# Introduction to Rings and Modules

*Lecture 12, Monday June 5 2023*
*Ari Feiglin*

**Definition 12.0.1:**

Let $R$ be a ring, a **left $R$-module** is an abelian group $(M, +)$ equipped with scalar multiplication

$$\cdot\colon R \times M \longrightarrow M$$

such that the following hold

(1) $(r+s)m = rm + sm$ for every $r, s \in R$ and $m \in M$.

(2) $r(m+n) = rm + rn$ for $r \in R$ and $m, n \in M$.

(3) $s(rm) = (sr)m$ for $r, s \in R$ and $m \in M$.

(4) $1_R m = m$ for $m \in M$.

A **right $R$-module** is an abelian group $(M, +)$ equipped with a right multiplication function $M \times R \to M$ which satisfies the above properties, where the multiplication's order is swapped.

Note that if $R$ is commutative then if $M$ is a left module, we can induce on $M$ a right module structure by defining

$$m \cdot r = r \cdot m$$

This satisfies the first and second properties trivially, and

$$(mr)s = s(rm) = (sr)m = m(sr) = m(rs)$$

where the final equality is due to $R$ being commutative. Thus if $R$ is commutative, we can think of left and right modules being equivalent and just saying $R$-modules.

**Note:**

If $R$ is a field, a left $R$-module is a vector space above $R$. Thus vector spaces are modules (the reverse is not true).

**Example 12.0.2:**

If $R$ is a ring, let $M = \{0_M\}$ be the trivial group. We define $r \cdot 0_M = 0_M$, and this defines a eft $R$-module, the so-called **trivial $R$-module**.

**Proposition 12.0.3:**

$0_R \cdot m = 0_M$ and $r \cdot 0_M = 0_M$.

**Proof:**

Note that $0_R \cdot m = (0_R + 0_R)m = 0_R \cdot m + 0_R \cdot m$, since $M$ is a group we can subtract $0_R \cdot m$ from both sides and get $0_R \cdot m = 0_M$ as required. And $r \cdot 0_M = r \cdot (0_M + 0_M) = r \cdot 0_M + r \cdot 0_M$ and subtracting $r \cdot 0_M$ we get $r \cdot 0_M = 0_R$. ■

**Proposition 12.0.4:**

$(-1_R)m = -m$

**Proof:**

Notice that $(-1_R)m + m = (-1_R + 1_R)m$ by distributivity, which equals $0_R m = 0_M$ so $(-1_R)m = -m$ as required. ■

**Example 12.0.5:**

(1) If $R$ is a ring, we define the module $M = (R, +)$ with multiplication $r \cdot m = rm \in R$. Thus $R$ is an $R$-module above itself.

(2) If $S$ is a ring and $M$ a module over $S$, and $f\colon R \longrightarrow S$ a ring homomorphism. We can induce on $R$-module structure on $M$ by

$$r \cdot m = f(r)m$$

This satisfies the axioms since

$$(r_1 + r_2)m = f(r_1 + r_2)m = (f(r_1) + f(r_2))m = f(r_1)m + f(r_2)m = r_1 m + r_2 m$$

the second axiom:

$$r(m + n) = f(r)(m + n) = f(r)m + f(r)n = rm + rn$$

the third axiom:

$$(r_1 r_2)m = f(r_1 r_2)m = (f(r_1)f(r_2))m = f(r_1)(f(r_2)m) = f(r_1)(r_2 m) = r_1(r_2 m)$$

the fourth axiom:

$$1_R m = f(1_R)m = 1_S m = m$$

(3) Let $L$ be a left module over $S$ and $R = M_n(S)$, the ring of matrices of size $n \times n$ over $S$. Let $M = L^n$, which is a left $R$-module defined by $[s\ell]_i = \sum_{k=1}^n s_{ik}\ell_k$, where $s \in R$, $\ell \in M$ (meaning $s_{ik} \in S$ and $\ell_k \in L$, so this multiplication is well-defined).

**Definition 12.0.6:**

If $R$ is a ring and $M$ a $R$-module, then $\varnothing \neq N \subseteq M$ is a **submodule** of $M$ if $N$ is closed under addition, and scalar multiplication by $R$. Meaning that if $n_1, n_2 \in N$ then $n_1 + n_2 \in N$ and if $r \in R$ and $n \in N$ then $rn \in N$.

Notice then that if $N$ is a submodule of $M$, then $N$ is a subgroup of $M$. This is since $0_M = 0_R \cdot n$ for $n \in N$ so $0_M \in N$. And if $n \in N$ then $-n = (-1_R)n \in N$, so $N$ is closed under inverses.

**Proposition 12.0.7:**

The submodules of a ring $R$, when viewed as a module over itself, are exactly its left ideals.

**Proof:**

If $I \subseteq R$ is a left-ideal of $R$ then it is by definition closed under addition and left multiplication by $R$, so it is a submodule. And if $N \subseteq R$ then it is by definition closed under addition and left scalar multiplication, so is by definition a left ideal of $R$. ■

**Proposition 12.0.8:**

Let $M$ be an $R$-module, and $m_1, \ldots, m_n \in M$. Then the smallest submodule containing these elements is

$$N = \{r_1 m_1 + \cdots + r_n m_n \mid r_i \in R\}$$

**Proof:**

This set is a submodule since if $r_1m_1 + \cdots + r_nm_n, s_1m_1 + \cdots + s_nm_n \in N$ then

$$r_1m_1 + \cdots + r_nm_n + s_1m_1 + \cdots + s_nm_n = (r_1 + s_1)m_1 + \cdots + (r_ns_n)m_n \in N$$

so $N$ is closed under addition, and if $r \in R$ then

$$r(r_1m_1 + \cdots + r_nm_n) = (rr_1)m_1 + \cdots + (rr_n)m_n \in N$$

so $N$ is also closed under left scalar multiplication, meaning $N$ is a submodule.
If $N'$ is another submodule containing $m_1, \dots, m_n$ then for any $r_1, \dots, r_n \in R$, it must contain $r_im_i$ for every $i$ since it is closed under scalar multiplication, and since it is also closed under addition it must contain $r_1m_1 + \cdots + r_nm_n$, meaning $N \subseteq N'$. ■

**Definition 12.0.9:**

If $M$ is an $R$-module, and $m_1, \dots, m_n \in M$ we define the **submodule generated by $m_1, \dots, m_n$** to be

$$\langle m_1, \dots, m_n \rangle = \{r_1m_1 + \cdots + r_nm_n \mid r_i \in R\}$$

the smallest submodule containing $m_1, \dots, m_n$.
And in general if $\mathscr{S} \subseteq M$, we define the **submodule generated by $\mathscr{S}$** to be

$$\langle \mathscr{S} \rangle = \{r_1s_1 + \cdots + r_ks_k \mid k \in \mathbb{N}, r_i \in R, s_i \in \mathscr{S}\}$$

This is the smallest submodule containing $\mathscr{S}$.

**Definition 12.0.10:**

Let $R$ be an integral domain and $M$ an $R$-module. We define its **torsion submodule** by

$$\mathrm{Tor}(M) = \{m \in M \mid \exists 0_R \neq r \in R \colon rm = 0_M\}$$

This is indeed a submodule, since if $m_1, m_2 \in \mathrm{Tor}(M)$ then there exists $r_1$ and $r_2$ such that $r_1m_1 = r_2m_2 = 0_M$. Since $R$ is an integral domain, $r_1r_2 \neq 0_R$ and

$$(r_1r_2)(m_1 + m_2) = r_1r_2m_1 + r_1r_2m_2 = r_2(r_1m_1) + r_1(r_2m_2) = 0_M$$

so $m_1 + m_2 \in \mathrm{Tor}(M)$, and if $m \in \mathrm{Tor}(M)$ where $rm = 0_M$, and $s \in R$ then

$$r(sm) = s(rm) = 0_M$$

so $sm \in \mathrm{Tor}(M)$ as well.

**Definition 12.0.11:**

Let $M$ be an $R$-module. $B \subseteq M$ is called a **basis** of $M$ if every element of $M$ can be written as a unique linear combination of elements in $B$. Meaning that for every $0_M \neq m \in M$, there exist distinct $b_i \in B$ and $r_i \in R$ such that

$$m = r_1b_1 + \cdots + r_nb_n$$

and if

$$m = r'_1b'_1 + \cdots + r'_mb'_m$$

then $n = m$ and there exists a permutation $\sigma \in S_n$ such that $b_{\sigma(i)} = b'_i$ and $r_{\sigma(i)} = r'_i$.
If $M$ has a basis, it is called **free**.

From linear algebra, we know that

**Theorem 12.0.12:**

Let $R$ be a field, then every $R$-module is free.

**Example 12.0.13:**

If $M$ is an abelian group, there is a unique way to define $M$ as a $\mathbb{Z}$-module. This is because for $n \geq 0$

$$n \cdot m = (1 + \cdots + 1)m = m + \cdots + m$$

and

$$(-n) \cdot m = (-m) + \cdots + (-m)$$

This does in fact define a $\mathbb{Z}$-module. Thus abelian groups and $\mathbb{Z}$-modules are equivalent.

**Example 12.0.14:**

Let $M = {}^{\mathbb{Z}}\!/_{6\mathbb{Z}}$, this is a $\mathbb{Z}$-module. Now suppose $B \subseteq M$ is a basis, then let $m \in M$ so

$$m = r_1 b_1 + \cdots + r_n b_n$$

but we know $(r+6)b = rb + 6b$ and $6b = 0$ so $(r+6)b = rb$ and so

$$m = (r_1 + 6)b_1 + \cdots + r_n b_n$$

is another linear combination equal to $m$, so these are not unique and therefore $B$ is not a basis.
So $M$ is not free. This is true in general for $M = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. And in even more generality, this works for finite (non-trivial) abelian groups $M$, since $|M| \cdot m = 0_M$.