MATH 101A: HOMEWORK

7. Answers to Homework 7

Rings are allowed to be noncommutative.

7.1. If M is an R-module then show that:

(a) The set of R-module homomorphisms $f : M \to M$ is a ring under *reverse composition*:

$$fg = g \circ f$$

This ring is called $\mathrm{End}_R(M)^{op}$.

This is straightforward. One point: you are supposed to assume the previous homeworks. For example, $\mathrm{End}_R(M)$ is a ring under composition is a special case of homework problem 5.2. Thus, you only need to show that reversing the order of multiplication gives a new ring out of an old one.

(b) In the case of the free R-module $M = R^n$, show that there is an isomorphism of rings

$$\mathrm{End}_R(R^n)^{op} \cong M_n(R)$$

There are two methods. The first is an easy computational proof. Define a mapping

$$\psi : M_n(R) \to \mathrm{End}_R(R^n)^{op}$$

by letting $\psi(A)$ be right multiplication by the matrix A. The key point is that:

$$\psi(A)\psi(B)(x) = [\psi(B) \circ \psi(A)](x) = \psi(B)(xA) = xAB = \psi(AB)(x).$$

There is another more interesting method that several students formulated correctly assuming that R is commutative. It requires two steps if R is commutative and three if R is not commutative.

Lemma 7.1. *(by Dipramit)* $\exists \phi : \mathrm{End}_R(R^n) \cong M_n(\mathrm{End}_R(R))$.

Proof (This argument holds in any additive category!) Let $\pi_i : M \to R$ and $\mu_i : R \to M$ be the projection and inclusion maps for $M = R^n$.

Date: December 21, 2007.

Then $\sum \mu_i \pi_i = id_M$. For any $f \in \operatorname{End}_R(M)$ let $\phi(f)$ be the matrix with coefficients:

$$\phi(f) = (\pi_i \circ f \circ \mu_j).$$

Then

$$\phi(f \circ g) = (\pi_i \circ f \circ g \circ \mu_j) = (\sum_{k=1}^{n} \pi_i \circ f \circ \mu_k \circ \pi_k \circ g \circ \mu_j) = \phi(f)\phi(g)$$

Several students noticed that the formula is the transpose of the usual formula which assigns a matrix to a linear map.

Lemma 7.2. *Matrix transpose gives an isomorphism*

$$()^t : M_n(R)^{op} \cong M_n(R^{op})$$

Proof If $AB = C$ then $c_{ij} = \sum_k a_{ik} b_{kj}$. If we transpose all three matrices using the notation $C^t = (c^t_{ij}) = (c_{ji})$ we get:

$$(AB)^t = (\sum_k a_{jk} b_{ki}) = (\sum_k a^t_{kj} b^t_{jk}) = (\sum_k b^t_{jk} * a^t_{kj}) = B^t * A^t$$

where $*$ indicates reverse multiplication in R (multiplication in R^{op} and in $M_n(R^{op})$).

Finally we need:

Lemma 7.3. $\rho : \operatorname{End}_R(R) \cong R^{op}$.

Proof The isomorphism is given by $\rho(f) = f(1)$. Thus:

$$\rho(fg) = fg(1) = f(g(1)1) = g(1)f(1) = \rho(g)\rho(f) = \rho(f) * \rho(g).$$

Putting the three lemmas together we have:

$$\operatorname{End}_R(R^n) \cong M_n(\operatorname{End}_R(R)) \cong M_n(R^{op}) \cong M_n(R)^{op}.$$

7.2. Let $A \subseteq B \subseteq M$ be submodules. Suppose that A is pure in M and B/A is pure in M/A. Then is B pure in M?

Yes, B is pure in M. If $x \in M$ and $r \in R$ so that $rx \in B$ we need to find an element $b \in B$ so that $rb = rx$.

Since B/A is pure in M/A, there is an element $b + A \in B/A$ so that $r(b + A) = r(x + A)$. But, the definition of the action of R on the quotient space is: $r(b + A) := rb + A$ and $r(x + A) := rx + A$. So, $rx - rb = r(x - b) \in A$ Since A is pure in M, there is an $a \in A$ so that $ra = r(x - b)$. But then $rx = r(a + b)$ and $a + b \in B$. So, we are done.

7.3. Let R be a PID which is not a field. Let $Q(R)$ be the field of fractions of R considered as an R-modules. [Think of the example $R = \mathbb{Z}$, $Q(R) = \mathbb{Q}$.]

(a) Show that $Q(R)$ is torsion-free.

Everyone got this. $r(a/b) = 0 \Rightarrow ra = 0 \Rightarrow r = 0$.

(b) Show that $Q(R)$ is not isomorphic to a submodule of R^n for any n.

Everyone used the fact that all submodules of R^n are free on a finite number of generators. (Note: submodules of R^n are not closed under multiplication and are thus not subrings.) Most student showed that $Q(R)$ is not finitely generated as an R-module and thus cannot be isomorphic to a submodule of R^n. Others showed that $Q(R)$ cannot be generated by linearly independent elements.

Roger gave the best proof of the first kind: Take any nonzero element $r \in R$ which is not a unit. Let M_n be the R-submodule of $Q(R)$ generated the element $1/r^n$ then

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \cdots$$

violates the ACC. So, $Q(R)$ is not a Noetherian R-module and thus cannot be a submodule of any finitely generated R-module.

Samuel gave the best proof of the second kind. He points out first that any two element of $Q(R)$ are linearly dependent over R since

$$sy\left(\frac{x}{s}\right) - tx\left(\frac{y}{t}\right) = 0.$$

Therefore, if $Q(R)$ is free, it is free on one generator, say x/s. But R has a nonunit r and $x/sr \in Q(R)$ is not an element of $R(x/s)$.

7.4. Find an example of a module M which is not Noetherian but every proper submodule is cyclic.

Most students used the example $M = \mathbb{Z}[1/p]/\mathbb{Z}$. The example I had in mind is $\mathbb{Z}[1/p]$ but this is not correct since $q\mathbb{Z}[1/p] \subsetneq \mathbb{Z}[1/p]$ is infinitely generated.

Let M_n be the cyclic subgroup of M generated by $1/p^n + \mathbb{Z}$. Then

$$M_1 \subsetneq M_2 \subsetneq \cdots$$

violates the ACC. So, M is not Noetherian as a $\mathbb{Z}$-module. On the other hand, every proper subgroup $N \subsetneq M$ is equal to M_n for some n. To see this take the smallest integer n so that $1/p^n + \mathbb{Z} \notin N$. Then $1/p^{n-1} + \mathbb{Z} \in N$ so $M_{n-1} \subseteq N$. If $M_{n-1} \neq N$ then N has an element $a/p^k + \mathbb{Z}$ where $k \geq n$ and $(a, p) = 1$. Multiplying by p^{n-k} we may assume that $k = n$. Since $(a, p) = 1$, there exist integers x, y so that

$xa + yp = 1$. Then we have the following (modulo $\mathbb{Z}$):

$$x\frac{a}{p^n} = \frac{1 - yp}{p^n} = \frac{1}{p^n} - \frac{y}{p^{n-1}} \in N$$

Since $y/p^{n-1} + \mathbb{Z} \in N$ we conclude that $1/p^n + \mathbb{Z} \in N$ which is a contradiction.