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

- $(M, +)$ is an abelian group —
  
  
  \begin{align*}
  & A1 \quad (x + y) + z = x + (y + z) \\
  & A2 \quad x + y = y + x \\
  & A3 \quad x + 0 = 0 + x = x \\
  & A4 \quad x + (-x) = (-x) + x = 0
  \end{align*}

  
  - Associativity
  - Commutativity
  - Additive Identity
  - Additive Inverse

- Scalar multiplication is distributive —
  \begin{align*}
  & D1 \quad (\lambda + \mu)x = \lambda x + \mu x \\
  & D2 \quad \lambda(x + y) = \lambda x + \lambda y
  \end{align*}

  
  - Distributivity
  - Distributivity

- Scalar multiplication is an action on $M$ —
  \begin{align*}
  & S1 \quad 1x = x \\
  & S2 \quad (\lambda \mu)x = \lambda(\mu x)
  \end{align*}

  
  - Identity
  - 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).

5. If $R = F[X]$ is the polynomial ring over a field $F$, then an $R$-module is an $F$-vector space $V$ ($F$ is a subring of $R$), with a map $T: V \to V$ 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 $T: V \to V$ 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 $f: M \to N$ such that $f(x + y) = f(x) + f(y)$ and $f(\lambda x) = \lambda f(x)$.

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

A submodule of an $R$-module $M$ is a subset $N \subseteq M$ such that $(N, +)$ 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 $\forall x, y \in N, \lambda, \mu \in R : \lambda x + \mu y \in N$. We write $N \leq M$ when $N$ is a submodule of $M$. 

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 $T : V \to V$, then submodules are invariant subspaces (subspaces $U$ such that $T(U) \subseteq U$). $R$-linear maps $(V,T) \to (W,S)$ are linear maps $f : V \to W$ 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 $i : N \to M$, $i(v) = v$, and projection $\pi : M \to M/N$, $\pi(v) = v + N$, are both $R$-linear maps.

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

- $\pi : M \to M/\text{Ker} f$ is the (surjective) projection map,
- $\tilde{f} : M/\text{Ker} f \to \text{Im} f$ is an $R$-module isomorphism,
- $i : \text{Im} f \to N$ 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 $(A + B)/B \cong A/(A \cap B)$. 
Definition The direct sum $N_1 \oplus N_2$ of two modules is the cartesian product $N_1 \times N_2 = \{(a_1, a_2) : a_1 \in N_1, a_2 \in N_2\}$ 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 $\{(a_i)_{i \in S} :$ only finitely many $a_i \neq 0\}$ of $\prod N_i$. In both cases addition and scalar multiplication are defined componentwise.

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

Definition Let $N_i$ be $R$-modules, then there are $R$-linear maps

- $i_i : N_i \to \bigoplus N_j; a \mapsto (0, \ldots, 0, a, 0, \ldots)$ where $a_i = a$ and $a_j = 0$ for $j \neq i$.
- $\pi_i : \prod N_j \to N_i; (a_j)_{j \in S} \mapsto a_i$.

Definition 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 $\tilde{N}_i = \text{Im} i_i = \{(a_j)_{j \in S} : a_j = 0$ for $j \neq i\}$ isomorphic to $N_i$. The direct sum is equal to the sum $\sum_i \tilde{N}_i$.

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

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

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

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

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

Universal properties of direct sums and direct products.

Direct Sums

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

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

Direct Products

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

Proof $h(x) = (f_i(x))_{i \in S}$
**Definition** Let \( N \) and \( M \) be \( R \)-modules. Then \( \text{Hom}_R(N, M) \) is the set of all \( R \)-linear maps from \( N \) to \( M \).

**Lemma** If \( R \) is commutative then \( \text{Hom}_R(N, M) \) 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 \( \lambda f \) 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 \( \text{Hom}_R(N, M) \) is always an abelian group.

**Universal properties of direct sums and products**

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

\[
\text{Hom}_R\left( \bigoplus_i N_i, M \right) \cong \prod_i \text{Hom}(N_i, M), \quad \text{Hom}_R(M, \prod_i N_i) \cong \prod_i \text{Hom}(M, N_i).
\]

Indeed, these bijections are \( R \)-linear isomorphisms when \( R \) is commutative (\( \mathbb{Z} \)-linear if \( R \) is not commutative).

**Exercises**

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

**Exact Sequences**

**Definition** A sequence of \( R \)-modules \( M_i \) and maps \( f_i : M_i \to M_{i+1} \)

\[
\ldots \xrightarrow{f_{i-2}} M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \ldots
\]

is called exact if \( \text{Ker} f_i = \text{Im} f_{i-1} \) (\( \leq M_i \)) for all \( i \).

**Examples**

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

Exact sequences are a very handy notational convenience.
**Definition** A sequence of elements \( \{e_i\} \) of a module \( M \) are *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 \( \{e_i\} \) *generates* (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** The following are equivalent for an \( R \)-module \( F \).

- \( F \) has a basis \( \{e_i : i \in S\} \),
- \( F \cong \bigoplus_{i \in S} R \),
- There is a map \( i : S \to F \) such that for any \( R \)-module \( M \) and any map \( \phi : S \to M \), there exists a unique \( R \)-linear map \( h : F \to M \) such that \( h \circ i = \phi \).

**Proof.** (sketch)

- \( a) \Rightarrow b). \) Show that the map \( f : \bigoplus_{i \in S} R \to F \) given by \( f((\lambda_i)_{i \in S}) = \sum \lambda_i e_i \) is an isomorphism.
- \( b) \Rightarrow c). \) \( h((\lambda_j)_{j \in S}) \) must be \( \sum \lambda_i i(j) \), and this works.
- \( c) \Rightarrow a). \) Let \( e_j = i(j) \) 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 \( h = \text{projection} \), 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 \( F \), \( \text{rk}_R F \), is the cardinality of the basis \( |S| \). If \( R \) is a field, the rank is also called the dimension of the vector space.

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

**Exercise:** Show that \( \mathbb{Q} \) and \( \mathbb{Z}/n\mathbb{Z} \) \((n > 0)\) are not \( \mathbb{Z} \)-modules.

**Questions**

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

B. If \( F' \leq F \) and \( F', F \) are free, is it true that \( \text{rk}_R F' \leq \text{rk}_R F \)?

C. If \( F \) is free and \( N \leq F \), 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** If \( M \) is an \( R \)-module and \( I \) is an ideal of \( R \), then \( IM \leq M \) 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** If \( R \) is commutative and \( F \) is a free \( R \)-module, then \( \text{rk}_R F \) 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 $F \cong \bigoplus_{i \in S} R$, $F/IF \cong \bigoplus_{i \in S} R/I$, so $\text{rk}_R F = |S| = \dim_{R/I}(F/IF)$ is uniquely determined.

**Lemma** If $R$ is an ID and $F$ is a free $R$-module of rank $n$, then any $n+1$ elements of $F$ are linearly dependent.

Proof. Without loss of generality $F = R^n$. Let $K = \text{Frac}(R)$ be the field of fractions of $R$. Then $F$ is a sub-$R$-module of $K^n$. Any $n+1$ elements $\{x_1, \ldots, x_{n+1}\}$ in the vector space $K^n$ are linearly dependent over $K$, so there exist $\lambda_i = p_i/q_i \in K$ not all zero, such that $\sum \lambda_i x_i = 0$. But $q = \prod q_i \neq 0$ and $\sum (q \lambda_i) x_i = 0$, where $q \lambda_i \in R$ and $q \lambda_i$ are not all zero. Hence the $x_i$ are $R$-linearly dependent.

**Definition** 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 $M$.

Note: by the lemma, this definition agrees with the earlier definition on free modules.

**Exercises**

1. Show that $\text{rk}_\mathbb{Z} \mathbb{Z}/n\mathbb{Z} = 0$ for $n > 0$.
2. Show that $\text{rk}_\mathbb{Z} \mathbb{Q} = 1$.

**Theorem** If $R$ is an ID and $F', F$ are free $R$-modules with $F' \leq F$ then $\text{rk}_R F' \leq \text{rk}_R F$.

Proof. If $\text{rk}_R F = n$ then any $n+1$ elements of $F'$ are linearly dependent, so $\text{rk}_R F' \leq n$.

In general Question C is false even when $R$ is an ID. For example, the submodules of the (free) module $R$ are just the 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** Let $R$ be a commutative ring. If $N$ is a free $R$-module with basis $A = \{e_1, \ldots, e_n\}$ and $M$ is a free $R$-module with basis $B = \{f_1, \ldots, f_m\}$. Then for any $R$-linear map $f: N \to M$ there exists a unique $m \times n$ matrix $[f]_{B,A} = (a_{ij})$ 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 $C = \{g_1, \ldots, g_p\}$ and $g: N \to P$, then $[gf]_{C,A} = [g]_{C,B} [f]_{B,A}$ where the product is given by matrix multiplication.

**Exercise:** Suppose $[f]_{B,A} = A$. Show that if $A'$ and $B'$ are also bases for $N$ and $M$ respectively then $[f]_{B',A} = PA$ and $[f]_{B',A'} = AQ^{-1}$ for some invertible matrices $P$ and $Q$. [Hint: $P = [1]_{B',B}$]
Claim 3. $\varphi$ is maximality of factor $y$ since

Claim 2. For all $I$ maximality of

Claim 1. For all $I$ maximality of

Lemma 7262 Modules over PIDs Spring 2003

Proof. Order $X$ by inclusion and apply Zorn’s lemma. If $C = \{I_\alpha : \alpha \in S\}$ is a chain of ideals, let $I = \bigcup I_\alpha$. 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 $I_\alpha$, so $I = (a) \subseteq I_\alpha \subseteq I$ and $I = I_\alpha$ is an upper bound for $C$. By Zorn, $X$ has a maximal element.

Theorem If $R$ is a PID and $M$ is a submodule of a free module $N \cong R^n$ of finite rank $n$, then $M$ is free of rank $m \leq n$. Moreover, there exists a basis $\{y_1, \ldots, y_n\}$ of $N$ and non-zero elements $a_1, \ldots, a_m \in R$ such that $\mathcal{a}_1 | a_2 | \cdots | a_m$ and $\{a_1 y_1, \ldots, a_m y_m\}$ is a basis for $M$.

Proof. Without loss of generality $N = R^n$. Write $\pi_i$ for the projection map of $N$ onto the $i$th 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 $\phi : N \to R$ and let $I_\phi = \phi(M)$. Pick a map $\nu : N \to R$ such that $I_\nu = (a_1)$ is maximal among these ideals. If $a \in M$ then there is one of the projections $\pi_i(a)$ non-zero, so $I_{a_i} \neq (0)$. Hence by maximality $a_1 \neq 0$. Also, there exists $y \in M$ such that $\nu(y) = a_1$.

Claim 1. For all $\phi : N \to R$, $a_1 | \phi(y)$. Pick any $\phi$ 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 $\phi' : N \to R$ is the $R$-linear map $r_1 \nu + r_2 \phi$. But then $d \in I_{\phi'}$, so $I_{\phi'} = (a_1) \subseteq (d) \subseteq I_{\phi'}$. By maximality of $I_{\nu'}$, $a_1 | d$, so $a_1 | \phi(y)$.

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

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

Claim 3. $N = R y_1 + \ker \nu$, $M = R a_1 y_1 + (M \cap \ker \nu)$.

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 $N = R y_1 + \ker \nu$. If $x \in R y_1 \cap \ker \nu$ then $x = a_1 y_1$ and $0 = \nu(x) = a$. Hence $x = 0$. Thus $N = R y_1 + \ker \nu$. A similar argument (using the fact that $\nu(M) = (a_1)$) shows $M = R a_1 y_1 + (M \cap \ker \nu)$.

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

If $\{x_1, \ldots, x_k\}$ is linearly independent in $M \cap \ker \nu$ then $\{y, x_1, \ldots, x_k\}$ 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 $\text{rk}_R \ker \nu < \text{rk}_R N$.

Claim 5. $M$ is free.

Using induction on $\text{rk}_R M$ we can assume $M \cap \ker \nu$ is free with basis $\{x_1, \ldots, x_k\}$. Then $M = R a_1 y_1 + (M \cap \ker \nu)$ has basis $\{a_1 y_1, x_1, \ldots, x_k\}$.

Completion of Proof.

Applying claim 5 to $\ker \nu \leq N$ we see that $\ker \nu$ is free. Claim 4 shows $\text{rk} \ker \nu < n$, so using induction on $n$ and considering $M \cap \ker \nu$ as a submodule of the free module $\ker \nu$ we have a basis $\{y_2, \ldots, y_n\}$ of $\ker \nu$ and basis $\{a_2 y_2, \ldots, a_m y_m\}$ of $M \cap \ker \nu$. Hence $\{y_1, \ldots, y_n\}$ is a basis of $N$ and $\{a_1 y_1, \ldots, a_m y_m\}$ is a basis for $M$ where $a_2 | a_3 | \cdots | a_m$. It remains to show $a_1 | a_2$.

Let $d = r_1 a_1 + r_2 a_2$ be the gcd of $a_1$ and $a_2$ and let $\phi = r_1 \pi_1 + r_2 \pi_2$ where $\pi_i$ are the projections to coordinates given by the basis $\{y_1, \ldots, y_n\}$. 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 $I_{\nu'}$ $(d) = (a_1)$ and $a_1 | a_2$. \qed
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 $a_1,\ldots, a_m$ with $a_i \neq 0$, $a_i \neq \text{unit}$, $a_1 \mid a_2 \mid \cdots \mid a_m$ 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 $x_1,\ldots, x_n$ and consider the $R$-linear map $\phi$ from a free module $N$ with basis $\{e_1,\ldots, e_n\}$ which sends $e_i$ to $x_i$. Then $x_i \in \text{Im} \phi$, so $\phi$ is surjective and $M \cong N/\text{Ker} \phi$. But Ker $\phi \leq N$, so there is a (new) basis $\{y_1,\ldots, y_n\}$ of $N$ such that Ker $\phi$ has basis $\{a_1 y_1,\ldots, a_m y_m\}$. Using this basis we have an isomorphism $N \cong R \oplus R \oplus \cdots \oplus R$ in which Ker $\phi$ is $Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_m \oplus (0) \oplus \cdots \oplus (0)$. But then $M \cong N/\text{Ker} \phi \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R'$ where $r = n - m$. Finally, any terms $R/(a_i)$ with $a_i = \text{unit}$ can be dropped, so we may assume the $a_i$ are not units.

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

**Proof.** $p^i M = (p_i)/+(a)/(a) = (p^i, a)/(a)$, so by the 2nd Isomorphism theorem, $p^{i-1}M/p^i M = (p^{i-1}, a)/(p^i, a)$. If $p^i \nmid a$ then $(p^{i-1}, a) = (p, a) = (\gcd(p^{i-1}, a))$, so $p^{i-1}M/p^i M = 0$. If $p^i \mid a$ then $(p^{i-1}, a)/(p, a)$ which, however, if $f: R \rightarrow (p^{i-1})/(p^i)$ is defined by $f(x) = p^{i-1}x + (p)$ then Ker $f = (p)$, so $(p^{i-1})/(p^i) \cong R/(p)$.

**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 $p^{i-1} M/p^i M \cong (R/(p))^k \cong (R/(p))^{k'}$ where $k = r + \#\{ j : p^i \mid a_j \}$, $k' = r' + \#\{ j : p^i \mid a_j' \}$. But $p^{i-1} M/p^i M = N/pN$ 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 $k = \dim_{R/(p)}(p^{i-1} M/p^i M) = k'$. Fixing $p$ and letting $i \rightarrow \infty$ 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 $p^i \mid a_1,\ldots, a_{m-s}$ and $p^i \mid a_{m-s+1},\ldots, a_m$. 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 $(a_i) = (a_i')$.

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

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 primes $p_1,\ldots, p_m$ (not necessarily distinct) and integers $b_1,\ldots, b_m > 0$, $r \geq 0$, 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 1st form of the Fundamental Theorem of Finitely generated modules over a PID using the Chinese Remainder Theorem: If $a = up_1^{b_1} \ldots p_r^{b_r}$ where $p_i$ are distinct primes and $a$ 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.

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

**Exercise:** Show that $r$ is the rank of $M$. [Hint: if $\{x_1,\ldots, x_k\}$ are linearly independent in $M$ then $\{a_1 x_1,\ldots, a_m x_k\}$ are linearly independent and lie in the submodule $R^r$ of $M$.]
Theorem Let $R$ be a PID and let $N$ and $M$ be free $R$-modules of rank $n$ and $m$ respectively. Let $\phi: N \to M$ be $R$-linear. Then there exist bases $A$ of $N$ and $B$ of $M$ such that $[\phi]_{B,A}$ is of the form

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

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 $M/\text{Im} \phi$ is clearly isomorphic to $R/(a_1) \oplus \cdots \oplus R/(a_r) \oplus R^{n-r}$. The result follows from the uniqueness of the invariant factors of this module.

Existence (Non-constructive)

Since $\text{Im} \phi \leq M$ and $M$ is free there is a basis $B = \{y_1, \ldots, y_m\}$ of $M$ such that $\text{Im} \phi$ has basis $\{a_1y_1, \ldots, a_ry_r\}$. Choose $y'_i \in N$ so that $\phi(y'_i) = a_iy_i$. Then there exists a unique linear map $\psi: \text{Im} \phi \to N$ such that $\psi(a_iy_i) = y'_i$. Let $\{z_1, \ldots, z_k\}$ be a basis for the (free) module $\ker \phi \leq N$. Since $\phi \psi = 1_{\text{Im} \phi}$, we have $M \cong \text{Im} \psi \oplus \ker \phi$, and so $A = \{y'_1, \ldots, y'_r, z_1, \ldots, z_k\}$ is a basis for $M$. The matrix $[\phi]_{B,A}$ 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 $d: R \to \mathbb{N}$ 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 $r = 0$.

Definition 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 $\phi$ and bases $A, A', B, B'$ with $A = [\phi]_{B,A}$ and $B = [\phi]_{B',A'}$.

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 $u \in R$, $U_i(u) = I_n + (u - 1)E_{ii}$, so $U_i(u)^{-1} = U_i(u^{-1})$ and $U_i(u)$ is invertible.

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

1. the matrix $AT_{ij}(\lambda)$ is obtained from $A$ by adding $\lambda$ times the $i$th column to the $j$th column of $A$,
2. the matrix $AS_{ij}$ is obtained by swapping the $i$th and $j$th columns of $A$,
3. the matrix $AU_i(u)$ is obtained by multiplying the $i$th 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
\[
\begin{pmatrix}
a_1 & 0 & \ldots & 0 \\
0 & & & \\
\vdots & & A' & \\
0 & & & 
\end{pmatrix}
\]
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 $i$th row with the 1st row and the $j$th 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 $i$th row for each $i$ we obtain a new matrix with 1st column $a_1, r_2, \ldots, r_m$. 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 $i$th row to the 1st row so that the 1st row becomes $a_1, a_2, \ldots, a_n$. Now add multiples of the 1st column to the other columns as above to get the 1st row $a_1, r_2, \ldots, r_n, a_{ij} = q_j a_1 + r_j, r_j = 0$ 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
\[
\begin{pmatrix}
a_2 & \ldots & 0 & \ldots & 0 \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
0 & \ldots & a_r & \ldots & 0 \\
0 & \ldots & 0 & \ldots & 0
\end{pmatrix}
\]
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. \hfill \Box

7262 Application to linear algebra Spring 2003

Recall that if $V$ is a $K$-vector space and $T: V \to V$ 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 $T^{i+1}(v) = T(T^i(v))$. Recall also that $K[X]$ is a PID, indeed it is a Euclidean domain if we define $d(f) = \deg f$.

**Lemma** Let $\bar{A} = \{\bar{e}_1, \ldots, \bar{e}_n\}$ be a $K$-basis for $V$ and let $N$ be a free $K[X]$-module with basis $A = \{e_1, \ldots, e_n\}$. Let $[T]_{\bar{A},A} = A$ and define maps $\psi: N \to N$ to have matrix $XI_n - A$ with respect to the basis $A$, and $\phi: N \to V$ so that $\phi(e_i) = \bar{e}_i$. Then the sequence
\[
N \xrightarrow{\psi} N \xrightarrow{\phi} V \to 0
\]
is exact.

**Proof.** We need to show $\phi$ is surjective and $\text{Im } \psi = \text{Ker } \phi$. First, $\phi$ is surjective since $\text{Im } \phi$ contains the elements $\bar{e}_i$ of a basis. Now $\psi(e_i) = Xe_i - \sum a_{ji} e_j$, so $\phi(\psi(e_i)) = T(e_i) - \sum a_{ji} \bar{e}_j = \cdots$. 

\[ \sum a_{ji} \bar{e}_j - \sum a_{ji} e_j = 0. \] Since this holds for each \( e_i, \phi \psi = 0 \) and \( \text{Ker} \phi \supseteq \text{Im} \phi \). Now assume \( v = \sum c_i(A) e_i \in \text{Ker} \phi \). 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 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 \( v = \psi(u) \in \text{Im} \psi \). Hence \( \text{Ker} \phi \subseteq \text{Im} \psi \). \hfill \Box

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

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

**Definition** 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 \( \phi: N \rightarrow N \) and bases \( A, A' \) of \( N \) such that \( A = [\phi]_{A,A} \) and \( B = [\phi]_{A',A'} \).

**Rational Canonical Form**

**Definition** Let \( K \) be a field and \( f(X) = \sum_{i=0}^{n} f_i X^i \in K[X] \) a monic polynomial. The **Companion matrix** to \( f \) is the matrix

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

where \( n = \deg f \).

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

\[
\begin{pmatrix}
C(a_1) & 0 & \cdots & 0 \\
0 & C(a_2) & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & C(a_r)
\end{pmatrix}
\]

where \( a_i(X) \in K[X] \) are the 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 \( V \cong K[X]/(a_1) \oplus \cdots \oplus K[X]/(a_r) \), 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 \( \{1, X, X^2, \ldots, X^{\deg a_i - 1}\} \) of \( K[X]/(a_i) \). \hfill \Box

**Definition** 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 \( m_A | f \). 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 provided the ideal is not $(0)$. Note that $m_A$ need not be irreducible.

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

**Proof.** (sketch)
The matrix $f(A)$ corresponds to multiplication by $f(X)$ in the module $K[X]/(a_1) \oplus \cdots \oplus K[X]/(a_r)$. But this is the zero map iff $a_i | f$ for all $i$. For the characteristic polynomial, note that if $B$ is similar to $A$ then $\det(XI_n - B) = \det(XI_n - PAP^{-1}) = \det(P(XI_n - A)P^{-1}) = \det(XI_n - A)$, so it is enough to check this for the Rational Canonical Form of a matrix.

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

**Proof.** $m_A = a_r | a_1 \ldots a_r = f$.

**Jordan Normal Form**

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

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

Note: $J_n(\lambda)$ 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 $\{1, (X - \lambda), \ldots, (X - \lambda)^{n-1}\}$.

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

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

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

**Corollary** A matrix is similar to a diagonal matrix iff $m_A(X)$ splits into distinct linear factors.
Let \( \lambda, \mu \) satisfy this condition. Hence \( f \circ g \) such that \( h = \phi \circ (\lambda \otimes x + \mu \otimes y, z) = \lambda \phi(x, z) + \mu \phi(y, z) \) and \( \phi(x, \lambda z + \mu w) = \lambda \phi(x, z) + \mu \phi(x, w) \) hold 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.

**Exercises**

1. Show that for any bilinear map \( \phi \), \( \phi(x, 0) = \phi(0, y) = 0 \).
2. If \( R \) is a subring of the ring \( S \) then the map \( S \times S \to S \) given by multiplication in \( S \) is bilinear.
3. Show that any bilinear map \( R^n \times R^m \to R \) can be represented by a unique matrix \( A \) so that \( \phi(u, v) = u^T Av \). (Elements of \( R^n \), \( R^m \) are considered as column vectors and \( T \) denotes transpose.

**Definition** The tensor product of two modules \( N_1 \) and \( N_2 \) is an \( R \)-module \( N_1 \otimes_R N_2 \), and a bilinear map \( \otimes : N_1 \times N_2 \to N_1 \otimes_R N_2 \) such that the following universal property holds. If \( M \) is any module and \( \phi : N_1 \times N_2 \to M \) is bilinear, then there exists a unique \( R \)-linear map \( h : N_1 \otimes_R N_2 \to M \) such that \( h(x \otimes y) = \phi(x, y) \) for all \( x \in N_1 \), \( y \in N_2 \).

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

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

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

\[
\lambda e_{x,z} + \mu e_{y,z} = e_{\lambda x + \mu y, z}, \quad - \lambda e_{x,z} + \mu e_{x,w} = e_{x, \lambda z + \mu w}
\]

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 \( \otimes : N_1 \times N_2 \to N_1 \otimes_R N_2 \) be defined as \( x \otimes y = e_{x,y} + K \in F/K \). We now check the various conditions.

1. \( \otimes : N_1 \times N_2 \to N_1 \otimes_R N_2 \) is bilinear.
\[
(\lambda x + \mu y) \otimes z = e_{\lambda x + \mu y, z} + K = (\lambda e_{x,z} + \mu e_{y,z}) - (\lambda e_{x,z} + \mu e_{y,z}) + K = (\lambda e_{x,z} + \mu e_{y,z}) + K = \lambda (x \otimes z) + \mu (y \otimes z).
\]

2. If \( \phi : N_1 \times N_2 \to M \) is bilinear then there exists \( h : N_1 \otimes_R N_2 \to M \) such that \( h(x \otimes y) = \phi(x, y) \).

Define \( h' : F \to M \) on the basis \( e_{x,y} \) of \( F \) by \( h'(e_{x,y}) = \phi(x, y) \). Clearly \( K \subseteq \ker h' \) so \( h' \) induces a map \( h : F/K \to M \) by \( h(z + K) = h'(z) \). Now \( h(x \otimes y) = h'(e_{x,y}) = \phi(x, y) \) as desired.

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). The following are a few examples.

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

**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 $x \otimes y = \sum \lambda_i \mu_j (e_i \otimes f_j)$. Hence $B$ 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 $\phi: N \times M \to R$ 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 $h: N \otimes M \to R$ 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: $\mathbb{C} \otimes \mathbb{C} \cong \mathbb{C}$, but $\mathbb{C} \otimes_R \mathbb{C} \cong \mathbb{R}^2 \otimes_R \mathbb{R}^2 \cong \mathbb{R}^4$, but $\mathbb{C} \not\cong \mathbb{R}^4$, so the subscript on the $\otimes$ is important.

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

**Proof.** Define $\otimes: N \times R/I \to N/I N$ 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 $\phi: N \times R/I \to M$ is bilinear, define $h': N 	o M$ 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 $IN \subseteq \ker h'$ and $h'$ induces a map $h: N/I N \to M$ such that $h(x \times (r + I)) = h(rx + IN) = h'((rx + I)) = \phi(rx, 1 + I) = \phi(x, r + I)$. Conversely if $h: N/I N \to M$ has this property then $h(x + IN) = h(x \times (1 + I)) = \phi(x, 1 + I) = h'(x)$ and so $h$ is uniquely determined.

**Exercises** (All the following exercises should be done using universal properties.)

1. Show that $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\gcd(n,m)\mathbb{Z}$.
2. Show that $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.
3. If $f: N \to N'$ and $g: M \to M'$ are $R$-linear, show that there exists a unique $R$-linear map $f \otimes g: N \otimes_R M \to N' \otimes_R M'$ such that $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$.
4. Show that tensor products are ‘commutative’, i.e., there exists an isomorphism $\phi: N \otimes_R M \to M \otimes_R N$ such that $\phi(x \otimes y) = y \otimes x$.
5. Show that tensor products are ‘associative’, i.e., $N_1 \otimes_R (N_2 \otimes_R N_3) \cong (N_1 \otimes_R N_2) \otimes_R N_3$.
6. Show that tensor products are ‘distributive’ over direct sums, i.e., $N \otimes_R (M \oplus M') \cong (N \otimes_R M) \oplus (N \otimes_R M')$. 
Throughout this section we shall assume all rings are commutative.

**Definition** An $R$-algebra is a ring $S$ with a ring homomorphism $i: R \to S$ such that $\text{Im } i$ 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 $\text{Im } i$ is automatically in the center.

In many cases $R$ will be a subring of $S$ and $i$ will be inclusion.

**Examples**

1. Any ring $R$ is a $\mathbb{Z}$-algebra.
2. $\mathbb{C}$ is an $\mathbb{R}$-algebra. In general if $K/F$ is a field extension then $K$ is an $F$-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 $i_1: R \to S_1$, $i_2: R \to S_2$ are $R$-algebras then an $R$-algebra homomorphism is a ring homomorphism $f: S_1 \to S_2$ such that $f(i_1(\lambda)) = i_2(\lambda)$.

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

**Proof.** Any element of $S \otimes_R N$ can be written as a sum $\sum \lambda_i \otimes x_i$. We wish to define for $\lambda \in S$, $\lambda(\lambda_i \otimes x_i) = (\lambda \lambda_i) \otimes x_i$ and extend to $S \otimes N$ linearly: $\lambda(\sum \lambda_i \otimes x_i) = \sum (\lambda \lambda_i \otimes x_i)$. We need to check that this is well-defined. Fix $\lambda \in S$ and consider the map $\phi_{\lambda}: S \times N \to S \otimes N$ 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 $h_{\lambda}: S \otimes N \to S \otimes N$ such that $h_{\lambda}(\mu \otimes x) = (\lambda \mu) \otimes x$.

It is not hard to check that $h_{\lambda \lambda} = h_{\lambda} h_{\lambda'}$ 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.

One important case of extension of scalars is to turn an $R$-module into a Frac $(R)$-module.

**Definition** 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 $\exists u \in S: us'm = usm'$. Write $\frac{m}{s}$ for the equivalence class of $(m, s)$.

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

**Proof.** (sketch) Addition is defined by $\frac{m}{s} + \frac{m'}{s'} = \frac{sm + szm'}{ss'}$, scalar multiplication is defined by $\frac{m}{s} \cdot \frac{m'}{s'} = \frac{mm'}{ss'}$. 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 $\frac{0}{1}$, identity for $+$), etc. etc.
homomorphism. 

Now suppose \( K \) is a multiplicatively closed multiplicative set of \( M \) and \( \phi \) is a ring homomorphism if the multiplication in \( K \otimes M \) is well-defined, associative, has identity 1

\[ s \otimes 1 = 1 \otimes s = s \]

for all \( s \in S \). Using the isomorphism \( S \otimes M \cong M \) we can write

\[ h(\xi) = \phi(\frac{1}{s}, x) \]

is uniquely determined. Conversely define \( h(\xi) = \phi(\frac{1}{s}, x) \) and show that this is well-defined, \( R \)-linear, and \( h(\xi \otimes x) = h(\frac{v}{w}) = \phi(\frac{1}{s}, rx) = r \phi(\frac{1}{s}, x) = \phi(\xi, x) \). Finally, check that the scalar multiplication by \( S^{-1}R \) agrees on \( S^{-1}M \) with that on \( S^{-1}R \otimes M \).

**Theorem** Let \( R \) be an ID with field of fractions \( K \). If \( M \) is an \( R \)-module then \( \text{rk}_R M = \dim_K K \otimes_R M \).

**Proof.** Assume \( \{ x_i : i \in S \} \) is \( K \)-linearly independent in \( M \). Consider the subset \( \{ 1 \otimes x_i : i \in S \} \) of \( K \otimes M \). If \( \lambda_i \in K \) then \( \lambda_i = \frac{p_i}{q_i} \) with \( p_i, q_i \in R \). If \( q = \prod q_i \) then we can write \( \lambda_i = \frac{p_i}{q_i} \) with common denominator \( q \). If \( \sum \lambda_i (1 \otimes x_i) = 0 \) then \( 0 = q \sum \lambda_i (1 \otimes x_i) = \sum p_i (1 \otimes x_i) = 1 \otimes \sum p_i x_i \).

Using the isomorphism \( K \otimes M \cong S^{-1}M \) with \( S = R \setminus \{ 0 \} \) we get \( 1 \otimes x = 0 \) iff \( \frac{v}{w} = \frac{1}{s} \) in \( S^{-1}M \) which is iff \( \exists u \in S : ux = 0 \). Hence \( \sum u p_i x_i = 0 \) for some \( u \neq 0 \). But then \( u p_i = 0 \) for all \( i \), so \( \lambda_i = 0 \) for all \( i \). Hence \( \{ 1 \otimes x_i : i \in S \} \) is \( K \)-linearly independent and \( \text{rk}_R M \leq \dim_K K \otimes_R M \).

Now suppose \( \{ v_i : i \in S \} \) is \( K \)-linearly independent in \( K \otimes M \). Using \( K \otimes M \cong S^{-1}M \) we can write \( v_i = \frac{a_i}{b_i} \). Suppose \( \sum \lambda_i x_i = 0 \in M \) with \( \lambda_i \in R \). Then \( \sum (q_i \lambda_i) v_i = 0 \) with \( q_i \lambda_i \in K \). Hence \( q_i \lambda_i = 0 \) and so \( \lambda_i = 0 \). Thus \( \{ x_i : i \in S \} \) is linearly independent in \( M \) and \( \text{rk}_R M \geq \dim_K K \otimes_R M \).

**Tensor products of \( R \)-algebras**

**Theorem** 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 \( (s_1 \otimes s_2)(s'_1 \otimes s'_2) = s_1 s'_1 \otimes s_2 s'_2 \).

**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 \( i : R \to S_1 \otimes_R S_2 \) 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 \( \phi_{s_1, s_2} : S_1 \times S_2 \to S_1 \otimes_R S_2 \) by \( \phi_{s_1, s_2}(s'_1, s'_2) = s_1 s'_1 \otimes s_2 s'_2 \). This is \( R \)-bilinear. Then there exists an \( R \)-linear \( h_{s_1, s_2} \in \text{Hom}_R(S_1 \otimes S_2, S_1 \otimes S_2) \) with \( h_{s_1, s_2}(s'_1 \otimes s'_2) = s_1 s'_1 \otimes s_2 s'_2 \). Now \( \text{Hom}_R(\ldots) \) is an \( R \)-module and the map \( h : S_1 \times S_2 \to \text{Hom}_R(S_1 \otimes S_2, S_1 \otimes S_2) \) given by \( (s_1, s_2) \to h_{s_1, s_2} \) is \( R \)-bilinear (check this). Hence there is a map \( g : S_1 \otimes S_2 \to \text{Hom}_R(S_1 \otimes S_2, S_1 \otimes S_2) \) with \( g(s_1 \otimes s_2)(s'_1 \otimes s'_2) = s_1 s'_1 \otimes s_2 s'_2 \). 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 \( s_1 \otimes s_2 \)).

**Exercise:** Show that \( R[X] \otimes_R R[Y] \cong R[X, Y] \) as an \( R \)-algebra. [Hint: first show this is an isomorphism of \( R \)-modules using \( f \otimes g \mapsto f(X)g(Y) \), then check that the isomorphism is a ring homomorphism.]
Definition A multilinear map $\phi : M^k \rightarrow N$ is a map that is $R$-linear in each variable, i.e.,
$\phi(x_1, \ldots, \lambda x_i + \mu x_j, \ldots, x_k) = \lambda \phi(x_1, \ldots, x_i, \ldots, x_k) + \mu \phi(x_1, \ldots, x_i', \ldots, x_k).$ The multilinear map $\phi$ is symmetric if $\phi(x_1, \ldots, x_k) = \phi(x_{\pi(1)}, \ldots, x_{\pi(k)})$ for all permutations $\pi \in S_k.$ The map $\phi$ is skew-symmetric if $\phi(x_1, \ldots, x_k) = \operatorname{sgn}(\pi)\phi(x_{\pi(1)}, \ldots, x_{\pi(k)})$ where $\operatorname{sgn}(\pi) = \pm 1$ is the sign of the permutation $\pi.$ The map $\phi$ is alternating if $\phi(x_1, \ldots, x_k) = 0$ 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 If $M$ is an $R$-module and $k \geq 0$ then there exists modules $T^k(M)$, (resp. $S^k(M)$, $\wedge^k(M)$), and multilinear (resp. symmetric, alternating) maps $\psi$ from $M^k$ to $T^k(M)$ (resp. $S^k(M)$, $\wedge^k(M)$) such that for any multilinear (resp. symmetric, alternating) map $\phi : M^k \rightarrow N$ there exists a unique $R$-linear map $h$ such that $h \circ \psi = \phi.$

Proof. (sketch) Let $T^0(M) = R$ and inductively define $R$-modules $T^{k+1}(M) = T^k(M) \otimes_R M,$ so that $T^k(M)$ is the tensor product of $k$ copies of $M.$ The Theorem for $T^k(M)$ holds by induction on $k$ and the universal property of tensor products. For symmetric maps, define $S^k(M) = T^k(M)/C^k(M),$ where $C^k(M)$ is the submodule of $T^k(M)$ 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 $\psi(x_1, \ldots, x_k) = (x_1 \otimes \cdots \otimes x_k) + C^k(M).$ It is easy to check that $\psi$ is symmetric, $h$ exists (use the result for $T^k(M)$ and show that $\operatorname{Ker} h \subseteq C^k(M)$), $h$ is unique (the $x_1 \otimes \cdots \otimes x_k + C^k(M)$ generate $S^k(M)).$ For alternating maps, define $\wedge^k(M) = T^k(M)/D^k(M),$ where $D^k(M)$ is the submodule of $T^k(M)$ 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 to the symmetric case. $\square$

Example $T^0(M) \cong S^0(M) \cong \wedge^0(M) \cong R,$ $T^1(M) \cong S^1(M) \cong \wedge^1(M) \cong M.$

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

$\otimes : T^i(M) \times T^j(M) \rightarrow T^{i+j}(M),$
$\odot : S^i(M) \times S^j(M) \rightarrow S^{i+j}(M),$
$\wedge : \wedge^i(M) \times \wedge^j(M) \rightarrow \wedge^{i+j}(M).$

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

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

Lemma $T(M), S(M), \wedge(M)$ 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 $a, b, c \in M \cong \wedge^1(M),$ $(a \wedge b) \wedge c = -a \wedge c \wedge b = +c \wedge (a \wedge b).$
Theorem Let $M$ be a free $R$-module of rank $n$ with basis $\{e_1, \ldots, e_n\}$, then

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

$$\mathcal{S}^k(M)$$ is free of rank $\binom{n+k-1}{k}$ with basis $\{e_{i_1} \circ \cdots \circ e_{i_k} : 1 \leq i_1 \leq \cdots \leq i_k \leq n\}$,

$$\wedge^k(M)$$ is free of rank $\binom{n}{k}$ with basis $\{e_{i_1} \wedge \cdots \wedge e_{i_k} : 1 \leq i_1 < \cdots < i_k \leq n\}$.

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

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

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

$$(x_1i + x_2j + x_3k) \wedge (y_1i + y_2j + y_3k) = (x_2y_3 - x_3y_2)\tilde{i} + (x_3y_1 - x_1y_3)\tilde{j} + (x_1y_2 - x_2y_1)\tilde{k}.$$ 

If we compose this map with the isomorphism $\wedge^2(M) \to \wedge^1(M)$ given by sending $\tilde{i}, \tilde{j}, \tilde{k}$ to $i, j, k$ 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 $\wedge^1(M)$ can be thought of as oriented line segments, the bivectors $\wedge^2(M)$ as oriented area elements, etc.

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

- $\mathcal{T}^k(f): \mathcal{T}^k(M) \to \mathcal{T}^k(N)$, $\mathcal{T}^k(f)(x_1 \otimes \cdots \otimes x_k) = f(x_1) \otimes \cdots \otimes f(x_k)$,
- $\mathcal{S}^k(f): \mathcal{S}^k(M) \to \mathcal{S}^k(N)$, $\mathcal{S}^k(f)(x_1 \circ \cdots \circ x_k) = f(x_1) \circ \cdots \circ f(x_k)$,
- $\wedge^k(f): \wedge^k(M) \to \wedge^k(N)$, $\wedge^k(f)(x_1 \wedge \cdots \wedge x_k) = f(x_1) \wedge \cdots \wedge f(x_k)$.

Proof. Use universal properties. □

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

Proof. Suppose $M$ has basis $\{e_1, \ldots, e_n\}$, then $\wedge^n(M)$ is of rank 1 with basis $\{e_1 \wedge \cdots \wedge e_n\}$. If $f$ has matrix $a_{ij}$ with respect to the basis $\{e_1, \ldots, e_n\}$ then $\wedge^n(f)(e_1 \wedge \cdots \wedge e_n) = f(e_1) \wedge \cdots \wedge f(e_n) = (\sum_{i_1} a_{i_11}e_{i_1}) \wedge \cdots \wedge (\sum_{i_n} a_{i_n1}e_{i_n}) = \sum_{i_1,i_2,\ldots,i_n} a_{i_11}a_{i_22} \cdots a_{i_n1}e_{i_1} \wedge \cdots \wedge e_{i_n}$. However, if $i_i = i_j$ for $i \neq j$ then $e_{i_1} \wedge \cdots \wedge e_{i_n} = 0$. Hence we can assume $i_i = j$ for some permutation $\pi \in S_n$. Also $e_{\pi(1)} \wedge \cdots \wedge e_{\pi(n)} = \text{sgn}(\pi)e_1 \wedge \cdots \wedge e_n$. Hence $\wedge^n(f)$ acts as multiplication by $\sum_{\pi \in S_n} a_{\pi(1)} \cdots a_{\pi(n)}$. But this is just $\det(a_{ij})$. □

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 the fact that $\wedge^n(f \circ g) = \wedge^n(f) \circ \wedge^n(g)$. 