Lecture 3:

Last time: $\alpha \in \overline{\mathbb{Q}}$ is an alg int if it is the root of a monic poly in $\mathbb{Z}[x]$.

$\mathcal{O}_K$ = integers in $K/\mathbb{Q}$, a subring

Goal: Thm: $(\mathcal{O}_K, +) \cong \mathbb{Z}^n$ where $n = [\mathbb{Q} : \mathbb{Z}]$

Ex: $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z} \oplus \mathbb{Z}i$, $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z} \oplus \mathbb{Z}\varphi$, $\varphi = \frac{1+\sqrt{5}}{2}$ [Mention correction to HW #1]

Integral basis: $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathcal{O}_K$ so that $\alpha = \sum a_i \alpha_i$, $a_i \in \mathbb{Z}$ for every $\alpha \in \mathcal{O}_K$.

Ex: $K = \mathbb{Q}(\zeta_n)$ with ζ_n = primitive n^{th} root of 1 $(= e^{2\pi i/n})$
$\mathcal{O}_K$ has integral basis $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{d-1}$ where $d = \varphi(n)$.

Why $\mathcal{O}_K$ is large: $\alpha \in K$ a root of $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$
Then $a_n \alpha \in \mathcal{O}_K$ as it is a root of $a_n^{n-1} \cdot f\left(\frac{x}{a_n}\right)$.
So if $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K, there is an $m \in \mathbb{Z}$ so that $\{m\alpha_1, \ldots, m\alpha_n\} \subseteq \mathcal{O}_K$, and so $\mathbb{Z}^n \subseteq \mathcal{O}_K$.
[To prove the thm, need to introduce the discriminant.]

Trace: $tr_{L/K} : L \longrightarrow K$ homomorphism

$$\alpha \longmapsto \sum \sigma_i(\alpha)$$

Bilinear form: $(\alpha, \beta) = tr_{L/K}(\alpha\beta)$
(symmetric)

Discriminant: (K-basis for L)

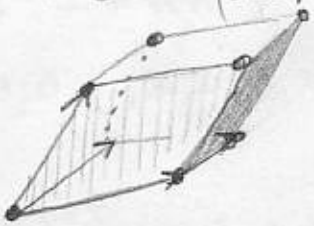
$$\operatorname{disc}(\alpha_1,\dots,\alpha_n) = \det\big(\underbrace{\operatorname{Tr}_{L/K}(\alpha_i\alpha_j)}_{G}\big) = \Big[\det\big(\underbrace{\sigma_i(\alpha_j)}_{A}\big)\Big]^2$$

$\uparrow$ Ex: Use $G = A^tA$.

Reasonableness: $v_1,\dots,v_n$ a basis of $\mathbb{R}^n$ with usual inner product.

$$G = \text{Gram matrix} = (v_i\cdot v_j) = V^tV \quad \text{where } V = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}$$

$$\det G = (\det V)^2 = \left(\begin{array}{c}\text{Volume of parallelopiped spanned} \\ \text{by } v_1,\dots,v_n\end{array}\right)$$



[Allude to geometry of numbers.]

Def: $K/\mathbb{Q}$ a number field. The discriminant of K is

$$\Delta_K = \operatorname{disc}(\text{integral basis of } \mathcal{O}_K)$$

Well-defined (modulo thm) $\vec{\alpha} = (\alpha_1,\dots,\alpha_n)$, $\vec{\beta} = (\beta_1,\dots,\beta_n)$ integral basis for $\mathcal{O}_K$. There is $M \in GL_n(\mathbb{Z})$ so that $\vec{\alpha} = M\vec{\beta}$. Then

$$G_\beta = (\operatorname{Tr}_{L/K}\beta_i\beta_j) = M^t(\operatorname{Tr}_{L/K}\alpha_i\alpha_j)M$$

As $\det M = \det M^t = \pm 1$, we have $\operatorname{disc}(\vec{\alpha}) = \operatorname{disc}(\vec{\beta})$

Ex: $\mathbb{Q}(i)$, integral basis $\{1, i\}$. $G = \operatorname{tr}_{\mathbb{Q}(i)/\mathbb{Q}}\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$

$$\Delta_{\mathbb{Q}(i)} = -4 \quad \left[\begin{array}{l}\text{Relate to} \\ 2 = -i(1+i)^2\end{array}\right] \qquad = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$$

Ex: $K = \mathbb{Q}(\sqrt{2})$, $\mathcal{O}_K \overset{\text{by HW}}{=} \mathbb{Z} \oplus \mathbb{Z}[\sqrt{2}]$

Two embeddings: $K \rightrightarrows \mathbb{R}$ with $\sigma_0 = id$, σ_1

$\sigma_1(a + b\sqrt{2}) = a - b\sqrt{2}$

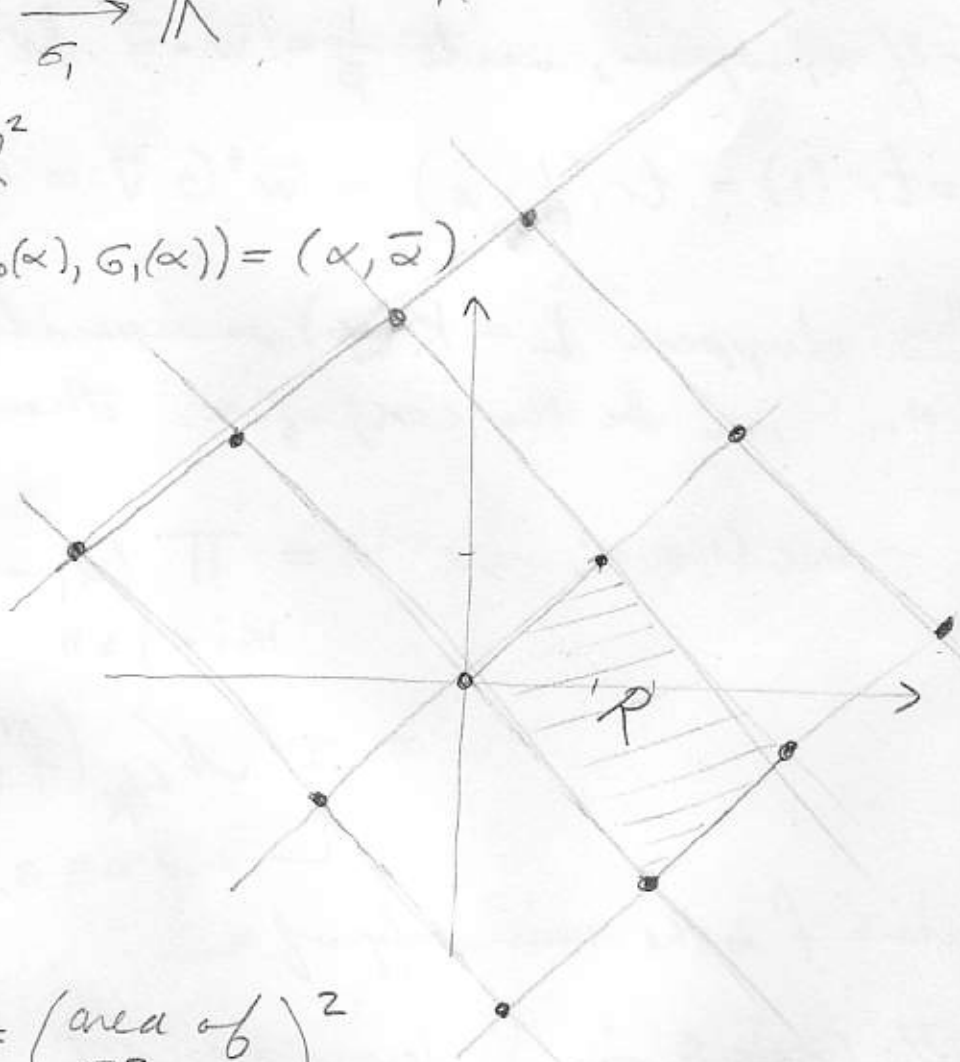
Combine: $K \xrightarrow{f} \mathbb{R}^2$

$\alpha \longmapsto (\sigma_0(\alpha), \sigma_1(\alpha)) = (\alpha, \bar{\alpha})$

$\Lambda = f(\mathcal{O}_K)$

$= \mathbb{Z}$-span of $f(1), f(\sqrt{2})$

embeds $\mathcal{O}_K$ in $\mathbb{R}^2$:



Check:

$(\alpha, \beta) = tr_{K/\mathbb{Q}}(\alpha\beta)$

$= f(\alpha) \cdot f(\beta)$

$\Delta_K = (\text{area of } R)^2 = (\text{area of } \mathbb{R}^2/\Lambda)^2$

$= 8$

Thm: L/K, char $= 0$. For $\alpha_1, \ldots, \alpha_n \in L$, $n = [L : K]$

$disc(\alpha_1, \ldots, \alpha_n) = 0 \iff \alpha_i$ are linearly dependent over K.

Pf: ($\Leftarrow$) if α_i are lin dependent, so are the cols of $(\sigma_i(\alpha_j)) \Rightarrow disc = 0$.