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.

Module Basics

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 $ax = 0$.

If $M_{\text{tor}} = \{0\}$, then we say M is *torsion-free*.

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 $M \cong N \oplus N'$.

Establishing the Structure Theorem

From here on out, we assume all modules are over principal ideal domains.

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 we may take this homomorphism to be surjective, meaning that any module N is a quotient $M/\ker(\varphi)$, where M is a free module, and $\varphi\colon M \to N$ is a surjective module homomorphism.

Corollary: Let E be a finitely generated module, and let E' be a submodule. Then, E' is finitely generated.

Proof. Let $\{v_1, \dots, v_n\}$ be generators for E. Since E is a module, there is a free module F with basis $\{x_1, \dots, x_n\}$ and a surjective module homomorphism $\varphi\colon F \to E$ such that $x_i \mapsto v_i$.

Then, $\varphi^{-1}(E') \subseteq F$ is a submodule that is free and finitely generated, so E' is finitely generated. □

Theorem: Let E be a finitely generated module with torsion submodule E_{tor}. Then, E/E_{tor} is free, and there exists a free submodule F of E such that

$$E = E_{\text{tor}} \oplus F.$$

Furthermore, the dimension of F is uniquely determined.

Proof. We start by proving that E/E_{tor} is torsion-free. For $x \in E$, write $\overline{x}$ to be the residue class modulo E_{tor}. If $- \neq b \in R$ is such that $b\overline{x} = 0$, then $bx \in E_{\text{tor}}$, so there exists $0 \neq c \in R$ such that $cbx = 0$. Thus, $x \in E_{\text{tor}}$, and $\overline{x} = 0$, meaning that E/E_{tor} is torsion-free (and finitely-generated, as it is a quotient of a

[I] Linear independence is defined for modules similar to how it is defined for vector spaces.

finitely generated module).

Let M be a finitely generated torsion-free module. Let $\{y_1,\dots,y_m\}$ be the set of generators of M, and let $\{v_1,\dots,v_n\}$ be a maximally linearly independent set. If $y\in\{y_1,\dots,y_m\}$, then there exist elements $a,b_1,\dots,b_n\in R$ not all zero such that

$$0 = ay + b_1v_1 + \cdots + b_nv_n,$$

and $a\neq 0$. Thus, $ay\in\langle v_1,\dots,v_n\rangle$, meaning that for any $j=1,\dots,m$, we may find $a_j\in R$ with $a_j\neq 0$ and $a_jy_j\in\langle v_1,\dots,v_n\rangle$.

Letting $a=a_1\cdots a_m$ be the product, we have $aM\subseteq\langle v_1,\dots,v_m\rangle$ with $a\neq 0$, so the map $x\mapsto ax$ is an injective homomorphism whose image is contained in a free module isomorphic to M, meaning M is a free module.

To obtain the free submodule F, we need a lemma.

Lemma: Let E and E' be modules, with E' free. If $f\colon E\to E'$ is a surjective homomorphism, there is a free submodule F of E such that restricting f to F induces an isomorphism between F and E', with $E=F\oplus\ker(f)$.

Proof. Let $\{x_i'\}_{i\in I}$ be a basis of E'. For each i, let x_i be an element of E such that $f(x_i)=x_i'$, and let $F=\left\langle\{x_i\}_{i\in I}\right\rangle$. The family $\{x_i\}_{i\in I}$ as selected is linearly independent, meaning F is free.

Given $x\in E$, there exist $a_i\in R$ such that

$$f(x)=\sum_{i\in I}a_ix_i',$$

and $x-\sum_{i\in I}a_ix_i\in\ker(f)$. Thus, $E=\ker(f)+F$. Furthermore, by linear independence, $\ker(f)\cap F=\{0\}$, so the sum is direct. □

We apply this lemma to the homomorphism $E\to E/E_{\text{tor}}$ to get the decomposition $E=E_{\text{tor}}\oplus F$; since F is isomorphic to E/E_{tor}, the dimension is unique. □

Definition. The dimension of F in the decomposition $E=E_{\text{tor}}\oplus F$ is known as the *rank* of E.

Definition. Let E be an R-module, and let $x\in E$. The map $a\mapsto ax$ is a homomorphism of R onto $\langle x\rangle$, whose kernel is a principal ideal $\langle m\rangle\subseteq R$. We say m is a *period* of x. Note that m is detemrined up to multiplication by a unit (assuming $m\neq 0$)

An element $0\neq c\in R$ is called an exponent for E (x) if $cE=0$ $(cx=0)$.