ואת יש צ"ל שם שגי שמ"ר שמסכה אלא $\sigma_{|\cdot|} \cong |\cdot|$. □

הרצאה 9

3/14/19

יהי K שדה, $\mathbb{C} \hookrightarrow K$ שיכון. שם מצוין שכל מורפ σ -

$$\sigma_{|x|} = \sigma_{|x|}$$

אם יש שני שיכונים, $\mathbb{C} \hookrightarrow K$ כך ש- $\sigma z = \tau$ אז $\sigma_{|z|} = \tau_{|z|}$. מהסיבה הזאת הם שקולים.

משפט: יהי K שדה מספרים, עם r שיכונים ממשיים, s צמדים של שיכונים מרוכבים, אז בסימון $\tau_1, \tau_{r+1}, \tau_{r+2}, \ldots, \tau_{r+s}$, ההעתקה -

$$\mathbb{C}^s \times \mathbb{R}^r \ni (x_1, \ldots, x_{r+s}) \longrightarrow K$$

משכנה צמורפיזם רציף של אלגברות,

$$\mathbb{C}^s \times \mathbb{R}^r \simeq \mathbb{R} \otimes_{\mathbb{Q}} K$$

כאשר, $\sigma_{|\cdot|}$ הם כל השיכונים המורכבים (עד כדי, שקילות).

~~[illegible]~~

הערה: יהי $K/\mathbb{Q}$ הרחבה סופית של שדה מספרים, $\mathcal{O}_K/\mathbb{Z}$ כשוויון שלמים, אזי $\mathcal{O}_K \simeq \mathbb{Z}^n$ כחבורות חיבוריות. נשים לב כי $\mathcal{O}_K$ הוא $\mathbb{Z}$ מודול חופשי מדרגה $n = [K : \mathbb{Q}]$.

משפט: תהי $K/\mathbb{Q}$ הרחבה ממשית, $\mathcal{O}_K \ni \beta_1, \ldots, \beta_n$ השלמים של K. אזי $n = [K : \mathbb{Q}]$.

נגדיר $\mathbb{Q} \hookrightarrow \mathbb{R}$ שיכון, $\sigma_{|\cdot|} = |\cdot|_\infty$ ו $\sigma_{|\cdot|} = |\cdot|_p$ אחרת, אזי -

$$1 = \prod_{q \in P(\mathbb{Q}) \cup \{\infty\}} |x|_q$$

נוסחת המכפלה לשדה מספרים K

יהי $\mathcal{O}_K = \mathbb{Z}[\alpha]$, $\mathcal{O}_K/N\# = \mathbb{Z}/n\mathbb{Z} = n$, $|x|_p = p^{-v_p(x)}$, $|x|_\infty = |N_{K/\mathbb{Q}}(x)|$ וקיבלנו כי -

$$\prod_{q \in P(\mathbb{Q}) \cup \{\infty\}} |x|_q = 1$$

כאשר $\sigma : \mathbb{Q} \hookrightarrow \mathbb{R}$ שיכון מטריאלי $|x|_\sigma = |x|_\infty$, ואחרת $|x|_\sigma = |x|_p$, אזי -

$$\prod_{\sigma : K \hookrightarrow \mathbb{C}} |x|_\sigma = |N_{K/\mathbb{Q}}(x)|$$

נוסחת המכפלה לשדה מספרים K

יהי $K/\mathbb{Q}$ שדה מספרים, $\mathcal{O}_K \ni \beta_1, \ldots, \beta_n$ השלמים של K ו $\mathcal{O}_K$ המודול שנוצר ע"י $\beta_1, \ldots, \beta_n$ אזי $\mathcal{O}_K = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n$.

הערה: יהי $\mathcal{O}_K/\mathbb{Z}$ כשוויון שלמים, $\mathcal{O}_K \simeq \mathbb{Z}^n$ כחבורות חיבוריות. נשים לב כי $\mathcal{O}_K$ הוא $\mathbb{Z}$ מודול חופשי מדרגה $n = [K : \mathbb{Q}]$.

תזכורת: יהי $\mathcal{O}_K/\mathbb{Z}$ כשוויון שלמים, $\mathcal{O}_K \ni \beta_1, \ldots, \beta_n$ השלמים של K, אזי $\mathcal{O}_K = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n$.

משפט: יהי $K/\mathbb{Q}$ הרחבה ממשית, $\mathcal{O}_K \ni \beta_1, \ldots, \beta_n$ השלמים של K ו $\mathcal{O}_K$ המודול שנוצר ע"י $\beta_1, \ldots, \beta_n$ אזי $\mathcal{O}_K = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n$.

משפט: יהי $x \neq 0$ מתקיים $\prod_{p \in P(\mathbb{Q})} |x|_p = 1$.

הוכחה: נתחיל ב-

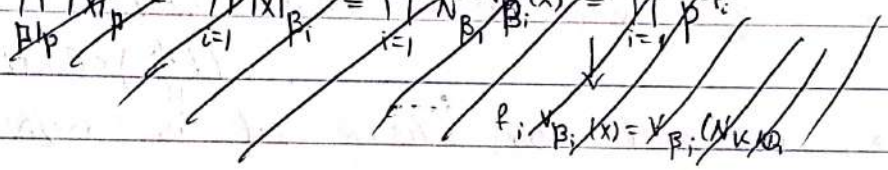
למה: יהי $p \in P(\mathbb{Q})$, יהי $x \in K$, אזי

$$\prod_{\mathfrak{p} \mid p} |x|_{\mathfrak{p}}^{f_{\mathfrak{p}}} = |N_{K/\mathbb{Q}}(x)|_p$$

כעת מוכיח את המשפט, כדלקמן -

$$1 = |N_{K/\mathbb{Q}}(x)|_p = \prod_{p \in P(\mathbb{Q})} \prod_{\mathfrak{p} \mid p} |x|_{\mathfrak{p}}^{f_{\mathfrak{p}}} = \prod_{\mathfrak{p} \in P(K)} |x|_{\mathfrak{p}}$$

לכן כדי להוכיח את המשפט, יהי p מספר ראשוני, $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ האידיאלים הראשוניים המקיימים $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ עבור $e_i \geq 1$.



נשים לב:

$$\exists \text{ ב-} \mathbb{Z} \text{ ב-} p \text{ ו-} \mathcal{O}_K \times \beta_1^{e_1} \cdots \beta_g^{e_g} = p\mathcal{O}_K$$

אז,

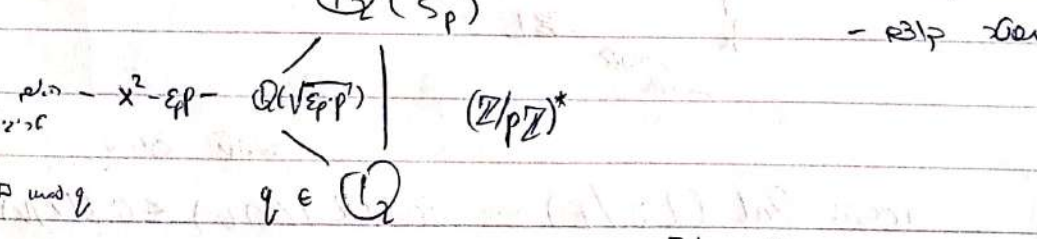
$$|N_{K/\mathbb{Q}}(x)|_p = p^{-\sum_{i=1}^{g} f_i \cdot e_i \cdot v_{\mathfrak{p}_i}(x)} = \prod_{i=1}^{g} |x|_{\mathfrak{p}_i}^{f_i \cdot e_i} = \prod_{\mathfrak{p} \mid p} |x|_{\mathfrak{p}}^{f_{\mathfrak{p}}}$$

יהי p ראשוני, $\sigma_1, \ldots, \sigma_r$ השיכונים השונים של K, $\sigma_{r+1}, \ldots, \sigma_{r+s}$ המרוכבים, עם $r+2s=n$. אזי,

$$|N_{K/\mathbb{Q}}(x)| = \left| \prod_{i=1}^{r+s} \sigma_i(x) \right| = \prod_{i=1}^{r} |\sigma_i x| \cdot \prod_{i=r+1}^{r+s} |\sigma_i x|^2 = \prod_{\mathfrak{p} \mid \infty} |x|_{\mathfrak{p}}$$

הרחבת שדות ראשונית

תזכורת משפט קודם -



$\mathfrak{P}/\mathfrak{p}$ הוא הרחבה נורמלית, אז יש איבר יחיד $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$ שמקיים -

$$\forall x \in \mathcal{O}_{L,\mathfrak{P}} \;.\; \sigma_{\mathfrak{P}} x \equiv x^{|k_{\mathfrak{P}}|} \pmod{\mathfrak{P}}$$

(משמשים בסכמה הבאה לסיומי)

$$1 \longrightarrow I_{\mathfrak{P}/\mathfrak{p}} \longrightarrow D_{\mathfrak{P}/\mathfrak{p}} \longrightarrow G_{\mathfrak{P}/\mathfrak{p}} \longrightarrow 1$$

$$\| \wr$$

$$\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$$

שמו לב שם ב-$\left(\frac{L/K}{\mathfrak{p}}\right)$. הוא שכל הסיומים מהצורה

$$\left\{ \left(\frac{L/K}{\mathfrak{P}}\right) \;\middle|\; \mathfrak{P}|\mathfrak{p} \right\} = \left(\frac{L/K}{\mathfrak{p}}\right)$$

כלומר - **מחלקה** של סיומים (כלומר **מחלקה** צמודות ב-$\mathrm{Gal}(L/K)$) זו **סט** מחלקות.

אם L/K הרחבה גלואה, (כלומר L/K גלואה, $\mathrm{Gal}(L/K)$ אבלית) אז -

מחלקה צמודות $\xleftrightarrow{1-1}$ איברים

$\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$ לכן.

נתייחס הבאה לו לכל הרחבות שמופיעות **בהרחבה כללית**:

נשים I_k את תת-החבורה השכיחה של $\mathcal{O}_L$, השומרת על 0.

אז, I_k - **אבלי** - מסמנים אם כמה $\mathfrak{P}|\mathfrak{p}$. לכן קבוצת סוגי $S \supseteq S_{\mathfrak{p}}$,

נגדיר I_k^S - **תת** חבורה של I_k הנוצרת ע"י S-$\mathfrak{P}$.

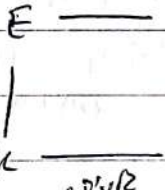
הטענה הבאה **מעניינת** אותנו:

$$\phi_{L/K} : I_k^S \longrightarrow \mathrm{Gal}(L/K)$$

$$\phi_{L/K}(\sigma) = \prod_i \left(\frac{L/K}{\mathfrak{P}_i}\right)^{a_i}$$

$\sigma = \prod \mathfrak{P}_i^{a_i}$

[הוכחה] נראה ש σ **מקיימת** את **התנאים** המופיעים



מכאן שגם,

$$\mathrm{res} : \mathrm{Gal}(L\mathfrak{F}/\mathfrak{F}) \longrightarrow \mathrm{Gal}(L/L\mathfrak{F}\cap K) \trianglelefteq \mathrm{Gal}(L/K)$$

בפרט, $\mathfrak{F}/K$ **אבלי**

אם $S \supseteq S_{\mathfrak{p}}$ **מתקיים**, נגדיר -

$$S(\mathfrak{F}) = \{ \mathfrak{P} \in P(\mathfrak{F}) \mid \mathfrak{P}|_K \in S \}$$

בפרט אם S היא **קבוצת** $\mathfrak{p}$ **הסופיים** ב-$\mathfrak{F}$, (כלומר **הסופיים** ב-K)

את $\mathfrak{F}$ **הראשיים** ב-$\mathfrak{F}$

טענה: $\phi_{E/L} = \phi_{L/K} \circ N_{E/K}$, כלומר $Gal(L/K) = Gal(E/K)/Gal(E/L)$.

הוכחה: יהי $\beta \in O_E$ כך ש-$\beta|_L = \alpha$, $(\beta) = \mathfrak{P}^e \cdot \mathfrak{Q}$, $(\alpha) = \mathfrak{p}^f \cdot \mathfrak{R}$, $f = f(\mathfrak{P}|\mathfrak{p})$. אז $\left(\frac{E/L}{\mathfrak{P}}\right) \in Gal(E/L)$.

נגדיר כעת את σ-

$$\left(\frac{E/L}{\mathfrak{P}}\right)x \equiv x^{N\mathfrak{p}^f} = x^{N\mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}} \pmod{\mathfrak{P}}$$

כלומר, $\mathfrak{P}$ - כלשהו שמעל $\mathfrak{p}$, לכן $x \in O_L$. (כמובן $x \in O_E$).

לכן $\forall x$,

$$\left(\frac{E/L}{\mathfrak{P}}\right)x \equiv x^{N\mathfrak{p}^f} \pmod{\mathfrak{P}}$$

~~מצד שני~~

מצד שני,

$$\left(\frac{L/K}{\mathfrak{p}}\right)x = x^{N\mathfrak{p}} \pmod{\mathfrak{P}}$$

$$\Rightarrow \left(\frac{L/K}{\mathfrak{p}}\right)x = x^{N\mathfrak{p}^f} \pmod{\mathfrak{P}}$$

כיוון ש-f הוא מסדר,

$$\left(\frac{E/L}{\mathfrak{P}}\right) = \left(\frac{E/K}{\mathfrak{P}}\right)^f$$

לפי הגדרת הנורם-שארית וכו'.

~~$\left(\frac{E/L}{\mathfrak{P}}\right) = \left(\frac{L/K}{\mathfrak{p}}\right)^f = \phi_{L/K}(\mathfrak{p})^f = \phi_{E/L}(\mathfrak{P})$~~

$$\phi_{L/K}(\mathfrak{p}) = \left(\frac{L/K}{\mathfrak{p}}\right) = \left(\frac{E/L}{\mathfrak{P}}\right)^f = \phi_{E/L}(\mathfrak{P}) = \phi_{L/K}(N_{E/K}(\mathfrak{P}))$$

41

מכיוון ש-E/L נורמלית, אזי-

$$\mathrm{Id} = \phi_{E/L} = \phi_{L/K} \circ N_{L/K}$$

$$\Rightarrow \boxed{N_{L/K}(I_L^{(S)}) \subseteq \ker \phi_{L/K}}$$

דוגמה: $\zeta_m = e^{\frac{2\pi i}{m}}$, $L = \mathbb{Q}(\zeta_m)$.

$$Gal(L/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^*$$

שכן-

$$\sigma_\alpha : (\mathbb{Z}/m\mathbb{Z})^* \to \sigma_\alpha(\sum \alpha_i \zeta_m^i) = \sum \alpha_i \zeta_m^{i \cdot \alpha}$$

יהי $\frac{a}{b}=\alpha$, $\mathbb{Z}\ni a,b$ כך ש- $a-m$, $m-$

$$\phi_{L/\mathbb{Q}}(\alpha)=\alpha \pmod m$$

$$\downarrow$$

$$\mathbb{Z}\alpha\leftrightarrow\alpha$$

ואז, אם נגדיר S כקבוצה של הראשוניים שמחלקים m, אז

$$\ker\phi_{L/\mathbb{Q}}=\left\{\frac{a}{b}\in I_S^{\mathbb{Q}} \mid a\equiv b \pmod m\right\}$$

כאשר - $I_S=\left\{\frac{a}{b}\mid a,b\in\mathbb{Z}\ \text{ש"ר ל-}S\right\}$.

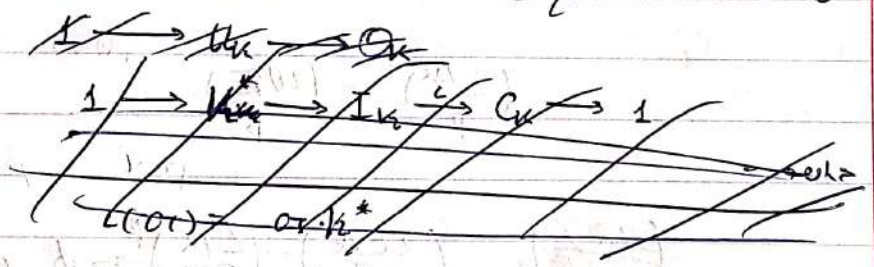
שדה מחלקה ! - ray class group

(מודה מחלקה רחב)

מודולוס - (מספר) המחלקה בלי.

יהי K שדה מספרים, עם חוג שלמים $\mathcal{O}_K$. ניזכר, שמ- $\mathfrak{p}_K$ ו- $\mathfrak{P}_K$ מקיימים, $\mathfrak{P}_K=\mathfrak{p}_K\mathcal{O}_K$. ושמ I_K-הבאים, הינם חבורה חופשית שם שוות $\mathfrak{P}_K$, ושמ $\mathcal{O}_K^*$.

יש סכמה מדהימה -



$$1\longrightarrow\mathcal{O}_K^*\longrightarrow I_K\longrightarrow C_K\longrightarrow 1$$

כאשר -

$$\mathcal{O}_K\ni a\mapsto(a)$$

הגדרה: מודולוס $\mathfrak{m}$ שדה K הוא מכפלה פורמלית -

$$\mathfrak{m}=\prod_{\mathfrak{p}\in M_K^f}\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}\cdot\prod_{\mathfrak{p}\in M_K^\infty}\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}$$

כך ש-

① $v_\mathfrak{p}(\mathfrak{m})$ כך שמספר סופי של $\mathfrak{p}$-ים

② כך ש $\mathfrak{p}$ ממשי, $v_\mathfrak{p}(\mathfrak{m})=0$

③ כך ש $\mathfrak{p}$ מרוכב, $v_\mathfrak{p}(\mathfrak{m})=0$

כאשר נסמן, נגדיר $\mathfrak{m}$ מודולוס ו- $\mathfrak{m}_0$ כי יסמן החלק הסופי של $\mathfrak{m}$,

$$\mathfrak{m}=\mathfrak{m}_0\cdot\mathfrak{m}_\infty$$

$$\mathfrak{m}_\infty=\prod_{\mathfrak{p}\in M_K^\infty}\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}\qquad\mathfrak{m}_0=\prod_{\mathfrak{p}\in M_K^f}\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}$$

חלק ארכימדי — חלק סופי

ע"י הגדרה שפיר p-טוטי. הוכיחו –

$$I_{uv}^{K} =: I_{u}^{K} I_{v}^{K} = I_{uv}$$

ל- u ו-v זרים. נקרא לפונקציה הכפלית S עם ערכים בחוגים שתקיים זאת פונקציה מולטיפלטיבית.

תזכורת יהי K שדה הקלאס מודולו m

$$H_{m}^{K} = \{ x \in K^{*} \mid x \equiv_{m} 1 \}$$

$$\{ 1 = (\sigma_{m}, K_{\mathfrak{O}}) \gcd(x\mathfrak{O}_{K}, \mathfrak{p}_{0}) \mid x \in K^{*} \} = I_{m}^{K} \quad (\text{כלומר } \mathfrak{p} \text{ זר ל- } m)$$

הצעה: יהי m מודולוס. נסמן ב- H_{m}^{K} את חבורת K^{*} –

$$n > (\frac{2}{\pi} - 1) d_{K}$$

$$\exists x \in (\mathfrak{a} - x) d_{K} n$$

יש מספר סופי, עד, $d|\lambda - x|$ מספיק קטן עבור x –

$$\exists \lambda \neq x \quad |\lambda - x| = d|\lambda - x| \leq |d\lambda - dx| < n$$

הוכחה: יהי $\mathfrak{p}$ ראשוני, אז –

טענה: לכל $x \neq \lambda$ ו- $|\lambda - x| < d|\lambda - x|$ מספיק קטן, אז $\lambda \equiv_{\mathfrak{p}^{n}} x$. ($n = 1$ יהי $\mathfrak{p}$ ראשוני)

[כי אחרת $|\lambda - x| \geq \varepsilon$, כך ש- $\varepsilon > d|\lambda - x|$ ⇐]

תכונות בסיסיות: $m \mid n \Rightarrow H_{n}^{K} \leq H_{m}^{K}$, $m \mid n \Rightarrow I_{n}^{K} \leq I_{m}^{K}$

כלל $m \mid \mathfrak{p}$.

יהי –

$$\lambda \equiv_{m} x \quad \text{לכל } \mathfrak{p} \text{ זר } m$$

באופן כללי,

$$\lambda \equiv_{\mathfrak{p}^{n}} x \iff (\mathfrak{p}^{n} \mathfrak{O}_{K} \mid \lambda - x)$$

אז,

אם נשים לב ש- $\mathfrak{p}^{n} \mathfrak{O}_{K} = \mathfrak{p}^{n} \mathfrak{O}_{K} \cdot \mathfrak{p}^{1}$ אז $\mathfrak{p}^{n} \mathfrak{O}_{K} \subsetneq \mathfrak{p}^{n+1}$

(זה נובע מהלמה הבאה...)

$$\lambda \equiv_{\mathfrak{p}^{n}} x \iff \frac{\lambda}{x} \equiv_{\mathfrak{p}^{n}} 1 \text{, כלומר } u = (1 - \frac{\lambda}{x}) \in \mathfrak{p}^{n}.$$

אם $\mathfrak{p}$ ראשוני, $n \in \mathbb{N}$, ו- $x \in \mathbb{Z}$, נגדיר

$$\mathfrak{p} \text{ זר } \lambda - x \iff 0 < \frac{d\lambda}{dx} \text{, כאשר } R = \mathfrak{p}^{n} \mathfrak{O}_{K} \text{ ו-} \mathfrak{p} \text{ זר } dx$$

אם $m = \mathfrak{p}^{n}$, אז נאמר,

$$\lambda \equiv_{m} x \quad (m \text{ מודולו})$$

יהי $\lambda, x \in K^{*}$, נקרא להגדיר –

נקרא להגדיר **שקילות כפלית מודולו** m.

$\varphi : K^* \longrightarrow I_K$

כשאנקמיים אל K_m ו- I_m, נשלח כאלים הומוס מ- I_m ל-

~~[illegible]~~

$$C_K^m = I^m / \varphi(K_m, 1)$$

לפי ה-ISO מקבל -

$$1 \longrightarrow K_{m,1} \longrightarrow I_m \longrightarrow C_K^m \longrightarrow 1$$

למה C_K^m נקראת חבורת המחלקה מקדם.