfrak{p}^c, \; y \in \mathfrak{p}^d \subseteq \mathfrak{p}^c$

לכן:

$(x+y) \subseteq \mathfrak{p}^c$

$(x+y) = \mathfrak{p}^c J$ וגם כי J לא זר ל-$\mathfrak{p}$.

לכן: $|x+y|_{\mathfrak{p}} = \frac{1}{q^{\ge c}} \le \frac{1}{q^c} = \max\left\{\frac{1}{q^c}, \frac{1}{q^d}\right\} =$

$\max\{|x|,|y|\} \le |x|+|y|$.

<u>הערה</u> הערכה נקראת לא-ארכימדית אם היא מקיימת את "אי-שוויון המשולש החזק" $|x+y| \le \max\{|x|,|y|\}$.

הערכה $|\cdot|$ על שדה K נותנת ל-K מבנה של מרחב מטרי: $d(x,y)=|x-y|$

$$|1|=1$$
$$|x\cdot 1|=|x|\cdot|1|=|x|$$
$$|-1|^2=|1|=1$$
$$|-1|=1$$

לכן מקבלים טופולוגיה מטרית:
בסיס של קבוצות פתוחות הינו
כדורים $B_\varepsilon(x)=\{y\in K: |x-y|<\varepsilon\}$

<u>הגדרה</u> שתי הערכות שקולות אם הן מגדירות את אותה הטופולוגיה המטרית.

<u>טענה</u> תהיינה $|\cdot|_1, |\cdot|_2$ שתי הערכות על K. הן שקולות אם ורק אם קיים $s>0$ כך ש- $|x|_2=|x|_1^s$ לכל $x\in K$.

<u>הוכחה</u> $(\Rightarrow)$ נניח $|x|_2=|x|_1^s$ לכל x.

ביחס ל-$|\cdot|_2$

$$B^2_\varepsilon(x)=\{y\in K: |y-x|_2<\varepsilon\}=\{y\in K: |y-x|_1<\varepsilon^s\}=B^1_{\varepsilon^s}(x)$$

לשתי ההערכות אותם הכדורים, לכן אותה טופולוגיה.

$(\Leftarrow$ $|x|<1 \iff$ הסדרה $1, x, x^2, x^3, \dots \to 0$

) $\{a_n\} \to L \iff$ לכל קבוצה פתוחה $L \in U$

קיים N כך ש- $a_n \in U$ לכל $n \geq N$

הנורמות הינה תכונה טופולוגית. לכן, אם

$|\cdot|_1, |\cdot|_2$ מגדירות את אותה הטופולוגיה, אזי

$|x|_1 < 1 \iff |x|_2 < 1$.

נוכל להניח כי $|\cdot|_1$ לא-טריוויאלית. אזי קיים $y \in K$

כך ש- $|y|_1 > 1 \iff |\frac{1}{y}|_1 < 1 \iff |\frac{1}{y}|_2 < 1 \iff |y|_2 > 1$.

אז קיים $s > 0$ כך ש- $|y|_2 = |y|_1^s$.

יהי $0 \neq x \in K$. יהי $\alpha \in \mathbb{R}$ כך ש- $|x|_1 = |y|_1^{\alpha}$.

תהי $\frac{m_i}{n_i}$ סדרה יורדת של מספרים רציונליים כך ש- $\frac{m_i}{n_i} \to \alpha$.

$n_i > 0$

$$|x|_1 = |y|_1^{\alpha} < |y|_1^{\frac{m_i}{n_i}}$$

$$|x^{n_i}|_1 < |y|_1^{m_i}$$

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

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

$$|x^{n_i}|_2 < |y^{m_i}|_2$$

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

$$|x|_2 \le |y|_2^{\alpha} \qquad i\to\infty$$

אם ניקח סדרה עולה $\frac{m_i}{n_i}\to\alpha$, נחליף את כל (האי-שוויונות ונקבל)

$$|x|_2 \ge |y|_2^{\alpha} \Rightarrow |x|_2 = |y|_2^{\alpha}$$

לכן:

$$|x|_2 = |y|_2^{\alpha} = |y|_1^{s\alpha} = (|y|_1^{\alpha})^s = |x|_1^s$$

וכאן x היה שרירותי.

<u>הערה</u> השתמשנו רק בעובדה $|x|_1<1 \Rightarrow |x|_2<1$.

לכן מקבלים:

אם $\{x\in K: |x|_2<1\} \supseteq \{x\in K: |x|_1<1\}$, אזי $|\cdot|_1, |\cdot|_2$ שקולות.

<u>טענה</u> תהי $|\cdot|$ הערכה על K. היא לא-ארכימדית (כלומר $|x+y|\le \max\{|x|,|y|\}$) אם ורק אם $|n|\le 1$ לכל $n\in\mathbb{Z}$. (יש הומ' יחיד של חוגים $\mathbb{Z}\to K$, חח"ע $\Leftrightarrow$ $\mathrm{char}\,K=0$)

<u>הוכחה</u> $\Leftarrow$) ברור $n=1+1+\dots+1$.

$\Rightarrow$) יהיו $x,y\in K$. בלי הגבלת הכלליות, $|x|\ge|y|$.

אזי

$$|x+y|^n = |(x+y)^n| = \left|\sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i\right| \le$$

$$\sum_{i=0}^{n} \left|\binom{n}{i}\right| |x|^{n-i}|y|^i \le \sum_{i=0}^{n} |x|^{n-i}|x|^i = (n+1)|x|^n$$

לכן:

$$|x+y| \le \underbrace{(n+1)^{1/n}}_{\to 1} |x|$$

$n \to \infty$

$$|x+y| \le |x| = \max\{|x|, |y|\}$$

<u>משפט</u> (אוסטרובסקי, 1912) אגב $|\cdot|$ הערכה לא-טריוויאלית על $\mathbb{Q}$. אזי היא שקולה ל- $|\cdot|_p$ עבור p, או ל- $|\cdot|_\infty$ (הערך המוחלט הרגיל).

<u>הוכחה</u> <u>מקרה 1</u> $|\cdot|$ לא-ארכימדי. אזי

$\{n \in \mathbb{Z} : |n| < 1\} \triangleleft \mathbb{Z}$ אידיאל ראשוני

לא-אפסי כי $|\cdot|$ לא-טריוויאלי.

לכן $\{n \in \mathbb{Z} : |n| < 1\} = p\mathbb{Z}$

עבור ראשוני p יחיד. $|n| = 1$ אם $n \in \mathbb{Z}$, $p \nmid n$.

$$\mathbb{Q} \ni x = p^c \frac{m'}{n'} \Rightarrow |x| = |p|^c = \left(\frac{1}{p}\right)^{sc} = |x|_p^s$$

כאשר $|p| = \left(\frac{1}{p}\right)^s$, $s > 0$. לכן $|\cdot|$ שקולה ל- $|\cdot|_p$.

<u>מקרה 2</u> $|\cdot|$ ארכימדי. יהיו $m,n\in\mathbb{Z}$ גדולים. מאי-שוויון
המשולש כי $|n|\le|1+\dots+1|\le n$ לכל $n\in\mathbb{N}$.

נפרוס את m בבסיס n:

$$m=a_0+a_1n+\dots+a_rn^r \qquad 0\le a_i<n$$

בפרט $|a_i|\le a_i<n$

$$|m|\le\sum_{i=0}^{r}|a_in^i|<\sum_{i=0}^{r}n|n|^r$$

$$r\le\log_n m=\frac{\ln m}{\ln n} \qquad =(r+1)n|n|^r$$

$$\le\left(1+\frac{\ln m}{\ln n}\right)n|n|^{\frac{\ln m}{\ln n}}$$

כל זה נכון אם נחליף את m ב-m^k:

$$|m|^k\le\left(1+\frac{k\ln m}{\ln n}\right)n|n|^{\frac{k\ln m}{\ln n}}$$

שורש k-י:

$$|m|\le\left(1+\frac{k\ln m}{\ln n}\right)^{1/k}n^{1/k}|n|^{\frac{\ln m}{\ln n}}$$

$k\to\infty$:

$$|m|\le|n|^{\frac{\ln m}{\ln n}}$$

$$|m|^{\frac{1}{\ln m}}\le|n|^{\frac{1}{\ln n}}$$

נחליף m,n:

$$|m|^{\frac{1}{\ln m}}=|n|^{\frac{1}{\ln n}}$$

נגדיר $s = \ln |n|^{\frac{1}{\ln n}} = \frac{\ln |n|}{\ln n} = \log_n |n|$

לא תלוי ב-n.

לכן, לכל $n\in\mathbb{N}$, $|n| = n^{\log_n |n|} = n^s = |n|_\infty^s$

ולכן $|x| = |x|_\infty^s$ לכל $x\in\mathbb{Q}$.

<u>הגדרה</u> יהי K שדה עם הערכה. סדרה $\{a_n\}$ $a_n\in K$

נקראת סדרת קושי אם לכל $0<\varepsilon$ קיים N כך

ש: $|a_n-a_m|<\varepsilon$ לכל $N\le m,n$.

האוסף של סדרות קושי הינו חוג R (חיבור וכפל איבר-איבר)

הסדרות <u>האפסיות</u> ($\{a_n\}\to 0 \iff$ לכל ε קיים N כך ש- $|a_n|<\varepsilon$ לכל $N\le n$)

הן אידיאל מקסימלי $I\triangleleft R$. (אכן, R חוג מקומי, I האידיאל המקסימלי היחיד)

אם $\{a_n\}\in R$ סדרת קושי לא אפסית, זה אומר שקיים ε כך ש- $\varepsilon<|a_n|$ עבור n מספיק גדול.

ואז $\left|\frac{1}{a_n}\right|$ גם סדרת קושי; לכן $\{a_n\}\in R^*$.

נסמן $\hat{K} = R/I$ שדה.

<u>טענה</u> תהי $\{a_n\}$ סדרת קושי ב-K. אזי הסדרה $\{|a_n|\}$ הינה סדרה מתכנסת של ממשיים.

<u>הוכחה</u> אכן, לכל ε קיים N כך ש- $|a_n-a_m|<\varepsilon$ עבור $N\le m,n$.

$$|a_n| = |a_m + (a_n - a_m)| < |a_m| + \varepsilon$$

$$|a_m| < |a_n| + \varepsilon$$

$$\big|\,|a_n| - |a_m|\,\big|_{\mathbb{R}} < \varepsilon$$

*ערך מוחלט של $\mathbb{R}$

לכן $|a_n|$ מתכנסת. נגדיר $\|\{a_n\}\| = \lim_{n\to\infty} |a_n|$.

<u>טענה</u> א) זו מגדירה הערכה על $\hat{K}$.

ב) $\hat{K}$ עם ההערכה הנ"ל הינו שדה שלם: לכל סדרת קושי יש גבול ב-$\hat{K}$.

<u>הערה</u> יהי $K=\mathbb{Q}$. אם $|\cdot|_\infty$, אזי $\hat{K}=\mathbb{R}$

אם $|\cdot|_p$, לפי הגדרה $\hat{K} = \mathbb{Q}_p$.

__דוגמא__ 1) הסדרה $1, p, p^2, p^3, \dots$ שואפת ל-0

בהערכה ה-p-אדית $|\cdot|_p$.

שני ממשיים ה"ח "קרובים" אם הם שקולים מודולו חזקה גבוהה של p.

$$\{|x|_p : x \in \mathbb{Q}\} = \{p^c : c \in \mathbb{Z}\} \cup \{0\}$$

לכן כל גבול של סדרה $|a_n|$ גם שייך לקבוצה הנ"ל.