## 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

$$RA = \bigcap_{\substack{N \supseteq A \\ N \text{ submodule of } M}} N.$$

Concretely,

$$RA = \{r_1 m_1 + \cdots + r_t m_t \mid r_i \in R, m_i \in A\}$$

is[1] the set of linear combinations of finite subsets 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?

**(2)** Let $R$ be a commutative ring. Let $R[x]$ be a polynomial ring over $R$, and consider $R[x]$ as an $R$-module.
  **(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 $R[x]$.

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

(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 $R$.

[1] If $A = \varnothing$, we allow $0$ as the "empty sum".

[2] Reuse something from 817!