Lecturas Matemáticas
Volumen **37** (2) (2016), páginas 107-113
ISSN 0120-1980

Homomorphisms from $R/(r)$ to $R/(s)$ for a principal ideal domain R

Homomorfismos de $R/(r)$ a $R/(s)$ para R un dominio de ideales principales

Javier Diaz-Vargas and Gustavo Vargas de los Santos

Universidad Autónoma de Yucatán, México

ABSTRACT. For a principal ideal domain R, we find the number of homomorphisms from $R/(r)$ to $R/(s)$, seen as modules or algebras over R. We determine also the number of R-module homomorphisms between two finitely generated R-modules.

***Key words*:** principal ideal domain, module homomorphism, algebra homomorphism, finitely generated module.

RESUMEN. Para R un dominio de ideales principales, encontramos el número de homomorfismos de $R/(r)$ to $R/(s)$, vistos como módulos o álgebras sobre R. También, determinamos el número de R-homomorfismos de módulos entre dos R-módulos finitamente generados.

***Palabras clave*:** dominio de ideales principales, homomorfismo de módulos, homomorfismo de álgebras, módulo finitamente generado.

2010 AMS Mathematics Subject Classification. Primary 15-01, 15-02; Secondary 16-01, 16-02; Third 11-01, 11-02.

1. Introduction

In an abstract algebra course, at undergraduate level, it is common to ask students to find the number of homomorphisms from $\mathbb{Z}_m$ to $\mathbb{Z}_n$, considering these as groups and as rings. They are usually asked for specific values of m and n. However, it is possible to give a precise answer for arbitrary m and n. See for example [2], where this problem is solved in general by using elementary group theory. In the same spirit, in [4], the number of homomorphisms between two dihedral groups is determined.

In [1], to determine the number of homomorphisms from $\mathbb{Z}_m$ to $\mathbb{Z}_n$, previous knowledge from group theory or ring theory is not assumed, except for the definition of group and ring homomorphism. With respect to number theory, some elementary facts on congruences are used which can be found on any introductory book such as [5]. Also, although the results are basically the same as those in [2], the proofs are more basic.

Now, in this article, in analogy to [1], we determine the number of homomorphisms from $R/(r)$ to $R/(s)$ when R is a principal ideal domain by viewing $R/(r)$ and $R/(s)$ first as R-modules and then as R-algebras. In both cases, we give precise answers. Using the decomposition of finitely generated modules over a principal domain as a product of cyclic modules, we also determine the number of homomorphisms of R-modules between two such modules, generalizing what we had found for cyclic modules.

It is possible to have an infinite number of R-module homomorphisms. However, as in [1], we get a finite number of R-algebra homomorphisms.

2. Module homomorphisms

Let R be a principal ideal domain and $r, s \in R, r, s \neq 0$. Consider $R/(r)$ and $R/(s)$ as R-modules and let $\varphi : R/(r) \to R/(s)$ be a map. If φ is an R-module homomorphism, then for $x + (r) \in R/(r)$,

$$\varphi(x + (r)) = x\varphi(1 + (r)),$$

so $\varphi(x+(r)) = x(a+(s)) = xa+(s)$, where $\varphi(1+(r)) = a+(s)$. So, the homomorphism is determined by its value $\varphi(1 + (r))$ in $1 + (r)$. Hence, we only need to find the values of $a+(s) \in R/(s)$ such that the function $\varphi(x+(r)) = xa+(s)$ is a module homomorphism.

If $\varphi(x + (r)) = ax + (s)$ is such an R-homomorphism, then

$$0 + (s) = r\varphi(1 + (r)) = ra + (s),$$

hence $ra \in (s)$. Conversely, suppose $\varphi(x + (r)) = xa + (s)$ with $ra \in (s)$. If $x_1 + (r) = x_2 + (r)$, then $x_1 - x_2 \in (r)$, and $x_1a - x_2a \in (s)$, since $ra \in (s)$. Hence,

$$\varphi(x_1 + (r)) = x_1a + (s) = x_2a + (s) = \varphi(x_2 + (r)),$$

so φ is well defined. Also,

$$\varphi(x + y + (r)) = (x + y)a + (s) = \varphi(x + (r)) + \varphi(y + (r)),$$

and

$$\varphi(z(x + (r))) = \varphi(zx + (r)) = z\varphi(x + (r)),$$

for all $z \in R$, and all $x + (r), y + (r) \in R/(r)$. Therefore, φ is an R-module homomorphism. Thus, we have established the following lemma.

Lemma 1. *The function $\varphi : R/(r) \to R/(s)$ is an R-module homomorphism if and only if $\varphi(x + (r)) = xa + (s)$ with $ra \in (s)$.*

Let $\hom_R(R/(r), R/(s))$ denote the abelian group (with the usual sum of functions) of module homomorphisms from $R/(r)$ to $R/(s)$. We can give to $\hom_R(R/(r), R/(s))$ the structure of an R-module by defining $(z\varphi)(x+(r)) = z\cdot\varphi(x+(r))$, for $z \in R$. Now, $s|ra$ if only if $h \mid a$, where $h\gcd(r,s) = s$. Let $f : \hom_R(R/(r), R/(s)) \to R/(\gcd(r,s))$ given by

$$f(\varphi) = \frac{a}{h} + (\gcd(r,s)).$$

This is an R-isomorphism of modules. Let $d = gcd(r,s)$. First we see that the f does not depend on the selection of the a. If $\varphi(1+(r)) = a+(s) = a'+(s)$, then $s \mid a-a'$. Since $s = hd$, we have that $d \mid (a-a')/h = a/h - a'/h$. So $a/h + (d) = a'/h + (d)$.

Now, consider $\varphi_1, \varphi_2 \in \hom_R(R/(r), R/(s))$, with $\varphi_1(x+(r)) = a_1x + (s)$ and $\varphi_2(x+(r)) = a_2x + (s)$. Then $(\varphi_1+\varphi_2)(x+(r)) = (a_1x+(s)) + (a_2x+(s)) = (a_1+a_2)x + (s)$. Hence

$$f(\varphi_1+\varphi_2) = \frac{a_1+a_2}{h} + (d) = \left(\frac{a_1}{h} + (d)\right) + \left(\frac{a_2}{h} + (d)\right) = f(\varphi_1) + f(\varphi_2).$$

Also, for $z \in R$, $(z\varphi)(1+(r)) = z(a+(s)) = za + (s)$. So

$$f(z\varphi) = \frac{za}{h} + (s) = z\left(\frac{a}{h} + (s)\right) = zf(\varphi).$$

Thus f is an R-module homomorphism.

Theorem 1. *For all $r, s \in R$; $r, s \neq 0$;*

$$\hom_R(R/(r), R/(s)) \approx R/(gcd(r,s))$$

where the set of module homomorphisms $hom_R(R/(r), R/(s))$ is endowed with the natural module structure (operations in the codomain).

Proof. We just need to show that the homomorphism f, defined as above, is bijective. Thus, suppose that $\varphi \in \ker f$. Then $\frac{a}{h} \in (d)$, $d = \gcd(r,s)$ and this implies that $s = dh \mid a$. Therefore, $\varphi(1+(r)) = a+(s) = (s)$, and φ is the zero homomorphism, i.e., $\ker f = \{0\}$. So, f is injective. Finally, to see that f is surjective, take any element $k+(d)$ and define φ by $\varphi(1+(r)) = kh + (s)$. Then,

$$rkh = rk\frac{s}{d} = \frac{r}{d}ks \in (s),$$

and by Lemma 1, $\varphi \in \hom_R(R/(r), R/(s))$. Furthermore, $f(\varphi) = \frac{kh}{h} + (d) = k + (d)$, showing that f is onto. This proves that f is an R-isomorphism of modules. □

A nice consequence of this theorem is that the number of homomorphisms is the same in both directions.

Now, we look at what happens when $r = 0$ or $s = 0$. When $r = 0$ and $s \neq 0$, the condition in Lemma 1 is always satisfied since $r = 0$, and thus $ra = 0 \in (s)$ is always true,

so every $\varphi(x+(r)) = xa+(s)$ is a homomorphism. Then, the map $\varphi \mapsto \varphi(1+(r))$ from $\hom_R(R/(r), R/(s))$ to $R/(s)$ is surjective, but also is an R-module homomorphism that is injective since the homomorphisms are defined by its value in $1+(r)$. Hence $\hom_R(R/(r), R/(s)) \approx R/(s)$. So, in this case the formula in Theorem 1 above holds if we take $\gcd(0, s) = s$.

When $r \neq 0$ and $s = 0$, the condition in Lemma 1 means that $ra = 0$, then $a = 0$, since $r \neq 0$. Hence, there is only one homomorphism, the trivial one. So, the symmetry fails.

Finally, when $r = s = 0, R/(r) \approx R/(s) \approx R$. It can be easily checked that $\hom_R(R, R) \approx R$, since $\hom_R(R, R)$ consist of all the functions $x \mapsto ax$, for $a \in R$.

Now, for the proof of Theorem 1, it is enough for R to be a GCD, that is, an integral domain in which any two nonzero elements have a gcd. As for the case where r or s is 0, it is enough to have an integral domain. For instance, this theorem applies to unique factorization domains, since they are GCD domains. It also applies to *Bezóut domains* — domains in which every finitely generated ideal is principal — because they are GCD domains, though not necessarily UFDs.

Theorem 1 tells us what happens to $\hom_R(M, M')$ when M, M' are cyclic modules. From here, we can generalize to the case when M, M' are finitely generated modules. In this case, say $M \approx R^m \times R/(r_1) \times R/(r_2) \times \cdots \times R/(r_k)$ and $M' \approx R^n \times R/(s_1) \times R/(s_2) \times \cdots \times R/(s_l)$ for some $m, n \geq 0$ and $r_1, r_2, \ldots, r_k, s_1, s_2, \ldots, s_l$ nonzero and nonunits (see [3, p. 225]). Of course, we can change R to $R/(0)$ and get $M \approx R/(r_1) \times R/(r_2) \times \cdots \times R/(r_k) \times R/(r_{k+1}) \times \cdots R/(r_{k+m})$ and $M' \approx R/(s_1) \times R/(s_2) \times \cdots \times R/(s_l) \times R/(s_{l+1}) \times \cdots \times R/(s_{l+n})$, where $r_i = 0$ for $i > k$ and $s_j = 0$ for $j > l$. Hence

$$\begin{aligned}\hom_R(M, M') &\approx \hom_R(\prod_{i=1}^{k+m} R/(r_i), \prod_{j=1}^{l+n} R/(s_j)) \\ &\approx \prod_{i=1}^{k+m}\prod_{j=1}^{l+n} \hom_R(R/(r_i), R/(s_j)).\end{aligned}$$

Now, looking at the different cases, we can conclude that

$$\hom_R(M, M') \approx [\prod_{i=1}^{k+m}\prod_{j=1}^{l} R/(\gcd(r_i, s_j))] \times R^{mn}.$$

But $\prod_{i=1}^{k+m}\prod_{j=1}^{l} R/(\gcd(r_i, s_j))$ can be reduced, since $r_i = 0$ for $i > k$, and therefore

$$\prod_{i=1}^{k+m}\prod_{j=1}^{l} R/(\gcd(r_i, s_j)) \approx [\prod_{i=1}^{k}\prod_{j=1}^{l} R/(\gcd(r_i, s_j))] \times [\prod_{j=1}^{l}(R/(s_j))^m].$$

Thus we have

Theorem 2. *Let R be a principal ideal domain and let M, M' be finitely generated R-modules. Then*

$$\hom_R(M, M') \approx [\prod_{i=1}^{k}\prod_{j=1}^{l} R/(\gcd(r_i, s_j))] \times [\prod_{j=1}^{l}(R/(s_j))^m] \times R^{mn}$$

where $M \approx R^m \times R/(r_1) \times R/(r_2) \times \cdots \times R/(r_k)$ and $M' \approx R^n \times R/(s_1) \times R/(s_2) \times \cdots \times R/(s_l)$ with $m, n \geq 0$ and $r_1, r_2, \ldots, r_k, s_1, s_2, \ldots, s_l$ nonzero and nonunits.

3. Algebra homomorphisms

The R-algebra homomorphisms are not required to preserve identity and the 0 homomorphism is allowed.

Suppose that $s \neq 0$ and that s is not a unit, consider $R/(r)$ and $R/(s)$ as R-algebras, and let $\psi : R/(r) \to R/(s)$ a map. If ψ is an R-algebra homomorphism, then ψ is also an R-module homomorphism, so $\psi(x + (r)) = xa + (s)$ for some $a \in R$ with $ra \in (s)$. Thus, in the same way as for homomorphisms of R-modules, we need to find the values of $a + (s) \in R/(s)$ such that $\psi(x + (r)) = xa + (s)$ is a homomorphism of R-algebras.

Also

$$a + (s) = \psi(1 + (r)) = \psi((1 + (r))^2) = a^2 + (s),$$

so $a^2 - a \in (s)$. We will see that these necessary conditions, $ra \in (s)$ and $a^2 - a \in (s)$, are also sufficient for a function $\psi : R/(r) \to R/(s)$ to be a homomorphism of R-algebras. Thus, suppose $ra \in (s)$ and $a^2 - a \in (s)$. We already know that ψ is well defined, and also that ψ is an R-module homomorphism, since $ra \in (s)$. Also, since $a^2 - a \in (s)$ then $xya^2 - xya = xy(a^2 - a) \in (s)$, so

$$\psi((x + (r))(y + (r))) = xya + (s) = xya^2 + (s) = \psi(x + (r))\psi(y + (r)).$$

Therefore φ is an R-algebra homomorphism. We have proved the following lemma.

Lemma 2. *The function $\varphi : R/(r) \to R/(s)$ given by $\psi(x + (r)) = xa + (s) = (x + (s))(a + (s)), a \in R$ is an R-algebra homomorphism if and only if*

$$ra \in (s),$$
$$a^2 - a \in (s).$$

To find the number of such $a + (s)$ that satisfy these conditions, which are equivalent to $r(a + (s)) = 0 + (s)$ and $(a + (s))^2 - (a + (s)) = 0 + (s)$, we need to prove the next theorem.

Theorem 3. *Let $f_1(x), f_2(x), \ldots, f_k(x) \in R[x]$, and for any $s \in R, s \neq 0$, let $N(s)$ denote the set of $x + (s) \in R/(s)$ such that*

$$\begin{aligned} f_1(x + (s)) &= 0 + (s) \\ f_2(x + (s)) &= 0 + (s) \\ &\vdots \\ f_k(x + (s)) &= 0 + (s). \end{aligned}$$

If $s = s_1 s_2$ where $\gcd(s_1, s_2) = 1$, then $|N(s)| = |N(s_1) \times N(s_2)|$. Furthermore, if s is not a unit, let $s = u \prod p^{\alpha}$ be a factorization of s with u a unit, then $|N(s)| = |\prod N(p^{\alpha})|$.

Proof. Since we are in a principal ideal domain, $(s_1) + (s_2) = (\gcd(s_1, s_2)) = (1) = R$. Then, by the *Chinese Remainder Theorem* (see [3, p. 131]) the map $x \mapsto (x+(s_1), x+(s_2))$ from R to $R/(s_1) \times R/(s_2)$ is a epimorphism. This induces the isomorphism $\theta : R/(s_1) \cap (s_2) \to R/(s_1) \times R/(s_2)$, given by $\theta(x + (s_1) \cap (s_2)) = (x + (s_1), x + (s_2))$. Of course, $(s_1) \cap (s_2) = (s_1 s_2) = (s)$.

Now, for $x + (s) \in N(s)$, $\theta(x + (s)) = (x + (s_1), x + (s_2)) \in N(s_1) \times N(s_2)$, then $\theta(N(s)) \subseteq N(s_1) \times N(s_2)$. Also, for $(y_1 + (s_1), y_2 + (s_2)) \in N(s_1) \times N(s_2)$, let $x + (s) = \theta^{-1}(y_1 + (s_1), y_2 + (s_2))$. So, $x + (s_1) = y_1 + (s_1)$ and $x + (s_2) = y_2 + (s_2)$; it follows that $x + (s) \in N(s)$. Hence $N(s_1) \times N(s_2) \subseteq \theta(N(s))$. We conclude that $\theta(N(s)) = N(s_1) \times N(s_2)$.

But θ is a bijection, thus when restricted to $N(s)$ we get a bijection from $N(s)$ to $\theta(N(s)) = N(s_1) \times N(s_2)$. Hence $|N(s)| = |N(s_1) \times N(s_2)|$.

By repeatedly applying this argument to the prime factorization of s, we obtain that $|N(s)| = |N(u) \prod N(p^{\alpha})|$, but clearly $|N(u)| = 1$, so we have the second assertion of the theorem. □

Now, we use this theorem with the polynomials $f_1(a) = ra$ and $f_2(a) = a^2 - a$ by first finding the number of solutions for some p^{α}, with p prime and $\alpha > 0$ an integer, and then using the last part of Theorem 3.

Let p be a prime element in R and $\alpha > 0$ an integer, then $a(a-1) = a^2 - a \in (p^{\alpha})$ has two solutions $0, 1$. This is so since $\gcd(a, a-1) = 1$, just one of them can be divisible by p, then $\gcd(p^{\alpha}, a) = 1$ or $\gcd(p^{\alpha}, a-1) = 1$. If $\gcd(p^{\alpha}, a) = 1$, then $p^{\alpha} | a - 1$, so $a + (p^{\alpha}) = 1 + (p^{\alpha})$. In the other case, $p^{\alpha} | a$, so $a + (p^{\alpha}) = 0 + (p^{\alpha})$.

But, $f_1(1 + (p^{\alpha})) = r(1 + (p^{\alpha})) = 0 + (p^{\alpha})$ if and only if $p^{\alpha} | r$, while $0 + (p^{\alpha})$ is always a solution. Thus, the system

$$\begin{aligned} ra &= 0 + (p^{\alpha}), \\ a^2 - a &= 0 + (p^{\alpha}) \end{aligned}$$

has two solutions if $p^{\alpha} | r$; otherwise, it has only one solution.

Now, if $s = u p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ is a prime factorization of s, with u a unit, the number of solutions to $f_1(a) = 0 + (p_i^{\alpha_i})$ and $f_2(a) = 0 + (p_i^{\alpha_i})$ is two if $p_i^{\alpha_i} | r$, and one, if $p_i^{\alpha_i} \not| r$.

So the number of solutions is 2^ℓ, where $\ell = |\{i : p_i^{\alpha_i}|r\}|$ is the number of elements in the set $\{i : p_i^{\alpha_i}|r\}$.

Theorem 4. *Let $s = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ be a prime factorization of s. The number of algebra homomorphisms $\psi : R/(r) \to R/(s)$ is 2^ℓ, where $\ell = |\{i : p_i^{\alpha_i}|r\}|$.*

In the case that s is a unit, clearly the only homomorphism is the zero homomorphism.

And if $s = 0$, then $R/(s) \approx R$, since $f(1)^2 = f(1)$, $f(1) = 0, 1$, because in R these are the only two solutions to $x^2 - x = 0$. Now, if $r = 0$, we get two homomorphisms the zero homomorphism and the identity. And, if $r \neq 0$ the fact that $rf(1) \in (s)$ implies that $f(1) = 0$, so we only have the zero homomorphism.

Acknowledgments

We are very grateful to the referee because his/her comments and suggestions allowed us to broaden the scope of this article.

References

[1] J. Diaz-Vargas and G. Vargas de los Santos, *The number of homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$*, Abstraction & Application **13** (2015), 1-3.

[2] J. A. Gallian and J. Van Buskirk, *The number of homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$*, Amer. Math. Monthly **91** (1984), no. 3, 196-197.

[3] T. W. Hungerford, *Algebra*, Springer-Verlag, 1989.

[4] J. Jhonson, *The number of group homomorphisms from D_m into D_n*, The College Mathematics Journal **44**, no. 3 (May 2013), 190-192.

[5] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An introduction to the theory of numbers*, Fifth Edition, John Wiley & Sons, Inc., 1991.

Recibido en marzo de 2016. Aceptado para publicación en septiembre de 2016.

JAVIER DIAZ-VARGAS
FACULTAD DE MATEMÁTICAS
UNIVERSIDAD AUTÓNOMA DE YUCATÁN
MÉRIDA, MÉXICO
e-mail: javier.diaz@correo.uady.mx

GUSTAVO VARGAS DE LOS SANTOS
FACULTAD DE MATEMÁTICAS
UNIVERSIDAD AUTÓNOMA DE YUCATÁN
MÉRIDA, MÉXICO
e-mail: tavov12@hotmail.com