Math 361

March 8, 2023

Today

- Field of fractions.

Today

- Field of fractions.
- Dedekind domains.

Today

- Field of fractions.
- Dedekind domains.
- Main theorem: the ring of integers in a number field is a Dedekind domain.

Today

- Field of fractions.
- Dedekind domains.
- Main theorem: the ring of integers in a number field is a Dedekind domain.
- Preliminaries for proof.

Today

- Field of fractions.
- Dedekind domains.
- Main theorem: the ring of integers in a number field is a Dedekind domain.
- Preliminaries for proof.
- Proof.

Field of fractions

Let R be a domain.

Field of fractions

Let R be a domain. **Goal:** create fractions a/b with $a, b \in R$, $b \neq 0$.

Field of fractions

Let R be a domain. **Goal:** create fractions a/b with $a, b \in R$, $b \neq 0$.

Equivalence relation: for $a, c \in R$ and $b, d \in R \setminus \{0\}$,

$$(a, b) \sim (c, d) \quad \text{if } ad = bc.$$

Field of fractions

Let R be a domain. **Goal:** create fractions a/b with $a, b \in R$, $b \neq 0$.

Equivalence relation: for $a, c \in R$ and $b, d \in R \setminus \{0\}$,

$$(a, b) \sim (c, d) \quad \text{if } ad = bc.$$

Define a/b to be the equivalence class of (a, b).

Field of fractions

Let R be a domain. **Goal:** create fractions a/b with $a, b \in R$, $b \neq 0$.

Equivalence relation: for $a, c \in R$ and $b, d \in R \setminus \{0\}$,

$$(a, b) \sim (c, d) \quad \text{if } ad = bc.$$

Define a/b to be the equivalence class of (a, b).
Define addition and multiplication of fractions as usual

Field of fractions

Let R be a domain. **Goal:** create fractions a/b with $a, b \in R$, $b \neq 0$.

Equivalence relation: for $a, c \in R$ and $b, d \in R \setminus \{0\}$,

$$(a, b) \sim (c, d) \quad \text{if } ad = bc.$$

Define a/b to be the equivalence class of (a, b).
Define addition and multiplication of fractions as usual to get a field.

The *quotient field* $Q(R)$ of R is the field of fractions $\{a/b : a \in R, b \in R \setminus \{0\}\}$.

Field of fractions

Let R be a domain. **Goal:** create fractions a/b with $a, b \in R$, $b \neq 0$.

Equivalence relation: for $a, c \in R$ and $b, d \in R \setminus \{0\}$,

$$(a, b) \sim (c, d) \quad \text{if } ad = bc.$$

Define a/b to be the equivalence class of (a, b).
Define addition and multiplication of fractions as usual to get a field.

The *quotient field* $Q(R)$ of R is the field of fractions $\{a/b : a \in R, b \in R \setminus \{0\}\}$. It is the smallest field containing R.

$$R \hookrightarrow Q(R)$$
$$r \mapsto r/1.$$

Quotient field

Proposition. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then K is the field of fractions of $\mathfrak{O}_K$.

Quotient field

Proposition. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then K is the field of fractions of $\mathfrak{O}_K$.

Proof. We have seen (in homework) that if $\alpha \in K$ then there exists a nonzero integer $c \in \mathbb{Z}$ such that $c\alpha = \beta \in \mathfrak{O}_K$.

Quotient field

Proposition. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then K is the field of fractions of $\mathfrak{O}_K$.

Proof. We have seen (in homework) that if $\alpha \in K$ then there exists a nonzero integer $c \in \mathbb{Z}$ such that $c\alpha = \beta \in \mathfrak{O}_K$.

Thus, $\alpha = \beta/c$ with $\beta, c \in \mathfrak{O}_K$.

Quotient field

Proposition. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then K is the field of fractions of $\mathfrak{O}_K$.

Proof. We have seen (in homework) that if $\alpha \in K$ then there exists a nonzero integer $c \in \mathbb{Z}$ such that $c\alpha = \beta \in \mathfrak{O}_K$.

Thus, $\alpha = \beta/c$ with $\beta, c \in \mathfrak{O}_K$. So every element of K is in the field of fractions of $\mathfrak{O}_K$.

Quotient field

Proposition. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then K is the field of fractions of $\mathfrak{O}_K$.

Proof. We have seen (in homework) that if $\alpha \in K$ then there exists a nonzero integer $c \in \mathbb{Z}$ such that $c\alpha = \beta \in \mathfrak{O}_K$.

Thus, $\alpha = \beta/c$ with $\beta, c \in \mathfrak{O}_K$. So every element of K is in the field of fractions of $\mathfrak{O}_K$.

Conversely, since K is a field and contains $\mathfrak{O}_K$, it contains the field of fractions of $\mathfrak{O}_K$. $\square$

Dedekind domains

Definition. A domain R is *integrally closed* if the only elements of its field of fractions $Q(R)$ that are integral over R are the elements of R, itself.

Dedekind domains

Definition. A domain R is *integrally closed* if the only elements of its field of fractions $Q(R)$ that are integral over R are the elements of R, itself.

Example. The ring $\mathbb{Z}$ is integrally closed:

Dedekind domains

Definition. A domain R is *integrally closed* if the only elements of its field of fractions $Q(R)$ that are integral over R are the elements of R, itself.

Example. The ring $\mathbb{Z}$ is integrally closed: $Q(\mathbb{Z}) = \mathbb{Q}$ and the elements of $\mathbb{Q}$ integral over $\mathbb{Z}$ are exactly the elements of $\mathbb{Z}$.

Dedekind domains

Definition A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Dedekind domains

Definition A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Theorem. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then $\mathfrak{O}_K$ is a Dedekind domain.

Preliminaries

Structure theorem for finitely-generated $\mathbb{Z}$-modules.

Preliminaries

Structure theorem for finitely-generated $\mathbb{Z}$-modules.

Let M be a finitely generated $\mathbb{Z}$-module. Then there exists a nonnegative integer r and a list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i such that M is isomorphic as a $\mathbb{Z}$-module to

$$\mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

Preliminaries

Structure theorem for finitely-generated $\mathbb{Z}$-modules.

Let M be a finitely generated $\mathbb{Z}$-module. Then there exists a nonnegative integer r and a list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i such that M is isomorphic as a $\mathbb{Z}$-module to

$$\mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

It is possible to take the n_i so that $n_i | n_{i+1}$ for all i, in which case, the above representation of M as a product of cyclic groups is unique.

Preliminaries

Structure theorem for finitely-generated $\mathbb{Z}$-modules.

Let M be a finitely generated $\mathbb{Z}$-module. Then there exists a nonnegative integer r and a list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i such that M is isomorphic as a $\mathbb{Z}$-module to

$$\mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

It is possible to take the n_i so that $n_i | n_{i+1}$ for all i, in which case, the above representation of M as a product of cyclic groups is unique.

Proof. We will give a constructive proof later in the course.

Preliminaries

Structure theorem for finitely-generated $\mathbb{Z}$-modules.

Let M be a finitely generated $\mathbb{Z}$-module. Then there exists a nonnegative integer r and a list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i such that M is isomorphic as a $\mathbb{Z}$-module to

$$\mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

It is possible to take the n_i so that $n_i | n_{i+1}$ for all i, in which case, the above representation of M as a product of cyclic groups is unique.

Proof. We will give a constructive proof later in the course. Probably.

Preliminaries

Structure theorem for finitely-generated $\mathbb{Z}$-modules.

Let M be a finitely generated $\mathbb{Z}$-module. Then there exists a nonnegative integer r and a list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i such that M is isomorphic as a $\mathbb{Z}$-module to

$$\mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}.$$

It is possible to take the n_i so that $n_i | n_{i+1}$ for all i, in which case, the above representation of M as a product of cyclic groups is unique.

Proof. We will give a constructive proof later in the course. Probably.

See the wiki page for the structure theorem for finitely generated modules over a PID.

Preliminaries

Proposition. Let R be a finite domain.

Preliminaries

Proposition. Let R be a finite domain. Then R is a field.

Preliminaries

Proposition. Let R be a finite domain. Then R is a field.

Proof. Homework.

Preliminaries

Proposition. Let R be a finite domain. Then R is a field.

Proof. Homework.

Idea: for $0 \neq r \in R$, consider the multiplication mapping

$$\begin{aligned} m_r \colon R &\to R \\ s &\mapsto rs. \end{aligned}$$

Preliminaries

Proposition. An ideal in a number ring contains the norm of each of its elements:

Preliminaries

Proposition. An ideal in a number ring contains the norm of each of its elements: if $\mathfrak{a}$ is an ideal in $\mathfrak{O}_K$, and $\alpha \in \mathfrak{a}$, then $\mathbb{Z} \ni N(\alpha) \in \mathfrak{a}$.

Preliminaries

Proposition. An ideal in a number ring contains the norm of each of its elements: if $\mathfrak{a}$ is an ideal in $\mathfrak{O}_K$, and $\alpha \in \mathfrak{a}$, then $\mathbb{Z} \ni N(\alpha) \in \mathfrak{a}$.

Proof. If $\alpha = 0$, no problem.

Preliminaries

Proposition. An ideal in a number ring contains the norm of each of its elements: if $\mathfrak{a}$ is an ideal in $\mathfrak{O}_K$, and $\alpha \in \mathfrak{a}$, then $\mathbb{Z} \ni N(\alpha) \in \mathfrak{a}$.

Proof. If $\alpha = 0$, no problem. Assume $\alpha \neq 0$.

Preliminaries

Proposition. An ideal in a number ring contains the norm of each of its elements: if $\mathfrak{a}$ is an ideal in $\mathfrak{O}_K$, and $\alpha \in \mathfrak{a}$, then $\mathbb{Z} \ni N(\alpha) \in \mathfrak{a}$.

Proof. If $\alpha = 0$, no problem. Assume $\alpha \neq 0$. With the usual notation:

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(n)$$

Preliminaries

Proposition. An ideal in a number ring contains the norm of each of its elements: if $\mathfrak{a}$ is an ideal in $\mathfrak{O}_K$, and $\alpha \in \mathfrak{a}$, then $\mathbb{Z} \ni N(\alpha) \in \mathfrak{a}$.

Proof. If $\alpha = 0$, no problem. Assume $\alpha \neq 0$. With the usual notation:

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(n) = \alpha \cdot \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

Preliminaries

Proposition. An ideal in a number ring contains the norm of each of its elements: if $\mathfrak{a}$ is an ideal in $\mathfrak{O}_K$, and $\alpha \in \mathfrak{a}$, then $\mathbb{Z} \ni N(\alpha) \in \mathfrak{a}$.

Proof. If $\alpha = 0$, no problem. Assume $\alpha \neq 0$. With the usual notation:

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(n) = \alpha \cdot \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

We have $\beta := \sigma_2(\alpha) \cdots \sigma_n(\alpha) = N(\alpha)/\alpha \in K$.

Preliminaries

Proposition. An ideal in a number ring contains the norm of each of its elements: if $\mathfrak{a}$ is an ideal in $\mathfrak{O}_K$, and $\alpha \in \mathfrak{a}$, then $\mathbb{Z} \ni N(\alpha) \in \mathfrak{a}$.

Proof. If $\alpha = 0$, no problem. Assume $\alpha \neq 0$. With the usual notation:

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(n) = \alpha \cdot \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

We have $\beta := \sigma_2(\alpha) \cdots \sigma_n(\alpha) = N(\alpha)/\alpha \in K$.

Each $\sigma_i(\alpha) \in \mathfrak{O}$. (Why?).

Preliminaries

Proposition. An ideal in a number ring contains the norm of each of its elements: if $\mathfrak{a}$ is an ideal in $\mathfrak{O}_K$, and $\alpha \in \mathfrak{a}$,
then $\mathbb{Z} \ni N(\alpha) \in \mathfrak{a}$.

Proof. If $\alpha = 0$, no problem. Assume $\alpha \neq 0$. With the usual notation:

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(n) = \alpha \cdot \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

We have $\beta := \sigma_2(\alpha) \cdots \sigma_n(\alpha) = N(\alpha)/\alpha \in K$.

Each $\sigma_i(\alpha) \in \mathfrak{O}$. (Why?). Hence, $\beta \in K \cap \mathfrak{O} = \mathfrak{O}_K$.

Preliminaries

Proposition. An ideal in a number ring contains the norm of each of its elements: if $\mathfrak{a}$ is an ideal in $\mathfrak{O}_K$, and $\alpha \in \mathfrak{a}$, then $\mathbb{Z} \ni N(\alpha) \in \mathfrak{a}$.

Proof. If $\alpha = 0$, no problem. Assume $\alpha \neq 0$. With the usual notation:

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(n) = \alpha \cdot \underbrace{\sigma_2(\alpha) \cdots \sigma_n(\alpha)}_{\beta}.$$

We have $\beta := \sigma_2(\alpha) \cdots \sigma_n(\alpha) = N(\alpha)/\alpha \in K$.

Each $\sigma_i(\alpha) \in \mathfrak{O}$. (Why?). Hence, $\beta \in K \cap \mathfrak{O} = \mathfrak{O}_K$.

Hence, $N(\alpha) = \alpha\beta \in \mathfrak{a}$. $\square$

Proof of main theorem.

Definition A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Theorem. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then $\mathfrak{O}_K$ is a Dedekind domain.

Proof of main theorem.

Definition A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Theorem. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then $\mathfrak{O}_K$ is a Dedekind domain.

Proof. (1) Noetherian.

Proof of main theorem.

Definition A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Theorem. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then $\mathfrak{O}_K$ is a Dedekind domain.

Proof. (1) Noetherian. We have seen that $\mathfrak{O}_K$ is a finitely generated $\mathbb{Z}$-module.

Proof of main theorem.

Definition A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Theorem. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then $\mathfrak{O}_K$ is a Dedekind domain.

Proof. (1) Noetherian. We have seen that $\mathfrak{O}_K$ is a finitely generated $\mathbb{Z}$-module.

Since $\mathbb{Z}$ is a Noetherian ring, it follows that $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.

Proof of main theorem.

Definition A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Theorem. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then $\mathfrak{O}_K$ is a Dedekind domain.

Proof. (1) Noetherian. We have seen that $\mathfrak{O}_K$ is a finitely generated $\mathbb{Z}$-module.

Since $\mathbb{Z}$ is a Noetherian ring, it follows that $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.

So every ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, it is finitely generated as a $\mathbb{Z}$-module.

Proof of main theorem.

Definition A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Theorem. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then $\mathfrak{O}_K$ is a Dedekind domain.

Proof. (1) Noetherian. We have seen that $\mathfrak{O}_K$ is a finitely generated $\mathbb{Z}$-module.

Since $\mathbb{Z}$ is a Noetherian ring, it follows that $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.

So every ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, it is finitely generated as a $\mathbb{Z}$-module.

These generators generate α as an ideal.

Proof of main theorem.

Definition A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Theorem. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then $\mathfrak{O}_K$ is a Dedekind domain.

Proof. (1) Noetherian. We have seen that $\mathfrak{O}_K$ is a finitely generated $\mathbb{Z}$-module.

Since $\mathbb{Z}$ is a Noetherian ring, it follows that $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.

So every ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, it is finitely generated as a $\mathbb{Z}$-module.

These generators generate α as an ideal.

Hence, $\mathfrak{O}_K$ is a Noetherian domain.

Proof of main theorem.

Definition A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Theorem. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then $\mathfrak{O}_K$ is a Dedekind domain.

Proof. (1) Noetherian. We have seen that $\mathfrak{O}_K$ is a finitely generated $\mathbb{Z}$-module.

Since $\mathbb{Z}$ is a Noetherian ring, it follows that $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.

So every ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, it is finitely generated as a $\mathbb{Z}$-module.

These generators generate α as an ideal.

Hence, $\mathfrak{O}_K$ is a Noetherian domain.

Alternatively: use the Hilbert basis theorem.

Proof of main theorem.

Definition A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal.

Theorem. Let K be a number field, and let $\mathfrak{O}_K$ be its ring of integers. Then $\mathfrak{O}_K$ is a Dedekind domain.

Proof. (1) Noetherian. We have seen that $\mathfrak{O}_K$ is a finitely generated $\mathbb{Z}$-module.

Since $\mathbb{Z}$ is a Noetherian ring, it follows that $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.

So every ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$, it is finitely generated as a $\mathbb{Z}$-module.

These generators generate α as an ideal.

Hence, $\mathfrak{O}_K$ is a Noetherian domain.

Alternatively: use the Hilbert basis theorem. (Overkill?).

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal.

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof:

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite.

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof:
We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

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

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$.

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi \colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi} \colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why?

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi \colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi} \colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined:

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi\colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi}\colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined: If $\beta' = \beta + rN$ with $r \in \mathfrak{O}_K$, then

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi \colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi} \colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined: If $\beta' = \beta + rN$ with $r \in \mathfrak{O}_K$, then
$\overline{\pi}(\beta') =$

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi \colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi} \colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined: If $\beta' = \beta + rN$ with $r \in \mathfrak{O}_K$, then $\overline{\pi}(\beta') = \overline{\pi}(\beta + rN) =$

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi \colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi} \colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined: If $\beta' = \beta + rN$ with $r \in \mathfrak{O}_K$, then
$\overline{\pi}(\beta') = \overline{\pi}(\beta + rN) = \overline{\beta} + \overline{r}\overline{N}$

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi\colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi}\colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined: If $\beta' = \beta + rN$ with $r \in \mathfrak{O}_K$, then $\overline{\pi}(\beta') = \overline{\pi}(\beta + rN) = \overline{\beta} + \overline{r}\overline{N} = \overline{\beta} \in \mathfrak{O}_K/\mathfrak{p}$.

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi \colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi} \colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined: If $\beta' = \beta + rN$ with $r \in \mathfrak{O}_K$, then $\overline{\pi}(\beta') = \overline{\pi}(\beta + rN) = \overline{\beta} + \overline{r}\overline{N} = \overline{\beta} \in \mathfrak{O}_K/\mathfrak{p}$.

Since $\mathfrak{O}_K/(N)$ is a finitely generated $\mathbb{Z}$-module,

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi \colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi} \colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined: If $\beta' = \beta + rN$ with $r \in \mathfrak{O}_K$, then $\overline{\pi}(\beta') = \overline{\pi}(\beta + rN) = \overline{\beta} + \overline{r}\overline{N} = \overline{\beta} \in \mathfrak{O}_K/\mathfrak{p}$.

Since $\mathfrak{O}_K/(N)$ is a finitely generated $\mathbb{Z}$-module, $\mathfrak{O}_K/(N) \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$.

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi\colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi}\colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined: If $\beta' = \beta + rN$ with $r \in \mathfrak{O}_K$, then
$\overline{\pi}(\beta') = \overline{\pi}(\beta + rN) = \overline{\beta} + \overline{r}\overline{N} = \overline{\beta} \in \mathfrak{O}_K/\mathfrak{p}$.

Since $\mathfrak{O}_K/(N)$ is a finitely generated $\mathbb{Z}$-module, $\mathfrak{O}_K/(N) \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$. But $\mathfrak{O}_K/(N)$ has no element of infinite order

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi\colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi}\colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined: If $\beta' = \beta + rN$ with $r \in \mathfrak{O}_K$, then
$\overline{\pi}(\beta') = \overline{\pi}(\beta + rN) = \overline{\beta} + \overline{r}\overline{N} = \overline{\beta} \in \mathfrak{O}_K/\mathfrak{p}$.

Since $\mathfrak{O}_K/(N)$ is a finitely generated $\mathbb{Z}$-module, $\mathfrak{O}_K/(N) \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$. But $\mathfrak{O}_K/(N)$ has no element of infinite order ($N\alpha = \alpha + \cdots + \alpha = 0 \in \mathfrak{O}_K/(N)$).

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi\colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi}\colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined: If $\beta' = \beta + rN$ with $r \in \mathfrak{O}_K$, then $\overline{\pi}(\beta') = \overline{\pi}(\beta + rN) = \overline{\beta} + \overline{r}\overline{N} = \overline{\beta} \in \mathfrak{O}_K/\mathfrak{p}$.

Since $\mathfrak{O}_K/(N)$ is a finitely generated $\mathbb{Z}$-module, $\mathfrak{O}_K/(N) \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$. But $\mathfrak{O}_K/(N)$ has no element of infinite order ($N\alpha = \alpha + \cdots + \alpha = 0 \in \mathfrak{O}_K/(N)$). So $r = 0$, and $\mathfrak{O}_K/(N)$ is finite.

Proof of main theorem.

Proof. (2) Every nonzero prime ideal is maximal. Idea of proof: We will show $\mathfrak{O}_K/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ prime $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite domain $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a field $\Rightarrow \mathfrak{p}$ maximal.

Take $0 \neq \alpha \in \mathfrak{p}$. Define $N := N(\alpha) \in \mathbb{Z}$. Surjections:

$$\begin{aligned} \pi \colon \mathfrak{O}_K &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned} \qquad \text{induces} \qquad \begin{aligned} \overline{\pi} \colon \mathfrak{O}_K/(N) &\to \mathfrak{O}_K/\mathfrak{p} \\ \beta &\mapsto \overline{\beta} \end{aligned}$$

Why? Answer: $N \in \mathfrak{p} \Rightarrow N \in \ker(\pi)$. So $\overline{\pi}$ is well-defined: If $\beta' = \beta + rN$ with $r \in \mathfrak{O}_K$, then $\overline{\pi}(\beta') = \overline{\pi}(\beta + rN) = \overline{\beta} + \overline{r}\overline{N} = \overline{\beta} \in \mathfrak{O}_K/\mathfrak{p}$.

Since $\mathfrak{O}_K/(N)$ is a finitely generated $\mathbb{Z}$-module, $\mathfrak{O}_K/(N) \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$. But $\mathfrak{O}_K/(N)$ has no element of infinite order ($N\alpha = \alpha + \cdots + \alpha = 0 \in \mathfrak{O}_K/(N)$). So $r = 0$, and $\mathfrak{O}_K/(N)$ is finite. Then $\overline{\pi}$ surjective $\Rightarrow \mathfrak{O}_K/\mathfrak{p}$ is a finite.

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$.

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$.

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$. We are done if we show α is integral over $\mathbb{Z}$. (Why?)

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$. We are done if we show α is integral over $\mathbb{Z}$. (Why?)

It suffices to produce a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$. (Why?)

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$. We are done if we show α is integral over $\mathbb{Z}$. (Why?)

It suffices to produce a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$. (Why?)

Take monic $f \in \mathfrak{O}_K[x]$ such that $f(\alpha) = 0$. Say
$f = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$. We are done if we show α is integral over $\mathbb{Z}$. (Why?)

It suffices to produce a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$. (Why?)

Take monic $f \in \mathfrak{O}_K[x]$ such that $f(\alpha) = 0$. Say $f = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Define the ring $B := \mathbb{Z}[b_0, \ldots, b_k] \subseteq \mathfrak{O}_K$.

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$. We are done if we show α is integral over $\mathbb{Z}$. (Why?)

It suffices to produce a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$. (Why?)

Take monic $f \in \mathfrak{O}_K[x]$ such that $f(\alpha) = 0$. Say $f = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Define the ring $B := \mathbb{Z}[b_0, \ldots, b_k] \subseteq \mathfrak{O}_K$. Then B is a finitely generated $\mathbb{Z}$-module. (Why?

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$. We are done if we show α is integral over $\mathbb{Z}$. (Why?)

It suffices to produce a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$. (Why?)

Take monic $f \in \mathfrak{O}_K[x]$ such that $f(\alpha) = 0$. Say
$f = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Define the ring $B := \mathbb{Z}[b_0, \ldots, b_k] \subseteq \mathfrak{O}_K$. Then B is a finitely generated $\mathbb{Z}$-module. (Why? Ans: $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.)

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$. We are done if we show α is integral over $\mathbb{Z}$. (Why?)

It suffices to produce a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$. (Why?)

Take monic $f \in \mathfrak{O}_K[x]$ such that $f(\alpha) = 0$. Say $f = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Define the ring $B := \mathbb{Z}[b_0, \ldots, b_k] \subseteq \mathfrak{O}_K$. Then B is a finitely generated $\mathbb{Z}$-module. (Why? Ans: $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.)

From f, we see that $B[\alpha] = \mathrm{Span}_B\{1, \alpha, \ldots, \alpha^{k-1}\}$.

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$. We are done if we show α is integral over $\mathbb{Z}$. (Why?)

It suffices to produce a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$. (Why?)

Take monic $f \in \mathfrak{O}_K[x]$ such that $f(\alpha) = 0$. Say $f = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Define the ring $B := \mathbb{Z}[b_0, \ldots, b_k] \subseteq \mathfrak{O}_K$. Then B is a finitely generated $\mathbb{Z}$-module. (Why? Ans: $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.)

From f, we see that $B[\alpha] = \mathrm{Span}_B\{1, \alpha, \ldots, \alpha^{k-1}\}$. So $M := B[\alpha]$ is a finitely generated B-module:

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$. We are done if we show α is integral over $\mathbb{Z}$. (Why?)

It suffices to produce a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$. (Why?)

Take monic $f \in \mathfrak{O}_K[x]$ such that $f(\alpha) = 0$. Say $f = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Define the ring $B := \mathbb{Z}[b_0, \ldots, b_k] \subseteq \mathfrak{O}_K$. Then B is a finitely generated $\mathbb{Z}$-module. (Why? Ans: $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.)

From f, we see that $B[\alpha] = \mathrm{Span}_B\{1, \alpha, \ldots, \alpha^{k-1}\}$. So $M := B[\alpha]$ is a finitely generated B-module:

$$\mathbb{Z} \underbrace{\subseteq}_{\text{f.g.}} B \underbrace{\subseteq}_{\text{f.g.}} B[\alpha].$$

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$. We are done if we show α is integral over $\mathbb{Z}$. (Why?)

It suffices to produce a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$. (Why?)

Take monic $f \in \mathfrak{O}_K[x]$ such that $f(\alpha) = 0$. Say $f = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Define the ring $B := \mathbb{Z}[b_0, \ldots, b_k] \subseteq \mathfrak{O}_K$. Then B is a finitely generated $\mathbb{Z}$-module. (Why? Ans: $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.)

From f, we see that $B[\alpha] = \mathrm{Span}_B\{1, \alpha, \ldots, \alpha^{k-1}\}$. So $M := B[\alpha]$ is a finitely generated B-module:

$$\mathbb{Z} \underbrace{\subseteq}_{\text{f.g.}} B \underbrace{\subseteq}_{\text{f.g.}} B[\alpha].$$

Therefore, $B[\alpha]$ is a f.g. $\mathbb{Z}$-module.

Proof of main theorem.

$\mathfrak{O}_K$ is integrally closed.

Take $\alpha \in K$ with α integral over $\mathfrak{O}_K$. We must show that $\alpha \in \mathfrak{O}_K$. We are done if we show α is integral over $\mathbb{Z}$. (Why?)

It suffices to produce a finitely generated $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$. (Why?)

Take monic $f \in \mathfrak{O}_K[x]$ such that $f(\alpha) = 0$. Say $f = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$.

Define the ring $B := \mathbb{Z}[b_0, \ldots, b_k] \subseteq \mathfrak{O}_K$. Then B is a finitely generated $\mathbb{Z}$-module. (Why? Ans: $\mathfrak{O}_K$ is a Noetherian $\mathbb{Z}$-module.)

From f, we see that $B[\alpha] = \mathrm{Span}_B\{1, \alpha, \ldots, \alpha^{k-1}\}$. So $M := B[\alpha]$ is a finitely generated B-module:

$$\mathbb{Z} \underbrace{\subseteq}_{\text{f.g.}} B \underbrace{\subseteq}_{\text{f.g.}} B[\alpha].$$

Therefore, $B[\alpha]$ is a f.g. $\mathbb{Z}$-module. Finally, $\alpha B[\alpha] \subseteq B[\alpha]$. $\square$