(*April 9, 2024*)

Discussion 08

Paul Garrett garrett@umn.edu https://www-users.cse.umn.edu/~garrett/

[08.1] Let $T \in \mathrm{Hom}_k(V)$ for a finite-dimensional k-vectorspace V, with k a field. Let W be a T-stable subspace. Prove that the minimal polynomial of T on W is a divisor of the minimal polynomial of T on V. Define a natural action of T on the quotient V/W, and prove that the minimal polynomial of T on V/W is a divisor of the minimal polynomial of T on V.

Discussion: Let $f(x)$ be the minimal polynomial of T on V, and $g(x)$ the minimal polynomial of T on W. (We need the T-stability of W for this to make sense at all.) Since $f(T) = 0$ on V, and since the restriction map

$$\mathrm{End}_k(V) \to \mathrm{End}_k(W)$$

is a ring homomorphism,

$$(\text{restriction of}) f(t) = f(\text{restriction of } T)$$

Thus, $f(T) = 0$ on W. That is, by definition of $g(x)$ and the PID-ness of $k[x]$, $f(x)$ is a multiple of $g(x)$, as desired.

Define $\overline{T}(v + W) = Tv + W$. Since $TW \subset W$, this is well-defined. Note that we cannot assert, and do not need, an *equality* $TW = W$, but only containment. Let $h(x)$ be the minimal polynomial of $\overline{T}$ (on V/W). Any polynomial $p(T)$ stabilizes W, so gives a well-defined map $\overline{p(T)}$ on V/W. Further, since the natural map

$$\mathrm{End}_k(V) \to \mathrm{End}_k(V/W)$$

is a ring homomorphism, we have

$$\overline{p(T)}(v + W) = p(T)(v) + W = p(T)(v + W) + W = p(\overline{T})(v + W)$$

Since $f(T) = 0$ on V, $f(\overline{T}) = 0$. By definition of minimal polynomial, $h(x)|f(x)$. ///

[08.2] Let $T \in \mathrm{Hom}_k(V)$ for a finite-dimensional k-vectorspace V, with k a field. Suppose that T is *diagonalizable* on V. Let W be a T-stable subspace of V. Show that T is diagonalizable on W.

Discussion: Since T is diagonalizable, its minimal polynomial $f(x)$ on V factors into linear factors in $k[x]$ (with zeros exactly the eigenvalues), and no factor is repeated. By the previous example, the minimal polynomial $g(x)$ of T on W divides $f(x)$, so (by unique factorization in $k[x]$) factors into linear factors without repeats. And this implies that T is diagonalizable when restricted to W. ///

[08.3] Let $T \in \mathrm{Hom}_k(V)$ for a finite-dimensional k-vectorspace V, with k a field. Suppose that T is *diagonalizable* on V, with *distinct eigenvalues*. Let $S \in \mathrm{Hom}_k(V)$ commute with T, in the natural sense that $ST = TS$. Show that S is diagonalizable on V.

Discussion: The hypothesis of *distinct eigenvalues* means that each eigenspace is *one-dimensional*. We have seen that commuting operators stabilize each other's eigenspaces. Thus, S stabilizes each one-dimensional λ-eigenspaces V_λ for T. By the one-dimensionality of V_λ, S is a scalar μ_λ on V_λ. That is, the basis of eigenvectors for T is unavoidably a basis of eigenvectors for S, too, so S is diagonalizable. ///

[08.4] Let $T \in \mathrm{Hom}_k(V)$ for a finite-dimensional k-vectorspace V, with k a field. Suppose that T is *diagonalizable* on V. Show that $k[T]$ contains the projectors to the eigenspaces of T.

Discussion: Though it is only implicit, we only want projectors P which *commute* with T.

Since T is diagonalizable, its minimal polynomial $f(x)$ factors into linear factors and has no repeated factors. For each eigenvalue λ, let $f_\lambda(x) = f(x)/(x-\lambda)$. The hypothesis that no factor is repeated implies that the *gcd* of all these $f_\lambda(x)$ is 1, so there are polynomials $a_\lambda(x)$ in $k[x]$ such that

$$1 = \sum_\lambda a_\lambda(x)\, f_\lambda(x)$$

For $\mu \neq \lambda$, the product $f_\lambda(x) f_\mu(x)$ picks up all the linear factors in $f(x)$, so

$$f_\lambda(T) f_\mu(T) = 0$$

Then for each eigenvalue μ

$$(a_\mu(T)\, f_\mu(T))^2 = (a_\mu(T)\, f_\mu(T))\,(1 - \sum_{\lambda\neq\mu} a_\lambda(T)\, f_\lambda(T)) = (a_\mu(T)\, f_\mu(T))$$

Thus, $P_\mu = a_\mu(T)\, f_\mu(T)$ has $P_\mu^2 = P_\mu$. Since $f_\lambda(T) f_\mu(T) = 0$ for $\lambda \neq \mu$, we have $P_\mu P_\lambda = 0$ for $\lambda \neq \mu$. Thus, these are projectors to the eigenspaces of T, and, being polynomials in T, commute with T.

For uniqueness, observe that the diagonalizability of T implies that V is the sum of the λ-eigenspaces V_λ of T. We know that any endomorphism (such as a projector) commuting with T stabilizes the eigenspaces of T. Thus, given an eigenvalue λ of T, an endomorphism P commuting with T and such that $P(V) = V_\lambda$ must be 0 on T-eigenspaces V_μ with $\mu \neq \lambda$, since

$$P(V_\mu) \subset V_\mu \cap V_\lambda = 0$$

And when restricted to V_λ the operator P is required to be the identity. Since V is the sum of the eigenspaces and P is determined completely on each one, there is only one such P (for each λ). ///

[08.5] Let V be a complex vector space with a (positive definite) inner product. Show that $T \in \mathrm{Hom}_k(V)$ cannot be a normal operator if it has any non-trivial Jordan block.

Discussion: The spectral theorem for normal operators asserts, among other things, that normal operators are diagonalizable, in the sense that there is a basis of eigenvectors. We know that this implies that the minimal polynomial has no repeated factors. Presence of a non-trivial Jordan block exactly means that the minimal polynomial *does* have a repeated factor, so this cannot happen for normal operators. ///

[08.6] Show that a positive-definite hermitian n-by-n matrix A has a unique positive-definite square root B (that is, $B^2 = A$).

Discussion: Even though the question explicitly mentions matrices, it is just as easy to discuss endomorphisms of the vector space $V = \mathbb{C}^n$.

By the spectral theorem, A is diagonalizable, so $V = \mathbb{C}^n$ is the sum of the eigenspaces V_λ of A. By hermitianness these eigenspaces are mutually orthogonal. By positive-definiteness A has *positive* real eigenvalues λ, which therefore have real square roots. Define B on each orthogonal summand V_λ to be the scalar $\sqrt{\lambda}$. Since these eigenspaces are mutually orthogonal, the operator B so defined really is hermitian, as we now verify. Let $v = \sum_\lambda v_\lambda$ and $w = \sum_\mu w_\mu$ be *orthogonal* decompositions of two vectors into eigenvectors v_λ with eigenvalues λ and w_μ with eigenvalues μ. Then, using the orthogonality of eigenvectors with distinct eigenvalues,

$$\langle Bv, w\rangle = \langle B\sum_\lambda v_\lambda, \sum_\mu w_\mu\rangle = \langle \sum_\lambda \lambda v_\lambda, \sum_\mu w_\mu\rangle = \sum_\lambda \lambda\langle v_\lambda, w_\lambda\rangle$$

$$= \sum_\lambda \langle v_\lambda, \lambda w_\lambda\rangle = \langle \sum_\mu v_\mu, \sum_\lambda \lambda w_\lambda\rangle = \langle v, Bw\rangle$$

Uniqueness is slightly subtler. Since we do not know *a priori* that two positive-definite square roots B and C of A *commute*, we *cannot* immediately say that $B^2 = C^2$ gives $(B+C)(B-C) = 0$, etc. If we *could* do that, then since B and C are both positive-definite, we could say

$$\langle (B+C)v, v\rangle = \langle Bv, v\rangle + \langle Cv, v\rangle > 0$$

so $B + C$ is positive-definite and, hence invertible. Thus, $B - C = 0$. But we cannot directly do this. We must be more circumspect.

Let B be a positive-definite square root of A. Then B commutes with A. Thus, B stabilizes each eigenspace of A. Since B is diagonalizable on V, it is diagonalizable on each eigenspace of A (from an earlier example). Thus, since all eigenvalues of B are *positive*, and $B^2 = \lambda$ on the λ-eigenspace V_λ of A, it must be that B is the scalar $\sqrt{\lambda}$ on V_λ. That is, B is uniquely determined. ///

[08.7] Given a square n-by-n complex matrix M, show that there are unitary matrices A and B such that AMB is *diagonal*.

Discussion: *We prove this for not-necessarily square M, with the unitary matrices of appropriate sizes.*

This asserted expression

$$M = \text{unitary} \cdot \text{diagonal} \cdot \text{unitary}$$

is called a **Cartan decomposition** of M.

First, if M is *(square) invertible*, then $T = MM^*$ is self-adjoint and invertible. From an earlier example, the spectral theorem implies that there is a self-adjoint (necessarily invertible) square root S of T. Then

$$1 = S^{-1}TS^{-1} = (S^{-1}M)({}^{-1}SM)^*$$

so $k_1 = S^{-1}M$ is unitary. Let k_2 be unitary such that $D = k_2 S k_2^*$ is diagonal, by the spectral theorem. Then

$$M = Sk_1 = (k_2 D k_2^*)k_1 = k_2 \cdot D \cdot (k_2^* k_1)$$

expresses M as

$$M = \text{unitary} \cdot \text{diagonal} \cdot \text{unitary}$$

as desired.

In the case of m-by-n (not necessarily invertible) M, we want to reduce to the invertible case by showing that there are m-by-m unitary A_1 and n-by-n unitary B_1 such that

$$A_1 M B_1 = \begin{pmatrix} M' & 0 \\ 0 & 0 \end{pmatrix}$$

where M' is *square* and invertible. That is, we can (in effect) do column and row reduction with *unitary* matrices.

Nearly half of the issue is showing that by left (or right) multiplication by a suitable unitary matrix A an arbitrary matrix M may be put in the form

$$AM = \begin{pmatrix} M_{11} & M_{12} \\ 0 & 0 \end{pmatrix}$$

with 0's below the r^{th} row, where the column space of M has dimension r. To this end, let $f_1, \dots, f_r$ be an orthonormal basis for the *column space* of M, and extend it to an orthonormal basis $f_1, \dots, f_m$ for the whole $\mathbb{C}^m$. Let $e_1, \dots, e_m$ be the standard orthonormal basis for $\mathbb{C}^m$. Let A be the linear endomorphism of $\mathbb{C}^m$ defined by $Af_i = e_i$ for all indices i. We claim that this A is unitary, and has the desired effect on

M. That is has the desired effect on M is by design, since any column of the original M will be mapped by A to the span of $e_1, \ldots, e_r$, so will have all 0's below the r^{th} row. A linear endomorphism is determined exactly by where it sends a basis, so all that needs to be checked is the unitariness, which will result from the orthonormality of the bases, as follows. For $v = \sum_i a_i f_i$ and $w = \sum_i b_i f_i$,

$$\langle Av, Aw\rangle = \langle \sum_i a_i\, Af_i, \sum_j b_j\, Af_j\rangle = \langle \sum_i a_i\, e_i, \sum_j b_j\, e_j\rangle = \sum_i a_i\overline{b_i}$$

by orthonormality. And, similarly,

$$\sum_i a_i\overline{b_i} = \langle \sum_i a_i\, f_i, \sum_j b_j\, f_j\rangle = \langle v, w\rangle$$

Thus, $\langle Av, Aw\rangle = \langle v, w\rangle$. To be completely scrupulous, we want to see that the latter condition implies that $A^*A = 1$. We have $\langle A^*Av, w\rangle = \langle v, w\rangle$ for all v and w. If $A^*A \neq 1$, then for some v we would have $A^*Av \neq v$, and for that v take $w = (A^*A - 1)v$, so

$$\langle (A^*A - 1)v, w\rangle = \langle (A^*A - 1)v, (A^*A - 1)v\rangle > 0$$

contradiction. That is, A is certainly unitary.

If we had had the foresight to prove that row rank is always equal to column rank, then we would know that a combination of the previous left multiplication by unitary and a corresponding right multiplication by unitary would leave us with

$$\begin{pmatrix} M' & 0 \\ 0 & 0 \end{pmatrix}$$

with M' *square* and invertible, as desired. ///

[08.8] Given a square n-by-n complex matrix M, show that there is a unitary matrix A such that AM is *upper triangular*.

Discussion: Let $\{e_i\}$ be the standard basis for $\mathbb{C}^n$. To say that a matrix is upper triangular is to assert that (with left multiplication of column vectors) each of the maximal family of nested subspaces (called a **maximal flag**)

$$V_0 = 0 \subset V_1 = \mathbb{C}e_1 \subset \mathbb{C}e_1 + \mathbb{C}e_2 \subset \ldots \subset \mathbb{C}e_1 + \ldots + \mathbb{C}e_{n-1} \subset V_n = \mathbb{C}^n$$

is stabilized by the matrix. Of course

$$MV_0 \subset MV_1 \subset MV_2 \subset \ldots \subset MV_{n-1} \subset V_n$$

is another maximal flag. Let f_{i+1} be a unit-length vector in the orthogonal complement to MV_i inside MV_{i+1} Thus, these f_i are an orthonormal basis for V, and, in fact, $f_1, \ldots, f_t$ is an orthonormal basis for MV_t. Then let A be the unitary endomorphism such that $Af_i = e_i$. (In an earlier example and in class we checked that, indeed, a linear map which sends one orthonormal basis to another is unitary.) Then

$$AMV_i = V_i$$

so AM is upper-triangular. ///

[08.9] Let Z be an m-by-n complex matrix. Let Z^* be its conjugate-transpose. Show that

$$\det(1_m - ZZ^*) = \det(1_n - Z^*Z)$$

Discussion: Write Z in the (rectangular) Cartan decomposition

$$Z = ADB$$

with A and B unitary and D is m-by-n of the form

$$D = \begin{pmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

where the diagonal d_i are the only non-zero entries. We grant ourselves that $\det(xy) = \det(x) \cdot \det(y)$ for square matrices x, y of the same size. Then

$$\det(1_m - ZZ^*) = \det(1_m - ADBB^*D^*A^*) = \det(1_m - ADD^*A^*) = \det(A \cdot (1_m - DD^*) \cdot A^*)$$

$$= \det(AA^*) \cdot \det(1_m - DD^*) = \det(1_m - DD^*) = \prod_i (1 - d_i\overline{d_i})$$

Similarly,

$$\det(1_n - Z^*Z) = \det(1_n - B^*D^*A^*ADB) = \det(1_n - B^*D^*DB) = \det(B^* \cdot (1_n - D^*D) \cdot B)$$

$$= \det(B^*B) \cdot \det(1_n - D^*D) = \det(1_n - D^*D) = \prod_i (1 - d_i\overline{d_i})$$

which is the same as the first computation. ///

[08.10] Give an example of two commuting diagonalizable operators S, T on a 4-dimensional vectorspace V over a field k such that each operator has exactly two eigenvalues, and the eigenspaces are two-dimensional, but/and the intersection of any S-eigenspace with any T-eigenspace is just 1-dimensional. Explain why this does not contradict results about simultaneous eigenvectors

Discussion: Let

$$S = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & \\ & & & 0 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{pmatrix}$$

act on $V = k^4$ (column vectors). Then the standard basis elements $e_1.e_2.e_3.e_4$ are the joint eigenvectors for S and T, with four different ordered pairs of eigenvalues.

The too-naive assertion that for commuting endomorphisms S, T the eigenvectors of S are eigenvectors for T is contradicted by this example, since any vector $ae_1 + be_2$ (with $a, b \in k$) is an eigenvector for S, but not for T unless $ab = 0$.

But, of course, this is perfectly fine, since there is still a basis consisting of joint eigenvectors. The point is that it is unwise to hastily choose a basis of eigenvectors for one operator, hoping or presuming that they'll be eigenvectors for the other operator. For example, $e_1 + e_2$, e_2, e_3, e_4 is a basis consisting of S-eigenvectors, but the first of these is not an eigenvector for T. ///

[08.11] Let T be a diagonalizable operator on a finite-dimensional vector space V over a field k. Suppose that some T-eigenspace is not one-dimensional. Exhibit a diagonalizable endomorphism S of V commuting with T *not* lying in $k[T]$.

Discussion: Let $P \in k[T]$ be the projector to the λ-eigenspace V_λ of T, with $\dim V_\lambda > 1$. Let A be a non-scalar endomorphism of V_λ. Such A exists exactly because $\dim V_\lambda > 1$. Then take $S = A \circ P$. This commutes with T, because for any $v \in V$

$$ST(v) = (AP)T(v) = A(TPv) = A(\lambda \cdot Pv) = \lambda \cdot APv = T(APv)$$

since $APv \in V_\lambda$. Yet, given a polynomial $f(x)$, take $v \in V_\lambda$, and compute

$$f(T)(v) = f(\lambda) \cdot v$$

so $f(T)$ is a scalar operator on V_λ. Thus, S is not of the form $f(T)$. ///

[08.12] Let $\lambda_1, \dots, \lambda_n$ be distinct elements of a field k. Let $\mu_1, \dots, \mu_n$ be arbitrary elements of k. Show that there is a unique polynomial $f(x)$ in $k[x]$ of degree $\leq n-1$ such that $f(\lambda_i) = \mu_i$ for all i.

Discussion: [This is Lagrange interpolation again.]

[08.13] Let T be a diagonalizable operator on a finite-dimensional vector space V over a field k. Suppose that all the eigenspaces are one-dimensional. Prove that any endomorphism commuting with T is in $k[T]$.

Discussion: We know that an endomorphism S commuting with T stabilizes the eigenspaces of T. Since each eigenspace V_λ is just one-dimensional, S acts by a scalar μ_λ on V_λ. Let $f(x)$ be the minimal polynomial of T, and $f_\lambda(x) = f(x)/(x-\lambda)$. These polynomials have *gcd* 1, so there are polynomials $a_\lambda(x)$ such that

$$1 = \sum_\lambda a_\lambda(x) \cdot f_\lambda(x)$$

As observed earlier,

$$\mathrm{id}_V = \sum_\lambda a_\lambda(T) \cdot f_\lambda(T)$$

and $f_\lambda(T)$ is 0 on V_μ for $\mu \neq \lambda$. Further, $P_\lambda = a_\lambda(T) f_\lambda(T)$ is in $k[T]$ and is the projector to V_λ. Then

$$S = \sum_\lambda \mu_\lambda \cdot P_\lambda \in k[T]$$

as claimed. ///

[08.14] Let S, T be commuting diagonalizable endomorphisms of a finite-dimensional vector space V over a field k. Suppose that there is a basis $\{v_1, \dots, v_n\}$ of simultaneous eigenvectors such that for $i \neq j$ the two vectors v_i and v_j either have different eigenvalues for S or have different eigenvalues for T. Show that there is a single diagonalizable operator R on V such that $k[S,T] = k[R]$.

Discussion: Let $P_\lambda \in k[S]$ be the projector to the λ-eigenspace of S, and $Q_\mu \in k[T]$ the projector to the μ-eigenspace of T. Since S and T commute, $P_\lambda Q_\mu = Q_\mu P_\lambda$ is a projector commuting with both S and T. We claim that $P_\lambda Q_\mu$ is the projector to the joint eigenspace where S is λ and T is μ. Certainly Q_μ maps the whole space to the μ eigenspace for T. Since P_λ commutes with T, it stabilizes this eigenspace, so $(P_\lambda Q_\mu)(V)$ is contained in the μ-eigenspace of T. Symmetrically, it is contained in the λ eigenspace for S, so is contained in the joint eigenspace. On the other hand, for a joint eigenvector v with $Sv = \lambda v$ and $Tv = \mu v$, we have

$$(P_\lambda Q_\mu)(v) = P_\lambda(Q_\mu v) = P_\lambda(v) = v$$

In the form the question is asked, let v_i have eigenvalue λ_i for S and μ_i for T. Then $E_i = P_{\lambda_i} Q_{\mu_i}$ is a family of mutually orthogonal projectors (meaning that $E_i E_j = 0$ unless $i = j$, in which case it is E_i), whose sum is the identity endomorphism on V.

Now **assume** that there are at least n distinct elements $\alpha_1, \ldots, \alpha_n$ in the field k, and let

$$R = \sum_i \alpha_i \cdot E_i \in k[S,T]$$

By arrangement R is diagonalizable and has one-dimensional eigenspaces. Since S and T commute with R, by an earlier example both S and T are in $k[R]$. Thus, $k[R] = k[S,T]$. ///

[08.15] Give an example of a diagonalizable operator T on a 2-dimensional complex vector space V (with hermitian inner product $\langle , \rangle$) with eigenvectors v, w such that application of the Gram-Schmidt process does *not* yield two orthonormal *eigenvectors*.

Discussion: Let $V = \mathbb{C}^2$ (column vectors) with the usual hermitian inner product, and let $T = \begin{pmatrix} 1 & 1 \\ 02 & \end{pmatrix}$. It has eigenvectors $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ (eigenvalue 1) and $v_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ (eigenvalue 2). These are not orthogonal to each other. If we apply Gram-Schmidt, instead of v_2 we have

$$v_2' = v_2 - \frac{\langle v_2, v_1 \rangle}{\langle v_1, v_1 \rangle} \cdot v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The latter vector is not an eigenvector. ///

[08.16] Let S be a hermitian operator on a finite-dimensional complex vector space V with hermitian inner product $\langle , \rangle$. Let W be a S-stable subspace of V. Show that S is hermitian on W.

Discussion: Let S_o be the restriction of S to W. If we show that for all $w, w' \in W$

$$\langle S_o w, w' \rangle = \langle w, S_o w' \rangle$$

then by the *uniqueness* of adjoints $S_o^* = S_o$. Indeed, because

$$\langle Sw, w' \rangle = \langle w, Sw' \rangle$$

for w, w' in the *whole* space V, the identity certainly holds for $w, w' \in W$. ///

[0.1] Remark: In a similar vein, one can directly show more generally that, for a *normal* endomorphism T on V stabilizing a subspace W, the restriction of T^* to W is the adjoint of the restriction of T to W.

[08.17] Let S, T be commuting hermitian operators on a finite-dimensional complex vector space V with hermitian inner product $\langle , \rangle$. Show that there is an orthonormal basis for V consisting of simultaneous eigenvectors for both S and T.

Discussion: First, the Spectral Theorem for S says that V is the *orthogonal* direct sum of the eigenspaces V_λ for S. We know that T stabilizes each such eigenspace. From the previous example, the restriction of T to each V_λ is still hermitian, so on each V_λ there is an orthonormal basis $\{e_i^\lambda\}$ consisting of eigenvectors for T (and λ-eigenvectors for S). Then, since the different eigenspaces V_λ are mutually orthogonal, the aggregate $\{e_i^\lambda\}$ is an orthonormal basis for all of V. ///

[08.18] Let k be a field, and V a finite-dimensional k vectorspace. Let Λ be a subset of the dual space V^*, with $|\Lambda| < \dim V$. Show that the **homogeneous system of equations**

$$\lambda(v) = 0 \ \ (\text{for all } \lambda \in \Lambda)$$

has a non-trivial (that is, non-zero) solution $v \in V$ (meeting all these conditions).

Discussion: The dimension of the span W of Λ is strictly less than $\dim V^*$, which we've proven is $\dim V^* = \dim V$. We may also identify $V \approx V^{**}$ via the natural isomorphism. With that identification, we may say that the set of solutions is $W^\perp$, and

$$\dim(W^\perp) + \dim W = \dim V^* = \dim V$$

Thus, $\dim W^\perp > 0$, so there are non-zero solutions. ///

[08.19] Let k be a field, and V a finite-dimensional k vectorspace. Let Λ be a *linearly independent* subset of the dual space V^*. Let $\lambda \to a_\lambda$ be a set map $\Lambda \to k$. Show that an **inhomogeneous system of equations**

$$\lambda(v) = a_\lambda \ \ (\text{for all } \lambda \in \Lambda)$$

has a solution $v \in V$ (meeting all these conditions).

Discussion: Let $m = |\Lambda|$, $\Lambda = \{\lambda_1, \dots, \lambda_m\}$. One way to use the linear independence of the functionals in Λ is to extend Λ to a basis $\lambda_1, \dots, \lambda_n$ for V^*, and let $e_1, \dots, e_n \in V^{**}$ be the corresponding dual basis for V^{**}. Then let $v_1, \dots, v_n$ be the images of the e_i in V under the natural isomorphism $V^{**} \approx V$. (This achieves the effect of making the λ_i be a dual basis to the v_i. We had only literally proven that one can go from a basis of a vector space to a dual basis of its dual, and not the reverse.) Then

$$v = \sum_{1 \le i \le m} a_{\lambda_i} \cdot v_i$$

is a solution to the indicated set of equations, since

$$\lambda_j(v) = \sum_{1 \le i \le m} a_{\lambda_i} \cdot \lambda_j(v_i) = a_{\lambda_j}$$

for all indices $j \le m$. ///

[08.20] Let T be a k-linear endomorphism of a finite-dimensional k-vectorspace V. For an eigenvalue λ of T, let V_λ be the generalized λ-eigenspace

$$V_\lambda = \{v \in V : (T - \lambda)^n v = 0 \text{ for some } 1 \le n \in \mathbb{Z}\}$$

Show that the projector P of V to V_λ (commuting with T) lies inside $k[T]$.

Discussion: First we do this assuming that the minimal polynomial of T factors into linear factors in $k[x]$.

Let $f(x)$ be the minimal polynomial of T, and let $f_\lambda(x) = f(x)/(x - \lambda)^e$ where $(x - \lambda)^e$ is the precise power of $(x - \lambda)$ dividing $f(x)$. Then the collection of all $f_\lambda(x)$'s has *gcd* 1, so there are $a_\lambda(x) \in k[x]$ such that

$$1 = \sum_\lambda a_\lambda(x)\, f_\lambda(x)$$

We claim that $E_\lambda = a_\lambda(T) f_\lambda(T)$ is a projector to the generalized λ-eigenspace V_λ. Indeed, for $v \in V_\lambda$,

$$v = 1_V \cdot v = \sum_\mu a_\mu(T) f_\mu(T) \cdot v = \sum_\mu a_\mu(T) f_\mu(T) \cdot v = a_\lambda(T) f_\lambda(T) \cdot v$$

since $(x - \lambda)^e$ divides $f_\mu(x)$ for $\mu \ne \lambda$, and $(T - \lambda)^e v = 0$. That is, it acts as the identity on V_λ. And

$$(T - \lambda)^e \circ E_\lambda = a_\lambda(T)\, f(T) = 0 \in \mathrm{End}_k(V)$$

so the image of E_λ is inside V_λ. Since E_λ is the identity on V_λ, it must be that the image of E_λ is *exactly* V_λ. For $\mu \neq \lambda$, since $f(x)|f_\mu(x)f_\lambda(x)$, $E_\mu E_\lambda = 0$, so these idempotents are *mutually orthogonal*. Then

$$(a_\lambda(T)f_\lambda(T))^2 = (a_\lambda(T)f_\lambda(T)) \cdot (1 - \sum_{\mu\neq\lambda} a_\mu(T)f_\mu(T)) = a_\lambda(T)f_\lambda(T) - 0$$

That is, $E_\lambda^2 = E_\lambda$, so E_λ is *a* projector to V_λ.

The mutual orthogonality of the idempotents will yield the fact that V is the direct sum of all the generalized eigenspaces of T. Indeed, for any $v \in V$,

$$v = 1 \cdot v = (\sum_\lambda E_\lambda)\, v = \sum_\lambda (E_\lambda v)$$

and $E_\lambda v \in V_\lambda$. Thus,

$$\sum_\lambda V_\lambda = V$$

To check that the sum is (unsurprisingly) direct, let $v_\lambda \in V_\lambda$, and suppose

$$\sum_\lambda v_\lambda = 0$$

Then $v_\lambda = E_\lambda v_\lambda$, for all λ. Then apply E_μ and invoke the orthogonality of the idempotents to obtain

$$v_\mu = 0$$

This proves the linear independence, and that the sum is direct.

To prove *uniqueness* of a projector E to V_λ commuting with T, note that any operator S commuting with T necessarily stabilizes all the generalized eigenspaces of T, since for $v \in V_\mu$

$$(T-\lambda)^e\, Sv = S\,(T-\lambda)^e v = S \cdot 0 = 0$$

Thus, E stabilizes all the V_μs. Since V is the direct sum of the V_μ and E maps V to V_λ, it must be that E is 0 on V_μ for $\mu \neq \lambda$. Thus,

$$E = 1 \cdot E_\lambda + \sum_{\mu\neq\lambda} 0 \cdot E_\mu = E_\lambda$$

That is, there is just one projector to V_λ that also commutes with T. *This finishes things under the assumption that $f(x)$ factors into linear factors in $k[x]$.*

The more general situation is similar. More generally, for a monic irreducible $P(x)$ in $k[x]$ dividing $f(x)$, with $P(x)^e$ the precise power of $P(x)$ dividing $f(x)$, let

$$f_P(x) = f(x)/P(x)^e$$

Then these f_P have *gcd* 1, so there are $a_P(x)$ in $k[x]$ such that

$$1 = \sum_P a_P(x) \cdot f_P(x)$$

Let $E_P = a_P(T)f_P(T)$. Since $f(x)$ divides $f_P(x) \cdot f_Q(x)$ for distinct irreducibles P, Q, we have $E_P \circ E_Q = 0$ for $P \neq Q$. And

$$E_P^2 = E_P(1 - \sum_{Q\neq P} E_Q) = E_P$$

so (as in the simpler version) the E_P's are mutually orthogonal idempotents. And, similarly, V is the direct sum of the subspaces

$$V_P = E_P \cdot V$$

We can also characterize V_P as the kernel of $P^e(T)$ on V, where $P^e(x)$ is the power of $P(x)$ dividing $f(x)$. If $P(x) = (x - \lambda)$, then V_P is the generalized λ-eigenspace, and E_P is the projector to it.

If E were another projector to V_λ commuting with T, then E stabilizes V_P for all irreducibles P dividing the minimal polynomial f of T, and E is 0 on V_Q for $Q \neq (x - \lambda)$, and E is 1 on V_λ. That is,

$$E = 1 \cdot E_{x-\lambda} + \sum_{Q \neq x-\lambda} 0 \cdot E_Q = E_P$$

This proves the uniqueness even in general. ///

[08.21] Let T be a matrix in Jordan normal form with entries in a field k. Let T_{ss} be the matrix obtained by converting all the off-diagonal 1's to 0's, making T diagonal. Show that T_{ss} is in $k[T]$.

Discussion: This implicitly demands that the minimal polynomial of T factors into linear factors in $k[x]$.

Continuing as in the previous example, let $E_\lambda \in k[T]$ be the projector to the generalized λ-eigenspace V_λ, and keep in mind that we have shown that V is the direct sum of the generalized eigenspaces, equivalent, that $\sum_\lambda E_\lambda = 1$. By definition, the operator T_{ss} is the scalar operator λ on V_λ. Then

$$T_{ss} = \sum_\lambda \lambda \cdot E_\lambda \in k[T]$$

since (from the previous example) each E_λ is in $k[T]$. ///

[08.22] Let $M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ be a matrix in a block decomposition, where A is m-by-m and D is n-by-n. Show that

$$\det M = \det A \cdot \det D$$

Discussion: One way to prove this is to use the formula for the determinant of an N-by-N matrix

$$\det C = \sum_{\pi \in S_N} \sigma(\pi)\, a_{\pi(1),1} \dots a_{\pi(N),N}$$

where c_{ij} is the $(i,j)^{th}$ entry of C, π is summed over the symmetric group S_N, and σ is the sign homomorphism. Applying this to the matrix M,

$$\det M = \sum_{\pi \in S_{m+n}} \sigma(\pi)\, M_{\pi(1),1} \dots M_{\pi(m+n),m+n}$$

where M_{ij} is the $(i,j)^{th}$ entry. Since the entries M_{ij} with $1 \leq j \leq m$ and $m < i \leq m+n$ are all 0, we should only sum over π with the property that

$$\pi(j) \leq m \quad \text{for} \quad 1 \leq j \leq m$$

That is, π stabilizes the subset $\{1, \dots, m\}$ of the indexing set. Since π is a bijection of the index set, necessarily such π stabilizes $\{m+1, m+2, \dots, m+n\}$, also. Conversely, each pair (π_1, π_2) of permutation π_1 of the first m indices and π_2 of the last n indices gives a permutation of the whole set of indices.

Let X be the set of the permutations $\pi \in S_{m+n}$ that stabilize $\{1, \dots, m\}$. For each $\pi \in X$, let π_1 be the restriction of π to $\{1, \dots, m\}$, and let π_2 be the restriction to $\{m+1, \dots, m+n\}$. And, in fact, if we plan

to index the entries of the block D in the usual way, we'd better be able to think of π_2 as a permutation of $\{1,\dots,n\}$, also. Note that $\sigma(\pi) = \sigma(\pi_1)\sigma(\pi_2)$. Then

$$\det M = \sum_{\pi\in X} \sigma(\pi)\, M_{\pi(1),1}\dots M_{\pi(m+n),m+n}$$

$$= \sum_{\pi\in X} \sigma(\pi)\,(M_{\pi(1),1}\dots M_{\pi(m),m})\cdot(M_{\pi(m+1),m+1}\dots M_{\pi(m+n),m+n})$$

$$= \left(\sum_{\pi_1\in S_m} \sigma(\pi_1)\, M_{\pi_1(1),1}\dots M_{\pi_1(m),m}\right)\cdot\left(\sum_{\pi_2\in S_n} \sigma(\pi_2)(M_{\pi_2(m+1),m+1}\dots M_{\pi_2(m+n),m+n}\right)$$

$$= \left(\sum_{\pi_1\in S_m} \sigma(\pi_1)\, A_{\pi_1(1),1}\dots A_{\pi_1(m),m}\right)\cdot\left(\sum_{\pi_2\in S_n} \sigma(\pi_2) D_{\pi_2(1),1}\dots D_{\pi_2(n),n}\right) = \det A\cdot\det D$$

where in the last part we have mapped $\{m+1,\dots,m+n\}$ bijectively by $\ell\to\ell-m$. ///

[08.23] The so-called *Kronecker product*[1] of an m-by-m matrix A and an n-by-n matrix B is

$$A\otimes B = \begin{pmatrix} A_{11}\cdot B & A_{12}\cdot B & \dots & A_{1m}\cdot B \\ A_{21}\cdot B & A_{22}\cdot B & \dots & A_{2m}\cdot B \\ & \vdots & & \\ A_{m1}\cdot B & A_{m2}\cdot B & \dots & A_{mm}\cdot B \end{pmatrix}$$

where, as it may appear, the matrix B is inserted as n-by-n blocks, multiplied by the respective entries A_{ij} of A. Prove that

$$\det(A\otimes B) = (\det A)^n\cdot(\det B)^m$$

at least for $m = n = 2$.

Discussion: If no entry of the first row of A is non-zero, then both sides of the desired equality are 0, and we're done. So suppose some entry A_{1i} of the first row of A is non-zero. If $i\neq 1$, then for $\ell = 1,\dots,n$ interchange the ℓ^{th} and $(i-1)n+\ell^{th}$ columns of $A\otimes B$, thus multiplying the determinant by $(-1)^n$. This is compatible with the formula, so we'll assume that $A_{11}\neq 0$ to do an induction on m.

We will manipulate n-by-n *blocks* of scalar multiples of B rather than actual scalars.

Thus, assuming that $A_{11}\neq 0$, we want to subtract multiples of the left column of n-by-n blocks from the blocks further to the right, to make the top n-by-n blocks all 0 (apart from the leftmost block, $A_{11}B$). In terms of manipulations of columns, for $\ell = 1,\dots,n$ and $j = 2,3,\dots,m$ subtract A_{1j}/A_{11} times the ℓ^{th} column of $A\otimes B$ from the $((j-1)n+\ell)^{th}$. Since for $1\le\ell\le n$ the ℓ^{th} column of $A\otimes B$ is A_{11} times the ℓ^{th} column of B, and the $((j-1)n+\ell)^{th}$ column of $A\otimes B$ is A_{1j} times the ℓ^{th} column of B, this has the desired effect of killing off the n-by-n blocks along the top of $A\otimes B$ except for the leftmost block. And the $(i,j)^{th}$ n-by-n block of $A\otimes B$ has become $(A_{ij}-A_{1j}A_{i1}/A_{11})\cdot B$. Let

$$A'_{ij} = A_{ij} - A_{1j}A_{i1}/A_{11}$$

and let D be the $(m-1)$-by-$(m-1)$ matrix with $(i,j)^{th}$ entry $D_{ij} = A'_{(i-1),(j-1)}$. Thus, the manipulation so far gives

$$\det(A\otimes B) = \det\begin{pmatrix} A_{11}B & 0 \\ * & D\otimes B\end{pmatrix}$$

[1] As we will see shortly, this is really a **tensor product**, and we will treat this question more sensibly.

By the previous example (or its tranpose)

$$\det \begin{pmatrix} A_{11}B & 0 \\ * & D \otimes B \end{pmatrix} = \det(A_{11}B) \cdot \det(D \otimes B) = A_{11}^n \det B \cdot \det(D \otimes B)$$

by the multilinearity of det.

And, at the same time subtracting A_{1j}/A_{11} times the first column of A from the j^{th} column of A for $2 \le j \le m$ does not change the determinant, and the new matrix is

$$\begin{pmatrix} A_{11} & 0 \\ * & D \end{pmatrix}$$

Also by the previous example,

$$\det A = \det \begin{pmatrix} A_{11} & 0 \\ * & D \end{pmatrix} = A_1 1 \cdot \det D$$

Thus, putting the two computations together,

$$\det(A \otimes B) = A_{11}^n \det B \cdot \det(D \otimes B) = A_{11}^n \det B \cdot (\det D)^n (\det B)^{m-1}$$

$$= (A_{11} \det D)^n \det B \cdot (\det B)^{m-1} = (\det A)^n (\det B)^m$$

as claimed. ///

Another approach to this is to observe that, in these terms, $A \otimes B$ is

$$\begin{pmatrix} A_{11} & 0 & \dots & 0 & & A_{1m} & 0 & \dots & 0 \\ 0 & A_{11} & & & & 0 & A_{1m} & & \\ \vdots & & \ddots & & \cdots & \vdots & & \ddots & \\ 0 & & & A_{11} & & 0 & & & A_{1m} \\ & & \vdots & & & & & \vdots & \\ A_{m1} & 0 & \dots & 0 & & A_{mm} & 0 & \dots & 0 \\ 0 & A_{m1} & & & & 0 & A_{mm} & & \\ \vdots & & \ddots & & \cdots & \vdots & & \ddots & \\ 0 & & & A_{m1} & & 0 & & & A_{mm} \end{pmatrix} \begin{pmatrix} B & 0 & \dots & 0 \\ 0 & B & & \\ \vdots & & \ddots & \\ 0 & & & B \end{pmatrix}$$

where there are m copies of B on the diagonal. By suitable permutations of rows and columns (with an interchange of rows for each interchange of columns, thus giving no net change of sign), the matrix containing the A_{ij}s becomes

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

with n copies of A on the diagonal. Thus,

$$\det(A \otimes B) = \det \begin{pmatrix} A & 0 & \dots & 0 \\ 0 & A & & \\ \vdots & & \ddots & \\ 0 & & & A \end{pmatrix} \cdot \det \begin{pmatrix} B & 0 & \dots & 0 \\ 0 & B & & \\ \vdots & & \ddots & \\ 0 & & & B \end{pmatrix} = (\det A)^n \cdot (\det B)^m$$

This might be more attractive than the first argument, depending on one's tastes. ///

[08.24] For distinct primes p, q, compute

$$\mathbb{Z}/p \otimes_{\mathbb{Z}/pq} \mathbb{Z}/q$$

where for a divisor d of an integer n the abelian group $\mathbb{Z}/d$ is given the $\mathbb{Z}/n$-module structure by

$$(r + n\mathbb{Z}) \cdot (x + d\mathbb{Z}) = rx + d\mathbb{Z}$$

Discussion: We claim that this tensor product is 0. To prove this, it suffices to prove that every $m \otimes n$ (the image of $m \times n$ in the tensor product) is 0, since we have shown that these *monomial* tensors always generate the tensor product.

Since p and q are relatively prime, there exist integers a, b such that $1 = ap + bq$. Then for all $m \in \mathbb{Z}/p$ and $n \in \mathbb{Z}/q$,

$$m \otimes n = 1 \cdot (m \otimes n) = (ap + bq)(m \otimes n) = a(pm \otimes n) + b(m \otimes qn) = a \cdot 0 + b \cdot 0 = 0$$

An auxiliary point is to recognize that, indeed, $\mathbb{Z}/p$ and $\mathbb{Z}/q$ really are $\mathbb{Z}/pq$-modules, and that the equation $1 = ap + bq$ still does make sense inside $\mathbb{Z}/pq$. ///

[08.25] Compute $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Q}$ with $0 < n \in \mathbb{Z}$.

Discussion: We claim that the tensor product is 0. It suffices to show that every $m \otimes n$ is 0, since these monomials generate the tensor product. For any $x \in \mathbb{Z}/n$ and $y \in \mathbb{Q}$,

$$x \otimes y = x \otimes (n \cdot \frac{y}{n}) = (nx) \otimes \frac{y}{n} = 0 \otimes \frac{y}{n} = 0$$

as claimed. ///

[08.26] Compute $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$ with $0 < n \in \mathbb{Z}$.

Discussion: We claim that the tensor product is 0. It suffices to show that every $m \otimes n$ is 0, since these monomials generate the tensor product. For any $x \in \mathbb{Z}/n$ and $y \in \mathbb{Q}/\mathbb{Z}$,

$$x \otimes y = x \otimes (n \cdot \frac{y}{n}) = (nx) \otimes \frac{y}{n} = 0 \otimes \frac{y}{n} = 0$$

as claimed. ///

[08.27] Compute $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Q}/\mathbb{Z})$ for $0 < n \in \mathbb{Z}$.

Discussion: Let $q : \mathbb{Z} \to \mathbb{Z}/n$ be the natural quotient map. Given $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Q}/\mathbb{Z})$, the composite $\varphi \circ q$ is a $\mathbb{Z}$-homomorphism from the free $\mathbb{Z}$-module $\mathbb{Z}$ (on one generator 1) to $\mathbb{Q}/\mathbb{Z}$. A homomorphism $\Phi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ is completely determined by the image of 1 (since $\Phi(\ell) = \Phi(\ell \cdot 1) = \ell \cdot \Phi(1)$), and since $\mathbb{Z}$ is *free* this image can be *anything* in the target $\mathbb{Q}/\mathbb{Z}$.

Such a homomorphism $\Phi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ factors through $\mathbb{Z}/n$ if and only if $\Phi(n) = 0$, that is, $n \cdot \Phi(1) = 0$. A complete list of representatives for equivalence classes in $\mathbb{Q}/\mathbb{Z}$ annihilated by n is $0, \frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n-1}{n}$. Thus, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Q}/\mathbb{Z})$ is in bijection with this set, by

$$\varphi_{i/n}(x + n\mathbb{Z}) = ix/n + \mathbb{Z}$$

In fact, we see that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Q}/\mathbb{Z})$ is an abelian group isomorphic to $\mathbb{Z}/n$, with

$$\varphi_{1/n}(x + n\mathbb{Z}) = x/n + \mathbb{Z}$$

as a generator. ///

[08.28] Compute $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$.

Discussion: We claim that this tensor product is isomorphic to $\mathbb{Q}$, via the $\mathbb{Z}$-linear map β induced from the $\mathbb{Z}$-bilinar map $B : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ given by

$$B : x \times y \to xy$$

First, observe that the monomials $x \otimes 1$ generate the tensor product. Indeed, given $a/b \in \mathbb{Q}$ (with a, b integers, $b \neq 0$) we have

$$x \otimes \frac{a}{b} = (\frac{x}{b} \cdot b) \otimes \frac{a}{b} = \frac{x}{b} \otimes (b \cdot \frac{a}{b}) = \frac{x}{b} \otimes a = \frac{x}{b} \otimes a \cdot 1 = (a \cdot \frac{x}{b}) \otimes 1 = \frac{ax}{b} \otimes 1$$

proving the claim. Further, any finite $\mathbb{Z}$-linear combination of such elements can be rewritten as a single one: letting $n_i \in \mathbb{Z}$ and $x_i \in \mathbb{Q}$, we have

$$\sum_i n_i \cdot (x_i \otimes 1) = (\sum_i n_i x_i) \otimes 1$$

This gives an outer bound for the size of the tensor product. Now we need an inner bound, to know that there is no *further* collapsing in the tensor product.

From the defining property of the tensor product there *exists* a (unique) $\mathbb{Z}$-linear map from the tensor product to $\mathbb{Q}$, through which B factors. We have $B(x, 1) = x$, so the induced $\mathbb{Z}$-linear map β is a bijection on $\{x \otimes 1 : x \in \mathbb{Q}\}$, so it is an isomorphism. ///

[08.29] Compute $(\mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Discussion: We claim that the tensor product is 0. It suffices to show that every $m \otimes n$ is 0, since these monomials generate the tensor product. Given $x \in \mathbb{Q}/\mathbb{Z}$, let $0 < n \in \mathbb{Z}$ such that $nx = 0$. For any $y \in \mathbb{Q}$,

$$x \otimes y = x \otimes (n \cdot \frac{y}{n}) = (nx) \otimes \frac{y}{n} = 0 \otimes \frac{y}{n} = 0$$

as claimed. ///

[08.30] Compute $(\mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$.

Discussion: We claim that the tensor product is 0. It suffices to show that every $m \otimes n$ is 0, since these monomials generate the tensor product. Given $x \in \mathbb{Q}/\mathbb{Z}$, let $0 < n \in \mathbb{Z}$ such that $nx = 0$. For any $y \in \mathbb{Q}/\mathbb{Z}$,

$$x \otimes y = x \otimes (n \cdot \frac{y}{n}) = (nx) \otimes \frac{y}{n} = 0 \otimes \frac{y}{n} = 0$$

as claimed. Note that we do *not* claim that $\mathbb{Q}/Z$ is a $\mathbb{Q}$-module (it is not!), but only that for given $y \in \mathbb{Q}/\mathbb{Z}$ there is another element $z \in \mathbb{Q}/\mathbb{Z}$ such that $nz = y$. That is, $\mathbb{Q}/Z$ is a **divisible** $\mathbb{Z}$-module. ///

[08.31] Prove that for a subring R of a commutative ring S, with $1_R = 1_S$, polynomial rings $R[x]$ behave well with respect to tensor products, namely that (as rings)

$$R[x] \otimes_R S \approx S[x]$$

Discussion: Given an R-algebra homomorphism $\varphi : R \to A$ and $a \in A$, let $\Phi : R[x] \to A$ be the unique R-algebra homomorphism $R[x] \to A$ which is φ on R and such that $\varphi(x) = a$. In particular, this works

for A an S-algebra and φ the restriction to R of an S-algebra homomorphism $\varphi : S \to A$. By the defining property of the tensor product, the bilinear map $B : R[x] \times S \to A$ given by

$$B(P(x) \times s) = s \cdot \Phi(P(x))$$

gives a unique R-module map $\beta : R[x] \otimes_R S \to A$. Thus, the tensor product has most of the properties necessary for it to be the free S-algebra on one generator $x \otimes 1$.

[0.2] Remark: However, we might be concerned about verification that each such β is an S-algebra map, rather than just an R-module map. We can certainly write an expression that appears to describe the multiplication, by

$$(P(x) \otimes s) \cdot (Q(x) \otimes t) = P(x)Q(x) \otimes st$$

for polynomials P, Q and $s, t \in S$. *If* it is *well-defined*, then it is visibly associative, distributive, etc., as required.

[0.3] Remark: The S-module structure itself is more straightforward: for any R-module M the tensor product $M \otimes_R S$ has a natural S-module structure given by

$$s \cdot (m \otimes t) = m \otimes st$$

for $s, t \in S$ and $m \in M$. But one could object that this structure is chosen at random. To argue that this is a *good* way to convert M into an S-module, we claim that for any other S-module N we have a natural isomorphism of abelian groups

$$\mathrm{Hom}_S(M \otimes_R S, N) \approx \mathrm{Hom}_R(M, N)$$

(where on the right-hand side we simply *forget* that N had more structure than that of R-module). The map is given by

$$\Phi \to \varphi_\Phi \quad \text{where} \quad \varphi_\Phi(m) = \Phi(m \otimes 1)$$

and has inverse

$$\Phi_\varphi \longleftarrow \varphi \quad \text{where} \quad \Phi_\varphi(m \otimes s) = s \cdot \varphi(m)$$

One might further carefully verify that these two maps are inverses.

[0.4] Remark: The definition of the tensor product does give an $\mathbb{R}$-linear map

$$\beta : R[x] \otimes_R S \to S[x]$$

associated to the R-bilinear $B : R[x] \times S \to S[x]$ by

$$B(P(x) \otimes s) = s \cdot P(x)$$

for $P(x) \in R[x]$ and $s \in S$. But it does not seem trivial to prove that this gives an isomorphism. Instead, it may be better to use the universal mapping property of a free algebra. In any case, there would still remain the issue of proving that the induced maps are S-algebra maps.

[08.32] Let K be a field extension of a field k. Let $f(x) \in k[x]$. Show that

$$k[x]/f \otimes_k K \approx K[x]/f$$

where the indicated quotients are by the ideals generated by f in $k[x]$ and $K[x]$, respectively.

Discussion: Upon reflection, one should realize that we want to prove isomorphism as $K[x]$-modules. Thus, we implicitly use the facts that $k[x]/f$ is a $k[x]$-module, that $k[x] \otimes_k K \approx K[x]$ as K-algebras, and that $M \otimes_k K$ gives a $k[x]$-module M a $K[x]$-module structure by

$$(\sum_i s_i x^i) \cdot (m \otimes 1) = \sum_i (x^i \cdot m) \otimes s_i$$

The map

$$k[x] \otimes_k K \approx_{\text{ring}} K[x] \to K[x]/f$$

has kernel (in $K[x]$) exactly of multiples $Q(x) \cdot f(x)$ of $f(x)$ by polynomials $Q(x) = \sum_i s_i x^i$ in $K[x]$. The inverse image of such a polynomial via the isomorphism is

$$\sum_i x^i f(x) \otimes s_i$$

Let I be the ideal generated in $k[x]$ by f, and $\tilde{I}$ the ideal generated by f in $K[x]$. The k-bilinear map

$$k[x]/f \times K \to K[x]/f$$

by

$$B : (P(x) + I) \times s \to s \cdot P(x) + \tilde{I}$$

gives *a* map $\beta : k[x]/f \otimes_k K \to K[x]/f$. The map β is *surjective*, since

$$\beta(\sum_i (x^i + I) \otimes s_i) = \sum_i s_i x^i + \tilde{I}$$

hits every polynomial $\sum_i s_i x^i$ mod $\tilde{I}$. On the other hand, if

$$\beta(\sum_i (x^i + I) \otimes s_i) \in \tilde{I}$$

then $\sum_i s_i x^i = F(x) \cdot f(x)$ for some $F(x) \in K[x]$. Let $F(x) = \sum_j t_j x^j$. With $f(x) = \sum_\ell c_\ell x^\ell$, we have

$$s_i = \sum_{j+\ell=i} t_j c_\ell$$

Then, using k-linearity,

$$\sum_i (x^i + I) \otimes s_i = \sum_i \left(x^i + I \otimes (\sum_{j+\ell=i} t_j c_\ell) \right) = \sum_{j,\ell} \left(x^{j+\ell} + I \otimes t_j c_\ell \right)$$

$$= \sum_{j,\ell} \left(c_\ell x^{j+\ell} + I \otimes t_j \right) = \sum_j (\sum_\ell c_\ell x^{j+\ell} + I) \otimes t_j = \sum_j (f(x) x^j + I) \otimes t_j = \sum_j 0 = 0$$

So the map is a bijection, so is an isomorphism. ///

[08.33] Let K be a field extension of a field k. Let V be a finite-dimensional k-vectorspace. Show that $V \otimes_k K$ is a good definition of the **extension of scalars** of V from k to K, in the sense that for any K-vectorspace W

$$\text{Hom}_K(V \otimes_k K, W) \approx \text{Hom}_k(V, W)$$

where in $\text{Hom}_k(V, W)$ we *forget* that W was a K-vectorspace, and only think of it as a k-vectorspace.

Discussion: This is a special case of a general phenomenon regarding *extension of scalars*. For any k-vectorspace V the tensor product $V \otimes_k K$ has a natural K-module structure given by

$$s \cdot (v \otimes t) = v \otimes st$$

for $s, t \in K$ and $v \in V$. To argue that this is a *good* way to convert k-vectorspaces V into K-vectorspaces, claim that for any other K-module W have a natural isomorphism of abelian groups

$$\mathrm{Hom}_K(V \otimes_k K, W) \approx \mathrm{Hom}_k(V, W)$$

On the right-hand side we *forget* that W had more structure than that of k-vectorspace. The map is

$$\Phi \to \varphi_\Phi \quad \text{where} \quad \varphi_\Phi(v) = \Phi(v \otimes 1)$$

and has inverse

$$\Phi_\varphi \longleftarrow \varphi \quad \text{where} \quad \Phi_\varphi(v \otimes s) = s \cdot \varphi(v)$$

To verify that these are mutual inverses, compute

$$\varphi_{\Phi_\varphi}(v) = \Phi_\varphi(v \otimes 1) = 1 \cdot \varphi(v) = \varphi(v)$$

and

$$\Phi_{\varphi_\Phi}(v \otimes 1) = 1 \cdot \varphi_\Phi(v) = \Phi(v \otimes 1)$$

which proves that the maps are inverses. ///

[0.5] Remark: In fact, the two spaces of homomorphisms in the isomorphism can be given natural structures of K-vectorspaces, and the isomorphism just constructed can be verified to respect this additional structure. The K-vectorspace structure on the left is clear, namely

$$(s \cdot \Phi)(m \otimes t) = \Phi(m \otimes st) = s \cdot \Phi(m \otimes t)$$

The structure on the right is

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

The latter has only the one presentation, since only W is a K-vectorspace.

[08.34] Let M and N be free R-modules, where R is a commutative ring with identity. Prove that $M \otimes_R N$ is free and

$$\mathrm{rank}\, M \otimes_R N = \mathrm{rank}\, M \cdot \mathrm{rank}\, N$$

Discussion: Let M and N be free on generators $i : X \to M$ and $j : Y \to N$. We claim that $M \otimes_R N$ is free on a set map

$$\ell : X \times Y \to M \otimes_R N$$

To verify this, let $\varphi : X \times Y \to Z$ be a set map. For each fixed $y \in Y$, the map $x \to \varphi(x, y)$ factors through a unique R-module map $B_y : M \to Z$. For each $m \in M$, the map $y \to B_y(m)$ gives rise to a unique R-linear map $n \to B(m, n)$ such that

$$B(m, j(y)) = B_y(m)$$

The linearity in the second argument assures that we still have the linearity in the first, since for $n = \sum_t r_t\, j(y_t)$ we have

$$B(m, n) = B(m, \sum_t r_t j(y_t)) = \sum_t r_t B_{y_t}(m)$$

which is a linear combination of linear functions. Thus, there is a unique map to Z induced on the tensor product, showing that the tensor product with set map $i \times j : X \times Y \to M \otimes_R N$ is free. ///

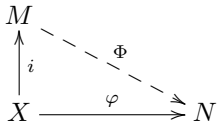
[08.35] Let M be a free R-module of rank r, where R is a commutative ring with identity. Let S be a commutative ring with identity containing R, such that $1_R = 1_S$. Prove that as an S module $M \otimes_R S$ is free of rank r.

Discussion: We prove a bit more. First, instead of simply an *inclusion* $R \subset S$, we can consider any ring homomorphism $\psi : R \to S$ such that $\psi(1_R) = 1_S$.

Also, we can consider arbitrary sets of generators, and give more details. Let M be free on generators $i : X \to M$, where X is a set. Let $\tau : M \times S \to M \otimes_R S$ be the canonical map. We claim that $M \otimes_R S$ is free on $j : X \to M \otimes_R S$ defined by

$$j(x) = \tau(i(x) \times 1_S)$$

Given an S-module N, we can be a little forgetful and consider N as an R-module via ψ, by $r \cdot n = \psi(r)n$. Then, given a set map $\varphi : X \to N$, since M is free, there is a unique R-module map $\Phi : M \to N$ such that $\varphi = \Phi \circ i$. That is, the diagram



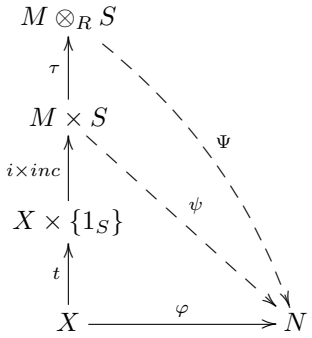
commutes. Then the map

$$\psi : M \times S \to N$$

by

$$\psi(m \times s) = s \cdot \Phi(m)$$

induces (by the defining property of $M \otimes_R S$) a unique $\Psi : M \otimes_R S \to N$ making a commutative diagram



where *inc* is the inclusion map $\{1_S\} \to S$, and where $t : X \to X \times \{1_S\}$ by $x \to x \times 1_S$. Thus, $M \otimes_R S$ is free on the composite $j : X \to M \otimes_R S$ defined to be the composite of the vertical maps in that last diagram. This argument does not depend upon finiteness of the generating set. ///

[08.36] For finite-dimensional vectorspaces V, W over a field k, prove that there is a natural isomorphism

$$(V \otimes_k W)^* \approx V^* \otimes W^*$$

where $X^* = \mathrm{Hom}_k(X, k)$ for a k-vectorspace X.

Discussion: For finite-dimensional V and W, since $V \otimes_k W$ is free on the cartesian product of the generators for V and W, the dimensions of the two sides match. We make an isomorphism from right to left. Create a bilinear map

$$V^* \times W^* \to (V \otimes_k W)^*$$

as follows. Given $\lambda \in V^*$ and $\mu \in W^*$, as usual make $\Lambda_{\lambda,\mu} \in (V \otimes_k W)^*$ from the bilinear map

$$B_{\lambda,\mu} : V \times W \to k$$

defined by

$$B_{\lambda,\mu}(v, w) = \lambda(v) \cdot \mu(w)$$

This induces a unique functional $\Lambda_{\lambda,\mu}$ on the tensor product. This induces a unique linear map

$$V^* \otimes W^* \to (V \otimes_k W)^*$$

as desired.

Since everything is finite-dimensional, bijectivity will follow from injectivity. Let $e_1, \ldots, e_m$ be a basis for V, $f_1, \ldots, f_n$ a basis for W, and $\lambda_1, \ldots, \lambda_m$ and $\mu_1, \ldots, \mu_n$ corresponding dual bases. We have shown that a basis of a tensor product of free modules is free on the cartesian product of the generators. Suppose that $\sum_{ij} c_{ij}\lambda_i \otimes \mu_j$ gives the 0 functional on $V \otimes W$, for some scalars c_{ij}. Then, for every pair of indices s, t, the function is 0 on $e_s \otimes f_t$. That is,

$$0 = \sum_{ij} c_{ij}\lambda_i(e_s)\,\lambda_j(f_t) = c_{st}$$

Thus, all constants c_{ij} are 0, proving that the map is injective. Then a dimension count proves the isomorphism. ///

[08.37] For a finite-dimensional k-vectorspace V, prove that the bilinear map

$$B : V \times V^* \to \mathrm{End}_k(V)$$

by

$$B(v \times \lambda)(x) = \lambda(x) \cdot v$$

gives an isomorphism $V \otimes_k V^* \to \mathrm{End}_k(V)$. Further, show that the composition of endormorphisms is the same as the map induced from the map on

$$(V \otimes V^*) \times (V \otimes V^*) \to V \otimes V^*$$

given by

$$(v \otimes \lambda) \times (w \otimes \mu) \to \lambda(w)v \otimes \mu$$

Discussion: The bilinear map $v \times \lambda \to T_{v,\lambda}$ given by

$$T_{v,\lambda}(w) = \lambda(w) \cdot v$$

induces a *unique* linear map $j : V \otimes V^* \to \mathrm{End}_k(V)$.

To prove that j is injective, we may use the fact that a basis of a tensor product of free modules is free on the cartesian product of the generators. Thus, let $e_1, \ldots, e_n$ be a basis for V, and $\lambda_1, \ldots, \lambda_n$ a dual basis for V^*. Suppose that

$$\sum_{i,j=1}^{n} c_{ij}\, e_i \otimes \lambda_j \to 0\mathrm{End}_k(V)$$

That is, for every e_ℓ,

$$\sum_{ij} c_{ij}\lambda_j(e_\ell)e_i = 0 \in V$$

This is

$$\sum_{i} c_{ij}e_i = 0 \quad \text{(for all } j\text{)}$$

Since the e_is are linearly independent, all the c_{ij}s are 0. Thus, the map j is injective. Then counting k-dimensions shows that this j is a k-linear isomorphism.

Composition of endomorphisms is a bilinear map

$$\mathrm{End}_k(V) \times \mathrm{End}_k(V) \xrightarrow{\circ} \mathrm{End}_k(V)$$

by

$$S \times T \to S \circ T$$

Denote by

$$c : (v \otimes \lambda) \times (w \otimes \mu) \to \lambda(w)v \otimes \mu$$

the allegedly corresonding map on the tensor products. The induced map on $(V \otimes V^*) \otimes (V \otimes V^*)$ is an example of a **contraction map** on tensors. We want to show that the diagram

$$\begin{array}{ccc} \mathrm{End}_k(V) \times \mathrm{End}_k(V) & \xrightarrow{\circ} & \mathrm{End}_k(V) \\ \uparrow{\scriptstyle j\times j} & & \uparrow{\scriptstyle j} \\ (V \otimes_k V^*) \times (V \otimes_k V^*) & \xrightarrow{c} & V \otimes_k V^* \end{array}$$

commutes. It suffices to check this starting with $(v \otimes \lambda) \times (w \otimes \mu)$ in the lower left corner. Let $x \in V$. Going up, then to the right, we obtain the endomorphism which maps x to

$$j(v \otimes \lambda) \circ j(w \otimes \mu)\ (x) = j(v \otimes \lambda)(j(w \otimes \mu)(x)) = j(v \otimes \lambda)(\mu(x)\, w)$$

$$= \mu(x)\, j(v \otimes \lambda)(w) = \mu(x)\, \lambda(w)\, v$$

Going the other way around, to the right then up, we obtain the endomorphism which maps x to

$$j(\, c((v \otimes \lambda) \times (w \otimes \mu)))\ (x) = j(\, \lambda(w)(v \otimes \mu)\,)\ (x) = \lambda(w)\, \mu(x)\, v$$

These two outcomes are the same. ///

[08.38] Under the isomorphism of the previous problem, show that the linear map

$$\mathrm{tr} : \mathrm{End}_k(V) \to k$$

is the linear map

$$V \otimes V^* \to k$$

induced by the bilinear map $v \times \lambda \to \lambda(v)$.

Discussion: Note that the induced map

$$V \otimes_k V^* \to k \quad \text{by} \quad v \otimes \lambda \to \lambda(v)$$

is another **contraction map** on tensors. Part of the issue is to compare the coordinate-bound trace with the induced (contraction) map $t(v \otimes \lambda) = \lambda(v)$ determined uniquely from the bilinear map $v \times \lambda \to \lambda(v)$. To this end, let $e_1, \ldots, e_n$ be a basis for V, with dual basis $\lambda_1, \ldots, \lambda_n$. The corresponding matrix coefficients $T_{ij} \in k$ of a k-linear endomorphism T of V are

$$T_{ij} = \lambda_i(Te_j)$$

(Always there is the worry about interchange of the indices.) Thus, in these coordinates,

$$\mathrm{tr}T = \sum_i \lambda_i(Te_i)$$

Let $T = j(e_s \otimes \lambda_t)$. Then, since $\lambda_t(e_i) = 0$ unless $i = t$,

$$\mathrm{tr}T = \sum_i \lambda_i(Te_i) = \sum_i \lambda_i(j(e_s \otimes \lambda_t)e_i) = \sum_i \lambda_i(\lambda_t(e_i) \cdot e_s) = \lambda_t(\lambda_t(e_t) \cdot e_s) = \begin{cases} 1 & (s = t) \\ 0 & (s \neq t) \end{cases}$$

On the other hand,

$$t(e_s \otimes \lambda_t) = \lambda_t(e_s) = \begin{cases} 1 & (s = t) \\ 0 & (s \neq t) \end{cases}$$

Thus, these two k-linear functionals agree on the monomials, which span, they are equal. ///

[08.39] Prove that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for two endomorphisms of a finite-dimensional vector space V over a field k, with trace defined as just above.

Discussion: Since the maps

$$\mathrm{End}_k(V) \times \mathrm{End}_k(V) \to k$$

by

$$A \times B \to \mathrm{tr}(AB) \quad \text{and/or} \quad A \times B \to \mathrm{tr}(BA)$$

are bilinear, it suffices to prove the equality on (images of) monomials $v \otimes \lambda$, since these span the endomophisms over k. Previous examples have converted the issue to one concerning $V \otimes_k^{} V^*$. (We have already shown that the isomorphism $V \otimes_k V^* \approx \mathrm{End}_k(V)$ is converts a *contraction* map on tensors to composition of endomorphisms, and that the trace on tensors defined as another contraction corresponds to the trace of matrices.) Let tr now denote the contraction-map trace on tensors, and (temporarily) write

$$(v \otimes \lambda) \circ (w \otimes \mu) = \lambda(w)\, v \otimes \mu$$

for the contraction-map composition of endomorphisms. Thus, we must show that

$$\mathrm{tr}\ (v \otimes \lambda) \circ (w \otimes \mu) = \mathrm{tr}\ (w \otimes \mu) \circ (v \otimes \lambda)$$

The left-hand side is

$$\mathrm{tr}\ (v \otimes \lambda) \circ (w \otimes \mu) = \mathrm{tr}(\, \lambda(w)\, v \otimes \mu) = \lambda(w)\, \mathrm{tr}(v \otimes \mu) = \lambda(w)\, \mu(v)$$

The right-hand side is

$$\mathrm{tr}\ (w \otimes \mu) \circ (v \otimes \lambda) = \mathrm{tr}(\, \mu(v)\, w \otimes \lambda) = \mu(v)\, \mathrm{tr}(w \otimes \lambda) = \mu(v)\, \lambda(w)$$

These elements of k are the same. ///

[08.40] Prove the *expansion by minors* formula for determinants, namely, for an n-by-n matrix A with entries a_{ij}, letting A^{ij} be the matrix obtained by deleting the i^{th} row and j^{th} column, for any fixed row index i,

$$\det A = (-1)^i \sum_{j=1}^{n} (-1)^j\, a_{ij}\ \det A^{ij}$$

and symmetrically for expansion along a column.

Discussion: [iou: prove that this formula is linear in each row/column, and invoke the uniqueness of determinants]

[08.41] Let M and N be free R-modules, where R is a commutative ring with identity. Prove that $M \otimes_R N$ is free and

$$\mathrm{rank}\, M \otimes_R N = \mathrm{rank}\, M \cdot \mathrm{rank}\, N$$

Discussion: Let M and N be free on generators $i : X \to M$ and $j : Y \to N$. We claim that $M \otimes_R N$ is free on a set map

$$\ell : X \times Y \to M \otimes_R N$$

To verify this, let $\varphi : X \times Y \to Z$ be a set map. For each fixed $y \in Y$, the map $x \to \varphi(x, y)$ factors through a unique R-module map $B_y : M \to Z$. For each $m \in M$, the map $y \to B_y(m)$ gives rise to a unique R-linear map $n \to B(m, n)$ such that

$$B(m, j(y)) = B_y(m)$$

The linearity in the second argument assures that we still have the linearity in the first, since for $n = \sum_t r_t\, j(y_t)$ we have

$$B(m, n) = B(m, \sum_t r_t j(y_t)) = \sum_t r_t B_{y_t}(m)$$

which is a linear combination of linear functions. Thus, there is a unique map to Z induced on the tensor product, showing that the tensor product with set map $i \times j : X \times Y \to M \otimes_R N$ is free. ///

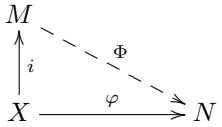
[08.42] Let M be a free R-module of rank r, where R is a commutative ring with identity. Let S be a commutative ring with identity containing R, such that $1_R = 1_S$. Prove that as an S module $M \otimes_R S$ is free of rank r.

Discussion: We prove a bit more. First, instead of simply an *inclusion* $R \subset S$, we can consider any ring homomorphism $\psi : R \to S$ such that $\psi(1_R) = 1_S$.

Also, we can consider arbitrary sets of generators, and give more details. Let M be free on generators $i : X \to M$, where X is a set. Let $\tau : M \times S \to M \otimes_R S$ be the canonical map. We claim that $M \otimes_R S$ is free on $j : X \to M \otimes_R S$ defined by

$$j(x) = \tau(i(x) \times 1_S)$$

Given an S-module N, we can be a little forgetful and consider N as an R-module via ψ, by $r \cdot n = \psi(r)n$. Then, given a set map $\varphi : X \to N$, since M is free, there is a unique R-module map $\Phi : M \to N$ such that $\varphi = \Phi \circ i$. That is, the diagram



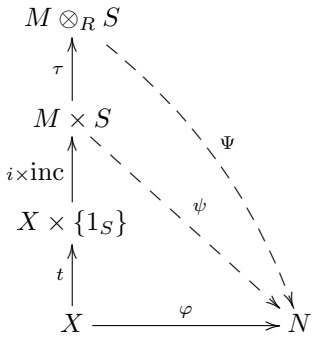
commutes. Then the map

$$\psi : M \times S \to N$$

by

$$\psi(m \times s) = s \cdot \Phi(m)$$

induces (by the defining property of $M \otimes_R S$) a unique $\Psi : M \otimes_R S \to N$ making a commutative diagram



where *inc* is the inclusion map $\{1_S\} \to S$, and where $t : X \to X \times \{1_S\}$ by $x \to x \times 1_S$. Thus, $M \otimes_R S$ is free on the composite $j : X \to M \otimes_R S$ defined to be the composite of the vertical maps in that last diagram. This argument does not depend upon finiteness of the generating set. ///

[08.43] For finite-dimensional vectorspaces V, W over a field k, prove that there is a natural isomorphism

$$(V \otimes_k W)^* \approx V^* \otimes W^*$$

where $X^* = \mathrm{Hom}_k(X, k)$ for a k-vectorspace X.

Discussion: For finite-dimensional V and W, since $V \otimes_k W$ is free on the cartesian product of the generators for V and W, the dimensions of the two sides match. We make an isomorphism from right to left. Create a bilinear map

$$V^* \times W^* \to (V \otimes_k W)^*$$

as follows. Given $\lambda \in V^*$ and $\mu \in W^*$, as usual make $\Lambda_{\lambda,\mu} \in (V \otimes_k W)^*$ from the bilinear map

$$B_{\lambda,\mu} : V \times W \to k$$

defined by

$$B_{\lambda,\mu}(v, w) = \lambda(v) \cdot \mu(w)$$

This induces a unique functional $\Lambda_{\lambda,\mu}$ on the tensor product. This induces a unique linear map

$$V^* \otimes W^* \to (V \otimes_k W)^*$$

as desired.

Since everything is finite-dimensional, bijectivity will follow from injectivity. Let $e_1, \ldots, e_m$ be a basis for V, $f_1, \ldots, f_n$ a basis for W, and $\lambda_1, \ldots, \lambda_m$ and $\mu_1, \ldots, \mu_n$ corresponding dual bases. We have shown that a basis of a tensor product of free modules is free on the cartesian product of the generators. Suppose that $\sum_{ij} c_{ij} \lambda_i \otimes \mu_j$ gives the 0 functional on $V \otimes W$, for some scalars c_{ij}. Then, for every pair of indices s, t, the function is 0 on $e_s \otimes f_t$. That is,

$$0 = \sum_{ij} c_{ij} \lambda_i(e_s)\, \lambda_j(f_t) = c_{st}$$

Thus, all constants c_{ij} are 0, proving that the map is injective. Then a dimension count proves the isomorphism. ///

[08.44] For a finite-dimensional k-vectorspace V, prove that the bilinear map

$$B : V \times V^* \to \mathrm{End}_k(V)$$

by

$$B(v \times \lambda)(x) = \lambda(x) \cdot v$$

gives an isomorphism $V \otimes_k V^* \to \mathrm{End}_k(V)$. Further, show that the composition of endormorphisms is the same as the map induced from the map on

$$(V \otimes V^*) \times (V \otimes V^*) \to V \otimes V^*$$

given by

$$(v \otimes \lambda) \times (w \otimes \mu) \to \lambda(w) v \otimes \mu$$

Discussion: The bilinear map $v \times \lambda \to T_{v,\lambda}$ given by

$$T_{v,\lambda}(w) = \lambda(w) \cdot v$$

induces a *unique* linear map $j : V \otimes V^* \to \mathrm{End}_k(V)$.

To prove that j is injective, we may use the fact that a basis of a tensor product of free modules is free on the cartesian product of the generators. Thus, let $e_1, \ldots, e_n$ be a basis for V, and $\lambda_1, \ldots, \lambda_n$ a dual basis for V^*. Suppose that

$$\sum_{i,j=1}^{n} c_{ij}\, e_i \otimes \lambda_j \to 0 \mathrm{End}_k(V)$$

That is, for every e_ℓ,

$$\sum_{ij} c_{ij} \lambda_j(e_\ell) e_i = 0 \in V$$

This is

$$\sum_{i} c_{ij} e_i = 0 \quad \text{(for all } j\text{)}$$

Since the e_is are linearly independent, all the c_{ij}s are 0. Thus, the map j is injective. Then counting k-dimensions shows that this j is a k-linear isomorphism.

Composition of endomorphisms is a bilinear map

$$\mathrm{End}_k(V) \times \mathrm{End}_k(V) \xrightarrow{\circ} \mathrm{End}_k(V)$$

by

$$S \times T \to S \circ T$$

Denote by

$$c : (v \otimes \lambda) \times (w \otimes \mu) \to \lambda(w) v \otimes \mu$$

the allegedly corresonding map on the tensor products. The induced map on $(V \otimes V^*) \otimes (V \otimes V^*)$ is an example of a **contraction map** on tensors. We want to show that the diagram

$$\begin{array}{ccc} \mathrm{End}_k(V) \times \mathrm{End}_k(V) & \xrightarrow{\circ} & \mathrm{End}_k(V) \\ {\scriptstyle j\times j}\uparrow & & \uparrow{\scriptstyle j} \\ (V \otimes_k V^*) \times (V \otimes_k V^*) & \xrightarrow{c} & V \otimes_k V^* \end{array}$$

commutes. It suffices to check this starting with $(v \otimes \lambda) \times (w \otimes \mu)$ in the lower left corner. Let $x \in V$. Going up, then to the right, we obtain the endomorphism which maps x to

$$j(v \otimes \lambda) \circ j(w \otimes \mu)\ (x) = j(v \otimes \lambda)(j(w \otimes \mu)(x)) = j(v \otimes \lambda)(\mu(x)\, w) = \mu(x)\, j(v \otimes \lambda)(w) = \mu(x)\, \lambda(w)\, v$$

Going the other way around, to the right then up, we obtain the endomorphism which maps x to

$$j(\, c((v \otimes \lambda) \times (w \otimes \mu)))\ (x) = j(\, \lambda(w)(v \otimes \mu)\,)\ (x) = \lambda(w)\, \mu(x)\, v$$

These two outcomes are the same. ///

[08.45] Via the isomorphism $\mathrm{End}_k(V) \approx V \otimes_k V^*$, show that the linear map

$$\mathrm{tr} : \mathrm{End}_k(V) \to k$$

is the linear map

$$V \otimes V^* \to k$$

induced by the bilinear map $v \times \lambda \to \lambda(v)$.

Discussion: Note that the induced map

$$V \otimes_k V^* \to k \quad \text{by} \quad v \otimes \lambda \to \lambda(v)$$

is another **contraction map** on tensors. Part of the issue is to compare the coordinate-bound trace with the induced (contraction) map $t(v \otimes \lambda) = \lambda(v)$ determined uniquely from the bilinear map $v \times \lambda \to \lambda(v)$. To this end, let $e_1, \ldots, e_n$ be a basis for V, with dual basis $\lambda_1, \ldots, \lambda_n$. The corresponding matrix coefficients $T_{ij} \in k$ of a k-linear endomorphism T of V are

$$T_{ij} = \lambda_i(Te_j)$$

(Always there is the worry about interchange of the indices.) Thus, in these coordinates,

$$\mathrm{tr}T = \sum_i \lambda_i(Te_i)$$

Let $T = j(e_s \otimes \lambda_t)$. Then, since $\lambda_t(e_i) = 0$ unless $i = t$,

$$\mathrm{tr}T = \sum_i \lambda_i(Te_i) = \sum_i \lambda_i(j(e_s \otimes \lambda_t)e_i) = \sum_i \lambda_i(\lambda_t(e_i) \cdot e_s) = \lambda_t(\lambda_t(e_t) \cdot e_s) = \begin{cases} 1 & (s = t) \\ 0 & (s \neq t) \end{cases}$$

On the other hand,

$$t(e_s \otimes \lambda_t) = \lambda_t(e_s) = \begin{cases} 1 & (s = t) \\ 0 & (s \neq t) \end{cases}$$

Thus, these two k-linear functionals agree on the monomials, which span, they are equal. ///

[08.46] Prove that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for two endomorphisms of a finite-dimensional vector space V over a field k, with trace defined as just above.

Discussion: Since the maps

$$\mathrm{End}_k(V) \times \mathrm{End}_k(V) \to k$$

by

$$A \times B \to \mathrm{tr}(AB) \quad \text{and/or} \quad A \times B \to \mathrm{tr}(BA)$$

are bilinear, it suffices to prove the equality on (images of) monomials $v \otimes \lambda$, since these span the endomophisms over k. Previous examples have converted the issue to one concerning $V_k^{\otimes} V^*$. (We have already shown that the isomorphism $V \otimes_k V^* \approx \mathrm{End}_k(V)$ is converts a *contraction* map on tensors to composition of endomorphisms, and that the trace on tensors defined as another contraction corresponds to the trace of matrices.) Let tr now denote the contraction-map trace on tensors, and (temporarily) write

$$(v \otimes \lambda) \circ (w \otimes \mu) = \lambda(w)\, v \otimes \mu$$

for the contraction-map composition of endomorphisms. Thus, we must show that

$$\mathrm{tr}\ (v \otimes \lambda) \circ (w \otimes \mu) = \mathrm{tr}\ (w \otimes \mu) \circ (v \otimes \lambda)$$

The left-hand side is

$$\mathrm{tr}\ (v \otimes \lambda) \circ (w \otimes \mu) = \mathrm{tr}(\, \lambda(w)\, v \otimes \mu) = \lambda(w)\, \mathrm{tr}(v \otimes \mu) = \lambda(w)\, \mu(v)$$

The right-hand side is

$$\mathrm{tr}\ (w \otimes \mu) \circ (v \otimes \lambda) = \mathrm{tr}(\, \mu(v)\, w \otimes \lambda) = \mu(v)\, \mathrm{tr}(w \otimes \lambda) = \mu(v)\, \lambda(w)$$

These elements of k are the same. ///

[08.47] Prove that tensor products are *associative*, in the sense that, for R-modules A, B, C, we have a *natural isomorphism*

$$A \otimes_R (B \otimes_R C) \approx (A \otimes_R B) \otimes_R C$$

In particular, *do* prove the *naturality*, at least the one-third part of it which asserts that, for every R-module homomorphism $f : A \to A'$, the diagram

$$\begin{array}{ccc} A \otimes_R (B \otimes_R C) & \xrightarrow{\approx} & (A \otimes_R B) \otimes_R C \\ \Big\downarrow{\scriptstyle f\otimes(1_B\otimes 1_C)} & & \Big\downarrow{\scriptstyle (f\otimes 1_B)\otimes 1_C} \\ A' \otimes_R (B \otimes_R C) & \xrightarrow{\approx} & (A' \otimes_R B) \otimes_R C \end{array}$$

commutes, where the two horizontal isomorphisms are those determined in the first part of the problem. (One might also consider maps $g : B \to B'$ and $h : C \to C'$, but these behave similarly, so there's no real compulsion to worry about them, apart from awareness of the issue.)

Discussion: Since all tensor products are over R, we drop the subscript, to lighten the notation. As usual, to make a (linear) map *from* a tensor product $M \otimes N$, we induce uniquely from a bilinear map on $M \times N$. We have done this enough times that we will suppress this part now.

The thing that is slightly less trivial is construction of maps *to* tensor products $M \otimes N$. These are always obtained by composition with the canonical bilinear map

$$M \times N \to M \otimes N$$

Important at present is that we can create n-fold tensor products, as well. Thus, we prove the indicated isomorphism by proving that both the indicated iterated tensor products are (naturally) isomorphic to the un-parenthesis'd tensor product $A \otimes B \otimes C$, with canonical map $\tau : A \times B \times C \to A \otimes B \otimes C$, such that for every trilinear map $\varphi : A \times B \times C \to X$ there is a unique linear $\Phi : A \otimes B \otimes C \to X$ such that

$$\begin{array}{ccc} A \otimes B \otimes C & & \\ \uparrow{\scriptstyle \tau} & \overset{\Phi}{\searrow} & \\ A \times B \times C & \xrightarrow[\varphi]{} & X \end{array}$$

The set map

$$A \times B \times C \approx (A \times B) \times C \to (A \otimes B) \otimes C$$

by

$$a \times b \times c \to (a \times b) \times c \to (a \otimes b) \otimes c$$

is linear in each single argument (for fixed values of the others). Thus, we are assured that there is a unique induced linear map

$$A \otimes B \otimes C \to (A \otimes B) \otimes C$$

such that

$$\begin{array}{ccc} A \otimes B \otimes C & & \\ \uparrow & \overset{i}{\searrow} & \\ A \times B \times C & \longrightarrow & (A \otimes B) \otimes C \end{array}$$

commutes.

Similarly, from the set map

$$(A \times B) \times C \approx A \times B \times C \to A \otimes B \otimes C$$

by

$$(a \times b) \times c \to a \times b \times c \to a \otimes b \otimes c$$

is linear in each single argument (for fixed values of the others). Thus, we are assured that there is a unique induced linear map

$$(A \otimes B) \otimes C \to A \otimes B \otimes C$$

such that

$$\begin{array}{ccc} (A \otimes B) \otimes C & & \\ \uparrow & \overset{j}{\searrow} & \\ (A \times B) \times C & \longrightarrow & A \otimes B \otimes C \end{array}$$

commutes.

Then $j \circ i$ is a map of $A \otimes B \otimes C$ to itself compatible with the canonical map $A \times B \times C \to A \otimes B \otimes C$. By uniqueness, $j \circ i$ is the identity on $A \otimes B \otimes C$. Similarly (just very slightly more complicatedly), $i \circ j$ must be the identity on the iterated tensor product. Thus, these two maps are mutual inverses.

To prove naturality in one of the arguments A, B, C, consider $f : C \to C'$. Let j_{ABC} be the isomorphism for a fixed triple A, B, C, as above. The diagram of maps of cartesian products (of sets, at least)

$$\begin{array}{ccc} (A \times B) \times C & \xrightarrow{j_{ABC}} & A \times B \times C \\ \downarrow{\scriptstyle (1_A \times 1_B) \times f} & & \downarrow{\scriptstyle 1_A \times 1_B \times f} \\ (A \times B) \times C & \xrightarrow{j} & A \times B \times C \end{array}$$

does commute: going down, then right, is

$$j_{ABC'}\left((1_A \times 1_B) \times f)((a \times b) \times c)\right) = j_{ABC'}\left((a \times b) \times f(c)\right) = a \times b \times f(c)$$

Going right, then down, gives

$$(1_A \times 1_B \times f)\left(j_{ABC}((a \times b) \times c)\right) = (1_A \times 1_B \times f)\left(a \times b \times c)\right) = a \times b \times f(c)$$

These are the same. ///

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

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

Show that the induced map

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

is no longer an injection.

Discussion: 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 $n \in \mathbb{Z}/2$. ///

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

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

is still surjective.

Discussion: 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. ///

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

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

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

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

Discussion: 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,

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

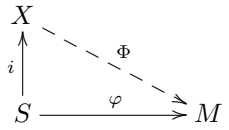
Thus, the map cannot possibly be surjective. ///

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

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



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

For naturality, for fixed S and M let the map $\varphi \to \Phi$ 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 $f : S \to S'$ be a set map. Let $i' : S' \to X'$ be a free module on S'. That is, $X' = FS'$. We must show that

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}}(FS, M) & \xleftarrow{j_{S,M}} & \mathrm{Hom}_{\mathrm{sets}}(S, GM) \\ {\scriptstyle -\circ Ff}\uparrow & & \uparrow{\scriptstyle -\circ f} \\ \mathrm{Hom}_{\mathbb{Z}}(FS', M) & \xleftarrow{j_{S',M}} & \mathrm{Hom}_{\mathrm{sets}}(S', GM) \end{array}$$

commutes, where $- \circ f$ is pre-composition by f, and $- \circ Ff$ is pre-composition by the induced map $Ff : FS \to FS'$ 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,

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

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

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

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

These are the same. ///

[08.52] 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

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

Discussion: 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. ///

[08.53] 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.

Discussion: 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. ///

[08.54] 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 $\tilde{M}$ with M as its top 3 rows, such that $\det \tilde{M} = 1$.

Discussion: 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 $e_1, \dots, e_5$ 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 $f_1, \dots, f_5$ 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 $i : E \to F$ be the inclusion. Consider $\bigwedge^3 : \bigwedge^3 E \to \bigwedge^3 F$. 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. ///

[08.55] 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.)

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

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

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 $i : S \to F$, 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. ///

[0.7] 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.

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

[08.56] 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

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

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 $r = s$.

Discussion: 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 natural isomorphism (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 $t : S \to F$ there is the natural (given $t : S \to F$, 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 $m \to i(\beta)(m)$ 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. ///

[0.9] 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

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

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. ///

[08.57] Let $\varphi : R \to S$ 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.)

Discussion: Let

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

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 $i(\varphi) : M \to \mathrm{Hom}_R(S, N)$ 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:

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

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

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

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

$$\begin{array}{ccc} \mathrm{Hom}_R(\mathrm{Res}^S_R M, N) & \xrightarrow{\quad i_{M,N} \quad} & \mathrm{Hom}_S(M, \mathrm{Hom}_R(S, N) \\ {\scriptstyle -\circ f}\uparrow & & \uparrow{\scriptstyle -\circ f} \\ \mathrm{Hom}_R(\mathrm{Res}^S_R M', N) & \xrightarrow{\quad i_{M',N} \quad} & \mathrm{Hom}_S(M', \mathrm{Hom}_R(S, N) \end{array}$$

commutes, where $-\circ f$ is pre-composition with f. (We use the same symbol for the map $f : M \to M'$ 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. ///

[08.58] 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 $\bigwedge^2(M/N)$?

Discussion: 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

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

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 $i : N \to M$ 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 $i : N \to M$ induces a natural map $\bigwedge^2 i : \bigwedge^2 \to \bigwedge^2 M$, 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

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

is in elementary divisor form. ///
