

$n \times n$ matrix A , $u = \alpha v$, $\alpha \neq 0$ or $u \in \text{span}\{v\}$

$u \in L$ or $u \notin L$, $\alpha \in \mathbb{R}$, $u = \alpha v$

$$x = u + y, u \in L, y \in \text{span}\{v\}$$

$$L \ni u - u = 0 = y \Rightarrow y = 0$$

Basis of L is v_1, \dots, v_{n-1} . $L = \text{span}\{v_1, \dots, v_{n-1}\}$

$$L_0 = L \cap V_0, V_0 = \text{span}\{v_1, \dots, v_{n-1}\}$$

$L_0 = \text{span}\{u_1, \dots, u_{n-1}\}$

$$\lambda = \sum_{i=1}^{n-1} r_i u_i + r_n v_n \in L$$

$$r_i = 0 \text{ for } i=1, \dots, n-1, r_n = 1$$

L is spanned by $u_1, \dots, u_{n-1}, \lambda$

12

V is a vector space over \mathbb{R} , n dimensional, L is a subspace of V .

If $x, y \in X$ then $\frac{x+y}{2} \in X$ and $x \in X$ implies $\frac{x+y}{2} \in X$.

If $x, y \in X$ then $\frac{x+y}{2} \in X$ and $x \in X$ implies $\frac{x+y}{2} \in X$.

If T is a linear transformation, $\text{Vol}(T) \leq \text{Vol}(T)$.

- 732N \Rightarrow $n=r+s$, pd

$$V^* : K \rightarrow \mathbb{R}^r \times \mathbb{C}^s =: V$$

$$V^*(x) = \underbrace{(\sigma_1(x), \dots, \sigma_{r+s}(x))}_{r+s}$$

$$K = \mathbb{Q}(u) \qquad K = \mathbb{Q}(\sqrt{2}) \qquad \text{: 2.12/3}$$

$$V^*(a+bi) = a+bi \in \mathbb{C} \qquad V^*(a+b\sqrt{2}) = (a+b\sqrt{2}, a-b\sqrt{2})$$

: 732)

$$V : K \rightarrow \mathbb{R}^{r+2s}$$

$$V(x) = (\sigma_1(x), \dots, \sigma_r(x), \operatorname{Re} \sigma_{r+1}(x), \operatorname{Im} \sigma_{r+1}(x), \dots)$$

... \mathbb{Q} σ_N , K \in $\sigma_1, \dots, \sigma_n \in K$ \Rightarrow \dots

$$M = \begin{pmatrix} -V(x_1) \\ \vdots \\ -V(x_n) \end{pmatrix}$$

$$D = \begin{pmatrix} \sigma_1(x_i) & \dots & \sigma_r(x_i) & \sigma_{r+1}(x_i) & \overline{\sigma_{r+1}(x_i)} & \dots \end{pmatrix}$$

$$\det M = (-2i)^s \det D$$

... 2 $\sigma_1, \dots, \sigma_n$ \Rightarrow \dots

$$\begin{pmatrix} \operatorname{Re} z \\ \operatorname{Im} z \end{pmatrix} = \underbrace{\begin{pmatrix} 1/2 & 1/2 \\ 1/2i & -1/2i \end{pmatrix}}_{\det (-2i)^{-1}} \begin{pmatrix} z \\ \bar{z} \end{pmatrix}$$

$$\Delta(\mathbb{Q}/\mathbb{Z}) \text{ } \dots \text{ } \Delta(x_1, \dots, x_n) \text{ } \dots \text{ } \Delta(x_1, \dots, x_n) = \det D^2 = (-2i)^s \cdot (\det M)^2$$

$$\Delta(x_1, \dots, x_n) = \det D^2 = (-2i)^s \cdot (\det M)^2$$

$S = O(n, \mathbb{R}) \Leftrightarrow \Delta(x_1, \dots, x_n) \neq 0, \forall \sigma \in S$

$DD^T = [\text{Tr}(x_i x_j)]_{i,j} = \Delta(x_1, \dots, x_n)^2$

$\Rightarrow \Delta(x_1, \dots, x_n) = \det DD^T = \det D^2$

□

□ \Rightarrow $N(\sigma) = \# \frac{O}{\mathbb{R}} = \frac{O}{\mathbb{R}}$

$N(\sigma) = \# \frac{O}{\mathbb{R}} = \frac{O}{\mathbb{R}}$

$\Delta(a/\mathbb{Z}) = N(\sigma)^2 \Delta(O/\mathbb{Z})$

$O = O$ \Rightarrow $\Delta(x_1, \dots, x_n) = \det p_a = [\text{Tr}_{K/Q}(ax_i ax_j)]_{i,j} = p_q [\text{Tr}_{K/Q}(x_i x_j)]_{i,j} p_a^T \Rightarrow$

$\Delta(x_1, \dots, x_n) = \det p_a = [\text{Tr}_{K/Q}(ax_i ax_j)]_{i,j} = p_q [\text{Tr}_{K/Q}(x_i x_j)]_{i,j} p_a^T \Rightarrow$

$\Delta(x_1, \dots, x_n) = \det p_a = [\text{Tr}_{K/Q}(ax_i ax_j)]_{i,j} = p_q [\text{Tr}_{K/Q}(x_i x_j)]_{i,j} p_a^T \Rightarrow$

$\Delta(x_1, \dots, x_n) = \det p_a = [\text{Tr}_{K/Q}(ax_i ax_j)]_{i,j} = p_q [\text{Tr}_{K/Q}(x_i x_j)]_{i,j} p_a^T \Rightarrow$

$\Rightarrow \Delta(ax_1, \dots, ax_n) = \det p_a^2 \Delta(x_1, \dots, x_n) =$

$= N_{K/Q}(a)^2 \Delta(x_1, \dots, x_n)$

□

$\Rightarrow \sqrt{N(\sigma)} \subseteq \mathbb{R}^n$ \Rightarrow $2^{-s} N(\sigma) \Delta(O/\mathbb{Z})^{1/2}$

$\Delta(x_1, \dots, x_n) = \det p_a = [\text{Tr}_{K/Q}(ax_i ax_j)]_{i,j} = p_q [\text{Tr}_{K/Q}(x_i x_j)]_{i,j} p_a^T \Rightarrow$

$\Delta(x_1, \dots, x_n) = \det p_a = [\text{Tr}_{K/Q}(ax_i ax_j)]_{i,j} = p_q [\text{Tr}_{K/Q}(x_i x_j)]_{i,j} p_a^T \Rightarrow$

$\Delta(x_1, \dots, x_n) = \det p_a = [\text{Tr}_{K/Q}(ax_i ax_j)]_{i,j} = p_q [\text{Tr}_{K/Q}(x_i x_j)]_{i,j} p_a^T \Rightarrow$

$\Delta(x_1, \dots, x_n) = \det p_a = [\text{Tr}_{K/Q}(ax_i ax_j)]_{i,j} = p_q [\text{Tr}_{K/Q}(x_i x_j)]_{i,j} p_a^T \Rightarrow$

□

$\text{Vol}(L) = |\det M|$

\Rightarrow $0 \neq a \in \mathbb{Z}$ \Rightarrow $2^{-s} N(\sigma) \Delta(O/\mathbb{Z})^{1/2}$

$|\text{Norm}_{K/Q}(a)| = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s N(\sigma) |\Delta(O/\mathbb{Z})|^{1/2}$

\Rightarrow $\{x_1, \dots, x_n, y_1, \dots, y_s\}$

$X_L = \{x_1, \dots, x_n, y_1, \dots, y_s\} \mid \sum |x_i|^2 + 2 \sum |y_j|^2 = 1\}$

עליון —: ג'ו'ס , ק'נ'ר , X_t ק'נ'ר ז'ר'ז'ו'ן .
 - ג'ו'ן \int ק'נ'ר , ρ ו'ן

$$\text{Vol}(X_t) = 2 \frac{r^{-s}}{n!} \prod^s \varepsilon^n$$

י'ו' ז'ר'ז'ו'ן

$$\text{Vol}(Z) = 2^{-s} \frac{N(\sigma)}{N(\sigma)} |\Delta(O/Z)|^{1/2}$$

$\square \ni \alpha \neq 0, \nu(\alpha) \in X_t$ ו' י'ט' , $\text{Vol}(X_t) > 2^n \text{Vol}(Z)$ - \underline{p}
 (י'ג'ו'ק'ו'ן ג'ו'ע'ו'ן)

$\varepsilon > 0, t = t(\varepsilon) - 0$ ק' $t > 0$ ו'ר'ז'ו'ן

$$\varepsilon^n = \varepsilon + n! \frac{2^{2s}}{\pi^s} \frac{N(\sigma)}{N(\sigma)} |\Delta(O/Z)|^{1/2}$$

$\nu(\alpha) \cap X_t \neq \emptyset$ ו'ו'ן $\nu(\alpha) \in X_t \Rightarrow \alpha = \alpha(\varepsilon)$ ו' $\varepsilon > 0$ ג'ו'ן

$\varepsilon = 0$ ו'ר'ז'ו'ן ק' a ו'ר'ז'ו'ן Z ו'ן ו'ן ו'ן ו'ן ו'ן

י'ט' ז'ר'ז'ו'ן $\varepsilon = 0$ ו'ר'ז'ו'ן $a + a$, $\nu(\alpha) \in X_t$, ו'ר'ז'ו'ן
 $- a$ ו'ן ו'ן

$$\text{Norm}(\alpha) = \prod_{i=1}^r |\sigma_i(\alpha)| \cdot \prod_{i=1}^s (\text{Re}(\sigma_{i+r}(\alpha))^2 + \text{Im}(\sigma_{i+r}(\alpha))^2) \ll$$

$$\leq \prod_{i=1}^r |x_i| \prod_{j=1}^s (z_j^2 + y_j^2) \leq \frac{1}{n^n} (\sum |x_i| + \sum (z_j^2 + y_j^2))^n \leq$$

$$\leq \frac{1}{n^n} \varepsilon^n \leq \frac{n!}{n^n} \cdot \frac{4^s}{\pi^s} \cdot \frac{N(\sigma)}{N(\sigma)} |\Delta(O/Z)|^{1/2}$$

\square

- \rightarrow ק'ו'ן י'ו'

$$C(K) = \frac{\text{Fract. Ideal}}{\text{Principle}}$$

- \rightarrow ו'ן ו'ן ו'ן ו'ן ו'ן ו'ן ו'ן ו'ן
 $\Gamma[0] = \{ \alpha \cdot \alpha \mid \alpha \in K^* \}$

$C(K) \rightarrow$ ו'ן ו'ן ו'ן ו'ן ו'ן ו'ן ו'ן ו'ן
 (י'ג'ו'ק'ו'ן ק'ו'ן) : ג'ו'ע'ו'ן

- \rightarrow ק' $\Gamma[0] \ni \alpha$ ו'ר'ז'ו'ן ו'ן ו'ן ו'ן ו'ן ו'ן ו'ן ו'ן

$$N(\alpha) = \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^s |\Delta(O/Z)|^{1/2} = M$$

$K \rightarrow$ ק' - $b \rightarrow$ ו'ן ו'ן

ציון: $C(K)$ - מספר

הציון μ של $C(K)$ הוא $\mu = \prod p_i^{a_i} \cdot \prod q_j^{b_j}$ כאשר $\sum a_i + \sum b_j = n$.
 $\mu \leq M \Leftrightarrow \prod p_i^{a_i} \leq M \Leftrightarrow \sum a_i \log p_i \leq \log M$

הציון μ של $C(K)$ הוא $\mu = \prod p_i^{a_i} \cdot \prod q_j^{b_j}$ כאשר $\sum a_i + \sum b_j = n$.
 נניח $b_1 = b \cdot h^{-1}$ ונניח $a \in \mathcal{O}_K$ אז $[h_1] = [h^{-1}]$ ונניח μ הוא מספר שלם.
 נניח $a = \prod p_i^{a_i} \cdot \prod q_j^{b_j}$ אז μ הוא מספר שלם.

$$|\text{Norm}(a)| \leq |\text{Norm}(h_1)| \cdot \mu$$

\Downarrow

$$|\text{Norm}(a)| \cdot |\text{Norm}(h_1)|^{-1} \leq \mu$$

נניח $[h_1] = [h^{-1}] = [h]$, $a = \prod p_i^{a_i} \cdot h^{-1}$ ונניח μ הוא מספר שלם.

μ $|\text{Norm}(a)| = |\text{Norm}(a h_1^{-1})| = |\text{Norm}(a)| \cdot |\text{Norm}(h_1^{-1})| \leq \mu$

הציון μ של $C(K)$ הוא $\mu = \prod p_i^{a_i} \cdot \prod q_j^{b_j}$ כאשר $\sum a_i + \sum b_j = n$.
 $\mu \leq M \Leftrightarrow \prod p_i^{a_i} \leq M \Leftrightarrow \sum a_i \log p_i \leq \log M$
 $\mu_k := \#C(K)$

הציון μ של $C(K)$ הוא $\mu = \prod p_i^{a_i} \cdot \prod q_j^{b_j}$ כאשר $\sum a_i + \sum b_j = n$.
 $n=3, r=1, s=1, \theta = \sqrt[3]{2}, K = \mathbb{Q}(\theta)$

$$\mu = \frac{3!}{3^3} \cdot \left(\frac{4}{\pi}\right)^1 \cdot \mu(\mathbb{Q}/\mathbb{Z}) \leq \frac{8}{\pi} \approx 2.55 < 4$$

הציון μ של $C(K)$ הוא $\mu = \prod p_i^{a_i} \cdot \prod q_j^{b_j}$ כאשר $\sum a_i + \sum b_j = n$.
 $\mu \leq M \Leftrightarrow \prod p_i^{a_i} \leq M \Leftrightarrow \sum a_i \log p_i \leq \log M$
 $\mu_k := \#C(K)$

הציון μ של $C(K)$ הוא $\mu = \prod p_i^{a_i} \cdot \prod q_j^{b_j}$ כאשר $\sum a_i + \sum b_j = n$.
 $\mu \leq M \Leftrightarrow \prod p_i^{a_i} \leq M \Leftrightarrow \sum a_i \log p_i \leq \log M$
 $\mu_k := \#C(K)$

ע"פ: 502

$$\frac{P}{2} \left| \begin{array}{c} x^2 + 14 \\ x^2 \end{array} \right| \begin{array}{c} \kappa - \beta_2^2 \\ z = \beta_2^2 \end{array}$$

$$3 \left| \begin{array}{c} x^2 - 1 \\ (x+1)(x-1) \end{array} \right| 3 = \beta_2 \cdot \beta_3', \quad f(\beta_2) = f(\beta_3') = 1$$

-62g

$$[\beta_2]^2 = 1$$

$$[\beta_3] = [\beta_3']^{-1}$$

$$\text{פר} \cdot \beta_2 = a + b\sqrt{14} \quad \text{ר"ל}$$

$$a = a^2 + 14b^2$$

$f=1$ פר $z=0$ ←

$$\Downarrow$$

$$b=0, a^2=2$$

2 זכרון $[\beta_2]$ פר. ע"פ β_2 פר
 $a + b\sqrt{14}$ זכרון β_3 פר
 β_3 פר β_2 פר

$$2, 3 \mid a^2 + b^2 \cdot 14$$

פר β_3 פר β_2 פר β_3, β_3' פר

$$2 + \sqrt{14} = \beta_2 \beta_3^2$$

$$4 \text{ זכרון } [\beta_3] \Leftrightarrow 2 \text{ זכרון } [\beta_3]^2 = [\beta_2], \text{ פר}$$

$$[\beta_3] \text{ פר} \quad \mathbb{Z}[\sqrt{14}] \cong \langle \beta_2 \rangle$$

1 < $|\Delta(O/\mathbb{Z})|$ פר, 1 = פר $\mathbb{Z}[\sqrt{14}]$ פר $\mathbb{Z}[\sqrt{14}] \cong \langle \beta_2 \rangle$

הוכחה: פר β_2 פר

$$|\Delta(O/\mathbb{Z})|^{1/2} \geq \frac{n^n}{n!} \left(\frac{4}{\pi}\right)^{n/2} \geq \frac{n^n}{n!} \cdot \left(\frac{4}{\pi}\right)^{n/2} > 1$$

$n = 1, 2, 3, \dots$
 \downarrow
 $5 \leq n$

המשפט: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ הם תת-גופים של \mathbb{C} .
 הפולינום $f(x) = x^4 - x^3 - x^2 - x - 1$ אינו מתפרק לריבועים על \mathbb{Q} .
 (122)

משפט: $S_n = \text{Gal}(x^n - x^{n-1} - 1, \mathbb{Q})$ שיהי, ז"ל n זוגי.

הוכחה: נניח $n=4$. הפולינום $f(x) = x^4 - x^3 - x^2 - x - 1$ אינו מתפרק לריבועים על \mathbb{Q} .
 נגזור $f'(x) = 4x^3 - 3x^2 - 2x - 1$.
 נראה כי $\gcd(f, f') = 1$.
 נניח $\gcd(f, f') = d(x)$. אז $d(x) \mid f(x)$ ו- $d(x) \mid f'(x)$.
 נניח $d(x) = (x - \alpha)^k$. אז $k \leq 4$.
 נגזור $f(x) = (x - \alpha)^k h(x)$. אז $f'(x) = k(x - \alpha)^{k-1} h(x) + (x - \alpha)^k h'(x)$.
 מכאן $(x - \alpha)^k \mid k(x - \alpha)^{k-1} h(x) + (x - \alpha)^k h'(x)$.
 נחלק ב- $(x - \alpha)^{k-1}$ נקבל $(x - \alpha) \mid kh(x) + (x - \alpha)h'(x)$.
 נניח $h(x) = (x - \alpha)^m g(x)$ כאשר $g(\alpha) \neq 0$. אז $h'(x) = m(x - \alpha)^{m-1} g(x) + (x - \alpha)^m g'(x)$.
 נציב ב- $(x - \alpha) \mid kh(x) + (x - \alpha)h'(x)$ נקבל $(x - \alpha) \mid k(x - \alpha)^m g(x) + (x - \alpha)^m g'(x)$.
 נחלק ב- $(x - \alpha)^m$ נקבל $(x - \alpha) \mid kg(x) + (x - \alpha)g'(x)$.
 נניח $g(x) = (x - \alpha)^n$. אז $g'(x) = n(x - \alpha)^{n-1}$.
 נציב ב- $(x - \alpha) \mid kg(x) + (x - \alpha)g'(x)$ נקבל $(x - \alpha) \mid k(x - \alpha)^n + (x - \alpha)^n n$.
 נחלק ב- $(x - \alpha)^n$ נקבל $(x - \alpha) \mid k + n$.
 מכאן $k + n = 0$. אבל $k \geq 1$ ו- $n \geq 0$. לכן $k = n = 0$.
 לכן $d(x) = 1$.
 לכן $f(x)$ אינו מתפרק לריבועים על \mathbb{Q} .

$\gcd(f, f') = 1$

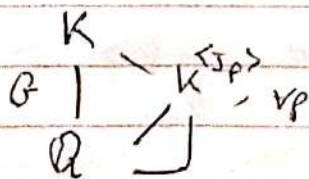
$f' = 4x^3 - 3x^2 - 2x - 1$

$f = x^4 - x^3 - x^2 - x - 1$

אם $\gcd(f, f') = d(x)$ אז $d(x) \mid f(x)$ ו- $d(x) \mid f'(x)$.
 נניח $d(x) = (x - \alpha)^k$. אז $k \leq 4$.

$f = (x - \alpha)^k h(x)$
 כאשר $h(\alpha) \neq 0$.

נניח $h(x) = (x - \alpha)^m g(x)$ כאשר $g(\alpha) \neq 0$.



$G \leq S_n$ - גורם f זוגי.

הוכחה: $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ הם תת-גופים של \mathbb{C} .

For $K = \mathbb{F}_p$, Galois group of $K^{\sqrt{p}} = \mathbb{Q}$ is $G = \langle \sigma \rangle$, where σ is the Frobenius automorphism.

For $K = \mathbb{Q}$, Galois group of $\mathbb{Q}^{\sqrt{p}}$ is $G = S_2$. For $G = S_n$, $n \geq 3$, the Galois group of $\mathbb{Q}^{\sqrt[n]{p}}$ is $G = S_n$.

Let $R = \mathbb{Z}[x]$. For $|R| \geq 2$, the Galois group of $\mathbb{Q}^{\sqrt[n]{p}}$ is $G = S_n$.

For $R = \mathbb{Z}[x]$, the Galois group of $\mathbb{Q}^{\sqrt[n]{p}}$ is $G = S_n$. For $R = \mathbb{Z}[x]$, the Galois group of $\mathbb{Q}^{\sqrt[n]{p}}$ is $G = S_n$.

$$\square \quad \langle S(\mathbb{Z}[x], \tau) \rangle = S(\mathbb{Z}[x], \tau)$$

$$\text{Unit}(O_K) \cong \mu_K \times \mathbb{Z}^{r+s-1}$$

$\left. \begin{array}{l} \text{Units} \\ \text{Gauss} \end{array} \right\}$