Math 361

February 3, 2023

Quiz comments

Proposition. (Division algorithm) Let K be a field, and let $f, g \in K[x]$ with $f \neq 0$. Then there exists $q, r \in K[x]$ such that

$$g = fq + r$$

where $0 \leq \deg(r) < \deg(f)$.

Quiz comments

Proposition. (Division algorithm) Let K be a field, and let $f, g \in K[x]$ with $f \neq 0$. Then there exists $q, r \in K[x]$ such that

$$g = fq + r$$

where $0 \leq \deg(r) < \deg(f)$.

Definition. Let L/K be a field extension. Then $\alpha \in L$ is *algebraic* over K if there exists a nonzero polynomial $f \in K[x]$ such that $f(\alpha) = 0$.

Today

- Review.
- Gauss's lemma.
- Ring of integers in a number field.
- Extended primitive element theorem
- Ring of integers in a quadratic extension.

Review

Let L/K be a field extension.

Review

Let L/K be a field extension.

- $\alpha \in L$ is *algebraic* over K is there exists a nonzero $f \in K[x]$ such that $f(\alpha) = 0$.

Review

Let L/K be a field extension.

- $\alpha \in L$ is *algebraic* over K is there exists a nonzero $f \in K[x]$ such that $f(\alpha) = 0$. If f is monic and irreducible, it is the minimal polynomial for α over K.

Review

Let L/K be a field extension.

- $\alpha \in L$ is *algebraic* over K is there exists a nonzero $f \in K[x]$ such that $f(\alpha) = 0$. If f is monic and irreducible, it is the minimal polynomial for α over K.
- $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$, in which case $K[\alpha] = K(\alpha)$.

Review

Let L/K be a field extension.

- $\alpha \in L$ is *algebraic* over K is there exists a nonzero $f \in K[x]$ such that $f(\alpha) = 0$. If f is monic and irreducible, it is the minimal polynomial for α over K.
- $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$, in which case $K[\alpha] = K(\alpha)$.
- L is an *algebraic extension* of K if every element of L is algebraic over K.

Review

Let L/K be a field extension.

- $\alpha \in L$ is *algebraic* over K is there exists a nonzero $f \in K[x]$ such that $f(\alpha) = 0$. If f is monic and irreducible, it is the minimal polynomial for α over K.
- $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$, in which case $K[\alpha] = K(\alpha)$.
- L is an *algebraic extension* of K if every element of L is algebraic over K.
- $[L : K] < \infty \Rightarrow L$ algebraic over K, and the dimension is the degree of the minimal polynomial.

Review

Let L/K be a field extension.

- $\alpha \in L$ is *algebraic* over K is there exists a nonzero $f \in K[x]$ such that $f(\alpha) = 0$. If f is monic and irreducible, it is the minimal polynomial for α over K.
- $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$, in which case $K[\alpha] = K(\alpha)$.
- L is an *algebraic extension* of K if every element of L is algebraic over K.
- $[L : K] < \infty \Rightarrow L$ algebraic over K, and the dimension is the degree of the minimal polynomial.
- *Algebraic numbers*: $\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$.

Review

Let L/K be a field extension.

- $\alpha \in L$ is *algebraic* over K is there exists a nonzero $f \in K[x]$ such that $f(\alpha) = 0$. If f is monic and irreducible, it is the minimal polynomial for α over K.
- $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$, in which case $K[\alpha] = K(\alpha)$.
- L is an *algebraic extension* of K if every element of L is algebraic over K.
- $[L : K] < \infty \Rightarrow L$ algebraic over K, and the dimension is the degree of the minimal polynomial.
- *Algebraic numbers*: $\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$. They form a subfield of $\mathbb{C}$.
- *Number field*: A subfield K of $\mathbb{C}$ that is finite over $\mathbb{Q}$.

Review

Let L/K be a field extension.

- $\alpha \in L$ is *algebraic* over K is there exists a nonzero $f \in K[x]$ such that $f(\alpha) = 0$. If f is monic and irreducible, it is the minimal polynomial for α over K.
- $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$, in which case $K[\alpha] = K(\alpha)$.
- L is an *algebraic extension* of K if every element of L is algebraic over K.
- $[L : K] < \infty \Rightarrow L$ algebraic over K, and the dimension is the degree of the minimal polynomial.
- *Algebraic numbers*: $\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$. They form a subfield of $\mathbb{C}$.
- *Number field*: A subfield K of $\mathbb{C}$ that is finite over $\mathbb{Q}$.
- If K is a number field, then $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$ for some algebraic number $\alpha \in K$.

Review: Integral elements

Definition. Let A and B be integral domains (rings with no zero divisors) with $A \subseteq B$.

Review: Integral elements

Definition. Let A and B be integral domains (rings with no zero divisors) with $A \subseteq B$. An element of $\alpha \in B$ is *integral over* A if

Review: Integral elements

Definition. Let A and B be integral domains (rings with no zero divisors) with $A \subseteq B$. An element of $\alpha \in B$ is *integral over* A if there exists a monic polynomial $p \in A[x]$ such that $p(\alpha) = 0$.

Review: Integral elements

Definition. Let A and B be integral domains (rings with no zero divisors) with $A \subseteq B$. An element of $\alpha \in B$ is *integral over* A if there exists a monic polynomial $p \in A[x]$ such that $p(\alpha) = 0$.

Theorem. Let A and B be domains with $A \subseteq B$, and let $\alpha \in B$. Then the following are equivalent.

Review: Integral elements

Definition. Let A and B be integral domains (rings with no zero divisors) with $A \subseteq B$. An element of $\alpha \in B$ is *integral over* A if there exists a monic polynomial $p \in A[x]$ such that $p(\alpha) = 0$.

Theorem. Let A and B be domains with $A \subseteq B$, and let $\alpha \in B$. Then the following are equivalent.

1. α is integral over A.

Review: Integral elements

Definition. Let A and B be integral domains (rings with no zero divisors) with $A \subseteq B$. An element of $\alpha \in B$ is *integral over* A if there exists a monic polynomial $p \in A[x]$ such that $p(\alpha) = 0$.

Theorem. Let A and B be domains with $A \subseteq B$, and let $\alpha \in B$. Then the following are equivalent.

1. α is integral over A.
2. $A[\alpha] := \{f(\alpha) : f \in A[x]\}$ is a finitely generated A-module.

Review: Integral elements

Definition. Let A and B be integral domains (rings with no zero divisors) with $A \subseteq B$. An element of $\alpha \in B$ is *integral over* A if there exists a monic polynomial $p \in A[x]$ such that $p(\alpha) = 0$.

Theorem. Let A and B be domains with $A \subseteq B$, and let $\alpha \in B$. Then the following are equivalent.

1. α is integral over A.
2. $A[\alpha] := \{f(\alpha) : f \in A[x]\}$ is a finitely generated A-module.
3. There exists a finitely generated A-module M in B such that $\alpha M \subseteq M$. (Here, $\alpha M = \{am : m \in M\}$).

Review: Integral elements

Definition. Let A and B be integral domains (rings with no zero divisors) with $A \subseteq B$. An element of $\alpha \in B$ is *integral over* A if there exists a monic polynomial $p \in A[x]$ such that $p(\alpha) = 0$.

Theorem. Let A and B be domains with $A \subseteq B$, and let $\alpha \in B$. Then the following are equivalent.

1. α is integral over A.
2. $A[\alpha] := \{f(\alpha) : f \in A[x]\}$ is a finitely generated A-module.
3. There exists a finitely generated A-module M in B such that $\alpha M \subseteq M$. (Here, $\alpha M = \{am : m \in M\}$).

Corollary. Let $A \subseteq B$ be domains. The set of elements of B that are integral over A forms a subring of B.

The algebraic integers

The *algebraic integers* are the elements of $\mathbb{C}$ that are integral over $\mathbb{Z}$:

$$\mathfrak{O} := \{\alpha \in \mathbb{C} : p(\alpha) = 0 \text{ for some monic } p \in \mathbb{Z}[x]\}.$$

The algebraic integers

The *algebraic integers* are the elements of $\mathbb{C}$ that are integral over $\mathbb{Z}$:

$$\mathfrak{O} := \{\alpha \in \mathbb{C} : p(\alpha) = 0 \text{ for some monic } p \in \mathbb{Z}[x]\}.$$

The algebraic integers form a subring of $\mathbb{C}$.

The algebraic integers

The *algebraic integers* are the elements of $\mathbb{C}$ that are integral over $\mathbb{Z}$:

$$\mathfrak{O} := \{\alpha \in \mathbb{C} : p(\alpha) = 0 \text{ for some monic } p \in \mathbb{Z}[x]\}.$$

The algebraic integers form a subring of $\mathbb{C}$.

Example. Since $\sqrt[3]{2}$ and i are algebraic integers,

The algebraic integers

The *algebraic integers* are the elements of $\mathbb{C}$ that are integral over $\mathbb{Z}$:

$$\mathfrak{O} := \{\alpha \in \mathbb{C} : p(\alpha) = 0 \text{ for some monic } p \in \mathbb{Z}[x]\}.$$

The algebraic integers form a subring of $\mathbb{C}$.

Example. Since $\sqrt[3]{2}$ and i are algebraic integers, there must be a monic $p \in \mathbb{Z}[x]$ such that $p(\sqrt[3]{2} + i) = 0$.

The algebraic integers

The *algebraic integers* are the elements of $\mathbb{C}$ that are integral over $\mathbb{Z}$:

$$\mathfrak{O} := \{\alpha \in \mathbb{C} : p(\alpha) = 0 \text{ for some monic } p \in \mathbb{Z}[x]\}.$$

The algebraic integers form a subring of $\mathbb{C}$.

Example. Since $\sqrt[3]{2}$ and i are algebraic integers, there must be a monic $p \in \mathbb{Z}[x]$ such that $p(\sqrt[3]{2} + i) = 0$. The determinant trick from last time, gives a method for calculating such a p.

Gauss's lemma

Let $f \in \mathbb{Z}[x]$. Gauss's lemma says the if f factors in $\mathbb{Q}[x]$, then it factors in $\mathbb{Z}[x]$.

Gauss's lemma

Let $f \in \mathbb{Z}[x]$. Gauss's lemma says the if f factors in $\mathbb{Q}[x]$, then it factors in $\mathbb{Z}[x]$.

In detail, suppose that $f = gh$ for $g, h \in \mathbb{Q}[x]$.

Gauss's lemma

Let $f \in \mathbb{Z}[x]$. Gauss's lemma says the if f factors in $\mathbb{Q}[x]$, then it factors in $\mathbb{Z}[x]$.

In detail, suppose that $f = gh$ for $g, h \in \mathbb{Q}[x]$. Then there exists a nonzero $\lambda \in \mathbb{Q}$ such that

$$\lambda g, \ \frac{1}{\lambda} h \in \mathbb{Z}[x].$$

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$)

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

$\alpha \in \mathfrak{O} \Rightarrow$ there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

$\alpha \in \mathfrak{O} \Rightarrow$ there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.
Therefore, α is algebraic over $\mathbb{Q}$ and has a minimal polynomial p.

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

$\alpha \in \mathfrak{O} \Rightarrow$ there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.
Therefore, α is algebraic over $\mathbb{Q}$ and has a minimal polynomial p.

Then $f(\alpha) = 0 \Rightarrow f = qp$ for some $q \in \mathbb{Q}[x]$.

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

$\alpha \in \mathfrak{O} \Rightarrow$ there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Therefore, α is algebraic over $\mathbb{Q}$ and has a minimal polynomial p.

Then $f(\alpha) = 0 \Rightarrow f = qp$ for some $q \in \mathbb{Q}[x]$. Since f and p are monic,

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

$\alpha \in \mathfrak{O} \Rightarrow$ there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. Therefore, α is algebraic over $\mathbb{Q}$ and has a minimal polynomial p.

Then $f(\alpha) = 0 \Rightarrow f = qp$ for some $q \in \mathbb{Q}[x]$. Since f and p are monic, so is q.

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

$\alpha \in \mathfrak{O} \Rightarrow$ there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.
Therefore, α is algebraic over $\mathbb{Q}$ and has a minimal polynomial p.

Then $f(\alpha) = 0 \Rightarrow f = qp$ for some $q \in \mathbb{Q}[x]$. Since f and p are monic, so is q.

Gauss's lemma implies there exist $\lambda \in \mathbb{Q}$ such that $\lambda q, \frac{1}{\lambda} p \in \mathbb{Z}[x]$.

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

$\alpha \in \mathfrak{O} \Rightarrow$ there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.
Therefore, α is algebraic over $\mathbb{Q}$ and has a minimal polynomial p.

Then $f(\alpha) = 0 \Rightarrow f = qp$ for some $q \in \mathbb{Q}[x]$. Since f and p are monic, so is q.

Gauss's lemma implies there exist $\lambda \in \mathbb{Q}$ such that $\lambda q, \frac{1}{\lambda} p \in \mathbb{Z}[x]$.

So $f = (\lambda q)\left(\frac{1}{\lambda} p\right)$.

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

$\alpha \in \mathfrak{O} \Rightarrow$ there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.
Therefore, α is algebraic over $\mathbb{Q}$ and has a minimal polynomial p.

Then $f(\alpha) = 0 \Rightarrow f = qp$ for some $q \in \mathbb{Q}[x]$. Since f and p are monic, so is q.

Gauss's lemma implies there exist $\lambda \in \mathbb{Q}$ such that $\lambda q, \frac{1}{\lambda} p \in \mathbb{Z}[x]$.

So $f = (\lambda q)\left(\frac{1}{\lambda} p\right)$.

Then $\lambda q \in \mathbb{Z}[x] \Rightarrow \lambda \in \mathbb{Z}$,

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

$\alpha \in \mathfrak{O} \Rightarrow$ there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.
Therefore, α is algebraic over $\mathbb{Q}$ and has a minimal polynomial p.

Then $f(\alpha) = 0 \Rightarrow f = qp$ for some $q \in \mathbb{Q}[x]$. Since f and p are monic, so is q.

Gauss's lemma implies there exist $\lambda \in \mathbb{Q}$ such that $\lambda q, \frac{1}{\lambda} p \in \mathbb{Z}[x]$.

So $f = (\lambda q)\left(\frac{1}{\lambda} p\right)$.

Then $\lambda q \in \mathbb{Z}[x] \Rightarrow \lambda \in \mathbb{Z}$, and $\frac{1}{\lambda} p \in \mathbb{Z}[x] \Rightarrow \frac{1}{\lambda} \in \mathbb{Z}$.

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

$\alpha \in \mathfrak{O} \Rightarrow$ there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.
Therefore, α is algebraic over $\mathbb{Q}$ and has a minimal polynomial p.

Then $f(\alpha) = 0 \Rightarrow f = qp$ for some $q \in \mathbb{Q}[x]$. Since f and p are monic, so is q.

Gauss's lemma implies there exist $\lambda \in \mathbb{Q}$ such that $\lambda q, \frac{1}{\lambda} p \in \mathbb{Z}[x]$.

So $f = (\lambda q)\left(\frac{1}{\lambda} p\right)$.

Then $\lambda q \in \mathbb{Z}[x] \Rightarrow \lambda \in \mathbb{Z}$, and $\frac{1}{\lambda} p \in \mathbb{Z}[x] \Rightarrow \frac{1}{\lambda} \in \mathbb{Z}$.

Therefore, $\lambda = \pm 1$.

Algebraic integers and minimal polynomials

Corollary. Let α be an algebraic number, i.e., a complex number that is algegraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Proof. ($\Leftarrow$) Duh.

($\Rightarrow$)

$\alpha \in \mathfrak{O} \Rightarrow$ there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.
Therefore, α is algebraic over $\mathbb{Q}$ and has a minimal polynomial p.

Then $f(\alpha) = 0 \Rightarrow f = qp$ for some $q \in \mathbb{Q}[x]$. Since f and p are monic, so is q.

Gauss's lemma implies there exist $\lambda \in \mathbb{Q}$ such that $\lambda q, \frac{1}{\lambda} p \in \mathbb{Z}[x]$.

So $f = (\lambda q)\left(\frac{1}{\lambda} p\right)$.

Then $\lambda q \in \mathbb{Z}[x] \Rightarrow \lambda \in \mathbb{Z}$, and $\frac{1}{\lambda} p \in \mathbb{Z}[x] \Rightarrow \frac{1}{\lambda} \in \mathbb{Z}$.
Therefore, $\lambda = \pm 1$. So $\frac{1}{\lambda} p = \pm p \in \mathbb{Z}[x]$, which implies $p \in \mathbb{Z}[x]$.$\square$

Another proof that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$

We just proved:

Another proof that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$

We just proved:

Corollary. A complex number α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

Another proof that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$

We just proved:

Corollary. A complex number α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

It follows that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$, i.e. a rational number that is integral over $\mathbb{Z}$ is an integer.

Another proof that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$

We just proved:

Corollary. A complex number α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

It follows that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$, i.e. a rational number that is integral over $\mathbb{Z}$ is an integer.

Proof. Certainly, $\mathbb{Z} \subseteq \mathfrak{O} \cap \mathbb{Q}$.

Another proof that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$

We just proved:

Corollary. A complex number α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

It follows that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$, i.e. a rational number that is integral over $\mathbb{Z}$ is an integer.

Proof. Certainly, $\mathbb{Z} \subseteq \mathfrak{O} \cap \mathbb{Q}$.

For the reverse inclusion, suppose that $a \in \mathfrak{O} \cap \mathbb{Q}$.

Another proof that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$

We just proved:

Corollary. A complex number α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

It follows that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$, i.e. a rational number that is integral over $\mathbb{Z}$ is an integer.

Proof. Certainly, $\mathbb{Z} \subseteq \mathfrak{O} \cap \mathbb{Q}$.

For the reverse inclusion, suppose that $a \in \mathfrak{O} \cap \mathbb{Q}$. The minimal polynomial for a over $\mathbb{Q}$ is $x - a$.

Another proof that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$

We just proved:

Corollary. A complex number α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

It follows that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$, i.e. a rational number that is integral over $\mathbb{Z}$ is an integer.

Proof. Certainly, $\mathbb{Z} \subseteq \mathfrak{O} \cap \mathbb{Q}$.

For the reverse inclusion, suppose that $a \in \mathfrak{O} \cap \mathbb{Q}$. The minimal polynomial for a over $\mathbb{Q}$ is $x - a$. By the Corollary, $x - a \in \mathbb{Z}[x]$.

Another proof that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$

We just proved:

Corollary. A complex number α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.

It follows that $\mathfrak{O} \cap \mathbb{Q} = \mathbb{Z}$, i.e. a rational number that is integral over $\mathbb{Z}$ is an integer.

Proof. Certainly, $\mathbb{Z} \subseteq \mathfrak{O} \cap \mathbb{Q}$.

For the reverse inclusion, suppose that $a \in \mathfrak{O} \cap \mathbb{Q}$. The minimal polynomial for a over $\mathbb{Q}$ is $x - a$. By the Corollary, $x - a \in \mathbb{Z}[x]$. In particular, $a \in \mathbb{Z}$. $\square$

Ring of integers in a number field

Let K be a *number field*:

Ring of integers in a number field

Let K be a *number field*: a finite field extension of $\mathbb{Q}$ in $\mathbb{C}$.

Ring of integers in a number field

Let K be a *number field*: a finite field extension of $\mathbb{Q}$ in $\mathbb{C}$.

Definition. The *ring of integers in* K is

$$\mathfrak{O}_K = \mathfrak{O} \cap K,$$

the algebraic integers lying in K.

Ring of integers in a number field

Let K be a *number field*: a finite field extension of $\mathbb{Q}$ in $\mathbb{C}$.

Definition. The *ring of integers in* K is

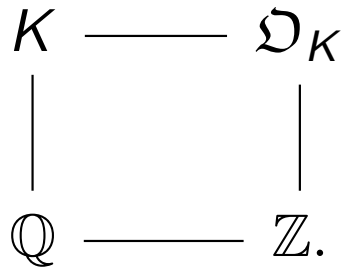
$$\mathfrak{O}_K = \mathfrak{O} \cap K,$$

the algebraic integers lying in K.

$$\begin{array}{ccc} K & \text{——} & \mathfrak{O}_K \\ | & & | \\ \mathbb{Q} & \text{——} & \mathbb{Z}. \end{array}$$

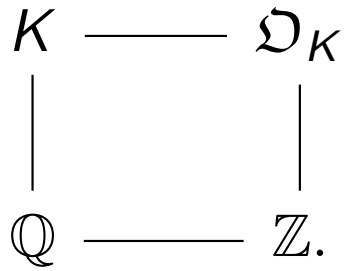
Extended primitive element theorem

$[K : \mathbb{Q}] < \infty$



Extended primitive element theorem

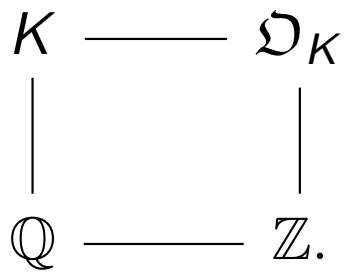
$[K : \mathbb{Q}] < \infty$



Lemma. If $\alpha \in K$, then there exists $c \in \mathbb{Z}$ such that $c\alpha \in \mathfrak{O}_K$.

Extended primitive element theorem

$[K : \mathbb{Q}] < \infty$

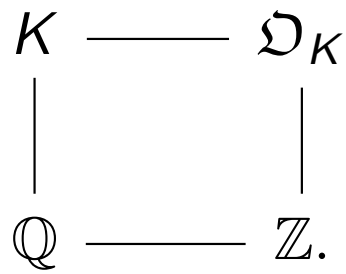


Lemma. If $\alpha \in K$, then there exists $c \in \mathbb{Z}$ such that $c\alpha \in \mathfrak{O}_K$.

Proof. HW.

Extended primitive element theorem

$[K : \mathbb{Q}] < \infty$



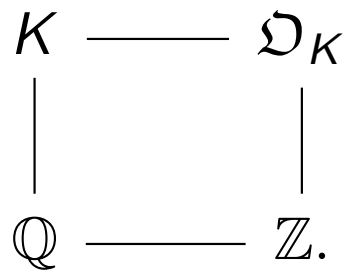
Lemma. If $\alpha \in K$, then there exists $c \in \mathbb{Z}$ such that $c\alpha \in \mathfrak{O}_K$.

Proof. HW.

Extended primitive element theorem. Let K be a number field. Then there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$.

Extended primitive element theorem

$[K : \mathbb{Q}] < \infty$



Lemma. If $\alpha \in K$, then there exists $c \in \mathbb{Z}$ such that $c\alpha \in \mathfrak{O}_K$.

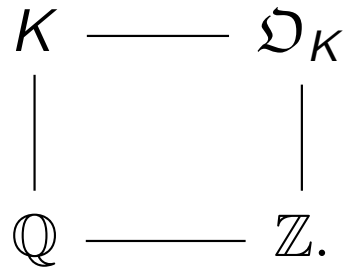
Proof. HW.

Extended primitive element theorem. Let K be a number field. Then there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$.

Proof. The ordinary primitive element theorem gives us $\alpha \in K$ such that $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.

Extended primitive element theorem

$[K : \mathbb{Q}] < \infty$



Lemma. If $\alpha \in K$, then there exists $c \in \mathbb{Z}$ such that $c\alpha \in \mathfrak{O}_K$.

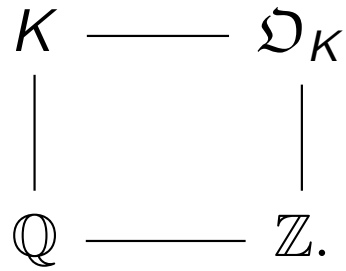
Proof. HW.

Extended primitive element theorem. Let K be a number field. Then there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$.

Proof. The ordinary primitive element theorem gives us $\alpha \in K$ such that $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$. By the Lemma, there exists $c \in \mathbb{Z}$ such that $\theta := c\alpha \in \mathfrak{O}_K$.

Extended primitive element theorem

$[K : \mathbb{Q}] < \infty$



Lemma. If $\alpha \in K$, then there exists $c \in \mathbb{Z}$ such that $c\alpha \in \mathfrak{O}_K$.

Proof. HW.

Extended primitive element theorem. Let K be a number field. Then there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta) = \mathbb{Q}[\theta]$.

Proof. The ordinary primitive element theorem gives us $\alpha \in K$ such that $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$. By the Lemma, there exists $c \in \mathbb{Z}$ such that $\theta := c\alpha \in \mathfrak{O}_K$.

Then $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ and $K = \mathbb{Q}[\alpha] = \mathbb{Q}[\theta]$. $\square$

Quadratic number fields

Suppose K is a number field with $[K : \mathbb{Q}] = 2$.

Quadratic number fields

Suppose K is a number field with $[K : \mathbb{Q}] = 2$. **Goal.** Find the ring of integers in K.

Quadratic number fields

Suppose K is a number field with $[K : \mathbb{Q}] = 2$. **Goal.** Find the ring of integers in K.

By the PET, there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta)$.

Quadratic number fields

Suppose K is a number field with $[K : \mathbb{Q}] = 2$. **Goal.** Find the ring of integers in K.

By the PET, there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta)$.

Minimal polynomial for θ: $p = x^2 + mx + n \in \mathbb{Z}[x]$.

Quadratic number fields

Suppose K is a number field with $[K : \mathbb{Q}] = 2$. **Goal.** Find the ring of integers in K.

By the PET, there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta)$.

Minimal polynomial for θ: $p = x^2 + mx + n \in \mathbb{Z}[x]$. So

$$\theta = \frac{-m \pm \sqrt{m^2 - 4n}}{2}.$$

Quadratic number fields

Suppose K is a number field with $[K : \mathbb{Q}] = 2$. **Goal.** Find the ring of integers in K.

By the PET, there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta)$.

Minimal polynomial for θ: $p = x^2 + mx + n \in \mathbb{Z}[x]$. So

$$\theta = \frac{-m \pm \sqrt{m^2 - 4n}}{2}.$$

Let $m^2 - 4n = r^2 d$ for $r, d \in \mathbb{Z}$ with d squarefree.

Quadratic number fields

Suppose K is a number field with $[K : \mathbb{Q}] = 2$. **Goal.** Find the ring of integers in K.

By the PET, there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta)$.

Minimal polynomial for θ: $p = x^2 + mx + n \in \mathbb{Z}[x]$. So

$$\theta = \frac{-m \pm \sqrt{m^2 - 4n}}{2}.$$

Let $m^2 - 4n = r^2 d$ for $r, d \in \mathbb{Z}$ with d squarefree. Since $\theta \notin \mathbb{Z}$, we have $d \neq 0, 1$.

Quadratic number fields

Suppose K is a number field with $[K : \mathbb{Q}] = 2$. **Goal.** Find the ring of integers in K.

By the PET, there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta)$.

Minimal polynomial for θ: $p = x^2 + mx + n \in \mathbb{Z}[x]$. So

$$\theta = \frac{-m \pm \sqrt{m^2 - 4n}}{2}.$$

Let $m^2 - 4n = r^2 d$ for $r, d \in \mathbb{Z}$ with d squarefree. Since $\theta \notin \mathbb{Z}$, we have $d \neq 0, 1$. So $\theta = \frac{-m \pm r\sqrt{d}}{2}$,

Quadratic number fields

Suppose K is a number field with $[K : \mathbb{Q}] = 2$. **Goal.** Find the ring of integers in K.

By the PET, there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta)$.

Minimal polynomial for θ: $p = x^2 + mx + n \in \mathbb{Z}[x]$. So

$$\theta = \frac{-m \pm \sqrt{m^2 - 4n}}{2}.$$

Let $m^2 - 4n = r^2 d$ for $r, d \in \mathbb{Z}$ with d squarefree. Since $\theta \notin \mathbb{Z}$, we have $d \neq 0, 1$. So $\theta = \frac{-m \pm r\sqrt{d}}{2}$, and

$$K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$$

Quadratic number fields

Suppose K is a number field with $[K : \mathbb{Q}] = 2$. **Goal.** Find the ring of integers in K.

By the PET, there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta)$.

Minimal polynomial for θ: $p = x^2 + mx + n \in \mathbb{Z}[x]$. So

$$\theta = \frac{-m \pm \sqrt{m^2 - 4n}}{2}.$$

Let $m^2 - 4n = r^2 d$ for $r, d \in \mathbb{Z}$ with d squarefree. Since $\theta \notin \mathbb{Z}$, we have $d \neq 0, 1$. So $\theta = \frac{-m \pm r\sqrt{d}}{2}$, and

$$K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$$

Quadratic number fields

Suppose K is a number field with $[K:\mathbb{Q}] = 2$. **Goal.** Find the ring of integers in K.

By the PET, there exists $\theta \in \mathfrak{O}_K$ such that $K = \mathbb{Q}(\theta)$.

Minimal polynomial for θ: $p = x^2 + mx + n \in \mathbb{Z}[x]$. So

$$\theta = \frac{-m \pm \sqrt{m^2 - 4n}}{2}.$$

Let $m^2 - 4n = r^2 d$ for $r, d \in \mathbb{Z}$ with d squarefree. Since $\theta \notin \mathbb{Z}$, we have $d \neq 0, 1$. So $\theta = \frac{-m \pm r\sqrt{d}}{2}$, and

$$K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}] = \mathrm{Span}_{\mathbb{Q}}\{1, \sqrt{d}\}.$$

Quadratic number fields

Let $\alpha \in K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$.

Quadratic number fields

Let $\alpha \in K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$. **Goal:** Determine when $\alpha \in \mathfrak{O}_K$.

Quadratic number fields

Let $\alpha \in K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$. **Goal:** Determine when $\alpha \in \mathfrak{O}_K$.

We have $\alpha = s + t\sqrt{d}$ with $s, t \in \mathbb{Q}$.

Quadratic number fields

Let $\alpha \in K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$. **Goal:** Determine when $\alpha \in \mathfrak{O}_K$.

We have $\alpha = s + t\sqrt{d}$ with $s, t \in \mathbb{Q}$. So there exists a, b, c not sharing a prime factor and such that

$$\alpha = \frac{a + b\sqrt{d}}{c}.$$

Quadratic number fields

Let $\alpha \in K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$. **Goal:** Determine when $\alpha \in \mathfrak{O}_K$.

We have $\alpha = s + t\sqrt{d}$ with $s, t \in \mathbb{Q}$. So there exists a, b, c not sharing a prime factor and such that

$$\alpha = \frac{a + b\sqrt{d}}{c}.$$

If $b = 0$, then $\alpha = \frac{a}{c} \in \mathbb{Q}$.

Quadratic number fields

Let $\alpha \in K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$. **Goal:** Determine when $\alpha \in \mathfrak{O}_K$.

We have $\alpha = s + t\sqrt{d}$ with $s, t \in \mathbb{Q}$. So there exists a, b, c not sharing a prime factor and such that

$$\alpha = \frac{a + b\sqrt{d}}{c}.$$

If $b = 0$, then $\alpha = \frac{a}{c} \in \mathbb{Q}$. If $\alpha \in \mathfrak{O}_K$, then $\alpha \in \mathfrak{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

Quadratic number fields

Let $\alpha \in K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$. **Goal:** Determine when $\alpha \in \mathfrak{O}_K$.

We have $\alpha = s + t\sqrt{d}$ with $s, t \in \mathbb{Q}$. So there exists a, b, c not sharing a prime factor and such that

$$\alpha = \frac{a + b\sqrt{d}}{c}.$$

If $b = 0$, then $\alpha = \frac{a}{c} \in \mathbb{Q}$. If $\alpha \in \mathfrak{O}_K$, then $\alpha \in \mathfrak{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

So one possibility is $\alpha \in \mathbb{Z}$, but we already know $\mathbb{Z} \subset \mathfrak{O}_K$.

Quadratic number fields

Let $\alpha \in K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[\sqrt{d}]$. **Goal:** Determine when $\alpha \in \mathfrak{O}_K$.

We have $\alpha = s + t\sqrt{d}$ with $s, t \in \mathbb{Q}$. So there exists a, b, c not sharing a prime factor and such that

$$\alpha = \frac{a + b\sqrt{d}}{c}.$$

If $b = 0$, then $\alpha = \frac{a}{c} \in \mathbb{Q}$. If $\alpha \in \mathfrak{O}_K$, then $\alpha \in \mathfrak{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

So one possibility is $\alpha \in \mathbb{Z}$, but we already know $\mathbb{Z} \subset \mathfrak{O}_K$.

From now on, suppose that $b \neq 0$.

Quadratic number fields

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

Quadratic number fields

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

The minimal polynomial for α over $\mathbb{Q}$ is

Quadratic number fields

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

The minimal polynomial for α over $\mathbb{Q}$ is

$$p(x) = \left(x - \frac{a + b\sqrt{d}}{c}\right)\left(x - \frac{a - b\sqrt{d}}{c}\right)$$

Quadratic number fields

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

The minimal polynomial for α over $\mathbb{Q}$ is

$$p(x) = \left(x - \frac{a + b\sqrt{d}}{c}\right)\left(x - \frac{a - b\sqrt{d}}{c}\right) = x^2 - \frac{2a}{c}x + \frac{a^2 - b^2 d}{c^2} \in \mathbb{Q}[x]$$

Quadratic number fields

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

The minimal polynomial for α over $\mathbb{Q}$ is

$$p(x) = \left(x - \frac{a + b\sqrt{d}}{c}\right)\left(x - \frac{a - b\sqrt{d}}{c}\right) = x^2 - \frac{2a}{c}x + \frac{a^2 - b^2 d}{c^2} \in \mathbb{Q}[x]$$

So $\alpha \in \mathfrak{O}_K$ exactly when

Quadratic number fields

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

The minimal polynomial for α over $\mathbb{Q}$ is

$$p(x) = \left(x - \frac{a + b\sqrt{d}}{c}\right)\left(x - \frac{a - b\sqrt{d}}{c}\right) = x^2 - \frac{2a}{c}x + \frac{a^2 - b^2 d}{c^2} \in \mathbb{Q}[x]$$

So $\alpha \in \mathfrak{O}_K$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Quadratic number fields

Summary: $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Quadratic number fields

Summary: $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Our problem is reduced to finding a, b, c satisfying the above.

Quadratic number fields

Summary: $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Our problem is reduced to finding a, b, c satisfying the above.

Let $q \neq 2$ be a prime integer factor of c.

Quadratic number fields

Summary: $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Our problem is reduced to finding a, b, c satisfying the above.

Let $q \neq 2$ be a prime integer factor of c.

Then $c|(2a) \Rightarrow q|(2a) \Rightarrow$

Quadratic number fields

Summary: $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Our problem is reduced to finding a, b, c satisfying the above.

Let $q \neq 2$ be a prime integer factor of c.

Then $c|(2a) \Rightarrow q|(2a) \Rightarrow q|a \Rightarrow q^2|a^2$

Quadratic number fields

Summary: $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Our problem is reduced to finding a, b, c satisfying the above.

Let $q \neq 2$ be a prime integer factor of c.

Then $c|(2a) \Rightarrow q|(2a) \Rightarrow q|a \Rightarrow q^2|a^2$

and $c^2|(a^2 - b^2 d) \Rightarrow q^2|(a^2 - b^2 d)$

Quadratic number fields

Summary: $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Our problem is reduced to finding a, b, c satisfying the above.

Let $q \neq 2$ be a prime integer factor of c.

Then $c|(2a) \Rightarrow q|(2a) \Rightarrow q|a \Rightarrow q^2|a^2$

and $c^2|(a^2 - b^2 d) \Rightarrow q^2|(a^2 - b^2 d) \Rightarrow q^2|(b^2 d)$

Quadratic number fields

Summary: $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Our problem is reduced to finding a, b, c satisfying the above.

Let $q \neq 2$ be a prime integer factor of c.

Then $c|(2a) \Rightarrow q|(2a) \Rightarrow q|a \Rightarrow q^2|a^2$

and $c^2|(a^2 - b^2 d) \Rightarrow q^2|(a^2 - b^2 d) \Rightarrow q^2|(b^2 d) \Rightarrow q|b$.

Quadratic number fields

Summary: $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Our problem is reduced to finding a, b, c satisfying the above.

Let $q \neq 2$ be a prime integer factor of c.

Then $c|(2a) \Rightarrow q|(2a) \Rightarrow q|a \Rightarrow q^2|a^2$

and $c^2|(a^2 - b^2 d) \Rightarrow q^2|(a^2 - b^2 d) \Rightarrow q^2|(b^2 d) \Rightarrow q|b$.

We have shown that a, b, c share a factor of q in this case,

Quadratic number fields

Summary: $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Our problem is reduced to finding a, b, c satisfying the above.

Let $q \neq 2$ be a prime integer factor of c.

Then $c|(2a) \Rightarrow q|(2a) \Rightarrow q|a \Rightarrow q^2|a^2$

and $c^2|(a^2 - b^2 d) \Rightarrow q^2|(a^2 - b^2 d) \Rightarrow q^2|(b^2 d) \Rightarrow q|b$.

We have shown that a, b, c share a factor of q in this case, but we have selected a, b, c not sharing any prime factors.

Quadratic number fields

Summary: $\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}.$$

Our problem is reduced to finding a, b, c satisfying the above.

Let $q \neq 2$ be a prime integer factor of c.

Then $c|(2a) \Rightarrow q|(2a) \Rightarrow q|a \Rightarrow q^2|a^2$

and $c^2|(a^2 - b^2 d) \Rightarrow q^2|(a^2 - b^2 d) \Rightarrow q^2|(b^2 d) \Rightarrow q|b$.

We have shown that a, b, c share a factor of q in this case, but we have selected a, b, c not sharing any prime factors.

Thus, we know c is a power of 2.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is a power of 2.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is a power of 2.

If $4|c$, then $4|(2a) \Rightarrow 2|a$

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is a power of 2.

If $4|c$, then $4|(2a) \Rightarrow 2|a \Rightarrow 2^2|a^2$

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is a power of 2.

If $4|c$, then $4|(2a) \Rightarrow 2|a \Rightarrow 2^2|a^2$ and $2^2|(a^2 - b^2 d)$

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is a power of 2.

If $4|c$, then $4|(2a) \Rightarrow 2|a \Rightarrow 2^2|a^2$ and $2^2|(a^2 - b^2 d) \Rightarrow 2|b$.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is a power of 2.

If $4|c$, then $4|(2a) \Rightarrow 2|a \Rightarrow 2^2|a^2$ and $2^2|(a^2 - b^2 d) \Rightarrow 2|b$.

So a, b, c share a factor of 2,

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is a power of 2.

If $4|c$, then $4|(2a) \Rightarrow 2|a \Rightarrow 2^2|a^2$ and $2^2|(a^2 - b^2 d) \Rightarrow 2|b$.

So a, b, c share a factor of 2, but they don't.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is a power of 2.

If $4|c$, then $4|(2a) \Rightarrow 2|a \Rightarrow 2^2|a^2$ and $2^2|(a^2 - b^2 d) \Rightarrow 2|b$.

So a, b, c share a factor of 2, but they don't.

So $c = 1$ or 2.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is 1 or 2.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is 1 or 2.

If $c = 1$, the equations are satisfied and $\alpha = a + b\sqrt{d} \in \mathfrak{O}_K$.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is 1 or 2.

If $c = 1$, the equations are satisfied and $\alpha = a + b\sqrt{d} \in \mathfrak{O}_K$.

This shows that

$$\mathbb{Z}[\sqrt{d}] \subseteq \mathfrak{O}_K.$$

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

and c is 1 or 2.

If $c = 1$, the equations are satisfied and $\alpha = a + b\sqrt{d} \in \mathfrak{O}_K$.

This shows that

$$\mathbb{Z}[\sqrt{d}] \subseteq \mathfrak{O}_K.$$

That leaves the case $c = 2$ to consider.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

If $c = 2$, the conditions become

$$a \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{4} \in \mathbb{Z}.$$

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{c} \in \mathfrak{O}$ exactly when

$$\frac{2a}{c} \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{c^2} \in \mathbb{Z},$$

If $c = 2$, the conditions become

$$a \in \mathbb{Z} \quad \text{and} \quad \frac{a^2 - b^2 d}{4} \in \mathbb{Z}.$$

Since $a \in \mathbb{Z}$, the condition becomes $\frac{a^2 - b^2 d}{4} \in \mathbb{Z}$.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{2} \in \mathfrak{O}$ if and only if

$$\frac{a^2 - b^2 d}{4} \in \mathbb{Z},$$

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{2} \in \mathfrak{O}$ if and only if

$$\frac{a^2 - b^2 d}{4} \in \mathbb{Z},$$

i.e., if and only if $a^2 - b^2 d = 0 \bmod 4$.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{2} \in \mathfrak{O}$ if and only if

$$\frac{a^2 - b^2 d}{4} \in \mathbb{Z},$$

i.e., if and only if $a^2 - b^2 d = 0 \bmod 4$.

Why must a and b both be odd?

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{2} \in \mathfrak{O}$ if and only if

$$\frac{a^2 - b^2 d}{4} \in \mathbb{Z},$$

i.e., if and only if $a^2 - b^2 d = 0 \bmod 4$.

Why must a and b both be odd? Answer: If either is even, the other is even and thus a, b, c share a prime factor.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{2} \in \mathfrak{O}$ if and only if

$$\frac{a^2 - b^2 d}{4} \in \mathbb{Z},$$

i.e., if and only if $a^2 - b^2 d = 0 \bmod 4$.

Why must a and b both be odd? Answer: If either is even, the other is even and thus a, b, c share a prime factor. So a and b are odd.

Quadratic number fields

$\alpha = \frac{a+b\sqrt{d}}{2} \in \mathfrak{O}$ if and only if

$$\frac{a^2 - b^2 d}{4} \in \mathbb{Z},$$

i.e., if and only if $a^2 - b^2 d = 0 \bmod 4$.

Why must a and b both be odd? Answer: If either is even, the other is even and thus a, b, c share a prime factor. So a and b are odd.

In this case, $a^2 = b^2 = 1 \bmod 4$, and

$$a^2 - b^2 d = 1 - d = 0 \bmod 4.$$

So $d = 1 \bmod 4$.

Quadratic number fields

Summary so far:

Quadratic number fields

Summary so far:

- If $d \neq 1 \bmod 4$, we have $\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}]$.

Quadratic number fields

Summary so far:

- If $d \neq 1 \bmod 4$, we have $\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}]$.
- If $d = 1 \bmod 4$, we have, in addition to $\mathbb{Z}[\sqrt{d}] \subset \mathfrak{O}_K$, the elements $\frac{a+b\sqrt{d}}{2} \in \mathfrak{O}_K$ when a and b are both odd integers.

Quadratic number fields

Summary so far:

- If $d \neq 1 \bmod 4$, we have $\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}]$.
- If $d = 1 \bmod 4$, we have, in addition to $\mathbb{Z}[\sqrt{d}] \subset \mathfrak{O}_K$, the elements $\frac{a+b\sqrt{d}}{2} \in \mathfrak{O}_K$ when a and b are both odd integers.

We claim that if $d = 1 \bmod 4$, then $\mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Quadratic number fields

Summary so far:

- If $d \neq 1 \bmod 4$, we have $\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}]$.
- If $d = 1 \bmod 4$, we have, in addition to $\mathbb{Z}[\sqrt{d}] \subset \mathfrak{O}_K$, the elements $\frac{a+b\sqrt{d}}{2} \in \mathfrak{O}_K$ when a and b are both odd integers.

We claim that if $d = 1 \bmod 4$, then $\mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Proof. First, note that $\frac{1+\sqrt{d}}{2} \in \mathfrak{O}_K$. So $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathfrak{O}_K$.

Quadratic number fields

Summary so far:

- If $d \neq 1 \bmod 4$, we have $\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}]$.
- If $d = 1 \bmod 4$, we have, in addition to $\mathbb{Z}[\sqrt{d}] \subset \mathfrak{O}_K$, the elements $\frac{a+b\sqrt{d}}{2} \in \mathfrak{O}_K$ when a and b are both odd integers.

We claim that if $d = 1 \bmod 4$, then $\mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Proof. First, note that $\frac{1+\sqrt{d}}{2} \in \mathfrak{O}_K$. So $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathfrak{O}_K$. Then check $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$:

Quadratic number fields

Summary so far:

- If $d \neq 1 \bmod 4$, we have $\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}]$.
- If $d = 1 \bmod 4$, we have, in addition to $\mathbb{Z}[\sqrt{d}] \subset \mathfrak{O}_K$, the elements $\frac{a+b\sqrt{d}}{2} \in \mathfrak{O}_K$ when a and b are both odd integers.

We claim that if $d = 1 \bmod 4$, then $\mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Proof. First, note that $\frac{1+\sqrt{d}}{2} \in \mathfrak{O}_K$. So $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathfrak{O}_K$. Then check $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$:

$\alpha = a + b\sqrt{d} = (a-b) + 2b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$

Quadratic number fields

Summary so far:

- If $d \neq 1 \bmod 4$, we have $\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}]$.
- If $d = 1 \bmod 4$, we have, in addition to $\mathbb{Z}[\sqrt{d}] \subset \mathfrak{O}_K$, the elements $\frac{a+b\sqrt{d}}{2} \in \mathfrak{O}_K$ when a and b are both odd integers.

We claim that if $d = 1 \bmod 4$, then $\mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Proof. First, note that $\frac{1+\sqrt{d}}{2} \in \mathfrak{O}_K$. So $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathfrak{O}_K$. Then check $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$:

$$\alpha = a + b\sqrt{d} = (a-b) + 2b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$$

If a and b are odd, then

Quadratic number fields

Summary so far:

- If $d \neq 1 \bmod 4$, we have $\mathfrak{O}_K = \mathbb{Z}[\sqrt{d}]$.
- If $d = 1 \bmod 4$, we have, in addition to $\mathbb{Z}[\sqrt{d}] \subset \mathfrak{O}_K$, the elements $\frac{a+b\sqrt{d}}{2} \in \mathfrak{O}_K$ when a and b are both odd integers.

We claim that if $d = 1 \bmod 4$, then $\mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Proof. First, note that $\frac{1+\sqrt{d}}{2} \in \mathfrak{O}_K$. So $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subseteq \mathfrak{O}_K$. Then check $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$:

$$\alpha = a + b\sqrt{d} = (a-b) + 2b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$$

If a and b are odd, then

$$\alpha = \frac{a+b\sqrt{d}}{2} = \left(\frac{a-b}{2}\right) + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}].$$

Quadratic number fields

Theorem. Let K be a field extension of $\mathbb{Q}$ with $[K:\mathbb{Q}] = 2$. Then $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is a square-free integer. Its ring of integers is

$$\mathfrak{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \neq 1 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d = 1 \bmod 4. \end{cases}$$

Quadratic number fields

Theorem. Let K be a field extension of $\mathbb{Q}$ with $[K:\mathbb{Q}] = 2$. Then $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is a square-free integer. Its ring of integers is

$$\mathfrak{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \neq 1 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d = 1 \bmod 4. \end{cases}$$

We have

$$\mathbb{Z}[\sqrt{d}] = \mathrm{Span}_{\mathbb{Z}}\{1, \sqrt{d}\} \quad \text{and} \quad \mathbb{Z}[\tfrac{1+\sqrt{d}}{2}] = \mathrm{Span}_{\mathbb{Z}}\{1, \tfrac{1+\sqrt{d}}{2}\}.$$

Quadratic number fields

Theorem. Let K be a field extension of $\mathbb{Q}$ with $[K:\mathbb{Q}] = 2$. Then $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is a square-free integer. Its ring of integers is

$$\mathfrak{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \neq 1 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d = 1 \bmod 4. \end{cases}$$

We have

$$\mathbb{Z}[\sqrt{d}] = \mathrm{Span}_{\mathbb{Z}}\{1, \sqrt{d}\} \quad \text{and} \quad \mathbb{Z}[\tfrac{1+\sqrt{d}}{2}] = \mathrm{Span}_{\mathbb{Z}}\{1, \tfrac{1+\sqrt{d}}{2}\}.$$

Example. If $K = \mathbb{Q}(\sqrt{5})$, then $\mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Quadratic number fields

Theorem. Let K be a field extension of $\mathbb{Q}$ with $[K:\mathbb{Q}] = 2$. Then $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 0, 1$ is a square-free integer. Its ring of integers is

$$\mathfrak{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \neq 1 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d = 1 \bmod 4. \end{cases}$$

We have

$$\mathbb{Z}[\sqrt{d}] = \mathrm{Span}_{\mathbb{Z}}\{1, \sqrt{d}\} \quad \text{and} \quad \mathbb{Z}[\tfrac{1+\sqrt{d}}{2}] = \mathrm{Span}_{\mathbb{Z}}\{1, \tfrac{1+\sqrt{d}}{2}\}.$$

Example. If $K = \mathbb{Q}(\sqrt{5})$, then $\mathfrak{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. On the other hand, $\mathfrak{O}_{\mathbb{Q}(\sqrt{7})} = \mathbb{Z}[\sqrt{7}]$.