Module Theory

Spring 2018

Paul Balister
University of Memphis

7262 1. Modules Spring 2018

Let R be a ring with a 1. A (left) R-**module** is a set M with addition $+\colon M \times M \to M$ and **scalar** multiplication $\times\colon R \times M \to M$ such that

- $(M, +)$ is an abelian group —

  A1 $(x + y) + z = x + (y + z)$ Associativity

  A2 $x + y = y + x$ Commutativity

  A3 $x + 0 = 0 + x = x$ Additive Identity

  A4 $x + (-x) = (-x) + x = 0$ Additive Inverse

- Scalar multiplication is distributive —

  D1 $(\lambda + \mu)x = \lambda x + \mu x$ Distributivity

  D2 $\lambda(x + y) = \lambda x + \lambda y$ Distributivity

- Scalar multiplication is an action on M —

  S1 $1x = x$ Identity

  S2 $(\lambda\mu)x = \lambda(\mu x)$ Associativity

Examples

1. If R is a field then an R-module is the same as an R-vector space.
2. If $R = \mathbb{Z}$ then any abelian group $(M, +)$ can be considered as a $\mathbb{Z}$-module by defining $n.x = x + \cdots + x$ (n times, $n > 0$) or $n.x = (-x) + \cdots + (-x)$ ($-n$ times $n < 0$) and $0.x = 0$.
3. If $M = R$ and scalar multiplication is given by multiplication in R then $M = R$ itself becomes an R-module.
4. If S is a subring of R then any R-module can be considered as an S-module by restricting scalar multiplication to $S \times M$. For example, a complex vector space can be considered as a real vector space (of twice the dimension), or as an abelian group ($\mathbb{Z}$-module). As a special case R itself can be considered as an S-module.
5. If $R = F[X]$ is the polynomial ring over a field F, then an R-module is an F-vector space V with a map $T\colon V \to V$ given by $T(v) = X.v$. Using the axioms one can prove that T is F-linear. Conversely, given any F-vector space V and linear map $T\colon V \to V$ we can turn V into an $F[X]$-module by defining scalar multiplication by $(\sum a_i X^i).v = \sum a_i T^i(v)$ where $T^0(v) = v$ and $T^{i+1}(v) = T^i(T(v))$.

In any module we have the equalities $0v = 0$ (first 0 in R, second 0 in M), $(-\lambda)v = -(\lambda v)$ (first $-$ in R, second $-$ in M).

An R-**linear map** between two R-modules M and N is a map $f\colon M \to N$ such that $f(x + y) = f(x) + f(y)$ and $f(\lambda x) = \lambda f(x)$.

An **isomorphism** is an R-linear map $f\colon M \to N$ such that f^{-1} exists and is also R-linear. Equivalently, it is a bijective R-linear map.

A subset N of an R-module M is called a **submodule** ($N \leq M$) if $(N,+)$ is a subgroup of $(M,+)$ and N is closed under scalar multiplication: $\lambda \in R, x \in N \Rightarrow \lambda x \in N$. Equivalently, $N \neq \emptyset$ and $\forall x, y \in N, \lambda, \mu \in R : \lambda x + \mu y \in N$.

Examples

1. If R is a field then R-linear maps = linear maps, submodules = subspaces.
2. If $R = \mathbb{Z}$ then R-linear maps = group homomorphisms, submodules = subgroups.
3. If $R = F[X]$ is the polynomial ring over a field F, and V is an R-module given as a vector space and a linear map $T\colon V \to V$, then submodules are invariant subspaces (subspaces U such that $T(U) \subseteq U$). R-linear maps $(V,T) \to (W,S)$ are linear maps $f\colon V \to W$ such that $f(T(v)) = S(f(v))$.
4. If R is considered as an R-module, then submodules = left ideals of R.

If $N \leq M$ are R-modules, the **quotient module** M/N is an R-module such that $(M/N,+)$ is the usual quotient group of $(M,+)$ by $(N,+)$ (since M is abelian, N is automatically normal), and scalar multiplication is defined by $\lambda(x+N) = \lambda x + N$.

Exercise: Show that this definition of scalar multiplication is well defined and that M/N is an R-module.

Examples

1. If R is a field, quotient modules = quotient spaces.
2. If $R = \mathbb{Z}$, quotient modules = quotient groups.
3. If R is a ring and I is an ideal of R then the quotient ring R/I is also an R-module. For example, $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-module.

If $N \leq M$ then inclusion $i\colon N \to M$, $i(v) = v$, and quotient map $\pi\colon M \to M/N$, $\pi(v) = v + N$, are both R-linear maps.

Theorem (1st Isomorphism Theorem)
If $f\colon M \to N$ is an R-linear map then $\operatorname{Ker} f \leq M$, $\operatorname{Im} f \leq N$ and $f = i \circ \tilde{f} \circ \pi$ where

- *$\pi\colon M \to M/\operatorname{Ker} f$ is the (surjective) quotient map,*
- *$\tilde{f}\colon M/\operatorname{Ker} f \to \operatorname{Im} f$ is an R-module isomorphism,*
- *$i\colon \operatorname{Im} f \to N$ is the (injective) inclusion map.*

Theorem (2nd Isomorphism Theorem)
If $N \leq M$ the there is a bijection between submodules L with $N \leq L \leq M$ and submodules L/N of M/N. Also $(M/N)/(L/N) \cong M/L$.

Theorem (3rd Isomorphism Theorem)
If $A, B \leq M$ are submodules then $B \leq A + B = \{a + b : a \in A, b \in B\}$, $A \cap B \leq A$, and $(A+B)/B \cong A/(A \cap B)$.

7262 2. Direct Sums and Products Spring 2018

The **direct sum** $N_1 \oplus N_2$ of two modules is the cartesian product $N_1 \times N_2$ with addition and scalar multiplication defined componentwise: $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$, $\lambda(a_1, a_2) = (\lambda a_1, \lambda a_2)$. More generally, if N_i, $i \in S$ are R-modules, the direct product $\prod_{i \in S} N_i$ is the cartesian product $\{(a_i)_{i \in S} : a_i \in N_i\}$ and the direct sum $\bigoplus_{i \in S} N_i$ is the subset $\{(a_i)_{i \in S} : \text{only finitely many } a_i \neq 0\}$ of $\prod N_i$. In both cases addition and scalar multiplication are defined componentwise.

Note: If there is a finite number of factors there is no difference between direct sum and direct product, however in general the direct sum is a submodule of the direct product.

Let N_i be R-modules, then define **inclusion** and **projection** maps

- $i_i \colon N_i \to \bigoplus N_j; a \mapsto (0, \ldots, 0, a, 0, \ldots)$ where the a is in the i'th component.
- $\pi_i \colon \prod N_j \to N_i; (a_j)_{j \in S} \mapsto a_i$.

If N_i, $i \in S$, are submodules of M then the sum $\sum N_i$ is the set of all finite sums $\sum a_i$, $a_i \in N_i$, of elements from the N_i. It is a submodule of M and is the smallest submodule containing every N_i. Note that if $S \neq \emptyset$ then $\bigcap N_i$ is a submodule of M and is the largest submodule contained in every N_i.

The direct sum $\bigoplus N_i$, and direct product $\prod N_i$, both contain submodules $\tilde{N}_i = \operatorname{Im} i_i = \{(a_j)_{j \in S} : a_j = 0 \text{ for } j \neq i\}$ isomorphic to N_i. The direct sum is equal to the sum $\sum_i \tilde{N}_i$, but the direct product is larger that $\sum_i \tilde{N}_i$ in general.

Lemma 2.1 *If $N_i \leq M$, $i \in S$, then the following are equivalent*

a) Every $x \in M$ can be written uniquely as $\sum_i a_i$, $a_i \in N_i$, with only finitely many $a_i \neq 0$.

b) $\sum_i N_i = M$ and for all i, $N_i \cap (\sum_{j \neq i} N_j) = (0)$.

In this case $M \cong \bigoplus N_i$.

Exercise: Suppose $f \colon M \to N$ and $g \colon N \to M$ are R-linear maps with $fg = 1_N$. Show that $M \cong \operatorname{Ker} f \oplus \operatorname{Im} g$.

Direct Sums

Let N_i be R-modules. For any R-module M and R-linear maps $f_i \colon N_i \to M$ there exists a unique R-linear map $h \colon \bigoplus N_i \to M$ such that $f_i = h \circ i_i$.

$$\begin{tikzcd}
N_i \arrow[r, "f_i"] \arrow[dr, "i_i"'] & M \\
& \bigoplus_j N_j \arrow[u, "h"']
\end{tikzcd}$$

Proof $h((a_i)_{i \in S}) = \sum_{i \in S} f_i(a_i)$

Direct Products

Let N_i be R-modules. For any R-module M and R-linear maps $f_i \colon M \to N_i$ there exists a unique R-linear map $h \colon M \to \prod N_i$ such that $f_i = \pi_i \circ h$.

$$\begin{tikzcd}
N_i & M \arrow[l, "f_i"'] \arrow[d, "h"] \\
& \prod_j N_j \arrow[ul, "\pi_i"]
\end{tikzcd}$$

Proof $h(x) = (f_i(x))_{i \in S}$

7262 3. Homomorphisms Spring 2018

Let N and M be R-modules. Then $\operatorname{Hom}_R(N,M)$ is the set of all R-linear maps $N \to M$.

Lemma 3.1 *If R is commutative then $\operatorname{Hom}_R(N,M)$ is an R-module under addition $(f+g)(x) = f(x) + g(x)$ and scalar multiplication $(\lambda f)(x) = \lambda f(x)$.*

Note that if R is not commutative λf may not be R-linear since $(\lambda f)(\mu x) = \lambda\mu x$ may not be the same as $\mu(\lambda f)(x) = \mu\lambda x$. However, we always have addition of R-linear maps, so $\operatorname{Hom}_R(N,M)$ is always an abelian group under addition (or more generally an S-module where S is the **center** of R, i.e., the subring of elements that commute with all elements of R).

Universal properties of direct sums and products

The universal properties of the last section can be restated as saying there are bijections

$$\operatorname{Hom}_R(\textstyle\bigoplus_i N_i, M) \cong \displaystyle\prod_i \operatorname{Hom}_R(N_i, M), \qquad \operatorname{Hom}_R(M, \textstyle\prod_i N_i) \cong \displaystyle\prod_i \operatorname{Hom}_R(M, N_i).$$

Indeed, these bijections are R-linear isomorphisms when R is commutative (S-linear if R is not commutative).

Exact Sequences

A sequence of R-modules M_i and maps $f_i \colon M_i \to M_{i+1}$

$$\dots \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \dots$$

is called **exact** if $\operatorname{Ker} f_i = \operatorname{Im} f_{i-1}$ ($\le M_i$) for all i.

Examples

1. The sequence $0 \longrightarrow M \xrightarrow{f} N$ is exact iff $f \colon M \to N$ is injective (the map $0 \to M$ must be the zero map, so does not need to be explicitly mentioned).
2. The sequence $M \xrightarrow{f} N \longrightarrow 0$ is exact iff $f \colon M \to N$ is surjective (the map $N \to 0$ must be the zero map, so does not need to be explicitly mentioned).
3. The sequence $0 \longrightarrow M \xrightarrow{f} N \longrightarrow 0$ is exact iff f is an isomorphism.
4. If $0 \longrightarrow K \xrightarrow{g} M \xrightarrow{f} N \longrightarrow 0$ is exact then $N \cong M/K$ (or more strictly $M/\operatorname{Im} g$ where $\operatorname{Im} g = \operatorname{Ker} f \cong K$).

Exact sequences are a very handy notational convenience.

Exercises

1. Show that if R is commutative then $\operatorname{Hom}_R(R,M) \cong M$ as R-modules.
2. Deduce that $\operatorname{Hom}_R(R^n, R^m) \cong R^{nm}$ (Think matrices!)
3. Show that $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A[n]$ where $A[n] = \{a \in A : na = 0\}$.

7262 4. Free Modules Spring 2018

A set of elements $\{e_i : i \in S\}$ of a module M is **linearly independent** if whenever $\sum \lambda_i e_i = 0$ then all $\lambda_i = 0$. (Here as always we assume the sum is finite, so $\lambda_i = 0$ for all but a finite number of i, even if the set $\{e_i\}$ is infinite). A set of elements $\{e_i\}$ **generate** (or **spans**) M if any $x \in M$ can be written as a (finite) linear combination $x = \sum \lambda_i e_i$. A **basis** is a linearly independent set that generates M.

Theorem 4.1 *The following are equivalent for an R-module F.*

a) F has a basis $\{e_i : i \in S\}$,

b) $F \cong \bigoplus_{i\in S} R$,

c) There is a function $e\colon S \to F$ such that for any R-module M and any function $\phi\colon S \to M$, there exists a unique R-linear map $h\colon F \to M$ such that $h \circ e = \phi$.

$$\begin{tikzcd} S \arrow[r, "\phi"] \arrow[dr, "e"'] & M \\ & F \arrow[u, "h"'] \end{tikzcd}$$

Proof. (sketch)
a)⇒b). Show that the map $f\colon \bigoplus_{i\in S} R \to F$, $f((\lambda_i)_{i\in S}) = \sum \lambda_i e_i$ is an isomorphism.
b)⇒c). $h((\lambda_j)_{j\in S})$ must be $\sum_j \lambda_j e(j)$, and this works.
c)⇒a). Let $e_j = e(j)$ for $j \in S$. For linear independence, let $M = \bigoplus_{j\in S} R$ and let $\phi(j) = (\delta_{jk})_{k\in S}$ where $\delta_{jk} = 1$ if $j = k$ and 0 otherwise. To generate F, let F' be the submodule of F generated by the e_j and consider $h =$ projection, and $h = 0$, as maps to $M = F/F'$. Uniqueness of h implies these are the same, so $F' = F$. □

If these conditions hold we say that F is a **free** R-module. The **rank** of F, $\operatorname{rk}_R F$, is the cardinality of the basis S. If R is a field, the rank is also called the **dimension**.

Note: in condition c) the image of the map $e\colon S \to F$ is a basis for F and c) just states that any function defined on a basis of F can be extended uniquely to an R-linear map on F.

Exercise: Show that $\mathbb{Q}$ and $\mathbb{Z}/n\mathbb{Z}$, $n > 1$, are *not* free $\mathbb{Z}$-modules.

Questions

A. Is $\operatorname{rk}_R F$ well defined? I.e., does $R^n \cong R^m$ imply $n = m$?

B. If $F' \le F$ and F', F are free, is it true that $\operatorname{rk}_R F' \le \operatorname{rk}_R F$?

C. If F is free and $N \le F$, is it true that N is free?

The answers to each of these questions is No in general, but Yes in some important special cases.

Lemma 4.2 *Assume M is an R-module and I is an ideal of R. Write $IM = \{\sum a_i m_i : a_i \in I,\, m_i \in M\}$. Then $IM \le M$ and M/IM is naturally an R/I-module.*

Proof. (sketch) Scalar multiplication is defined by $(\lambda + I)(x + IM) = \lambda x + IM$. Check this is well defined and satisfies all the axioms. □

Theorem 4.3 *If R is commutative and F is a free R-module, then $\operatorname{rk}_R F$ is well-defined. In particular, any two bases have the same number of elements.*

Proof. Let I be a maximal ideal of R. Then R/I is a field and F/IF is an R/I-vector space. Since $F \cong \bigoplus_{i\in S} R$, $F/IF \cong \bigoplus_{i\in S} R/I$ (check this!), so $\operatorname{rk}_R F = |S| = \dim_{R/I}(F/IF)$ is uniquely determined. □

Lemma 4.4 *If R is an ID and F is a free R-module, then any subset of F with strictly more than $\operatorname{rk}_R F$ elements is linearly dependent.*

Proof. Without loss of generality $F = \bigoplus_{i\in S} R$. Let $K = \operatorname{Frac}(R)$ be the field of fractions of R. Then $V = \bigoplus_{i\in S} K$ is an R-module and F is a sub-R-module of V. Any set $\{v_i\}$ of elements of F of size larger than $\dim_K V = |S|$ are linearly dependent in V, so there exist $\lambda_i = p_i/q_i \in K$ not all zero, and all but finitely many zero, such that $\sum \lambda_i v_i = 0$. But $q = \prod_{\lambda_i\neq 0} q_i \neq 0$ and $\sum (q\lambda_i)v_i = 0$, where $q\lambda_i \in R$ and $q\lambda_i$ are not all zero. Hence the v_i are R-linearly dependent. □

If R is an ID, define the **rank** of *any* R-module M to be the supremum of the cardinalities of the linearly independent sets in M. By Lemma 4.4 this definition agrees with the earlier definition on free modules.

Exercise: Show that $\operatorname{rk}_{\mathbb{Z}} \mathbb{Q} = 1$ and $\operatorname{rk}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) = 0$ for $n > 0$.

Theorem 4.5 *If R is an ID, M is an R-module, and $N \leq M$, then $\operatorname{rk}_R N \leq \operatorname{rk}_R M$.*

Proof. Any linearly independent set in N must still be linearly independent in M. □

In general Question C is false even when R is an ID. For example, the submodules of the (free, rank 1) R-module R are just the (left = two sided) ideals I of R. However, I is only free of rank 1 if it has a basis $\{e_1\}$ of size 1. But then $I = Re_1 = (e_1)$ is principal. Thus Question C can *only* be true if R is a PID. We shall see that it *is* true for a PID in the next section.

Matrices

Lemma 4.6 *Assume R is commutative. If N is a free R-module with basis $\mathcal{A} = \{e_1, \dots, e_n\}$ and M is a free R-module with basis $\mathcal{B} = \{f_1, \dots, f_m\}$. Then for any R-linear map $f\colon N \to M$ there exists a unique $m \times n$ matrix $[f]_{\mathcal{B},\mathcal{A}} = (a_{ij})$ with entries in R such that $f(e_i) = \sum a_{ji} f_j$. Conversely, any such matrix gives rise to an R-linear map. Furthermore, if P is another R-module with basis $\mathcal{C} = \{g_1, \dots, g_p\}$ and $g\colon N \to P$, then $[gf]_{\mathcal{C},\mathcal{A}} = [g]_{\mathcal{C},\mathcal{B}}[f]_{\mathcal{B},\mathcal{A}}$ where the product is given by matrix multiplication.*

Exercise: Suppose $[f]_{\mathcal{B},\mathcal{A}} = A$. Show that if $\mathcal{A}'$ and $\mathcal{B}'$ are also bases for N and M respectively then $[f]_{\mathcal{B}',\mathcal{A}} = PA$ and $[f]_{\mathcal{B},\mathcal{A}'} = AQ^{-1}$ for some invertible matrices P and Q. [Hint: $P = [1]_{\mathcal{B}',\mathcal{B}}$.]

7262 5. Modules over PIDs Spring 2018

Lemma 5.1 *Any non-empty collection $\mathcal{X}$ of ideals of a PID has a maximal element.*

Proof. Order $\mathcal{X}$ by inclusion and apply Zorn's lemma. If $\mathcal{C} = \{I_\alpha : \alpha \in S\}$ is a chain of ideals, let $I = \cup I_\alpha$. It is easy to check that I is an ideal. But R is a PID, so $I = (a)$ for some $a \in R$. This a must lie in some I_α, so $I = (a) \subseteq I_\alpha \subseteq I$ and $I = I_\alpha$ is an upper bound for $\mathcal{C}$. By Zorn, $\mathcal{X}$ has a maximal element. □

Theorem 5.2 *If R is a PID and M is a submodule of a free R-module N of rank n, then M is free of rank $m \leq n$. Moreover, there exists a basis $\{y_1, \dots, y_n\}$ of N and non-zero $a_1, \dots, a_m \in R$ such that $a_1 \mid a_2 \mid \cdots \mid a_m$ and $\{a_1 y_1, \dots, a_m y_m\}$ is a basis of M.*

Proof. Without loss of generality $N = R^n$. Write π_i for the projection map of N onto the ith factor R. If $M = 0$ then the result is clear with $m = 0$, so suppose $M \neq 0$. Consider the set of R-linear maps $\phi \colon N \to R$ and write $I_\phi = \phi(M)$. Pick a map $\nu \colon N \to R$ such that $I_\nu = (a_1)$ is maximal among these ideals. If $a \in M$, $a \neq 0$, then one of the projections $\pi_i(a)$ is non-zero, so $I_{\pi_i} \neq (0)$. Hence by maximality $a_1 \neq 0$. Also, there exists $y \in M$ such that $\nu(y) = a_1$.

Claim 1. For all $\phi \colon N \to R$, $a_1 \mid \phi(y)$.

Pick any ϕ and let $d = r_1 a_1 + r_2 \phi(y)$ be a gcd of a_1 and $\phi(y)$ in R. Then $d = \phi'(y)$ where $\phi' \colon N \to R$ is the R-linear map $r_1 \nu + r_2 \phi$. But then $d \in I_{\phi'}$, so $I_\nu = (a_1) \subseteq (d) \subseteq I_{\phi'}$. By maximality of I_ν, $a_1 \mid d$, so $a_1 \mid \phi(y)$.

Claim 2. $y = a_1 y_1$ for some $y_1 \in N$.

Since $a_1 \mid \pi_i(y)$ for all i and $y = (\pi_1(y), \dots, \pi_n(y))$, $y = a_1 y_1$ for some $y_1 \in N$.

Claim 3. $N = Ry_1 \oplus \operatorname{Ker} \nu$, $M = Ra_1 y_1 \oplus (M \cap \operatorname{Ker} \nu)$.

Since $y = a_1 y_1$, $a_1 = \nu(y) = a_1 \nu(y_1)$. Since R is an ID, $\nu(y_1) = 1$. If $x \in M$ then $x = \nu(x) y_1 + (x - \nu(x) y_1)$. But $\nu(x - \nu(x) y_1) = \nu(x) - \nu(x) = 0$. Hence $N = Ry_1 + \operatorname{Ker} \nu$. If $x \in Ry_1 \cap \operatorname{Ker} \nu$ then $x = a y_1$ and $0 = \nu(x) = a$. Hence $x = 0$. Thus $N = Ry_1 \oplus \operatorname{Ker} \nu$. A similar argument (using the fact that $\nu(M) = (a_1)$) shows $M = Ra_1 y_1 \oplus (M \cap \operatorname{Ker} \nu)$.

Claim 4. $\operatorname{rk}_R(M \cap \operatorname{Ker} \nu) < \operatorname{rk}_R M$, $\operatorname{rk}_R \operatorname{Ker} \nu < \operatorname{rk}_R N$.

If $\{x_1, \dots, x_k\}$ is linearly independent in $M \cap \operatorname{Ker} \nu$ then $\{y, x_1, \dots, x_k\}$ is linearly independent in M, since if $\lambda y + \sum \lambda_i x_i = 0$ then $0 = \nu(\lambda y + \sum \lambda_i x_i) = \lambda$ and $\sum \lambda_i x_i = 0$. A similar proof shows $\operatorname{rk}_R \operatorname{Ker} \nu < \operatorname{rk}_R N$.

Claim 5. M is free.

Using induction on $\operatorname{rk}_R M$ we can assume $M \cap \operatorname{Ker} \nu$ is free with basis $\{x_1, \dots, x_k\}$. Then $M = Ra_1 y_1 \oplus (M \cap \operatorname{Ker} \nu)$ has basis $\{a_1 y_1, x_1, \dots, x_k\}$.

Completion of Proof.

Applying Claim 5 to $\operatorname{Ker} \nu \leq N$ we see that $\operatorname{Ker} \nu$ is free. Claim 4 shows $\operatorname{rk} \operatorname{Ker} \nu < n$, so using induction on n and considering $M \cap \operatorname{Ker} \nu$ as a submodule of the free module $\operatorname{Ker} \nu$ we have a basis $\{y_2, \dots, y_n\}$ of $\operatorname{Ker} \nu$ and basis $\{a_2 y_2, \dots, a_m y_m\}$ of $M \cap \operatorname{Ker} \nu$. Hence $\{y_1, \dots, y_n\}$ is a basis of N and $\{a_1 y_1, \dots, a_m y_m\}$ is a basis for M where $a_2 \mid a_3 \mid \cdots \mid a_m$. Let $d = r_1 a_1 + r_2 a_2 = \gcd(a_1, a_2)$ and let $\phi = r_1 \pi_1 + r_2 \pi_2$ where π_i are the projections to coordinates given by the basis $\{y_1, \dots, y_n\}$. Then $\phi(a_1 y_1 + a_2 y_2) = r_1 a_1 + r_2 a_2 = d$,

$I_\nu = (a_1) \subseteq (d) \subseteq I_\phi$. Hence by maximality of I_ν, $(d) = (a_1)$ and $a_1 \mid a_2$. □

Theorem (Fundamental Theorem of Finitely generated modules over a PID.) *Let M be a finitely generated R-module where R is a PID. Then there exists $a_1, \dots, a_m$ with $a_i \neq 0$, $a_i \neq$ unit, $a_1 \mid a_1 \mid \cdots \mid a_m$ and $r \geq 0$ such that $M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$. Moreover, r, m, and the ideals (a_i) are uniquely determined by M.*

Proof. (Existence) Let M be generated by $x_1, \dots, x_n$ and consider the R-linear map ϕ from a free module N with basis $\{e_1, \dots, e_n\}$ which sends e_i to x_i. Then $x_i \in \operatorname{Im}\phi$, so ϕ is surjective and $M \cong N/\operatorname{Ker}\phi$. But $\operatorname{Ker}\phi \leq N$, so there is a (new) basis $\{y_1, \dots, y_n\}$ of N such that $\operatorname{Ker}\phi$ has basis $\{a_1 y_1, \dots, a_m y_m\}$. Using this basis we have an isomorphism $N \cong R \oplus R \oplus \cdots \oplus R$ in which $\operatorname{Ker}\phi$ is $Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_m \oplus (0) \oplus \cdots \oplus (0)$. But then $M \cong N/\operatorname{Ker}\phi \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^r$ where $r = n - m$. Finally, any terms $R/(a_i)$ with $a_i =$ unit can be dropped, so we may assume the a_i are not units. □

Lemma 5.3 *If p is a prime of the PID R, and $M = R/(a)$ then $p^{i-1}M/p^iM = 0$ if $p^i \nmid a$ and $p^{i-1}M/p^iM \cong R/(p)$ if $p^i \mid a$.*

Proof. Let $f\colon R \to p^{i-1}M/p^iM$ be defined by $f(x) = p^{i-1}(x + (a)) + p^iM$. This is clearly surjective and $\operatorname{Ker} f = \{x : p^{i-1}x \in (a, p^i)\}$. But $(a, p^i) = (\gcd(a, p^i)) \supseteq (p^{i-1})$ if $p^i \nmid a$, so in this case $\operatorname{Ker} f = R$. If $p^i \mid a$ then $\operatorname{Ker} f = pR$. The result follows. □

Proof. (Uniqueness) Pick any prime p of R and $i \geq 1$. If

$$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m) \cong R^{r'} \oplus R/(a'_1) \oplus \cdots \oplus R/(a'_{m'})$$

Then $p^{i-1}M/p^iM \cong (R/(p))^k \cong (R/(p))^{k'}$ where $k = r + \#\{j : p^i \mid a_j\}$, $k' = r' + \#\{j : p^i \mid a'_j\}$. But $p^{i-1}M/p^iM = N/pN$ where $N = p^{i-1}M$, so can be considered as an $R/(p)$-module. But R is a PID, so (p) is maximal and $R/(p)$ is a field. Hence $k = \dim_{R/(p)}(p^{i-1}M/p^iM) = k'$. Fixing p and letting $i \to \infty$ we see $r = r'$. Also, if $\#\{j : p^i \mid a_j\} = s$ and $a_1 \mid \cdots \mid a_m$ then we must have $p^i \nmid a_1, \dots, a_{m-s}$ and $p^i \mid a_{m-s+1}, \dots, a_m$. Thus knowledge of $k = k'$ for all p and all i gives the prime factorizations of the a_i and a'_i up to a unit. Hence $m = m'$ and $(a_i) = (a'_i)$. □

The factors $R/(a_i)$ are called the **invariant factors** of M.

Theorem 5.4 *Let M be a finitely generated R-module where R is a PID. Then there exists primes $p_1, \dots, p_m$ (not necessarily distinct) and integers $b_1, \dots, b_m > 0$, $r \geq 0$, such that $M \cong R^r \oplus R/(p_1^{b_1}) \oplus R/(p_2^{b_2}) \oplus \cdots \oplus R/(p_m^{b_m})$. Moreover, r, m, and the ideals $(p_i^{b_i})$ are uniquely determined by M up to order.*

Proof. (sketch) Follows from the Fundamental Theorem of Finitely generated modules over a PID using the Chinese Remainder Theorem: If $a = up_1^{b_1} \dots p_r^{b_r}$ where p_i are distinct primes and u is a unit then $R/(a) \cong R/(p_1^{b_1}) \oplus \cdots \oplus R/(p_r^{b_r})$ as an R-module. The proof of this is the same as the proof of the CRT for rings. The proof of the uniqueness of the representation is similar to the uniqueness proof above. □

The factors $R/(p_i^{b_i})$ are called the **elementary divisors** of M.

7262 6. Smith Normal Form Spring 2018

Theorem 6.1 *Let R be a PID and let N and M be free R-modules of rank n and m respectively. Let $\phi\colon N \to M$ be R-linear. Then there exist bases $\mathcal{A}$ of N and $\mathcal{B}$ of M such that $[\phi]_{\mathcal{B},\mathcal{A}}$ is of the form*

$$\begin{pmatrix} a_1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \dots & 0 \\ 0 & \dots & a_r & \dots & 0 \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix}$$

with $a_1 \mid a_2 \mid \cdots \mid a_r$. Moreover the a_i are unique up to associates.

Proof. (Uniqueness of the a_i)
The module $M/\operatorname{Im}\phi$ is clearly isomorphic to $R/(a_1) \oplus \cdots \oplus R/(a_r) \oplus R^{m-r}$. The result follows from the uniqueness of the invariant factors of this module.
Existence (Non-constructive)
Since $\operatorname{Im}\phi \leq M$ and M is free there is a basis $\mathcal{B} = \{y_1, \dots, y_m\}$ of M such that $\operatorname{Im}\phi$ has basis $\{a_1y_1, \dots, a_ry_r\}$. Choose $y_i' \in N$ so that $\phi(y_i') = a_iy_i$. Then there exists a unique linear map $\psi\colon \operatorname{Im}\phi \to N$ such that $\psi(a_iy_i) = y_i'$. Let $\{z_1, \dots, z_k\}$ be a basis for the (free) module $\operatorname{Ker}\phi \leq N$. Since $\phi\psi = 1_{\operatorname{Im}\phi}$, we have $M \cong \operatorname{Im}\psi \oplus \operatorname{Ker}\phi$, and so $\mathcal{A} = \{y_1', \dots, y_r', z_1, \dots, z_k\}$ is a basis for M. The matrix $[\phi]_{\mathcal{B},\mathcal{A}}$ is of the required form. □

We shall give a constructive proof of this theorem in the case when R is a Euclidean domain. Recall that if R is a ED, there exists a function $d\colon R \to \mathbb{N}$ such that for any $a, b \in R$, $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ with $d(r) < d(b)$ or $r = 0$.

Two $m \times n$ matrices A and B are **equivalent** if there exist invertible matrices P and Q such that $B = PAQ$.

Exercise: A and B are equivalent iff there exists an R-linear map ϕ and bases $\mathcal{A}, \mathcal{A}', \mathcal{B}, \mathcal{B}'$ with $A = [\phi]_{\mathcal{B},\mathcal{A}}$ and $B = [\phi]_{\mathcal{B}',\mathcal{A}'}$.

Elementary row and column operations

Let E_{ij} be the $n \times n$ matrix with 1 in the (i, j) place and 0 elsewhere. If $i \neq j$, let $T_{ij}(\lambda) = I_n + \lambda E_{ij}$. Note that $T_{ij}(\lambda)^{-1} = T_{ij}(-\lambda)$, so $T_{ij}(\lambda)$ is invertible. Let $S_{ij} = I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}$. Then $S_{ij}^2 = I_n$ so S_{ij} is invertible. Although not strictly needed, we also define for any unit $u \in R$, $U_i(n) = I_n + (u-1)E_{ii}$, so $U_i(u)^{-1} = U_i(u^{-1})$ and $U_i(u)$ is invertible.

Lemma 6.2 *If $A \in M_{m,n}(R)$ then*

1. *the matrix $AT_{ij}(\lambda)$ is obtained from A by adding λ times the ith column to the jth column of A,*
2. *the matrix AS_{ij} is obtained by swapping the ith and jth columns of A,*

3. the matrix $AU_i(u)$ is obtained by multiplying the ith column of A by u.

If $T_{ij}(\lambda)$, S_{ij}, $U_i(u)$ are defined as $m \times m$ matrices then similar statements hold for $T_{ij}(\lambda)A$, $S_{ij}A$, $U_i(u)A$ with 'column' replaced with 'row'.

Constructive Proof of Existence in Theorem for EDs.
First we show that A is equivalent to a matrix of the form

$$\begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}$$

with every entry of A' divisible by a_1. The proof is by induction on the $\min_{ij} d(a_{ij})$. If $A = 0$ then we are done, so we may assume there are non-zero entries in $A = (a_{ij})$. Let a_{ij} be a non-zero entry with minimal value of $d(a_{ij})$. Then by swapping the ith row with the 1st row and the jth column with the 1st column we can assume $d(a_{11}) = \min_{ij} d(a_{ij})$. Let $a_1 = a_{11}$ and for each $i > 1$ write $a_{i1} = q_i a_1 + r_i$. then by adding $-q_i$ times the first row to the ith row for each i we obtain a new matrix with 1st column $a_1, r_2, \dots, r_m$. Now each r_i is either 0 or $d(r_i) < d(a_1)$. If $d(r_i) < d(a_1)$ and $r_i \neq 0$ then we are done by induction, so we may assume all the $r_i = 0$. Similarly adding multiples of the 1st column to the other columns we get a matrix of the above form. If now remains to show that we can assume a_1 divides all the entries of A'. Assume otherwise and assume there is an entry a_{ij} that is not divisible by a_1. Add the ith row to the 1st row so that the 1st row becomes $a_1, a_{i2}, \dots, a_{in}$. Now add multiples of the 1st column to the other columns as above to get the 1st row $a_1, r_2, \dots, r_n$, $a_{ij} = q_j a_1 + r_j$, $r_j = 0$ or $d(r_j) < d(a_1)$. But now at least one of the non-zero r_j has $d(r_j) < d(a_1)$ and we are done by induction.

Now use induction on n to show that A' is equivalent to a matrix of the form

$$\begin{pmatrix} a_2 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \dots & 0 \\ 0 & \dots & a_r & \dots & 0 \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix}$$

However, if a_1 divides every entry of A' then it must divide every entry of $PA'Q$ for any P, Q. Hence $a_1 \mid a_2$ and A is equivalent to a matrix of the required form. □

7262 7. Application to linear algebra Spring 2018

If V is a K-vector space and $T\colon V \to V$ is a K-linear map, then we can regard V as a $K[X]$-module by defining $(\sum a_i X^i).v = \sum a_i T^i(v)$ where $T^0(v) = v$ and $T^{i+1}(v) = T(T^i(v))$. Note that $K[X]$ is a PID, indeed it is a Euclidean domain with $d(f) = \deg f$.

Lemma 7.1 *Let $\bar{\mathcal{A}} = \{\bar{e}_1, \dots, \bar{e}_n\}$ be a K-basis for V and let N be a free $K[X]$-module with basis $\mathcal{A} = \{e_1, \dots, e_n\}$. Let $A = [T]_{\bar{\mathcal{A}},\bar{\mathcal{A}}}$ and define $\psi\colon N \to N$ so that $[\psi]_{\mathcal{A},\mathcal{A}} = XI_n - A$, and $\phi\colon N \to V$ so that $\phi(e_i) = \bar{e}_i$. Then the sequence*

$$\begin{tikzcd} N \arrow[r, "\psi"] & N \arrow[r, "\phi"] & V \arrow[r] & 0 \end{tikzcd}$$

is exact.

Proof. We need to show ϕ is surjective and $\operatorname{Im}\psi = \operatorname{Ker}\phi$. First, ϕ is surjective since $\operatorname{Im}\phi$ contains the elements $\bar{e}_i$ of a basis. Now $\psi(e_i) = Xe_i - \sum a_{ji}e_j$, so $\phi\psi(e_i) = T(\bar{e}_i) - \sum a_{ji}\bar{e}_j = \sum a_{ji}\bar{e}_j - \sum a_{ji}\bar{e}_j = 0$. Since this holds for each e_i, $\phi\psi = 0$ and $\operatorname{Ker}\phi \supseteq \operatorname{Im}\phi$. Now assume $v = \sum c_i(X)e_i \in \operatorname{Ker}\phi$. If $k \geq 0$ then $X^k e_i - A^k e_i = (X - A)(X^{k-1} + \cdots + A^{k-1})e_i = (X - A)u = \psi(u)$ for some u, where we regard the matrix A as a linear map on N. Thus $(c_i(X) - c_i(A))e_i \in \operatorname{Im}\psi$, so there exists $u \in N$ such that $v = \psi(u) + \sum c_i(A)e_i = \psi(u) + \sum c'_i e_i$ with $c'_i \in K$. But then $0 = \phi(v) = \phi\psi(u) + \phi(\sum c'_i e_i) = \sum c'_i \bar{e}_i$. Thus $c'_i = 0$ and $v = \psi(u) \in \operatorname{Im}\psi$. Hence $\operatorname{Ker}\phi \subseteq \operatorname{Im}\psi$. □

Corollary 7.2 *Write $XI_n - A$ in Smith Normal Form over the PID $K[X]$ and assume the diagonal elements are $a_1(X), \dots, a_r(X)$. Then $r = n$ and $V \cong K[X]/(a_1) \oplus \cdots \oplus K[X]/(a_n)$ as a $K[X]$-module.*

Proof. We choose bases of N so that the matrix of ψ is in Smith Normal Form. Then under this isomorphism $N \cong K[X] \oplus \cdots \oplus K[X]$ and $\operatorname{Im}\psi$ is $(a_1) \oplus \cdots \oplus (a_r)$ and $N/\operatorname{Im}\psi \cong K[X]/(a_1) \oplus \cdots \oplus K[X]/(a_r) \oplus K[X]^{n-r}$. But $V \cong N/\operatorname{Im}\psi$ and V is finite dimensional as a K-vector space. Thus $n = r$ and the result follows. □

Note: Typically some of the a_is will be units (constants) in $K[X]$. The invariant factors are just the non-constant a_is.

The **minimal polynomial** m_A of an $n \times n$ matrix A is a monic polynomial such that $m_A(A) = 0$ and for all $f \in K[X]$, if $f(A) = 0$ then $m_A \mid f$. The **characteristic polynomial** of A is $\det(XI_n - A)$.

Note: The set of $f \in K[X]$ such that $f(A) = 0$ is an ideal and $K[X]$ is a PID, so such an m_A exists, however m_A need not be irreducible.

We shall use basic properties of the **determinant**, $\det A$, of a matrix A. This is defined for any square matrix with entries in a commutative ring, and satisfies $\det AB = \det A \det B$. For diagonal matrices, $\det A$ is the product of the diagonal entries. In particular $\det I_n = 1$.

Lemma 7.3 *If A is an $n \times n$ matrix with entries in the field K then the minimal polynomial of A is $m_A(X) = a_r(X) = \operatorname{lcm}\{a_i(X)\}$, the last monic invariant factor of* *the $K[X]$-module given by the action of A on K^n. The characteristic polynomial is* $\det(XI_n - A) = a_1 \dots a_r$*, the product of the monic invariant factors.*

Proof. By multiplying by units (constants) in $K[X]$, we may assume $a_i(X)$ are monic. The matrix $f(A)$ corresponds to multiplication by $f(X)$ in the module $K[X]/(a_1) \oplus \dots \oplus K[X]/(a_r)$. But this is the zero map iff $a_i \mid f$ for all i. Thus m_A is the lcm of the a_is, which is just a_r (up to multiplication by a constant). Sine m_A and a_r are both monic, $m_A = a_r$. For the characteristic polynomial, $\det(XI_n - A) = \det[\psi]_{\mathcal{A},\mathcal{A}}$ where ψ is the map in Lemma 7.1. We saw in Corollary 7.2 that we could write ψ in Smith normal form so that $[\psi]_{\mathcal{B},\mathcal{C}}$ is diagonal, with entries $a_i(X)$ (or monic units, i.e., 1s) on the diagonal. Thus $\det[\psi]_{\mathcal{B},\mathcal{C}} = a_1 \dots a_r$. Now $[1]_{\mathcal{A},\mathcal{B}}[1]_{\mathcal{B},\mathcal{A}} = I_n$, so $\det[1]_{\mathcal{A},\mathcal{B}} \det[1]_{\mathcal{B},\mathcal{A}} = 1$ and $\det[1]_{\mathcal{A},\mathcal{B}}$ is a unit in $K[X]$, i.e., a constant. Similarly $\det[1]_{\mathcal{C},\mathcal{A}}$ is a constant. Thus as $[\psi]_{\mathcal{A},\mathcal{A}} = [1]_{\mathcal{A},\mathcal{B}}[\psi]_{\mathcal{B},\mathcal{C}}[1]_{\mathcal{C},\mathcal{A}}$, $\det[\psi]_{\mathcal{A},\mathcal{A}} = \det[1]_{\mathcal{A},\mathcal{B}} \det[\psi]_{\mathcal{B},\mathcal{C}} \det[1]_{\mathcal{C},\mathcal{A}}$ is a constant multiple of $a_1 \dots a_r$. Since the characteristic polynomial is monic, it must be $a_1 \dots a_r$. □

Corollary (Cayley-Hamilton Theorem) *If* $f(X) = \det(XI_n - A)$ *then* $f(A) = 0$.

Proof. $m_A = a_r \mid a_1 \dots a_r = f$. □

Two $n \times n$ matrices A and B are **similar** iff there exists an invertible matrix P such that $B = PAP^{-1}$.

Exercise: A and B are similar if there exists an R-linear map $\phi\colon N \to N$ and bases $\mathcal{A}, \mathcal{A}'$ of N such that $A = [\phi]_{\mathcal{A},\mathcal{A}}$ and $B = [\phi]_{\mathcal{A}',\mathcal{A}'}$.

Let K be a field and $f(X) = X^n + f_{n-1}X^{n-1} + \dots + f_0 \in K[X]$ a monic polynomial of degree n. The **companion matrix** to f is the $n \times n$ matrix

$$C(f) = \begin{pmatrix} 0 & 0 & \dots & -f_0 \\ 1 & 0 & \dots & -f_1 \\ 0 & 1 & \dots & -f_2 \\ 0 & 0 & \dots & -f_{n-1} \end{pmatrix}$$

Theorem (Rational Canonical Form) *Any $n \times n$ matrix A over a field K is similar to a matrix of the form*

$$\begin{pmatrix} C(a_1) & 0 & \dots & 0 \\ 0 & C(a_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & C(a_r) \end{pmatrix}$$

where $a_i(X) \in K[X]$ are the monic invariant factors of the $K[X]$ module given by the the action of the linear map A on the K-vector space K^n.

Proof. Using the isomorphism $V \cong K[X]/(a_1) \oplus \dots \oplus K[X]/(a_r)$, it is enough to show that the linear map given by multiplication by X on $K[X]/(a_i)$ has matrix $C(a_i)$ in the K-basis $\{1, X, X^2, \dots, X^{\deg a_i - 1}\}$ of $K[X]/(a_i)$. □

The **Jordan block** $J_n(\lambda)$ is the $n \times n$ matrix

$$\begin{pmatrix} \lambda & 0 & 0 & \dots & 0 \\ 1 & \lambda & 0 & \dots & 0 \\ 0 & 1 & \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix}$$

Theorem (Jordan Normal Form) *Suppose $m_A(X)$ splits in $K[X]$. The A is similar to a matrix of the form*

$$\begin{pmatrix} J_{n_1}(\lambda_1) & 0 & \dots & 0 \\ 0 & J_{n_2}(\lambda_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_{n_r}(\lambda_r) \end{pmatrix}$$

where $(X-\lambda_i)^{n_i}$ are the elementary factors of the $K[X]$-module given by the action of A on K^n.

Proof. Write $V \cong K[X]/(p_1^{n_1}) \oplus \cdots \oplus K[X]/(p_r^{n_r})$ in terms of elementary divisors. The minimal polynomial is the lcm of all the $p_i^{n_i}$, so each p_i must be a product of linear factors. But p_i is irreducible, so $p_i = X - \lambda_i$ for some $\lambda_i \in K$. The result follows as $J_n(\lambda)$ is the matrix of the linear map given by multiplication by X on the K-vector space $K[X]/((X-\lambda)^n)$ with respect to the basis $\{1, (X-\lambda), \dots, (X-\lambda)^{n-1}\}$. □

Corollary 7.4 *A matrix is similar to a diagonal matrix iff $m_A(X)$ splits into distinct linear factors in $K[X]$.*

Proof. Similar matrices have the same minimal polynomial, and the minimal polynomial of a diagonal matrix is just $\prod(X-\lambda_i)$ with the product over the distinct diagonal entries λ_i. For the converse, if the minimal polynomial splits into distinct linear factors, then the Jordan normal form exists and is diagonal since all the elementary divisors (being factors of m_A) are linear. □

7262 8. Tensor products Spring 2018

For this section we shall assume R is a *commutative* ring.

If N_1, N_2, M are R-modules, a **bilinear map** $\phi\colon N_1 \times N_2 \to M$ is a map such that $\phi(\lambda x + \mu y, z) = \lambda\phi(x, z) + \mu\phi(y, z)$ and $\phi(x, \lambda z + \mu w) = \lambda\phi(x, z) + \mu\phi(x, w)$ for all $\lambda, \mu \in R$, $x, y \in N_1$, $z, w \in N_2$. In other words, it is R-linear in each variable if we keep the other variable fixed.

The **tensor product** of N_1 and N_2 is an R-module $N_1 \otimes_R N_2$, and a bilinear map $\otimes\colon N_1 \times N_2 \to N_1 \otimes_R N_2$ such that the following universal property holds. If M is any module and $\phi\colon N_1 \times N_2 \to M$ is bilinear, then there exists a unique R-linear map $h\colon N_1 \otimes_R N_2 \to M$ such that $h(x \otimes y) = \phi(x, y)$ for all $x \in N_1$, $y \in N_2$. One should think of $x \otimes y$ as a 'product' of an element of N_1 with an element of N_2

$$\begin{tikzcd}
N_1 \times N_2 \arrow[r, "\phi"] \arrow[dr, "\otimes"'] & M \\
 & N_1 \otimes N_2 \arrow[u, "h"']
\end{tikzcd}$$

Theorem 8.1 *The tensor product of two modules exists and is unique up to isomorphism.*

Proof. (Uniqueness) Let $\otimes\colon N_1 \times N_2 \to N_1 \otimes_R N_2$ and $\otimes'\colon N_1 \times N_2 \to N_1 \otimes'_R N_2$ be two tensor products. Taking $\phi = \otimes'$ and using the fact that $\otimes$ is a tensor product gives a map $h\colon N_1 \otimes_R N_2 \to N_1 \otimes'_R N_2$ such that $h(x \otimes y) = x \otimes' y$. Similarly there is a map $g\colon N_1 \otimes'_R N_2 \to N_1 \otimes_R N_2$ such that $g(x \otimes' y) = x \otimes y$. Now take $\phi = \otimes$ and $\otimes$ as the tensor product. There exists a unique map $f\colon N_1 \otimes_R N_2 \to N_1 \otimes_R N_2$ such that $f(x \otimes y) = x \otimes y$. However, both $f = g \circ h$ and $f = 1$ satisfy this condition. Hence $g \circ h = 1$. Similarly $h \circ g = 1$ and so h and g are isomorphisms.

$$\begin{tikzcd}
 & N_1 \otimes N_2 \\
N_1 \times N_2 \arrow[ur, "\otimes"] \arrow[r, "\otimes'"] \arrow[dr, "\otimes"'] & N_1 \otimes' N_2 \arrow[u, "g"'] \\
 & N_1 \otimes N_2 \arrow[u, "h"']
\end{tikzcd}$$

Proof. (Existence) Let $F = \bigoplus_{i \in N_1 \times N_2} R$ be a free module with basis $\{e_{x,y} : x \in N_1, y \in N_2\}$. Let $K \leq F$ be the submodule generated by all elements of the form

$$\lambda e_{x,z} + \mu e_{y,z} - e_{\lambda x + \mu y, z}, \qquad \lambda e_{x,z} + \mu e_{x,w} - e_{x, \lambda z + \mu w}$$

where $\lambda, \mu \in R$, $x, y \in N_1$, $z, w \in N_2$. Define $N_1 \otimes_R N_2$ to be F/K and let $\otimes\colon N_1 \times N_2 \to N_1 \otimes_R N_2$ be defined as $x \otimes y = e_{x,y} + K \in F/K$. We now check the various conditions.
1. $\otimes\colon N_1 \times N_2 \to N_1 \otimes_R N_2$ is bilinear.
$(\lambda x + \mu y) \otimes z = e_{\lambda x + \mu y, z} + K = (\lambda e_{x,z} + \mu e_{y,z}) - (\lambda e_{x,z} + \mu e_{y,z} - e_{\lambda x + \mu y, z}) + K = (\lambda e_{x,z} + \mu e_{y,z}) + K = \lambda(x \otimes z) + \mu(y \otimes z)$. Similarly $x \otimes (\lambda z + \mu w) = \lambda(x \otimes z) + \mu(x \otimes w)$.
2. If $\phi\colon N_1 \times N_2 \to M$ is bilinear then $\exists h\colon N_1 \otimes_R N_2 \to M$ such that $h(x \otimes y) = \phi(x, y)$.
Define $h'\colon F \to M$ on the basis $e_{x,y}$ of F by $h'(e_{x,y}) = \phi(x, y)$. Clearly $K \leq \operatorname{Ker} h'$ so h' induces a map $h\colon F/K \to M$ by $h(z + K) = h'(z)$. Now $h(x \otimes y) = h'(e_{x,y}) = \phi(x, y)$.
3. This h is unique.
Since any element of F is a linear combination of the $e_{x,y}$, any element of $N_1 \otimes N_2 = F/K$ is a linear combination of the $x \otimes y = e_{x,y} + K$. Thus h is determined on a generating set, and so is unique. □

The construction above is quite general, but not very easy to work with. In many important cases it is possible to give easier descriptions of the tensor product. In each case all we need to do to show that a description is correct is to show that it satisfies the universal property of a tensor product (by uniqueness of the tensor product).

Theorem 8.2 *If N and M are free R-modules with bases $\{e_1, \dots, e_n\}$ and $\{f_1, \dots, f_n\}$ respectively, then $N \otimes_R M$ is free with basis $\mathcal{B} = \{e_i \otimes f_j : 1 \leq i \leq n,\ 1 \leq j \leq m\}$.*

Proof. We know from the proof of the previous theorem that $N \otimes M$ is generated by the $x \otimes y$. But if we write $x = \sum \lambda_i e_i$, $y = \sum \mu_j f_j$ then $x \otimes y = \sum_{ij} \lambda_i \mu_j (e_i \otimes f_j)$. Hence $\mathcal{B}$ generates $N \otimes M$. Now suppose $\sum \lambda_{ij}(e_i \otimes f_j) = 0$. Fix i_0 and j_0 and consider the bilinear map $\phi\colon N \times M \to R$ given by $\phi(\sum \mu_i e_i, \sum \nu_j f_j) = \mu_{i_0} \nu_{j_0}$. It is easily checked that this is a well-defined bilinear map. But then there is an R-linear map $h\colon N \otimes M \to R$ with $h(\sum \lambda_{ij}(e_i \otimes f_j)) = \sum \lambda_{ij} h(e_i \otimes f_j) = \sum \lambda_{ij} \phi(e_i, f_j) = \lambda_{i_0, j_0}$. If $\sum \lambda_{ij}(e_i \otimes f_j) = 0$ then $\lambda_{i_0, j_0} = 0$. Since this holds for all i_0, j_0 the $e_i \otimes f_j$ are linearly independent. □

Note: $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \cong \mathbb{C}$, but $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{R}^2 \cong \mathbb{R}^4$, but $\mathbb{C} \not\cong \mathbb{R}^4$, so the subscript on the $\otimes$ is important.

Theorem 8.3 *If N is an R-module and I is an ideal of R then $N \otimes_R R/I \cong N/IN$.*

Proof. Define $\otimes\colon N \times R/I \to N/IN$ by $x \otimes (r + I) = rx + IN$. First we show that this is well-defined. If $r' + I = r + I$ then $r' - r \in I$, so $r'x - rx \in IN$ and $rx + IN = r'x + IN$. We then check it is bilinear, which is easy. Now, if $\phi\colon N \times R/I \to M$ is bilinear, define $h'\colon N \to M$ by $h'(x) = \phi(x, 1 + I)$. This is R-linear. If $x \in IN$ then $x = \sum a_i x_i$ with $a_i \in I$ and $x_i \in N$. Then $h'(x) = \phi(\sum a_i x_i, 1 + I) = \sum a_i \phi(x_i, 1 + I) = \sum \phi(x_i, a_i + I) = \sum \phi(x_i, 0 + I) = 0$. Thus $IN \leq \operatorname{Ker} h'$ and h' induces a map $h\colon N/IN \to M$ such that $h(x \times (r+I)) = h(rx + IN) = h'(rx) = \phi(rx, 1+I) = r\phi(x, 1+I) = \phi(x, r+I)$. Conversely if $h\colon N/IN \to M$ has this property then $h(x + IN) = h(x \otimes (1 + I)) = \phi(x, 1 + I) = h'(x)$ and so h is uniquely determined. □

Exercises

1. Show that any bilinear map $R^n \times R^m \to R$ can be represented by a unique matrix A so that $\phi(u, v) = u^T A v$. (Elements of R^n, R^m are considered as column vectors and ^{T} denotes transpose.)
2. Show that $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\gcd(n, m)\mathbb{Z}$.
3. Show that $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.
4. If $f\colon N \to N'$ and $g\colon M \to M'$ are R-linear, show that there exists a unique R-linear map $f \otimes g\colon N \otimes_R M \to N' \otimes_R M'$ such that $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$.
5. Show that tensor products are 'commutative': $N \otimes_R M \cong M \otimes_R N$.
6. Show that tensor products are 'associative': $N_1 \otimes_R (N_2 \otimes_R N_3) \cong (N_1 \otimes_R N_2) \otimes_R N_3$.
7. Show that tensor products are 'distributive' over direct sums: $N \otimes_R (M \oplus M') \cong (N \otimes_R M) \oplus (N \otimes_R M')$.

7262 9. Extension of Scalars Spring 2018

An R-**algebra** is a ring S with a ring homomorphism $i\colon R \to S$ such that $\operatorname{Im} i$ is in the center of S.

Note: The **center** of S is the set of elements $z \in S$ such that $zs = sz$ for all $s \in S$, so if the ring S is commutative then $\operatorname{Im} i$ is automatically in the center.

Throughout this section we shall assume all rings are commutative.

Examples

1. Any ring R is a $\mathbb{Z}$-algebra.
2. If R is a subring of a commutative ring S then S is an R-algebra.
3. If I is an ideal of R then R/I is an R-algebra. The polynomial ring $R[X]$ is an R-algebra. If S is a multiplicative subset of R then $S^{-1}R$ is an R-algebra. In particular, if R is an ID then the field of fractions of R is an R-algebra.
4. If S is an R-algebra then it is also an R-module with scalar multiplication $R \times S \to S$ given by $\lambda.x = i(\lambda)x$. More generally, if M is an S-module then it is also an R-module with scalar multiplication given by $\lambda.x = i(\lambda)x$, $\lambda \in R$, $x \in M$.

One can define R-algebra homomorphisms, sub-R-algebras, quotient R-algebras etc., as for rings with the extra condition that the i maps are preserved, e.g., if $i_1\colon R \to S_1$, $i_2\colon R \to S_2$ are R-algebras then an R-algebra homomorphism is a ring homomorphism $f\colon S_1 \to S_2$ such that $f(i_1(\lambda)) = i_2(\lambda)$.

Theorem 9.1 *If N is an R-module and S is an R-algebra, then $S \otimes_R N$ is an S-module.*

Proof. Define for $\lambda, \mu \in S$, $\lambda(\mu \otimes x) = (\lambda\mu) \otimes x$ and extend to $S \otimes N$ linearly: $\lambda(\sum \mu_i \otimes x_i) = \sum \lambda\mu_i \otimes x_i$. We need to check that this is well-defined. Fix $\lambda \in S$ and consider the map $\phi_\lambda\colon S \times N \to S \otimes N$ given by $\phi_\lambda(\mu, x) = (\lambda\mu) \otimes x$. This map is bilinear (here we need that scalar multiplication by R commutes with S), so gives a unique map $h_\lambda\colon S \otimes N \to S \otimes N$ such that $h_\lambda(\mu \otimes x) = (\lambda\mu) \otimes x$. It is not hard to check that $h_{\lambda\lambda'} = h_\lambda \circ h_{\lambda'}$ and $h_{\lambda+\lambda'} = h_\lambda + h_{\lambda'}$. From this it is simple to check that this defines a scalar multiplication on $S \otimes_R N$ and $S \otimes_R N$ is an S-module. □

Examples

1. R/I is an R-algebra ($i = \pi$ is the projection map), so for any R-module M we can turn $R/I \otimes_R M = M/IM$ into an R/I-module.
2. If $M \cong R^n$ is a free R-module then $S \otimes_R M \cong S^n$ is a free S-module of the same rank. For example, one can turn a real n-dimensional vector space V into a complex n-dimensional vector space $\mathbb{C} \otimes_{\mathbb{R}} V$ (but $2n$-dimensional as an $\mathbb{R}$-vector space). $\mathbb{R}$-linear maps $f\colon U \to V$ become $\mathbb{C}$-linear maps $1 \otimes f\colon \mathbb{C} \otimes U \to \mathbb{C} \otimes V$ (with the same matrix as f if one uses the obvious new bases $\{1 \otimes e_i\}$).

Let R be a commutative ring and S a multiplicative subset of R, so $1 \in S$ and $a, b \in S$ imply $ab \in S$. Let M be an R-module. Define $S^{-1}M$ to be the set $M \times S/\sim$ where $(m, s) \sim (m', s')$ iff $\exists u \in S\colon us'm = usm'$. Write $\frac{m}{s}$ for the equivalence class of (m, s).

Lemma 9.2 *$S^{-1}M$ is an $S^{-1}R$-module (and hence also an R-module).*

Proof. (sketch) Addition is defined by $\frac{m}{s} + \frac{m'}{s'} = \frac{s'm+sm'}{ss'}$, scalar multiplication is defined by $\frac{r}{s}\frac{m'}{s'} = \frac{rm'}{ss'}$. One needs to check to following: 1) $\sim$ is an equivalence relation, 2) $+$ is well-defined, 3) $(S^{-1}M, +)$ is an abelian group ($+$ is associative, commutative, identity $\frac{0}{1}$, inverses $-\frac{m}{s} = \frac{-m}{s}$), 4) scalar multiplication is well-defined, 5) $S^{-1}M$ is an $S^{-1}R$-module (multiplication distributes over addition both ways, is associative, and $\frac{1}{1}\frac{m}{s} = \frac{m}{s}$). □

Theorem 9.3 *If S is a multiplicative set and M is an R-module then $S^{-1}R \otimes M \cong S^{-1}M$ as an $S^{-1}R$-module (or as an R-module).*

Proof. (sketch) Define $\otimes\colon S^{-1}R \times M \to S^{-1}M$ by $\frac{r}{s} \otimes x = \frac{rx}{s}$. Check this is well-defined (if $\frac{r}{s} = \frac{r'}{s'}$ then $\frac{rx}{s} = \frac{r'x}{s'}$) and is bilinear. If $\phi\colon S^{-1}R \times M \to N$ is bilinear and $h(\frac{r}{s} \otimes x) = \phi(\frac{r}{s}, x)$ then $h(\frac{x}{s}) = \phi(\frac{1}{s}, x)$ is uniquely determined. Conversely define $h(\frac{x}{s}) = \phi(\frac{1}{s}, x)$ and show that this is well-defined, R-linear, and $h(\frac{r}{s} \otimes x) = h(\frac{rx}{s}) = \phi(\frac{1}{s}, rx) = r\phi(\frac{1}{s}, x) = \phi(\frac{r}{s}, x)$. Finally, check that the scalar multiplication by $S^{-1}R$ agrees on $S^{-1}M$ with that on $S^{-1}R \otimes M$. □

Theorem 9.4 *If S_1 and S_2 are two R-algebras then $S_1 \otimes_R S_2$ can be made into an R-algebra with multiplication $(s_1 \otimes s_2)(s_1' \otimes s_2') = s_1s_1' \otimes s_2s_2'$.*

Proof. S_1 and S_2 are R-modules, so $S_1 \otimes_R S_2$ is an R-module. Thus we have an abelian group structure under $+$ and an R-linear map $i\colon R \to S_1 \otimes_R S_2$ given by $i(\lambda) = \lambda(1 \otimes 1)$. This will be a ring homomorphism if the multiplication in $S_1 \otimes_R S_2$ is defined as above. It is therefore enough to show that the multiplication is well-defined, associative, has identity $1 \otimes 1$, and is distributive over $+$.

Fix s_1, s_2 and define $\phi_{s_1,s_2}\colon S_1 \times S_2 \to S_1 \otimes_R S_2$ by $\phi_{s_1,s_2}(s_1', s_2') = s_1s_1' \otimes s_2s_2'$. This is R-bilinear. Then there exists an R-linear $h_{s_1,s_2} \in \mathrm{Hom}_R(S_1 \otimes S_2, S_1 \otimes S_2)$ with $h_{s_1,s_2}(s_1' \otimes s_2') = s_1s_1' \otimes s_2s_2'$. Now $\mathrm{Hom}_R(\dots)$ is an R-module and the map $h\colon S_1 \times S_2 \to \mathrm{Hom}_R(S_1 \otimes S_2, S_1 \otimes S_2)$ given by $(s_1, s_2) \to h_{s_1,s_2}$ is R-bilinear (check this). Hence there is a map $g\colon S_1 \otimes S_2 \to \mathrm{Hom}_R(S_1 \otimes S_2, S_1 \otimes S_2)$ with $g(s_1 \otimes s_2)(s_1' \otimes s_2') = s_1s_1' \otimes s_2s_2'$. Define multiplication on $S_1 \otimes_R S_2$ by $\alpha\beta = g(\alpha)(\beta)$. The axioms can be checked easily from the formula for $(s_1 \otimes s_2)(s_1' \otimes s_2')$ (Note: a typical element of $S_1 \otimes_R S_2$ is a *sum* of elements of the form $s_1 \otimes s_2$). □

Exercises

1. Show that $R[X] \otimes_R R[Y] \cong R[X, Y]$ as an R-algebra. [Hint: $f \otimes g \mapsto f(X)g(Y)$.]
2. Let R be an ID with field of fractions K. If M is an R-module then $\mathrm{rk}_R M = \dim_K(K \otimes_R M)$ (where we define $\mathrm{rk}_R M$ as the size of the largest R-linearly independent subset of M).

10. Symmetric & Alternating

A **multilinear** map $\phi\colon M^k \to N$ is a map that is R-linear in each variable, i.e., $\forall i\colon \phi(x_1,\dots,\lambda x_i+\mu x_i',\dots,x_k) = \lambda\phi(x_1,\dots,x_i,\dots,x_k)+\mu\phi(x_1,\dots,x_i',\dots,x_k)$. The multilinear map ϕ is **symmetric** if $\phi(x_1,\dots,x_k)=\phi(x_{\pi(1)},\dots,x_{\pi(k)})$ for all permutations $\pi\in S_k$. The map ϕ is **skew-symmetric** if $\phi(x_1,\dots,x_k)=\operatorname{sgn}(\pi)\phi(x_{\pi(1)},\dots,x_{\pi(k)})$ where $\operatorname{sgn}(\pi)=\pm1$ is the sign of the permutation π. The map ϕ is **alternating** if $\phi(x_1,\dots,x_k)=0$ whenever $x_i=x_j$ for some $i\neq j$.

Exercise: Show that alternating always implies skew-symmetric and skew-symmetric implies alternating provided $2x=0\Rightarrow x=0$ in N.

Theorem 10.1 *If M is an R-module and $k\geq 0$ then there exists modules $\mathcal{T}^k(M)$, (resp. $\operatorname{Sym}^k(M)$, $\bigwedge^k(M)$), and multilinear (resp. symmetric, alternating) maps $\psi\colon M^k\to \mathcal{T}^k(M)$ (resp. $\operatorname{Sym}^k(M)$, $\bigwedge^k(M)$), such that for any multilinear (resp. symmetric, alternating) map $\phi\colon M^k\to N$ there exists a unique R-linear map h such that $h\circ\psi=\phi$.*

Proof. (sketch) Let $\mathcal{T}^0(M)=R$ and inductively define $\mathcal{T}^{k+1}(M)=\mathcal{T}^k(M)\otimes_R M$, so that $\mathcal{T}^k(M)$ is the tensor product of k copies of M. The Theorem for $\mathcal{T}^k(M)$ holds by induction on k and the universal property of tensor products. For symmetric maps, define $\operatorname{Sym}^k(M)=\mathcal{T}^k(M)/\mathcal{C}^k(M)$, where $\mathcal{C}^k(M)$ is the submodule of $\mathcal{T}^k(M)$ generated by elements of the form $(x_1\otimes x_2\otimes\cdots\otimes x_k)-(x_{\pi(1)}\otimes x_{\pi(2)}\otimes\cdots\otimes x_{\pi(k)})$, $x_i\in M$, $\pi\in S_k$, and $\psi(x_1,\dots,x_k)=(x_1\otimes\cdots\otimes x_k)+\mathcal{C}^k(M)$. It is easy to check that ψ is symmetric, h exists (use the result for $\mathcal{T}^k(M)$ and show that $\operatorname{Ker} h\subseteq \mathcal{C}^k(M)$), h is unique (the $x_1\otimes\cdots\otimes x_k+\mathcal{C}^k(M)$ generate $\operatorname{Sym}^k(M)$). For alternating maps, define $\bigwedge^k(M)=\mathcal{T}^k(M)/\mathcal{D}^k(M)$, where $\mathcal{D}^k(M)$ is the submodule of $\mathcal{T}^k(M)$ generated by elements of the form $x_1\otimes\cdots\otimes x_k$ with $x_i=x_j$ for some $i\neq j$. The proof is similar. □

Example $\mathcal{T}^0(M)\cong\operatorname{Sym}^0(M)\cong\bigwedge^0(M)\cong R$, $\mathcal{T}^1(M)\cong\operatorname{Sym}^1(M)\cong\bigwedge^1(M)\cong M$.

For all $i,j\geq 0$ there are bilinear maps

$$\otimes\colon \mathcal{T}^i(M)\times\mathcal{T}^j(M)\to\mathcal{T}^{i+j}(M),$$
$$\odot\colon \operatorname{Sym}^i(M)\times\operatorname{Sym}^j(M)\to\operatorname{Sym}^{i+j}(M),$$
$$\wedge\colon \textstyle\bigwedge^i(M)\times\bigwedge^j(M)\to\bigwedge^{i+j}(M),$$

The map $\otimes$ is the usual tensor product, using the associativity of $\otimes$ so that $\mathcal{T}^{i+j}(M)\cong\mathcal{T}^i(M)\otimes_R\mathcal{T}^j(M)$. The other two maps are the maps corresponding to $\otimes$ on the quotient spaces $\operatorname{Sym}^k(M)$ and $\bigwedge^k(M)$ (check these are well defined).

Let $\mathcal{T}(M)=\bigoplus_{k=0}^\infty\mathcal{T}^k(M)$, $\operatorname{Sym}(M)=\bigoplus_{k=0}^\infty\operatorname{Sym}^k(M)$, $\bigwedge(M)=\bigoplus_{k=0}^\infty\bigwedge^k(M)$. Then by extending $\otimes$, $\odot$, $\wedge$ linearly we get multiplication maps on $\mathcal{T}(M)$, $\operatorname{Sym}(M)$, $\bigwedge(M)$.

Lemma 10.2 *$\mathcal{T}(M)$, $\operatorname{Sym}(M)$, $\bigwedge(M)$ are R-algebras under the multiplication maps $\otimes$, $\odot$, $\wedge$ respectively.*

Note: $\otimes$, $\odot$, $\wedge$ are all associative and $\odot$ is symmetric. However $\wedge$ is *not* skew-symmetric, since for example $a, b, c \in M \cong \bigwedge^1(M)$, $(a \wedge b) \wedge c = -a \wedge c \wedge b = +c \wedge (a \wedge b)$.

Theorem 10.3 *Let M be a free R-module of rank n with basis $\{e_1, \dots, e_n\}$. then*

$$\mathcal{T}^k(M) \text{ is free of rank } n^k \text{ with basis } \{e_{i_1} \otimes \cdots \otimes e_{i_k} : 1 \le i_1, i_2, \dots, i_k \le n\},$$

$$\mathrm{Sym}^k(M) \text{ is free of rank } \tbinom{n+k-1}{k} \text{ with basis } \{e_{i_1} \odot \ldots \odot e_{i_k} : 1 \le i_1 \le \cdots \le i_k \le n\},$$

$$\textstyle\bigwedge^k(M) \text{ is free of rank } \tbinom{n}{k} \text{ with basis } \{e_{1_1} \wedge \cdots \wedge e_{i_k} : 1 \le i_1 < \cdots < i_k \le n\}.$$

Example Suppose $R = \mathbb{R}$, $M = \mathbb{R}^3$, then $\bigwedge(M)$ is an 8-dimensional space which is the direct sum of $\bigwedge^0(M) \cong \mathbb{R}$ (1-dim space of **scalars**), $\bigwedge^1(M) \cong \mathbb{R}^3$ (3-dim space of **vectors**), $\bigwedge^2(M) \cong \mathbb{R}^3$ (3-dim space of **bivectors**, or **pseudovectors**), and $\bigwedge^3(M) \cong \mathbb{R}$ (1-dim space of **trivectors**, or **pseudoscalars**). Suppose we pick a basis $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ of M. Then $\bigwedge(M)$ has basis

$$\{1, \quad \mathbf{i}, \quad \mathbf{j}, \quad \mathbf{k}, \quad \mathbf{j} \wedge \mathbf{k}, \quad \mathbf{k} \wedge \mathbf{i}, \quad \mathbf{i} \wedge \mathbf{j}, \quad \mathbf{i} \wedge \mathbf{j} \wedge \mathbf{k}\}$$

Define $\tilde{\mathbf{i}} = \mathbf{j} \wedge \mathbf{k}$, $\tilde{\mathbf{j}} = \mathbf{k} \wedge \mathbf{i}$, $\tilde{\mathbf{k}} = \mathbf{i} \wedge \mathbf{j}$. The map $\wedge\colon \bigwedge^1(M) \times \bigwedge^1(M) \to \bigwedge^2(M)$ is

$$(x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}) \wedge (y_1\mathbf{i} + y_2\mathbf{j} + y_3\mathbf{k}) = (x_2y_3 - x_3y_2)\tilde{\mathbf{i}} + (x_3y_1 - x_1y_3)\tilde{\mathbf{j}} + (x_1y_2 - x_2y_1)\tilde{\mathbf{k}}.$$

If we compose this map with the isomorphism $\bigwedge^2(M) \to \bigwedge^1(M)$ given by sending $\tilde{\mathbf{i}}$, $\tilde{\mathbf{j}}$, $\tilde{\mathbf{k}}$ to $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ respectively, then this is just the vector cross product on $\mathbb{R}^3$.

The map $\wedge$ is called the **exterior product** and is very important in differential geometry. For real vector spaces M, the **vectors** $\bigwedge^1(M)$ can be thought of as oriented line segments, the **bivectors** $\bigwedge^2(M)$ as oriented area elements, etc..

Theorem 10.4 *If $f\colon M \to N$ is an R-linear map then there are R-linear maps*

- $\mathcal{T}^k(f)\colon \mathcal{T}^k(M) \to \mathcal{T}^k(N)$; $\mathcal{T}^k(f)(x_1 \otimes \cdots \otimes x_k) = f(x_1) \otimes \cdots \otimes f(x_k)$,
- $\mathrm{Sym}^k(f)\colon \mathrm{Sym}^k(M) \to \mathrm{Sym}^k(N)$; $\mathrm{Sym}^k(f)(x_1 \odot \ldots \odot x_k) = f(x_1) \odot \ldots \odot f(x_k)$,
- $\bigwedge^k(f)\colon \bigwedge^k(M) \to \bigwedge^k(N)$; $\bigwedge^k(f)(x_1 \wedge \cdots \wedge x_k) = f(x_1) \wedge \cdots \wedge f(x_k)$,

Proof. Use universal properties. □

Theorem 10.5 *If M is free of rank n and $f\colon M \to M$ is R-linear, then the map $\bigwedge^n(M)$ is given by multiplication by $\det f$ on the rank 1 module $\bigwedge^n M$.*

Proof. Suppose M has basis $\{e_1, \dots, e_n\}$, then $\bigwedge^n(M)$ is of rank 1 with basis $\{e_1 \wedge \cdots \wedge e_n\}$. If f has matrix a_{ij} with respect to the basis $\{e_1, \dots, e_n\}$ then $\bigwedge^n(f)(e_1 \wedge \cdots \wedge e_n) = f(e_1) \wedge \cdots \wedge f(e_n) = (\sum_{i_1} a_{i_1 1} e_{i_1}) \wedge \cdots \wedge (\sum_{i_n} a_{i_n n} e_{i_n}) = \sum_{i_1, i_2, \dots, i_n} a_{i_1 1} a_{i_2 2} \ldots a_{i_n n} e_{i_1} \wedge \cdots \wedge e_{i_n}$. However, if $i_i = i_j$ for $i \ne j$ then $e_{i_1} \wedge \cdots \wedge e_{i_n} = 0$. Hence we can assume $i_j = \pi(j)$ for some permutation $\pi \in S_n$. Also $e_{\pi(1)} \wedge \cdots \wedge e_{\pi(n)} = \mathrm{sgn}(\pi) e_1 \wedge \cdots \wedge e_n$. Hence $\bigwedge^n(f)$ acts as multiplication by $\sum_{\pi \in S_n} \mathrm{sgn}(\pi) a_{\pi(1)1} \ldots a_{\pi(n)n} = \det(a_{ij})$. □

This theorem can be used as a definition for the determinant of a linear map. Various properties of det become clear using this definition. For example $\det f$ is independent of the basis, and $\det(fg) = (\det f)(\det g)$ follows from $\bigwedge^n(f \circ g) = \bigwedge^n(f) \circ \bigwedge^n(g)$.