Math 361

February 1, 2023

Quiz

1. Let K be a field. State the *division algorithm* for $K[x]$.
2. Let L/K be a field extension. What does it mean to say $\alpha \in L$ is *algebraic* over K.
3. Let L/K be a field extension, and suppose that $\alpha \in L$ is algebraic over K. What is the definition of the *minimal polynomial* for α over K?

Today

- Module discussion from last time.
- Algorithm for finding the minimal polynomial.
- Integral elements in an extension of rings.

Algorithm for finding minimal polynomial

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Then, the degree of the minimal polynomial is the smallest d such that $1, \alpha, \alpha^2, \cdots, \alpha^d$ are K-linearly dependent.

Algorithm for finding minimal polynomial

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Then, the degree of the minimal polynomial is the smallest d such that $1, \alpha, \alpha^2, \cdots, \alpha^d$ are K-linearly dependent. For that d, the minimal polynomial may be derived from the dependency relation.

Algorithm for finding minimal polynomial

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Then, the degree of the minimal polynomial is the smallest d such that $1, \alpha, \alpha^2, \cdots, \alpha^d$ are K-linearly dependent. For that d, the minimal polynomial may be derived from the dependency relation.

Example. Consider $i \in \mathbb{C}/\mathbb{Q}$.

Algorithm for finding minimal polynomial

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Then, the degree of the minimal polynomial is the smallest d such that $1, \alpha, \alpha^2, \cdots, \alpha^d$ are K-linearly dependent. For that d, the minimal polynomial may be derived from the dependency relation.

Example. Consider $i \in \mathbb{C}/\mathbb{Q}$. We have that 1 and i are linearly independent over $\mathbb{Q}$,

Algorithm for finding minimal polynomial

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Then, the degree of the minimal polynomial is the smallest d such that $1, \alpha, \alpha^2, \cdots, \alpha^d$ are K-linearly dependent. For that d, the minimal polynomial may be derived from the dependency relation.

Example. Consider $i \in \mathbb{C}/\mathbb{Q}$. We have that 1 and i are linearly independent over $\mathbb{Q}$, but 1, i, and i^2 are dependent:

Algorithm for finding minimal polynomial

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Then, the degree of the minimal polynomial is the smallest d such that $1, \alpha, \alpha^2, \cdots, \alpha^d$ are K-linearly dependent. For that d, the minimal polynomial may be derived from the dependency relation.

Example. Consider $i \in \mathbb{C}/\mathbb{Q}$. We have that 1 and i are linearly independent over $\mathbb{Q}$, but 1, i, and i^2 are dependent:

$$1(1) + 0(i) + 1(i^2) = 0.$$

Algorithm for finding minimal polynomial

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Then, the degree of the minimal polynomial is the smallest d such that $1, \alpha, \alpha^2, \cdots, \alpha^d$ are K-linearly dependent. For that d, the minimal polynomial may be derived from the dependency relation.

Example. Consider $i \in \mathbb{C}/\mathbb{Q}$. We have that 1 and i are linearly independent over $\mathbb{Q}$, but 1, i, and i^2 are dependent:

$$1(1) + 0(i) + 1(i^2) = 0.$$

Let

$$p(x) = 1 \cdot 1 + 0 \cdot x + 1 \cdot x^2 = 1 + x^2.$$

Algorithm for finding minimal polynomial

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Then, the degree of the minimal polynomial is the smallest d such that $1, \alpha, \alpha^2, \cdots, \alpha^d$ are K-linearly dependent. For that d, the minimal polynomial may be derived from the dependency relation.

Example. Consider $i \in \mathbb{C}/\mathbb{Q}$. We have that 1 and i are linearly independent over $\mathbb{Q}$, but 1, i, and i^2 are dependent:

$$1(1) + 0(i) + 1(i^2) = 0.$$

Let

$$p(x) = 1 \cdot 1 + 0 \cdot x + 1 \cdot x^2 = 1 + x^2.$$

Then $p(i) = 0$,

Algorithm for finding minimal polynomial

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Then, the degree of the minimal polynomial is the smallest d such that $1, \alpha, \alpha^2, \cdots, \alpha^d$ are K-linearly dependent. For that d, the minimal polynomial may be derived from the dependency relation.

Example. Consider $i \in \mathbb{C}/\mathbb{Q}$. We have that 1 and i are linearly independent over $\mathbb{Q}$, but 1, i, and i^2 are dependent:

$$1(1) + 0(i) + 1(i^2) = 0.$$

Let

$$p(x) = 1 \cdot 1 + 0 \cdot x + 1 \cdot x^2 = 1 + x^2.$$

Then $p(i) = 0$, and since p is already monic, we do not have to scale it.

Integral elements

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

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

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 $p(\alpha) = 0$.

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 $p(\alpha) = 0$.

Examples.

- If A is a field, then integral over A means

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 $p(\alpha) = 0$.

Examples.

- If A is a field, then integral over A means algebraic over A.

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 $p(\alpha) = 0$.

Examples.

- If A is a field, then integral over A means algebraic over A.
- $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$

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 $p(\alpha) = 0$.

Examples.

- If A is a field, then integral over A means algebraic over A.
- $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$ ($p(x) = x^2 - x - 1$).

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 $p(\alpha) = 0$.

Examples.

- If A is a field, then integral over A means algebraic over A.
- $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$ ($p(x) = x^2 - x - 1$).
- i is integral over $\mathbb{Z}$

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 $p(\alpha) = 0$.

Examples.

- If A is a field, then integral over A means algebraic over A.
- $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$ ($p(x) = x^2 - x - 1$).
- i is integral over $\mathbb{Z}$ ($p(x) = x^2 + 1$).

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 $p(\alpha) = 0$.

Examples.

- If A is a field, then integral over A means algebraic over A.
- $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$ ($p(x) = x^2 - x - 1$).
- i is integral over $\mathbb{Z}$ ($p(x) = x^2 + 1$).
- $\frac{2}{3}$ is not integral over $\mathbb{Z}$ even though it's a zero of $p(x) = 3x - 2$.

Which rational numbers integral over $\mathbb{Z}$?

Proposition. A rational number is integral over $\mathbb{Z}$ if and only if it is an integer.

Which rational numbers integral over $\mathbb{Z}$?

Proposition. A rational number is integral over $\mathbb{Z}$ if and only if it is an integer.

Proof. ($\Leftarrow$) Let $a \in \mathbb{Z}$. Then $x - a \in \mathbb{Z}[x]$ shows that a is integral over $\mathbb{Z}$.

Which rational numbers integral over $\mathbb{Z}$?

Proposition. A rational number is integral over $\mathbb{Z}$ if and only if it is an integer.

Proof. ($\Leftarrow$) Let $a \in \mathbb{Z}$. Then $x - a \in \mathbb{Z}[x]$ shows that a is integral over $\mathbb{Z}$.

($\Rightarrow$) Conversely, suppose that $\frac{a}{b} \in \mathbb{Q}$ in lowest terms is integral over $\mathbb{Z}$.

Which rational numbers integral over $\mathbb{Z}$?

Proposition. A rational number is integral over $\mathbb{Z}$ if and only if it is an integer.

Proof. ($\Leftarrow$) Let $a \in \mathbb{Z}$. Then $x - a \in \mathbb{Z}[x]$ shows that a is integral over $\mathbb{Z}$.

($\Rightarrow$) Conversely, suppose that $\frac{a}{b} \in \mathbb{Q}$ in lowest terms is integral over $\mathbb{Z}$. Then there exists $p = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ with $c_i \in \mathbb{Z}$ such that $p(a/b) = 0$:

Which rational numbers integral over $\mathbb{Z}$?

Proposition. A rational number is integral over $\mathbb{Z}$ if and only if it is an integer.

Proof. ($\Leftarrow$) Let $a \in \mathbb{Z}$. Then $x - a \in \mathbb{Z}[x]$ shows that a is integral over $\mathbb{Z}$.

($\Rightarrow$) Conversely, suppose that $\frac{a}{b} \in \mathbb{Q}$ in lowest terms is integral over $\mathbb{Z}$. Then there exists $p = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ with $c_i \in \mathbb{Z}$ such that $p(a/b) = 0$:

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0.$$

Which rational numbers integral over $\mathbb{Z}$?

Proposition. A rational number is integral over $\mathbb{Z}$ if and only if it is an integer.

Proof. ($\Leftarrow$) Let $a \in \mathbb{Z}$. Then $x - a \in \mathbb{Z}[x]$ shows that a is integral over $\mathbb{Z}$.

($\Rightarrow$) Conversely, suppose that $\frac{a}{b} \in \mathbb{Q}$ in lowest terms is integral over $\mathbb{Z}$. Then there exists $p = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ with $c_i \in \mathbb{Z}$ such that $p(a/b) = 0$:

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0.$$

Clear denominators by multiplying through by b^n:

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n = 0.$$

Which rational numbers integral over $\mathbb{Z}$?

Proposition. A rational number is integral over $\mathbb{Z}$ if and only if it is an integer.

Proof. ($\Leftarrow$) Let $a \in \mathbb{Z}$. Then $x - a \in \mathbb{Z}[x]$ shows that a is integral over $\mathbb{Z}$.

($\Rightarrow$) Conversely, suppose that $\frac{a}{b} \in \mathbb{Q}$ in lowest terms is integral over $\mathbb{Z}$. Then there exists $p = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ with $c_i \in \mathbb{Z}$ such that $p(a/b) = 0$:

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0.$$

Clear denominators by multiplying through by b^n:

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n = 0.$$

We see that

$$a^n = 0 \bmod b.$$

Which rational numbers integral over $\mathbb{Z}$?

Proposition. A rational number is integral over $\mathbb{Z}$ if and only if it is an integer.

Proof. ($\Leftarrow$) Let $a \in \mathbb{Z}$. Then $x - a \in \mathbb{Z}[x]$ shows that a is integral over $\mathbb{Z}$.

($\Rightarrow$) Conversely, suppose that $\frac{a}{b} \in \mathbb{Q}$ in lowest terms is integral over $\mathbb{Z}$. Then there exists $p = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ with $c_i \in \mathbb{Z}$ such that $p(a/b) = 0$:

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0.$$

Clear denominators by multiplying through by b^n:

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n = 0.$$

We see that

$$a^n = 0 \bmod b.$$

If $b \neq 1$, then some prime in the factorization of b must divide a,

Which rational numbers integral over $\mathbb{Z}$?

Proposition. A rational number is integral over $\mathbb{Z}$ if and only if it is an integer.

Proof. ($\Leftarrow$) Let $a \in \mathbb{Z}$. Then $x - a \in \mathbb{Z}[x]$ shows that a is integral over $\mathbb{Z}$.

($\Rightarrow$) Conversely, suppose that $\frac{a}{b} \in \mathbb{Q}$ in lowest terms is integral over $\mathbb{Z}$. Then there exists $p = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ with $c_i \in \mathbb{Z}$ such that $p(a/b) = 0$:

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0.$$

Clear denominators by multiplying through by b^n:

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1 ab^{n-1} + c_0 b^n = 0.$$

We see that

$$a^n = 0 \bmod b.$$

If $b \neq 1$, then some prime in the factorization of b must divide a, but that cannot happen since a/b is in lowest terms. $\square$

Important theorem about integral elements

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

Important theorem about integral elements

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.

Important theorem about integral elements

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.

Important theorem about integral elements

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, $\alpha M = \{\alpha m : m \in M\}$).

Important theorem about integral elements

α is integral over $A \Longrightarrow A[\alpha]$ is a f.g. A-module.

Important theorem about integral elements

α is integral over $A \Longrightarrow A[\alpha]$ is a f.g. A-module.

Proof. Since α is integral, there exists $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in A$ such that $p(\alpha) = 0$.

Important theorem about integral elements

α is integral over $A \Longrightarrow A[\alpha]$ is a f.g. A-module.

Proof. Since α is integral, there exists $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in A$ such that $p(\alpha) = 0$. Therefore,

$$\alpha^n = -a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1}.$$

Important theorem about integral elements

α is integral over $A \Longrightarrow A[\alpha]$ is a f.g. A-module.

Proof. Since α is integral, there exists $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in A$ such that $p(\alpha) = 0$. Therefore,

$$\alpha^n = -a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1}.$$

Thus, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ generates $A[\alpha]$ as an A-module.

Important theorem about integral elements

$A[\alpha]$ f.g. A-module $\Rightarrow \exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M$

Important theorem about integral elements

$A[\alpha]$ f.g. A-module $\Rightarrow \exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M$

Proof. Let $M = A[x]$.

Important theorem about integral elements

$A[\alpha]$ f.g. A-module $\Rightarrow \exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M$

Proof. Let $M = A[x]$. Then $\alpha M \subseteq M$. $\square$

Important theorem about integral elements

$\exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M \Rightarrow \alpha$ is integral over A

Important theorem about integral elements

$\exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M \Rightarrow \alpha$ is integral over A

Proof. Say M is generated by $b_1, \ldots, b_n \in B$ as an A-module.

Important theorem about integral elements

$\exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M \Rightarrow \alpha$ is integral over A

Proof. Say M is generated by $b_1, \ldots, b_n \in B$ as an A-module. Since $\alpha M \subseteq M$, there exist $a_{ij} \in A$ such that

$$\begin{aligned}
\alpha b_1 &= a_{11} b_1 + \cdots + a_{1n} b_n \\
\alpha b_2 &= a_{21} b_1 + \cdots + a_{2n} b_n \\
&\vdots \qquad \vdots \\
\alpha b_n &= a_{n1} b_1 + \cdots + a_{nn} b_n.
\end{aligned}$$

Important theorem about integral elements

$\exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M \Rightarrow \alpha$ is integral over A

Proof. Say M is generated by $b_1, \ldots, b_n \in B$ as an A-module. Since $\alpha M \subseteq M$, there exist $a_{ij} \in A$ such that

$$\begin{aligned}
\alpha b_1 &= a_{11} b_1 + \cdots + a_{1n} b_n \\
\alpha b_2 &= a_{21} b_1 + \cdots + a_{2n} b_n \\
&\vdots \qquad \vdots \\
\alpha b_n &= a_{n1} b_1 + \cdots + a_{nn} b_n.
\end{aligned}$$

Letting $T = (a_{ij})$ and $b = (b_1, \ldots, b_n)^t$, we get $\alpha b = Tb$.

Important theorem about integral elements

$\exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M \Rightarrow \alpha$ is integral over A

Proof. Say M is generated by $b_1, \ldots, b_n \in B$ as an A-module. Since $\alpha M \subseteq M$, there exist $a_{ij} \in A$ such that

$$\begin{aligned}
\alpha b_1 &= a_{11} b_1 + \cdots + a_{1n} b_n \\
\alpha b_2 &= a_{21} b_1 + \cdots + a_{2n} b_n \\
&\vdots \qquad \vdots \\
\alpha b_n &= a_{n1} b_1 + \cdots + a_{nn} b_n.
\end{aligned}$$

Letting $T = (a_{ij})$ and $b = (b_1, \ldots, b_n)^t$, we get $\alpha b = Tb$.
Then $(\alpha I_n - T)b = 0$,

Important theorem about integral elements

$\exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M \Rightarrow \alpha$ is integral over A

Proof. Say M is generated by $b_1, \ldots, b_n \in B$ as an A-module. Since $\alpha M \subseteq M$, there exist $a_{ij} \in A$ such that

$$\begin{aligned}
\alpha b_1 &= a_{11} b_1 + \cdots + a_{1n} b_n \\
\alpha b_2 &= a_{21} b_1 + \cdots + a_{2n} b_n \\
&\vdots \qquad \vdots \\
\alpha b_n &= a_{n1} b_1 + \cdots + a_{nn} b_n.
\end{aligned}$$

Letting $T = (a_{ij})$ and $b = (b_1, \ldots, b_n)^t$, we get $\alpha b = Tb$.
Then $(\alpha I_n - T)b = 0$, which implies $\det(\alpha I_n - T) = 0$.

Important theorem about integral elements

$\exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M \Rightarrow \alpha$ is integral over A

Proof. Say M is generated by $b_1, \ldots, b_n \in B$ as an A-module. Since $\alpha M \subseteq M$, there exist $a_{ij} \in A$ such that

$$\begin{aligned}
\alpha b_1 &= a_{11} b_1 + \cdots + a_{1n} b_n \\
\alpha b_2 &= a_{21} b_1 + \cdots + a_{2n} b_n \\
&\vdots \qquad \vdots \\
\alpha b_n &= a_{n1} b_1 + \cdots + a_{nn} b_n.
\end{aligned}$$

Letting $T = (a_{ij})$ and $b = (b_1, \ldots, b_n)^t$, we get $\alpha b = Tb$.

Then $(\alpha I_n - T)b = 0$, which implies $\det(\alpha I_n - T) = 0$. Define $p(x) = \det(xI_n - T)$.

Important theorem about integral elements

$\exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M \Rightarrow \alpha$ is integral over A

Proof. Say M is generated by $b_1, \ldots, b_n \in B$ as an A-module. Since $\alpha M \subseteq M$, there exist $a_{ij} \in A$ such that

$$\begin{aligned}
\alpha b_1 &= a_{11} b_1 + \cdots + a_{1n} b_n \\
\alpha b_2 &= a_{21} b_1 + \cdots + a_{2n} b_n \\
&\vdots \qquad \vdots \\
\alpha b_n &= a_{n1} b_1 + \cdots + a_{nn} b_n.
\end{aligned}$$

Letting $T = (a_{ij})$ and $b = (b_1, \ldots, b_n)^t$, we get $\alpha b = Tb$.

Then $(\alpha I_n - T)b = 0$, which implies $\det(\alpha I_n - T) = 0$. Define $p(x) = \det(xI_n - T)$. Then $p(\alpha) = 0$.

Important theorem about integral elements

$\exists$ f.g. A-module $M \subseteq B$ such that $\alpha M \subseteq M \Rightarrow \alpha$ is integral over A

Proof. Say M is generated by $b_1, \ldots, b_n \in B$ as an A-module. Since $\alpha M \subseteq M$, there exist $a_{ij} \in A$ such that

$$\begin{aligned}
\alpha b_1 &= a_{11} b_1 + \cdots + a_{1n} b_n \\
\alpha b_2 &= a_{21} b_1 + \cdots + a_{2n} b_n \\
&\vdots \qquad \vdots \\
\alpha b_n &= a_{n1} b_1 + \cdots + a_{nn} b_n.
\end{aligned}$$

Letting $T = (a_{ij})$ and $b = (b_1, \ldots, b_n)^t$, we get $\alpha b = Tb$.

Then $(\alpha I_n - T)b = 0$, which implies $\det(\alpha I_n - T) = 0$. Define $p(x) = \det(xI_n - T)$. Then $p(\alpha) = 0$. We take a closer look at p on the next page.

Important theorem about integral elements

We defined $p(x) = \det(xI_n - T)$:

Important theorem about integral elements

We defined $p(x) = \det(xI_n - T)$:

$$p(x) = \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix} = x^n + \text{ lots.}$$

Important theorem about integral elements

We defined $p(x) = \det(xI_n - T)$:

$$p(x) = \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix} = x^n + \text{ lots.}$$

So p is

Important theorem about integral elements

We defined $p(x) = \det(xI_n - T)$:

$$p(x) = \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix} = x^n + \text{ lots.}$$

So p is monic,

Important theorem about integral elements

We defined $p(x) = \det(xI_n - T)$:

$$p(x) = \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix} = x^n + \text{ lots.}$$

So p is monic, has coefficients in A,

Important theorem about integral elements

We defined $p(x) = \det(xI_n - T)$:

$$p(x) = \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix} = x^n + \text{ lots.}$$

So p is monic, has coefficients in A, and vanishes at α.

Important theorem about integral elements

We defined $p(x) = \det(xI_n - T)$:

$$p(x) = \det \begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix} = x^n + \text{ lots.}$$

So p is monic, has coefficients in A, and vanishes at α. Therefore, α is integral over B. $\square$

Integral elements form a subring

Lemma. Let $A \subseteq B \subseteq C$ be rings. If B is finitely generated as an A-module and C is finitely generated as a B-module, then C is finitely generated as an A-module.

Integral elements form a subring

Lemma. Let $A \subseteq B \subseteq C$ be rings. If B is finitely generated as an A-module and C is finitely generated as a B-module, then C is finitely generated as an A-module.

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

Integral elements form a subring

Lemma. Let $A \subseteq B \subseteq C$ be rings. If B is finitely generated as an A-module and C is finitely generated as a B-module, then C is finitely generated as an A-module.

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

Proof. Let $\alpha, \beta \in B$ be integral over A.

Integral elements form a subring

Lemma. Let $A \subseteq B \subseteq C$ be rings. If B is finitely generated as an A-module and C is finitely generated as a B-module, then C is finitely generated as an A-module.

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

Proof. Let $\alpha, \beta \in B$ be integral over A. Consider

$$A \subseteq A[\alpha]$$

Integral elements form a subring

Lemma. Let $A \subseteq B \subseteq C$ be rings. If B is finitely generated as an A-module and C is finitely generated as a B-module, then C is finitely generated as an A-module.

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

Proof. Let $\alpha, \beta \in B$ be integral over A. Consider

$$A \subseteq A[\alpha] \subseteq A[\alpha][\beta]$$

Integral elements form a subring

Lemma. Let $A \subseteq B \subseteq C$ be rings. If B is finitely generated as an A-module and C is finitely generated as a B-module, then C is finitely generated as an A-module.

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

Proof. Let $\alpha, \beta \in B$ be integral over A. Consider

$$A \subseteq A[\alpha] \subseteq A[\alpha][\beta] = A[\alpha, \beta].$$

Integral elements form a subring

Lemma. Let $A \subseteq B \subseteq C$ be rings. If B is finitely generated as an A-module and C is finitely generated as a B-module, then C is finitely generated as an A-module.

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

Proof. Let $\alpha, \beta \in B$ be integral over A. Consider

$$A \subseteq A[\alpha] \subseteq A[\alpha][\beta] = A[\alpha, \beta].$$

Then $M := A[\alpha, \beta] \subseteq B$ is a f.g. A-module

Integral elements form a subring

Lemma. Let $A \subseteq B \subseteq C$ be rings. If B is finitely generated as an A-module and C is finitely generated as a B-module, then C is finitely generated as an A-module.

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

Proof. Let $\alpha, \beta \in B$ be integral over A. Consider

$$A \subseteq A[\alpha] \subseteq A[\alpha][\beta] = A[\alpha, \beta].$$

Then $M := A[\alpha, \beta] \subseteq B$ is a f.g. A-module and

$$(\alpha + \beta)M \subseteq M \quad \text{and} \quad (\alpha\beta)M \subseteq M. \square$$

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 the proof of the Theorem, above, gives a method for calculating such a p.