Math 306 Topics in Algebra, Spring 2013
Homework 9 Solutions

(1) (5 pts) Show that, when R is a commutative ring and M is an R-module, $\mathrm{Hom}_R(M,M)$ is an R-algebra.

Solution: It is not hard to show that $\mathrm{Hom}_R(M,M)$ is indeed an R-module (we talked about this in class). To show it is an R-algebra, have map

$$R \longrightarrow \mathrm{Hom}_R(M,M)$$
$$r \longmapsto f_r\colon M \to M, \quad m \mapsto rm$$

This map lands in the center of $\mathrm{Hom}_R(M,M)$ since, for any $g \in \mathrm{Hom}_R(M,M)$, $(g \circ f_r)(m) = g(f_r(m)) = g(rm) = rg(m)$ (the last equality uses that g is a module homomorphism), while on the other hand we have $(f_r \circ g)(m) = f_r(g(m)) = rg(m)$.

(2) (5 pts) Section 10.2, problem 1 (p. 350).

Solution: Straightforward (using the submodule criterion from class is the most efficient way to do this).

(3) (7 pts) Section 10.2, problem 9 (p. 350).

Solution: Let $\phi, \psi \in \mathrm{Hom}_R(R,M)$. Suppose $\phi(1) = \psi(1) = m$. Then we must have $\phi(a) = \phi(a \cdot 1) = a\phi(1) = am$ and $\psi(a) = \psi(a \cdot 1) = a\psi(1) = am$ for any $a \in R$ (since ϕ and ψ are homomorphisms). Since a was arbitrary, $\phi = \psi$. So any homomorphism in $\mathrm{Hom}_R(R,M)$ looks like a map from R to M that sends a to am for some m. Call this map ϕ_m.

Now define a map

$$f\colon \mathrm{Hom}_R(R,M) \longrightarrow M$$
$$\phi_m \longmapsto m$$

To see this is an R-module homomorphism, first note that, for any $r \in R$,

$$(\phi_m + r\phi_{m'})(1) = \phi_m(1) + r\phi_{m'}(1) = m + rm' = \phi_{m+rm'}(1).$$

Hence

$$f(\phi_m + r\phi_{m'}) = f(\phi_{m+rm'}) = m + rm' = f(\phi_m) + rf(\phi_{m'}).$$

To see that f is injective, suppose $f(\phi_m) = 0$. This means $m = 0$. It follows that $\phi_m(r) = 0$ for all r. This means that $\phi_m = 0 \in \mathrm{Hom}_R(R,M)$. So the kernel of f is trivial and f is injective.

To see that f is surjective, first show that ϕ_m is an R-module homomorphism:

$$\phi_m(r + ar') = (r + ar')m = rm + ar'm = \phi_m(r) + a\phi_m(r').$$

Thus given an $m \in M$, there exists a $\phi_m \in \mathrm{Hom}_R(R,M)$ such that $f(\phi_m) = m$.

(4) (5 pts) Section 10.3, problem 4 (p. 356).

Solution: Suppose that A is a finite abelian group (or $\mathbb{Z}$-module) of order n. Then by Lagrange's Theorem, for each $a \in A$, $na = 0$. Hence A is a torsion $\mathbb{Z}$-module. An example of an infinite abelian group that is a torsion $\mathbb{Z}$-module is $\prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ (also $\mathbb{Q}/\mathbb{Z}$ or polynomials over $\mathbb{Z}/2\mathbb{Z}$ would do).

(5) (4 pts) Show that the sequence of modules

$$0 \longrightarrow A \xrightarrow{\ i\ } A \oplus C \xrightarrow{\ p\ } C \longrightarrow 0,$$

where i and p are the canonical inclusion and projection, is exact.

Solution: For exactness at A, it is clear that the kernel of i is only 0, so i is injective. Similarly it is clear that p is surjective. Kernel of p is A, which is precisely the image of i, so sequence is exact at $A \oplus C$.

Notice that i and p are the only maps that make this sequence exact.

(6) (5 pts) Suppose $A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow A_4$ is exact. For $1 \leq k \leq 4$, set

$$C_k = \ker(A_k \longrightarrow A_{k+1}) = \operatorname{im}(A_{k-1} \longrightarrow A_k) = \operatorname{coker}(A_{k-2} \longrightarrow A_{k-1}).$$

(Note that, depending on k, some of these equivalent expressions for C_k may not make sense. For example, to define C_1, you have to use $C_1 = \ker(A_1 \to A_2)$ since the other two formulations would be in terms of A_0 and A_{-1} which we do not have. Similarly for C_5, you have to use $C_5 = \operatorname{coker}(A_3 \to A_4)$). Show that the sequences

$$0 \longrightarrow C_k \longrightarrow A_k \longrightarrow C_{k+1} \longrightarrow 0$$

are exact (you will have to define the maps as well). This therefore gives an example of how an exact sequence can be broken into (and spliced from) short exact sequences (the picture of how this works was drawn in class).

Solution: For $k = 1, 2, 3$, the exactness of

$$0 \longrightarrow C_k \longrightarrow A_k \longrightarrow C_{k+1} \longrightarrow 0$$

simply comes down to the fact that, given a homomorphism $f\colon M \to N$, the sequence

$$0 \longrightarrow \ker(f) \xrightarrow{i} M \xrightarrow{f} \operatorname{im}(f) \longrightarrow 0$$

is exact. For the last one ($k = 4$), we have a sequence

$$0 \longrightarrow C_4 = \operatorname{im}(A_3 \to A_4) \xrightarrow{i} A_4 \xrightarrow{\text{quotient}} C_5 = \operatorname{coker}(A_3 \to A_4) \longrightarrow 0$$

but this is clearly also exact.

(7) (4 pts/part) For this problem, recall that by an extension we mean the entire exact sequence

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0,$$

so that if there are two sequences with the same modules but different homomorphisms between them, we consider those extensions to be different.

(a) Show that any extension of C by A has $|C| \cdot |A|$ elements (sometimes this number is infinity).
(b) How many inequivalent extensions of $\mathbb{Z}/3\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$ are there? How about extensions of $\mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}/3\mathbb{Z}$?
(c) If p is a prime, show that there are exactly p inequivalent abelian extensions of $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{Z}/p\mathbb{Z}$: the split extension and the extensions

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{p} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{i} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

where p is multiplication by p and i is the multiplication by i for $1 \leq i \leq p-1$.

Solution:

(a) Using exactness and First Isomorphism Theorem, we argued in class that $B/\operatorname{Im}(f) \cong C$, and, since f is injective, $\operatorname{Im}(f) \cong A$. Hence $B/A \cong C$ and so $|B|/|A| = |C|$. In other words, if A and C are fixed, we must have, for any extension B, that $|B| = |C| \cdot |A|$.
(b) By part (a), the extension in both case has to have size six. It also has to be a $\mathbb{Z}$-module, so it has to be an abelian group. The only abelian group of size six is $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. So the only extension in both cases is the split extension. (If we were talking about exact sequences of groups, and not just abelian groups, then S_3 would actually also be an extension of $\mathbb{Z}/3\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$, but not the other way around.)
(c) To see that the given extensions are really extensions, note that p is clearly injective, that $\operatorname{Im}(p) = \{0, p, 2p, ..., (p-1)p\} = \ker(i)$, and that i is surjective since $\mathbb{Z}/p\mathbb{Z}$ is cyclic of prime order and i is a non-zero homomorphism (any nonzero homomorphism to $\mathbb{Z}/p\mathbb{Z}$ must be surjective since any of the elements generates the group, so that if a non-zero element is in the image of the homomorphism, so is every other element of $\mathbb{Z}/p\mathbb{Z}$). So these extensions, along with the split one, give p extensions of $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{Z}/p\mathbb{Z}$. It is not hard to see that these are inequivalent (one square in the map between two of these sequences would not commute).

To see that this is all of them, first note that, by part (a), the only possibilities for an extension are $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^2\mathbb{Z}$, since those are the only non-isomorphic abelian groups of order p^2. The first one gives the split extension and there are no other maps that work with this extension; inclusion and projection are the only possibility. So this leaves $\mathbb{Z}/p^2\mathbb{Z}$ as the only possibility. So suppose we have an exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{f} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{g} \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

All the groups in this sequence are cyclic. Since f is injective, it must send 1 to an element of order p in $\mathbb{Z}/p^2\mathbb{Z}$, namely one of p, $2p$, ..., $(p-1)p$. In any case, the image is the unique subgroup of $\mathbb{Z}/p^2\mathbb{Z}$ or order p. It is not hard to show that all choices of sending the generator to an element of order p will result in equivalent extensions, so we might as well assume that $f(1) = p$ and so f is indeed the map p from above.

The kernel of g now has to be this subgroup of $\mathbb{Z}/p^2\mathbb{Z}$ or order p. Now, g is determined by where it sends the generator, and setting $g(1) = i$, $1 \leq i \leq p-1$ determines all the nontrivial homomorphisms. Each one of these is precisely multiplication by i and is surjective. Furthermore, the kernel of each of these is precisely as desired, so this takes care of all the possibilities.