Math 361

April 12, 2023

Quiz

State and prove Minkowski's lattice point theorem for centrally symmetric convex sets centered at the origin. (You may assume I am familiar with all of the background results needed for the proof.)

Project ideas

Ideas?

Project ideas

Ideas? Some of my ideas:

1. **Discriminants.** Let $K = \mathbb{Q}(\theta)$, and let f be the minimal polynomial for θ. The *discriminant* of f is the discriminant of $\mathbb{Z}[1, \theta, \ldots, \theta^{n-1}]$ where $n = \deg(f) = [K : \mathbb{Q}]$. Show how to compute the discriminant of f from the coefficients of f and its derivative using *resultants*.

Project ideas

Ideas? Some of my ideas:

1. **Discriminants.** Let $K = \mathbb{Q}(\theta)$, and let f be the minimal polynomial for θ. The *discriminant* of f is the discriminant of $\mathbb{Z}[1, \theta, \ldots, \theta^{n-1}]$ where $n = \deg(f) = [K : \mathbb{Q}]$. Show how to compute the discriminant of f from the coefficients of f and its derivative using *resultants*.
2. **Ramification.** Prove that a rational prime p ramifies in a number field K if and only if $p|\Delta$.

Project ideas

Ideas? Some of my ideas:

1. **Discriminants.** Let $K = \mathbb{Q}(\theta)$, and let f be the minimal polynomial for θ. The *discriminant* of f is the discriminant of $\mathbb{Z}[1, \theta, \ldots, \theta^{n-1}]$ where $n = \deg(f) = [K : \mathbb{Q}]$. Show how to compute the discriminant of f from the coefficients of f and its derivative using *resultants*.
2. **Ramification.** Prove that a rational prime p ramifies in a number field K if and only if $p|\Delta$.
3. **Stickelberger's criterion.** Prove that the discriminant of a number field is 0 or 1 modulo 4.

Project ideas

Ideas? Some of my ideas:

1. **Discriminants.** Let $K = \mathbb{Q}(\theta)$, and let f be the minimal polynomial for θ. The *discriminant* of f is the discriminant of $\mathbb{Z}[1, \theta, \ldots, \theta^{n-1}]$ where $n = \deg(f) = [K : \mathbb{Q}]$. Show how to compute the discriminant of f from the coefficients of f and its derivative using *resultants*.
2. **Ramification.** Prove that a rational prime p ramifies in a number field K if and only if $p|\Delta$.
3. **Stickelberger's criterion.** Prove that the discriminant of a number field is 0 or 1 modulo 4.
4. **Polynomial factorization modulo p.** How does one efficiently factor a polynomial modulo p? (There is a wiki page on the subject. Berlekamp's algorithm is the most basic.)

Project ideas

Ideas? Some of my ideas:

1. **Discriminants.** Let $K = \mathbb{Q}(\theta)$, and let f be the minimal polynomial for θ. The *discriminant* of f is the discriminant of $\mathbb{Z}[1, \theta, \ldots, \theta^{n-1}]$ where $n = \deg(f) = [K : \mathbb{Q}]$. Show how to compute the discriminant of f from the coefficients of f and its derivative using *resultants*.
2. **Ramification.** Prove that a rational prime p ramifies in a number field K if and only if $p|\Delta$.
3. **Stickelberger's criterion.** Prove that the discriminant of a number field is 0 or 1 modulo 4.
4. **Polynomial factorization modulo p.** How does one efficiently factor a polynomial modulo p? (There is a wiki page on the subject. Berlekamp's algorithm is the most basic.)
5. **Sage.** What calculations related to our class can Sage do?

Today

- Definition and first properties of the class group.
- Proof that the class group is finite.

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,

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

□

First observations

Proposition. Two ordinary ideals $\mathfrak{a}$ and $\mathfrak{b}$ represent the same element in $\mathcal{H}$ if and only if there exist $\alpha, \beta \in \mathfrak{O}_K \setminus \{0\}$ such $\alpha\mathfrak{a} = \beta\mathfrak{b}$.

First observations

Proposition. Two ordinary ideals $\mathfrak{a}$ and $\mathfrak{b}$ represent the same element in $\mathcal{H}$ if and only if there exist $\alpha, \beta \in \mathfrak{O}_K \setminus \{0\}$ such $\alpha\mathfrak{a} = \beta\mathfrak{b}$.

Proof. We have $\mathfrak{a} = \mathfrak{b} \bmod \mathcal{P}$ if and only if there exists $\gamma \in K \setminus \{0\}$ such that $(\gamma\mathfrak{O}_K)\mathfrak{a} = \mathfrak{b}$.

First observations

Proposition. Two ordinary ideals $\mathfrak{a}$ and $\mathfrak{b}$ represent the same element in $\mathcal{H}$ if and only if there exist $\alpha, \beta \in \mathfrak{O}_K \setminus \{0\}$ such $\alpha\mathfrak{a} = \beta\mathfrak{b}$.

Proof. We have $\mathfrak{a} = \mathfrak{b} \bmod \mathcal{P}$ if and only if there exists $\gamma \in K \setminus \{0\}$ such that $(\gamma\mathfrak{O}_K)\mathfrak{a} = \mathfrak{b}$.

Write $\gamma = \alpha/\beta$ to get the result. □

First observations

Another way of thinking of $\mathcal{H}$:

First observations

Another way of thinking of $\mathcal{H}$:

Write $\mathfrak{a} \sim \mathfrak{b}$ for ideals $\mathfrak{a}$ and $\mathfrak{b}$ if there exist $\alpha, \beta \in \mathfrak{O}_K$ if $\alpha\mathfrak{a} = \beta\mathfrak{b}$.

First observations

Another way of thinking of $\mathcal{H}$:

Write $\mathfrak{a} \sim \mathfrak{b}$ for ideals $\mathfrak{a}$ and $\mathfrak{b}$ if there exist $\alpha, \beta \in \mathfrak{O}_K$ if $\alpha\mathfrak{a} = \beta\mathfrak{b}$.

Then $\mathcal{H}$ is the set of equivalence classes of (ordinary) ideals $[\mathfrak{a}]$ with multiplication

$$[\mathfrak{a}][\mathfrak{b}] := [\mathfrak{ab}].$$

$h = 1$ 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.

$h = 1$ 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.

Proof. ($\Rightarrow$) $\mathfrak{O}_K$ a UFD

$h = 1$ 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.

Proof. ($\Rightarrow$) $\mathfrak{O}_K$ a UFD $\Rightarrow$ $\mathfrak{O}_K$ a PID.

$h = 1$ 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.

Proof. ($\Rightarrow$) $\mathfrak{O}_K$ a UFD $\Rightarrow$ $\mathfrak{O}_K$ a PID.

Let I be a fractional ideal.

$h = 1$ 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.

Proof. ($\Rightarrow$) $\mathfrak{O}_K$ a UFD $\Rightarrow$ $\mathfrak{O}_K$ a PID.

Let I be a fractional ideal. So $I = \frac{1}{\beta}\mathfrak{a}$ for some nonzero $\beta \in \mathfrak{O}_K$ and some nonzero ordinary ideal $\mathfrak{a}$.

$h = 1$ 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.

Proof. ($\Rightarrow$) $\mathfrak{O}_K$ a UFD $\Rightarrow$ $\mathfrak{O}_K$ a PID.

Let I be a fractional ideal. So $I = \frac{1}{\beta}\mathfrak{a}$ for some nonzero $\beta \in \mathfrak{O}_K$ and some nonzero ordinary ideal $\mathfrak{a}$.
Since $\mathfrak{O}_K$ is a PID, we have $\mathfrak{a} = (\alpha)$ for some $\alpha \in \mathfrak{O}_K$.

$h = 1$ 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.

Proof. ($\Rightarrow$) $\mathfrak{O}_K$ a UFD $\Rightarrow$ $\mathfrak{O}_K$ a PID.

Let I be a fractional ideal. So $I = \frac{1}{\beta}\mathfrak{a}$ for some nonzero $\beta \in \mathfrak{O}_K$ and some nonzero ordinary ideal $\mathfrak{a}$.
Since $\mathfrak{O}_K$ is a PID, we have $\mathfrak{a} = (\alpha)$ for some $\alpha \in \mathfrak{O}_K$.
Hence, $I = (\alpha/\beta)\mathfrak{O}_K$ is principal.

$h = 1$ 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.

Proof. ($\Rightarrow$) $\mathfrak{O}_K$ a UFD $\Rightarrow$ $\mathfrak{O}_K$ a PID.

Let I be a fractional ideal. So $I = \frac{1}{\beta}\mathfrak{a}$ for some nonzero $\beta \in \mathfrak{O}_K$ and some nonzero ordinary ideal $\mathfrak{a}$.
Since $\mathfrak{O}_K$ is a PID, we have $\mathfrak{a} = (\alpha)$ for some $\alpha \in \mathfrak{O}_K$.
Hence, $I = (\alpha/\beta)\mathfrak{O}_K$ is principal.

($\Leftarrow$) Suppose that $\mathcal{H}$ is trivial, and let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$.

$h = 1$ 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.

Proof. ($\Rightarrow$) $\mathfrak{O}_K$ a UFD $\Rightarrow$ $\mathfrak{O}_K$ a PID.

Let I be a fractional ideal. So $I = \frac{1}{\beta}\mathfrak{a}$ for some nonzero $\beta \in \mathfrak{O}_K$ and some nonzero ordinary ideal $\mathfrak{a}$.
Since $\mathfrak{O}_K$ is a PID, we have $\mathfrak{a} = (\alpha)$ for some $\alpha \in \mathfrak{O}_K$.
Hence, $I = (\alpha/\beta)\mathfrak{O}_K$ is principal.

($\Leftarrow$) Suppose that $\mathcal{H}$ is trivial, and let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. We may regard $\mathfrak{a}$ as a fractional ideal, and since $\mathcal{H}$ is trivial, it follows that $\mathfrak{a}$ is a principal fractional ideal.

$h = 1$ 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.

Proof. ($\Rightarrow$) $\mathfrak{O}_K$ a UFD $\Rightarrow$ $\mathfrak{O}_K$ a PID.

Let I be a fractional ideal. So $I = \frac{1}{\beta}\mathfrak{a}$ for some nonzero $\beta \in \mathfrak{O}_K$ and some nonzero ordinary ideal $\mathfrak{a}$.
Since $\mathfrak{O}_K$ is a PID, we have $\mathfrak{a} = (\alpha)$ for some $\alpha \in \mathfrak{O}_K$.
Hence, $I = (\alpha/\beta)\mathfrak{O}_K$ is principal.

($\Leftarrow$) Suppose that $\mathcal{H}$ is trivial, and let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. We may regard $\mathfrak{a}$ as a fractional ideal, and since $\mathcal{H}$ is trivial, it follows that $\mathfrak{a}$ is a principal fractional ideal.

Thus, $\mathfrak{a} = \alpha\mathfrak{O}_K$ for some nonzero element $\alpha \in K$.

$h = 1$ 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.

Proof. ($\Rightarrow$) $\mathfrak{O}_K$ a UFD $\Rightarrow$ $\mathfrak{O}_K$ a PID.

Let I be a fractional ideal. So $I = \frac{1}{\beta}\mathfrak{a}$ for some nonzero $\beta \in \mathfrak{O}_K$ and some nonzero ordinary ideal $\mathfrak{a}$.
Since $\mathfrak{O}_K$ is a PID, we have $\mathfrak{a} = (\alpha)$ for some $\alpha \in \mathfrak{O}_K$.
Hence, $I = (\alpha/\beta)\mathfrak{O}_K$ is principal.

($\Leftarrow$) Suppose that $\mathcal{H}$ is trivial, and let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. We may regard $\mathfrak{a}$ as a fractional ideal, and since $\mathcal{H}$ is trivial, it follows that $\mathfrak{a}$ is a principal fractional ideal.

Thus, $\mathfrak{a} = \alpha\mathfrak{O}_K$ for some nonzero element $\alpha \in K$. Since $\mathfrak{a} \subseteq \mathfrak{O}_K$, it follows that $\alpha \in \mathfrak{O}_K$,

$h = 1$ 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.

Proof. ($\Rightarrow$) $\mathfrak{O}_K$ a UFD $\Rightarrow$ $\mathfrak{O}_K$ a PID.

Let I be a fractional ideal. So $I = \frac{1}{\beta}\mathfrak{a}$ for some nonzero $\beta \in \mathfrak{O}_K$ and some nonzero ordinary ideal $\mathfrak{a}$.
Since $\mathfrak{O}_K$ is a PID, we have $\mathfrak{a} = (\alpha)$ for some $\alpha \in \mathfrak{O}_K$.
Hence, $I = (\alpha/\beta)\mathfrak{O}_K$ is principal.

($\Leftarrow$) Suppose that $\mathcal{H}$ is trivial, and let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. We may regard $\mathfrak{a}$ as a fractional ideal, and since $\mathcal{H}$ is trivial, it follows that $\mathfrak{a}$ is a principal fractional ideal.

Thus, $\mathfrak{a} = \alpha\mathfrak{O}_K$ for some nonzero element $\alpha \in K$. Since $\mathfrak{a} \subseteq \mathfrak{O}_K$, it follows that $\alpha \in \mathfrak{O}_K$, and thus, $\mathfrak{a}$ is the principal ideal $(\alpha) \subseteq \mathfrak{O}_K$. $\square$

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. We will prove this in an upcoming lecture.

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.
□

Example

Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathfrak{O}_K = \mathrm{Span}_{\mathbb{Z}}\{1, \sqrt{-5}\}$. The discriminant of K is

$$\Delta = \det \begin{pmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{pmatrix}^2 = (-2\sqrt{-5})^2 = -20.$$

Example

Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathfrak{O}_K = \mathrm{Span}_{\mathbb{Z}}\{1, \sqrt{-5}\}$. The discriminant of K is

$$\Delta = \det \begin{pmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{pmatrix}^2 = (-2\sqrt{-5})^2 = -20.$$

Then K has 2 complex embeddings. So each element of $\mathcal{H}$ is represented by an ideal with norm at most

$$\left(\frac{2}{\pi}\right)\sqrt{|\Delta|} < 2.9.$$

Example

Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathfrak{O}_K = \mathrm{Span}_{\mathbb{Z}}\{1, \sqrt{-5}\}$. The discriminant of K is

$$\Delta = \det \begin{pmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{pmatrix}^2 = (-2\sqrt{-5})^2 = -20.$$

Then K has 2 complex embeddings. So each element of $\mathcal{H}$ is represented by an ideal with norm at most

$$\left(\frac{2}{\pi}\right)\sqrt{|\Delta|} < 2.9.$$

So each element of $\mathcal{H}$ is represented by an ideal with norm either 1 or 2.

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1:

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2:

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a}$

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a} \Rightarrow (2) \subseteq \mathfrak{a}$

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a} \Rightarrow (2) \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} | (2)$.

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a} \Rightarrow (2) \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} | (2)$.

We have the factorization $(2) =$

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a} \Rightarrow (2) \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} | (2)$.

We have the factorization $(2) = (2, 1 + \sqrt{-5})^2$.

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a} \Rightarrow (2) \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} | (2)$.

We have the factorization $(2) = (2, 1 + \sqrt{-5})^2$.

Take norms: $(2) = (2, 1 + \sqrt{-5})^2 \Rightarrow 4 = N(2, 1 + \sqrt{-5})^2$.

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a} \Rightarrow (2) \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} | (2)$.

We have the factorization $(2) = (2, 1 + \sqrt{-5})^2$.

Take norms: $(2) = (2, 1 + \sqrt{-5})^2 \Rightarrow 4 = N(2, 1 + \sqrt{-5})^2$.
So $\mathfrak{a} = (2, 1 + \sqrt{-5})$.

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a} \Rightarrow (2) \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} | (2)$.

We have the factorization $(2) = (2, 1 + \sqrt{-5})^2$.

Take norms: $(2) = (2, 1 + \sqrt{-5})^2 \Rightarrow 4 = N(2, 1 + \sqrt{-5})^2$.
So $\mathfrak{a} = (2, 1 + \sqrt{-5})$.

Is $(2, 1 + \sqrt{-5})$ principal?

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a} \Rightarrow (2) \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} | (2)$.

We have the factorization $(2) = (2, 1 + \sqrt{-5})^2$.

Take norms: $(2) = (2, 1 + \sqrt{-5})^2 \Rightarrow 4 = N(2, 1 + \sqrt{-5})^2$.
So $\mathfrak{a} = (2, 1 + \sqrt{-5})$.

Is $(2, 1 + \sqrt{-5})$ principal?

Answer: No.

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a} \Rightarrow (2) \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} | (2)$.

We have the factorization $(2) = (2, 1 + \sqrt{-5})^2$.

Take norms: $(2) = (2, 1 + \sqrt{-5})^2 \Rightarrow 4 = N(2, 1 + \sqrt{-5})^2$.
So $\mathfrak{a} = (2, 1 + \sqrt{-5})$.

Is $(2, 1 + \sqrt{-5})$ principal?

Answer: No. To prove this, suppose not, and take norms.

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a} \Rightarrow (2) \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} | (2)$.

We have the factorization $(2) = (2, 1 + \sqrt{-5})^2$.

Take norms: $(2) = (2, 1 + \sqrt{-5})^2 \Rightarrow 4 = N(2, 1 + \sqrt{-5})^2$.
So $\mathfrak{a} = (2, 1 + \sqrt{-5})$.

Is $(2, 1 + \sqrt{-5})$ principal?

Answer: No. To prove this, suppose not, and take norms.

Thus, $\mathcal{H}$ is minimally generated by (1) and $(2, 1 + \sqrt{-5})$,

Example

What are the ideals of $\mathfrak{O}_K$ with norm 1 or 2?

Norm 1: $\mathfrak{O}_K = (1)$.

Norm 2: If $N(\mathfrak{a}) = 2$, then $2 \in \mathfrak{a} \Rightarrow (2) \subseteq \mathfrak{a} \Rightarrow \mathfrak{a} | (2)$.

We have the factorization $(2) = (2, 1 + \sqrt{-5})^2$.

Take norms: $(2) = (2, 1 + \sqrt{-5})^2 \Rightarrow 4 = N(2, 1 + \sqrt{-5})^2$.
So $\mathfrak{a} = (2, 1 + \sqrt{-5})$.

Is $(2, 1 + \sqrt{-5})$ principal?

Answer: No. To prove this, suppose not, and take norms.

Thus, $\mathcal{H}$ is minimally generated by (1) and $(2, 1 + \sqrt{-5})$,

and $h = 2$.

Corollary

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