Defn: A discrete subgp of $\mathbb{R}^n$ of rk n is called a *lattice* in $\mathbb{R}^n$.

That is, a lattice $H = \bigoplus_{i=1}^{n} \mathbb{Z} e_i$ Denote $e = (e_1, \dots, e_n)$,

Let $P_e = \{x \in \mathbb{R}^n \mid x = \sum_{i=1}^{n} x_i e_i,\ 0 \le x_i < 1\}$.

Called the *fundamental domain* of H w.r.t. e.

Lem 1.3: Volume $\mu(P_e)$ is indep of choice of e (basis of H).

Pf: If $H = \bigoplus_{j=1}^{n} \mathbb{Z} f_j$, then $(f_1, \dots, f_n) = (e_1 \dots e_n) T$

for $T \in GL_n(\mathbb{Z})$, $\mu(P_f) = |\det T| \mu(P_e)$, and $\det T = \pm 1$ □

Defn: Call $\mu(P_e)$ (which is indep of e) the *volume* of H, denote as $v(H)$.

Ex: $H = \mathbb{Z} \cdot 2 \oplus \mathbb{Z} \cdot (1+i) \subseteq \mathbb{R}^2$, $v(H) = 2$.

Thm 1.4: $H \subseteq \mathbb{R}^n$ lattice. $S \subseteq \mathbb{R}^n$ a measurable set, s.t. $\mu(S) > v(H)$.

Then $\exists\ x, y \in S$, s.t. $x - y \in H \setminus \{0\}$

Pf: $\mathbb{R}^n = \coprod_{h \in H} (h + P_e) \Rightarrow S = \coprod_{h \in H} (S \cap (h + P_e))$

$$\mu(S) = \sum_{h \in H} \mu(S \cap (h + P_e)) = \sum_{h \in H} \mu((-h + S) \cap P_e)$$

each $(-h+S) \cap P_e \subseteq P_e$, summation of vol $> \mu(P_e)$

$\Rightarrow \exists\ h_1 \neq h_2$, $((-h_1 + S) \cap P_e) \cap ((-h_2 + S) \cap P_e) \neq \phi$

$\Rightarrow \exists\ x \in S,\ y \in S,\ -h_1 + x = -h_2 + y \in P_e$

$\Rightarrow x - y = h_1 - h_2 \in H \setminus \{0\}$. □

Recall $S \subseteq \mathbb{R}^n$ is called a convex subset if $x, y \in S$, then $\forall\, x + (1-\alpha)y \in S$, $\forall\ 0 \le \alpha \le 1$.

Ex: 

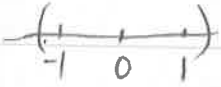
non-Ex: 

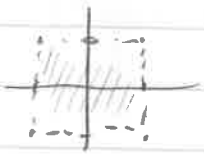
Cor. 1.5: $H \subseteq \mathbb{R}^n$ lattice, $S \subseteq \mathbb{R}^n$ measurable, symmetric w.r.t. 0, and convex. Assume one of the following:

(a) $\mu(S) > 2^n v(H)$

(b) $\mu(S) \ge 2^n v(H)$ and S and cpt

Then $S \cap (H - \{0\}) \neq \phi$.

(Ex: dim 1, $H = \mathbb{Z}$, 

dim 2. 

Pf: First, note for S, $x \in S$, $-x \in S$ (Symmetry) $\Rightarrow \frac{1}{2}(x) + \frac{1}{2}(-x) = 0 \in S$

thus $\forall\, x \in S$, $\forall\, \alpha \in [0,1]$, $\alpha \cdot x + (1-\alpha)\cdot 0 = \alpha x \in S$

If (a) true, let $S' = \frac{1}{2}S \Rightarrow \mu(S') = \frac{1}{2^n}\mu(S) > v(H)$

, Thm 1.4 $\Rightarrow \exists\, x, y \in S'$, $x - y \in H \setminus \{0\}$.

$2x \in S$, $2y \in S \Rightarrow -2x, -2y \in S$

$\Rightarrow x - y \in \frac{1}{2}\cdot(2x) + \frac{1}{2}(-2y) \in S \cap (H \setminus \{0\})$

If (b) true, then $\forall\, \varepsilon > 0$, $(1+\varepsilon)S$ satisfies (a)

$\Rightarrow (1+\varepsilon)S \cap (H - \{0\}) \neq \phi$

$(1+\varepsilon)S$ cpt, $H - \{0\}$ discrete $\Rightarrow$ $\cap$ is finite $\Rightarrow$ cpt.

Lem 1.1 $\Rightarrow$ $\bigcap_{\varepsilon>0} \left((1+\varepsilon)S \cap (H - \{0\}) \right) \neq \phi$.

It suffices to show $\bigcap_{\varepsilon>0} (1+\varepsilon)S = S$

RHS $\subseteq$ LHS, since $x \in S \Rightarrow \frac{1}{1+\varepsilon} \cdot x + (1 - \frac{1}{1+\varepsilon}) \cdot 0 \in S$.

$\Rightarrow x = (1+\varepsilon) \cdot \frac{1}{1+\varepsilon} x \in (1+\varepsilon)S$

To show LHS $\subseteq$ RHS, let $y \in$ LHS, if $y \notin$ RHS,
then $d(y, S) = \delta_0 > 0$ (since S is cpt)

$\forall \varepsilon > 0$, $y = (1+\varepsilon) y'$ for $y' \in S$

$\Rightarrow \delta_0 = d(y, S) \leq d\left((1+\varepsilon)y', y'\right) = d(\varepsilon y', 0) = \varepsilon \cdot d(y', 0)$

but $d(y', 0)$ is bounded (S cpt)

$\Rightarrow \delta_0 = 0$ contradiction $\square$

§2. Canonical embedding of a number field.

Let $[K:\mathbb{Q}]=n$. Exactly n $\mathbb{Q}$-emb of $K \hookrightarrow \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

namely, if $K=\mathbb{Q}(x)$, $\mathrm{Irr}(x,\mathbb{Q}) = \prod_{i=1}^{n}(T-x_i)$, $x_i \in \mathbb{C}$,

$\sigma_i : K \hookrightarrow \mathbb{C}$, $\mathbb{Q} \mapsto \mathbb{Q}$, $x \mapsto x_i$,

Denote $\alpha : \mathbb{C} \to \mathbb{C}$ the complex conjugation: $z \mapsto \bar{z}$.

Then for any i, $\alpha \circ \sigma_i : K \xrightarrow{\sigma_i} \mathbb{C} \xrightarrow{\alpha} \mathbb{C}$ is also $\mathbb{Q}$-emb

$\Rightarrow \alpha \circ \sigma_i = \sigma_j$ for some j

Then $\alpha \circ \sigma_i = \sigma_i \Leftrightarrow \sigma_i(K) \subseteq \mathbb{R}$. (since $\mathbb{C}^{\alpha}=\mathbb{R}$)

Thus, if $r_1 := \#\{\, i \mid \alpha \circ \sigma_i = \sigma_i \,\}$, then must $2 \mid n-r_1$, $n-r_1=2r_2$.

Can order σ_i so that $\sigma_i(K) \subseteq \mathbb{R}$, $1 \le i \le r_1$,

and $\sigma_{j+r_2} = \alpha \circ \sigma_j$, $r_1+1 \le j \le r_1+r_2$

i.e., $\sigma_1, \cdots \sigma_{r_1}, \sigma_{r_1+1}, \cdots \sigma_{r_1+r_2}, \overline{\sigma_{r_1+1}}, \cdots, \overline{\sigma_{r_1+r_2}}$

Ex: K quad field, $\Rightarrow$ $K=\mathbb{Q}(\sqrt{d})$ $d>0$; real quad

$K=\mathbb{Q}(\sqrt{-d})$ $d>0$; imag quad.

$\Rightarrow$ $r_1=2, r_2=0$

$r_1=0, r_2=1$

* In HW, have $f(T)=T^3+T-1$ is given in $\mathbb{Q}[T]$, and has a unique real root. Write $f(T)=(T-\alpha)(T-\beta)(T-\bar{\beta}) \in \mathbb{Q}[T]$ for $\alpha \in \mathbb{R}$, $\beta \in \mathbb{C}-\mathbb{R}$

Let $K=\mathbb{Q}[\alpha]$, then $\sigma_1 : \alpha \mapsto \alpha$

$\sigma_2 : \alpha \mapsto \beta$

$\sigma_3 : \alpha \mapsto -\beta$

$\Rightarrow r_1=1, r_2=1$

(note, if use $L=\mathbb{Q}[\beta]$, also $r_1=1$, $r_2=1$)

Note the first r_1+r_2 emb decide the last r_2 emb.

Defn: Let $\sigma: K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

$$\sigma(x) = (\sigma_1(x), \cdots \sigma_{r_1}(x), \sigma_{r_1+1}(x), \cdots, \sigma_{r_1+r_2}(x))$$

Call it the canonical embedding of K.

(Note that $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$ as $\mathbb{R}$-vec space)

Prop 2.1: Suppose $M \subseteq K$ is a free $\mathbb{Z}$-mod of rk n, $M = \bigoplus_{i=1}^{n} \mathbb{Z} \cdot x_i$

Then $\sigma(M) \subseteq \mathbb{R}^n$ is a lattice, and volume

$$v(\sigma(M)) = 2^{-r_2} \left| \det (\sigma_i(x_j))_{1 \le i,j \le n} \right|$$

Pf: $x_i \mapsto \sigma(x_i) \subseteq \mathbb{R}^n$ is

$$\left(\sigma_1(x_i), \cdots, \sigma_{r_1}(x_i), R(\sigma_{r_1+1}(x_i)), I(\sigma_{r_1+1}(x_i)) \cdots\right) \circledast_i$$

where R, I means real part, imaginary part.

$R(z) = \frac{1}{2}(z+\bar{z})$, $I(z) = \frac{1}{2i}(z-\bar{z})$.

Consider the det of matrix $\begin{pmatrix} \circledast_1 \\ \vdots \\ \circledast_n \end{pmatrix}$.

change $[R(\sigma_{r_1+1}(x_i)), I(\ )] = (\frac{1}{2}(z+\bar{z}), \frac{1}{2i}(z-\bar{z}))$

to $(z, \frac{1}{2i}(z-\bar{z})) \to \frac{1}{2i}(z, z-\bar{z}) \to \frac{1}{2i}(z, -\bar{z}) \to \frac{-1}{2i}(z, \bar{z})$

$$\Rightarrow \det = \left(\frac{-1}{2i}\right)^{r_2} \left| \sigma_1(x_i) \cdots, \sigma_{r_1}(x_i), \sigma_{r_1+1}(x_i), \sigma_{r_1+1+r_2}(x_i), \cdots \right|$$

$$\Rightarrow |\det| = \left(\frac{1}{2}\right)^{r_2} \left|\det \sigma_i(x_j)\right| \neq 0, \text{ since } \left|\det \sigma_i(x_j)\right| = \sqrt{\left|D_{K/\mathbb{Q}}(x_1, \cdots x_n)\right|} \neq 0.$$

This show $\sigma(x_1) \cdots, \sigma(x_n)$ are lin. indep over $\mathbb{R} \Rightarrow \sigma(M)$ is lattice,

and volume is precisely the det. $\square$

Defn If $A = \bigoplus_{i=1}^{n} \mathbb{Z} e_i$, let $d_K = D(e_1, \cdots, e_n) \in \mathbb{Z}$ (call it the absolute discriminant of K.

← recall a bit about discriminant.

Rmk if $A = \bigoplus \mathbb{Z} f_i$ for another basis, then $(e_1 \cdots e_n) = T(f_1 \cdots f_n)$ with $T \in GL_n(\mathbb{Z})$, $\Rightarrow D(f_1 \cdots f_n) = |\det T|^2 D(e_1 \cdots e_n) = D(e_1 \cdots e_n)$.
Thus, d_K is well-defined elt in $\mathbb{Z}$.

Prop 2.2 $d = d_K$. $\{0\} \neq \alpha \subseteq A$ ideal. Then $\sigma(A)$, $\sigma(\alpha) \subseteq \mathbb{R}^n$ are lattices, and $v(\sigma(A)) = 2^{-r_2} |d|^{1/2}$, $v(\sigma(\alpha)) = 2^{-r_2} |d|^{1/2} \cdot N(\alpha)$.

Pf A fin free $\mathbb{Z}$-mod of rk n.
$\alpha \subseteq A \Rightarrow \alpha$ fin free of rk $\leq n$. But for any $x \in \alpha - \{0\}$, $\alpha \supseteq A \cdot x$ which is free of rk $n \Rightarrow \alpha$ free of rk n.
Prop 2.1. $\Rightarrow \sigma(A)$, $\sigma(\alpha)$ are lattices.

$v(\sigma(A))$ is by Prop. 2.1 (Recall $D(e_1, \cdots, e_n) = \left(\det(\sigma_i(e_j))\right)^2$)
For $v(\sigma(\alpha))$ Note $N(\alpha) = \#|A/\alpha|$
Recall v calculates volume of fundamental domain
Choose basis $A = \bigoplus \mathbb{Z} \cdot e_i$, s.t $\alpha = \bigoplus \mathbb{Z} \cdot a_i e_i$, $a_1 | a_2 \cdots | a_n$
fund dom of A $\{\sum \alpha_i e_i \quad 0 \leq \alpha_i < 1\}$
α $\{\sum \alpha_i a_i e_i, \ 0 \leq \alpha_i < 1\}$
$\Rightarrow v(\sigma(\alpha)) = |\prod a_i| \cdot v(\sigma(A)) = N(\alpha) \cdot v(\sigma(A))$. □

A lemma for later use.

Lem 2.3 Let $B_t = \left\{ (y_1, \cdots, y_{r_1}, \gamma_1, \cdots, \gamma_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \text{ s.t } \sum |y_i| + 2\sum |\gamma_j| \leq t \right\}$
Let $t \geq 0$,

Then $\mu(B_t) = 2^{r_1} \cdot \left(\frac{\pi}{2}\right)^{r_2} \cdot \frac{t^n}{n!}$ ⊛

Pf Denote $\mu(B_t) = V(r_1, r_2, t)$, pf by double induction on r_1, r_2.
$V(1, 0, t) = V(|y_1| \leq t) = 2t$
$V(0, 1, t) = V(2|\gamma_1| \leq t) = \frac{\pi}{4} t^2$.

Assume true for $V(r_1, r_2, t)$, Consider $V(r_1+1, r_2, t)$

i.e, $|y| + \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |\beta_j| \le t$.

$$V(r_1+1, r_2, t) = \int_{-t}^{t} V(r_1, r_2, t-|y|)\, dy$$

$$= 2\int_0^t 2^{r_1} \cdot \left(\frac{\pi}{2}\right)^{r_2} \cdot \frac{(t-y)^n}{n!}\, dy = \circledast$$

Consider also $V(r_1, r_2+1, t)$. $\sum |y_i| + 2\sum |\beta_j| + 2|\beta| \le t$.

$$V(r_1, r_2+1, t) = \int_{|\beta| \le t/2} V(r_1, r_2, t-2|\beta|)\, d\mu(\beta)$$

Let $\beta = \rho e^{i\theta}$, $\rho \in \mathbb{R}^{\ge 0}$, $0 \le \theta \le 2\pi$

then, $= \int_0^{\frac{t}{2}} \int_0^{2\pi} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{(t-2\rho)^n}{n!}\, \rho\, d\rho\, d\theta = \circledast$

↑ check.

□

§3. Pf of Main Thm.

Goal: for $[K:\mathbb{Q}]=n$, $\#|C(A)| < \infty$

Recall strategy: For each ideal class $\beta \in C(A)$, assign a value $n_\beta \in \mathbb{Z}^{>0}$.

Show: ① $n_\beta \le N$ for some N, $\forall \beta \in C(A)$

② For each $n \le N$, $\#\{\beta \mid n_\beta = n\} <$ finite

Prop 3.1 $\alpha \subseteq A$ ideal, then $\exists\, x \in \alpha$, s.t.

$$|N(x)| \le \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}} \, N(\alpha)$$

Pf: $N(x) = \prod_{i=1}^{n} \sigma_i(x) \Rightarrow |N(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \cdot \prod_{j=r_1+1}^{r_2} |\sigma_j(x)|_{\mathbb{C}}^2$

geometric mean inequality: $x_i > 0$, then $(x_1 \cdots x_n)^{\frac{1}{n}} \le \frac{1}{n}(\sum x_i)$

$$\Rightarrow |N(x)| \le \left(\frac{1}{n} \sum |\sigma_i(x)| + \frac{2}{n} \sum |\sigma_j(x)| \right)^n$$

Let $B_t = \{(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2},\ \sum |y_i| + 2\sum |z_j| \le t\}$

Note B_t is convex, symm to 0, cpt, and $\mu(B_t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \cdot \frac{t^n}{n!}$

Let $t_0 = \left(2^{n-r_1} \cdot \pi^{-r_2} \cdot n! \cdot |d|^{\frac{1}{2}} \cdot N(\alpha)\right)^{\frac{1}{n}}$.

then $\mu(B_{t_0}) = 2^{n-r_2}|d|^{\frac{1}{2}} N(\alpha) = 2^n \cdot v(\sigma(\alpha))$.

By Cor. 1.5, $\exists\, x \in \alpha \setminus \{0\}$, s.t. $\sigma(x) \in B_{t_0}$

$$\Rightarrow |N(x)| \le \left(\frac{t_0}{n}\right)^n = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} |d|^{\frac{1}{2}} \cdot N(\alpha) \qquad \square$$

Cor 3.2 Let $\bar{\alpha} \in C(A) = I(A)/P(A)$, then $\exists\, \beta \subseteq A$ an integral ideal, $\bar{\beta} = \bar{\alpha}$, s.t. $N(\beta) \le \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{1/2}$ ⊛

Pf: Pick any α a frac ideal in the class $\bar{\alpha}$,
α^{-1} is also frac ideal, $\Rightarrow \exists\, y \neq 0$, $y\alpha^{-1} \subseteq A$.

Take $x \in y\alpha^{-1}$ s.t. Prop 3.1 is satisfied, i.e.

$$|N(x)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \cdot |d|^{1/2} \cdot N(y\alpha^{-1})$$

Let $\beta = xy^{-1}\alpha \subseteq A$, then $\bar{\beta} = \bar{\alpha}$, and

since N is multiplicative,
$\Rightarrow N(\beta) \cdot N(y\alpha^{-1}) = |N(x)|$
$\Rightarrow N(\beta) \le$ RHS of ⊛. □

Thm 3.3 (Dirichlet, ~1830s) For number field K, $\#|C(A)| < \infty$

Pf: For any $\bar{\alpha} \in C(A)$ (By Cor 3.2), $\exists\, \beta$ integral, $\bar{\beta} = \bar{\alpha}$, and $N(\beta) \le N$ for some $N \ge$ RHS of ⊛

Let $1 \le q \le N$, $q \in \mathbb{Z}$,

Claim. $\exists$ fin. many integral ideals $\beta \subseteq A$, s.t. $N(\beta) = q$.

Pf: $\#(A/\beta) = q \Rightarrow A/\beta$ is an abelian gp of order q

$\Rightarrow q \cdot (A/\beta) = 0 \Rightarrow q \cdot 1 \in \beta$, i.e. $q \in \beta$.

$\Rightarrow A \cdot q \subseteq \beta \subseteq A \Rightarrow$ fin. many such possible β (by considering prime decomposition of Aq and β)

Conclude, $\#|C(A)| \le \sum_{q=1}^{N} \#\{\beta \mid N(\beta) = q\} < \infty$. □

Lem 3.4 $[K:\mathbb{Q}]=n\geq 2$, then $|d|\geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$.

Pf By Cor 3.2, $|d|^{\frac{1}{2}} \geq N(\beta)\cdot\left(\frac{\pi}{4}\right)^{r_2}\frac{n^n}{n!} \geq \left(\frac{\pi}{4}\right)^{r_2}\cdot\frac{n^n}{n!}$

$$\Rightarrow |d| \geq \left(\frac{\pi}{4}\right)^{2r_2}\frac{n^{2n}}{(n!)^2} \geq \left(\frac{\pi}{4}\right)^{n}\cdot\frac{n^{2n}}{(n!)^2} = a_n.$$

$$a_2 = \left(\frac{\pi}{4}\right)^2\cdot\frac{2^4}{2^2} = \frac{\pi^2}{4}.$$

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} \geq \frac{\pi}{4}(1+2+\cdots) \geq \frac{3\pi}{4}$$

$$\Rightarrow a_n \geq \frac{\pi^2}{4}\cdot\left(\frac{3\pi}{4}\right)^{n-2} = \frac{\pi}{3}\cdot\left(\frac{3\pi}{4}\right)^{n-1}. \quad \square$$

Some example calculation.

* $K=\mathbb{Q}(i)$, $A=\mathbb{Z}[i]$.

By Cor 3.2, for any $\bar{\alpha}\in C(A)$, $\exists\ \beta\subseteq A$, $N(\beta)\leq\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d|^{\frac{1}{2}}$

Note $d=\left(\det(\sigma_i(x_j))\right)^2$, $x_1=1, x_2=i$, $\Rightarrow d=\left(\det\begin{pmatrix}1 & 1\\ i & -i\end{pmatrix}\right)^2=-4$.

$$\Rightarrow N(\beta)\leq\left(\frac{4}{\pi}\right)^1\cdot\frac{2!}{2^2}\sqrt{4} = \frac{4}{\pi} = 1+\varepsilon < 2.$$

$N(\beta)<2 \Rightarrow N(\beta)=1 \Rightarrow \beta=A! \Rightarrow C(A)=\{1\}! \Rightarrow A$ is PID!
(this gives another pf that $\mathbb{Z}[i]$ is PID).

* $K = \mathbb{Q}(\sqrt{6})$, $A = \mathbb{Z}[\sqrt{6}] = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\sqrt{6}$

$$d = \left(\begin{vmatrix} 1 & \sqrt{6} \\ 1 & -\sqrt{6} \end{vmatrix} \right)^2 = 24.$$

$$\left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{1/2} = 1 \cdot \frac{2}{4} \cdot \sqrt{24} = \sqrt{6} = 2.44\ldots$$

$\Rightarrow \forall\, \bar{\alpha} \in C(A),\ \exists\, \beta \subseteq A,\ \bar{\beta} = \bar{\alpha},\ N(\beta) \leq 2.44 \Rightarrow N(\beta) \leq 2.$

Note $(2, \sqrt{6})$ has norm 2, since $\mathbb{Z}[\sqrt{6}] / (2, \sqrt{6}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Claim: $(2, \sqrt{6})$ is the unique ideal of norm 2.

Pf: $\#|A/I| = 2 \Rightarrow 2 \in I \Rightarrow I = (2, a_1 + b_1\sqrt{6}, \ldots, a_n + b_n\sqrt{6})$

can modify $a_i, b_i \in \{0, 1\}$

impossible to have $1 \in I$, or $1 + \sqrt{6} \in I$, otherwise $I = A$.

only possible is $I = (2, \sqrt{6})$.

$\Rightarrow \#|C(A)| \leq 1 + 1 = 2.$

However, after careful analysis, $(2, \sqrt{6}) = (2 + \sqrt{6})$!

$2 = (2 + \sqrt{6})(\sqrt{6} - 2)$

$\sqrt{6} = (2 + \sqrt{6})(3 - \sqrt{6})$

$\Rightarrow \#|C(A)| = 1 \Rightarrow A$ is PID!

Chapter 5, Dirichlet's unit thm

§1. Main Thm

$[K:\mathbb{Q}]=n$, $r_1+2r_2=n$. Study $A^\times$.

Main Thm (Dirichlet's unit thm). Let $r=r_1+r_2-1$, then

$$A^\times \simeq \mathbb{Z}^r \times H,$$

where H is a finite cyclic group. In fact

$$H=\{x\in K^\times \mid x^m=1 \text{ for some } m\} \text{ (i.e., all roots of unity)}$$

Pf is long, $\rightsquigarrow$ 3 steps.

Step 1: The finite part (torsion part) H.

Recall $\sigma: K \hookrightarrow \mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$, $x\mapsto(\sigma_1(x),\cdots,\sigma_{r_1+r_2}(x))$

Consider $L: K^\times \longrightarrow \mathbb{R}^{r_1+r_2}$

$$x \longmapsto \left(\log|\sigma_1(x)|,\cdots,\log|\sigma_{r_1+r_2}(x)|\right), \text{ here } |\cdot|=|\cdot|_{\mathbb{C}}$$

note $x\neq 0 \Rightarrow \sigma_i\neq 0 \Rightarrow L$ is well-defined

It is a group homo $L(xy)=L(x)+L(y)$.

Call it: logarithmic embedding of $K^\times$. (it is NOT injective!)

Lem 1.1: $x\in A^\times \Leftrightarrow x\in A$, and $N(x)=\pm 1$.

Pf: "$\Rightarrow$" $N(x)N(x^{-1})=N(1)=1$, and $N(x), N(x^{-1})\in\mathbb{Z}$, $\Rightarrow N(x)=\pm 1$.

"$\Leftarrow$" If $N(x)=\pm 1$, $\mathrm{Irr}(x,\mathbb{Q})=T^n+a_{n-1}T^{n-1}+\cdots+a_1T+a_0$

$\Rightarrow N(x)=(-1)^n a_0 \Rightarrow a_0=\pm 1$

$\Rightarrow x(x^{n-1}+a_{n-1}x^{n-2}+\cdots+a_1)=\mp 1 \Rightarrow x\in A^\times$. $\square$

Lem 1.2: Let $B\subseteq \mathbb{R}^{r_1+r_2}$ a cpt subset, then $B'=L^{-1}(B)\cap A^\times$ is finite set

Pf: B bnded $\Rightarrow \exists$ some $\alpha>0$, $\alpha^{-1}\le|\sigma_i(x)|\le\alpha$, $\forall x\in B'$, $\forall 1\le i\le r_1+r_2$

$\Rightarrow \alpha^{-1}\le|\sigma_i(x)|\le\alpha$, $\forall\ 1\le i\le n$.

Note $\mathrm{Irr}(x,\mathbb{Q})$ is a factor of $\prod_{i=1}^{n}(T-\sigma_i(x))$

$|\sigma_i(x)|$ bnded $\Rightarrow$ coeff of $\prod(T-\sigma_i(x))$ are bnded

but $\prod_{i=1}^{n}(T-\sigma_i(x)) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0 \in \mathbb{Z}[T]$

$\Rightarrow$ only fin many possibilities of a_i

$\Rightarrow$ only fin many possibilities of x. $\square$

Now, Step 1 of Pf of Main Thm:

Let $H := \ker L \cap A^\times = L^{-1}(\{0\}) \cap A^\times$ a finite set by Lem 1.1.

By Chapter 1, Cor 3.7, any fin subgp of $K^\times$ (any field) is a cyclic gp, consisting of roots of unity.

On the other hand, if $x \in K^\times$ s.t. $x^m = 1$ for some m, then $x \in A^\times$, and $0 = L(x^m) = m L(x) \Rightarrow x \in H$.

Now, the image $L(A^\times) \subseteq \mathbb{R}^{r_1+r_2}$ is a discrete subgp.

It is discrete bec for any cpt $B \subseteq \mathbb{R}^{r_1+r_2}$, $L(A^\times) \cap B$ is finite

$\Rightarrow L(A^\times) \simeq \mathbb{Z}^s$ for some $s \le r_1+r_2$ (using Chap 4, Thm 1.2).

i.e. $A^\times / H \simeq L(A^\times)$

This implies $A^\times \simeq H \times \mathbb{Z}^s$ (bec $\mathbb{Z}^s$ is a free group),

(e.g. see Lemma below Thm 3.1 of Chap 1).

which is recall: if $M \twoheadrightarrow N$ a surj. hom of A-mod st N is fin. free, then $M \simeq N \oplus \ker f$.

In conclusion, we have $A^\times \simeq H \times \mathbb{Z}^s$. It remains to show $s = r_1 + r_2 - 1$. $\square$

Step 2 We show $s \le r_1 + r_2 - 1$

Note $x \in A^\times \Rightarrow N(x) = \pm 1 \Rightarrow 1 = |N(x)| = \prod_{i=1}^{n} |\sigma_i(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \cdot \prod_{j=r_1+1}^{r_1+r_2} |\sigma_i(x)|^2$.

$\Rightarrow$ If $(y_1, \ldots, y_{r_1+r_2}) \in L(A^\times)$, then $\sum_{i=1}^{r_1} y_i + 2\sum_{j=r_1+1}^{r_1+r_2} y_j = 0$ $\circledast$

i.e. $L(A^\times) \subseteq W \subseteq \mathbb{R}^{r_1+r_2}$ where W the hyperplane $\circledast$

and $\dim_{\mathbb{R}} W = r_1 + r_2 - 1 \Rightarrow s \le r_1 + r_2 - 1$. $\square$