On Skew-Morphisms of Rings

By

Saima Aslam

**Department of Mathematics & Statistics
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad
Pakistan
2017**

Morphisms (Mathematics)

Cyclic groups

Linear algebraic groups

On Skew-Morphisms of Rings

By

Saima Aslam

Supervised by

Dr. Sajida Kousar

Department of Mathematics & Statistics
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad
Pakistan
2017

On Skew-Morphisms of Rings

By

Saima Aslam

A Dissertation
Submitted in the Partial Fulfillment of the
Requirements for the Degree of
MASTER OF SCIENCE
IN
MATHEMATICS

Supervised by

Dr. Sajida Kousar

Department of Mathematics & Statistics
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad
Pakistan
2017

Certificate

On Skew-Morphisms of Rings

By

Saima Aslam

A DISSERTATION SUBMITTED IN THE PARTIAL FULFILLMENT OF THE

REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN MATHEMATICS

We accept this dissertation as confirming to the required standard

1. ______________________
Dr. Sajida Kousar
(supervisor)

2. ______________________
Dr. Tahir Mahmood
(Internal Examiner)

3. ______________________
Dr. Khadija Maqbool
(Chairperson)

4. ______________________
Prof. Dr. Muhammad Shabir
(External Examiner)

Department of Mathematics & Statistics
Faculty of Basic & Applied Sciences
International Islamic University, Islamabad
Pakistan
2017

Forwarding Sheet by Research Supervisor

The Thesis entitled ***On Skew-Morphisms of Rings*** submitted by ***Saima Aslam*** Reg. No 252-FBAS/MSMA/F15 in partial fulfillment of MS Degree in Mathematics has been completed under my guidance and supervision. I am satisfied with the quality of her research work and allow her to submit this thesis for further process to graduate with Master of Science degree from the Department of Mathematics & Statistics, as per IIUI rules and regulations.

Date ....

Dr. Sajida Kousar
Assistant Professor
Department of Maths & Stats,
International Islamic University,
Islamabad.

Dedicated to

My Parents

Abstract

The skew morphism of a group G is used to decompose G into disjoints sets A and B where both A and B are subgroups of G such that $A \cap B = \{1\}$ and $AB = G$. In mathematics, a ring is one of the fundamental algebraic structures used in abstract algebra. It consists of a set equipped with two binary operations that generalize the arithmetic operations of addition and multiplication. Through this generalization, theorem from arithmetic is extended to non-numerical objects such as polynomials, series, matrices and functions.

In our work we will present a number of previously unknown properties of skew morphism of rings. We will also prove a number of theorems about skew morphism of ring which will extend recent theorems of Conder [4].

The concept of structure preserving maps commonly known as homomorphism between two algebraic structures was widely discussed by many algebraists. Skew-morphisms are different from the conventional homomorphism. In skew-morphisms rather than multiplying the images the power functions are used. It helps to answers the problems that are not solved by the usual homomorphism.

In 2002, Jajcay and Siran discussed the decomposition of skew-morphism of cyclic groups. They addressed one of the central problems of the theory of regular maps, that is, the problem of classification of finite group admitting a regular Cayley Map.

1.Kovacs, R. Nedela, 2011 discussed the decomposition of skew-morphism of cyclic groups.

The dihedral group Dn, that is, the group formed by rotation and reflections of a regular n-gon is a non-abelain solvable group with many applications in geometry. Zhang and Du, 2016 introduced the skew-morphisms of dihedral groups.

In the year 2016, Conder et al., determined the cyclic complements and skew morphism of groups.

Using the existing literature here we want to establish a link between skew-morphism of groups and skew-morphism of rings. The thesis is divided into three chapters.

Chapter 1, is essentially an introduction. It is survey aimed at recalling some basic definitions and facts of groups, rings, ideals and ring homomorphism.

Chapter 2, deals with skew-morphism of groups and we also introduce the concept of Kernel and Fix of skew-morphism of groups. While some important results and skew-morphism of direct product are also presented in this chapter.

Chapter 3, concerned with study of skew-morphism of rings. Here we present the Kernel and Fix of skew-morphism of rings. In this chapter we also deal with some important results, finite examples and skew-morphism of direct products.

Author's Declaration

I hereby declare that thesis neither as a whole nor as a part has been copied from any source. It is further declared that I have prepared this thesis entirely on basis of my personal efforts made under the sincere guidance of my kind supervisor. No portion of work presented in this thesis has been submitted in support of an application for any degree or qualification of this or any other institute of learning.

Saima Aslam
MS Mathematics
Reg.No 252-FBAS/MSMA/F15
Department of Mathematics and Statistics
Faculty of Basic and Applied Sciences
International Islamic University Islamabad, Pakistan.

a finite number of elements. The number of elements in group G is called the order of G, denoted by $|G|$. Otherwise if the set G contains infinite number of elements then it is said to be an infinite group. Let for an element a of group G if $a^n = e$ for some positive integer n, then tbe smallest such positive integer is called the order of a and is denoted by $|a|$.

Example 1.1.2. 1. The set $G = \{e, a\}$ where the operation of multiplication is defined as

·	e	a
e	c	a
a	a	e

is an abelian group.

2. Under the operation of usual addition the set of all integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ are examples of abelian groups .

3. The set of all matrices whose order is $n \times m$ denoted by $M_{n\times m}(G)$ over a group $(G, *)$ forms also a group where the binary operation is defined as

$$[a_{ij}] \odot [b_{ij}] = [a_{ij} * b_{ij}].$$

If G is abelian, that is the binary operation on G is commutative then $M_{n\times m}(G)$ is abelian.

4. The set map (X, G) of all functions from a non-empty set X into a group $(G, *)$ also forms a group, where the binary operation, for all $x \in X$ is defined as

$$(f \odot g)(x) = f(x) * g(x) \text{ for all } f, g \in map(X, G)$$

If the group G is abelian, that is the binary operation on G is commutative then the map (X, G) is also abelian.

Definition 1.1.3. [11] If the pairs $(G_1, .)$ and $(G_2, *)$ are any two groups, then $G = G_1 \times G_2$ is called a group under the binary operation defined as

$$(g_1, g_2)(g_1^{'}, g_2^{'}) = (g_1.g_1^{'}, g_2 * g_2^{'})$$

Where (e_{G_1}, e_{G_2}) is the identity and (g_1^{-1}, g_2^{-1}) is the inverse of (g_1, g_2) in $G_1 \times G_2$. If both G_1 and G_2 are abelian then $G_1 \times G_2$ is also abelian.

Definition 1.1.4. [11] Let the set G be a group and H be a subset of G where H is non-empty set. Then H is called a subgroup of G(denoted by $H \leq G$) if under the binary operation of group G, H is itself a group. That is, under the binary operation of G associativity holds for all elements in H, H contains an identity element also for each element in H an inverse element in H exists.

Example 1.1.5.

1. Every group G has at least two subgroups, namely the identity group $\{e\}$ and group G itself. These are said to be the trivial subgroups of G.
2. For any number $n \in \mathbb{Z}$, under addition the set $n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ is a subgroup of set of integers $\mathbb{Z}$.

Proposition 1.1.6. [11] *Let G be a group and H is a subgroup of $G \Leftrightarrow x^{-1}y \in H$ for all $x, y \in H$.*

Proposition 1.1.7. [11] *If $\{H_i : i = 1, 2, ..., n\}$ is any collection of subgroups of a group G. Then $\cap_{i=1}^{n} H_i \leq G$.*

Proof. Since each $H_i \leq G \Rightarrow e \in H_i$ for all $i = 1, 2, ..., n \Rightarrow e \in \cap_{i=1}^{n} H_i$. Let $a, b \in \cap_{i=1}^{n} H_i \Rightarrow a, b \in H_i \quad \forall i = 1, 2, ..., n$
Since H_i is a subgroup $\Rightarrow ab^{-1} \in H_i$ for all $i = 1, 2, ..., n \Rightarrow ab^{-1} \in \cap_{i=1}^{n} H_i$
Thus, intersection of subgroups is a subgroup of G. □

Proposition 1.1.8. [11] *If $\{H_i : i = 1, 2, ..., n\}$ is any collection of subgroups of a group G. Then the union of subgroups of a group G do not form a subgroup of group G. However, $H_i \cup H_j$ is a subgroup if and only if $H_i \subseteq H_j$ or $H_j \subseteq H_i$.*

Proposition 1.1.9. *If* $H, K \leq G$, *then* $HK \leq G \Leftrightarrow HK = KH$.

Proof. Firstly suppose that $HK = KH$. To prove $HK \leq G$. As $e \in H, e \in K$, so $ee \in HK$. This implies that $e \in HK \Rightarrow HK \neq \varphi$. Now let $x_1 = h_1k_1, x_2 = h_2k_2 \in HK$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Now

$$\begin{aligned} x_1x_2^{-1} =&(h_1k_1)(h_2k_2)^{-1} \\ =&(h_1k_1)(k_2^{-1}h_2^{-1}) \\ =&h_1(k_1k_2^{-1})h_2^{-1} \\ =&h_1k_3h_2^{-1} \\ =&h_3k_3 \end{aligned}$$

Since $HK = KH$. Thus, we get $x_1x_2^{-1} \in HK$.
Conversely, assume that $HK \leq G$. To prove $HK = KH$. As $H, K \leq G$ and $HK \leq G$. If $x \in HK$, then $x^{-1} \in HK$, that is, $x^{-1} = hk$ for some $h \in H, k \in K \Rightarrow x = (x^{-1})^{-1} = k^{-1}h^{-1} \in KH$. We get that $HK \subseteq KH$. Since $KH \subseteq HK \Rightarrow HK = KH$.

□

1.1.1 Normal Subgroup

Definition 1.1.10. [11] Let G be a group and H be a subgroup of G, that is, H is itself a group under binary operation of G. For any element a in G the set $Ha = \{ha : h \in H\}$ is said to be the right coset of H in G. Similarly, $aH = \{ah : h \in H\}$ is said to be the left coset of H in G.

Definition 1.1.11. [11] Let G be a group and H be a subgroup of G, that is, H forms a group under binary operation of G. Then the number of left cosets is equal to the number of right coset of H in G, where the cosets are distinct called the index of H in G and is denoted by $|G : H|$.

Example 1.1.12. Consider the symmetric group $G = S_3 = \{1, (123), (132), (12), (13), (23)\}$. Then $H = \{1, (12)\} \leq G$ and

$$\begin{aligned}(123)H &= \{(123)1, (123)(12)\}\\ &= \{(123), (13)\}\end{aligned}$$

similarly,

$$\begin{aligned}H(123) &= \{1(123), (12)(123)\}\\ &= \{(123), (23)\}\end{aligned}$$

So in general left cosets are not equal to the right cosets. But for a subgroup $H \leq G$, if

$$aH = Ha \text{ for all } a \in G.$$

then H is said to be a normal subgroup in G(denoted by $H \trianglelefteq G$)[11]. That is equivalent to for all $a \in G$ $aHa^{-1} = H$. In other words

Definition 1.1.13. [11] Let G be a group and H be its subgroup, that is, H is itself a group under the binary operation of G. Then H is called a normal subgroup of G if for every element $a \in H$ and for all $x \in G, xax^{-1} \in H$. Clearly, the sets $\{e\}$ and G are trivial normal subgroups.

Example 1.1.14.

1. Every subgroup of G is normal, if G is an abelian group, that is, G is commutative under the given binary operation.
2. Let G be any group. Then the set $Z(G) = \{x \in G : gx = xg \quad \forall g \in G\}$ which forms the center of G is normal in G.

Proposition 1.1.15. [11] *If H and K are normal subgroups of G. Then the intersection of H and K is normal in G.*

Proof. Since intersection of subgroups is a subgroup. This implies that the intersection of H and K is a subgroup. Let us assume that $t \in H \bigcap K \Rightarrow t \in H$ and $t \in K$

Since K is normal in G and also H is normal in G, this implies that for all $g \in G, \quad gtg^{-1} \in H, gtg^{-1} \in K$. Hence, $H \bigcap K \trianglelefteq G$. □

Definition 1.1.16. [11] If G is a group and N is a normal subgroup of G, that is, for all $g \in G \quad gtg^{-1} \in N$ where $t \in N$ then the quotient group G/N has elements $\{gN : g \in G\}$, the cosets of N in G, and operation $(gN).(hN) = (gh)N$.

Definition 1.1.17. [11] Let G be a group, and H and K be normal subgroups of G such that $G = HK$ and $H \cap K = \{e\}$. Then G is said to be the direct product of H and K, denoted by

$$G = H \times K.$$

1.1.2 Homomorphism

Definition 1.1.18. [11] Let the pairs $(G, .)$ and $(G^{'}, *)$ be two groups. A map $\theta : (G, .) \to (G^{'}, *)$ is called a group homomorphism or simply homomorphism if the group operations are preserved, that is,

$$\theta(g_1.g_2) = \theta(g_1) * \theta(g_2), \text{ for all } g_1, g_2 \in G.$$

1. If θ is surjective, then it is called an epimorphism.
2. If θ is injective, then θ is called a monomorphism. We can say that G is embedded into $G^{'}$.
3. If θ is bijective, then θ is called an isomorphism, denoted by $G \cong G^{'}$.

Example 1.1.19. Let $G = (\mathbb{Z}, +)$ and $G' = (2\mathbb{Z}, +)$. A map $\theta : G \to G'$ be defined by $\theta(n) = 2n$. Then

$$\theta(n_1 + n_2) = 2(n_1 + n_2) = 2n_1 + 2n_2 = \theta(n_1) + \theta(n_2)$$

We get θ is homomorphism.
Now let $t \in 2\mathbb{Z}$, then $t = 2n$ where $n \in Z$. As $\theta(n) = 2n = t$. This implies θ is onto. Now consider

$$\theta(n_1) = \theta(n_2)$$

$$2n_1 = 2n_2$$

$$\Rightarrow n_1 = n_2.$$

Thus θ is one-one. Hence $\mathbb{Z}$ is isomorphic to $2\mathbb{Z}$.

4. An isomorphism that is homomorphism together with bijection from G to itself is called an automorphism.

Proposition 1.1.20. [11] *Let G be a group and N be normal in G, that is, the product for all $g \in G, \quad gtg^{-1} \in N$ where $t \in N$. Then the map $\theta : G \to G/N$ defined by $\theta(g) = gN$ is a homomorphism called natural homomorphism.*

Proof.

$$\theta(g_1g_2) = g_1g_2N = g_1Ng_2N = \theta(g_1)\theta(g_2)$$

$$\Rightarrow \theta(g_1g_2) = \theta(g_1)\theta(g_2).$$

We get θ is a homomorphism. Now let $gN \in G/N$ where $g \in G$ and $\theta(g) = gN$. This implies θ is onto. Thus θ is epimorphism but clearly, θ is not one-one. □

Remark 1.1.21. [11] If $\theta : G \to G^{'}$ is a homomorphism, then $\theta(e_G) = e_{G'}$. And $\theta(a^{-1}) = (\theta(a))^{-1}$, for all $a \in G$. If G is abelian then its homomorphic image $Im\theta = \{\theta(a) : a \in G\}$ is abelian. However any mapping satisfying these conditions need not to be homomorphism.

Example 1.1.22. Let $(R, +)$ be an abelian group and $\phi : R \to R$ be defined as $\phi(x) = x^3$ for all $x \in R$. Here 0 is additive identity, where

$$\phi(0) = 0 \text{ and } \phi(-x) = -x^3 = -\phi(x).$$

But $\phi(x + y) \neq \phi(x) + \phi(y)$. Then ϕ is not a homomorphism.

Remark 1.1.23. [11] $Im\phi = \{\phi(g) : g \in G\}$ is a subgroup of G. and $Ker\phi = \{g \in G : \phi(g) = 1_{G'}\}$ is a normal subgroup of G.

1.2 Ring

Definition 1.2.1. [2] A non-empty set R together with two binary operations usually called addition and multiplication, denoted by $+$ and $\cdot$ (which is only symbolic representations) is called a ring if

1. The pair $(R, +)$ is an abelian group;
2. The pair $(R, \cdot)$ is a semigroup;
3. Distributive laws(both left and right) hold, that is for all $a, b, c \in R$

$$a.(b + c) = a.b + a.c;$$

$$(b + c).a = b.a + c.a\,.$$

Remark 1.2.2. [2] If R contains multiplicative identity 1, that is, $1.a = a.1 = a$ for all $a \in R$. Then the set R is called a ring with identity. If R is commutative under multiplication, that is, $a.b = b.a$ for all $a, b \in R$. Then the set R is said to be a commutative ring.

Example 1.2.3. 1. If $(R, +)$ is any abelian group, theu the operation of multiplication for all $a, b \in R$ defined by

$$a.b = 0_R$$

turns R into commutative ring.

2. The set of all integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ are well known examples of commutative rings with identity under the operations of usual addition and usual multiplication.

3. The set of all functions from a non-empty set X onto a ring $(R, +, .)$ denoted by $map(X, R)$ is also a ring where the binary operation for all $x \in X$ is defined as

$$(f \oplus g)(x) = f(x) + g(x)$$

$$(f \odot g)(x) = f(x) * g(x).$$

The *map*(X, R) is said to be a commutative ring witb identity if R is a commutative ring with identity, that is, $1.a = a.1 = a$ and $a.b = b.a$ for all $a, b \in R$.

4. If $R_1, R_2, ..., R_n$ be rings then their product $R_1 \times R_2 \times ... \times R_n$ is also a ring under component wise addition and multiplication.

Definition 1.2.4. [2] A non-empty subset S of a ring R is called a sub ring of R if S is itself a ring under the binary operations of R. That is,

1. $(S, +)$ is an abelian group;
2. $(S, .)$ is a semigroup;
3. distributive laws hold on S.

As associative, commutative and distributive laws are tbe properties that are true for every element of R, so they are true for elements in S as well. Now we are left with the following conditions.

1. Both binary operations (addition and multiplication) are defined on S, that is, $a + b \in S$ and $a.b \in S$ for all $a, b \in S$;
2. additive identity $0 \in S$;
3. for all $a \in S$, $-a \in S$.

These axioms are equivalent to $a - b \in S$ and $a.b \in S$ for all $a, b \in S$.

Example 1.2.5.

1. Every ring R has two trivial subrings $\{0\}$ and R. All otber subrings are nontrivial.
2. If we consider set of real numbers $\mathbb{R}$ then the set of rational numbers $\mathbb{Q}$ is a subring of $\mathbb{R}$.

3. The set of Gussian integers $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ is a subring of complex numbers $\mathbb{C}$.

4. If $S_1, S_2, S_3..., S_n$ are subrings of $R_1, R_2, R_3, ..., R_n$ respectively, then $S_1 \times S_2 \times S_3... \times S_n$ is a sub ring of $R_1 \times R_2 \times R_3, ... \times R_n$.

5. If S is a subring of R, that is $a - b \in S$ and $a.b \in S$ for all $a, b \in S$, then $M_n(S)$ is a subring of $M_n(R)$.

In the next section we will discuss a special type of subsets of a ring R called ideals of R. We start with the definition of ideal.

1.2.1 Ideal

Definition 1.2.6. [2] Let R be a ring. A non-empty subset I of R is said to be a left ideal of R if it satisfies the following axioms:

1. $(I, +)$ is a subgroup of $(R, +)$, that is, for all $a, b \in I, a - b \in I$;

2. $ra \in I$ for all $r \in R$ and $a \in I$.

Similarly, a non-empty subset I of R is said to be a right ideal of R if it satisfies the following axioms:

1. $(I, +)$ is a subgroup of $(R, +)$, that is, $a - b \in I$ for all $a, b \in I$;

2. $ar \in I$ for all $r \in R$ and $a \in I$.

If I is both a left and a right ideal of R, then I is called a two sided or simply an ideal of R. The zero ideal $\{0\}$ and the ring R are examples of two sided ideals in any ring R.

It is not difficult to verify that every ideal is a subring but the converse is not necessarily true. For example the set of integers $\mathbb{Z}$ is a subring of the set of real numbers $\mathbb{R}$ but $\mathbb{Z}$ is not an ideal of $\mathbb{R}$.

Example 1.2.7.

1. Every ring R has at least two ideals $\{0_R\}$ and R itself. These two ideals R and $\{0_R\}$ are usually referred to as the trivial ideals of R.
2. For any integer n, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.
3. If I is an ideal of R, that is, I is both left and right ideal of R then $M_{n\times m}(I)$ is an ideal of $M_{n\times m}(R)$.
4. The set of all matrices (having the order $n \times n$) whose last row is zero forms a right ideal in the ring of all $n \times n$ matrices under usual addition and multiplication of matrices. It is not a left ideal. The set of all matrices (having the order $n \times n$) whose last column is zero forms a left ideal but not a right ideal.

Proposition 1.2.8. [2] *Intersection of any collection of ideals of R forms again an ideal.*

Proof. Let $\{I_{\lambda:\lambda\in\Lambda}\}$ be a collection of ideals of R. Now let $a, b \in \bigcap_{\lambda\in\Lambda} I_\lambda$ then $a, b \in I_\lambda$ for each $\lambda \in \Lambda$. Therefore $a - b \in I_\lambda$ and $ar, ra \in I_\lambda$ for each $\lambda \in \Lambda$. This implies that $a - b \in \bigcap_{\lambda\in\Lambda} I_\lambda$ and $ra, ar \in \bigcap_{\lambda\in\Lambda} I_\lambda$. Thus intersection of ideals is again an ideal. □

Definition 1.2.9. The sum $A + B$ of ideals A, B of a ring R is called direct sum if $A \bigcap B = 0_R$. It is denoted by $A \oplus B$.

Proposition 1.2.10. [2] *A ring R is direct sum of its ideals A and B if and only if every element of R is uniquely written as $r = a + b$, $\forall\, a \in A$ and $b \in B$, that is every element of R has unique representation.*

Proof. First suppose that R is direct sum of A and B. We have to prove that each element of R uniquely expressible as $r = a + b$. Suppose on contrary that $r \in R$ can be written as $r = a + b$ and $r = a^{'} + b^{'}$ then

$$a + b = a^{'} + b^{'}$$

$$\Rightarrow a - a^{'} = b^{'} - b.$$

Since $a - a^{'} \in A$ and $b^{'} - b = a - a^{'}$. This implies that $a - a^{'} \in B$. Then this implies that $a - a^{'} \in A \cap B$. Since $A \cap B = \{0_R\}$, so $a - a^{'} = 0$. Thus we get $a = a^{'}$, similarly $b = b^{'}$. Now conversely, assume $R = A + B$. Let $0 \neq r \in A \cap B$ and $r = 0_R + r$ and also $r = r + 0_R$. This implies that $0_R + r = r + 0_R$. Then we get $r = 0$. Hence, $A \cap B = 0 \Rightarrow R = A \oplus B$. □

Definition 1.2.11. [2] Let for a ring R, I be the two sided (both left and right)ideal of R. If we define a relation on R by "$a \sim b \Leftrightarrow a - b \in I$" $\forall a, b \in R$, then it is quite easy to verify that $\sim$ is an equivalence relation and it partitions R into disjoint classes

$$[a] = \{b \in R : a \sim b\} = \{b \in R : a - b \in I\}$$

$$= \{b \in R : b \in a + I\} = a + I$$

The equivalence class $a+I$ is said to be a coset of I in R. the set of all such cosets is denoted by R/I. The set R/I is a ring under addition and multiplication defined by

$$a + I \oplus b + I = (a + b) + I$$

$$(a + I) \odot (b + I) = (a.b) + I$$

The ring R/I is said to be quotient or factor ring. Note that, R/I is a commutative ring with identity $1 + I$. If R is a commutative ring with identity 1, that is, $1.a = a.1 = a$ and $a.b = b.a$ for all $a, b \in R$. Now we will define structure preserving maps for rings as we have already defined for groups.

1.2.2 Ring Homomorphism

Definition 1.2.12. [2] Let $(R, +, .)$ and $(R^{'}, +^{'}, .^{'})$ be any two rings. A map $f : R \to R$ is called a ring homomorphism if ring operations are preserved, that is,

$$f(a + b) = f(a) +^{'} f(b) \text{ and } f(ab) = f(a).^{'} f(b)$$

If the mapping f is surjective, injective or bijective, then f is called epimorphism, monomorphism or isomorphism (respectively).

Example 1.2.13. 1. $\theta : R \to R'$ defined by $\theta(r) = 0_{R'}$ $\forall r \in R$ is a ring bomomorphism called trivial homomorphism.

2. $\theta : M_n(R) \to R$ defined by $\theta(A) = detA$ for all $A \in M_n(R)$ is a ring homomorphism.

Chapter 2

Skew-Morphism of Groups

In this chapter, we will discuss the skew-morphism of groups. The results discussed in this chapter are taken from [4].

2.1 Skew-Morphism of Groups

Definition 2.1.1. Consider a group G, a bijection $\phi : \mathbf{G} \to \mathbf{G}$ of the elements of group G that fixes the identity of G, is called a skew-morphism of G with associated power function $\pi : \mathbf{G} \to \mathbb{Z}$ if for all $c, d \in \mathbf{G}$

$$\phi(cd) = \phi(c)\phi^{\pi(c)}(d).$$

Example 2.1.2. $\mathbb{Z}_2$ has only one skew-morphism (namely identity).
Let $\phi : \mathbb{Z}_2 \to \mathbb{Z}_2$ be defined as $\phi(x) = x$ and $\pi : \mathbf{G} \to \mathbb{Z}$ be defined by $\pi(x) = n \, \forall x \in \mathbf{G}$. It is clearly a bijection. Now, consider

$$\phi(0+0) = 0 = \phi(0) + \phi^{\pi(0)}(0)$$

$$\phi(1+1) = 0 = \phi(1) + \phi^{\pi(1)}(1)$$

Similarly,

$$\phi(0+1) = 1 = \phi(0) + \phi^{\pi(0)}(1) = \phi(1+0)$$

Clearly, it is skew-morphism of group.

Example 2.1.3. Let $\mathbb{Z}_3 = \{\bar{0},\ \bar{1},\ \bar{2}\}$. A map $\phi : \mathbb{Z}_3 \to \mathbb{Z}_3$ defined as

$$\phi(0) = 0,\ \phi(1) = 2,\ \phi(2) = 1$$

To check it is skew-morphism:

$$\phi(0+0) = 0 = \phi(0) + \phi(0)$$

$$\phi(1+1) = 1 = \phi(1) + \phi(1)$$

$$\phi(2+2) = 2 = \phi(2) + \phi(2)$$

$$\phi(1+2) = 0 = \phi(1) + \phi(2)$$

Similarly,

$$\phi(0+w) = \phi(w) = \phi(0) + \phi(w)$$

So it is automorphism in group w.r.t $'+'$ and also it is skew-morphism with $\pi(x) = 1$. We get

$$Auto(Z_3, +) = \{i,\ \phi\}.$$

This implies that skew-morphism of group= $\{i,\ \phi\}$.

Example 2.1.4.

1. $\mathbb{Z}_4$ has two skew-morphisms, namely the two automorphism of $\mathbb{Z}_4$;
2. $\mathbb{Z}_2 \times \mathbb{Z}_2 (\cong V_4)$ has six skew-morphisms, namely the six automorphisms;
3. $\mathbb{Z}_5$ has four skew-morphisms, namely the four automorphism of$\mathbb{Z}_5$;
4. $\mathbb{Z}_6$ has four skew-morphisms, two automorphism and two others with kernel $\mathbb{Z}_3$;
5. $\mathbb{Z}_7$ has six skew-morphisms, namely the six automorphism of $\mathbb{Z}_7$;
6. $\mathbb{Z}_8$ has six skew-morphisms, four automorphism and two others with kernel $\mathbb{Z}_4$;
7. $\mathbb{Z}_4 \times \mathbb{Z}_2$ has 16 skew-morphisms: eight automorphisms and eight others with kernel $\mathbb{Z}_4$;

8. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has 168 skew-morphisms, all of which are automorphisms.

Lemma 2.1.5. *Let for a group* $\mathbf{G}$, ϕ *be a skew-morphism with associated power function* π, *that is, a map from the group* $\mathbf{G}$ *into the set of integers* $\mathbb{Z}$ *such that* $\pi(x) = n \, \forall x \in \mathbf{G}$. *Then* $\phi^n(vw) = \phi^n(v)\phi^{\sigma(n,v)}(w)$ *where* $\sigma(n,v) = \sum_{0 \leq i < n} \pi(\phi^i(v))$, *for all* $v, w \in \mathbf{G}$ *and* $n \in \mathbb{Z}$.

Proof. We will prove by using mathematical induction. if $n = 1$, then $\phi(vw) = \phi(v)\phi^{\sum_{i=0}^{1-1} \pi(\phi^i(v))}(w) = \phi(v)\phi^{\pi(\phi^0(v))}(w) = \phi(v)\phi^{\pi(v)}(w)$. Now assnme that statement is true for all $n \leq k-1$. This implies that,

$$\begin{aligned} \phi^k(vw) =& \phi(\phi^{k-1}(vw)) \\ =& \phi(\phi^{k-1}(v)\phi^{\sum_{i=0}^{k-2}}\pi(\phi^i(v))(w)) \\ =& \phi(\phi^{k-1}(v))\phi^{\pi(\phi^{k-1}(v))}(\phi^{\sum_{i=0}^{k-2} \pi(\phi^i(v))}(w))) \\ =& \phi^k(v)\phi^{\sum_{i=0}^{k-1} \pi(\phi^i(v))}(w). \end{aligned}$$

Hence, we get that
$\phi^k(vw) = \phi^k(v)\phi^{\sum_{i=0}^{k-1} \pi(\phi^i(v))}(w) \, \forall v, w \in \mathbf{G}$. □

Now in the next lemma we will explain the power function for the product of two elements in $\mathbf{G}$.

Lemma 2.1.6. *Let for a group* $\mathbf{G}$, ϕ *be a skew-morphism and let* π *be the power function of* ϕ, *that is, a map from the group* $\mathbf{G}$ *into the set of integers* $\mathbb{Z}$ *such that* $\pi(x) = n \, \forall x \in \mathbf{G}$. *Then we have for all* $u, v \in \mathbf{G}$

$$\pi(uv) \equiv \sum_{i=0}^{\pi(u)-1} \pi(\phi^i(v))(mod n).$$

Proof. Let u, v and $w \in \mathbf{G}$. Consider $\phi(uvw) = \phi((uv)w)$. As ϕ is skew-morphism of group. This implies that $\phi((uv)w) = \phi(uv)\phi^{\pi(uv)}(w)$

$$= \quad \phi(u)\phi^{\pi(u)}(v)\phi^{\pi(uv)}(w) \tag{2.1.1}$$

Now, consider

$$\begin{aligned}\phi(uvw) =&\phi(u(vw)) = \phi(u)\phi^{\pi(u)}(vw)\\ =&\phi(u)\phi^{\pi(u)-1}(\phi(vw))\\ =&\phi(u)\phi^{\pi(u)-1}(\phi(v)\phi^{\pi(v)}(w))\\ =&\phi(u)\phi^{\pi(u)-2}(\phi(\phi(v)\phi^{\pi(v)}(w)))\\ =&\phi(u)\phi^{\pi(u)-2}(\phi^2(v)\phi^{\pi(\phi(v))})(\phi^{\pi(v)}(w))\\ =&\phi(u)\phi^{\pi(u)}(v)\phi^{\sum_{i=0}^{\pi(u)-1}\pi(\phi^i(v))}(w) \qquad (2.1.2)\end{aligned}$$

From (2.1.1) and (2.1.2) we get

$$\pi(u) \equiv \sum_{i=0}^{\pi(u)-1} \pi(\phi^i(v))(modn)$$

□

Note 2.1.7. ϕ is an automorphism of $\mathbf{G}$ if the power function π takes constant value 1. More generally, the kernel of skew-morphism ϕ is defined as subset $\{g \in \mathbf{G} \mid \pi(g) = 1\}$ of $\mathbf{G}$, and denoted by $K_{\mathbf{G}}$.

2.2 Kernel and Fix of Skew-Morphism of Groups

Definition 2.2.1. The kernel of ϕ is defined as the subset $\{g \in \mathbf{G} | \pi(a) = 1\}$ of $\mathbf{G}$, and denoted by $K_{\mathbf{G}}$.

Definition 2.2.2. The Fix of ϕ is defined as the subset $F = Fix(\phi) = \{g \in \mathbf{G} : \phi(g) = g\}$ of $\mathbf{G}$, and denoted by $Fix(\phi) = F$.

Lemma 2.2.3. *Let ϕ be a skew-morphism for a group $\mathbf{G}$ and π be the associated power function of ϕ, that is, a map from a group $\mathbf{G}$ into the set of integers $\mathbb{Z}$ such that $\pi(x) = n$ for all $x \in \mathbf{G}$. Then the set $K_{\mathbf{G}} = \{g \in \mathbf{G} | \pi(g) = 1\}$ is a subgroup of $\mathbf{G}$.*

Proof. The unit element $1_{\mathbf{G}}$ obviously belongs to $K_{\mathbf{G}}$. As $\pi(1_{\mathbf{G}}) = 1$. This implies that $1_{\mathbf{G}} \in K_{\mathbf{G}}$. Now let $g \in K_{\mathbf{G}}$. Then this implies that $\pi(g) = 1$.

Consider $\mathbf{1} = \pi(1) = \pi(gg^{-1}) = \sum_{i=0}^{\pi(g)-1} \pi(\phi^i(g^{-1})) = \pi(\phi^0(g^{-1})) = \pi(g^{-1})$. Now let $g_1, g_2 \in K_{\mathbf{G}}$. This implies that $\pi(g_1) = 1 = \pi(g_2)$. Now consider

$$\begin{aligned}\pi(g_1g_2^{-1}) = &\sum_{i=0}^{\pi(g_1)-1} \pi(\phi^i(g_2^{-1}))\\ =&\pi(\phi^0(g_2^{-1})) = \pi(g_2^{-1}) = 1.\end{aligned}$$

Then this implies that $g_1g_2^{-1} \in K_{\mathbf{G}}$. Hence, $K_{\mathbf{G}}$ is a subgroup of $\mathbf{G}$. □

Lemma 2.2.4. *Let for a group* $\mathbf{G}$, ϕ *be a skew-morphism and* π *be the associated power function of* ϕ, *that is, a map from a group* $\mathbf{G}$ *into the set of integers* $\mathbb{Z}$ *such that* $\pi(x) = n$ *for all* $x \in \mathbf{G}$. *Then* $\pi(a) = \pi(b) \Leftrightarrow a$ *and* b *belongs to the same right coset of the subgroup* $K_{\mathbf{G}}$ *in group* $\mathbf{G}$.

Proof. Let a and b belongs to the same right coset of the subgroup $K_{\mathbf{G}}$ in group $\mathbf{G}$. Then this implies $a = cb$ for some $c \in K_{\mathbf{G}}$. And also

$$\pi(a) = \pi(cb) = \sum_{i=0}^{\pi(c)-1} \pi(\phi^i(b)) = \pi(b).$$

Now conversely suppose that $\pi(a) = \pi(b)$. Then

$$\begin{aligned}1 =&\pi(aa^{-1}) = \sum_{i=0}^{\pi(a)-1} \pi(\phi^i(a^{-1}))\\ =&\sum_{i=0}^{\pi(b)-1} \pi(\phi^i(a^{-1})) = \pi(ba^{-1}).\end{aligned}$$

Thus, we get $ba^{-1} \in K_{\mathbf{G}}$. Hence result holds. □

Lemma 2.2.5. *Let for a group* $\mathbf{G}$, ϕ *be a skew-morphism and* π *be the associated power function of* ϕ, *that is, a map from a group* $\mathbf{G}$ *into the set of integers* $\mathbb{Z}$ *such that* $\pi(x) = n$ *for all* $x \in \mathbf{G}$. *Then the set* $Fix(\phi) = \{l \in \mathbf{G} | \phi(l) = l\}$ *is a subgroup of* $\mathbf{G}$.

Proof. As $\phi(1_{\mathbf{G}}) = 1$. This implies $1_{\mathbf{G}} \in Fix(\phi)$. Now let $l \in Fix(\phi)$. Then this implies that $\phi(l) = l$. Consider

$$\phi(l^{-1}l) = \phi(l^{-1})\phi^{\pi(l^{-1})}(l)$$

$$1 = \phi(l^{-1})\phi(l)$$
$$l^{-1} = \phi(l^{-1}).$$

Now let $l_1, l_2 \in Fix(\phi)$. Then $\phi(l_1) = l_1$ and $\phi(l_2) = l_2$. Now again consider

$$\begin{aligned}\phi(l_1 l_2^{-1}) =& \phi(l_1)\phi^{\pi(l_1)}(l_2^{-1})\\ =& l_1\phi(l_2^{-1}) = l_1 l_2^{-1}\\ \Rightarrow & l_1 l_2^{-1} \in Fix(\phi)\end{aligned}$$

Hence, the set $Fix(\phi) = \{l \in \mathbf{G} | \phi(l) = l\}$ is a subgroup of $\mathbf{G}$. □

Lemma 2.2.6. *Let for a group* $\mathbf{G}$, ϕ *be a skew-morphism and let* π *be the associated power function of* ϕ*, that is, a map from a group* $\mathbf{G}$ *into the set of integers* $\mathbb{Z}$ *such that* $\pi(x) = n$ *for all* $x \in \mathbf{G}$*. Then the intersection* $K_{\mathbf{G}} \cap Fix(\phi)$ *is a normal subgroup of* $Fix(\phi)$*.*

Proof. Let $m \in K_{\mathbf{G}} \cap Fix(\phi)$ and $n \in Fix(\phi)$. This implies that $m \in K_{\mathbf{G}}$ and $m, n \in Fix(\phi)$. Then this implies that $\pi(m) = 1, \phi(m) = m$ and $\phi(n) = n$. Consider $\pi(nmn^{-1}) = \pi(mnn^{-1}) = \pi(m) = 1$. This implies that $nmn^{-1} \in K_{\mathbf{G}}$. Now again consider

$$\begin{aligned}\phi(nmn^{-1}) =& \phi(nm)\phi^{\pi(nm)}(n^{-1})\\ =& \phi(n)\phi^{\pi(m)}(n)\phi(n^{-1})\\ =& \phi(n)\phi(n)\phi(n^{-1}) = nmn^{-1}\end{aligned}$$

Thus, we get $nmn^{-1} \in Fix(\phi)$. Hence, the intersection $K_{\mathbf{G}} \bigcap Fix(\phi)$ gives a normal subgroup of $Fix(\phi)$. □

2.3 Some Important Results

Proposition 2.3.1. *Let for a group* $\mathbf{G}$, ϕ *be any skew-morphism, and let* W *be a subgroup of* $K = K_{\mathbf{G}}$*, that is, normal in* $\mathbf{G}$ *and is preserved by* ϕ*, that is,* $\phi(W) = W$*. Then the mapping* $\phi^* : \mathbf{G}/W \to \mathbf{G}/W$ *defined as* $\phi^*(xW) = \phi(x)W$ *is a well-defined skew-morphism of* $\mathbf{G}/W$*.*

Proof. Firstly, if $w \in W$ and $x \in \mathbf{G}$ then $\phi(xw) = \phi(x)\phi(w) \in \phi(x)W$, since ϕ preserves W, and so the mapping ϕ^* is well defined. As π be the power function of ϕ. Now we have to show skew-morphism of group. Consider

$$\phi^*(xW) = \phi^*(yW)$$

$$\Rightarrow \phi(x)W = \phi(y)W$$

$$\Leftrightarrow xW = yW.$$

Thus, the mapping ϕ^* is one-one. Now for every $\phi(x)W \in \mathbf{G}/W$ where $\phi(x) \in \mathbf{G}$ there exist $xW \in \mathbf{G}/W$ where $x \in \mathbf{G}$ such that $\phi^*(xW) = \phi(x)W$. This implies that the map ϕ^* is a bijection. Now again consider

$$\begin{aligned}\phi^*((xW).(yW)) =& \phi^*(xyW)\\ =& \phi(xy)W = \phi(x)\phi^{\pi(x)}(y)W \quad \because (\phi \text{ is skew-morphism of group})\\ =& \phi(x)W\phi^{\pi(x)}(y)W = \phi^*(xW)\phi^{*(\pi(x))}(yW).\end{aligned}$$

Hence, clearly the map ϕ^* is skew-morphism of group. □

Proposition 2.3.2. *Let $\mathbf{G}$ be any given finite group. Then if $\mathbf{G}'$ is any finite group with a complementary subgroup factorisation $\mathbf{G}' = \mathbf{G}Y$ where Y is cyclic, and y is a generator of Y, then the rule $yr = \phi(r)y^{\pi(r)}$ (for $r \in \mathbf{G}$) gives a skew-morphism ϕ of $\mathbf{G}$ with associated power function π, that is, a map from a group $\mathbf{G}$ into the set of integers $\mathbb{Z}$ such that $\pi(x) = n$ for all $x \in G$.*

Proof. Let $\mathbf{G}'$ be any finite group that has a complementary subgroup factorisation. Note that $Y\mathbf{G} = \mathbf{G}Y (= \mathbf{G}')$, since $\mathbf{G}Y$ is a subgroup of $\mathbf{G}'$. As Y is cyclic so let y be a generator of Y. Then for any $r \in \mathbf{G}$, we know that $yr \in Y\mathbf{G} = \mathbf{G}Y$, so $yr = r'y^j$ for some $r' \in \mathbf{G}$ and some $j \in \mathbb{Z}$, both of which are uniquely determined by r. We can now define functions $\phi : \mathbf{G} \to \mathbf{G}$ and $\pi : \mathbf{G} \to \mathbb{Z}$ by taking

$$\phi(r) = r' \text{ and } \pi(r) = j \text{ whenever } yr = r'y^j \text{ where } r' \in \mathbf{G} \text{ and } j \in \mathbb{Z}.$$

To show $yr = \phi(r)y^{\pi(r)}$ (for $r \in$ G) gives a skew-morphism ϕ of G with associated power function π, that is, a map from a group G into the set of integers $\mathbb{Z}$ such that $\pi(x) = n$ for all $x \in$ G. We consider $\phi(r) = \phi(s)$. This implies $yry^{-\pi(r)} = yry^{-\pi(s)}$. Then this implies that $r^{-1}s = (yr)^{-1}ys = y^{\pi(s)-\pi(r)} \in Y$. So we obtain $r^{-1}s = 1$. Clearly, ϕ is a bijection. Now again consider

$$y(rs) = (yr)s = \phi(r)y^{\pi(r)}(s)$$

Particularly let $\pi(r) = 2$

$$\begin{aligned}\phi(r)y^2(s) =& \phi(r)y(ys)\\ =& \phi(r)y(\phi(s)y^{\pi(r)}) = \phi(r)(y\phi(s))y^{\pi(s)}\\ =& \phi(r)(\phi(\phi(s))y^{\pi(\phi(s))}y^{\pi(s)}\\ =& \phi(r)\phi^2(s)y^{\pi(s)+\pi(\phi(s))} = \phi(r)\phi^2(s)y^{\pi(rs)}\end{aligned}$$

So in general

$$\begin{aligned}y(rs) =& \phi(r)\phi^{\pi(r)}(s)y^{\pi(rs)}\\ =& \phi(r)\phi^{\pi(r)}(s)y^{j} \quad \because (j = \pi(rs))\end{aligned}$$

Thus, we get $\phi(rs) = \phi(r)\phi^{\pi(r)}(s)$, so that ϕ is skew-morphism of G. □

Now it is obvious question that whether the inverse of skew-morphism of group gives us again an skew-morphism of group. For this purpose we have following lemma.

Lemma 2.3.3. *If for a finite group* G, *ϕ is a skew-morphism then so is ϕ^i whenever i is coprime to the order $|\phi|$ of ϕ. Hence in particular, the inverse of every skew-morphism of group forms again a skew-morphism of group .*

Proof. Let ϕ is a skew-morphism of group G, that is for all $v, w \in$ G $\phi(vw) = \phi(v)\phi^{\pi(v)}(w)$. Consider $\phi[\phi^{-1}(v)\phi^{-1(\pi(v))}(w)] = \phi[\phi^{-1}(v)]\phi^{\pi(\phi^{-1}(v))}[\phi^{-1(\pi(v))}(w)]$ $= v\phi^{\pi(\phi^{-1(v)})}(\phi^{-1(\pi(v))}(w))$.

Thus, we obtain

$$\phi[\phi^{-1}(v)\phi^{-1(\pi(v))}(w)] = v\phi^{\pi(\phi^{-1(v)})}(\phi^{-1(\pi(v))}(w)) \tag{2.3.1}$$

As $v \in Fix\phi$. This implies that $\phi(v) = v$. Clearly $\phi^{-1}(v) = v$. Then $\pi(\phi^{-1}(v)) = \pi(v)$.

Let

$$\pi(\phi^{-1}(v)) = i = \pi(v)$$

$$\begin{aligned}\phi^{\pi(\phi-1(v))}(\phi^{-1(\pi(v))}(w)) &= \phi^{i}(\phi^{-1(i)}(w)) \\ &= \phi^{i}(\phi^{-i}(w)) = w\end{aligned}$$

We get $\phi[\phi^{-1}(v)\phi^{-1(\pi(v))}(w)] = vw$. Thus, we get that $[\phi^{-1}(v)\phi^{-1(\pi(v))}(w)] = \phi^{-1}(vw)$. Hence, ϕ^{-1} is also a skew-morphism of group. □

Lemma 2.3.4. *Let for a finite group* $\mathbf{G}$ ϕ *be a skew-morphism with associated power function* π, *that is a map from a group* $\mathbf{G}$ *into the set of integers* $\mathbb{Z}$ *such that* $\pi(x) = n$ *for all* $x \in \mathbf{G}$. *Then* ϕ^i, *that is, composition of* ϕ *is a skew-morphism of* $\mathbf{G}$ *if and only if for every* $a \in \mathbf{G}$ *there is some* $k_i, a \in \mathbb{Z}_{|\phi|}$ *such that* $\varrho(i,a) = \pi(\phi^{i-1}(a)) + ... + \pi(\phi(a)) + \pi(a) \equiv iK_{i,a} mod|\phi|$. *Moreover, when this happens, the power function of* ϕ^i *takes* a *to* k_i, a *for all* $a \in \mathbf{G}$, *and if* $K_{\mathbf{G}}$ *is preserved by* ϕ, *then* $K^i_{\mathbf{G}} = ker(\phi^i)$ *contains*$K_{\mathbf{G}}$.

Proof. Suppose $\varrho(i,a) = \pi(\phi^{i-1}(a)) + ... + \pi(\phi(a)) + \pi(a) \equiv iK_{i,a} mod|\phi|$. Also ϕ is skew-morphism of group. We prove this by mathematical induction.

If **n**=1, then we get

$$\phi(xy) = \phi(x)\phi^{\pi(\phi^0(x))}(y)$$

$$\phi(xy) = \phi(x)\phi^{\pi(x)}(y).$$

Now suppose it is true for $n \leq k-1$.

$$\begin{aligned}\phi^k(xy) &= \phi(\phi^{k-1}(xy)) \\ &= \phi(\phi^{k-1}(x)\phi^{\sum_{i=0}^{k-2}\pi(\phi^i(x))}(y)) = \phi^k(x)\phi^{\pi(\phi^{k-1}(x))}(\phi^{\sum_{i=0}^{k-2}\pi(\phi^i(x))}(y)) \\ &= \phi^k(x)\phi^{\sum_{i=0}^{k-1}\pi(\phi^i(x))}(y) = \phi^k(x)\phi^{\varrho(k,x)}(y).\end{aligned}$$

Thus, ϕ^k is a skew-morphism of group.

Conversely, suppose $\phi : \mathbf{G} \to \mathbf{G}$ and $\pi : \mathbf{G} \to \mathbb{Z}$. Also ϕ^i is skew-morphism of group. Since,

$$\pi(xy) = \sum_{i=0}^{\pi(x)-1} \pi(\phi^i(y)).$$

Consider $\pi(xy) = \varrho(\pi(x), y)$. Particularly, let $\pi(x) = 2$

$$\begin{aligned}\varrho(2, y) =& \pi(xy) = \sum_{i=0}^{1} \pi(\phi^i(y)) \\ =& \pi(\phi^0(y)) + \pi(\phi^1(y)) = \pi(y) + \pi(\phi(y))\end{aligned}$$

We get $\varrho(2, y) = \pi(y) + \pi(\phi(y))$. In general $\varrho(i, y) = \sum_{j=0}^{i-1} \pi(\phi^j(y))$. Now to prove $K_{\mathbf{G}} \subseteq Ker\phi^i = K^i_{\mathbf{G}}$. As $K_{\mathbf{G}} = \{a \in \mathbf{G} : \pi(a) = 1\}$. Let $a \in K_{\mathbf{G}}$ and $K_{\mathbf{G}}$ is preserved by ϕ, that is, $a \in K_{\mathbf{G}}$. This implies that $\pi(a) = 1$. Also $\phi(a) \in K_{\mathbf{G}}$. Then this implies that $\pi(\phi(a)) = 1$. Now we have to check $\phi^j(a) \in K_{\mathbf{G}}$. Particularly, let $j = 2$

$$\pi(\phi^2(a)) = \pi(\phi(\phi(a)))$$

$$\Rightarrow \phi(\pi(\phi(a))) = \phi(1) = 1$$

We get that $\phi^2(a) \in K_{\mathbf{G}}$. In general $\phi^j(a) \in K_{\mathbf{G}}$. Then,

$$\pi(\phi^j(a)) = 1 \qquad \text{for every } j$$

$$\Rightarrow \varrho(i, a) = \sum_{0 \leq j < i} \pi(\phi^j(a)) = 1 + 1 + ... + 1 = i$$

When this happens then, the power function of ϕ^i takes a to $K_{i,a}$. Implies that $K_{i,a} = 1$. Then $a \in Ker\phi^i$. Finally, we get $K_{\mathbf{G}} \subseteq K^i_{\mathbf{G}} = Ker\phi^i$. □

In following proposition we will explain the relation between group automorphism and skew-morphism of group.

Proposition 2.3.5. *Every group automorphism gives a skew-morphism, but converse is not necessarily true. A skew-morphism of a finite group* $\mathbf{G}$ *is an automorphism of group* $\mathbf{G} \Leftrightarrow$ *its power function takes constant value* 1, *or equivalently, its kernel is* $\mathbf{G}$.

Proof. Let $\phi : \mathbf{G} \to \mathbf{G}$ be a group automorphism. As skew-morphism ϕ is a permutation and also a group homomorphism. Then this implies

$$\phi(st) = \phi(s)\phi(t)$$

To show skew-morphism of group:
Consider $\phi(st) = \phi(s)\phi^{\pi(s)}(t)$. Since $\pi : \mathbf{G} \to \mathbb{Z}$ defined by

$$\pi(s) = 1\,\forall s \in \mathbf{G}.$$

We get $\phi(st) = \phi(s)\phi^{\pi(s)}(t) = \phi(s)\phi(t)$. Thus, the map ϕ is a skew-morphism of group. But every skew-morphism of group need not to be a automorphism because for skew-morphism we can't restrict our power function. □

2.4 Skew-Morphism of Direct products

Now onward we will take two skew-morphisms of two groups and check their direct product is a skew-morphism or not.

Definition 2.4.1. If $\phi : \mathbf{G} \to \mathbf{G}$ and $\nu : \mathbf{G}' \to \mathbf{G}'$ are bijections on the sets $\mathbf{G}$ and $\mathbf{G}'$, then their direct product $\phi \times \nu$ is the permutation of cartesian product $\mathbf{G} \times \mathbf{G}'$ given by $(\phi \times \nu)(r, s) = (\phi(r), \nu(s))\ \forall(r, s) \in \mathbf{G} \times \mathbf{G}'$.
If ϕ and ν are skew-morphisms of the groups $\mathbf{G}$ and $\mathbf{G}'$, then it is not always the case that $\phi \times \nu$ is a skew-morphism of $\mathbf{G} \times \mathbf{G}'$, but there are some important and helpful situations where it is.

Lemma 2.4.2. *If ϕ and ν are skew-morphism of groups $\mathbf{G}$ and $\mathbf{G}'$, then it is not always the case that $\phi \times \nu$ is a skew-morphism of $\mathbf{G} \times \mathbf{G}'$.*

Proof. Let ϕ and ν are skew-morphism of groups $\mathbf{G}$ and $\mathbf{G}'$. Also ϕ and ν are bijections, then their direct product $\phi \times \nu$ is the permutation of the cartesian product $\mathbf{G} \times \mathbf{G}'$ given by

$$(\phi \times \nu)(r, s) = (\phi(r), \nu(s)) \text{ for all } (r, s) \in \mathbf{G} \times \mathbf{G}'.$$

Now to show skew-morphism of group:

$$\text{Consider}\quad \begin{aligned}(\phi\times\nu)((r,s)(t,u)) =&(\phi\times\nu)((rt),(su))\\ =&(\phi(rt),\nu(su))\\ =&(\phi(r)\phi^{\pi(r)}(t),\nu(s)\nu^{\pi(s)}(u))\end{aligned}$$

We get

$$(\phi\times\nu)((r,s)(t,u)) = \ (\phi(r)\phi^{\pi(r)}(t),\nu(s)\nu^{\pi(s)}(u)) \qquad (2.4.1)$$

Now we have to show $(\phi\times\nu)((r,s)(t,u)) = (\phi\times\nu)(r,s)(\phi\times\nu)^{\pi(r,s)}(t,u)$. Consider

$$\begin{aligned}(\phi\times\nu)(r,s)(\phi\times\nu)^{\pi(r,s)}(t,u) =&(\phi(r),\nu(s))((\phi\times\nu)^{\pi(r,s)}(t),(\phi\times\nu)^{\pi(r,s)}(u))\\ =&(\phi(r)\phi^{\pi(r,s)}(t),\nu(s)\nu^{\pi(r,s)}(u)).\end{aligned}$$

We get $(\phi\times\nu)(r,s)(\phi\times\nu)^{\pi(r,s)}(t,u) = \ (\phi(r)\phi^{\pi(r,s)}(t),\nu(s)\nu^{\pi(r,s)}(u))$ (2.4.2)

However, if the power functions $\underline{\pi(r) = \pi(r,s) = \pi(s)}$, then by equating (2.4.1) and (2.4.2) this property holds. Hence, $(\phi\times\nu)$ is a skew-morphism of group.

□

Lemma 2.4.3. *Let for a finite group* $\mathbf{G}$, ϕ *be any skew-morphism and let* $\mathbf{G}'$ *be any finite group. Then* ϕ *can be extended to a skew-morphism* θ *of the direct product* $\mathbf{G}\times\mathbf{G}'$, *such that* $\theta|_{\mathbf{G}} = \phi$ *and* $K_{\mathbf{G}\times\mathbf{G}'} = K_{\mathbf{G}}\times\mathbf{G}'$. *In particular,if* ϕ *is not an group automorphism of* $\mathbf{G}$, *then* θ *is not an group automorphism of* $\mathbf{G}\times\mathbf{G}'$.

Proof. Let $\phi:\mathbf{G}\rightarrow\mathbf{G}$ be any skew-morphism of group and $i:\mathbf{G}'\rightarrow\mathbf{G}'$ be any automorphism. Then $\theta = \phi\times i:\mathbf{G}\times\mathbf{G}'\rightarrow\mathbf{G}\times\mathbf{G}'$ defined by

$$\theta(m,e) = (\phi(m),i(e)) = (\phi(m),e)$$

Moreover θ is automorphism because $\phi:\mathbf{G}\rightarrow\mathbf{G}$ and $i:\mathbf{G}'\rightarrow\mathbf{G}'$ are automorphisms.

As $K_{\mathbf{G}} = \mathbf{G}$ such that $K_{\mathbf{G}\times\mathbf{G}'} = K_{\mathbf{G}} \times \mathbf{G}' = \mathbf{G} \times \mathbf{G}'$. We are going to show that $\theta((m,n)(o,p)) = \theta(m,n)\theta^{\psi(m,n)}(o,p)$.

Consider $\theta(m,n)\theta^{\psi(m,n)}(o,p) = (\phi(m),n)(\phi^{\psi(m,n)}(o),p)$

We get

$$\theta(m,n)\theta^{\psi(m,n)}(o,p) =(\phi(m)\phi^{\psi(m,n)}(o),np) \tag{2.4.3}$$

Now,

$$\theta(mo,np) = (\phi(mo),np)$$

$$\theta(mo,np) =(\phi(m)\phi^{\pi(m)}(o),np) \tag{2.4.4}$$

We get required condition if $\psi(m,n) = \pi(m)$. Then, the result holds. □

Chapter 3

Skew-Morphism of Rings

The purpose of this chapter is to summarise the research and it will be divided in two sections. In the first section of this chapter we will define and explain skew-morphism of rings. In the second section of this chapter using skew-morphisms, their kernels and principal ideals of rings we will construct quotients of rings and related results.

3.1 Skew-Morphism of Rings

Definition 3.1.1. For a ring $(\mathbf{R}, +, .)$ a map $\phi : \mathbf{R} \to \mathbf{R}$ is called a skew-morphism of the ring $\mathbf{R}$. If for all $s, t \in \mathbf{R}$

1. ϕ is a bijection;

2. $\phi(0) = 0$, that is, ϕ fixes the identity element;

3. $\phi(s + t) = \phi(s) + \phi^{\pi(s)}(t)$ and $\phi(st) = \phi(s)\phi(t)$.

Where π is a power function, that is, a map from $\mathbf{R}$ into $\mathbf{Z}^+ = \mathbb{N}$ such that $\pi(0) = 1$ and $\pi(st) < \pi(s)+\pi(t)$. In the following theorem we will explain effect of composition of skew-morphism on addition and multiplication of elements in $\mathbf{R}$.

Theorem 3.1.2. *Let* $\mathbf{R}$ *be a ring and* ϕ *be a skew-morphism of ring* $\mathbf{R}$ *with associated power function* π*, that is, a map from* $\mathbf{R}$ *into* $\mathbb{Z}^+ = \mathbb{N}$ *such that* $\pi(0) = 1$ *and* $\pi(wx) < \pi(w) + \pi(x)$*. Then for all* $w, x \in \mathbf{R}$

1. $\phi^k(w+x) = \phi^k(w) + \phi^{\sum_{i=0}^{k-1}\pi(\phi^i(w))}(x)$;
2. $\phi^k(wx) = \phi^k(w)\phi^k(x)$.

Proof. We will prove by using mathematical induction on k. If n=1, then $\phi(w+x) = \phi(w) + \phi^{\pi(w)}(x) = \phi(w) + \phi^{\pi(\phi^0(w))}(x)$. Now assume that statement is true for all $n \leq k-1$. This implies that,

$$\begin{aligned}\phi^k(w+x) =& \phi(\phi^{k-1}(w+x)) = \phi(\phi^{k-1}(w) + \phi^{\sum_{i=0}^{k-2}\pi(\phi^i(w))}(x))\\ =& \phi^k(w) + \phi^{\pi(\phi^{k-1}(w))}(\phi^{\sum_{i=0}^{k-2}\pi(\phi^i(w))}(x))\\ =& \phi^k(w) + \phi^{\sum_{i=0}^{k-1}\pi(\phi^i(w))}(x).\end{aligned}$$

Thus, we obtain

$$\phi^k(w+x) = \phi^k(w) + \phi^{\sum_{i=0}^{k-1}\pi(\phi^i(w))}(x)\ \forall w, x \in \mathbf{R}.$$

Now consider

$$\phi^k(wx) = \phi^{k-1}(\phi(wx)) = \phi^{k-1}(\phi(w)\phi(x)).$$

Hence, we get that for every $w, x \in \mathbf{R}$

$$\phi^k(wx) = \phi^k(w)\phi^k(x).$$

□

In the Definition 3.1.1 we assumed that $\pi(st) < \pi(s) + \pi(t)$. So now in this theorem we will explain the power function for sum of two elements in $\mathbf{R}$.

Theorem 3.1.3. *For a ring* $\mathbf{R}$ *and* ϕ *a skew-morphism of the ring* $\mathbf{R}$ *with power function* π.

$$\pi(s+t) = \sum_{i=0}^{\pi(s)-1} \pi(\phi^i(t))\, for\ all\, s, t \in \mathbf{R}.$$

Proof. Let s, t and $u \in \mathbf{R}$. Consider $\phi(s+t+u) = \phi((s+t)+u)$. As the map ϕ is skew-morphism of ring. This implies that

$$\begin{aligned}\phi((s+t)+u) =& \phi(s+t) + \phi^{\pi(s+t)}(u)\\ =& \phi(s) + \phi^{\pi(s)}(t) + \phi^{\pi(s+t)}(u) \qquad (3.1.1)\end{aligned}$$

Now consider

$$\begin{aligned}\phi(s+t+u) =& \phi(s+(t+u))\\ =& \phi(s) + \phi^{\pi(s)}(t+u) \because (\phi \text{ is skew-morphism of ring})\\ =& \phi(s) + \phi^{\pi(s)-1}(\phi(t+u))\\ =& \phi(s) + \phi^{\pi(s)-1}(\phi(t) + \phi^{\pi(t)}(u))\\ =& \phi(s) + \phi^{\pi(s)-2}(\phi(\phi(t) + \phi^{\pi(t)}(u)))\\ =& \phi(s) + \phi^{\pi(s)-2}(\phi^2(t) + \phi^{\pi(\phi(t))}(\phi^{\pi(t)}(u)))\\ =& \phi(s) + \phi^{\pi(s)}(t) + \phi^{\sum_{i=0}^{\pi(s)-1} \pi(\phi^i(t))}(u) \qquad (3.1.2)\end{aligned}$$

From (3.1.1) and (3.1.2) we obtain

$$\pi(s+t) = \sum_{i=0}^{\pi(s)-1} \pi(\phi^i(t)).$$

□

3.2 Kernel of Skew-Morphism

Definition 3.2.1. The kernel of skew-morphism ϕ is defined as the subset $\{r \in \mathbf{R} | \pi(a) = 1\}$ of $\mathbf{R}$ and is denoted by $K_{\mathbf{R}}$.

Now we check that whether the kernel of skew-morphism of ring gives us an ideal or sub ring in $\mathbf{R}$. For this we have the following theorems.

Theorem 3.2.2. *For a ring* $\mathbf{R}$ *and* ϕ *a skew-morphism of a ring* $\mathbf{R}$. *The kernel defined as* $K_{\mathbf{R}} = \{r \in \mathbf{R} : \pi(r) = 1\}$ *is a subring of ring* $\mathbf{R}$.

Proof. Suppose $v, w \in \mathbf{R}$, then

$$\phi(v-w) = \phi(v) + \phi^{\pi(v)}(-w).$$

If $v, w \in K_{\mathbf{R}}$, then we get $\pi(v) = 1 = \pi(w)$. Now if we consider that $0 = w + (-w)$, then by applying power function on both sides we get

$$1 = \pi(0) = \pi(\phi^0(-w)) \quad \because (\pi(w) = 1)$$

We get $\pi(-w) = 1$. Now again consider $\pi(v-w) = \pi(\phi^0(-w)) = \pi(-w) = 1$. Thus, this implies that $v - w$ belongs to $K_{\mathbf{R}}$. Particularly,

$$\pi(vw) < \pi(v) + \pi(w)$$

$$\pi(vw) < 1 + 1 = 2$$

Implies that $\pi(vw) = 1$. Thus, $vw \in K_{\mathbf{R}}$. So, we get that $K_{\mathbf{R}}$ is a subring. □

Remark 3.2.3. Kernel is not an ideal. It gives an ideal if $\pi(r) = 1$ for all $r \in \mathbf{R}$. In this case skew-morphism is an automorphism.

Theorem 3.2.4. *Let $K_{\mathbf{R}}$ be the kernel of ϕ, where ϕ a skew-morphism of the ring $\mathbf{R}$ with π to be an associated power function. Then for all $v, w \in \mathbf{R}$*

$$\pi(v) = \pi(w)$$

$$\Leftrightarrow v + K_{\mathbf{R}} = w + K_{\mathbf{R}}.$$

Proof. As we know that

$$v + K_{\mathbf{R}} = w + K_{\mathbf{R}}$$

$$\Leftrightarrow v - w \in K_{\mathbf{R}}$$

$$\Leftrightarrow \pi(v-w) = 1$$

$$\Leftrightarrow \pi(\phi^0(-w)) + \pi(\phi^1(-w)) + \ldots + \pi(\phi^{\pi(v)-1}(-w)) = 1$$

$$\Leftrightarrow \pi(-w) + \ldots + \pi(\phi^{\pi(v)-1}(-w)) = 1$$

$$\Leftrightarrow \pi(-w) = 1 \text{ and } \pi(v) = 1 \ \because \pi(a) \geq 1 \forall a \in \mathbf{R}.$$

Thus,

$$\begin{aligned} v + K_{\mathbf{R}} &= w + K_{\mathbf{R}} \\ &\Leftrightarrow \pi(v) = \pi(w). \end{aligned}$$

□

3.3 Fix of Skew-Morphism

Definition 3.3.1. The Fix of skew-morphism ϕ is defined as the subset $Fix(\phi) = \{r \in \mathbf{R} : \phi(r) = r\}$ of $\mathbf{R}$.

Now we would like to investigate behavior of the set $Fix(\phi)$. Either it gives us an ideal or a subring. For this purpose we will prove the following theorems.

Theorem 3.3.2. *Let for a ring* $\mathbf{R}$, ϕ *be a skew-morphism of a ring* $\mathbf{R}$. *Then the set* $Fix(\phi) = \{r \in \mathbf{R} : \phi(r) = r\}$ *is a subring of* $\mathbf{R}$.

Proof. Let $s, v \in Fix(\phi)$ this implies that $\phi(s) = s$ and $\phi(v) = v$. Consider

$$\phi(s - v) = \phi(s) + \phi^{\pi(s)}(-v) = \phi(s) + \phi^{\pi(s)-1}(\phi(-v))$$

$$\begin{aligned} \text{If we consider} \quad 0 &= -v + v \\ 0 &= \phi(0) = \phi(-v + v) \\ &= \phi(-v) + \phi^{\pi(-v)}(v) \\ &= \phi(-v) + \phi^{\pi(-v)-1}(\phi(v)) \\ &= \phi(-v) + v \end{aligned}$$

Thus, we get that

$$\phi(-v) = -v$$

Now using this we get

$$\begin{aligned} \phi(s - v) &= \phi(s) + \phi^{\pi(s)-1}(\phi(-v)) \\ &= \phi(s) + \phi^{\pi(s)-1}(-v) \end{aligned}$$

We get $\phi(s-v) = s-v$. That is, $s-v \in Fix(\phi)$. Now $\phi(sv) = \phi(s)\phi(v) = sv$ imply that, $sv \in Fix(\phi)$. Thus, we get that $Fix(\phi)$ is a subring of $\mathbf{R}$. □

Remark 3.3.3. Let ϕ be a skew-morphism of a ring $\mathbf{R}$. Then $Fix(\phi) = \{r \in \mathbf{R} : \phi(r) = r\}$ is not an ideal in $\mathbf{R}$.

Proof. Let $r, u \in Fix(\phi)$. This implies that $\phi(r) = r$ and $\phi(u) = u$. As we have previously prove that $\phi(r-u) = r-u$. Thus, $r-u \in Fix(\phi)$.
Now let $r \in Fix(\phi)$ and $u \in \mathbf{R}$. Then this implies that $\phi(r) = r$.
Consider

$$\phi(ru) = \phi(r)\phi(u) = r\phi(u)$$

$$\Rightarrow ru \notin Fix(\phi)$$

Thus, $Fix(\phi)$ is not an ideal. □

Theorem 3.3.4. *Let ϕ be a skew-morphism of a ring $\mathbf{R}$. Then $Fix(\phi) \cap K_{\mathbf{R}}$ is a subring in $\mathbf{R}$.*

Proof. Both $Fix(\phi)$ and $K_{\mathbf{R}}$ are subrings so $Fix(\phi) \cap K_{\mathbf{R}}$ is a subring. □

3.4 Some Important Results

Proposition 3.4.1. *Let ϕ be a skew-morphism of a ring $\mathbf{R}$ with power function π. Let I be an ideal in $\mathbf{R}$ with $u - v \in I \Leftrightarrow \phi(u) - \phi(v) \in I \, \forall u, v \in \mathbf{R}$. Then the mapping $\phi^* : \mathbf{R}/I \to \mathbf{R}/I$ defined by $\phi^*(u+I) = \phi(u) + I$ gives a skew-morphism with power function*

$$\pi^*(u+I) = \pi(u) \text{ for all } u \in \mathbf{R}.$$

Proof. Clearly, mapping $\phi^* : \mathbf{R}/I \to \mathbf{R}/I$ defined by $\phi^*(u+I) = \phi(u) + I$ is a bijection. Now if we define

$$\pi^* : \mathbf{R}/I \to \mathbb{Z}^+$$

as

$$\pi^*(u+I) = \pi(u)\,\forall u \in \mathbf{R},$$

then

$$\pi^*(I) = \pi^*(0+I) = \pi^*(0) = 1.$$

Also,

$$\begin{aligned}\pi^*((u+I)(v+I)) &= \pi(uv) + I\\ &= \pi(uv) < \pi(u) + \pi(v)\\ &= \pi^*(u+I) + \pi^*(v+I)\end{aligned}$$

and

$$\begin{aligned}\phi^*((u+I)+(v+I)) =&\phi^*((u+v)+I)\\ =&\phi(u+v)+I\\ =&\phi(u)+\phi^{\pi(u)}(v)+I\\ =&(\phi(u)+I)+(\phi^{\pi(u)}(v)+I)\\ =&\phi^*(u+I)+\phi^{*(\pi(u))}(v)+I\\ =&\phi^*(u+I)+\phi^{*(\pi^*(u+I))}(v+I)\end{aligned}$$

$$\begin{aligned}\phi^*((u+I)(v+I)) =&\phi^*((uv)+I) = \phi(uv)+I\\ =&\phi(u)\phi(v)+I\\ =&(\phi(u)+I)(\phi(v)+I)\\ =&\phi^*(u+I)\phi^*(v+I).\end{aligned}$$

□

Theorem 3.4.2. *Let* $\mathbf{R}$ *be a ring and* ϕ *be a skew-morphism of a ring* $\mathbf{R}$. *Let* $I \subset K_{\mathbf{R}}$*(kernel of skew-morphism) be an ideal of the ring* $\mathbf{R}$. *Then image of* I *under skew-morphism* ϕ *is also an ideal of* $\mathbf{R}$.

Proof. Since ϕ is skew-morphism of the ring $\mathbf{R}$. Let I be an ideal of the ring $\mathbf{R}$ and $\phi(I) = \{\phi(i) : \quad i \in I\}$. As $\phi(0) = 0$. This implies $0 \in I'$. Now we have to show that $\phi(s) - \phi(u) \in \phi(I)$ where $s, u \in I$. Since I is an ideal implies $s - u \in I \subset K_{\mathbf{R}}$ implies $\pi(s) = \pi(u)$. Consider $0 = u - u$, then

$$0 = \phi(0) = \phi(u - u) = \phi^{\pi(u)}(-u) + \phi(u)$$

Thus, we get that

$$\phi^{\pi(u)}(-u) = -\phi(u).$$

Similarly,

$$\begin{aligned} \phi(-u + u) =& 0 = \phi(-u) + \phi^{\pi(-u)}(u) \\ \Rightarrow \phi(-u) =& - \phi^{\pi(-u)}(u). \end{aligned}$$

Consider

$$\begin{aligned} \phi(s) - \phi(u) =& \phi(s) + (-\phi(u)) \\ =& \phi(s) + \phi^{\pi(u)}(-u) \\ =& \phi(s) + \phi^{\pi(s)}(-u) \\ =& \phi(s - u) \in \phi(I). \end{aligned}$$

Let $\phi(s) \in \phi(I)$, where $s \in I$ and $r' \in \mathbf{R}$. Since ϕ is a bijection so there exist $r \in \mathbf{R}$ such that $\phi(r) = r'$ and we have

$$r'\phi(s) = \phi(r)\phi(s) = \phi(rs) \in \phi(I).$$

Similarly, $\phi(s)r' \in \phi(I) \Rightarrow \phi(I)$ is an ideal of $\mathbf{R}$. □

Theorem 3.4.3. *Let for a ring $\mathbf{R}$ and ϕ be a skew-morphism of the ring $\mathbf{R}$. Then the inverse image under ϕ of an ideal $I \subset K_{\mathbf{R}}$ of ring $\mathbf{R}$ is also an ideal of* $\mathbf{R}$.

Proof. Let ϕ be a skew-morphism of the ring $\mathbf{R}$ and I ia an ideal in $\mathbf{R}$. Consider $\phi^{-1}(I) = \{v \in \mathbf{R} : \phi(v) \in I\}$. Since I is an ideal of $\mathbf{R}$ implies $0 \in I$. As we know that $\phi(0) = 0 \Rightarrow 0 \in \phi^{-1}(I)$. Let $u, v \in \phi^{-1}(I) \Rightarrow \phi(u), \phi(v) \in I \subset K_{\mathbf{R}}$. That is, $\pi(\phi(u)) = \pi(\phi(v)) = 1$. From above we have $\pi(\phi(-v)) = 1$. Since I is an ideal, we have

$$\phi(u) - \phi(v) \in I$$

$$\Rightarrow \phi(u) + (-\phi(v))$$

$$\Rightarrow \phi(u) + \phi^{\pi(v)}(-v) \in I$$

$$\Rightarrow \phi(u) + \phi^{\pi(u)}(-v) \in I$$

$$\Rightarrow \phi(u - v) \in I$$

$$\Rightarrow u - v \in \phi^{-1}(I).$$

Let $u \in \phi^{-1}(I) \Rightarrow \phi(u) \in I$. We have

$$\phi(ru) = \phi(r)\phi(u) \in I \, \forall r \in R$$

$$\Rightarrow ru \in \phi^{-1}(I)$$

$\Rightarrow \phi^{-1}(I)$ is an ideal of $\mathbf{R}$. □

Note 3.4.4. The point wise addition and composition of skew-morphisms of a ring $\mathbf{R}$ are not skew-morphism. So collection of skew-morphisms need not to be a ring.

Proposition 3.4.5. *Let* R *be any finite ring. Then if* R' *is any finite ring with a complementary ideal factorisation* $\mathrm{R}' = \mathbf{R} + Y$ *where* Y *is principal, and* y *is a generator of* Y*. Then the rule* $y + s = \phi(s) + y^{\pi(s)}$ *(for* $s \in \mathbf{R}$*) defines a skew-morphism* ϕ *of* $\mathbf{R}$ *with power function* π*, that is,* $\phi(x + y) = \phi(x) + \phi^{\pi(x)}(y)$ *and* $\phi(xy) = \phi(x)\phi(y)$.

Proof. Let $\mathbf{R}'$ be any finite ring that has a complementary ideal factorisation. Note that $Y + \mathbf{R} = \mathbf{R} + Y = \mathbf{R}'$, since $\mathbf{R} + Y$ gives a subring of $\mathbf{R}'$. Also let y

be a generator of Y. Then for any $s \in \mathbf{R}$, we know that $y+s \in Y+\mathbf{R} = \mathbf{R}+Y$, so $y+s = s^{'}+jy$ for some $s^{'} \in \mathbf{R}$ and some $j \in \mathbb{Z}$, both of which are uniquely determined by s. We can now define functions $\phi : \mathbf{R} \to \mathbf{R}$ and $\pi : \mathbf{R} \to \mathbb{Z}$ by taking

$$\phi(s) = s^{'} \text{ and } \pi(s) = j \text{ whenever } y+s = s^{'}+jy \text{ where } s^{'} \in \mathbf{R} \text{ and } j \in \mathbb{Z}.$$

To show $y+s = \phi(s)+jy$ (for $s \in \mathbf{R}$) defines a skew-morphism ϕ of ring $\mathbf{R}$ with associated power function π. We consider $\phi(s) = \phi(u)$. This implies $y+s-jy = y+u-jy$. Then this implies that $s = u$. Clearly, ϕ is a bijection. Now again consider

$$y+(s+u) = (y+s)+u = (s^{'}+jy)+u$$

Particularly let $\pi(s) = 2$

$$\begin{aligned}\phi(s)+2y+u =&\phi(s)+y+(y+u)\\ =&\phi(s)+y+(\phi(u)+\pi(u)y)\\ =&\phi(s)+(y+\phi(u))+\pi(u)y\\ =&\phi(s)+\phi^{2}(u)+\pi(\phi(u))y+\pi(u)y\\ =&\phi(s)+\phi^{\pi(s)}(u)+y[\pi(\phi(u))+\pi(u)]\end{aligned}$$

So in general, $j = \pi(s) > 2$

$$\begin{aligned}y+(s+u) =&\phi(s)+\phi^{\pi(s)}(u)+y\sum_{i=0}^{\pi(s)-1}\pi(\phi^{i}(u))y\\ =&\phi(s)+\phi^{\pi(s)}(u)+\pi(s+u)y\\ =&\phi(s)+\phi^{\pi(s)}(u)+jy \because (\pi(s+u)=j)\\ =&\phi(s+u)+jy\end{aligned}$$

Thus, we get $\phi(s+u) = \phi(s)+\phi^{\pi(s)}(u)$. Similarly, $\phi(su) = \phi(s)\phi(u)$, so that ϕ is a skew-morphism of ring $\mathbf{R}$. □

Now it is obvious question that whether the inverse of skew-morphism of a ring gives us again a skew-morphism of the same ring. For this purpose we have following lemma.

Lemma 3.4.6. *Let for a finite ring* $\mathbf{R}$, ϕ *be a skew-morphism of the ring* $\mathbf{R}$. *Then the restriction of inverse of skew-morphism on* $Fix(\phi)$ *is a skew-morphism.*

Proof. Let ϕ be a skew-morphism of the ring $\mathbf{R}$. Consider

$$\begin{aligned}\phi[\phi^{-1}(t)+\phi^{-1(\pi(t))}(v)] =&\phi[\phi^{-1}(t)]+\phi^{\pi(\phi^{-1}(t))}[\phi^{-1(\pi(t))}(v)]\\ =&t+\phi^{\pi(\phi^{-1(t)})}(\phi^{-1(\pi(t))}(v))\\ =&t+\phi^{\pi(\phi^{-1(t)})}(\phi^{-1(\pi(t))}(v))\end{aligned}$$

As $t \in Fix(\phi)$, this implies that $\phi(t)=t$. Clearly, $\phi^{-1}(t)=t$, then $\pi(\phi^{-1}(t))=\pi(t)$.

Let

$$\pi(\phi^{-1}(t))=i=\pi(t)$$

$$\begin{aligned}\Rightarrow \phi^{\pi(\phi-1(t))}(\phi^{-1(\pi(t))}(v)) =&\phi^{i}(\phi^{-1(i)}(v))\\ =&\phi^{i}(\phi^{-i}(v))=v\end{aligned}$$

We get $\phi[\phi^{-1}(t)+\phi^{-1(\pi(t))}(v)] = t+v$. Thus, we get that $[\phi^{-1}(t)+\phi^{-1(\pi(t))}(v)]=\phi^{-1}(t+v)$. Now consider $\phi^{-1}(tv)=tv=\phi^{-1}(t)\phi^{-1}(v)$. Hence, ϕ^{-1} is also a skew-morphism of the ring $\mathbf{R}$. □

Lemma 3.4.7. *Let for a finite ring* $\mathbf{R}$, ϕ *be a skew-morphism of the ring* $\mathbf{R}$, *with power function* π. *Then* ϕ^{i} *is a skew-morphism of ring* $\mathbf{R}$ *if and only if for every* $a \in \mathbf{R}$, *there is some* $K_{i,a} \in \mathbb{Z}_{|\phi|}$ *such that* $\varrho(i,a)=\pi(\phi^{i-1}(a))+ \ldots. +\pi(\phi(a))+\pi(a) \equiv iK_{i,a} mod|\phi|$. *Moreover when this happens the power function of* ϕ^{i} *takes* a *to* $K_{i,a}$ *for all* $a \in \mathbf{R}$ *and if* $K_{\mathbf{R}}$ *is preserved by* ϕ *then* $ker\phi^{i}=K^{i}_{\mathbf{R}}$ *contains* $K_{\mathbf{R}}$.

Proof. Suppose $\varrho(i,a)=\pi(\phi^{i-1}(a))+\ldots.+\pi(\phi(a))+\pi(a) \equiv iK_{i,a} mod|\phi|$. Also ϕ is a skew-morphism of the ring $\mathbf{R}$. We prove this by mathematical induction on k.

If n=1, then we have

$$\phi(r+u)=\phi(r)+\phi^{\pi(\phi^{0}(r))}(u)$$

$$\phi(r+u) = \phi(r) + \phi^{\pi(r)}(u).$$

Now suppose it is true for $n \leq k-1$.

$$\begin{aligned}
\phi^k(r+u) =& \phi(\phi^{k-1}(r+u)) \\
=& \phi(\phi^{k-1}(r) + \phi^{\sum_{i=0}^{k-2}\pi(\phi^i(r))}(u)) \\
=& \phi^k(r) + \phi^{\pi(\phi^{k-1}(r))}(\phi^{\sum_{i=0}^{k-2}\pi(\phi^i(r))}(u)) \\
=& \phi^k(r) + \phi^{\sum_{i=0}^{k-1}\pi(\phi^i(r))}(u) \\
=& \phi^k(r) + \phi^{\varrho(k,r)}(u).
\end{aligned}$$

also $\phi^k(ru) = \phi^{k-1}(\phi(ru)) = \phi^{k-1}(\phi(r)\phi(u))$.

Thus, ϕ^k is a skew-morphism of the ring $\mathbf{R}$.

Conversely, ϕ^i is skew-morphism of the ring $\mathbf{R}$ with power function π . Since, we have

$$\pi(r+u) = \sum_{i=0}^{\pi(r)-1} \pi(\phi^i(u)).$$

Consider $\pi(r+u) = \varrho(\pi(r), u)$. Particularly, let $\pi(r) = 2$

$$\begin{aligned}
\varrho(2,u) =& \pi(r+u) \\
=& \sum_{i=0}^{1} \pi(\phi^i(u)) \\
=& \pi(\phi^0(u)) + \pi(\phi^1(u)) \\
=& \pi(u) + \pi(\phi(u))
\end{aligned}$$

We get that $\varrho(2,u) = \pi(u) + \pi(\phi(u))$.

In general, $\varrho(i,u) = \sum_{j=0}^{i-1}\pi(\phi^j(u))$. Now to prove $K_{\mathbf{R}} \subseteq Ker\phi^i = K^i_{\mathbf{R}}$. As $K_{\mathbf{R}} = \{r \in \mathbf{R} : \pi(r) = 1\}$. Let $a \in K_{\mathbf{R}}$ and $K_{\mathbf{R}}$ be preserved by ϕ, that is, $a \in K_{\mathbf{R}}$. This implies that $\pi(a) = 1$. Also $\phi(a) \in K_{\mathbf{R}}$. Then this implies that $\pi(\phi(a)) = 1$. Now we have to check $\phi^j(a) \in K_{\mathbf{R}}$. Particularly, let $j = 2$

$$\pi(\phi^2(a)) = \pi(\phi(\phi(a)))$$

$$\Rightarrow \phi(\pi(\phi(a))) = \phi(1) = 1$$

We get that $\phi^2(a) \in K_{\mathbf{R}}$. In general $\phi^j(a) \in K_{\mathbf{R}}$. Then,

$$\pi(\phi^j(a)) = 1 \qquad\qquad \text{for every } j$$

$$\Rightarrow \varrho(i,a) = \sum_{0 \le j < i} \pi(\phi^j(a)) = 1 + 1 + \ldots\ldots. + 1 = i$$

When this happens, then the power function of ϕ^i takes a to $K_{i,a}$. Implies that $K_{i,a} = 1$. Thus $a \in Ker\phi^i$. Finally, we get $K_{\mathbf{R}} \subseteq K^i_{\mathbf{R}} = Ker\phi^i$. □

In following proposition we will explain the relation between ring automorphism and skew-morphism of ring.

Proposition 3.4.8. *Every ring automorphism is a skew-morphism of a ring* $\mathbf{R}$. *But converse is not necessarily true.*

Proof. Let $\phi : \mathbf{R} \to \mathbf{R}$ be a ring automorphism. As skew-morphism ϕ is a bijection and also a ring homomorphism. Then this implies

$$\phi(vw) = \phi(v)\phi(w)$$

$$\phi(v+w) = \phi(v) + \phi(w)$$

Thus, the map ϕ is a skew-morphism of the ring $\mathbf{R}$ with power function $\pi(v) = 1\, \forall v \in \mathbf{R}$. But every skew-morphism of ring need not to be a automorphism because for skew-morphism we can't restrict our power function. □

In following theorems we will explain the concept how ring with identity gives us only one skew-morphism and ring without identity can give us more then one skew-morphisms.

Remark 3.4.9. Let $\mathbf{R}^1$ be a ring with identity. Then $\mathbf{R}^1$ has only one skew-morphism namely the identity map with power function $\pi(r)$ depends on r.

Example 3.4.10. The ring $\mathbb{Z}_4$ has only one skew-morphism (namely identity).

Let $\phi : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ be defined as

$$\phi(\bar{0}) = \bar{0},\ \phi(\bar{1}) = \bar{1},\ \phi(\bar{2}) = \bar{3},\ \phi(\bar{3}) = \bar{2}$$

Thus, ϕ is not a skew-morphism.

Theorem 3.4.11. *Let given a ring* $\mathbf{R}$ *without identity, then* $\phi : \mathbf{R} \rightarrow \mathbf{R}$ *may have more then one skew-morphism.*

Proof. If $\mathbf{R}$ is without identity, then $Auto(\mathbf{R}) \neq \{i\}$. As $Auto(\mathbf{R}) \subseteq Skew(\mathbf{R})$. This implies that $skew(\mathbf{R}) \neq \{i\}$. □

Example 3.4.12. Let $\mathbf{R} = \{e, f, g\}$ be a ring where binary operations are defined as

·	e	f	g
e	e	e	e
f	e	e	e
g	e	e	e

+	e	f	g
e	e	f	g
f	f	g	e
g	g	e	f

And the map $\phi : \mathbf{R} \rightarrow \mathbf{R}$ is defined as $\phi(e) = e, \phi(f) = g, \phi(g) = f$. Then

$$\phi(s + t) = \phi(s) + \phi(t)$$

$$\phi(s \cdot t) = e = \phi(s) \cdot \phi(t).$$

Thus, the map ϕ is skew-morphism of ring.

In the above example the automorphism of $(R, +)$ imply skew-morphism of the ring $\mathbf{R}$. However, this is not true in all the cases.

Example 3.4.13. Let $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. A map $\phi : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ be defined as

$$\phi(\bar{0}) = \bar{0},\ \phi(\bar{1}) = \bar{2},\ \phi(\bar{2}) = \bar{1}$$

Then

$$\phi(\bar{0} + \bar{0}) = \bar{0} = \phi(\bar{0}) + \phi(\bar{0})$$

$$\phi(\bar{1}+\bar{1}) = \bar{1} = \phi(\bar{1}) + \phi(\bar{1})$$

$$\phi(\bar{2}+\bar{2}) = \bar{2} = \phi(\bar{2}) + \phi(\bar{2})$$

$$\phi(\bar{1}+\bar{2}) = \bar{0} = \phi(\bar{1}) + \phi(\bar{2})$$

Similarly,

$$\phi(\bar{0}+\bar{u}) = \phi(\bar{u}) = \phi(\bar{0}) + \phi(\bar{u})$$

So ϕ is an automorphism of $(\mathbb{Z}_3, +)$ but $\phi(\bar{1}.\bar{2}) = \bar{1} \neq \phi(\bar{1})\phi(\bar{2})$. So ϕ is not a skew-morphism of the ring $(\mathbb{Z}_3, +, .)$.

Remark 3.4.14. If ϕ is homomorphism of $(\mathbf{R}, .)$, then in general it does not imply skew-morphism of the ring $(\mathbf{R}, +, .)$.

Example 3.4.15. Let $R = \{h, i, j\}$ be a ring where binary operations are defined as

·	h	i	j
h	i	i	i
i	i	i	i
j	i	i	i

+	h	i	j
h	h	i	j
i	i	j	h
j	j	h	i

A map $\phi : \mathbf{R} \to \mathbf{R}$ be defined as

$$\phi(h) = j, \quad \phi(i) = i, \quad \phi(j) = h$$

Consider

$$\phi(x \cdot y) = i = \phi(x) \cdot \phi(y).$$

Now consider

$$\phi(h+j) = \phi(j) = h$$

Similarly, consider other side then

$$\phi(h) + \phi^{\pi(h)}(j) = \begin{cases} j & ; \text{if } \pi(h) \text{ is odd} \\ i & ; \text{if } \pi(h) \text{ is even} \end{cases}$$

Thus, $\phi(h+j) \neq \phi(h) + \phi^{\pi(h)}(j)$

Hence, if ϕ is homomorphism of $(\mathbf{R}, .)$, then this does not imply skew-morphism of $(\mathbf{R}, +, .)$.

Proposition 3.4.16. *Let for a ring* $\mathbf{R}$, ϕ *be a skew-morphism of ring and* π *be a associated power function, that is, a map from* $\mathbf{R}$ *into* $\mathbb{Z}^+$ *such that* $\pi(0) = 1$ *and* $\pi(xy) < \pi(x) + \pi(y)$. *If* $\pi(\phi(a)) = \pi(a)$. *Then*

$$\pi(a+k) = \pi(a) \text{ where } k \in K_{\mathbf{R}}.$$

Proof. Let $k \in K_{\mathbf{R}}$. Then

$$\begin{aligned}\pi(a+k) = &\sum_{i=0}^{\pi(a)-1} \pi(\phi^i(k)) : \quad k \in K_{\mathbf{R}}\\ =&\pi(\phi^0(k)) + \pi(\phi^1(k)) + \ldots + \pi(\phi^{\pi(a)-1})\\ =&\pi(k) + \pi(\phi^1(k) + \ldots + \pi(\phi^{\pi(a)-1}))\\ =&1 + 1 \ldots + 1\\ =&\pi(a).1\\ =&\pi(a).\end{aligned}$$

□

3.5 Skew-Morphism of Direct Products

As we know that the cartesian product of any two rings is also a ring under component wise addition and multiplication. So, in this section we will take two skew-morphisms of two rings and check their direct product is a skew-morphism of ring or not.

Lemma 3.5.1. *Let for a ring* O, ϕ *be any skew-morphism of the ring* O. *Suppose* P *be any finite ring. Then* ϕ *can be extended to skew-morphism* θ *of direct product* $O \times P$, *such that*

$$\theta|_{O \cong O \times \{e\}} = \phi \text{ and } K_{O \times P} = K_O \times P$$

In particular, if ϕ is not an automorphism of O, then θ is not an automorphism of $O \times P$.

Proof. Let $\phi : O \to O$ be any skew-morphism of ring and $i : P \to P$ be the identity automorphism. Then $\theta = \phi \times i : O \times P \to O \times P$ defined by

$$\theta(l, e) = (\phi(l), i(e)) = (\phi(l), e)$$

θ is an automorphism because $\phi : O \to O$ and $i : P \to P$ are automorphisms. As $K_O = O$ such that $K_{O\times P} = K_O \times P = O \times P$. We are going to prove that $\theta((l, m) + (n, o)) = \theta(l, m) + \theta^{\psi(l,m)}(n, o)$.

Consider $\theta(l, m) + \theta^{\psi(l,m)}(n, o) = (\phi(l), m) + (\phi^{\psi(l,m)}(n), o)$

We get

$$\theta(l, m) + \theta^{\psi(l,m)}(n, o) =(\phi(l) + \phi^{\psi(l,m)}(n), m + o) \tag{3.5.1}$$

Now,

$$\theta(l + n, m + o) = (\phi(l + n), m + o)$$

$$\theta(l + n, m + o) =(\phi(l) + \phi^{\pi(l)}(n), m + o) \tag{3.5.2}$$

We get required condition if $\psi(l, m) = \pi(l)$. Then, the result holds.

Consider

$$\begin{aligned}\theta((l, m)(n, o)) &=\theta(ln, mo)\\ &=(\phi(ln), mo)\\ &=(\phi(l)\phi(n), mo)\\ &=(\phi(l), m)(\phi(n), o)\\ &=\theta(l, m)\theta(n, o)\end{aligned}$$

□

Theorem 3.5.2. *Let $\mathbf{R}_1$ and $\mathbf{R}_2$ be the two rings. If $\phi_1 : \mathbf{R}_1 \to \mathbf{R}_1$ and $\phi_2 : \mathbf{R}_2 \to \mathbf{R}_2$ be two skew-morphisms with their power functions π_1 and π_2. Then $\phi : \mathbf{R}_1 \times \mathbf{R}_2 \to \mathbf{R}_1 \times \mathbf{R}_2$ be a skew-morphism of ring.*

In particular, if ϕ is not an automorphism of O, then θ is not an automorphism of $O \times P$.

Proof. Let $\phi : O \to O$ be any skew-morphism of ring and $i : P \to P$ be the identity automorphism. Then $\theta = \phi \times i : O \times P \to O \times P$ defined by

$$\theta(l, e) = (\phi(l), i(e)) = (\phi(l), e)$$

θ is an automorphism because $\phi : O \to O$ and $i : P \to P$ are automorphisms. As $K_O = O$ such that $K_{O\times P} = K_O \times P = O \times P$. We are going to prove that $\theta((l, m) + (n, o)) = \theta(l, m) + \theta^{\psi(l,m)}(n, o)$.

Consider $\theta(l, m) + \theta^{\psi(l,m)}(n, o) = (\phi(l), m) + (\phi^{\psi(l,m)}(n), o)$

We get

$$\theta(l, m) + \theta^{\psi(l,m)}(n, o) =(\phi(l) + \phi^{\psi(l,m)}(n), m + o) \tag{3.5.1}$$

Now,

$$\theta(l + n, m + o) = (\phi(l + n), m + o)$$

$$\theta(l + n, m + o) =(\phi(l) + \phi^{\pi(l)}(n), m + o) \tag{3.5.2}$$

We get required condition if $\psi(l, m) = \pi(l)$. Then, the result holds.

Consider

$$\begin{aligned}\theta((l, m)(n, o)) =&\theta(ln, mo)\\ =&(\phi(ln), mo)\\ =&(\phi(l)\phi(n), mo)\\ =&(\phi(l), m)(\phi(n), o)\\ =&\theta(l, m)\theta(n, o)\end{aligned}$$

□

Theorem 3.5.2. *Let $\mathbf{R}_1$ and $\mathbf{R}_2$ be the two rings. If $\phi_1 : \mathbf{R}_1 \to \mathbf{R}_1$ and $\phi_2 : \mathbf{R}_2 \to \mathbf{R}_2$ be two skew-morphisms with their power functions π_1 and π_2. Then $\phi : \mathbf{R}_1 \times \mathbf{R}_2 \to \mathbf{R}_1 \times \mathbf{R}_2$ be a skew-morphism of ring.*

Proof. Let $\phi : \mathbf{R}_1 \times \mathbf{R}_2 \to \mathbf{R}_1 \times \mathbf{R}_2$ be defined as

$$\phi(a_1, b_2) = (\phi_1(a_1), \phi_2(b_2))\ \forall a_1 \in \mathbf{R}_1,\ \forall b_2 \in \mathbf{R}_2.$$

Consider

$$\phi(a_1, b_2) = \phi(a_1^{'}, b_2{}')$$

$$(\phi_1(a_1), \phi_2(b_2)) = (\phi_1(a_1^{'}), \phi_2(b_2^{'})).$$

We get

$$\phi_1(a_1) = \phi_1(a_1^{'}) \text{ and } \phi_2(b_2) = \phi_2(b_2^{'}).$$

Since ϕ_1 and ϕ_2 are skew-morphisms. This implies that $a_1 = a_1^{'}$ and $b_2 = b_2^{'}$ Then this implies that $(a_1, b_2) = (a_1^{'}, b_2^{'})$. Thus, it is one-one.
Let $(a^{'}, b^{'}) \in \mathbf{R}_1 \times \mathbf{R}_2$ where $a^{'} \in \mathbf{R}_1$ and $b^{'} \in \mathbf{R}_2$, since ϕ_1 and ϕ_2 are bijections on $\mathbf{R}_1$ and $\mathbf{R}_2$. So there exists $a \in \mathbf{R}_1$ and $b \in \mathbf{R}_2$ such that $\phi_1(a) = a^{'}$ and $\phi_2(b) = b^{'}$

$$\phi(a, b) = (\phi_1(a), \phi_2(b)) = (a^{'}, b^{'})$$

Thus ϕ is onto. Hence, ϕ is a bijection. clearly

$$\phi^n(a, b) = \phi^{n-1}(\phi(a, b))$$

$$= \phi^{n-1}(\phi_1(a), \phi_2(b))$$

$$= (\phi_1^n(a), \phi_2^n(b)).$$

Consider

$$\begin{aligned}
\phi((a_1, b_2)(a_1^{'}, b_2^{'})) =& \phi(a_1 a_1^{'}, b_2 b_2^{'}) = (\phi_1(a_1 a_1^{'}), \phi_2(b_2 b_2^{'})) \\
=& (\phi_1(a_1)\phi_1(a_1^{'}), \phi_2(b_2)\phi_2(b_2^{'})) \\
=& (\phi_1(a_1), \phi_2(b_2))(\phi_1(a_1^{'}), \phi_2(b_2^{'})) \\
=& \phi(a_1, b_2)\phi(a_1^{'}, b_2^{'})
\end{aligned}$$

Now, let
$$\begin{aligned}
\phi((a_1, b_2) + (a_1^{'}, b_2^{'})) =& \phi((a_1 + b_1^{'}), (b_2 + b_2^{'})) \\
=& (\phi_1(a_1) + \phi_1^{\pi_1(a_1)}(a_1^{'}), (\phi_2(b_2) + \phi_2^{\pi_2(b_2)}(b_2^{'}))) \\
=& (\phi_1(a_1), \phi_2(b_2)) + (\phi_1^{\pi_1(a_1)}(a_1^{'}) + \phi_2^{\pi_2(b_2)}(b_2^{'}))
\end{aligned}$$

By considering other side

$$\phi(a_1,b_2)+\phi^{\pi(a_1,b_2)}(a_1',b_2')=(\phi(a_1,b_2)+(\phi_1^{\pi(a_1,b_2)}(a_1'),\phi_2^{\pi(a_1,b_2)}(b_2'))$$

$$=(\phi_1(a_1),\phi_2(b_2))+(\phi_1^{\pi(a_1,b_2)}(a_1'),\phi_2^{\pi(a_1,b_2)}(b_2'))$$

$$=(\phi_1(a_1)+\phi_1^{\pi(a_1,b_2)}(a_1'),\phi_2(b_2)+\phi_2^{\pi(a_1,b_2)}(b_2'))$$

If the power functions $\pi_1(a_1)=\pi_2(b_2)=\pi(a_1,b_2)$ for all $a_1\in\mathbf{R}_1, b_2\in\mathbf{R}_2$. Thus ϕ is a skew-morphism. □

Bibliography

[1] M. Bachraty and R. Jajcay, *Powers of skew-morphisms*, Springer Proceedings in Mathematics and Statistics. **159** (2016), 1-26.

[2] D. M . Burton, *"A First Course in Rings and Ideals"*, Addison-wesley Co, 1970.

[3] P. M. Cohn, *"Introduction to Ring Theory"*, Addison-wesley Co, 2000.

[4] M. D. E. Condor, R. Jajcay, and T. W. Tucker, *cyclic complements and skew morphisms of groups*, J. Albegra. **453** (2016), 68-100.

[5] I. N. Herstein, *"A First Course in Abstract Algebra"*, Addison Wesley Educational Publishers Inc., 2003.

[6] I. N. Herstein, *"Abstract Algebra"*, Prantice Hall, New Jersey, 1996.

[7] M. V. Horoevski, *Automorphisms of finite groups*, Math. USSR Sb. **22** (1974), 584-594.

[8] J. ir and R. Jajcay, *Skew morphisms of regular Cayley maps*, Discrete Math. **244** (2002), 167-179.

[9] I. Kovcs and R. Nedela, *Skew-morphisms of cyclic p-groups*, Ars Math. Contemp. 4 (2011), 329-349.

[10] I. Kovcs and R. Nedela, *Decomposition of skew-morphisms of cyclic groups*, Ars Math. Contemp. 4 (2011), 329-349.

[11] J.S. Rose, *"A Course on Group Theory"*, Cambridge University Press, Cambridge, 1978.

[12] J. Y. Zhang and S.F. Du, *Skew-morphisms of dihedral groups*, submitted.