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

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

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.

Remark 3. In the preceding examples 2 (when $m = n$), 3, 5, and 6 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 section 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 $T \in \text{End}_F(V) = \text{Hom}_F(V, V)$ 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 $f(T) \in \text{End}_F(V)$ is given by evaluation (discussed earlier). Explicitly, if $f = a_0 + a_1 x + \cdots + a_n x^n$, then $f(T) = a_0 I + a_1 T + \cdots a_n T^n$.

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 5).

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 section 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 section 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 is not always true.

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. Define addition and scalar multilication 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 6).

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 7).

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 section 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

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

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 section 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 $f(x) = x + I$ 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.

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 8).

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 that 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-homomprhisms going to or from a direct sum of two R-modules.

Verify these statements (see Exercise 9).

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 10).

We now give a simple example. See Exercise 4 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 $r_1m_1 + \cdots + r_km_k = 0$. 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 ideal which are not 0 (see Exercise 11).

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 bases for the two free modules, one obtains a

matrix for f with respect to the pair of bases exactly as in the case of vector spaces. If one chooses a different pair of 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 δ_x is defined as earlier

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

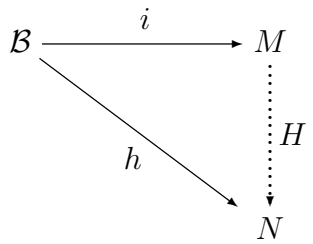
is a basis. We then have for $f \in R^{(X)}$ the formula

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

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:



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

As usual this yields a one-to-one correspondence

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

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 16. An alternate proof for the finitely generated case using the theory of determinants appears in Exercise 17.

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 18.

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

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 are called *I-torsion*.

Modules 3. Let R be a PID which is not a field. Let $a \in R$. Determine precisely when $R/(a)$ will be a field.

Modules 4 (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 5. Verify that the vector space V is an $F[x]$-module under the definition of scalar multiplication given in Example 6.

Modules 6. State and prove the Universal Mapping Property for quotient modules.

Modules 7. Prove the First Isomorphism Theorem for Modules (Theorem 9).

Modules 8. a. State and prove the Universal Mapping Property for quotient rings.

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

Modules 9. 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 10. 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 11. 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 ρ_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 12. 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 13. 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 14. Let $R = \mathbb{Z}[x]$. Show that there exist ideals in R which are not principal.

Modules 15. 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 $\mathbf{Z}$ 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 16. 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 17. 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 18. 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 $R = \mathrm{Hom}_F(V, V_1 \oplus V_2) \approx \mathrm{Hom}_F(V, V_1) \oplus \mathrm{Hom}_F(V, V_2)$ 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 17). 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 19. 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 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 $(M_1 \oplus M_2)/\mathrm{tor}(M_1 \oplus M_2)$.

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

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

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

Modules 20. 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 always holds for finite m and n if R is a commutative integral domain.

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 21. Let R be an artibrary 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 $n \times n$ 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. 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 22. 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 θ 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^o (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 23. 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.

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

and

Yuri Berest.

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.