MAT 511 **Exam 2** Name SOLUTIONS

10/25/13 (due Tuesday 10/29/13 at 6:00 pm)

150 points

Rules: You may consult your notes, our text and/or other books, and may discuss the exam with me, but no other outside help (including internet) is permitted. If you have questions, they should be directed to me. No discussion of the exam with other students, even at a superficial level, is permitted. I will hold additional office hours on Monday, 10/28, from 10:00 - 11:00 am and 4:00 - 5:00 pm, and on Tuesday, 10/29, 11:30 am - 12:30 pm, and will respond to email inquiries over the weekend. Hints are available upon request, at no charge.

1.(15) Let G be a finite group and $N \trianglelefteq G$. Let $x \in N$. Suppose $\mathbf{C}_G(x) \subseteq N$. Show that the conjugacy class of x in G is the union of $|G : N|$ conjugacy classes in N. More generally, express the ratio $|cl_G(x)|/|cl_N(x)|$ in terms of $|G : N|$ and $|\mathbf{C}_G(x) : \mathbf{C}_G(x) \cap N|$.

First of all, $|cl_G(x)| = |G : C_G(x)| = |G:N|\,|N : C_G(x)|$ since $C_G(x) \subseteq N$

$= |G:N|\,|N : C_N(x)|$ since $C_N(x) = C_G(x) \cap N = C_N(x)$

$= |G:N|\,|cl_N(x)|$.

Second, if $y \in cl_G(x)$, then $cl_N(y) \subseteq cl_G(y) = cl_G(x)$.

Claim $C_G(y)$ is conjugate to $C_G(x)$ in G. Indeed, since $y \in cl_G(x)$, $y = gxg^{-1}$ for some $g \in G$. Then $g\,C_G(x)\,g^{-1} = C_G(y)$. → go to p. 7

2.(25) Find $\mathbf{C}_{S_n}(\sigma)$ and $\mathbf{C}_{A_n}(\sigma)$ in each case (a)-(c) below. The groups are abelian in cases (a) and (c) - identify them as products of cyclic groups. (For part (b), if you wish, you may show the centralizer is isomorphic to a product of a cyclic group and a dihedral group.)

(a) $\sigma = (12345)(678)$, $n = 8$.

$|cl_{S_8}(6)| = \frac{5!}{5} \cdot \frac{3!}{3}$ so $|C_{S_8}(6)| = \frac{|S_8|}{|cl_{S_8}(6)|} = \frac{8!}{8!/15} = 15$

Since $|6| = 5 \cdot 3 = 15$ and $\langle 6 \rangle \subseteq C_{S_8}(6)$, $\langle 6 \rangle = C_{S_8}(6)$

Since $6 \in A_8$, $\langle 6 \rangle \leq A_8$, hence $C_{A_8}(6) = C_{S_8}(6) = \langle 6 \rangle \cong Z_{15}$

(b) $\sigma = (123)(567)$, $n = 7$.

$|cl_{S_7}(6)| = \frac{7 \cdot 6 \cdot 5}{3} \cdot \frac{4 \cdot 3 \cdot 2}{3} \cdot \frac{1}{2}$ ← since the factors could be switched, e.g. $(123)(567) = (567)(123)$

so $|C_{S_7}(6)| = \frac{|S_7|}{|cl_{S_7}(6)|} = \frac{7!}{7!/18} = 18$. Since (123) and (567) commute, $C_{S_7}(6)$ contains $\langle (123) \rangle \langle (567) \rangle$, which has order 9, as well as $\langle (15)(26)(37) \rangle$, which has order 2, and intersects $\langle (123) \rangle \langle (567) \rangle$ trivially. Then $C_{S_7}(6) = \langle (123), (567), (15)(26)(37) \rangle$.

Let $x = (123)$, $y = (567)$, $z = (15)(26)(37)$.

Then $|xy| = 3$, and xy commutes with x and z. Moreover, $|x| = 3$, $|z| = 2$, and $x^z = x^{-1}$. Then $\langle x, z \rangle \cong D_3$ (equivalently, $\langle x, z \rangle \cong S_3$) and $C_{S_7}(6) \cong \langle xy \rangle \times \langle x, z \rangle \cong Z_3 \times S_3$.

Then $C_{A_7}(6) = C_{S_7}(6) \cap A_7 = \langle (123), (567) \rangle \cong Z_3 \times Z_3$

(c) $\sigma = (123)$, $n = 5$.

$|cl_{S_5}(6)| = \frac{5 \cdot 4 \cdot 3}{3}$ and

$|C_{S_5}(6)| = \frac{|S_5|}{|cl_{S_5}(6)|} = \frac{5!}{\frac{5 \cdot 4 \cdot 3}{3}}$

$= 6$. Since $(123), (45) \in C_{S_5}(6)$, $C_{S_5}(6) = \langle (123), (45) \rangle \cong Z_3 \times Z_2 \cong Z_6$. $C_{A_5}(6) = \langle (123) \rangle \cong Z_3$

(d) Suppose $\sigma \in A_n$ has a cycle of even length, or has two cycles of the same length. Show $cl_{S_n}(\sigma) = cl_{A_n}(\sigma)$.

Suppose $\sigma = \sigma_1 \cdots \sigma_k$ is a factorization into disjoint cycles, and one, say σ_1 has even length. Since σ_1 commutes with itself and disjoint cycles commute, $\sigma_1 \in C_{S_n}(\sigma)$, and since σ_1 has even length, σ_1 is odd. Then $C_{A_n}(\sigma) = C_{S_n}(\sigma) \cap A_n \neq C_{S_n}(\sigma)$. $|C_{S_n}(\sigma) : C_{A_n}(\sigma)| = 2$, so $|cl_{S_n}(\sigma)| = \frac{|S_n|}{|C_{S_n}(\sigma)|} = \frac{2!|A_n|}{2|C_{A_n}(\sigma)|} = |cl_{A_n}(\sigma)|$.

3.(20) Let $n \geq 5$. (a) Suppose N is a proper normal subgroup of S_n. Prove $N = A_n$.

Let $1 \neq N \trianglelefteq S_n$. Then $N \cap A_n \trianglelefteq A_n$, and since $n \geq 5$, A_n is simple, so either $N \cap A_n = A_n$ or $N \cap A_n = 1$. If $N \cap A_n = A_n$, then $A_n \leq N \lneq S_n$, which implies $N = A_n$ since $|S_n : A_n| = 2$. Suppose $N \cap A_n = 1$. Let $x, y \in N$ with $x \neq 1$, $y \neq 1$. Then x and y are both odd, so xy is even. Then $xy \in N \cap A_n$, so $xy = 1_{S_n}$. Setting $x = y$ we have that x has order 2. Then for any y, $xy = 1_{S_n} \Rightarrow y = x^{-1} = x$. Thus $N = \{1, x\}$. Since N is normal, this implies $x^\sigma = x$ for all $\sigma \in S_n$. But $x \neq 1$, so there are at least two distinct elements with the same cycle-type as x, so $x^\sigma \neq x$ for some $\sigma \in S_n$. Contradiction. Thus $N = A_n$.

If σ has two cycles of the same length, and they have even length, then we have just shown $cl_{S_n}(\sigma) = cl_{A_n}(\sigma)$. Suppose σ_1 and σ_2 have odd length, say $\sigma_1 = (a_1, \ldots, a_k)$, $\sigma_2 = (b_1, \ldots, b_k)$. Then $\tau = (a_1 b_1)(a_2 b_2) \cdots (a_k b_k)$ is odd and lies in $C_{S_n}(\sigma)$. Then by the same string of equalities as above, $cl_{S_n}(\sigma) = cl_{A_n}(\sigma)$.

(b) Suppose H is a subgroup of S_n satisfying $1 < |S_n : H| < n$. Prove that $H = A_n$. (Hint: Use part (a).) Conclude that any group of order 60 that acts faithfully on a set Ω with $|\Omega| = 5$ is isomorphic to A_5.[1]

Let S_n act on S_n/H by left multiplication. The kernel of this action is a normal subgroup $K \trianglelefteq S_n$ with $K \leq H$ and $|S_n : K|$ dividing $k!$, where $k = |S_n : H|$. Since $H \lneq S_n$, $K \neq S_n$. Since $|S_n| = n!$ does not divide $k!$ (since $k < n$), $K \neq 1_{S_n}$. Then $K = A_n$ by part (a). Then $A_n \leq H \lneq S_n$, so $A_n = H$ since $|S_n : A_n| = 2$. $\square$

[1] The last statement applies to the group of rotational symmetries of the icosahedron, as shown in class.

(b) A left R-module M is *simple* if it has no proper submodules (i.e., the only R-submodules of M are 0_M and M). Assume R is a ring with 1. Prove: A unital left R-module M is simple if and only if M is isomorphic to R/I as a left R-module, for some maximal left ideal I of R.

Let $x \in M$ with $x \neq 0$. Then the submodule generated by x is $Rx = \{rx \mid r \in R\}$, which is not equal to zero since $x = 1_R x \in Rx$, and $x \neq 0$. Since M is simple, $Rx = M$ (i.e., M is cyclic). Let $\varphi : R \longrightarrow M$ be defined by $\varphi(r) = rx$. Then $\text{im}(\varphi) = Rx = M$, so φ is surjective. Let $I = \ker \varphi$. Since φ is a left R-module homomorphism, I is a left R-submodule of R, that is, I is a left ideal of R. By the 1st isomorphism theorem for modules, φ induces an isomorphism $\overline{\varphi} : R/I \longrightarrow M$.

(c) Prove: if M is a simple left R-module and $\varphi : M \longrightarrow M$ is a nonzero R-module homomorphism, then φ is an isomorphism. (cont'd on p. 8.)

Since $\text{im}(\varphi)$ is a submodule of M, and $\text{im}(\varphi) \neq 0_M$ since φ is nonzero, $\text{im}(\varphi) = M$ since M is simple. Thus φ is surjective. $\ker(\varphi)$ is a submodule of M, and $\ker(\varphi) \neq M$ since φ is nonzero, hence $\ker(\varphi) = 0_M$ since M is simple. Then φ is injective. Therefore φ is an isomorphism. □

(d) Let $\text{End}(M)$ be the set of R-module homomorphisms from M to itself, with addition defined pointwise, $(f+g)(x) = f(x) + g(x)$, and multiplication defined by functional composition. Then $\text{End}(M)$ is a ring with $1_{\text{End}(M)} = \text{id}_M$.

Prove: if M is a simple left R-module, then $\text{End}(M)$ is a division ring.

Let $\varphi \in \text{End}(M)$, $\varphi \neq 0_{\text{End}(M)}$. Then by part (b), φ is an isomorphism. Then (by HW 5.2(b)), $\varphi^{-1} : M \longrightarrow M$ is an R-module homomorphism, so $\varphi^{-1} \in \text{End}(M)$. Since $\varphi^{-1} \circ \varphi = \text{id}_M = 1_{\text{End}(M)}$ and $\varphi \circ \varphi^{-1} = \text{id}_M = 1_{\text{End}(M)}$, φ is a unit in $\text{End}(M)$. Therefore $\text{End}(M)$ is a division ring. □

4.(20) Suppose G is a group, and H is a normal subgroup of G satisfying $\mathrm{Aut}(H) = \mathrm{Inn}(H)$ and $\mathbf{Z}(H) = 1$. Prove $G \cong H \times \mathbf{C}_G(H)$.

First of all, $H \cap \mathbf{C}_G(H) = \{g \in H \mid gh = hg \ \forall\ h \in H\} = Z(G)$, which equals 1_G by assumption. Let $g \in G$ and consider the function $\varphi : H \longrightarrow H$ given by $\varphi(x) = gxg^{-1}$. (Note $\mathrm{im}(\varphi) = H$ since $H \trianglelefteq G$.) Then $\varphi \in \mathrm{Aut}(H)$, so $\varphi \in \mathrm{Inn}(H)$ by hypothesis. Then $\exists\ h \in H$ such that $\varphi(x) = hxh^{-1}$ for all $x \in H$. Then $gxg^{-1} = hxh^{-1}$ for all $x \in H$, which implies $h^{-1}gx = xh^{-1}g$ for all $x \in H$. Thus $h^{-1}g \in \mathbf{C}_G(H)$. Then $g = h(h^{-1}g) \in H \cdot \mathbf{C}_G(H)$. Since g was arbitrary, this shows $G = H\,\mathbf{C}_G(H)$. It remains to show $\mathbf{C}_G(H) \trianglelefteq G$. Let $g \in G$ and $y \in \mathbf{C}_G(H)$. Write $g = hc$ with $h \in H$, $c \in \mathbf{C}_G(H)$. Then $\mathbf{C}_G(H)^g = \mathbf{C}_G(H)^{hc} = (\mathbf{C}_G(H)^c)^h = \mathbf{C}_G(H)^h = \mathbf{C}_G(H)$ since h commutes with every element of $\mathbf{C}_G(H)$. Then $\mathbf{C}_G(H) \trianglelefteq G$. Then $G \cong H \times \mathbf{C}_G(H)$. □

5.(25) Let R be a ring.

(a) Prove the third isomorphism theorem for left R-modules, namely, if K is a submodule of a left R-module M, then there is a one-to-one correspondence between submodules of M/K and submodules of M containing K, and the corresponding quotients are isomorphic as R-modules.

Let K be a submodule of M. Then K is an additive subgroup of M, so by the third isomorphism theorem for groups, there is a one-to-one correspondence between the additive subgroups of M/K and the additive subgroups of M containing K. More precisely, every subgroup S of M/K has the form $S = L/K$ for a unique subgroup L of M containing K. Claim S is a submodule of M/K if and only if L is a submodule of M. Indeed, for any $r \in R$, $l \in L$, $r \cdot (l + K) \in L/K \iff rl + K \in L/K \iff rl + K = l' + K$ for some $l' \in L \iff rl \in l' + K$ for some $l' \in L \iff rl \in L$, since $K \subseteq L$. This proves the claim, and the one-to-one correspondence then follows from the third isomorphism theorem for groups. (Continued on page 7.)

6.(20) Suppose both horizontal sequences in the diagram of groups and homomorphisms below are exact, and the diagram commutes. Prove: (a) if α and γ are isomorphisms, then β is an isomorphism, and, (b) under the same hypothesis, if the top sequence splits, then the bottom sequence splits.[2]

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 1 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 1 \end{array}$$

Let $b \in \ker(\beta)$. Then $\beta(b) = 1_{B'}$, so $g' \circ \beta(b) = 1_{C'}$. Then $(\gamma \circ g)(b) = 1_{C'}$. Since γ is injective and $\gamma(g(b)) = 1_{C'}$, $g(b) = 1_C$. Then $b \in \ker(g)$ so $b \in \operatorname{im}(f)$. Let $a \in A$ with $f(a) = b$. Then $f'(\alpha(a)) = (f' \circ \alpha)(a) = (\beta \circ f)(a) = \beta(f(a)) = \beta(b) = 1_{B'}$. Then $\alpha(a) = 1_{A'}$ since $\ker f' = 1_{A'}$. Then $a = 1_A$ since α is injective. Then $b = f(\alpha) = f(1_A) = 1_B$. Thus $\ker(\beta) = 1_B$ so β is injective. Let $b' \in B$. Since γ is surjective, $g'(b') = \gamma(c)$ for some $c \in C$. Since g is surjective, $c = g(b)$ for some $b \in B$.

(continued on p. 8)

7.(25) Let R be a ring and M a *right* R-module.[3]

(a) Show that the set $\operatorname{Hom}_R(M, R)$ of right R-module homomorphisms $\varphi\colon M \longrightarrow R$ has a natural structure as a *left* R-module, and that every right R-module homomorphism $f\colon M \longrightarrow N$ naturally induces a left R-module homomorphism $f^*\colon \operatorname{Hom}_R(N, R) \longrightarrow \operatorname{Hom}_R(M, R)$.[4]

Let $\varphi, \psi \in \operatorname{Hom}_R(M, R)$, and $r \in R$. Define $\varphi + \psi : M \to R$ by $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$, and $r \cdot \varphi : M \to R$ by $(r \cdot \varphi)(x) = r\varphi(x)$. It is straightforward to check that $\varphi + \psi$ and $r \cdot \varphi$ are additive homomorphisms. Let $s \in R$ and $x \in M$. Then $(\varphi + \psi)(xs) = \varphi(xs) + \psi(xs) = \varphi(x)s + \psi(x)s = (\varphi(x) + \psi(x))s = (\varphi + \psi)(x) \cdot s$, and $(r \cdot \varphi)(xs) = r\varphi(xs) = r\varphi(x)s = (r\varphi)(x) \cdot s$. Thus $\varphi + \psi$ and $r\varphi$ are right R-module homomorphisms, so $\varphi + \psi \in \operatorname{Hom}_R(M, R)$ and $r\varphi \in \operatorname{Hom}_R(M, R)$.

(continued on page 8)

[2] An exact sequence $1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$ *splits* iff there exists a homomorphism $s\colon C \longrightarrow B$ such that $g \circ s = \mathrm{id}_C$. Note that your argument applies *mutatis mutandis* to such diagrams of left R-modules and R-module homomorphisms, with the 1's replaced with 0's.

[3] If R is commutative and M is a right R-module, then the underlying abelian group M also has a left R-module structure, defined by $r \cdot x := x \cdot r$.

[4] $\operatorname{Hom}_R(M, R)$ is called the *dual module* of M.

(b) Assume R is a ring with 1, and M is a finitely-generated free (unital) right R-module. Prove that $\mathrm{Hom}_R(M, R)$ is free.

Let X be a basis for R. Since R is finitely generated, X must be finite. (This is an exercise – see web page for the argument.) Write $X = \{x_1, \dots, x_n\}$. Let $\varphi_1, \dots, \varphi_n \in \mathrm{Hom}_R(M, R)$ be defined by $\varphi_i\left(\sum_{j=1}^{n} x_j r_j\right) = r_i$. Claim $\{\varphi_1, \dots, \varphi_n\}$ is a basis of M. Let $\varphi \in \mathrm{Hom}_R(M, R)$. Let $s_j = \varphi(x_j)$. Then $\varphi = \sum_{i=1}^{n} s_i \varphi_i$, since $\varphi\left(\sum_{j=1}^{n} x_j r_j\right) = \sum_{j=1}^{n} \varphi(x_j) r_j = \sum_{i=1}^{n} s_j r_j = \sum_{i=1}^{n} s_i \varphi_i\left(\sum x_j r_j\right)$. Thus $\langle \{\varphi_1, \dots, \varphi_n\} \rangle = \mathrm{Hom}_R(M, R)$. Continued on page 9.

(c) Find an example of a nonzero right R-module M satisfying $\mathrm{Hom}_R(M, R) = 0$. (Hint: There are such examples with $R = \mathbb{Z}$.)

Let $M = \mathbb{Z}_n$ ($n \geq 1$), a module over $R = \mathbb{Z}$. If $\varphi : \mathbb{Z}_n \to \mathbb{Z}$ is a homomorphism, then $0 = \varphi(0) = \varphi(n \cdot x) = n\,\varphi(x)$, hence $\varphi(x) = 0$, for every $x \in \mathbb{Z}_n$. Thus $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}) = 0$.

(d) Show, if $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is an exact sequence of right R-module homomorphisms, then

$$0 \longrightarrow \mathrm{Hom}_R(C, R) \xrightarrow{g^*} \mathrm{Hom}_R(B, R) \xrightarrow{f^*} \mathrm{Hom}_R(A, R)$$

is exact, and give an example to show

$$0 \longrightarrow \mathrm{Hom}_R(C, R) \xrightarrow{g^*} \mathrm{Hom}_R(B, R) \xrightarrow{f^*} \mathrm{Hom}_R(A, R) \longrightarrow 0$$

need not be exact. (Hint: Use your answer to part (c) to construct the counter-example.)

$\ker(g^*) = 0$: Suppose $\varphi \in \mathrm{Hom}_R(C, R)$ with $g^*(\varphi) = 0$. Then $\varphi \circ g = 0$, so $\varphi(g(x)) = 0 \ \forall\, x \in B$. Since g is surjective this implies $\varphi(c) = 0 \ \forall\, c \in C$, hence $\varphi = 0$.

$\ker(f^*) = \mathrm{im}(g^*)$: Suppose $\varphi \in \mathrm{Hom}_R(B, R)$ with $f^*(\varphi) = 0$. Then $\varphi \circ f = 0$, so $\mathrm{im}(f) \subseteq \ker \varphi$. Then $\ker(g) \subseteq \ker(\varphi)$ by exactness. Then φ induces a well-defined homomorphism $\overline{\varphi} : C \longrightarrow R$; defined by $\overline{\varphi}(c) = \varphi(b)$ where $g(b) = c$; if $g(b') = c$, then $0 = c - c = g(b) - g(b') = g(b - b')$, so $b - b' \in \ker(g) \subseteq \ker(\varphi)$, so $0 = \varphi(b - b') = \varphi(b) - \varphi(b')$, $\varphi(b) = \varphi(b')$

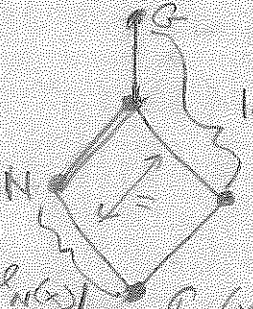
① (continued) $g C_G(x) g^{-1} = C_G(y)$. To see this, note $z \in C_G(x) \Rightarrow y^{gzg^{-1}} = (y^{g^{-1}})^{gz} = x^{gz} = (x^z)^g = x^g = y$ $\Rightarrow gzg^{-1} \in C_G(y)$, and similarly, $z \in C_G(y) \Rightarrow g^{-1}zg \in C_G(x) \Rightarrow z \in g C_G(x) g^{-1}$. This proves the claim. Then, since $N \trianglelefteq G$, $C_G(y) = C_G(x)^g \subseteq N^g \subseteq N$ as well, so $|cl_G(x)| = |cl_G(y)| = |G:N|\,|cl_N(y)|$ by the first part of the proof. Then $\{cl_N(y) \mid y \in cl_G(x)\}$ is a partition of $cl_G(x)$ into sets of size $\frac{|cl_G(x)|}{|G:N|}$; hence there are $|G:N|$ sets in the partition.

In general, we have $\frac{|cl_G(x)|}{|cl_N(x)|} = \frac{|G:C_G(x)|}{|N:C_N(x)|} =$

$\frac{|G:C_G(x)|}{|N:C_G(x)\cap N|} = \frac{|G|/|C_G(x)|}{|N|/|C_G(x)\cap N|} = (|G|/|N|)\left(\frac{|C_G(x)|}{|C_G(x)\cap N|}\right)$

$= |G:N| / |C_G(x) : C_G(x)\cap N|$

$(= |G : NC_G(x)|)$



Again, $\forall\, y \in cl_G(x)$, $y \in N$ and $cl_G(y) = cl_G(x) \subseteq N$, with $|cl_N(y)| = |cl_N(x)|$. Thus $cl_G(x)$ breaks into $\frac{|G:N|}{|C_G(x) : C_G(x)\cap N|}$ conjugacy classes in N, each of size $|N : C_G(x)\cap N|$. □

5(a) (continued) By the third isomorphism theorem for groups, the composite $\varphi : M \longrightarrow M/K \longrightarrow (M/K)/(L/K)$ induces an isomorphism $\overline{\varphi} : M/L \longrightarrow (M/K)/(L/K)$ of additive groups. This map $\overline{\varphi}$ is given by $\overline{\varphi}(m+L) = (m+K) + L/K$. Then $\overline{\varphi}(r\cdot(m+L)) = \overline{\varphi}(rm+L) = (rm+K) + L/K =$ $r(m+K) + L/K = r\cdot((m+K)+L/K) = r\overline{\varphi}(m+L)$. Thus $\overline{\varphi}$ is an R-module homomorphism. (over)

Alternatively, each of the two maps whose composite is φ is an R-module homomorphism (by HW #5.2(a)), so φ and $\overline{\varphi}$ are R-module homomorphisms. Since $\overline{\varphi}$ is a bijection, $\overline{\varphi}$ is an R-module isomorphism. □

5(b) (continued) By the third isomorphism theorem for modules, submodules (left ideals) of R containing I correspond to submodules of $R/I \cong M$, which is simple, so the only left ideals of R containing I are I and R, hence I is a maximal left ideal. □

---

(6) (continued) Consider $b' \cdot \beta(b)^{-1}$. We have $g'(b'\beta(b)^{-1})$ $= g'(b') \cdot g'(\beta(b))^{-1} = \gamma(c) \cdot (g' \circ \beta)(b)^{-1} = \gamma(c) \cdot (\gamma \circ g)(b)^{-1}$ $= \gamma(c)\gamma(g(b))^{-1} = \gamma(c)\gamma(c)^{-1} = 1_{C'}$. Thus $b'\beta(b)^{-1} \in \ker(g')$ so $b'\beta(b)^{-1} \in \operatorname{im}(f')$. Let $a' \in A'$ with $f'(a') = b'\beta(b)^{-1}$. Since α is surjective, $a' = \alpha(a)$ for some $a \in A$. Let $b_0 = f(a)b \in B$. Then $\beta(b_0) = \beta(f(a)\,b) =$ $\beta(f(a))\,\beta(b) = (\beta \circ f)(a)\,\beta(b) = (f' \circ \alpha)(a)\,\beta(b)$ $= f'(\alpha(a))\,\beta(b) = f'(a')\beta(b) = (b'\beta(b)^{-1})\beta(b) = b'$. Thus $\beta(b_0) = b'$. Since b' was arbitrary, this shows β is surjective. Thus β is an isomorphism.

(continued on p. 9)

7(a) (continued) Moreover, $(r+s)\varphi = r\varphi + s\varphi$, $r(\varphi+\psi) = r\varphi + r\psi$, and $r(s\varphi) = (rs)\varphi$. For example, $r(\varphi+\psi)(x)$ $= r(\varphi(x) + \psi(x)) = r\varphi(x) + r\psi(x) = (r\varphi + r\psi)(x)$ for all $x \in M$, hence $r(\varphi+\psi) = r\varphi + r\psi$. The other axioms are verified similarly. Thus $\operatorname{Hom}_R(M, R)$ is a left R-module. Let $f: M \to N$, and define $f^*: \operatorname{Hom}_R(N, R) \to \operatorname{Hom}_R(M, R)$ by $f^*(\varphi) = \varphi \circ f$. ($M \xrightarrow{f} N \xrightarrow{\varphi} R$, $\varphi \circ f$). Continued on p. 9

(6) (continued) Suppose $\exists\ s: C \to B$ with $g \circ s = id_C$. Let $s': C' \to B'$ be defined by $s' = \beta \circ s \circ \gamma^{-1}$. Then $g' \circ s = g' \circ \beta \circ s \circ \gamma^{-1} = \gamma \circ g \circ s \circ \gamma^{-1} = \gamma \circ id_C \circ \gamma^{-1}$ $= \gamma \circ \gamma^{-1} = id_{C'}$. Conversely, if $s': C' \to B'$ with $g' \circ s' = id_{C'}$, then $s = \gamma^{-1} \circ g' \circ \beta$ satisfies $g \circ s = id_C$. Thus the top sequence splits iff the bottom sequence splits.

7(a) continued (from p. 8) Then $f^*(\varphi) = \varphi \circ f$ is a right R-module homomorphism because both f and φ are. Moreover, $f^*(\varphi + \psi) = (\varphi + \psi) \circ f =$ $\varphi \circ f + \psi \circ f = f^*(\varphi) + f^*(\psi)$ and $f^*(r\varphi) =$ $(r\varphi) \circ f = r(\varphi \circ f) = r f^*(\varphi)$, since, e.g.,
$(\varphi + \psi) \circ f(x) = (\varphi + \psi)(f(x)) = \varphi(f(x)) + \psi(f(x))$
$= (\varphi \circ f)(x) + (\psi \circ f)(x) = (\varphi \circ f + \psi \circ f)(x)$.
Thus f^* is a left R-module homomorphism. □

7(b) continued Suppose $\sum_{j=1}^{n} s_j \varphi_j = 0$. Then for every $1 \le i \le n$, $\sum_{j=1}^{n} s_j \varphi_j(x_i) = 0$. Then, since $\varphi_j(x_i) = 1_R$ if $i = j$ and $= 0_R$ if $i \neq j$, $s_i \cdot 1_R = 0$ for all i, hence $s_i = 0$ $\forall\ i$. Then $\{\varphi_1, \dots, \varphi_n\}$ is linearly independent. Thus $\mathrm{Hom}_R(M, R)$ is a free left R-module. □

7(c) continued Then $\bar{\varphi}$ is well-defined. Since $\bar{\varphi} \circ g = \varphi$, $g^*(\bar{\varphi}) = \varphi$, hence $\varphi \in \mathrm{im}\, g^*$. Thus $\ker f^* \subseteq \mathrm{im}\, g^*$. For the converse, observe that $g \circ f = 0$, hence $\varphi \circ (g \circ f) = 0$ for all $\varphi \in \mathrm{Hom}_R(C, R)$. Then $(f^* \circ g^*)(\varphi) = f^*(\varphi \circ g) =$ $\varphi \circ g \circ f = 0$, for all φ, hence $f^* \circ g^* = 0$, so $\mathrm{im}(g^*) \subseteq \ker(f^*)$. This proves exactness. (over)

Consider the exact sequence of $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}_n \longrightarrow 0 \qquad (n>1)$$

where $f(x) = nx$ and $g(x) = \bar{x}$. By (b), $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}) = 0$. The dual sequence is then

$$0 \longrightarrow 0 \xrightarrow{g^*} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) \xrightarrow{f^*} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) \longrightarrow 0.$$

This sequence is exact at 0 and the middle term $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z})$, but f^* is not onto: for any $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z})$, $(f^*(\varphi))(x) = (\varphi \circ f)(x) = \varphi(nx) = n\varphi(x)$, so $(f^*(\varphi))(1) = n\varphi(1)$. Then the identity function $\psi(x) = x$ doesn't lie in $\mathrm{im}(f^*)$, since $1 = \psi(1) \neq n\varphi(1)$ for any φ.