# Math 361

January 30, 2023

# Today

- Quiz reminder.
- Finish proof from last time.
- Algebraic numbers, number fields.
- Primitive element theorem.
- Modules
  - definition
  - finitely generated
  - bases (free modules)
  - homomorphisms, kernels, images
  - submodules, quotient modules

# Finish theorem from last time

**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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ over $K$.

**Proof continued.**

Conversely, suppose that $\alpha$ 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 $\alpha$ over $K$.

**Proof continued.**

Conversely, suppose that $\alpha$ 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.

# $K[\alpha]$ 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 $\alpha$ over $K$.

**Proof continued.**

Conversely, suppose that $\alpha$ 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 $\alpha$ over $K$.

**Proof continued.**

Conversely, suppose that $\alpha$ 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 $\alpha$ over $K$.

**Proof continued.**

Conversely, suppose that $\alpha$ 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 $\alpha$ over $K$.

**Proof continued.**

Conversely, suppose that $\alpha$ 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 $\alpha$ over $K$.

**Proof continued.**

Conversely, suppose that $\alpha$ 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 $\alpha$ over $K$.

**Proof continued.**

Conversely, suppose that $\alpha$ 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 $p$.

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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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 $\alpha$ 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

$$fh + gp = \gcd(h, p) = 1.$$

# $K[\alpha]$ 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 $\alpha$ 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

$$fh + gp = \gcd(h, p) = 1.$$

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 $\alpha$ 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

$$fh + gp = \gcd(h, p) = 1.$$

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 $\alpha$ 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

$$fh + gp = \gcd(h, p) = 1.$$

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 $\alpha$ 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 $\alpha$ over $K$.

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

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

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

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

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

**Corollary.** If $[L : K] < \infty$ and $\alpha \in L$, then $\alpha$ 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*.

# Algebraic numbers

The set of *algebraic numbers* is

$$\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

# Algebraic numbers

The set of *algebraic numbers* is

$$\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

**Examples.**

# Algebraic numbers

The set of *algebraic numbers* is

$$\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

**Examples.** All rational numbers,

# Algebraic numbers

The set of *algebraic numbers* is

$$\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

**Examples.** All rational numbers, $\sqrt{2}$,

# Algebraic numbers

The set of *algebraic numbers* is

$$\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

**Examples.** All rational numbers, $\sqrt{2}$, $\sqrt[3]{5}$,

# Algebraic numbers

The set of *algebraic numbers* is

$$\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

**Examples.** All rational numbers, $\sqrt{2}$, $\sqrt[3]{5}$, and $e^{2k\pi/n}$ for $\neq 1$ and $k = 0, 1, \ldots n-1$.

# Algebraic numbers

The set of *algebraic numbers* is

$$\mathbb{A} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

**Examples.** All rational numbers, $\sqrt{2}$, $\sqrt[3]{5}$, and $e^{2k\pi/n}$ for $\neq 1$ and $k = 0, 1, \ldots n-1$.

A complex number that is not algebraic is *transcendental*.

# Algebraic numbers

**Proposition.** $\mathbb{A}$ is a field.

# Algebraic numbers

**Proposition.** $\mathbb{A}$ is a field.

**Proof.** It suffices to show that $\mathbb{A}$ is closed under addition and multiplication and that every nonzero element of $\mathbb{A}$ has a multiplicative inverse.

# Algebraic numbers

**Proposition.** $\mathbb{A}$ is a field.

**Proof.** It suffices to show that $\mathbb{A}$ is closed under addition and multiplication and that every nonzero element of $\mathbb{A}$ has a multiplicative inverse. Let $\alpha, \beta \in \mathbb{A}$.

# Algebraic numbers

**Proposition.** $\mathbb{A}$ is a field.

**Proof.** It suffices to show that $\mathbb{A}$ is closed under addition and multiplication and that every nonzero element of $\mathbb{A}$ has a multiplicative inverse. Let $\alpha, \beta \in \mathbb{A}$.

$\alpha$ algebraic over $\mathbb{Q} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$

# Algebraic numbers

**Proposition.** $\mathbb{A}$ is a field.

**Proof.** It suffices to show that $\mathbb{A}$ is closed under addition and multiplication and that every nonzero element of $\mathbb{A}$ has a multiplicative inverse. Let $\alpha, \beta \in \mathbb{A}$.

$\alpha$ algebraic over $\mathbb{Q} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$

$\beta$ alg. over $\mathbb{Q} \Rightarrow \beta$ alg. over $\mathbb{Q}(\alpha)$

# Algebraic numbers

**Proposition.** $\mathbb{A}$ is a field.

**Proof.** It suffices to show that $\mathbb{A}$ is closed under addition and multiplication and that every nonzero element of $\mathbb{A}$ has a multiplicative inverse. Let $\alpha, \beta \in \mathbb{A}$.

$\alpha$ algebraic over $\mathbb{Q} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$

$\beta$ alg. over $\mathbb{Q} \Rightarrow \beta$ alg. over $\mathbb{Q}(\alpha) \Rightarrow [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] < \infty$

# Algebraic numbers

**Proposition.** $\mathbb{A}$ is a field.

**Proof.** It suffices to show that $\mathbb{A}$ is closed under addition and multiplication and that every nonzero element of $\mathbb{A}$ has a multiplicative inverse. Let $\alpha, \beta \in \mathbb{A}$.

$\alpha$ algebraic over $\mathbb{Q} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$

$\beta$ alg. over $\mathbb{Q} \Rightarrow \beta$ alg. over $\mathbb{Q}(\alpha) \Rightarrow [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] < \infty$

$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha), \mathbb{Q}] < \infty$

# Algebraic numbers

**Proposition.** $\mathbb{A}$ is a field.

**Proof.** It suffices to show that $\mathbb{A}$ is closed under addition and multiplication and that every nonzero element of $\mathbb{A}$ has a multiplicative inverse. Let $\alpha, \beta \in \mathbb{A}$.

$\alpha$ algebraic over $\mathbb{Q} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$

$\beta$ alg. over $\mathbb{Q} \Rightarrow \beta$ alg. over $\mathbb{Q}(\alpha) \Rightarrow [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] < \infty$

$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha), \mathbb{Q}] < \infty \Rightarrow \mathbb{Q}(\alpha, \beta) \subset \mathbb{A}$

# Algebraic numbers

**Proposition.** $\mathbb{A}$ is a field.

**Proof.** It suffices to show that $\mathbb{A}$ is closed under addition and multiplication and that every nonzero element of $\mathbb{A}$ has a multiplicative inverse. Let $\alpha, \beta \in \mathbb{A}$.

$\alpha$ algebraic over $\mathbb{Q} \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$

$\beta$ alg. over $\mathbb{Q} \Rightarrow \beta$ alg. over $\mathbb{Q}(\alpha) \Rightarrow [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] < \infty$

$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha), \mathbb{Q}] < \infty \Rightarrow \mathbb{Q}(\alpha, \beta) \subset \mathbb{A}$

In particular, $\alpha + \beta, \alpha\beta \in \mathbb{A}$ and if $\alpha \neq 0$, then $\alpha^{-1} \in \mathbb{A}$. $\square$

# Primitive element theorem

**Definition.** A *number field* is a subfield $K \subseteq \mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$.

# Primitive element theorem

**Definition.** A *number field* is a subfield $K \subseteq \mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$.

**Theorem.** If $K$ is a number field, then there exists an algebraic number $\theta$ such that $K = \mathbb{Q}(\theta)$.

# Primitive element theorem

**Definition.** A *number field* is a subfield $K \subseteq \mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$.

**Theorem.** If $K$ is a number field, then there exists an algebraic number $\theta$ such that $K = \mathbb{Q}(\theta)$.

**Proof.** See Theorem 2.2 in our text.

# Modules

Let $R$ be a ring. An *$R$-module* or *module over $R$* is an abelian group $M$ and

# Modules

Let $R$ be a ring. An *$R$-module* or *module over $R$* is an abelian group $M$ and an operation

$$R \times M \to M$$
$$(r, m) \mapsto rm$$

such that

# Modules

Let $R$ be a ring. An *$R$-module* or *module over $R$* is an abelian group $M$ and an operation

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto rm \end{aligned}$$

such that for all $r, s \in R$ and $m, n \in M$

- $(r + s)m = rm + sm$,

# Modules

Let $R$ be a ring. An *$R$-module* or *module over $R$* is an abelian group $M$ and an operation

$$R \times M \to M$$
$$(r, m) \mapsto rm$$

such that for all $r, s \in R$ and $m, n \in M$

- $(r + s)m = rm + sm$,
- $r(m + n) = rm + rn$,

# Modules

Let $R$ be a ring. An *$R$-module* or *module over $R$* is an abelian group $M$ and an operation

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto rm \end{aligned}$$

such that for all $r, s \in R$ and $m, n \in M$

- $(r + s)m = rm + sm$,
- $r(m + n) = rm + rn$,
- $r(sm) = (rs)m$, and

# Modules

Let $R$ be a ring. An *$R$-module* or *module over $R$* is an abelian group $M$ and an operation

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto rm \end{aligned}$$

such that for all $r, s \in R$ and $m, n \in M$

- $(r + s)m = rm + sm$,
- $r(m + n) = rm + rn$,
- $r(sm) = (rs)m$, and
- $1 \cdot m = m$.

# Examples of modules

- ⋆ If $R$ is a field, then $R$-modules are exactly vector spaces over $R$.

# Examples of modules

- ⋆ If $R$ is a field, then $R$-modules are exactly vector spaces over $R$.
- ⋆ $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$ module:

# Examples of modules

$\star$ If $R$ is a field, then $R$-modules are exactly vector spaces over $R$.

$\star$ $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$ module:

If $a \in \mathbb{Z}$ and $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$, then $a\overline{b} := \overline{ab} \in \mathbb{Z}/n\mathbb{Z}$.

# Examples of modules

$\star$ Let $R$ be a ring, and let $n$ be a positive integer. Define

$$R^n := \{(r_1, \ldots, r_n) : r_i \in R\},$$

the Cartesian product of $R$ with itself $n$ times.

# Examples of modules

$\star$ Let $R$ be a ring, and let $n$ be a positive integer. Define

$$R^n := \{(r_1, \ldots, r_n) : r_i \in R\},$$

the Cartesian product of $R$ with itself $n$ times.

Then $R^n$ is an $R$-module via

$$\begin{aligned} r(r_1, \ldots, r_n) &:= (rr_1, \ldots, rr_n) \\ (r_1, \ldots, r_n) + (s_1, \ldots, s_n) &:= (r_1 + s_1, \ldots, r_n + s_n) \end{aligned}$$

for all $r \in R$ and $(r_1, \ldots, r_n), (s_1, \ldots, s_n) \in R^n$.

# Examples of modules

$\star$ Let $R$ be a ring, and let $n$ be a positive integer. Define

$$R^n := \{(r_1, \ldots, r_n) : r_i \in R\},$$

the Cartesian product of $R$ with itself $n$ times.

Then $R^n$ is an $R$-module via

$$r(r_1, \ldots, r_n) := (rr_1, \ldots, rr_n)$$
$$(r_1, \ldots, r_n) + (s_1, \ldots, s_n) := (r_1 + s_1, \ldots, r_n + s_n)$$

for all $r \in R$ and $(r_1, \ldots, r_n), (s_1, \ldots, s_n) \in R^n$.

Letting $n = 1$, we see that $R$ is, itself, and $R$-module.

# Examples of modules

$\star$ Let $R$ be a ring, and let $n$ be a positive integer. Define

$$R^n := \{(r_1, \ldots, r_n) : r_i \in R\},$$

the Cartesian product of $R$ with itself $n$ times.

Then $R^n$ is an $R$-module via

$$\begin{aligned} r(r_1, \ldots, r_n) &:= (rr_1, \ldots, rr_n) \\ (r_1, \ldots, r_n) + (s_1, \ldots, s_n) &:= (r_1 + s_1, \ldots, r_n + s_n) \end{aligned}$$

for all $r \in R$ and $(r_1, \ldots, r_n), (s_1, \ldots, s_n) \in R^n$.

Letting $n = 1$, we see that $R$ is, itself, and $R$-module.

Finally, define $R^0 = \{0\}$, the *trivial* $R$-module.

# Examples of modules

- ⋆ If $R$ is a ring, then the ring of polynomials $R[x]$ is an $R$-module.

# Examples of modules

- ⋆ If $R$ is a ring, then the ring of polynomials $R[x]$ is an $R$-module.
- ⋆ Abelian groups $G$ are exactly $\mathbb{Z}$-modules:

# Examples of modules

$\star$ If $R$ is a ring, then the ring of polynomials $R[x]$ is an $R$-module.

$\star$ Abelian groups $G$ are exactly $\mathbb{Z}$-modules:

If $g \in G$ and $n \in \mathbb{Z}_{>0}$, define

$$ng = \underbrace{g + \cdots + g}_{n-\text{times}}.$$

# Examples of modules

$\star$ If $R$ is a ring, then the ring of polynomials $R[x]$ is an $R$-module.

$\star$ Abelian groups $G$ are exactly $\mathbb{Z}$-modules:

If $g \in G$ and $n \in \mathbb{Z}_{>0}$, define

$$ng = \underbrace{g + \cdots + g}_{n-\text{times}}.$$

It $n \in \mathbb{Z}_{<0}$, define $ng = (-n)(-g)$,

# Examples of modules

$\star$ If $R$ is a ring, then the ring of polynomials $R[x]$ is an $R$-module.

$\star$ Abelian groups $G$ are exactly $\mathbb{Z}$-modules:

If $g \in G$ and $n \in \mathbb{Z}_{>0}$, define

$$ng = \underbrace{g + \cdots + g}_{n-\text{times}}.$$

It $n \in \mathbb{Z}_{<0}$, define $ng = (-n)(-g)$, and finally, for $0 \in \mathbb{Z}$, define $0g = 0$, where the second $0$ is the additive identity for $G$.

# Examples of modules

**Important**: $R$-ideals are exactly subsets $I \subseteq R$ that are $R$-modules with respect to the natural operation: if $r \in R$ and $i \in I$, then $ri$ is just multiplication in $R$.

# Finitely-generated modules

An $R$-module $M$ is *generated by* $X \subseteq M$

# Finitely-generated modules

An $R$-module $M$ is *generated by* $X \subseteq M$ if each $m \in M$ is a finite $R$-linear combination of elements of $X$:

# Finitely-generated modules

An $R$-module $M$ is *generated by* $X \subseteq M$ if each $m \in M$ is a finite $R$-linear combination of elements of $X$:

$$m = \sum_{x \in X} r_x x$$

where each $r_x$ is an element of $R$ and $r_x = 0$ for all but finitely many $x$.

# Finitely-generated modules

An $R$-module $M$ is *generated by* $X \subseteq M$ if each $m \in M$ is a finite $R$-linear combination of elements of $X$:

$$m = \sum_{x \in X} r_x x$$

where each $r_x$ is an element of $R$ and $r_x = 0$ for all but finitely many $x$. Notation:

$$M = \sum_{x \in X} Rx.$$

# Finitely-generated modules

An $R$-module $M$ is *generated by* $X \subseteq M$ if each $m \in M$ is a finite $R$-linear combination of elements of $X$:

$$m = \sum_{x \in X} r_x x$$

where each $r_x$ is an element of $R$ and $r_x = 0$ for all but finitely many $x$. Notation:

$$M = \sum_{x \in X} Rx.$$

We say $M$ is *finitely generated* if

# Finitely-generated modules

An $R$-module $M$ is *generated by* $X \subseteq M$ if each $m \in M$ is a finite $R$-linear combination of elements of $X$:

$$m = \sum_{x \in X} r_x x$$

where each $r_x$ is an element of $R$ and $r_x = 0$ for all but finitely many $x$. Notation:

$$M = \sum_{x \in X} Rx.$$

We say $M$ is *finitely generated* if it is generated by a finite set.

# Bases for modules

A *basis* for an $R$-module $M$ is a subset $B \subseteq M$ such that every element of $M$ can be written *uniquely* as a finite $R$-linear combination of $B$.

# Bases for modules

A *basis* for an $R$-module $M$ is a subset $B \subseteq M$ such that every element of $M$ can be written *uniquely* as a finite $R$-linear combination of $B$. Equivalently, $B$ is $R$-linearly independent and spans $M$.

# Bases for modules

A *basis* for an $R$-module $M$ is a subset $B \subseteq M$ such that every element of $M$ can be written *uniquely* as a finite $R$-linear combination of $B$. Equivalently, $B$ is $R$-linearly independent and spans $M$.

A *free* $R$-module is an $R$-module with a basis.

# Bases for modules

A *basis* for an $R$-module $M$ is a subset $B \subseteq M$ such that every element of $M$ can be written *uniquely* as a finite $R$-linear combination of $B$. Equivalently, $B$ is $R$-linearly independent and spans $M$.

A *free* $R$-module is an $R$-module with a basis.

Unlike vector spaces, modules do not necessarily have bases.

# Bases for modules

A *basis* for an $R$-module $M$ is a subset $B \subseteq M$ such that every element of $M$ can be written *uniquely* as a finite $R$-linear combination of $B$. Equivalently, $B$ is $R$-linearly independent and spans $M$.

A *free* $R$-module is an $R$-module with a basis.

Unlike vector spaces, modules do not necessarily have bases.

**Example.** The $\mathbb{Z}$-module $\mathbb{Z}/5\mathbb{Z}$ has no basis.

# Bases for modules

A *basis* for an $R$-module $M$ is a subset $B \subseteq M$ such that every element of $M$ can be written *uniquely* as a finite $R$-linear combination of $B$. Equivalently, $B$ is $R$-linearly independent and spans $M$.

A *free* $R$-module is an $R$-module with a basis.

Unlike vector spaces, modules do not necessarily have bases.

**Example.** The $\mathbb{Z}$-module $\mathbb{Z}/5\mathbb{Z}$ has no basis.

Is $\emptyset$ or $\{0\}$ a basis?

# Bases for modules

A *basis* for an $R$-module $M$ is a subset $B \subseteq M$ such that every element of $M$ can be written *uniquely* as a finite $R$-linear combination of $B$. Equivalently, $B$ is $R$-linearly independent and spans $M$.

A *free* $R$-module is an $R$-module with a basis.

Unlike vector spaces, modules do not necessarily have bases.

**Example.** The $\mathbb{Z}$-module $\mathbb{Z}/5\mathbb{Z}$ has no basis.

Is $\emptyset$ or $\{0\}$ a basis? No: $\mathrm{Span}_{\mathbb{Z}}\,\emptyset = \mathrm{Span}_{\mathbb{Z}}\{0\} \neq \mathbb{Z}/5\mathbb{Z}$.

# Bases for modules

A *basis* for an $R$-module $M$ is a subset $B \subseteq M$ such that every element of $M$ can be written *uniquely* as a finite $R$-linear combination of $B$. Equivalently, $B$ is $R$-linearly independent and spans $M$.

A *free* $R$-module is an $R$-module with a basis.

Unlike vector spaces, modules do not necessarily have bases.

**Example.** The $\mathbb{Z}$-module $\mathbb{Z}/5\mathbb{Z}$ has no basis.

Is $\emptyset$ or $\{0\}$ a basis? No: $\mathrm{Span}_{\mathbb{Z}} \emptyset = \mathrm{Span}_{\mathbb{Z}}\{0\} \neq \mathbb{Z}/5\mathbb{Z}$.
Otherwise, take $x \neq 0 \in \mathbb{Z}/5\mathbb{Z}$.

# Bases for modules

A *basis* for an $R$-module $M$ is a subset $B \subseteq M$ such that every element of $M$ can be written *uniquely* as a finite $R$-linear combination of $B$. Equivalently, $B$ is $R$-linearly independent and spans $M$.

A *free* $R$-module is an $R$-module with a basis.

Unlike vector spaces, modules do not necessarily have bases.

**Example.** The $\mathbb{Z}$-module $\mathbb{Z}/5\mathbb{Z}$ has no basis.

Is $\emptyset$ or $\{0\}$ a basis? No: $\mathrm{Span}_{\mathbb{Z}} \emptyset = \mathrm{Span}_{\mathbb{Z}}\{0\} \neq \mathbb{Z}/5\mathbb{Z}$.
Otherwise, take $x \neq 0 \in \mathbb{Z}/5\mathbb{Z}$. Note that $5 \neq 0 \in \mathbb{Z}$, and

# Bases for modules

A *basis* for an $R$-module $M$ is a subset $B \subseteq M$ such that every element of $M$ can be written *uniquely* as a finite $R$-linear combination of $B$. Equivalently, $B$ is $R$-linearly independent and spans $M$.

A *free* $R$-module is an $R$-module with a basis.

Unlike vector spaces, modules do not necessarily have bases.

**Example.** The $\mathbb{Z}$-module $\mathbb{Z}/5\mathbb{Z}$ has no basis.

Is $\emptyset$ or $\{0\}$ a basis? No: $\mathrm{Span}_{\mathbb{Z}} \emptyset = \mathrm{Span}_{\mathbb{Z}}\{0\} \neq \mathbb{Z}/5\mathbb{Z}$.
Otherwise, take $x \neq 0 \in \mathbb{Z}/5\mathbb{Z}$. Note that $5 \neq 0 \in \mathbb{Z}$, and

$$5 \cdot x = 0 \in \mathbb{Z}/5\mathbb{Z}$$

is a non-trivial linear relation.

# Module homomorphisms

A *homomorphism* of $R$-modules $M$ and $N$ is a mapping $\phi\colon M \to N$ that preserves addition and scalar multiplication

# Module homomorphisms

A *homomorphism* of $R$-modules $M$ and $N$ is a mapping $\phi\colon M \to N$ that preserves addition and scalar multiplication for all $u, v \in M$ and $r \in R$:

$$\phi(u+v) = \phi(u) + \phi(v)$$
$$\phi(ru) = r\phi(u).$$

# Module homomorphisms

A *homomorphism* of $R$-modules $M$ and $N$ is a mapping $\phi\colon M \to N$ that preserves addition and scalar multiplication for all $u, v \in M$ and $r \in R$:

$$\phi(u+v) = \phi(u) + \phi(v)$$
$$\phi(ru) = r\phi(u).$$

(Difference from a ring homomorphism?)

# Module homomorphisms

A *homomorphism* of $R$-modules $M$ and $N$ is a mapping $\phi\colon M \to N$ that preserves addition and scalar multiplication for all $u, v \in M$ and $r \in R$:

$$\phi(u+v) = \phi(u) + \phi(v)$$
$$\phi(ru) = r\phi(u).$$

(Difference from a ring homomorphism?)

A homomorphism is an *isomorphism* if it is bijective (in which case, the inverse is a homomorphism (exercise!)).

# Module homomorphisms

A *homomorphism* of $R$-modules $M$ and $N$ is a mapping $\phi\colon M \to N$ that preserves addition and scalar multiplication for all $u, v \in M$ and $r \in R$:

$$\phi(u+v) = \phi(u) + \phi(v)$$
$$\phi(ru) = r\phi(u).$$

(Difference from a ring homomorphism?)

A homomorphism is an *isomorphism* if it is bijective (in which case, the inverse is a homomorphism (exercise!)). The *kernel* of a homomorphism $\phi$ is

$$\ker(\phi) := \phi^{-1}(0) := \{m \in M : \phi(m) = 0\},$$

# Module homomorphisms

A *homomorphism* of $R$-modules $M$ and $N$ is a mapping $\phi\colon M \to N$ that preserves addition and scalar multiplication for all $u, v \in M$ and $r \in R$:

$$\phi(u+v) = \phi(u) + \phi(v)$$
$$\phi(ru) = r\phi(u).$$

(Difference from a ring homomorphism?)

A homomorphism is an *isomorphism* if it is bijective (in which case, the inverse is a homomorphism (exercise!)). The *kernel* of a homomorphism $\phi$ is

$$\ker(\phi) := \phi^{-1}(0) := \{m \in M : \phi(m) = 0\},$$

and the *image* is

$$\mathrm{im}(\phi) := \phi(M) := \{\phi(m) : m \in M\}.$$

# Submodules and quotient modules

A *submodule* of an $R$-module $M$ is a subset $N \subseteq M$ that is itself an $R$-module (under the operations inherited from $M$).

# Submodules and quotient modules

A *submodule* of an $R$-module $M$ is a subset $N \subseteq M$ that is itself an $R$-module (under the operations inherited from $M$).

**Exercise:** $N$ is a submodule if and only if it is nonempty and closed under addition and scalar multiplication.

# Submodules and quotient modules

A *submodule* of an $R$-module $M$ is a subset $N \subseteq M$ that is itself an $R$-module (under the operations inherited from $M$).

**Exercise:** $N$ is a submodule if and only if it is nonempty and closed under addition and scalar multiplication.

Let $M$ be an $R$-module with submodule $N$.

# Submodules and quotient modules

A *submodule* of an $R$-module $M$ is a subset $N \subseteq M$ that is itself an $R$-module (under the operations inherited from $M$).

**Exercise:** $N$ is a submodule if and only if it is nonempty and closed under addition and scalar multiplication.

Let $M$ be an $R$-module with submodule $N$. The *quotient module* $M/N$ is the set of *cosets*

$$\overline{m} = m + N := \{m + n : n \in N\}$$

# Submodules and quotient modules

A *submodule* of an $R$-module $M$ is a subset $N \subseteq M$ that is itself an $R$-module (under the operations inherited from $M$).

**Exercise:** $N$ is a submodule if and only if it is nonempty and closed under addition and scalar multiplication.

Let $M$ be an $R$-module with submodule $N$. The *quotient module* $M/N$ is the set of *cosets*

$$\overline{m} = m + N := \{m + n : n \in N\}$$

with addition and scalar multiplication defined by

$$\overline{m} + \overline{m'} := \overline{m + m'} \quad \text{and}$$

# Submodules and quotient modules

A *submodule* of an $R$-module $M$ is a subset $N \subseteq M$ that is itself an $R$-module (under the operations inherited from $M$).

**Exercise:** $N$ is a submodule if and only if it is nonempty and closed under addition and scalar multiplication.

Let $M$ be an $R$-module with submodule $N$. The *quotient module* $M/N$ is the set of *cosets*

$$\overline{m} = m + N := \{m + n : n \in N\}$$

with addition and scalar multiplication defined by

$$\overline{m} + \overline{m'} := \overline{m + m'} \quad \text{and} \quad r\overline{m} := \overline{rm}.$$

# Examples of $\mathbb{Z}$-modules

# Examples of $\mathbb{Z}$-modules

$\mathbb{Z}[x]$ generating set:

# Examples of $\mathbb{Z}$-modules

$\mathbb{Z}[x]$ generating set: $\{1, x, x^2, \ldots\}$

# Examples of $\mathbb{Z}$-modules

$\mathbb{Z}[x]$ generating set: $\{1, x, x^2, \ldots\}$

$\mathbb{Z}[i]$ generating set:

# Examples of $\mathbb{Z}$-modules

$\mathbb{Z}[x]$ generating set: $\{1, x, x^2, \ldots\}$

$\mathbb{Z}[i]$ generating set: $\{1, i\}$

# Examples of $\mathbb{Z}$-modules

| | | |
|---|---|---|
| $\mathbb{Z}[x]$ | generating set: | $\{1, x, x^2, \ldots\}$ |
| $\mathbb{Z}[i]$ | generating set: | $\{1, i\}$ |
| $\mathbb{Z}$ | generating set: | |

# Examples of $\mathbb{Z}$-modules

| | | |
|---|---|---|
| $\mathbb{Z}[x]$ | generating set: | $\{1, x, x^2, \ldots\}$ |
| $\mathbb{Z}[i]$ | generating set: | $\{1, i\}$ |
| $\mathbb{Z}$ | generating set: | $\{1\}$ |

# Examples of $\mathbb{Z}$-modules

| | | |
|---|---|---|
| $\mathbb{Z}[x]$ | generating set: | $\{1, x, x^2, \ldots\}$ |
| $\mathbb{Z}[i]$ | generating set: | $\{1, i\}$ |
| $\mathbb{Z}$ | generating set: | $\{1\}$ |
| $\mathbb{Z}[x, y]/(x^2, y^2)$ | generating set: | |

# Examples of $\mathbb{Z}$-modules

| | | |
|---|---|---|
| $\mathbb{Z}[x]$ | generating set: | $\{1, x, x^2, \ldots\}$ |
| $\mathbb{Z}[i]$ | generating set: | $\{1, i\}$ |
| $\mathbb{Z}$ | generating set: | $\{1\}$ |
| $\mathbb{Z}[x, y]/(x^2, y^2)$ | generating set: | $\{1, x, y, xy\}$. |

# Finitely-generated free modules

**Proposition.** A finitely-generated $R$-module $M$ is free if and only if it is isomorphic to $R^n$ for some $n \geq 0$.

# Finitely-generated free modules

**Proposition.** A finitely-generated $R$-module $M$ is free if and only if it is isomorphic to $R^n$ for some $n \geq 0$.

**Proof.** If $b_1, \ldots, b_n$ is a basis, define $\phi\colon M \to R^n$ by $b_i \mapsto e_i$ and extending linearly:

# Finitely-generated free modules

**Proposition.** A finitely-generated $R$-module $M$ is free if and only if it is isomorphic to $R^n$ for some $n \geq 0$.

**Proof.** If $b_1, \ldots, b_n$ is a basis, define $\phi\colon M \to R^n$ by $b_i \mapsto e_i$ and extending linearly:

$$\phi(\textstyle\sum_{i=1}^n r_i b_i) := \sum_{i=1}^n r_i \phi(b_i) = \sum_{i=1}^n r_i e_i = (r_1, \ldots, r_n) \in R^n.$$

# Finitely-generated free modules

**Proposition.** A finitely-generated $R$-module $M$ is free if and only if it is isomorphic to $R^n$ for some $n \geq 0$.

**Proof.** If $b_1, \ldots, b_n$ is a basis, define $\phi\colon M \to R^n$ by $b_i \mapsto e_i$ and extending linearly:

$$\phi(\textstyle\sum_{i=1}^n r_i b_i) := \sum_{i=1}^n r_i \phi(b_i) = \sum_{i=1}^n r_i e_i = (r_1, \ldots, r_n) \in R^n.$$

Conversely, if $\phi\colon M \to R^n$ is an isomorphism, then

# Finitely-generated free modules

**Proposition.** A finitely-generated $R$-module $M$ is free if and only if it is isomorphic to $R^n$ for some $n \geq 0$.

**Proof.** If $b_1, \ldots, b_n$ is a basis, define $\phi\colon M \to R^n$ by $b_i \mapsto e_i$ and extending linearly:

$$\phi(\textstyle\sum_{i=1}^n r_i b_i) := \sum_{i=1}^n r_i \phi(b_i) = \sum_{i=1}^n r_i e_i = (r_1, \ldots, r_n) \in R^n.$$

Conversely, if $\phi\colon M \to R^n$ is an isomorphism, then define $b_i = \phi^{-1}(e_i)$ for $i = 1, \ldots, n$ to get a basis. $\square$.

# Finitely-generated free modules

**Proposition.** A finitely-generated $R$-module $M$ is free if and only if it is isomorphic to $R^n$ for some $n \geq 0$.

**Proof.** If $b_1, \ldots, b_n$ is a basis, define $\phi\colon M \to R^n$ by $b_i \mapsto e_i$ and extending linearly:

$$\phi(\textstyle\sum_{i=1}^n r_i b_i) := \sum_{i=1}^n r_i \phi(b_i) = \sum_{i=1}^n r_i e_i = (r_1, \ldots, r_n) \in R^n.$$

Conversely, if $\phi\colon M \to R^n$ is an isomorphism, then define $b_i = \phi^{-1}(e_i)$ for $i = 1, \ldots, n$ to get a basis. $\square$.

**Example.**

$$\begin{aligned} \mathbb{Z}[i] &\to \mathbb{Z}^2 \\ a + bi &\mapsto (a, b), \end{aligned}$$