Generation of Modules, Direct Sums and Free Modules

Kevin James

Definition

Suppose $N_1, \ldots, N_n$ are R-submodules of M.

1. $N_1 + \cdots + N_n = \{\sum_{i=1}^{n} a_i \quad | \quad a_i \in N_i\}$.

Definition

Suppose $N_1, \ldots, N_n$ are R-submodules of M.

1. $N_1 + \cdots + N_n = \{\sum_{i=1}^n a_i \quad | \quad a_i \in N_i\}$.
2. For $A \subseteq M$, let
   $RA = \{\sum_{i=1}^m r_i a_i \quad | \quad r_i \in R; a_i \in A; 0 < m \in \mathbb{Z}\}$, and
   $R\emptyset = \{0\}$.

Definition

Suppose $N_1, \ldots, N_n$ are R-submodules of M.

1. $N_1 + \cdots + N_n = \{\sum_{i=1}^n a_i \quad | \quad a_i \in N_i\}$.
2. For $A \subseteq M$, let $RA = \{\sum_{i=1}^m r_i a_i \quad | \quad r_i \in R; a_i \in A; 0 < m \in \mathbb{Z}\}$, and $R\emptyset = \{0\}$.
    - If $A = \{a_1, \ldots, a_n\}$, then $RA = Ra_1 + \cdots + Ra_n$.

Definition

Suppose $N_1, \ldots, N_n$ are R-submodules of M.

1. $N_1 + \cdots + N_n = \{\sum_{i=1}^{n} a_i \quad | \quad a_i \in N_i\}$.
2. For $A \subseteq M$, let
   $RA = \{\sum_{i=1}^{m} r_i a_i \quad | \quad r_i \in R; a_i \in A; 0 < m \in \mathbb{Z}\}$, and
   $R\emptyset = \{0\}$.
   - If $A = \{a_1, \ldots, a_n\}$, then $RA = Ra_1 + \cdots + Ra_n$.
   - We call RA the submodule of M generated by A.

Definition

Suppose $N_1, \ldots, N_n$ are R-submodules of M.

1. $N_1 + \cdots + N_n = \{\sum_{i=1}^n a_i \quad | \quad a_i \in N_i\}$.
2. For $A \subseteq M$, let $RA = \{\sum_{i=1}^m r_i a_i \quad | \quad r_i \in R; a_i \in A; 0 < m \in \mathbb{Z}\}$, and $R\emptyset = \{0\}$.
   - If $A = \{a_1, \ldots, a_n\}$, then $RA = Ra_1 + \cdots + Ra_n$.
   - We call RA the submodule of M generated by A.
   - If $N = RA$ for $A \subseteq M$, then we say that A is a set of generators for N.

Definition

Suppose $N_1, \ldots, N_n$ are R-submodules of M.

1. $N_1 + \cdots + N_n = \{\sum_{i=1}^n a_i \mid a_i \in N_i\}$.
2. For $A \subseteq M$, let
   $RA = \{\sum_{i=1}^m r_i a_i \mid r_i \in R; a_i \in A; 0 < m \in \mathbb{Z}\}$, and
   $R\emptyset = \{0\}$.
   - If $A = \{a_1, \ldots, a_n\}$, then $RA = Ra_1 + \cdots + Ra_n$.
   - We call RA the submodule of M generated by A.
   - If $N = RA$ for $A \subseteq M$, then we say that A is a set of generators for N.
3. If $N \leq M$ and $N = RA$ where $|A| < \infty$, then we say that N is finitely generated.

Definition

Suppose $N_1, \ldots, N_n$ are R-submodules of M.

1. $N_1 + \cdots + N_n = \{\sum_{i=1}^n a_i \quad | \quad a_i \in N_i\}$.
2. For $A \subseteq M$, let
   $RA = \{\sum_{i=1}^m r_i a_i \quad | \quad r_i \in R; a_i \in A; 0 < m \in \mathbb{Z}\}$, and
   $R\emptyset = \{0\}$.
   - If $A = \{a_1, \ldots, a_n\}$, then $RA = Ra_1 + \cdots + Ra_n$.
   - We call RA the submodule of M generated by A.
   - If $N = RA$ for $A \subseteq M$, then we say that A is a set of generators for N.
3. If $N \leq M$ and $N = RA$ where $|A| < \infty$, then we say that N is finitely generated.
4. If $N = Ra$, then N is said to be cyclic.

Note

1. Since $1 \in R$, $A \subseteq RA$.

Note

1. Since $1 \in R$, $A \subseteq RA$.
2. RA is the smallest submodule containing A.

Note

1. Since $1 \in R$, $A \subseteq RA$.
2. RA is the smallest submodule containing A.
3. If $N_i = RA_i$ for $1 \leq i \leq m$, then $N_1 + \cdots + N_m = R[A_1 \cup \cdots \cup A_m]$.

Note

1. Since $1 \in R$, $A \subseteq RA$.
2. RA is the smallest submodule containing A.
3. If $N_i = RA_i$ for $1 \leq i \leq m$, then $N_1 + \cdots + N_m = R[A_1 \cup \cdots \cup A_m]$.
4. If $N \leq M$, there may be many different generating sets. If N is finitely generated, then there is a minimal size among all generating sets. We call a generating set of this size a <u>minimal generating set</u>. It is not necessarily unique.

Note

1. Since $1 \in R$, $A \subseteq RA$.
2. RA is the smallest submodule containing A.
3. If $N_i = RA_i$ for $1 \leq i \leq m$, then $N_1 + \cdots + N_m = R[A_1 \cup \cdots \cup A_m]$.
4. If $N \leq M$, there may be many different generating sets. If N is finitely generated, then there is a minimal size among all generating sets. We call a generating set of this size a minimal generating set. It is not necessarily unique.

Example

Let $R = F[x_1, x_2, \ldots]$ where F is a field.
Take $A = \{x_1, \ldots\}$ and $N = RA$.
Note that R is a cyclic $R - module$, while

Note

1. Since $1 \in R$, $A \subseteq RA$.
2. RA is the smallest submodule containing A.
3. If $N_i = RA_i$ for $1 \leq i \leq m$, then $N_1 + \cdots + N_m = R[A_1 \cup \cdots \cup A_m]$.
4. If $N \leq M$, there may be many different generating sets. If N is finitely generated, then there is a minimal size among all generating sets. We call a generating set of this size a minimal generating set. It is not necessarily unique.

Example

Let $R = F[x_1, x_2, \ldots]$ where F is a field.
Take $A = \{x_1, \ldots\}$ and $N = RA$.
Note that R is a cyclic $R - module$, while
N is a proper subset of R is not finitely generated.

Example

Suppose that V is a vector space over a field F and $T : V \to V$ is a linear transformation. When is V cyclic as an $F[x]$-module with structure as before $(p(x) \cdot \vec{v} = \sum_{i=1}^{d_p} p_i T^i(\vec{v}))$.

Example

Suppose that V is a vector space over a field F and $T : V \to V$ is a linear transformation. When is V cyclic as an $F[x]$-module with structure as before $(p(x) \cdot \vec{v} = \sum_{i=1}^{d_p} p_i T^i(\vec{v}))$.

Definition

Suppose that $M_1, \ldots, M_k$ are R-modules. Then $M_1 \times \cdots \times M_k$ is an R module with addition and R-action defined component-wise.

Example

Suppose that V is a vector space over a field F and $T : V \to V$ is a linear transformation. When is V cyclic as an $F[x]$-module with structure as before $(p(x) \cdot \vec{v} = \sum_{i=1}^{d_p} p_i T^i(\vec{v}))$.

Definition

Suppose that $M_1, \ldots, M_k$ are R-modules. Then $M_1 \times \cdots \times M_k$ is an R module with addition and R-action defined component-wise.

Note

$M_1 \times \cdots \times M_k$ is referred to as the <u>external direct sum</u> and denoted $M_1 \oplus \cdots \oplus M_k$. When the number of modules is not finite, the definition of direct sum and direct product may differ.

Proposition

Suppose that $N_1, \ldots, N_k \leq M$. The following are equivalent.

1. *The map $\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$ defined by $\pi((a_1, \ldots, a_k)) = \sum_{i=1}^{k} a_i$. is an isomorphism.*
2. $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0, \forall 1 \leq j \leq k.$
3. *Every $x \in N_1 + \cdots + N_k$ has a unique expression of the form $x = \sum_{i=1}^{k} a_i$ with $a_i \in N_i$.*

Proposition

Suppose that $N_1, \ldots, N_k \leq M$. *The following are equivalent.*

1. *The map* $\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$ *defined by* $\pi((a_1, \ldots, a_k)) = \sum_{i=1}^{k} a_i$. *is an isomorphism.*
2. $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = 0, \forall 1 \leq j \leq k$.
3. *Every* $x \in N_1 + \cdots + N_k$ *has a unique expression of the form* $x = \sum_{i=1}^{k} a_i$ *with* $a_i \in N_i$.

Definition

Suppose that $N_i, \ldots, N_k \leq M$ and $M = N_1 + \cdots + N_k$ and $N_i, \ldots, N_k$ satisfy the condition of the previous Proposition. Then we write $M = N_1 \oplus \cdots \oplus N_k$

Definition

An R-module F is said to be free on a set A if $\forall 0_F \neq x \in F$ there exists a unique choice of $r_1, \ldots, r_n \in R$; $a_1, \ldots, a_n \in A$ such that $x = \sum_{i=1}^{n} r_i a_i$.

Definition

An R-module F is said to be free on a set A if $\forall 0_F \neq x \in F$ there exists a unique choice of $r_1, \ldots, r_n \in R$; $a_1, \ldots, a_n \in A$ such that $x = \sum_{i=1}^{n} r_i a_i$.
In this case, we say that A is a basis set or a set of free generators for F.

Definition

An R-module F is said to be free on a set A if $\forall 0_F \neq x \in F$ there exists a unique choice of $r_1, \ldots, r_n \in R$; $a_1, \ldots, a_n \in A$ such that $x = \sum_{i=1}^{n} r_i a_i$.
In this case, we say that A is a basis set or a set of free generators for F.
If R is commutative then $|A|$ is called the rank of F.

Definition

An R-module F is said to be free on a set A if $\forall 0_F \neq x \in F$ there exists a unique choice of $r_1, \ldots, r_n \in R$; $a_1, \ldots, a_n \in A$ such that $x = \sum_{i=1}^n r_i a_i$.
In this case, we say that A is a basis set or a set of free generators for F.
If R is commutative then $|A|$ is called the rank of F.

Example

Take $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $N_1 = N_2 = \mathbb{Z}/2\mathbb{Z}$.

Definition

An R-module F is said to be free on a set A if $\forall 0_F \neq x \in F$ there exists a unique choice of $r_1, \ldots, r_n \in R$; $a_1, \ldots, a_n \in A$ such that $x = \sum_{i=1}^n r_i a_i$.
In this case, we say that A is a basis set or a set of free generators for F.
If R is commutative then $|A|$ is called the rank of F.

Example

Take $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $N_1 = N_2 = \mathbb{Z}/2\mathbb{Z}$.
Then, each element of M can be uniquely written as $n_1 + n_2$ ($n_i \in N_i$). However, $n_1 = 3n_1 = 5n_1 = \ldots$. Thus, M is not a free $\mathbb{Z}$-module on $\{(0,1),(1,0)\}$.

Theorem

For any set A, there is a free R-module $F(A)$ on the set A. Further, $F(A)$ satisfies the following universal property. If M is any R-module and $\phi : A \to M$ is any map. Then there is a unique homomorphism $\Phi : F(A) \to M$ satisfying $\Phi(a) = \phi(a)$.

$$\begin{array}{ccc} A & \xhookrightarrow{\textit{inclusion}} & F(A) \\ & \phi \searrow & \downarrow \Phi \\ & & M \end{array}$$

Theorem

For any set A, there is a free R-module $F(A)$ on the set A. Further, $F(A)$ satisfies the following universal property. If M is any R-module and $\phi : A \to M$ is any map. Then there is a unique homomorphism $\Phi : F(A) \to M$ satisfying $\Phi(a) = \phi(a)$.

$$\begin{array}{ccc} A & \xhookrightarrow{\text{inclusion}} & F(A) \\ & \phi \searrow & \downarrow \Phi \\ & & M \end{array}$$

Corollary

1. *If F_1 and F_2 are free over A, there exists a unique isomorphism $\phi : F_1 \to F_2$ with $\phi|_A = id$.*
2. *If F is any free R-module with basis A, then $F \cong F(A)$. In particular, F has the same universal property as $F(A)$.*