

הרצאה 3

א שני מספרים, $n = [K:Q]$.

בגניס. הביג הקטני אג קיומה של איגול.

יהי $\sigma_K \neq I \neq 0$ איגול, אפי קיני $|\sigma_K/I| = N(I)$.

אבחיג קני כי $I \neq 0$ אג קיי $\sigma_K \neq I$ כי $\sigma_K \neq I$.

$J = II'$ אפי $J \neq 0 \Leftrightarrow I \neq 0$.

טענה יהי $P \neq 0$ איגול ראשון. אג $e \geq 1$,

$$N(P^e) = (N(P))^e$$

הוכחה σ_K אהום זקני. אכן יש פירוק יחוד

של איגולים אהכלה של איגולים ראשונים.

אכן $P^e \neq P^{e+1}$. יהי $X \in P^e \setminus P^{e+1}$.

אפי $P^e \neq P^{e+1} \supseteq X \sigma_K + P^{e+1} \supseteq P^e$.

אוב, אפי יהיוג הבירוק, $X \sigma_K + P^{e+1} = P^e$.

אבל, מקבלים איזומורפיזם של מרחבים וקטוריים

$$\sigma_K/P \rightarrow P^e/P^{e+1}$$

$$x+P \mapsto x\gamma + P^{e+1}$$

אכן $|P^e/P^{e+1}| = |\sigma_K/P| = N(P)$, וצוים איזומורפיזם e .

$$0 \neq I \triangle \sigma_k$$

יהי גורם ראשוני

$$I = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

כלומר p_1, \dots, p_r גורמים ראשוניים שונים.

$$N(I) = N(p_1)^{e_1} N(p_2)^{e_2} \dots N(p_r)^{e_r}$$

הזוגות האי-זוגיים $p_1^{e_1}, p_2^{e_2}, \dots, p_r^{e_r}$ נוספים

יו-מיון סטטיסטיים בציונים, כלומר gcd הם זוגיים

$$\sigma_k / I \cong \sigma_k / p_1^{e_1} \times \dots \times \sigma_k / p_r^{e_r} \quad \text{היסודיות}$$

$$N(I) = N(p_1^{e_1}) \times \dots \times N(p_r^{e_r})$$

כלומר

$$= N(p_1)^{e_1} \times \dots \times N(p_r)^{e_r}$$

גורם ראשוני יהיה $0 \neq I, J \triangle \sigma_k$, $N(IJ) = N(I)N(J)$

גורם ראשוני יהיה $0 \neq P \triangle \sigma_k$, כלומר gcd נוספים

$$1 \leq f \leq n = [k:\mathbb{Q}], \text{ כלומר } N(P) = p^f$$

$$P \cap \mathbb{Z} = p\mathbb{Z}$$

הוכחה ע"י האינדיקטור σ_k/p בסה"כ σ_k/p שזה, נחשב
 ויקטור אחד σ_k/p , σ_k/p שזה סוגי ממילין ק.
 האינדיקטור בגוף \mathbb{F}_p

$$\sigma_k = \sum_{i=1}^n \alpha_i$$

$$\frac{\sigma_k}{p\sigma_k} = \sum_{i=1}^n \frac{\alpha_i}{p\sigma_k}$$

$$N(p\sigma_k) = p^n$$

$$N(p) | p^n \Leftrightarrow p | p\sigma_k$$

אבחנה (גורמים בוג) יהי $\alpha \in \sigma_k$. $N(\alpha\sigma_k) = |N_{K/Q}(\alpha)|$. האינדיקטור $N(\alpha\sigma_k)$

גורמים: יהי A גורם זניק

$$\mathcal{I}_A = \left\{ \begin{array}{l} \text{חבורה אבליה של איטלים} \\ \text{שבריים, גורם נכס איטלים} \end{array} \right\}$$

איטל $\rightarrow \underline{a} = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, $e_1, \dots, e_r \in \mathbb{Z}$
 שבר p_1, \dots, p_r האיטלים

$$\mathcal{I}_A \supseteq P_A = \left\{ \begin{array}{l} \text{איטלים שבריים (איטלים)} \\ x \in A, \quad x \in \text{Frac } A \end{array} \right\}$$

חבורה המתחלקת: $Cl_A = \mathbb{Z}_A / P_A$

אלו $A = \sigma_k$, נוסחן $Cl_{\sigma_k} = Cl_k$. רוצים

להוכיח כי Cl_k הינה חבורה סוביי.

לענה יהי $M > 0$. יש זין מספר סוביי של

אייגנליים $\sigma_k \Delta I \neq 0$ כך $e \in N(I) \subseteq M$.

הוכחה יהי I איגול עם $N(I) \subseteq M$.

$$I = p_1^{e_1} \dots p_r^{e_r}$$

$$N(I) = N(p_1)^{e_1} \dots N(p_r)^{e_r}$$

נאמר נל $N(p_i)$ חזקה של האינרס. אבל

יש זין מספר סוביי של האינרס $M \geq p$. אבל

p נטה יש מספר סוביי של איגנליים האינרס

$$P \Delta \sigma_k \text{ כך } e \in N(I) \Leftrightarrow P | p \sigma_k \text{ חזקה של } p.$$

אנחנו רוצים להוכיח שיש מספרים k , שקיים מספר $M \in \mathbb{N}$ גלוי ו- k , עם הגיונה הבאה:

כאשר $\exists \sigma_k \in I \neq 0$ קיים איבר $\gamma \in I \neq 0$ כך

$$|N_{k/\mathbb{Q}}(\gamma)| \leq M \cdot N(I) - \epsilon$$

מכאן יש קונו אג הסופי של \mathcal{O}_k ?

אכן, זהו $\mathcal{O}_k \in \mathbb{C}$. נבחר $\gamma \in I^{-1}$.
 אם האגרה הנייט, קיים $\sigma_k \in I \neq 0$ כך ϵ .

$$N(\gamma \sigma_k) = |N_{k/\mathbb{Q}}(\gamma)| \leq N(I) \cdot M.$$

אם $\gamma \sigma_k \in I$ אז $\sigma_k \in I$ ו- $\gamma \in I^{-1}$.
 אך $\sigma_k \in I$ אינו אדם. $\sigma_k \in I$ אינו אדם. $\sigma_k \in I$ אינו אדם.
 כך $\exists \sigma_k \in I$ - ϵ .

ברור כי $\exists \sigma_k \in \mathbb{C}$, כי האגרה האגרה האגרה.
 אם $N(I) = \frac{N(\gamma \sigma_k)}{N(I)} \leq M$, יש וק מספר סופי של
 אפשרויות $\sigma_k \in I$.

כספן מספר סופי של איברים של \mathcal{O}_K .

הערה בחוקי נז'ינג $\exists \epsilon \in \mathcal{O}_K^{-1}$ שהוא איגול של ϵ .

אכן, יהי $\underline{a} \in \mathcal{O}_K^{-1}$ איגול עבורו, אולי

$$\underline{a} = \frac{a_1}{b_1} \sigma_{1K} + \dots + \frac{a_r}{b_r} \sigma_{rK}, \quad a_i, b_i \in \mathcal{O}_K$$

אולי $(\underbrace{b_1 b_2 \dots b_r}_{\text{מכונה}} \sigma_{iK}) \cdot \underline{a}$ הינו איגול של ϵ

ועליון שייך למחלקה \mathcal{O}_K^{-1} .

אולי יהי K שגו מספרים, $n = [K:\mathbb{Q}]$, $K = \mathbb{Q}(\theta)$

יש n שינויים $K \hookrightarrow \mathbb{C}$.

יהיו $\sigma_1, \sigma_2, \dots, \sigma_r : K \hookrightarrow \mathbb{R}$

$\tau_1, \bar{\tau}_1, \tau_2, \bar{\tau}_2, \dots, \tau_s, \bar{\tau}_s : K \hookrightarrow \mathbb{C}$

שינויים של שינויים לא ממשיים $\bar{\tau}_i = \sum_{\sigma \in \text{הכללה}} \tau_i$

$$n = r + 2s$$

$$K = \mathbb{Q}(\sqrt[3]{2}) \quad \underline{\text{Lernzettel}}$$

אנחנו יודעים

אנחנו יודעים

$$\sqrt[3]{2} \mapsto \sqrt[3]{2}$$

$$L = 1$$

$$\zeta_3 = e^{2\pi i/3}$$

$$\sqrt[3]{2} \mapsto \sqrt[3]{2} \cdot \zeta_3$$

$$= -\frac{1}{2} + i \frac{\sqrt{3}}{2}$$

$$\mapsto \sqrt[3]{2} \cdot \zeta_3^2 = \sqrt[3]{2} \cdot \overline{\zeta_3}$$

$$s = 1$$

$$L: K \rightarrow \mathbb{R}^n$$

רצף

$$L(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \operatorname{Re} \tau_1(\alpha), \operatorname{Im} \tau_1(\alpha), \dots, \operatorname{Re} \tau_s(\alpha), \operatorname{Im} \tau_s(\alpha))$$

$$\beta_1, \dots, \beta_n \in I \quad \text{אנחנו יודעים} \quad 0 \neq I \triangleleft \mathcal{O}_K \quad \text{אנחנו יודעים}$$

$$I = \mathbb{Z}\beta_1 + \dots + \mathbb{Z}\beta_n \quad \text{אנחנו יודעים}$$

$$\Gamma = L(I) = \mathbb{Z} \cdot L(\beta_1) + \dots + \mathbb{Z} \cdot L(\beta_n)$$

\mathbb{R}^n - אנו יודעים

הנפח של התא של σ הוא $\text{vol}(\Gamma)$

$$\text{vol}(\Gamma) = \left| \det \begin{pmatrix} \mathcal{L}(\beta_1) \\ \vdots \\ \mathcal{L}(\beta_n) \end{pmatrix} \right|$$

B

התא של σ הוא $\mathcal{L}(\beta_i) \in \mathbb{R}^n$

ה' $\alpha_1, \dots, \alpha_n \in \sigma_K$ הם בסיס

$$\sigma_K = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n$$

$$\beta_i = \sum_{j=1}^n c_{ij} \alpha_j \quad \text{כאשר } c_{ij} \in \mathbb{Z} \quad \text{ה'}$$

$$\mathcal{L}(\beta_i) = \sum_j c_{ij} \mathcal{L}(\alpha_j) \quad \text{כאשר}$$

$$\text{כאשר } A = \begin{pmatrix} \mathcal{L}(\alpha_1) \\ \vdots \\ \mathcal{L}(\alpha_n) \end{pmatrix} \quad \text{ה'}$$

$$B = C \cdot A^T$$

" c_{ij} "

$$|\det C| = \omega(I)$$

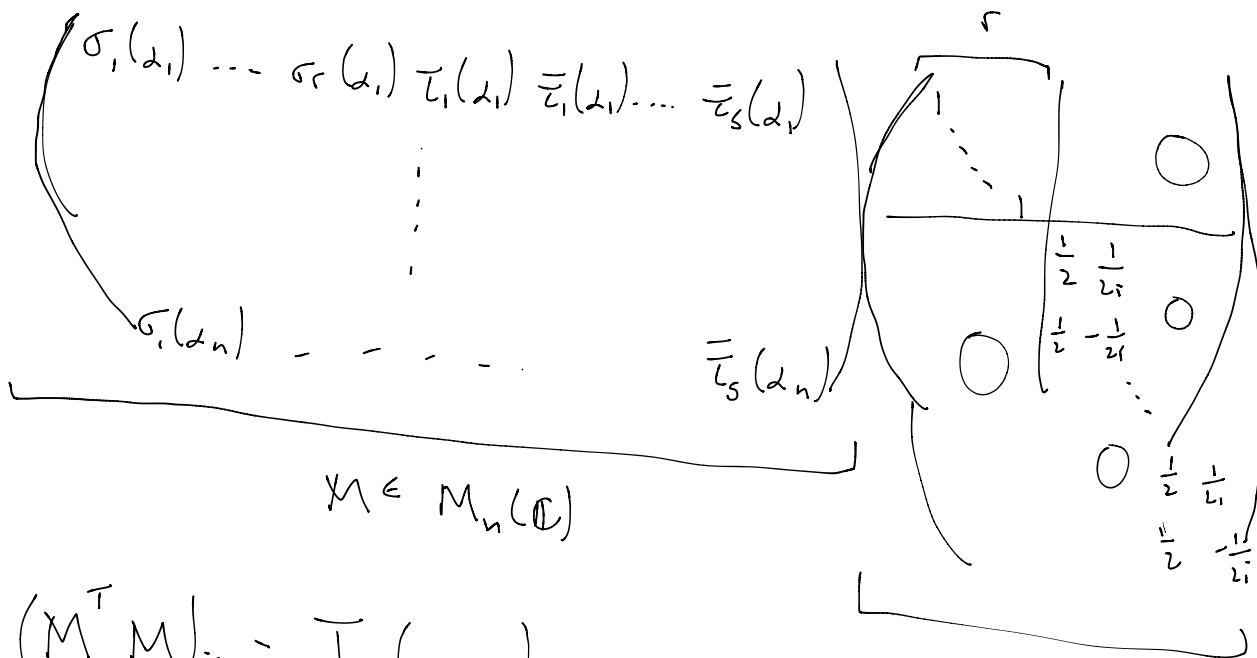
כאשר ω היא הנורמה

$$|\det B| = |\det A| \cdot \omega(I)$$

כאשר ω

$$A = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} =$$

יש לה ω



$$(M^T M)_{ij} = \prod_{k=1}^r \alpha_i \alpha_j$$

$$(\det M)^2 = d_k$$

כאשר d_k היא הנורמה של α_i

$$|\det M| = \sqrt{|d_k|}$$

$$\text{vol}(\Gamma) = |\det B| = \frac{1}{2^s} \cdot \sqrt{|\det A|} \cdot \mathcal{N}(I) \quad \text{כדי}$$

$$X_t \in \mathbb{R}^n \quad \text{יציב, } t > 0 \text{ יציב}$$

$$X_t = \{(x_1, \dots, x_r, y_{11}, y_{12}, \dots, y_{s1}, y_{s2}) \in \mathbb{R}^n :$$

$$|x_1| + \dots + |x_r| + 2\sqrt{y_{11}^2 + y_{12}^2} + \dots + 2\sqrt{y_{s1}^2 + y_{s2}^2} < t\}$$

$$\text{vol}(X_t) = \frac{2^{r-s} \pi^s t^n}{n!} \quad \text{כדי}$$

$$\forall \varepsilon > 0, \exists t > 0 \text{ כזה ש-}$$

$$2^n \text{vol}(\Gamma) < \text{vol}(X_t) < 2^n \text{vol}(\Gamma) + \varepsilon$$

כל נקודה $\gamma \in \Gamma$ (כל נקודה) $\gamma \in X_t$ כזה ש-
 $\Gamma = \cup(I), \quad \gamma = \cup(\gamma)$

$0 \neq y \in I$ irrat

$$|N_{\kappa/\mathbb{Q}}(y)|^{\frac{1}{n}} = |\sigma_1(y) \cdots \sigma_r(y) \tau_1(y) \bar{\tau}_1(y) \cdots \tau_s(y) \bar{\tau}_s(y)|^{\frac{1}{n}} \leq_{\text{AM-GM}} \frac{1}{n} (|\sigma_1(y)| + \cdots + |\bar{\tau}_s(y)|)$$

$$\frac{1}{n} (|\sigma_1(y)| + \cdots + \sigma_r(y) + 2 \sqrt{(\operatorname{Re} \tau_1(y))^2 + (\operatorname{Im} \tau_1(y))^2} + \cdots) < \frac{t}{n}$$

\uparrow
 $(y) \in X_t$

$$|N_{\kappa/\mathbb{Q}}(y)| < \frac{t^n}{n^n}$$

$\therefore \exists \delta$

$\prod_{j=1}^n \int_{\delta}^1 \dots$

$$\operatorname{vol}(X_t) < 2^n \operatorname{vol}(\Gamma) + \varepsilon$$

$$\frac{2^{r-s} \pi^s t^n}{n!} < 2^{r+s} \sqrt{|d_\kappa|} N(I) + \varepsilon$$

$$|N_{K/\mathbb{Q}}(\gamma)| \leq \frac{t^n}{n^n} < \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|} N(I) + \frac{\varepsilon n! \sqrt{|d_K|}}{2^{r-s} \pi^s n^n}$$

$\gamma \in \mathcal{O}_K$, $\varepsilon > 0$, $\varepsilon \rightarrow 0$ כפי שרואים
 $N_{K/\mathbb{Q}}(\gamma) \in \mathbb{Z}$

לכן, קיים $0 \neq \gamma \in I$ כך $|\gamma| < \varepsilon$

$$|N_{K/\mathbb{Q}}(\gamma)| \leq \underbrace{\frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}}_{M} \cdot N(I)$$

$M =$
 מספר מניין קטן

כבר ראינו שזה קורה אם \mathcal{O}_K אינו גורם של \mathcal{O}_K .

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}], \quad K = \mathbb{Q}(\sqrt{-1}) \quad \text{Baby Example}$$

אנחנו יודעים מהתנייה כי \mathcal{O}_K גורם של \mathcal{O}_K אם \mathcal{O}_K אינו גורם של \mathcal{O}_K .
 גורם ראשוני, לכן \mathcal{O}_K אינו גורם של \mathcal{O}_K .

כאן נציג את ההסתברות של קייבנסקי

$$M = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$$

$$K = \mathbb{Q}(\sqrt{-1})$$

$$n = 2$$

$$r = 0, s = 1$$

התבטא את d כפונקציה של d $K = \mathbb{Q}(\sqrt{d})$, $d_K = -4$

$$d_K \equiv \begin{cases} d, & d \equiv 1 \pmod{4} \\ 4d, & d \equiv 2, 3 \pmod{4} \end{cases}$$

$$M = \frac{2!}{2^2} \cdot \left(\frac{4}{\pi}\right) \cdot \sqrt{4} = \frac{4}{\pi} < 2$$

כדי לבדוק את ההסתברות של קייבנסקי

$$I = \mathcal{O}_K = \mathbb{Z} \Leftrightarrow N(I) = 1 \Leftrightarrow N(I) \leq M < 2 \text{ ו} I$$

$$1 - \mathcal{O}_K$$

הוא

$$\Leftrightarrow \mathcal{O}_K = \{e\} \Leftrightarrow \text{יש רק אחד מהסתברות}$$

$$\mathcal{O}_K \text{ גורם להאט}$$

משפט זירינקה של הית'ווג

σ_K מונג אל נמה σ_K למה גחום (א/א)!

החבורה σ_K^* של איברים הפיניג של σ_K

מונג אל ההבול בין איברים של σ_K ואיגלוים (אליים של σ_K)

בהינתן שיה מספרים K , יהי

$$\mu(K) = \left\{ \alpha \in K, \begin{matrix} \alpha^n = 1 \\ \alpha \neq -1 \end{matrix} \right\} \subseteq K^*$$

↑
גחיה סוביג

משפט (זירינקה) יהי K שיה מספרים, r, s

$$\sigma_K^* \cong \mu(K) \times \mathbb{Z}^{r+s-1}$$

נתיים אליו

$$\sigma_K^* = \mathbb{Z}^* = \mu(\mathbb{Q}) = \{\pm 1\} \quad \begin{matrix} r=1 & K=\mathbb{Q} \\ s=0 & \end{matrix} \quad \underline{\text{12/11}}$$

כך נקבע $\sigma_1, \dots, \sigma_r, \tau_1, \dots, \tau_s$ "ה"

$$\theta: K \rightarrow \underbrace{\mathbb{R}^r \times \mathbb{C}^s}_{\text{ז"נ}} = W$$

$$\theta(\alpha) = (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \tau_1(\alpha), \dots, \tau_s(\alpha))$$

$$w = (w_1, \dots, w_r, w'_1, \dots, w'_s)$$

כך נקבע $w \in W$

$$N(w) = w_1 w_2 \dots w_r |w'_1|^2 \dots |w'_s|^2$$

$$N(\theta(\alpha)) = N_{K/\mathbb{Q}}(\alpha).$$

$$\bar{\sigma}_K^* = \{ \alpha \in \bar{\sigma}_K : N_{K/\mathbb{Q}}(\alpha) = \pm 1 \}$$

ה"נ

$$G = \{ w \in W : |N(w)| = 1 \}$$

$$U = \theta(\bar{\sigma}_K^*) = \theta(\bar{\sigma}_K) \cap G.$$

$$\theta: \bar{\sigma}_K^* \rightarrow U$$

ה"נ

ה"נ

כך נקבע U

$$W^* = (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \quad \text{לג' 2.1, ה, ג, ד, ה}$$

$$L: W^* \rightarrow \mathbb{R}^{r+s}$$

$$L(x_1, \dots, x_r, y_1, \dots, y_s) = (\log|x_1|, \dots, \log|x_r|, 2\log|y_1|, \dots, 2\log|y_s|)$$

L הוא מורפיזם של חבורות.

$$L(G) = \{(z_1, \dots, z_{r+s}) \in \mathbb{R}^{r+s} : z_1 + z_2 + \dots + z_{r+s} = 0\} = H$$

$$(\ker L) \cap U = \Theta(\mu(K)) \quad \text{למה 1}$$

$$\text{הוכחה} \geq \text{הניבון} \geq \text{ג' 2.1}$$

יש לבדוק

$$\ker L = \{(x_1, \dots, y_s) \in W^*\} = \{\pm 1\}^r \times \underbrace{(\mathbb{S}^1)^s}_{\text{מקבץ היחידה}} \leftarrow \text{קומפקטיות}$$

\mathbb{C}^{-2}

$$G = N^{-1}(\{\pm 1\}) \leftarrow \text{סקינ' כ'}$$

$N: W \rightarrow \mathbb{R}$ הליבה

$$\sigma_k = \sum \alpha_1 + \dots + \sum \alpha_n$$

$$\theta(\sigma_k) = \sum \theta(\alpha_1) + \dots + \sum \theta(\alpha_n)$$

שרינג, דאָסן
סקיור וויסויגט'י

$$U \cap (\ker L) = (\ker L) \cap U \cap \theta(\sigma_k)$$

דאָסן

קוואַדראַט, ערע טאָבי זיסויגט'יג,
דאָסן סאָב'י

יהי m הסדר של החבורה הנכאג. אזי

$$X = U \cap (\ker L) \quad \text{דאָסן}$$

$$x = \theta(\alpha), \quad \alpha \in \sigma_k^*$$

$$x^m = 1 \Rightarrow \alpha^m = 1 \Rightarrow \alpha \in \mu(K).$$

$H \cong \mathbb{R}^{r+s-1}$ דאָסן $L(U)$ היינו שרינג גגיון

הוכחה ברור כי $L(U)$ צה גג-חבורה צוויג

לגורוניה שהיא זיסוקטיג. מספיק, לגורוניה

עכנה $B \subseteq H$ גג-קבוזה רסונה, פגונה, התיגין
 $B \cap L(u)$ סובי, גהי $\alpha \in \sigma_k^*$ נק $-e$

$$L(\theta(\alpha)) \in L(u) \cap B$$

מ- B מסגליב רסנה ער $\sigma_1(\alpha), \dots, \sigma_r(\alpha), \tau_1(\alpha), \dots, \tau_s(\alpha)$

עכני, רסנה ער הרקנה, הרסניקום האובייני
 ער α :

$$(X - \sigma_1(\alpha)) \dots (X - \sigma_r(\alpha)) (X - \tau_1(\alpha)) \dots (X - \tau_s(\alpha))$$

שהוא חקרה ער הרסניקום, הרסניקום ער α , עכני

הרסניקום ג- \neq . עכני יס מסר סובי ער

בולקוניה אובייני אבסוייב. עכני מסר סובי

ער α אבסוייג, עכני

$$B \cap L(u)$$

סובי

דוגמה 3 $L(U)$ ה'יון ע'רין ע'לם $H \rightarrow$

$$L(U) \simeq \mathbb{Z}^{\Gamma+s-1} \quad \text{כ'ן} \quad \text{כ'ן}$$

$$L(U) \simeq U / (\ker L) \cap U$$

$$U \simeq (\ker L) \cap U \times L(U)$$

ג'ו'ן