Counting Homomorphism between Rings

Vinod S[1, 3, *],Biju G S[2,3] and N Ganesh[2,3]
[1]Department of Mathematics, Government College for Women, Thiruvananthapuram, Kerala, INDIA
[2]Department of Mathematics, College of Engineering, Thiruvananthapuram, Kerala, INDIA
[3]Department of Collegiate Education, Kerala, INDIA.

Abstract: A function between two rings preserve both additive and multiplicative structure is called a ring homomorphism. In this paper we characterize and compute all ring homomorphism from $\mathbb{R}^n$ to $\mathbb{R}^m$.

Keywords: ***Homomorphism, Rings, idempotent elements, integral domain, continuous function.***

1. INTRODUCTION

Finding the number of ring homomorphism between two rings is a basic problem in abstract algebra. Given two finite rings, is it possible to determine the ring homomorphism between them? Certainly if the rings were specific enough, then answer to the question is easy. But we are given two finite rings on the general form, the answer is much difficult. The subject of ring homomorphism is well studied in the introductory course on abstract algebra, butvery little research has been done in this area.

In 1984, Joseph Gallian and Games Van Buskrik determined the number of ring homomorphism from $\mathbb{Z}_m$ to $\mathbb{Z}_n$,where m and n are natural numbers[2]. After four years, Gallian and Jungreis[6] determined all ring homomorphisms between $Z_m[i]$ into $Z_n[i]$ where $i^2 + 1 = 0$ and also the number of ring homomorphisms between rings of the form $Z_m[\rho]$ into $Z_n[\rho]$, where $\rho^2 + \rho + 1 = 0$.In 2010, Alex Cameron[1] compute the number of ring homomorphisms between the rings of the form $Z_m[\rho]$ into $Z_n[\rho]$, where $\rho^2 + 2 = 0$ and as a consequence he also compute the number of ring homomorphisms from $Z_m[\rho]$ into $Z_n[\rho]$, where $\rho^2 - 2 = 0$. In [2], Mohammad Saleh and Hasan Yousef compute and characterize the ring homomorphisms from $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_r}$ into $\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \dots \times \mathbb{Z}_{k_s}$, a result that generalizes [1]. In this paper we characterize and compute all ring homomorphism from $\mathbb{Z}^n$ to $\mathbb{Z}^m$, $\mathbb{Q}^n$ to $\mathbb{Q}^m$ and $\mathbb{R}^n$ to $\mathbb{R}^m$.

2.

2. NOTATIONS AND BASIC RESULTS.

Most of the notations, functions and terms we mentioned below are standard and can be found in [3]

or [6].We use the following standard Notations : $\mathbb{N}$ the set of natural numbers, $\mathbb{Z}$ the set of integers, $\mathbb{Q}$ the set of rational numbers and $\mathbb{R}$ the set of real number . Also for any ring R and for any natural number n, denote $\mathbb{R}^n$ for the ring of n- copies of $\mathbb{R}$. Let R_1 and R_2 be two rings. We denote Hom $(R_1: R_2)$ for the ring of all homomorphisms from R_1 to R_2 and |Hom $(R_1: R_2)$| for the cardinality of Hom $(R_1: R_2)$.

Now we prove some basic results in ring homomorphism.

Theorem2.1: Let R and S be two rings and $\phi: R \to S$ be a ring homomorphism. If x is an idempotent element of R then $\phi(x)$ is an idempotent elements of S.

Proof: Let x is an idempotent element of R. Then $x^2 = x$ .Since $\phi: R \to S$ be a ring homomorphism

$\phi(x) = \phi(x^2) = \phi(x)\phi(x)$. Hence $\phi(x)$ is an idempotent element of S.

Theorem2.2: The idempotent elements of an integral domain D are 0 and 1(unity of D).
Proof: Let a be an idempotent element of the integral domain D. Then $a = a^2$ and hence $a(a-1) = 0$. Since D has no zero divisors, we have either $a = 0$ or $a = 1$.

3. MAIN RESULTS

Now we are going to prove our main results.

Lemma 3.1: Let R and $R_i (1 \le i \le n)$ are rings, then $|Hom(R: \prod_{i=1}^n R_i)| = |\prod_{i=1}^n Hom(R: R_i)|$

Proof: Let $f_i: R \to R_i (1 \le i \le n)$ be a ring homomorphism. Define a function $f: R \to \prod_{i=1}^n R_i$ by $f(x) =$

$\big(f_1(x), f_2(x), \dots, f_n(x)\big)\ \forall\, x \in R$. Then for $x, y \in R$;

$$f(x)f(y) = \big(f_1(x), f_2(x), \dots, f_n(x)\big)\big(f_1(y), f_2(y), \dots, f_n(y)\big)$$

$$= \big(f_1(x)f_1(y), f_2(x)f_2(y), \dots, f_n(x)f_n(y)\big)$$

$= (f_1(xy), f_2(xy), \ldots, f_n(xy))$

$= f(xy).$

Also $f(x+y) = \big(f_1(x+y), f_2(x+y), \ldots, f_n(x+y)\big)$

$= (f_1(x)+f_1(y), f_2(x)+f_2(y), \ldots, f_n(x)+f_n(y))$

$= \big(f_1(x), f_2(x), \ldots, f_n(x)\big) + \big(f_1(y), f_2(y), \ldots, f_n(y)\big)$

$= f(x) + f(y)$

Hence $f: R \to \prod_{i=1}^{n} R_i$ is a ring homomorphism.

Conversely let $h: R \to \prod_{i=1}^{n} R_i$ be a ring homomorphism where $h(x) = \big(h_1(x), h_2(x), \ldots, h_n(x)\big)\ \forall\, x \in R$.

Then for $x, y \in R$,

$\big(h_1(x+y), h_2(x+y), \ldots, h_n(x+y)\big) = h(x+y)$

$= h(x) + h(y)$, since h is homomorphism

(A) $= \big(h_1(x), h_2(x), \ldots, h_n(x)\big) + \big(h_1(y), h_2(y), \ldots, h_n(y)\big)$

$= \big(h_1(x)+h_1(y), h_2(x)+h_2(y), \ldots, h_n(x)+h_n(y)\big)$

Also $\big(h_1(xy), h_2(xy), \ldots, h_n(xy)\big) = h(xy)$

$= h(x).h(y)$

(B) $= \big(h_1(x), h_2(x), \ldots, h_n(x)\big)\big(h_1(y), h_2(y), \ldots, h_n(y)\big)$

$= \big(h_1(x)h_1(y), h_2(x)h_2(y), \ldots, h_n(x)h_n(y)\big)$

Hence from (A) and (B), $h_i: R \to R_i (1 \le i \le n)$ is a ring homomorphism.

Now we define a function $\psi: Hom(\mathrm{R}: \prod_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{R_i}) \to \prod_{i=1}^{n} Hom(R: R_i)$ by $\psi(h) = (h_1, h_2, \ldots, h_n)\ \forall\, h \in Hom(\mathrm{R}: \prod_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{R_i})$; where $h(x) = \big(h_1(x), h_2(x), \ldots, h_n(x)\big)\ \forall\, x \in R.$ Now it is clear that ψ is a bijection and $|Hom(\mathrm{R}: \prod_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{R_i})| = |\prod_{i=1}^{n} Hom(R: R_i)|$.

First we will characterize all ring homomorphisms and the number of ring homomorphisms from $\mathbb{Z}^n$ to $\mathbb{Z}^m$.

Theorem3.1: The number of ring homomorphism from $\mathbb{Z}^n$ to $\mathbb{Z}$ is $n+1$.

Proof: Let $\phi: \mathbb{Z}^n \to \mathbb{Z}$ be a ring homomorphism. For $1 \le i \le n$; denote e_i for the n-tuple whose i^{th}component is 1 and 0's elsewhere. Since $e_i$is an idempotent and ϕ is a ring homomorphism $\phi(e_i)$ is an idempotent element in $\mathbb{Z}$ and hence $\phi(e_i) = 0$ *or* 1. Also $\phi(e_i) = \phi(e_j) = 1$ for some $i \ne j$ then we have a contradiction,

$$0 = \phi(0) = \phi(e_i e_j) = \phi(e_i)\phi(e_j) = 1.1 = 1.$$

Thus $\phi(e_i)$ assume the value 1 for at most one value of i.

If $\phi(e_i) = 0\ \forall\, i (1 \le i \le n)$,then for any $x = (x_1, x_2, \ldots, x_i, \ldots, x_n) \in \mathbb{Z}^n$;

$\phi(x) = \phi(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} \phi(x_i e_i) = \sum_{i=1}^{n} x_i \phi(e_i) = 0$ and hence ϕ is the trivial ring homomorphism.

If $\phi(e_k) = 1$ *and* $\phi(e_i) = 0\ \forall\, i \ne k$,then for any $x = (x_1, x_2, \ldots, x_k, \ldots, x_n) \in \mathbb{Z}^n$;

$\phi(x) = \phi(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} \phi(x_i e_i) = \sum_{i=1}^{n} x_i \phi(e_i) = x_k$.

Also it is clear that the map $\phi(x) = \phi(x_1, x_2, \ldots, x_k, \ldots, x_n) = x_k$ is a ring homomorphism. Hence n such non-trivial homomorphisms are there. So the number of Ring homomorphisms from $\mathbb{Z}^n$ to $\mathbb{Z}$ is $n+1$.

Theorem3.2: The number of distinct ring homomorphisms from $\mathbb{Z}^n$ to $\mathbb{Z}^m$ is $(n+1)^m$.

Proof: The number of ring homomorphism from $\mathbb{Z}^n$ to $\mathbb{Z}$ is $n+1$. Hence from Theorem 2.3, the number of distinct ring homomorphism from $\mathbb{Z}^n$ to $\mathbb{Z}^m$ is $(n+1)^m$.

Now we will characterize all ring homomorphism and the number of ring homomorphism from $\mathbb{Q}^n$ to $\mathbb{Q}^m$.

Theorem3.3: The number of distinct ring homomorphism from $\mathbb{Q}^n$ to $\mathbb{Q}$ is $n+1$.

Proof: Let $\phi: \mathbb{Q}^n \to \mathbb{Q}$ be a ring homomorphism. For $1 \le i \le n$; denote e_i for the n-tuple whose i^{th}component is 1 and 0's elsewhere. Since $e_i$is an idempotent and ϕ is a ring homomorphism $\phi(e_i)$ is an idempotent element in $\mathbb{Q}$ and hence $\phi(e_i) = 0 \; or \; 1$. Also $\phi(e_i) = \phi(e_j) = 1$ for some $i \ne j$ then we have a contradiction

$$0 = \phi(0) = \phi(e_i\, e_j) = \phi(e_i)\phi(e_j) = 1.1 = 1.$$

Thus $\phi(e_i)$ assume the value 1 for at most one value of i.

Step1: $\phi(ne_i) = n\phi(e_i) \; \forall \, n \in \mathbb{Z} \; and \; \forall \, 1 \le i \le n$.

The argument is clear since ϕ is a ring homomorphism and $n \in \mathbb{Z}$.

Step2: $\phi(re_i) = r\phi(e_i) \; \forall \, r \in \mathbb{Q} \; and \; \forall \, 1 \le i \le n$.

let $= \frac{p}{q}$, where $p \in \mathbb{Z} \; and \; q \in \mathbb{N}$. Then $rq = p$ and hence $rq\, e_i = p\, e_i$.

So $\phi(rq\, e_i) = \phi(p\, e_i) => q\phi(r\, e_i) = p\phi(e_i) => \phi(r\, e_i) = \frac{p}{q}\phi(e_i) =>$

$\phi(re_i) = r\phi(e_i) \; \forall \, r \in \mathbb{Q} \; and \; \forall \, 1 \le i \le n$.Hence the proof of step 2 is over.

Step3: Characterize all ring homomorphisms from $\mathbb{Q}^n$ to $\mathbb{Q}$

If $\phi(e_i) = 0 \;\; \forall \, i, then$ for any $= (x_1, x_2, \dots, x_i, \dots, x_n) \in \mathbb{Q}^n$;

$\phi(x) = \phi(\sum_{i=1}^n x_i\, e_i) = \sum_{i=1}^n \phi(x_i\, e_i) = \sum_{i=1}^n x_i\, \phi(e_i) = 0$. Hence ϕ is the trivial ring homomorphism.

If $\phi(e_k) = 1 \; and \; \phi(e_i) = 0 \;\; \forall \, i \ne k$ then for any $x = (x_1, x_2, \dots, x_k, \dots, x_n) \in \mathbb{Q}^n$;

$\phi(x) = \phi(\sum_{i=1}^n x_i\, e_i) = \sum_{i=1}^n \phi(x_i\, e_i) = \sum_{i=1}^n x_i\, \phi(e_i) = x_k$. Also it is clear that the map $\phi(x) =$

$\phi(x_1, x_2, \dots, x_k, \dots, x_n) = x_k$ is a ring homomorphism. Hence n such non-trivial homomorphisms are there. So the number of ring homomorphism from $\mathbb{Q}^n$ to $\mathbb{Q}$ is $n+1$.

Theorem3.3: The number of distinct ring homomorphism from $\mathbb{Q}^n$ to $\mathbb{Q}^m$ is $(n+1)^m$.

Proof: The number of ring homomorphism from $\mathbb{Q}^n$ to $\mathbb{Q}$ is $n+1$.. Hence from Theorem 2.3, the number of distinct ring homomorphism from $\mathbb{Q}^n$ to $\mathbb{Q}^m$ is $(n+1)^m$.

Now we will characterize all ring homomorphism and the number of ring homomorphisms from $\mathbb{R}^n$ to $\mathbb{R}^m$.

Theorem3.4: The number of distinct ring homomorphism from and $\mathbb{R}^n$ to $\mathbb{R}$ is $n+1$.

Proof: Let $\phi: \mathbb{R}^n \to \mathbb{R}$ be a ring homomorphism. For $1 \le i \le n$; denote e_i for the n-tuple whose i^{th}component is 1 and 0's elsewhere. Since $e_i$is an idempotent and ϕ is a ring homomorphism $\phi(e_i)$ is an idempotent element in $\mathbb{R}$ and hence $\phi(e_i) = 0 \; or \; 1$. Also $\phi(e_i) = \phi(e_j) = 1$ for some $i \ne j$ then we have a contradiction

$$0 = \phi(0) = \phi(e_i\, e_j) = \phi(e_i)\phi(e_j) = 1.1 = 1.$$

Thus $\phi(e_i)$ assume the value 1 for at most one value of i.

Step1: $\phi(ne_i) = n\phi(e_i) \; \forall \, n \in \mathbb{Z} \; and \; \forall \, 1 \le i \le n$.

The argument is clear since ϕ is a ring homomorphism and $n \in \mathbb{Z}$.

Step2: $\phi(re_i) = r\phi(e_i) \; \forall \, r \in \mathbb{Q} \; and \; \forall \, 1 \le i \le n$.

Let r $= \frac{p}{q}$, where $p \in \mathbb{Z} \; and \; q \in \mathbb{N}$. Then $rq = p$ and hence $rq\, e_i = p\, e_i$.

So $\phi(rq\, e_i) = \phi(p\, e_i) => q\phi(r\, e_i) = p\phi(e_i) => \phi(r\, e_i) = \frac{p}{q}\phi(e_i) =>$

$\phi(re_i) = r\phi(e_i) \; \forall \, r \in \mathbb{Q} \; and \; \forall \, 1 \le i \le n$.Hence the proof of step 2 is over.

Step3: For $a < b$ and $a, b \in \mathbb{R}$, $\phi(ae_i) \leq b\phi(e_i)\ \forall\ 1 \leq i \leq n$.

Since $a < b$ and $a, b \in \mathbb{R}$, we have $b - a > 0$.So $b - a = t^2$, for some $t \in \mathbb{R}$.

This imply$(b - a)\, e_i = t^2\, e_i = t^2\, e_i{}^2 = t\, e_i . t\, e_i$, since $e_i{}^2 = e_i$.

Hence $\phi\big((b - a)\, e_i\big) = \phi(t\, e_i . t\, e_i) = \phi(t\, e_i)\phi(t\, e_i) = [\phi(t\, e_i)]^2 \geq 0$

This gives $\phi\big((b - a)\, e_i\big) = \phi(b\, e_i) - \phi(a\, e_i) \geq 0$

That is $\phi(ae_i) \leq b\phi(e_i)\ \forall\ 1 \leq i \leq n$ and the step 3 is completed.

Step4: $\phi: \mathbb{R}^n \to \mathbb{R}$ is continuous.

Let $a = (a_1, a_2, \dots, a_n) \in \mathbb{R}^n$ and $\varepsilon > 0$ be given.

Chose a rational number r $such$ $that$ $0 < r < \varepsilon$. Then for any $y = (y_1, y_2, \dots, y_n) \in$ B(a ; r),

where B(a ; r) denote the open ball centered at a and radius r in $\mathbb{R}^n$, we have

$$|y_i - a_i| < r\ \forall\ 1 \leq i \leq n$$

$$=> \quad -r < y_i - a_i < r$$

$$=> \quad -r < y_i - a_i < r$$

$$=> \quad \phi(-r\, e_i) < \phi((y_i - a_i)\, e_i) < \phi(r\, e_i)\ \ \forall\ i\ (1 \leq i \leq n) \quad \text{; by step 3.}$$

$$=> \quad -r\,\phi(e_i) < \phi(y_i\, e_i - a_i\, e_i) < r\phi(e_i)\ \ \forall\ i\ (1 \leq i \leq n\,) \ \text{; by step 2.}$$

$$=> \quad -r\,\phi(e_i) < \phi(y_i\, e_i) - \phi(a_i\, e_i) < r\phi(e_i)\ \ \forall\ i\ (1 \leq i \leq n)$$

$$=> \quad |\phi(y_i\, e_i) - \phi(a_i\, e_i)| < r\phi(e_i)\ \forall\ i\ (1 \leq i \leq n)$$

$$=> \quad |\phi(y_i\, e_i) - \phi(a_i\, e_i)| < r\ \ \forall\ i\ (1 \leq i \leq n)\ \text{; since } \phi(e_i) = 0\ or\ 1$$

$$=> \quad |\phi(y_i\, e_i) - \phi(a_i\, e_i)| < r\ \ \forall\ i\ (1 \leq i \leq n)$$

$$=> \quad |\phi(y_i\, e_i) - \phi(a_i\, e_i)| < r < \frac{r}{n} < \frac{\varepsilon}{n}\ \ \forall\ i\ (1 \leq i \leq n)\text{......(A)}$$

$$\begin{aligned}
\text{Hence}\quad |\phi(y) - \phi(a)| &= |\phi((y_1, y_2, \dots, y_n)) - \phi((a_1, a_2, \dots, a_n))| \\
&= |\phi(\textstyle\sum_{i=1}^{n} y_i\, e_i) - \phi(\sum_{i=1}^{n} a_i\, e_i)| \\
&= |(\textstyle\sum_{i=1}^{n} \phi(y_i\, e_i) - (\sum_{i=1}^{n} \phi(a_i\, e_i)| \\
&= |(\textstyle\sum_{i=1}^{n} \phi(y_i\, e_i) - \phi(a_i\, e_i)| \\
&\leq \textstyle\sum_{i=1}^{n} |\phi(y_i\, e_i) - \phi(a_i\, e_i)| \ \text{; by triangle inequality of } \mathbb{R} \\
&\leq \textstyle\sum_{i=1}^{n} \frac{\varepsilon}{n} = \varepsilon \ \text{; by (A) above.}
\end{aligned}$$

Thus $\phi: \mathbb{R}^n \to \mathbb{R}$ is continuous and the step 4 is completed.

Step5: $\phi(xe_i) = x\phi(e_i)\ \forall\ x \in \mathbb{R}$ and $\forall\ 1 \leq i \leq n$.

Let $x \in \mathbb{R}$ and $\forall\ 1 \leq i \leq n$. Then there exist a rational sequence r_m such that $r_m \to x$ in $\mathbb{R}$.

Then $r_m\, e_i \to x\, e_i$ in the space $\mathbb{R}^n$. Sine ϕ is continuous at x, we have ,

$\phi(x\, e_i) = \lim_{m\to\infty} \phi(r_m\, e_i) = (\lim_{m\to\infty} r_m)\phi(e_i) = x\phi(e_i)$ and hence step 5 is over.

Step6: Characterize all ring homomorphism from $\mathbb{R}^n$to$\mathbb{R}$.

Let $x = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$. If $\phi(e_i) = 0\ \ \forall\ i(1 \leq i \leq n)$;

Then, $\phi(x) = \phi(\sum_{i=1}^{n} x_i\, e_i) = \sum_{i=1}^{n} \phi(x_i\, e_i) = \sum_{i=1}^{n} x_i\phi(e_i) = 0$ and hence ϕ

is the trivial ring homomorphism. Otherwise, $ie,$ If $\phi(\, e_k) = 1$ and If $\phi(\, e_i) = 0\ \ \forall\, i \neq k;$

$$\phi(x) = \phi(x_1\,, x_2\,, \dots\,, x_n) = \phi(\textstyle\sum_{i=1}^{n} x_i\, e_i) = \sum_{i=1}^{n} \phi(x_i\, e_i) = \sum_{i=1}^{n} x_i \phi(\, e_i) = x_k \phi(\, e_k) = x_k.$$

Clearly ϕ is a ring homomorphism. Hence non-trivial ring homomorphism from $\mathbb{R}^n$ to $\mathbb{R}$ has the form

$\phi(x_1\,, x_2\,, \dots\,, x_n) = x_k;(1 \leq k \leq n)$. So the number of ring homomorphisms from $\mathbb{R}^n$ to $\mathbb{R}$ is $n + 1$.

Theorem3.5: The number of distinct ring homomorphism from $\mathbb{R}^n$ to $\mathbb{R}^m$is $(n + 1)^m$.

Proof: The number of ring homomorphism from $\mathbb{R}^n$ to $\mathbb{R}$ is $n + 1$. Hence from Theorem 2.3, the number of distinct ring homomorphism from $\mathbb{R}^n$ to $\mathbb{R}^m$ is $(n + 1)^m$.

REFERENCES

[1] Alex Cameron, *"Counting ring homomorphisms*", IIME Journal, *Volume*13, No. 2, 65-67

[2] J.A. Gallian and J. Van Buskrik, *The number of homomorphisms from* $\mathbb{Z}_m$ *to* $\mathbb{Z}_n$, Amer. Math. Monthly 91(1984)196-197

[3] J.A Gallian, *Contemporary Abstract Algebra*, D.C.Heath and Company. 3rd Edition,1994

[4] J. A. Gallian and D. S. Jungreis, "*Homomorphisms from* $Z_m[i]$ *into* $Z_n[i]$ *and* $Z_m[\rho]$ *into* $Z_n[\rho]$*, where* $i^2 + 1 = 0$ *and* $\rho^2 + \rho + 1 = 0$" American Mathematical Monthly 95(1988), 247−299.

[5] H. Kestleman, *Automorphisms of the field of complex numbers*, Proceedings of the London Mathematical Society (2), 53,1951, 1-12

[6] M. Misaghian, *"Factor Rings and their decompositions in the Eisenstein integers Ring Z[ω]",* American Journal Of Mathematics 5 No. 1 (2013): 58−68

[6] Mohmmad saleh and Hassan Yousef, *The American Mathematical Monthly*, 105(1998)259-260

[7] M. Saleh, H. Yousef, and J. Abu Hlail, *"The number of ring homomorphisms from* $Z_n[\xi] \times Z_m[\xi]$ *into* $Z_k[\xi]$, An-Najah J., 2000, 47−53

[8] Paul B Yale, *Automorphisms of the complex numbers*, Mathematic Magazine,*Volume* 39, No3(may 1966), 135-147

[9] Tom M. Apostol, *Mathematical Analysis*, Addition-Wesley Publishing Company. 1974, 2nd Edition