Module Theory, Part I: Introduction, Module Homomorphisms

Jay Havaldar

Definition: Let R be a ring. A module M over a ring R is an abelian group (with operation $+$) and a map $R \times M \to M$ which satisfies distributivity and associativity. If R has a 1, then we require that $1m = m$ for each $m \in M$.

These axioms should look fairly familiar. if R is a field, then a module is exactly a vector space over R. A module is nothing more than a generalization of vector spaces.

Definition: A submodule is a closed subgroup N of an R-module M which is closed under the action of R.

Example A significant example is modules over $\mathbb{Z}$. The action of an integer on $m \in M$ is defined straightforwardly as:

$$nm = m + m + \cdots + m$$

Where we are adding m to itself n times. This is the only possible action of $\mathbb{Z}$ over M, because of associativity and distributivity. What we have from this is that:

$\mathbb{Z}$-modules are exactly abelian groups.

In particular, $\mathbb{Z}$-submodules are exactly submodules of subgroups.

Example By associativity, we can define a module over $F[x]$, where F is a field. We simply need to define how $1, x$ act on elements in the module. Let V be a vector space over F -- we will make V an $F[x]$ module, by identifying the action of x with a linear transformation $T : V \to V$.

Conversely, if we have any module V over $F[x]$, then in particular V is a module over F. But we know that:

$$x(v + w) = xv + xw$$
$$x(av) = ax(v)$$

So this means that indeed x is a linear transformation. So there is a natural isomorphism between vector spaces V over F equipped with a linear transformation T and modules V over $F[x]$.

Consequently, the $F[x]$-submodules of V are exactly vector subspaces of V which are invariant under T.

Proposition

> A nonempty N of an R-module M is a submodule iff $x + ry \in N$ for each $x, y \in N$, $r \in R$.

Let $r = -1$ and we get the subgroup criterion. Let $x = 0$ and we get closure under elements of R. The converse case is fairly straightforward.

0.1 Quotient Modules and Module Homomorphisms

Definition: Let R be a ring and M, N are R-modules. Then an R-module homomorphism φ is a map from M to N so that:

$$\varphi(x+y) = \varphi(x) + \varphi(y)$$
$$\varphi(rx) = r\varphi(x)$$

As expected, an isomorphism is surjective as well as injective. The kernel and images are respectively submodules of M, N as expected. Finally, we define $Hom_R(M, N)$ to be the set of all R-module homomorphisms from M to N.

For example, $\mathbb{Z}$-module homomorphisms are simply abelian group homomorphisms (since the second criterion is implied by the first above). Over a field, the F-module homomorphisms are simply linear transformations between vector spaces. Note, however, that R-module homomorphisms where R is a ring do not necessarily have any connection to ring homomorphisms -- specifically because there is no requirement that a module homomorphism send identity to identity.

Proposition

> $Hom_R(M, N)$ is an R-module.

We can define addition and multiplication in the usual way:

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m)$$
$$(r\varphi)(m) = r(\varphi(m))$$

Furthermore, if $M = N$ then we can have a well-defined ring structure; multiplication is just composition. Indeed, $Hom_R(M, M)$ is a ring with identity -- and indeed it has a special name.

Definition: The ring $Hom_R(M, M)$ is called the endomorphism ring of M and is denoted $End(M)$ or $End_R(M)$.

Proposition

> Let R be a ring and let M, N be R-modules with N a submodule of M. Then M/N (an abelian quotient group) can be made into a module over R by defining:

$$r(x+N) = rx + N$$

And we have a natural projection map $\pi : M \to M/N$ with kernel N.

Finally, we define the sum of two modules:

$$A + B = \{a + b \ : \ a \in A, b \in B\}$$

So that we can once more define the isomorphism theorems.

Theorem (Isomorphism Theorems)

- Let M, N be R-modules and let $\varphi : M \to N$ be a module homomorphism. Then $M/(ker\varphi) \cong \varphi(M)$.
- Let A, B be submodules of R-module M. Then we have: $(A+B)/B \cong A/(A\cap B)$.
- Let M be an R-module and let A, B be submodules of M with $A \subset B$. Then $(M/A)/(B/A) \cong M/B$.
- Let N be a submodule of the R-module M. Then there is a bijection between submodules of M containing N and submodules of M/N given by $A \mapsto A/N$.