MATH 357

Yellow Group

February 2021

0.1

In part (a), we simply verify the module axioms for $O = \hom_R(M, N)$:

- It is clear from the definitions that O is an abelian group.
- *Distributive property in O.* $r(\varphi + \psi)(m) = r(\varphi(m) + \psi(m)) = r\varphi(m) + r\psi(m)$
- *Distributive property in R.* $((r + s)\varphi)(m) = (r + s)\varphi(m) = r\varphi(m) + s\varphi(m) = (r\varphi)(m) + (s\varphi)(m)$
- *Associativity.* $(r\phi)\psi(m) = r\phi\psi(m) = r(\phi\psi)(m)$

We conclude that O is an R-module. Part (b) is again an exercise in definitions. Put $E = \mathrm{end}_R(M)$

- E is an abelian group with additive identity $0(x) = 0$ and inverses $-\varphi(x) = \varphi(-x)$.
- Multiplication is associative: $(\varphi \circ \psi) \circ \theta = \varphi \circ (\psi \circ \theta)$ by normal function operations.
- Closure of multiplication holds since compositions of group homomorphisms are group homomorphisms. (MATH 356)
- The distributive property holds: $\varphi(x) \circ (\psi + \theta)(x) = \varphi \circ (\phi(x) + \theta(x)) = \varphi \circ \psi(x) + \varphi \circ \theta(x)$

So E is a ring.

0.2 Goodman 8.1.32, 8.1.10

First, we are asked to give a proof of Goodman proposition 8.1.32 (a $\iff$ b). Let M be an R-module, and let $B = \{x_1 ... x_n\}$ be a set of distinct nonzero elements of M. Define,

$$\varphi : (r_1, ... r_n) \mapsto r_1 x_1 + ... + r_n x_n$$

By the distributive property, it is clear that $\varphi : R^n \to M$ is a module homomorphism. Since B is a linearly independent list, for every $x \in M$, there is at most one linear combination

$$x = r_1 x_1 + ... + r_n x_n$$

this implies that φ is one to one. Similarly, since B is a generating set, every element x can be written as a linear combination of elements of B. This implies that φ is onto, and hence a bijection. We conclude that φ is an isomorphism.

The proof of the reverse direction is exactly the same.

Next, we show the equivalence of (a) and (c). Suppose again that B is a basis for M. Observe that $\varphi_i : r \mapsto x_i$ is one to one, since $r_1 x_i = r_2 x_i \Rightarrow r_1 x_i - r_2 x_i = (r_1 - r_2) x_i = 0$, so $r_1 = r_2$. Now, put $M' = R x_1 \oplus ... \oplus R x_n$. It is clear that $M' \subset M$, since every element in M' is a linear combination of elements of B. To see inclusion in the other direction, suppose $x \in M$. Since B is a basis for M, B generates M, so we can write

$$x = r_1 x_1 + ... + r_n x_n$$

for some $r_1, ... r_n \in R$. But clearly $r_i x_i \in R x_i$ for each $1 \leq i \leq n$, so

$$r_1 x_1 + ... + r_n x_n \in R x_1 \oplus ... \oplus R x_n = M'$$

So $M' \subset M$, and we are done.

Now we show the reverse direction. Suppose each φ_i is one to one, and that $M = M'$. Let $x \in M$ be given, then $x \in M' = R x_1 \oplus ... \oplus R x_n$, so we can write $x = r_1 x_1 + ... r_n x_n$ for $r_i \in R$. Since x was arbitrary, we have that B is a generating set. The hypothesis that each φ_i is one to one implies that B is linearly independent, and we are done.

0.3

The forwards direction is clear: if $\rho : C_m \to GL_n(\mathbb{C})$ is a group homomorphism, then $\rho(e) = \rho(g^m) = A^m = I$. For the reverse direction, suppose $A^m = I$. We simply need to verify that the map ρ is a group homomorphism, that is, it is operation-preserving. We have,

- *Identity.* We have that $\rho(e) = \rho(g^m) = A^m = I$.
- *Operation-preserving.* Let $g^i, g^j \in C_m$ be arbitrary, then we have $\rho(g^i \cdot g^j) = \rho(g^{i+j}) = A^{i+j} = A^i A^j = \rho(g^i)\rho(g^j)$, and we are done.

We connclude that ρ is a group homormorphism, and hence a representation.

0.4 Advanced problem A: Goodman 8.2.7 (Diamond isomorphism theorem)

Let $\varphi : M \to \overline{M}$ be an onto R-module homomorphism, and let $A \triangleleft M$ be a submodule. Put $N = \ker \varphi$. First, we are asked to show that $\varphi^{-1}\varphi(A) = A + N$. To see this, let $m \in \varphi^{-1}\varphi(A)$ be given. Then $\varphi(m) \in \varphi(A)$, so $\varphi(m) = \varphi(a)$ for some $a \in A$. Then

$$0 = \varphi(m) - \varphi(a) = \varphi(m - a)$$

so $n = m - a \in \ker \varphi = N$. But clearly, $m = a + n$, so $m \in A + N$. We conclude that $\varphi^{-1}\varphi(A) \subseteq A + N$. To show inclusion in the other direction, instead suppose that $m \in A + N$. Then $m = a + n$ for $a \in A, n \in N$. We have,

$$\varphi(m) = \varphi(a) + \varphi(n) = \varphi(a) \in \varphi(A)$$

so $m \in \varphi^{-1}\varphi(A)$. This implies that $A + N \subseteq \varphi^{-1}\varphi(A)$, and we are done.

Next, we are asked to show that $(A + N)/N \cong \varphi(A) \cong A/(A \cap N)$. For the sake of brevity we omit the more tedious details, but one can check that the maps

$$F : (A + N)/N \to \varphi(A) := (a + n)N \mapsto \varphi(a)$$

and

$$G : (A + N)/N \to A/(A \cap N) := (a + n)N \mapsto a(A \cap N)$$

are module isomorphisms.

0.5 Advanced problem B: Goodman 8.2.4 (Correspondence theorem)

Let $\varphi : M \to \overline{M}$ be an onto R-module homomorphism with kernel N, and define the map $F : A \mapsto \varphi^{-1}(A)$. We are asked to show that F is a bijection between R-submodules of $\overline{M}$ and R-submodules of M containing N. By a previous proposition, F is a bijection between subgroups of $\overline{M}$ and N-superset subgroups of M. Then we simply verify that F takes submodules to submodules. Let $A \lhd \overline{M}$ be a submodule, and let $a \in \varphi^{-1}(A), r \in R$ be given. Since A is a submodule of $\overline{M}$, it is an abelian subgroup – proposition 2.7.13 then guarantees that $\varphi^{-1}(A)$ is an abelian subgroup of M. Next, we have

$$\varphi(ra) = r\varphi(a) \in rA \in A$$

so $ra \in \varphi^{-1}(A)$, hence $\varphi^{-1}(A)$ is closed under left multiplication by elements in R. We conclude that $\varphi^{-1}(A)$ is a submodule, as desired.

0.6 Advanced problem C: Goodman 8.1.7

Let V be an $1 < n$-dimensional vector space over K, and let $R = \text{end}_K(V)$ be the ring of linear maps $V \mapsto V$. Let $S = \{v_1, ...v_n\} \subset V$ be a generating set for (V, R); we will show that S is not linearly independent. Since $\dim(V) > 1$ and since S generates V, S contains at least two distinct, nonzero elements v_1, v_2. Let $T \in R$ be any linear map that sends $v_1 \mapsto -v_2$. (It is a basic fact from linear algebra that such a map exists) Then if $1 \in R$ is the identity map, we have

$$Tv_1 + 1v_2 = -v_2 + v_2 = 0$$

but since $T, 1 \neq 0$, we have that v_1, v_2 are not linearly independent. We conclude that (V, R) is not free.

0.7 Advanced problem D

(a) Let $\rho : G \to V$ be a degree-1 representation of G. Since ρ is of degree 1, V is 1-dimensional. This implies that linear maps

$V \mapsto V$ are simply scalars in the underlying field F (rather, 1x1 matrices with entries in F) which of course commute. The rest is straightforward: using the commutative property of F, for every $g_1, g_2 \in G$,

$$\rho(-g_1 - g_2 + g_1 + g_2) = \rho(g_1)^{-1}\rho(g_2)^{-1}\rho(g_1)\rho(g_2) = I$$

so the commutator $[g_1, g_2] \in K = \ker \rho$. Since K is the kernel of a group homomorphism, it is a normal subgroup, and since K contains all commutators by the above argument, we have that G/K is abelian.

(b) The trivial representation $\rho : g \mapsto I$ is a simple counterexample, eg, if G is the nonabelian symmetric group S_3, then

$$\rho(1,2)\rho(2,3) = I \cdot I = \rho(2,3)\rho(1,2)$$

and

$$(1,2)(2,3) = (123) \neq (2,3)(1,2)$$

As a side remark, I'm having a really tough time coming up with nondegenerate counterexamples! In particular, I have been experimenting with representations of nonabelian groups that are not one to one, with little success...