Mathematics 505 Winter 2004

1. Find a commutative ring R, a short exact sequence of R-modules, and an R-module M, so that applying $M \otimes_R -$ to the short exact sequence yields a sequence which is not exact. Give reasons why the original sequence is exact and the new sequence isn't.

   Solution. Let $R = \mathbf{Z}$. Here is a short exact sequence of $\mathbf{Z}$-modules:

   $$0 \to \mathbf{Z} \xrightarrow{2} \mathbf{Z} \to \mathbf{Z}/2 \to 0.$$

   This is short exact because the left-hand map (multiplication by 2) is injective, and the right-hand term, $\mathbf{Z}/2$, is isomorphic to the quotient of the middle term by the image of the left term.

   Now let $M = \mathbf{Z}/2$, and tensor with M:

   $$0 \to \mathbf{Z}/2 \otimes_{\mathbf{Z}} \mathbf{Z} \xrightarrow{1\otimes 2} \mathbf{Z}/2 \otimes_{\mathbf{Z}} \mathbf{Z} \to \mathbf{Z}/2 \otimes_{\mathbf{Z}} \mathbf{Z}/2 \to 0.$$

   Over any ring R, $M \otimes_R R \cong M$, so we can compute the first two terms easily. Over the integers, $\mathbf{Z}/m \otimes_{\mathbf{Z}} \mathbf{Z}/n \cong \mathbf{Z}/(m,n)$, so we can compute the last term, also. So our sequence is:

   $$0 \to \mathbf{Z}/2 \xrightarrow{f} \mathbf{Z}/2 \to \mathbf{Z}/2 \to 0.$$

   This is not exact. There are at least two ways to see this: if it were exact, then the order of the middle group would be the product of the orders of the other two groups (because the right-hand group would be the quotient of the middle group by the left-hand group). Since $2 \neq 2 \cdot 2$, the sequence isn't exact.

   Alternatively, you can identify the map f:

   $$f : \mathbf{Z}/2 \otimes_{\mathbf{Z}} \mathbf{Z} \to \mathbf{Z}/2 \otimes_{\mathbf{Z}} \mathbf{Z}$$

   is defined by $f(a \otimes b) = a \otimes 2b$. Since we are tensoring over the integers, $a \otimes 2b = 2a \otimes b$. Since a is in $\mathbf{Z}/2$, $2a = 0$, and thus $2a \otimes b = 0$, and so $f(a \otimes b) = 0$ for all basic tensors $a \otimes b \in \mathbf{Z}/2 \otimes_{\mathbf{Z}} \mathbf{Z}$. Since the basic tensors generate any tensor product, the map f must be the zero map. In particular, it is not one-to-one, and so the sequence isn't exact.

2. State the two classification theorems for finitely generated modules over a principal ideal domain, including an explanation of what uniqueness means in each theorem.

Solution. Let R be a principal ideal domain, and let M be a finitely generated R-module.

- Then M is isomorphic to

$$R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$

for some integer $r \geq 0$ and some nonzero, non-unit elements $a_i \in R$, such that $a_1 | a_2 | \cdots | a_m$. This expression is unique, in the sense that if M is also isomorphic to

$$R^s \oplus R/(b_1) \oplus \cdots \oplus R/(b_n)$$

for some $s \geq 0$ and $b_j \in R$ satisfying the same conditions as the a_i, then $r = s$, $m = n$, and for each i, $(a_i) = (b_i)$. That is, a_i and b_i differ only by a unit multiple.

Note that without the requirement that each a_i be nonzero and a non-unit, you don't have uniqueness: $R \oplus R \cong R \oplus R/(0) \cong R \oplus R \oplus R/(1)$, so there are three ways of writing the same module.

- Also, M is isomorphic to

$$R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_k^{\alpha_k})$$

for some integer $r \geq 0$, prime elements $p_i \in R$, and integers $\alpha_i \geq 1$. This expression is unique, in the sense that if M is also isomorphic to

$$R^s \oplus R/(q_1^{\beta_1}) \oplus \cdots \oplus R/(q_\ell^{\beta_\ell})$$

for some integer $s \geq 0$, primes $q_j \in R$, and integers $\beta_j \geq 1$, then $r = s$, $k = \ell$, and one can reorder the q_j's so that for each i, $\alpha_i = \beta_i$ and p_i and q_i differ only by a unit multiple.

3. Let F be a field, let V be an F-vector space, and let $\mathbf{B}$ be a basis for V. Show that the set

$$\mathbf{B}^* = \{v^* : v \in \mathbf{B}\}$$

is linearly independent in V^*. Also show that if V is infinite-dimensional, then $\mathbf{B}^*$ does not span V^*.

(Recall that the element $v^* \in \mathbf{B}^*$ is defined by the following: for $w \in \mathbf{B}$,

$$v^*(w) = \begin{cases} 1 & \text{if } v = w, \\ 0 & \text{if } v \neq w.) \end{cases}$$

Solution. To show that $\mathbf{B}^*$ is linearly independent, I need to show that any finite subset of $\mathbf{B}^*$ is linearly independent. So let $v^* = c_1 v_1^* + \cdots + c_n v_n^* = 0$ for some $v_i \in \mathbf{B}$ and some scalars c_i. By the definition of these dual elements, $v^*(v_i) = c_i$, and since $v^* = 0$, I also know that $v^*(v_i) = 0$. Thus I can conclude that each coefficient c_i is zero, and so the set $\mathbf{B}^*$ is linearly independent.

Now assume that V is infinite-dimensional with basis $\mathbf{B}$. Define $\alpha \in V^*$ by

$$\alpha(v) = 1 \text{ for all } v \in \mathbf{B}.$$

(Note that α is not defined by $\alpha(v) = 1$ for all $v \in V$ – α is only 1 when evaluated on basis elements. Note also that I haven't defined α using some sort of infinite sum, because infinite sums are not defined in vector spaces.)

Then α is not in the span of $\mathbf{B}^*$: every element in $\mathbf{B}^*$ is nonzero on exactly one element of $\mathbf{B}$, by definition, and so (since linear combinations are always finite sums) any linear combination of elements from $\mathbf{B}^*$ will be nonzero on only finitely many elements of $\mathbf{B}$. Since $\mathbf{B}^*$ is infinite, α is nonzero on infinitely many such elements, and so is not a linear combination of elements of $\mathbf{B}^*$.

4. Let F be a field, $n \geq 1$ an integer, and A an $n \times n$ matrix with entries in F. Show that A is similar to its transpose. (You can use standard facts about the transpose, like $(BC)^t = C^t B^t$ and $(P^{-1})^t = (P^t)^{-1}$.)

   Solution. Using rational canonical form, one can show that A is similar to a matrix B over F if and only if A is similar to B over any extension field of F. So to show that A is similar to A^t, we may work in an extension K of F which contains all of the eigenvalues of A. Over such a field, A is similar to its Jordan form J: there is a matrix $P \in GL_n(K)$ such that $PAP^{-1} = J$. Take the transpose (and use the "standard facts" mentioned above):

   $$(P^t)^{-1} A^t P^t = J^t.$$

   That is, since A is similar to J, then A^t is similar to J^t. So it suffices to show that J is similar to J^t. To do that, it suffices to consider the case in which J consists of a single Jordan block. (If you don't believe this yet, it should become clear in the rest of the proof.) So assume that J is a Jordan block with eigenvalue λ, which means that J represents a linear transformation T so that with respect to some basis $\{v_1, \dots, v_n\}$, T acts as follows:

   $$T(v_i) = \begin{cases} \lambda v_1 & \text{if } i = 1, \\ \lambda v_i + v_{i-1} & \text{if } 2 \leq i \leq n. \end{cases}$$

   (Equivalently, as many of you noted, you can conjugate J by the matrix with 1's down the anti-diagonal, from top right to bottom left, and 0's elsewhere.) Then the matrix for T with respect to the basis $\{v_n, \dots, v_1\}$ is precisely J^t. So if I reverse the order of the basis, I get the transpose of the Jordan block. (Thus if J has more than one block, if I do this block-by-block, I will get the transpose of J.)

   Alternatively, if you don't want to worry about doing things block by block, you can conjugate the transpose of the Jordan form of A by the matrix with 1's down the anti-diagonal. The result will have be of Jordan form, with the same Jordan blocks as for A, but in reverse order. This is similar to the Jordan form for A (since shuffling the Jordan blocks around leads to similar matrices).

5. Let R be a principal ideal domain. A corollary of Baer's criterion is: an R-module M is injective if and only if $rM = M$ for every nonzero $r \in R$.

   (a) Use this to show that if M is injective, so is every quotient of M.

   (b) Show that if R is not a field, then there are no nonzero finitely generated injective R-modules. (Equivalently, show that if there is a nonzero finitely generated injective R-module, then R must be a field.)

Solution. (a) If M is injective, then $rM = M$ for every nonzero $r \in R$. If N is any submodule of M, then I claim that $r(M/N) = M/N$. Clearly $r(M/N) \subseteq M/N$. On the other hand, the elements of M/N are cosets $m + N$, and since $rM = M$, I can write the coset $m + N$ as $rm' + N$ for some $m' \in M$. Thus $r(M/N) \supseteq M/N$, and so by Baer's criterion, M/N is injective.

(b) Suppose M is a nonzero finitely generated R-module. It suffices to show that M has a quotient which is not injective. By the classification theorem,

$$M \cong R^n \oplus R/(a_1) \oplus \cdots \oplus R/(a_m),$$

where either $n > 0$ or $m > 0$ (and the a_i's are nonzero, non-units). In particular, M has as a quotient either R or $R/(a)$ for some nonzero, non-unit $a \in R$. If R is not a field, then there is some nonzero element $r \in R$ which does not have a multiplicative inverse. Then rR is a proper subset of R: the element 1 is contained in R, but is not in rR (if it were, then there would be an element $s \in R$ such that $rs = 1$, which would mean that r had an inverse). Thus R is not an injective R-module.

If R is not a quotient of M, then $R/(a)$ is for some nonzero, non-unit $a \in R$. Since a is not a unit, $R/(a)$ is not the zero module. On the other hand, $a(R/(a)) = 0$, so $a(R/(a)) \neq R/(a)$. Thus $R/(a)$ is not injective. By part (b), M cannot be injective.

(Equivalently, if you assume that M is finitely generated and injective, then using the last paragraph, you can deduce that M must be isomorphic to R^n for some n, and thus R is a quotient of M. Therefore $rR = R$ for every nonzero $r \in R$, and so the equation $1 = rs$ can always be solved – every nonzero $r \in R$ has a multiplicative inverse. Thus R is a field.)

6. (extra-credit) Prove the corollary of Baer's criterion mentioned in the previous problem.

   Solution. Recall that Baer's criterion says that if R is a ring, then a (left) R-module M is injective if and only if every for every left ideal I in R, every R-module homomorphism $f : I \to M$ can be extended to an R-module homomorphism $g : R \to M$.

   That is, if $\iota : I \to R$ is the inclusion map, given f, there exists a map g making this diagram commute:

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r, "\iota"] \arrow[d, "f"] & R \arrow[dl, dashed, "g"] \\ & M & \end{tikzcd}$$

   Suppose that $rM = M$ for all nonzero $r \in R$. To show that M is injective, given an ideal I in R, since R is a PID, then $I = (r)$ for some r. So any R-module map from I to M is determined by where r goes. Suppose $f : I \to M$ is defined by $f(r) = x$. Then $x = ry$ for some $y \in M$ (since $M = rM$), and the map $g : R \to M$ defined by $g(1) = y$ extends f.

   Now suppose that M is injective, and fix $x \in M$ and $r \in R$, with r nonzero. I want to find an element $y \in M$ such that $ry = x$. Define $h : R \to R$ by $h(s) = rs$. Since R is an integral domain, this map is injective; thus for any map $k : R \to M$, I can complete this diagram:

$$\begin{tikzcd} 0 \arrow[r] & R \arrow[r, "h"] \arrow[d, "k"] & R \arrow[dl, dashed, "\ell"] \\ & M & \end{tikzcd}$$

   In particular, define k by $k(1) = x$, and let $y = \ell(1)$. Then since $\ell \circ h = k$, I find that $k(1) = x$ equals $\ell(h(1)) = ry$.

   Equivalently, suppose that M is injective, and fix $x \in M$ and $r \in R$ with r nonzero. I want to find an element $y \in M$ such that $ry = x$. I would like to define a map $(r) \to M$ by $r \mapsto x$, but I don't know immediately if there is such an R-module map. (In general, there won't be – you can't map an arbitrary element r of a ring to an arbitrary element of some module; for example, if $R = \mathbf{Z}/6$ and $M = \mathbf{Z}/2$, then I can't map the element $2 \in R$ to $1 \in M$, because $3 \cdot 2 = 0$ in R, but $3 \cdot 1 \neq 0$ in M.) The key thing here is that since R is an integral domain, (r) is a *free* R-module of rank 1, generated by r. So in this case, you can send r to any element of M and get an R-module map.

   Once you have this map, extend it to a map $g : R \to M$ and let $y = g(1)$.