Module MA3428: Algebraic Topology II
Hilary Term 2011
Part I (Sections 1 and 2)

D. R. Wilkins

Contents

1 Rings and Modules

1.1 Rings and Fields

Definition A *ring* consists of a set R on which are defined operations of *addition* and *multiplication* that satisfy the following properties:

- the ring is an Abelian group with respect to the operation of addition;
- the operation of multiplication on the ring is associative, and thus $x(yz) = (xy)z$ for all elements x, y and z of the ring.
- the operations of addition and multiplication satisfy the *Distributive Law*, and thus $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all elements x, y and z of the ring.

Let R be a ring. Then R is an Abelian group with respect to the operation of addition, and therefore $x + (y + z) = (x + y) + z$ and $x + y = y + x$ for all $x, y \in R$. Also the ring R contains a unique *zero element* 0_R characterized by the property that $x + 0_R = x$ for all $x \in R$. Moreover given any element x of R, there exists a unique element $-x$ of R for which $x + (-x) = 0_R$. This element $-x$ is the *negative* of the element x. An element x of a ring R is said to be *non-zero* if $x \neq 0_R$.

The operation of *subtraction* in a ring R is defined such that $x - y = x + (-y)$ for all $x, y \in R$, where $-y$ is the unique element of R for which $y + (-y) = 0_R$.

Lemma 1.1 *Let R be a ring, and let 0_R be the zero element of R. Then $x0_R = 0_R$, $0_R x = 0_R$, $(-x)y = -(xy)$ and $x(-y) = -(xy)$ for all elements x and y of R.*

Proof Let $x, y \in R$. It follows from the Distributive Law that

$$xy = x(y + 0_R) = xy + x0_R \quad \text{and} \quad yx = (y + 0_R)x = yx + 0_R x.$$

On subtracting xy and yx respectively from both sides of these two equations, we find that $x0_R = 0_R$ and $0_R x = 0_R$. It also follows from the Distributive Law that

$$xy + (-x)y = (x + (-x))y = 0_R y = 0_R$$

and

$$xy + x(-y) = x(y + (-y)) = x0_R = 0_R.$$

Therefore $(-x)y = -(xy)$ and $x(-y) = -(xy)$, as required. ∎

Definition A subset S of a ring R is said to be a *subring* of R if $0_R \in S$, $a + b \in S$, $-a \in S$ and $ab \in S$ for all $a, b \in S$, where 0_R denotes the zero element of the ring R.

Definition A ring R is said to be *commutative* if $xy = yx$ for all $x, y \in R$.

Not every ring is commutative: an example of a non-commutative ring is provided by the ring of $n \times n$ matrices with real or complex coefficients when $n > 1$.

Definition A ring R is said to be *unital* if it possesses a (necessarily unique) non-zero multiplicative identity element 1_R satisfying $1_R x = x = x 1_R$ for all $x \in R$.

Definition A unital commutative ring R is said to be an *integral domain* if the product of any two non-zero elements of R is itself non-zero.

Let R be an integral domain. We define $n.r$ for all integers n and elements r of R so that $0.r = 0_R$, where 0_R is the zero element of R, and $(n + 1).r = n.r + r$ for all integers n. Thus

$$1.r = r, \quad 2.r = r + r, \quad 3.r = r + r + r, \quad \text{etc.},$$

and $(-n).r = -(n.r)$ for all integers n. Now $\{n \in \mathbb{Z} : n.1_R = 0_R\}$ is a subgroup of the group $\mathbb{Z}$ of integers. A basic result of number theory therefore ensures that there exists a unique non-negative integer p such that

$$\{n \in \mathbb{Z} : n.1_R = 0_R\} = p\mathbb{Z},$$

where $p\mathbb{Z}$ denotes the subgroup of $\mathbb{Z}$ consisting of all integers that are divisible by the non-negative integer p. This non-negative integer p is the *characteristic* $\operatorname{char} R$ of the ring.

Lemma 1.2 *Let R be an integral domain for which $\operatorname{char} R = 0$, where $\operatorname{char} R$ denotes the characteristic of R. Then $n.r \neq 0_R$ for all non-zero elements r of R, and for all non-zero integers n. Thus if $r \in R$, $m, n \in N$, $r \neq 0_R$ and $m \neq n$ then $m.r \neq n.r$.*

Proof If $\operatorname{char} R = 0$ then $n.1_R \neq 0_R$ for all non-zero integers n. Now it follows from the Distributive Law and the definition of $n.r$ that $n.r = (n.1_R)r$ for all $n \in \mathbb{Z}$ and $r \in R$. Thus if $n \neq 0$ and $r \neq 0_R$ then $n.r$ is the product of two non-zero elements of the integral-domain R, and therefore $n.r \neq 0_R$. It follows that if $r \in R$, $m, n \in N$, $r \neq 0_R$ and $m \neq n$ then $(m - n).r \neq 0_R$, and therefore $m.r \neq n.r$, as required. ∎

Lemma 1.3 *Let R be an integral domain for which* $\operatorname{char} R = p$*, where $p > 0$ and where* $\operatorname{char} R$ *denotes the characteristic of R. Then the characteristic p of R is a prime number. Moreover let $m, n \in \mathbb{Z}$ and $r \in R$, where $r \neq 0_R$. Then $m.r = n.r$ if and only if $n - m$ is divisible by the prime number p.*

Proof If $p > 0$, where $p = \operatorname{char} R$ then p is the smallest positive integer for which $p.1_R = 0_R$. Suppose that $p = jk$, where j and k are positive integers. Then it follows from the Distributive Law that

$$(j.1_R)(k.1_R) = (jk).1_R = p.1_R = 0_R.$$

But R is an integral domain, and therefore the product of two non-zero elements of R is always non-zero. We conclude therefore that either $j.1_R = 0_R$, in which case p divides j, or else $k.1_R = 0_R$, in which case p divides k. Thus p cannot be factored as the product of two positive integers that are both strictly less than p, and therefore the characteristic p of the integral domain R is a prime number.

Let $m, n \in \mathbb{Z}$ and $r \in R$, where $r \neq 0_R$. Then $n.r - m.r = (n - m).r = ((n - m).1_R)r$. Thus if $m.r = n.r$ then $((n - m).1_R)r = 0_R$. But $r \neq 0_R$, and the product of any two non-zero elements of the integral domain R is always non-zero. It follows that $(n - m).1_R = 0_R$, and therefore $n - m$ is divisible by the characteristic p of the integral domain R, as required. ∎

Definition A *field* consists of a set on which are defined operations of *addition* and *multiplication* that satisfy the following properties:

- the field is an Abelian group with respect to the operation of addition;
- the non-zero elements of the field constitute an Abelian group with respect to the operation of multiplication;
- the operations of addition and multiplication satisfy the *Distributive Law*, and thus $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all elements x, y and z of the field.

An examination of the relevant definitions shows that a unital commutative ring R is a field if and only if, given any non-zero element x of R, there exists an element x^{-1} of R such that $xx^{-1} = 1_R$. Moreover a ring R is a field if and only if the set of non-zero elements of R is an Abelian group with respect to the operation of multiplication.

Lemma 1.4 *A field is an integral domain.*

Proof A field is a unital commutative ring. Let x and y be non-zero elements of a field K. Then there exist elements x^{-1} and y^{-1} of K such that $xx^{-1} = 1_R$ and $yy^{-1} = 1_R$. Then $xyy^{-1}x^{-1} = 1_R$. It follows that $xy \neq 0_R$, since $0_R(y^{-1}x^{-1}) = 0_R$ and $1_R \neq 0_R$. ∎

The set $\mathbb{Z}$ of integers is an integral domain with respect to the usual operations of addition and multiplication. The sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ of rational, real and complex numbers are fields.

1.2 Left Modules

Definition Let R be a unital ring. A set M is said to be a *left module over the ring* R (or *left* R*-module*) if

(i) given any $x, y \in M$ and $r \in R$, there are well-defined elements $x + y$ and rx of M,

(ii) M is an Abelian group with respect to the operation $+$ of addition,

(iii) the identities

$$r(x + y) = rx + ry, \qquad (r + s)x = rx + sx,$$

$$(rs)x = r(sx), \qquad 1_R x = x$$

are satisfied for all $x, y \in M$ and $r, s \in R$, where 1_R denotes the multiplicative identity element of the ring R.

Let M be a left module over a unital ring R. Then M is an Abelian group with respect to the operation of addition, and therefore $x+(y+z) = (x+y)+z$ and $x+y = y+x$ for all $x, y \in M$. Also the left module M contains a unique *zero element* 0_M characterized by the property that $x+0_M = x$ for all $x \in M$. Moreover given any element x of M, there exists a unique element $-x$ of M for which $x + (-x) = 0_M$. This element $-x$ is the *negative* of the element x. An element x of a left module M is said to be *non-zero* if $x \neq 0_M$.

The operation of *subtraction* in a left module M is defined such that $x - y = x + (-y)$ for all $x, y \in M$, where $-y$ is the unique element of M for which $y + (-y) = 0_M$.

Lemma 1.5 *Let M be a left module over a unital ring R, and let and let 0_R and 0_M be the zero elements of R and M respectively. Then $0_R x = 0_M$, $r0_M = 0_M$ and $(-r)x = r(-x) = -(rx)$ for all $r \in R$ and $x \in M$.*

Proof Let $r \in R$ and $x \in M$. Then

$$rx = (r + 0_R)x = rx + 0_R x.$$

On subtracting rx from both sides of this equation, we find that $0_R x = 0_M$. Similarly

$$rx = r(x + 0_M) = rx + r0_M,$$

and therefore $r0_M = 0_M$. Also

$$(-r)x + rx = ((-r) + r)x = 0_R x = 0_M$$

and

$$r(-x) + rx + r((-x) + x) = r0_M = 0_M,$$

and therefore $(-r)x = r(-x) = -(rx)$, as required. ∎

1.3 Modules over a Unital Commutative Ring

We have defined the concept of a *left module* over a unital ring. There is a corresponding concept of a right module. A right module is an Abelian group with respect to the operation of addition. Furthermore elements of a right module M over a unital ring R may be multiplied on the right by elements of the ring R. Moreover, in order that M be a right module over a unital ring R, the following identities must be satisfied for all $x, y \in M$ and $r, s \in R$:

$$(x + y)r = xr + yr, \qquad x(r + s) = xr + xs,$$

$$x(rs) = (xr)s \quad \text{and} \quad x1_R = x,$$

where 1_R denotes the multiplicative identity element of the ring R.

If the multiplication operation on the ring R is non-commutative, then the concept of *right module* is essentially distinct from that of *left module* over this ring R. But if the unital ring R is commutative then there is no essential distinction between left modules and right modules over R: in this case it is purely a question of context, tradition and convenience whether the product of an element x of the module and an element r of the ring is denoted by rx or by xr. Accordingly both left and right modules over a unital commutative ring may be described as *modules* over that ring.

Example If K is a field, then the definition of a module over the field K coincides with that of a vector space over K. Thus vector spaces are examples of modules where the ring of coefficients is a field.

Example Let $(M, +)$ be an Abelian group, and let $x \in M$. If n is a positive integer then we define nx to be the sum $x + x + \cdots + x$ of n copies of x. If n is a negative integer then we define $nx = -(|n|x)$, and we define $0x = 0_M$, where 0_M denotes the zero element of the Abelian group M. This enables us to regard any Abelian group as a module over the ring $\mathbb{Z}$ of integers. Conversely, any module over the ring $\mathbb{Z}$ of integers is also an Abelian group.

Example Any unital commutative ring can be regarded as a module over itself in the obvious fashion. The operation of left multiplication of elements of a unital commutative ring R by elements of R itself coincides with the operation of multiplication defined on the ring R.

Example Let K be a field, and let $K[X]$ denote the ring of polynomials in a single indeteminant with coefficients in the field X. The ring $K[X]$ is a unital commutative ring, and elements of $K[X]$ are polynomials of the form

$$a_0 + a_1X + a_2X^2 + \cdots + a_dX^d,$$

where $a_0, a_1, \ldots, a_d \in K$. The operations of addition, subtraction and multiplication of such polynomials are defined in the usual fashion. Let V be a vector space over the field K, and let $T: V \to V$ be a linear operator on V. Define $p(X)v = p(T)v$ for all $p(X) \in K[X]$, so that

$$(a_0 + a_1X + a_2X^2 + \cdots + a_dX^d)v = a_0v + a_1Tv + a_2T^2v + \cdots + a_dT^dv$$

for all $v \in V$ and $a_0, a_1, \ldots, a_d \in K$. Then this operation of multiplication of elements of the vector space V by polynomials with coefficients in the field K gives the vector space V the structure of a module over the polynomial ring $K[X]$. Moreover any module over the polynomial ring $K[X]$ can be described in this fashion. For if V is a module over $K[X]$ then V is a vector space over the field K: each element of the field K may be regarded as a constant polynomial, and therefore the algebraic operation under which elements of the module V are multiplied on the left by polynomials restricts to an operation whereby elements of V are multiplied on the left by constant polynomials, and accordingly by elements of the field K. Moreover the function that sends $v \in V$ to the product Xv obtained on left multiplying v by the polynomial X (where $X = 1_RX$) is a linear transformation $T: V \to V$, and basic properties of modules then ensure that $p(X)v = p(T)v$ for all $p(X) \in K[X]$.

1.4 Submodules and Quotient Modules

Definition Let R be a unital ring, and let M be a left R-module. A non-empty subset L of M is said to be a *submodule* of M if $x + y \in L$ and $rx \in L$ for all $x, y \in L$ and $r \in R$.

Let M be a left module over a unital ring R, and let L be a submodule of M. Then L contains at least one element x, and therefore contains the zero element 0_M of M, because $0_M = 0_R x$. Thus every submodule of a left module contains the zero element of that module. Also $-x \in L$ for all $x \in L$, because $-x = (-1_R)x$, where 1_R denotes the multiplicative identity element of the unital ring R.

Example A subset L of a ring R is said to be a *left ideal* of R if $0_R \in L$, $-x \in L$, $x + y \in L$ and $rx \in L$ for all $x, y \in L$ and $r \in R$. Any unital ring R may be regarded as a left R-module, where multiplication on the left by elements of R is defined in the obvious fashion using the multiplication operation on the ring R itself. A subset of R is then a submodule of R (when R is regarded as a left module over itself) if and only if this subset is a left ideal of R.

Given any submodule L of the left R-module M, we denote by M/L the set of cosets of L in M. These cosets are the subsets of M that are of the form $L + x$ for some $x \in M$, where

$$L + x = \{l + x : l \in L\}.$$

Let x and y be elements of M. If $y \in L + x$ then $y = l_y + x$ for some $l_y \in L$. But then $x = (-l_y) + y$, and therefore $x \in L + y$. Moreover

$$l + y = l + l_y + x \in L + x$$

and

$$l + x = l + (-l_y) + y \in L + y$$

for all $l \in L$. Thus if $y \in L + x$ then $L + y = L + x$. It follows that $L + x = L + y$ if and only if $x - y \in L$.

Let $x, x', y, y' \in M$ and $r \in R$. Suppose that $L + x = L + x'$ and $L + y = L + y'$. Then $x' - x \in L$ and $y' - y \in L$. But then

$$(x + y) - (x' + y') = (x - x') + (y - y') \in L,$$

because the operation of addition on M is both commutative and associative, and

$$rx - rx' = r(x - x') \in L,$$

and therefore $L + (x + y) = L + (x' + y')$ and $L + rx = L + rx'$. It follows that there is a well-defined operation of addition on the set M/L of cosets of L in M, where

$$(L + x) + (L + y) = L + (x + y)$$

for all $x, y \in M$. This addition operation on M/L is associative and commutative. Also $L+(L+x) = (L+0_M)+(L+x) = L+x$ and $(L+(-x))+(L+x) = L + ((-x) + x) = L + 0_M = L$ for all $x \in M$. It follows that the set M/L of cosets of L in M is an Abelian group with respect to the operation of addition of cosets. We define $r(L + x) = L + rx$ for all $r \in R$. Then

$$\begin{aligned} r((L + x) + (L + y)) &= r(L + (x + y)) = L + r(x + y) \\ &= L + (rx + ry) = (L + rx) + (L + ry) \\ &= r(L + x) + r(L + y), \\ (r + s)(L + x) &= L + (r + s)x = L + (rx + sx) \\ &= (L + rx) + (L + sx) \\ &= r(L + x) + s(L + x), \\ (rs)(L + x) &= L + (rs)x = L + r(sx) = r(L + sx) \\ &= r(s(L + x)), \end{aligned}$$

and

$$1_R(L + x) = L + 1_R x = L + x$$

for all $r, s \in R$ and $x, y \in M$. It follows that the set M/L of left cosets of L in M is itself a left module over the unital ring R.

Definition Let M be a left module over a unital ring R, and let L be a submodule of M. The corresponding *quotient module* M/L is the left R-module M/L whose elements are the cosets of L in M, with operations of addition of cosets and left multiplication of cosets by elements of the ring R defined such that

$$(L + x) + (L + y) = L + x + y \quad \text{and} \quad r(L + x) = L + rx$$

for all $x, y \in M$ and $r \in R$.

1.5 Homomorphisms of Left Modules

Definition Let M and N be left modules over some unital ring R. A function $\varphi: M \to N$ is said to be a *homomorphism of left R-modules* if $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(rx) = r\varphi(x)$ for all $x, y \in M$ and $r \in R$. A homomorphism of R-modules is said to be an isomorphism if it is invertible.

Let M and N be left modules over a unital ring R. A homomorphism $\varphi: M \to N$ from M to N is said to be a *monomorphism* if it is injective. A

homomorphism $\varphi: M \to N$ from M to N is said to be a *epimorphism* if it is surjective. A homomorphism $\varphi: M \to N$ from M to N is said to be an *isomorphism* if it is bijective. A homomorphism $\varphi: M \to M$ from M to itself is referred to as an *endomorphism* of M. An isomorphism $\varphi: M \to M$ from M to itself is referred to as an *automorphism* of M.

Let $\varphi: M \to N$ be an isomorphism from M to N. Then the function φ has a well-defined inverse $\varphi^{-1}: N \to M$. Let $u, v \in N$, and let $x = \varphi^{-1}(u)$ and $y = \varphi^{-1}(v)$. Then $\varphi(x) = u$ and $\varphi(y) = v$, and therefore

$$\varphi(x + y) = \varphi(x) + \varphi(y) = u + v \quad \text{and} \quad \varphi(rx) = r\varphi(x) = ru.$$

It follows that

$$\varphi^{-1}(u + v) = \varphi^{-1}(u) + \varphi^{-1}(v) \quad \text{and} \quad \varphi^{-1}(ru) = r\varphi^{-1}(u).$$

Thus the inverse $\varphi^{-1}: N \to M$ of any left R-module isomorphism $\varphi: M \to N$ is itself a left R-module isomorphism.

Lemma 1.6 *Let M and N be left modules over a unital ring R, and let $\varphi: M \to N$ be a left R-module homomorphism from M to N. Then $\varphi(0_M) = 0_N$, where 0_M and 0_N denote the zero elements of the left modules M and N respectively. Moreover $\varphi(-x) = -\varphi(x)$ for all $x \in M$.*

Proof Let $x \in M$. Then

$$\varphi(x) = \varphi(x + 0_M) = \varphi(x) + \varphi(0_M).$$

On subtracting $\varphi(x)$ from both sides of this identity, we find that $0_N = \varphi(0_M)$. It follows that

$$\varphi(x) + \varphi(-x) = \varphi(x + (-x)) = \varphi(0_M) = 0_N,$$

and therefore $\varphi(-x) = -\varphi(x)$, as required. ∎

Definition Let M and N be left modules over some unital ring R, and let $\varphi: M \to N$ be a left R-module homomorphism. The *kernel* $\ker \varphi$ of the homomorphism φ is defined so that

$$\ker \varphi = \{x \in M : \varphi(x) = 0_N\},$$

where 0_N denotes the zero element of the module N.

The kernel $\ker\varphi$ of a left R-module homomorphism $\varphi\colon M \to N$ is itself a left R-module. Indeed let $x, y \in \ker\varphi$ and $r \in R$. Then

$$\varphi(x+y) = \varphi(x) + \varphi(y) = 0_N + 0_N = 0_N$$

and

$$\varphi(rx) = r\varphi(x) = r0_N = 0_N,$$

and therefore $x + y \in \ker\varphi$ and $rx \in \ker\varphi$.

The *image* or *range* $\varphi(M)$ of a left R-module homomorphism $\varphi\colon M \to N$ is defined such that

$$\varphi(N) = \{\varphi(x) : x \in M\}.$$

The image of any left R-module homomorphism is itself a left R-module.

Proposition 1.7 *Let M and N be left modules over a unital ring R, let $\varphi\colon M \to N$ be a left R-module homomorphism from M and N, and let L be a submodule of M. Suppose that $L \subset \ker\varphi$. Then $\varphi\colon M \to N$ induces a homomorphism $\overline{\varphi}\colon M/L \to N$ defined on the quotient module M/L, where $\overline{\varphi}(L+x) = \varphi(x)$ for all $x \in M$. This induced homomorphism is injective if and only if $L = \ker\varphi$.*

Proof Let $x, x' \in M$. Then $L + x = L + x'$ if and only if $x' - x \in L$. Also $\varphi(x'-x) = \varphi(x') - \varphi(x)$, and therefore $\varphi(x) = \varphi(x')$ if and only if $x' - x \in \ker\varphi$. But $L \subset \ker\varphi$. It follows that if $L+x = L+x'$ then $\varphi(x) = \varphi(x')$, and therefore there exists a well-defined function $\overline{\varphi}\colon M/L \to N$ characterized by the property that $\overline{\varphi}(L+x) = \varphi(x)$ for all $x \in M$. The function from M/L to N characterized by this property is uniquely determined. Moreover the function $\overline{\varphi}$ is injective if and only if $L + x = L + x'$ whenever $\varphi(x) = \varphi(x')$. It follows that $\overline{\varphi}\colon M/L \to N$ is injective if and only if $L = \ker\varphi$.

Let $x, y \in M$. Then

$$\begin{aligned}\overline{\varphi}((L+x)+(L+y)) &= \overline{\varphi}(L+x+y) = \varphi(x+y) = \varphi(x) + \varphi(y) \\ &= \overline{\varphi}(L+x) + \overline{\varphi}(L+y).\end{aligned}$$

Also

$$\overline{\varphi}(r(L+x)) = \overline{\varphi}(L+rx) = \varphi(rx) = r\varphi(x)$$

for all $r \in R$. It follows that $\overline{\varphi}\colon M/L \to N$ is a homomorphism of left R-modules with the required properties. ∎

The following corollary follows immediately on applying Proposition 1.7.

Corollary 1.8 *Let M and N be left modules over a unital ring R, and let $\varphi\colon M \to N$ be a left R-module homomorphism from M and N. Then $\varphi(M) \cong M/\ker\varphi$.*

1.6 Direct Sums of Left Modules

Definition Let $M_1, M_2, \ldots, M_k$ be left modules over a unital ring R. The *direct sum* $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ of the modules $M_1, M_2, \ldots, M_k$ is defined to be the set of ordered k-tuples $(x_1, x_2, \ldots, x_k)$, where $x_i \in M_i$ for $i = 1, 2, \ldots, k$. This direct sum is itself a left R-module, where

$$\begin{aligned}(x_1, x_2, \ldots, x_k) + (y_1, y_2, \ldots, y_k) &= (x_1 + y_1, x_2 + y_2, \ldots, x_k + y_k),\\ r(x_1, x_2, \ldots, x_k) &= (rx_1, rx_2, \ldots, rx_k)\end{aligned}$$

for all $x_i, y_i \in M_i$ and $r \in R$.

Definition Let R be a unital ring, and let n be a positive integer. We define the left R-module R^n to be the direct sum of n copies of the ring R. The elements of this left R-module R^n are thus represented as n-tuples $(r_1, r_2, \ldots, r_n)$ whose components are elements of the ring R.

Definition Let M be a left module over some unital ring R. Given any subset X of M, the submodule of M generated by the set X is defined to be the intersection of all submodules of M that contain the set X. It is therefore the smallest submodule of M that contains the set X. A left R-module M is said to be *finitely-generated* if it is generated by some finite subset of itself.

Lemma 1.9 *Let M be a left module over some unital ring R. Then the submodule of M generated by some finite subset $\{x_1, x_2, \ldots, x_k\}$ of M consists of all elements of M that are of the form*

$$r_1x_1 + r_2x_2 + \cdots + r_kx_k$$

for some $r_1, r_2, \ldots, r_k \in R$.

Proof The subset of M consisting of all elements of M of this form is clearly a submodule of M. Moreover it is contained in every submodule of M that contains the set $\{x_1, x_2, \ldots, x_k\}$. The result follows. ∎

1.7 Right Modules

Definition Let R be a unital ring. A set M is said to be a *right module over R* (or *right R-module*) if

(i) given any $x, y \in M$ and $r \in R$, there are well-defined elements $x + y$ and xr of M,

(ii) M is an Abelian group with respect to the operation $+$ of addition,

(iii) the identities

$$(x+y)r = xr + yr, \qquad x(r+s) = xr + xs,$$

$$x(rs) = (xr)s, \qquad x1_R = x$$

are satisfied for all $x, y \in M$ and $r, s \in R$, where 1_R denotes the multiplicative identity element of the ring R.

Let R be a unital ring that is not necessarily commutative, and let $+$ and $\times$ denote the operations of addition and multiplication defined on R. We denote by R^{op} the ring $(R, +, \times^{\mathrm{op}})$, where the underlying set of R^{op} is R itself, the operation of addition on R^{op} coincides with that on R, but where the operation of multiplication in the ring R^{op} is the operation $\times^{\mathrm{op}}$ defined so that $r \times^{\mathrm{op}} s = s \times r$ for all $r, s \in R$. Note that the multiplication operation on the ring R^{op} coincides with that on the ring R if and only if the ring R is commutative.

Any right module over the ring R may be regarded as a left module over the ring R^{op}. Indeed let M_R be a right R-module, and let $r.x = xr$ for all $x \in M_R$ and $r \in R$. Then

$$r.(s.x) = r.(xs) = (xs)r = x(s \times r) = x(r \times^{\mathrm{op}} s) = (r \times^{\mathrm{op}} s).x$$

for all $x \in M_R$ and $r, s \in R$. Also all other properties required of left modules over the ring R^{op} are easily seen to be satisfied. It follows that any general results concerning left modules over unital rings yield corresponding results concerning right modules over unital rings.

Note that if the unital ring R is commutative then $r \times^{\mathrm{op}} s = s \times r = r \times s$ for all $r, s \in R$, and therefore the multiplication operations $\times^{\mathrm{op}}$ and $\times$ coincide. Thus if R is a unital commutative ring then the identity function of R is an isomorphism between the rings R and R^{op}, and thus R^{op} is the same ring as R. It follows that any right module over the ring R may be regarded as a left module over R, and vice versa.

2 Free Modules

2.1 Linear Independence in Modules

Let M be a left module over a unital ring R, and let $x_1, x_2, \ldots, x_k$ be elements of M. A *linear combination* of the elements $x_1, x_2, \ldots, x_k$ with *coefficients* $r_1, r_2, \ldots, r_k$ is an element of M that is represented by means of an expression of the form

$$r_1x_1 + r_2x_2 + \cdots + r_kx_k,$$

where $r_1, r_2, \ldots, r_k$ are elements of the ring R.

Definition Let M be a left module over a unital ring R. The elements of a subset X of M are said to be *linearly dependent* if there exist distinct elements $x_1, x_2, \ldots, x_k$ of X (where $x_i \neq x_j$ for $i \neq j$) and elements $r_1, r_2, \ldots, r_k$ of the ring R, not all zero, such that

$$r_1x_1 + r_2x_2 + \cdots + r_kx_k = 0_M,$$

where 0_M denotes the zero element of the module M.

The elements of a subset X of M are said to be *linearly independent* over the ring R if they are not linearly dependent over R.

Let M be a left module over a unital ring R, and let X be a (finite or infinite) subset of M. The set X generates M as a left R-module if and only if, given any non-zero element m of M, there exist $x_1, x_2, \ldots, x_k \in X$ and $r_1, r_2, \ldots, r_k \in R$ such that

$$m = r_1x_1 + r_2x_2 + \cdots + r_kx_k$$

(see Lemma 1.9). In particular, a left module M over a unital ring R is generated by a finite set $\{x_1, x_2, \ldots, x_k\}$ if and only if any element of M can be represented as a linear combination of $x_1, x_2, \ldots, x_k$ with coefficients in the ring R.

A left module over a unital ring is freely generated by the empty set if and only if it is the zero module.

Definition Let M be a left module over a unital ring R, and let X be a subset of M. The left module M is said to be *freely generated* by the set X if the following conditions are satisfied:

(i) the elements of X are linearly independent over the ring R;

(ii) the module M is generated by the subset X.

Definition A left module over a unital ring is said to be *free* if there exists some subset of the module which freely generates the module.

Definition Let M be a left module over a unital ring R. Elements

$$x_1, x_2, \ldots, x_k$$

of M are said to constitute a *free basis* of M if these elements are distinct, and if the left R-module M is freely generated by the set $\{x_1, x_2, \ldots, x_k\}$.

Example Let K be a field, let V be a finite-dimensional vector space over K, and let $b_1, b_2, \ldots, b_n$ be a basis of V. Then V is a left K-module, and moreover V is freely generated by the set B, where $B = \{b_1, b_2, \ldots, b_n\}$. Indeed, given any vector space W over K, and given any function $f\colon B \to W$, there is a unique linear transformation $\varphi\colon V \to W$ that extends f. Moreover

$$\varphi\left(\sum_{j=1}^{n} x_j b_j\right) = \sum_{j=1}^{n} x_j f(b_j)$$

for all $x_1, x_2, \ldots, x_n \in K$. This linear transformation is a homomorphism of left modules over the field K.

Lemma 2.1 *Let M be a left module over an unital ring R. Elements*

$$x_1, x_2, \ldots, x_k$$

of M constitute a free basis of that left module if and only if, given any element m of M, there exist uniquely determined elements $r_1, r_2, \ldots, r_k$ of the ring R such that

$$m = r_1 x_1 + r_2 x_2 + \cdots + r_k x_k.$$

Proof First suppose that $x_1, x_2, \ldots, x_k$ is a list of elements of M with the property that, given any element m of M, there exist uniquely determined elements $r_1, r_2, \ldots, r_k$ of R such that

$$m = r_1 x_1 + r_2 x_2 + \cdots + r_k x_k.$$

Then the elements $x_1, x_2, \ldots, x_k$ generate M. Also the uniqueness of the coefficients $r_1, r_2, \ldots, r_k$ ensures that the zero element 0_M of M cannot be expressed as a linear combination of $x_1, x_2, \ldots, x_k$ unless the coeffients involved are all zero. Therefore these elements are linearly independent and thus constitute a free basis of the left module M.

Conversely suppose that $x_1, x_2, \ldots, x_k$ is a free basis of M. Then any element of M can be expressed as a linear combination of the free basis vectors. We must prove that the coefficients involved are uniquely determined. Let $r_1, r_2, \ldots, r_k$ and $s_1, s_2, \ldots, s_k$ be elements of the coefficient ring R satisfying

$$r_1x_1 + r_2x_2 + \cdots + r_kx_k = s_1x_1 + s_2x_2 + \cdots + s_kx_k.$$

Then

$$(r_1 - s_1)x_1 + (r_2 - s_2)x_2 + \cdots + (r_k - s_k)x_k = 0_M.$$

But then $r_j - s_j = 0$ and thus $r_j = s_j$ for $j = 1, 2, \ldots, n$, since the elements of any free basis are required to be linearly independent. This proves that any element of M can be represented in a unique fashion as a linear combination of the elements of a free basis of M, as required. ∎

Proposition 2.2 *Let M be a free left module over a unital ring R, and let X be a subset of M that freely generates M. Then, given any left R-module N, and given any function $f\colon X \to N$ from X to N, there exists a unique left R-module homomorphism $\varphi\colon M \to N$ such that $\varphi|X = f$.*

Proof We first prove the result in the special case where M is freely generated by a finite set X. Thus suppose that $X = \{x_1, x_2, \ldots, x_k\}$, where the elements $x_1, x_2, \ldots, x_k$ are distinct. Then these elements are linearly independent over R and therefore, given any element m of M, there exist uniquely-determined elements $r_1, r_2, \ldots, r_k$ of R such that

$$m = r_1x_1 + r_2x_2 + \cdots + r_kx_k.$$

(see Lemma 2.1). It follows that, given any left R-module N, and given any function $f\colon X \to N$ from X to N, there exists a function $\varphi\colon M \to N$ from M to N which is characterized by the property that

$$\varphi(r_1x_1 + r_2x_2 + \cdots + r_kx_k) = r_1f(x_1) + r_2f(x_2) + \cdots + r_kf(x_k).$$

for all $r_1, r_2, \ldots, r_k$. Moreover this function is an R-module homomorphism, and is the unique R-module homomorphism from M to N that extends $f\colon X \to N$.

Now consider the case when M is freely generated by an infinite set X. Let N be an R-module, and let $f\colon X \to N$ be a function from X to N. For each finite subset Y of X, let M_Y denote the submodule of M that is generated by Y. Then the result we have just proved for modules freely generated by finite sets ensures that there exists a unique R-module homomorphism $\varphi_Y\colon M_Y \to N$ from M_Y to N such that $\varphi_Y(x) = f(x)$ for all $x \in Y$.

Let Y and Z be finite subsets of X, where $Y \cap Z \neq \emptyset$. We claim that $M_Y \cap M_Z = M_{Y \cap Z}$. Clearly $M_{Y \cap Z} \subset M_Y$ and $M_{Y \cap Z} \subset M_Z$. Let $Y \cup Z = \{x_1, x_2, \ldots, x_k\}$, where $x_1, x_2, \ldots, x_k$ are distinct. Then, given any element m of $M_Y \cap M_Z$, there exist uniquely-determined elements $r_1, r_2, \ldots, r_k$ of R such that

$$m = r_1 x_1 + r_2 x_2 + \cdots + r_k x_k.$$

But this element m is expressible as a linear combination of elements of Y alone, and as a linear combination of elements of Z alone. Therefore, for each index i between 1 and k, the corresponding coefficient r_i is zero unless both $x_i \in Y$ and $x_i \in Z$. But this ensures that x is expressible as a linear combination of elements that belong to $Y \cap Z$. This verifies that $M_Y \cap M_Z = M_{Y \cap Z}$.

Now there exist unique left R-module homomorphisms $\varphi_Y \colon M_Y \to N$ and $\varphi_Z \colon M_Z \to N$ from M_Y and M_Z respectively to N such that $\varphi_Y(x) = f(x)$ for all $x \in Y$ and $\varphi_Z(x) = f(x)$ for all $x \in Z$. Then the restrictions of these left R-module homomorphisms to $M_{Y \cap Z}$ are left R-module homomorphisms from $M_{Y \cap Z}$ to N that extend $f|Y \cap Z \colon Y \cap Z \to N$. But we have shown that any extension of this function to an R-module homomorphism from $M_{Y \cap Z}$ to N is uniquely-determined. But $M_{Y \cap Z} = M_Y \cap M_Z$. Therefore

$$\varphi_Y | M_Y \cap M_Z = \varphi_Z | M_Y \cap M_Z = \varphi_{Y \cap Z}.$$

Let $m \in M$. Then m can be represented as a linear combination of the elements of some finite subset Y of X with coefficients in the ring R. But then $m \in M_Y$. It follows that M is the union of the submodules M_Y as Y ranges over all finite subsets of the generating set X.

Now there is a well-defined function $\varphi \colon M \to N$ characterized by the property that $\varphi(m) = \varphi_Y(m)$ whenever m belongs to M_Y for some finite subset Y of X. Indeed suppose that some element m of M belongs to both M_Y and M_Z, where Y and Z are finite subsets of M. Then $m \in M_{Y \cap Z}$, since we have shown that $M_Y \cap M_Z = M_{Y \cap Z}$. But then $\varphi_Y(m) = \varphi_{Y \cap Z}(m) = \varphi_Z(m)$. This result ensures that the homomorphisms $\varphi \colon M_Y \to N$ defined on the submodules M_Y of M generated by finite subsets Y of X can be pieced together to yield the required function $\varphi \colon M \to N$. Moreover, given elements x and y of M, there exists some finite subset Y of M such that $x \in M_Y$ and $y \in M_Y$. Then

$$\varphi(x + y) = \varphi_Y(x + y) = \varphi_Y(x) + \varphi_Y(y) = \varphi(x) + \varphi(y),$$

and

$$\varphi(rx) = \varphi_Y(rx) = r\varphi_Y(x) = r\varphi(x)$$

for all $r \in R$. Thus the function $\varphi: M \to N$ is a left R-module homomorphism. The uniqueness of the left R-module homomorphisms φ_Y then ensures that $\varphi: M \to N$ is the unique left R-module homomorphism from M to N that extends $f: X \to N$, as required. ∎

Proposition 2.3 *Let R be a unital ring, let M and N be left R-modules, let F be a free left R-module, let $\pi: M \to N$ be a surjective left R-module homomorphism, and let $\varphi: F \to N$ be a left R-module homomorphism. Then there exists an left R-module homomorphism $\psi: F \to M$ such that $\varphi = \pi \circ \psi$.*

Proof Let X be a subset of the free left R-module F that freely generates F. Now, because the left R-module homomorphism $\pi: M \to N$ is surjective, there exists a function $f: F \to M$ such that $\pi(f(x)) = \varphi(x)$ for all $x \in X$. It then follows from Proposition 2.2 that there exists a left R-module homomorphism $\psi: F \to M$ such that $\psi(x) = f(x)$ for all $x \in X$. Then $\pi(\psi(x)) = \pi(f(x)) = \varphi(x)$ for all $x \in X$. But it also follows from Proposition 2.2 that any left R-module homomorphism from F to N that extends $\varphi|X \to X \to N$ is uniquely determined. Therefore $\pi \circ \psi = \varphi$, as required. ∎

Proposition 2.4 *Let R be a unital ring, let M be a left R-module, let F be a free left R-module and let $\pi: M \to F$ be a surjective left R-module homomorphism. Then $M \cong \ker \pi \oplus F$.*

Proof It follows from Proposition 2.3 (applied to the identity automorphism of F) that there exists a left R-module homomorphism $\psi: F \to M$ with the property that $\pi(\psi(f)) = f$ for all $f \in F$. Let $\theta: \ker \pi \oplus F \to M$ be defined so that $\theta(k, f) = k + \psi(f)$ for all $f \in F$. Then $\theta: \ker \pi \oplus F \to M$ is a left R-module homomorphism. Now

$$\pi(m - \psi(\pi(m))) = \pi(m) - (\pi \circ \psi)(\pi(m)) = \pi(m) - \pi(m) = 0_F,$$

where 0_F denotes the zero element of F. Therefore $m - \psi(\pi(m)) \in \ker \pi$ for all $m \in M$. But then $m = \theta(m - \psi(\pi(m)), \pi(m))$ for all $m \in M$. Thus $\theta: \ker \pi \oplus F \to M$ is surjective.

Now let $(k, f) \in \ker \theta$, where $k \in \ker \pi$ and $f \in F$. Then $\psi(f) = -k$. But then $f = \pi(\psi(f)) = -\pi(k) = 0_F$. Also $k = \psi(O_F) = 0_M$, where 0_M denotes the zero element of the module M. Therefore the homomorphism $\theta: \ker \pi \oplus F \to M$ has trivial kernel and is therefore injective. This homomorphism is also surjective. It is therefore an isomorphism between $\ker \pi \oplus F$ and M. The result follows. ∎

Lemma 2.5 *Let F be a left module over a unital ring R, let X be a set, and let $i: X \to F$ be a function. Suppose that this function $i: X \to F$ satisfies the following* universal property*:*

given any left R-module M, and given any function $f: X \to M$, there exists a unique R-module homomorphism $\varphi: F \to M$ such that $\varphi \circ i = f$.

Then the function $i: X \to F$ is injective, and F is freely generated by $i(X)$.

Proof The ring R has at least two elements, since the zero element 0_R and the multiplicative identity element 1_R are distinct elements of the unital ring R. Let x and y be distinct elements of the set X, and let $f: X \to R$ be a function satisfying $f(x) = 0_R$ and $f(y) = 1_R$. The ring R may be regarded as a left R-module over itself. It follows from the universal property of $i: X \to F$ described above that there exists a unique R-module homomorphism $\theta: F \to R$ such that $\theta \circ i = f$. Then $\theta(i(x)) = 0_R$ and $\theta(i(y)) = 1_R$. But $0_R \neq 1_R$. It follows that $i(x) \neq i(y)$. Thus the function $i: X \to F$ is injective.

Let M be a left R-module, and let $g: i(X) \to M$ be a function defined on $i(X)$. Then there exists a unique homomorphism $\varphi: F \to M$ such that $\varphi \circ i = g \circ i$. But then $\varphi|i(X) = g$. Thus the function $g: i(X) \to M$ extends uniquely to a homomorphism $\varphi: F \to M$. This shows that F is freely generated by $i(X)$, as required. ∎

2.2 Construction of Free Modules

Let X be a set, and let R be a unital ring with zero element 0_R and multiplicative identity element 1_R. We say that a function $\sigma: X \to R$ has *at most finitely many non-zero values* if the subset $\operatorname{supp}\sigma$ of X is finite, where

$$\operatorname{supp}\sigma = \{x \in X : \sigma(x) \neq 0_R\}.$$

Let σ and τ be functions from X to R that have at most finitely many non-zero values. Then the sum $\sigma + \tau$ of the functions σ and τ also has at most finitely many non-zero values, where $(\sigma + \tau)(x) = \sigma(x) + \tau(x)$ for all $x \in X$. Indeed

$$\operatorname{supp}(\sigma + \tau) \subset \operatorname{supp}\sigma \cup \operatorname{supp}\tau.$$

Also the function $r\sigma$ has at most finitely many non-zero values for all $r \in R$, where $(r\sigma)(x) = r\sigma(x)$ for all $x \in X$, since $\operatorname{supp}(r\sigma) \subset \operatorname{supp}\sigma$. Moreover the set $F_R X$ of functions from X to R that have at most finitely many non-zero values, with these operations of addition and of multiplication by elements of R, is a left R-module. Indeed $F_R X$ is an Abelian group with respect to the operation of addition of functions, and

$$(r + s)\sigma = r\sigma + s\sigma, \quad r(\sigma + \tau) = r\sigma + r\tau,$$

$$r(s\sigma) = (rs)\sigma \quad \text{and} \quad 1_R\sigma = \sigma$$

for all $r, s \in R$ and $\sigma, \tau \in F_R X$.

Proposition 2.6 *Let R be a unital ring, let X be a set, and let $F_R X$ be the left R-module whose elements are functions from X to R with only finitely many non-zero values. For each element x of X, let $\lambda_x : X \to R$ be the function defined such that*

$$\lambda_x(y) = \begin{cases} 1_R & \text{if } y = x; \\ 0_R & \text{if } y \neq x. \end{cases}.$$

Then the left R-module $F_R X$ is freely generated by the set $\{\lambda_x : x \in X\}$.

Proof Let $x_1, x_2, \ldots, x_k$ be distinct elements of X, let $r_1, r_2, \ldots, r_k$ be elements of the ring R, and let $\sigma = \sum_{j=1}^{k} r_j \lambda_{x_j}$. Then $\sigma(x_i) = r_i$ for $i = 1, 2, \ldots, r$. Also $\sigma(x) = 0$ for all $x \in X \setminus \{x_1, x_2, \ldots, x_k\}$. It follows that if

$$\sum_{j=1}^{k} r_j \lambda_{x_j} = 0$$

then $r_1 = r_2 = \cdots = r_k = 0$. Thus the elements $\lambda_{x_1}, \lambda_{x_2}, \ldots, \lambda_{x_k}$ of $F_R X$ are linearly independent over the ring R.

Let $B = \{\lambda_x : x \in R\}$. We have shown that the elements of every finite subset of B are linearly independent over R. It follows that the elements of B itself are linearly independent over R. Now any element of $F_R X$ can be represented as a linear combination of elements of B. Indeed

$$\sigma = \sum_{x \in \operatorname{supp} \sigma} \sigma(x) \lambda_x$$

for all $\sigma \in F_R X$, where

$$\operatorname{supp} \sigma = \{x \in X : \sigma(x) \neq 0_R\}.$$

It follows that the subset B of $F_R X$ generates $F_R X$. Thus B is a free basis of $F_R X$, as required. ∎

Corollary 2.7 *Let R be a unital ring, let X be a set, and let $F_R X$ be the left R-module whose elements are functions from X to R with only finitely many non-zero values. $i_X : X \to F_R X$ the function that sends x to λ_x for all $x \in X$, where*

$$\lambda_x(y) = \begin{cases} 1_R & \text{if } y = x; \\ 0_R & \text{if } y \neq x. \end{cases}$$

Then, given any left R-module M, and given any function $f: X \to M$, there exists a unique left R-module homomorphism $\varphi: F_R X \to M$ such that $\varphi \circ i_X = f$. Moreover

$$\varphi(\sigma) = \sum_{x \in \operatorname{supp} \sigma} \sigma(x) f(x)$$

for all $\sigma \in F_R X$, where

$$\operatorname{supp} \sigma = \{x \in X : \sigma(x) \neq 0_R\}.$$

Proof The existence and uniqueness of the left R-module homomorphism $\varphi: F_R X \to M$ follows on combining the results of Proposition 2.6 and Proposition 2.2.

Let $\sigma \in F_R X$. Then

$$\sigma = \sum_{x \in \operatorname{supp} \sigma} \sigma(x) \lambda_x$$

and therefore

$$\varphi(\sigma) = \sum_{x \in \operatorname{supp} \sigma} \sigma(x) \varphi(\lambda_x) = \sum_{x \in \operatorname{supp} \sigma} \sigma(x) f(x),$$

as required. ∎

Definition Let X be a set, and let R be a unital ring. We define the *free left R-module* on the set X to be the module $F_R X$ whose elements are represented as functions from X to R with at most finitely many non-zero values, where $(\sigma + \tau)(x) = \sigma(x) + \tau(x)$ and $(r\sigma)(x) = r\sigma(x)$ for all $\sigma, \tau \in F_R X$, $r \in R$ and $x \in X$.

Abelian groups are modules over the ring $\mathbb{Z}$ of integers. The construction of free modules therefore associates to any set X a corresponding free Abelian group $F_{\mathbb{Z}} X$.

Definition Let X be a set. The *free Abelian group* on the set X is the module $F_{\mathbb{Z}} X$ whose elements can be represented as functions from X to $\mathbb{Z}$ that have only finitely many non-zero values.

2.3 The Rank of a Free Module over an Integral Domain

Let M be a free module over a unital commutative ring R. A subset of M is said to be a *free basis* of M if it freely generates M.

A free module M over a unital commutative ring is said to be of *finite rank* if there exists a finite subset of M that freely generates M.

Suppose that the unital ring R is a field. Then any module over R is a vector space over R. It follows from the basic theorems of linear algebra that any finitely generated R-module is a finite-dimensional vector space over R. Moreover any two bases of this vector space have the same number of elements. The number of elements in any basis of the vector space is the *dimension* of the vector space. We see therefore that the number of elements in any free basis of an R-module of finite rank does not depend on the choice of free basis in the particular case where the coefficient ring R is a field.

Now let us consider the case of Abelian groups. An Abelian group is a module over the ring $\mathbb{Z}$ of integers. The ring of integers is an integral domain. Let d be a non-negative integer, let m be a positive integer, and let

$$m\mathbb{Z}^d = \{z \in \mathbb{Z}^d : z = mw \text{ for some } w \in \mathbb{Z}^d\}.$$

Then any element of the quotient group $\mathbb{Z}^d/m\mathbb{Z}^d$ is a coset of $m\mathbb{Z}^d$ in $\mathbb{Z}^d$ of the form

$$m\mathbb{Z}^d + (n_1, n_2, \ldots, n_d),$$

where $n_j \in \{0, 1, \ldots, m-1\}$ for $j = 1, 2, \ldots, d$, and therefore $\mathbb{Z}^d/m\mathbb{Z}^d$ is a finite group of order m^d. It follows that if d and e are non-negative integers, and if $\mathbb{Z}^d \cong \mathbb{Z}^e$ then $d = e$. We conclude from this that if M is a free module of finite rank over the ring $\mathbb{Z}$ (i.e., if M is a free Abelian group of finite rank), then any two free bases of M have the same number of elements. The number of elements in any free basis of M is the *rank* of M.

It can be proved that if R is an integral domain, and if M is a free module of finite rank over the integral domain R then any two free bases of M have the same number of elements.

Definition Let M be a free module of finite rank over an integral domain R. The *rank* of M is the number of elements in any free basis of M.

Let M be a free module of rank d over an integral domain R. Then $M \cong R^d$. Indeed let $b_1, b_2, \ldots, b_d$ be elements of M that constitute a free basis of M. Then, given any element x of M, there exist uniquely-determined elements $r_1, r_2, \ldots, r_d$ of the coefficient ring R such that

$$x = r_1 b_1 + r_2 b_2 + \cdots + r_d b_d.$$

It follows that there exists an R-module isomorphism $\theta: M \to R^d$ defined such that

$$\theta(r_1 b_1 + r_2 b_2 + \cdots + r_d b_d) = (r_1, r_2, \ldots, r_d)$$

for all $r_1, r_2, \ldots, r_d \in R$.