On Structures of Some Groups of Morphisms

Mohd.Altab Hossain[*] and Subrata Majumdar

Department of Mathematics, University of Rajshahi, Rajshahi-6205, Bangladesh.
Professor, Department of Mathematics, University of Rajshahi, Rajshahi-6205, Bangladesh.
email:al_math_bd@yahoo.com

Abstract: *In some categories, certain subgroups of Hom(A,A) for some groups of morphisms A → A are very useful and interesting. In this paper, the author's main aim is to study some such groups. Specifically, the automorphism groups of A, A being a group or a topological space, have been studied in certain cases.*
Keywords: *Category, morphism, homomorphism, homeomorphis, free product, structure.*

I.   Introduction

Hossain[1,3] studied the automorphism groups and Hossain and Majumdar[5] studied the endomorphism semigroups of the special semigroups[2] having a set of generators such that each non-zero element is expressible uniquely in terms of the generators using each generator at most once. Some important structures for this class were determined in those studies. In the consequences of [1] and [3], the study of this paper has been done. Sometimes terminologies of Zassenhaus[7] and Scott[6] have been used in this study. For convenience of the study the following preliminaries are very necessary:

As gluing operations one needs *direct product*, *semidirect product*, *free product* etc. If G_1 and G_2 are two groups, the direct product $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$ of G_1 and G_2 is a group with multiplication given by $(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2' g_2')$. Its cardinality is obviously $|G| \cdot |H|$. Sometimes $G \times H$ is termed the *external direct product*. It has two natural subgroups $G \times 1 = \{(g,1) \mid g \in G\}$ and $1 \times H = \{(1,h) \mid h \in H\}$.

Clearly, $G \cong G \times 1$ since $g \mapsto (g,1)$ is an isomorphism of $G \to G \times 1$, and similarly $H \cong 1 \times H$. So, one thinks of $G \times H$ as a group containing a copy of G. If G_1 and G_2 are additive abelian groups, direct product in that case is replaced just by the direct sum of the groups.

Let H and K be two groups, and let $\varphi : K \to Aut(H)$ be a homomorphism. The *semidirect product* of H by K via φ is the set of ordered pairs $\{(h,k) \mid h \in H, k \in K\}$ together with the binary operation defined by $(h_1, k_1)(h_2, k_2) = (h_1 \varphi_{k_1}(h_2), k_1 k_2)$, where φ_k. is written for $\varphi(k)$, $k \in K$ is a group. This group is denoted by $H \times_\varphi K$ for the semidirect product of the group H by the group K. write $N \rtimes_\phi K$ for the semidirect product.

The present authors now define another type of group product termed *free product* as follows:
Given any collection $\{G_i : i \in I\}$ of groups their free product exists and can be defined as follows:
Assume that for each $i \in I$ there is a homomorphism φ_i of G_i into a fixed group G . Then we say that G is the free product of the groups $G_i, i \in I$ if and only if for any group H and for any homomorphism $\psi_i : G_i \to H, i \in I$ there exists a unique homomorphism $f : G \to H$ such that $\psi_i = f\varphi_i$ for every $i \in I$.

On the other hand, a group G is said to be the free product of its subgroups $A_\alpha, \alpha \in I$ if the subgroups A_α generate G i.e., every element g of G is the product of a finite number of the elements of the A_α: $g = a_1 a_2 \cdots a_n, \quad \alpha_i \in A_{\alpha_i}, (i = 1, 2, \cdots, n)$, and the expression is unique. In this case, the free product includes the component groups as subgroups.

Specifically, if one only deals with abelian groups, it can be seen that the free product of abelian groups is again abelian. In that case, the free product equals the direct product.

The wreath product[4] of transformation groups G and H on sets A and B respectively, written $G \varsigma H$, is the group of all permutations θ on $A \times B$ such that $\theta((a,b)) = (\gamma_b(a), \eta(b))$, $a \in A$, $b \in B$, where $\eta \in H$ and for each $b \in B$, γ_b is a permutation of G on A, but for different b's the choice of the permutations γ_b are independent. Here, we recall the following theorems:

THEOREM 1.1[1]:
(i) $Aut \mathbf{Z}^+ \cong \{1\}$, the group with one element,
(ii) $Aut \mathbf{Q}^+ \cong \mathbf{Q}^+$,
(iii) $Aut\ (N(2)) \cong \{1\}$, the group with one element.

If S a finite direct sum , where each S_α is any of $\mathbf{Z}^+, \mathbf{Q}^+$ or $N(2)$; then
THEOREM 1.2[1]: $Aut\ S \cong (Aut\ S_{\beta_1} \varsigma\ S_{n_1}) \times \cdots \cdots \times (Aut\ S_{\beta_r} \varsigma\ S_{n_r})$, where ς denotes the wreath product, $(i \le i \le r)$.

II. Group of Morphisms and Automorphism Groups

Let A be an object of a category C. If a subset $G(A)$ of $Hom(A,A)$ is a group under composition of morphisms of C with 1_A as the identity element, $G(A)$ will be called a **group of morphisms** of A. Morphism is actually a structure-preserving map from one mathematical structure to another. In theory of sets, linear algebras, groups, topologies, morphisms are repectively functions, linear transformations, group homomorphisms and continuous functions.

Now the subset of $Hom(A,A)$ consisting of all $f \in Hom(A,A)$ for which the inverse exists is the largest group of morphisms of A and contains all groups of morphisms of A. This group will be called the *automorphism group* of A and denoted by $Aut A$. FNow for an object A of certain categories, $AutA$ is sometimes very interesting, and has some important structures.

For example, if the object A is V, a vector space over the field F, then $Aut A = Aut V =$ the group of all invertible linear operators of V, and hence $Aut V \cong M^{n \times n}(F)$, the group of all $n \times n$ non-singular matrices with entries in F. For $\mathbf{R}$ and $\mathbf{C}$ in place of V, these are $GL(n, \mathbf{R})$ and $GL(n, \mathbf{C})$ respectively. It is known that several subgroups of $GL(n, \mathbf{R})$ and $GL(n, \mathbf{C})$ are very important and widely used in theoretical physics. If the object A is a group or a topological space, $Aut A$ has different structure, and the aim in this study is to determine it using the notions of the mentioned few works. In this paper, the structures of $Aut\ A$ have been determined for those cases when A is any one of cyclic groups, the additive group $\mathbf{Q}$ of rational numbers, the additive group $\mathbf{R}$ of real numbers and the topological space $\mathbf{R}$.

For obtaining the structures of $Aut\ A$, the concepts of cyclic groups C_n infinite or finite with one generator, the additive group $\mathbf{Z}_n$ of the residue classes of the integers modulo some positive integers, say, n, additive group $\mathbf{Q}$ of rational numbers, additive group R of real numbers and the real topological spaces etc. have been used. The group of all automorphisms of G, i.e., the group of all 1-1 homomorphisms of G onto itself is denoted by $Aut G$. It is assumed here that group homomorphisms, group isomorphisms and group automorphisms etc. are known well to the readers.

III. Automorphism Groups of Real numbers and Real Topological spaces

It is easy to see that if G is infinite cyclic with generator x, then the only automorphisms of G are given by the maps $x \xrightarrow{\alpha} x$ and $x \xrightarrow{\beta} x^{-1}$. Hence $Aut\ G$ is the cyclic group of order 2 generated by β, i.e., $Aut\ G = C_2(\beta)$.

For a finite cyclic group G, the situation is more complex. If x is a generator of G, then the automorphisms of G are precisely the homomorphisms of G given by the maps $x \xrightarrow{f_i} x^i$, where i is any integer relatively prime to n. Thus the order of $Aut\ G$ is $\phi(n)$, where n is the order of G and ϕ is the Euler function. We now determine the structure of $Aut\ C_n$. This is done by a manner different to that used in Scott

(1964) and Zassenhaus (1958). Consider the ring $\mathbf{Z}_n$ of the residue classes of the integers modulo n ($n \geq 2$). Then the set of elements $\bar{r} \in \mathbf{Z}_n$, with $(r, n) = 1$ is a group under multiplication. For, since there are integers a, b such that $a\,r + b\,n = 1$ and so, we have $\bar{a}\,\bar{r} = 1$, $\bar{a}$ is the multiplicative inverse of $\bar{r}$, the bar denoting the residue class modulo n. The authors denote this group by $[n]$. Clearly the order of $[n]$ is $\phi(n)$, where ϕ is the Euler function. Now the map $\psi : Aut\, C_n \to [n]$ given by $\psi(f) = \bar{r}$, where C_n being the cyclic group of order n and $f(x) = x^r$, is an isomorphism. Thus this can be obtained in the following theorem.

Theorem 3.1[3]: $Aut\, C_n \cong [n]$.

For the structure of the group $[n]$, it needs to prove that:

Theorem 3.2[3]: If a and b are two relatively prime integers, then $[ab] \cong [a] \times [b]$ (direct product).

Proof: The elements of $[ab]$ are $\overline{aq_{j(r_i)} + r_i}$, where $\{r_k\}$ is the set of all positive integers less than a and relatively prime to a, and for a fixed r_i, $aq_{j(r_i)} + r_i$ is the set of integers in

$\{a + r_i, 2a + r_i, \cdots, (b-1)a + r_i\}$ which are relatively prime to a.

Define $\psi : [ab] \to [a]$ by $\psi(\overline{aq_{j(r_i)} + r_i}) = \bar{\bar{r}} \in [a]$. Then, ψ is an onto homomorphism and

$Ker\psi = \{\overline{aq_{j(r_i)} + 1}\}$. Now, $\bar{\psi} : Ker\psi \to [b]$ given by $\bar{\psi}(\overline{aq_{j(r_i)} + r_i}) = \overline{\overline{aq_{j(r_i)} + r_i}} \in [b]$ is an isomorphism.

Hence the sequence of abelian multiplicative groups and group homomorphisms

(A) $\qquad\qquad 1 \to [b] \xrightarrow{\ \bar{\psi}^{-1}\ } [ab] \xrightarrow{\ \psi\ } [a] \to 1$ is exact. Also, $\psi^* : [ab] \to [b]$ given by

$\psi^*(\overline{aq_{j(r_i)} + r_i}) = \overline{\overline{aq_{j(r_i)} + r_i}} \in [b]$ is a well defined homomorphism and $\psi^* \bar{\psi}^{-1} = 1_{[b]}$. Thus the sequence (A) splits. Hence $[ab] \cong [a] \times [b]$.

Theorem 3.3[3]: (i) If p is an odd prime, $[p^n] \cong C_{\phi(p^n)}$ for each positive integer n.

(ii) $[2^n] \cong C_2 \times C_{2^{n-2}}$ for each $n \geq 2$.

Proof: (i) The order of $[p^n] = \phi(p^n)$

$$= p^{n-1}(p-1).$$

The element $\bar{2}$ of $[p^n]$ must have order exactly $p^{n-1}(p-1)$. Hence $\bar{2}$ is a generator of $[p^n]$. Thus, $[p^n] \cong C_{\phi(p^n)}$.

(ii) For $n = 2$ and 3, the result is easily verified; for $[2^2] = <\bar{3}>$ and $[2^3] = <\bar{3}> \times <\bar{5}>$.

The authors first noted that for each $\bar{a} \in [2^n]$, $\bar{a}^{2^{n-2}} = \bar{1}$, the identity element of $[2^n]$. For $n = 2, 3, 4, 5$, this is true. Let it be true for $n \geq 2$, let a be any integer then $a^{2^{n-2}} = k2^n + 1$, for some integer k, so that $a^{2^{n-1}} = k^2 2^{2n} + k2^{n+1} + 1 = l2^n + 1$, where $l = k^2 2^n + 2k$. Hence $\bar{a}^{2^{n-1}} = \bar{\bar{1}}$, where $\bar{\bar{1}}$ is the identity element of $[2^{n+1}]$.

The order of $\bar{3}$ in $[2^n]$ is exactly 2^{n-2}. To do so we show that for all $n \geq 4$, $\bar{3}^{2^{n-3}} \neq \bar{1}$ in $[2^n]$, i.e., $3^{2^{n-3}} \neq k2^n + 1$ for any integer k.

By the above paragraph, there exists an integer l such that $3^{2^{n-3}} = l2^{n-1} + 1$. Hence the authors had to show that l is odd. This can be done by induction on n. This is seen to be true for $n = 4$. Assume that for $n > 4$, $3^{2^{n-3}} = l2^{n-1} + 1$, where l is odd. Squaring both sides,

$3^{2^{n-2}} = l^2 2^{2n-2} + l2^n + 1 = (l^2 2^{n-2} + l)2^n + 1 = l'2^n + 1,$ where l' is odd. Hence $\overline{3}$ has order 2^{n-2} in $[2^n]$ i.e., $<\overline{3}>$, the cyclic subgroup generated by $\overline{3}$ in $[2^n]$ has order 2^{n-2}.

Let $y \in [2^n]$, but $y \notin <\overline{3}>$. Then, $y^2 \in <\overline{3}>$, since the order of $[2^n]$ is 2^{n-1}. Now y^2 cannot be equal to an odd power of $\overline{3}$, for then y will be of order 2^{n-1}, which is impossible by the second paragraph of our proof. Hence $y^2 = \overline{3}^{2r}$, for some non-negative integer r. Then $\overline{3}^r y^{-1}$ has order 2 and it does not belong to $<\overline{3}>$. Therefore $[2^n] \cong <\overline{3}> \times <\overline{3}^r y^{-1}>$, the internal direct product. Thus, $[2^n] \cong C_2 \times C_{2^{n-2}}$.

Therefore, the consequences of theorems 3.1, 3.2 and 3.3 together establish the theoremstated below:

Theorem 3.4: Let n be positive integer $n = p_1^{e1} \cdots p_r^{er}$ where $p_1, \cdots, p_r$ are prime numbers with $p_1 < p_2 < \cdots < p_r$ and $e_1, e_2, \cdots, e_r$ are positive integers. Then

$$Aut\, C_n \cong [n] \cong \begin{cases} C_{2^{e_1-2}} \times \times C_2 \times C_{\phi(p_2^{e_2})} \times \cdots \times C_{\phi(p_r^{e_r})} & if\ p_1 = 2, \\ C_{\phi(p_1^{e_1})} \times \cdots \times C_{\phi(p_r^{e_r})} & if\ p_1 \neq 2. \end{cases}$$

It is clear that theorem 3.4 describe the structure of $Aut\, C_n$ for an arbitrary positive integer $n \geq 2$.

Now the following propositions will focus the structure of $Aut\,$Qand AutR , where Q is the additive group of rational numbers and R is the additive group of real numbers.

Proposition 3.5: $Aut\, \mathbf{Q} \cong \mathbf{Q}^*$, where $\mathbf{Q}^*$is the multiplicative group of all non-zero rationals.

Proof: Consider the map $\varphi : Aut\, \mathbf{Q} \rightarrow \mathbf{Q}^*$given by $\varphi(f) = f(1)$, and the map $\psi : \mathbf{Q}^* \rightarrow Aut\, \mathbf{Q}$ given by $\psi(x) = f$, where, for each $y \in \mathbf{Q}, f(y) = yx$. Then φ and ψ are homomorphisms.

Now, for each $x \in \mathbf{Q}^*$, $(\varphi\psi)(x) = \varphi(\psi(x)) = (\psi(x))(1) = x$, by the definitions of φ and ψ . Hence $\varphi\psi = 1_{\mathbf{Q}^*}$.

Also, for each $f \in Aut\, \mathbf{Q}, (\psi\varphi)(f) = \psi(\varphi(f)) = \psi(f(1)) = g \in Aut\, \mathbf{Q}$, where, for each $y \in \mathbf{Q}$, $g(y) = yf(1) = f(y)$ so that $g = f$. Thus, $(\psi\varphi)(f) = f$. Therefore $(\psi\varphi = 1_{AutQ}$.Therefore φ and ψ are isomorphism so that $Aut\, \mathbf{Q} \cong \mathbf{Q}^*$.

The authors noted from the above proposition 3.5 that$Hom(\mathbf{Q}, \mathbf{Q})$, the additive group of all additive endomorphisms of **Q**, is given by$Hom(\mathbf{Q}, \mathbf{Q}) = \{ f:\mathbf{Q} \rightarrow \mathbf{Q})/ f(x)=ax, a \in \mathbf{Q}\} \cong \mathbf{Q}$. Here, the isomorphism is given by $f \longleftrightarrow f(1)$.

Therefore, Aut**R**, where **R** is the additive group of real numbers, is now clear and is given by:

Proposition 3.6: $Aut\, \mathbf{R} \cong \mathbf{R}^*$, where$\mathbf{R}^*$ is the multiplicative group of all non-zero real numbers.

Proof: The map $\varphi : Aut\, \mathbf{R} \rightarrow \mathbf{R}^*$ given by $\varphi(f) = f(1)$gives the required isomorphism for result of the aboveProposition 3.6. The arguments similar to those in the proof of Proposition3.5, prove the statement.

Note that if **R** is the additive group of all real numbers and $\mathbf{R}^+$is the multiplicative group of all positive real numbers, then the map $\varphi : \mathbf{R} \rightarrow \mathbf{R}^+$ given by $\varphi(x) = e^x$ is an isomorphism of **R** onto $\mathbf{R}^+$. So, $(\mathbf{R}, +) \cong (\mathbf{R}^+, \times)$. Since $(\mathbf{R}^+, \times)$ is a subgroup of index 2 in the group $(\mathbf{R}^*, \times)$, $Aut(\mathbf{R}, +)$ contains an isomorphic copy of $(\mathbf{R}, +)$ as a subgroup of index 2.

We shall now determine the structure of the automorphism group of the topological space $\mathbb{R}$with the usual metric topology. It is the group of all homeomorphisms of the real line, i.e., with the topology induced by the metric d where $d(x,y) = |x - y|$. We denote this group by $Aut\mathbb{R}$.

We note that the functions $x \rightarrow cx$(magnification), $x \rightarrow x^n$, and $x \rightarrow x^{\frac{1}{n}}$, where c is any non-zero real number and n is any odd positive integer, are homeomorphisms of $\mathbb{R}$ onto itself, i.e., automorphisms of the real line. Also, $x \rightarrow x + a$(translation) is an automorphism of this space for each real number a. The map $x \rightarrow x^{2n}$is not a homeomorphism since it is not 1-1.The trigonometric functions are not 1-1, the exponential functions are not onto and the logarithmic function is not defined on the whole of $\mathbb{R}$. The map $x \rightarrow cx$ includes as a particular case the reflection $x \rightarrow -x$ at the point 0. It is clear that the reflection about any point is a homeomorphism.Therefore, the homeomorphisms of the real line consist of all reflections, all magnifications, all translations and all maps $x \rightarrow x^a$(a an odd integer or its reciprocal), and their compositions.Now, every

translation is a composition of two reflections. For, if we consider the translation $\tau_a : x \rightarrow x + a$, we can verify that $\tau_a = \rho_{\frac{a}{2}} \rho_0$, where $\rho_{\frac{a}{2}}$ and ρ_0 are reflections at the points $\frac{a}{2}$ and 0 respectively. In fact, *Aut***R** is generated by

(i)   All maps $\mu_c : x \rightarrow cx$, where c is any non-zero real numbers,

(ii) All maps $\pi_{2m+1} : x \rightarrow x^{2m+1}$ and $\pi'_{2n+1} : x \rightarrow x^{\frac{1}{2n+1}}$, where m, n are any positive integers, and

(iii) All maps $\rho_a : x \rightarrow x + a, \ a \in \mathbf{R}$.

Now, it can be easily verified that $M = \{\mu_c\}_{c \in R^*} \cong R^*$, R^* being the multiplicative group of all non-zero real numbers, and $P = \{\pi_{2m+1}, \pi'_{2n+1}\}_{m, n \in N} \cong Q_{odd}$, where Q_{odd} is the multiplicative group of all rational numbers of the form $\dfrac{2m+1}{2n+1}$. Hence $R = \{\rho_a\}_{a \in R} \cong \mathbf{R}$, the additive group of all real numbers and thus we have the proposition:

Proposition: 3.7: $Aut\, R \cong R^* * Q_{odd} * R$, where $*$ the denote the free product.

Concluding remark: The structure of automorphism groups of finite cyclic groups is known through the theorem 3.1, theorem 3.3 and theorem 3.4. For the additive group **Q** of rationals and **R** of real numbers, *Aut* **Q** and *Aut* **R** are to be known by proposition 3.5 and finally, the automorphism group of real topological spaces has been determined by proposition 3.7.

References

[1].   M. A. Hossain, The automorphism group of special semigroups. *Journal of Math.and Mathematical Sciences* 25(2010):9-12.
[2].   M. A. Hossain and S. Majumdar, On some characterizations of special semigroups, *Rajshahi University Journal of Sciences* 35 (2007): 119-125.
[3].   M. A. Hossain and S. Majumdar, On automorphism groups of some particular groups,
       Submitted to J. Bangladesh Acad. of sci. 2016.
[4].   S. Majumdar, K.K. Dey and M. A. Hossain, Direct product and Wreath productof transformation semigroups, *GANIT J. Bangladesh Math. Soc*. 31(2011): 1-7.
[5].   S. Majumdar and M.A.Hossain, The endomorphism semigroup of a special semigroup. *J.Bangladesh Acad. of sci.* 32(1) (2008): 55-60
[6].   W.R. Scott, Grouptheory, Prentice-Hall Inc.,Engleood Cliffs, New Jersy(1964).
[7].   H. Zassenhaus,The Theory of Groups. Chelsea, NewYork(1958).