Generators, Linear dependence, and Bases

Definition: Let R be a ring and M be a (left) R-module. A linear combination of finitely many elements $m_1, \dots, m_n$ of M is an element of the form $r_1 m_1 + \cdots + r_n m_n \in M$ for some $r_1, \dots, r_n \in R$.

Definition: Let R be a ring and M be a (left) R-module. Let A be a subset of M. The submodule of M **generated by** A is the submodule RA of M given by the three equivalent following descriptions:

- RA is the unique smallest R-submodule of M containing A.
- $RA = \bigcap N_\lambda$, where N_λ ranges over all submodules of M containing A.
- $RA = \{r_1 m_1 + \cdots + r_t m_t \mid r_i \in R, m_i \in A\}$, the set of linear combinations of elements of A.

Definition: Let R be a ring and M be a (left) R-module. Let A be a subset of M.

- We say that A **generates** M if $RA = M$.
- We say that A is **linearly independent** if for $m_1, \dots, m_t \in A$ distinct and any $r_1, \dots, r_t \in R$,
$$r_1 m_1 + \cdots + r_t m_t = 0 \quad \text{implies} \quad r_1 = \cdots = r_t = 0.$$
- We say that A is a **basis** of M if A is linearly independent and generates M.
- We say that M is **free** if there exists a basis A for M.

(1) Let $R = \mathbb{Z}$ and consider the R-module $M = \mathbb{Z}/n$ for some $n > 1$.

(a) Explain why any nonempty subset of M is *not* linearly independent.

(b) Explain why M is *not* a free module.

(c) An R-module is **cyclic** if it is generated by a single element. Show that M is cyclic.

(d) Does every generating set of M consist of a single element?

(a) Let $S \neq \varnothing$ and $m \in S$. Then $n \cdot m = 0$ but $n \neq 0$ in $\mathbb{Z}$, so M is not linearly independent.

(b) M has no nonempty linearly independent subset, there there can be no nonempty basis. Also, the empty set is not a basis, since it does not span M.

(c) The element $[1]_n$ spans M, since any element $[i]_n$ can be written as $i \cdot [1]_n$.

(d) No; $\{[0]_n, [1]_n\}$ is also a generating set, for example.

(2) Let R be a commutative ring. Let $R[x]$ be a polynomial ring over R.

(a) Explain why $\{1, x, x^2, x^3, \dots\}$ is a basis for $R[x]$ as an R-module.

(b) Give an example of a set that is R-linearly independent in $R[x]$ that is not a basis.

(c) Give an example of a set that generates $R[x]$ that is not a basis.

(d) Give a different example of a basis for $R[x]$.

(a) Any element of $R[x]$ can be written as $r_n x^n + \cdots + r_0$ for some $r_0, \dots, r_n \in R$, so these elements generate. If $r_n x^n + \cdots + r_0$ is the zero of $R[x]$ then all the coefficients are zero, so these elements are linearly independent.

(b) The set $\{1\}$ works, for example.

(c) The set $\{1, x, x^2, \dots, 2\}$ works, for example.

(d) The set $\{-1, x, x^2, \dots\}$ is another basis.

(3) Show that an R-module M is cyclic if and only if $M \cong R/I$ for some left ideal I.

[1] This includes 0 as the "empty sum".

For a module of the form R/I, the element $1 + I$ is a generator, since any element $r + I$ can be written as $r(1 + I)$. If $\psi : R/I \to M$ is an isomorphism, then $\psi(1 + I)$ is a generator, since any element can be written as $\psi(r + I) = \psi(r(1 + I)) = r\psi(1 + I)$. Thus, if $M \cong R/I$, then M is cyclic.

Now suppose that M is cyclic, and write $M = Rm$. Consider the homomorphism $\phi : R \to M$ given by $\phi(r) = rm$. This map is an R-module homomorphism by an argument similar to class. The image of ϕ is $Rm = M$, so ϕ is cyclic. The kernel of ϕ is a submodule of R, which is a left ideal. By the First Isomorphism Theorem, we are done.

(4) Let $R = \mathbb{Z}[x]$ and I be the ideal $(2, x)$, considered as an R-module.
  (a) Explain[2] why I is not cyclic.
  (b) Show that I is not free.
  (c) Give an example of a pair of modules $N \subseteq M$ where N requires more generators than M.
  (d) Give an example of a pair of modules $N \subseteq M$ where M is free and N is not.

(5) We say that an R-module M is **simple** if the only submodules of M are 0 and M. Let R be a commutative ring. Show that M is simple if and only if $M \cong R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ of R.

(6) Let R be a commutative ring, and x, y be two indeterminates.
  (a) Show that $R[x, y]$ is a free $R[x]$-module, and find a basis.
  (b) Show that $R[x, y]$ is a free R module, and find a basis.

[2] Reuse something from 817!