Lectures 21-24: number field; adeles; strong approximation.

Wednesday, November 18, 2015 11:06 AM

- A finite extension k of $\mathbb{Q}$ is called a number field.

Let $\mathcal{O}_k := \{\alpha \in k \mid \alpha$ is integral over $\mathbb{Z}$, $\}$.

i.e. $\exists\, a_i \in \mathbb{Z}$, $\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0 = 0$

Theorem. $\mathcal{O}_k$ is a finitely generated, free $\mathbb{Z}$-module. And

$$\operatorname{rank}_{\mathbb{Z}} \mathcal{O}_k = \dim_{\mathbb{Q}} k.$$

Used without proof: $\alpha, \beta \in \overline{\mathbb{Q}}$ integral over $\mathbb{Z} \Rightarrow \alpha+\beta$ and $\alpha\cdot\beta$ are integral over $\mathbb{Z}$.

Lemma. $\alpha \in \overline{\mathbb{Q}}$ integral over $\mathbb{Z} \Rightarrow$ the minimal polynomial $f(t)$ of α over $\mathbb{Q}$ has integer coefficients.

Proof. Suppose $g(\alpha) = 0$ where $g \in \mathbb{Z}[x]$ is a monic polynomial. Then for any other root α_i of f we have $g(\alpha_i) = 0$ as $f(t) \mid g(t)$. Hence α_i's are integral. Therefore all the coefficients of f are integral over $\mathbb{Z}$. Since $\mathbb{Z}$ is UFD, it is integrally closed, i.e. $x \in \mathbb{Q}$ and x integral over $\mathbb{Z}$ implies $x \in \mathbb{Z}$. Therefore $f \in \mathbb{Z}[t]$. ■

Corollary. $N_{k/\mathbb{Q}}(\mathcal{O}_k) \subseteq \mathbb{Z}$ and $\operatorname{tr}_{k/\mathbb{Q}}(\mathcal{O}_k) \subseteq \mathbb{Z}$.

Lemma $\forall \alpha \in k$, $\exists\, n \in \mathbb{Z} \setminus \{0\}$, $n\alpha \in \mathcal{O}_k$.

Proof. Suppose $\alpha^m + \frac{a_{m-1}}{b}\alpha^{m-1} + \cdots + \frac{a_1}{b}\alpha + \frac{a_0}{b} = 0$ where $a_i, b \in \mathbb{Z}$.

Then $(b\alpha)^m + a_{m-1}(b\alpha)^{m-1} + \cdots + a_1 b^{m-2}(b\alpha) + a_0 b^{m-1} = 0$

$\Rightarrow b\alpha \in \mathcal{O}_k$. ■

Used without proof: $B : k \times k \to \mathbb{Q}$, $B(x,y) := \operatorname{tr}_{k/\mathbb{Q}}(xy)$ is a non-degenerate bilinear form.

Definition. For any $\mathbb{Z}$-submodule M of k, let

Definition. For any $\mathbb{Z}$-submodule M of k, let

$$M^* := \{x \in k \mid B(x, M) \subseteq \mathbb{Z}\}.$$

Lemma ⓞ M^* is a $\mathbb{Z}$-submodule of k.

① $M_1 \subseteq M_2 \Rightarrow M_1^* \supseteq M_2^*$

② Suppose $k = \mathbb{Q}\alpha_1 \oplus \cdots \oplus \mathbb{Q}\alpha_d$, and $M = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_d$.

Then $\exists\, \alpha_i^* \in k$ s.t. $B(\alpha_i^*, \alpha_j) = \delta_{ij}$

(the dual basis with respect to B) and

$$M^* = \mathbb{Z}\alpha_1^* \oplus \cdots \oplus \mathbb{Z}\alpha_d^*.$$

Proof. ⓞ Since B is bilinear, $\forall\, x_1, x_2 \in M^*$,

$$B(x_1 - x_2, M) \subseteq B(x_1, M) - B(x_2, M)$$
$$\subseteq \mathbb{Z} - \mathbb{Z} = \mathbb{Z}.$$

① $x \in M_2^* \Rightarrow B(x, M_2) \subseteq \mathbb{Z}$; $B(x, M_1) \subseteq B(x, M_2)$ $\Rightarrow x \in M_1^*$.

② Let $V_j := \{x \in k \mid 1 \le i \le d,\ i \ne j,\ B(x, \alpha_i) = 0\}$.

$\Rightarrow$ V_j is a non-zero vector space.

Since B is non-degenerate, $B(V_j, \alpha_j) \ne 0$.

Let $\tilde{\alpha}_j \in V_j$ s.t. $B(\tilde{\alpha}_j, \alpha_j) \ne 0$. Let

$$\alpha_j^* := \frac{1}{B(\tilde{\alpha}_j, \alpha_j)}\, \tilde{\alpha}_j.$$

So $B(\alpha_i^*, \alpha_j) = \delta_{ij}$. Therefore

$$B(\oplus \mathbb{Z}\alpha_i^*, \oplus \mathbb{Z}\alpha_j) \subseteq \mathbb{Z},$$

and

$$k = \oplus \mathbb{Q}\alpha_i^*.$$

If $\sum q_i \alpha_i^* \in M^*$, then

$$q_j = B(\textstyle\sum_i q_i \alpha_i^*, \alpha_j) \in \mathbb{Z}.$$

Thus $M^* = \oplus \mathbb{Z}\alpha_i^*$. ∎

Idea of proof: A submodule of a f.g. free $\mathbb{Z}$-module is a free $\mathbb{Z}$-module.

Proof of theorem. Suppose $k = \bigoplus_{i=1}^{d} \mathbb{Q}\alpha_i$. Then, $\exists\, n_i \in \mathbb{Z}\setminus\{0\}$, $n_1\alpha_1, \dots, n_d\alpha_d \in \mathcal{O}_k$. Let $M := \bigoplus_i \mathbb{Z}\, n_i\alpha_i$. So

$M \subseteq \mathcal{O}_k \Rightarrow$ $\mathcal{O}_k^* \subseteq M^*$; M^* is a f.g. free $\mathbb{Z}$-mod; $\mathcal{O}_k \subseteq \mathcal{O}_k^*$ $\Rightarrow$ $\mathcal{O}_k$ is a f.g. free $\mathbb{Z}$-mod.

Since $S^{-1}\mathcal{O}_k = k$ where $S = \mathbb{Z}\setminus\{0\}$, we have $\operatorname{rank}_{\mathbb{Z}} \mathcal{O}_k = \dim_{\mathbb{Q}} k$. ■

Corollary. $\mathcal{O}_k$ is a Noetherian ring.

(it is in fact Noeth. $\mathbb{Z}$-module.)

Corollary. $\mathcal{O}_k$ is a Dedekind domain.

[(This we did not prove in class.) Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_k$. Then $\mathbb{Z}\cap\mathfrak{p}$ is a non-zero prime ideal of $\mathbb{Z}$. So $\mathbb{Z}\cap\mathfrak{p} = p\mathbb{Z}$ for some prime p. $\mathcal{O}_k/\mathfrak{p}$ is an integral extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{F}_p$ is a field, $\mathcal{O}_k/\mathfrak{p}$ is a field. Hence any non-zero prime ideal of $\mathcal{O}_k$ is maximal, i.e. it has Krull dimension 1.

Since $\mathcal{O}_k$ is the integral closure of $\mathbb{Z}$ in k, it is integrally closed.

And $\mathcal{O}_k$ is Noetherian.]

Definition/Lemma. Suppose $k = \mathbb{Q}\alpha_1 \oplus \cdots \oplus \mathbb{Q}\alpha_d$. Let

$$D(\alpha_1, \dots, \alpha_d) = \det\left[\operatorname{tr}_{k/\mathbb{Q}}(\alpha_i\alpha_j)\right] \in \mathbb{Q}^\times.$$

[Since $B(v,w) := \operatorname{tr}_{k/\mathbb{Q}}(vw)$ is non-degenerate $D(\alpha_1,\dots,\alpha_d) \neq 0$.].

Lemma. Suppose $k = \bigoplus_{i=1}^{d} \mathbb{Q}\alpha_i = \bigoplus_{i=1}^{d} \mathbb{Q}\beta_i$. Then $\exists\, g \in GL_d(\mathbb{Q})$ s.t.

① $\beta_i = \sum_j g_{ij}\alpha_j$ ② $D(\beta_1, \dots, \beta_d) = D(\alpha_1, \dots, \alpha_d) \det(g)^2$.

Pf. Since α_i's and β_i's are $\mathbb{Q}$-basis, $\exists\, g \in GL_d(\mathbb{Q})$ that satisfy ① $[B(\beta_i, \beta_j)] = [\sum g \dots B(\dots]$

satisfy ①. $[B(\beta_i,\beta_j)] = [\sum_{l,l'} g_{il}\, g'_{jl}\, B(\alpha_i,\alpha_j)]$

$= g\,[B(\alpha_i,\alpha_j)]\,g^t$

$\Rightarrow D(\beta_1,\beta_2,\cdots,\beta_d) = \det(g)^2 \cdot D(\alpha_1,\cdots,\alpha_d)$. ■

Def/Lemma. Suppose $\mathcal{O}_k = \bigoplus \mathbb{Z}\alpha_i$. Then $D(\alpha_1,\cdots,\alpha_d)$ does NOT depend on the choice of $\{\alpha_i\}$. It is called the discriminant of k.

Pf. If $\mathcal{O}_k = \bigoplus \mathbb{Z}\beta_i$, then $\exists\, g \in GL_n(\mathbb{Z})$ s.t. $\beta_i = \sum g_{ij}\alpha_j$.

$\Rightarrow D(\beta_1,\cdots,\beta_d) = \det(g)^2\, D(\alpha_1,\cdots,\alpha_d) = D(\alpha_1,\cdots,\alpha_d)$. ■

Let $\sigma_1,\cdots,\sigma_r : k \to \mathbb{R}$ and $\tau_1,\overline{\tau_1},\cdots,\tau_s,\overline{\tau_s} : k \to \mathbb{R}$ be all the embeddings of k into $\mathbb{C}$.

Proposition $k \otimes_{\mathbb{Q}} \mathbb{R} \simeq \underbrace{\mathbb{R}\oplus\cdots\oplus\mathbb{R}}_{r} \oplus \underbrace{\mathbb{C}\oplus\cdots\oplus\mathbb{C}}_{s} =: L_{r,s}$ as $\mathbb{R}$-algeb.

where $a\otimes 1 \mapsto (\sigma_1(a),\cdots,\sigma_r(a),\tau_1(a),\cdots,\tau_s(a))$.

Proof. By primitive element theorem, $\exists\,\alpha\in k$, $k = \mathbb{Q}[\alpha]$. Let $f(t)\in\mathbb{Q}[t]$ be the minimal polynomial of α over $\mathbb{Q}$. So

- $k \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{Q}[\alpha]\otimes_{\mathbb{Q}}\mathbb{R} \simeq \mathbb{Q}[t]/\langle f(t)\rangle \otimes_{\mathbb{Q}} \mathbb{R}$

  $\simeq \mathbb{R}[t]/\langle f(t)\rangle$

- $f(t) = \prod_{i=1}^{r} \underbrace{(t-\sigma_i(\alpha))}_{\text{irr. / }\mathbb{R}} \cdot \prod_{j=1}^{s} \underbrace{[(t-\tau_j(\alpha))(t-\overline{\tau_j}(\alpha))]}_{\text{irreducible / }\mathbb{R}}$

- By Chinese Remainder Theorem,

$$
\begin{aligned}
k \otimes_{\mathbb{Q}} \mathbb{R} &\simeq \mathbb{Q}[t]/\langle f(t)\rangle \otimes_{\mathbb{Q}} \mathbb{R} \qquad (\alpha\otimes 1 \mapsto t\otimes 1)\\
&\mapsto \mathbb{R}[t]/\langle f(t)\rangle \qquad (t \mapsto \overline{t})\\
&\simeq \bigoplus_{i=1}^{r} \mathbb{R}[t]/\langle t-\alpha_i\rangle \oplus \bigoplus_{j=1}^{s} \mathbb{R}[t]/\langle (t-\beta_j)(t-\overline{\beta_j})\rangle \qquad (t \mapsto (\alpha_1,\cdots,\alpha_r,\beta_1,\cdots,\beta_s))\\
&\simeq \bigoplus_{i=1}^{r} \mathbb{R} \oplus \bigoplus_{j=1}^{s} \mathbb{C}.
\end{aligned}
$$

■

$$\cong \bigoplus_{i=1}^{r} \mathbb{R} \oplus \bigoplus_{j=1}^{s} \mathbb{C}. \qquad \blacksquare$$

Corollary. $a_1, \dots, a_d \in k$ are $\mathbb{Q}$-linearly independent

$$\Updownarrow$$

$T(a_1), \dots, T(a_d) \in L_{r,s}$ are $\mathbb{R}$-linearly independent

where $T(a) = (\sigma_1(a), \dots, \sigma_r(a), \tau_1(a), \dots, \tau_s(a))$.

Proof. a_i's are $\mathbb{Q}$-linearly independ. $\iff$

$a_i \otimes 1$'s are $\mathbb{R}$-linearly independ. $\iff$

$T(a_i)$'s are $\mathbb{R}$-linearly independ. $\blacksquare$

Corollary. $T(\mathcal{O}_k)$ is a lattice in $L_{r,s}$.

Proof. We have proved that $\mathcal{O}_k = \bigoplus_{i=1}^{d} \mathbb{Z}\, a_i$. So

$T(a_i)$'s are linearly independ. over $\mathbb{R}$. $\Longrightarrow$

$$T(\mathcal{O}_k) = \bigoplus_{i=1}^{d} \mathbb{Z}\, T(a_i) \subseteq L_{r,s} = \bigoplus_{i=1}^{d} \mathbb{R}\, T(a_i). \qquad \blacksquare$$

Theorem. $\mathrm{vol}\left(L_{r,s}/T(\mathcal{O}_k)\right) = \sqrt{|D_k|}/2^s$ with respect to the Lebesgue measure on $L_{r,s}$.

Proof. $\mathrm{vol}\left(L_{r,s}/T(\mathcal{O}_k)\right)$

$$= \left| \det \begin{bmatrix} \sigma_1(a_1) & \cdots & \sigma_r(a_1) & \mathrm{Re}(\tau_1(a_1)) & \mathrm{Im}(\tau_1(a_1)) & \cdots & \mathrm{Re}(\tau_s(a_1)) & \mathrm{Im}(\tau_s(a_1)) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(a_d) & \cdots & \sigma_r(a_d) & \mathrm{Re}(\tau_1(a_d)) & \mathrm{Im}(\tau_1(a_d)) & \cdots & \mathrm{Re}(\tau_s(a_d)) & \mathrm{Im}(\tau_s(a_d)) \end{bmatrix} \right|$$

$$= \left| \det A(a_1, \dots, a_d) \right|$$

$$\det \begin{bmatrix} \overbrace{I}^{r} & & & \\ & \begin{matrix} 1 & i \\ 1 & -i \end{matrix} & & \\ & & \ddots & \\ & & & \begin{matrix} 1 & i \\ 1 & -i \end{matrix} \end{bmatrix} \quad \text{(s-copies of } \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}\text{)}$$

$$A(a_1, \dots, a_d) = \begin{bmatrix} \sigma_1(a_1) & \cdots & \sigma_r(a_1) & \tau_1(a_1) & \overline{\tau_1(a_1)} & \cdots & \tau_s(a_1) & \overline{\tau_s(a_1)} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(a_d) & \cdots & \sigma_r(a_d) & \tau_1(a_d) & \overline{\tau_1(a_d)} & \cdots & \tau_s(a_d) & \overline{\tau_s(a_d)} \end{bmatrix}$$

Notice that $\{\sigma_1, \dots, \sigma_r, \tau_1, \overline{\tau_1}, \dots, \tau_s, \overline{\tau_s}\} = \{\theta : k \to \mathbb{C} \mid \text{embed.}\}$

So $\mathrm{vol}(L_{r,s}/T(\mathcal{O}_k)) = \frac{1}{2^s}\left|\det[\theta_j(a_i)]\right|$.

On the other hand, $[\theta_j(a_i)][\theta_j(a_i)]^t = [\sum_{l=1}^{d}\theta_l(a_i a_j)]$

$= [\mathrm{tr}_{k/\mathbb{Q}}(a_i a_j)]$.

$\Rightarrow \det[\theta_j(a_i)]^2 = D_k \Rightarrow |\det[\theta_j(a_i)]| = \sqrt{|D_k|}$.

$\Rightarrow \mathrm{vol}(L_{r,s}/T(\mathcal{O}_k)) = \sqrt{|D_k|}/2^s$. ■

Theorem. For any $0 \neq \mathfrak{a} \trianglelefteq \mathcal{O}_k$, $\exists\, a \in \mathfrak{a}$ s.t.

$$|N_{k/\mathbb{Q}}(a)| \leq \left(\frac{4}{\pi}\right)^s \cdot \frac{d!}{d^d} \cdot \sqrt{|D_k|} \cdot N(\mathfrak{a}),$$

where $N(\mathfrak{a}) = |\mathcal{O}_k/\mathfrak{a}|$.

Lemma (Minkowski's convex body) Let $\Delta \subseteq \mathbb{R}^n$ be a lattice, $\mathcal{C}$ a convex symmetric subset of $\mathbb{R}^n$. If $\mathrm{vol}(\mathcal{C}) > 2^n \mathrm{vol}(\mathbb{R}^n/\Delta)$, then $\exists\, 0 \neq v \in \Delta \cap \mathcal{C}$.

Proof of lemma. Let $\pi : \mathbb{R}^n \longrightarrow \mathbb{R}^n/\Delta$. Since

$\mathrm{vol}(\frac{1}{2}\mathcal{C}) > \mathrm{vol}(\mathbb{R}^n/\Delta)$, $\exists\, c_1 \neq c_2 \in \mathcal{C}$ s.t. $\pi(\frac{1}{2}c_1) = \pi(\frac{1}{2}c_2)$.

$\Rightarrow 0 \neq \frac{c_1 - c_2}{2} \in \Delta$.

$c_2 \in \mathcal{C} \Rightarrow -c_2 \in \mathcal{C}$; $c_1 \in \mathcal{C}$; $\mathcal{C}$: convex $\Rightarrow \frac{c_1 - c_2}{2} \in \mathcal{C}$ $\Rightarrow 0 \neq \frac{c_1 - c_2}{2} \in \Delta \cap \mathcal{C}$.

■

Proof of theorem.

- Let $\mathcal{C}_c := \{(x_1, \cdots, x_r; y_1, \cdots, y_s) \in L_{r,s} \mid \sum_{i=1}^{r}|x_i| + 2\sum_{j=1}^{s}|y_j| \leq c\}$

So $\mathcal{C}_c$ is a symmetric convex subset of $L_{r,s}$.

- For $(x_1, \cdots, x_r; y_1, \cdots, y_s) \in L_{r,s}$, let $N(\vec{x}; \vec{y}) := \prod_{i=1}^{r}|x_i| \cdot \prod_{j=1}^{s}|y_j|^2$.

- $|N_{k/\mathbb{Q}}(a)| = \left|\prod_{i=1}^{r}\sigma_i(a) \cdot \prod_{j=1}^{s}\tau_j(a)\cdot\overline{\tau_j(a)}\right|$

$= N(T(a))$.

- For any $(\vec{x}; \vec{y}) \in \mathcal{C}_c$, we have

r s

• For any $(\vec{x};\vec{y}) \in C_c$, we have

$$\sqrt[d]{N(\vec{x};\vec{y})} \le \left(\sum_{i=1}^{r} |x_i| + 2\sum_{j=1}^{s} |y_j|\right)/d \le \frac{c}{d}.$$

$$\Rightarrow N(\vec{x};\vec{y}) \le \left(\frac{c}{d}\right)^d.$$

• $\mathrm{vol}(C_c) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \cdot \frac{1}{d!} \cdot c^d$ (?)

• $\mathrm{vol}\left(L_{r,s}/T(\mathfrak{A})\right) = N(\mathfrak{A}) \cdot \mathrm{vol}\left(L_{r,s}/T(\mathcal{O}_k)\right)$

$$= \frac{1}{2^s}\sqrt{|D_k|} \cdot N(\mathfrak{A}).$$

• We choose c such that $\mathrm{vol}(C_c) = 2^d \,\mathrm{vol}\left(L_{r,s}/\mathfrak{A}\right)^+$.

$$\Rightarrow c^d = \frac{2^d}{2^r} \cdot \frac{1}{\pi^s} \cdot d! \cdot \sqrt{|D_k|} \cdot N(\mathfrak{A})^+.$$

$$= \left(\frac{4}{\pi}\right)^s \cdot d! \cdot \sqrt{|D_k|} \cdot N(\mathfrak{A})^+.$$

$\Rightarrow$ by Minkowski's convex body theorem, $\exists\, (v_0;w_0) \in T(\mathcal{O}_k) \cap C_c$

$$\Rightarrow N(v_0;w_0) \le \frac{c^d}{d^d} = \left(\frac{4}{\pi}\right)^s \cdot \frac{d!}{d^d} \cdot \sqrt{|D_k|} \cdot N(\mathfrak{A})^+$$

$$\Rightarrow \exists\, 0 \neq a \in \mathfrak{A},\ |N_{k/\mathbb{Q}}(a)| \le \left(\frac{4}{\pi}\right)^s \cdot \frac{d!}{d^d} \cdot \sqrt{|D_k|} \cdot N(\mathfrak{A}). \quad \blacksquare$$

Here are a few properties of a Dedekind domain.

Theorem Let D be a Dedekind domain. Then

① $\forall \mathfrak{p} \in \mathrm{Spec}(D) \setminus \{0\}$, $S_{\mathfrak{p}}^{-1}D$ is a Discrete Valuation Ring where $S_{\mathfrak{p}} := D \setminus \mathfrak{p}$. I.e. $\exists\, v_{\mathfrak{p}} : k^\times \to \mathbb{Z}$ s.t.

ⓐ $v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$

ⓑ $v_{\mathfrak{p}}(x+y) \ge \min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\}$ if $x+y \neq 0$.

ⓒ $S_{\mathfrak{p}}^{-1}D = \{x \in k \mid v_{\mathfrak{p}}(x) \ge 0\}$

Here k is the field of fractions of D.

② $\forall \mathfrak{p} \in \mathrm{Spec}(D) \setminus \{0\}$, $\exists\, x_{\mathfrak{p}} \in \mathfrak{p}$ s.t. $S_{\mathfrak{p}}^{-1}\mathfrak{p} = S_{\mathfrak{p}}^{-1}D\, x_{\mathfrak{p}}$

($S_{\mathfrak{p}}^{-1}\mathfrak{p}$ is a principle ideal.)

③ Any $\mathfrak{p}$-primary ideal is a power of $\mathfrak{p}$.

③ Any $\mathfrak{p}$-primary ideal is a power of $\mathfrak{p}$.

④ Any non-zero ideal can be uniquely written as a product of non-zero prime ideals.

(Using primary decomposition and part ③.)

⑤ $\bigcap_{\mathfrak{p} \in \mathrm{Max}(D)} S_{\mathfrak{p}}^{-1} D = D$.

⑥ A D-submodule M of the field F of fractions of D is called a <u>fractional ideal</u> if $\exists\, a \in F^{\times}$ s.t. $aM \subseteq D$.

The set $\mathcal{F}$ of fractional ideals form a group under multiplication: $M_1 \cdot M_2 := \{ m_1 m_2 \mid m_i \in M_i \}$.

<u>Definition</u>. The class group Cl_k of k is $\mathcal{F}/\mathcal{P}$ where $\mathcal{F}$ is the group of fractional ideals and $\mathcal{P}$ is the group of principal fractional ideals, i.e. $\mathcal{P} := \{ a\mathcal{O}_k \mid a \in k^{\times} \}$.

<u>Observe</u>. $\forall M_1, M_2 \in \mathcal{F}$, $M_1 \equiv M_2 \pmod{\mathcal{P}} \iff$
$\exists\, a \in k^{\times}$, $M_2 = aM_1$.

<u>Theorem</u> $\forall M \in \mathcal{F}$, $\exists\, \mathfrak{a} \trianglelefteq \mathcal{O}_k$ s.t. ① $M \sim \mathfrak{a}$
② $N(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^s \cdot \frac{d!}{d^d} \cdot \sqrt{|D_k|}$.

<u>Proof</u>. Let $\mathfrak{b} \trianglelefteq \mathcal{O}_k$ be s.t. $M^{-1} \sim \mathfrak{b}$. By the previous result
$\exists_{\neq} b \in \mathfrak{b}$, $|N_{k/\mathbb{Q}}(b)| \leq \left(\frac{4}{\pi}\right)^s \cdot \frac{d!}{d^d} \cdot \sqrt{|D_k|} \cdot N(\mathfrak{b})$.
$\Rightarrow$ $\langle b \rangle = \mathfrak{b} \cdot \mathfrak{a}$ for some $\mathfrak{a} \trianglelefteq \mathcal{O}_k$.
$\Rightarrow$
$$\begin{cases} M \sim \mathfrak{b}M = M \cdot \mathfrak{b} \cdot \mathfrak{a} \sim \mathfrak{a} \\ |N_{k/\mathbb{Q}}(b)| = N(\mathfrak{b}) \cdot N(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^s \cdot \frac{d!}{d^d} \cdot \sqrt{|D_k|} \cdot N(\mathfrak{b}). \end{cases}$$
$\Rightarrow$
$$\begin{cases} M \sim \mathfrak{a} \\ N(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^s \cdot \frac{d!}{d^d} \cdot \sqrt{|D_k|}. \end{cases}$$
■

Corollary. The class number $h := |Cl_k| < \infty$.

Pf. Each class has a representative $\mathfrak{a}$ s.t.

$$\left.\begin{array}{l} |\mathcal{O}_k/\mathfrak{a}| \ll_k 1 \\ \mathcal{O}_k : \text{f.g. free abelian gp} \end{array}\right\} \Rightarrow \text{the \# of such ideals is finite.}$$

■

. Let $k_{\mathfrak{p}}$ be the completion of k with respect to $|x|_{\mathfrak{p}} := \left(\frac{1}{|\mathcal{F}_{\mathfrak{p}}|}\right)^{v_{\mathfrak{p}}(x)}$ where $\mathcal{F}_{\mathfrak{p}} := \mathcal{O}_k/\mathfrak{p}$. [We did not prove the next result in class, but similar argument was presented for $\mathbb{Q}_p$.]

Proposition Let $\{0=\alpha_0, \alpha_1, \dots, \alpha_{q-1}\}$ be a set of representatives of $\mathcal{O}_k/\mathfrak{p}$ in $\mathcal{O}_k$. Let $x_{\mathfrak{p}} \in \mathfrak{p}$ such that $S_{\mathfrak{p}}^{-1}\mathfrak{p} = S_{\mathfrak{p}}^{-1}\mathfrak{p}\, x_{\mathfrak{p}}$.

Then any $x \in k_{\mathfrak{p}}^{\times}$ can be uniquely written as

$$x = \sum_{n=n_0}^{\infty} D_n(x)\, x_{\mathfrak{p}}^n$$

where $D_n(x) = \alpha_j$ for some j; $D_{n_0}(x) \neq 0$.

Proof. By the definition of x, $\exists$ a Cauchy sequence $\{x_m\}_{m=1}^{\infty} \subseteq k$ s.t. $x = \lim_{m\to\infty} x_m$.

$$\forall l, \exists n_l \text{ s.t. } m \geq n_l \Rightarrow x_m - x_{n_l} \in \left(S_{\mathfrak{p}}^{-1}\mathcal{O}_k\right) x_{\mathfrak{p}}^{l}.$$

$$\Rightarrow v_{\mathfrak{p}}(x_m - x_{n_l}) \geq l.$$

So either $x=0$ or $v_{\mathfrak{p}}(x_m)$ is constant for large enough m.

$\Rightarrow$ After passing to a subseq., we have

① $y_m := x_{\mathfrak{p}}^{-n_0} x_m \in S_{\mathfrak{p}}^{-1}\mathcal{O}_k \setminus S_{\mathfrak{p}}^{-1}\mathfrak{p}$.

② $y_{m+1} - y_m \in \left(S_{\mathfrak{p}}^{-1}\mathcal{O}_k\right) x_{\mathfrak{p}}^{m+1}$ for any $m \in \mathbb{Z}^+$.

Since $\mathcal{F}_{\mathfrak{p}} = \mathcal{O}_k/\mathfrak{p} \simeq S_{\mathfrak{p}}^{-1}\mathcal{O}_k / S_{\mathfrak{p}}^{-1}\mathfrak{p}$, $\forall m \exists!\, i_{m+1}$ s.t.

$$y_{m+1} - y_m \in \alpha_{i_{m+1}} x_{\mathfrak{p}}^{m+1} + \left(S_{\mathfrak{p}}^{-1}\mathcal{O}_k\right) x_{\mathfrak{p}}^{m+2}.$$

So by induction we have $y_m \in \alpha_{i_0} + \alpha_{i_1} x_{\mathfrak{p}} + \cdots + \alpha_{i_m} x_{\mathfrak{p}}^{m} + \left(S_{\mathfrak{p}}^{-1}\mathcal{O}_k\right) x_{\mathfrak{p}}^{m+1}$

$$\Rightarrow x = \sum_{j=n_0}^{\infty} \alpha_{i_j} x_{\mathfrak{p}}^{j}.$$

so by induction we have $y_m \in \alpha_{i_0} + \alpha_{i_1} x_{\mathfrak{p}} + \cdots + \alpha_{i_m} x_{\mathfrak{p}}^m + \left(\mathfrak{p}^{m+1} \mathcal{O}_k\right) x_{\mathfrak{p}}^{m+1}$

Hence $x = \sum_{j=0}^{\infty} \alpha_{i_j} x_{\mathfrak{p}}^{n_0+j}$.

One can get the uniqueness, first by getting $\underline{n_0}$ (which is essentially $v_{\mathfrak{p}}(x)$.) and proving the uniqueness inductively. □

Corollary. $\mathcal{O}_k$ is dense in $\mathcal{O}_{\mathfrak{p}} := \{x \in k_{\mathfrak{p}} \mid v_{\mathfrak{p}}(x) \geq 0\}$

and $\mathcal{O}_{k/\mathfrak{p}}$ is naturally isomorphic with $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$

and $\mathfrak{p}\mathcal{O}_{\mathfrak{p}} = \{x \in k_{\mathfrak{p}} \mid v_{\mathfrak{p}}(x) > 0\} = x_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$.

Proof. • By the above proposition, since α_i's and $x_{\mathfrak{p}}$ are in $\mathcal{O}_k$, we have that $\mathcal{O}_k$ is dense in $\mathcal{O}_{\mathfrak{p}}$.

• $\{x \in k_{\mathfrak{p}} \mid v_{\mathfrak{p}}(x) > 0\} = \{\sum_{n=1}^{\infty} \alpha_{i_n} x_{\mathfrak{p}}^n\}$

$= x_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}$

$\Rightarrow \mathfrak{p}\mathcal{O}_{\mathfrak{p}} = \{x \in k_{\mathfrak{p}} \mid v_{\mathfrak{p}}(x) > 0\}$.

• $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ can be represented by α_i's $\Rightarrow \mathcal{O}_{k/\mathfrak{p}} \simeq \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. ■

Theorem. $\mathcal{O}_k$ is dense in $\prod_{\mathfrak{p} \in V_f(k)} \mathcal{O}_{\mathfrak{p}}$.

Proof. Let $(y_{\mathfrak{p}}) \in \prod \mathcal{O}_{\mathfrak{p}}$. Let U be an open nbhd of 0.

$\Rightarrow U = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{n_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}} \cdot \prod_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}$, where S is a finite set.

Now we need to find $x \in \mathcal{O}_k$ s.t.

$$x - y_{\mathfrak{p}} \in \mathfrak{p}^{n_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}} \quad \text{for any } \mathfrak{p} \in S.$$

By the previous corollary, $\exists\ y'_{\mathfrak{p}} \in \mathcal{O}_k$ s.t.

$$y_{\mathfrak{p}} - y'_{\mathfrak{p}} \in \mathfrak{p}^{n_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}.$$

So it is enough to find $x \in \mathcal{O}_k$ s.t. $x - y'_{\mathfrak{p}} \in \mathfrak{p}^{n_{\mathfrak{p}}}$. Thus

$$\mathcal{O}_k \longrightarrow \bigoplus_{\mathfrak{p}\in S} \mathcal{O}_k/\mathfrak{p}^{n_\mathfrak{p}}$$

is onto, which is equivalent to

$$\exists x \in \bigcap_{i=1}^{l} \mathfrak{p}_i^{n_i} \text{ s.t. } x-1 \in \mathfrak{p}_0^{n_0} \iff \mathcal{O}_k = \underbrace{\bigcap_{i=1}^{l} \mathfrak{p}_i^{n_i} + \mathfrak{p}_0^{n_0}}_{\mathfrak{a}}.$$

$\mathfrak{a} \supseteq \mathfrak{p}_0^{n_0} \Longrightarrow$ the only maximal ideal that can contain $\mathfrak{a}$ is $\mathfrak{p}_0$.

$\mathfrak{a} \supseteq \bigcap_{i=1}^{l} \mathfrak{p}_i^{n_i} \Longrightarrow$ the only maximal ideals that can contain $\mathfrak{a}$ are $\mathfrak{p}_1, \cdots, \mathfrak{p}_l$

$\Bigg\} \Rightarrow \mathfrak{a} = \mathcal{O}_k$. ■

<u>Corollary.</u> k is dense in $\prod'_{\mathfrak{p}\in V_f(k)} k_\mathfrak{p} := \{(y_\mathfrak{p}) \mid N(\mathfrak{p}) \gg 1 \Rightarrow y_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}\}$.

<u>Proof.</u> Let $(y_\mathfrak{p})_{\mathfrak{p}\in V_f(k)} \in \prod' k_\mathfrak{p}$ and $U = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n_\mathfrak{p}}\mathcal{O}_\mathfrak{p} \cdot \prod_{\mathfrak{p}\notin S} \mathcal{O}_\mathfrak{p}$.

By enlarging S, if necessary, we can and will assume that $y_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$ for $\mathfrak{p} \notin S$. So we need to find $x \in k$ such that

① $x - y_\mathfrak{p} \in \mathfrak{p}^{n_\mathfrak{p}}\mathcal{O}_\mathfrak{p}$ if $\mathfrak{p} \in S$

② $x \in \mathcal{O}_\mathfrak{p}$ if $\mathfrak{p} \notin S$.

By the above proposition, $\exists\, y'_\mathfrak{p} \in \mathcal{O}_k$ s.t.

$$y_\mathfrak{p} - x_\mathfrak{p}^{-m_\mathfrak{p}} y'_\mathfrak{p} \in \mathfrak{p}^{n_\mathfrak{p}}\mathcal{O}_\mathfrak{p}$$

So we need to find

① $x \in \bigcap_{\mathfrak{p}\notin S} S_\mathfrak{p}^{-1}\mathcal{O}_k$

② $x - \frac{y'_\mathfrak{p}}{x_\mathfrak{p}^{m_\mathfrak{p}}} \in S_\mathfrak{p}^{-1}\mathcal{O}_k\, x_\mathfrak{p}^{n_\mathfrak{p}}$ for $\mathfrak{p} \in S$.

$$② \Leftrightarrow \underbrace{\left(\prod_{\mathfrak{p}'\in S} x_{\mathfrak{p}'}^{m_{\mathfrak{p}'}}\right)}_{a} x - y''_\mathfrak{p} \in S_\mathfrak{p}^{-1}\mathcal{O}_k \cdot \left(\prod_{\mathfrak{p}'\in S} x_{\mathfrak{p}'}^{n_{\mathfrak{p}'}}\right) x_\mathfrak{p}^{n_\mathfrak{p}} = S_\mathfrak{p}^{-1}\mathcal{O}_k \cdot x_\mathfrak{p}^{m''_\mathfrak{p}}$$

By the previous theorem, $\exists\, y \in \mathcal{O}_k$ s.t.

$$y - y''_\mathfrak{p} \in S_\mathfrak{p}^{-1}\mathcal{O}_k \cdot x_\mathfrak{p}^{m''_\mathfrak{p}} \quad \text{for } \mathfrak{p} \in S.$$

$$y - y''_{\mathfrak{p}} \in S_{\mathfrak{p}}^{-} \mathcal{O}_k \cdot x_{\mathfrak{p}}' \qquad \text{for } \mathfrak{p} \in S.$$

So we need to find $x \in k$ s.t.

① $x \in \bigcap_{\mathfrak{p} \notin S} S_{\mathfrak{p}}^{-1} \mathcal{O}_k$

② $ax - y \in \bigcap_{\mathfrak{p} \in S} S_{\mathfrak{p}}^{-1} \mathcal{O}_k \cdot x_{\mathfrak{p}}^{m''_{\mathfrak{p}}}$ ⊛

where $a = \prod_{\mathfrak{p} \in S} x_{\mathfrak{p}}^{m'_{\mathfrak{p}}}$ and $m''_{\mathfrak{p}} > m'_{\mathfrak{p}}$.

By the above theorem $\exists\, x' \in \mathcal{O}_k$ s.t.

$$\begin{cases} x' \in \mathcal{O}_{\mathfrak{p}} \cdot a & \forall\, \mathfrak{p} \notin S \\ x' - y \in \mathcal{O}_{\mathfrak{p}} \cdot x_{\mathfrak{p}}^{m''_{\mathfrak{p}}} & \forall\, \mathfrak{p} \in S \end{cases}$$

$\Rightarrow x = a^{-1} x'$ satisfies ⊛. ∎

Corollary. $k + \prod_{v \in V_\infty} k_v \cdot \prod_{v \in V_f} \mathcal{O}_v = \mathbb{A}_k$.

Proof. k is dense in $\prod'_{v \in V_f} k_v$ and $\prod_{v \in V_f} \mathcal{O}_v$ is a non-empty open subset. So $k + \prod_{v \in V_f} \mathcal{O}_v = \prod'_{v \in V_f} k_v \rightsquigarrow \checkmark$. ∎

Proposition. k is a lattice in $\mathbb{A}_k$.

Proof. We have proved that $\mathcal{O}_k$ is a lattice in $\prod_{v \in V_\infty} k_v$. Let $\mathcal{F}_\infty$ be a fundamental domain of $\mathcal{O}_k$ in $\prod_{v \in V_\infty} k_v$ which contains a nbhd of 0. So it is enough to prove that $\mathcal{F}_\infty \cdot \prod_{\mathfrak{p} \in V_f} \mathcal{O}_{\mathfrak{p}}$ is a fundamental domain of k in $\mathbb{A}_k$.

Step 1. $k + \mathcal{F}_\infty \cdot \prod_{\mathfrak{p} \in V_f} \mathcal{O}_{\mathfrak{p}} = \mathbb{A}_k$.

Proof of step 1.

$\forall\, (y_v)_{v \in V(k)}$,

① $\exists\, x_1 \in k$ s.t. $(y_{\mathfrak{p}})_{\mathfrak{p} \in V_f} - x_1 \in \prod \mathcal{O}_{\mathfrak{p}}$

② $\exists\, x_2 \in \mathcal{O}_k$ s.t. $(y_v - x_1)_{v \in V_\infty} - x_2 \in \mathcal{F}_\infty$.

$\exists\, x_2 \in \mathcal{O}_k$ s.t. $(y_v - x_1)_{v\in V_\infty} - x_2 \subset \mathcal{T}_\infty$.

$$\Rightarrow (y_v)_{v\in V} - (x_1+x_2) \in \mathcal{F}_\infty \cdot \prod \mathcal{O}_{\mathfrak{p}}.$$

Step 2. $(y_v)_{v\in V},\ x+(y_v)_{v\in V} \in \mathcal{F}_\infty \cdot \prod \mathcal{O}_{\mathfrak{p}}$, $x \in k$ $\Rightarrow x=0$.

Proof of step 2. $\forall \mathfrak{p} \in V_f(k)$, $y_{\mathfrak{p}}, x+y_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}} \Rightarrow x \in \bigcap_{\mathfrak{p}} (k \cap \mathcal{O}_{\mathfrak{p}})$

$\Rightarrow x \in \bigcap_{\mathfrak{p}} (S_{\mathfrak{p}}^{-1}\mathcal{O}_k) = \mathcal{O}_k$.

$(y_v)_{v\in V_\infty},\ x+(y_v)_{v\in V_\infty} \in \mathcal{F}_\infty$

$\Rightarrow x=0$. ∎

We normalize the Haar measures of local fields as follows:

- $\int_{\mathcal{O}_{\mathfrak{p}}} |dx|_{\mathfrak{p}} = 1$ for $\mathfrak{p} \in V_f(k)$
- $\int_{[0,1]} |dx|_v = 1$ for a real embedding v.
- $|dx|_v = i\, dz\, d\bar{z}$ if $k_v \simeq \mathbb{C}$.

$$i\, dz \wedge d\bar{z} = i\,(dx+i\,dy)\wedge(dx-i\,dy)$$
$$= -\,(dy\wedge dx - dx\wedge dy)$$
$$= 2\, dx\wedge dy.$$

→ twice the usuall Lebesgue mensure.

On $\mathbb{A}_k$ we take the induced (restricted product) measure.

Proposition. $|\omega|(\mathbb{A}_{k/k}) = \sqrt{|D_k|}$.

Proof. In the proof of the above proposition, we saw that $\mathcal{F}_\infty \cdot \prod \mathcal{O}_{\mathfrak{p}}$ is a fundamental domain of k in $\mathbb{A}_k$. So

$$|\omega|(\mathbb{A}_{k/k}) = |\omega|\left(\mathcal{F}_\infty \cdot \prod \mathcal{O}_{\mathfrak{p}}\right) = |\omega|_\infty(\mathcal{F}_\infty) \cdot \prod_{\mathfrak{p}} |\omega|_{\mathfrak{p}}(\mathcal{O}_{\mathfrak{p}})$$
$$= |\omega|_\infty(\mathcal{F}_\infty) = (2^s) \cdot \frac{\sqrt{|D_k|}}{2^s} = \sqrt{|D_k|}.$$

where s is the number of complex embedding of k up to conjugation. [Notice that $|\omega|_\infty = 2^s$. Lebesgue measure

$r \quad s$

$$\prod_{v \in V_\infty} K_v \simeq K \otimes_{\mathbb{Q}} \mathbb{C} \cdot J$$ ∎

Remark. The adelic point of view is the best way to avoid emphasizing on Archimedean places. This way one gets a better connection between number fields and global function fields, i.e. finite extensions of $\mathbb{F}_q(t)$.

Remark. Suppose k is a global function field with constant field $\mathbb{F}_q$ and genus g. Then using Riemann-Roch theorem one can prove

$$|\omega(\mathbb{A}_k/k)| = q^{g-1} .$$