Linear Algebra

Jim Coykendall

September 13, 2004

Chapter 1

Preliminaries

1.1 Basics and Definitions

This course will cover basic graduate linear algebra. In this course we will have a view towards some algebraic $K-$theory (which in very loose terms can be thought of as linear algebra over a ring). The beginning of the course will be a quick overview of some of the basics of linear algebra (over a field). Included will be inner product spaces and some applications. We will then delve a bit into general module theory and then specialize again to modules over a PID to get the canoncial forms of a matrix. We will end up with some basic category theory (on a "need to know" basis) and introduce algebraic $K-$theory.

In this section we will (for completeness) record some definitions and rehash some things that we will need to know in this course.

Definition 1.1.1. *A nonempty set G is said to be a group if G is equipped with a binary operation $G \times G \longrightarrow G$ $(\circ)$ such that the following hold.*

a) $x \circ (y \circ z) = (x \circ y) \circ z$ *for all* $x, y, z \in G$.

b) There exists $e \in G$ *such that* $e \circ x = x \circ e = x$ *for all* $x \in G$.

c) For all $x \in G$ *there exists* $y \in G$ *such that* $x \circ y = y \circ x = e$.

We note that in many instances, our groups will be *abellian*. That is, $x \circ y = y \circ x$ for all $x, y \in G$ (and in this case we will often write "$x + y$" for "$x \circ y$").

Definition 1.1.2. *A nonempty set R is said to be a ring if R is equipped with two binary operations ($+$ and $\circ$) such that the following hold.*

a) $(R, +)$ *is an abelian group.*

b) $x \circ (y \circ z) = (x \circ y) \circ z$ *for all* $x, y, z \in R$.

c) $x \circ (y + z) = x \circ y + x \circ z$ *and* $(x + y) \circ z = x \circ z + y \circ z$ *for all* $x, y, z \in R$.

Notationally, we will omit the $\circ$ notation for a ring and just write "xy" instead of $x \circ y$. Additionally, we will (almost always) assume that our ring is *commutative*, that is $xy = yx$ for all $x, y \in R$. Even more frequently, we will assume that our ring has an identity (that is, an element $1_R \in R$ such that $1_R x = x 1_R = x$ for all $x \in R$).

Definition 1.1.3. *We say that a ring, D, with identity is a division ring if the nonzero elements of D form a group under multiplication. If D is a commutative division ring, we say that D is a field.*

Here is an important result (hand in hand with the axiom of choice) that will be used from time to time.

Lemma 1.1.4 (Zorn's Lemma). *Let Γ be a partially ordered set with the property that every chain in Γ has an upper bound (in Γ). Then Γ has a maximal element.*

Just for giggles, here is an application of Zorn's Lemma

Theorem 1.1.5. *Let R be a ring with identity. Then R has a maximal (left) ideal. What is more, any ideal I is contained in a maximal ideal $\mathfrak{M}$.*

Proof. Let $I \subsetneq R$ be our (left) ideal (if you merely want existence of a maximal ideal you can take $I = (0)$). Let $\Gamma = \{J | J \text{ is a proper (left) ideal of } R \text{ containing } I\}$ with the partial ordering being set-theoretic containment. Note that *Gamma* is nonempty as $I \in \Gamma$.

To apply Zorn's Lemma, we need to verify that every chain in Γ has an upper bound in Γ. Let $C = \{I_j\}$ be a chain (that is, a linearly ordered subset of Γ). We claim that $U := \bigcup I_j$ is an upper bound for C (more precisely, the fact that it is an upper bound is clear...we merely have to show that $U \in \Gamma$).

To this end, we first claim that U is an (left) ideal of R. Indeed, if $x, y \in U$ then $x \in I_\alpha$ and $y \in I_\beta$. Since I_α and I_β are elements of C, then we will assume that $I_\alpha \subseteq I_\beta$ without loss of generality. Hence $x - y \in I_\beta \subseteq U$. Showing that $rx \in U$ is similar.

To see that U is proper, note that if it is not, then $1 \in U$ and hence $1 \in I_\alpha$ for some α. Hence I_α is not proper which is a contradiction.

Since U is an upper bound in Γ, Zorn's Lemma applies and hence Γ has a maximal element $\mathfrak{M}$. This element $\mathfrak{M}$ is a maximal ideal of R containing I and we are done. □

We will shortly use this technique to show that every vector space has a basis. But before we put the cart before the horse, here is what a vector space is.

Definition 1.1.6. *Let $\mathbb{F}$ be a field. A vector space over $\mathbb{F}$ is an abelian group $(V, +)$ equipped with a scalar multiplication (a map from $\mathbb{F} \times V \longrightarrow V$) such that for all $v, w \in V$ and $\alpha, \beta \in \mathbb{F}$*

a) $\alpha(v + w) = \alpha v + \alpha w$

b) $\alpha(\beta v) = (\alpha\beta)v$

c) $(\alpha + \beta)v = \alpha v + \beta v$

d) $1_{\mathbb{F}}v = v$.

Example 1.1.7. *Standard examples of vector spaces are* $\mathbb{R}^n$ *(over* $\mathbb{R}$*) and* $\mathbb{C}^n$ *(over* $\mathbb{R}$ *or* $\mathbb{C}$*). Other examples of real vector spaces are* $M_n(\mathbb{R})$ *and the real-valued functions on* (a, b) *(or continuous functions on* (a, b)*).*

Example 1.1.8. *The set of functions* $f : \mathbb{R} \longrightarrow \mathbb{R}$ *is a real vector space. Can you find a basis for this vector space?*

Chapter 2

Vector Spaces and Inner Product Spaces

2.1 The Basics of Vector Spaces

For completeness of this chapter, we recall the definition of a vector space.

Definition 2.1.1. *Let $\mathbb{F}$ be a field. A vector space over $\mathbb{F}$ is an abelian group $(V,+)$ equipped with a scalar multiplication (a map from $\mathbb{F} \times V \longrightarrow V$) such that for all $v, w \in V$ and $\alpha, \beta \in \mathbb{F}$*

a) $\alpha(v+w) = \alpha v + \alpha w$

b) $\alpha(\beta v) = (\alpha\beta)v$

c) $(\alpha+\beta)v = \alpha v + \beta v$

d) $1_{\mathbb{F}} v = v$.

Definition 2.1.2. *A subset $U \subseteq V$ of a vector space over $\mathbb{F}$ is said to be a subspace, if U is an $\mathbb{F}-$vector space.*

Definition 2.1.3. *Let V be a vector space over $\mathbb{F}$ and X a subset of V. We say the set X is linearly independent if the relation*

$$\sum_{i=1}^{n} \alpha_i x_i = 0$$

(with $\alpha_i \in \mathbb{F}$ and $x_i \in X$) implies that $\alpha_i = 0$ for all $1 \leq i \leq n$. If the set X is not linearly independent, we say that it is linearly dependent.

Definition 2.1.4. *Let V be a vector space over the field $\mathbb{F}$ and X a subset of V. We say that X spans V if every element of V can be written in the form*

$$\sum_{i=1}^{n} \alpha_i x_i$$

with $\alpha_i \in \mathbb{F}$ *and* $x_i \in X$.

We remark here that if $X \subseteq V$ is a subset of the vector space V, then the subspace spanned by X is precisely

$$U = \bigcap_{W \subseteq V, W \text{ subspace containing } X} W.$$

In particular, X spans V precisely when $U = V$.

Definition 2.1.5. *Let* V *be a vector space and* $X \subseteq V$ *a subset. We say that* X *is a basis of* V *if* X *is linearly independent and* X *spans* V.

Here is a big theorem that will help us to classify all vector spaces over an arbitrary field $\mathbb{F}$.

Theorem 2.1.6. *Any vector space,* V*, (over a division ring,* D*) has a basis. Additionally, any linarly independent subset of* V *can be expanded to a basis of* V.

Before we prove this theorem, we introduce the following lemma.

Lemma 2.1.7. *Let* V *be a vector space over a division ring* D*. Then* V *contains a maximal linearly independent subset (and more generally, any linearly independent subset is contained in a maximal linearly independent subset).*

Proof. This one has Zorn's Lemma written all over it. We first suppose that V is a nonzero vector space. Let v be a nonzero vector in V. As a set unto itself, $\{v\}$ is a linearly independent subset of V ($\alpha v = 0 \Longrightarrow \alpha = 0$). We let Γ be the set of all linearly independent subsets of V (partially ordered by inclusion). By the above remark, Γ is nonempty. We wish to apply Zorn's Lemma, so let $\mathfrak{C}$ be a chain in Γ. Consider the set

$$X = \bigcup_{B \subset \mathfrak{C}} B.$$

Certainly X is an upper bound for $\mathfrak{C}$ if X is actually in Γ (that is, if X is linearly independent). To this end, suppose that

$$\sum_{i=1}^{n} \alpha_i x_i = 0$$

with $\alpha_i \in D$ and $x_i \in X$. But each $x_i \in \mathfrak{C}$ and hence (since the list of x_i's is finite and $\mathfrak{C}$ is a chain) there is a B in the chain $\mathfrak{C}$ such that $x_i \in B$ for all $1 \leq i \leq n$. But as a member of the chain, B is a linearly independent set and hence $\alpha_i = 0$ for all $a \leq i \leq n$. Hence Zorn's Lemma applies and the proof

is complete. (To get the parenthetical part of the Lemma, consider Γ be the collection of linearly independent subsets of V that contain our given linearly independent set). □

We will now use this lemma to prove the previous theorem.

Proof. To prove the theorem, we will show that a maximal linearly independent subset of V is a basis. Let X be our maximal limearly independent subset of V (guaranteed by the previous lemma). To show that X is a basis of V, it suffices to show that X spans V.

Suppose that X does not span V, and choose $v \in V \setminus \langle X \rangle$. Since X is maximal with respect to being linearly independent, the set $X \bigcup \{v\}$ must be linearly dependent. Hence there exists $a, a_1, \cdots, a_n \in D$ and $v_1, \cdots, v_n \in X$ such that

$$av = a_1 v_1 + \cdots + a_n v_n.$$

Multiplying the left side by a^{-1} (note that $a \neq 0$) we obtain

$$v = a^{-1} a_1 v_1 + \cdots + a^{-1} a_n v_n \in \langle X \rangle$$

which is a contradiction.

□

Corollary 2.1.8. *If V is a vector space and L is a linearly independent subset of V, then L can be expanded to a basis of V.*

We end this section by defining the dimension of a vector space to be the cardinality of its basis set. Of course the basis set is not unique, but its cardinality is (we have not proved this, but I'll bet that you were betting on this). We will formally record the definition.

Definition 2.1.9. *Let V be a vector space over the field $\mathbb{F}$. We define $dim_{\mathbb{F}}(V) = |X|$ where X is a basis for V over $\mathbb{F}$.*

We will formally record the following theorem and leave it as an exercise for the reader (it is in fact an interesting exercise in set theory).

Theorem 2.1.10. *Let V be a vector space and let X and Y be bases for V. Then $|X| = |Y|$.*

2.2 Direct sums, quotients, and linear transformations

In this section we will look at an important construction called the direct sum which will allow us to build new vector spaces from old (externally) and additionally any vector space over a field can be decomposed uniquely (internally) in this fashion. We will also produce some standard results on quotient spaces

and linear transformations that are usually contained in an elementary linear algebra course to lay the groundwork for our later generalizations.

Proposition 2.2.1. *If U, V are subspaces of W then $U+V = \{u+v | u \in U, v \in V\}$ is a subspace of W.*

This is called the sum of the subspaces U and V. We next present a way to construct a special kind of a sum called a direct sum.

Proposition 2.2.2. *Let V and W be vector spaces over $\mathbb{F}$. The abelian group $V \oplus W$ is a vector space with scalar multiplication given by*

$$\alpha(v, w) = (\alpha v, \alpha w)$$

for all $v \in V$, $w \in W$ and $\alpha \in \mathbb{F}$.

Proof. Exercise. □

The difference between the sum and the direct sum is that there may be some "overlap" in a sum.

Example 2.2.3. *Consider the space $\mathbb{R}^3$ (as an $\mathbb{R}-$vector space). Let $U_1 = \langle (1,0,0), (0,1,0) \rangle$, $U_2 = \langle (0,0,1) \rangle$, $U_3 = \langle (1,0,0), (0,1,0) \rangle$, and $U_4 = \langle (0,1,0), (0,0,1) \rangle$. $\mathbb{R}^3 = U_1 \oplus U_2$ and $\mathbb{R}^3 = U_3 + U_4$ but $\mathbb{R}^3 \neq U_3 \oplus U_4$.*

We now define the direct sum more generally.

Proposition 2.2.4. *Let $\{V_i\}_{i \in I}$ be a collection of vector spaces over a field $\mathbb{F}$. Then the abelian group $\oplus_{i \in I} V_i$ is a a vector space with scalar multiplication given by $\alpha\{v_i\}_{i \in I} = \{\alpha v_i\}_{i \in I}$.*

Proof. Exercise. □

A natural question is when is a vector space a direct sum of two of its subspaces? But before we answer this we need some more technical details.

Proposition 2.2.5. *Let $W \subseteq V$ be vector spaces over $\mathbb{F}$. Then the abelian group V/W is a vector space with scalar multiplication given by $\alpha(v + W) = \alpha v + W$.*

Definition 2.2.6. *Let V and W be vector spaces over $\mathbb{F}$. A function $\phi : V \longrightarrow W$ is called a linear transformation if*

a) $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$ for all $v_1, v_2 \in V$ and

b) $\phi(\alpha v) = \alpha \phi(v)$ for all $v \in V$ and $\alpha \in \mathbb{F}$.

A linear transformation is the vector space analog of an abelian group homomorphism. We say that a linear tranformation is surjective (onto) if it is surjective as a map of sets. We say that a linear transformation is injective (1-1) if it is injective as a map of sets. A linear transformation that is both one to one and onto is called an isomorphism.

Definition 2.2.7. *Let $\phi : V \longrightarrow W$ be a linear tranformation. Then $ker(\phi) = \{v \in V | \phi(v) = 0\}$ and $im(\phi) = \{\phi(v) | v \in V\}$.*

Recall that ϕ is one to one if and only if $\ker(\phi) = 0$ and ϕ is onto if and only if $\text{im}(\phi) = W$.

Theorem 2.2.8. *Let $\{U_i\}_{i \in I}$ be subspaces of W. Then $W \cong \oplus_{i \in I} U_i$ if and only if $W = \sum_{i \in I} U_i$ and $U_i \bigcap (\sum_{i \neq j} U_j) = 0$ for all $i \neq j$.*

Before we prove this, we remark that the general sum $\sum_{i \in I} U_i$ consists of all finite sums $u_1 + u_2 + \cdots + u_n$ where $u_k \in U_{i_k}$.

Proof. We will prove the direction ($\Longleftarrow$) and leave the other direction for the energetic reader. Suppose that W is the sum of the subspaces U_i and that $U_i \bigcap U_j = 0$ for all $i \neq j$. Consider the map

$$\phi : \oplus_{i \in I} U_i \longrightarrow W$$

given by $\phi(\{u_i\}) = \sum u_i$ (note that only finitely many of the terms in this sequence are nonzero). Since W is the sum of all of the U_i's, this map is onto. Now suppose that $\{u_i\}_{i \in I} \in \ker(\phi)$. Since only finitely many of the u_i's are nonzero (say $x_{i_1}, x_{i_2}, \cdots, x_{i_k}$ are the nonzero entries), this means that

$$x_{i_1} + x_{i_2} + \cdots + x_{i_k} = 0.$$

Note that we can assume that $k \geq 2$ (otherwise we are done). This equation implies that

$$x_{i_1} = -x_{i_2} - \cdots - x_{i_k} \in U_{i_1} \bigcap (\sum_{j \neq i_1} U_j)$$

and hence, by assumption, $x_{i_1} = 0$ which is a contradiction. This concludes the proof.

□

Here is a (truly wonderful) related result. This result classifies all vector spaces over a field $\mathbb{F}$.

Theorem 2.2.9. *Let V be a vector space over $\mathbb{F}$. Then $V \cong \oplus_{i \in I} \mathbb{F}$. What is more the cardinality of I coincides with the cardinality of (any) basis of V over $\mathbb{F}$.*

Proof. Let $X = \{x_i\}_{i \in I}$ be a basis for V over $\mathbb{F}$. We define a map $\phi : V \longrightarrow \oplus_{i \in I} \mathbb{F}$ by $\phi(\sum \alpha_i x_i) = \{\alpha_i\}_{i \in I}$. Verify that this is a linear transformation, and is both one to one and onto. □

We conclude this section with a hodge-podge of "familiar" linear algebra results.

Proposition 2.2.10. *Let V, W be vector spaces over $\mathbb{F}$ and $\phi : V \longrightarrow W$ a linear transformation. Then ϕ induces an isomorphism $\overline{\phi} : V/ker(\phi) \cong im(\phi)$.*

Proof. Consider the map $\overline{\phi} : V/\ker(\phi) \longrightarrow \text{im}(\phi)$ given by $\overline{\phi}(v + \ker(\phi)) = \phi(v)$. To see that $\overline{\phi}$ is well defined, assume that $v + \ker(\phi) = w + \ker(\phi)$. This means that $v - w \in \ker(\phi)$ and hence $\phi(v) = \phi(w)$ and so the map is well defined. It should also be noted that it is straightforward that $\overline{\phi}$ is onto.

To see that $\overline{\phi}$ is one to one, note that $\overline{\phi}(v + \ker\phi) = 0$ implies that $\phi(v) = 0$ and hence that $v \in \ker(\phi)$. So $\overline{\phi}$ is one to one. □

Corollary 2.2.11. *Let $\phi : V \longrightarrow W$ be a linear transformation. Then $dim(V) = dim(ker(\phi)) + dim(im(\phi))$.*

Proof. Exercise. □

Proposition 2.2.12. *Let V and W be finite deimensional vector spaces over $\mathbb{F}$ with bases $\{v_1, v_2, \cdots, v_n\}$ and $\{w_1, w_2, \cdots, w_m\}$ respectively. If $\phi : V \longrightarrow W$ is a linear transformation then ϕ can be represented as an element of $M_{m,n}(\mathbb{F})$.*

Proof. The important thing here is that ϕ is determined completely by its action on the basis elements of V. We have the following system of equations:

$$\begin{aligned}
\phi(v_1) &= \alpha_{1,1}w_1 + \alpha_{2,1}w_2 + \cdots + \alpha_{m,1}w_m \\
\phi(v_2) &= \alpha_{1,2}w_1 + \alpha_{2,2}w_2 + \cdots + \alpha_{m,2}w_m \\
&\vdots \\
\phi(v_n) &= \alpha_{1,n}w_1 + \alpha_{2,n}w_2 + \cdots + \alpha_{m,n}w_m
\end{aligned}$$

With this data in hand, it is a straightforward computations to see that the $m \times n$ matrix $\{\alpha_{i,j}\}$ $1 \leq i \leq n$, $1 \leq j \leq m$ is the matrix that we seek. □

We note here that the set of linear transformations from V to W forms a vector space (over the same field, $\mathbb{F}$). We will call this vector space $\text{Hom}_{\mathbb{F}}(V, W)$.

Chapter 3

Inner Product Spaces

In this (brief) chapter we will look at the notion of an inner product space. In this chapter we will assume that the fields in question are either the real numbers, $\mathbb{R}$ or the complex numbers $\mathbb{C}$.

3.1 The basics

Definition 3.1.1. *Let V be a vector space over $\mathbb{F}$ ($= \mathbb{R}$ or $\mathbb{C}$). We say that V is an inner product space if there exists a map $\langle \cdot \rangle : V \times V \longrightarrow \mathbb{F}$ such that for all $u, v, w \in V$ and $\alpha, \beta \in \mathbb{F}$ we have*

a) $\langle u, v \rangle = \overline{\langle v, u \rangle}$

b) $\langle u, u \rangle \geq 0$ *and* $\langle u, u \rangle = 0$ *if and only if* $u = 0$

c) $\langle \alpha u + \beta v, w \rangle = \alpha \langle u, w \rangle + \beta \langle v, w \rangle$.

Note that as a consequence, we have that for all $\lambda \in \mathbb{F}$, $\langle u, \lambda v \rangle = \overline{\lambda} \langle u, v \rangle$.

Example 3.1.2. *Consider the standard "dot product" for $\mathbb{R}^n$.*

Example 3.1.3. *Let $V = \{f : [0,1] \longrightarrow \mathbb{C} | f$ is continuous.$\}$. This is an inner product space with $\langle f, g \rangle = \int_0^1 f(t)\overline{g(t)}dt$.*

Note the the second property gives us a natural way to define length.

Definition 3.1.4. *Let V be an inner product space and $v \in V$. We define the length of v to be*

$$\|v\| = \sqrt{\langle v, v \rangle}.$$

Note that $\|v\| = 0$ if and only if $v = 0$.

Lemma 3.1.5. *Let V be an inner product space (over $\mathbb{F}$) and let $v \in V$. Then $\|\alpha v\| = |\alpha| \ \|v\|$ for all $\alpha \in \mathbb{F}$.*

Proof. We will prove this result in the generality of the complex numbers $\mathbb{C}$. Note that $\|\alpha v\| = \sqrt{\langle \alpha v, \alpha v\rangle}$. But note that $\langle \alpha v, \alpha v\rangle = \alpha\langle v, \alpha v\rangle = \alpha\overline{\langle \alpha v, v\rangle} = \alpha\overline{\alpha}\overline{\langle v, v\rangle} = \alpha\overline{\alpha}\langle v, v\rangle$.

So we have that $\|\alpha v\| = \sqrt{\langle \alpha v, \alpha v\rangle} = \sqrt{\alpha\overline{\alpha}}\sqrt{\langle v, v\rangle} = |\alpha|\ \|v\|$.

□

We are now going to produce and prove the famous Schwartz Inequality. But first we will need a lemma.

Lemma 3.1.6. *Let $a, b, c \in \mathbb{R}$ with $a > 0$ and $a\lambda^2 + 2b\lambda + c \geq 0$ for all $\lambda \in \mathbb{R}$ then $b^2 \leq ac$.*

Proof. Set $\lambda := -\frac{b}{a}$. By assumption we have that

$$\frac{b^2}{a} - \frac{2b^2}{a} + c \geq 0.$$

This gives that $c \geq \frac{b^2}{a}$ and hence $ac \geq b^2$. □

Here is the Schwartz Inequality.

Theorem 3.1.7. *Let V be an inner product space and $u, v \in V$, then $|\langle u, v\rangle| \leq \|u\|\ \|v\|$.*

Proof. We will assume without loss of generality that $u \neq 0$ (the theorem is easily seen to be true in this case). We will also begin by assuming that $\langle u, v\rangle \in \mathbb{R}$.

Note that for all $\lambda \in \mathbb{R}$ wehave that $\langle \lambda u + v, \lambda u + v\rangle \geq 0$. This implies that $\lambda^2\langle u, u\rangle + 2\lambda u, v\rangle + \langle v, v\rangle \geq 0$. Let $a = \langle u, u\rangle, b = \langle u, v\rangle, c = \langle v, v\rangle$ and apply the lemma: Since $b^2 \leq ac$ we have that

$$|\langle u, v\rangle|^2 \leq \|u\|^2\ \|v\|^2$$

and we are done.

Generally, if $\alpha = \langle u, v\rangle \notin \mathbb{R}$ then $\alpha \neq 0$ and so

$$\langle \frac{1}{\alpha}u, v\rangle = \frac{1}{\alpha}\langle u, v\rangle = 1 \in \mathbb{R}.$$

Therefore we have that $1 = |\langle \frac{1}{\alpha}u, v\rangle| \leq \|\frac{1}{\alpha}u\|\ \|v\| = \frac{\|u\|\ \|v\|}{\alpha}$. Hence

$$\alpha = |\langle u, v\rangle| \leq \|u\|\ \|v\|$$

and we are done.

□

In the next couple of examples we will produce some applications of the Schwartz Inequality.

Example 3.1.8. *Let $V = \mathbb{F}^n$ (with $\mathbb{F}$ either $\mathbb{R}$ or $\mathbb{C}$). Let $u = (\alpha_1, \cdots, \alpha_n)$ and $v = (\beta_1, \cdots, \beta_n)$. Using the standard inner product we have that*

$$|\alpha_1\overline{\beta_1}+\alpha_2\overline{\beta_2}+\cdots+\alpha_n\overline{\beta_n}|^2 \leq (|\alpha_1|^2+|\alpha_2|^2+\cdots+|\alpha_n|^2)(|\beta_1|^2+|\beta_2|^2+\cdots+|\beta_n|^2).$$

Example 3.1.9. *For this example, we will let $V = \{f : [0,1] \longrightarrow \mathbb{F} | f \text{ is continuous}\}$. We have seen that $\langle f, g\rangle = \int_0^1 f(t)\overline{g(t)}dt$ is an inner product. By the Scwartz Inequality we have that*

$$|\int_0^1 f(t)\overline{g(t)}dt|^2 \leq \int_0^1 |f(t)|^2dt \int_0^1 |g(t)|^2dt.$$

Here is another geometric consequence of living in an inner product space.

Definition 3.1.10. *Let V be an inner product space and $u, v \in V$. We say that u and v are orthogonal if $\langle u, v\rangle = 0$. We say that the set $\{x_i\}$ of nonzero vectors is orthogonal if $\langle x_i, x_j\rangle = 0$ for all $i \neq j$. Additionally we say that an orthogonal set is orthonormal if $\langle x_i, x_i\rangle = 1$ for all i.*

This should be familiar from the "old days" of dot products.

Definition 3.1.11. *Let V be an inner product space and S a subset of V. We define $S^\perp = \{x \in V | \langle x, s\rangle = 0 \text{ for all } s \in S\}$.*

We record the following result.

Theorem 3.1.12. *Let V be an inner product space and S a subset of V. Then $S^\perp$ is a subspace of V.*

Proof. Exercise. □

Proposition 3.1.13. *Let $W \subset V$ be inner product spaces. Then the following hold.*

a) $V \subseteq V^{\perp\perp}$.

b) $V = V^{\perp\perp\perp}$.

Proof. Exercise. □

We will now show that a finite dimensional inner product space has an orthonormal basis. The techniques used will introduce the "Gram-Schmidt" process.

Lemma 3.1.14. *If $\{x_i\}$ is an orthonormal set, then $\{x_i\}$ is a linearly independent set. Additionally, if $w = \sum \alpha_i x_i$ and the set $\{x_i\}$ is orthonormal then $\alpha_i = \langle w, x_i\rangle$.*

Proof. Suppose that $r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0$. This implies that $\langle r_1x_1 + r_2x_2 + \cdots + r_nx_n, x_i\rangle = 0$. Hence $r_i\langle x_i, x_i\rangle = 0$ and so $r_i = 0$. This gives the "linear independence" statement.

Finally note that

$$\langle w, x_i\rangle = \langle \alpha_1x_1 + \alpha_2x_2 + \cdots + \alpha_nx_n\rangle = \alpha_i\langle x_i, x_i\rangle = \alpha_i$$

and we are done. □

Lemma 3.1.15. *If $\{v_1, v_2, \cdots, v_n\}$ is an orthonormal set in V and $w \in V$ then*

$$u = w - \langle w, v_1\rangle v_1 - \langle w, v_2\rangle v_2 - \cdots - \langle w, v_n\rangle v_n$$

is orthogonal to $\{v_1, v_2, \cdots, v_n\}$.

Proof. Exercise. □

Theorem 3.1.16. *Any finite dimensional inner product space has an orthonormal set as a basis.*

Proof. Let $\{v_1, v_2, \cdots, v_n\}$ be a basis for V over $\mathbb{F}$. From this basis, we will use the Gram-Schmidt process to construct an orthomormal set of n elements and this will establish the theorem.

We begin by normalizing v_1 by declaring

$$w_1 = \frac{v_1}{\|v_1\|}.$$

We now let $u_2 = v_2 - \langle v_2, w_1\rangle w_1$ and note that $u_2 \perp w_1$. Normalize again by setting

$$w_2 = \frac{u_2}{\|u_2\|}.$$

Assume that we have constructed the orthonormal set $\{w_1, w_2, \cdots, w_m\}$. We let

$$u_{m+1} = v_{m+1} - \langle v_{m+1}, w_1\rangle w_1 - \langle v_{m+1}, w_2\rangle - \cdots - \langle v_{m+1}, w_m\rangle w_m$$

and normalize by letting

$$w_{m+1} = \frac{u_{m+1}}{\|u_{m+1}\|}.$$

This completes the proof.

□

Theorem 3.1.17. *Let V be a finite dimensional inner product space and $W \subseteq V$ a subspace. Then $V = W \oplus W^{\perp}$.*

Proof. Note first that if $z \in W \bigcap W^{\perp}$ then (since $z \in W$ and $z \in W^{\perp}$) we have that $\langle z, z \rangle = 0$ and hence $z = 0$. So we have $W \bigcap W^{\perp} = 0$.

It only remains to show that $W + W^{\perp} = V$. To this end, let $\{w_1, w_2, \cdots, w_r\}$ be an orthonormal basis for W, and let $v \in V$ and consider

$$v_0 = v - \langle v, w_1 \rangle - \langle v, w_2 \rangle w_2 - \cdots - \langle v, w_r \rangle w_r$$

and note that $v_0 \perp w_i$ for all i. Hence $v_0 \perp W$ and hence $v_0 \in W^{\perp}$. This concludes the proof.

□

Corollary 3.1.18. *Let V be a finite dimensional inner product space and $W \subseteq V$ a subspace. Then $W^{\perp\perp} = W$.*

Proof. Let $w \in W$ and note that for all $x \in W^{\perp}$ we have that $\langle w, x \rangle =)$ and hence $w \in W^{\perp\perp}$.

Also note that $V = W \oplus W^{\perp} = W^{\perp} \oplus W^{\perp\perp}$ and hence $textdim(V) = \dim(V^{\perp\perp})$. Since $V \subseteq V^{\perp\perp}$ and $\dim(V^{\perp\perp})$ is finite, we have that $V = V^{\perp\perp}$. □

With inner product spaces come some nice geometry and this is one reason that they are so useful in analysis. We leave this chapter with a couple of definitions for culture.

Definition 3.1.19. *A Banach space is a vector space that is complete normed vector space.*

Definition 3.1.20. *A Hilbert space is a complete inner product space.*

Chapter 4

Modules

4.1 Introduction and preliminaries

The theory of modules is central in the algebra and damn near everywhere where algebra and its techniques are useful. Modules can be thought of as a generalization of two familiar notions: the notion of a vector space and the notion of an abelian group.

Even in the days of calculus, we saw that the study of vector and vector spaces were essential in being able to implement the techniques of multivariable calculus and differential equations effectively. The notion of a vector space is the notion of a mathematical structure that is closed under addition (the sum of two vectors is a vector). More correctly the set of vectors form an abelian group under addition. What sets a vector space apart from an ordinary abelian group is the fact that the set of vectors is equipped with "scalar multiplication" where the scalars come from a field (in elementary courses, usually $\mathbb{R}$ or $\mathbb{C}$).

The notion of an $R-$module is the generalization of "vector space" where the scalars are taken from some ring R (instead of the more specific "field". Since a vector space and its generalization, the $R-$module is first and foremost an abelian group, we also think of $R-$modules as the generalization of abelian group (e.g. an abelian group equipped with "scalar" multiplication from R).

Since the ring R need not be commutative, we will make the definition of left $R-$module first. Throughout this course there will be many theorems for left $R-$modules. The reader should realize that any such theorem has an analog theorem for right $R-$modules.

Definition 4.1.1. *A left $R-$ module is an abelian group $(M,+)$ equipped with a function $R \times M \to M$ (we write $(r,m) \mapsto rm$) such that for all $r,s \in R$ and $a,b \in M$ we have*

a) $r(a+b)=ra+rb$

b) $(r+s)a=ra+sa$

c) r(sa)=(rs)a

We remark here that if $1 \in R$ and $1_R a = a$ for all $a \in M$ then M is called a unitary $R-$module (this will be the default assumption). If R is a division ring we call M a left vector space. As an exercise verify that $0_R(a) = 0_M = (r)0_M$ for all $r \in R$ and $a \in M$.

Example 4.1.2. *Note that any abelian group is a $\mathbb{Z}$ module. The set of continuous functions from $[0,1]$ to $\mathbb{R}$ is an $\mathbb{R}-$vector space. If R is any ring and I is a left ideal of R, then I is a left $R-$module. (It is worth noting that $\mathbb{Z}_2$ is a $\mathbb{Z}-$ module, but not an ideal of $\mathbb{Z}$.) For another example, if $R \subseteq S$ are rings, then S is an $R-$module. For a more exotic example (which we will see again later) let $\mathbb{F}$ be a field and V a vector space over $\mathbb{F}$ and $T : V \longrightarrow V$ a linear transformation. Then V is an $F[x]$ module via*

$$f(x)v = f(T)v.$$

Finally, we note that the analog of $\mathbb{R}$ is a module. More precisely, if R is a ring then

$$\oplus_{\alpha \in \Lambda} R$$

is an $R-$module with "scalar" multiplication given by

$$r\{s_\alpha\}_{\alpha \in \Lambda} = \{rs_\alpha\}_{\alpha \in \Lambda}.$$

Next we generalize the familiar notion of linear transformation (abelian group homomorphism).

Definition 4.1.3. *Let A, B be $R-$modules and $f : A \longrightarrow B$ be a function. We say that f is an (left) $R-$module homomorphism if*

a) $f(x+y) = f(x) + f(y)$ for all $x, y \in A$.

b) $f(rx) = rf(x)$ for all $r \in R$, $x \in A$.

If R is a division ring, then this is called a linear transformation.

Lemma 4.1.4. *$\phi : M \longrightarrow N$ is an $R-$module homomorphism if and only if $\phi(x + ry) = \phi(x) + r\phi(y)$ for all $x, y \in M$ and for all $r \in R$.*

Proof. Exercise. □

Example 4.1.5. *If A, B are any abelian groups then "$\mathbb{Z}-$ module homomorphism" is synonomous with "abelian group homomorphism".*

Example 4.1.6. *The function $f_n : \mathbb{Z} \longrightarrow \mathbb{Z}$ given by $f_n(x) = nx$ is a $\mathbb{Z}-$module homomorphism, but not a ring homomorphism. The same is true of the function $g : R[x] \longrightarrow R[x]$ given by $g(r(x)) = xr(x)$ (i.e., this is an $R-$module homomorphism which is not a ring homomorphism.*

As is the case with our other morphisms, we can talk about "mono" (injective), "epi" (surjective), and bijective $R-$module homomorphisms. The terminology will be analogous to earlier terminology in groups and rings.

It is important at this juncture to introduce an important class of abelian groups that are, in certain important cases, also $R-$modules.

Proposition 4.1.7. *Let M and N be $R-$modules. The set $Hom_R(M,N) = \{\phi : M \longrightarrow N | \phi$ is an $R-$module homomorphism.$\}$ is an abelian group (under pointwise addition of functions). Additionally, if R is commutative, then $Hom_R(M,N)$ is an $R-$module.*

Proof. We will leave the fact that $\mathrm{Hom}_R(M,N)$ is an abelian group as an exercise and verify the second statement. If R is commutative then we define the scalar multiplication by

$$(r\phi)(x) = r(\phi(x))$$

for all $r \in R$. Then it is easy to see that $\mathrm{Hom}_R(M,N)$ is an $R-$module. □

Definition 4.1.8. *Let M be a left $R-$module and N a subgroup of M. We say that N is a (left) submodule of M if $rN \subseteq N$ for all $r \in R$.*

Proposition 4.1.9. *Let R be a ring and M a (unitary) left R module. Then $N \subseteq M$ is a left $R-$submodule of M if and only if N is nonempty and $x+ry \in N$ for all $x, y \in N$ and $r \in R$.*

Proof. The necessity of the condition is straightforward. Assume that for all $x, y \in N$ and $r \in R$, $x + ry \in N$. Choose $r = -1$ to see that for all $x, y \in N$, $x-y \in N$. So N is an abelian group. Now choose $x = 0$ to see that $rN \subseteq N$. □

Example 4.1.10. *If M is a $\mathbb{Z}-$module then any subgroup of M is a $\mathbb{Z}-$submodule of M.*

Example 4.1.11. *If $f : A \longrightarrow B$ is an $R-$homomorphism, then $ker(f) = \{x | f(x) = 0\}$ is an $R-$submodule of A. Additionally, $Im(f) = \{f(x) | x \in A\}$ is an $R-$submodule of B. If $C \subseteq B$ is an $R-$submodule of B then $f^{-1}(C) = \{x \in A | f(x) \in C\}$ is an $R-$submodule of A.*

Example 4.1.12. *If X is a subset of some $R-$module, A, then $\langle X \rangle$ (the $R-$submodule spanned by X) is the intersection of all $R-$submodules of A containing X. That is:*

$$\langle X \rangle = \bigcap_{X \subseteq M \subseteq A} M.$$

If $X = \bigcup_{i \in I} B_i$ where each B_i is an $R-$submodule of A, then $\langle X \rangle$ is called the sum of the B_i's and if $I = \{1, 2, \cdots, n\}$ then $\langle X \rangle = B_1 + B_2 + \cdots + B_n$.

We conclude this section with a special and important class of $R-$modules.

Definition 4.1.13. *Let R be commutative with 1. An $R-$algebra is a ring A with identity equipped with a ring homomorphism $f : R \longrightarrow A$ $(f(1_R) = 1_A)$ such that $f(R)$ is contained in the center of A.*

Proposition 4.1.14. *If A is an $R-$algebra, then A is an $R-$module.*

Proof. We define $a(r) = r(a) = f(r)a$. Note that $1(a) = f(1)a = 1_A a = a$. For the second property $(r+s)a = (f(r+s))a = (f(r) + f(s))a = f(r)a + f(s)a = ra + sa$. Also $(rs)a = (f(rs))a = (f(r)f(s))a = f(r)(f(s)a) = f(r)(sa) = r(sa)$ and finally $r(a+b) = f(r)(a+b) = f(r)a + f(r)b = ra + rb$. □

Example 4.1.15. *A good canonical example of an $R-$algebra is the matrix ring $M_n(R)$. The relevant homomorphism is the map that takes the element $r \in R$ to the $n \times n$ diagonal matrix with all r's on the diagonal.*

Definition 4.1.16. *If A and B are $R-$algebras then an $R-$algebra homomorphism $\phi : A \longrightarrow B$ is a ring homomorphism such that*

a) $\phi(1_A) = 1_B$ and

b) $\phi(ra) = r\phi(a)$ for all $r \in R$ and $a \in A$.

4.2 Quotient Structures and the Homomorphism Theorems

The idea of quotient structure is the analog of what we have seen in the theory of groups and rings. We begin with the following theorem.

Theorem 4.2.1. *Let $B, C \subseteq A$ be modules.*

a) The quotient group A/B is an $R-$module with $R-$action given by $r(a + B) = ra + B$.

b) The map $\pi_B : A \longrightarrow A/B$ given by $\pi_B(a) = a + B$ is an $R-$module homomorphism with kernal B.

c) There is an $R-$module homomorphism $B/(B \bigcap C) \cong (B + C)/C$.

d) If $C \subseteq B$ then $B/C \subseteq A/C$ and $(A/C)/(B/C) \cong A/B$.

Proof. For part a) it suffices to show that the action is well-defined. Suppose that $x + B = y + B$. Hence $x - y \in B$ and so $r(x - y) \in B$. We conclude that $rx + B = ry + B$ and the action is well-defined. Showing that the multiplication satisfies the axioms is easy since A is an $R-$module. Part b) is routine. Parts c) and d) are consequences of the next theorem and we leave them for exercises. □

An application of the next result is the "best way" to prove parts c) and d) of the above theorem. There are myriad others. This is called the first isomorphism theorem.

Theorem 4.2.2. *Let $f : A \longrightarrow B$ be an $R-$module homomorphism, then f induces and $R-$module isomorphism*

$$\overline{f} : A/ker(f) \xrightarrow{\cong} Im(f).$$

Proof. Define the map

$$\overline{f} : A/\ker(f) \longrightarrow \mathrm{Im}(f)$$

via $\overline{f}(a+\ker(f)) = f(a)$. Since f is an $R-$module homomorphism, it is easy to see that $\overline{f}$ is as well. It is also clear that $\overline{f}$ is onto the image of f. It remains to show that $\overline{f}$ is one to one, and so assume that $\overline{f}(a+\ker(f)) = 0 = f(a)$. This means that $a \in \ker(f)$ and we are done. □

For our last result we will produce a corollary that shows submodule corresponce in quotient structures.

Corollary 4.2.3. *If R is a ring and $B \subseteq A$ are $R-$modules then there is a 1-1 correspondence between submodules of A/B and submodules of A containing B.*

Proof. Let C be a submodule of A containing B. We know that from a previous result that $C/B \subseteq A/B$. On the other hand, assume that M is a submodule of A/B. Consider the canonical projection

$$\pi_B : A \longrightarrow A/B.$$

Now consider the submodule of A: $\pi_B^{-1}(M)$. Verify that $M \longleftrightarrow \pi_B^{-1}(M)$ gives pur 1-1 cprrespondence. □

4.3 The Direct Product and Direct Sum

As one may expect the universal constructions of direct product and direct sum have an important analog in the theory of modules. We will see that the central theorems from abelian group theory carry over in this realm, and in particular we will see later that any $R-$module is the homomorphic image of a particular direct sum of special $R-$modules.

Theorem 4.3.1. *Let $\{A_i\}_{i\in I}$ be a family of $R-$modules and $\prod_{i\in I} A_i$ and $\oplus_{i\in I} A_i$ be respectively the direct product and direct sum of the family as abelian groups.*

a) The direct product $\prod_{i\in I} A_i$ is an $R-$module with $R-$action given by $r\{a_i\}_{i\in I} = \{ra_i\}_{i\in I}$.

b) The direct sum $\oplus_{i\in I} A_i$ is an $R-$submodule of $\prod_{i\in I} A_i$ with the inherited $R-$action.

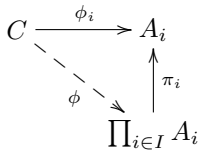
c) For all $k \in I$ the canonical projection $\pi_k : \prod_{i\in I} A_i \longrightarrow A_k$ ($\pi_k(\{a_i\}) = a_k$) is an $R-$module epimorphism.

d) For each $k \in I$ the canonical injection $\iota_k : A_k \longrightarrow \oplus_{i\in I} A_i$ ($\iota_k(a) = \{x_i\}_{i\in I}$ where $x_i = 0$ if $i \neq k$ and $x_k = a$) is an $R-$module monomorphism.

Proof. The proof of this is extremely similar to the proof of the analog theorem from group theory. □

As was the case earlier, the direct product and direct sum are (unique) solutions to certain universal mapping problems.

Theorem 4.3.2. *If R is a ring, $\{A_i | i \in I\}$ is a family of $R-$modules, C is an $R-$module and $\{\phi_i : C \longrightarrow A_i | i \in I\}$ is a family of $R-$module homomorphisms then there is a unique $R-$module homomorphism $\phi : C \longrightarrow \prod_{i\in I} A_i$ such that $\pi_i\phi = \phi_i$ for all $i \in I$. Additionally $\prod_{i\in I} A_i$ is uniquely determined (up to isomorphism) by this property.*

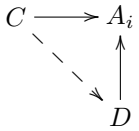


Proof. $\phi(c) = \{\phi_i(c)\}_{i\in I}$ is the map (verify that this is indeed an $R-$module homomorphism). Assume that ξ is another such $R-$module homomorphism satisfying the universal mapping problem.

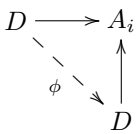
We write $\xi(c) = \{c_i\}$ and note that $\pi_i(\xi(c)) = c_i = \phi_i(c)$. Hence each $c_i = \phi_i(c)$ and $xi \equiv \phi$.

We will next demonstrate that the direct product is the unique (up to isomorphism) solution to this universal mapping problem.

Assume that D is another solution to this universal mapping problem (i.e. D is an $R-$module that has the same properties as the direct product). We have the diagram:

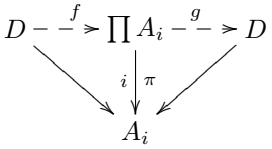


in particular, replacing C with D we obtain

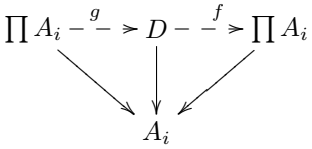


and we note that $\phi = 1_D$ is an obvious solution to this mapping problem and so ϕ must be precisely 1_D by uniqueness.

We now consider the augmented diagram



Considering the "big triangle" we see that $gf = 1_D$ must be the solution by uniqueness. Augmenting the diagram from a different perspective (swapping the roles of D and $\prod A_i$ since they are both solutions to the universal mapping problem) we get the diagram

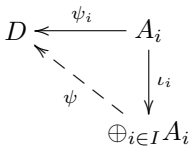


and in a similar fashion to the above, we obtain that $fg = 1_{\prod A_i}$.

In conclusion, we obtain that $gf = 1_D$ and $fg = 1_{\prod A_i}$ and hence $D \cong \prod A_i$. □

There is a dual result with respect the direct sum (more precisely, the direct sum rears its head as the solution to the dual mapping problem).

Theorem 4.3.3. *If R is a ring, $\{A_i | i \in I\}$ is a family of $R-$modules, D is an $R-$module and $\{\psi_i : A_i \longrightarrow D | i \in I\}$ is a family of $R-$module homomorphisms, then there is a unique $R-$module homomorphism $\psi : \oplus_{i \in I} A_i \longrightarrow D$ such that $\psi \iota_i = \psi_i$ for all $i \in I$. What is more, the direct sum is uniquely determined up to isomorphism by this property.*



Proof. The proof here is "dual" (e.g. essentially the same with the arrows reversed) to the previous proof. The unique map in question is $\psi(\{a_i\}) = \sum_{i \in I} \psi_i(a_i)$. Note that since $\{a_i\} \in \oplus_{i \in I} A_i$ all but finitely many of the a_i's are 0 and hence the sum $\sum_{i \in I} \psi_i(a_i)$ is finite and "makes sense". □

We conclude this brief look at these constructions with the following result, which is a nice characterization of when an $R-$ module is a direct sum of some of its submodules.

Proposition 4.3.4. *Let R be a ring and $\{A_i\}_{i \in I}$ a family of $R-$ submodules of A such that*

a) A is the sum of the family $\{A_i\}$.

b) For all $k \in I$, $A_k \bigcap \overline{A_k} = 0$ where $\overline{A_k}$ is the sum of $\{A_i\}_{i \neq k}$.

Then $A \cong \oplus_{i \in I} A_i$.

Proof. Define $\phi : \oplus_{i \in I} A_i \longrightarrow A$ by $\phi(\{a_i\}) = \sum_{i \in I} a_i$. Since $\{a_i\}$ is an element of $\oplus A_i$, this sum is finite. The verification that ϕ is an $R-$module homomorphism is routine. We will show that ϕ is one to one and onto.

To see that ϕ is one to one, suppose that $\{a_i\} \in \ker(\phi)$ and that at least one of the a_i's (say a_k) is nonzero. We therefore have that

$$-a_k = \sum_{i \neq k} a_i$$

and hence a_k is an element of both A_k and the submodule of A generated by the family $\{A_i\}_{i \neq k}$. By assumtion, this means that $a_k = 0$ which is our contradiction, and hence $\ker(\phi) = 0$.

For the onto-ness (what a word) let $a \in A$. Since the sum of the A_i's is precisely A, we know that there is a (finite) sum $a_{i_1} + \cdots + a_{i_k}$ that is equal to a. Let $\{x_j\}$ be the sequence defined by $x_{i_1} = a_{i_1}, \cdots, x_{i_k} = a_{i_k}$ and $x_j = 0$ for all other indices. Note that $\phi(\{x_j\}) = a$. □

4.4 Exact Sequences

Exact sequences are the genesis of some very very important tools in commutative algebra, homological algebra, algebraic K-theory, and algebraic topology. Exact sequences of $R-$modules can contain such (seemingly) diverse information as factorization information of a commutative ring and the basic genus structure of a topological space.

Definition 4.4.1. *A sequence of $R-$module homomorphisms*

$$\cdots \longrightarrow A_{n-1} \xrightarrow{f_n} A_n \xrightarrow{f_{n+1}} A_{n+1} \longrightarrow \cdots$$

is called exact at A_n if $Im(f_n) = ker(f_{n+1})$. We say that the sequence is exact if it is exact at A_n for all n.

Definition 4.4.2. *An exact sequence of the form*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is called a short exact sequence (SES) if f is one to one, g is onto and $ker(g) = Im(f)$.

As it turns out, short exact sequences are the building blocks of general exact sequences in the following sense. If

$$\cdots \longrightarrow A_{n-1} \xrightarrow{f} A_n \xrightarrow{g} A_{n+1} \longrightarrow \cdots$$

then this sequence can be obtained by "splicing together" certain short exact sequences (as an exercise you should try to figure out how this is done).

Example 4.4.3. *a) The sequence* $0 \longrightarrow A \xrightarrow{f} B$ *is exact if and only if* f *is 1-1, the sequence* $B \xrightarrow{g} C \longrightarrow 0$ *is exact if and only if* g *is onto, the sequence* $0 \longrightarrow A \xrightarrow{h} B \longrightarrow 0$ *is exact if and only if* h *is onto.*

b) If $n \neq 0$*, the sequence* $0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{\pi_n} \mathbb{Z}_n \longrightarrow 0$ *with* $f(k) = nk$ *and* $\pi_n(a) = \overline{a}$ *(the reduction of a modulo n) is a short exact sequence.*

c) Any sequence of the form $0 \longrightarrow A \xrightarrow{f} A \oplus C \xrightarrow{g} C \longrightarrow 0$ *with* $f(a) = (a, 0)$ *and* $g(a, c) = c$ *is short exact. (It should be noted that there are usually many ways to have the maps make the sequence be exact, for example if* $A = C$*, we could also have* $f(a) = (a, a)$ *and* $g(x, y) = x - y$*). This example is a special kind of short exact sequence called a split exact sequence. Since the middle term is the sum of the second and fourth, there are maps* $h : C \longrightarrow A \oplus C$ *such that* $gh = 1_C$ *and there is a* $k : A \oplus C \longrightarrow A$ *such that* $kf = 1_A$*. In other words we could "run" the sequence in reverse. An example of a short exact sequence that does not split is given above in b) if* $n \neq 1$*.*

We now introduce a couple of results that are fundamental if you wish to apply the concept of exactness. The proofs of most of these will be omitted as exercises, but all of them require an interesting (and fun) technique known as a "diagram chase." This technique will be demonstrated in the proof of the short five lemma (but all of the diagram chase proofs are similar.

This first result is called the five lemma.

Proposition 4.4.4. *Consider the following commutative diagram of* $R-$*module homomorphisms with exact rows*

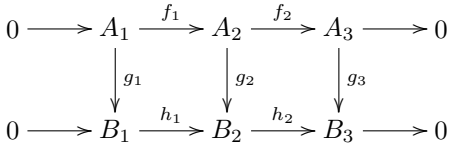
$$\begin{array}{ccccccccc} A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & A_3 & \xrightarrow{f_3} & A_4 & \xrightarrow{f_4} & A_5 \\ \downarrow{\scriptstyle g_1} & & \downarrow{\scriptstyle g_2} & & \downarrow{\scriptstyle g_3} & & \downarrow{\scriptstyle g_4} & & \downarrow{\scriptstyle g_5} \\ B_1 & \xrightarrow{h_1} & B_2 & \xrightarrow{h_2} & B_3 & \xrightarrow{h_3} & B_4 & \xrightarrow{h_4} & B_5 \end{array}$$

a) If g_2 *and* g_4 *are onto and* g_5 *is one to one then* g_3 *is onto.*

b) If g_2 *and* g_4 *are one to one and* g_1 *is onto then* g_3 *is one to one.*

Now we produce a corollary which is often referred to as the short five lemma.

Corollary 4.4.5. *Consider the following commutative diagram of* $R-$*module homomorphisms with exact rows*



a) If g_1 and g_3 are onto then g_2 is onto.

b) If g_1 and g_3 are one to one then g_2 is one to one.

c) If g_1 and g_3 are isomorphisms that g_2 is an isomorphism.

Before beginning the proof, we note that this follows directly from the five lemma, but we will prove this result from scratch to demonstrate the technique of diagram chasing.

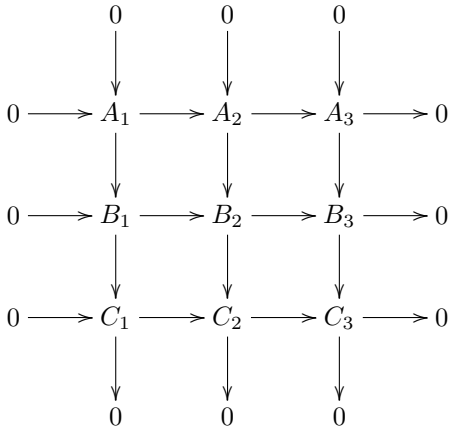
Proof. Of course c) follows directly from a) and b) so we will only show a) and b).

For a) let $b_2 \in B_2$. The only direction that we can go is to the left so let $b_3 = h_2(b_2) \in B_3$. Since g_3 is onto, there is a $a_3 \in A_3$ such that $g_3(a_3) = b_3$. Additionally, f_2 is onto, so we can find $a_2 \in A_2$ such that $f_2(a_2) = a_3$. Now we consider $x = g_2(a_2) \in B_2$ (if $x = b_2$ we are done, but there is no guarantee of this). Note that by commutativity of the diagram, we have that $h_2(x) = b_3 = h_2(b_2)$ and hence $h_2(b_2 - x) = 0$, that is, $b_2 - x \in \ker(h_2) = \text{im}(h_1)$. Consequently, there is a $b_1 \in B_1$ such that $h_1(b_1) = b_2 - x$. Now since g_1 is onto there is an $a_1 \in A_1$ such that $g_1(a_1) = b_1$, and by the commutativity of the diagram $g_2(f_1(a_1)) = b_2 - x$. Notice that $y = f_1(a_1) \in A_2$ and $g_2(y + a_2) = g_2(y) + g_2(a_2) = b_2 - x + x = b_2$ and hence g_2 is onto.

For b) assume that $a_2 \in \ker(g_2)$, and hence $g_2(a_2) = 0$ and so $h_2(g_2(a_2)) = g_3(f_2(a_2)) = 0$ by commutativity of the diagram. Since g_3 is one to one, we have that $f_2(a_2) = 0$, so $a_2 \in \ker(f_2) = \text{im}(f_1)$. So we can find (a unique, since f_1 is one to one) element a_1 such that $f(a_1) = a_2$. Note that $g_2(f_1(a_1)) = 0 = h_1(g_1(a_1))$ Since both h_1 and g_1 are one to one, a_1 must be 0, and hence $a_2 = f_1(a_1) = f_1(0) = 0$ and g_2 is one to one. This completes the proof. □

The next result is known as the 3×3 lemma.

Theorem 4.4.6. *Consider the following commutative diagram of $R-$module homomorphisms*

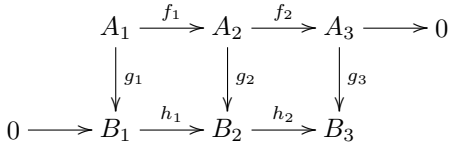


a) If the columns and the bottom two rows are exact, then the top row is exact.

b) If the columns and the top two rows are exact, then the bottom row is exact.

Our final "homological theorem" is the very famous snake lemma and it is one of the major tools of homological algebra and its applications. The important part of the result is the existence of the well-defined homomorphism ∂ called the boundary map which allows passage from n^{th} homology to $(n-1)^{\text{th}}$ homology.

Theorem 4.4.7. *Consider the following commutative diagram with exact rows*



then there is an exact sequence

$$ker(g_1) \xrightarrow{\alpha_1} ker(g_2) \xrightarrow{\alpha_2} ker(g_3) \xrightarrow{\partial} coker(g_1) \xrightarrow{\beta_1} coker(g_2) \xrightarrow{\beta_2} coker(g_3)\,.$$

Additionally, if f_1 is one to one, then so is α_1 and if h_2 is onto, then so is β_2.

We will close out this section with a result that characterizes when a short exact sequence is a split exact sequence.

Theorem 4.4.8. *Let R be a ring and*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

a short exact sequence of $R-$module homomorphisms. Then the following conditions are equivalent.

a) There is an $R-$module homomorphism $h : C \longrightarrow B$ such that $gh = 1_C$.

b) There is an $R-$module homomorphism $k : B \longrightarrow A$ such that $kf = 1_A$.

c) $B \cong A \oplus C$.

We remark that this will be our formal definition of a split exact sequence; namely a split exact sequence is a short exact sequence satisfying one, and hence all, of the above conditions.

Proof. For a)$\Longrightarrow$ b) we need to find an intelligent way to associate an element of A with a given element $b \in B$. We do this by "cleaning" b. Given a $b \in B$, we are not guaranteed an element $a \in A$ such that $f(a) = b$, so we consider $hg(b) \in B$. Note that $g(b - hg(b)) = g(b) - ghg(b) = g(b) - g(b) = 0$. We conclude that $b - hg(b) \in \ker(g) = \text{im}(f)$. With this insight, we define $k(b) = f^{-1}(b - hg(b))$. Since f is one to one, this assignment is well-defined. Suppose that $f^{-1}(b_1 - hg(b_1)) = a_1$ and that $f^{-1}(b_2 - hg(b_2)) = a_2$ and note that $f(a_1 + a_2) = b_1 + b_2 - hg(b_1 + b_2)$. Hence we have that $k(b_1 + b_2) = f^{-1}(b_1 + b_2 - hg(b_1 + b_2)) = a_1 + a_2 = k(b_1) + k(b_2)$. The proof that $k(rb) = rk(b)$ is similar. Note that $kf(a_1) = f^{-1}(f(a_1) - hgf(a_1)) = f^{-1}(f(a_1)) = a_1$ and so a) implies b).

For b)$\Longrightarrow$ c) consider the map $\phi : B \longrightarrow A \oplus C$ given by $\phi(b) = (k(b), g(b))$ (verify that this is an $R-$module homomorphism). First let $b \in \ker(\phi)$. So we have $k(b) = 0$ and $g(b) = 0$. This means that $b \in \ker(g) = \text{im}(f)$ and so there is an $a \in A$ such that $b = f(a)$. Therefore $0 = k(b) = k(f(a)) = a$. Since $a = 0$, we have that $b = 0$ and ϕ is one to one.

Now let $(a, c) \in A \oplus C$ be arbitrary. Since g is onto we can select $b \in B$ such that $g(b) = c$. Unfortunately, it may not be the case that $k(b) = a$. We can, however, vary b by any element of $\ker(g) = \text{im}(f)$. Some computations show that the appropriate element to choose is $b - fk(b) + f(a)$. Indeed note that $\phi(b - fk(b) + f(a)) = (k(b - fk(b) + f(a)), g(b - fk(b) + f(a)) = (k(b) - kfk(b) + kf(a), g(b)) = (a, c)$ and ϕ is an isomorphism.

For now we leave c)$\Longrightarrow$ a) as an exercise.

□

4.5 Free Modules

Free modules are, in a certain sense, the easiest modules to picture (they are most like the more familiar vector spaces). Free modules are also the "mothers of all modules" in the sense that every $R-$module is the homomorphic image of a free $R-$module. Free modules are precisely that modules that have a notion of a basis (a very nice generating set) and we begin with the definition of a basis.

Definition 4.5.1. *A subset X of an $R-$module M is said to be linearly independent if given any $x_1, x_2, \cdots, x_n \in X$, the relation*

$$\sum_{i=1}^{n} r_i x_i = 0$$

implies that $r_i = 0$ *for all* $1 \leq i \leq n$.

We remark (surprise, surprise) that a set that is not linearly independent is called linearly dependent. Also if M is generated by X, we say that X spans M. Finally we tie these together by saying that a linearly independent subset of M that spans M (if such a subset of M exists) is called a basis of M. Modules which actually have a basis are free modules that we have been alluding to.

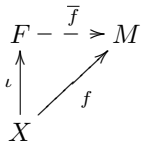
Theorem 4.5.2. *Let R be a ring with identity and F a unitary $R-$module. The following conditions are equivalent.*

a) F has a nonempty basis.

b) F is the (internal) direct sum of a family of cyclic $R-$modules each of which is isomorphic to R as an $R-$module.

c) F is $R-$module isomorphic to a direct sum of some number of copies of the $R-$module R.

d) There exists a nonempty set X and a function $\iota : X \hookrightarrow F$ such that given any unitary $R-$module M and function $f : X \longrightarrow M$, there exists a unique $R-$module homomorphism $\overline{f} : F \longrightarrow M$ such that $\overline{f}\iota = f$.



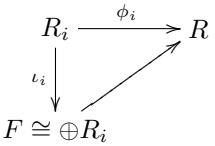
Proof. We first consider a) implies b). Let X be a basis of F. Note that if $x \in X$ then $R \cong Rx$ as a left $R-$module (since the singleton set $\{x\}$ is linearly independent). Also note that $F = \sum_{x \in X} Rx$ (but the sum may not be direct and that is what we need to show). Suppose that $m \in Rx \bigcap (\sum_{y \in X \setminus x} R_y)$ then we can write

$$rx = \sum r_i y_i$$

and hence the set X is linearly dependent.

The implication b) implies c) is easy and is left to the reader.

For c) implies d) let $F \oplus R_i$ with each R_i isomorphic is R via $R_i \xrightarrow{\phi_i} R$. So (for all i we have the commutative diagram



Define $X = \{x_i\}_{i \in I}$ where x_i is such that $\phi_i(x_i) = 1_R$. So our function *iota* : $X \longrightarrow F$ assigns to each cyclic generator its image in F. That is $\iota(x_i) = \iota_i(x_i)$ and say that $f : X \longrightarrow M$ makes the assignment $f(x_i) = m_i \in M$. The desired homomorphism is the homomorphism that obeys the rule:

$$\overline{f}(\sum r_i \iota_i(x_i)) = \sum r_i m_i$$

and uniqueness is an easy exercise.

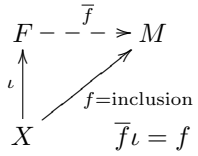
We leave the last implication to the reader.

□

Here is an important corollary that reflects the universal nature and importance of free modules.

Corollary 4.5.3. *Every unitary module M over a ring with identity is the homomorphic image of a free $R-$module. In fact, if M is finitely generated, then the free module may be chosen to be finitely generated.*

Proof. Let X be a generating set of M and consider the diagram



In the diagram above the module F is free on the set X (note that if X is finite then F is finitely generated). We have an induced homomorphism $\overline{f} : F \longrightarrow M$ and $X \subset \text{im}(\overline{f})$ therefore since X is a generating set, $\text{im}(\overline{f}) = M$ and this gets the first statement. Also as was pointed out earlier, if M is finfitely generated (that is, X my be chosed to be finite) then F is finitely generated. □

Here we do a little specialization to the case of vector spaces.

Lemma 4.5.4. *A maximal linearly independent subset of a vector spcae V over a division ring D is a basis of V.*

Proof. Let X be a maximal linearly independent subset (how do we know such an animal exists...we don't yet, but will later see that in important cases these do exist). Let W be a subspace of V spanned by X. If $W = V$ then we are done so we selesct $a \in V \setminus W$. Of course $\{a\} \bigcup X$ must be linearly dependent, so we have an equation of the form

$$ra + \sum r_i x_i = 0$$

with $x_i \in X$, $r, r_i \in R$ and $r \neq 0$ (if the last condition does not hold then the linear independence of the set X would force all of the r_i's to be 0 as well).

Manipulating this equation gives us that

$$a = \sum -r^{-1} r_i x_i \in V$$

which is a contradiction. Hence there is no $a \in V \setminus W$ and so $V = W$ and we are done. □

Here is a big module structure theorem for modules over a division ring (vector spaces). This is why "linear algebra" is much easier that modules in general...over a field modules are always free.

Theorem 4.5.5. *Every vector space V over a division ring D has a basis and is therefore free. More generally, every linearly independent subset of V is contained in a basis of V.*

Before we prove this theorem, we also remark that if every unitary module over a ring with identity, D, is free, then D is a division ring.

We also point out that this business about "every linearly independent subset of V is contained in a basis for V" does not extend to free modules over a general ring. Indeed if you consider the simple example of $\mathbb{Z}$ as a $\mathbb{Z}$ module, consider the maximal linearly independent subset $\{2\}$. This set is not contained in a basis for $\mathbb{Z}$, because any two element subset of the integers is linearly independent. The problem here is that $\{2\}$ does not span $\mathbb{Z}$ and we immediately see the contrasting situation of a ring not being a division ring (i.e., we can see that we somehow need $\frac{1}{2}$ to be an integer for the set $\{2\}$ to have a chance of spanning $\mathbb{Z}$).

Proof. We will prove the more general statement and capture it all at once.

Suppose that X is a linearly independent subset of V (note that such a set has to exist in a nonzero vector space). Consider the collection of linearly independent subsets of V that contain X (and we will call it Γ). This is a partially ordered set under inclusion. Let $\{\mathfrak{C}_i\}$ be a chain in Γ. Note that $C = \bigcup_i \mathfrak{C}_i$ is linearly independent (verify!) and hence is an upper bound for the chain in Γ. Thus Zorn's Lemma gives the existence existence of a maximal element and this establishes the theorem. □

Remark 4.5.6. *If R is a ring that has a division ring as a homomorphic image (e.g. any commutative ring with identity), then R has the invariant dimension property. That is for any free module F over R, any two bases have the same cardinality. If R has the invariant dimension property, then two free modules E and F are isomorphic if and only if they have the same rank. For an example of a ring which does not have the invariant dimension property consider K, a field, and $F = \oplus_{n=1}^{\infty} K$. If $R = Hom_K(F, F)$. For any n, $R \cong \oplus_{m=1}^{n} R$ (check this).*

In closing we look at a couple of familiar properties of vector spaces. The proofs are left as exercises.

Theorem 4.5.7. *Let W be a subspace of V.*

a) $dim_D(W) \leq dim_D(V)$.

b) If $dim_D(W) = dim_D(V)$ and $dim_D(V)$ is finite, then $W = V$.

c) $dim_D(V) = dim_D(W) + dim_D(V/W)$.

d) *If* $f : V \longrightarrow W$ *is a linear transformation then* $dim_D(V) = dim_D(ker(f)) + dim_D(im(f))$.

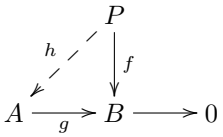
e) *If* V *and* W *are finite dimensional then* $dim_D(V) + dim_D(W) = dim_D(V \bigcap W) + dim_D(V + W)$.

Example 4.5.8. *Build a* 2×2 *matrix and examine the above theorem.*

4.6 Projective and Injective Modules

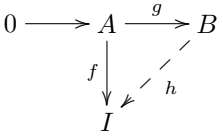
We will define and prove some of the analogous results for projectives and injectives. Please note the "dual" (arrow reversing) nature of some of the definitions and results. For many projective (respectively injective) results there is a very similar injective (resp. projective) result.

Definition 4.6.1. *Consider the following diagram of* $R-$*modules with the bottom row exact.*



We say that P *is projective if there is an* $R-$*module homomorphism* $h : P \longrightarrow A$ *such that* $gh = f$.

Definition 4.6.2. *Consider the following diagram of* $R-$*modules with the top row exact.*

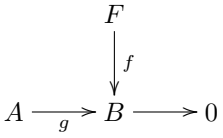


We say that I *is injective if there is an* $R-$*module homomorphism* $h : B \longrightarrow I$ *such that* $hg = f$.

We will now investigate some of the consequences of these definitions in tandem.

Theorem 4.6.3. *Every (unitary) free module over* R *is projective.*

Proof. Consider the following diagram



Let F be free on the set X (and we will denote the canonical injection from X into F by $\iota : X \hookrightarrow F$). Since g is onto, there is $a_i \in A$ such that $g(a_i) = f\iota(x_i)$ for all i. Therefore we have a function $f^* : X \longrightarrow A$ such that $f^*(x_i) = a_i$. Since F is free, this induces an $R-$module homomorphism $h : F \longrightarrow A$ such that $h\iota(x_i) = a_i$. Therefore $gh\iota(x_i) = g(a_i) = f\iota(x_i)$ and hence $gh = f$. Hence F is projective. □

Definition 4.6.4. *Let D be an abelian group. We say that D is divisible if given $d \in D$ and $0 \neq n \in \mathbb{Z}$, there exists a $d' \in D$ such that $nd' = d$.*

Basically, in a divisible group we can divide by any nonzero integer.

Lemma 4.6.5. *D is divisible if and only if D is an injective $\mathbb{Z}-$module.*

Proof. ($\Longleftarrow$) Let D be injective and $d \in D$ and n be a nonzero integer. Consider the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & \langle n \rangle & \xrightarrow{\subseteq} & \mathbb{Z} \\ & & {\scriptstyle f}\downarrow & \swarrow_{h} & \\ & & D & & \end{array}$$

Let $d' = h(1)$ and therefore $nd' = nh(1) = h(n) = f(n) = d$ and hence D is divisible.

The other direction is an exercise. □

Note that in the parallel results coming up many of the proofs are dual (in some places the proofs are more different).

Theorem 4.6.6. *The following conditions on the $R-$module P are equivalent.*

a) P is projective.

b) Every short exact sequence of the form $0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$ is split exact.

c) There is an $R-$module K and a free module F such that $F \cong P \oplus K$.

Theorem 4.6.7. *The following conditions on the $R-$module I are equivalent.*

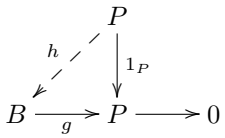
a) I is injective.

b) Every short exact sequence of the form $0 \longrightarrow I \longrightarrow B \longrightarrow C \longrightarrow 0$ is split exact.

c) I is a direct summand of any module of which it is a submodule.

Proof. We will provide a proof of the projective result. Try to do the injective one yourself.

For a) implies b) consider the short exact sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P \longrightarrow 0$. We now consider the diagram



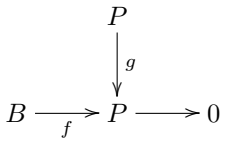
Since P is projective, there exists $h : P \longrightarrow B$ such that $gh = 1_P$, and hence the short exact sequence splits.

For b) implies c), we assume b) and assume that P is our given projective module. We know that any R module is the homomorphic image of a free module F (i.e. we have the onto map $F \xrightarrow{\phi} P \longrightarrow 0$. Hence we have the short exact sequence

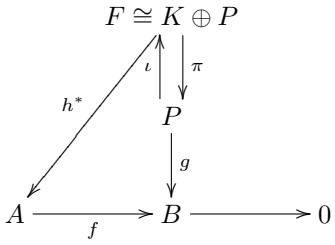
$$0 \longrightarrow \ker(\phi) \longrightarrow F \xrightarrow{\phi} P \longrightarrow 0.$$

Since the sequence must split, we have that $F \cong P \oplus \ker(\phi)$ and we have established b) implies c).

For the implication c) implies a) consider the following diagram.



Keeping in mind that there is a free module F with $F \cong K \oplus P$, we expand the diagram



where $\pi(k, p) = p$ and $\iota(p) = (0, p)$ (note $\pi\iota = 1_P$). Since any free module is projective there is an $h^* : F \longrightarrow A$ such that $fh^* = g\pi$. Now consider the map $P \longrightarrow A$ given by $h^*\iota$. Note that $f(h^*\iota) = g\pi\iota = g$ and hence P is projective. □

We note here the the proof of the dual injective theorem requires the result that will be recorded later that says that every $R-$module can be embedded in an injective $R-$module.

Corollary 4.6.8. *Let $\{P_i\}_{i\in I}$ be a family of $R-$modules. $\oplus_{i\in I} P_i$ is projective if and only if P_i is projective for all $i \in I$.*

Proof. If each P_i is projective, then for all i there is a Q_i such that $Q_i \oplus P_i$ is free. Hence we have the free module

$$\oplus_{i\in I}(P_i \oplus Q_i) \cong (\oplus_{i\in I} P_i) \oplus (\oplus_{i\in I} Q_i)$$

and hence the module $\oplus_{i\in I} P_i$ (being the summand of a free module) is projective.

On the other hand, assume that $\oplus_{i\in I} P_i \cong P_i \oplus (\oplus_{j\neq i} P_j$ is projective. So we can find an $R-$module K so that $K \oplus_{i\in I} P_i$ is free and hence $P_i \oplus (K \oplus (\oplus_{j\neq i} P_j))$ is free and hence P_i is projective. □

Corollary 4.6.9. *Let $\{I_j\}_{j\in\Gamma}$ be a family of $R-$modules. $\prod_{j\in\Gamma} I_j$ is injective if and only if I_j is injective for all $i \in \Gamma$.*

Proof. Very similar to the previous. Exercise. □

Corollary 4.6.10. *Every $R-$module is the homomorphic image of a projective $R-$module.*

Proof. Any free is projective. □

Theorem 4.6.11. *Every $R-$module M can be embedded in an injective $R-$module.*

Proof. Exercise. As a hint, first show that M (considered as an abelian group) can be embedded in a divisible abelian group D. Now embed M (as an $R-$module) in the $R-$module $\mathrm{Hom}_{\mathbb{Z}}(R, D)$. □

4.7 Hom

The notation $\mathrm{Hom}_R(A, B)$ will denote the set of $R-$module homomorphisms $f : A \longrightarrow B$. The is an abelian group under the standard addition (and note that the addition respects the standard function composition of $R-$module homomorphisms.

We consider $R-$module homomorphisms $\gamma : C \longrightarrow A$ and $\xi : B \longrightarrow D$. The map $\eta : \mathrm{Hom}_R(A, B) \longrightarrow \mathrm{Hom}_R(C, D)$ given by

$$f \mapsto \xi f \gamma$$

is an $R-$module homomorphism. We call this the homomorphism induced by ξ and γ. Note that if $B = D$ and $\xi = 1_D$, then the map is $f \mapsto f\gamma$ (denoted $\overline{\gamma}$). If $A = C$ and $\gamma = 1_A$ then the map is $f \mapsto \xi f$ (and is denoted $\overline{\xi}$). We will motly be considering these special cases.

Theorem 4.7.1. *Let R be a ring. The sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$ is exact if and only if for all $R-$modules D the sequence*

$$0 \longrightarrow Hom_R(D, A) \xrightarrow{\overline{f}} Hom_R(D, B) \xrightarrow{\overline{g}} Hom_R(D, C)$$

is exact.

Additionally $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *is exact if and only if for every* $R-$*module* D *the sequence*

$$0 \longrightarrow Hom_R(C, D) \xrightarrow{\overline{g}} Hom_R(B, D) \xrightarrow{\overline{f}} Hom_R(A, D)$$

is exact.

We say that the "Hom functor" is left exact.

We will prove the first statement and leave the proof of the second as an exercise.

Proof. It would probably be helpful to see a diagram of how the induced maps on Hom actually "work". Suppose we have the exact sequence $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$. This sequence induces

$$0 \longrightarrow \mathrm{Hom}_R(C, D) \xrightarrow{\overline{g}} \mathrm{Hom}_R(B, D) \xrightarrow{\overline{f}} \mathrm{Hom}_R(A, D)$$

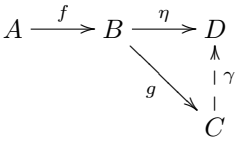
$$\gamma \longmapsto \gamma g$$

$$\eta \longmapsto \eta f$$

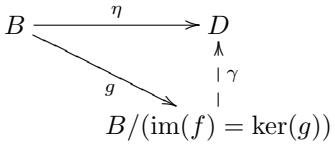
First we will show that $\overline{g}$ is one to one. Assume that γg is the $0-$map. So $\gamma g(b) = 0$ for all $b \in B$. But since g is onto, this means that for all $c \in C$ there exists a $b_c \in B$ such that $g(b_c) = c$. Hecn $\gamma(c) = 0$ for all $c \in C$ (that is γ is the $0-$map) and hence $\overline{g}$ is injective.

We now note that $\overline{f}\overline{g}(\gamma) = \overline{f}(\gamma g) = \gamma f g = 0$ as fg is the $0-$map. Hence we have that $\mathrm{im}(\overline{g}) \subseteq \ker(\overline{f})$. We now need to show the other containment.

Let $\eta \in \ker(\overline{f})$, that is, $\eta f = 0$. Consider the following diagram



basically we have to show the existence of a γ such that $\gamma g = \eta$. As g is onto, we have that $C \cong B/\ker(g) = B/\mathrm{im}(f)$. So we (need to) have



We define γ by $\gamma(b + \ker(g)) = \eta(b)$. Note if $b \in \ker(g) = \text{im}(f)$ then $\eta(b) = \eta f(a) = 0$ so this map is well-defined. It is also easy to verify that this is a homomorphism. Finally note that the diagram commutes since if $b \in B$ then $\gamma g(b) = \gamma(g(b) + \ker(g)) = \eta(b)$.

This shows that the exactness of the original sequence gives the exactness of the "Hom" sequence. The other direction is an exercise.

□

Example 4.7.2. *Hom the sequences of* $\mathbb{Z}-$*modules* $0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}_2 \longrightarrow 0$ *and* $0 \longrightarrow \mathbb{Z} \xrightarrow{incl} \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$.

We will see in the next thereom that split exact sequences are decidedly more well-behaved.

Theorem 4.7.3. *The following conditions on* $R-$*modules are equivalent.*

a) $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ *is split exact.*

b) $0 \longrightarrow Hom_R(D, A) \xrightarrow{\overline{f}} Hom_R(D, B) \xrightarrow{\overline{g}} Hom_R(D, C) \longrightarrow 0$ *is split exact for every* D.

c) $0 \longrightarrow Hom_R(C, D) \xrightarrow{\overline{g}} Hom_R(B, D) \xrightarrow{\overline{f}} Hom_R(A, D) \longrightarrow 0$ *is split exact for every* D.

Proof. We will show the equivalence of a) and c), the other equivalence being left as an exercise.

For the implication a) implies b) if suffices to show that there is an $\overline{h}$ such that $\overline{g}\overline{h}$ is the identity on $\text{Hom}_R(D, C)$. Since the original sequence is split exact there exists $h : C \longrightarrow B$ such that $gh = 1_C$. It is easy to see that the induced homomorphism $\overline{gh} = \overline{g}\overline{h} = 1_{\text{Hom}_R(D,C)}$ hence $\overline{g}$ is onto and the Hom sequence is split exact.

On the other hand, assume that the Hom sequence is split exact for all D. Let $D = C$ and $\phi : C \longrightarrow B$ be such that $\overline{g}(\phi) = 1_C = g\phi$. Note that this implies that $0 \longrightarrow A \longrightarrow B \xrightarrow{g} C \longrightarrow 0$ is split exact. The equivalence of a) and c) is similar.

□

Theorem 4.7.4. *The following conditions on the* $R-$*module* P *are equivalent.*

a) P *is projective.*

b) If $\phi : B \longrightarrow C$ *is onto then* $\overline{\phi} : Hom_R(P, B) \longrightarrow Hom_R(P, C)$ *is onto.*

c) If $0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\phi} C \longrightarrow 0$ *is a short exact sequence then* $0 \longrightarrow Hom_R(P, A) \xrightarrow{\overline{\psi}} Hom_R(P, B) \xrightarrow{\overline{\phi}} Hom_R(P, C) \longrightarrow 0$ *is a short exact sequence.*

Theorem 4.7.5. *The following conditions on the $R-$module I are equivalent.*

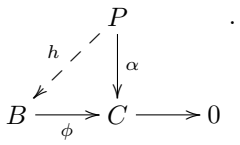
a) I is injective.

b) If $\xi : A \longrightarrow B$ is one to one then $\overline{\xi} : Hom_R(B, I) \longrightarrow Hom_R(A, I)$ is onto.

c) If $0 \longrightarrow A \xrightarrow{\xi} B \xrightarrow{\eta} C \longrightarrow 0$ is a short exact sequence then $0 \longrightarrow Hom_R(C, I) \xrightarrow{\overline{\eta}} Hom_R(B, I) \xrightarrow{\overline{\xi}} Hom_R(A, I) \longrightarrow 0$ is a short exact sequence.

We will prove the first "projective" result.

Proof. For a) implies b) we assume that P is projective and $\phi : B \longrightarrow C$ is onto and $\alpha \in \mathrm{Hom}_R(P, C)$. Consider the diagram



That is there is an h such that $\phi h = \alpha$ and hence $\overline{\phi}$ is onto.

For the implication b) implies a), given $\alpha \in \mathrm{Hom}_R(P, C)$ there exists $h \in \mathrm{Hom}_R(P, B)$ such that $\phi h = \alpha$ which is precisely what it means for P to be projective.

The implication b) implies c) is easy and so we will establish the converse. Suppose $\phi : B \longrightarrow C$ is onto and so we have the short exact sequence $0 \longrightarrow \ker(\phi) \longrightarrow B \longrightarrow C \longrightarrow 0$. This gives rise to the short exact sequence $0 \longrightarrow \mathrm{Hom}_R(P, \ker(\phi)) \longrightarrow \mathrm{Hom}_R(P, B) \longrightarrow \mathrm{Hom}_R(P, C) \longrightarrow 0$. Hence $\overline{\phi}$ is onto.

□

We conclude this section with a final functorial fact about Hom (the proof will be left as an exercise).

Theorem 4.7.6. *Let $A, B, \{A_i | i \in I\}, \{B_j | j \in J\}$ be $R-$modules. Then we have the following isomorphisms.*

a) $Hom_R(\oplus_{i \in I} A_i, B) \cong \prod_{i \in I} Hom_R(A_i, B)$.

b) $Hom_R(A, \prod_{j \in J} B_j) \cong \prod_{j \in J} Hom_R(A, B_j)$.

4.8 The Tensor Product

Although it can be done in much more generality, here we will (at least begin with) the tensor product of modules over a commutative ring with identity. The tensor product can be done in the more general case (but care must be taken using left, right, and bi-modules when necessary). The tensor product is a universal construction (it is the solution to a certain univeral mapping problem involving bilinear maps) and it crops up all over commutative algebra and mathematics in general (Einstein used them for example).

Definition 4.8.1. *Let A, B, C be $R-$ modules. A bilinear map $F : A \times B \longrightarrow C$ is a function such that for all $a, a_i \in A$, $b, b_i \in B$ and $r \in R$ we have*

a) $f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)$.

b) $f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$.

c) $f(ra, b) = f(a, rb) = rf(a, b)$.

We now define the tensor product of two modules.

Definition 4.8.2. *Let A and B be modules over R and let F be the free abelian group on the set $A \times B$. Let K be the subgroup of F generated by all elements of the form*

a) $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$

b) $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$

c) $(ra, b) - (a, rb)$

where $a, a_1, a_2 \in A$, $b, b_1, b_2 \in B$ and $r \in R$.

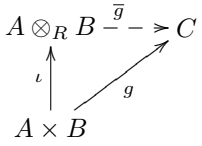
The quotient F/K is called the tensor product (over R) of A and B and is denoted $A \otimes_R B$.

We denote the coset $(a, b) + K$ by $a \otimes b$ (and this is called a tensor). Practically, think of $A \otimes_R B$ as generated by tensors of the form $a \otimes b$ subject the the relations a), b), and c) above.

We also point out that the map $\iota : A \times B \longrightarrow A \otimes_R B$ given by $(a, b) \mapsto a \otimes b$ is a bilinear map (verify this).

Here is a theorem which shows where tensor product "came from." This theorem shows that the tensor product is the unique solution to a mapping problem concerning bilinear maps.

Theorem 4.8.3. *If A, B, C are $R-$modules and $g : A \times B \longrightarrow C$ is a bilinear map then there exists a unique $R-$module homomorphism $\overline{g} : A \otimes_R B \longrightarrow C$ such that $\overline{g}\iota = g$ (where $\iota(a, b) = a \otimes b$ is the canonical bilinear map). $A \otimes_R B$ is uniquely determined up to isomorphism by this property.*



Proof. Let F be free abelian on $A \times B$ and K the subgroup described above. The map $g : A \times B \longrightarrow C$ is bilinear and induces a homomorphism $g^* : F \longrightarrow C$. The fact that g is bilinear shows that g^* takes every element of K to 0 (that is, $K \subseteq \ker(g^*)$). So g^* induces $\overline{g} : F/K \longrightarrow C$, that is $\overline{g} : A \otimes_R B \longrightarrow C$. Note that $\overline{g}\iota(a, b) = \overline{g}(a \otimes b) = g(a, b)$ and hence $\overline{g}\iota = g$.

Now if $h : A \otimes_R B \longrightarrow C$ is another such homomorphism then

$$h(a \otimes b) = g(a, b) = \overline{g}(a \otimes b)$$

and hence h and $\overline{g}$ agree on tensors. Therefore $h = \overline{g}$. □

Here is a useful corollary which we will be building upon.

Corollary 4.8.4. *Let A, A', B, B' be $R-$modules and $f : A \longrightarrow A'$ and $g : B \longrightarrow B'$ be $R-$module homomorphisms, then there exists a unique homomorphism*

$$A \otimes_R B \longrightarrow A' \otimes B'$$

such that $a \otimes b \mapsto f(a) \otimes g(b)$ for all $a \in A$ and $b \in B$.

Proof. One merely needs to verify that $(a, b) \mapsto (f(a) \otimes g(b))$ is a bilinear map. □

This next result is the "right exactness" of tensor product.

Theorem 4.8.5. *If D is an $R-$module then $- \otimes_R D$ is right exact. That is, if*

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is exact, then so is

$$A \otimes_R D \xrightarrow{f \otimes 1_D} B \otimes_R D \xrightarrow{g \otimes 1_D} C \otimes_R D \longrightarrow 0$$

Proof. Since g is onto, every generator $c \otimes d$ of $C \otimes_R D$ is of the form $g(b) \otimes d = (g \otimes 1_D)(b \otimes d)$ and hence every generator of $C \otimes_R D$ is in the image of $g \otimes 1_D$. So $g \otimes 1_D$ is onto.

Now note that $(g \otimes 1_D)((f \otimes 1_D)(\sum_{i=1}^n (a_i \otimes d_i))) = (g \otimes 1_D)(\sum_{i=1}^n (f(a_i) \otimes d_i) = \sum_{i=1}^n (gf(a_i) \otimes d_i)$. Since $gf = 0$, we have that this is a sum of zeros and hence $\text{im}(f \otimes 1_D) \subseteq \ker(g \otimes 1_D)$.

For the last bit, we have to show that $\ker(g \otimes 1_D) \subseteq \text{im}(f \otimes 1_D)$. To this end we consider

$$\pi : B \otimes_R D \longrightarrow (B \otimes_R D)/(\text{im}(f \otimes 1_D)$$

and we note that there exists a homomorphism $\xi : (B \otimes_R D)/(\text{im}(f \otimes 1_D) \longrightarrow C \otimes_R D$ such that $\xi(\pi(b \otimes d)) = (g \otimes 1_D)(b \otimes d) = g(b) \otimes d$. It suffices to show that ξ is an isomorphism.

Consider $\eta : C \times D \longrightarrow (B \otimes_R D)/(\text{im}(f \otimes 1_D)$ given by $(c, d) \mapsto \pi(b \otimes d)$ where $g(b) = c$. (Note if $g(b_1) = c$ then $g(b - b_1) = 0$ and there is an $a \in A$ such that $f(a) = b - b_1$; since $f(a) \otimes d \in \text{im}(f \otimes 1_D$, $\pi(f(a) \otimes d) = 0$ and hence $\pi(b \otimes d) = \pi((f(a) + b_1) \otimes d) = \pi(b_1 \otimes d)$ and so the map is well-defined). It is easy to see that η is bilinear and so there exists a unique $\overline{eta} : C \otimes_R D \longrightarrow (B \otimes_R D)/\text{im}(f \otimes 1_D)$ such that $\overline{\eta}(c \otimes d) = \pi(b \otimes d)$. Hence given any generator $c \times d$, we have

$$\xi\overline{\eta}(c \otimes d) = \xi(\pi(b \otimes d)) = g(b) \otimes d = c \otimes d$$

and hence $\xi\overline{\eta}$ is the identity. In a similar fashion $\overline{\eta}\xi$ is the identity and the proof is complete.

□

Theorem 4.8.6. *There is an $R-$module isomorphism*

$$A \otimes_R R \cong A.$$

Proof. The assignment $(a, r) = ra$ is a bilinear map and so we obtain the $R-$module homomorphism $f : A \otimes_R R \longrightarrow A$ with $f(a \otimes r) = ra$. We now consider the $R-$module homomorphism $g : A \longrightarrow A \otimes_R R$ given by $g(a) = a \otimes 1$. Note that $gf = 1_{A \otimes_R R}$ and $fg = 1_A$, and hence f is an isomorphism. □

Other properties such as (adjoint) associativity will be discussed in exercises. We end with a couple of theorems concerning the behavior of tensor product with free modules.

Theorem 4.8.7. *Let A, A_i, B, B_j be $R-$modules. Then there are isomorphisms*

a) $(\oplus_{i \in I} A_i) \otimes_R B \cong \oplus_{i \in I}(A_i \otimes_R B)$.

b) $A \otimes_R (\oplus_{j \in J} B_j) \cong \oplus_{j \in J}(A \otimes_R B_j)$.

Proof. For a) consider the bilinear map $(\{a_i\}, b) \mapsto \{a_i \otimes b\}$ (note that almost every $a_i = 0$). Show this induces the relevant isomorphism. The proof for b) is simliar. □

Corollary 4.8.8. *Let F be a free $R-$module then*

$$F \otimes_R B \cong \oplus i \in IB$$

where $|I| = rank(F)$.

Proof. Note that $F \otimes_R B \cong (\oplus_{i \in I} R) \otimes_R B \cong \oplus_{i \in I}(R \otimes_R B) \cong \oplus_{i \in I} B$. □

4.9 Flatness

Flatness is a certain generalization of freeness (and projectivity). A flat module is a module that makes tensoring exact. More precisely, we have the following definition.

Definition 4.9.1. *We say that the $R-$module M is flat if given any short exact sequence*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

the corresponding sequence

$$0 \longrightarrow A \otimes_R M \xrightarrow{f \otimes 1_M} B \otimes_R M \xrightarrow{g \otimes 1_M} C \otimes_R M \longrightarrow 0$$

is exact.

We note that since tensoring gets you "most" of the exact sequence for free anyway, an equivalent characterization of a flat module M is one for which given any one to one map $f : A \longrightarrow B$, the corresponding map $f \otimes 1_M : A \otimes_R M \longrightarrow B \otimes_R M$ is one to one.

Here is a theorem that we record to show the pecking order.

Theorem 4.9.2. *Let M be an $R-$module. For the following list of properties, we have the implications a) $\Longrightarrow$ b) $\Longrightarrow$ c).*

a) M is free.

b) M is projective.

c) M is flat.

We leave the proof of the previous result and the next corollary as exercises.

Corollary 4.9.3. *Let M_i be a family of $R-$modules. $\oplus_{i \in I} M_i$ is flat if and only if M_i is flat for each i.*

Bibliography