# Math 361

March 10, 2023

# Today

- Review some Noetherian stuff.

# Today

- Review some Noetherian stuff.
- Review and finish proof that $\mathfrak{O}_K$ is Dedekind.

# Today

- Review some Noetherian stuff.
- Review and finish proof that $\mathfrak{O}_K$ is Dedekind.
- Fractional ideals.

# Today

- Review some Noetherian stuff.
- Review and finish proof that $\mathfrak{O}_K$ is Dedekind.
- Fractional ideals.
- Every nonzero ideal in $\mathfrak{O}_K$ is uniquely expressible as a product of prime ideals.

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

**Prop.** If $S$ is finitely generated as an $R$-module, then $S$ is Noetherian.

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

**Prop.** If $S$ is finitely generated as an $R$-module, then $S$ is Noetherian.

**Proof (not using the HBT).**

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

**Prop.** If $S$ is finitely generated as an $R$-module, then $S$ is Noetherian.

**Proof (not using the HBT).** Let $I$ be an ideal of $S$.

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

**Prop.** If $S$ is finitely generated as an $R$-module, then $S$ is Noetherian.

**Proof (not using the HBT).** Let $I$ be an ideal of $S$. Since a finitely generated module over a Noetherian ring is Noetherian, $S$ is a Noetherian $R$-module.

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

**Prop.** If $S$ is finitely generated as an $R$-module, then $S$ is Noetherian.

**Proof (not using the HBT).** Let $I$ be an ideal of $S$. Since a finitely generated module over a Noetherian ring is Noetherian, $S$ is a Noetherian $R$-module.

Let $I$ be an ideal of $S$,

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

**Prop.** If $S$ is finitely generated as an $R$-module, then $S$ is Noetherian.

**Proof (not using the HBT).** Let $I$ be an ideal of $S$. Since a finitely generated module over a Noetherian ring is Noetherian, $S$ is a Noetherian $R$-module.

Let $I$ be an ideal of $S$, i.e., an $S$-submodule of $S$.

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

**Prop.** If $S$ is finitely generated as an $R$-module, then $S$ is Noetherian.

**Proof (not using the HBT).** Let $I$ be an ideal of $S$. Since a finitely generated module over a Noetherian ring is Noetherian, $S$ is a Noetherian $R$-module.

Let $I$ be an ideal of $S$, i.e., an $S$-submodule of $S$. Then $I$ is an $R$-submodule of $S$.

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

**Prop.** If $S$ is finitely generated as an $R$-module, then $S$ is Noetherian.

**Proof (not using the HBT).** Let $I$ be an ideal of $S$. Since a finitely generated module over a Noetherian ring is Noetherian, $S$ is a Noetherian $R$-module.

Let $I$ be an ideal of $S$, i.e., an $S$-submodule of $S$. Then $I$ is an $R$-submodule of $S$. Since $S$ is a Noetherian $R$-module, $I$ is finitely generated as an $R$-module.

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

**Prop.** If $S$ is finitely generated as an $R$-module, then $S$ is Noetherian.

**Proof (not using the HBT).** Let $I$ be an ideal of $S$. Since a finitely generated module over a Noetherian ring is Noetherian, $S$ is a Noetherian $R$-module.

Let $I$ be an ideal of $S$, i.e., an $S$-submodule of $S$. Then $I$ is an $R$-submodule of $S$. Since $S$ is a Noetherian $R$-module, $I$ is finitely generated as an $R$-module. Say $I = \mathrm{Span}_R\{s_1, \ldots, s_k\}$ with the $s_i \in S$.

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

**Prop.** If $S$ is finitely generated as an $R$-module, then $S$ is Noetherian.

**Proof (not using the HBT).** Let $I$ be an ideal of $S$. Since a finitely generated module over a Noetherian ring is Noetherian, $S$ is a Noetherian $R$-module.

Let $I$ be an ideal of $S$, i.e., an $S$-submodule of $S$. Then $I$ is an $R$-submodule of $S$. Since $S$ is a Noetherian $R$-module, $I$ is finitely generated as an $R$-module. Say $I = \mathrm{Span}_R\{s_1, \ldots, s_k\}$ with the $s_i \in S$. Then $I = (s_1, \ldots, s_k)$

# Noetherian stuff

Suppose that $R \subseteq S$ is an extension of rings and that $R$ is Noetherian.

**Theorem.** If $S$ is finitely generated as a ring over $R$, then $S$ is Noetherian.

**Proof.** Hilbert basis theorem. $\square$

**Prop.** If $S$ is finitely generated as an $R$-module, then $S$ is Noetherian.

**Proof (not using the HBT).** Let $I$ be an ideal of $S$. Since a finitely generated module over a Noetherian ring is Noetherian, $S$ is a Noetherian $R$-module.

Let $I$ be an ideal of $S$, i.e., an $S$-submodule of $S$. Then $I$ is an $R$-submodule of $S$. Since $S$ is a Noetherian $R$-module, $I$ is finitely generated as an $R$-module. Say $I = \mathrm{Span}_R\{s_1, \ldots, s_k\}$ with the $s_i \in S$. Then $I = (s_1, \ldots, s_k) = \mathrm{Span}_S\{s_1, \ldots, s_k\}$. $\square$

# Finish result from last time

See slides from last time.

# 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 $\alpha I \subseteq \mathfrak{O}_K$

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

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 $\alpha I \subseteq \mathfrak{O}_K$

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

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

Question: Is every (ordinary) ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ 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 $\alpha I \subseteq \mathfrak{O}_K$

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

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

Question: Is every (ordinary) ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ a fractional ideal?
Answer: Yes. For instance, $1 \cdot \mathfrak{a} \subseteq \mathfrak{a}$.

# 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 $\alpha I \subseteq \mathfrak{O}_K$

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

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

Question: Is every (ordinary) ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ a fractional ideal?
Answer: Yes. For instance, $1 \cdot \mathfrak{a} \subseteq \mathfrak{a}$.

Question: In the definition, could the condition be "$c \in K \setminus \{0\}$ such that $cI \subseteq \mathfrak{O}_K$"?

# 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 $\alpha I \subseteq \mathfrak{O}_K$

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

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

Question: Is every (ordinary) ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ a fractional ideal?
Answer: Yes. For instance, $1 \cdot \mathfrak{a} \subseteq \mathfrak{a}$.

Question: In the definition, could the condition be "$c \in K \setminus \{0\}$ such that $cI \subseteq \mathfrak{O}_K$"? Answer: Yes.

# 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 $\alpha I \subseteq \mathfrak{O}_K$

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

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

Question: Is every (ordinary) ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ a fractional ideal?
Answer: Yes. For instance, $1 \cdot \mathfrak{a} \subseteq \mathfrak{a}$.

Question: In the definition, could the condition be "$c \in K \setminus \{0\}$ such that $cI \subseteq \mathfrak{O}_K$"? Answer: Yes. We can write $c = \alpha/\beta$ with $\alpha, \beta \in \mathfrak{O}_K$.

# 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 $\alpha I \subseteq \mathfrak{O}_K$

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

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

Question: Is every (ordinary) ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$ a fractional ideal?
Answer: Yes. For instance, $1 \cdot \mathfrak{a} \subseteq \mathfrak{a}$.

Question: In the definition, could the condition be "$c \in K \setminus \{0\}$ such that $cI \subseteq \mathfrak{O}_K$"? Answer: Yes. We can write $c = \alpha/\beta$ with $\alpha, \beta \in \mathfrak{O}_K$. Then $\beta c \in \mathfrak{O}_K$, and $\beta c I \subseteq \mathfrak{O}_K$.

# Fractional ideals

- Suppose $I \subset K$ is a fractional ideal of $\mathfrak{O}_K$.

# Fractional ideals

- Suppose $I \subset K$ is a fractional ideal of $\mathfrak{O}_K$. Take $\alpha \in \mathfrak{O}_K$ such that $\alpha I \subseteq \mathfrak{O}_K$.

# Fractional ideals

- Suppose $I \subset K$ is a fractional ideal of $\mathfrak{O}_K$. Take $\alpha \in \mathfrak{O}_K$ such that $\alpha I \subseteq \mathfrak{O}_K$. Then $\alpha I$ is an $\mathfrak{O}_K$-submodule of $\mathfrak{O}_K$,

# Fractional ideals

- Suppose $I \subset K$ is a fractional ideal of $\mathfrak{O}_K$. Take $\alpha \in \mathfrak{O}_K$ such that $\alpha I \subseteq \mathfrak{O}_K$. Then $\alpha I$ is an $\mathfrak{O}_K$-submodule of $\mathfrak{O}_K$, i.e., an ideal.

# Fractional ideals

- Suppose $I \subset K$ is a fractional ideal of $\mathfrak{O}_K$. Take $\alpha \in \mathfrak{O}_K$ such that $\alpha I \subseteq \mathfrak{O}_K$. Then $\alpha I$ is an $\mathfrak{O}_K$-submodule of $\mathfrak{O}_K$, i.e., an 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

**Proposition.** Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of $K$.

# Fractional ideals

**Proposition.** Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of $K$.

**Proof.** ($\Rightarrow$) First, suppose that $I$ is a fractional ideal of $\mathfrak{O}_K$,

# Fractional ideals

**Proposition.** Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of $K$.

**Proof.** $(\Rightarrow)$ First, suppose that $I$ is a fractional ideal of $\mathfrak{O}_K$, and take $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$.

# Fractional ideals

**Proposition.** Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of $K$.

**Proof.** $(\Rightarrow)$ First, suppose that $I$ is a fractional ideal of $\mathfrak{O}_K$, and take $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$. Then $\alpha I$ is an ideal of the Noetherian ring $\mathfrak{O}_K$.

# Fractional ideals

**Proposition.** Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of $K$.

**Proof.** $(\Rightarrow)$ First, suppose that $I$ is a fractional ideal of $\mathfrak{O}_K$, and take $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$. Then $\alpha I$ is an ideal of the Noetherian ring $\mathfrak{O}_K$. Hence, $\alpha I$ is finitely generated as an $\mathfrak{O}_K$-module.

# Fractional ideals

**Proposition.** Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of $K$.

**Proof.** ($\Rightarrow$) First, suppose that $I$ is a fractional ideal of $\mathfrak{O}_K$, and take $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$. Then $\alpha I$ is an ideal of the Noetherian ring $\mathfrak{O}_K$. Hence, $\alpha I$ is finitely generated as an $\mathfrak{O}_K$-module. We have an isomorphism of $\mathfrak{O}_K$-modules:

$$I \to \alpha I$$
$$x \mapsto \alpha x.$$

# Fractional ideals

**Proposition.** Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of $K$.

**Proof.** ($\Rightarrow$) First, suppose that $I$ is a fractional ideal of $\mathfrak{O}_K$, and take $\alpha \in \mathfrak{O}_K \setminus \{0\}$ such that $\alpha I \subseteq \mathfrak{O}_K$. Then $\alpha I$ is an ideal of the Noetherian ring $\mathfrak{O}_K$. Hence, $\alpha I$ is finitely generated as an $\mathfrak{O}_K$-module. We have an isomorphism of $\mathfrak{O}_K$-modules:

$$
\begin{aligned}
I &\to \alpha I \\
x &\mapsto \alpha x.
\end{aligned}
$$

Hence, $I$ is a finitely generated as an $\mathfrak{O}_K$-module (just multiply the generators of $\alpha I$ by $\alpha^{-1}$ to get generators for $I$).

# Fractional ideals

**Proposition.** Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of $K$.

# Fractional ideals

**Proposition.** Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of $K$.

**Proof.** $(\Leftarrow)$ Conversely, suppose that $I = \mathrm{Span}_{\mathfrak{O}_K}\{x_1, \ldots, x_m\}$ is a finitely-generated $\mathfrak{O}_K$-submodule of $K$.

# Fractional ideals

**Proposition.** Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of $K$.

**Proof.** $(\Leftarrow)$ Conversely, suppose that $I = \mathrm{Span}_{\mathfrak{O}_K}\{x_1, \ldots, x_m\}$ is a finitely-generated $\mathfrak{O}_K$-submodule of $K$. Since $K$ is the quotient field of $\mathfrak{O}_K$, we can write $x_i = \alpha_i/\beta_i$ with $\beta_i \neq 0$ for all $i$.

# Fractional ideals

**Proposition.** Fractional ideals of $\mathfrak{O}_K$ are exactly finitely generated $\mathfrak{O}_K$-submodules of $K$.

**Proof.** $(\Leftarrow)$ Conversely, suppose that $I = \mathrm{Span}_{\mathfrak{O}_K}\{x_1, \ldots, x_m\}$ is a finitely-generated $\mathfrak{O}_K$-submodule of $K$. Since $K$ is the quotient field of $\mathfrak{O}_K$, we can write $x_i = \alpha_i/\beta_i$ with $\beta_i \neq 0$ for all $i$. Define $\alpha = \prod_{i=1}^{m} \beta_i$. Then $\alpha I \subseteq \mathfrak{O}_K$. So $I$ is finitely generated. $\square$

# Fractional ideals

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

# Fractional ideals

**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

**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

**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. $\square$

# Fractional ideals

**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. $\square$

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

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

**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*

**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*

**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*

**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*

**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.

We will prove Steps 3 and 4 on the board, assuming Steps 1 and 2.