*J. Bangladesh Acad. Sci., Vol. 40, No. 2, 109-115, 2016*

# ON AUTOMORPHISM GROUPS OF SOME PARTICULAR GROUPS

MOHD. ALTAB HOSSAIN* AND SUBRATA MAJUMDAR

*Department of Mathematics, University of Rajshahi, Rajshahi-6205, Bangladesh*

## ABSTRACT

The cyclic groups, the additive group **Q** of rational numbers and the additive group **R** of real numbers are sometimes very useful elements in many studies. In this paper, the authors concentrated their intuition in determining the structures of the automorphism groups of these useful groups in the light of previous works.

Key words: Automorphism, Cyclic group, Additive group, Generator, Object, Structure

## INTRODUCTION

Majumdar and Mallick (1987) studied a class of abelian groups having a set of generators such that each non-zero element of the group is expressible uniquely in terms of the generators using each generator its inverse, but not both, at most once. Following it a class of commutative semigroups termed special semigroups was studied by Hossain and Majumdar (2007). Later, the studies of endomorphism semigroups and the automorphism groups for this class of groups were done by Majumdar *et al.* (2008) and Hossain (2010), respectively. Some important structures for this class were determined in those studies. Now for an object ***A*** of certain categories, the automorphism group of ***A*** denoted by *Aut****A*** 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 $\boldsymbol{V}$, 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 **R** and **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 $G$, $Aut\,A\,(= Aut\,G)$ has different structure, and the aim of this study was to determine it using the notions of their above mentioned few works. In this paper, the structures of $Aut\,G$ have been determined for those cases when the group $G$ is any one of cyclic groups, the additive group **Q** of rational numbers and the additive group **R** of real numbers. Sometimes, a few terminologies of Zassenhaus (1958) and Scott (1964) have been also used in this study.

*Corresponding author: <al_math_bd@yahoo.com>.

## PRELIMINARIES AND PREVIOUS RESULTS

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 $A$. Then the subset of $Hom(A, A)$ consisting of all $f \in Hom(A, A)$ for which the inverse exists in 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 $AutA$. For obtaining the structures of this class of groups, a few objects and gluing operations are very necessary. The cyclic groups infinite or finite with one generator, the additive group of the residue classes of the integers modulo some positive integers, say, $n$, additive group of rational numbers, additive group of real numbers etc. are main objects in this study, and these are denoted by $C_\infty$ or $C_n$, $\mathbf{Z}_n$, $\mathbf{Q}$ and R, respectively. The group of all automorphisms of $G$, i.e., the group of all 1-1 homomorphisms of G onto itself is denoted by $AutG$. It is assumed here that group homomorphisms, group isomorphisms and group automorphisms etc. are known well to the readers.

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 $\mathrm{G} \times 1 = \{(\mathrm{g},1) \mid \mathrm{g} \in \mathrm{G}\}$ and $1 \times \mathrm{H} = \{(1,\mathrm{h}) \mid \mathrm{h} \in \mathrm{H}\}$.

Clearly, $G \cong G \times 1$ since $g \to (g, 1)$ 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 ¨ is the set of ordered pairs $\{(h,k) \mid \ h \in H, k \in K\}$ together with the binary operation defined by $(h_1, k_1)(h_2, k_2) = (h_1 \ddot{}_{k_1}(h_2), k_1 k_2)$, where $\ddot{}_k$. is written for $\ddot{}(k)$, $k \in K$ is a group. This group is denoted by $H \times_{\ddot{}} K$ for the semidirect product of the group $H$ by the group $K$. write $\boldsymbol{N} \rtimes \phi K$ 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 $\ddot{}_i$ 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 $\cdot_i : G_i \to H, i \in I$ there exists a unique homomorphism

$f: G \to H$ such that $\cdot_i = f^{\cdot\cdot}{}_i$ for every $i \in I$.

On the other hand, a group $G$ is said to be the free product of its subgroups $A_{\sim}, \sim \in I$ if the subgroups $A_{\sim}$ generate $G$ i.e., every element $g$ of $G$ is the product of a finite number of the elements of the $A_{\sim}$: $g = a_1 a_2 \cdots a_n$, $\sim_i \in A_{\sim_i}, (i = 1, 2, \cdots, n)$, 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 of transformation groups $G$ and $H$ on sets $A$ and $B$, respectively, written $G \wr H$, is the group of all permutations $\bar{}$ on $A \times B$ such that $\bar{}((a,b)) = (¥_b(a), ¦(b))$, $a \in A$, $b \in B$, where $¦ \in H$ and for each $b \in B$, $¥_b$ is a permutation of $G$ on $A$, but for different $b$'s the choice of the permutations $¥_b$ are independent.

Now one can recall the structures obtained from earlier one research work Hossain (2010) in the following way:

If $\boldsymbol{Z}^+$, $\boldsymbol{Q}^+$ and $\boldsymbol{N}(2)$ represent the additive group of all positive integers, additive group of all positive rationals and additive group of all positive rationals having denominators $2^x$ for any non-negative integer respectively, then

THEOREM 1:

*(i) Aut* $\boldsymbol{Z}^+ \cong$ *{1}, the group with one element,*

*(ii) Aut* $\boldsymbol{Q}^+ \cong \boldsymbol{Q}^+$,

*(iii) Aut (*$\boldsymbol{N}$*(2))* $\cong$ *{1}, the group with one element.*

If $S$ a finite direct sum, where each $S_\alpha$ is any of $\boldsymbol{Z}^+$, $\boldsymbol{Q}^+$ or $\boldsymbol{N}(2)$; then

THEOREM 2**:**

*Aut* $S \cong (Aut\ S_{\beta_1} \wr S_{n_1}) \times \cdots\cdots \times (Aut\ S_{\beta_r} \wr S_{n_r})$, *where* $\wr$ *denotes the wreath product,* $(i \le i \le r)$.

## AUTOMORPHISM GROUP OF CYCLIC GROUPS

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 $x \longrightarrow^{\sim} x$ and $x \longrightarrow x^{-1}$. Hence *Aut G* is the cyclic group of order 2 generated by , i.e., $Aut\ G = C_2(\ )$.

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 $¤(n)$, where *n* is the order of *G* and ¤ 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 $ar+bn=1$ 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 $¤(n)$, where ¤ is the Euler function.

Now the map $\cdot : Aut\, C_n \to [n]$ given by $\cdot(f)=\bar{r}$, 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: $Aut\, C_n \cong [n]$.

One can now establish the structure of the group $[n]$. For this purpose, it needs to prove that:

THEOREM 4: 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 $\cdot : [ab] \to [a]$ by $\cdot(\overline{aq_{j(r_i)}+r_i}) = \bar{\bar{r}} \in [a]$. Then, $\psi$ is an onto homomorphism and $Ker \cdot = \{aq_{j(r_i)}+\bar{1}\}$. Now, $\bar{\cdot} : Ker \cdot \to [b]$ given by $\bar{\cdot}(\overline{aq_{j(r_i)}+r_i}) = \overline{\overline{aq_{j(r_i)}+r_i}} \in [b]$ is an isomorphism.

Hence the sequence of abelian multiplicative groups and group homomorphisms

(*A*) $1 \to [b] \xrightarrow{\bar{\cdot}^{-1}} [ab] \xrightarrow{\cdot} [a] \to 1$ is exact. Also, $\cdot^{*} : [ab] \to [b]$ given by $\cdot^{*}(\overline{aq_{j(r_i)}+r_i}) = \overline{\overline{aq_{j(r_i)}+r_i}} \in [b]$ is a well defined homomorphism and $\cdot^{*}\bar{\cdot}^{-1} = 1_{[b]}$. Thus the sequence $(A)$ splits. Hence $[ab] \cong [a] \times [b]$.

THEOREM 5: (i) If *p* is an odd prime, $[p^n] \cong C_{¤(p^n)}$ 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 $\bar{3}$ has order $2^{n-2}$ in $[2^n]$ i.e., $<\bar{3}>$, the cyclic subgroup generated by $\bar{3}$ in $[2^n]$ has order $2^{n-2}$.

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

The structure of $Aut\, C_n$ for an arbitrary positive integer $n \geq 2$ follows from the above three theorems 1, 2 and 3, and can be stated as:

THEOREM 6: Let *n* be positive integer $n = p_1^{e^1} \cdots p_r^{e_r}$ 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

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

## THE AUTOMORPHISM GROUPS OF Q AND R

The following propositions describe the structure of $Aut\, \mathbf{Q}$ and *Aut* **R**, where **Q** is the additive group of rational numbers and **R** is the additive group of real numbers.

PROPOSITION 7:

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

Proof: Let $f \in Aut\ \mathbf{Q}$ and let $f(x) = 1$. Then, $x \neq 0$. Let $m,\ n \in \mathbf{Z},\ n \neq 0$. Then, $f(m) = mx$. Let $f(m) = mx$ $f(\frac{m}{n}) = y$, then $f(m) = f(n\frac{m}{n}) = n\,f(\frac{m}{n}) = n\,y$. So, $f(\frac{m}{n}) = y = \frac{m}{n}x = \frac{m}{n}f(1)$.

Conversely, let $x \neq 0$ be any element of **Q.** Define $f: \mathbf{Q} \to \mathbf{Q}$ as follows: $\frac{m}{n},\ m,\ n \in \mathbf{Z}$ for each $m,\ n \in \mathbf{Z},\ n \neq 0,\ f(\frac{m}{n}) = \frac{m}{n}x$. Then, $f(1) = x$, and so, $f(\frac{m}{n}) = \frac{m}{n}f(1)$. Clearly $f$ is an isomorphism of Q. Here $f^{-1}(\frac{m}{n}) = \frac{m}{n}\frac{1}{x}$.

Consider the map $\ddot{}: Aut\ \mathbf{Q}$ ì $\mathbf{Q}^*$ given by $\ddot{}(f) = f(1)$**.** Clearly $f(1) \neq 0$**, so that** $f(1) \in \mathbf{Q}^*$. It can seen that, if $f, g \in Aut\ \mathbf{Q}$**, then** $\ddot{}(fg) = (fg)(1) = f(1)g(1) = \ddot{}(f)\ddot{}(g)$, Thus $\ddot{}$ is a homorphism**.**

Next consider the map $\cdot: \mathbf{Q}^* \to Aut\ \mathbf{Q}$ given by $\cdot(x) = f$, where, for each $y \in \mathbf{Q}$, $f(y) = yx$. For $x_1,\ x_2 \in \mathbf{Q}^*$**,** let $\cdot(x_1) = f_1,\ \cdot(x_2) = f_2$**,** then $\cdot(x_1x_2) = f$, where, for each $y \in \mathbf{Q},\ f(y) = y(x_1x_2) = y(x_2x_1) = (yx_2)x_1 = f_1(yx_2) = f_1(f_2(y)) = (f_1f_2)(y)$. Thus $f = f_1f_2$, i.e., $\cdot(x_1x_2) = \cdot(x_1)\cdot(x_2)$. Hence $\cdot$ is also a homomorphism.

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

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

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

Finally, *Aut* **R**, the group of automorphisms of **R** where **R** is the additive group of real numbers, will now be determined.

PROPOSITION 8: $Aut\ \mathbf{R} \cong \mathbf{R}^*$**,** where $\mathbf{R}^*$ is the multiplicative group of all non-zero real numbers.

Proof: The map $\ddot{}: Aut\ \mathbf{R} \to \mathbf{R}^*$ given by $\ddot{}(f) = f(1)$ gives the required isomorphism for result of the above Proposition 8. The arguments similar to those in the proof of Proposition7, prove the statement.

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 $\ddot{}$**:** $\mathbf{R} \to \mathbf{R}^+$ given by $\ddot{}(x) = e^x$ 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.

## CONCLUDING REMARK

The structure of automorphism groups of finite cyclic groups is known through the theorems 3, 5 and 6. For the additive groups **Q** of rational numbers and **R** of real numbers, *Aut* **Q** and *Aut* **R** are to be known by Propositions **7** and **8**. Moreover, in future, automorphism groups of the category of some objects in topological spaces will be determined due to perspective of the present work.

## REFERENCES

Hossain, M. A. 2010. The automorphism group of special semigroups. *Journal of Math. and Mathematical Sciences* **25**: 9-12.

Hossain, M. A. and S. Majumdar. 2007. On some characterizations of special semigroups. *Rajshahi University Journal of Sciences* **35**: 119-125.

Majumdar, S. and A. K. Mallick. 1987. Special abelian groups. *The Nepali Math. Science Report* **12**(2).

Majumdar, S., K. K. Dey and M. A. Hossain. 2011. Direct product and Wreath product of transformation semigroups. *GANIT J. Bangladesh Math. Soc*. **31**: 1-7.

Majumdar, S. and M.A. Hossain. 2008. The endomorphism semigroup of a special semigroup. *J. Bangladesh Acad. Sci.* **32(1)**: 55-60.

Scott, W. R. 1964. Group theory. Prentice-Hall Inc., Engleood Cliffs, New Jersy.

Zassenhaus, H. 1958. The Theory of Groups. Chelsea, New York.

(*Received revised manuscript on 17 August, 2016*)