Summary of results:
Modules Over Commutative Rings

Alan Haynes, haynes@math.uh.edu
Last update: February 1, 2022

In all of what follows R will denote a commutative ring with identity 1. An ***R*-module** is an Abelian group $(M, +)$ together with a binary operation $\cdot : R \times M \to R$ called **scalar multiplication** (which we will simply write as $r \cdot x = rx$) satisfying the following properties, for all $r, s \in R$ and $x, y \in M$:

(i) $(rs)x = r(sx)$,

(ii) $1x = x$,

(iii) $(r + s)x = rx + sx$, and

(iv) $r(x + y) = rx + ry$.

You should notice that the requirements on M, together with properties (i)-(iv), are exactly the same in form as the requirements for being a vector space, the only difference being that R is not required to be a field. The trade-off for relaxing this requirement on R is that some of the important properties which are true for vector spaces are no longer true, in general, for R-modules. In particular, not every R-module has an R-linearly independent generating set (i.e. a basis; definitions will be given below). Therefore, although the basic algebraic structure in this setting is similar to that encountered in a first course on linear algebra, some care must be exercised in proceeding.

To familiarize ourselves with the definition, here a list of some commonly occurring examples of modules:

(1) As already mentioned, any vector space is a module over its field of scalars.

(2) If $n \in \mathbb{N}$ then the direct product of *additive groups* $R^n = R \times \cdots \times R$ (n-times) can be thought of as an R-module in a natural way, with scalar multiplication defined componentwise. The module R^n is called the **free module of rank *n* over *R*** (more justification for this terminology will be given below).

(3) Any Abelian group $(G, +)$ can be thought of as a $\mathbb{Z}$-module in a natural way, with scalar multiplication defined by $nx =$

$x + \cdots + x$ (n-times), for all $n \in \mathbb{N}$ and $x \in G$, and extended in the obvious way to all of $\mathbb{Z} \times G$.

(4) If $S \subseteq R$ is a commutative ring with identity then $(R, +)$ can be thought of in a natural way as an S-module.

(5) Generalizing the previous example, if M is an R-module and $S \subseteq R$ is a subring of R (with identity) then M can also be thought of in a natural way as an S-module.

(6) If M is an additive subgroup of R then M will be an R-module (with scalar multiplication corresponding to multiplication in R) if and only if for every $r \in R$ and $x \in M$, we have $rx \in M$. Equivalently, M will be an R-module if and only if it is an ideal of R.

(7) If I is an ideal of R then the additive group R/I is an R-module, with scalar multiplication defined by

$$r(x + I) = rx + I.$$

The fact that I is an ideal guarantees that this operation is well defined, i.e. that it does not depend on the choice of representative for the coset $x + I$.

(8) Suppose that M is an R-module and that I is an ideal of R. If $ax = 0$ for all $a \in I$ and $x \in M$ then M can also be thought of as an (R/I)-module, with scalar multiplication defined by

$$(r + I)x = rx.$$

Note that if $r + I = s + I$ in R/I then $rx - sx = (r - s)x = 0$, so $rx = sx$ in M. This shows that scalar multiplication in this example is well defined.

(9) Following from the previous example, let $(G, +)$ be a finite Abelian group with exponent $n \in \mathbb{N}$ (recall that the exponent of a finite group is the least common multiple of the orders of all of its elements). We know from example (3) that G is a $\mathbb{Z}$-module. For every $x \in G$ and for every element r in the ideal $n\mathbb{Z} \subseteq \mathbb{Z}$ we have that $rx = 0$. Therefore, as described in the previous example, G can be thought of in a natural way as a $(\mathbb{Z}/n\mathbb{Z})$-module.

Given an R-module M, a subset $\mathcal{A} \subseteq M$ is called a **generating set** for M over R if, for every $x \in M$, there exists an $n \in \mathbb{N}$, $r_1, \ldots, r_n \in R$, and $x_1, \dots, x_n \in \mathcal{A}$ with

$$x = r_1x_1 + \cdots + r_nx_n.$$

If M can be generated by a finite set $\mathcal{A}$ then we say that M is a **finitely generated** R-module.

We say that a set $\mathcal{A} \subseteq M$ is ***R*-linearly independent** if whenever

$$r_1x_1 + \cdots + r_nx_n = 0,$$

for some $n \in \mathbb{N},\ r_1, \dots, r_n \in R$, and for distinct elements $x_1, \dots, x_n \in \mathcal{A}$, it must be the case that $r_1 = \cdots = r_n = 0$. Otherwise we say that $\mathcal{A}$ is ***R*-linearly dependent**. A module M is called **torsion free** if whenever $rx = 0$, for some $r \in R$ and $x \in M$, it must be the case that $r = 0$ or $x = 0$.

If M contains an R-linearly independent, generating set $\mathcal{A}$, then M is called a **free module**, and $\mathcal{A}$ is called an ***R*-basis** (or simply a **basis**, if there is no ambiguity) for M. Not every module is a free module. In order to better appreciate this fact, consider the following examples.

(9) Suppose that R is an integral domain and that M is an R-module which is not torsion free (e.g. a finite Abelian group G viewed as a $\mathbb{Z}$-module). Then there exist nonzero elements $r \in R$ and $x \in M$ with $rx = 0$. If $\mathcal{A} \subseteq M$ is any generating set for M then there exist $n \in \mathbb{N},\ r_1, \dots, r_n \in R$, and $x_1, \dots, x_n \in M$ with

$$x = r_1x_1 + \cdots + r_nx_n.$$

We can assume without loss of generality that none of the r_i's are 0, and also (by grouping together like terms if necessary) that the x_i's are distinct. Multiplying both sides of this equation by r gives

$$0 = rx = (rr_1)x_1 + \cdots + (rr_n)x_n.$$

Since R is an integral domain, none of the coefficients rr_i on the right hand side are 0. Therefore the set $\mathcal{A}$ is R-linearly dependent. This shows that there are no linearly independent generating sets for M, so M is not a free module.

(10) If we drop the assumption that R is an integral domain in the previous example, then we cannot reach the same conclusion. To see this, take $R = \mathbb{Z}/6\mathbb{Z}$ and let M be the additive group of R, viewed as an R-module (as in example (4) above). Then

M is not torsion free, because $rx = 0$ with $r = 2$ and $x = 3$. However, the set $\{1\}$ is a basis for M, so M is a free module.

(11) As another example of a module which is not free, let $M = (\mathbb{Q}, +)$ and let $R = \mathbb{Z}$. Integer multiplies of a rational number cannot increase the denominator, therefore any generating set for $\mathbb{Q}$ must contain more than one element. However, if $x_1 = p_1/q_1$ and $x_2 = p_2/q_2$ are distinct, non-zero elements of $\mathbb{Q}$ then

$$q_1 p_2 x_1 + (-q_2 p_1) x_2 = 0,$$

and $q_1 p_2$ and $-q_2 p_1$ are non-zero integers. Therefore any generating set for $\mathbb{Q}$ over $\mathbb{Z}$ is linearly dependent, and $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

(12) In the previous example, if we had considered $\mathbb{Q}$ as a $\mathbb{Q}$-module then of course it would have been a free module, since $\{1\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}$. More generally, since a module over a field is a vector space, and since any vector space has a basis, any module over a field is a free module.

If an R-module M is a free module then any basis for M over R will have the same cardinality (for completeness we point out that this is not true in general for modules over non-commutative rings, which we have not defined). The cardinality of any basis for a free module M over R is called the **rank** of M over R. If M is a free R-module of rank $n \in \mathbb{N}$ then, by choosing a basis, we may identify M (isomorphically) with R^n. This justifies calling R^n *the* free module of rank n over R.

In the special case when R is a PID, we have several important structure results. The first result is a generalization of the non-torsion part of the conclusion of the Fundamental Theorem for Finitely Generated Abelian Groups.

Theorem 1. *Suppose that R is a PID and that M is an R-module which is finitely generated and torsion free, and which can be generated by n elements and no fewer. Then*

(i) M is a free module of rank n over R, and

(ii) any generating set consisting of n elements forms an R-basis for M.

The second structural result is an example of what is sometimes referred to as a 'stacked basis theorem.'

Theorem 2. *Suppose that R is a PID, that N is a free R-module of rank $n \in \mathbb{N}$, and that $M \subseteq N$ is a sub-module of N. Then*

(i) M is a free module of rank $m \leq n$, and

(ii) There is a basis $y_1, \ldots, y_n$ for N and non-zero elements $r_1, \ldots, r_n \in R$ satisfying $r_i | r_{i+1}$ for each $1 \leq i < n$, and for which $r_1 y_1, \ldots, r_m y_m$ is a basis for M.

This theorem is extremely useful in many problems, for example when working with sub-lattices of finitely generated lattices in locally compact Abelian groups, a situation which occurs often in both number theory and dynamical systems.