Step 3 Finally, show $s = r_1 + r_2 - 1$

Have
$$\begin{array}{ccccc}
\{x \in A, |N(x)|=1\} = A^\times & \xrightarrow{\sigma}_{\sim} & U := \sigma(A^\times) & \xrightarrow{\log|\cdot|} & \Gamma = L(A^\times) \\
\downarrow & & \downarrow & & \downarrow \\
\{x \in K, |N(x)|=1\} & \xrightarrow{\sigma}_{\sim} & G = \sigma(\{\}) & \xrightarrow{\log|\cdot|} & W \\
\downarrow & & \downarrow & & \downarrow \\
K^\times & \xrightarrow{\sigma} & (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} & \xrightarrow{\log|\cdot|} & \mathbb{R}^{r_1+r_2}
\end{array}$$

where $W :=$ the image of $\log|\cdot|$, which is precisely the hyperplane above.
Now, we WANT: $\Gamma \cong \mathbb{Z}^s \subseteq W$ to be a full lattice.

Thm 1.3: Suppose $B \subseteq \mathbb{R}^n$ a discrete subgp ($\Rightarrow B \cong \mathbb{Z}^r$), then B is a lattice ($\Leftrightarrow r = n$) $\Leftrightarrow$ $\exists$ a bnded subset $M \subseteq \mathbb{R}^n$, s.t. $\mathbb{R}^n = \bigcup_{\gamma \in B} (M + \gamma)$

Pf: "$\Rightarrow$": Let $\Gamma = \bigoplus_{i=1}^n \mathbb{Z} e_i$, then let $M := \{\sum_{i=1}^n \alpha_i e_i,\ 0 \le \alpha_i < 1\}$.

"$\Leftarrow$": let $V_0 = \mathbb{R}$-span of vectors in B, $V_0 \subseteq \mathbb{R}^n$, WANT, $V_0 = \mathbb{R}^n$.
Take any $v \in \mathbb{R}^n$, since $\mathbb{R}^n = \bigcup_{\gamma \in B} (M + \gamma)$.

thus $\forall\ k \ge 1$, $kv = a_k + \gamma_k$ for some $a_k \in M$, $\gamma_k \in B$.
M bnded $\Rightarrow \lim \frac{a_k}{k} = 0$
$$v = \lim_{k\to\infty} \frac{a_k}{k} + \frac{\gamma_k}{k} = 0 + \lim_{k\to\infty} \frac{\gamma_k}{k} \in V_0 \quad (V_0 \text{ is closed})$$ □

Claim ⊛ : $\exists$ cpt subset $T \subseteq G$, s.t. $G = \bigcup_{u \in U = \sigma(A^\times)} uT$

Suppose Claim ⊛ is true,

then $W = \bigcup_{\gamma \in \Gamma} (\log(|T|) + \gamma)$.

By Lem 1.3, it suffices to show $\log(|T|)$ is bnded.

$T \subseteq G \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ cpt $\Rightarrow \exists \alpha > 0$ s.t. if $(x_1, \dots, x_{r_1}, y_1, \dots, y_{r_2}) \in T$, then $|x_i|, |y_j| \le \alpha$.

also $\prod |x_i| \cdot \prod |y_j|^2 = 1$ since $T \subseteq G$.

$\Rightarrow |x_i|, |y_j| \ge \frac{1}{\alpha^{n-1}}$, $\forall i, j$.

i.e. $\exists \tilde{\alpha} > 0$, s.t $\frac{1}{\tilde{\alpha}} \le |x_i|, |y_j| \le \tilde{\alpha}$.

$\Rightarrow \log(|T|) \subseteq (-\log \tilde{\alpha}, \log \tilde{\alpha})^{r_1 + r_2}$ is bnded.

This completes pf of Main Thm ! except Claim ⊛

Lem 1.4 : Let $q \in \mathbb{Z}^{>0}$, then $\exists$ fin. many $a \in A$, up to multiplication by elts in $A^\times$, s.t. $|N(a)| = q$.

pf : $|N(a)| = q \Leftrightarrow N(Aa) = q$

In pf of chapter 4, Thm 3.3, showed, $\exists$ fin. many ideal β s.t $N(\beta) = q$ □

Now prove Claim ⊗ : $\exists$ cpt $T \subseteq G$, s.t. $G = \bigcup_{u \in U} uT$.

Recall $\sigma(A) \subseteq \mathbb{R}^n$ is a lattice. Let $C \subseteq \mathbb{R}^n$, sym to 0, convex, cpt, and $\mu(C) > 2^n \mu(\sigma(A))$.

Previous Chapter, Cor 1.5 $\Rightarrow C \cap (\sigma(A) - \{0\}) \neq \phi$.
For any $g \in G$, ($\Rightarrow g = (x_1, \dots, x_{r_1}, y_1, \dots, y_{r_2})$, $\prod |x_i| \prod |y_j|^2 = 1$)

then gC still sym to 0, convex, cpt, and $\mu(gC) = \mu(C)$
here gC is def by coordinate-wise multiplication.

$\Rightarrow gC \cap (\sigma(A) - \{0\}) \neq \phi$, $\forall g \in G$.

Now, for any $x = (x_1, \dots, x_{r_1}, y_1, \dots, y_{r_2}) \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$,
denote for short $|N(x)| = \prod |x_i| \prod |y_j|^2$.
And for $S \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, denote $|N(S)| = \{|N(x)|, x \in S\}$.

For each $g \in G$, let $a_g \in gC \cap (\sigma(A) - \{0\})$.
then $|N(a_g)| \in |N(gC)| = |N(C)|$

(C cpt $\Rightarrow$ C bnded $\Rightarrow$ $|N(C)|$ bnded in $\mathbb{R}^{\geq 0}$.
$\Rightarrow \exists$ only finite many integers in $|N(C)|$.
Thus by Lem 1.4 above, $\exists$ fin. many $a_1, \dots, a_m \in A$, (a whose norm $\in |N(C)|$), s.t.

$$gC \cap \left(\bigcup_{i=1}^{m} a_i U \right) \neq \phi, \quad \forall g \in G.$$

(i.e, those a_g above $\in \{\sigma(a_1), \dots, \sigma(a_m)\}$ up to units)

Now, let $T = G \cap \left(\bigcup_{i=1}^{m} a_i^{-1} C \right)$, we check it satisfies Claim ⊗.

① "T is cpt."

C cpt $\Rightarrow a_i^{-1}C$ cpt $\Rightarrow \bigcup a_i^{-1}C$ cpt

$G \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ closed (easy to see by defn)

$\Rightarrow T$ is cpt (a closed subset of cpt set is cpt)

② "$G = \bigcup_{u \in U} uT$."

Let $g \in G$, consider $g^{-1}C$, it meets some $a_i U$

i.e. $g^{-1}C = a_i u$, for some $c \in C$, $u \in U$.

$\Rightarrow g = \underbrace{c \cdot a_i^{-1}}_{\in T} \cdot \underbrace{u^{-1}}_{\in U} \in RHS.$ □

Cor. of Main Thm: Let $r = r_1 + r_2 - 1$, then $\exists u_1, \dots, u_r \in A^X$, s.t.

$\forall u \in A^X$, $u = \zeta \cdot u_1^{n_1} \cdots u_r^{n_r}$ for some $n_i \in \mathbb{Z}$, ζ a root of unity in K^X.

Pf: obv.

(call the set $(u_1, \dots, u_r)$ a set of fundamental system of units of K (not unique!)

§2. Units in imaginary quadratic fields.

$K = \mathbb{Q}(\sqrt{-m})$, $m > 0$, squarefree

$r_1 = 0$, $r_2 = 1$ $\quad r = r_1 + r_2 - 1 = 0$.

Unit Thm $\Rightarrow A^\times \simeq H = \{$roots of unity in $K^\times\}$

We can also explicitly prove above.

Case ①. $m \equiv 1, 2 \pmod 4$ $\quad (-m \equiv 3, 2 \pmod 4) \Rightarrow A = \mathbb{Z}[\sqrt{-m}]$

$x = a + b\sqrt{-m} \in A^\times \Leftrightarrow N(x) = \pm 1 \Leftrightarrow a^2 + mb^2 = \pm 1 \Leftrightarrow a^2 + mb^2 = 1$

$\begin{cases} \text{if } m \geq 2, \Rightarrow b = 0,\ a = \pm 1 & x = \pm 1 \Rightarrow A^\times = \{\pm 1\} \\ m = 1, \Rightarrow \begin{cases} b = 0 \\ a = \pm 1 \end{cases}, \begin{cases} b = \pm 1 \\ a = 0 \end{cases} & x = \pm 1, \pm i \Rightarrow A^\times = \{\pm 1, \pm i\} \end{cases}$

Case ②. $m \equiv 3 \pmod 4 \Rightarrow -m \equiv 1 \pmod 4 \Rightarrow A = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \left(\frac{1+\sqrt{-m}}{2}\right)$

$x = a + b\left(\frac{1+\sqrt{-m}}{2}\right) \in A^\times \Leftrightarrow \left(a + \frac{b}{2}\right)^2 + m \cdot \left(\frac{b}{2}\right)^2 = \pm 1$

$\Leftrightarrow (2a+b)^2 + mb^2 = 4$

$\begin{cases} m > 3 \Rightarrow m \geq 7 \Rightarrow b = 0 \Rightarrow a = \pm 1 \Rightarrow A^\times = \{\pm 1\} \\ m = 3, \begin{cases} b = 0 \\ a = \pm 1 \end{cases} \text{ or } \begin{cases} b = 1 \\ a = 0, -1 \end{cases} \text{ or } \begin{cases} b = -1 \\ a = 0, 1 \end{cases} \Rightarrow A^\times = \left\{\pm 1, \pm\left(\frac{1+\sqrt{-3}}{2}\right), \pm\left(\frac{1-\sqrt{-3}}{2}\right)\right\} \end{cases}$

Rmk. $A^\times = \{\pm 1\}$ except when $m = 1$ or 3.

§3. Units in real quadratic fields

$K = \mathbb{Q}(\sqrt{d})$, $d > 0$, sqfree

$r_1 = 2, r_2 = 0, \quad r = r_1 + r_2 - 1 = 1 \Rightarrow A^\times \simeq \mathbb{Z} \times H$

Since $H \subseteq K \subseteq \mathbb{R}$ roots of unity in $\mathbb{R}$ $= \{\pm\} \Rightarrow H = \{\pm 1\} \Rightarrow A^\times \simeq \mathbb{Z} \times \{\pm 1\}$

Denote $(A^\times)^+ :=$ positive units, then $(A^\times)^+ \simeq \mathbb{Z}$, a cyclic gp.

Only two generators of $\mathbb{Z}$: $-1, +1$.

$\Rightarrow$ only two generators of $(A^\times)^+$, $\chi, 1/\chi$.

Only one of χ or $1/\chi$ > 1; call it <u>the fundamental unit</u> of K.

<u>Case 1</u> $d \equiv 2, 3 \pmod 4$ $A = \mathbb{Z}[\sqrt{d}]$

Suppose $\chi = a + b\sqrt{d}$ is the <u>fundamental unit</u>, i.e. $\chi > 1$

then $N(\chi) = a^2 - d \cdot b^2 = \pm 1$

$\chi^{-1} = a - b\sqrt{d} < 1$

$-\chi = -a - b\sqrt{d} < 0$

$-\chi^{-1} = -a + b\sqrt{d} < 0.$

$\Rightarrow \begin{cases} a + b\sqrt{d} > 1 > 0 > -a + b\sqrt{d} \Rightarrow a > 0 \\ a + b\sqrt{d} > 1 > a - b\sqrt{d} \Rightarrow b > 0. \end{cases}$

i.e. if χ is fund unit, then $a, b > 0$, and $(A^\times)^+ \simeq \{(a+b\sqrt{d})^n,\ n \in \mathbb{Z}\}$

Let $\chi_n = (a+b\sqrt{d})^n$, $n > 0$, and write $\chi_n = a_n + b_n\sqrt{d}$.

then $\chi_{n+1} = (a+b\sqrt{d})(a_n + b_n\sqrt{d})$

$= (aa_n + dbb_n) + (ab_n + ba_n)\sqrt{d}$

$= a_{n+1} + b_{n+1}\sqrt{d}$

$\Rightarrow a_{n+1} > a_n, \quad b_{n+1} > b_n$

In order to find χ_1 the fund unit, write down $d \cdot 1^2, d \cdot 2^2, \cdots$

stop when ± 1 becomes a square in $\mathbb{Z}$.

Ex: $d=2$, $d\cdot 1^2=2$ ✓ $2-1=1 \Rightarrow x_1=1+\sqrt{2}$

$d=3$, $d\cdot 1^2=3$ ✓ $3+1=4 \Rightarrow x_1=2+\sqrt{3}$

$d=6$, $d\cdot b^2: 6, 24$ ✓, $24+1=5^2 \Rightarrow x_1=5+2\sqrt{6}$

$d=7$, $d\cdot b^2: 7, 28, 63$ ✓ $63+1=8^2 \Rightarrow x_1=8+3\sqrt{7}$

Case ②, $d\equiv 1 \pmod 4$ $A=\mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\left(\frac{1+\sqrt{d}}{2}\right)$

any $x\in A$ is $x=\frac{1}{2}(a+b\sqrt{d})$, $a,b\in\mathbb{Z}$, $2\mid a-b$.

$N(x)=\pm 1 \Rightarrow a^2-db^2=\pm 4$.

Let $x_1=\frac{1}{2}(a_1+b_1\sqrt{d})$ the fund unit, then $x_n=x_1^n=\frac{1}{2^n}(a_n+b_n\sqrt{d})$

then again $a_{n+1}>a_n$, $b_{n+1}>b_n$

To find x_1, use similar strategy: write down $d\cdot 1^2, d\cdot 2^2, \dots$, ± 4 to get a square in $\mathbb{Z}$.

Ex $d=5$, $5\cdot 1^2$ ✓ $5+4=3^2 \Rightarrow x_1=\frac{1}{2}(3+\sqrt{5})$

$d=13$, $13\cdot 1^2$ ✓ $13-4=3^2 \Rightarrow x_1=\frac{1}{2}(3+\sqrt{13})$

$d=17$, $17\cdot 1^2$, $17\cdot 2^2=68$ ✓ $68-4=8^2$, $x_1=\frac{1}{2}(8+2\sqrt{17})$

Chapter 6 , Galois theory

Common Notations: $K \subseteq E \subseteq F$ field ext. If $K \subseteq E \subseteq F$, call E an intermediate ext.

$f: E \to F$ field hom, always $f(0)=0$, $f(1)=1$. ($\Rightarrow f$ injective)

§1. Galois extension

Defn $f: E \to F$ is called a <u>K-homomorphism</u> if f is a field hom and is also a K-mod homomorphism.

Equivalently, f is a K-hom $\Leftrightarrow$ f is a field hom and $f(k)=k$, $\forall k \in K$.

Denote $\mathrm{Aut}_K F := \{\sigma: F \to F$ K-automorphism (i.e., K-hom + bijection)$\}$.

Note ① if $[F:K]<\infty$, then any K-hom is a K-automorphism.

② $\mathrm{Aut}_K F$ is a gp (not nece. ab.)

Lem 1.1 $K \subseteq F$, $f \in K[T]$, $u \in F$, s.t. $f(u)=0$, $\sigma \in \mathrm{Aut}_K F$.
Then $f(\sigma(u))=0$.

Pf: Easy. It says $\mathrm{Aut}_K F$ acts on F-roots of $f(T)$.

Ex: (1) $\mathrm{Aut}_K K = \{id\}$

(2) $\mathrm{Aut}_K F = \{id\} \not\Rightarrow F=K$! e.g. $\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = \{id\}$

(3) $\mathrm{Aut}_{\mathbb{R}} \mathbb{C} = \mathrm{Aut}_{\mathbb{R}} \mathbb{R}[i] = \{id, \text{conj}\} \simeq \mathbb{Z}/2\mathbb{Z}$.

(4) $\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \simeq \mathbb{Z}/2\mathbb{Z}$.

(5) $\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(6) $\mathrm{Aut}_{\mathbb{F}_p} \mathbb{F}_{p^n} \simeq \mathbb{Z}/n\mathbb{Z}$.

(7) $\mathrm{Aut}_{\mathbb{F}_p(x)} \mathbb{F}_p(x^{\frac{1}{p}}) \simeq \{id\}$.

No.

Date

Lem 1.2. Let $K \subseteq E \subseteq F$, Let $H \subseteq \mathrm{Aut}_K F$ subgp. Then

(1) $H' := F^H := \{x \in F \mid \sigma(x) = x, \ \forall \sigma \in H\}$ is an intermed. ext.
i.e. $K \subseteq H' \subseteq F$.

(2) $E' := \mathrm{Aut}_E F := \{\sigma \in \mathrm{Aut}_K F \mid \sigma(u) = u, \ \forall u \in E\} \subseteq \mathrm{Aut}_K F$ is a subgp.

Pf. easy. Call H': fixed fied of H.

Defn. $K \subseteq F$. If $(\mathrm{Aut}_K F)' = F^{\mathrm{Aut}_K F} = K$, then say F is a Galois extension of K. Also say F is Galois over K, or F/K is Galois.
(In this case, also use $\mathrm{Ga}(F/K) := \mathrm{Aut}_K F$

Thm 1.3. (Fundamental Thm of Galois theory, the finite case)

Suppose $K \subseteq F$, $[F:K] < \infty$, and F is Galois over K. Then there is a bijection between

$$\{E \mid K \subseteq E \subseteq F, \text{ intermediate ext}\} \longrightarrow \{H \mid H \subseteq \mathrm{Aut}_K F \text{ subgp}\}$$

given by: $E \longmapsto E' := \mathrm{Aut}_E F$,

such that

(1) If $K \subseteq E_1 \subseteq E_2 \subseteq F$, then $[E_2 : E_1] = [E_1' : E_2']$

(2) For $K \subseteq E \subseteq F$, F/E is Galois, Then E/K is Galois $\Leftrightarrow E' \subseteq \mathrm{Aut}_K F$ is normal subgp.
In this case $\mathrm{Aut}_K F / E' \simeq \mathrm{Aut}_K E$.

Rmk: (1) $\Rightarrow \#|\mathrm{Aut}_K F| = [F:K]$.

To prove Thm, it suffices to show $\begin{cases} (E')' = E. & \Rightarrow \text{injection} \\ (H')' = H & \Rightarrow \text{surjection} \end{cases}$

Lem. 14. $K \subseteq L \subseteq F$, $K \subseteq M \subseteq F$. $H < G = \mathrm{Aut}_K F$. Then

(1) $F' = 1$, $K' = G$; $1' = F$. (recall $G' = K \Leftrightarrow F/K$ Gal)
(2) $L \subseteq M \Rightarrow M' < L'$; $H < J \Rightarrow J' < H'$.
(3) $L \subseteq L''$; $H < H''$ (here $L'' = (L')'$, etc)
(4) $L' = L'''$; $H' = H'''$.

Pf: (1), (2), (3) trivial.
For (4): (3) $\Rightarrow L' < (L')'' = L'''$, and $L \subseteq L''$, use (2) $\Rightarrow L''' < L'$ $\Rightarrow L' = L'''$.
Similarly $H' = H'''$. □

Lem 15. $K \subseteq L \subseteq M \subseteq F$. If $[M:L] < \infty$, then $[L':M'] \leq [M:L]$.
(In particular, $[F:K] < \infty \Rightarrow |\mathrm{Aut}_K F| \leq [F:K]$)

Pf. Induction on $n = [M:L]$. $n = 1$ trivial.
Suppose true for $[M:L] < n$. Consider when $[M:L] = n$. (> 1)
Let $u \in M - L$.

$$\begin{array}{ccc} F & \longmapsto & \mathrm{Aut}_F F = 1 \\ \cup & & \wedge \\ M & \longmapsto & M' \\ \cup & & \wedge \\ L(u) & \longmapsto & L(u)' \\ \cup & & \wedge \\ L & \longmapsto & L' \\ \cup & & \wedge \\ K & \longmapsto & \mathrm{Aut}_K F \end{array}$$

If $[L(u):L] < n$, i.e. $M \neq L(u)$, then induction hypo $\Rightarrow$
$[M:L] = [M:L(u)]\,[L(u):L] \geq [L(u)':M']\,[L':L(u)'] = [L':M']$.

Otherwise, $M = L(u)$.

Let $f(T) = \mathrm{Irr}(u, L)$, then $[M:L] = \deg f(T)$.

$= \#\{\text{roots of } f(T) \text{ in } \bar{L}\}$.

Also, $[L':M'] = [\mathrm{Aut}_L F : \mathrm{Aut}_{L(u)} F]$

We define a map from left cosets $M' \backslash L'$ to $\{\text{roots of } f(T) \text{ in } F\}$

$$\sigma \cdot \mathrm{Aut}_{L(u)} F \longmapsto \sigma(u)$$

Since $\mathrm{Aut}_{L(u)} F$ fixes u, this map is well-def.

Claim. The map is injective.

if $\sigma_1(u) = \sigma_2(u) \Rightarrow \sigma_1 \cdot \sigma_2^{-1}(u) = u$.

$\Rightarrow \sigma_1 \cdot \sigma_2^{-1}$ fixes $L(u)$

$\Rightarrow \sigma_1 \cdot \sigma_2^{-1} \in \mathrm{Aut}_{L(u)} F$ □.

Inj map $\Rightarrow \#|M' \backslash L'| \leq \#\{\text{roots of } f(T) \text{ in } F\} \leq \{\text{roots in } \bar{L}\} = [M:L]$

i.e. $[L':M'] \leq [M:L]$. □.