Algebra II - Homework 2

Pablo Sánchez Ocal

February 6th, 2017

Exercise 1

Let R a ring, consider the category of left R-modules.

1. Prove that a morphism $f : A \longrightarrow B$ is a monomorphism if and only if the underlying function f is injective. For this, notice that the same argument as used with sets works, since all the functions are in fact morphisms of modules.

   $\Rightarrow$) Let f be a monomorphism. Suppose $x, y \in A$ with $f(x) = f(y)$, let $Z = \{0\}$ be the zero module and define the functions $g_x : Z \longrightarrow A$ as $g_x(0) = x$ and $g_y : Z \longrightarrow A$ as $g_x(0) = y$. Clearly both g_x and g_y are morphisms of modules. Since $f \circ g_x(0) = f(x) = f(y) = f \circ g_y(0)$ this means $f \circ g_x = f \circ g_y$, hence since f is a monomorphism we get that $g_x = g_y$, thus $x = g_x(0) = g_y(0) = y$ and f is injective.

   $\Leftarrow$) Let f be injective. Suppose we have $g_1, g_2 : Z \longrightarrow A$ morphisms of modules with $f \circ g_1 = f \circ g_2$. If there is $x \in A$ with $g_1(x) \neq g_2(x)$, by the injectivity of f we have that $f \circ g_1(x) \neq f \circ g_2(x)$. However, this is a contradiction. Hence, there is no such $x \in A$, that is, $g_1(x) = g_2(x)$ for every $x \in A$, that is, $g_1 = g_2$ and f is a monomorphism.

2. Prove that a morphism $f : A \longrightarrow B$ is an epimorphism if and only if the underlying function f is surjective. One of the directions is the same as in sets, since all the functions are in fact morphisms of modules. For the other, we need a bit of finesse.

   $\Leftarrow$) Let f be surjective. Suppose we have $g_1, g_2 : B \longrightarrow Z$ morphisms of modules with $g_1 \circ f = g_2 \circ f$. Let $y \in B$, then by surjectivity of f there is an $x \in A$ with $f(x) = y$. Now:
   $$g_1(y) = g_1 \circ f(x) = g_2 \circ f(x) = g_2(y),$$
   hence $g_1 = g_2$ and f is an epimorphism.

   $\Rightarrow$) Let f be an epimorphism. Let $y \in B$ and suppose there is no $x \in A$ with $f(x) = y$. Let $Z = \langle y \rangle_R$ and define the functions $g_1 : B \longrightarrow Z$ as $g_1(b) = b$ when $b \in \langle y \rangle_R$, $g_1(b) = 0$ when $b \notin \langle y \rangle_R$ and $g_2 : B \longrightarrow Z$ as $g_2(b) = 0$ for every $b \in B$. Since g_1 is the identyty on $\langle y \rangle_R$ and 0 everywhere else, its is a morphism of modules. Clearly g_2 is a morphism of modules too. Now we have that $f(A) \subset B \setminus \langle y \rangle_R$ hence $g_1 \circ f = g_2 \circ f$, meaning that $g_1 = g_2$ since f is an epimorphism. However, this is a contradiction since $g_1(y) \neq g_2(y)$. Thus there is no such $y \in B$, that is, for every $y \in B$ there is an $x \in A$ with $f(x) = y$, that is, f is surjective.

Exercise 4

For a group G, consider $\mathbb{Z}[G]$ the group ring of G over $\mathbb{Z}$, we will call left G-modules to left $\mathbb{Z}[G]$-modules.

1. Show that the induced function on M a G-module defines a left action of G on M. We want to see that:

$$\begin{array}{rcccc} \varphi & : & G \times M & \longrightarrow & M \\ & & (\sigma, m) & \longmapsto & \sigma m \end{array}$$

   is a left action. Notice that M being a G-module means that we have a multiplication (notice the sum is finite):

$$\begin{array}{rcccc} \phi & : & \mathbb{Z}[G] \times M & \longrightarrow & M \\ & & \left(\sum_{g\in G} a_g g, m\right) & \longmapsto & \left(\sum_{g\in G} a_g g\right) m \end{array}$$

   and using the properties of ϕ we will see that φ is a left action, since for $id, \sigma, \tau \in G$ and $m \in M$:

   (a) $\varphi(\mathrm{id}, m) = \phi(id, m) = m$ because M is a G-module via ϕ,

   (b) $\varphi(\sigma\tau, m) = \phi(\sigma\tau, m) = \phi(\sigma, \phi(\tau, m)) = \varphi(\sigma, \phi(\tau, m))$ because M is a G-module via ϕ.

   This proves that φ is a left action.

2. Let M, N be G-modules, we want to see that $f : N \longrightarrow M$ is a G-module homomorphism if and only if f is a homomorphism of abelian groups and $f(\sigma n) = \sigma f(n)$ for every $\sigma \in G$, $n \in N$.

   $\Rightarrow$) Let f be a module homomorphism. This means that:

   (a) $f(n_1 + n_1) = f(n_1) + f(n_2)$ for every $n_1, n_2 \in N$, that is, f is a homomorphism of abelian groups,

   (b) $f(rn) = rf(n)$ for every $r \in \mathbb{Z}[G]$ (in particular when $r = \sigma \in G$), $n \in N$.

   $\Leftarrow$) The fact that f is a homomorphism of abelian groups implies that $f(n_1 + n_1) = f(n_1) + f(n_2)$ for every $n_1, n_2 \in N$. For the $\mathbb{Z}[G]$-linearity, we notice that for every

$a_g \in \mathbb{Z}$ for $g \in G$ and $n \in N$ we have (notice the sum is finite):

$$\begin{aligned}
f\left(\left(\sum_{g\in G} a_g g\right) n\right) &= f((a_{g_1}g_1 + \cdots + a_{g_k}g_k)n) = f(a_{g_1}g_1 n + \cdots + a_{g_k}g_k n) \\
&= f(\overbrace{g_1 n + \cdots + g_1 n}^{a_{g_1}} + \cdots + \overbrace{g_k n + \cdots + g_k n}^{a_{g_k}}) \\
&= \overbrace{f(g_1 n) + \cdots + f(g_1 n)}^{a_{g_1}} + \cdots + \overbrace{f(g_k n) + \cdots + f(g_k n)}^{a_{g_k}}) \\
&= \overbrace{g_1 f(n) + \cdots + g_1 f(n)}^{a_{g_1}} + \cdots + \overbrace{g_k f(n) + \cdots + g_k f(n)}^{a_{g_k}}) \\
&= a_{g_1}g_1 f(n) + \cdots + a_{g_k}g_k f(n) = \left(\sum_{g\in G} a_g g\right) f(n)
\end{aligned}$$

proving $\mathbb{Z}[G]$-linearity. Notice how we had to develop until we could use that f was a homomorphism of abelian groups and then again more until we could use G-linearity.

3. Let M be a G-module and set M^G the set of G-invariants of M. We show that $(M^G, +)$ is an abelian subgroup of $(M, +)$.

   We clearly have $M^G \subset M$ as sets. Moreover, for every $m, n \in M^G$, every $\sigma \in G$, we have that $\sigma(m - n) = \sigma m - \sigma n = m - n$, hence $m - n \in M^G$ and M^G is closed under addition. Moreover, since M is a module we have that $(M, +)$ is abelian, thus $(M^G, +)$ is also abelian. As desired, $M^G \leq M$.

Exercise 5

With the notation as above, we will work with G-modules and abelian groups.

1. Let $\mathbb{Z}$ be a G-module with trivial action (we will use this fact multiple times without explicit mention to it). Now, for any G-module M, we have an isomorphism of abelian groups $M^G \cong \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$. For this, we define:

$$\begin{array}{rcccl} \psi & : & M^G & \longrightarrow & \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M). \\ & & m & \longmapsto & f_m : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & M \\ 1 & \longmapsto & m \end{array} \end{array}$$

   Notice how as a module homomorphism, it is enough to define $f_m(1)$ so that the whole function f_m is defined. We now proceed to see that ψ is in fact a group isomorphism.

   (a) ψ is well defined; that is, f_m is a module homomorphism for every $m \in M$, since for every $k_1, k_2 \in \mathbb{Z}$ we have $f_m(k_1+k_2) = k_1m+k_2m = f_m(k_1)+f_m(k_2)$, and for every $\sigma \in G$, $k \in \mathbb{Z}$ we have $f_m(\sigma k) = f_m(k) = km = m + \cdots + m = \sigma m + \cdots + \sigma m = \sigma(m + \cdots + m) = \sigma(km) = \sigma f_m(k)$. Hence in virtue of Exercise 4b above, f is a G-module homomorphism.

   (b) ψ is injective; let $f_m = f_n$ for certain $m, n \in M$, this means that $m = f_m(1) = f_n(1) = n$.

   (c) ψ is surjective; let $f \in \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$, set $m = f(1)$. We just have to check that $m \in M^G$, which is clear since $\sigma m = \sigma f(1) = f(\sigma 1) = f(1) = m$. Now $\psi(m) = f$.

   (d) ψ is a group morphism; let $m, n \in M$, we have that $\psi(m + n)(1) = m + n = \psi(m)(1) + \psi(n)(1) = (\psi(m) + \psi(n))(1)$, hence $\psi(m + n) = \psi(m) + \psi(n)$, as desired.

   By the above, we clearly have that setting the functor $F(\cdot) = \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, \cdot)$, the assignments $M \longmapsto F(M)$ and $M \longmapsto M^G$ it coincide. In virtue of Exercise 3, F is left exact.

2. With the following example we will show that F is not right exact. Let $G = \{t^n : n \in \mathbb{Z}\}$.

   (a) Show that $\mathbb{Z}[G] = \mathbb{Z}[t, t^{-1}]$.
   $\subseteq$) An element of $\mathbb{Z}[G]$ is a finite sum of the form $\sum_{i=-n}^{m} a_i t^i$ with $n, m \in \mathbb{N}$ and $a_i \in \mathbb{Z}$ (since $t^i \in G$) for $i = -n, \ldots, m$. This can clearly be seen as a polynomial with integer coefficients in the variables t, t^{-1}.
   $\supseteq$) A polynomial with integer coefficients in the variables t, t^{-1} is a finite sum of the form $\sum_{i=-n}^{m} a_i t^i$ with $n, m \in \mathbb{N}$ and $a_i \in \mathbb{Z}$ for $i = -n, \ldots, m$. This can clearly be seen as an element of $\mathbb{Z}[G]$.

(b) Let $M = \mathbb{Z}[G]$ a G-module under left multiplication, $N = \{n \in M : n = m(t-1) \text{ for some } m \in M\} = \mathbb{Z}[t,t^{-1}](t-1)$. We want to see that N is a G-submodule of M. For this, clearly $N \subset M$, for $n_1, n_2 \in N$ we have $n_1 - n_2 = m_1(t-1) - m_2(t-1) = (m_1 - m_2)(t-1) \in N$ since $m_1 - m_2 \in M$ (this means N is closed under addition) and thus $(N,+)$ is abelian because $(M,+)$ is abelian. Moreover, let $r \in \mathbb{Z}[G]$, then for every $n \in N$ we have $rn = rm(t-1) \in N$ since $rm \in M$, hence N is closed under left multiplication. This means that N is a G-submodule of M.

(c) Show that $M/N \cong \mathbb{Z}$ as abelian groups and the action of G on $\mathbb{Z}$ induced by this isomorphism is trivial. For this, we define:

$$\begin{array}{cccc} \psi & : & M & \longrightarrow & \mathbb{Z} \\ & & p(t,t^{-1}) & \longmapsto & p(1,1) \end{array}$$

notice that since ψ is an evaluation morphism and we are evaluating in an invertible element, it is well defined and indeed a morphism. Now notice that $\ker(\psi) = N$:

$\supseteq$) Let $n \in N$, then $\psi(n) = \psi(m)(1-1) = 0$ and $n \in \ker(\psi)$.

$\subseteq$) Let $n \in \ker(\psi)$, that is, $\psi(n) = 0$. For $k \in \mathbb{N}$ large enough, we can write $n = \sum_{i=-k}^{k} a_i t^i$ for $a_i \in \mathbb{Z}$ for $i = -k, \dots, k$. Hence $t^k n = \sum_{i=0}^{2k} a_{i-k} t^i \in \mathbb{Z}[t]$, and we have $\psi(t^k n) = \psi(t^k)\psi(n) = 0$, hence we can divide by $(t-1)$ and obtain that $t^k n = q(t-1)$ for $q \in \mathbb{Z}[t]$. This means that $n = (q/t^k)(t-1) \in N$ since $q/t^k \in M$.

By the First Isomorphism Theorem, we have that $M/N \cong \mathbb{Z}$. Moreover, consider the induced action:

$$\begin{array}{ccc} G \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (t^n, k) & \longmapsto & \psi(t^n)k \end{array}$$

where $n \in \mathbb{Z}$. Obviously $\psi(t^n) = 1$, and thus this is the trivial action.

(d) Consider now the exact sequence of G-modules:

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

since we saw above that G acts on $\mathbb{Z}$ trivially, we are in the case discussed where applying the functor F and looking at the G-invariants are the same thing. Thus applying F (or rather considering the G-invariants), we obtain a sequence:

$$0 \longrightarrow N^G \longrightarrow M^G \longrightarrow (M/N)^G \cong \mathbb{Z}^G \cong \mathbb{Z} \longrightarrow 0.$$

We are interested in looking at the surjectivity of $M^G \longrightarrow \mathbb{Z}$. For this, we compute M^G. Since M is considered as a G-module by left multiplication, we have that for a finite sum $\sum_{i=-n}^{n} a_i t^i$ with $n \in \mathbb{N}$ large enough and $a_i \in \mathbb{Z}$ for $i = -n, \dots, n$, multiplication by an element $t^k \in G$ with $k \in \mathbb{Z}$ yields

$\sum_{i=-n}^{n} a_i t^{i+k}$. This is a translation of all the coefficients different than 0, meaning that for having such a sum invariant it can only be the sum 0. That is, $M^G = \{0\}$. However, a morphism $\{0\} \longrightarrow \mathbb{Z}$ can never be surjective, hence F is not right exact, as desired.

Exercise 6

Let R be an integral domain.

1. Let I, J be nonzero ideals of R, show that $I \cap J \neq (0)$. Suppose that $I \cap J = (0)$, I, J being nonzero means that for any $0 \neq i \in I$ and $0 \neq j \in J$ we have $ij \in I$, $ij \in J$, hence $ij \in I \cap J$ thus $ij = 0$. This is a contradiction with the fact that R is an integral domain. Hence $I \cap J \neq (0)$.

2. Let I be an ideal of R that is free as an R-module. Show that I is principal. We will use the Lemma proven in class saying that for A, B submodules of M an R-module, then $A \oplus B \cong A + B$ if and only if $A \cap B = (0)$. Now, I being free means that there is a basis $\{x_j\}_{j \in J}$ of elements of R such that $I \cong \oplus_{j \in J} Rx_j$. Now since $I \subset R$ because it is an ideal, we must have that I is an internal direct sum by the natural inclusion. However, since $Rx_i \oplus Rx_j = Rx_i + Rx_j$ if and only if $Rx_i \cap Rx_j = (0)$, but by the section above this never happens, we have that I with $|J| > 1$ cannot be an internal direct sum. Hence we can only have $|J| = 0$ (that is, $J = \emptyset$) and thus $I = (0)$, which is clearly principal, or $|J| = 1$ (that is $J = \{x\}$) and thus $I = Rx = (x)$, which is clearly principal.

Exercise 7

Let R be a ring, F an R-module generated by $S = \{x_1, \dots, x_n\} \subset F$.

1. Suppose that F is free and S is an R-basis. For any module M and elements $m_1, \dots, m_n \in M$, prove that there exists an unique R-module homomorphism $f : F \longrightarrow M$ with $f(x_i) = m_i$ for $i = 1, \dots, n$. We define:

$$f \quad : \quad \begin{array}{ccc} F & \longrightarrow & M \\ \sum_{i=1}^n r_i x_i & \longmapsto & \sum_{i=1}^n r_i m_i \end{array}$$

where $r_i \in R$ for $i = 1, \dots, n$. Now:

   (a) f is well defined; the sum $\sum_{i=1}^n r_i m_i$ is indeed an element of M because this is a module.

   (b) f is a morphism of groups:

$$\begin{aligned} f\left(\sum_{i=1}^n r_i x_i + \sum_{i=1}^n s_i x_i\right) &= f\left(\sum_{i=1}^n (r_i + s_i) x_i\right) = \sum_{i=1}^n (r_i + s_i) m_i \\ &= \sum_{i=1}^n r_i m_i + \sum_{i=1}^n s_i m_i = f\left(\sum_{i=1}^n r_i x_i\right) + f\left(\sum_{i=1}^n s_i x_i\right) \end{aligned}$$

   (c) f is R-linear, for $r \in R$ we have:

$$f\left(r \sum_{i=1}^n r_i x_i\right) = f\left(\sum_{i=1}^n r r_i m_i\right) = \sum_{i=1}^n r r_i m_i = r \sum_{i=1}^n r_i m_i = r f\left(\sum_{i=1}^n r_i x_i\right)$$

   (d) f is unique: if g a morphism of modules such that $g(x_i) = m_i$ for $i = 1, \dots, n$ we obtain that:

$$f\left(\sum_{i=1}^n r_i x_i\right) = \sum_{i=1}^n r_i m_i = \sum_{i=1}^n r_i g(x_i) = \sum_{i=1}^n g(r_i x_i) = g\left(\sum_{i=1}^n r_i m_i\right)$$

   thus $f = g$.

2. We want to construct a $\mathbb{Z}$-module homomorphism $f\mathbb{Z} \oplus \mathbb{Z} \longrightarrow \mathbb{Z}$ such that $f(x_1) = 1$. First, notice that letting $y = x_2/2$, $\{x_1, y\}$ form a basis of $\mathbb{Z} \oplus \mathbb{Z}$ as a free module. By the definition of x_1, x_2 and x_3 we have that $x_3 = x_1 + x_2/2$, thus applying f we obtain that $f(x_3) = f(x_1) + f(x_2)/2$. It is easy to check that if we set:

$$\begin{cases} f(x_2) = 2\, f(x_3) = 2 \\ f(x_2) = 4\, f(x_3) = 3 \end{cases} \implies \begin{cases} f(x_1) = 1 \\ f(y) = 1 \end{cases}$$

thus in virtue of the above, f is uniquely determined (since we have determined its value on a basis) but we have multiple choices for the values of x_2 and x_3.

3. Show that there exists no $\mathbb{Z}$-module homomorphism $f\mathbb{Z} \oplus \mathbb{Z} \longrightarrow \mathbb{Z}$ such that $f(x_1) = 1$ and $f(x_2) = 1$, regardless of what we try to pick for $f(x_3)$. Notice that $y = x_2/2$, hence $f(y) = f(x_2)/2 = 1/2$, but $1/2 \notin \mathbb{Z}$. This implies that there is no value to be assigned to y, that is, no such homomorphism f exists.