# Modules

As usual we will assume that all rings have an identity element, denoted $1$.

**Definition 1.** Let $R$ be an associative ring (with identity). Let $M$ be an additively written abelian group with identity element $0$.

We call $M$ a left $R$-*module*, if there is a binary operation

$$\begin{array}{rcl} \cdot : \ R \times M & \longrightarrow & M \\ (r, m) & \mapsto & r \cdot m \end{array}$$

for all $m \in M$ and for all $r \in R$ such that the following hold:

1. $1 \cdot m = m$
2. $(rs) \cdot m = r \cdot (s \cdot m)$
3. $r \cdot (m + n) = r \cdot m + r \cdot n$
4. $(r + s) \cdot m = r \cdot m + s \cdot m$

for all $m, n \in M$ and all $r, s \in R$.

One normally abbreviates $r \cdot m$ simply as $rm$.

One can define a right $R$-module in a similar manner by writing the element from the ring on the right. The concepts of left and right are different for non-commutative rings since the second condition depends on the order of the multiplication in $R$.

**Example 2.** There are a number of examples analogous to those in the case of fields.

1. $R^n$ for $n > 0$ an integer. The left $R$-module structure is given coordinate-wise:
   a. $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$, for $a_i \in R$, $b_i \in R$.
   b. $c(a_1, \ldots, a_n) = (ca_1, \ldots, ca_n)$ for $c \in R$. $a_i \in R$.
2. $R^{m \times n}$ for $m, n > 0$ integers. The left $R$-module structure is defined coordinate-wise as it was for fields.
3. Let $S$ be a non-empty set and $R^S$ the set of all functions from $S$ to $R$. Addition and scalar multiplication for $R^S$ is given as in calculus by computing pointwise:
   a. $(f + g)(s) = f(s) + g(s)$ for $f, g \in R^S$, $s \in S$.
   b. $(af)(s) = af(s)$ for $f \in R^S$, $s \in S$, $a \in R$.

   In addition, one can define multiplication of two such functions by

c. $(f \cdot g)(s) = f(s) \cdot g(s)$ for $f, g \in R^S$, $s \in S$.

One can also consider $R^{(S)}$ the subset consisting of those functions with finite support. Note that multiplication gives a ring structure on $R^S$ in all cases, but if $S$ is infinite, $R^{(S)}$ is not a ring since it does not contain an identity element (the function that is 1 everywhere has support equal to $S$). However, both of these, $R^S$ and $R^{(S)}$, are $R$-modules.

4. Let $S$ be a non-empty set and let $M$ be a left-$R$-module over the ring $R$. We denote by $M^S$ the set of all functions from $S$ to $M$. Addition and scalar multiplication for $M^S$ is given as in the preceding example:

   a. $(f+g)(s) = f(s) + g(s)$ for $f, g \in m^S$, $s \in S$.
   b. $(af)(s) = af(s)$ for $f \in M^S$, $s \in S$, $a \in R$.

   As we did for vector spaces one can also define $M^{(S)}$ to be the submodule of $M^S$ consisting of those functions with finite support (i.e., non-zero at only a finite number of elements of $S$).

5. $R[x]$ the set of all polynomials with coefficients in $R$, treated formally. Addition and scalar multiplication are given by the usual formulas:

   a. $\sum_{i=0}^{i=n} a_i x^i + \sum_{i=0}^{i=n} b_i x^i = \sum_{i=0}^{i=n} (a_i + b_i) x^i$ for $a_i \in R$, $b_i \in R$.
   b. $c \sum_{i=0}^{i=n} a_i x^i = \sum_{i=0}^{i=n} c a_i x^i$

   Again, the same cautions apply here as in the case of a field – these are formal polynomials, not functions.

   In addition, one can define multiplication in the usual way and obtain a ring:

   c. $(\sum_{i=0}^{i=n} a_i x^i) \cdot (\sum_{i=0}^{i=m} b_i x^i) = \sum_{i=0}^{i=n+m} c_i x^i$
   where $c_i \in R$ are given by $c_i = \sum a_k b_l$ where the sum is taken over all $k, l$ such that $i = k + l$ (that is, the terms which have the same $x^i$ are added together).

6. $R[[x]]$ the set of all formal power series with coefficients in $R$. Addition and scalar multiplication are given by the usual formulas:

   a. $\sum_{i=0}^{i=\infty} a_i x^i + \sum_{i=0}^{i=\infty} b_i x^i = \sum_{i=0}^{i=\infty} (a_i + b_i) x^i$ for $a_i \in R$, $b_i \in R$.
   b. $c \sum_{i=0}^{i=\infty} a_i x^i = \sum_{i=0}^{i=\infty} c a_i x^i$

   As in the previous example, "formal" means that two power series in $R[[x]]$ are equal if an only if all of their corresponding coefficients are equal. Another way to think of this is that there is a one-to-one correspondence between $R[[x]]$ and $R^{\mathbb{N}_0}$ for $\mathbb{N}_0$ the set of non-negative integers. This correspondence does not preserve the multiplication defined below.

   $R[x]$ is the subring of $R[[x]]$ consisting of those power series whose coefficients $a_i$ are all 0 for sufficiently large $i$.

   In addition, one can define multiplication in the usual way to give a ring structure:

c. $(\sum_{i=0}^{i=\infty} a_i x^i) \cdot (\sum_{i=0}^{i=\infty} b_i x^i) = \sum_{i=0}^{i=\infty} c_i x^i$
where $c_i \in R$ are given by $c_i = \sum a_k b_l$ where the sum is taken over all $k, l$ such that $i = k + l$ just as for polynomials. The term $c_i$ is given by a finite sum (with $i + 1$ terms) since $k, l \geq 0$.

It should again be noted that this is NOT the same multiplication (not the same ring) as example 3.

7. Let $R \subseteq S$ be rings with $R$ a subring of $S$: that is, the addition and multiplication of elements in $R$ is the same as that when they are considered elements of $S$. Further the identity element of $R$ is equal to the identity element of $S$. It is easy to check that $S$ is a left- and right- $R$-module over $R$ since the required axioms are just a subset of the statements that are valid for the ring $S$. We thus obtain many examples this way as we did in the case of fields. Further, if $M$ is an $S$-module, then $M$ is also an $R$-module using the same multiplication, as can easily be checked.

8. The previous example can be generalized: If $h : R \longrightarrow S$ is a ring homomorphism, and $M$ is any $S$-module, then $M$ becomes a left $R$-module via

$$r \cdot m = h(r)m \ .$$

The easy verification is left to the reader.

9. Just as in the case of fields and vector spaces we can form collections of functions to construct modules and rings.

a. Let $M$ and $N$ be $R$-modules for $R$ a commutative ring. We write $\mathrm{Hom}_R(M, N)$ to denote the set of all $R$-module homomorpshisms $f : M \longrightarrow N$. Just as in the case of vector spaces we add such functions by adding their values and multiply by a scalar (i.e., an element of $R$) by multiplying the value of the function by the scalar. This makes $\mathrm{Hom}_R(M, N)$ into an $R$-module.

b. Let $M$ be a module over the commutative ring $R$. Then $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ is a not only a module but also a ring where composition plays the role of multiplication, just as in the case of vector spaces over a field.

**Remark 3.** In the preceding examples 2 (when $m = n$), 3, 5, 6 and 9b there is also a multiplication defined. For $R$ commutative, in each case we obtain what is called an $R$-algebra. That is, a set $A$ which is a module over $R$, is a ring, and for which the scalar multiplication and multiplication are compatible, that is, satisfy:

d. $c(fg) = (cf)g = f(cg)$ for all $c \in R$ and $f, g \in A$.

In all examples except for matrices (with $n > 1$), these are commutative $R$-algebras, that is, the multiplication in the ring is commutative. If elements of $R$ commute with all elements of $S$ then Example 7 will be an $R$-algebra as well. By using an $R$-algebra $A$ (instead of $M$) in 4 one could also define a multiplication as in 4, which would yield another example of an $R$-algebra: $A^S$. See the chapter on "Some Useful Definitions".

**Remark 4.** For the ring $\mathbb{Z}$ modules are easy to understand: $\mathbb{Z}$-modules and abelian groups are exactly the same thing. For any $\mathbb{Z}$-module must be an abelian group $A$ and every element in $\mathbb{Z}$ is the sum (or negative) of a sum of copies of $1$. Hence the fact that for a module $1 \cdot a = a$ holds for all elements together with the other properties of scalar multiplication uniquely determines the scalar multiplication in terms of the addition in $A$:

$$k \cdot a = \begin{cases} a + \cdots + a \ \ (k \text{ times}) & \text{if } k > 0 \\ 0 & \text{if } k = 0 \\ -(a + \cdots + a) \ \ (|k| \text{ times}) & \text{if } k < 0 \end{cases}$$

It is easy to check now (induction broken down by the cases of the definition) that defining scalar multiplication by this formula makes the abelian group $A$ into a $\mathbb{Z}$-module.

For example, if $n > 1$ is an integer, then $\mathbb{Z}_n$, the integers modulo $n$ is an abelian group under addition and is thus a $\mathbb{Z}$-module. Note that in essence we've already used this idea when we discussed the characteristic of a ring or field.

One can also consider $\mathbb{Z}_n \times \mathbb{Z}_m$ as a module over $\mathbb{Z}$ in a similar way – addition is defined coordinate-wise, and scalar multiplication is given by $k(x, y) = (kx, ky)$.

See Exercise 1 for a generalization of this idea to describe modules over the ring $\mathbb{Z}_n$ and Exercise 2 to extend the idea to modules over quotient rings (see below).

**Example 5.** Let $R$ be a ring and let $n, m > 0$ be integers. Then using the usual definition of addition and multiplication for matrices makes $\mathcal{R} = R^{n \times n}$ into a ring. If we let $\mathcal{M} = R^{n \times m}$, then $\mathcal{M}$ is an abelian group using the usual definition of addition and is a (left) $R$-module by using scalar multiplication by elements of $R$ on the left. For $A \in \mathcal{R}$ and $M \in \mathcal{M}$ the usual properties of matrix multiplication show that $\mathcal{M}$ is an $\mathcal{R}$-module if we define $A \cdot M$ to be matrix multiplication:

(1) $I \cdot M = M$, for the identity matrix $I \in \mathcal{R}$, $M \in \mathcal{M}$,

(2) $A \cdot (B \cdot M) = (A \cdot B) \cdot M$, for all $A, B \in \mathcal{R}$, $M \in \mathcal{M}$

(3) $A \cdot (M_1 + M_2) = A \cdot M_1 + A \cdot M_2$, for all $A \in \mathcal{R}$, $M_i \in \mathcal{M}$,

(4) $(A_1 + A_2) \cdot M = A_1 \cdot M + A_2 \cdot M$, for all $A_i \in \mathcal{R}$, $M \in \mathcal{M}$.

**Example 6** (Main Example: "$T$-Modules"). .

A. **Linear Transformation Version**

Let $F$ be a field and $V$ a finite dimensional vector space of dimension $n$ over $F$. Let $T \in \operatorname{End}_F(V) = \operatorname{Hom}_F(V, V)$ be a fixed linear transformation (operator). We use $T$ to make $V$ a module over the ring $F[x]$ via

$$f \cdot v = f(T)(v)$$

for $f \in F[x]$ and $v \in V$. Here the linear transformation $f(T) \in \mathrm{End}_F(V)$ is given by evaluation (discussed earlier). Explicitly, if $f = a_0 + a_1x + \cdots + a_nx^n$, then $f(T) = a_0I + a_1T + \cdots + a_nT^n$.

It is easy to check that this makes $V$ into an $F[x]$-module. For example, if $f = 1$, then $f(T) = I$ is the identity and hence $1 \cdot v = f(T)(v) = I(v) = v$. Complete the verification (Exercise 6).

B. **Matrix Version**
If one picks a basis for $V$ in the preceding, then one obtains a version in terms of matrices. We're given a fixed matrix $A \in F^{n\times n}$ and the module is the vector space of columns $F^{n\times 1}$. For $f \in F[x]$ scalar multiplication is given by ordinary matrix multiplication

$$f \cdot C = f(A) \cdot C \ .$$

We will study a fixed linear transformation (or matrix) by combining what we know already about linear transformations with some new ideas on the structure of $R$-modules in case $R$ is a PID. In order to do the latter, we need to understand a bit more about modules. Fortunately, parts of this are relatively easy to do after we generalize to modules things we're already done for vector spaces. This part we will outline here. The final structure theorem for modules over a PID will be carried out in the next chapter using the ideas developed below.

**Remark 7.** Part A above could also be studied when $V$ has infinite dimension. In this case it would not necessarily be true that the module is finitely generated over $F[x]$ and the structure theorem we prove in the next chapter would not apply. In addition the resulting module structure on $V$ would also not necessarily be torsion as in the case where $V$ has finite dimension. That is, in the general case essentially everything which made the finite dimensional case work out nicely will not always hold.

## Quotient Modules

Let $M$ be an $R$-module. A subset $N$ of $M$ is called a *submodule* if it is an $R$-module with respect to the operations of addition and scalar multiplication it inherits from $M$. As we observed for the analogous situation in vector spaces, we have the following lemma:

**Lemma 8.** *A subset $N$ of the $R$-module $M$ is a submodule if and only if $N$ satisfies*

*a. $N$ is non-empty,*

*b. if $n, n' \in N$, then $n + n' \in N$,*

*c. if $n \in N$ and $r \in R$, then $rn \in N$.*

Exactly as in the case of vector spaces we can define quotient modules, $M/N$, which will have similar properties. For $m \in M$ define the *coset* $m+N = \{\, m + n \mid n \in N \,\}$.

Any two such cosets are either equal or disjoint and consequenctly $M$ is the disjoint union of the cosets of $N$ in $M$. Next define the *quotient module*

$$M/N = \{\, m + N \mid m \in M \,\}$$

as the set of all cosets of $N$. Define addition and scalar multiplication by

$$(m+N) + (m'+N) \;=\; (m+m') + N$$

for $m, m' \in M$ and

$$r(m+N) \;=\; (rm) + N$$

for $m \in M$ and $r \in R$.

It is now easy to check that $M/N$ is an $R$-module – the proof is essentially the same as that for vector spaces: just replace the word "field" by "ring" and "vector space" by "$R$-module".

Let $M$ and $M'$ be $R$-modules. An *$R$-module homomorphism* is a function $f : M \longrightarrow M'$ satisfying

$$f(x+y) \;=\; f(x) + f(y)$$

for all $x, y \in M$ and

$$f(rx) \;=\; rf(x)$$

for all $r \in R$ and all $x \in M$. A one-to-one, onto $R$-homomorphism is called an *isomorphism* of $R$-modules. The *image* of $f$ is

$$\operatorname{im} f = \{\, f(x) \mid x \in M \,\} \subseteq M'$$

and the *kernel* of $f$ is the set

$$\ker f = \{\, x \in M \mid f(x) = 0 \,\} \subseteq M \;.$$

Both are easily seen to be submodules.

There is a surjective $R$-module homomorphism

$$p :\; M \longrightarrow M/N$$

given by $f(m) = m + N$ with $\ker p = N$.

There is a Universal Mapping Property for quotient modules just as there is for quotient vector spaces – both the statement and proof can be given by the just stated principle (see Exercise 7).

Just as in the case of vector spaces one has the First Isomorphism Theorem:

**Theorem 9.** *If $f :\; M \longrightarrow M'$ is an $R$-module homomorphism, then $M/\ker f \approx \operatorname{im} f$ as $R$-modules.*

The proof follows as earlier (see Exercise 8).

An $R$-module $M$ is called *cyclic* if it contains an element $m_1$ that generates it, that is, $Rm_1 = M$ where $Rm_1 = \{ rm_1 \mid r \in R \}$ is the set of $R$-linear combinations of the one element set $\{ m_1 \}$.

**Lemma 10.** *If $M$ is a cyclic $R$-module, then there exists an $R$-submodule $I$ of $R$ (that is, $I$ is a left ideal of $R$) such that $M \approx R/I$.*

*Proof.* Consider the function $f : R \longrightarrow M$ given by $f(r) = rm_1$. It is an $R$-module homomorphism as is easily checked. Thus for $M$ cyclic generated by $m_1$, $f$ is onto. Then $I = \ker f \subseteq R$ is an $R$-submodule of $R$ (i.e., an abelian group under addition which satisfies $ri \in I$ for all $r \in R$ and $i \in I$ – that is, the definition of left ideal). By the First Isomorphism Theorem, $M \approx R/\ker f$ as $R$-modules. □

Hence for a PID $R$ every cylic module looks like $R$ or $R/(a)$ for some non-zero $a \in R$. In particular, for $\mathbb{Z}$ all cyclic modules look like $\mathbb{Z}$ or $\mathbb{Z}_n$ for some positive integer $n$. For $F[x]$, cyclic modules look like $F[x]$ or $F[x]/(f)$ for some monic polynomial $f$.

Cylic modules are special cases of what are called finitely generated $R$-modules: A module $M$ is *finitely generated* if there exists a finite subset $\{ m_1, \ldots, m_k \} \subseteq M$ such that $M = \{ r_1 m_1 + \cdots + r_k m_k \mid r_i \in R \}$. $M$ is said to be *generated* by the set $\{ m_1, \ldots, m_k \}$. In the next chapter we show that in case $R$ is a PID every finitely generated module is a direct sum of cyclic modules.

## Quotient Rings

Let $R$ be a ring and let $I$ be a two-sided ideal of $R$, that is, a subset of $R$ which is an abelian group under addition and which satisfies $ir, ri \in I$ for all $i \in I$ and all $r \in R$. Note that $R$ is a (left) $R$-module if scalar multiplication is defined by multiplication on the left; similarly one can make $R$ a right $R$-module by multiplying on the right. Saying that $I$ is a two-sided ideal of $R$ is thus the same thing as saying that it is both a left and right $R$-submodule. If $R$ were a commutative ring, we would not need to distinguish between left and right so that ideals are easier to describe.

For $r \in R$ we define the *coset*

$$r + I = \{ r + i \mid i \in I \}$$

just as we would in the case of modules (or vector spaces). $R$ is the disjoint union of these cosets and we define the *quotient ring* as the set

$$R/I = \{ r + I \mid r \in R \}$$

with addition defined as we did for modules

$$(r + I) + (r' + I) \quad = \quad (r + r') + I$$

for $r, r' \in R$. Define multiplication by

$$(r+I)(r'+I) \;=\; rr'+I$$

for $r, r' \in R$. It is now stright-forward to check that $R/I$ becomes a ring under this definition (compare with the earlier exercises giving special cases for $\mathbb{Z}_n = \mathbb{Z}/(n)$ and $F[x]/(f)$ in the chapter on "Equivalence Relations").

If $R$ and $R'$ are rings, a function $f:\ R \longrightarrow R'$ is called a *ring homomorphism* if it satisfies

$$f(x+y) \;=\; f(x)+f(y)$$

for all $x, y \in R$,

$$f(xy) \;=\; f(x)f(y)$$

for all $x, y \in R$ and

$$f(1) \;=\; 1\,.$$

A one-to-one, onto ring homomorphism is called a *ring isomorphism.*

The *image* of $f$ is

$$\operatorname{im} f = \{\, f(x) \mid x \in R \,\} \subseteq R'$$

and the *kernel* of $f$ is the set

$$\ker f = \{\, x \in R \mid f(x) = 0 \,\} \subseteq R\,.$$

It is easy to check that $\ker f$ is a two-sided ideal of $R$ and that $\operatorname{im} f$ is a subring of $R'$.

There is a surjective ring homomorphism

$$p:\ R \longrightarrow R/I$$

given by $p(x) = x + I$ with $\ker p = I$.

**Remark 11.** Requiring that rings contain $1$ means that they have lots of useful properties that one expects. In some instances however this leads to additional complications that one should keep in mind.

First of all, ring homomorphisms must take $1$ to $1$.

In many cases, but not always, one is only interested in rings that are non-trivial, that is $1 \neq 0$ (note that if $1 = 0$, then $R = \{0\}$). Thus it would be necessary to require that $I \neq R$ in order that $R/I$ not be the trivial ring.

A *subring* $S$ of a ring $R$ is defined to be a subset of $R$ which is not only a ring under the addition and multiplication it inherits from $R$, but it must also contain the SAME identity element as $R$. This is not too surprising as one natural condition one would expect is that the inclusion $S \longrightarrow R$ is a ring homomorphism (which of course requires that $S$ contain the identity of $R$).

There is a Universal Mapping Property for quotient rings, analogous to the one for quotient modules (or quotient vector spaces).

And as one expects there is a First Isomorphism Theorem:

**Theorem 12.** *If $f : R \longrightarrow R'$ is ring homomorphism, then $R/\ker f \approx \operatorname{im} f$ (an isomorphism of rings).*

Verify these statements (Exercise 9).

Note that $R/I$ is an $R$-module via $r \cdot (s+I) = rs + I$.

See Exercise 2 to obtain a description of all $R/I$-modules as simply an $R$-module $M$ which is annihilated by all elements of $I$ ("$M$ is $I$-torsion").

## Direct Sums of Modules

Let $M_1$ and $M_2$ be $R$-modules. One defines the *external direct sum* as the set of ordered pairs

$$M_1 \oplus M_2 = \{ (m_1, m_2) \mid m_i \in M_i \}$$

with addition defined by

$$(m_1, m_2) + (n_1, n_2) = (m_1 + n_1, m_2 + n_2)$$

for $m_i, n_i \in M_i$ and scalar multiplication defined by

$$r(m_1, m_2) = (rm_1, rm_2)$$

for $r \in R$ and $m_i \in M_i$.

There is a concept of *internal direct sum* as well and as in the case of vector spaces there is a natural isomorphism between the two descriptions.

As in the case of vector spaces there is a simple way to describe all $R$-homomorphisms going to or from a direct sum of two $R$-modules.

Verify these statements (see Exercise 10).

## Direct Products of Rings

Let $R_1$ and $R_2$ be rings. One defines the *direct product* as the set of ordered pairs

$$R_1 \times R_2 = \{ (r_1, r_2) \mid r_i \in R_i \}$$

with addition defined by

$$(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$$

and multiplication defined by

$$(r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$$

for $r_i, s_i \in R_i$. The identity of $R_1 \times R_2$ is $(1,1)$. Note that the subset $\{ (r_1, 0) \mid r_1 \in R_1 \}$ is a two-sided ideal in $R_1 \times R_2$ but it is not a subring. Further, the natural function $i_1 : R_1 \longrightarrow R_1 \times R_2$ given by $i_i(r_1) = (r_1, 0)$ preserves addition and multiplication, but does not take $1$ to $(1,1)$, the identity of $R_1 \times R_2$, that is, it is not a ring homomorphism. Thus in describing $R_1 \times R_2$ internally one must be a bit careful in the choice of words. Nevertheless, there is an internal description of this concept which you should understand (see Exercise 11).

We now give a simple example. See Exercise 5 for a slight generalization.

**Proposition 13** (Chinese Remainder Theorem). *Let $a, b \in R$ for $R$ a PID. If $(a,b) = 1$, then there is a natural ring isomorphism*

$$R/(ab) \longrightarrow R/(a) \times R/(b)$$

*given by $x + (ab) \mapsto (x + (a), x + (b))$. The function is also an isomorphism of $R$-modules.*

*Proof.* There is a ring homomorphism $f : R \longrightarrow R/(a) \times R/(b)$ given by the natural surjection $R \longrightarrow R/(a)$ in the first factor and similarly $R \longrightarrow R/(b)$ in the second. An element $x \in R$ lies in the kernel if and only if it goes to $0$ in each coordinate: that is, $x + (a)$ is the zero of $R/(a)$, or $x + (a) = (a)$, so $x \in (a)$, or $a|x$; similarly, $b|x$. Now since $(a,b) = 1$ we have (proved earlier) that $ab|x$, that is $x \in (ab)$. On the other hand, every element of $(ab)$ is divisible by both $a$ and $b$ so $\ker f = (ab)$.

We next show that $f$ is onto and hence by the First Isomorphism Theorem for Rings we have $\operatorname{im} f \approx R/\ker f$, which is precisely the statement we need to prove. Since $(a,b) = 1$ in the PID $R$, there exist $r, s \in R$ such that $ra + sb = 1$. Given an arbitrary element $(x + (a), y + (b)) \in R/(a) \times R/(b)$ we need to find a $z \in R$ that maps to it. Just take $z = yra + xsb$.

Since $ra+sb = 1$, we have $xra+xsb = x$ yielding $x+(a) = xra+xsb+(a) = xsb+(a)$ so that $z + (a) = yra + xsb + (a) = xsb + (a) = x + (a)$. A similar argument gives $z + (b) = y + (b)$. □

## Bases, Free Modules and Matrices

Let $R$ be a ring and $M$ an $R$-module. Elements $m_1, \ldots, m_k$ of $M$ are said to be *linearly dependent* if there exist elements $r_1, \ldots, r_k$ of $R$, not all of which are $0$, so that $r_1 m_1 + \cdots + r_k m_k = 0$. A subset which is not linearly dependent is called *linearly independent.* A subset $\mathcal{B}$ of $M$ is called a *basis* for $M$, if

1. every element of $M$ is an $R$-linear combination of elements in $\mathcal{B}$, and

2. $\mathcal{B}$ is linearly independent over $R$.

Just as in the case of vector spaces, given an element $m \in M$ we can write it as a unique linear combination of the basis. In case $\mathcal{B}$ is finite and ordered, we then obtain coordinates of $m$ with respect to that ordered basis: $[m]_{\mathcal{B}}$. A module $M$ is called a *free* $R$-module if it contains a basis.

In the case of fields, every vector space has a basis. For rings, it is rarely true that every module contains a basis. For example, if $n > 1$ $\mathbb{Z}_n$ is a $\mathbb{Z}$-module which is not free: The dependence relation $n \cdot z = 0$ (note that $n \neq 0$ in $\mathbb{Z}$) holds for every $z \in \mathbb{Z}_n$. So there are no non-empty linearly independent subsets, and hence no bases. Similarly for any ring $R$ which contains a proper left ideal, $R/I \neq 0$ will be a cyclic module which is not free since all non-empty subsets will be dependent. In fact this method will always exhibit modules over $R$ which have no bases if there are any proper left ideals which are not $0$ (see Exercise 12).

However, for $n$ a positive integer $R^n$ is a free $R$-module since the usual elements and the usual proof show that $\{e_1, \ldots, e_n\}$ is a basis where $e_i \in R^n$ has $1$ in the $i$-th position and $0$ elsewhere. Thus there are many examples of free $R$-modules. We'll give more (and up to isomorphism all) below.

If one has an $R$-module homomorphism $f : M_1 \longrightarrow M_2$ from one finitely generated free module to another, upon choosing ordered bases for the two free modules, one obtains a matrix for $f$ with respect to the pair of ordered bases exactly as in the case of vector spaces. If one chooses a different pair of ordered bases, then there are change of basis matrices exactly as in the case of fields. The details are essentially the same as the ones we carried out earlier. There are some differences in case the ring $R$ is non-commutative which will be noted in our discussion below.

**Theorem 14** (Existence of Free Modules). *For every set $X$ there exists an $R$-module $R_X$ and one-to-one function $i : X \longrightarrow R_X$ such that $i(X)$ is a basis for the free module $R_X$.*

*Proof.* In fact we've seen the necessary idea used for vector spaces earlier and given in our list of examples above. Consider $R^{(X)} \subseteq R^X$, the set of functions from $X$ to $R$ which have finite support, that is, are not $0$ for only finitely many elements in $X$. The set $\{\delta_x \mid x \in X\}$ where $\delta_x$ is defined as earlier

$$\delta_x(y) = \begin{cases} 0 & y \neq x \\ 1 & y = x \end{cases}$$

is a basis. We then have for $f \in R^{(X)}$ the formula

$$f = \sum_{x \in X} f(x)\delta_x .$$

Verification of the formula is exactly as in the case for vector spaces, and the formula immediately implies that this set is a basis. The proof of the theorem is completed by defining $R_X = R^{(X)}$ and defining $i : X \longrightarrow F_X$ by $i(x) = \delta_x$. □

The fact that free modules satisfy a universal mapping property with respect to their bases as do vector spaces is proved exactly the same as it was for vector spaces. An alternate (equivalent) definition of free module is then

**Definition 15** (Free Module). Let $M$ be a module over a ring $R$ and let $\mathcal{B}$ be a subset of $M$. $M$ is a *free* $R$*-module* with basis $\mathcal{B}$ if for any $R$-module $N$ and any function $h : \mathcal{B} \longrightarrow N$, there exists a unique $R$-module homomorphism $H : M \longrightarrow N$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathcal{B} \arrow[r, "i"] \arrow[dr, "h"'] & M \arrow[d, dotted, "H"] \\
 & N
\end{tikzcd}$$

that is, $H \circ i = h$.

As usual this yields a one-to-one correspondence

$$\mathrm{Hom}_{\mathsf{Set}}(\mathcal{B}, N) \longleftrightarrow \mathrm{Hom}_R(M, N) .$$

Here $\mathrm{Hom}_R(M, N)$ is (just as for vector spaces) the set of all $R$-module homomorphisms from $M$ to $N$. The set becomes an $R$-module under point-wise addition of functions and scalar multiplication (as before).

**Remark 16.** If $X$ is a finite set with $n$ elements, then $F_X \approx F^n$.

In general, if there is a one-to-one, onto function from $X$ to $Y$, then $F_X \approx F_Y$ is immediate from the definition of free modules (and the Universal Mapping Property of the given basis).

The central question then is the converse: If we are given an isomorphism $F_X \approx F_Y$, does this imply that $|X| = |Y|$? If this implication is valid for the ring $R$, the ring is said to have *invariant basis number*, sometimes denoted by IBN.

For commutative rings any two bases for the same free module always have exactly the same number of elements. An outline of the proof of this is given in the exercises at the end. The idea is to show that it follows from the corresponding result for fields. See Exercise 17. An alternate proof for the finitely generated case using the theory of determinants appears in Exercise 18.

If the ring $R$ is not commutative, then it is possible for a free module to have bases of different sizes. Examples are constructed in the exercises using just the linear algebra we have already developed (plus some observations about infinite sets). See Exercise 19.

In fact, the invariance of the size of a basis is only a question in case the bases are finite. Simple arguments using cardinal numbers show that the case where the two bases for the same module are infinite must always have the same cardinality.

**Proposition 17.** *Let $M$ be a finitely generated $R$-module. Then for some integer $n > 0$ there exists a surjective homomorphism $R^n \longrightarrow M$. That is, $M$ is isomorphic to a quotient module of a finitely generated free module.*

*Proof.* Let $M$ be generated by $m_1, \ldots, m_n$. Consider the free module with $n$ generators, $R^n$. Letting $h(e_i) = m_i$ gives the $R$-module homomorphism $H: R^n \longrightarrow M$ whose image will contain all linear combinations of the $m_i$ and hence is onto. Thus $M \approx R^n / \ker H$. □

**Proposition 18.** *Let $M$ be an $R$-module. Then $M$ is the quotient of some free $R$-module.*

*Proof.* Clearly there is a surjection $F_M \longrightarrow M$ induced by the identity function on $M$. This is clearly not a very efficient choice of generating set for $M$. □

# Exercises

Recall that all of our rings have associative multiplication and contain an identity element.

**Modules 1.** Let $\mathbb{Z}_n$ denote the ring of integers modulo $n$ for some positive integer $n > 1$. Show that $A$ being a $\mathbb{Z}_n$-module is exactly the same thing as requiring that $A$ be an abelian group with the property that for every element $a \in A$, then $na = 0$. Elements satisfying the equation $na = 0$ are called $n$*-torsion.*

$A$ being a $\mathbb{Z}_n$-module is also the same thing as saying that $A$ is an $n$-torsion $\mathbb{Z}$-module.

**Modules 2.** Let $R$ be a commutative ring with ideal $I \neq R$. Then $R/I$ is a commutative ring with 1. Show that $M$ being an $R/I$-module is exactly the same as requiring that $M$ be an $R$-module such that $im = 0$ for all $i \in I$ and all $m \in M$. Such elements of $M$ are called $I$*-torsion.*

**Modules 3.** Let $M$ be a module over the ring $R$. Assume that $A$, $B \subseteq M$ are submodules. Prove that there is a natural isomorphism $f : A/(A \cap B) \longrightarrow (A+B)/B$. Give $f$ explicitly.

**Modules 4.** Let $R$ be a PID which is not a field. Let $a \in R$. Determine precisely when $R/(a)$ will be a field.

**Modules 5** (Chinese Remainder Theorem). Let $R$ be a commutative ring with ideals $I$ and $J$.

a. Show that the following sequence is an exact sequence of $R$-modules:

$$0 \longrightarrow I \cap J \xrightarrow{inc} R \xrightarrow{f} R/I \times R/J \xrightarrow{p} R/(I+J) \longrightarrow 0$$

where *inc* denotes inclusion, $f(x) = (x+I, x+J)$ and $p(r+I, s+J) = r-s+(I+J)$.

b. Conclude that there is an induced exact sequence of $R$-modules

$$0 \longrightarrow R/(I \cap J) \xrightarrow{f} R/I \times R/J \xrightarrow{p} R/(I+J) \longrightarrow 0 .$$

c. If $I + J = R$, show that $I \cap J = IJ$ and further there there is a ring isomorphism

$$R/(I \cap J) \xrightarrow{f} R/I \times R/J .$$

d. Give a version of the preceding three parts in case $R$ is a non-commutative ring with 2-sided ideals $I$ and $J$ (that is, for $r \in R$, $i \in I$ we have both $ri \in I$ and $ir \in I$). [Replace $IJ$ by $IJ + JI$ in the last part.]

e. Let $R$ be a PID. Let $a \in R$ be arbitrary. What is the largest number of non-trivial cyclic direct summands one can decompose $R/(a)$ into? How does the number depend on $a$?

**Modules 6.** Verify that the vector space $V$ is an $F[x]$-module under the definition of scalar multiplication given in Example 6.

**Modules 7.** State and prove the Universal Mapping Property for quotient modules.

**Modules 8.** Prove the First Isomorphism Theorem for Modules (Theorem 9).

**Modules 9.** a. State and prove the Universal Mapping Property for quotient rings.

b. Prove the First Isomorphism Theorem for Rings (Theorem 12).

**Modules 10.** Prove results for modules that are analogous to those for vector spaces:

a. Define the internal direct sum of a module in terms of two submodules. Prove there is a natural isomorphism with the corresponding external description.

b. Determine how one gives $R$-homorphisms to and from a direct sum of two $R$-modules. State these in terms of a universal mapping property (with corresponding commutative diagrams).

**Modules 11.** Prove analogous results for rings:

a. Give an internal description of the direct product of two rings. Prove there is a natural isomorphism with the corresponding external description given above.

b. How does one determine ring homomorphisms to or from a direct product of rings? Can you describe either of your answers in terms of a universal mapping property? Why is the term "direct product" rather than "direct sum" used?

**Modules 12.** Let $R$ be a non-trivial ring. Assume that the only left ideals of $R$ are $0$ and $R$. That is, the method used earlier to show there is a non-zero cyclic module over $R$ which does not have a basis fails for such a ring.

a. Show that every non-zero element of $R$ has a left inverse. [Hint: For non-zero $a$ consider the function $\rho_a : R \longrightarrow R$ given by $\rho_a(x) = xa$. What kind of function is $\rho_a$? What must $\operatorname{im} \rho_a$ be?]

b. Show that if every non-zero element of $R$ has a left inverse, then every non-zero element of $R$ has a two-sided inverse. Conclude that if $R$ is commutative, then $R$ is a field.

Such a ring $R$ is called a *division ring* or *skew field.* A large part of linear algebra can be developed for such rings in the same fashion as we have done here. The parts involving eigenvalues and determinants can not be done however.

**Modules 13.** Let $R$ be a division ring. Let $M$ be a finitely generated module over $R$. Prove that $M$ has a basis; that is, $M$ is a free $R$-module.

**Modules 14.** Let $R$ be a division ring. Let $M$ be a finitely generated module over $R$. Prove that any two bases for $M$ have the same number of elements.

**Modules 15.** Let $R = \mathbb{Z}[x]$. Show that there exist ideals in $R$ which are not principal.

**Modules 16.** Let $R$ be a commutative ring. An ideal $I \subseteq R$ is called *maximal* if $I \neq R$ and if $J$ is an ideal with $I \subseteq J \subseteq R$ then either $J = I$ or $J = R$.

An ideal $I \subseteq R$ is called *prime* if $I \neq R$ and if whenever $a, b \in R$ are such that $ab \in I$ then it must be that either $a \in I$ or $b \in I$.

a. Prove that a maximal ideal must be a prime ideal.

b. Prove that $I$ is a maximal ideal if and only if $R/I$ is a field.

c. Prove that $I$ is a prime ideal if and only if $R/I$ is a domain.

d. Let $R$ be a principal ideal domain (such as $\mathbb{Z}$ or $F[x]$). Determine all maximal ideals and all prime ideals of $R$.

e. Give an example to show that prime ideals are not always maximal.

**Modules 17.** Let $R$ be a commutative ring which is not a field. Let $M$ be a free module with basis $\mathcal{B}$.

a. Let $I \subseteq R$ be a proper ideal. Let $IM$ be the submodule of $M$ generated by all products $im$ for $i \in I$ and $m \in M$, that is, the set of all possible finite sums of such elements. Let $\overline{M} = M/IM$ and write $\overline{m} = m + IM$. Show that $\overline{M}$ is an $\overline{R} = R/I$ module. Let $\overline{\mathcal{B}}$ be the image of $\mathcal{B}$ under the homomorphism $p : M \longrightarrow \overline{M}$. Show that $\overline{M}$ is a free $\overline{R}$-module with basis $\overline{\mathcal{B}}$ and that $\mathcal{B} \longrightarrow \overline{\mathcal{B}}$ given by $b \mapsto \overline{b}$ is a one-to-one correspondence.

b. Assume that every commutative ring $R$ (with $1$) contains a maximal ideal $I$. (This follows from a straightforward argument using the Axiom of Choice in the form of Zorn's Lemma.) Prove that any two bases for a free module $M$ over the commutative ring $R$ have the same cardinality (same number of elements).

**Modules 18.** Let $R$ be a ring, $M$ a free $R$-module with bases $\mathcal{A}$ having $n$ elements and basis $\mathcal{B}$ having $m$ elements. Let $A = [I]_{\mathcal{A},\mathcal{B}} \in R^{m\times n}$ and $B = [I]_{\mathcal{B},\mathcal{A}} \in R^{n\times m}$. Then $AB = I_m$ and $BA = I_n$.

a. Assume $m > n$. By enlarging matrices by adding rows or columns of $0$ in appropriate places, construct new square matrices $A', B' \in R^{m\times m}$ such that $A'B' = I_m$.

b. Assume that $R$ is a commutative ring and that one has already developed determinants over commutative rings, conclude that the equation of the preceding part cannot be valid.

**Modules 19.** Let $F$ be a field and $V_1$ an infinite dimensional vector space over $F$ (e.g., $V_1 = F[x]$). Take $V_2 = V_1$, $V = V_1 \oplus V_2$ and let $R = \mathrm{End}_F(V) = \mathrm{Hom}_F(V, V)$.

a. Verify that $\dim V = \dim V_1 = \dim V_2$. (Do this at least in the case of $V_1 = F[x]$, i.e., countable dimension. The question about sets is: Show that the cardinality of the disjoint union of two copies of the same infinite set is equal to the cardinality of the original set.)

b. Show that $R = \operatorname{Hom}_F(V, V_1 \oplus V_2) \approx \operatorname{Hom}_F(V, V_1) \oplus \operatorname{Hom}_F(V, V_2)$ are isomorphic as left $R$-modules. Conclude that $R \approx R \oplus R$ as left $R$-modules.

c. Conclude that there exist $a, b, c, d \in R$ such that the matrices $A = (a, b)^t$ and $B = (c, d)$ satisfy $BA = ca + db = 1 = I_1$ and

$$AB = \begin{bmatrix} ac & ad \\ bc & bd \end{bmatrix}$$

is $I_2$ (so $ac = 1$, $bc = 0$, $ad = 0$, $bd = 1$) (compare to Exercise 18). So there can be no straight-forward generalization of determinants to non-commutative rings having all of the properties one has for commutative rings.

d. Show that for all positive integers $n$, $R \approx R^n$ as left $R$-modules.

e. Show that $R \approx R^{2\times 2}$ as rings.

f. Show that for all positive integers $n$, $R \approx R^{n\times n}$ as rings.

**Modules 20.** Let $R$ be a commutative ring and let $M$ be an $R$-module. An element $m \in M$ is called a *torsion* element if there exists a non-zero element $r \in R$ such that $rm = 0$. Let $\operatorname{tor}(M)$ denote the set of torsion elements in $M$. Assume now and for the rest of the problem, that $R$ is a domain (i.e., if $ab = 0$ for elements $a, b \in R$, then either $a = 0$ or $b = 0$).

a. Show that $\operatorname{tor}(M)$ is a submodule of $M$ (i.e., is non-empty and closed under addition and scalar multiplication by arbitrary elements of $R$).

b. For $M_1$ and $M_2$ $R$-modules, determine $\operatorname{tor}(M_1 \oplus M_2)$.

c. If $N_1 \subseteq M_1$ is a submodule and $N_2 \subseteq M_2$ is a submodule, give an explicit isomorphism $(M_1 \oplus M_2)/(N_1 \oplus N_2) \longrightarrow M_1/N_1 \oplus M_2/N_2$ and verify that it is an isomorphism. Compute $(M_1 \oplus M_2)/\operatorname{tor}(M_1 \oplus M_2)$.

d. Let $M = R^m$, the direct sum of $m$ copies of $R$. What is $\operatorname{tor}(M)$?

e. Consider the quotient module $M/\operatorname{tor}(M)$. Show that it contains no non-zero torsion elements.

f. If $R$ is a commutative ring and $a \in R$ is non-zero, compute $\operatorname{tor}(R/(a))$ where $R/(a)$ is considered as an $R$-module.

**Modules 21.** Let $R$ be a commutative ring with an identity element 1. Let $M$ be a module over $R$. Assume that $M$ is a free module (has a basis). Let $N$ be a submodule of $M$.

a. It is not always true that $N$ will have a basis. Let $I$ be an ideal of $R$. By comparing the definitions, note that if we think of $R$ as a module over itself (free of rank $1$), then $I$ is just a submodule of $R$. Show that any two non-zero elements of $I$ are linearly dependent. Let $F[x,y]$ be the ring of polynomials in two variables over the field $F$. Let $I$ be the ideal of $F[x,y]$ generated by $x$ and $y$:

$$I = \{ xf + yg \mid f,g \in F[x,y] \} \ .$$

By the previous observation, if $I$ were to have a basis, the basis could have at most one non-zero element (i.e., the ideal $I$ would have to be principal). Show that this is not possible. [Hint: Consider the degree function (total degree in $x$ and $y$). If $h$ were to be the single element in the basis, what would its degree have to be? What are all polynomials of this degree? Can any one of them work?]

b. Let $M$ be a free module over $R$ of rank $n$. Assume that $N$ is a submodule of $M$ that happens to be free and whose rank is $m$. In the previous problem you have shown that if $n = 1$, then $m \leq 1$, i.e., $m \leq n$. Prove this inequality always holds for finite $m$ and $n$ if $R$ is a commutative integral domain.

$\boxed{\text{c.}}$ Prove the same result for any commutative ring $R$ with identity. If you can't get the general case, try doing cases for small values of $m$ and $n$.

**Modules 22.** Let $R$ be an arbitrary ring. A ring $R$ is said to have *invariant basis number* (IBN) if $R^k \approx R^l$ as $R$-modules, then $k = l$ (i.e., any two bases of the free module $R^k$ have the same size). Let $[R,R]$ be the subgroup of $R$ under addition generated by all elements (additive commutators) $xy - yx$ for $x, y \in R$. Define $H_0(R) = R/[R,R]$ (a group under addition). Clearly if $R$ and $S$ are isomorphic rings, then $H_0(R) \approx H_0(S)$ as abelian groups. If $R$ is commutative, then this group under $+$ also has a ring structure; in general it doesn't. Let $n$ be a positive integer and let $M_n(R)$ be the ring of $n \times n$ matrices with entries in $R$. Define the trace $\mathrm{Tr} : M_n(R) \longrightarrow H_0(R)$ as usual: $\mathrm{Tr}(A) = a_{11} + a_{22} + \cdots + a_{nn} + [R,R]$ for $A = (a_{ij})$.

a. Show that $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ for any $m \times n$ matrix $A$ and any $n \times m$ matrix $B$ with entries in $R$.

b. Show that trace induces a group isomorphism $\mathrm{Tr} : H_0(M_n(R)) \longrightarrow H_0(R)$. [Remark: This is a special case of what happens for *Morita equivalent* rings (the two rings have essentially the same categories of modules).]

c. Show that if $R^k \approx R^l$ as rings, then $\mathrm{Tr}(I_k) = \mathrm{Tr}(I_l)$.

d. Compute $\mathrm{Tr}(I_n)$. Prove that if $1$ has infinite order (that is, $1+1+\cdots+1$ is never $0$ for any positive number of terms) in the abelian group $H_0(R)$, then $R$ has IBN.

e. More precisely show that if $m, n < o(1)$ where $o(1)$ is the order of $1$ in $H_0(R)$ (the smallest number of times $1$ added to itself gives $0$), and $R^m \approx R^n$, then $n = m$.

f. $\boxed{\star}$ Let $F$ be a field, $V$ an infinite dimensional vector space over $F$, and $R = \mathrm{End}_F(V) = \mathrm{Hom}_F(V, V)$. Compute $H_0(R)$. [The other parts of this problem are straightforward; this part is not.]

Remark: One can also define the trace of a finitely generated projective (a direct summand of a free module $R^k$) $R$-module using these ideas. The result is what is known as the Hattori-Stallings trace.

**Modules 23.** Let $R$ be an arbitrary ring. $R$ is said to have *invariant basis number* (IBN) if for non-negative integers $m$, $n$ whenever $R^m \approx R^n$, then $m = n$.

a. Let $\theta : R^n \longrightarrow R^n$ be a homomorphism of $R$-modules. Assume that $R$ satisfies: Any $\theta$ which is surjective must be an isomorphism. Show that $R$ has IBN.

b. Show that any noetherian ring (ascendending chain condition on left ideals, or ACC) has IBN.

c. Prove that any artinian ring (descending chain condition on left ideals, or DCC) has IBN. [Give a dual proof (reverse arrows).]

d. Restate IBN in terms of matrices. Show that $R$ satisfies IBN if and only if $R^\circ$ (the opposite ring: has the same set with the same addition, but multiplication is given by $a \star b = ba$ where $ba$ was the original multiplication in $R$) does.

e. Show that if $R \longrightarrow S$ is a homomorphism of rings and $S$ satisfies IBN, then so does $R$. So subrings of rings with IBN, satisfy IBN. What about homomorphic images? [Remark: Using similar arguments one can show any direct (inverse) limit of rings satisfying IBN also does.]

**Modules 24.** An element $e$ in a ring is called *idempotent* if $e^2 = e$.

a. Show that the only idempotent in a local ring is the identity.

b. An $R$-module $M$ is called *indecomposable* if it cannot be written as the direct sum of two proper submodules. Show that if $M$ is an $R$-module, then $M$ is indecomposable if $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ is a local ring.

c. If $M$ is an indecomposable $R$ module which satisfies both the ACC and DCC on submodules, then $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ is a local ring.

Example: $F$ a field. Show that $R = F[x]/(x^n)$ for $n > 0$ is a local ring. Hence considered as an $R$-module, it is indecomposable.

# History of the Notes

The Notes for the course *Math 4330, Honors Linear Algebra* at Cornell University have been developed over the last ten years or so mainly by the following (in chronological order):

Gerhard O. Michler

R. Keith Dennis

Martin Kassabov

W. Frank Moore

Yuri Berest.

Harrison Tsai also contributed a number of interesting exercises that appear at the ends of several sections of the notes.

Most sections have been revised so many times the original author may no longer recognize it. The intent is to provide a modern treatement of linear algebra using consistent terminology and notation. Some sections are written simply to provide a central source of information such as those on "Useful Definitions", "Subobjects", and "Universal Mapping Properties" rather than as a chapter as one might find in a traditional textbook. Additionally there are sections whose intent is to provide proofs of some results which are not given in the lectures, but rather provide them as part of a more thorough development of a tangential topic (e.g., Zorn's Lemma to develop cardinal numbers and the existence of bases and dimension in the general case).

A large number of challenging exercises from many different sources have been included. Although most should be readily solvable by students who have mastered the material, a few even more challenging ones still remain.

Much still remains to be done. Corrections and suggestions for additional exercises, topics and supplements are always welcome.

Keith Dennis

e-mail address: **math4330@rkd.math.cornell.edu**

# Modules over a PID

Let $R$ be a principal ideal domain. A module $M$ over $R$ is said to be *finitely generated* if there is a finite subset of $M$ such that every element of $M$ is an $R$-linear combination of elements in this set; that is, in the terminology used for vector spaces, the set spans $M$.

**Theorem 1** (Stacked Basis Theorem for Finitely Generated Modules over a PID). *Let $R$ be a principal ideal domain. Let $M$ be a free module of rank $m$ and let $M'$ be a submodule of $M$. Then*

*a. $M'$ is free of rank $n$, $0 \leq n \leq m$.*

*b. If $M'$ is not $0$, then there exists a basis $\{e_1, \ldots, e_m\}$ of $M$ and non-zero elements $a_1, \ldots, a_n$ of $R$ such that $\{a_1 e_1, \ldots, a_n e_n\}$ is a basis for $M'$. Further the $a_i$ satisfy $a_i \mid a_{i+1}$ for $1 \leq i < n$.*

*c. The elements $a_i$ are uniquely determined up to multiplication by units.*

**Remark 2.** Let $N$ be a finitely generated $R$-module with generating set having $m$ elements. Then there is a surjective homomorphism $S : R^m \longrightarrow N$ given by sending the basis elements to the $m$ generating elements. Let $M' = \ker S$. The Stacked Basis Theorem implies that there exists a nice choice of bases so that the matrix for the inclusion map of $\ker S = M' \approx R^n$ into $M = R^m$ with respect to these bases only has non-zero entries on the diagonal, namely the $a_i$.

**Definition 3.** Let $R$ be a principal ideal domain. A matrix $A \in R^{m\times n}$ is said to be in *Smith Normal Form* if all entries off the diagonal are zero, and if $a_{11}, \ldots, a_{k,k}$ are all the non-zero entries, then $a_{i,i} \mid a_{i+1,i+1}$ for $1 \leq i < k$.

**Proposition 4.** *Let $R$ be a PID and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_\ell \subseteq \cdots$ be a chain of ideals of $R$. Then there exists an integer $n_0$ such that $I_j = I_{n_0}$ for all $j \geq n_0$.*

*Proof.* Let $I = \bigcup_{j\geq 1} I_j$. Let $a, b \in I$, say $a \in I_i$ and $b \in I_j$. Given any pair of integers $1 \leq i, j$, then either $I_i \subseteq I_j$ if $i < j$ or $I_j \subseteq I_i$ if $j < i$. Then both $a$ and $b$ lie in one, say $I_i$, and so does their sum. It easily follows then that $I$ is an ideal of $R$. As $R$ is a PID, there exists a $d \in R$ so that $I = (d)$. But $d \in I_{n_0}$ for some $n_0$. Hence $(d) \subseteq I_{n_0} \subseteq I_j \subseteq I = (d)$ if $j \geq n_0$. Hence all are equal as asserted. □

**Definition 5.** A module $M$ is called *noetherian* if for any sequence of submodules $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots \subseteq M_\ell \subseteq \cdots$ there exists an integer $n_0$ such that $M_j = M_{n_0}$ for all $j \geq n_0$.

A ring $R$ is called *noetherian* if $R$ considered as a module is noetherian.

This condition is also referred to as the *ascending chain condition.*

We've thus proved that a PID is a noetherian ring, that is, it contains no infinite proper ascending chains of ideals.

Now let $T\colon\ R^n \longrightarrow R^m$ be a homomorphism and assume $\mathcal{A}$ is a basis for $R^n$ and $\mathcal{B}$ is a basis for $R^m$. Then the matrix of $T$ with respect to these two bases is $[T]_{\mathcal{A},\mathcal{B}}$, an $m \times n$ matrix. Via the interpretation of Theorem 1 as given in Remark 2, we ask the more general question:

**Question 6.** Given any homomorphism $T\colon\ R^n \longrightarrow R^m$ do there exists bases $\mathcal{A}'$ and $\mathcal{B}'$ so that $[T]_{\mathcal{A}',\mathcal{B}'}$ is in Smith Normal Form?

An equivalent version for matrices is the following:

**Question 7.** Let $A \in R^{m\times n}$. Is $A$ equivalent to a matrix $B \in R^{m\times n}$ in Smith Normal Form? That is, do there exist invertible matrices $Q \in R^{m\times m}$ and $P \in R^{n\times n}$ so that $B = QAP$ is in Smith Normal Form?

For a PID we now show how to solve the general problem which will in particular solve the case for the inclusion map of Theorem 1. For $a, b \in R$, not both $0$, there exist $r, s \in R$ such that $ra+sb = d$ for $d = \gcd(a, b)$. Since $d \mid a$ and $d \mid b$, $a' = a/d$ and $b' = b/d$ are elements of $R$ and $ra' + sb' = 1$. Hence we have an invertible matrix

$$\begin{bmatrix} r & s \\ -b' & a' \end{bmatrix}.$$

Further note that

$$\begin{bmatrix} r & s \\ -b' & a' \end{bmatrix}\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}.$$

In case $a \mid b$, $1 \cdot a + 0 \cdot b = a$, then the matrix is actually an elementary matrix

$$\begin{bmatrix} 1 & 0 \\ -b' & 1 \end{bmatrix}.$$

For a euclidean ring (e.g., $\mathbb{Z}$ or $F[x]$) it is easy to see the first $2 \times 2$ matrix is the product of elementary matrices (just use the euclidean algorithm). However, for an arbitrary PID, this is not always the case. Using topological methods one can show that the invertible matrix

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

(of determinant $1$) with entries in the ring $R = \mathbb{R}[x]/(1 - x^2 - y^2)$ (the ring of "polynomial functions on the unit circle") is not the product of elementary matrices.

Assume $A$ is an $m \times n$ matrix which is not $0$ and let $\ell(A)$ denote the gcd of all its entries. We give an argument to show that there is sequence of steps (essentially bounded by the total number of primes in the factorization of $\ell(A)$) to put the matrix in Smith Normal Form.

If $A$ has all entries $0$ in the first column, apply a column operation (right multiply by the appropriate elementary matrix) to place at least one non-zero element in the first column.

Let $A = \left[a_{ij}\right]$. Take $i < j$ and let $a = a_{i,1}$ and $b = a_{j,1}$. Construct the $m \times m$ matrix $L$ which is the same as the identity matrix in all positions except for the $(i,i), (i,j), (j,i), (j,j)$ positions. Place the four entries of the above matrix in these positions ($r$ in $(i,i)$, $s$ in $(i,j)$, $-b'$ in $(j,i)$ and $a'$ in $(j,j)$). Then the multiplication $LA$ will replace the $(i,1)$ entry by $d$ and the $(j,1)$ entry by $0$.

By applying this process $m-1$ times (for the pairs $(1,1)$, $(j,1)$, $j = m$ through $2$), the first column of $L_2 \cdots L_m A$ will have a single non-zero entry $d_1$ in the $(1,1)$ position. This entry will be the gcd of the entries of the first column. Now $(d_1) \subseteq (\ell(A))$.

If $d_1$ divides all the entries in the first row, we can apply elementary column operations to remove those entries without disturbing the first column. This will yield a single non-zero entry $d$ in the first row and first column.

If not, similarly applying column operations (multiplication on the right by the same type of matrices) can then make the first row have a single non-zero entry $d_2$ (the gcd of the entries in the first row of our modified matrix) and $(d_1) \subseteq (d_2) \subseteq (\ell(A))$.

Unfortunately, the operations from the right may have messed up the first column. However, we may repeat the process to fill the first column with $0$ except for the $(1,1)$ entry, call it $d_3$. Again we have $(d_1) \subseteq (d_2) \subseteq (d_3) \subseteq (\ell(A))$. Repeating the process over and over again must ultimately stabilize by Proposition 4 as there are no infinite strictly ascending chains of ideals in a PID. Once $d_i = d_{i+1}$ we can clean out the remaining entries of the relevant row or column without disturbing the row/column we just finished cleaning (as we observed in the first step).

The $d$ in the $(1,1)$ position is now the only non-zero entry in the first row and column. If this $d$ divides all other entries in the matrix, great. If not, there is some entry it does not divide. Add that column to the first column and start over. Repeat the entrire procedure until the $(1,1)$ entry divides all other entries in the matrix. That entry is now our $a_1$ which we wanted to find.

Let $A'$ be the $(m-1) \times (n-1)$ matrix obtained from $A$ be removing the first row and column. Iterate the same procedure until the normal form has been constructed.

This proves the existence part of the following theorem.

**Theorem 8** (Smith Normal Form for Matrices over a PID). *Let $R$ be a PID and let $M \in R^{m\times n}$ be a matrix. Then there exist invertible matrices $P \in R^{m\times m}$ and $Q \in R^{n\times n}$ so that $A = PMQ$ is in Smith Normal Form. The Smith Normal Form is unique up to multiplication of the diagonal elements by units. Equivalently, the chain of ideals $(a_{1,1}) \subseteq (a_{2,2}) \subseteq \cdots \subseteq (a_{k,k})$ associated to the non-zero elements $a_{i,i}$ on the diagonal is unique.*

**Remark 9.** This reduction process is extremely important for solving both mathematical and practical problems. It is implemented in most systems for doing computational mathematics. Usually one even has the option of obtaining not only the Smith Normal Form, but also the matrices $Q$ and $P$,

**Lemma 10.** *Let $R$ be a ring and $M_1$, $M_2$ modules. Let $N_i \subseteq M_i$ be submodules. Then there is a natural isomorphism*

$$(M_1 \oplus M_2)/(N_1 \oplus N_2) \longrightarrow M_1/N_1 \oplus M_2/N_2 \ .$$

*Proof.* This is left as an exercise. □

**Corollary 11.** *If $N$ is a finitely generated module over a PID $R$, then there exist non-units $a_1, \dots, a_k \in R$ with $a_1 \mid a_2 \mid \cdots \mid a_k$ and an integer $l \geq 0$ such that*

$$M \approx R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_k) \oplus R^l \ .$$

*The integers $k$ and $l$ are uniquely determined by $N$. The $a_i$ are unique up to multiplication by units.*

**Corollary 12.** *If $A$ is a finitely generated abelian group, then there exist integers $1 < n_1, n_2, \dots, n_k$ and $l \geq 0$ with $n_1 \mid n_2 \mid \cdots \mid n_k$ such that*

$$A \approx \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k} \oplus \mathbb{Z}^l \ .$$

*The integers $k$, $l$, and $n_i$ are uniquely determined by $A$.*

**Remark 13.** The number of terms and the $(a_i)$ are uniquely determined by the module, but the particular decomposition is not. For example, if $p$ is a prime there are several ways to decompose $A = \mathbb{Z}_p \oplus \mathbb{Z}_p$ as an internal direct sum. Note that different bases for $A$ considered as a vector space over $\mathbb{Z}_p$ may give different decompositions as a sum of two one-dimensional subspaces. How many different ways can this be done? However, in all cases there are exactly two summands, each isomorphic to $\mathbb{Z}_p$.

**Definition 14.** An $R$-module $M$ is called *cyclic* if there exists an element $m \in M$ so that $M = Rm = \{rm \mid r \in R\}$. The element $m$ is called a *generator* of $M$.

**Lemma 15.** *Let $R$ be a commutative ring. Any cyclic module $M$ is isomorphic to $R/I$ for some ideal $I$ of $R$. Conversely every $R/I$ is a cyclic module.*

*Proof.* This follows via the First Isomorphism Theorem as the kernel of the surjective map $R \longrightarrow M$ given by $r \mapsto rm$ has kernel an ideal of $R$. The converse is clear. □

*Proof.* To prove Corollary 11 note that by Lemma 10, the Stacked Basis Theorem, and the discussion following it, we obtain an isomorphism of $N \approx M/\ker T$ as a sum of cyclic modules of the form $R/(b)$ for various $b \in R$. If $b$ is a unit, the quotient is $R/R$, the zero module. Omit these terms. This leaves only the terms corresponding to non-units and $0$ (the terms from $n+1$ to $m$, if any). Renumber the $a_i$ to $a_1, a_2, \dots, a_k$ and let $l = m - n$.

Corollary 12 is immediate from the first for the PID $\mathbb{Z}$. □

In all cases we've written the finitely generated module as a sum of cyclic modules. The cyclic modules are of two types: either $R$ (a free module), or $R/(a)$ for some non-zero $a$. The second type are what are called *torsion* modules.

**Definition 16.** Let $M$ be an $R$-module. An element $m \in M$ is called *torsion* if there exists a non-zero element $r \in R$ so that $rm = 0$. We let $\operatorname{tor}(M)$ denote the set of all torsion elements of $M$,

**Lemma 17.** *Let $M$ be an $R$-module. If $R$ is a commutative domain, then $\operatorname{tor}(M)$ is a submodule of $M$.*

*Proof.* This is left as a homework exercise. □

In general for $M$ a module over a commutative domain $R$, one has a short exact sequence

$$0 \longrightarrow \operatorname{tor}(M) \longrightarrow M \longrightarrow M/\operatorname{tor}(M) \longrightarrow 0\ .$$

For $M$ finitely generated and $R$ a PID, the result above shows that the sequence splits (not a natural map), and that the module $M/\operatorname{tor}(M)$ is a free $R$-module.

It is always true that $M/\operatorname{tor}(M)$ is a torsion-free module (see exercises). If a module over a PID is finitely generated and torsion free, Corollary 11 implies that it is in fact free. This statement may be false if the module is not finitely generated even if $R$ is a PID (see Exercise 7).

**Corollary 18.** *Let $R$ be a PID. Then every finitely generated torsion-free module $M$ is free.*

Our main application of these ideas to linear algebra comes from the next conclusion.

**Corollary 19.** *Let $V$ be a finite dimensional vector space over the field $F$ and let $T : V \longrightarrow V$ be a linear transformation. Then $V$ is an $F[x]$-module via $f \cdot v = f(T)(v)$ and there exist monic non-scalar polynomials $f_1, f_2, \ldots, f_k \in F[x]$ with $f_1 \mid f_2 \mid \cdots \mid f_k$ such that there is an $F[x]$-module isomorphism*

$$V \approx F[x]/(f_1) \oplus \cdots \oplus F[x]/(f_k)\ .$$

*The $f_i$ and $k$ are unique.*

**Definition 20.** The $f_i$ that appear in the corollary are called the *invariant factors* of $T$.

*Proof.* Now $T \in \operatorname{End}_F(V) = \operatorname{Hom}_F(V, V)$ which has dimension $n^2 = (\dim V)^2$. Thus the set $\left\{ I, T, T^2, \ldots, T^{n^2} \right\}$ must be linearly dependent over $F$ as it has $1 + n^2$ elements. Therefore there exists a non-zero polynomial $f \in F[x]$ of degree at most $n^2$, so that $f(T) = 0$. Thus $V$ is a torsion $F[x]$-module with all elements of $V$ annihilated by the single element $f$: $f \cdot v = f(T)(v) = 0$. Thus this corollary is a consequence of the first one.

Alternatively one can note that $F[x]$ has infinite dimension over $F$ and as $V$ is of finite dimension over $F$ there can be no copies of $F[x]$ in the decomposition of the $F[x]$-module $V$. □

**Definition 21.** Let $V$ be a finite dimensional vector space over the field $F$. Let $T \in \operatorname{End}_F(V) = \operatorname{Hom}_F(V, V)$ be a linear transformation. The unique non-zero monic generator of the ideal

$$\{ f \in F[x] \mid f(T) = 0 \}$$

is called the *minimal polynomial* of $T$.

Note that the minimal polynomial of $T$ must then be $f_k$ since all other $f_i$ divide the last one, and each annihilates its respective cyclic module.

**Definition 22.** A subspace $W \subseteq V$ is $T$*-invariant* if $T(w) \in W$ for all $w \in W$.

A $T$-invariant subspace $W \subseteq V$ is called *cyclic* (with respect to $T$) if there exists a vector $w_0 \in W$ such that $\left\{ T^i(w_0) \;\middle|\; 0 \leq i \right\}$ spans $W$. (That is, $W$ is a cyclic $F[x]$-module.)

Another way to describe the result of the last corollary is the following: Let $V_i$ be the image of the submodule $F[x]/(f_i)$ under the inverse of the isomorphism given in the corollary. Then there is a decomposition of $V$ into an internal direct sum of subspaces $V_1, V_2, \ldots, V_k$ such that

(1) $V_i$ is $T$-invariant,

(2) $V_i$ is cyclic,

(3) $T$ restricted to $V_i$ has minimal polynomial $f_i$,

(4) $f_i \mid f_{i+1}$ for $1 \leq i < k$.

It is easy to show (see exercises) that for $f \in F[x]$, a non-scalar monic polynomial, $f = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$, then $M = F[x]/(f)$ is an $F[x]$-module, a finite dimensional vector space over $F$ and $\mathcal{B} = \left\{ \overline{1}, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}} \right\}$ is a basis over $F$. Here $\overline{g}$ denotes the image of $g$ in $M$ under the natural surjection $F[x] \longrightarrow M$. If $S : M \longrightarrow M$ denotes the linear transformation given by $S(\overline{g}) = \overline{x}\,\overline{g}$, then its matrix with respect to $\mathcal{B}$

$$C(f) = [S]_{\mathcal{B}}$$

is called the *companion matrix* of the polynomial $f$. In fact $f$ is the minimal polynomial of $S$, and of $C(f)$.

An easy computation shows that the $n \times n$ compation matrix is

$$C(f) = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

**Corollary 23** (Rational Canoncial Form). *Let $V$ be a finite dimensional vector space over a field and let $T \in \mathrm{End}_F(V) = \mathrm{Hom}_F(V,V)$. Then there exists a basis $\mathcal{B}$ and non-scalar monic polynomials $f_1, \ldots, f_k$ so that*

$$[T]_{\mathcal{B}} = \begin{bmatrix} C(f_1) & 0 & 0 & \cdots & 0 & 0 \\ 0 & C(f_2) & 0 & \cdots & 0 & 0 \\ 0 & 0 & C(f_3) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & C(f_{k-1}) & 0 \\ 0 & 0 & 0 & \cdots & 0 & C(f_k) \end{bmatrix}$$

*and $f_i \mid f_{i+1}$ for $1 \le i < k$. The integer $k$ and the polynomials $f_i$ are uniquely determined by $T$.*

Let $R$ be a commutative ring with ideals $I$ and $J$ such that $I + J = R$ (they are said to be *relatively prime* or *comaximal*). Applying the Chinese Remainder Theorem yields that $R/IJ \approx R/I \oplus R/J$ as $R$-modules. For a sum of cyclic modules, one can use this isomorphism to obtain fewer terms (in case the hypotheses are satisfied for some pair of ideals that appear) or one can use it to obtain more terms if one can factor one of the ideals into a product of relatively prime ideals. We now push the latter idea to the limit:

If we take a decomposition and write $a_i = \prod_{j=1}^{t} p_j^{e_{ij}}$ where $p_j$, $1 \le j \le t$ are all the primes that appear in the $a_i$, then

$$\begin{aligned} M &= \bigoplus_{i=1}^{k} R/(a_i) \\ &= \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{t} R/(p_j^{e_{ij}}) \\ &= \bigoplus_{j=1}^{t} \bigoplus_{i=1}^{k} R/(p_j^{e_{ij}}) \; ; \end{aligned}$$

that is, if we write $M_p$ for the summand corresponding to a given prime $p$ we have

$$M = \bigoplus_{j=1}^{t} M_{p_j} \, .$$

The component $M_p$ is sometimes called the *primary* component of $M$ for the prime $p$.

**Definition 24.** A module is called *indecomposable* if it cannot be written as the internal direct sum of two non-zero submodules.

**Lemma 25.** *Let $R$ be a PID. Then $R$ and $R/(p^n)$ for $p$ a prime and $n \ge 1$ are the only cyclic indecomposable $R$-modules.*

*Proof.* The easy proof is left as an exercise. □

This lemma asserts then that no further decomposition of our module is possible.

**Definition 26.** The $p_j^{e_{ij}}$ that appear in the decomposition are called the *elementary divisors* of $T$.

We now study a single cyclic module $R/(p^e)$ for $p \in F[x]$ a monic prime. Let's first consider the case where $p = x$. Then the minimal polynomial being $x^e$ just means that the linear transformation $S$ (= "multiplication by $x$") is nilpotent on the vector space $F[x]/(x^e)$. The companion matrix is just the $e \times e$ matrix with 1 in all positions just below the main diagonal:

$$C(x^e) = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}.$$

You may recall that you obtained this matrix for a nilpotent linear transformation in one of your early exercises.

We now look at another special case, $p = x - c$. However, we apply the preceding result to the transformation $S - cI$ which is nilpotent and has matrix $C(x^e)$. Hence $S$ has matrix $cI + C(x^e)$ using the same basis as in the previous case:

$$\begin{aligned} J_e(c) &= cI + C(x^e) \\ &= \begin{bmatrix} c & 0 & 0 & \cdots & 0 & 0 \\ 1 & c & 0 & \cdots & 0 & 0 \\ 0 & 1 & c & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c & 0 \\ 0 & 0 & 0 & \cdots & 1 & c \end{bmatrix}. \end{aligned}$$

We call the square matrix $J_e(c)$ a *basic Jordan block* of size $e$.

For a given primary component $M_c$ (note name change), corresponding to the prime $p = x - c$, we can order the terms by non-increasing exponents:

$$M_c = F[x]/((x-c)^{\ell_1}) \oplus F[x]/((x-c)^{\ell_2}) \oplus \cdots \oplus F[x]/((x-c)^{\ell_s})$$

with $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_s$.

Then the linear transformation $S$ ("multiplication by $x$") on $M_c$ has matrix

$$J(c) = \begin{bmatrix} J_{\ell_1}(c) & 0 & 0 & \cdots & 0 & 0 \\ 0 & J_{\ell_2}(c) & 0 & \cdots & 0 & 0 \\ 0 & 0 & J_{\ell_3}(c) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & J_{\ell_{s-1}}(c) & 0 \\ 0 & 0 & 0 & \cdots & 0 & J_{\ell_s}(c) \end{bmatrix}.$$

Finally we obtain

**Corollary 27** (Jordan Normal Form). *Let $V$ be a finite dimensional vector space over the field $F$ and let $T \in \mathrm{End}_F(V) = \mathrm{Hom}_F(V,V)$. Assume that the minimal polynomial $f$ of $T$ is a product of linear polynomials. Let the factorization be $f = (x-c_1)^{n_1}(x-c_2)^{n_2}\cdots(x-c_k)^{n_k}$ with $c_i$ distinct and $n_i > 0$. Then*

*a. There exist unique $T$-invariant subspaces $V_i$ such that $V = \bigoplus_{i=1}^k V_i$ with the minimal polynomial of $T$ restricted to $V_i$ being $(x-c_i)^{n_i}$;*

*b. There exists a basis for $V$ so that the matrix for $T$ with respect to this basis has the form*

$$\begin{bmatrix} J(c_1) & 0 & 0 & \cdots & 0 & 0 \\ 0 & J(c_2) & 0 & \cdots & 0 & 0 \\ 0 & 0 & J(c_3) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & J(c_{k-1}) & 0 \\ 0 & 0 & 0 & \cdots & 0 & J(c_k) \end{bmatrix}.$$

*The matrix is unique up to the order in which the Jordan blocks occur on the diagonal.*

*Proof.* Although the first statement follows from our earlier discussion, a version exists for any factorization of the minimal polynomial into pairwise relatively prime factors. See the even more general version for finitely generated torsion modules over a PID in the exercises at the end.

The second part is immediate from the earlier discussion. □

Throughout the discussion, we've avoided proving the various uniqueness statements. See the exercises below for a proof in a sequence of steps.

# Exercises

**ModulesPID 1.** A module is called *indecomposable* if it cannot be written as the internal direct sum of two non-zero submodules.

a. Show that if $R$ is a commutative domain, then $R$ is an indecomposable $R$-module.

b. Show that the only indecomposable modules cyclic modules over a PID are $R$ and $R/(p^n)$ for $p$ a prime and $n \geq 1$ an integer.

c. Show that $\mathbb{Q}$ is a $\mathbb{Z}$-module which is indecomposable but not finitely generated.

d. Let $R$ be a commutative domain that is not a field. Let $F$ be its field of fractions. Show that $F$ is an indecomposable $R$-module which is not finitely generated.

**ModulesPID 2.** A module $M$ is called *simple* if it is non-zero and the only proper submodules are $0$ and $M$.

a. Show that if $R$ is a commutative ring (with $1$) and $I$ is a maximal ideal, then $R/I$ is a simple $R$-module. Conversely, show that every simple module is isomorphic to such a cyclic module.

b. If $R$ is a PID, show that any simple module is isomorphic to $R/(p)$ for some prime $p$.

**ModulesPID 3.** Let $R$ be a PID. Let $m = (r_1, \ldots, r_n) \in R^n$ and assume that $\gcd(r_1, \ldots, r_n) = 1$. Show that there exists a basis for $R^n$ which contains this element. First observe that this is equivalent to finding a matrix $A \in R^{n \times n}$ with $m$ as its first row (or column). Argue by induction on $n$. The case $n = 1$ is trivial, and for the case $n = 2$ use the $2 \times 2$ matrix on the second page. In general reduce to a smaller size matrix using an argument similar to that used in the first step of constructing the Smith Normal Form.

**ModulesPID 4.** Let $R$ be a PID and let $T : R^n \longrightarrow R$ be a homomorphism. One then obtains a short exact sequence

$$0 \longrightarrow \ker T \longrightarrow R^n \longrightarrow \operatorname{im} T \longrightarrow 0 .$$

Show that this seqence splits: that $R^n = \ker T \oplus Rx$ for $x \in R^n$ for which $T(x) = d$, $(d) = \operatorname{im} T$. And further $\ker T$ is a free module of rank $n-1$. [Apply the preceding exercise.]

**ModulesPID 5.** Let $M$ be a finitely generated torsion-free module over a commutative domain $R$. Let $S$ be $R$ with $0$ removed. Let $F$ be the field of fractions of $R$.

a. This part generalizes the construction of the field of fractions. Define an equivalence relation on $M \times S$ by $(m,s) \sim (n,t)$ if $tm = sn$. Show that this is an equivalence relation and let $m/s$ be the equivalence class of $(m,s)$. Let $\mathrm{Frac}(M) = \{ m/s \mid m \in M,\ s \in S \}$.

b. Define addition and scalar multiplication by elements of $F$ and show that $\mathrm{Frac}(M)$ is a finite dimensional vector space over $F$.

c. Show that $\theta(m) = m/1$ gives an injective homomorphism $\theta : M \longrightarrow \mathrm{Frac}(M)$.

d. Choose a basis for $\mathrm{Frac}(M)$ over $F$ and a corresponding isomorphism $\mathrm{Frac}(M) \approx F^m$. Now $R^m \subseteq F^m$ in a natural way. Let $\gamma$ be the composition of $\theta$ with this isomorphism. Let $m_i$, $1 \le i \le n$ be a finite set of generators of $M$ over $R$. Write $\gamma(m_i) \in F^m$ as $(a_1(i)/b_1(i), \ldots, a_m(i)/b_m(i))$. Let $b$ be the least common multiple of the denominators $b_j(i)$. Then $M \approx bM \approx \gamma(bM) \subseteq R^m$.

e. Assume now that $R$ is a PID. Apply the result of the preceding problem to conclude that $M$ is a free module.

**ModulesPID 6.** Let $R$ be a commutative ring. Let $I \subseteq R$ be an ideal. If $I \neq 0$ is free as an $R$-module, show that $I$ is a principal ideal.

**ModulesPID 7.** a. Show that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module. Show that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

b. Let $R$ be a commutative domain that is not a field. Let $F$ be its field of fractions. Show that $F$ is not a finitely generated $R$-module. Show that $F$ is not a free $R$-module.

**ModulesPID 8.** Let $R$ be a principal ideal domain (PID). Let $m,n$ be positive integers and let $A \in R^{m\times n}$, the set of $m \times n$ matrices with entries in $R$. Define $\ell(A)$ to be the ideal of $R$ generated by the entries of $A$ (that is, the set of all $R$-linear combinations of the entries $a_{ij}$ of $A$).

a. If $B \in R^{p\times m}$, show that $\ell(BA) \subseteq \ell(B) \cap \ell(A)$. Similarly if $C \in R^{n\times q}$, $\ell(AC) \subseteq \ell(A) \cap \ell(C)$.

b. In case $P \in R^{m\times m}$ and $Q \in R^{n \times n}$ have inverses, conclude that $\ell(PAQ) = \ell(A)$. That is, $\ell(B)$ gives the same value for any matrix $B$ which is equivalent to $A$.

c. A matrix $A \in R^{m\times n}$ is said to be in *Smith Normal Form* if the only non-zero entries of $A$ are on the diagonal, say $a_1, \ldots, a_k$ with $a_i \mid a_{i+1}$ for $1 \le i < k$. Compute $\ell(A)$ for $A$ in Smith Normal Form (SNF).

d. If $b_1, b_2 \in R$ are arbitrary non-zero elements, let $A$ be the matrix

$$\begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix}.$$

Using row and column operations (as described earlier), put this matrix in Smith Normal Form

$$\begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} .$$

(You should be able to do this with 3 operations.) Describe $a_1$ and $a_2$ in terms of $b_1$ and $b_2$. Show that $b_1 b_2 = a_1 a_2$. Do not use determinants.

e. Let $b_1, \ldots, b_k$ be arbitrary non-zero elements of $R$ and let $A$ be the $k \times k$ matrix with these as its diagonal entries. Indicate how by repeatedly applying the previous part, the SNF of $A$ can be determined. Note that each step of your procedure should always give a diagonal matrix with the same product (i.e., the determinant) of diagonal entries. What is $a_1$? What is $a_n$? Give a formula for $a_i$ in terms of the prime factorizations of the $b_i$. [Hint: Phrase correctly and this will be easy!]

Remark: The following theorem can be proven:
If $R$ is a PID and $A \in R^{m \times n}$ is non-zero, there exists a unique matrix $B$ in SNF which is equivalent to $A$. (As usual for statements about a PID, we ignore multiplication by units.)

**ModulesPID 9.** Let $T \in \mathrm{End}_F(V) = \mathrm{Hom}_F(V, V)$ for $V$ a finite dimensional vector space over $F$.

a. Give a formula for the last invariant factor of $T$ in terms of the elementary divisors of $T$. This should be a very nice description.

b. Determine all of the invariant factors of $T$ in terms of the elementary divisors of $T$. Give a formula for the number of invariant factors in terms of the elementary divisors.

c. Determine the elementary divisors in terms of the invariant factors. Give a formula for the total number in the list as an easy to describe sum over the invariant factors.

**ModulesPID 10.** Let $R$ be a commutative ring and let $M$ be an $R$-module. An element $m \in M$ is called a *torsion* element if there exists a non-zero element $r \in R$ such that $rm = 0$. Let $\mathrm{tor}(M)$ denote the set of torsion elements in $M$. Assume now and for the rest of the problem, that $R$ is a domain (i.e., if $ab = 0$ for elements $a, b \in R$, then either $a = 0$ or $b = 0$).

a. Show that $\mathrm{tor}(M)$ is a submodule of $M$ (i.e., is non-empty and closed under addition and scalar multiplication by arbitrary elements of $R$).

b. For $M_1$ and $M_2$ $R$-modules, determine $\mathrm{tor}(M_1 \oplus M_2)$.

c. If $N_1 \subseteq M_1$ is a submodule and $N_2 \subseteq M_2$ is a submodule, give an explicit isomorphim $(M_1 \oplus M_2)/(N_1 \oplus N_2) \longrightarrow M_1/N_1 \oplus M_2/N_2$ with details of proof. Compute $(M_1 \oplus M_2)/\,\mathrm{tor}(M_1 \oplus M_2)$.

d. Let $M = R^m$, the direct sum of $m$ copies of $R$. What is $\operatorname{tor}(M)$?

e. Consider the quotient module $M/\operatorname{tor}(M)$. Show that it contains no non-zero torsion elements.

f. If $R$ is a commutative ring and $a \in R$ is non-zero, compute $\operatorname{tor}(R/(a))$.

**ModulesPID 11.** Give an example of a ring $R$ and module $M$ with $\operatorname{tor}(M)$ not a submodule.

**ModulesPID 12.** Let $M$ be a finitely generated torsion module over a PID $R$. Let $\operatorname{Ann}(M) = \{ r \in R \mid rm = 0 \, \forall m \in M \}$ be the annihilator of $M$.

a. Show that $\operatorname{Ann}(M)$ is a non-zero ideal of $R$.

b. If $(r) = \operatorname{Ann}(M)$ and $r = ab$ for $\gcd(a,b) = 1$, show that $M = M_a \oplus M_b$ for $M_s = \{ m \in M \mid sm = 0 \}$.

c. Let $p \in R$ be a prime. By abuse of notation, we write

$$M_p = \left\{ m \in M \;\middle|\; p^k m = 0 \text{ for some } k > 0 \right\} .$$

Show that $M = \bigoplus_p M_p$ gives a unique decomposition into a finite sum where each component $M_p$ is annihilated by some (finite) power of the prime $p$.

**ModulesPID 13.** Let $R$ be a PID and $M$ a finitely generated $R$-module with $\operatorname{Ann}(M) = (p^n)$ (such as one of the components in the last part of the preceding exercise). Let $F = R/(p)$, a field.

a. For each $i$, $0 \le i < n$, show that $p^i M = \left\{ p^i m \;\middle|\; m \in M \right\}$ is a submodule of $M$ with $p^{i+1}M \subset p^i M$. Show that $p^i M / p^{i+1} M$ is a vector space over the field $F$.

b. Show the the number of cyclic summands of $M$ is uniquely determined by $M$ and equal to $\dim_F M/pM$.

c. Give a formula for the number of summands in $M$ which are of the form $R/(p^j)$ for a fixed $j \ge 1$. The formula should involve the numbers $\dim_F p^i M / p^{i+1} M$. Conclude that the number of such terms is uniquely determined by $M$.

d. Show that if $N \approx M$, then the integers determined above for $M$ are equal to the ones for $N$ obtained by the same procedure.

**ModulesPID 14.** Let $R$ be a commutative ring with $1$. Let $M$ be a finitely generated free $R$-module, say $M \approx R^n$. Let $I \subsetneq R$ be a maximal ideal and let $F = R/I$, a field.

a. Let $IM$ be the set of all finite sums of elements of the form $im$ for $i \in I$ and $m \in M$. This is a submodule of $M$. Show that $M/IM$ is a finite dimensional vector space over the field $F$. How is $\dim_F M/IM$ related to the integer $n$? Prove your statement. Conclude that $n$ only depends on $M$, and not on the basis.

b. If $J$ were a different maximal ideal, let $K = R/J$. How are $\dim_F M/IM$ and $\dim_K M/JM$ related?

**ModulesPID 15.** Let $F$ be a field and let $f \in F[x]$ be a monic polynomial not equal to 1: $f = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$. Then $M = F[x]/(f)$ is an $F[x]$-module and a finite dimensional vector space over $F$. For $g \in F[x]$ write $\overline{g}$ for the image of $g$ in $M$ under the natural surjection $F[x] \longrightarrow M$. Let $\mathcal{B} = \left\{\overline{1}, \overline{x}, \overline{x^2}, \ldots, \overline{x^{n-1}}\right\}$. Prove the $\mathcal{B}$ is an ordered basis of $M$. Let $S : M \longrightarrow M$ be the linear transformation given by $S(\overline{g}) = \overline{x}\,\overline{g}$. Compute the matrix of $S$ with respect to $\mathcal{B}$. This matrix, $C(f)$, is called the *companion matrix* of the polynomial $f$. Prove that $f$ is the minimal polynomial of $S$, and of $C(f)$.

**ModulesPID 16.** a. Let $F$ be a field and let $R = F[x]$. Consider the exact sequence

$$R^2 \xrightarrow{S} R^2 \longrightarrow M \longrightarrow 0$$

where $S$ is given by left multiplication by the diagonal matrix $A$

$$\begin{bmatrix} x-a & 0 \\ 0 & x-b \end{bmatrix}.$$

where $a \neq b$ are different elements of $F$. Then

$$\begin{aligned} M &\approx \operatorname{coker} S \\ &\approx (R \oplus R)/((x-a),(x-b)) \\ &\approx R/(x-a) \oplus R/(x-b) \end{aligned}$$

as $R$-modules and

$$\approx F \oplus F$$

as a vector space over $F$. As an $F[x]$ module, $x$ acts as multiplication by $a$ on the first factor and multiplication by $b$ on the second factor (i.e., $M$ is the sum of two cyclic modules). The Chinese Remainder Theorem shows that in fact $M$ is a cyclic module. Verify this two differet ways:

(1) Apply the preceding problem to the matrix $A$ and argue as above;

(2) Apply the Chinese Remainder theorem directly.

In both cases give an $F$-basis for the two-dimensional vector space $M$ and give the matrix of the linear transformation "multiplication by $x$" on $M$.

b. If $M = R/(f_1) \oplus F/(f_2)$ is the direct sum of two arbitrary non-zero cyclic $R$-modules, explicitly give

(1) $M$ as a direct sum of two cyclic $R$-modules $R/(a_1) \oplus R/(a_2)$ with $a_1 \mid a_2$;

(2) take the union of an $F$-basis for $R/(a_1)$ and one for $R/(a_2)$ and give the matrix for the linear transformation "multiplication by $x$" with respect to this basis.

**ModulesPID 17.** A module $M$ is called *noetherian* if for any sequence of submodules $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots \subseteq M_\ell \subseteq \cdots$ there exists an integer $n_0$ such that $M_j = M_{n_0}$ for all $j \geq n_0$.

A module $M$ satisfies the *maximum condition* if every non-empty collection of submodules contains a maximal element. A submodule $N$ in the collection is *maximal* if no other module in the collection contains it strictly.

Prove that for a module $M$ the following three statements are equivalent:

(1) $M$ is noetherian;

(2) $M$ satisfies the maximum condition;

(3) Every submodule of $M$ is finitely generated.

To prove (1) implies (2) try to construct an ascending sequence of submodules. For (2) implies (3), consider the collection of finitely generated submodules of $M$. For (3) implies (1) consider the generators of the union of the ascending chain of submodules.

**ModulesPID 18.** A ring $R$ is called *noetherian* if $R$ considered as a module is noetherian. Show the if $R$ is noetherian, then so is $R^n$ for all $n \geq 1$. Given an induction argument using the surjective projection map $\pi_n : R^n \longrightarrow R$ on the last coordinate.

**ModulesPID 19.** Let

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be a short exact sequence of $R$-modules. Show that $M_2$ is noetherian if and only if $M_1$ and $M_3$ are noetherian.

**ModulesPID 20.** Show that a finite direct sum of noetherian modules is noetherian.

**ModulesPID 21.** Show that a module over a noetherian ring is noetherian if and only if it is finitely generated.

**ModulesPID 22.** Let $M$ be a finitely generated noetherian module. Then $M$ is a direct sum of a finite number of indecomposable modules. Argue as follows: Unless $M$ is indecomposable, it must be possible to write it as $M = M_1 \oplus M_2$ for some non-zero indecomposable submodule $M_1$, with $M_2$ not $0$. For if not, one can construct an infinite strictly increasing ascending chain of submodules. Next consider the collection of all submodules $N$ of $M$ with $M = N \oplus N'$ and $N$ a finite sum of indecomposables. Pick a maximal element and argue that it must equal $M$.

**ModulesPID 23.** Let $M$ be a finitely generated torsion-free module over a commutative domain $R$. Let $I$ be a maximal ideal of $R$, and let $F = R/I$.

a. Show that $M/IM$ is a finite dimensional vector space over the field $F$. Give an example to show that it is not necessarily true that $M$ is a free module.

b. If $J$ were a different maximal ideal, let $K = R/J$. How are $\dim_F M/IM$ and $\dim_K M/JM$ related? Give an example to show that these numbers need not be equal.

**ModulesPID 24.** Let $V$ be a finite dimensional vector space with proper subspace $W$ (i.e., $W \neq 0, V$). Let $T : V \longrightarrow V$ be a linear transformation having $W$ as an invariant subspace. Let $h$ be the minimal polynomial of $T$, $h_1$ the minimal polynomial of $T$ restricted to $W$, and $h_2$ the minimal polynomial of the linear transformation $T$ induces on the quotient $V/W$.

a. Show that $h_1 | h$ and $h_2 | h$.

b. Show $h | h_1 h_2$.

c. If $h_1$ and $h_2$ are relatively prime, show that $h = h_1 h_2$.

d. Give an example to show that the result of the previous part is false if $h_1$ and $h_2$ are not relatively prime.

**ModulesPID 25.** Let $T : V \longrightarrow V$ be a linear transformation on the finite dimensional vector space over the field $F$. An element $c \in F$ is called a *characteristic value* (*eigenvalue*) of $T$ if there exists a non-zero vector $v \in V$ such that $T(v) = cv$. The vector $v$ is called a *characteristic vector* (*eigenvector*) associated to $c$.

a. If $c_1, \ldots, c_k$ are distinct characteristic values of $T$ with associated characteristic vectors $v_i$, show that the set $\{v_1, \ldots, v_k\}$ is a linearly independent set.

b. Let $V_i = \ker(c_i I - T)$. Show that $V_1 + \cdots + V_k$ is a direct sum. The subspace $V_i$ is called the *characteristic subspace* associated to the characteristic value $c_i$.

c. If $\dim V = n$ and $T$ has $n$ distinct characteristic values, show that there exists a basis $\mathcal{B}$ for $V$ such that $[T]_{\mathcal{B}}$ is diagonal.

**ModulesPID 26.** Let $M = \{ f(x) \in \mathbb{Q}[x] \mid f(n) \in \mathbb{Z} \text{ for all } n \in \mathbb{Z} \}$ (i.e., the polynomials with rational coefficients which take on integral values at all the integers). Show that $M$ is a free module (of infinite rank) over $\mathbb{Z}$ by proving that the set of binomial coefficient polynomials $\{ \binom{x}{k} \mid k \geq 0 \}$ is a basis for $M$.