Abstract

We show that if E is a module defined over a principal ideal domain R, then E is uniquely decomposable as $E \cong R^r \oplus R/\langle q_1\rangle \oplus \cdots \oplus R/\langle q_n\rangle$, where R^r is a free module of rank r, and $q_1|q_2|\cdots|q_n$, a result known as the structure theorem for modules over principal ideal domains. To do this, we provide an overview of results from the theory of modules before stating and proving the result.

Definition. Let A be a ring. A *left A-module* M is an abelian group with an operation of A on M such that

$$(a+b)x = ax + bx$$
$$a(x+y) = ax + ay$$

for all $a, b \in A$ and $x, y \in M$.

If M is an A-module, then $N \subseteq M$ is known as a *submodule* of N is a subgroup such that $AN \subseteq N$.

One of the most important submodules is the torsion submodule.

Definition. Let A be an integral domain, and let M be an A-module. The *torsion submodule* of M, denoted M_{tor}, is the subset of elements $x \in M$ such that there exists a nonzero $a \in A$ with $ax = 0$.

From here on out, we assume that all our modules are over integral domains.

Just as there are isomorphism theorems for groups and rings, there are isomorphism theorems for modules. There is also a rich theory of morphisms between modules that we will discuss elsewhere.

Definition. Let $\mathfrak{a} \subseteq A$ be a left ideal, and let M be a module. We define $\mathfrak{a}M$ to be the set of all elements

$$a_1x_1 + \cdots + a_nx_n,$$

where $a_i \in \mathfrak{a}$ and $x_i \in M$.

We will now discuss modules generated by some subset of the module M. These will become important as we go deeper into establishing the structure theorem.

Definition. Let M be an A-module, and let $S \subseteq M$. A linear combination of elements of S is a finite sum of the form

$$\sum_{x \in S} a_x x,$$

where $a_x \in A$.

If N is the set of all linear combinations of S, then N is a submodule of M, known as the submodule generated by S, written $N = A\langle S\rangle$.

If S consists of one element x, the module generated by x is written Ax, or $\langle x\rangle$, which we call a principal module.

Definition. A module M is said to be finitely generated if it has a finite number of generators.

If M is an A-module, and $\{M_i\}_{i\in I}$ is a family of submodules, we have a family of inclusion homomorphisms $\lambda_i \colon M_i \to M$, which induces a module homomorphism $\lambda \colon \bigoplus_{i\in I} M_i \to M$, where

$$\lambda\big((x_i)_{i\in I}\big) = \sum_{i\in I} x_i,$$

are finite sums.

Now, if $\lambda \colon \bigoplus_{i\in I} M_i \to M$ is an isomorphism, then the family $\{M_i\}_{i\in I}$ is a direct sum decomposition of M.

If M is a module, and N, N' are submodules such that $N + N' = M$ and $N \cap N' = \{0\}$, then we have a module isomorphism $M \cong N \oplus N'$.

Definition. If M is an A-module, then a subset $S \subseteq M$ is called a *basis* if S is nonempty, linearly independent,[I] and generates M.

A *free module* is a module that admits a basis.

Theorem: Let M be a free A-module with basis $\{x_i\}_{i\in I}$. Then, if N is an A-module with $\{y_i\}_{i\in I} \subseteq N$ indexed by the same indexing set as $\{x_i\}_{i\in I}$, then there is a unique module homomorphism $f\colon M \to N$ such that $f(x_i) = y_i$ for all i.

Proof. Let $x = \sum_{i\in I} a_i x_i$, where the $\{a_i\}_{i\in I}$ are unique. Define

$$f(x) = \sum_{i\in I} a_i y_i,$$

which yields a unique homomorphism between M and N. □

Note that by definition, if M is a free module with basis $\{x_i\}_{i\in I}$, then we must have

$$M = \bigoplus_{i\in I} Ax_i,$$

and that if $\mathfrak{a} \subseteq A$ is a two-sided ideal, then there is an isomorphism of A-modules[II]

$$M/\mathfrak{a}M \cong \bigoplus_{i\in I} Ax_i/\mathfrak{a}x_i,$$

and each $Ax_i/\mathfrak{a}x_i$ is isomorphic to $A/\mathfrak{a}$ as an A-module.

A module of the form $M = Ax$ for some $x \in M$ is known as *principal*, and the map $a \mapsto ax$ is a module homomorphism that induces an isomorphism $A/\mathfrak{a} \cong M$, where $\mathfrak{a}$ is the kernel.

Just as there are free modules with bases, there is such a thing as a free module generated by a set S, denoted $A[S]$. If S is a group, this gives rise to the group algebra.

[I] Linear independence is defined for modules similar to how it is defined for vector spaces.
[II] The quotient module $M/\mathfrak{a}M$ is defined analogously to a quotient group or quotient vector space.