Today we will discuss the most basic definitions and elementary results regarding number fields.

Note that our definitions are subtly different from those in the textbook.

Recall that a number field \( K \) is any finite algebraic extension of the field of rational numbers \( \mathbb{Q} \).

An algebraic integer in such a number field \( K \) is any \( \alpha \in K \) that is a root of a monic polynomial \( P(X) \in \mathbb{Z}[X] \).

Let's look at some examples. The rational numbers \( \mathbb{Q} \) is clearly a number field.

Given any \( z \in \mathbb{Z} \) we have a corresponding monic (irreducible) polynomial \( P(X) = X - z \in \mathbb{Z}[X] \) for which \( z \) is a root, thus all integers are algebraic integers.

The field \( \mathbb{Q}(i) \) is a number field of degree 2 and all Gaussian integers \( \alpha \in \mathbb{Z}[i] \) are algebraic integers. To see why, let \( \alpha = a + bi \in \mathbb{Z}[i] \).

Then \( P(X) = (X - \alpha)(X - \bar{\alpha}) = X^2 - 2aX + a^2 + b^2 \in \mathbb{Z}[X] \) is a monic polynomial of the desired form.
Algebraic Integers

Today we will discuss the most basic definitions and elementary results regarding number fields.

Note that our definitions are subtly different from those in the textbook. Recall that a number field is any finite algebraic extension of the field of rational numbers $\mathbb{Q}$.

An algebraic integer in such a number field $K$ is any $\alpha \in K$ that is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$.

Let's look at some examples. The rational numbers $\mathbb{Q}$ is clearly a number field. Given any $z \in \mathbb{Z}$ we have a corresponding monic (irreducible) polynomial $P(X) = X - z \in \mathbb{Z}[X]$ for which $z$ is a root, thus all integers are algebraic integers.

The field $\mathbb{Q}(i)$ is a number field of degree 2 and all Gaussian integers $\alpha \in \mathbb{Z}[i]$ are algebraic integers. To see why, let $\alpha = a + ib \in \mathbb{Z}[i]$. Then $P(X) = (X - \alpha)(X - \overline{\alpha}) = X^2 - 2aX + a^2 + b^2 \in \mathbb{Z}[X]$ is a monic polynomial of the desired form.
Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook.

Recall that a number field $K$ is any finite algebraic extension of the field of rational numbers $\mathbb{Q}$. An algebraic integer in such a number field $K$ is any $\alpha \in K$ that is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$. Let's look at some examples.

The rational numbers $\mathbb{Q}$ is clearly a number field. Given any $z \in \mathbb{Z}$ we have a corresponding monic (irreducible) polynomial $P(X) = X - z \in \mathbb{Z}[X]$ for which $z$ is a root, thus all integers are algebraic integers.

The field $\mathbb{Q}(i)$ is a number field of degree 2 and all Gaussian integers $\alpha \in \mathbb{Z}[i]$ are algebraic integers. To see why, let $\alpha = a + bi \in \mathbb{Z}[i]$. Then $P(X) = (X - \alpha)(X - \overline{\alpha}) = X^2 - 2aX + a^2 + b^2 \in \mathbb{Z}[X]$ is a monic polynomial of the desired form.
Algebraic Integers

Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook.

Recall that a *number field* is any finite algebraic extension of the field of rational numbers \( \mathbb{Q} \).

Let's look at some examples.

The rational numbers \( \mathbb{Q} \) is clearly a number field.

Given any \( z \in \mathbb{Z} \) we have a corresponding monic (irreducible) polynomial \( P(X) = X - z \in \mathbb{Z}[X] \) for which \( z \) is a root, thus all integers are algebraic integers.

The field \( \mathbb{Q}(i) \) is a number field of degree 2 and all Gaussian integers \( \alpha \in \mathbb{Z}[i] \) are algebraic integers.

To see why, let \( \alpha = a + bi \in \mathbb{Z}[i] \).

Then \( P(X) = (X - \alpha)(X - \alpha^*) = X^2 - 2ax + a^2 + b^2 \in \mathbb{Z}[X] \) is a monic polynomial of the desired form.
Algebraic Integers

Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook. Recall that a number field is any finite algebraic extension of the field of rational numbers $\mathbb{Q}$. An algebraic integer in such a number field $K$ is any $\alpha \in K$ that is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$. 

Let’s look at some examples. The rational numbers $\mathbb{Q}$ is clearly a number field. Given any $z \in \mathbb{Z}$ we have a corresponding monic (irreducible) polynomial $P(X) = X - z \in \mathbb{Z}[X]$ for which $z$ is a root, thus all integers are algebraic integers.

The field $\mathbb{Q}(i)$ is a number field of degree 2 and all Gaussian integers $\alpha \in \mathbb{Z}[i]$ are algebraic integers. To see why, let $\alpha = a + bi \in \mathbb{Z}[i]$. Then $P(X) = (X - \alpha)(X - \bar{\alpha}) = X^2 - 2aX + a^2 + b^2 \in \mathbb{Z}[X]$ is a monic polynomial of the desired form.
Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook.

Recall that a \textit{number field} is any finite algebraic extension of the field of rational numbers $\mathbb{Q}$. An \textit{algebraic integer} in such a number field $K$ is any $\alpha \in K$ that is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$.

Let’s look at some examples.
Algebraic Integers

Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook.
Recall that a *number field* is any finite algebraic extension of the field of rational numbers \( \mathbb{Q} \). An *algebraic integer* in such a number field \( K \) is any \( \alpha \in K \) that is a root of a monic polynomial \( P(X) \in \mathbb{Z}[X] \).

Let’s look at some examples.
The rational numbers \( \mathbb{Q} \) is clearly a number field.
Algebraic Integers

Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook.

Recall that a *number field* is any finite algebraic extension of the field of rational numbers \( \mathbb{Q} \). An *algebraic integer* in such a number field \( K \) is any \( \alpha \in K \) that is a root of a monic polynomial \( P(X) \in \mathbb{Z}[X] \).

Let’s look at some examples.

The rational numbers \( \mathbb{Q} \) is clearly a number field. Given any \( z \in \mathbb{Z} \) we have a corresponding monic (irreducible) polynomial
Algebraic Integers

Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook.

Recall that a *number field* is any finite algebraic extension of the field of rational numbers \( \mathbb{Q} \). An *algebraic integer* in such a number field \( K \) is any \( \alpha \in K \) that is a root of a monic polynomial \( P(X) \in \mathbb{Z}[X] \).

Let’s look at some examples.

The rational numbers \( \mathbb{Q} \) is clearly a number field. Given any \( z \in \mathbb{Z} \) we have a corresponding monic (irreducible) polynomial \( P(X) = X - z \in \mathbb{Z}[X] \).
Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook. Recall that a *number field* is any finite algebraic extension of the field of rational numbers $\mathbb{Q}$. An *algebraic integer* in such a number field $K$ is any $\alpha \in K$ that is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$. 

Let’s look at some examples.

The rational numbers $\mathbb{Q}$ is clearly a number field. Given any $z \in \mathbb{Z}$ we have a corresponding monic (irreducible) polynomial $P(X) = X - z \in \mathbb{Z}[X]$ for which $z$ is a root,
Algebraic Integers

Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook.

Recall that a number field is any finite algebraic extension of the field of rational numbers $\mathbb{Q}$. An algebraic integer in such a number field $K$ is any $\alpha \in K$ that is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$.

Let’s look at some examples.

The rational numbers $\mathbb{Q}$ is clearly a number field. Given any $z \in \mathbb{Z}$ we have a corresponding monic (irreducible) polynomial $P(X) = X - z \in \mathbb{Z}[X]$ for which $z$ is a root, thus all integers are algebraic integers.
Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook.

Recall that a number field is any finite algebraic extension of the field of rational numbers $\mathbb{Q}$. An algebraic integer in such a number field $K$ is any $\alpha \in K$ that is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$.

Let’s look at some examples.

The rational numbers $\mathbb{Q}$ is clearly a number field. Given any $z \in \mathbb{Z}$ we have a corresponding monic (irreducible) polynomial $P(X) = X - z \in \mathbb{Z}[X]$ for which $z$ is a root, thus all integers are algebraic integers.

The field $\mathbb{Q}(i)$ is a number field of degree 2
Algebraic Integers

Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook.

Recall that a *number field* is any finite algebraic extension of the field of rational numbers \( \mathbb{Q} \). An *algebraic integer* in such a number field \( K \) is any \( \alpha \in K \) that is a root of a monic polynomial \( P(X) \in \mathbb{Z}[X] \).

Let’s look at some examples.

The rational numbers \( \mathbb{Q} \) is clearly a number field. Given any \( z \in \mathbb{Z} \) we have a corresponding monic (irreducible) polynomial \( P(X) = X - z \in \mathbb{Z}[X] \) for which \( z \) is a root, thus all integers are algebraic integers.

The field \( \mathbb{Q}(i) \) is a number field of degree 2 and all Gaussian integers \( \alpha \in \mathbb{Z}[i] \) are algebraic integers.
Algebraic Integers

Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook. Recall that a number field is any finite algebraic extension of the field of rational numbers \( \mathbb{Q} \). An algebraic integer in such a number field \( K \) is any \( \alpha \in K \) that is a root of a monic polynomial \( P(X) \in \mathbb{Z}[X] \).

Let’s look at some examples.

The rational numbers \( \mathbb{Q} \) is clearly a number field. Given any \( z \in \mathbb{Z} \) we have a corresponding monic (irreducible) polynomial \( P(X) = X - z \in \mathbb{Z}[X] \) for which \( z \) is a root, thus all integers are algebraic integers.

The field \( \mathbb{Q}(i) \) is a number field of degree 2 and all Gaussian integers \( \alpha \in \mathbb{Z}[i] \) are algebraic integers. To see why, let \( \alpha = a + ib \in \mathbb{Z}[i] \).
Algebraic Integers

Today we will discuss the most basic definitions and elementary results regarding number fields. Note that our definitions are subtly different from those in the textbook.

Recall that a number field is any finite algebraic extension of the field of rational numbers $\mathbb{Q}$. An algebraic integer in such a number field $K$ is any $\alpha \in K$ that is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$.

Let’s look at some examples.

The rational numbers $\mathbb{Q}$ is clearly a number field. Given any $z \in \mathbb{Z}$ we have a corresponding monic (irreducible) polynomial $P(X) = X - z \in \mathbb{Z}[X]$ for which $z$ is a root, thus all integers are algebraic integers.

The field $\mathbb{Q}(i)$ is a number field of degree 2 and all Gaussian integers $\alpha \in \mathbb{Z}[i]$ are algebraic integers. To see why, let $\alpha = a + ib \in \mathbb{Z}[i]$. Then

$$P(X) = (X - \alpha)(X - \overline{\alpha}) = X^2 - 2aX + a^2 + b^2 \in \mathbb{Z}[X]$$

is a monic polynomial of the desired form.
Note that if \( \overline{\mathbb{Q}} \) is an algebraic closure of \( \mathbb{Q} \) containing an algebraic integer \( \alpha \) and \( \sigma \) is any element of the Galois group, then \( \sigma(\alpha) \) is also an algebraic integer.
Note that if $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ containing an algebraic integer $\alpha$ and $\sigma$ is any element of the Galois group,
Note that if \( \overline{\mathbb{Q}} \) is an algebraic closure of \( \mathbb{Q} \) containing an algebraic integer \( \alpha \) and \( \sigma \) is any element of the Galois group, then \( \sigma(\alpha) \) is also an algebraic integer.
Note that if $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ containing an algebraic integer $\alpha$ and $\sigma$ is any element of the Galois group, then $\sigma(\alpha)$ is also an algebraic integer.

If it makes you more comfortable,
Note that if $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ containing an algebraic integer $\alpha$ and $\sigma$ is any element of the Galois group, then $\sigma(\alpha)$ is also an algebraic integer.

If it makes you more comfortable, you may take $\overline{\mathbb{Q}} \subset \mathbb{C}$. 
Note that if $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ containing an algebraic integer $\alpha$ and $\sigma$ is any element of the Galois group, then $\sigma(\alpha)$ is also an algebraic integer.

If it makes you more comfortable, you may take $\overline{\mathbb{Q}} \subset \mathbb{C}$. Suppose $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$. 
Note that if \( \overline{\mathbb{Q}} \) is an algebraic closure of \( \mathbb{Q} \) containing an algebraic integer \( \alpha \) and \( \sigma \) is any element of the Galois group, then \( \sigma(\alpha) \) is also an algebraic integer.

If it makes you more comfortable, you may take \( \overline{\mathbb{Q}} \subset \mathbb{C} \).

Suppose \( \alpha \) is a root of a monic polynomial \( P(X) \in \mathbb{Z}[X] \). This polynomial factors
Note that if \( \overline{\mathbb{Q}} \) is an algebraic closure of \( \mathbb{Q} \) containing an algebraic integer \( \alpha \) and \( \sigma \) is any element of the Galois group, then \( \sigma(\alpha) \) is also an algebraic integer.

If it makes you more comfortable, you may take \( \overline{\mathbb{Q}} \subset \mathbb{C} \).

Suppose \( \alpha \) is a root of a monic polynomial \( P(X) \in \mathbb{Z}[X] \). This polynomial factors (over \( \mathbb{Z} \), in fact)
Note that if $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ containing an algebraic integer $\alpha$ and $\sigma$ is any element of the Galois group, then $\sigma(\alpha)$ is also an algebraic integer.

If it makes you more comfortable, you may take $\overline{\mathbb{Q}} \subset \mathbb{C}$. Suppose $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$. This polynomial factors (over $\mathbb{Z}$, in fact) into a product of powers of irreducible polynomials.
Note that if $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ containing an algebraic integer $\alpha$ and $\sigma$ is any element of the Galois group, then $\sigma(\alpha)$ is also an algebraic integer.

If it makes you more comfortable, you may take $\overline{\mathbb{Q}} \subset \mathbb{C}$.

Suppose $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$. This polynomial factors (over $\mathbb{Z}$, in fact) into a product of powers of irreducible polynomials. Necessarily $\alpha$ is a root of (just) one of these irreducible factors of $P(X)$. 
Note that if $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ containing an algebraic integer $\alpha$ and $\sigma$ is any element of the Galois group, then $\sigma(\alpha)$ is also an algebraic integer.

If it makes you more comfortable, you may take $\overline{\mathbb{Q}} \subset \mathbb{C}$.

Suppose $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$. This polynomial factors (over $\mathbb{Z}$, in fact) into a product of powers of irreducible polynomials. Necessarily $\alpha$ is a root of (just) one of these irreducible factors of $P(X)$. Any element of the Galois group must take $\alpha$ to a root of that same irreducible factor,
Note that if $\mathbb{Q}$ is an algebraic closure of $\mathbb{Q}$ containing an algebraic integer $\alpha$ and $\sigma$ is any element of the Galois group, then $\sigma(\alpha)$ is also an algebraic integer.

If it makes you more comfortable, you may take $\mathbb{Q} \subset \mathbb{C}$.

Suppose $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$. This polynomial factors (over $\mathbb{Z}$, in fact) into a product of powers of irreducible polynomials. Necessarily $\alpha$ is a root of (just) one of these irreducible factors of $P(X)$. Any element of the Galois group must take $\alpha$ to a root of that same irreducible factor, thus a root of the product $P(X)$. 
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$.

Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof:

From the "Basic Background Results" handout, $\mathbb{Z}[X]$ is a unique factorization domain where the irreducible elements are irreducible over $\mathbb{Q}$.

Let $R(X) \in \mathbb{Z}[X]$ be a monic polynomial with root $\alpha$ and factor $R(X)$ into a product of powers of irreducible polynomials (note the units of $\mathbb{Z}[X]$ are $\pm 1$):

$$R(X) = \pm P_1^{e_1}(X) \cdots P_n^{e_n}(X).$$

Clearly we may assume that each $P_i(X)$ is monic since $R(X)$ is.

Since $\alpha$ is a root of $R(X)$, it must be a root of some $P_i(X)$, which is irreducible over $\mathbb{Q}$. 
Theorem

If \( \alpha \) is an algebraic integer,

\[ P(X) \in \mathbb{Z}[X] \text{ is irreducible over } \mathbb{Q}. \]

Thus this monic polynomial is unique to \( \alpha \) and the degree of the polynomial is the degree of \( \alpha \) as an algebraic element over \( \mathbb{Q} \).

Proof:

From the “Basic Background Results” handout, \( \mathbb{Z}[X] \) is a unique factorization domain where the irreducible elements are irreducible over \( \mathbb{Q} \).

Let \( R(X) \in \mathbb{Z}[X] \) be a monic polynomial with root \( \alpha \), and factor \( R(X) \) into a product of powers of irreducible polynomials (note the units of \( \mathbb{Z}[X] \) are \( \pm 1 \)):

\[ R(X) = \pm P_{\epsilon_1}^1(X) \cdots P_{\epsilon_n}^n(X). \]

Clearly we may assume that each \( P_{\epsilon_i}(X) \) is monic since \( R(X) \) is.

Since \( \alpha \) is a root of \( R(X) \), it must be a root of some \( P_{\epsilon_i}(X) \), which is irreducible over \( \mathbb{Q} \).
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$.
Theorem

If \( \alpha \) is an algebraic integer, then \( \alpha \) is a root of a monic polynomial \( P(X) \in \mathbb{Z}[X] \) that is irreducible over \( \mathbb{Q} \). Thus this monic polynomial is unique to \( \alpha \).
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$. 

Proof:

From the "Basic Background Results" handout, $\mathbb{Z}[X]$ is a unique factorization domain where the irreducible elements are irreducible over $\mathbb{Q}$.

Let $R(X) \in \mathbb{Z}[X]$ be a monic polynomial with root $\alpha$ and factor $R(X)$ into a product of powers of irreducible polynomials (note the units of $\mathbb{Z}[X]$ are $\pm 1$):

$$ R(X) = \pm P_{e_1}^{e_1}(X) \cdots P_{e_n}^{e_n}(X). $$

Clearly we may assume that each $P_i(X)$ is monic since $R(X)$ is.

Since $\alpha$ is a root of $R(X)$, it must be a root of some $P_i(X)$, which is irreducible over $\mathbb{Q}$. 
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof:
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof: From the “Basic Background Results” handout,
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof: From the “Basic Background Results” handout, $\mathbb{Z}[X]$ is a unique factorization domain where the irreducible elements are irreducible over $\mathbb{Q}$. 
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof: From the “Basic Background Results” handout, $\mathbb{Z}[X]$ is a unique factorization domain where the irreducible elements are irreducible over $\mathbb{Q}$. Let $R(X) \in \mathbb{Z}[X]$ be a monic polynomial with root $\alpha$
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof: From the “Basic Background Results” handout, $\mathbb{Z}[X]$ is a unique factorization domain where the irreducible elements are irreducible over $\mathbb{Q}$. Let $R(X) \in \mathbb{Z}[X]$ be a monic polynomial with root $\alpha$ and factor $R$ into a product of powers of irreducible polynomials.
Theorem

If \( \alpha \) is an algebraic integer, then \( \alpha \) is a root of a monic polynomial \( P(X) \in \mathbb{Z}[X] \) that is irreducible over \( \mathbb{Q} \). Thus this monic polynomial is unique to \( \alpha \) and the degree of the polynomial is the degree of \( \alpha \) as an algebraic element over \( \mathbb{Q} \).

Proof: From the “Basic Background Results” handout, \( \mathbb{Z}[X] \) is a unique factorization domain where the irreducible elements are irreducible over \( \mathbb{Q} \). Let \( R(X) \in \mathbb{Z}[X] \) be a monic polynomial with root \( \alpha \) and factor \( R \) into a product of powers of irreducible polynomials (note the units of \( \mathbb{Z}[X] \) are \( \pm 1 \)): 
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof: From the “Basic Background Results” handout, $\mathbb{Z}[X]$ is a unique factorization domain where the irreducible elements are irreducible over $\mathbb{Q}$. Let $R(X) \in \mathbb{Z}[X]$ be a monic polynomial with root $\alpha$ and factor $R$ into a product of powers of irreducible polynomials (note the units of $\mathbb{Z}[X]$ are $\pm 1$):

$$R(X) = \pm P_1^{e_1}(X) \cdots P_n^{e_n}(X).$$
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof: From the “Basic Background Results” handout, $\mathbb{Z}[X]$ is a unique factorization domain where the irreducible elements are irreducible over $\mathbb{Q}$. Let $R(X) \in \mathbb{Z}[X]$ be a monic polynomial with root $\alpha$ and factor $R$ into a product of powers of irreducible polynomials (note the units of $\mathbb{Z}[X]$ are $\pm 1$):

$$R(X) = \pm P_1^{e_1}(X) \cdots P_n^{e_n}(X).$$

Clearly we may assume that each $P_i(X)$ is monic since $R$ is.
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof: From the “Basic Background Results” handout, $\mathbb{Z}[X]$ is a unique factorization domain where the irreducible elements are irreducible over $\mathbb{Q}$. Let $R(X) \in \mathbb{Z}[X]$ be a monic polynomial with root $\alpha$ and factor $R$ into a product of powers of irreducible polynomials (note the units of $\mathbb{Z}[X]$ are $\pm 1$):

$$R(X) = \pm P_1^{e_1}(X) \cdots P_n^{e_n}(X).$$

Clearly we may assume that each $P_i(X)$ is monic since $R$ is. Since $\alpha$ is a root of $R$, 

Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof: From the “Basic Background Results” handout, $\mathbb{Z}[X]$ is a unique factorization domain where the irreducible elements are irreducible over $\mathbb{Q}$. Let $R(X) \in \mathbb{Z}[X]$ be a monic polynomial with root $\alpha$ and factor $R$ into a product of powers of irreducible polynomials (note the units of $\mathbb{Z}[X]$ are $\pm 1$):

$$R(X) = \pm P_1^{e_1}(X) \cdots P_n^{e_n}(X).$$

Clearly we may assume that each $P_i(X)$ is monic since $R$ is. Since $\alpha$ is a root of $R$, it must be a root of some $P_i(X)$,
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof: From the “Basic Background Results” handout, $\mathbb{Z}[X]$ is a unique factorization domain where the irreducible elements are irreducible over $\mathbb{Q}$. Let $R(X) \in \mathbb{Z}[X]$ be a monic polynomial with root $\alpha$ and factor $R$ into a product of powers of irreducible polynomials (note the units of $\mathbb{Z}[X]$ are $\pm 1$):

$$R(X) = \pm P_{1}^{e_1}(X) \cdots P_{n}^{e_n}(X).$$

Clearly we may assume that each $P_{i}(X)$ is monic since $R$ is. Since $\alpha$ is a root of $R$, it must be a root of some $P_{i}(X)$, which is irreducible over $\mathbb{Q}$. 
Theorem

If $\alpha$ is an algebraic integer, then $\alpha$ is a root of a monic polynomial $P(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$. Thus this monic polynomial is unique to $\alpha$ and the degree of the polynomial is the degree of $\alpha$ as an algebraic element over $\mathbb{Q}$.

Proof: From the “Basic Background Results” handout, $\mathbb{Z}[X]$ is a unique factorization domain where the irreducible elements are irreducible over $\mathbb{Q}$. Let $R(X) \in \mathbb{Z}[X]$ be a monic polynomial with root $\alpha$ and factor $R$ into a product of powers of irreducible polynomials (note the units of $\mathbb{Z}[X]$ are $\pm 1$):

$$R(X) = \pm P_1^{e_1}(X) \cdots P_n^{e_n}(X).$$

Clearly we may assume that each $P_i(X)$ is monic since $R$ is. Since $\alpha$ is a root of $R$, it must be a root of some $P_i(X)$, which is irreducible over $\mathbb{Q}$. 

As an example, consider \( \alpha = e^{2\pi i/3} \) which is a cube root of unity, thus a root of \( X^3 - 1 \). Of course 1 is also a root of that polynomial, thus \( X - 1 \) | \( X^3 - 1 \): 
\[
X^3 - 1 = (X - 1)(X^2 + X + 1).
\]
If you lack faith, you may check that \( \alpha \) is a root of the latter degree 2 polynomial. Is \( X^2 + X + 1 \) irreducible? Why?

This is actually just one example of a more general phenomenon. Take any \( p \)-th root of unity \( \omega \) where \( p \) is a prime. Then \( \omega \) is a root of \( X^p - 1 \). As above, 1 is also a root of this polynomial, and we thus get 
\[
X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \cdots + 1).
\]
Is the latter factor here always irreducible? Is \( \omega \) a root of that latter factor?
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity,
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. 

Of course 1 is also a root of that polynomial, thus $X - 1 \mid X^3 - 1$: 

$$X^3 - 1 = (X - 1)(X^2 + X + 1).$$

If you lack faith, you may check that $\alpha$ is a root of the latter degree 2 polynomial.

Is $X^2 + X + 1$ irreducible? Why?

This is actually just one example of a more general phenomenon. Take any $p$-th root of unity $\omega$ where $p$ is a prime. Then $\omega$ is a root of $X^p - 1$. As above, 1 is also a root of this polynomial, and we thus get 

$$X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \cdots + 1).$$

Is the latter factor here always irreducible? Is $\omega$ a root of that latter factor?
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial,
As an example, consider \( \alpha = e^{2i\pi/3} \) which is a cube root of unity, thus a root of \( X^3 - 1 \). Of course 1 is also a root of that polynomial, thus \( X - 1 | X^3 - 1 \):
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial, thus $X - 1|X^3 - 1$: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. 
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial, thus $X - 1 \mid X^3 - 1$: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. If you lack faith,
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial, thus $X - 1 | X^3 - 1$: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. If you lack faith, you may check that $\alpha$ is a root of the latter degree 2 polynomial.
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial, thus $X - 1 | X^3 - 1$: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. If you lack faith, you may check that $\alpha$ is a root of the latter degree 2 polynomial. Is $X^2 + X + 1$ irreducible?
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial, thus $X - 1 | X^3 - 1$: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. If you lack faith, you may check that $\alpha$ is a root of the latter degree 2 polynomial. Is $X^2 + X + 1$ irreducible? Why?
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial, thus $X - 1 | X^3 - 1$: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. If you lack faith, you may check that $\alpha$ is a root of the latter degree 2 polynomial. Is $X^2 + X + 1$ irreducible? Why?

This is actually just one example of a more general phenomenon.
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial, thus $X - 1\mid X^3 - 1$: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. If you lack faith, you may check that $\alpha$ is a root of the latter degree 2 polynomial. Is $X^2 + X + 1$ irreducible? Why?

This is actually just one example of a more general phenomenon.

Take any $p$-th root of unity $\omega$
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial, thus $X - 1 | X^3 - 1$: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. If you lack faith, you may check that $\alpha$ is a root of the latter degree 2 polynomial. Is $X^2 + X + 1$ irreducible? Why?

This is actually just one example of a more general phenomenon.

Take any $p$-th root of unity $\omega$ where $p$ is a prime.
As an example, consider \( \alpha = e^{2i\pi/3} \) which is a cube root of unity, thus a root of \( X^3 - 1 \). Of course 1 is also a root of that polynomial, thus \( X - 1 | X^3 - 1 \): \( X^3 - 1 = (X - 1)(X^2 + X + 1) \). If you lack faith, you may check that \( \alpha \) is a root of the latter degree 2 polynomial. Is \( X^2 + X + 1 \) irreducible? Why?

This is actually just one example of a more general phenomenon. Take any \( p \)-th root of unity \( \omega \) where \( p \) is a prime. Then \( \omega \) is a root of \( X^p - 1 \).
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial, thus $X - 1 | X^3 - 1$: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. If you lack faith, you may check that $\alpha$ is a root of the latter degree 2 polynomial. Is $X^2 + X + 1$ irreducible? Why?

This is actually just one example of a more general phenomenon.

Take any $p$-th root of unity $\omega$ where $p$ is a prime. Then $\omega$ is a root of $X^p - 1$. As above, 1 is also a root of this polynomial,
As an example, consider \( \alpha = e^{2i\pi/3} \) which is a cube root of unity, thus a root of \( X^3 - 1 \). Of course 1 is also a root of that polynomial, thus \( X - 1 | X^3 - 1 \): \( X^3 - 1 = (X - 1)(X^2 + X + 1) \). If you lack faith, you may check that \( \alpha \) is a root of the latter degree 2 polynomial. Is \( X^2 + X + 1 \) irreducible? Why?

This is actually just one example of a more general phenomenon.

Take any \( p \)-th root of unity \( \omega \) where \( p \) is a prime. Then \( \omega \) is a root of \( X^p - 1 \). As above, 1 is also a root of this polynomial, and we thus get

\[
X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \cdots + 1).
\]
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial, thus $X - 1 | X^3 - 1$: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. If you lack faith, you may check that $\alpha$ is a root of the latter degree 2 polynomial. Is $X^2 + X + 1$ irreducible? Why?

This is actually just one example of a more general phenomenon.

Take any $p$-th root of unity $\omega$ where $p$ is a prime. Then $\omega$ is a root of $X^p - 1$. As above, 1 is also a root of this polynomial, and we thus get

$$X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \cdots + 1).$$

Is the latter factor here always irreducible?
As an example, consider $\alpha = e^{2i\pi/3}$ which is a cube root of unity, thus a root of $X^3 - 1$. Of course 1 is also a root of that polynomial, thus $X - 1 | X^3 - 1$: $X^3 - 1 = (X - 1)(X^2 + X + 1)$. If you lack faith, you may check that $\alpha$ is a root of the latter degree 2 polynomial. Is $X^2 + X + 1$ irreducible? Why?

This is actually just one example of a more general phenomenon.

Take any $p$-th root of unity $\omega$ where $p$ is a prime. Then $\omega$ is a root of $X^p - 1$. As above, 1 is also a root of this polynomial, and we thus get

$$X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \cdots + 1).$$

Is the latter factor here always irreducible? Is $\omega$ a root of that latter factor?
Corollary

The rational integers \( \mathbb{Z} \) is the set (ring) of all algebraic integers of degree 1, thus the set (ring) of all algebraic integers in \( \mathbb{Q} \), and the Gaussian integers \( \mathbb{Z}[i] \) is the set (ring) of all algebraic integers in \( \mathbb{Q}(i) \).

Proof:
The first statement is obvious since by Theorem 1 an algebraic integer in \( \mathbb{Q} \) must be the root of a monic polynomial of degree 1 in \( \mathbb{Z}[X] \).

For the second, any non-zero algebraic integer in \( \mathbb{Q}(i) \) is algebraic of degree 1 or 2 over \( \mathbb{Q} \). In the former case we must have a rational integer (i.e., an element of \( \mathbb{Z} \)). In the latter case we have an algebraic element \( \alpha = a + bi \in \mathbb{Q}(i) \) with minimal polynomial \( P(X) = (X - \alpha)(X - \alpha^* ) = X^2 - 2aX + a^2 + b^2 \), so by Theorem 1 \( \alpha \) is an algebraic integer if and only if \( 2a, a^2 + b^2 \in \mathbb{Z} \).
Corollary

The rational integers \( \mathbb{Z} \) is the set (ring) of all algebraic integers of degree 1,
Corollary

The rational integers \( \mathbb{Z} \) is the set (ring) of all algebraic integers of degree 1, thus the set (ring) of all algebraic integers in \( \mathbb{Q} \),
Corollary

The rational integers \( \mathbb{Z} \) is the set (ring) of all algebraic integers of degree 1, thus the set (ring) of all algebraic integers in \( \mathbb{Q} \), and the Gaussian integers \( \mathbb{Z}[i] \) is the set (ring) of all algebraic integers in \( \mathbb{Q}(i) \).
Corollary

The rational integers \( \mathbb{Z} \) is the set (ring) of all algebraic integers of degree 1, thus the set (ring) of all algebraic integers in \( \mathbb{Q} \), and the Gaussian integers \( \mathbb{Z}[i] \) is the set (ring) of all algebraic integers in \( \mathbb{Q}(i) \).

Proof:
Corollary

The rational integers \( \mathbb{Z} \) is the set (ring) of all algebraic integers of degree 1, thus the set (ring) of all algebraic integers in \( \mathbb{Q} \), and the Gaussian integers \( \mathbb{Z}[i] \) is the set (ring) of all algebraic integers in \( \mathbb{Q}(i) \).

Proof: The first statement is obvious since by Theorem 1 an algebraic integer in \( \mathbb{Q} \) must be the root of a monic polynomial of degree 1 in \( \mathbb{Z}[X] \).
Corollary

The rational integers \( \mathbb{Z} \) is the set (ring) of all algebraic integers of degree 1, thus the set (ring) of all algebraic integers in \( \mathbb{Q} \), and the Gaussian integers \( \mathbb{Z}[i] \) is the set (ring) of all algebraic integers in \( \mathbb{Q}(i) \).

Proof: The first statement is obvious since by Theorem 1 an algebraic integer in \( \mathbb{Q} \) must be the root of a monic polynomial of degree 1 in \( \mathbb{Z}[X] \). For the second,
Corollary

The rational integers $\mathbb{Z}$ is the set (ring) of all algebraic integers of degree 1, thus the set (ring) of all algebraic integers in $\mathbb{Q}$, and the Gaussian integers $\mathbb{Z}[i]$ is the set (ring) of all algebraic integers in $\mathbb{Q}(i)$.

Proof: The first statement is obvious since by Theorem 1 an algebraic integer in $\mathbb{Q}$ must be the root of a monic polynomial of degree 1 in $\mathbb{Z}[X]$. For the second, any non-zero algebraic integer in $\mathbb{Q}(i)$ is algebraic of degree 1 or 2 over $\mathbb{Q}$. 
Corollary

The rational integers $\mathbb{Z}$ is the set (ring) of all algebraic integers of degree 1, thus the set (ring) of all algebraic integers in $\mathbb{Q}$, and the Gaussian integers $\mathbb{Z}[i]$ is the set (ring) of all algebraic integers in $\mathbb{Q}(i)$.

Proof: The first statement is obvious since by Theorem 1 an algebraic integer in $\mathbb{Q}$ must be the root of a monic polynomial of degree 1 in $\mathbb{Z}[X]$. For the second, any non-zero algebraic integer in $\mathbb{Q}(i)$ is algebraic of degree 1 or 2 over $\mathbb{Q}$. In the former case we must have a rational integer (i.e., an element of $\mathbb{Z}$).
Corollary

The rational integers $\mathbb{Z}$ is the set (ring) of all algebraic integers of degree 1, thus the set (ring) of all algebraic integers in $\mathbb{Q}$, and the Gaussian integers $\mathbb{Z}[i]$ is the set (ring) of all algebraic integers in $\mathbb{Q}(i)$.

Proof: The first statement is obvious since by Theorem 1 an algebraic integer in $\mathbb{Q}$ must be the root of a monic polynomial of degree 1 in $\mathbb{Z}[X]$. For the second, any non-zero algebraic integer in $\mathbb{Q}(i)$ is algebraic of degree 1 or 2 over $\mathbb{Q}$. In the former case we must have a rational integer (i.e., an element of $\mathbb{Z}$). In the latter case we have an algebraic element $\alpha = a + ib \in \mathbb{Q}(i)$ with minimal polynomial
Corollary

The rational integers $\mathbb{Z}$ is the set (ring) of all algebraic integers of degree 1, thus the set (ring) of all algebraic integers in $\mathbb{Q}$, and the Gaussian integers $\mathbb{Z}[i]$ is the set (ring) of all algebraic integers in $\mathbb{Q}(i)$.

Proof: The first statement is obvious since by Theorem 1 an algebraic integer in $\mathbb{Q}$ must be the root of a monic polynomial of degree 1 in $\mathbb{Z}[X]$. For the second, any non-zero algebraic integer in $\mathbb{Q}(i)$ is algebraic of degree 1 or 2 over $\mathbb{Q}$. In the former case we must have a rational integer (i.e., an element of $\mathbb{Z}$). In the latter case we have an algebraic element $\alpha = a + ib \in \mathbb{Q}(i)$ with minimal polynomial

$$P(X) = (X - \alpha)(X - \overline{\alpha}) = X^2 - 2aX + a^2 + b^2,$$
**Corollary**

The rational integers \( \mathbb{Z} \) is the set (ring) of all algebraic integers of degree 1, thus the set (ring) of all algebraic integers in \( \mathbb{Q} \), and the Gaussian integers \( \mathbb{Z}[i] \) is the set (ring) of all algebraic integers in \( \mathbb{Q}(i) \).

**Proof:** The first statement is obvious since by Theorem 1 an algebraic integer in \( \mathbb{Q} \) must be the root of a monic polynomial of degree 1 in \( \mathbb{Z}[X] \). For the second, any non-zero algebraic integer in \( \mathbb{Q}(i) \) is algebraic of degree 1 or 2 over \( \mathbb{Q} \). In the former case we must have a rational integer (i.e., an element of \( \mathbb{Z} \)). In the latter case we have an algebraic element \( \alpha = a + ib \in \mathbb{Q}(i) \) with minimal polynomial

\[
P(X) = (X - \alpha)(X - \overline{\alpha}) = X^2 - 2aX + a^2 + b^2,
\]

so by Theorem 1 \( \alpha \) is an algebraic integer if and only if \( 2a, a^2 + b^2 \in \mathbb{Z} \).
We immediately see that $a = z/2$ for some $z \in \mathbb{Z}$. 
We immediately see that $a = z/2$ for some $z \in \mathbb{Z}$. If $z$ is odd, then $4a^2 \in \mathbb{Z}$,
We immediately see that $a = z/2$ for some $z \in \mathbb{Z}$. If $z$ is odd, then $4a^2 \in \mathbb{Z}$, $4(a^2 + b^2) \equiv 0 \mod 4$, $4b^2 \in \mathbb{Z}$, forcing $b = z'/2$ for some $z' \in \mathbb{Z}$ and thus $4b^2 \equiv 0, 1 \mod 4$ depending on whether $z'$ is even or odd. Therefore $4(a^2 + b^2) \equiv 1, 2 \mod 4$. This contradiction shows that $z$ is even so that $a \in \mathbb{Z}$. Now $b^2 \in \mathbb{Z}$, forcing $b \in \mathbb{Z}$, too.
We immediately see that $a = z/2$ for some $z \in \mathbb{Z}$. If $z$ is odd, then $4a^2 \in \mathbb{Z}$, $4(a^2 + b^2) \equiv 0 \mod 4$, and $4a^2 \equiv 1 \mod 4$. But now $4b^2 \in \mathbb{Z}$, forcing $b = z'/2$ for some $z' \in \mathbb{Z}$ and thus $4b^2 \equiv 0, 1 \mod 4$ depending on whether $z'$ is even or odd. Therefore $4(a^2 + b^2) \equiv 1, 2 \mod 4$. This contradiction shows that $z$ is even so that $a \in \mathbb{Z}$. Now $b^2 \in \mathbb{Z}$, forcing $b \in \mathbb{Z}$, too.
We immediately see that $a = z/2$ for some $z \in \mathbb{Z}$. If $z$ is odd, then $4a^2 \in \mathbb{Z}$, $4(a^2 + b^2) \equiv 0 \mod 4$, and $4a^2 \equiv 1 \mod 4$. But now $4b^2 \in \mathbb{Z}$, forcing $b = z'/2$ for some $z' \in \mathbb{Z}$ and thus $4b^2 \equiv 0, 1 \mod 4$ depending on whether $z'$ is even or odd. Therefore $4(a^2 + b^2) \equiv 1, 2 \mod 4$. This contradiction shows that $z$ is even so that $a \in \mathbb{Z}$. Now $b^2 \in \mathbb{Z}$, forcing $b \in \mathbb{Z}$, too.
We immediately see that $a = z/2$ for some $z \in \mathbb{Z}$. If $z$ is odd, then $4a^2 \in \mathbb{Z}$, $4(a^2 + b^2) \equiv 0 \mod 4$, and $4a^2 \equiv 1 \mod 4$. But now $4b^2 \in \mathbb{Z}$, forcing $b = z'/2$ for some $z' \in \mathbb{Z}$.
We immediately see that $a = z/2$ for some $z \in \mathbb{Z}$. If $z$ is odd, then $4a^2 \in \mathbb{Z}$, $4(a^2 + b^2) \equiv 0 \pmod{4}$, and $4a^2 \equiv 1 \pmod{4}$. But now $4b^2 \in \mathbb{Z}$, forcing $b = z'/2$ for some $z' \in \mathbb{Z}$ and thus $4b^2 \equiv 0, 1 \pmod{4}$.
We immediately see that $a = z/2$ for some $z \in \mathbb{Z}$. If $z$ is odd, then $4a^2 \in \mathbb{Z}$, $4(a^2 + b^2) \equiv 0 \mod 4$, and $4a^2 \equiv 1 \mod 4$. But now $4b^2 \in \mathbb{Z}$, forcing $b = z'/2$ for some $z' \in \mathbb{Z}$ and thus $4b^2 \equiv 0, 1 \mod 4$ depending on whether $z'$ is even or odd.
We immediately see that $a = z/2$ for some $z \in \mathbb{Z}$. If $z$ is odd, then
$4a^2 \in \mathbb{Z}$, $4(a^2 + b^2) \equiv 0 \mod 4$, and $4a^2 \equiv 1 \mod 4$. But now $4b^2 \in \mathbb{Z}$,
forcing $b = z'/2$ for some $z' \in \mathbb{Z}$ and thus $4b^2 \equiv 0, 1 \mod 4$ depending
on whether $z'$ is even or odd. Therefore $4(a^2 + b^2) \equiv 1, 2 \mod 4$. 

We immediately see that $a = z/2$ for some $z \in \mathbb{Z}$. If $z$ is odd, then $4a^2 \in \mathbb{Z}$, $4(a^2 + b^2) \equiv 0 \mod 4$, and $4a^2 \equiv 1 \mod 4$. But now $4b^2 \in \mathbb{Z}$, forcing $b = z'/2$ for some $z' \in \mathbb{Z}$ and thus $4b^2 \equiv 0, 1 \mod 4$ depending on whether $z'$ is even or odd. Therefore $4(a^2 + b^2) \equiv 1, 2 \mod 4$. This contradiction shows that $z$ is even so that $a \in \mathbb{Z}$. 
We immediately see that $a = z/2$ for some $z \in \mathbb{Z}$. If $z$ is odd, then $4a^2 \in \mathbb{Z}$, $4(a^2 + b^2) \equiv 0 \mod 4$, and $4a^2 \equiv 1 \mod 4$. But now $4b^2 \in \mathbb{Z}$, forcing $b = z'/2$ for some $z' \in \mathbb{Z}$ and thus $4b^2 \equiv 0, 1 \mod 4$ depending on whether $z'$ is even or odd. Therefore $4(a^2 + b^2) \equiv 1, 2 \mod 4$. This contradiction shows that $z$ is even so that $a \in \mathbb{Z}$. Now $b^2 \in \mathbb{Z}$,
We immediately see that \( a = z/2 \) for some \( z \in \mathbb{Z} \). If \( z \) is odd, then \( 4a^2 \in \mathbb{Z} \), \( 4(a^2 + b^2) \equiv 0 \mod 4 \), and \( 4a^2 \equiv 1 \mod 4 \). But now \( 4b^2 \in \mathbb{Z} \), forcing \( b = z'/2 \) for some \( z' \in \mathbb{Z} \) and thus \( 4b^2 \equiv 0,1 \mod 4 \) depending on whether \( z' \) is even or odd. Therefore \( 4(a^2 + b^2) \equiv 1,2 \mod 4 \). This contradiction shows that \( z \) is even so that \( a \in \mathbb{Z} \).

Now \( b^2 \in \mathbb{Z} \), forcing \( b \in \mathbb{Z} \), too.
Along the same lines as the argument above,
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of $\mathbb{Q}$.

**Example:** Suppose $K$ is a degree 2 number field and write $K = \mathbb{Q}(\sqrt{D})$ where $D$ is a square-free rational integer. If $D \equiv 2, 3 \pmod{4}$, then the algebraic integers in $K$ is the ring $\mathbb{Z}[\sqrt{D}]$. If $D \equiv 1 \pmod{4}$, then the algebraic integers in $K$ is the ring $\mathbb{Z}[\frac{1 + \sqrt{D}}{2}]$.

**Proposition**

Suppose $K$ is a number field and $\alpha \in K$. Then the following are equivalent:

1) $\alpha$ is an algebraic integer;
2) there is a finitely generated non-zero $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$.

**Proof:** Suppose $\alpha$ is an algebraic integer with minimal polynomial $P(X) \in \mathbb{Z}[X]$ (always assumed to be monic). If $n$ is the degree of $P$, then we readily see that for the $\mathbb{Z}$-module $M$ generated by $1, \alpha, \ldots, \alpha^{n-1}$, $\alpha M \subseteq M$. 
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of $\mathbb{Q}$.

**Example:**

Suppose $K$ is a degree 2 number field and write $K = \mathbb{Q}(\sqrt{D})$ where $D$ is a square-free rational integer.

If $D \equiv 2, 3 \mod 4$, then the algebraic integers in $K$ is the ring $\mathbb{Z}[\sqrt{D}]$.

If $D \equiv 1 \mod 4$, then the algebraic integers in $K$ is the ring $\mathbb{Z}[\frac{1 + \sqrt{D}}{2}]$.

**Proposition**

Suppose $K$ is a number field and $\alpha \in K$.

Then the following are equivalent:

1) $\alpha$ is an algebraic integer;

2) there is a finitely generated non-zero $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$.

**Proof:**

Suppose $\alpha$ is an algebraic integer with minimal polynomial $P(X) \in \mathbb{Z}[X]$ (always assumed to be monic).

If $n$ is the degree of $P$, then we readily see that for the $\mathbb{Z}$-module $M$ generated by $1, \alpha, \ldots, \alpha^{n-1}$, $\alpha M \subseteq M$. 
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of \( \mathbb{Q} \).

**Example:** Suppose \( K \) is a degree 2 number field and write \( K = \mathbb{Q}(\sqrt{D}) \).
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of $\mathbb{Q}$.

**Example**: Suppose $K$ is a degree 2 number field and write $K = \mathbb{Q}(\sqrt{D})$ where $D$ is a square-free rational integer.
Along the same lines as the argument above, one can give the following
description of algebraic integers in a quadratic extension of \( \mathbb{Q} \).

**Example:** Suppose \( K \) is a degree 2 number field and write \( K = \mathbb{Q}(\sqrt{D}) \) where \( D \) is a square-free rational integer. If \( D \equiv 2, 3 \mod{4} \)
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of \( \mathbb{Q} \).

**Example**: Suppose \( K \) is a degree 2 number field and write \( K = \mathbb{Q}(\sqrt{D}) \) where \( D \) is a square-free rational integer. If \( D \equiv 2, 3 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[\sqrt{D}] \).
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of $\mathbb{Q}$.

**Example:** Suppose $K$ is a degree 2 number field and write $K = \mathbb{Q}(\sqrt{D})$ where $D$ is a square-free rational integer. If $D \equiv 2, 3 \pmod{4}$ then the algebraic integers in $K$ is the ring $\mathbb{Z}[\sqrt{D}]$. If $D \equiv 1 \pmod{4}$
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of $\mathbb{Q}$.

**Example:** Suppose $K$ is a degree 2 number field and write $K = \mathbb{Q}(\sqrt{D})$ where $D$ is a square-free rational integer. If $D \equiv 2, 3 \mod 4$ then the algebraic integers in $K$ is the ring $\mathbb{Z}[\sqrt{D}]$. If $D \equiv 1 \mod 4$ then the algebraic integers in $K$ is the ring $\mathbb{Z}[(1 + \sqrt{D})/2]$. 


Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of \( \mathbb{Q} \).

**Example:** Suppose \( K \) is a degree 2 number field and write \( K = \mathbb{Q}(\sqrt{D}) \) where \( D \) is a square-free rational integer. If \( D \equiv 2, 3 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[\sqrt{D}] \). If \( D \equiv 1 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[(1 + \sqrt{D})/2] \).

**Proposition**
Along the same lines as the argument above, one can give the following
description of algebraic integers in a quadratic extension of $\mathbb{Q}$.

**Example:** Suppose $K$ is a degree 2 number field and write $K = \mathbb{Q}(\sqrt{D})$
where $D$ is a square-free rational integer. If $D \equiv 2, 3 \mod 4$ then the
algebraic integers in $K$ is the ring $\mathbb{Z}[\sqrt{D}]$. If $D \equiv 1 \mod 4$ then the
algebraic integers in $K$ is the ring $\mathbb{Z}[(1 + \sqrt{D})/2]$.

**Proposition**

*Suppose $K$ is a number field and $\alpha \in K$.***
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of \( \mathbb{Q} \).

**Example:** Suppose \( K \) is a degree 2 number field and write \( K = \mathbb{Q}(\sqrt{D}) \) where \( D \) is a square-free rational integer. If \( D \equiv 2, 3 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[\sqrt{D}] \). If \( D \equiv 1 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[(1 + \sqrt{D})/2] \).

**Proposition**

*Suppose \( K \) is a number field and \( \alpha \in K \). Then the following are equivalent:*
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of \( \mathbb{Q} \).

**Example:** Suppose \( K \) is a degree 2 number field and write \( K = \mathbb{Q}(\sqrt{D}) \) where \( D \) is a square-free rational integer. If \( D \equiv 2, 3 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[\sqrt{D}] \). If \( D \equiv 1 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[(1 + \sqrt{D})/2] \).

**Proposition**

*Suppose \( K \) is a number field and \( \alpha \in K \). Then the following are equivalent:
1) \( \alpha \) is an algebraic integer;*
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of \( \mathbb{Q} \).

**Example:** Suppose \( K \) is a degree 2 number field and write \( K = \mathbb{Q}(\sqrt{D}) \) where \( D \) is a square-free rational integer. If \( D \equiv 2, 3 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[\sqrt{D}] \). If \( D \equiv 1 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[(1 + \sqrt{D})/2] \).

**Proposition**

*Suppose \( K \) is a number field and \( \alpha \in K \). Then the following are equivalent:

1) \( \alpha \) is an algebraic integer;
2) there is a finitely generated non-zero \( \mathbb{Z} \)-module \( M \subset K \) such that \( \alpha M \subseteq M \).*
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of $\mathbb{Q}$.

**Example**: Suppose $K$ is a degree 2 number field and write $K = \mathbb{Q}(\sqrt{D})$ where $D$ is a square-free rational integer. If $D \equiv 2, 3 \mod 4$ then the algebraic integers in $K$ is the ring $\mathbb{Z}[\sqrt{D}]$. If $D \equiv 1 \mod 4$ then the algebraic integers in $K$ is the ring $\mathbb{Z}[(1 + \sqrt{D})/2]$.

**Proposition**

Suppose $K$ is a number field and $\alpha \in K$. Then the following are equivalent:
1) $\alpha$ is an algebraic integer;
2) there is a finitely generated non-zero $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$.

**Proof:**
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of \( \mathbb{Q} \).

**Example:** Suppose \( K \) is a degree 2 number field and write \( K = \mathbb{Q}(\sqrt{D}) \) where \( D \) is a square-free rational integer. If \( D \equiv 2, 3 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[\sqrt{D}] \). If \( D \equiv 1 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[(1 + \sqrt{D})/2] \).

**Proposition**

Suppose \( K \) is a number field and \( \alpha \in K \). Then the following are equivalent:

1) \( \alpha \) is an algebraic integer;
2) there is a finitely generated non-zero \( \mathbb{Z} \)-module \( M \subset K \) such that \( \alpha M \subseteq M \).

**Proof:** Suppose \( \alpha \) is an algebraic integer with minimal polynomial \( P(X) \in \mathbb{Z}[X] \).
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of \( \mathbb{Q} \).

**Example:** Suppose \( K \) is a degree 2 number field and write \( K = \mathbb{Q}(\sqrt{D}) \) where \( D \) is a square-free rational integer. If \( D \equiv 2, 3 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[\sqrt{D}] \). If \( D \equiv 1 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[(1 + \sqrt{D})/2] \).

**Proposition**

Suppose \( K \) is a number field and \( \alpha \in K \). Then the following are equivalent:

1) \( \alpha \) is an algebraic integer;
2) there is a finitely generated non-zero \( \mathbb{Z} \)-module \( M \subset K \) such that \( \alpha M \subseteq M \).

**Proof:** Suppose \( \alpha \) is an algebraic integer with minimal polynomial \( P(X) \in \mathbb{Z}[X] \) (always assumed to be monic).
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of \( \mathbb{Q} \).

**Example:** Suppose \( K \) is a degree 2 number field and write \( K = \mathbb{Q}(\sqrt{D}) \) where \( D \) is a square-free rational integer. If \( D \equiv 2, 3 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[\sqrt{D}] \). If \( D \equiv 1 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[(1 + \sqrt{D})/2] \).

**Proposition**

Suppose \( K \) is a number field and \( \alpha \in K \). Then the following are equivalent:

1) \( \alpha \) is an algebraic integer;
2) there is a finitely generated non-zero \( \mathbb{Z} \)-module \( M \subset K \) such that \( \alpha M \subseteq M \).

**Proof:** Suppose \( \alpha \) is an algebraic integer with minimal polynomial \( P(X) \in \mathbb{Z}[X] \) (always assumed to be monic). If \( n \) is the degree of \( P \),
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of $\mathbb{Q}$.

**Example:** Suppose $K$ is a degree 2 number field and write $K = \mathbb{Q}(\sqrt{D})$ where $D$ is a square-free rational integer. If $D \equiv 2, 3 \mod 4$ then the algebraic integers in $K$ is the ring $\mathbb{Z}[\sqrt{D}]$. If $D \equiv 1 \mod 4$ then the algebraic integers in $K$ is the ring $\mathbb{Z}[(1 + \sqrt{D})/2]$.

**Proposition**

Suppose $K$ is a number field and $\alpha \in K$. Then the following are equivalent:
1) $\alpha$ is an algebraic integer;
2) there is a finitely generated non-zero $\mathbb{Z}$-module $M \subset K$ such that $\alpha M \subseteq M$.

**Proof:** Suppose $\alpha$ is an algebraic integer with minimal polynomial $P(X) \in \mathbb{Z}[X]$ (always assumed to be monic). If $n$ is the degree of $P$, then we readily see that for the $\mathbb{Z}$-module $M$ generated by $1, \alpha, \ldots, \alpha^{n-1}$,
Along the same lines as the argument above, one can give the following description of algebraic integers in a quadratic extension of \( \mathbb{Q} \).

**Example:** Suppose \( K \) is a degree 2 number field and write \( K = \mathbb{Q}(\sqrt{D}) \) where \( D \) is a square-free rational integer. If \( D \equiv 2, 3 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[\sqrt{D}] \). If \( D \equiv 1 \mod 4 \) then the algebraic integers in \( K \) is the ring \( \mathbb{Z}[(1 + \sqrt{D})/2] \).

**Proposition**

Suppose \( K \) is a number field and \( \alpha \in K \). Then the following are equivalent:

1) \( \alpha \) is an algebraic integer;

2) there is a finitely generated non-zero \( \mathbb{Z} \)-module \( M \subset K \) such that \( \alpha M \subseteq M \).

**Proof:** Suppose \( \alpha \) is an algebraic integer with minimal polynomial \( P(X) \in \mathbb{Z}[X] \) (always assumed to be monic). If \( n \) is the degree of \( P \), then we readily see that for the \( \mathbb{Z} \)-module \( M \) generated by 1, \( \alpha, \ldots, \alpha^{n-1} \), \( \alpha M \subseteq M \).
Now suppose there is some non-zero finitely generated \( \mathbb{Z} \) module \( M \subset K \) with \( \alpha M \subset M \).
Now suppose there is some non-zero finitely generated \( \mathbb{Z} \) module \( M \subset K \) with \( \alpha M \subset M \). Let \( M \) be generated by \( \beta_1, \ldots, \beta_n \in K \).
Now suppose there is some non-zero finitely generated $\mathbb{Z}$ module $M \subset K$ with $\alpha M \subset M$. Let $M$ be generated by $\beta_1, \ldots, \beta_n \in K$. Then for all $i = 1, \ldots, n$
Now suppose there is some non-zero finitely generated \( \mathbb{Z} \) module \( M \subset K \) with \( \alpha M \subset M \). Let \( M \) be generated by \( \beta_1, \ldots, \beta_n \in K \). Then for all \( i = 1, \ldots, n \) we may write \( \alpha \beta_i = \sum_{j=1}^{n} a_{i,j} \beta_j \) where \( a_{i,j} \in \mathbb{Z} \).
Now suppose there is some non-zero finitely generated \( \mathbb{Z} \) module \( M \subset K \) with \( \alpha M \subset M \). Let \( M \) be generated by \( \beta_1, \ldots, \beta_n \in K \). Then for all \( i = 1, \ldots, n \) we may write \( \alpha \beta_i = \sum_{j=1}^n a_{i,j} \beta_j \) where \( a_{i,j} \in \mathbb{Z} \). We now set \( A \) to be the \( n \times n \) matrix
Now suppose there is some non-zero finitely generated $\mathbb{Z}$ module $M \subset K$ with $\alpha M \subset M$. Let $M$ be generated by $\beta_1, \ldots, \beta_n \in K$. Then for all $i = 1, \ldots, n$ we may write $\alpha \beta_i = \sum_{j=1}^{n} a_{i,j} \beta_j$ where $a_{i,j} \in \mathbb{Z}$. We now set $A$ to be the $n \times n$ matrix with diagonal entries $\alpha - a_{i,i}$ and off-diagonal entries $-a_{i,j}$.
Now suppose there is some non-zero finitely generated \( \mathbb{Z} \) module \( M \subset K \) with \( \alpha M \subset M \). Let \( M \) be generated by \( \beta_1, \ldots, \beta_n \in K \). Then for all \( i = 1, \ldots, n \) we may write \( \alpha \beta_i = \sum_{j=1}^{n} a_{i,j} \beta_j \) where \( a_{i,j} \in \mathbb{Z} \). We now set \( A \) to be the \( n \times n \) matrix with diagonal entries \( \alpha - a_{i,i} \) and off-diagonal entries \( -a_{i,j} \), so that our system of equations implies that the determinant of \( A \) is zero.
Now suppose there is some non-zero finitely generated \( \mathbb{Z} \) module \( M \subset K \) with \( \alpha M \subset M \). Let \( M \) be generated by \( \beta_1, \ldots, \beta_n \in K \). Then for all \( i = 1, \ldots, n \) we may write \( \alpha \beta_i = \sum_{j=1}^{n} a_{i,j} \beta_j \) where \( a_{i,j} \in \mathbb{Z} \). We now set \( A \) to be the \( n \times n \) matrix with diagonal entries \( \alpha - a_{i,i} \) and off-diagonal entries \( -a_{i,j} \), so that our system of equations implies that the determinant of \( A \) is zero. This determinant of \( A \) gives us our monic polynomial \( P(X) \in \mathbb{Z}[X] \) of degree \( n \) where \( \alpha \) is a root.
Now suppose there is some non-zero finitely generated \( \mathbb{Z} \) module \( M \subset K \) with \( \alpha M \subset M \). Let \( M \) be generated by \( \beta_1, \ldots, \beta_n \in K \). Then for all \( i = 1, \ldots, n \) we may write \( \alpha \beta_i = \sum_{j=1}^{n} a_{i,j} \beta_j \) where \( a_{i,j} \in \mathbb{Z} \). We now set \( A \) to be the \( n \times n \) matrix with diagonal entries \( \alpha - a_{i,i} \) and off-diagonal entries \( -a_{i,j} \), so that our system of equations implies that the determinant of \( A \) is zero. This determinant of \( A \) gives us our monic polynomial \( P(X) \in \mathbb{Z}[X] \) of degree \( n \) where \( \alpha \) is a root (though we do not, and need not, assert that \( P \) is irreducible over \( \mathbb{Q} \)).
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $O_K$.

Proof:
We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)MN \subseteq MN$ and $(\alpha \beta)MN \subseteq MN$.

Lemma
If $\alpha \in K$ for some number field $K$, then $z\alpha \in O_K$ for some non-zero $z \in \mathbb{Z}$. In particular, $K$ is the quotient field of $O_K$.

Proof:
Since $\alpha$ is necessarily algebraic over $\mathbb{Q}$, there is a non-zero polynomial $P(X) = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ with $P(\alpha) = 0$. Multiplying $P(X)$ by $a_n^{-1}n$, we see that $a_n\alpha$ is an algebraic integer. Since $O_K \supseteq \mathbb{Z}$, its quotient field is $K$. 

Math 681, Friday, January 15
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$.

Proof:

We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers.

Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$.

Then one readily sees that $(\alpha \pm \beta) MN \subseteq MN$ and $(\alpha \beta) MN \subseteq MN$.

Lemma

If $\alpha \in K$ for some number field $K$, then $z \alpha \in \mathcal{O}_K$ for some non-zero $z \in \mathbb{Z}$.

In particular, $K$ is the quotient field of $\mathcal{O}_K$.

Proof:

Since $\alpha$ is necessarily algebraic over $\mathbb{Q}$, there is a non-zero polynomial $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ with $P(\alpha) = 0$.

Multiplying $P(X)$ by $a_n^{-1}n$, we see that $a_n \alpha$ is an algebraic integer.

Since $\mathcal{O}_K \supseteq \mathbb{Z}$, its quotient field is $K$. 

Math 681, Friday, January 15

January 15, 2021
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathcal{O}_K$. 

Proof:

We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers.

Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$.

Then one readily sees that $(\alpha \pm \beta) MN \subseteq MN$ and $(\alpha \beta) MN \subseteq MN$.

Lemma

If $\alpha \in K$ for some number field $K$, then $z\alpha \in \mathcal{O}_K$ for some non-zero $z \in \mathbb{Z}$.

In particular, $K$ is the quotient field of $\mathcal{O}_K$.

Proof:

Since $\alpha$ is necessarily algebraic over $\mathbb{Q}$, there is a non-zero polynomial $P(X) = a_n X^n + \ldots + a_0 \in \mathbb{Z}[X]$ with $P(\alpha) = 0$.

Multiplying $P(X)$ by $a_n^{-1}$, we see that $a_n \alpha$ is an algebraic integer. Since $\mathcal{O}_K \supseteq \mathbb{Z}$, its quotient field is $K$. 

Math 681, Friday, January 15

January 15, 2021
Corollary

*The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathcal{O}_K$.*

Proof:

(Continued later)
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathfrak{O}_K$.

Proof: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication,
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathcal{O}_K$.

Proof: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers.
**Corollary**

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathcal{O}_K$.

**Proof:** We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition.
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathfrak{O}_K$.

Proof: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. 
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathcal{O}_K$.

Proof: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)MN \subseteq MN$. 

Math 681, Friday, January 15
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathcal{O}_K$.

**Proof**: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)MN \subseteq MN$ and $(\alpha \beta)MN \subseteq MN$. 
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathcal{O}_K$.

Proof: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)MN \subseteq MN$ and $(\alpha \beta)MN \subseteq MN$.

Lemma
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathfrak{O}_K$.

Proof: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)MN \subseteq MN$ and $(\alpha \beta)MN \subseteq MN$.

Lemma

If $\alpha \in K$ for some number field $K$, 

Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathcal{O}_K$.

Proof: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)MN \subseteq MN$ and $(\alpha \beta)MN \subseteq MN$.

Lemma

If $\alpha \in K$ for some number field $K$, then $z\alpha \in \mathcal{O}_K$ for some non-zero $z \in \mathbb{Z}$. 
**Corollary**

The set of algebraic integers in a given number field \( K \) is a subring of \( K \), denoted \( \mathfrak{O}_K \).

**Proof:** We only have to show that the set of algebraic integers in \( K \) is closed under addition and multiplication, so let \( \alpha, \beta \in K \) be algebraic integers. Get \( \mathbb{Z} \)-modules \( M \) and \( N \) as in the Proposition with \( \alpha M \subseteq M \) and \( \beta N \subseteq N \). Then one readily sees that \((\alpha \pm \beta)MN \subseteq MN \) and \((\alpha \beta)MN \subseteq MN \).

**Lemma**

If \( \alpha \in K \) for some number field \( K \), then \( z\alpha \in \mathfrak{O}_K \) for some non-zero \( z \in \mathbb{Z} \). In particular, \( K \) is the quotient field of \( \mathfrak{O}_K \).
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathcal{O}_K$.

Proof: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta) MN \subseteq MN$ and $(\alpha \beta) MN \subseteq MN$.

Lemma

If $\alpha \in K$ for some number field $K$, then $z\alpha \in \mathcal{O}_K$ for some non-zero $z \in \mathbb{Z}$. In particular, $K$ is the quotient field of $\mathcal{O}_K$.

Proof:
**Corollary**

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathfrak{O}_K$.

**Proof:** We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)MN \subseteq MN$ and $(\alpha \beta)MN \subseteq MN$.

**Lemma**

If $\alpha \in K$ for some number field $K$, then $z\alpha \in \mathfrak{O}_K$ for some non-zero $z\in\mathbb{Z}$. In particular, $K$ is the quotient field of $\mathfrak{O}_K$.

**Proof:** Since $\alpha$ is necessarily algebraic over over $\mathbb{Q}$,
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathfrak{O}_K$.

Proof: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)MN \subseteq MN$ and $(\alpha \beta)MN \subseteq MN$.

Lemma

If $\alpha \in K$ for some number field $K$, then $z\alpha \in \mathfrak{O}_K$ for some non-zero $z \in \mathbb{Z}$. In particular, $K$ is the quotient field of $\mathfrak{O}_K$.

Proof: Since $\alpha$ is necessarily algebraic over over $\mathbb{Q}$, there is a non-zero polynomial $P(X) = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ with $P(\alpha) = 0$. 
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathcal{O}_K$.

Proof: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)M N \subseteq M N$ and $(\alpha\beta)M N \subseteq M N$.

Lemma

If $\alpha \in K$ for some number field $K$, then $z\alpha \in \mathcal{O}_K$ for some non-zero $z \in \mathbb{Z}$. In particular, $K$ is the quotient field of $\mathcal{O}_K$.

Proof: Since $\alpha$ is necessarily algebraic over $\mathbb{Q}$, there is a non-zero polynomial $P(X) = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ with $P(\alpha) = 0$. Multiplying $P(X)$ by $a_n^{-1}$,
**Corollary**

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathcal{O}_K$.

**Proof:** We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)MN \subseteq MN$ and $(\alpha\beta)MN \subseteq MN$.

**Lemma**

If $\alpha \in K$ for some number field $K$, then $z\alpha \in \mathcal{O}_K$ for some non-zero $z \in \mathbb{Z}$. In particular, $K$ is the quotient field of $\mathcal{O}_K$.

**Proof:** Since $\alpha$ is necessarily algebraic over $\mathbb{Q}$, there is a non-zero polynomial $P(X) = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ with $P(\alpha) = 0$. Multiplying $P(X)$ by $a_n^{n-1}$, we see that $a_n\alpha$ is an algebraic integer.
Corollary

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathfrak{O}_K$.

Proof: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)MN \subseteq MN$ and $(\alpha \beta)MN \subseteq MN$.

Lemma

If $\alpha \in K$ for some number field $K$, then $z\alpha \in \mathfrak{O}_K$ for some non-zero $z \in \mathbb{Z}$. In particular, $K$ is the quotient field of $\mathfrak{O}_K$.

Proof: Since $\alpha$ is necessarily algebraic over $\mathbb{Q}$, there is a non-zero polynomial $P(X) = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ with $P(\alpha) = 0$. Multiplying $P(X)$ by $a_n^{n-1}$, we see that $a_n\alpha$ is an algebraic integer. Since $\mathfrak{O}_K \supseteq \mathbb{Z}$,
**Corollary**

The set of algebraic integers in a given number field $K$ is a subring of $K$, denoted $\mathfrak{O}_K$.

**Proof**: We only have to show that the set of algebraic integers in $K$ is closed under addition and multiplication, so let $\alpha, \beta \in K$ be algebraic integers. Get $\mathbb{Z}$-modules $M$ and $N$ as in the Proposition with $\alpha M \subseteq M$ and $\beta N \subseteq N$. Then one readily sees that $(\alpha \pm \beta)MN \subseteq MN$ and $(\alpha \beta)MN \subseteq MN$.

**Lemma**

If $\alpha \in K$ for some number field $K$, then $z\alpha \in \mathfrak{O}_K$ for some non-zero $z \in \mathbb{Z}$. In particular, $K$ is the quotient field of $\mathfrak{O}_K$.

**Proof**: Since $\alpha$ is necessarily algebraic over over $\mathbb{Q}$, there is a non-zero polynomial $P(X) = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ with $P(\alpha) = 0$. Multiplying $P(X)$ by $a_n^{n-1}$, we see that $a_n\alpha$ is an algebraic integer. Since $\mathfrak{O}_K \supseteq \mathbb{Z}$, its quotient field is $K$. 

**Math 681, Friday, January 15 January 15, 2021**
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K: \mathbb{Q}]$.

Proof:

Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module.

Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, ..., \alpha_n$ of algebraic integers ($n = [K: \mathbb{Q}]$).

Let $\text{Tr}$ denote the trace from $K$ to $\mathbb{Q}$.

For any fixed non-zero $\alpha \in K$ the function $f_\alpha(x) := \text{Tr}(x\alpha)$ is an element of the dual space of $K$ viewed as an $n$-dimensional vector space over $\mathbb{Q}$ (i.e., $f_\alpha(x) : K \to \mathbb{Q}$ is a linear transformation of $\mathbb{Q}$ vector spaces).

Since the trace is non-trivial (there is $\beta \in K$ with $\text{Tr}(\beta) \neq 0$), we have a homomorphism $\alpha \mapsto f_\alpha$ from $K$ to its dual with a trivial kernel.
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$. 

Proof:
Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated. Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, \ldots, \alpha_n$ of algebraic integers ($n = [K : \mathbb{Q}]$).

Let Tr denote the trace from $K$ to $\mathbb{Q}$. For any fixed non-zero $\alpha \in K$, the function $f_\alpha(x) := \text{Tr}(x\alpha)$ is an element of the dual space of $K$ viewed as an $n$-dimensional vector space over $\mathbb{Q}$ (i.e., $f_\alpha(x) : K \to \mathbb{Q}$ is a linear transformation of $\mathbb{Q}$ vector spaces). Since the trace is non-trivial (there is a $\beta \in K$ with $\text{Tr}(\beta) \neq 0$), we have a homomorphism $\alpha \mapsto f_\alpha$ from $K$ to its dual with a trivial kernel.
Theorem

For a number field \( K \), the ring of integers \( \mathcal{O}_K \) is a free \( \mathbb{Z} \)-module of rank \( [K : \mathbb{Q}] \).

Proof:

Since \( \mathcal{O}_K \supseteq \mathbb{Z} \) is an integral domain, it is a torsion-free \( \mathbb{Z} \)-module. Since \( \mathbb{Z} \) is a principal ideal domain, to prove \( \mathcal{O}_K \) is a free \( \mathbb{Z} \)-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any \( \mathbb{Q} \)-basis for \( K \), we see that there is such a basis \( \alpha_1, \ldots, \alpha_n \) of algebraic integers (\( n = [K : \mathbb{Q}] \)).

Let \( \text{Tr} \) denote the trace from \( K \) to \( \mathbb{Q} \).

For any fixed non-zero \( \alpha \in K \) the function \( f_\alpha(x) \equiv \text{Tr}(x_\alpha) \) is an element of the dual space of \( K \) viewed as \( n \)-dimensional vector space over \( \mathbb{Q} \). Since the trace is non-trivial (there is a \( \beta \in K \) with \( \text{Tr}(\beta) \neq 0 \)), we have a homomorphism \( \alpha \mapsto f_\alpha \) from \( K \) to its dual with a trivial kernel.
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain,
For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

**Proof:** Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module.
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain,
Theorem

For a number field $K$, the ring of integers $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathfrak{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, 

Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, \ldots, \alpha_n$ of algebraic integers
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, \ldots, \alpha_n$ of algebraic integers ($n = [K : \mathbb{Q}]$).
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, \ldots, \alpha_n$ of algebraic integers ($n = [K : \mathbb{Q}]$).

Let $\text{Tr}$ denote the trace from $K$ to $\mathbb{Q}$. 
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, \ldots, \alpha_n$ of algebraic integers ($n = [K : \mathbb{Q}]$).

Let $\text{Tr}$ denote the trace from $K$ to $\mathbb{Q}$. For any fixed non-zero $\alpha \in K$
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, \ldots, \alpha_n$ of algebraic integers ($n = [K : \mathbb{Q}]$).

Let $\text{Tr}$ denote the trace from $K$ to $\mathbb{Q}$. For any fixed non-zero $\alpha \in K$ the function $f_{\alpha}(x) := \text{Tr}(x\alpha)$
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, \ldots, \alpha_n$ of algebraic integers ($n = [K : \mathbb{Q}]$).

Let $\text{Tr}$ denote the trace from $K$ to $\mathbb{Q}$. For any fixed non-zero $\alpha \in K$ the function $f_\alpha(x) := \text{Tr}(x\alpha)$ is an element of the dual space of $K$ viewed as an $n$-dimensional vector space over $\mathbb{Q}$.
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, \ldots, \alpha_n$ of algebraic integers ($n = [K : \mathbb{Q}]$).

Let $\text{Tr}$ denote the trace from $K$ to $\mathbb{Q}$. For any fixed non-zero $\alpha \in K$ the function $f_\alpha(x) := \text{Tr}(x\alpha)$ is an element of the dual space of $K$ viewed as an $n$-dimensional vector space over $\mathbb{Q}$ (i.e., $f_\alpha(x) : K \to \mathbb{Q}$ is a linear transformation of $\mathbb{Q}$ vector spaces).
**Theorem**  
*For a number field* $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.  

**Proof:** Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, \ldots, \alpha_n$ of algebraic integers ($n = [K : \mathbb{Q}]$).

Let $\text{Tr}$ denote the trace from $K$ to $\mathbb{Q}$. For any fixed non-zero $\alpha \in K$ the function $f_\alpha(x) := \text{Tr}(x\alpha)$ is an element of the dual space of $K$ viewed as an $n$-dimensional vector space over $\mathbb{Q}$ (i.e., $f_\alpha(x) : K \to \mathbb{Q}$ is a linear transformation of $\mathbb{Q}$ vector spaces). Since the trace is non-trivial...
**Theorem**

*For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.***

**Proof:** Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, \ldots, \alpha_n$ of algebraic integers ($n = [K : \mathbb{Q}]$).

Let $\text{Tr}$ denote the trace from $K$ to $\mathbb{Q}$. For any fixed non-zero $\alpha \in K$ the function $f_\alpha(x) := \text{Tr}(x\alpha)$ is an element of the dual space of $K$ viewed as an $n$-dimensional vector space over $\mathbb{Q}$ (i.e., $f_\alpha(x) : K \to \mathbb{Q}$ is a linear transformation of $\mathbb{Q}$ vector spaces). Since the trace is non-trivial (there is a $\beta \in K$ with $\text{Tr}(\beta) \neq 0$),
Theorem

For a number field $K$, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Proof: Since $\mathcal{O}_K \supseteq \mathbb{Z}$ is an integral domain, it is a torsion-free $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a principal ideal domain, to prove $\mathcal{O}_K$ is a free $\mathbb{Z}$-module it suffices to show that it is finitely generated.

Applying the Lemma to elements of any $\mathbb{Q}$-basis for $K$, we see that there is such a basis $\alpha_1, \ldots, \alpha_n$ of algebraic integers ($n = [K : \mathbb{Q}]$).

Let $\text{Tr}$ denote the trace from $K$ to $\mathbb{Q}$. For any fixed non-zero $\alpha \in K$ the function $f_\alpha(x) := \text{Tr}(x\alpha)$ is an element of the dual space of $K$ viewed as an $n$-dimensional vector space over $\mathbb{Q}$ (i.e., $f_\alpha(x) : K \rightarrow \mathbb{Q}$ is a linear transformation of $\mathbb{Q}$ vector spaces). Since the trace is non-trivial (there is a $\beta \in K$ with $\text{Tr}(\beta) \neq 0$), we have a homomorphism $\alpha \mapsto f_\alpha$ from $K$ to its dual with a trivial kernel.
Since $K$ is isomorphic to its dual
Since $K$ is isomorphic to its dual (it’s a finite dimensional vector space over $\mathbb{Q}$)
Since $K$ is isomorphic to its dual (it’s a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$: 

$$\text{Tr}(\alpha'_i \alpha'_j) = \begin{cases} 
1 & \text{if } i = j, \\
0 & \text{otherwise}. 
\end{cases}$$

Now choose a non-zero $z \in \mathbb{Z}$ such that $z \alpha'_i \in \mathcal{O}_K$ for all $i$. Let $\alpha \in \mathcal{O}_K$. Then $\alpha z \alpha'_i \in \mathcal{O}_K$ for all $i$ and hence $\text{Tr}(\alpha z \alpha'_i)$ is, too.

Writing $\alpha = \sum_{i=1}^{n} a_i \alpha_i$ with $a_i \in \mathbb{Q}$ for all $i$, we have $\text{Tr}(\alpha z \alpha'_i) = za_i \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. This shows that $\mathcal{O}_K \subseteq z^{-1} \alpha_1 \mathbb{Z} \oplus \cdots \oplus z^{-1} \alpha_n \mathbb{Z}$.

Finally, since $\mathbb{Z}$ is Noetherian and $\mathcal{O}_K$ is a $\mathbb{Z}$-submodule of a finitely generated $\mathbb{Z}$-module, it must be finitely generated as well. Clearly the rank of $\mathcal{O}_K$ must be at least $n = [K: \mathbb{Q}]$ and no larger than $n$. 

Math 681, Friday, January 15

January 15, 2021
Since $K$ is isomorphic to its dual (it’s a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$:

$$\text{Tr}(\alpha'_i; \alpha_j) = \begin{cases} 
1 & \text{if } i = j, \\
0 & \text{otherwise}.
\end{cases}$$
Since $K$ is isomorphic to its dual (it’s a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$:

$$\text{Tr}(\alpha'_i; \alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Now choose a non-zero $z \in \mathbb{Z}$ such that $z\alpha'_i \in \mathfrak{O}_K$ for all $i$. 
Since $K$ is isomorphic to its dual (it’s a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$:

$$\text{Tr}(\alpha'_i; \alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise}. \end{cases}$$

Now choose a non-zero $z \in \mathbb{Z}$ such that $z \alpha'_i \in \mathcal{O}_K$ for all $i$. Let $\alpha \in \mathcal{O}_K$. 


Since $K$ is isomorphic to its dual (it’s a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$:

$$\text{Tr}(\alpha'_i \alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Now choose a non-zero $z \in \mathbb{Z}$ such that $z\alpha'_i \in \mathcal{O}_K$ for all $i$. Let $\alpha \in \mathcal{O}_K$. Then $\alpha z \alpha'_i \in \mathcal{O}_K$ for all $i$. 
Since $K$ is isomorphic to its dual (it's a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$:

$$\text{Tr}(\alpha'_i, \alpha'_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Now choose a non-zero $z \in \mathbb{Z}$ such that $z\alpha'_i \in \mathcal{O}_K$ for all $i$. Let $\alpha \in \mathcal{O}_K$. Then $\alpha z\alpha'_i \in \mathcal{O}_K$ for all $i$ and hence $\text{Tr}(\alpha z\alpha'_i)$ is, too.
Since $K$ is isomorphic to its dual (it’s a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$:

$$\text{Tr}(\alpha'_i; \alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise}. \end{cases}$$

Now choose a non-zero $z \in \mathbb{Z}$ such that $z\alpha'_i \in \mathfrak{O}_K$ for all $i$. Let $\alpha \in \mathfrak{O}_K$. Then $\alpha z \alpha'_i \in \mathfrak{O}_K$ for all $i$ and hence $\text{Tr}(\alpha z \alpha'_i)$ is, too. Writing $\alpha = \sum_{i=1}^n a_i \alpha_i$ with $a_i \in \mathbb{Q}$ for all $i$, ...
Since $K$ is isomorphic to its dual (it’s a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$:

$$\text{Tr}(\alpha'_i \alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Now choose a non-zero $z \in \mathbb{Z}$ such that $z \alpha'_i \in \mathcal{O}_K$ for all $i$. Let $\alpha \in \mathcal{O}_K$. Then $\alpha z \alpha'_i \in \mathcal{O}_K$ for all $i$ and hence $\text{Tr}(\alpha z \alpha'_i)$ is, too. Writing $\alpha = \sum_{i=1}^{n} a_i \alpha_i$ with $a_i \in \mathbb{Q}$ for all $i$, we have

$$\text{Tr}(\alpha z \alpha'_i) = za_i \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$
Since $K$ is isomorphic to its dual (it’s a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$:

$$\text{Tr}(\alpha'_i \alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise}. \end{cases}$$

Now choose a non-zero $z \in \mathbb{Z}$ such that $z \alpha'_i \in \mathcal{O}_K$ for all $i$. Let $\alpha \in \mathcal{O}_K$. Then $\alpha z \alpha'_i \in \mathcal{O}_K$ for all $i$ and hence $\text{Tr}(\alpha z \alpha'_i)$ is, too. Writing $\alpha = \sum_{i=1}^n a_i \alpha_i$ with $a_i \in \mathbb{Q}$ for all $i$, we have

$$\text{Tr}(\alpha z \alpha'_i) = z a_i \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$  This shows that

$$\mathcal{O}_K \subseteq z^{-1} \alpha_1 \mathbb{Z} \oplus \cdots \oplus z^{-1} \alpha_n \mathbb{Z}.$$
Since $K$ is isomorphic to its dual (it’s a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$:

$$\text{Tr}(\alpha'_i; \alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise}. \end{cases}$$

Now choose a non-zero $z \in \mathbb{Z}$ such that $z\alpha'_i \in \mathcal{O}_K$ for all $i$. Let $\alpha \in \mathcal{O}_K$. Then $\alpha z \alpha'_i \in \mathcal{O}_K$ for all $i$ and hence $\text{Tr}(\alpha z \alpha'_i)$ is, too. Writing $\alpha = \sum_{i=1}^n a_i \alpha_i$ with $a_i \in \mathbb{Q}$ for all $i$, we have

$$\text{Tr}(\alpha z \alpha'_i) = za_i \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}. \quad \text{This shows that} \quad \mathcal{O}_K \subseteq z^{-1} \alpha_1 \mathbb{Z} \oplus \cdots \oplus z^{-1} \alpha_n \mathbb{Z}. \quad \text{Finally, since } \mathbb{Z} \text{ is Noetherian and } \mathcal{O}_K \text{ is a } \mathbb{Z}-\text{submodule of a finitely generated } \mathbb{Z}-\text{module,}$$
Since $K$ is isomorphic to its dual (it’s a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$:

$$\text{Tr}(\alpha'_i; \alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise}. \end{cases}$$

Now choose a non-zero $z \in \mathbb{Z}$ such that $z\alpha'_i \in \mathfrak{O}_K$ for all $i$. Let $\alpha \in \mathfrak{O}_K$. Then $\alpha z \alpha'_i \in \mathfrak{O}_K$ for all $i$ and hence $\text{Tr}(\alpha z \alpha'_i)$ is, too. Writing $\alpha = \sum_{i=1}^n a_i \alpha_i$ with $a_i \in \mathbb{Q}$ for all $i$, we have

$$\text{Tr}(\alpha z \alpha'_i) = za_i \in \mathfrak{O}_K \cap \mathbb{Q} = \mathbb{Z}. \text{ This shows that } \mathfrak{O}_K \subseteq z^{-1}\alpha_1\mathbb{Z} \oplus \cdots \oplus z^{-1}\alpha_n\mathbb{Z}. \text{ Finally, since } \mathbb{Z} \text{ is Noetherian and } \mathfrak{O}_K \text{ is a } \mathbb{Z}-\text{submodule of a finitely generated } \mathbb{Z}-\text{module, it must be finitely generated as well.}$$
Since $K$ is isomorphic to its dual (it's a finite dimensional vector space over $\mathbb{Q}$) there is a dual basis $\alpha'_1, \ldots, \alpha'_n$:

$$\text{Tr}(\alpha'_i\alpha_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise}. \end{cases}$$

Now choose a non-zero $z \in \mathbb{Z}$ such that $z\alpha'_i \in \mathcal{O}_K$ for all $i$. Let $\alpha \in \mathcal{O}_K$. Then $\alpha z\alpha'_i \in \mathcal{O}_K$ for all $i$ and hence $\text{Tr}(\alpha z\alpha'_i)$ is, too. Writing $\alpha = \sum_{i=1}^n a_i \alpha_i$ with $a_i \in \mathbb{Q}$ for all $i$, we have

$$\text{Tr}(\alpha z\alpha'_i) = z a_i \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}.$$  

This shows that $\mathcal{O}_K \subseteq z^{-1} \alpha_1 \mathbb{Z} \oplus \cdots \oplus z^{-1} \alpha_n \mathbb{Z}$. Finally, since $\mathbb{Z}$ is Noetherian and $\mathcal{O}_K$ is a $\mathbb{Z}$-submodule of a finitely generated $\mathbb{Z}$-module, it must be finitely generated as well. Clearly the rank of $\mathcal{O}_K$ must be at least $n = [K : \mathbb{Q}]$ and no larger than $n$. 

We thus see that \( \mathcal{O}_K = \alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n \mathbb{Z} \) for some algebraic integers \( \alpha_1, \ldots, \alpha_n \).
We thus see that $\mathcal{O}_K = \alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n \mathbb{Z}$ for some algebraic integers $\alpha_1, \ldots, \alpha_n$.

In the case of quadratic extensions,
We thus see that $\mathcal{O}_K = \alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n \mathbb{Z}$ for some algebraic integers $\alpha_1, \ldots, \alpha_n$.

In the case of quadratic extensions, we may take $\alpha_i = \alpha^{i-1}$ for a particular $\alpha \in \mathcal{O}_K$. 
We thus see that $\mathcal{O}_K = \alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n \mathbb{Z}$ for some algebraic integers $\alpha_1, \ldots, \alpha_n$.

In the case of quadratic extensions, we may take $\alpha_i = \alpha^{i-1}$ for a particular $\alpha \in \mathcal{O}_K$, i.e., $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$.
We thus see that \( \mathcal{O}_K = \alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n \mathbb{Z} \) for some algebraic integers \( \alpha_1, \ldots, \alpha_n \).

In the case of quadratic extensions, we may take \( \alpha_i = \alpha^{i-1} \) for a particular \( \alpha \in \mathcal{O}_K \), i.e., \( \mathcal{O}_K = \mathbb{Z}[\alpha] \) for some \( \alpha \in \mathcal{O}_K \). It is a fact of life that this isn’t always the case.
We thus see that $\mathcal{O}_K = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}$ for some algebraic integers $\alpha_1, \ldots, \alpha_n$.

In the case of quadratic extensions, we may take $\alpha_i = \alpha^{i-1}$ for a particular $\alpha \in \mathcal{O}_K$, i.e., $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. It is a fact of life that this isn’t always the case. In other words, there are number fields $K$ where $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_K$. 
We thus see that $\mathcal{O}_K = \alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n \mathbb{Z}$ for some algebraic integers $\alpha_1, \ldots, \alpha_n$.

In the case of quadratic extensions, we may take $\alpha_i = \alpha^{i-1}$ for a particular $\alpha \in \mathcal{O}_K$, i.e., $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. It is a fact of life that this isn’t always the case. In other words, there are number fields $K$ where $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_K$. This even occurs in with degree 3,
We thus see that $\mathcal{O}_K = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}$ for some algebraic integers $\alpha_1, \ldots, \alpha_n$.

In the case of quadratic extensions, we may take $\alpha_i = \alpha^{i-1}$ for a particular $\alpha \in \mathcal{O}_K$, i.e., $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. It is a fact of life that this isn’t always the case. In other words, there are number fields $K$ where $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_K$. This even occurs in with degree 3, the soonest it could happen!
We thus see that $\mathcal{O}_K = \alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n \mathbb{Z}$ for some algebraic integers $\alpha_1, \ldots, \alpha_n$.

In the case of quadratic extensions, we may take $\alpha_i = \alpha^{i-1}$ for a particular $\alpha \in \mathcal{O}_K$, i.e., $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. It is a fact of life that *this isn’t always the case*. In other words, there are number fields $K$ where $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_K$. This even occurs in with degree 3, the soonest it could happen! This is just one of many technical obstacles faced by algebraic number theorists.
We thus see that $\mathcal{O}_K = \alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n \mathbb{Z}$ for some algebraic integers $\alpha_1, \ldots, \alpha_n$.

In the case of quadratic extensions, we may take $\alpha_i = \alpha^{i-1}$ for a particular $\alpha \in \mathcal{O}_K$, i.e., $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. It is a fact of life that this isn’t always the case. In other words, there are number fields $K$ where $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_K$. This even occurs in with degree 3, the soonest it could happen! This is just one of many technical obstacles faced by algebraic number theorists. We’ll see clever ways around this
We thus see that $\mathcal{O}_K = \alpha_1 \mathbb{Z} \oplus \cdots \oplus \alpha_n \mathbb{Z}$ for some algebraic integers $\alpha_1, \ldots, \alpha_n$.

In the case of quadratic extensions, we may take $\alpha_i = \alpha^{i-1}$ for a particular $\alpha \in \mathcal{O}_K$, i.e., $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. It is a fact of life that this isn’t always the case. In other words, there are number fields $K$ where $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_K$. This even occurs in with degree 3, the soonest it could happen! This is just one of many technical obstacles faced by algebraic number theorists. We’ll see clever ways around this (well, kind of)
We thus see that $O_K = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}$ for some algebraic integers $\alpha_1, \ldots, \alpha_n$.

In the case of quadratic extensions, we may take $\alpha_i = \alpha^{i-1}$ for a particular $\alpha \in O_K$, i.e., $O_K = \mathbb{Z}[\alpha]$ for some $\alpha \in O_K$. It is a fact of life that this isn't always the case. In other words, there are number fields $K$ where $O_K \neq \mathbb{Z}[\alpha]$ for all $\alpha \in O_K$. This even occurs in with degree 3, the soonest it could happen! This is just one of many technical obstacles faced by algebraic number theorists. We'll see clever ways around this (well, kind of) later on.