MATH 611 **Due Wed Sept 23, 1992**

IMPORTANT NOTE. In this course, all rings and modules are unitary. Furthermore, if R and S are rings and $\rho\colon R \to S$, then for ρ to be a ring morphism [a.k.a. homomorphism] it is required that $\rho(1) = 1$. Furthermore if $R \subseteq S$ then for R to be considered a subring of S it is required that the identity element of R be the same as the identity element of S. **This is different from the usage in Hungerford.**

1. Let V be a vector space over a field K and φ, ψ endomorphisms on V. Let V_φ be the $K[X]$-module determined by the conditions that if $p(X) = c \in K$, then $p(X)v = cv$ (where the RHS denotes the vector space scalar multiplication), and $Xv = \varphi(v)$. Let V_ψ be analogously defined. Then φ and ψ are similar if and only if V_φ and V_ψ are isomorphic as $K[X]$-modules.

2. **a)** If M is an abelian group then the set of all homomorphisms $\varphi\colon M \to M$ (**endomorphisms** of M) is a ring in an obvious way. This **ring** is denoted by $\operatorname{End}_{\mathbb{Z}} M$.

b) An R-module is essentially the same as an abelian group M together with a ring morphism $R \to \operatorname{End}_{\mathbb{Z}} M$.

3. Let M be an R-module and $m \in M$. Define $\operatorname{ann} m = \{r \in R \mid rm = 0\}$ (the **annihilator** of m). (Note: In the commutative case, Hungerford uses the notation $\mathcal{O}_m$.)

a) $\operatorname{ann} m$ is a left ideal.

b) If Rm is the submodule of M generated by m then $Rm \approx R/\operatorname{ann} m$.

c) An R-module M is **cyclic** (i.e. generated by a singleton) if and only if $M \approx R/L$ for some left ideal L.

Definition. If R is an **integral domain** then an R-module M is **torsion free** if $\operatorname{ann} m = 0$ for every $m \neq 0 \in M$.

Definition. If N is a submodule of an R-module M, then N is **essential** in M if every non-zero element of M has a non-trivial multiple in N. I. e. $(\forall\, m \neq 0 \in M)\,(\exists\, r \in R)\ 0 \neq rm \in N$.

4. **a)** If M is a *torsion free* module over an integral domain R and S is a **subset** of M, then S is a maximal linearly independent subset of M if and only if S generates an essential submodule of M.

b) If M is a torsion free module over an integral domain M and there exists a **finite** subset S of M consisting of n elements which generates an essential submodule of M, then any subset of M containing *more than* n elements is linearly dependent. (Compare Hungerford, Theorem 2.7, p. 185.)

Definition. If M is an R-module then we define the **rank** of M in the following two cases:

(1) If R is commutative or more generally R has the invariant dimension property and if M is a **free** R-module, then $\operatorname{rank} M$ is the cardinality of a basis for M.

(2) If R is an integral domain and M is a **torsion free** R-module, then $\operatorname{rank} M$ is the cardinality of any maximal linearly independent subset of M.

There are certain other cases where it makes sense to define $\operatorname{rank} M$. However it is not possible to extend the concept of rank in complete generality to all modules over an arbitrary rang. Furthermore, the term "rank" is sometimes used both in group theory and module theory with other meanings than the one above.
In order for the second definition to make sense, we need to know that all maximal linearly independent subsets of M have the same cardinality. This is in fact true.
If R is an integral domain and M is a free R-module, then R is torsion free and so both definition (1) and (2) apply. It is not obvious that they agree in this case, but they do.

5. If M is a torsion free module over an integral domain M then $\operatorname{rank} M$ as given by (2) in the above definition is well defined.

September 23 Answers

1. NOTE: In this course, as in most of contemporary algebra, in order for a map $\varphi\colon A \to B$ to be called an isomorphism it must be both a monomorphism (one-to-one) and a surjection ("onto").

One first needs to prove that if V_φ is a $K[X]$-module and $\theta\colon V_\varphi \to V_\varphi$, then θ is a homomorphism of $K[X]$-modules if and only if θ is a K-linear transformation and $\theta(Xv) = X\theta(v)$. In fact, "$(\Rightarrow)$: " is obvious. On the other hand, if θ is K-linear and $\theta(Xv) = X\theta(V)$ and $p(X)$ is an arbitary element in $K[X]$ (i.e. a polynomial) then $\theta(p(X)v) = p(X)\theta(v)$ because *blah blah blah.*

Now if $\theta\colon V_\varphi \to V_\psi$ then the condition $\theta(Xv) = X\theta(v)$ translates to $\theta\varphi(v) = \psi\theta(v)$. This is true for **all** $v \in V$ if and only if $\theta\varphi = \psi\theta$. If, in addition θ^{-1} exists then we can multiply this equation *on the left* by θ^{-1} to see that it is equivalent to $\varphi = \theta^{-1}\psi\theta$.

Summarizing: There exists an invertible linear transformation θ (i.e. an isomorphism) from V into itself such that $\varphi = \theta^{-1}\psi\theta$ if and only if there exists $\theta\colon V_\varphi \to V_\psi$ which is $K[X]$-linear and an isomorphism.
But this says that φ is similar to ψ if and only if V_φ and V_ψ are isomorphic as $K[X]$-modules.

2. **a)** In order to prove that $\operatorname{End}_{\mathbb{Z}} M$ is a ring, there are all sorts of annoying little details to verify, most of which are pretty much obvious. The most important thing is to be aware of what these points are. The most important thing to **note** is that, by definition, if $\varphi, \psi \in \operatorname{End}_{\mathbb{Z}} M$ then

$$\varphi = \psi \iff (\forall m \in M)\, \varphi(m) = \psi(m).$$

Now for $\varphi, \psi \in \operatorname{End}_{\mathbb{Z}} M$, $\varphi + \psi$ and $\varphi\psi$ are defined by setting

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \qquad \text{and}$$
$$(\varphi\psi)(m) = \psi(\varphi(m)).$$

The items that need to be checked are: (1) $\varphi + \psi$ and $\varphi\psi$ are in fact homomorphisms. (2) The above addition is commutative and associative, i.e. $\varphi + \psi = \psi + \varphi$ and if also $\chi \in \operatorname{End}_{\mathbb{Z}} M$ then $\chi(\varphi\psi) = (\chi\varphi)\psi$. (Refer to the above note for the meaning of these equalities.) (3) Multiplication is associative (although probably not commutative). (4) The two distributive laws hold. (5) There exists a map commonly called the zero map which acts as the zero element in the ring $\operatorname{End}_{\mathbb{Z}} M$. (6) There exists a map commonly

called the identity map which acts as the multiplicative identity in this ring. I.e. if we denote the identity map by 1_M, then for all $\varphi \in \operatorname{End}_{\mathbb{Z}} M$, $1_M\varphi = \varphi 1_m = \varphi$.
b) Now if a homomorphism $\rho\colon R \to \operatorname{End}_{\mathbb{Z}} M$ is given then we can define a multiplication between R and M by setting rm equal to $(\rho(r))(m)$. (Please become comfortable with this kind of notation. What it means is that if $\rho(r) = \varphi \in \operatorname{End}_{\mathbb{Z}} M$ then rm is defined to be $\varphi(m)$, which makes sense because $m \in M$ and $\varphi\colon M \to M$.) One needs to check all the axioms to see that this does in fact make M into R-module. (This is tedious, but you can be fairly sketchy.)
On the other hand, if we start with a multiplication between R and M then we can define $\rho \in \operatorname{End}_{\mathbb{Z}} M$ as follows: if $r \in R$ then $\rho(r)\colon M \to M$ is defined by setting $(\rho(r))(m) = rm$. One needs to check to see that for each $r \in R$, $\rho(r)$ is in fact an endomorphism of the abelian group M, i.e. that $\rho(r)(m_1 + m_2) = \rho(r)(m_1) + \rho(r)(m_2)$. Furthermore, one needs to see that ρ is a homomorphism of rings between R and $\operatorname{End}_{\mathbb{Z}} M$, i.e. that $\rho(r_1 + r_2) = \rho(r_1) + \rho(r_2)$ and that $\rho(r_1 r_2) = \rho(r_1)\rho(r_2)$. This last equation means that for all $m \in M$, $\rho(r_1 r_2)(m) = \rho(r_1)[\,\rho(r_2)(m)]$.

3. **a)** The proof that $\operatorname{ann} m$ is a left ideal is completely routine. Note that if R is not commutative then $\operatorname{ann} m$ is usually not a right ideal.
b) Start by defining a map $\varphi\colon R \to Rm$ by simply setting $\varphi(r) = rm$. By the very definition of the cyclic module Rm this is surjective. Note also that the definition of $\operatorname{ann} m$ can be rephrased as stating that $r \in \operatorname{ann} m$ if and only if $\varphi(r) = 0$. Thus $\operatorname{Ker}\varphi = \operatorname{ann} m$. For convenience, write $L = \operatorname{ann} m$. Now, as is done in Hungerford, Theorem 1.7, p.172, one can define a map $\bar{\varphi}\colon R/L \to Rm$ by setting $\bar{\varphi}(r + L) = \varphi(r)$. If you don't use Theorem 1.7 you need to check that this is *well defined*, i.e. that if $r + L = r' + L$ then $\varphi(r) = \varphi(r')$. You also need to check that if it a *monomorphism*, i.e. that $\bar{\varphi}(r + L) = 0$ if and only if $r + L = 0 + L$. And finally you need to know that $\bar{\varphi}$ is an R-linear map. (Theorem 1.7 really saves a lot of work.) Since $\bar{\varphi}$ is surjective because φ is, it follows that $\bar{\varphi}$ is an isomorphism from $R/\operatorname{ann} m$ onto Rm.
b) This is almost just a rewording of part **b)**. We've already shown that every cyclic module is isomorphic to R/L for some left ideal L. (L is usually not unique, although it is if R is commutative. (This is not obvious, but not extremely hard.)) It remains to see that if a module is isomorphic to R/L for some left ideal L then it must be cyclic. It suffices to show that R/L is always cyclic for every L. But in fact one easily shows that R/L is generated as an R-module by the coset $1 + L$.

4. **Oops!** What part **a)** of this problem should have said is that if S is a **linearly independent** subset of M then S is a maximal linearly independent set if and only if it generates an essential submodule of M.

In fact, under the assumption that S is linearly independent it is easy to see that S is a maximal linearly independent set of M if and only if for each $m \notin S$ there is an equation of the form

$$rm = \sum r_i s_i$$

with the s_i distinct elements of S, and $r, r_i \in R$ with almost all $r_i = 0$ but $r \neq 0$. But this is exactly equivalent to saying that if $0 \neq m \in M$ then some non-zero multiple of m is in the submodule generated by S. (We need only worry about those m with $m \notin S$. Note that $r \neq 0$ and $m \neq 0$ implies $rm \neq 0$ since by assumption M is torsion free.) And that's the same as saying that the submodule generated by S is an essential submodule of M.

a) This is a complete steal from the proof of Theorem 2.7, p. 185. If S contains n elements and generates an essential submodule of M and T contains more than n elements, then one by one replaces elements of S by elements of T, at each step retaining the property that the submodule generated by the new set is an essential submodule of M. The only alteration is that since one can't divide we're not able to conclude that this submodule is actually all of M. Finally, one arrives at a subset T' of T containing n elements which generates an essential submodule of M. Then T' cannot be all of T (WHY?) so there exists $t \in T$ with $t \notin T'$. Then since T' generates an essential submodule of M, some non-zero multiple of t belongs to the submodule generated by T', i.e. $rt = \sum_1^n r_i t_i$ with $t_i \in T'$ and $r \neq 0$. Then $-rt + \sum r_i t_i = 0$ is a non-trivial relation among elements of T, so T is linearly dependent.

5. Well, this is partly another "oops!" I should have told you to only deal with the case of finite rank, since you don't know the set theory (or the algebra!) for the infinite rank case.

Okay, so assume that M contains a maximal linearly independent set S with n elements. Then if S' is any other maximal linearly independent set, S' cannot have more than n elements, otherwise by problem **4** it couldn't be linearly independent. (Note that this excludes the possibility that S' is infinite.) On the other hand, if S' had less than n elements then by problem **4** S couldn't be linearly independent, another contradiction. Thus we see that all maximal linearly independent subsets of M must have exactly n elements.