Math 361

March 27, 2023

Quiz

Remember that we will have a quiz on Wednesday. Our cumulative topics sheet is posted.

Today

- The norm of an ideal.
- $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

Norm of an ideal

Let K be a number field, and let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$.

Norm of an ideal

Let K be a number field, and let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$.

Recall the argument showing that $\mathfrak{O}_K/\mathfrak{a}$ is finite.

Norm of an ideal

Let K be a number field, and let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$.

Recall the argument showing that $\mathfrak{O}_K/\mathfrak{a}$ is finite.

Definition. The *norm* of the nonzero ideal $\mathfrak{a}$ is

$$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|\,.$$

Norm of an ideal

Let K be a number field, and let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$.

Recall the argument showing that $\mathfrak{O}_K/\mathfrak{a}$ is finite.

Definition. The *norm* of the nonzero ideal $\mathfrak{a}$ is

$$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|\,.$$

Exercise. Let $K = \mathbb{Q}(\sqrt{-14})$ and $\mathfrak{a} = (6, 1+\sqrt{-14}) \subset \mathfrak{O}_K$. Compute $N(\mathfrak{a})$.

Norm of an ideal

Proposition. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$ and pick a $\mathbb{Z}$-module basis $\{\alpha_1, \ldots, \alpha_n\}$ for $\mathfrak{a}$. Then

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \ldots, \alpha_n]}{\Delta} \right|^{1/2}$$

where Δ is the discriminant of K (i.e., the discriminant of any $\mathbb{Z}$-basis for $\mathfrak{O}_K$).

Norm of an ideal

Proposition. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$ and pick a $\mathbb{Z}$-module basis $\{\alpha_1, \ldots, \alpha_n\}$ for $\mathfrak{a}$. Then

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \ldots, \alpha_n]}{\Delta} \right|^{1/2}$$

where Δ is the discriminant of K (i.e., the discriminant of any $\mathbb{Z}$-basis for $\mathfrak{O}_K$).

Proof. $\mathbb{Z}$-basis for $\mathfrak{O}_K$: $\{\omega_1, \ldots, \omega_n\}$.

Norm of an ideal

Proposition. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$ and pick a $\mathbb{Z}$-module basis $\{\alpha_1, \ldots, \alpha_n\}$ for $\mathfrak{a}$. Then

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \ldots, \alpha_n]}{\Delta} \right|^{1/2}$$

where Δ is the discriminant of K (i.e., the discriminant of any $\mathbb{Z}$-basis for $\mathfrak{O}_K$).

Proof. $\mathbb{Z}$-basis for $\mathfrak{O}_K$: $\{\omega_1, \ldots, \omega_n\}$.

Write $(\alpha_1, \ldots, \alpha_n)^t = C\,(\omega_1, \ldots, \omega_n)^t$ for some integer matrix C.

Norm of an ideal

Proposition. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$ and pick a $\mathbb{Z}$-module basis $\{\alpha_1, \ldots, \alpha_n\}$ for $\mathfrak{a}$. Then

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \ldots, \alpha_n]}{\Delta} \right|^{1/2}$$

where Δ is the discriminant of K (i.e., the discriminant of any $\mathbb{Z}$-basis for $\mathfrak{O}_K$).

Proof. $\mathbb{Z}$-basis for $\mathfrak{O}_K$: $\{\omega_1, \ldots, \omega_n\}$.

Write $(\alpha_1, \ldots, \alpha_n)^t = C\,(\omega_1, \ldots, \omega_n)^t$ for some integer matrix C.

Change of basis formula for the discriminant:

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\omega_1, \ldots, \omega_n] = \det(C)^2 \Delta.$$

Norm of an ideal

Proposition. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$ and pick a $\mathbb{Z}$-module basis $\{\alpha_1, \ldots, \alpha_n\}$ for $\mathfrak{a}$. Then

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \ldots, \alpha_n]}{\Delta} \right|^{1/2}$$

where Δ is the discriminant of K (i.e., the discriminant of any $\mathbb{Z}$-basis for $\mathfrak{O}_K$).

Proof. $\mathbb{Z}$-basis for $\mathfrak{O}_K$: $\{\omega_1, \ldots, \omega_n\}$.

Write $(\alpha_1, \ldots, \alpha_n)^t = C\,(\omega_1, \ldots, \omega_n)^t$ for some integer matrix C.

Change of basis formula for the discriminant:

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\omega_1, \ldots, \omega_n] = \det(C)^2 \Delta.$$

The result then follows from the commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathfrak{a} & \longrightarrow & \mathfrak{O}_K & \longrightarrow & \mathfrak{O}_K/\mathfrak{a} & \longrightarrow & 0 \\
 & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \\
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{C} & \mathbb{Z}^n & \longrightarrow & \operatorname{cok} C & \longrightarrow & 0
\end{array}$$

Norm of an ideal

Corollary. Let $0 \neq \alpha \in \mathfrak{O}_K$, and consider the principal ideal (α). Then

$$N((\alpha)) = |N(\alpha)|$$

where $N(\alpha)$ is the norm we defined previously for elements of K.

Norm of an ideal

Corollary. Let $0 \neq \alpha \in \mathfrak{O}_K$, and consider the principal ideal (α). Then

$$N((\alpha)) = |N(\alpha)|$$

where $N(\alpha)$ is the norm we defined previously for elements of K.

Proof.

Norm of an ideal

Corollary. Let $0 \neq \alpha \in \mathfrak{O}_K$, and consider the principal ideal (α). Then

$$N((\alpha)) = |N(\alpha)|$$

where $N(\alpha)$ is the norm we defined previously for elements of K.

Proof. $\mathbb{Z}$-basis for $\mathfrak{O}_K$: $\{\omega_1, \ldots, \omega_n\}$.

Norm of an ideal

Corollary. Let $0 \neq \alpha \in \mathfrak{O}_K$, and consider the principal ideal (α). Then

$$N((\alpha)) = |N(\alpha)|$$

where $N(\alpha)$ is the norm we defined previously for elements of K.

Proof. $\mathbb{Z}$-basis for $\mathfrak{O}_K$: $\{\omega_1, \ldots, \omega_n\}$.

$\mathbb{Z}$-basis for (α): $\{\alpha\omega_1, \ldots, \alpha\omega_n\}$.

Norm of an ideal

Corollary. Let $0 \neq \alpha \in \mathfrak{O}_K$, and consider the principal ideal (α). Then

$$N((\alpha)) = |N(\alpha)|$$

where $N(\alpha)$ is the norm we defined previously for elements of K.

Proof. $\mathbb{Z}$-basis for $\mathfrak{O}_K$: $\{\omega_1, \ldots, \omega_n\}$.

$\mathbb{Z}$-basis for (α): $\{\alpha\omega_1, \ldots, \alpha\omega_n\}$.

$$\Delta[\alpha\omega_1, \ldots, \alpha\omega_n] = \prod_{i=1}^{n} \sigma_i(\alpha\omega_j)^2$$

Norm of an ideal

Corollary. Let $0 \neq \alpha \in \mathfrak{O}_K$, and consider the principal ideal (α). Then

$$N((\alpha)) = |N(\alpha)|$$

where $N(\alpha)$ is the norm we defined previously for elements of K.

Proof. $\mathbb{Z}$-basis for $\mathfrak{O}_K$: $\{\omega_1, \ldots, \omega_n\}$.

$\mathbb{Z}$-basis for (α): $\{\alpha\omega_1, \ldots, \alpha\omega_n\}$.

$$\begin{aligned}\Delta[\alpha\omega_1, \ldots, \alpha\omega_n] &= \prod_{i=1}^{n} \sigma_i(\alpha\omega_j)^2 \\ &= \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)^2 \left(\prod_{i=1}^{n} \sigma_i(\omega_j)^2\right)\end{aligned}$$

Norm of an ideal

Corollary. Let $0 \neq \alpha \in \mathfrak{O}_K$, and consider the principal ideal (α). Then

$$N((\alpha)) = |N(\alpha)|$$

where $N(\alpha)$ is the norm we defined previously for elements of K.

Proof. $\mathbb{Z}$-basis for $\mathfrak{O}_K$: $\{\omega_1, \ldots, \omega_n\}$.

$\mathbb{Z}$-basis for (α): $\{\alpha\omega_1, \ldots, \alpha\omega_n\}$.

$$\begin{aligned}
\Delta[\alpha\omega_1, \ldots, \alpha\omega_n] &= \prod_{i=1}^{n} \sigma_i(\alpha\omega_j)^2 \\
&= \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)^2 \left(\prod_{i=1}^{n} \sigma_i(\omega_j)^2\right) \\
&= N(\alpha)^2 \Delta.
\end{aligned}$$

Norm of an ideal

Corollary. Let $0 \neq \alpha \in \mathfrak{O}_K$, and consider the principal ideal (α). Then

$$N((\alpha)) = |N(\alpha)|$$

where $N(\alpha)$ is the norm we defined previously for elements of K.

Proof. $\mathbb{Z}$-basis for $\mathfrak{O}_K$: $\{\omega_1, \ldots, \omega_n\}$.

$\mathbb{Z}$-basis for (α): $\{\alpha\omega_1, \ldots, \alpha\omega_n\}$.

$$\begin{aligned}
\Delta[\alpha\omega_1, \ldots, \alpha\omega_n] &= \prod_{i=1}^{n} \sigma_i(\alpha\omega_j)^2 \\
&= \left(\prod_{i=1}^{n} \sigma_i(\alpha)\right)^2 \left(\prod_{i=1}^{n} \sigma_i(\omega_j)^2\right) \\
&= N(\alpha)^2 \Delta.
\end{aligned}$$

The result now follows from the Proposition.

Norm of an ideal

Example. Let d be a square-free integer not equal to 0 or 1.

Norm of an ideal

Example. Let d be a square-free integer not equal to 0 or 1.

Let $a, b \in \mathbb{Z}$ and consider the principal ideal $\mathfrak{a} = (a + b\sqrt{d})$ in $\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}$.

Norm of an ideal

Example. Let d be a square-free integer not equal to 0 or 1.

Let $a, b \in \mathbb{Z}$ and consider the principal ideal $\mathfrak{a} = (a + b\sqrt{d})$ in $\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}$. Then

$$\left|\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}/\mathfrak{a}\right|$$

Norm of an ideal

Example. Let d be a square-free integer not equal to 0 or 1.

Let $a, b \in \mathbb{Z}$ and consider the principal ideal $\mathfrak{a} = (a + b\sqrt{d})$ in $\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}$. Then

$$\left|\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}/\mathfrak{a}\right| = N(\mathfrak{a}) = |N(a + b\sqrt{d})|$$

Norm of an ideal

Example. Let d be a square-free integer not equal to 0 or 1.

Let $a, b \in \mathbb{Z}$ and consider the principal ideal $\mathfrak{a} = (a + b\sqrt{d})$ in $\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}$. Then

$$\begin{aligned} \left|\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}/\mathfrak{a}\right| &= N(\mathfrak{a}) = |N(a + b\sqrt{d})| \\ &= |(a + b\sqrt{d})(a - b\sqrt{d})| \end{aligned}$$

Norm of an ideal

Example. Let d be a square-free integer not equal to 0 or 1.

Let $a, b \in \mathbb{Z}$ and consider the principal ideal $\mathfrak{a} = (a + b\sqrt{d})$ in $\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}$. Then

$$\begin{aligned} \left|\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}/\mathfrak{a}\right| &= N(\mathfrak{a}) = |N(a + b\sqrt{d})| \\ &= |(a + b\sqrt{d})(a - b\sqrt{d})| \\ &= |a^2 - db^2|. \end{aligned}$$

Norm of an ideal

Proposition Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero ideals of $\mathfrak{O}_K$. Then

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

Norm of an ideal

Proposition Let $\mathfrak{a}$ and $\mathfrak{b}$ be nonzero ideals of $\mathfrak{O}_K$. Then

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Proof. Isomorphism theorems from algebra. See Theorem 5.12 in our text.

Norm of an ideal

Proposition. Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{O}_K$.

Norm of an ideal

Proposition. Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{O}_K$.

1. If $\alpha \in \mathfrak{a}$, then $N(\mathfrak{a})|N(\alpha)$.

Norm of an ideal

Proposition. Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{O}_K$.

1. If $\alpha \in \mathfrak{a}$, then $N(\mathfrak{a})|N(\alpha)$.

Proof. If $\alpha \in \mathfrak{a}$, then the principal ideal (α) is contained in $\mathfrak{a}$.

Norm of an ideal

Proposition. Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{O}_K$.

1. If $\alpha \in \mathfrak{a}$, then $N(\mathfrak{a})|N(\alpha)$.

Proof. If $\alpha \in \mathfrak{a}$, then the principal ideal (α) is contained in $\mathfrak{a}$.

Therefore $\mathfrak{a}|(\alpha)$,

Norm of an ideal

Proposition. Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{O}_K$.

1. If $\alpha \in \mathfrak{a}$, then $N(\mathfrak{a})|N(\alpha)$.

Proof. If $\alpha \in \mathfrak{a}$, then the principal ideal (α) is contained in $\mathfrak{a}$.

Therefore $\mathfrak{a}|(\alpha)$, i.e., there exists an ideal $\mathfrak{b}$ such that $(\alpha) = \mathfrak{a}\mathfrak{b}$.

Norm of an ideal

Proposition. Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{O}_K$.

1. If $\alpha \in \mathfrak{a}$, then $N(\mathfrak{a})|N(\alpha)$.

Proof. If $\alpha \in \mathfrak{a}$, then the principal ideal (α) is contained in $\mathfrak{a}$.

Therefore $\mathfrak{a}|(\alpha)$, i.e., there exists an ideal $\mathfrak{b}$ such that $(\alpha) = \mathfrak{a}\mathfrak{b}$.

Taking norms yields

$$N((\alpha)) = |N(\alpha)| = N(\mathfrak{a})N(\mathfrak{b}).$$

The result follows.

Norm of an ideal

2. $N(\mathfrak{a}) = 1$ if and only if $\mathfrak{a} = (1) = \mathfrak{O}_K$.

Norm of an ideal

2. $N(\mathfrak{a}) = 1$ if and only if $\mathfrak{a} = (1) = \mathfrak{O}_K$.

Proof. Immediate from the definition of the norm.

Norm of an ideal

3. If $N(\mathfrak{a})$ is prime, $\mathfrak{a}$ is prime.

Norm of an ideal

3. If $N(\mathfrak{a})$ is prime, $\mathfrak{a}$ is prime.

Proof.

Norm of an ideal

3. If $N(\mathfrak{a})$ is prime, $\mathfrak{a}$ is prime.

Proof. Factor $\mathfrak{a}$ into primes:

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}.$$

Norm of an ideal

3. If $N(\mathfrak{a})$ is prime, $\mathfrak{a}$ is prime.

Proof. Factor $\mathfrak{a}$ into primes:

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}.$$

Taking norms:

$$N(\mathfrak{a}) = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{e_i}. \tag{1}$$

Norm of an ideal

3. If $N(\mathfrak{a})$ is prime, $\mathfrak{a}$ is prime.

Proof. Factor $\mathfrak{a}$ into primes:

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}.$$

Taking norms:

$$N(\mathfrak{a}) = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{e_i}. \tag{1}$$

If $\mathfrak{p}$ is prime, then $\mathfrak{p} \neq \mathfrak{O}_K$, and hence $N(\mathfrak{p}) > 1$.

Norm of an ideal

3. If $N(\mathfrak{a})$ is prime, $\mathfrak{a}$ is prime.

Proof. Factor $\mathfrak{a}$ into primes:

$$\mathfrak{a} = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}.$$

Taking norms:

$$N(\mathfrak{a}) = \prod_{i=1}^{k} N(\mathfrak{p}_i)^{e_i}. \tag{1}$$

If $\mathfrak{p}$ is prime, then $\mathfrak{p} \neq \mathfrak{O}_K$, and hence $N(\mathfrak{p}) > 1$.

Therefore, if $N(\mathfrak{a})$ is prime, so is $\mathfrak{a}$.

Norm of an ideal

4. $N(\mathfrak{a}) \in \mathfrak{a}$.

Norm of an ideal

4. $N(\mathfrak{a}) \in \mathfrak{a}$.

Proof. Let $\alpha \in \mathfrak{O}_K$.

Norm of an ideal

4. $N(\mathfrak{a}) \in \mathfrak{a}$.

Proof. Let $\alpha \in \mathfrak{O}_K$.

$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|$

Norm of an ideal

4. $N(\mathfrak{a}) \in \mathfrak{a}$.

Proof. Let $\alpha \in \mathfrak{O}_K$.

$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}| \Longrightarrow N(\mathfrak{a})\alpha = 0 \in \mathfrak{O}_K/\mathfrak{a}$,

Norm of an ideal

4. $N(\mathfrak{a}) \in \mathfrak{a}$.

Proof. Let $\alpha \in \mathfrak{O}_K$.

$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}| \Longrightarrow N(\mathfrak{a})\alpha = 0 \in \mathfrak{O}_K/\mathfrak{a}$, i.e., $N(\mathfrak{a})\alpha \in \mathfrak{a}$.

Norm of an ideal

4. $N(\mathfrak{a}) \in \mathfrak{a}$.

Proof. Let $\alpha \in \mathfrak{O}_K$.

$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}| \Longrightarrow N(\mathfrak{a})\alpha = 0 \in \mathfrak{O}_K/\mathfrak{a}$, i.e., $N(\mathfrak{a})\alpha \in \mathfrak{a}$.

Letting $\alpha = 1$ gives the result.

Norm of an ideal

5. If $\mathfrak{a}$ is prime, then $\mathfrak{a}$ contains a unique rational prime p

Norm of an ideal

5. If $\mathfrak{a}$ is prime, then $\mathfrak{a}$ contains a unique rational prime p and $N(\mathfrak{a}) = p^m$ for some $1 \leq m \leq n := [K : \mathbb{Q}]$.

Norm of an ideal

5. If $\mathfrak{a}$ is prime, then $\mathfrak{a}$ contains a unique rational prime p and $N(\mathfrak{a}) = p^m$ for some $1 \leq m \leq n := [K : \mathbb{Q}]$.

Proof. Let $N(\mathfrak{a}) = \prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization of $N(\mathfrak{a})$.

Norm of an ideal

5. If $\mathfrak{a}$ is prime, then $\mathfrak{a}$ contains a unique rational prime p and $N(\mathfrak{a}) = p^m$ for some $1 \leq m \leq n := [K : \mathbb{Q}]$.

Proof. Let $N(\mathfrak{a}) = \prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization of $N(\mathfrak{a})$. Since $N(\mathfrak{a}) \in \mathfrak{a}$,

$$\prod_{i=1}^{k} (p_i)^{e_i} \subseteq \mathfrak{a},$$

Norm of an ideal

5. If $\mathfrak{a}$ is prime, then $\mathfrak{a}$ contains a unique rational prime p and $N(\mathfrak{a}) = p^m$ for some $1 \leq m \leq n := [K : \mathbb{Q}]$.

Proof. Let $N(\mathfrak{a}) = \prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization of $N(\mathfrak{a})$. Since $N(\mathfrak{a}) \in \mathfrak{a}$,

$$\prod_{i=1}^{k} (p_i)^{e_i} \subseteq \mathfrak{a},$$

and, hence,

$$\mathfrak{a} | \prod_{i=1}^{k} (p_i)^{e_i}.$$

Norm of an ideal

5. If $\mathfrak{a}$ is prime, then $\mathfrak{a}$ contains a unique rational prime p and $N(\mathfrak{a}) = p^m$ for some $1 \leq m \leq n := [K : \mathbb{Q}]$.

Proof. Let $N(\mathfrak{a}) = \prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization of $N(\mathfrak{a})$. Since $N(\mathfrak{a}) \in \mathfrak{a}$,

$$\prod_{i=1}^{k} (p_i)^{e_i} \subseteq \mathfrak{a},$$

and, hence,

$$\mathfrak{a} | \prod_{i=1}^{k} (p_i)^{e_i}.$$

If $\mathfrak{a}$ is prime, there exists i such that $\mathfrak{a} | (p_i)$, which means $(p_i) \subseteq \mathfrak{a}$ or, equivalently, $p_i \in \mathfrak{a}$.

Norm of an ideal

Step 5 proof continued: We have seen that if $\mathfrak{a}$ is prime, then there exists a rational prime $p = p_i \in \mathfrak{a}$.

Norm of an ideal

Step 5 proof continued: We have seen that if $\mathfrak{a}$ is prime, then there exists a rational prime $p = p_i \in \mathfrak{a}$.

If there exists an rational prime $q \neq p$ in $\mathfrak{a}$, we would have

Norm of an ideal

Step 5 proof continued: We have seen that if $\mathfrak{a}$ is prime, then there exists a rational prime $p = p_i \in \mathfrak{a}$.

If there exists an rational prime $q \neq p$ in $\mathfrak{a}$, we would have

$$1 \in (p, q) = (p) + (q) \subseteq \mathfrak{a}$$

Norm of an ideal

Step 5 proof continued: We have seen that if $\mathfrak{a}$ is prime, then there exists a rational prime $p = p_i \in \mathfrak{a}$.

If there exists an rational prime $q \neq p$ in $\mathfrak{a}$, we would have

$$1 \in (p, q) = (p) + (q) \subseteq \mathfrak{a}$$

However, since $\mathfrak{a}$ is prime, it does not contain 1. So there exists a unique rational prime $\mathfrak{a}$.

Norm of an ideal

Step 5 proof continued: We have seen that if $\mathfrak{a}$ is prime, then there exists a rational prime $p = p_i \in \mathfrak{a}$.

If there exists an rational prime $q \neq p$ in $\mathfrak{a}$, we would have

$$1 \in (p, q) = (p) + (q) \subseteq \mathfrak{a}$$

However, since $\mathfrak{a}$ is prime, it does not contain 1. So there exists a unique rational prime $\mathfrak{a}$.

From the first part of this problem, we have $N(\mathfrak{a})|N(p)$.

Norm of an ideal

Step 5 proof continued: We have seen that if $\mathfrak{a}$ is prime, then there exists a rational prime $p = p_i \in \mathfrak{a}$.

If there exists an rational prime $q \neq p$ in $\mathfrak{a}$, we would have

$$1 \in (p, q) = (p) + (q) \subseteq \mathfrak{a}$$

However, since $\mathfrak{a}$ is prime, it does not contain 1. So there exists a unique rational prime $\mathfrak{a}$.

From the first part of this problem, we have $N(\mathfrak{a})|N(p)$.

Since $N(p) = p^n$, the result follows.

Norm of an ideal

Summary:

Proposition. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$.

Norm of an ideal

Summary:

Proposition. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. Then

1. If $\alpha \in \mathfrak{a}$, then $N(\mathfrak{a})|N(\alpha)$.

Norm of an ideal

Summary:

Proposition. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. Then

1. If $\alpha \in \mathfrak{a}$, then $N(\mathfrak{a})|N(\alpha)$.
2. $N(\mathfrak{a}) = 1$ if and only if $\mathfrak{a} = (1) = \mathfrak{O}_K$.

Norm of an ideal

Summary:

Proposition. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. Then

1. If $\alpha \in \mathfrak{a}$, then $N(\mathfrak{a})|N(\alpha)$.
2. $N(\mathfrak{a}) = 1$ if and only if $\mathfrak{a} = (1) = \mathfrak{O}_K$.
3. If $N(\mathfrak{a})$ is prime, $\mathfrak{a}$ is prime.

Norm of an ideal

Summary:

Proposition. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. Then

1. If $\alpha \in \mathfrak{a}$, then $N(\mathfrak{a})|N(\alpha)$.
2. $N(\mathfrak{a}) = 1$ if and only if $\mathfrak{a} = (1) = \mathfrak{O}_K$.
3. If $N(\mathfrak{a})$ is prime, $\mathfrak{a}$ is prime.
4. $N(\mathfrak{a}) \in \mathfrak{a}$.

Norm of an ideal

Summary:

Proposition. Let $\mathfrak{a}$ be a nonzero ideal of $\mathfrak{O}_K$. Then

1. If $\alpha \in \mathfrak{a}$, then $N(\mathfrak{a})|N(\alpha)$.
2. $N(\mathfrak{a}) = 1$ if and only if $\mathfrak{a} = (1) = \mathfrak{O}_K$.
3. If $N(\mathfrak{a})$ is prime, $\mathfrak{a}$ is prime.
4. $N(\mathfrak{a}) \in \mathfrak{a}$.
5. If $\mathfrak{a}$ is prime, then $\mathfrak{a}$ contains a unique rational prime p and $N(\mathfrak{a}) = p^m$ for some $1 \leq m \leq n := [K : \mathbb{Q}]$.

Norm of an ideal

Corollary

1. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$. Then there are only a finite number of ideals $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, Equivalently, there are finitely many ideals $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$.

Norm of an ideal

Corollary

1. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$. Then there are only a finite number of ideals $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, Equivalently, there are finitely many ideals $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$.
2. If $a \in \mathbb{Z}$, there are finitely many ideals $\mathfrak{a}$ of $\mathfrak{O}_K$ containing a.

Norm of an ideal

Corollary

1. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$. Then there are only a finite number of ideals $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, Equivalently, there are finitely many ideals $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$.
2. If $a \in \mathbb{Z}$, there are finitely many ideals $\mathfrak{a}$ of $\mathfrak{O}_K$ containing a.
3. There are finitely many ideals with a given norm.

Norm of an ideal

Corollary

1. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$. Then there are only a finite number of ideals $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, Equivalently, there are finitely many ideals $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$.
2. If $a \in \mathbb{Z}$, there are finitely many ideals $\mathfrak{a}$ of $\mathfrak{O}_K$ containing a.
3. There are finitely many ideals with a given norm.

Proof.

Norm of an ideal

Corollary

1. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$. Then there are only a finite number of ideals $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, Equivalently, there are finitely many ideals $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$.
2. If $a \in \mathbb{Z}$, there are finitely many ideals $\mathfrak{a}$ of $\mathfrak{O}_K$ containing a.
3. There are finitely many ideals with a given norm.

Proof.

1. This is an immediate consequence of prime factorization of ideals.

Norm of an ideal

Corollary

1. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$. Then there are only a finite number of ideals $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, Equivalently, there are finitely many ideals $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$.
2. If $a \in \mathbb{Z}$, there are finitely many ideals $\mathfrak{a}$ of $\mathfrak{O}_K$ containing a.
3. There are finitely many ideals with a given norm.

Proof.

1. This is an immediate consequence of prime factorization of ideals.
2. We have $a \in \mathfrak{a}$ if and only if $\mathfrak{a}|(a)$.

Norm of an ideal

Corollary

1. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$. Then there are only a finite number of ideals $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, Equivalently, there are finitely many ideals $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$.
2. If $a \in \mathbb{Z}$, there are finitely many ideals $\mathfrak{a}$ of $\mathfrak{O}_K$ containing a.
3. There are finitely many ideals with a given norm.

Proof.

1. This is an immediate consequence of prime factorization of ideals.
2. We have $a \in \mathfrak{a}$ if and only if $\mathfrak{a}|(a)$. So this result follows from the previous part of this Corollary applied to the principal ideal (a).

Norm of an ideal

Corollary

1. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$. Then there are only a finite number of ideals $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, Equivalently, there are finitely many ideals $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$.
2. If $a \in \mathbb{Z}$, there are finitely many ideals $\mathfrak{a}$ of $\mathfrak{O}_K$ containing a.
3. There are finitely many ideals with a given norm.

Proof.

1. This is an immediate consequence of prime factorization of ideals.
2. We have $a \in \mathfrak{a}$ if and only if $\mathfrak{a}|(a)$. So this result follows from the previous part of this Corollary applied to the principal ideal (a).
3. Fix $a \in \mathbb{Z}_{>0}$. If $\mathfrak{a}$ is an ideal with $N(\mathfrak{a}) = a$,

Norm of an ideal

Corollary

1. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$. Then there are only a finite number of ideals $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, Equivalently, there are finitely many ideals $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$.
2. If $a \in \mathbb{Z}$, there are finitely many ideals $\mathfrak{a}$ of $\mathfrak{O}_K$ containing a.
3. There are finitely many ideals with a given norm.

Proof.

1. This is an immediate consequence of prime factorization of ideals.
2. We have $a \in \mathfrak{a}$ if and only if $\mathfrak{a}|(a)$. So this result follows from the previous part of this Corollary applied to the principal ideal (a).
3. Fix $a \in \mathbb{Z}_{>0}$. If $\mathfrak{a}$ is an ideal with $N(\mathfrak{a}) = a$, then from the previous Proposition, we have $a \in \mathfrak{a}$.

Norm of an ideal

Corollary

1. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$. Then there are only a finite number of ideals $\mathfrak{b}$ such that $\mathfrak{b}|\mathfrak{a}$, Equivalently, there are finitely many ideals $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$.
2. If $a \in \mathbb{Z}$, there are finitely many ideals $\mathfrak{a}$ of $\mathfrak{O}_K$ containing a.
3. There are finitely many ideals with a given norm.

Proof.

1. This is an immediate consequence of prime factorization of ideals.
2. We have $a \in \mathfrak{a}$ if and only if $\mathfrak{a}|(a)$. So this result follows from the previous part of this Corollary applied to the principal ideal (a).
3. Fix $a \in \mathbb{Z}_{>0}$. If $\mathfrak{a}$ is an ideal with $N(\mathfrak{a}) = a$, then from the previous Proposition, we have $a \in \mathfrak{a}$. The result then follows from the previous part of this Corollary. $\square$

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. The number ring $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. The number ring $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

Proof. ($\Leftarrow$) We already know that a PID is a UFD.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. The number ring $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

Proof. ($\Leftarrow$) We already know that a PID is a UFD.

($\Rightarrow$) Suppose that $\mathfrak{O}_K$ is a UFD, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_K$.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. The number ring $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

Proof. ($\Leftarrow$) We already know that a PID is a UFD.

($\Rightarrow$) Suppose that $\mathfrak{O}_K$ is a UFD, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_K$.

We have $\mathfrak{p} \ni N(\mathfrak{p}) = \pi_1 \cdots \pi_k$ where the π_is are irreducibles in $\mathfrak{O}_K$.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. The number ring $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

Proof. ($\Leftarrow$) We already know that a PID is a UFD.

($\Rightarrow$) Suppose that $\mathfrak{O}_K$ is a UFD, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_K$.

We have $\mathfrak{p} \ni N(\mathfrak{p}) = \pi_1 \cdots \pi_k$ where the π_is are irreducibles in $\mathfrak{O}_K$.

Since $\mathfrak{p}$ is prime, it follows that $\pi_i \in \mathfrak{p}$ from some i.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. The number ring $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

Proof. ($\Leftarrow$) We already know that a PID is a UFD.

($\Rightarrow$) Suppose that $\mathfrak{O}_K$ is a UFD, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_K$.

We have $\mathfrak{p} \ni N(\mathfrak{p}) = \pi_1 \cdots \pi_k$ where the π_is are irreducibles in $\mathfrak{O}_K$.

Since $\mathfrak{p}$ is prime, it follows that $\pi_i \in \mathfrak{p}$ from some i. Hence, $(\pi_i) \subseteq \mathfrak{p}$.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. The number ring $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

Proof. ($\Leftarrow$) We already know that a PID is a UFD.

($\Rightarrow$) Suppose that $\mathfrak{O}_K$ is a UFD, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_K$.

We have $\mathfrak{p} \ni N(\mathfrak{p}) = \pi_1 \cdots \pi_k$ where the π_is are irreducibles in $\mathfrak{O}_K$.

Since $\mathfrak{p}$ is prime, it follows that $\pi_i \in \mathfrak{p}$ from some i. Hence, $(\pi_i) \subseteq \mathfrak{p}$.

In a UFD every irreducible is prime.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. The number ring $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

Proof. ($\Leftarrow$) We already know that a PID is a UFD.

($\Rightarrow$) Suppose that $\mathfrak{O}_K$ is a UFD, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_K$.

We have $\mathfrak{p} \ni N(\mathfrak{p}) = \pi_1 \cdots \pi_k$ where the π_is are irreducibles in $\mathfrak{O}_K$.

Since $\mathfrak{p}$ is prime, it follows that $\pi_i \in \mathfrak{p}$ from some i. Hence, $(\pi_i) \subseteq \mathfrak{p}$.

In a UFD every irreducible is prime. So (π_i) is a prime ideal. Primes are maximal in a number ring.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. The number ring $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

Proof. ($\Leftarrow$) We already know that a PID is a UFD.

($\Rightarrow$) Suppose that $\mathfrak{O}_K$ is a UFD, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_K$.

We have $\mathfrak{p} \ni N(\mathfrak{p}) = \pi_1 \cdots \pi_k$ where the π_is are irreducibles in $\mathfrak{O}_K$.

Since $\mathfrak{p}$ is prime, it follows that $\pi_i \in \mathfrak{p}$ from some i. Hence, $(\pi_i) \subseteq \mathfrak{p}$.

In a UFD every irreducible is prime. So (π_i) is a prime ideal. Primes are maximal in a number ring. Hence, $(\pi_i) = \mathfrak{p}$.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. The number ring $\mathfrak{O}_K$ is a UFD if and only if it is a PID.

Proof. ($\Leftarrow$) We already know that a PID is a UFD.

($\Rightarrow$) Suppose that $\mathfrak{O}_K$ is a UFD, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_K$.

We have $\mathfrak{p} \ni N(\mathfrak{p}) = \pi_1 \cdots \pi_k$ where the π_is are irreducibles in $\mathfrak{O}_K$.

Since $\mathfrak{p}$ is prime, it follows that $\pi_i \in \mathfrak{p}$ from some i. Hence, $(\pi_i) \subseteq \mathfrak{p}$.

In a UFD every irreducible is prime. So (π_i) is a prime ideal. Primes are maximal in a number ring. Hence, $(\pi_i) = \mathfrak{p}$.

The result now follows since every ideal of $\mathfrak{O}_K$ is a product of prime ideals. $\square$

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. Suppose that $\mathfrak{O}_K$ is not a UFD, and let $\pi \in \mathfrak{O}_K$ be irreducible but not prime.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. Suppose that $\mathfrak{O}_K$ is not a UFD, and let $\pi \in \mathfrak{O}_K$ be irreducible but not prime. Let $(\pi) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ be the prime factorization of (π).

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. Suppose that $\mathfrak{O}_K$ is not a UFD, and let $\pi \in \mathfrak{O}_K$ be irreducible but not prime. Let $(\pi) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ be the prime factorization of (π). Then no $\mathfrak{p}_i$ is principal.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. Suppose that $\mathfrak{O}_K$ is not a UFD, and let $\pi \in \mathfrak{O}_K$ be irreducible but not prime. Let $(\pi) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ be the prime factorization of (π). Then no $\mathfrak{p}_i$ is principal.

Proof. For the sake of contradiction, suppose $\mathfrak{p}_i = (\alpha)$ from some i and some $\alpha \in \mathfrak{O}_K$.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. Suppose that $\mathfrak{O}_K$ is not a UFD, and let $\pi \in \mathfrak{O}_K$ be irreducible but not prime. Let $(\pi) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ be the prime factorization of (π). Then no $\mathfrak{p}_i$ is principal.

Proof. For the sake of contradiction, suppose $\mathfrak{p}_i = (\alpha)$ from some i and some $\alpha \in \mathfrak{O}_K$. Then since $\mathfrak{p}_i | (\pi)$, it follows that $(\pi) \subseteq \mathfrak{p}_i = (\alpha)$.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. Suppose that $\mathfrak{O}_K$ is not a UFD, and let $\pi \in \mathfrak{O}_K$ be irreducible but not prime. Let $(\pi) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ be the prime factorization of (π). Then no $\mathfrak{p}_i$ is principal.

Proof. For the sake of contradiction, suppose $\mathfrak{p}_i = (\alpha)$ from some i and some $\alpha \in \mathfrak{O}_K$. Then since $\mathfrak{p}_i | (\pi)$, it follows that $(\pi) \subseteq \mathfrak{p}_i = (\alpha)$.

Hence, $\pi = \alpha\beta$ from some $\beta \in \mathfrak{O}_K$.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. Suppose that $\mathfrak{O}_K$ is not a UFD, and let $\pi \in \mathfrak{O}_K$ be irreducible but not prime. Let $(\pi) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ be the prime factorization of (π). Then no $\mathfrak{p}_i$ is principal.

Proof. For the sake of contradiction, suppose $\mathfrak{p}_i = (\alpha)$ from some i and some $\alpha \in \mathfrak{O}_K$. Then since $\mathfrak{p}_i | (\pi)$, it follows that $(\pi) \subseteq \mathfrak{p}_i = (\alpha)$.

Hence, $\pi = \alpha\beta$ from some $\beta \in \mathfrak{O}_K$.

Since $\mathfrak{p}$ is prime, so is α.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. Suppose that $\mathfrak{O}_K$ is not a UFD, and let $\pi \in \mathfrak{O}_K$ be irreducible but not prime. Let $(\pi) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ be the prime factorization of (π). Then no $\mathfrak{p}_i$ is principal.

Proof. For the sake of contradiction, suppose $\mathfrak{p}_i = (\alpha)$ from some i and some $\alpha \in \mathfrak{O}_K$. Then since $\mathfrak{p}_i | (\pi)$, it follows that $(\pi) \subseteq \mathfrak{p}_i = (\alpha)$.

Hence, $\pi = \alpha\beta$ from some $\beta \in \mathfrak{O}_K$.

Since $\mathfrak{p}$ is prime, so is α. Since π is irreducible, β is a unit.

$\mathfrak{O}_K$ is a UFD iff it's a PID

Proposition. Suppose that $\mathfrak{O}_K$ is not a UFD, and let $\pi \in \mathfrak{O}_K$ be irreducible but not prime. Let $(\pi) = \prod_{i=1}^{k} \mathfrak{p}_i^{e_i}$ be the prime factorization of (π). Then no $\mathfrak{p}_i$ is principal.

Proof. For the sake of contradiction, suppose $\mathfrak{p}_i = (\alpha)$ from some i and some $\alpha \in \mathfrak{O}_K$. Then since $\mathfrak{p}_i | (\pi)$, it follows that $(\pi) \subseteq \mathfrak{p}_i = (\alpha)$.

Hence, $\pi = \alpha\beta$ from some $\beta \in \mathfrak{O}_K$.

Since $\mathfrak{p}$ is prime, so is α. Since π is irreducible, β is a unit.

Hence, π is prime—a contradiction. $\square$