(*January 14, 2009*)

[21.1] 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.

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

[21.2] 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.

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. ///

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

[21.3] 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.

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. ///

[21.4] 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

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

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

Our definition of *free module* says that $FS = X$ is free on a (set) map $i : S \to X$ 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

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

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

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

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

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

The map in the direction $\varphi \to \Phi$ 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

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

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

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

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

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

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

These are the same. ///

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

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

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

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

Then, expanding by minors,

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

as desired. ///

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

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

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

Then the usual stunt gives

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

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

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

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

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

Since A has an inverse B,

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

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

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

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

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

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

[21.7] Let

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

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

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

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

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

Let $i : E \to F$ 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. ///

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

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

Or is it only

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

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

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

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

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

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

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. ///

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

[0.0.3] **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.*

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

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

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 $r = s$.

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

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

by

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

We also use the fact (from an example just above) that for F free on $t : S \to F$ 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. ///

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

Now let's prove (again?) that

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

by

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

is an isomorphism. The map in the other direction is

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

First,

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

Second,

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

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

[21.10] Write an explicit isomorphism

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

and verify that it is what is claimed.

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

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

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

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

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

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

by

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

To see that this is well-defined, first compute

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

Since

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

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

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

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

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

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

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

[21.11] 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.)

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:

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

which proves the S-linearity.

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

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

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

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

as hoped. (Again, the equality

$$\left(s \cdot \Phi(m)\right)(1_S) = \Phi(m)(s \cdot 1_S)$$

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

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

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. ///

[21.12] Let

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

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

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

First,

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

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

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

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

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

Then

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

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

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

(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. ///