Math 361

March 20, 2023

Today

- Every nonzero ideal in $\mathfrak{O}_K$ is uniquely expressible as a product of prime ideals.

Fractional ideals

Let K be a number field with ring of integers $\mathfrak{O}_K$.

Fractional ideals

Let K be a number field with ring of integers $\mathfrak{O}_K$.

Definition. An $\mathfrak{O}_K$-submodule I is a *fractional ideal* of $\mathfrak{O}_K$ if 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 with ring of integers $\mathfrak{O}_K$.

Definition. An $\mathfrak{O}_K$-submodule I is a *fractional ideal* of $\mathfrak{O}_K$ if there exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$

- We can take $\alpha \in K \setminus \{0\}$ in the definition.

Fractional ideals

Let K be a number field with ring of integers $\mathfrak{O}_K$.

Definition. An $\mathfrak{O}_K$-submodule I is a *fractional ideal* of $\mathfrak{O}_K$ if there exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$

- We can take $\alpha \in K \setminus \{0\}$ in the definition.
- Every ordinary ideal is a fractional ideal.

Fractional ideals

Let K be a number field with ring of integers $\mathfrak{O}_K$.

Definition. An $\mathfrak{O}_K$-submodule I is a *fractional ideal* of $\mathfrak{O}_K$ if there exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$

- We can take $\alpha \in K \setminus \{0\}$ in the definition.
- Every ordinary ideal is a fractional ideal.
- $\alpha I \subseteq \mathfrak{O}_K$ is an ordinary ideal.

Fractional ideals

Let K be a number field with ring of integers $\mathfrak{O}_K$.

Definition. An $\mathfrak{O}_K$-submodule I is a *fractional ideal* of $\mathfrak{O}_K$ if there exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$

- We can take $\alpha \in K \setminus \{0\}$ in the definition.
- Every ordinary ideal is a fractional ideal.
- $\alpha I \subseteq \mathfrak{O}_K$ is an ordinary ideal.
- The fractional ideals are exactly the $\mathfrak{O}_K$-submodules of K of the form $\alpha^{-1}\mathfrak{a}$ for some ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ and nonzero $\alpha \in \mathfrak{O}_K$.

Fractional ideals

Let K be a number field with ring of integers $\mathfrak{O}_K$.

Definition. An $\mathfrak{O}_K$-submodule I is a *fractional ideal* of $\mathfrak{O}_K$ if there exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$

- We can take $\alpha \in K \setminus \{0\}$ in the definition.
- Every ordinary ideal is a fractional ideal.
- $\alpha I \subseteq \mathfrak{O}_K$ is an ordinary ideal.
- The fractional ideals are exactly the $\mathfrak{O}_K$-submodules of K of the form $\alpha^{-1}\mathfrak{a}$ for some ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ and nonzero $\alpha \in \mathfrak{O}_K$.
- Fractional ideals are exactly the finitely generated $\mathfrak{O}_K$-submodules of K.

Fractional ideals

Let K be a number field with ring of integers $\mathfrak{O}_K$.

Definition. An $\mathfrak{O}_K$-submodule I is a *fractional ideal* of $\mathfrak{O}_K$ if there exists $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$

- We can take $\alpha \in K \setminus \{0\}$ in the definition.
- Every ordinary ideal is a fractional ideal.
- $\alpha I \subseteq \mathfrak{O}_K$ is an ordinary ideal.
- The fractional ideals are exactly the $\mathfrak{O}_K$-submodules of K of the form $\alpha^{-1}\mathfrak{a}$ for some ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ and nonzero $\alpha \in \mathfrak{O}_K$.
- Fractional ideals are exactly the finitely generated $\mathfrak{O}_K$-submodules of K.

Fractional ideals

The product of two fractional ideals I, J in $\mathfrak{O}_K$ is the $\mathfrak{O}_K$-submodule of K

$$IJ = \mathrm{Span}_{\mathfrak{O}_K}\{ij : i \in I, j \in J\}.$$

Fractional ideals

The product of two fractional ideals I, J in $\mathfrak{O}_K$ is the $\mathfrak{O}_K$-submodule of K

$$IJ = \mathrm{Span}_{\mathfrak{O}_K}\{ij : i \in I, j \in J\}.$$

Proposition. The set of nonzero fractional ideals in a number field K forms an abelian group under multiplication.

Fractional ideals

The product of two fractional ideals I, J in $\mathfrak{O}_K$ is the $\mathfrak{O}_K$-submodule of K

$$IJ = \mathrm{Span}_{\mathfrak{O}_K}\{ij : i \in I, j \in J\}.$$

Proposition. The set of nonzero fractional ideals in a number field K forms an abelian group under multiplication. If I is a nonzero fractional ideal of $\mathfrak{O}_K$, then its inverse is

$$I^{-1} = \{x \in K : xI \subseteq \mathfrak{O}_K\}.$$

Fractional ideals

The product of two fractional ideals I, J in $\mathfrak{O}_K$ is the $\mathfrak{O}_K$-submodule of K

$$IJ = \mathrm{Span}_{\mathfrak{O}_K}\{ij : i \in I, j \in J\}.$$

Proposition. The set of nonzero fractional ideals in a number field K forms an abelian group under multiplication. If I is a nonzero fractional ideal of $\mathfrak{O}_K$, then its inverse is

$$I^{-1} = \{x \in K : xI \subseteq \mathfrak{O}_K\}.$$

Proof. The only difficult property to prove is that I^{-1} is the inverse of I.

Fractional ideals

The product of two fractional ideals I, J in $\mathfrak{O}_K$ is the $\mathfrak{O}_K$-submodule of K

$$IJ = \mathrm{Span}_{\mathfrak{O}_K}\{ij : i \in I, j \in J\}.$$

Proposition. The set of nonzero fractional ideals in a number field K forms an abelian group under multiplication. If I is a nonzero fractional ideal of $\mathfrak{O}_K$, then its inverse is

$$I^{-1} = \{x \in K : xI \subseteq \mathfrak{O}_K\}.$$

Proof. The only difficult property to prove is that I^{-1} is the inverse of I. We do that in the proof of the upcoming theorem. $\square$

In $\mathfrak{O}_K$, *to contain is to divide*

Note: $I \subseteq J \Rightarrow J^{-1} \subseteq I^{-1}$.

In $\mathfrak{O}_K$, *to contain is to divide*

Note: $I \subseteq J \Rightarrow J^{-1} \subseteq I^{-1}$.

Definition. If I, J are ideals in a ring R, then I *divides* J, denoted $I|J$ if

In $\mathfrak{O}_K$, *to contain is to divide*

Note: $I \subseteq J \Rightarrow J^{-1} \subseteq I^{-1}$.

Definition. If I, J are ideals in a ring R, then I *divides* J, denoted $I|J$ if there exists an ideal H such that $J = IH$.

In $\mathfrak{O}_K$, *to contain is to divide*

Note: $I \subseteq J \Rightarrow J^{-1} \subseteq I^{-1}$.

Definition. If I, J are ideals in a ring R, then I *divides* J, denoted $I|J$ if there exists an ideal H such that $J = IH$.

Proposition. (*To contain is to divide.*)

In $\mathfrak{O}_K$, *to contain is to divide*

Note: $I \subseteq J \Rightarrow J^{-1} \subseteq I^{-1}$.

Definition. If I, J are ideals in a ring R, then I *divides* J, denoted $I|J$ if there exists an ideal H such that $J = IH$.

Proposition. (*To contain is to divide.*) Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in $\mathfrak{O}_K$. Then $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$.

In $\mathfrak{O}_K$, *to contain is to divide*

Note: $I \subseteq J \Rightarrow J^{-1} \subseteq I^{-1}$.

Definition. If I, J are ideals in a ring R, then I *divides* J, denoted $I|J$ if there exists an ideal H such that $J = IH$.

Proposition. (*To contain is to divide.*) Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in $\mathfrak{O}_K$. Then $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{b} \subseteq \mathfrak{a}$.

Proof. On board. $\square$

Prime factorization of ideals

Theorem. Let K be a number field. Every nonzero ideal of $\mathfrak{O}_K$ can be factored into a product of prime ideals, uniquely up to the order of factors.

Prime factorization of ideals

Theorem. Let K be a number field. Every nonzero ideal of $\mathfrak{O}_K$ can be factored into a product of prime ideals, uniquely up to the order of factors.

Outline of proof.

Prime factorization of ideals

Theorem. Let K be a number field. Every nonzero ideal of $\mathfrak{O}_K$ can be factored into a product of prime ideals, uniquely up to the order of factors.

Outline of proof.

Step 1. $\mathfrak{a} \neq 0$ an ideal $\Rightarrow \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$ for some nonzero prime ideals $\mathfrak{p}_i$.

Prime factorization of ideals

Theorem. Let K be a number field. Every nonzero ideal of $\mathfrak{O}_K$ can be factored into a product of prime ideals, uniquely up to the order of factors.

Outline of proof.

Step 1. $\mathfrak{a} \neq 0$ an ideal $\Rightarrow \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$ for some nonzero prime ideals $\mathfrak{p}_i$.

Step 2. $I \cdot I^{-1} = (1) = \mathfrak{O}_K$ for any nonzero fractional ideal I.

Prime factorization of ideals

Theorem. Let K be a number field. Every nonzero ideal of $\mathfrak{O}_K$ can be factored into a product of prime ideals, uniquely up to the order of factors.

Outline of proof.

Step 1. $\mathfrak{a} \neq 0$ an ideal $\Rightarrow \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$ for some nonzero prime ideals $\mathfrak{p}_i$.

Step 2. $I \cdot I^{-1} = (1) = \mathfrak{O}_K$ for any nonzero fractional ideal I.

Step 3. Every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ is a product of prime ideals.

Prime factorization of ideals

Theorem. Let K be a number field. Every nonzero ideal of $\mathfrak{O}_K$ can be factored into a product of prime ideals, uniquely up to the order of factors.

Outline of proof.

Step 1. $\mathfrak{a} \neq 0$ an ideal $\Rightarrow \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$ for some nonzero prime ideals $\mathfrak{p}_i$.

Step 2. $I \cdot I^{-1} = (1) = \mathfrak{O}_K$ for any nonzero fractional ideal I.

Step 3. Every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ is a product of prime ideals.

Step 4. Prime factorization of ideals in $\mathfrak{O}_K$ is unique.

Prime factorization of ideals

Theorem. Let K be a number field. Every nonzero ideal of $\mathfrak{O}_K$ can be factored into a product of prime ideals, uniquely up to the order of factors.

Outline of proof.

Step 1. $\mathfrak{a} \neq 0$ an ideal $\Rightarrow \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$ for some nonzero prime ideals $\mathfrak{p}_i$.

Step 2. $I \cdot I^{-1} = (1) = \mathfrak{O}_K$ for any nonzero fractional ideal I.

Step 3. Every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ is a product of prime ideals.

Step 4. Prime factorization of ideals in $\mathfrak{O}_K$ is unique.

Prove Steps 3, Step 4, then Step 1 on the board.

Prime factorization of ideals

Step 2. $I \cdot I^{-1} = (1) = \mathfrak{O}_K$ for any nonzero fractional ideal I.

Prime factorization of ideals

Step 2. $I \cdot I^{-1} = (1) = \mathfrak{O}_K$ for any nonzero fractional ideal I.

Proof.

Step 2.1 Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. (By "proper" we mean $\mathfrak{a} \subsetneq \mathfrak{O}_K$.) Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Prime factorization of ideals

Step 2. $I \cdot I^{-1} = (1) = \mathfrak{O}_K$ for any nonzero fractional ideal I.

Proof.

Step 2.1 Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. (By "proper" we mean $\mathfrak{a} \subsetneq \mathfrak{O}_K$.) Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Step 2.2 Claim: if $\mathfrak{a}$ is a nonzero ideal and $\mathfrak{a}S \subseteq \mathfrak{a}$ for any subset $S \subseteq K$, then $S \subseteq \mathfrak{O}_K$.

Prime factorization of ideals

Step 2. $I \cdot I^{-1} = (1) = \mathfrak{O}_K$ for any nonzero fractional ideal I.

Proof.

Step 2.1 Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. (By "proper" we mean $\mathfrak{a} \subsetneq \mathfrak{O}_K$.) Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Step 2.2 Claim: if $\mathfrak{a}$ is a nonzero ideal and $\mathfrak{a}S \subseteq \mathfrak{a}$ for any subset $S \subseteq K$, then $S \subseteq \mathfrak{O}_K$.

Step 2.3 Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{O}_K$. Claim: $\mathfrak{p}^{-1}\mathfrak{p} = (1) = \mathfrak{O}_K$. So $\mathfrak{p}^{-1}$ is the multiplicative inverse of $\mathfrak{p}$.

Prime factorization of ideals

Step 2. $I \cdot I^{-1} = (1) = \mathfrak{O}_K$ for any nonzero fractional ideal I.

Proof.

Step 2.1 Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. (By "proper" we mean $\mathfrak{a} \subsetneq \mathfrak{O}_K$.) Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Step 2.2 Claim: if $\mathfrak{a}$ is a nonzero ideal and $\mathfrak{a}S \subseteq \mathfrak{a}$ for any subset $S \subseteq K$, then $S \subseteq \mathfrak{O}_K$.

Step 2.3 Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{O}_K$. Claim: $\mathfrak{p}^{-1}\mathfrak{p} = (1) = \mathfrak{O}_K$. So $\mathfrak{p}^{-1}$ is the multiplicative inverse of $\mathfrak{p}$.

Step 2.4 For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Prime factorization of ideals

Step 2. $I \cdot I^{-1} = (1) = \mathfrak{O}_K$ for any nonzero fractional ideal I.

Proof.

Step 2.1 Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. (By "proper" we mean $\mathfrak{a} \subsetneq \mathfrak{O}_K$.) Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Step 2.2 Claim: if $\mathfrak{a}$ is a nonzero ideal and $\mathfrak{a}S \subseteq \mathfrak{a}$ for any subset $S \subseteq K$, then $S \subseteq \mathfrak{O}_K$.

Step 2.3 Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{O}_K$. Claim: $\mathfrak{p}^{-1}\mathfrak{p} = (1) = \mathfrak{O}_K$. So $\mathfrak{p}^{-1}$ is the multiplicative inverse of $\mathfrak{p}$.

Step 2.4 For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Step 2.5 If I is a nonzero fractional ideal, then $II^{-1} = \mathfrak{O}_K$.

Prime factorization of ideals

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Prime factorization of ideals

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Proof. Pick a prime $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. (Why is this possible?)

Prime factorization of ideals

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Proof. Pick a prime $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. (Why is this possible?) It suffices to show $\mathfrak{O}_K \subsetneq \mathfrak{p}^{-1}$. (Why?)

Prime factorization of ideals

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Proof. Pick a prime $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. (Why is this possible?) It suffices to show $\mathfrak{O}_K \subsetneq \mathfrak{p}^{-1}$. (Why?)

Our problem is to find a non-integer $\gamma \in \mathfrak{p}^{-1}$.

Prime factorization of ideals

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Proof. Pick a prime $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. (Why is this possible?) It suffices to show $\mathfrak{O}_K \subsetneq \mathfrak{p}^{-1}$. (Why?)

Our problem is to find a non-integer $\gamma \in \mathfrak{p}^{-1}$.

Take $0 \neq \alpha \in \mathfrak{p}$.

Prime factorization of ideals

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Proof. Pick a prime $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. (Why is this possible?) It suffices to show $\mathfrak{O}_K \subsetneq \mathfrak{p}^{-1}$. (Why?)

Our problem is to find a non-integer $\gamma \in \mathfrak{p}^{-1}$.

Take $0 \neq \alpha \in \mathfrak{p}$. Then we may pick nonzero primes $\mathfrak{p}_i$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (\alpha) \subseteq \mathfrak{p}.$$

with r minimal.

Prime factorization of ideals

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Proof. Pick a prime $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. (Why is this possible?) It suffices to show $\mathfrak{O}_K \subsetneq \mathfrak{p}^{-1}$. (Why?)

Our problem is to find a non-integer $\gamma \in \mathfrak{p}^{-1}$.

Take $0 \neq \alpha \in \mathfrak{p}$. Then we may pick nonzero primes $\mathfrak{p}_i$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (\alpha) \subseteq \mathfrak{p}.$$

with r minimal. We may assume $\mathfrak{p}_1 = \mathfrak{p}$. (Why?)

Prime factorization of ideals

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Proof. Pick a prime $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. (Why is this possible?) It suffices to show $\mathfrak{O}_K \subsetneq \mathfrak{p}^{-1}$. (Why?)

Our problem is to find a non-integer $\gamma \in \mathfrak{p}^{-1}$.

Take $0 \neq \alpha \in \mathfrak{p}$. Then we may pick nonzero primes $\mathfrak{p}_i$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (\alpha) \subseteq \mathfrak{p}.$$

with r minimal. We may assume $\mathfrak{p}_1 = \mathfrak{p}$. (Why?) By minimality of r, we have $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (\alpha)$.

Prime factorization of ideals

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Proof. Pick a prime $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. (Why is this possible?) It suffices to show $\mathfrak{O}_K \subsetneq \mathfrak{p}^{-1}$. (Why?)

Our problem is to find a non-integer $\gamma \in \mathfrak{p}^{-1}$.

Take $0 \neq \alpha \in \mathfrak{p}$. Then we may pick nonzero primes $\mathfrak{p}_i$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (\alpha) \subseteq \mathfrak{p}.$$

with r minimal. We may assume $\mathfrak{p}_1 = \mathfrak{p}$. (Why?) By minimality of r, we have $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (\alpha)$. Take $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (\alpha)$.

Prime factorization of ideals

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Proof. Pick a prime $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. (Why is this possible?) It suffices to show $\mathfrak{O}_K \subsetneq \mathfrak{p}^{-1}$. (Why?)

Our problem is to find a non-integer $\gamma \in \mathfrak{p}^{-1}$.

Take $0 \neq \alpha \in \mathfrak{p}$. Then we may pick nonzero primes $\mathfrak{p}_i$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (\alpha) \subseteq \mathfrak{p}.$$

with r minimal. We may assume $\mathfrak{p}_1 = \mathfrak{p}$. (Why?) By minimality of r, we have $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (\alpha)$. Take $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (\alpha)$.
Let $\gamma := \alpha^{-1}\beta$.

Prime factorization of ideals

Step 2.1. Let $\mathfrak{a} \subseteq \mathfrak{O}_K$ be a proper nonzero ideal. Claim: $\mathfrak{O}_K \subsetneq \mathfrak{a}^{-1}$.

Proof. Pick a prime $\mathfrak{p}$ such that $\mathfrak{a} \subseteq \mathfrak{p}$. (Why is this possible?) It suffices to show $\mathfrak{O}_K \subsetneq \mathfrak{p}^{-1}$. (Why?)

Our problem is to find a non-integer $\gamma \in \mathfrak{p}^{-1}$.

Take $0 \neq \alpha \in \mathfrak{p}$. Then we may pick nonzero primes $\mathfrak{p}_i$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (\alpha) \subseteq \mathfrak{p}.$$

with r minimal. We may assume $\mathfrak{p}_1 = \mathfrak{p}$. (Why?) By minimality of r, we have $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (\alpha)$. Take $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (\alpha)$. Let $\gamma := \alpha^{-1}\beta$. Then $\gamma \in \mathfrak{p}^{-1}$ but $\gamma \notin \mathfrak{O}_K$.

Prime factorization of ideals

Step 2.2. If $\mathfrak{a}$ is a nonzero ideal and $\mathfrak{a}S \subseteq \mathfrak{a}$ for any subset $S \subseteq K$, then $S \subseteq \mathfrak{O}_K$.

Prime factorization of ideals

Step 2.2. If $\mathfrak{a}$ is a nonzero ideal and $\mathfrak{a}S \subseteq \mathfrak{a}$ for any subset $S \subseteq K$, then $S \subseteq \mathfrak{O}_K$.

Proof. Let $\theta \in S$.

Prime factorization of ideals

Step 2.2. If $\mathfrak{a}$ is a nonzero ideal and $\mathfrak{a}S \subseteq \mathfrak{a}$ for any subset $S \subseteq K$, then $S \subseteq \mathfrak{O}_K$.

Proof. Let $\theta \in S$. Then $M := \mathfrak{a}$ is a finitely generated $\mathbb{Z}$-submodule of K such that $\theta M \subseteq M$.

Prime factorization of ideals

Step 2.3. Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{O}_K$.
Claim: $\mathfrak{p}^{-1}\mathfrak{p} = (1) = \mathfrak{O}_K$. So $\mathfrak{p}^{-1}$ is the multiplicative inverse of $\mathfrak{p}$.

Prime factorization of ideals

Step 2.3. Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{O}_K$.
Claim: $\mathfrak{p}^{-1}\mathfrak{p} = (1) = \mathfrak{O}_K$. So $\mathfrak{p}^{-1}$ is the multiplicative inverse of $\mathfrak{p}$.

Proof. $\mathfrak{O}_K \subset \mathfrak{p}^{-1} \Rightarrow \mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1}$. Definition of $\mathfrak{p}^{-1} \Rightarrow \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$.

Prime factorization of ideals

Step 2.3. Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{O}_K$.
Claim: $\mathfrak{p}^{-1}\mathfrak{p} = (1) = \mathfrak{O}_K$. So $\mathfrak{p}^{-1}$ is the multiplicative inverse of $\mathfrak{p}$.

Proof. $\mathfrak{O}_K \subset \mathfrak{p}^{-1} \Rightarrow \mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1}$. Definition of $\mathfrak{p}^{-1} \Rightarrow \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$.

So $\mathfrak{p}\mathfrak{p}^{-1}$ is an ideal containing the maximal ideal $\mathfrak{p}$.

Prime factorization of ideals

Step 2.3. Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{O}_K$.
Claim: $\mathfrak{p}^{-1}\mathfrak{p} = (1) = \mathfrak{O}_K$. So $\mathfrak{p}^{-1}$ is the multiplicative inverse of $\mathfrak{p}$.

Proof. $\mathfrak{O}_K \subset \mathfrak{p}^{-1} \Rightarrow \mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1}$. Definition of $\mathfrak{p}^{-1} \Rightarrow \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$.

So $\mathfrak{p}\mathfrak{p}^{-1}$ is an ideal containing the maximal ideal $\mathfrak{p}$.

Two possibilities: $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}_K$.

Prime factorization of ideals

Step 2.3. Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{O}_K$.
Claim: $\mathfrak{p}^{-1}\mathfrak{p} = (1) = \mathfrak{O}_K$. So $\mathfrak{p}^{-1}$ is the multiplicative inverse of $\mathfrak{p}$.

Proof. $\mathfrak{O}_K \subset \mathfrak{p}^{-1} \Rightarrow \mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1}$. Definition of $\mathfrak{p}^{-1} \Rightarrow \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$.

So $\mathfrak{p}\mathfrak{p}^{-1}$ is an ideal containing the maximal ideal $\mathfrak{p}$.

Two possibilities: $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}_K$.

If $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, Step 2.2 says $\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$, in contradiction to Step 2.1.

Prime factorization of ideals

Step 2.3. Let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{O}_K$.
Claim: $\mathfrak{p}^{-1}\mathfrak{p} = (1) = \mathfrak{O}_K$. So $\mathfrak{p}^{-1}$ is the multiplicative inverse of $\mathfrak{p}$.

Proof. $\mathfrak{O}_K \subset \mathfrak{p}^{-1} \Rightarrow \mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1}$. Definition of $\mathfrak{p}^{-1} \Rightarrow \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$.

So $\mathfrak{p}\mathfrak{p}^{-1}$ is an ideal containing the maximal ideal $\mathfrak{p}$.

Two possibilities: $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}_K$.

If $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, Step 2.2 says $\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$, in contradiction to Step 2.1.

Done.

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof. Let $\mathcal{A}$ be the set of nonzero ideals without the desired property.

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof. Let $\mathcal{A}$ be the set of nonzero ideals without the desired property.

If $\mathcal{A} \neq \emptyset$, choose a maximal element $\mathfrak{a} \in \mathcal{A}$.

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof. Let $\mathcal{A}$ be the set of nonzero ideals without the desired property.

If $\mathcal{A} \neq \emptyset$, choose a maximal element $\mathfrak{a} \in \mathcal{A}$. Choose a prime $\mathfrak{p}$ containing $\mathfrak{a}$.

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof. Let $\mathcal{A}$ be the set of nonzero ideals without the desired property.

If $\mathcal{A} \neq \emptyset$, choose a maximal element $\mathfrak{a} \in \mathcal{A}$. Choose a prime $\mathfrak{p}$ containing $\mathfrak{a}$.

$\mathfrak{a} \subset \mathfrak{p} \subset \mathfrak{O}_K \Rightarrow \mathfrak{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof. Let $\mathcal{A}$ be the set of nonzero ideals without the desired property.

If $\mathcal{A} \neq \emptyset$, choose a maximal element $\mathfrak{a} \in \mathcal{A}$. Choose a prime $\mathfrak{p}$ containing $\mathfrak{a}$.

$\mathfrak{a} \subset \mathfrak{p} \subset \mathfrak{O}_K \Rightarrow \mathfrak{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1} \Rightarrow \mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K$

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof. Let $\mathcal{A}$ be the set of nonzero ideals without the desired property.

If $\mathcal{A} \neq \emptyset$, choose a maximal element $\mathfrak{a} \in \mathcal{A}$. Choose a prime $\mathfrak{p}$ containing $\mathfrak{a}$.

$\mathfrak{a} \subset \mathfrak{p} \subset \mathfrak{O}_K \Rightarrow \mathfrak{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1} \Rightarrow \mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K$

If $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, then $\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$, by Step 2.2, contradicting Step 2.1.

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof. Let $\mathcal{A}$ be the set of nonzero ideals without the desired property.

If $\mathcal{A} \neq \emptyset$, choose a maximal element $\mathfrak{a} \in \mathcal{A}$. Choose a prime $\mathfrak{p}$ containing $\mathfrak{a}$.

$\mathfrak{a} \subset \mathfrak{p} \subset \mathfrak{O}_K \Rightarrow \mathfrak{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1} \Rightarrow \mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K$

If $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, then $\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$, by Step 2.2, contradicting Step 2.1. So $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$.

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof. Let $\mathcal{A}$ be the set of nonzero ideals without the desired property.

If $\mathcal{A} \neq \emptyset$, choose a maximal element $\mathfrak{a} \in \mathcal{A}$. Choose a prime $\mathfrak{p}$ containing $\mathfrak{a}$.

$\mathfrak{a} \subset \mathfrak{p} \subset \mathfrak{O}_K \Rightarrow \mathfrak{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1} \Rightarrow \mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K$

If $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, then $\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$, by Step 2.2, contradicting Step 2.1. So $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$. By maximality of $\mathfrak{a}$, we have $(\mathfrak{a}\mathfrak{p}^{-1})(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathfrak{O}_K$.

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof. Let $\mathcal{A}$ be the set of nonzero ideals without the desired property.

If $\mathcal{A} \neq \emptyset$, choose a maximal element $\mathfrak{a} \in \mathcal{A}$. Choose a prime $\mathfrak{p}$ containing $\mathfrak{a}$.

$\mathfrak{a} \subset \mathfrak{p} \subset \mathfrak{O}_K \Rightarrow \mathfrak{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1} \Rightarrow \mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K$

If $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, then $\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$, by Step 2.2, contradicting Step 2.1. So $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$. By maximality of $\mathfrak{a}$, we have $(\mathfrak{a}\mathfrak{p}^{-1})(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathfrak{O}_K$.

By definition of $\mathfrak{a}^{-1}$, we have $\mathfrak{p}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1}$

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof. Let $\mathcal{A}$ be the set of nonzero ideals without the desired property.

If $\mathcal{A} \neq \emptyset$, choose a maximal element $\mathfrak{a} \in \mathcal{A}$. Choose a prime $\mathfrak{p}$ containing $\mathfrak{a}$.

$\mathfrak{a} \subset \mathfrak{p} \subset \mathfrak{O}_K \Rightarrow \mathfrak{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1} \Rightarrow \mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K$

If $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, then $\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$, by Step 2.2, contradicting Step 2.1. So $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$. By maximality of $\mathfrak{a}$, we have $(\mathfrak{a}\mathfrak{p}^{-1})(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathfrak{O}_K$.

By definition of $\mathfrak{a}^{-1}$, we have $\mathfrak{p}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1}$

But then $\mathfrak{O}_K = \mathfrak{a}\mathfrak{p}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K$,

Prime factorization of ideals

Step 2.4. For every nonzero ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, we have $\mathfrak{a}\mathfrak{a}^{-1} = (1) = \mathfrak{O}_K$.

Proof. Let $\mathcal{A}$ be the set of nonzero ideals without the desired property.

If $\mathcal{A} \neq \emptyset$, choose a maximal element $\mathfrak{a} \in \mathcal{A}$. Choose a prime $\mathfrak{p}$ containing $\mathfrak{a}$.

$$\mathfrak{a} \subset \mathfrak{p} \subset \mathfrak{O}_K \Rightarrow \mathfrak{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1} \Rightarrow \mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K$$

If $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$, then $\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K$, by Step 2.2, contradicting Step 2.1. So $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$. By maximality of $\mathfrak{a}$, we have $(\mathfrak{a}\mathfrak{p}^{-1})(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = \mathfrak{O}_K$.

By definition of $\mathfrak{a}^{-1}$, we have $\mathfrak{p}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1}$

But then $\mathfrak{O}_K = \mathfrak{a}\mathfrak{p}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{O}_K$, forcing $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{O}_K$. Contradiction.