Math 361

April 14, 2023

Projects

Today

Every element of the class group $\mathcal{H}$ is represented by an ideal with norm at most

$$\left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}.$$

Review

- If $\mathfrak{a}$ is an ideal of K, why is $N(\mathfrak{a}) \in \mathfrak{a}$?

Review

- If $\mathfrak{a}$ is an ideal of K, why is $N(\mathfrak{a}) \in \mathfrak{a}$?
- Why are there only finitely many ideals of a given norm?

Fractional ideals

Let K be a number field, and let $I \subseteq K$ be an $\mathfrak{O}_K$-module. Recall that I is a *fractional ideal* of $\mathfrak{O}_K$ if it satisfies any of the following equivalent conditions:

Fractional ideals

Let K be a number field, and let $I \subseteq K$ be an $\mathfrak{O}_K$-module. Recall that I is a *fractional ideal* of $\mathfrak{O}_K$ if it satisfies any of the following equivalent conditions:

1. There exists $\alpha \in K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.

Fractional ideals

Let K be a number field, and let $I \subseteq K$ be an $\mathfrak{O}_K$-module. Recall that I is a *fractional ideal* of $\mathfrak{O}_K$ if it satisfies any of the following equivalent conditions:

1. There exists $\alpha \in K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.
2. There exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.

Fractional ideals

Let K be a number field, and let $I \subseteq K$ be an $\mathfrak{O}_K$-module. Recall that I is a *fractional ideal* of $\mathfrak{O}_K$ if it satisfies any of the following equivalent conditions:

1. There exists $\alpha \in K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.
2. There exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.
3. There exists an ordinary ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ and $\alpha \in K \setminus \{0\}$ such that $I = \alpha\mathfrak{a}$.

Fractional ideals

Let K be a number field, and let $I \subseteq K$ be an $\mathfrak{O}_K$-module. Recall that I is a *fractional ideal* of $\mathfrak{O}_K$ if it satisfies any of the following equivalent conditions:

1. There exists $\alpha \in K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.
2. There exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.
3. There exists an ordinary ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ and $\alpha \in K \setminus \{0\}$ such that $I = \alpha\mathfrak{a}$.
4. There exists an ordinary ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ and $\beta \in \mathfrak{O}_K \setminus \{0\}$ such that $I = \frac{1}{\beta}\mathfrak{a}$.

Fractional ideals

Let K be a number field, and let $I \subseteq K$ be an $\mathfrak{O}_K$-module. Recall that I is a *fractional ideal* of $\mathfrak{O}_K$ if it satisfies any of the following equivalent conditions:

1. There exists $\alpha \in K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.
2. There exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.
3. There exists an ordinary ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ and $\alpha \in K \setminus \{0\}$ such that $I = \alpha\mathfrak{a}$.
4. There exists an ordinary ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ and $\beta \in \mathfrak{O}_K \setminus \{0\}$ such that $I = \frac{1}{\beta}\mathfrak{a}$.
5. I is finitely generated as an $\mathfrak{O}_K$-module.

Principal fractional ideals

A *principal fractional ideal* is defined to be a fractional ideal generated as an $\mathfrak{O}_K$-module by a single element.

Principal fractional ideals

A *principal fractional ideal* is defined to be a fractional ideal generated as an $\mathfrak{O}_K$-module by a single element.

Thus, a nonzero principal fractional ideal has the form $\alpha\mathfrak{O}_K$ for some $\alpha \in K \setminus \{0\}$.

The class group

Definition. The *class group* of $\mathfrak{O}_K$ is the quotient group

$$\mathcal{H} = \mathcal{F}/\mathcal{P}.$$

The class group

Definition. The *class group* of $\mathfrak{O}_K$ is the quotient group

$$\mathcal{H} = \mathcal{F}/\mathcal{P}.$$

The *class number* of $\mathfrak{O}_K$ is the size of this group:

$$h_K = |\mathcal{H}|.$$

First observations

Proposition. Every element of $\mathcal{H}$ is represented by an ordinary ideal of $\mathfrak{O}_K$.

First observations

Proposition. Every element of $\mathcal{H}$ is represented by an ordinary ideal of $\mathfrak{O}_K$.

Proof. Let $I = \alpha\mathfrak{a}$ where $\alpha \in K \setminus \{0\}$ and $\mathfrak{a}$ is an ordinary ideal.

First observations

Proposition. Every element of $\mathcal{H}$ is represented by an ordinary ideal of $\mathfrak{O}_K$.

Proof. Let $I = \alpha\mathfrak{a}$ where $\alpha \in K \setminus \{0\}$ and $\mathfrak{a}$ is an ordinary ideal.

Then $\alpha\mathfrak{O}_K$ is a principal fractional ideal.

First observations

Proposition. Every element of $\mathcal{H}$ is represented by an ordinary ideal of $\mathfrak{O}_K$.

Proof. Let $I = \alpha\mathfrak{a}$ where $\alpha \in K \setminus \{0\}$ and $\mathfrak{a}$ is an ordinary ideal.

Then $\alpha\mathfrak{O}_K$ is a principal fractional ideal.

Therefore,

$$I = \alpha\mathfrak{a} = (\alpha\mathfrak{O}_K)\mathfrak{a} = \mathfrak{a} \bmod \mathcal{P}.$$

□

$h = 1$ if and only if $\mathfrak{O}_K$ is a UFD

Proposition. $\mathfrak{O}_K$ is a UFD if and only if $h_K = 1$, i.e., if and only if the class group is trivial.

The class group is finite

Theorem. Every element of $\mathcal{H}$ is represented by an ideal with norm at most

$$\left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}$$

where $2t$ is the number of complex embeddings of K and Δ is the discriminant of K.

The class group is finite

Theorem. Every element of $\mathcal{H}$ is represented by an ideal with norm at most

$$\left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}$$

where $2t$ is the number of complex embeddings of K and Δ is the discriminant of K.

Proof. Main goal for today.

The class group is finite.

Corollary. The class group $\mathcal{H}$ is finite.

The class group is finite.

Corollary. The class group $\mathcal{H}$ is finite.

Proof. Recall that there are finitely many ideals with a given norm.

The class group is finite.

Corollary. The class group $\mathcal{H}$ is finite.

Proof. Recall that there are finitely many ideals with a given norm.

By the previous theorem, each element of $\mathcal{H}$ is represented by an ideal of norm at most $(2/\pi)^t\sqrt{|\Delta|}$.

The class group is finite.

Corollary. The class group $\mathcal{H}$ is finite.

Proof. Recall that there are finitely many ideals with a given norm.

By the previous theorem, each element of $\mathcal{H}$ is represented by an ideal of norm at most $(2/\pi)^t\sqrt{|\Delta|}$.

There are only finitely many positive integers less than this bound.
$\square$

Corollary

Corollary. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$, and let $h = |\mathcal{H}|$ be the class number of K. Then

1. $\mathfrak{a}^h$ is principal, and
2. If $u \in \mathbb{N}$ is relatively prime to h, and $\mathfrak{a}^u$ is principal, then $\mathfrak{a}$ is principal.

Corollary

Corollary. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$, and let $h = |\mathcal{H}|$ be the class number of K. Then

1. $\mathfrak{a}^h$ is principal, and
2. If $u \in \mathbb{N}$ is relatively prime to h, and $\mathfrak{a}^u$ is principal, then $\mathfrak{a}$ is principal.

Example. We saw that the class number of $\mathbb{Q}(\sqrt{-5})$ is 2.

Corollary

Corollary. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$, and let $h = |\mathcal{H}|$ be the class number of K. Then

1. $\mathfrak{a}^h$ is principal, and
2. If $u \in \mathbb{N}$ is relatively prime to h, and $\mathfrak{a}^u$ is principal, then $\mathfrak{a}$ is principal.

Example. We saw that the class number of $\mathbb{Q}(\sqrt{-5})$ is 2. Therefore, for example, $(2, 1+\sqrt{-5})^2$ is principal.

Review

Let K be a number field of degree n with real embeddings $\sigma_1, \ldots, \sigma_s$, and complex embeddings $\sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma}_{s+t}$.

Review

Let K be a number field of degree n with real embeddings $\sigma_1, \ldots, \sigma_s$, and complex embeddings $\sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma}_{s+t}$.
$\mathbb{Q}$-algebra embedding:

$$\begin{aligned}\sigma_K = \sigma \colon K &\to \mathbb{L}^{s,t} := \mathbb{R}^s \times \mathbb{C}^t \\ \alpha &\mapsto (\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \ldots, \sigma_{s+t}(\alpha)),\end{aligned}$$

Review

Let K be a number field of degree n with real embeddings $\sigma_1, \dots, \sigma_s$, and complex embeddings $\sigma_{s+1}, \overline{\sigma}_{s+1}, \dots, \sigma_{s+t}, \overline{\sigma}_{s+t}$.
$\mathbb{Q}$-algebra embedding:

$$\begin{aligned} \sigma_K = \sigma \colon K &\to \mathbb{L}^{s,t} := \mathbb{R}^s \times \mathbb{C}^t \\ \alpha &\mapsto (\sigma_1(\alpha), \dots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \dots, \sigma_{s+t}(\alpha)), \end{aligned}$$

and our identification

$$\begin{aligned} \mathbb{R}^s \times \mathbb{C}^t &\simeq \mathbb{R}^n \\ (x_1, \dots, x_s, z_1, \dots, z_t) &\mapsto (x_1, \dots, x_s, u_1, v_1, \dots, u_t, v_t) \end{aligned}$$

Review

Define the *norm* of $q = (x_1, \ldots, x_s, z_1, \ldots, z_t) \in \mathbb{R}^s \times \mathbb{C}^t$ to be

$$N(q) = x_1 \cdots x_s z_1 \overline{z_1} \cdots z_t \overline{z_t} = x_1 \cdots x_s |z_1|^2 \cdots |z_t|^2$$

Review

Define the *norm* of $q = (x_1, \ldots, x_s, z_1, \ldots, z_t) \in \mathbb{R}^s \times \mathbb{C}^t$ to be

$$N(q) = x_1 \cdots x_s z_1 \overline{z_1} \cdots z_t \overline{z_t} = x_1 \cdots x_s |z_1|^2 \cdots |z_t|^2$$

It is consistent with our earlier definition: for $\alpha \in K$,

$$N(\alpha) = \sigma_1(\alpha) \cdots \sigma_s(\alpha) \sigma_{s+1}(\alpha) \overline{\sigma}_{s+1}(\alpha) \cdots \sigma_{s+1}(\alpha) \overline{\sigma}_{s+t}(\alpha) = N(\sigma(\alpha)).$$

Review

Main result from last Monday's lecture:

Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{O}_K$. Identifying $\mathbb{L}^{s,t}$ with $\mathbb{R}^n$, regard $\sigma(\mathfrak{a}) \subset \mathbb{R}^n$. Then $\sigma(\mathfrak{a})$ is a lattice with fundamental domain of volume

$$2^{-t} N(\mathfrak{a}) \sqrt{|\Delta|}$$

where Δ is the discriminant of K.

Review

Main result from last Monday's lecture:

Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{O}_K$. Identifying $\mathbb{L}^{s,t}$ with $\mathbb{R}^n$, regard $\sigma(\mathfrak{a}) \subset \mathbb{R}^n$. Then $\sigma(\mathfrak{a})$ is a lattice with fundamental domain of volume

$$2^{-t} N(\mathfrak{a}) \sqrt{|\Delta|}$$

where Δ is the discriminant of K.

(Store this information on the blackboard.)

Theorem 1

Theorem. If $\mathfrak{a}$ is a nonzero ideal of $\mathfrak{O}_K$, then there exists $0 \neq \alpha \in \mathfrak{O}_K$ such that

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}.$$

Theorem 1

Theorem. If $\mathfrak{a}$ is a nonzero ideal of $\mathfrak{O}_K$, then there exists $0 \neq \alpha \in \mathfrak{O}_K$ such that

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}.$$

Proof.

Fix a real number $\varepsilon > 0$, and select positive real numbers $c_1, \ldots, c_{s+t}$ such that

$$c_1 \cdots c_{s+t} = \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}.$$

Theorem 1

Theorem. If $\mathfrak{a}$ is a nonzero ideal of $\mathfrak{O}_K$, then there exists $0 \neq \alpha \in \mathfrak{O}_K$ such that

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}.$$

Proof.
Fix a real number $\varepsilon > 0$, and select positive real numbers $c_1, \dots, c_{s+t}$ such that

$$c_1 \cdots c_{s+t} = \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}.$$

(Store this information on the blackboard.)

Theorem 1

Define $X_\varepsilon \in \mathbb{R}^n$ as

Theorem 1

Define $X_\varepsilon \in \mathbb{R}^n$ as

$x = (x_1, \ldots, x_s, x_{s+1}, y_{s+1}, \ldots, x_{s+t}, y_{s+t}) \in \mathbb{R}^n$ such that

Theorem 1

Define $X_\varepsilon \in \mathbb{R}^n$ as

$x = (x_1, \ldots, x_s, x_{s+1}, y_{s+1}, \ldots, x_{s+t}, y_{s+t}) \in \mathbb{R}^n$ such that

- $|x_1| < c_1 + \varepsilon$,

Theorem 1

Define $X_\varepsilon \in \mathbb{R}^n$ as

$x = (x_1, \ldots, x_s, x_{s+1}, y_{s+1}, \ldots, x_{s+t}, y_{s+t}) \in \mathbb{R}^n$ such that

- $|x_1| < c_1 + \varepsilon$,
- $|x_2| < c_2, \ldots, |x_s| < c_s$,

Theorem 1

Define $X_\varepsilon \in \mathbb{R}^n$ as

$x = (x_1, \ldots, x_s, x_{s+1}, y_{s+1}, \ldots, x_{s+t}, y_{s+t}) \in \mathbb{R}^n$ such that

- $|x_1| < c_1 + \varepsilon$,
- $|x_2| < c_2, \ldots, |x_s| < c_s$,
- $|x_{s+1}^2 + y_{s+1}^2| < c_{s+1}, \ldots, |x_{s+t}^2 + y_{s+t}^2| < c_{s+t}$.

Theorem 1

Define $X_\varepsilon \in \mathbb{R}^n$ as

$x = (x_1, \dots, x_s, x_{s+1}, y_{s+1}, \dots, x_{s+t}, y_{s+t}) \in \mathbb{R}^n$ such that

- $|x_1| < c_1 + \varepsilon$,
- $|x_2| < c_2, \dots, |x_s| < c_s$,
- $|x_{s+1}^2 + y_{s+1}^2| < c_{s+1}, \dots, |x_{s+t}^2 + y_{s+t}^2| < c_{s+t}$.

Then X_ε is centrally symmetric about the origin and convex (exercise).

Theorem 1

Define $X_\varepsilon \in \mathbb{R}^n$ as

$x = (x_1, \ldots, x_s, x_{s+1}, y_{s+1}, \ldots, x_{s+t}, y_{s+t}) \in \mathbb{R}^n$ such that

- $|x_1| < c_1 + \varepsilon$,
- $|x_2| < c_2, \ldots, |x_s| < c_s$,
- $|x_{s+1}^2 + y_{s+1}^2| < c_{s+1}, \ldots, |x_{s+t}^2 + y_{s+t}^2| < c_{s+t}$.

Then X_ε is centrally symmetric about the origin and convex (exercise).

- If $\alpha \in X_\varepsilon$, we have $|N(\alpha)| \leq$

Theorem 1

Define $X_\varepsilon \in \mathbb{R}^n$ as

$x = (x_1, \dots, x_s, x_{s+1}, y_{s+1}, \dots, x_{s+t}, y_{s+t}) \in \mathbb{R}^n$ such that

- $|x_1| < c_1 + \varepsilon$,
- $|x_2| < c_2, \dots, |x_s| < c_s$,
- $|x_{s+1}^2 + y_{s+1}^2| < c_{s+1}, \dots, |x_{s+t}^2 + y_{s+t}^2| < c_{s+t}$.

Then X_ε is centrally symmetric about the origin and convex (exercise).

- If $\alpha \in X_\varepsilon$, we have $|N(\alpha)| \leq (c_1 + \varepsilon)c_2 \dots c_{s+t}$.

Theorem 1

Define $X_\varepsilon \in \mathbb{R}^n$ as

$x = (x_1, \ldots, x_s, x_{s+1}, y_{s+1}, \ldots, x_{s+t}, y_{s+t}) \in \mathbb{R}^n$ such that

- $|x_1| < c_1 + \varepsilon$,
- $|x_2| < c_2, \ldots, |x_s| < c_s$,
- $|x_{s+1}^2 + y_{s+1}^2| < c_{s+1}, \ldots, |x_{s+t}^2 + y_{s+t}^2| < c_{s+t}$.

Then X_ε is centrally symmetric about the origin and convex (exercise).

- If $\alpha \in X_\varepsilon$, we have $|N(\alpha)| \leq (c_1 + \varepsilon)c_2 \ldots c_{s+t}$.
- $\mathrm{vol}(X_\varepsilon) >$

Theorem 1

Define $X_\varepsilon \in \mathbb{R}^n$ as

$x = (x_1, \ldots, x_s, x_{s+1}, y_{s+1}, \ldots, x_{s+t}, y_{s+t}) \in \mathbb{R}^n$ such that

- $|x_1| < c_1 + \varepsilon$,
- $|x_2| < c_2, \ldots, |x_s| < c_s$,
- $|x_{s+1}^2 + y_{s+1}^2| < c_{s+1}, \ldots, |x_{s+t}^2 + y_{s+t}^2| < c_{s+t}$.

Then X_ε is centrally symmetric about the origin and convex (exercise).

- If $\alpha \in X_\varepsilon$, we have $|N(\alpha)| \leq (c_1 + \varepsilon)c_2 \ldots c_{s+t}$.
- $\mathrm{vol}(X_\varepsilon) > [(2c_1) \cdots 2c_s][(\pi c_{s+1}) \cdots (\pi c_{s+t})]$.

Theorem 1

$$\mathrm{vol}(X_\varepsilon) > [(2c_1)\cdots 2c_s][(\pi c_{s+1})\cdots(\pi c_{s+t})]$$

Theorem 1

$$\begin{aligned}\mathrm{vol}(X_\varepsilon) &> [(2c_1)\cdots 2c_s][(\pi c_{s+1})\cdots(\pi c_{s+t})] \\ &= 2^s\pi^t(c_1\cdots c_{s+t})\end{aligned}$$

Theorem 1

$$\begin{aligned}\mathrm{vol}(X_\varepsilon) &> [(2c_1)\cdots 2c_s][(\pi c_{s+1})\cdots(\pi c_{s+t})] \\ &= 2^s\pi^t(c_1\cdots c_{s+t}) \\ &= 2^s\pi^t\left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}\end{aligned}$$

Theorem 1

$$\begin{aligned}\mathrm{vol}(X_\varepsilon) &> [(2c_1)\cdots 2c_s][(\pi c_{s+1})\cdots(\pi c_{s+t})]\\ &= 2^s\pi^t(c_1\cdots c_{s+t})\\ &= 2^s\pi^t\left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|}\\ &= 2^{s+t}N(\mathfrak{a})\sqrt{|\Delta|}\end{aligned}$$

Theorem 1

$$\begin{aligned}
\mathrm{vol}(X_\varepsilon) &> [(2c_1)\cdots 2c_s][(\pi c_{s+1})\cdots(\pi c_{s+t})] \\
&= 2^s \pi^t (c_1 \cdots c_{s+t}) \\
&= 2^s \pi^t \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|} \\
&= 2^{s+t} N(\mathfrak{a})\sqrt{|\Delta|} \\
&= 2^{s+2t} \cdot 2^{-t} N(\mathfrak{a})\sqrt{|\Delta|}
\end{aligned}$$

Theorem 1

$$\begin{aligned}
\mathrm{vol}(X_\varepsilon) &> [(2c_1)\cdots 2c_s][(\pi c_{s+1})\cdots(\pi c_{s+t})] \\
&= 2^s \pi^t (c_1 \cdots c_{s+t}) \\
&= 2^s \pi^t \left(\frac{2}{\pi}\right)^t N(\mathfrak{a})\sqrt{|\Delta|} \\
&= 2^{s+t} N(\mathfrak{a})\sqrt{|\Delta|} \\
&= 2^{s+2t} \cdot 2^{-t} N(\mathfrak{a})\sqrt{|\Delta|} \\
&= 2^n \,\mathrm{vol}(F)
\end{aligned}$$

where F is a fundamental domain for $\sigma(\mathfrak{a})$.

Theorem 1

By Minkowski's theorem, X_ε contains a nonzero point in the lattice $\sigma(\mathfrak{a})$.

Theorem 1

By Minkowski's theorem, X_ε contains a nonzero point in the lattice $\sigma(\mathfrak{a})$.

There exists $0 \neq \beta \in \mathfrak{a}$ such that $\sigma(\beta) \in X_\varepsilon$.

Theorem 1

For each $\varepsilon > 0$, define $A_\varepsilon = \{\beta \in \mathfrak{a} : \beta \neq 0, \sigma(\beta) \in X_\varepsilon\}$

Theorem 1

For each $\varepsilon > 0$, define $A_\varepsilon = \{\beta \in \mathfrak{a} : \beta \neq 0, \sigma(\beta) \in X_\varepsilon\} \neq \emptyset$.

Theorem 1

For each $\varepsilon > 0$, define $A_\varepsilon = \{\beta \in \mathfrak{a} : \beta \neq 0, \sigma(\beta) \in X_\varepsilon\} \neq \emptyset$.

$$A_1 \supseteq A_{1/2} \supseteq A_{1/3} \supseteq \cdots \supseteq A_{1/k} \supseteq \cdots .$$

Take $\alpha \in \bigcap_{k \geq 1} A_{1/k}$.

Theorem 1

For each $\varepsilon > 0$, define $A_\varepsilon = \{\beta \in \mathfrak{a} : \beta \neq 0, \sigma(\beta) \in X_\varepsilon\} \neq \emptyset$.

$$A_1 \supseteq A_{1/2} \supseteq A_{1/3} \supseteq \cdots \supseteq A_{1/k} \supseteq \cdots .$$

Take $\alpha \in \bigcap_{k \geq 1} A_{1/k}$. since $\alpha \in A_{1/k}$ for all $k \geq 1$, we have

$$|N(\alpha)| < (c_1 + 1/k)c_2 \cdots c_{s+t}.$$

Hence,

$$|N(\alpha)| \leq c_1 \cdots c_{s+t} =$$

Theorem 1

For each $\varepsilon > 0$, define $A_\varepsilon = \{\beta \in \mathfrak{a} : \beta \neq 0, \sigma(\beta) \in X_\varepsilon\} \neq \emptyset$.

$$A_1 \supseteq A_{1/2} \supseteq A_{1/3} \supseteq \cdots \supseteq A_{1/k} \supseteq \cdots .$$

Take $\alpha \in \bigcap_{k \geq 1} A_{1/k}$. since $\alpha \in A_{1/k}$ for all $k \geq 1$, we have

$$|N(\alpha)| < (c_1 + 1/k) c_2 \cdots c_{s+t}.$$

Hence,

$$|N(\alpha)| \leq c_1 \cdots c_{s+t} = \left(\frac{2}{\pi}\right)^t N(\mathfrak{a}) \sqrt{|\Delta|}.$$

□

Theorem 2

Theorem. Every element of the class group $\mathcal{H}$ is represented by an ideal with norm at most

$$\left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}.$$

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}$.

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}$.

$(\beta) \subseteq \mathfrak{b}$

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}$.

$(\beta) \subseteq \mathfrak{b} \Rightarrow (\beta)\mathfrak{b}^{-1} \subseteq \mathfrak{O}_K$.

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}$.

$(\beta) \subseteq \mathfrak{b} \Rightarrow (\beta)\mathfrak{b}^{-1} \subseteq \mathfrak{O}_K$. Define $\mathfrak{a} = (\beta)\mathfrak{b}^{-1}$.

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}$.

$(\beta) \subseteq \mathfrak{b} \Rightarrow (\beta)\mathfrak{b}^{-1} \subseteq \mathfrak{O}_K$. Define $\mathfrak{a} = (\beta)\mathfrak{b}^{-1}$.

Then $\mathfrak{a}$ is an ideal representing $\mathfrak{c}$:

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}$.

$(\beta) \subseteq \mathfrak{b} \Rightarrow (\beta)\mathfrak{b}^{-1} \subseteq \mathfrak{O}_K$. Define $\mathfrak{a} = (\beta)\mathfrak{b}^{-1}$.

Then $\mathfrak{a}$ is an ideal representing $\mathfrak{c}$: $[\mathfrak{a}] = [\mathfrak{b}^{-1}]$

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}$.

$(\beta) \subseteq \mathfrak{b} \Rightarrow (\beta)\mathfrak{b}^{-1} \subseteq \mathfrak{O}_K$. Define $\mathfrak{a} = (\beta)\mathfrak{b}^{-1}$.

Then $\mathfrak{a}$ is an ideal representing $\mathfrak{c}$: $[\mathfrak{a}] = [\mathfrak{b}^{-1}] = [\mathfrak{c}]$,

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}$.

$(\beta) \subseteq \mathfrak{b} \Rightarrow (\beta)\mathfrak{b}^{-1} \subseteq \mathfrak{O}_K$. Define $\mathfrak{a} = (\beta)\mathfrak{b}^{-1}$.

Then $\mathfrak{a}$ is an ideal representing $\mathfrak{c}$: $[\mathfrak{a}] = [\mathfrak{b}^{-1}] = [\mathfrak{c}]$,

Finally,

$$N(\mathfrak{a}) =$$

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}$.

$(\beta) \subseteq \mathfrak{b} \Rightarrow (\beta)\mathfrak{b}^{-1} \subseteq \mathfrak{O}_K$. Define $\mathfrak{a} = (\beta)\mathfrak{b}^{-1}$.

Then $\mathfrak{a}$ is an ideal representing $\mathfrak{c}$: $[\mathfrak{a}] = [\mathfrak{b}^{-1}] = [\mathfrak{c}]$,

Finally,

$$N(\mathfrak{a}) = N((\beta))N(\mathfrak{b}^{-1})$$

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}$.

$(\beta) \subseteq \mathfrak{b} \Rightarrow (\beta)\mathfrak{b}^{-1} \subseteq \mathfrak{O}_K$. Define $\mathfrak{a} = (\beta)\mathfrak{b}^{-1}$.

Then $\mathfrak{a}$ is an ideal representing $\mathfrak{c}$: $[\mathfrak{a}] = [\mathfrak{b}^{-1}] = [\mathfrak{c}]$,

Finally,

$$N(\mathfrak{a}) = N((\beta))N(\mathfrak{b}^{-1}) = \frac{|N(\beta)|}{N(\mathfrak{b})}$$

Theorem 2

Proof. Take $[\mathfrak{c}] \in \mathcal{H}$ with $\mathfrak{c}$ an ideal.

Let $\mathfrak{b}$ be an ideal representing $[\mathfrak{c}^{-1}]$.

Take $0 \neq \beta \in \mathfrak{b}$ with $|N(\beta)| \leq \left(\frac{2}{\pi}\right)^t N(\mathfrak{b})\sqrt{|\Delta|}$.

$(\beta) \subseteq \mathfrak{b} \Rightarrow (\beta)\mathfrak{b}^{-1} \subseteq \mathfrak{O}_K$. Define $\mathfrak{a} = (\beta)\mathfrak{b}^{-1}$.

Then $\mathfrak{a}$ is an ideal representing $\mathfrak{c}$: $[\mathfrak{a}] = [\mathfrak{b}^{-1}] = [\mathfrak{c}]$,

Finally,

$$N(\mathfrak{a}) = N((\beta))N(\mathfrak{b}^{-1}) = \frac{|N(\beta)|}{N(\mathfrak{b})} \leq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta|}.$$

□