28. Exterior powers

While many of the arguments here have analogues for tensor products, it is worthwhile to repeat these arguments with the relevant variations, both for practice, and to be sensitive to the differences.

1. *Desiderata*

Again, we review missing items in our development of linear algebra.

We are missing a development of determinants of matrices whose entries may be in commutative rings, rather than fields. We would like an *intrinsic* definition of determinants of endomorphisms, rather than one that depends upon a choice of coordinates, even if we eventually prove that the determinant is independent of the coordinates. We anticipate that Artin's axiomatization of determinants of matrices should be mirrored in much of what we do here.

We want a direct and natural proof of the Cayley-Hamilton theorem. Linear algebra over *fields* is insufficient, since the introduction of the indeterminate x in the definition of the characteristic polynomial takes us outside the class of vector spaces over fields.

We want to give a conceptual proof for the *uniqueness* part of the structure theorem for finitely-generated modules over principal ideal domains. Multi-linear algebra over fields is surely insufficient for this.

2. *Definitions, uniqueness, existence*

Let R be a commutative ring with 1. We only consider R-modules M with the property that $1 \cdot m = m$ for all $m \in M$. Let M and X be R-modules. An R-multilinear map

$$B : \underbrace{M \times \ldots \times M}_{n} \longrightarrow X$$

is **alternating** if $B(m_1, \ldots, m_n) = 0$ whenever $m_i = m_j$ for two indices $i \neq j$.

As in earlier discussion of free modules, and in discussion of polynomial rings as free algebras, we will define exterior powers by *mapping properties*. As usual, this allows an easy proof that exterior powers (if they exist) are *unique* up to *unique isomorphism*. Then we give a modern construction.

An exterior n^{th} power $\bigwedge_R^n M$ over R of an R-module M is an R-module $\bigwedge_R^n M$ with an alternating R-multilinear map (called the **canonical map**)[1]

$$\alpha : \underbrace{M \times \ldots \times M}_{n} \longrightarrow \bigwedge\nolimits_R^n M$$

such that, for every alternating R-multilinear map

$$\varphi : \underbrace{M \times \ldots \times M}_{n} \longrightarrow X$$

there is a *unique* R-linear map

$$\Phi : \bigwedge\nolimits_R^n M \longrightarrow X$$

such that $\varphi = \Phi \circ \alpha$, that is, such that the diagram

$$\begin{tikzcd}
\bigwedge_R^n M \arrow[dr, dashed, "\Phi"] & \\
M \times \ldots \times M \arrow[u, "\alpha"] \arrow[r, "\varphi"] & X
\end{tikzcd}$$

commutes.

[2.0.1] **Remark:** If there is no ambiguity, we may drop the subscript R on the exterior power $\bigwedge_R^n M$, writing simply $\bigwedge^n M$.

The usual notation does not involve any symbol such as α, but in our development it is handy to have a name for this map. The standard notation denotes the image $\alpha(m \times n)$ of $m \times n$ in the exterior product by

$$\text{image of } m_1 \times \ldots \times m_n \text{ in } \bigwedge\nolimits^n M = m_1 \wedge \ldots \wedge m_n$$

In practice, the implied R-multilinear alternating map

$$M \times \ldots \times M \longrightarrow \bigwedge\nolimits^n M$$

called α here is often left anonymous.

[1] There are many different *canonical maps* in different situations, but context should always make clear what the properties are that are expected. Among other things, this potentially ambiguous phrase allows us to avoid trying to give a permanent symbolic name to the maps in question.

The following proposition is typical of uniqueness proofs for objects defined by mapping property requirements. It is essentially identical to the analogous argument for tensor products. Note that internal details of the objects involved play no role. Rather, the argument proceeds by manipulation of arrows.

[2.0.2] **Proposition:** Exterior powers $\alpha : M \times \ldots \times M \longrightarrow \bigwedge^n M$ are unique up to unique isomorphism. That is, given two exterior n^{th} powers

$$\alpha_1 : M \times \ldots \times M \longrightarrow E_1$$

$$\alpha_2 : M \times \ldots \times M \longrightarrow E_2$$

there is a *unique R-linear isomorphism* $i : E_1 \longrightarrow E_2$ such that the diagram

$$\begin{tikzcd} & E_1 \arrow[dd, "i"] \\ M \times \ldots \times M \arrow[ur, "\alpha_1"] \arrow[dr, "\alpha_2"'] & \\ & E_2 \end{tikzcd}$$

commutes, that is, $\alpha_2 = i \circ \alpha_1$.

Proof: First, we show that for a n^{th} exterior power $\alpha : M \times \ldots \times M \longrightarrow T$, the only map $f : E \longrightarrow E$ compatible with α is the identity. That is, the identity map is the only map f such that

$$\begin{tikzcd} & E \arrow[dd, "f"] \\ M \times \ldots \times M \arrow[ur, "\alpha"] \arrow[dr, "\alpha"'] & \\ & E \end{tikzcd}$$

commutes. Indeed, the definition of a n^{th} exterior power demands that, given the alternating multilinear map

$$\alpha : M \times \ldots \times M \longrightarrow E$$

(with E in the place of the earlier X) there is a unique linear map $\Phi : E \longrightarrow E$ such that the diagram

$$\begin{tikzcd} E \arrow[dr, dashed, "\Phi"] & \\ M \times \ldots \times M \arrow[u, "\alpha"] \arrow[r, "\alpha"] & E \end{tikzcd}$$

commutes. The identity map on E certainly has this property, so is the *only* map $E \longrightarrow E$ with this property.

Looking at two n^{th} exterior powers, first take $\alpha_2 : M \times \ldots \times M \longrightarrow E_2$ in place of the $\varphi : M \times \ldots \times M \longrightarrow X$. That is, there is a unique linear $\Phi_1 : E_1 \longrightarrow E_2$ such that the diagram

$$\begin{tikzcd} E_1 \arrow[dr, dashed, "\Phi_1"] & \\ M \times \ldots \times M \arrow[u, "\alpha_1"] \arrow[r, "\alpha_2"] & E_2 \end{tikzcd}$$

commutes. Similarly, reversing the roles, there is a unique linear $\Phi_2 : E_2 \longrightarrow E_1$ such that

$$\begin{tikzcd} E_2 \arrow[rr, dashed, "\Phi_2"] & & \\ M \times \ldots \times M \arrow[u, "\alpha_2"] \arrow[rr, "\alpha_1"'] & & E_1 \end{tikzcd}$$

commutes. Then $\Phi_2 \circ \Phi_1 : E_1 \longrightarrow E_1$ is compatible with α_1, so is the identity, from the first part of the proof. And, symmetrically, $\Phi_1 \circ \Phi_2 : E_2 \longrightarrow E_2$ is compatible with α_2, so is the identity. Thus, the maps Φ_i are mutual inverses, so are isomorphisms. ///

For existence, we express the n^{th} exterior power $\bigwedge^n M$ as a quotient of the tensor power

$$\bigotimes^n M = \underbrace{M \otimes \ldots \otimes M}_{n}$$

[2.0.3] **Proposition:** n^{th} exterior powers $\bigwedge^n M$ exist. In particular, let I be the submodule of $\bigotimes^n M$ generated by all tensors

$$m_1 \otimes \ldots \otimes m_n$$

where $m_i = m_j$ for some $i \neq j$. Then

$$\bigwedge^n M = \bigotimes^n M/I$$

The alternating map

$$\alpha : M \times \ldots \times M \longrightarrow \bigwedge^n M$$

is the composite of the quotient map $\bigotimes^n \longrightarrow \bigwedge^n M$ with the canonical multilinear map $M \times \ldots \times M \longrightarrow \bigotimes^n M$.

Proof: Let $\varphi : M \times \ldots \times M \longrightarrow X$ be an alternating R-multilinear map. Let $\tau : M \times \ldots \times M \longrightarrow \bigotimes^n M$ be the tensor product. By properties of the tensor product there is a unique R-linear $\Psi : \bigotimes^n M \longrightarrow X$ through which φ factors, namely $\varphi = \Psi \circ \tau$.

Let $q : \bigotimes^n \longrightarrow \bigwedge^n M$ be the quotient map. We claim that Ψ factors through q, as $\Psi = \Phi \circ q$, for a linear map $\Phi : \bigwedge^n M \longrightarrow X$. That is, we claim that there is a commutative diagram

$$\begin{tikzcd} \bigotimes^n M \arrow[dr, "q"] \arrow[ddrr, bend left, "\Psi"] & & \\ & \bigwedge^n M \arrow[dr, dashed, "\Phi"] & \\ & M \times \ldots \times M \arrow[u, "\alpha"] \arrow[uul, bend left, "\tau"] \arrow[r, "\varphi"] & X \end{tikzcd}$$

Specifically, we claim that $\Psi(I) = 0$, where I is the submodule generated by $m_1 \otimes \ldots \otimes m_n$ with $m_i = m_j$ for some $i \neq j$. Indeed, using the fact that φ is alternating,

$$\Psi(m_1 \otimes \ldots \otimes_m) = \Psi(\tau(m_1 \times \ldots \times m_n)) = \varphi(m_1 \times \ldots \times m_n) = 0$$

That is, $\ker \Psi \supset I$, so Ψ factors through the quotient $\bigwedge^n M$.

Last, we must check that the map $\alpha = q \circ \tau$ is alternating. Indeed, with $m_i = m_j$ (and $i \neq j$),

$$\alpha(m_1 \times \ldots \times m_n) = (q \circ \tau)(m_1 \times \ldots \times m_n) = q(m_1 \otimes \ldots \otimes m_n)$$

Since $m_i = m_j$, that monomial tensor is in the submodule I, which is the kernel of the quotient map q. Thus, α is alternating. ///

---

3. *Some elementary facts*

Again,[2] the naive notion of *alternating* would entail that, for example, in $\bigwedge^2 M$

$$x \wedge y = -y \wedge x$$

More generally, in $\bigwedge^n M$,

$$\ldots \wedge m_i \wedge \ldots \wedge m_j \wedge \ldots = - \ldots \wedge m_j \wedge \ldots \wedge m_i \wedge \ldots$$

(interchanging the i^{th} and j^{th} elements) for $i \neq j$. However, this isn't the definition. Again, the *definition* is that

$$\ldots \wedge m_i \wedge \ldots \wedge m_j \wedge \ldots = 0 \quad \text{if } m_i = m_j \text{ for any } i \neq j$$

This latter condition is strictly stronger than the change-of-sign requirement if 2 is a 0-divisor in the underlying ring R. As in Artin's development of determinants from the alternating property, we do recover the change-of-sign property, since

$$0 = (x+y) \wedge (x+y) = x \wedge x + x \wedge y + y \wedge x + y \wedge y = 0 + x \wedge y + y \wedge x + 0$$

which gives

$$x \wedge y = -y \wedge x$$

The natural induction on the number of 2-cycles in a permutation π proves

[3.0.1] Proposition: For $m_1, \ldots, m_n$ in M, and for a permutation π of n things,

$$m_{\pi(1)} \wedge \ldots \wedge m_{\pi(n)} = \sigma(\pi) \cdot m_1 \wedge \ldots \wedge m_n$$

Proof: Let $\pi = s\tau$, where s is a 2-cycle and τ is a permutation expressible as a product of fewer 2-cycles than π. Then

$$m_{\pi(1)} \wedge \ldots \wedge m_{\pi(n)} = m_{s\tau(1)} \wedge \ldots \wedge m_{s\tau(n)} = -m_{\tau(1)} \wedge \ldots \wedge m_{\tau(n)}$$
$$= -\sigma(\tau) \cdot m_1 \wedge \ldots \wedge m_n = \sigma(\pi) \cdot m_1 \wedge \ldots \wedge m_n$$

as asserted. ///

[3.0.2] Proposition: The *monomial* exterior products $m_1 \wedge \ldots \wedge m_n$ generate $\bigwedge^n M$ as an R-module, as the m_i run over all elements of M.

Proof: Let X be the submodule of $\bigwedge^n M$ generated by the monomial tensors, $Q = (\bigwedge^n M)/X$ the quotient, and $q : \bigwedge^n M \longrightarrow X$ the quotient map. Let

$$B : M \times \ldots \times M \longrightarrow Q$$

---

[2] We already saw this refinement in the classical context of determinants of matrices, as axiomatized in the style of Emil Artin.

be the 0-map. A defining property of the n^{th} exterior power is that there is a unique R-linear

$$\beta : \bigwedge^n M \longrightarrow Q$$

making the usual diagram commute, that is, such that $B = \beta \circ \alpha$, where $\alpha : M \times \ldots \times M \longrightarrow \bigwedge^n M$. Both the quotient map q and the 0-map $\bigwedge^n M \longrightarrow Q$ allow the 0-map $M \times \ldots \times M \longrightarrow Q$ to factor through, so by the uniqueness the quotient map is the 0-map. That is, Q is the 0-module, so $X = \bigwedge^n M$. ///

[3.0.3] **Proposition:** Let $\{m_\beta : \beta \in B\}$ be a set of generators for an R-module M, where the index set B is *ordered*. Then the monomials

$$m_{\beta_1} \wedge \ldots \wedge m_{\beta_n} \qquad \text{with} \quad \beta_1 < \beta_2 < \ldots < \beta_n$$

generate $\bigwedge^n M$.

Proof: First, claim that the monomials

$$m_{\beta_1} \wedge \ldots \wedge m_{\beta_n} \qquad \text{(no condition on } \beta_i\text{s)}$$

generate the exterior power. Let I be the submodule generated by them. If I is proper, let $X = (\bigwedge^n M)/I$ and let $q : \bigwedge^n M \longrightarrow X$ be the quotient map. The composite

$$q \circ \alpha : \underbrace{M \times \ldots \times M}_{n} \longrightarrow \bigwedge^n M \longrightarrow X$$

is an alternating map, and is 0 on any $m_{\beta_1} \times \ldots \times m_{\beta_n}$. In each variable, separately, the map is linear, and vanishes on generators for M, so is 0. Thus, $q \circ \alpha = 0$. This map certainly factors through the 0-map $\bigwedge^n M \longrightarrow X$. But, using the defining property of the exterior power, the uniqueness of a map $\bigwedge^n M \longrightarrow X$ through which $q \circ \alpha$ factors implies that $q = 0$, and $X = 0$. Thus, these monomials generate the whole.

Now we will see that we can reorder monomials to put the indices in ascending order. First, since

$$m_{\beta_1} \wedge \ldots \wedge m_{\beta_n} = \alpha(m_{\beta_1} \times \ldots \times m_{\beta_n})$$

and α is alternating, the monomial is 0 if $m_{\beta_i} = m_{\beta_j}$ for $\beta_i \neq \beta_j$. And for a permutation π of n things, as observed just above,

$$m_{\beta_{\pi(1)}} \wedge \ldots \wedge m_{\beta_{\pi(n)}} = \sigma(\pi) \cdot m_{\beta_1} \wedge \ldots \wedge m_{\beta_n}$$

where σ is the parity function on permutations. Thus, to express elements of $\bigwedge^n M$ it suffices to use only monomials with indices in ascending order. ///

4. *Exterior powers $\bigwedge^n f$ of maps*

Still R is a commutative ring with 1.

An important type of map on an exterior power $\bigwedge^n M$ arises from R-linear maps on the module M. That is, let

$$f : M \longrightarrow N$$

be an R-module map, and attempt to define

$$\bigwedge^n f : \bigwedge^n M \longrightarrow \bigwedge^n N$$

by

$$(\bigwedge^n f)(m_1 \wedge \ldots \wedge m_n) = f(m_1) \wedge \ldots \wedge f(m_n)$$

Justifiably interested in being sure that this formula makes sense, we proceed as follows.

If the map is *well-defined* then it is defined completely by its values on the monomial exterior products, since these generate the exterior power. To prove well-definedness, we invoke the defining property of the n^{th} exterior power. Let $\alpha' : N \times \ldots \times N \longrightarrow \bigwedge^n N$ be the canonical map. Consider

$$B : \underbrace{M \times \ldots \times M}_{n} \overset{f\times\ldots\times f}{\longrightarrow} \underbrace{N \times \ldots \times N}_{n} \overset{\alpha'}{\longrightarrow} \bigwedge{}^n N$$

given by

$$B(m_1 \times \ldots \times m_n) = f(m_1) \wedge \ldots \wedge f(m_n)$$

For fixed index i, and for fixed $m_j \in M$ for $j \neq i$, the composite

$$m \longrightarrow \alpha'(\ldots \times f(m_{i-1}) \times f(m) \times f(m_{i+1}) \wedge \ldots)$$

is certainly an R-linear map in m. Thus, B is R-multilinear. As a function of each single argument in $M \times \ldots \times M$, the map B is linear, so B is multilinear. Since α' is alternating, B is alternating. Then (by the defining property of the exterior power) there is a unique R-linear map Φ giving a commutative diagram

$$\begin{tikzcd}
\bigwedge^n M \arrow[rrd, dashed, "\Phi=\wedge^n f"] & & \\
M \times \ldots \times M \arrow[u, "\alpha"] \arrow[r, "f\times\ldots\times f"] & N \times \ldots \times N \arrow[r, "\alpha'"] & \bigwedge^n N
\end{tikzcd}$$

the formula for $\bigwedge^n f$ is the induced linear map Φ on the n^{th} exterior power. Since the map arises as the unique induced map via the defining property of $\bigwedge^n M$, it is certainly well-defined.

---

5. *Exterior powers of free modules*

The main point here is that free modules over commutative rings with identity behave much like vector spaces over fields, with respect to multilinear algebra operations. In particular, we prove **non-vanishing** of the n^{th} exterior power of a free module of rank n, which (as we will see) proves the existence of determinants.

At the end, we discuss the natural bilinear map

$$\bigwedge{}^s M \times \bigwedge{}^t M \longrightarrow \bigwedge{}^{s+t} M$$

by

$$(m_1 \wedge \ldots \wedge m_s) \times (m_{s+1} \wedge \ldots \wedge m_{s+t}) \longrightarrow m_1 \wedge \ldots \wedge m_s \wedge m_{s+1} \wedge \ldots \wedge m_{s+t}$$

which does not require free-ness of M.

[5.0.1] **Theorem:** Let F be a free module of rank n over a commutative ring R with identity. Then $\bigwedge^\ell F$ is free of rank $\binom{n}{\ell}$. In particular, if $m_1, \ldots, m_n$ form an R-basis for F, then the monomials

$$m_{i_1} \wedge \ldots \wedge m_{i_\ell} \quad \text{with } i_1 < \ldots < i_\ell$$

are an R basis for $\bigwedge^\ell F$.

Proof: The elementary discussion just above shows that the monomials involving the basis and with strictly ascending indices *generate* $\bigwedge^\ell F$. The remaining issue is to prove linear independence.

First, we prove that $\bigwedge^n F$ is free of rank 1. We know that it is generated by

$$m_1 \wedge \ldots \wedge m_n$$

But for all we know it might be that

$$r \cdot m_1 \wedge \ldots \wedge m_n = 0$$

for some $r \neq 0$ in R. We must prove that this does not happen. To do so, we make a non-trivial alternating (multilinear) map

$$\varphi : \underbrace{F \times \ldots \times F}_{n} \longrightarrow R$$

To make this, let $\lambda_1, \ldots, \lambda_n$ be a *dual basis*[3] for $\mathrm{Hom}_R(F, R)$, namely,

$$\lambda_i(m_j) = \begin{cases} 1 & i = j \\ 0 & \text{(else)} \end{cases}$$

For arbitrary $x_1, \ldots, x_n$ in F, let[4]

$$\varphi(x_1 \times \ldots \times x_n) = \sum_{\pi \in S_n} \sigma(\pi) \lambda_1(x_{\pi(1)}) \ldots \lambda_n(x_{\pi(n)})$$

where S_n is the group of permutations of n things. Suppose that for some $i \neq j$ we have $x_i = x_j$. Let i' and j' be indices such that $\pi(i') = i$ and $\pi(j') = j$. Let s still be the 2-cycle that interchanges i and j. Then the $n!$ summands can be seen to cancel in pairs, by

$$\sigma(\pi) \lambda_1(x_{\pi(1)}) \ldots \lambda_n(x_{\pi(n)}) + \sigma(s\pi) \lambda_1(x_{s\pi(1)}) \ldots \lambda_n(x_{s\pi(n)})$$

$$= \sigma(\pi) \left(\prod_{\ell \neq i', j'} \lambda_\ell(x_{\pi(\ell)}) \right) \cdot \left(\lambda_i(x_{\pi(i')} \lambda_i(x_{\pi(j')}) - \lambda_i(x_{s\pi(i')}) \lambda_i(x_{s\pi(j')}) \right)$$

Since s just interchanges $i = \pi(i')$ and $j = \pi(j')$, the rightmost sum is 0. This proves the alternating property of φ.

To see that φ is not trivial, note that when the arguments to φ are the basis elements $m_1, \ldots, m_n$, in the expression

$$\varphi(m_1 \times \ldots \times m_n) = \sum_{\pi \in S_n} \sigma(\pi) \lambda_1(m_{\pi(1)}) \ldots \lambda_n(m_{\pi(n)})$$

$\lambda_i(m_{\pi(i)}) = 0$ unless $\pi(i) = i$. That is, the only non-zero summand is with $\pi = 1$, and we have

$$\varphi(m_1 \times \ldots \times m_n) = \lambda_1(m_1) \ldots \lambda_n(m_n) = 1 \in R$$

Then φ induces a map $\Phi : \bigwedge^n F \longrightarrow R$ such that

$$\Phi(m_1 \wedge \ldots \wedge m_n) = 1$$

For $r \in R$ such that $r \cdot (m_1 \wedge \ldots \wedge m_n) = 0$, apply Φ to obtain

$$0 = \Phi(0) = \Phi(r \cdot m_1 \wedge \ldots \wedge m_n) = r \cdot \Phi(m_1 \wedge \ldots \wedge m_n) = r \cdot 1 = r$$

---

[3] These exist, since (by definition of free-ness of F) given a set of desired images $\varphi(m_i) \in R$ of the basis m_i, there is a unique map $\Phi : F \longrightarrow R$ such that $\Phi(m_i) = \varphi(m_i)$.

[4] This formula is suggested by the earlier discussion of determinants of *matrices* following Artin.

This proves that $\bigwedge^n F$ is free of rank 1.

The case of $\bigwedge^\ell F$ with $\ell < n$ reduces to the case $\ell = n$, as follows. We already know that monomials $m_{i_1} \wedge \ldots \wedge m_{i_\ell}$ with $i_1 < \ldots < i_\ell$ *span* $\bigwedge^\ell F$. Suppose that

$$\sum_{i_1 < \ldots < i_\ell} r_{i_1 \ldots i_\ell} \cdot m_{i_1} \wedge \ldots \wedge m_{i_\ell} = 0$$

The trick is to consider, for a fixed ℓ-tuple $j_1 < \ldots < j_\ell$ of indices, the R-linear map

$$f : \bigwedge^\ell F \longrightarrow \bigwedge^n F$$

given by

$$f(x) = x \wedge (m_1 \wedge m_2 \wedge \ldots \wedge \widehat{m_{j_1}} \wedge \ldots \wedge \widehat{m_{j_\ell}} \wedge \ldots \wedge m_n)$$

where

$$m_1 \wedge m_2 \wedge \ldots \wedge \widehat{m_{j_1}} \wedge \ldots \wedge \widehat{m_{j_\ell}} \wedge \ldots \wedge m_n)$$

is the monomial with exactly the m_{j_t}s *missing*. Granting that this map is well-defined,

$$0 = f(0) = f\left(\sum_{i_1 < \ldots < i_\ell} r_{i_1 \ldots i_\ell} \cdot m_{i_1} \wedge \ldots \wedge m_{i_\ell}\right) = \pm r_{j_1 \ldots j_\ell} m_1 \wedge \ldots \wedge m_n$$

since all the other monomials have some repeated m_t, so are 0. That is, any such relation must have all coefficients 0. This proves the linear independence of the indicated monomials.

To be sure that these maps f are well-defined, [5] we prove a more systematic result, which will finish the proof of the theorem.

[5.0.2] **Proposition:** Let M be an R-module. [6] Let s, t be positive integers. The canonical alternating multilinear map

$$\alpha : M \times \ldots \times M \longrightarrow \bigwedge^{s+t} M$$

induces a natural bilinear map

$$B : (\bigwedge^s M) \times (\bigwedge^t M) \longrightarrow \bigwedge^{s+t} M$$

by

$$(m_1 \wedge \ldots \wedge m_s) \times (m_{s+1} \wedge \ldots \wedge m_{s+t}) \longrightarrow m_1 \wedge \ldots \wedge m_s \wedge m_{s+1} \wedge \ldots \wedge m_{s+t}$$

Proof: For fixed choice of the last t arguments, the map α on the first s factors is certainly alternating multilinear. Thus, from the defining property of $\bigwedge^s M$, α factors uniquely through the map

$$\bigwedge^s M \times \underbrace{M \times \ldots \times M}_{t} \longrightarrow \bigwedge^{s+t} M$$

defined (by linearity) by

$$(m_1 \wedge \ldots \wedge m_s) \times m_{s+1} \times \ldots \times m_{s+t} = m_1 \wedge \ldots \wedge m_s \wedge m_{s+1} \wedge \ldots \wedge m_{s+t}$$

[5] The importance of verifying that symbolically reasonable expressions make sense is often underestimated. Seemingly well-defined things can easily be ill-defined. For example, $f : \mathbb{Z}/3 \longrightarrow \mathbb{Z}/5$ defined [sic] by $f(x) = x$, or, seemingly more clearly, by $f(x + 3\mathbb{Z}) = x + 5\mathbb{Z}$. This is not well-defined, since $0 = f(0) = f(3) = 3 \neq 0$.

[6] In particular, M need not be free, and need not be finitely-generated.

Indeed, by the defining property of the exterior power, for each fixed choice of last t arguments the map is linear on $\bigwedge^s M$. Further, for fixed choice of first arguments α on the last t arguments is alternating multilinear, so α factors through the expected map

$$(\bigwedge^s M) \times (\bigwedge^t M) \longrightarrow \bigwedge^{s+t} M$$

linear in the $\bigwedge^t M$ argument for each choice of the first. That is, this map is bilinear. ///

---

6. *Determinants revisited*

The fundamental idea is that for an endomorphism T of a free R-module M of rank n (with R commutative with unit), $\det T \in R$ is determined as

$$Tm_1 \wedge \ldots \wedge Tm_n = (\det T) \cdot (m_1 \wedge \ldots \wedge m_n)$$

Since $\bigwedge^n M$ is free of rank 1, all R-linear endomorphisms are given by scalars: indeed, for an endomorphism A of a rank-1 R-module with generator e,

$$A(re) = r \cdot Ae = r \cdot (s \cdot e)$$

for all $r \in$, for some $s \in R$, since $Ae \in R \cdot e$.

This gives a *scalar* $\det T$, intrinsically defined, assuming that we verify that this does what we want.

And certainly this would give a pleasant proof of the *multiplicativity* of determinants, since

$$(\det ST) \cdot (m_1 \wedge \ldots \wedge m_n) = (ST)m_1 \wedge \ldots \wedge (ST)m_n = S(Tm_1) \wedge \ldots \wedge S(Tm_n)$$

$$= (\det S)\,(Tm_1 \wedge \ldots \wedge Tm_n) = (\det S)(\det T)(m_1 \wedge \ldots \wedge m_n)$$

Note that we use the fact that

$$(\det T) \cdot (m_1 \wedge \ldots \wedge m_n) = Tm_1 \wedge \ldots \wedge Tm_n$$

for *all* n-tuples of elements m_i in F.

Let $e_1, \ldots, e_n$ be the standard basis of k^n. Let $v_1, \ldots, v_n$ be the columns of an n-by-n matrix. Let T be the endomorphism (of column vectors) given by (left multiplication by) that matrix. That is, $Te_i = v_i$. Then

$$v_1 \wedge \ldots \wedge v_n = Te_1 \wedge \ldots \wedge Te_n = (\det T) \cdot (e_1 \wedge \ldots \wedge e_n)$$

The leftmost expression in the latter line is an alternating multilinear $\bigwedge^n(k^n)$-valued function. (Not k-valued.) But since we know that $\bigwedge^n(k^n)$ is one-dimensional, and is spanned by $e_1 \wedge \ldots \wedge e_n$, (once again) we know that there is a unique scalar $\det T$ such that the right-hand equality holds. That is, the map

$$v_1 \times \ldots \times v_n \longrightarrow \det T$$

where T is the endomorphism given by the matrix with columns v_i, is an alternating k-valued map. And it is 1 for $v_i = e_i$.

This translation back to matrices verifies that our intrinsic determinant meets our earlier axiomatized requirements for a determinant. ///

Finally we note that the basic formula for determinants of matrices that followed from Artin's axiomatic characterization, at least in the case of entires in *fields*, is valid for matrices with entries in commutative rings (with units). That is, for an n-by-n matrix A with entries A_{ij} in a commutative ring R with unit,

$$\det A = \sum_{\pi \in S_n} \sigma(\pi) A_{\pi(1),1} \ldots A_{\pi(n),n}$$

where S_n is the symmetric group on n things and $\sigma(\pi)$ is the sign function on permutations. Indeed, let $v_1, \ldots, v_n$ be the rows of A, let $e_1, \ldots, e_n$ be the standard basis (row) vectors for R^n, and consider A as an endomorphism of R^n. As in the previous argument, $A \cdot e_j = e_j A = v_j$ (where A acts by right matrix multiplication). And $v_i = \sum_j A_{ij} e_j$. Then

$$(\det A)\, e_1 \wedge \ldots \wedge e_n = (A \cdot e_1) \wedge \ldots \wedge (A \cdot e_n) = v_1 \wedge \ldots \wedge v_n = \sum_{i_1, \ldots, i_n} (A_{1i_1} e_{i_1}) \wedge \ldots \wedge (A_{ni_n} e_{i_n})$$

$$= \sum_{\pi \in S_n} (A_{1\pi(1)} e_{\pi(1)}) \wedge \ldots \wedge (A_{n\pi(n)} e_{\pi(n)}) = \sum_{\pi \in S_n} (A_{1\pi(1)} \ldots A_{n\pi(n)})\, e_{\pi(1)} \wedge \ldots \wedge e_{\pi(n)}$$

$$= \sum_{\pi \in S_n} (A_{\pi^{-1}(1),1} \ldots A_{\pi^{-1}(n)}, n)\, \sigma(\pi) e_1 \wedge \ldots \wedge e_n$$

by reordering the e_is, using the alternating multilinear nature of $\bigwedge^n(R^n)$. Of course $\sigma(\pi) = \sigma(\pi^{-1})$. Replacing π by π^{-1} (thus replacing π^{-1} by π) gives the desired

$$(\det A)\, e_1 \wedge \ldots \wedge e_n = \sum_{\pi \in S_n} (A_{\pi(1),1} \ldots A_{\pi(n)}, n)\, \sigma(\pi) e_1 \wedge \ldots \wedge e_n$$

Since $e_1 \wedge \ldots \wedge e_n$ is an R-basis for the free rank-one R-module $\bigwedge^n(R^n)$, this proves that $\det A$ is given by the asserted formula. ///

[6.0.1] **Remark:** Indeed, the point that $e_1 \wedge \ldots \wedge e_n$ is an R-basis for the free rank-one R-module $\bigwedge^n(R^n)$, as opposed to being 0 or being annihilated by some non-zero elements of R, is exactly what is needed to make the earlier seemingly field-oriented arguments work more generally.

---

7. *Minors of matrices*

At first, one might be surprised at the following phenomenon.

Let

$$M = \begin{pmatrix} a & b & c \\ x & y & z \end{pmatrix}$$

with entries in some commutative ring R with unit. Viewing each of the two rows as a vector in R^3, inside $\bigwedge^2 R^3$ we compute (letting e_1, e_2, e_3 be the standard basis)

$$(ae_1 + be_2 + ce_3) \wedge (xe_1 + ye_2 + ze_3)$$

$$= \left\{ \begin{array}{rcrcr} & & axe_1 \wedge e_1 & + & aye_1 \wedge e_2 & + & aze_1 \wedge e_3 \\ + & & bxe_2 \wedge e_1 & + & bye_2 \wedge e_2 & + & bze_2 \wedge e_3 \\ + & & cxe_3 \wedge e_1 & + & cye_3 \wedge e_2 & + & cze_3 \wedge e_3 \end{array} \right.$$

$$= \left\{ \begin{array}{ccccc} 0 & + & aye_1 \wedge e_2 & + & aze_1 \wedge e_3 \\ -bxe_1 \wedge e_2 & + & 0 & + & bze_2 \wedge e_3 \\ -cxe_1 \wedge e_3 & + & -cye_2 \wedge e_3 & + & 0 \end{array} \right.$$

$$= (ay - bx)\, e_1 \wedge e_2 + (az - cx)\, e_1 \wedge e_3 + (bz - cy)\, e_2 \wedge e_3$$

$$= \begin{vmatrix} a & b \\ x & y \end{vmatrix} e_1 \wedge e_2 + \begin{vmatrix} a & c \\ x & z \end{vmatrix} e_1 \wedge e_3 + \begin{vmatrix} b & c \\ y & z \end{vmatrix} e_2 \wedge e_3$$

where, to fit it on a line, we have written

$$\begin{vmatrix} a & b \\ x & y \end{vmatrix} = \det \begin{pmatrix} a & b \\ x & y \end{pmatrix}$$

That is, *the coefficients in the second exterior power are the determinants of the two-by-two minors.*

At some point it becomes unsurprising to have

[7.0.1] **Proposition:** Let M be an m-by-n matrix with $m < n$, entries in a commutative ring R with identity. Viewing the rows $M_1, \ldots, M_m$ of M as elements of R^n, and letting $e_1, \ldots, e_n$ be the standard basis of R^n, in $\bigwedge^m R^n$

$$M_1 \wedge \ldots \wedge M_n = \sum_{i_1 < \ldots < i_m} \det(M^{i_1 \ldots i_m}) \cdot e_{i_1} \wedge \ldots \wedge e_{i_m}$$

where $M^{i_1 \ldots i_m}$ is the m-by-m matrix consisting of the i_1^{th}, i_2^{th}, ..., i_m^{th} columns of M.

Proof: Write

$$M_i = \sum_j r_{ij} e_j$$

Then

$$M_1 \wedge \ldots \wedge M_m = \sum_{i_1, \ldots, i_m} (M_{1i_1} e_{i_1}) \wedge (M_{2i_2} e_{i_2}) \wedge \ldots \wedge (M_{mi_m} e_{i_n})$$

$$= \sum_{i_1, \ldots, i_m} M_{1i_1} \ldots M_{mi_m} \; e_{i_1} \wedge e_{i_2} \wedge \ldots \wedge e_{i_m}$$

$$= \sum_{i_1 < \ldots < i_m} \sum_{\pi \in S_m} \sigma(\pi) \, M_{1,i_{\pi(1)}} \ldots M_{m,i_{\pi(i)}} \; e_{i_1} \wedge \ldots \wedge e_{i_m}$$

$$= \sum_{i_1 < \ldots < i_m} \det M^{i_1 \ldots i_m} \, e_{i_1} \wedge \ldots \wedge e_{i_m}$$

where we reorder the $e_{i_j}s$ via π in the permutations group S_m of $\{1, 2, \ldots, m\}$ and $\sigma(\pi)$ is the sign function on permutation. This uses the general formula for the determinant of an n-by-n matrix, from above. ///

---

8. *Uniqueness in the structure theorem*

Exterior powers give a decisive trick to give an *elegant* proof of the uniqueness part of the structure theorem for finitely-generated modules over principal ideal domains. This will be the immediate application of

[8.0.1] **Proposition:** Let R be a commutative ring with identity. Let M be a free R-module with R-basis $m_1, \ldots, m_n$. Let $d_1, \ldots, d_n$ be elements of R, and let

$$N = R \cdot d_1 m_1 \oplus \ldots \oplus R \cdot d_n m_n \subset M$$

Then, for any $1 < \ell \in \mathbb{Z}$, we have

$$\bigwedge\nolimits^\ell N = \bigoplus_{j_1 < \ldots < j_\ell} R \cdot (d_{j_1} \ldots d_{j_\ell}) \cdot (m_{j_1} \wedge \ldots \wedge m_{j_\ell}) \subset \bigwedge\nolimits^\ell M$$

[8.0.2] **Remark:** We do not need to assume that R is a PID, nor that $d_1 | \ldots | d_n$, in this proposition.

Proof: Without loss of generality, by re-indexing, suppose that $d_1, \ldots, d_t$ are non-zero and $d_{t+1} = d_{t+2} = \ldots = d_n = 0$. We have already shown that the ordered monomials $m_{j_1} \wedge \ldots \wedge m_{j_\ell}$ are a basis for the free

R-module $\bigwedge^\ell M$, whether or not R is a PID. Similarly, the basis $d_1 m_1, \ldots, d_t m_t$ for N yields a basis of the ℓ-fold monomials for $\bigwedge^\ell N$, namely

$$d_{j_1} m_{j_1} \wedge \ldots \wedge d_{j_\ell} m_{j_\ell} \quad \text{with } j_1 < \ldots < j_\ell \le t$$

By the multilinearity,

$$d_{j_1} m_{j_1} \wedge \ldots \wedge d_{j_\ell} m_{j_\ell} = (d_{j_1} d_{j_2} \ldots d_{j_\ell}) \cdot (m_{j_1} \wedge \ldots \wedge m_{j_\ell})$$

This is all that is asserted. ///

At last, we prove the uniqueness of elementary divisors.

[8.0.3] **Corollary:** Let R be a principal ideal domain. Let M be a finitely-generated free R-module, and N a submodule of M. Then there is a basis $m_1, \ldots, m_n$ of M and *elementary divisors* $d_1 | \ldots | d_n$ in R such that

$$N = Rd_1 m_1 \oplus \ldots \oplus Rd_n m_n$$

The ideals Rd_i are uniquely determined by M, N.

Proof: The *existence* was proven much earlier. Note that the *highest* elementary divisor d_n, or, really, the ideal Rd_n, is determined *intrinsically* by the property

$$Rd_n = \{r \in R : r \cdot (M/N) = 0\}$$

since d_n is a least common multiple of all the d_is. That is, Rd_n is the **annihilator** of M/N.

Suppose that t is the last index so that $d_t \neq 0$, so $d_1, \ldots, d_t$ are non-zero and $d_{t+1} = d_{t+2} = \ldots = d_n = 0$. Using the proposition, the annihilator of $\bigwedge^2 M / \bigwedge^2 N$ is $R \cdot d_{t-1} d_t$, since d_{t-1} and d_t are the two largest non-zero elementary divisors. Since Rd_t is uniquely determined, Rd_{t-1} is uniquely determined.

Similarly, the annihilator of $\bigwedge^i M / \bigwedge^i N$ is $Rd_{t-i+1} \ldots d_{t-1} d_t$, which is uniquely determined. By induction, d_t, d_{t-1}, $\ldots$, d_{t-i+2} are uniquely determined. Thus, d_{t-i+1} is uniquely determined. ///

---

9. *Cartan's lemma*

To further illustrate computations in exterior algebra, we prove a result that arises in differential geometry, often accidentally disguised as something more than the simple exterior algebra it is.

[9.0.1] **Proposition:** *(Cartan)* Let V be a vector space over a field k. Let v_1, $\ldots$, v_n be linearly independent vectors in V. Let w_1, $\ldots$, w_n be any vectors in V. Then

$$v_1 \wedge w_1 + \ldots + v_n \wedge w_n = 0$$

if and only if there is a *symmetric* matrix with entries $A_{ij} \in k$ such that

$$w_i = \sum_i A_{ij} \, v_j$$

Proof: First, prove that if the identity holds, then the w_j's lie in the span of the v_i's. Suppose not. Then, by renumbering for convenience, we can suppose that $w_1, v_1, \ldots, v_n$ are linearly independent. Let $\eta = v_2 \wedge \ldots \wedge v_n$. Then

$$\Big(v_1 \wedge w_1 + \ldots + v_n \wedge w_n\Big) \wedge \eta = 0 \wedge \eta = 0 \in \bigwedge^{n+1} V$$

On the other hand, the exterior products of η with all summands but the first are 0, since some v_i with $i \geq 2$ is repeated. Thus,

$$\Big(v_1 \wedge w_1 + \ldots + v_n \wedge w_n\Big) \wedge \eta = v_1 \wedge w_1 \wedge \eta = v_1 \wedge w_1 \wedge v_2 \wedge \ldots \wedge v_n \neq 0$$

This contradiction proves that the w_j's do all lie in the span of the v_i's if the identity is satisfied. Let A_{ij} be elements of k expressing the w_j's as linear combinations

$$w_i = \sum_i A_{ij}\, v_j$$

We need to prove that $A_{ij} = A_{ji}$.

Let

$$\omega = v_1 \wedge \ldots \wedge v_n \in \bigwedge^n V$$

By our general discussion of exterior powers, by the linear independence of the v_i this is non-zero. For $1 \leq i \leq n$, let

$$\omega_i = v_1 \wedge \ldots \wedge \widehat{v_i} \wedge \ldots \wedge v_n \in \bigwedge^{n-1} V$$

where the hat indicates omission. In any linear combination $v = \sum_j c_j\, v_j$ we can pick out the i^{th} coefficient by exterior product with ω_i, namely

$$v \wedge \omega_i = \Big(\sum_j c_j\, v_j\Big) \wedge \omega_i = \sum_j c_j\, v_j \wedge \omega_i = c_i\, v_i \wedge \omega_i = (-1)^{i-1}\, c_i\, \omega$$

For $i < j$, let

$$\omega_{ij} = v_1 \wedge \ldots \wedge \widehat{v_i} \wedge \ldots \wedge \widehat{v_j} \wedge \ldots \wedge v_n \in \bigwedge^{n-2} V$$

Then, using the hypothesis of the lemma,

$$\begin{aligned} 0 \wedge \omega_{ij} \;&=\; \Big(v_1 \wedge w_1 + \ldots + v_n \wedge w_n\Big) \wedge \omega_{ij} = v_1 \wedge w_1 \wedge \omega_{ij} + \ldots + v_n \wedge w_n \wedge \omega_{ij} \\ &= v_i \wedge w_i \wedge \omega_{ij} + v_j \wedge w_j \wedge \omega_{ij} \end{aligned}$$

since all the other monomials vanish, having repeated factors. Thus, moving things around slightly,

$$w_i \wedge v_i \wedge \omega_{ij} = -\, w_j \wedge v_j \wedge \omega_{ij}$$

By moving the v_i and v_j across, flipping signs as we go, with $i < j$, we have

$$v_i \wedge \omega_{ij} = (-1)^{i-1} \omega_j \qquad\qquad v_j \wedge \omega_{ij} = (-1)^{j-2} \omega_i$$

Expanding the equality $w_i \wedge v_i \wedge \omega_{ij} = -\, w_j \wedge v_j \wedge \omega_{ij}$, the left-hand side is

$$w_i \wedge v_i \wedge \omega_{ij} = (-1)^{i-1} w_i \wedge \omega_i = (-1)^{i-1} \sum_k A_{ik} v_k \wedge \omega_j = (-1)^{i-1} A_{ij} v_i \wedge \omega_j = (-1)^{i-1}\, (-1)^{j-1}\, A_{ij} \omega$$

while, similarly, the right-hand side is

$$-w_j \wedge v_j \wedge \omega_{ij} = (-1)\, (-1)^{j-2}\, (-1)^{i-1} A_{ji} \omega$$

Equating the transformed versions of left and right sides,

$$A_{ij} \;=\; A_{ji}$$

Reversing this argument gives the converse. Specifically, suppose that $w_i = \sum_j A_{ij}\, v_j$ with $A_{ij} = A_{ji}$. Let W be the span of $v_1, \ldots, v_n$ inside W. Then running the previous computation backward directly yields

$$\Big(v_1 \wedge w_1 + \ldots + v_n \wedge w_n\Big) \wedge \omega_{ij} = 0$$

for all $i < j$. The monomials ω_{ij} span $\bigwedge^{n-2} W$ and we have shown the non-degeneracy of the pairing

$$\bigwedge^{n-2} W \;\times\; \bigwedge^2 W \longrightarrow \bigwedge^n W \qquad \text{by} \qquad \alpha \times \beta \longrightarrow \alpha \wedge \beta$$

Thus,

$$v_1 \wedge w_1 + \ldots + v_n \wedge w_n = 0 \in \bigwedge^2 W \subset \bigwedge^2 V$$

as claimed. ///

---

10. *Cayley-Hamilton Theorem*

[10.0.1] **Theorem:** (*Cayley-Hamilton*) Let T be a k-linear endomorphism of a finite-dimensional vector space V over a field k. Let $P_T(x)$ be the characteristic polynomial

$$P_T(x) = \det(x \cdot 1_V - T)$$

Then

$$P_T(T) = 0 \in \mathrm{End}_k(V)$$

[10.0.2] **Remarks:** Cayley and Hamilton proved the cases with $n = 2, 3$ by direct computation. The theorem can be made a corollary of the structure theorem for finitely-generated modules over principal ideal domains, if certain issues are glossed over. For example, how should an indeterminate x act on a vectorspace? It would be premature to say that $x \cdot 1_V$ acts as T on V, even though at the end this is *exactly* what is supposed to happen, because, if $x = T$ at the outset, then $P_T(x)$ is simply 0, and the theorem asserts nothing. Various misconceptions can be turned into false proofs. For example, it is *not* correct to argue that

$$P_T(T) = \det(T - T) = \det 0 = 0 \qquad \text{(incorrect)}$$

However, the argument given just below *is* a *correct* version of this idea. Indeed, in light of these remarks, we must clarify what it means to *substitute* T for x. Incidental to the argument, *intrinsic* versions of *determinant* and *adjugate* (or *cofactor*) endomorphism are described, in terms of multi-linear algebra.

Proof: The module $V \otimes_k k[x]$ is free of rank $\dim_k V$ over $k[x]$, and is the object associated to V on which the indeterminate x reasonably acts. Also, V is a $k[T]$-module by the action $v \longrightarrow Tv$, so $V \otimes_k k[x]$ is a $k[T] \otimes_k k[x]$-module. The **characteristic polynomial** $P_T(x) \in k[x]$ of $T \in \mathrm{End}_k(V)$ is the determinant of $1 \otimes x - T \otimes 1$, defined intrinsically by

$$\bigwedge\nolimits^n_{k[x]} (T \otimes 1 - 1 \otimes x) = P_T(x) \cdot 1 \qquad \text{(where } n = \dim_k V = \mathrm{rk}_{k[x]} V \otimes_k k[x])$$

where the first 1 is the identity in $k[x]$, the second 1 is the identity map on V, and the last 1 is the identity map on $\bigwedge^n_{k[x]}(V \otimes_k k[x])$.

To *substitute* T for x is a special case of the following procedure. Let R be a commutative ring with 1, and M an R-module with $1 \cdot m = m$ for all $m \in M$. For an ideal I of R, the quotient $M/I \cdot M$ is the natural associated R/I-module, and every R-endomorphism α of M such that

$$\alpha(I \cdot M) \;\subset\; I \cdot M$$

descends to an R/I-endomorphism of $M/I\cdot M$. In the present situation,

$$R = k[T]\otimes_k k[x] \qquad\qquad M = V\otimes_k k[x]$$

and I is the ideal generated by $1\otimes x - T\otimes 1$. Indeed, $1\otimes x$ is the image of x in this ring, and $T\otimes 1$ is the image of T. Thus, $1\otimes x - T\otimes 1$ should map to 0.

To prove that $P_T(T) = 0$, we will *factor* $P_T(x)\cdot 1$ so that after substituting T for x the resulting endomorphism $P_T(T)\cdot 1$ has a literal factor of $T - T = 0$. To this end, consider the natural $k[x]$-bilinear map

$$\langle,\rangle \;:\; \textstyle\bigwedge_{k[x]}^{n-1} V\otimes_k k[x] \;\;\times\;\; V\otimes_k k[x] \;\;\longrightarrow\;\; \textstyle\bigwedge_{k[x]}^{n} V\otimes_k k[x]$$

of free $k[x]$-modules, identifying $V\otimes_k k[x]$ with its first exterior power. Letting $A = 1\otimes x - T\otimes 1$, for all $m_1,\ldots,m_n$ in $V\otimes_k k[x]$,

$$\langle \textstyle\bigwedge^{n-1} A(m_1\wedge\ldots\wedge m_{n-1}),\; Am_n\rangle \;=\; P_T(x)\cdot m_1\wedge\ldots\wedge m_n$$

By definition, the *adjugate* or *cofactor* endomorphism A^{adg} of A is the adjoint of $\bigwedge^{n-1} A$ with respect to this pairing. Thus,

$$\langle m_1\wedge\ldots\wedge m_{n-1},\; (A^{\mathrm{adg}}\circ A)\, m_n\rangle \;=\; P_T(x)\cdot m_1\wedge\ldots\wedge m_n$$

and, therefore,

$$A^{\mathrm{adg}}\circ A \;=\; P_T(x)\cdot 1 \qquad\qquad (\text{on } V\otimes_k k[x])$$

Since $\langle,\rangle$ is $k[x]$-bilinear, A^{adg} is a $k[x]$-endomorphism of $V\otimes_k k[x]$. To verify that A^{adg} commutes with $T\otimes 1$, it suffices to verify that A^{adg} commutes with A. To this end, further extend scalars on all the free $k[x]$-modules $\bigwedge_{k[x]}^{\ell} V\otimes_k k[x]$ by tensoring with the field of fractions $k(x)$ of $k[x]$. Then

$$A^{\mathrm{adg}}\cdot A \;=\; P_T(x)\cdot 1 \qquad\qquad (\text{now on } V\otimes_k k(x))$$

Since $P_T(x)$ is monic, it is non-zero, hence, invertible in $k(x)$. Thus, A is invertible on $V\otimes_k k(x)$, and

$$A^{\mathrm{adg}} \;=\; P_T(x)\cdot A^{-1} \qquad\qquad (\text{on } V\otimes_k k(x))$$

In particular, the corresponding version of A^{adg} commutes with A on $V\otimes_k k(x)$, and, thus, A^{adg} commutes with A on $V\otimes_k k[x]$.

Thus, A^{adg} descends to an R/I-linear endomorphism of $M/I\cdot M$, where

$$R = k[T]\otimes_k k[x] \qquad M = V\otimes_k k[x] \qquad I = R\cdot A \qquad\qquad (\text{with } A = 1\otimes x - T\otimes 1)$$

That is, on the quotient $M/I\cdot M$,

$$(\text{image of })A^{\mathrm{adg}}\cdot(\text{image of })(1\otimes x - T\otimes 1) \;=\; P_T(T)\cdot 1_{M/IM}$$

The image of $1\otimes x - T\otimes 1$ here is 0, so

$$(\text{image of })A^{\mathrm{adg}}\cdot 0 \;=\; P_T(T)\cdot 1_{M/IM}$$

This implies that

$$P_T(T) \;=\; 0 \qquad\qquad (\text{on } M/IM)$$

Note that the composition

$$V \longrightarrow V\otimes_k k[x] = M \longrightarrow M/IM$$

is an isomorphism of $k[T]$-modules, and, *a fortiori*, of k-vectorspaces. ///

[10.0.3] **Remark:** This should not be the first discussion of this result seen by a novice. However, all the issues addressed are genuine!

11. *Worked examples*

[28.1] Consider the injection $\mathbb{Z}/2 \xrightarrow{t} \mathbb{Z}/4$ which maps

$$t : x + 2\mathbb{Z} \longrightarrow 2x + 4\mathbb{Z}$$

Show that the induced map

$$t \otimes 1_{\mathbb{Z}/2} : \mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/2 \longrightarrow \mathbb{Z}/4 \otimes_{\mathbb{Z}} \mathbb{Z}/2$$

is no longer an injection.

We claim that $t \otimes 1$ is the 0 map. Indeed,

$$(t \otimes 1)(m \otimes n) = 2m \otimes n = 2 \cdot (m \otimes n) = m \otimes 2n = m \otimes 0 = 0$$

for all $m \in \mathbb{Z}/2$ and $n \in \mathbb{Z}/2$. ///

[28.2] Prove that if $s : M \longrightarrow N$ is a *surjection* of $\mathbb{Z}$-modules and X is any other $\mathbb{Z}$ module, then the induced map

$$s \otimes 1_Z : M \otimes_{\mathbb{Z}} X \longrightarrow N \otimes_{\mathbb{Z}} X$$

is still surjective.

Given $\sum_i n_i \otimes x_i$ in $N \otimes_{\mathbb{Z}} X$, let $m_i \in M$ be such that $s(m_i) = n_i$. Then

$$(s \otimes 1)(\sum_i m_i \otimes x_i) = \sum_i s(m_i) \otimes x_i = \sum_i n_i \otimes x_i$$

so the map is surjective. ///

[11.0.1] **Remark:** Note that the only issue here is hidden in the verification that the induced map $s \otimes 1$ exists.

[28.3] Give an example of a surjection $f : M \longrightarrow N$ of $\mathbb{Z}$-modules, and another $\mathbb{Z}$-module X, such that the induced map

$$f \circ - : \mathrm{Hom}_{\mathbb{Z}}(X, M) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(X, N)$$

(by post-composing) *fails* to be surjective.

Let $M = \mathbb{Z}$ and $N = \mathbb{Z}/n$ with $n > 0$. Let $X = \mathbb{Z}/n$. Then

$$\mathrm{Hom}_{\mathbb{Z}}(X, M) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) = 0$$

since

$$0 = \varphi(0) = \varphi(nx) = n \cdot \varphi(x) \in \mathbb{Z}$$

so (since n is not a 0-divisor in $\mathbb{Z}$) $\varphi(x) = 0$ for all $x \in \mathbb{Z}/n$. On the other hand,

$$\mathrm{Hom}_{\mathbb{Z}}(X, N) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/n) \approx \mathbb{Z}/n \neq 0$$

Thus, the map cannot possibly be surjective. ///

[28.4] Let $G : \{\mathbb{Z} - \text{modules}\} \longrightarrow \{\text{sets}\}$ be the functor that forgets that a module is a module, and just retains the underlying set. Let $F : \{\text{sets}\} \longrightarrow \{\mathbb{Z} - \text{modules}\}$ be the functor which creates the free module FS on the set S (*and* keeps in mind a map $i : S \longrightarrow FS$). Show that for any set S and any $\mathbb{Z}$-module M

$$\mathrm{Hom}_{\mathbb{Z}}(FS, M) \approx \mathrm{Hom}_{\mathrm{sets}}(S, GM)$$

Prove that the isomorphism you describe is *natural* in S. (It is also natural in M, but don't prove this.)

Our definition of *free module* says that $FS = X$ is free on a (set) map $i : S \longrightarrow X$ if for every set map $\varphi : S \longrightarrow M$ with R-module M gives a unique R-module map $\Phi : X \longrightarrow M$ such that the diagram

$$\begin{tikzcd} X \arrow[dr, dashed, "\Phi"] & \\ S \arrow[u, "i"] \arrow[r, "\varphi"'] & M \end{tikzcd}$$

commutes. Of course, given Φ, we obtain $\varphi = \Phi \circ i$ by composition (in effect, restriction). We claim that the required isomorphism is

$$\mathrm{Hom}_{\mathbb{Z}}(FS, M) \xleftrightarrow{\Phi \longleftrightarrow \varphi} \mathrm{Hom}_{\mathrm{sets}}(S, GM)$$

Even prior to naturality, we must prove that this is a bijection. Note that the set of maps of a set into an R-module has a natural structure of R-module, by

$$(r \cdot \varphi)(s) = r \cdot \varphi(s)$$

The map in the direction $\varphi \longrightarrow \Phi$ is an *injection*, because two maps φ, ψ mapping $S \longrightarrow M$ that induce the same map Φ on X give $\varphi = \Phi \circ i = \psi$, so $\varphi = \psi$. And the map $\varphi \longrightarrow \Phi$ is *surjective* because a given Φ is induced from $\varphi = \Phi \circ i$.

For naturality, for fixed S and M let the map $\varphi \longrightarrow \Phi$ be named $j_{S,M}$. That is, the isomorphism is

$$\mathrm{Hom}_{\mathbb{Z}}(FS, M) \xleftarrow{j_{S,X}} \mathrm{Hom}_{\mathrm{sets}}(S, GM)$$

To show naturality in S, let $f : S \longrightarrow S'$ be a set map. Let $i' : S' \longrightarrow X'$ be a free module on S'. That is, $X' = FS'$. We must show that

$$\begin{tikzcd} \mathrm{Hom}_{\mathbb{Z}}(FS, M) & \mathrm{Hom}_{\mathrm{sets}}(S, GM) \arrow[l, "j_{S,M}"'] \\ \mathrm{Hom}_{\mathbb{Z}}(FS', M) \arrow[u, "- \circ Ff"] & \mathrm{Hom}_{\mathrm{sets}}(S', GM) \arrow[l, "j_{S',M}"'] \arrow[u, "- \circ f"'] \end{tikzcd}$$

commutes, where $- \circ f$ is pre-composition by f, and $- \circ Ff$ is pre-composition by the induced map $Ff : FS \longrightarrow FS'$ on the free modules $X = FS$ and $X' = FS'$. Let $\varphi \in \mathrm{Hom}_{\mathrm{set}}(S', GM)$, and $x = \sum_s r_s \cdot i(s) \in X = FS$, Go up, then left, in the diagram, computing,

$$(j_{S,M} \circ (- \circ f))(\varphi)(x) = j_{S,M}(\varphi \circ f)(x) = j_{S,M}(\varphi \circ f)\left(\sum_s r_s i(s)\right) = \sum_s r_s (\varphi \circ f)(s)$$

On the other hand, going left, then up, gives

$$((- \circ Ff) \circ j_{S',M})(\varphi)(x) = (j_{S',M}(\varphi) \circ Ff)(x) = (j_{S',M}(\varphi))\, Ff(x)$$

$$= (j_{S',M}(\varphi))\left(\sum_s r_s i'(fs)\right) = \sum_s r_s \varphi(fs)$$

These are the same. ///

[28.5] Let $M = \begin{pmatrix} m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix}$ be a 2-by-3 integer matrix, such that the *gcd* of the three 2-by-2 minors is 1. Prove that there exist three integers m_{11}, m_{12}, m_{33} such that

$$\det \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix} = 1$$

This is the easiest of this and the following two examples. Namely, let M_i be the 2-by-2 matrix obtained by omitting the i^{th} column of the given matrix. Let a, b, c be integers such that

$$a \det M_1 - b \det M_2 + c \det M_3 = \gcd(\det M_1, \det M_2, \det M_3) = 1$$

Then, expanding by minors,

$$\det \begin{pmatrix} a & b & c \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix} = a \det M_1 - b \det M_2 + c \det M_3 = 1$$

as desired. ///

[28.6] Let a, b, c be integers whose *gcd* is 1. Prove (without manipulating matrices) that there is a 3-by-3 integer matrix with top row $(a\ b\ c)$ with determinant 1.

Let $F = \mathbb{Z}^3$, and $E = \mathbb{Z} \cdot (a, b, c)$. We claim that, since $\gcd(a, b, c) = 1$, F/E is torsion-free. Indeed, for $(x, y, z) \in F = \mathbb{Z}^3$, $r \in \mathbb{Z}$, and $r \cdot (x, y, z) \in E$, there must be an integer t such that $ta = rx$, $tb = ry$, and $tc = rz$. Let u, v, w be integers such that

$$ua + vb + wz = \gcd(a, b, c) = 1$$

Then the usual stunt gives

$$t = t \cdot 1 = t \cdot (ua + vb + wz) = u(ta) + v(tb) + w(tc) = u(rx) + v(ry) + w(rz) = r \cdot (ux + vy + wz)$$

This implies that $r|t$. Thus, dividing through by r, $(x, y, z) \in \mathbb{Z} \cdot (a, b, c)$, as claimed.

Invoking the Structure Theorem for finitely-generated $\mathbb{Z}$-modules, there is a basis f_1, f_2, f_3 for F and $0 < d_1 \in \mathbb{Z}$ such that $E = \mathbb{Z} \cdot d_1 f_1$. Since F/E is torsionless, $d_1 = 1$, and $E = \mathbb{Z} \cdot f_1$. Further, since both (a, b, c) and f_1 generate E, and $\mathbb{Z}^\times = \{\pm 1\}$, without loss of generality we can suppose that $f_1 = (a, b, c)$.

Let A be an endomorphism of $F = \mathbb{Z}^3$ such that $Af_i = e_i$. Then, writing A for the matrix giving the endomorphism A,

$$(a, b, c) \cdot A = (1, 0, 0)$$

Since A has an inverse B,

$$1 = \det 1_3 = \det(AB) = \det A \cdot \det B$$

so the determinants of A and B are in $\mathbb{Z}^\times = \{\pm 1\}$. We can adjust A by right-multiplying by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

to make $\det A = +1$, and retaining the property $f_1 \cdot A = e_1$. Then

$$A^{-1} = 1_3 \cdot A^{-1} = \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} \cdot A^{-1} = \begin{pmatrix} a & b & c \\ * & * & * \\ * & * & * \end{pmatrix}$$

That is, the original (a, b, c) is the top row of A^{-1}, which has integer entries and determinant 1. ///

[28.7] Let

$$M = \begin{pmatrix} m_{11} & m_{12} & m_{13} & m_{14} & m_{15} \\ m_{21} & m_{22} & m_{23} & m_{24} & m_{25} \\ m_{31} & m_{32} & m_{33} & m_{34} & m_{35} \end{pmatrix}$$

and suppose that the *gcd* of all determinants of 3-by-3 minors is 1. Prove that there exists a 5-by-5 integer matrix $\widetilde{M}$ with M as its top 3 rows, such that $\det \widetilde{M} = 1$.

Let $F = \mathbb{Z}^5$, and let E be the submodule generated by the rows of the matrix. Since $\mathbb{Z}$ is a PID and F is free, E is free.

Let $e_1, \ldots, e_5$ be the standard basis for $\mathbb{Z}^5$. We have shown that the monomials $e_{i_1} \wedge e_{i_2} \wedge e_{i_3}$ with $i_1 < i_2 < i_3$ are a basis for $\bigwedge^3 F$. Since the *gcd* of the determinants of 3-by-3 minors is 1, some determinant of 3-by-3 minor is non-zero, so the rows of M are linearly independent over $\mathbb{Q}$, so E has rank 3 (rather than something less). The structure theorem tells us that there is a $\mathbb{Z}$-basis $f_1, \ldots, f_5$ for F and divisors $d_1 | d_2 | d_3$ (all non-zero since E is of rank 3) such that

$$E = \mathbb{Z} \cdot d_1 f_1 \oplus \mathbb{Z} \cdot d_2 f_2 \oplus \mathbb{Z} \cdot d_3 f_3$$

Let $i : E \longrightarrow F$ be the inclusion. Consider $\bigwedge^3 : \bigwedge^3 E \longrightarrow \bigwedge^3 F$. We know that $\bigwedge^3 E$ has $\mathbb{Z}$-basis

$$d_1 f_1 \wedge d_2 f_2 \wedge d_3 f_3 = (d_1 d_2 d_3) \cdot (f_1 \wedge f_2 \wedge f_3)$$

On the other hand, we claim that the coefficients of $(d_1 d_2 d_3) \cdot (f_1 \wedge f_2 \wedge f_3)$ in terms of the basis $e_{i_1} \wedge e_{i_2} \wedge e_{i_3}$ for $\bigwedge^3 F$ are exactly (perhaps with a change of sign) the determinants of the 3-by-3 minors of M. Indeed, since both f_1, f_2, f_3 and the three rows of M are bases for the rowspace of M, the f_is are linear combinations of the rows, and *vice versa* (with integer coefficients). Thus, there is a 3-by-3 matrix with determinant ± 1 such that left multiplication of M by it yields a new matrix with rows f_1, f_2, f_3. At the same time, this changes the determinants of 3-by-3 minors by at most $\pm$, by the multiplicativity of determinants.

The hypothesis that the *gcd* of all these coordinates is 1 means exactly that $\bigwedge^3 F / \bigwedge^3 E$ is torsion-free. (If the coordinates had a common factor $d > 1$, then d would annihilate the quotient.) This requires that $d_1 d_2 d_3 = 1$, so $d_1 = d_2 = d_3 = 1$ (since we take these divisors to be positive). That is,

$$E = \mathbb{Z} \cdot f_1 \oplus \mathbb{Z} \cdot f_2 \oplus \mathbb{Z} \cdot f_3$$

Writing f_1, f_2, and f_3 as row vectors, they are $\mathbb{Z}$-linear combinations of the rows of M, which is to say that there is a 3-by-3 integer matrix L such that

$$L \cdot M = \begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix}$$

Since the f_i are also a $\mathbb{Z}$-basis for E, there is another 3-by-3 integer matrix K such that

$$M = K \cdot \begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix}$$

Then $LK = LK = 1_3$. In particular, taking determinants, both K and L have determinants in $\mathbb{Z}^\times$, namely, ± 1.

Let A be a $\mathbb{Z}$-linear endomorphism of $F = \mathbb{Z}^5$ mapping f_i to e_i. Also let A be the 5-by-5 integer matrix such that right multiplication of a row vector by A gives the effect of the endomorphism A. Then

$$L \cdot M \cdot A = \begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix} \cdot A = \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix}$$

Since the endormorphism A is invertible on $F = \mathbb{Z}^5$, it has an inverse endomorphism A^{-1}, whose matrix has integer entries. Then

$$M = L^{-1} \cdot \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} \cdot A^{-1}$$

Let

$$\Lambda = \begin{pmatrix} L^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}$$

where the $\pm 1 = \det A = \det A^{-1}$. Then

$$\Lambda \cdot \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \end{pmatrix} \cdot A^{-1} = \Lambda \cdot 1_5 \cdot A^{-1} = \Lambda \cdot A^{-1}$$

has integer entries and determinant 1 (since we adjusted the ± 1 in Λ). At the same time, it is

$$\Lambda \cdot A^{-1} = \begin{pmatrix} L^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix} \cdot \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ * \\ * \end{pmatrix} \cdot A^{-1} = \begin{pmatrix} M \\ * \\ * \end{pmatrix} = \text{5-by-5}$$

This is the desired integer matrix $\tilde{M}$ with determinant 1 and upper 3 rows equal to the given matrix.
///

[28.8] Let R be a commutative ring with unit. For a *finitely-generated* free R-module F, prove that there is a (natural) isomorphism

$$\mathrm{Hom}_R(F, R) \approx F$$

Or is it only

$$\mathrm{Hom}_R(R, F) \approx F$$

instead? (*Hint:* Recall the definition of a free module.)

For *any* R-module M, there is a (natural) isomorphism

$$i : M \longrightarrow \mathrm{Hom}_R(R, M)$$

given by

$$i(m)(r) = r \cdot m$$

This is *injective*, since if $i(m)(r)$ were the 0 homomorphism, then $i(m)(r) = 0$ for all r, which is to say that $r \cdot m = 0$ for all $r \in R$, in particular, for $r = 1$. Thus, $m = 1 \cdot m = 0$, so $m = 0$. (Here we use the standing assumption that $1 \cdot m = m$ for all $m \in M$.) The map is *surjective*, since, given $\varphi \in \mathrm{Hom}_R(R, M)$, we have

$$\varphi(r) = \varphi(r \cdot 1) = r \cdot \varphi(1)$$

That is, $m = \varphi(1)$ determines φ completely. Then $\varphi = i(\varphi(m))$ and $m = i(m)(1)$, so these are mutually inverse maps. This did *not* use finite generation, nor free-ness. ///

Consider now the other form of the question, namely whether or not

$$\mathrm{Hom}_R(F, R) \approx F$$

is valid for F finitely-generated and free. Let F be free on $i : S \longrightarrow F$, with finite S. Use the natural isomorphism

$$\mathrm{Hom}_R(F, R) \approx \mathrm{Hom}_{\mathrm{sets}}(S, R)$$

discussed earlier. The right-hand side is the collection of R-valued functions on S. Since S is finite, the collection of *all* R-valued functions on S is just the collection of functions which vanish off a finite subset. The latter was our construction of the free R-module on S. So we have the isomorphism. ///

[11.0.2] **Remark:** Note that if S is not finite, $\mathrm{Hom}_R(F, R)$ is too large to be isomorphic to F. If F is not free, it may be too small. Consider $F = \mathbb{Z}/n$ and $R = \mathbb{Z}$, for example.

[11.0.3] **Remark:** And this discussion needs a *choice* of the generators $i : S \longrightarrow F$. In the language style which speaks of generators as being chosen elements of the module, we have most certainly *chosen a basis*.

[28.9] Let R be an integral domain. Let M and N be free R-modules of finite ranks r, s, respectively. Suppose that there is an R-bilinear map

$$B : M \times N \longrightarrow R$$

which is *non-degenerate* in the sense that for every $0 \neq m \in M$ there is $n \in N$ such that $B(m, n) \neq 0$, and *vice versa*. Prove that $r = s$.

All tensors and homomorphisms are over R, so we suppress the subscript and other references to R when reasonable to do so. We use the important identity (proven afterward)

$$\mathrm{Hom}(A \otimes B, C) \xrightarrow{i_{A,B,C}} \mathrm{Hom}(A, \mathrm{Hom}(B, C))$$

by

$$i_{A,B,C}(\Phi)(a)(b) = \Phi(a \otimes b)$$

We also use the fact (from an example just above) that for F free on $t : S \longrightarrow F$ there is the natural (given $t : S \longrightarrow F$, anyway!) isomorphism

$$j : \mathrm{Hom}(F, R) \approx \mathrm{Hom}_{\mathrm{sets}}(S, R) = F$$

for modules E, given by

$$j(\psi)(s) = \psi(t(s))$$

where we use construction of free modules on sets S that they are R-valued functions on S taking non-zero values at only finitely-many elements.

Thus,

$$\mathrm{Hom}(M \otimes N, R) \xrightarrow{i} \mathrm{Hom}(M, \mathrm{Hom}(N, R)) \xrightarrow{j} \mathrm{Hom}(M, N)$$

The bilinear form B induces a linear functional β such that

$$\beta(m \otimes n) = B(m, n)$$

The hypothesis says that for each $m \in M$ there is $n \in N$ such that

$$i(\beta)(m)(n) \neq 0$$

That is, for all $m \in M$, $i(\beta)(m) \in \mathrm{Hom}(N, R) \approx N$ is 0. That is, the map $m \longrightarrow i(\beta)(m)$ is *injective*. So the existence of the non-degenerate bilinear pairing yields an injection of M to N. Symmetrically, there is an injection of N to M.

Using the assumption that R is a PID, we know that a submodule of a free module is free of lesser-or-equal rank. Thus, the two inequalities

$$\mathrm{rank}\, M \leq \mathrm{rank}\, N \qquad \mathrm{rank}\, N \leq \mathrm{rank}\, M$$

from the two inclusions imply equality. ///

[11.0.4] **Remark:** The hypothesis that R is a PID may be too strong, but I don't immediately see a way to work around it.

Now let's prove (again?) that

$$\mathrm{Hom}(A \otimes B, C) \xrightarrow{\quad i \quad} \mathrm{Hom}(A, \mathrm{Hom}(B, C))$$

by

$$i(\Phi)(a)(b) = \Phi(a \otimes b)$$

is an isomorphism. The map in the other direction is

$$j(\varphi)(a \otimes b) = \varphi(a)(b)$$

First,

$$i(j(\varphi))(a)(b) = j(\varphi)(a \otimes b) = \varphi(a)(b)$$

Second,

$$j(i(\Phi))(a \otimes b) = i(\Phi)(a)(b) = \Phi(a \otimes b)$$

Thus, these maps are mutual inverses, so each is an isomorphism. ///

[28.10] Write an explicit isomorphism

$$\mathbb{Z}/a \otimes_{\mathbb{Z}} \mathbb{Z}/b \longrightarrow \mathbb{Z}/\gcd(a, b)$$

and verify that it is what is claimed.

First, we know that monomial tensors generate the tensor product, and for any $x, y \in \mathbb{Z}$

$$x \otimes y = (xy) \cdot (1 \otimes 1)$$

so the tensor product is generated by $1 \otimes 1$. Next, we claim that $g = \gcd(a, b)$ annihilates every $x \otimes y$, that is, $g \cdot (x \otimes y) = 0$. Indeed, let r, s be integers such that $ra + sb = g$. Then

$$g \cdot (x \otimes y) = (ra + sb) \cdot (x \otimes y) = r(ax \otimes y) = s(x \otimes by) = r \cdot 0 + s \cdot 0 = 0$$

So the generator $1 \otimes 1$ has order dividing g. To prove that that generator has order *exactly* g, we construct a bilinear map. Let

$$B : \mathbb{Z}/a \times \mathbb{Z}/b \longrightarrow \mathbb{Z}/g$$

by

$$B(x \times y) = xy + g\mathbb{Z}$$

To see that this is well-defined, first compute

$$(x + a\mathbb{Z})(y + b\mathbb{Z}) = xy + xb\mathbb{Z} + ya\mathbb{Z} + ab\mathbb{Z}$$

Since

$$xb\mathbb{Z} + ya\mathbb{Z} \subset b\mathbb{Z} + a\mathbb{Z} = \gcd(a, b)\mathbb{Z}$$

(and $ab\mathbb{Z} \subset g\mathbb{Z}$), we have

$$(x + a\mathbb{Z})(y + b\mathbb{Z}) + g\mathbb{Z} = xy + xb\mathbb{Z} + ya\mathbb{Z} + ab\mathbb{Z} + \mathbb{Z}$$

and well-definedness. By the defining property of the tensor product, this gives a unique linear map β on the tensor product, which on monomials is

$$\beta(x \otimes y) = xy + \gcd(a, b)\mathbb{Z}$$

The generator $1 \otimes 1$ is mapped to 1, so the image of $1 \otimes 1$ has order $\gcd(a, b)$, so $1 \otimes 1$ has order divisible by $\gcd(a, b)$. Thus, having already proven that $1 \otimes 1$ has order at most $\gcd(a, b)$, this must be its order.

In particular, the map β is injective on the cyclic subgroup generated by $1 \otimes 1$. That cyclic subgroup is the whole group, since $1 \otimes 1$. The map is also surjective, since $\cdot 1 \otimes 1$ hits $r \bmod \gcd(a, b)$. Thus, it is an isomorphism. ///

[28.11] Let $\varphi : R \longrightarrow S$ be commutative rings with unit, and suppose that $\varphi(1_R) = 1_S$, thus making S an R-algebra. For an R-module N prove that $\mathrm{Hom}_R(S, N)$ is (*yet another*) good definition of *extension of scalars* from R to S, by checking that for every S-module M there is a natural isomorphism

$$\mathrm{Hom}_R(\mathrm{Res}^S_R M, N) \approx \mathrm{Hom}_S(M, \mathrm{Hom}_R(S, N)$$

where $\mathrm{Res}^S_R M$ is the R-module obtained by forgetting S, and letting $r \in R$ act on M by $r \cdot m = \varphi(r)m$. (*Do* prove naturality in M, also.)

Let

$$i : \mathrm{Hom}_R(\mathrm{Res}^S_R M, N) \longrightarrow \mathrm{Hom}_S(M, \mathrm{Hom}_R(S, N)$$

be defined for $\varphi \in \mathrm{Hom}_R(\mathrm{Res}^S_R M, N)$ by

$$i(\varphi)(m)(s) = \varphi(s \cdot m)$$

This makes *some* sense, at least, since M is an S-module. We must verify that $i(\varphi) : M \longrightarrow \mathrm{Hom}_R(S, N)$ is S-linear. Note that the S-module structure on $\mathrm{Hom}_R(S, N)$ is

$$(s \cdot \psi)(t) = \psi(st)$$

where $s, t \in S$, $\psi \in \mathrm{Hom}_R(S, N)$. Then we check:

$$\left(i(\varphi)(sm)\right)(t) = i(\varphi)(t \cdot sm) = i(\varphi)(stm) = i(\varphi)(m)(st) = \left(s \cdot i(\varphi)(m)\right)(t)$$

which proves the S-linearity.

The map j in the other direction is described, for $\Phi \in \mathrm{Hom}_S(M, \mathrm{Hom}_R(S,N))$, by

$$j(\Phi)(m) = \Phi(m)(1_S)$$

where 1_S is the identity in S. Verify that these are mutual inverses, by

$$i(j(\Phi))(m)(s) = j(\Phi)(s\cdot m) = \Phi(sm)(1_S) = (s\cdot\Phi(m))\,(1_S) = \Phi(m)(s\cdot 1_S) = \Phi(m)(s)$$

as hoped. (Again, the equality

$$(s\cdot\Phi(m))\,(1_S) = \Phi(m)(s\cdot 1_S)$$

is the definition of the S-module structure on $\mathrm{Hom}_R(S,N)$.) In the other direction,

$$j(i(\varphi))(m) = i(\varphi)(m)(1_S) = \varphi(1\cdot m) = \varphi(m)$$

Thus, i and j are mutual inverses, so are isomorphisms.

For naturality, let $f : M \longrightarrow M'$ be an S-module homomorphism. Add indices to the previous notation, so that

$$i_{M,N} : \mathrm{Hom}_R(\mathrm{Res}^S_R M, N) \longrightarrow \mathrm{Hom}_S(M, \mathrm{Hom}_R(S,N)$$

is the isomorphism discussed just above, and $i_{M',N}$ the analogous isomorphism for M' and N. We must show that the diagram

$$\begin{tikzcd}
\mathrm{Hom}_R(\mathrm{Res}^S_R M, N) \arrow[r, "i_{M,N}"] & \mathrm{Hom}_S(M, \mathrm{Hom}_R(S,N)) \\
\mathrm{Hom}_R(\mathrm{Res}^S_R M', N)) \arrow[u, "-\circ f"] \arrow[r, "i_{M',N}"] & \mathrm{Hom}_S(M', \mathrm{Hom}_R(S,N)) \arrow[u, "-\circ f"']
\end{tikzcd}$$

commutes, where $-\circ f$ is pre-composition with f. (We use the same symbol for the map $f : M \longrightarrow M'$ on the modules whose S-structure has been forgotten, leaving only the R-module structure.) Starting in the lower left of the diagram, going up then right, for $\varphi \in \mathrm{Hom}_R(\mathrm{Res}^S_R M', N)$,

$$(i_{M,N} \circ (-\circ f)\;\varphi)\,(m)(s) = (i_{M,N}(\varphi\circ f))\,(m)(s) = (\varphi\circ f)(s\cdot m) = \varphi(f(s\cdot m))$$

On the other hand, going right, then up,

$$((-\circ f)\circ i_{M',N}\;\varphi)\,(m)(s) = (i_{M',N}\;\varphi)\,(fm)(s) = \varphi(s\cdot fm) = \varphi(f(s\cdot m))$$

since f is S-linear. That is, the two outcomes are the same, so the diagram commutes, proving functoriality in M, which is a part of the naturality assertion. ///

[28.12] Let

$$M = \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z} \qquad N = \mathbb{Z}\oplus 4\mathbb{Z}\oplus 24\mathbb{Z}\oplus 144\mathbb{Z}$$

What are the elementary divisors of $\bigwedge^2(M/N)$?

First, note that this is *not* the same as asking about the structure of $(\bigwedge^2 M)/(\bigwedge^2 N)$. Still, we can address that, too, after dealing with the question that *was* asked.

First,

$$M/N = \mathbb{Z}/\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/24\mathbb{Z}\oplus\mathbb{Z}/144\mathbb{Z} \approx \mathbb{Z}/4\oplus\mathbb{Z}/24\oplus\mathbb{Z}/144$$

where we use the obvious slightly lighter notation. Generators for M/N are

$$m_1 = 1\oplus 0\oplus 0 \quad m_2 = 0\oplus 1\oplus 0 \quad m_3 = 0\oplus 0\oplus 1$$

where the 1s are respectively in $\mathbb{Z}/4$, $\mathbb{Z}/24$, and $\mathbb{Z}/144$. We know that $e_i \wedge e_j$ *generate* the exterior square, for the 3 pairs of indices with $i < j$. Much as in the computation of $\mathbb{Z}/a \otimes \mathbb{Z}/b$, for e in a $\mathbb{Z}$-module E with $a \cdot e = 0$ and f in E with $b \cdot f = 0$, let r, s be integers such that

$$ra + sb = \gcd(a, b)$$

Then

$$\gcd(a, b) \cdot e \wedge f = r(ae \wedge f) + s(e \wedge bf) = r \cdot 0 + s \cdot 0 = 0$$

Thus, $4 \cdot e_1 \wedge e_2 = 0$ and $4 \cdot e_1 \wedge e_3 = 0$, while $24 \cdot e_2 \wedge e_3 = 0$. If there are no further relations, then we could have

$$\bigwedge^2(M/N) \approx \mathbb{Z}/4 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/24$$

(so the elementary divisors would be $4, 4, 24$.)

To prove, in effect, that there are no further relations than those just indicated, we must construct suitable alternating bilinear maps. Suppose for $r, s, t \in \mathbb{Z}$

$$r \cdot e_1 \wedge e_2 + s \cdot e_1 \wedge e_3 + t \cdot e_2 \wedge e_3 = 0$$

Let

$$B_{12} : (\mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3) \times (\mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3) \longrightarrow \mathbb{Z}/4$$

by

$$B_{12}(xe_1 + ye_2 + ze_3,\ \xi e_1 + \eta e_2 + \zeta e_3) = (x\eta - \xi y) + 4\mathbb{Z}$$

(As in earlier examples, since $4|4$ and $4|24$, this is *well-defined.*) By arrangement, this B_{12} is alternating, and induces a unique linear map β_{12} on $\bigwedge^2(M/N)$, with

$$\beta_{12}(e_1 \wedge e_2) = 1 \qquad \beta_{12}(e_1 \wedge e_3) = 0 \qquad \beta_{12}(e_2 \wedge e_3) = 0$$

Applying this to the alleged relation, we find that $r = 0 \bmod 4$. Similar contructions for the other two pairs of indices $i < j$ show that $s = 0 \bmod 4$ and $t = 0 \bmod 24$. This shows that we have all the relations, and

$$\bigwedge^2(M/N) \approx \mathbb{Z}/4 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/24$$

as hoped/claimed. ///

Now consider the other version of this question. Namely, letting

$$M = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \qquad N = \mathbb{Z} \oplus 4\mathbb{Z} \oplus 24\mathbb{Z} \oplus 144\mathbb{Z}$$

compute the elementary divisors of $(\bigwedge^2 M)/(\bigwedge^2 N)$.

Let e_1, e_2, e_3, e_4 be the standard basis for $\mathbb{Z}^4$. Let $i : N \longrightarrow M$ be the inclusion. We have shown that exterior powers of free modules are free with the expected generators, so M is free on

$$e_1 \wedge e_2,\ \ e_1 \wedge e_3,\ \ e_1 \wedge e_4,\ \ e_2 \wedge e_3,\ \ e_2 \wedge e_4,\ \ e_3 \wedge e_4$$

and N is free on

$$(1 \cdot 4)\, e_1 \wedge e_2,\ \ (1 \cdot 24)\, e_1 \wedge e_3,\ \ (1 \cdot 144)\, e_1 \wedge e_4,\ \ (4 \cdot 24)\, e_2 \wedge e_3,\ \ (4 \cdot 144)\, e_2 \wedge e_4,\ \ (24 \cdot 144)\, e_3 \wedge e_4$$

The inclusion $i : N \longrightarrow M$ induces a natural map $\bigwedge^2 i : \bigwedge^2 \longrightarrow \bigwedge^2 M$, taking $r \cdot e_i \wedge e_j$ (in N) to $r \cdot e_i \wedge e_j$ (in M). Thus, the quotient of $\bigwedge^2 M$ by (the image of) $\bigwedge^2 N$ is visibly

$$\mathbb{Z}/4 \oplus \mathbb{Z}/24 \oplus \mathbb{Z}/144 \oplus \mathbb{Z}/96 \oplus \mathbb{Z}/576 \oplus \mathbb{Z}/3456$$

The integers $4, 24, 144, 96, 576, 3456$ do not quite have the property $4|24|144|96|576|3456$, so are not elementary divisors. The problem is that neither $144|96$ nor $96|144$. The only primes dividing all these integers are 2 and 3, and, in particular,

$$4 = 2^2,\ 24 = 2^3 \cdot 3,\ 144 = 2^4 \cdot 3^2,\ 96 = 2^5 \cdot 3,\ 576 = 2^6 \cdot 3^2,\ 3456 = 2^7 \cdot 3^3,$$

From Sun-Ze's theorem,

$$\mathbb{Z}/(2^a \cdot 3^b) \approx \mathbb{Z}/2^a \oplus \mathbb{Z}/3^b$$

so we can rewrite the summands $\mathbb{Z}/144$ and $\mathbb{Z}/96$ as

$$\mathbb{Z}/144 \oplus \mathbb{Z}/96 \approx (\mathbb{Z}/2^4 \oplus \mathbb{Z}/3^2) \oplus (\mathbb{Z}/2^5 \oplus \mathbb{Z}/3) \approx (\mathbb{Z}/2^4 \oplus \mathbb{Z}/3) \oplus (\mathbb{Z}/2^5 \oplus \mathbb{Z}/3^2) \approx \mathbb{Z}/48 \oplus \mathbb{Z}/288$$

Now we do have $4|24|48|288|576|3456$, and

$$(\textstyle\bigwedge^2 M)/(\bigwedge^2 N) \approx \mathbb{Z}/4 \oplus \mathbb{Z}/24 \oplus \mathbb{Z}/48 \oplus \mathbb{Z}/288 \oplus \mathbb{Z}/576 \oplus \mathbb{Z}/3456$$

is in elementary divisor form. ///

Exercises

28.[11.0.1] Show that there is a natural isomorphism

$$f_X : \Pi_s \operatorname{Hom}_R(M_s, X) \approx \operatorname{Hom}_R(\oplus_s M_s, X)$$

where everything is an R-module, and R is a commutative ring.

28.[11.0.2] For an abelian group A (equivalently, $\mathbb{Z}$-module), the *dual* group ($\mathbb{Z}$-module) is

$$A^* = \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z})$$

Prove that the dual group of a direct sum is the direct product of the duals. Prove that the dual group of a *finite* abelian group A is isomorphic to A (although not *naturally* isomorphic).

28.[11.0.3] Let R be a commutative ring with unit. Let M be a finitely-generated free module over R. Let $M^* = \operatorname{Hom}_R(M, R)$ be the dual. Show that, for each integer $\ell \geq 1$, the module $\bigwedge^\ell M$ is dual to $\bigwedge^\ell M^*$, under the bilinear map induced by

$$\langle m_1 \wedge \ldots \wedge m_\ell,\ \mu_1 \wedge \ldots \wedge \mu_\ell \rangle \ = \ \det\{\langle m_i, \mu_j \rangle\}$$

for $m_i \in M$ and $\mu_j \in M^*$.

28.[11.0.4] Let $v_1, \ldots, v_n$ be linearly independent vectors in a vector space V over a field k. For each pair of indices $i < j$, take another vector $w_{ij} \in V$. Suppose that

$$\sum_{i<j} v_i \wedge v_j \wedge w_{ij} = 0$$

Show that the w_{ij}'s are in the span of the v_k's. Let

$$w_{ij} = \sum_k c_{ij}^k\, v_k$$

Show that, for $i < j < k$,

$$c_{ij}^k - c_{ik}^j + c_{jk}^i = 0$$

28.[11.0.5] Show that the *adjugate* (that is, *cofactor*) matrix of a 2-by-2 matrix with entries in a commutative ring R is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\mathrm{adg}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

28.[11.0.6] Let M be an n-by-n matrix with entries in a commutative ring R with unit, viewed as an endomorphism of the free R-module R^n by left matrix multiplication. Determine the matrix entries for the adjugate matrix M^{adg} in terms of those of M.