Math 361

January 27, 2023

Questions from last time

Let $\phi\colon R \to S$ be a ring homomorphism, and suppose S is an integral domain. Suppose $\phi(1_R) \neq 1_S$.

Questions from last time

Let $\phi \colon R \to S$ be a ring homomorphism, and suppose S is an integral domain. Suppose $\phi(1_R) \neq 1_S$. Then $\phi = 0$.

Questions from last time

Let $\phi\colon R \to S$ be a ring homomorphism, and suppose S is an integral domain. Suppose $\phi(1_R) \neq 1_S$. Then $\phi = 0$.

Proof. We have

$$\phi(1_R) = \phi(1_R \cdot 1_R) = \phi(1_R)\phi(1_R)$$

Questions from last time

Let $\phi\colon R \to S$ be a ring homomorphism, and suppose S is an integral domain. Suppose $\phi(1_R) \neq 1_S$. Then $\phi = 0$.

Proof. We have

$$\phi(1_R) = \phi(1_R \cdot 1_R) = \phi(1_R)\phi(1_R) \quad \Rightarrow \quad \phi(1_R)(\phi(1_R) - 1_S) = 0.$$

Questions from last time

Let $\phi\colon R \to S$ be a ring homomorphism, and suppose S is an integral domain. Suppose $\phi(1_R) \neq 1_S$. Then $\phi = 0$.

Proof. We have

$$\phi(1_R) = \phi(1_R \cdot 1_R) = \phi(1_R)\phi(1_R) \quad \Rightarrow \quad \phi(1_R)(\phi(1_R) - 1_S) = 0.$$

Since S is a domain and $\phi(1_R) \neq 1_S$, we have $\phi(1_R) = 0$.

Questions from last time

Let $\phi\colon R \to S$ be a ring homomorphism, and suppose S is an integral domain. Suppose $\phi(1_R) \neq 1_S$. Then $\phi = 0$.

Proof. We have

$$\phi(1_R) = \phi(1_R \cdot 1_R) = \phi(1_R)\phi(1_R) \quad \Rightarrow \quad \phi(1_R)(\phi(1_R) - 1_S) = 0.$$

Since S is a domain and $\phi(1_R) \neq 1_S$, we have $\phi(1_R) = 0$. Let $r \in R$. Then

$$\phi(r) = \phi(1_R \cdot r) = \phi(1_R)\phi(r) = 0 \cdot \phi(r) = 0. \qquad \square$$

Questions from last time

Let $\phi\colon R \to S$ be a ring homomorphism, and suppose S is an integral domain. Suppose $\phi(1_R) \neq 1_S$. Then $\phi = 0$.

Proof. We have

$$\phi(1_R) = \phi(1_R \cdot 1_R) = \phi(1_R)\phi(1_R) \quad \Rightarrow \quad \phi(1_R)(\phi(1_R) - 1_S) = 0.$$

Since S is a domain and $\phi(1_R) \neq 1_S$, we have $\phi(1_R) = 0$. Let $r \in R$. Then

$$\phi(r) = \phi(1_R \cdot r) = \phi(1_R)\phi(r) = 0 \cdot \phi(r) = 0. \qquad \square$$

Question: What is wrong with the mapping $\phi\colon \mathbb{Z} \to \mathbb{Z}$ given by $\phi(a) = 2a$?

Questions from last time

Let $\phi\colon R \to S$ be a ring homomorphism, and suppose S is an integral domain. Suppose $\phi(1_R) \neq 1_S$. Then $\phi = 0$.

Proof. We have

$$\phi(1_R) = \phi(1_R \cdot 1_R) = \phi(1_R)\phi(1_R) \quad \Rightarrow \quad \phi(1_R)(\phi(1_R) - 1_S) = 0.$$

Since S is a domain and $\phi(1_R) \neq 1_S$, we have $\phi(1_R) = 0$. Let $r \in R$. Then

$$\phi(r) = \phi(1_R \cdot r) = \phi(1_R)\phi(r) = 0 \cdot \phi(r) = 0. \qquad \square$$

Question: What is wrong with the mapping $\phi\colon \mathbb{Z} \to \mathbb{Z}$ given by $\phi(a) = 2a$? Answer: it's not a ring homomorphism. For example,

$$2 = \phi(1) = \phi(1 \cdot 1) \neq \phi(1)\phi(1) = 4.$$

Question for last time

Let $\phi\colon R \to S$ be a ring homomorphism. Then $\mathrm{im}(\phi)$ is a ring, and $\phi(1_R)$ is the identity of $\mathrm{im}(\phi)$.

Question for last time

Let $\phi\colon R \to S$ be a ring homomorphism. Then $\mathrm{im}(\phi)$ is a ring, and $\phi(1_R)$ is the identity of $\mathrm{im}(\phi)$.

Example: Let $\phi\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ be given by $\phi(a) = 3a$.

Question for last time

Let $\phi\colon R \to S$ be a ring homomorphism. Then $\mathrm{im}(\phi)$ is a ring, and $\phi(1_R)$ is the identity of $\mathrm{im}(\phi)$.

Example: Let $\phi\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ be given by $\phi(a) = 3a$.

Now we have $3 = \phi(1) = \phi(1 \cdot 1) = 3 \cdot 3 = 3$.

Question for last time

Let $\phi\colon R \to S$ be a ring homomorphism. Then $\mathrm{im}(\phi)$ is a ring, and $\phi(1_R)$ is the identity of $\mathrm{im}(\phi)$.

Example: Let $\phi\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ be given by $\phi(a) = 3a$.

Now we have $3 = \phi(1) = \phi(1 \cdot 1) = 3 \cdot 3 = 3$.

The image of ϕ is

Question for last time

Let $\phi\colon R \to S$ be a ring homomorphism. Then $\operatorname{im}(\phi)$ is a ring, and $\phi(1_R)$ is the identity of $\operatorname{im}(\phi)$.

Example: Let $\phi\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ be given by $\phi(a) = 3a$.

Now we have $3 = \phi(1) = \phi(1 \cdot 1) = 3 \cdot 3 = 3$.

The image of ϕ is $\{0, 3\}$, which is a ring with identity 3.

Question for last time

Let $\phi\colon R \to S$ be a ring homomorphism. Then $\mathrm{im}(\phi)$ is a ring, and $\phi(1_R)$ is the identity of $\mathrm{im}(\phi)$.

Example: Let $\phi\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ be given by $\phi(a) = 3a$.

Now we have $3 = \phi(1) = \phi(1 \cdot 1) = 3 \cdot 3 = 3$.

The image of ϕ is $\{0, 3\}$, which is a ring with identity 3.

The kernel of ϕ is

Question for last time

Let $\phi\colon R \to S$ be a ring homomorphism. Then $\text{im}(\phi)$ is a ring, and $\phi(1_R)$ is the identity of $\text{im}(\phi)$.

Example: Let $\phi\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ be given by $\phi(a) = 3a$.

Now we have $3 = \phi(1) = \phi(1 \cdot 1) = 3 \cdot 3 = 3$.

The image of ϕ is $\{0, 3\}$, which is a ring with identity 3.

The kernel of ϕ is $\{0, 2, 4\}$,

Question for last time

Let $\phi\colon R \to S$ be a ring homomorphism. Then $\mathrm{im}(\phi)$ is a ring, and $\phi(1_R)$ is the identity of $\mathrm{im}(\phi)$.

Example: Let $\phi\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ be given by $\phi(a) = 3a$.

Now we have $3 = \phi(1) = \phi(1 \cdot 1) = 3 \cdot 3 = 3$.

The image of ϕ is $\{0, 3\}$, which is a ring with identity 3.

The kernel of ϕ is $\{0, 2, 4\}$, and

$$\mathbb{Z}/6\mathbb{Z} \Big/ \ker(\phi) \xrightarrow{\sim} \mathrm{im}(\phi)$$

$$a \mapsto 3a.$$

Today

1. Field extensions.
2. Algebraic elements in an extension.
3. The minimal polynomial of an algebraic element.
4. Finite extensions are algebraic.

Field extensions

A *field extension* is a pair of fields $K \subseteq L$.

Field extensions

A *field extension* is a pair of fields $K \subseteq L$. In that case, L is automatically a vector space over K.

Field extensions

A *field extension* is a pair of fields $K \subseteq L$. In that case, L is automatically a vector space over K. It's dimension is denoted

$$[L : K] := \dim_K L,$$

Field extensions

A *field extension* is a pair of fields $K \subseteq L$. In that case, L is automatically a vector space over K. It's dimension is denoted

$$[L : K] := \dim_K L,$$

Standard notation:

$$\begin{tikzcd} L \arrow[d, dash, "{[L:K]}"] \\ K. \end{tikzcd}$$

Field extensions

A *field extension* is a pair of fields $K \subseteq L$. In that case, L is automatically a vector space over K. It's dimension is denoted

$$[L : K] := \dim_K L,$$

Standard notation:

$$\begin{array}{c} L \\ \Big| \, {\scriptstyle [L:K]} \\ K. \end{array}$$

If $[L : K] < \infty$, we say that L is a *finite field extension of K*.

Field extensions

A *field extension* is a pair of fields $K \subseteq L$. In that case, L is automatically a vector space over K. It's dimension is denoted

$$[L : K] := \dim_K L,$$

Standard notation:

$$\begin{array}{c} L \\ \Big| \, {\scriptstyle [L:K]} \\ K. \end{array}$$

If $[L : K] < \infty$, we say that L is a *finite field extension of* K.

We usually denote a field extension $K \subseteq L$ by L/K.

Example

$\mathbb{Q}(i)/\mathbb{Q}$:

$$\begin{array}{c} \mathbb{Q}(i) \\ \Big| \, 2 \\ \mathbb{Q} \end{array}$$

Example

$\mathbb{Q}(i)/\mathbb{Q}$:

$$\begin{array}{c} \mathbb{Q}(i) \\ \Big| \, 2 \\ \mathbb{Q} \end{array}$$

$\mathbb{Q}$-basis: $\{1, i\}$.

Field extensions

Proposition. Suppose K, H and L are fields with $K \subseteq H \subseteq L$, and suppose that $[L : K] < \infty$. Then $[L : H] < \infty$ and $[H : K] < \infty$, and

$$[L : K] = [L : H][H : K].$$

$$\begin{tikzcd}
L \arrow[d, dash, "{[L:H]}"] \\
H \arrow[d, dash, "{[H:K]}"] \\
K
\end{tikzcd}$$

Field extensions

Proposition. Suppose K, H and L are fields with $K \subseteq H \subseteq L$, and suppose that $[L : K] < \infty$. Then $[L : H] < \infty$ and $[H : K] < \infty$, and

$$[L : K] = [L : H][H : K].$$

$$\begin{array}{c} L \\ \Big| {\scriptstyle [L:H]} \\ H \\ \Big| {\scriptstyle [H:K]} \\ K \end{array}$$

Proof. Homework.

Algebraic elements

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 $f(\alpha) = 0$.

Algebraic elements

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 $f(\alpha) = 0$.

Examples.

1. $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$.

Algebraic elements

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 $f(\alpha) = 0$.

Examples.

1. $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$.
2. What about π over $\mathbb{Q}$?

Algebraic elements

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 $f(\alpha) = 0$.

Examples.

1. $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$.
2. What about π over $\mathbb{Q}$?
3. Let t be an indeterminate. Is t over $\mathbb{Q}(t^2)$?

Algebraic elements

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 $f(\alpha) = 0$.

Examples.

1. $\sqrt{2}$ and i are algebraic over $\mathbb{Q}$.
2. What about π over $\mathbb{Q}$?
3. Let t be an indeterminate. Is t over $\mathbb{Q}(t^2)$? How about t over $\mathbb{Q}$?

Minimal polynomial

Proposition. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then there exists a unique *monic* polynomial $p \in K[x]$ of minimal positive degree such that $p(\alpha) = 0$.

Minimal polynomial

Proposition. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then there exists a unique *monic* polynomial $p \in K[x]$ of minimal positive degree such that $p(\alpha) = 0$.

Proof Let $I = \{f \in K[x] : f(\alpha) = 0\}$.

Minimal polynomial

Proposition. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then there exists a unique *monic* polynomial $p \in K[x]$ of minimal positive degree such that $p(\alpha) = 0$.

Proof Let $I = \{f \in K[x] : f(\alpha) = 0\}$. Then since $K[x]$ is a PID, $I = (p)$ for some $p \in K[x]$.

Minimal polynomial

Proposition. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then there exists a unique *monic* polynomial $p \in K[x]$ of minimal positive degree such that $p(\alpha) = 0$.

Proof Let $I = \{f \in K[x] : f(\alpha) = 0\}$. Then since $K[x]$ is a PID, $I = (p)$ for some $p \in K[x]$. We may assume p is monic.

Minimal polynomial

Proposition. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then there exists a unique *monic* polynomial $p \in K[x]$ of minimal positive degree such that $p(\alpha) = 0$.

Proof Let $I = \{f \in K[x] : f(\alpha) = 0\}$. Then since $K[x]$ is a PID, $I = (p)$ for some $p \in K[x]$. We may assume p is monic. If f is any nonzero element of I, we may write $f = pq$ for some nonzero $q \in K[x]$.

Minimal polynomial

Proposition. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then there exists a unique *monic* polynomial $p \in K[x]$ of minimal positive degree such that $p(\alpha) = 0$.

Proof Let $I = \{f \in K[x] : f(\alpha) = 0\}$. Then since $K[x]$ is a PID, $I = (p)$ for some $p \in K[x]$. We may assume p is monic. If f is any nonzero element of I, we may write $f = pq$ for some nonzero $q \in K[x]$. We have

$$\deg(f) = \deg(pq) = \deg(p) + \deg(q) \geq \deg(p).$$

Minimal polynomial

Proposition. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then there exists a unique *monic* polynomial $p \in K[x]$ of minimal positive degree such that $p(\alpha) = 0$.

Proof Let $I = \{f \in K[x] : f(\alpha) = 0\}$. Then since $K[x]$ is a PID, $I = (p)$ for some $p \in K[x]$. We may assume p is monic. If f is any nonzero element of I, we may write $f = pq$ for some nonzero $q \in K[x]$. We have

$$\deg(f) = \deg(pq) = \deg(p) + \deg(q) \geq \deg(p).$$

If $\deg(f) = \deg(p)$, then

Minimal polynomial

Proposition. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then there exists a unique *monic* polynomial $p \in K[x]$ of minimal positive degree such that $p(\alpha) = 0$.

Proof Let $I = \{f \in K[x] : f(\alpha) = 0\}$. Then since $K[x]$ is a PID, $I = (p)$ for some $p \in K[x]$. We may assume p is monic. If f is any nonzero element of I, we may write $f = pq$ for some nonzero $q \in K[x]$. We have

$$\deg(f) = \deg(pq) = \deg(p) + \deg(q) \geq \deg(p).$$

If $\deg(f) = \deg(p)$, then $\deg(q) = 0$. So q is a nonzero element of K.

Minimal polynomial

Proposition. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then there exists a unique *monic* polynomial $p \in K[x]$ of minimal positive degree such that $p(\alpha) = 0$.

Proof Let $I = \{f \in K[x] : f(\alpha) = 0\}$. Then since $K[x]$ is a PID, $I = (p)$ for some $p \in K[x]$. We may assume p is monic. If f is any nonzero element of I, we may write $f = pq$ for some nonzero $q \in K[x]$. We have

$$\deg(f) = \deg(pq) = \deg(p) + \deg(q) \geq \deg(p).$$

If $\deg(f) = \deg(p)$, then $\deg(q) = 0$. So q is a nonzero element of K. Two polynomials are, by definition, equal if and only if their coefficients are equal. So if $\deg(f) = \deg(p)$ and f is monic, it follows that $f = p$.

Minimal polynomial

Proposition. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then there exists a unique *monic* polynomial $p \in K[x]$ of minimal positive degree such that $p(\alpha) = 0$.

Proof Let $I = \{f \in K[x] : f(\alpha) = 0\}$. Then since $K[x]$ is a PID, $I = (p)$ for some $p \in K[x]$. We may assume p is monic. If f is any nonzero element of I, we may write $f = pq$ for some nonzero $q \in K[x]$. We have

$$\deg(f) = \deg(pq) = \deg(p) + \deg(q) \geq \deg(p).$$

If $\deg(f) = \deg(p)$, then $\deg(q) = 0$. So q is a nonzero element of K. Two polynomials are, by definition, equal if and only if their coefficients are equal. So if $\deg(f) = \deg(p)$ and f is monic, it follows that $f = p$.

Definition. The polynomial p in the above proposition is called the *minimal polynomial for α over K*.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof. Suppose p is the minimal polynomial and $p = fg$.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof. Suppose p is the minimal polynomial and $p = fg$. Then $f \neq 0$ and $g \neq 0$, but $p(\alpha) = f(\alpha)g(\alpha) = 0$.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof. Suppose p is the minimal polynomial and $p = fg$. Then $f \neq 0$ and $g \neq 0$, but $p(\alpha) = f(\alpha)g(\alpha) = 0$. WLOG, $f(\alpha) = 0$.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof. Suppose p is the minimal polynomial and $p = fg$. Then $f \neq 0$ and $g \neq 0$, but $p(\alpha) = f(\alpha)g(\alpha) = 0$. WLOG, $f(\alpha) = 0$. We must have $\deg(f) > 0$.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof. Suppose p is the minimal polynomial and $p = fg$. Then $f \neq 0$ and $g \neq 0$, but $p(\alpha) = f(\alpha)g(\alpha) = 0$. WLOG, $f(\alpha) = 0$. We must have $\deg(f) > 0$. We have

$$\deg(p) = \deg(f) + \deg(g).$$

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof. Suppose p is the minimal polynomial and $p = fg$. Then $f \neq 0$ and $g \neq 0$, but $p(\alpha) = f(\alpha)g(\alpha) = 0$. WLOG, $f(\alpha) = 0$. We must have $\deg(f) > 0$. We have

$$\deg(p) = \deg(f) + \deg(g).$$

By minimality of p,

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof. Suppose p is the minimal polynomial and $p = fg$. Then $f \neq 0$ and $g \neq 0$, but $p(\alpha) = f(\alpha)g(\alpha) = 0$. WLOG, $f(\alpha) = 0$. We must have $\deg(f) > 0$. We have

$$\deg(p) = \deg(f) + \deg(g).$$

By minimality of p, we have $\deg(f) = \deg(p)$, and hence

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof. Suppose p is the minimal polynomial and $p = fg$. Then $f \neq 0$ and $g \neq 0$, but $p(\alpha) = f(\alpha)g(\alpha) = 0$. WLOG, $f(\alpha) = 0$. We must have $\deg(f) > 0$. We have

$$\deg(p) = \deg(f) + \deg(g).$$

By minimality of p, we have $\deg(f) = \deg(p)$, and hence $\deg(g) = 0$.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof. Suppose p is the minimal polynomial and $p = fg$. Then $f \neq 0$ and $g \neq 0$, but $p(\alpha) = f(\alpha)g(\alpha) = 0$. WLOG, $f(\alpha) = 0$. We must have $\deg(f) > 0$. We have

$$\deg(p) = \deg(f) + \deg(g).$$

By minimality of p, we have $\deg(f) = \deg(p)$, and hence $\deg(g) = 0$. Since $g \neq 0$, it follows that g is a nonzero constant, hence a unit in $K[x]$.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof. Suppose p is the minimal polynomial and $p = fg$. Then $f \neq 0$ and $g \neq 0$, but $p(\alpha) = f(\alpha)g(\alpha) = 0$. WLOG, $f(\alpha) = 0$. We must have $\deg(f) > 0$. We have

$$\deg(p) = \deg(f) + \deg(g).$$

By minimality of p, we have $\deg(f) = \deg(p)$, and hence $\deg(g) = 0$. Since $g \neq 0$, it follows that g is a nonzero constant, hence a unit in $K[x]$.

We prove the converse on the next page.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof continued. To prove the converse, assume p is irreducible and monic.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof continued. To prove the converse, assume p is irreducible and monic. Let f be the minimal polynomial for α over K.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof continued. To prove the converse, assume p is irreducible and monic. Let f be the minimal polynomial for α over K. Apply the division algorithm:

$$p = qf + r$$

for some $q, r \in K[x]$ with $\deg r < \deg f$.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof continued. To prove the converse, assume p is irreducible and monic. Let f be the minimal polynomial for α over K. Apply the division algorithm:

$$p = qf + r$$

for some $q, r \in K[x]$ with $\deg r < \deg f$. We have
$0 = p(\alpha) = q(\alpha)f(\alpha) + r(\alpha) =$

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof continued. To prove the converse, assume p is irreducible and monic. Let f be the minimal polynomial for α over K. Apply the division algorithm:

$$p = qf + r$$

for some $q, r \in K[x]$ with $\deg r < \deg f$. We have $0 = p(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof continued. To prove the converse, assume p is irreducible and monic. Let f be the minimal polynomial for α over K. Apply the division algorithm:

$$p = qf + r$$

for some $q, r \in K[x]$ with $\deg r < \deg f$. We have $0 = p(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$. If $r \neq 0$, we contradict the minimality of f.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof continued. To prove the converse, assume p is irreducible and monic. Let f be the minimal polynomial for α over K. Apply the division algorithm:

$$p = qf + r$$

for some $q, r \in K[x]$ with $\deg r < \deg f$. We have $0 = p(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$. If $r \neq 0$, we contradict the minimality of f. So $r = 0$ and $p = qf$.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof continued. To prove the converse, assume p is irreducible and monic. Let f be the minimal polynomial for α over K. Apply the division algorithm:

$$p = qf + r$$

for some $q, r \in K[x]$ with $\deg r < \deg f$. We have $0 = p(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$. If $r \neq 0$, we contradict the minimality of f. So $r = 0$ and $p = qf$. Then p irreducible and $f \notin K$ imply q is a unit, i.e., $q \in K \setminus \{0\}$.

The minimal polynomial and irreducibility

Proposition. Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let p be a monic polynomial such that $p(\alpha) = 0$. Then p is the minimal polynomial for α over K if and only if p is irreducible.

Proof continued. To prove the converse, assume p is irreducible and monic. Let f be the minimal polynomial for α over K. Apply the division algorithm:

$$p = qf + r$$

for some $q, r \in K[x]$ with $\deg r < \deg f$. We have $0 = p(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$. If $r \neq 0$, we contradict the minimality of f. So $r = 0$ and $p = qf$. Then p irreducible and $f \notin K$ imply q is a unit, i.e., $q \in K \setminus \{0\}$. Finally, since p and f are both monic, $p = f$.

$K[\alpha]$ versus $K(\alpha)$

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K.

$K[\alpha]$ versus $K(\alpha)$

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let $K[\alpha]$ be the smallest subring of L containing α, and let $K(\alpha)$ be the smallest subfield of L containing α.

$K[\alpha]$ versus $K(\alpha)$

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let $K[\alpha]$ be the smallest subring of L containing α, and let $K(\alpha)$ be the smallest subfield of L containing α.

Then

$$K[\alpha] := \{f(\alpha) : f \in K[x]\},$$

$K[\alpha]$ versus $K(\alpha)$

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let $K[\alpha]$ be the smallest subring of L containing α, and let $K(\alpha)$ be the smallest subfield of L containing α.

Then

$$K[\alpha] := \{f(\alpha) : f \in K[x]\},$$

and

$$K(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\}.$$

$K[\alpha]$ versus $K(\alpha)$

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let $K[\alpha]$ be the smallest subring of L containing α, and let $K(\alpha)$ be the smallest subfield of L containing α.

Then

$$K[\alpha] := \{f(\alpha) : f \in K[x]\},$$

and

$$K(\alpha) := \left\{\frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0\right\}.$$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$.

$K[\alpha]$ versus $K(\alpha)$

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let $K[\alpha]$ be the smallest subring of L containing α, and let $K(\alpha)$ be the smallest subfield of L containing α.

Then

$$K[\alpha] := \{f(\alpha) : f \in K[x]\},$$

and

$$K(\alpha) := \left\{\frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0\right\}.$$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$

$K[\alpha]$ versus $K(\alpha)$

Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K. Let $K[\alpha]$ be the smallest subring of L containing α, and let $K(\alpha)$ be the smallest subfield of L containing α.

Then

$$K[\alpha] := \{f(\alpha) : f \in K[x]\},$$

and

$$K(\alpha) := \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\}.$$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof.
First suppose that $[K(\alpha) : K] = n < \infty$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof.
First suppose that $[K(\alpha) : K] = n < \infty$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n + 1$ (not necessarily distinct) elements in a vector space of dimension n, so

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof.
First suppose that $[K(\alpha) : K] = n < \infty$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n + 1$ (not necessarily distinct) elements in a vector space of dimension n, so they are linearly dependent.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof.
First suppose that $[K(\alpha) : K] = n < \infty$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n + 1$ (not necessarily distinct) elements in a vector space of dimension n, so they are linearly dependent. This means $\sum_{i=0}^{n} c_i \alpha^i = 0$ for some $c_i \in K$, not all zero.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof.
First suppose that $[K(\alpha) : K] = n < \infty$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n + 1$ (not necessarily distinct) elements in a vector space of dimension n, so they are linearly dependent. This means $\sum_{i=0}^{n} c_i \alpha^i = 0$ for some $c_i \in K$, not all zero. Define the polynomial $f(x) = \sum_{i=0}^{n} c_i x^i$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof.
First suppose that $[K(\alpha) : K] = n < \infty$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n + 1$ (not necessarily distinct) elements in a vector space of dimension n, so they are linearly dependent. This means $\sum_{i=0}^{n} c_i \alpha^i = 0$ for some $c_i \in K$, not all zero. Define the polynomial $f(x) = \sum_{i=0}^{n} c_i x^i$. Then $f \in K[x]$ and $f(\alpha) = 0$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof.
First suppose that $[K(\alpha) : K] = n < \infty$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n + 1$ (not necessarily distinct) elements in a vector space of dimension n, so they are linearly dependent. This means $\sum_{i=0}^{n} c_i \alpha^i = 0$ for some $c_i \in K$, not all zero. Define the polynomial $f(x) = \sum_{i=0}^{n} c_i x^i$. Then $f \in K[x]$ and $f(\alpha) = 0$. So α is algebraic over K.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof.
First suppose that $[K(\alpha) : K] = n < \infty$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n + 1$ (not necessarily distinct) elements in a vector space of dimension n, so they are linearly dependent. This means $\sum_{i=0}^{n} c_i \alpha^i = 0$ for some $c_i \in K$, not all zero. Define the polynomial $f(x) = \sum_{i=0}^{n} c_i x^i$. Then $f \in K[x]$ and $f(\alpha) = 0$. So α is algebraic over K.

Proof continued on next page.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued.

Conversely, suppose that α is algebraic over K, and let $p = \sum_{i=0}^{n} a_i x^i$ be its minimal polynomial.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued.

Conversely, suppose that α is algebraic over K, and
let $p = \sum_{i=0}^{n} a_i x^i$ be its minimal polynomial.
We first claim that $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ are linearly independent.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued.

Conversely, suppose that α is algebraic over K, and
let $p = \sum_{i=0}^{n} a_i x^i$ be its minimal polynomial.
We first claim that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are linearly independent. If not,

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued.

Conversely, suppose that α is algebraic over K, and
let $p = \sum_{i=0}^{n} a_i x^i$ be its minimal polynomial.
We first claim that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are linearly independent. If not, then there is a nontrivial linear relation $\sum_{i=0}^{n-1} b_i \alpha^i$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued.

Conversely, suppose that α is algebraic over K, and let $p = \sum_{i=0}^{n} a_i x^i$ be its minimal polynomial.
We first claim that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are linearly independent. If not, then there is a nontrivial linear relation $\sum_{i=0}^{n-1} b_i \alpha^i$.
Defining $f = \sum_{i=0}^{n-1} b_i x^i$, we have

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued.

Conversely, suppose that α is algebraic over K, and
let $p = \sum_{i=0}^{n} a_i x^i$ be its minimal polynomial.
We first claim that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are linearly independent. If not, then there is a nontrivial linear relation $\sum_{i=0}^{n-1} b_i \alpha^i$.
Defining $f = \sum_{i=0}^{n-1} b_i x^i$, we have $f \in K[x]$ and $f(\alpha) = 0$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued.

Conversely, suppose that α is algebraic over K, and
let $p = \sum_{i=0}^{n} a_i x^i$ be its minimal polynomial.
We first claim that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ are linearly independent. If not, then there is a nontrivial linear relation $\sum_{i=0}^{n-1} b_i \alpha^i$.
Defining $f = \sum_{i=0}^{n-1} b_i x^i$, we have $f \in K[x]$ and $f(\alpha) = 0$.
However, $\deg(f) < \deg(p) = n$, which contradicts the minimality of p.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued.

Conversely, suppose that α is algebraic over K, and
let $p = \sum_{i=0}^{n} a_i x^i$ be its minimal polynomial.
We first claim that $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ are linearly independent. If not, then there is a nontrivial linear relation $\sum_{i=0}^{n-1} b_i \alpha^i$.
Defining $f = \sum_{i=0}^{n-1} b_i x^i$, we have $f \in K[x]$ and $f(\alpha) = 0$.
However, $\deg(f) < \deg(p) = n$, which contradicts the minimality of p.

Proof continued on next page.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Now define $V = \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Now define $V = \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We have seen that $\dim V = n = \deg(p)$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Now define $V = \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We have seen that $\dim V = n = \deg(p)$. Our goal is to prove that V is a field.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha):K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha):K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Now define $V = \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We have seen that $\dim V = n = \deg(p)$. Our goal is to prove that V is a field. We then have

$$K(\alpha) \subseteq V$$

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Now define $V = \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We have seen that $\dim V = n = \deg(p)$. Our goal is to prove that V is a field. We then have

$$K(\alpha) \subseteq V \subseteq K[\alpha]$$

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Now define $V = \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We have seen that $\dim V = n = \deg(p)$. Our goal is to prove that V is a field. We then have

$$K(\alpha) \subseteq V \subseteq K[\alpha] \subseteq K(\alpha).$$

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Now define $V = \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We have seen that $\dim V = n = \deg(p)$. Our goal is to prove that V is a field. We then have

$$K(\alpha) \subseteq V \subseteq K[\alpha] \subseteq K(\alpha).$$

It then follows that $K[\alpha] = V = K(\alpha)$, and we are done.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Now define $V = \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We have seen that $\dim V = n = \deg(p)$. Our goal is to prove that V is a field. We then have

$$K(\alpha) \subseteq V \subseteq K[\alpha] \subseteq K(\alpha).$$

It then follows that $K[\alpha] = V = K(\alpha)$, and we are done.

Proof continued on next page.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Claim: $V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a field.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Claim: $V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a field.

Why is V closed under multiplication?

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Claim: $V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a field.

Why is V closed under multiplication? Answer: since $p(\alpha) = 0$, we have $\alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Claim: $V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a field.

Why is V closed under multiplication? Answer: since $p(\alpha) = 0$, we have $\alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i$.

Most of the rest of the field properties follow since $V \subseteq L$, and L is a field.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Claim: $V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a field.

Why is V closed under multiplication? Answer: since $p(\alpha) = 0$, we have $\alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i$.

Most of the rest of the field properties follow since $V \subseteq L$, and L is a field.

It remains to show that nonzero elements of V have inverses.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Claim: $V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a field.

Why is V closed under multiplication? Answer: since $p(\alpha) = 0$, we have $\alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i$.

Most of the rest of the field properties follow since $V \subseteq L$, and L is a field.

It remains to show that nonzero elements of V have inverses.

Proof continued on next page.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i\alpha^i$ for some $b_i \in K$,

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$, then define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$, then define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. So $h(\alpha) =$

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$, then define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. So $h(\alpha) = v$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$, then define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. So $h(\alpha) = v$.

Since p is irreducible, it is prime.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$, then define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. So $h(\alpha) = v$.

Since p is irreducible, it is prime. So the only prime factor that both h and p could share is p.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$, then define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. So $h(\alpha) = v$.

Since p is irreducible, it is prime. So the only prime factor that both h and p could share is p. But $\deg(h) < \deg(p)$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$, then define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. So $h(\alpha) = v$.

Since p is irreducible, it is prime. So the only prime factor that both h and p could share is p. But $\deg(h) < \deg(p)$. So $\gcd(h, p) = 1$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$, then define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. So $h(\alpha) = v$.

Since p is irreducible, it is prime. So the only prime factor that both h and p could share is p. But $\deg(h) < \deg(p)$. So $\gcd(h, p) = 1$. Therefore, there exist $f, g \in K[x]$ such that

$$fh + gp = 1.$$

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$, then define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. So $h(\alpha) = v$.

Since p is irreducible, it is prime. So the only prime factor that both h and p could share is p. But $\deg(h) < \deg(p)$. So $\gcd(h, p) = 1$. Therefore, there exist $f, g \in K[x]$ such that

$$fh + gp = 1.$$

So $1 = f(\alpha)h(\alpha) + g(\alpha)p(\alpha)$

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$, then define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. So $h(\alpha) = v$.

Since p is irreducible, it is prime. So the only prime factor that both h and p could share is p. But $\deg(h) < \deg(p)$. So $\gcd(h, p) = 1$. Therefore, there exist $f, g \in K[x]$ such that

$$fh + gp = 1.$$

So $1 = f(\alpha)h(\alpha) + g(\alpha)p(\alpha) = f(\alpha)v$.

$K[\alpha]$ versus $K(\alpha)$

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Proof continued. Let $0 \neq v \in V := \mathrm{Span}_K\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$. We claim v has a multiplicative inverse in V. Write $v = \sum_{i=0}^{n-1} b_i \alpha^i$ for some $b_i \in K$, then define $h = \sum_{i=0}^{n-1} b_i x^i \in K[x]$. So $h(\alpha) = v$.

Since p is irreducible, it is prime. So the only prime factor that both h and p could share is p. But $\deg(h) < \deg(p)$. So $\gcd(h, p) = 1$. Therefore, there exist $f, g \in K[x]$ such that

$$fh + gp = 1.$$

So $1 = f(\alpha)h(\alpha) + g(\alpha)p(\alpha) = f(\alpha)v$. Thus, the multiplicative inverse of v is $f(\alpha)$.

Finite extensions are algebraic

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Finite extensions are algebraic

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Corollary. If $[L : K] < \infty$ and $\alpha \in L$, then α is algebraic over K.

Finite extensions are algebraic

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Corollary. If $[L : K] < \infty$ and $\alpha \in L$, then α is algebraic over K.

Proof. Suppose $[L : K] < \infty$ and $\alpha \in L$.

Finite extensions are algebraic

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Corollary. If $[L : K] < \infty$ and $\alpha \in L$, then α is algebraic over K.

Proof. Suppose $[L : K] < \infty$ and $\alpha \in L$. Then since $K(\alpha)$ is a K-subvector space of L, it follows that $[K(\alpha) : K] < \infty$.

Finite extensions are algebraic

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Corollary. If $[L : K] < \infty$ and $\alpha \in L$, then α is algebraic over K.

Proof. Suppose $[L : K] < \infty$ and $\alpha \in L$. Then since $K(\alpha)$ is a K-subvector space of L, it follows that $[K(\alpha) : K] < \infty$. The result then follows from the Theorem.

Finite extensions are algebraic

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha):K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha):K] = \deg(p)$ where p is the minimal polynomial for α over K.

Corollary. If $[L:K] < \infty$ and $\alpha \in L$, then α is algebraic over K.

Proof. Suppose $[L:K] < \infty$ and $\alpha \in L$. Then since $K(\alpha)$ is a K-subvector space of L, it follows that $[K(\alpha):K] < \infty$. The result then follows from the Theorem.

Definition. A field extension L/K is *algebraic* if every element of L is algebraic over K.

Finite extensions are algebraic

Theorem. Let L/K be a field extension. Then $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. In this case, $K[\alpha] = K(\alpha)$ and $[K(\alpha) : K] = \deg(p)$ where p is the minimal polynomial for α over K.

Corollary. If $[L : K] < \infty$ and $\alpha \in L$, then α is algebraic over K.

Proof. Suppose $[L : K] < \infty$ and $\alpha \in L$. Then since $K(\alpha)$ is a K-subvector space of L, it follows that $[K(\alpha) : K] < \infty$. The result then follows from the Theorem.

Definition. A field extension L/K is *algebraic* if every element of L is algebraic over K.

Big point. We have just seen that *finite extensions are algebraic*.