Journal of Algebraic Structures and Their Applications
ISSN: 2382-9761
www.as.yazd.ac.ir

Algebraic Structures and Their Applications Vol. 1 No. 1 (2014), pp 49-56.

AUTOMORPHISM GROUP OF GROUPS OF ORDER pqr

MODJTABA GHORBANI* AND FARZANEH NOWROOZI LARKI

Communicated by M.A. Iranmanesh

Abstract. Hölder in 1893 characterized all groups of order pqr where $p > q > r$ are prime numbers. In this paper, by using new presentations of these groups, we compute their full automorphism group.

1. Introduction

By an automorphism of an algebraic structure G we mean a one-to-one mapping $f : G \to G$ preserving the law of composition in G. The set of all such f under composition of mapping forms a group which is denoted by $Aut(G)$. In this paper we are going to study $Aut(G)$ when G is a group.

The topic of automorphism group of a group has interested researches for years. For example, we are aware of automorphism group of abelian groups [3, 14], but for non-abelian groups the problem is

MSC(2010): Primary:20D45 Secondary:20F28

Keywords: Affine group, Frobenius group, automorphism group.

Received: 20 May 2014, Accepted: 18 Nov 2014.

*Corresponding author

© 2014 Yazd University .

so much complicated. Finite groups whose automorphism group is abelian were first considered by G. A. Miller, who studied a group of order 64 with an abelian automorphism group of order 128 [12]. In general, the problem of classification of non-abelian groups with abelian automorphism group is still an open problem, but in special cases this problem is solved, see for example [1, 2, 4, 8, 9, 10, 11, 13, 15]. Let G be a group of order pqr where $p > q > r$, the aim of this paper is to compute the full automorphism group of G. Our characterization of $Aut(G)$ is accomplished in three main steps. The first observation is that to compute the presentation of G and then by using Theorem 1, we describe the full automorphism group of G. In [6] the presentations of groups of order pqr are introduced. Let $T_{p,q} = \langle a, b : \ a^p = b^q = 1, bab^{-1} = a^u\rangle$ and $o(u) = q$ in $\mathbb{Z}_p^*$. We can prove that all groups of order $pqr (p > q > r)$ are isomorphic to exactly one of the following presentations:

- $G_1 = \mathbb{Z}_{pqr}$,
- $G_2 = \mathbb{Z}_r \times T_{p,q}(q|p-1)$,
- $G_3 = \mathbb{Z}_q \times T_{p,r}(r|p-1)$,
- $G_4 = F_{p,qr}(qr|p-1)$,
- $G_5 = \mathbb{Z}_p \times T_{q,r}(r|q-1)$,
- $G_{i+5} = \langle a, b, c : a^p = b^q = c^r = 1, ab = ba, c^{-1}bc = b^u, c^{-1}ac = a^{v^i}\rangle$, where $r|p-1, q-1, o(u) = r$ in $\mathbb{Z}_q^*$ and $o(v) = r$ in $\mathbb{Z}_p^*$ $(1 \leq i \leq r-1)$.

By using above presentations, we can conclude that there are six groups of order $2pq$ as follows:

- $R_1 = \mathbb{Z}_{2pq}$,
- $R_2 = D_{2pq}$,
- $R_3 = \mathbb{Z}_2 \times T_{p,q}$,
- $R_4 = \mathbb{Z}_p \times D_{2q}$,
- $R_5 = \mathbb{Z}_q \times D_{2p}$,
- $R_6 = \langle a, b, c : \ a^p = b^q = c^2 = 1, bab^{-1} = a^u, bc = cb, cac = a^{-1}\rangle$, where D_{2n} denotes the dihedral group of order $2n$.

By a similar method, one can see there are seven groups of order $3pq$ as follows:

- $S_1 = \mathbb{Z}_{3pq}$,
- $S_2 = \mathbb{Z}_3 \times T_{p,q}(q|p-1)$,
- $S_3 = \mathbb{Z}_q \times T_{p,3}(3|p-1)$,
- $S_4 = F_{p,3q}(3q|p-1)$,
- $S_5 = \mathbb{Z}_p \times T_{q,3}(3|q-1)$,
- $S_6 = \langle a, b, c : a^p = b^q = c^3 = 1, ab = ba, c^{-1}bc = b^w, c^{-1}ac = a^s\rangle$, where $o(w) = 3$ in $\mathbb{Z}_q^*$ and $o(s) = 3$ in $\mathbb{Z}_p^*$,
- $S_7 = \langle a, b, c : a^p = b^q = c^3 = 1, ab = ba, c^{-1}bc = b^{w^2}, c^{-1}ac = a^s\rangle$, where $o(w) = 3$ in $\mathbb{Z}_q^*$ and $o(s) = 3$ in $\mathbb{Z}_p^*$.

First we compute explicit formulas for groups of order pqr where $r = 2, 3$ and then we apply our method to compute the full automorphism group of groups of order pqr. Here, our notation is standard and mainly taken from the standard books of group theory such as [5, 7, 16].

2. Main Results and Discussions

Let $G = H \times K$ be direct product of groups H and K. It is natural to ask how the automorphisms of G are related to those of H and K.

Theorem 2.1. [7] *Let H, K be the normal subgroups of G such that $G = H \times K$. Then*

- $Aut(H) \times Aut(K) \hookrightarrow Aut(G)$,
- *If G be finite and $(|G|, |H|) = 1$, then $Aut(H) \times Aut(K) \cong Aut(G)$.*

Lemma 2.2. [5] *The automorphism group of dihedral D_{2n} is isomorphic to the affine group $Aff(\mathbb{Z}_n) = \{f : x \to ax + b : \ (a, n) = 1\}$.*

2.1. **Automorphism group of groups of order $2pq$.** Here we determine the full automorphism group of groups of order $2pq$. To do this, first we compute the automorphism group of Frobenius group. A Frobenius group of order pq where p is prime and $q|p-1$ is a group with the following presentation:

$$F_{p,q} = \langle a, b : \ a^p = b^q = 1, b^{-1}ab = a^u \rangle, \tag{1}$$

where u is an element of order q in multiplicative group $\mathbb{Z}_p^*$. If q be a prime number, then $F_{p,q} \cong T_{p,q}$. Here, we determine the automorphism group of $F_{p,q}$.

Lemma 2.3. *We have*

$$|Aut(F_{p,q})| = p(p-1).$$

Proof. Let u is an element of order q in multiplicative group $\mathbb{Z}_p^*$. By considering the presentation of $F_{p,q}$ in equation (1), one can see that all elements of this group are as follows:

$$\{1, a, \cdots, a^{p-1}, b, ba, \cdots, ba^{p-1}, \cdots b^{q-1}, b^{q-1}a, \cdots, b^{q-1}a^{p-1}\}.$$

Let $\alpha \in Aut(F_{p,q})$, since $\langle a \rangle$ is a characteristic subgroup of $F_{p,q}$ then necessarily $\alpha(\langle a \rangle) = \langle a \rangle$ and then there exist $1 \le i \le p-1$ such that $\alpha(a) = a^i$. We claim that $\alpha(b) = ba^j$, where $0 \le j \le p-1$. Suppose to the contrary that $\alpha(b) = b^r a^s$, where r, s are integers with $1 < r \le q-1$. Since $\alpha(b^{-1}ab) = a^{ui}$, then $a^{-s}b^{-r}a^ib^ra^s = a^{ui}$. This leads us to conclude that $u^{r-1} = 1 \ (mod\ p)$, a contradiction. Hence, $r = 1$ and thus $|Aut(F_{p,q})| \ge p(p-1)$. Consequently, all automorphisms of $Aut(F_{p,q})$ are of form $\alpha_{i,j}$ where $\alpha_{i,j}(a) = a^i$ and $\alpha_{i,j}(b) = ba^j$. On the other hand, all such automorphisms are distinct and for $\alpha_{r,s}, \alpha_{i,j} \in Aut(F_{p,q})$ we have $\alpha_{r,s}\alpha_{i,j} \in Aut(F_{p,q})$. This completes the proof.

Theorem 2.4. *Let p is a prime number and $q|p-1$, then*

$$Aut(F_{p,q}) \cong F_{p,p-1}.$$

Proof. Consider two following maps

$$\beta : \begin{cases} a \to a^{t^{-1}} \\ b \to b \end{cases}, \alpha : \begin{cases} a \to a \\ b \to ba \end{cases}$$

where t is an element of order $p-1$ in $\mathbb{Z}_p^*$ and t^{-1} is its inverse. One can prove that α, β are distinct homomorphisms of $F_{p,q}$ where $o(\alpha) = p-1$ and $o(\beta) = p$. Consequently,

$$\begin{aligned} \alpha\beta(a) &= \alpha(a) = a^{t^{-1}} = \beta\alpha^t(a), \\ \alpha\beta(b) &= \alpha(b) = ba. \end{aligned}$$

On the other hand, $\beta\alpha^t(b) = \beta(ba^t) = b(a^{t^{-1}})^t = ba$ and so $\alpha\beta(b) = \beta\alpha^t(b)$. Hence, for all $x \in F_{p,q}$, $\alpha\beta(x) = \beta\alpha^t(x)$ and thus

$$\beta^{-1}\alpha\beta = \alpha^t.$$

Let also

$$H = \langle \alpha, \beta : \ \alpha^p = \beta^{p-1} = id, \beta^{-1}\alpha\beta = \alpha^t \rangle,$$

where $t^{p-1} \equiv 1 \ (mod\ p)$. Then $H \cong F_{p,p-1}$ is a subgroup of $Aut(F_{p,q})$ of order $p(p-1)$ and by Lemma 2, the proof is completed.

Corollary 2.5. *The automorphism group of groups of order $2pq$ are as follows:*

(1) $Aut(R_1) = \mathbb{Z}_{2pq}^*$,
(2) $Aut(R_2) = Aff(\mathbb{Z}_{pq})$,
(3) $Aut(R_3) = F_{p,p-1}$,
(4) $Aut(R_4) = \mathbb{Z}_{p-1} \times Aff(\mathbb{Z}_q)$,
(5) $Aut(R_5) = \mathbb{Z}_{q-1} \times Aff(\mathbb{Z}_p)$,
(6) $Aut(R_6) = \mathbb{Z}_{p-1} \times_\varphi \mathbb{Z}_p$,

where $\times_\varphi$ denotes to the semi-direct product.

Proof. By using Lemma 1 and Theorems 1, 2 the proofs of parts $(1)-(5)$ are clear, hence we compute the automorphism group of R_6. At first notice that the center of R_6 is identity and so we have

$$R_6 \cong Inn(R_6) \leq Aut(R_6).$$

Thus, $2pq \mid |Aut(R_6)|$. We claim that R_6 has respectively $p, p(q-1), p(q-1)$ and $p-1$ elements of orders $2, q, 2q$ and p. To do this, note that the order of ca^t $(0 \leq t \leq p-1)$ is two. On the other hand,

$$(b^j a^i)^n = b^{nj} a^{(r^{j(n-1)} + \cdots + r^j + 1)i}.$$

This implies that $(b^j a^i)^q = 1$ for $1 \leq j \leq q-1$ and $0 \leq i \leq p-1$. Finally, by a similar way, one can see that for $0 \leq i \leq p-1$ and $1 \leq j \leq q-1$, we have $(cb^j a^i)^{2q} = (a^i)^p = 1$. This confirms our claim. In continuing, we prove that $|Aut(R_6)| = p(p-1)$. Suppose $\alpha \in Aut(R_6)$ be an arbitrary automorphism. Similar to the proof of Lemma 2, one can show that there exist $0 \leq j, t \leq p-1$ and $1 \leq i \leq p-1$ such that $\alpha(a) = a^i$ and $\alpha(b) = ba^j$. On the other hand, $\alpha(c)$ is an element of order two and thus $\alpha(c) = ca^t$ for some $1 \leq t \leq p-1$. Since $\alpha(bc) = \alpha(cb)$ we have:

$$\begin{aligned} &\alpha(b)\alpha(c) = \alpha(c)\alpha(b) \\ &\Rightarrow ba^j ca^t = ca^t ba^j \Rightarrow cba^j ca^t = a^t ba^j \\ &\Rightarrow bca^j ca^t = a^t ba^j \Rightarrow a^{-j+t} = b^{-1} a^t ba^j = a^{tr+j} \\ &\Rightarrow a^{tr+2j-t} = 1 \Rightarrow a^{t(r-1)+2j} = 1. \end{aligned}$$

This results that $p | t(r-1) + 2j$ or $t(r-1) + 2j \equiv 0 (mod\ p)$ $(0 \leq t, j \leq p-1)$ and consequently, $|Aut(R_6)| = p(p-1)$. In other words,

$$Aut(R_6) = \{a_{i,j,t} : \ a_{i,j,t}(a) = a^i, \ a_{i,j,t}(b) = ba^j, \ a_{i,j,t}(c) = ca^t\}.$$

Choose two automorphisms α, β of $Aut(R_6)$ as follows:

$$\alpha : \begin{cases} a \to a \\ b \to ba \\ c \to c \end{cases}, \beta : \begin{cases} a \to a^2 \\ b \to b \\ c \to c \end{cases}.$$

Then

$$H = C_{Aut(R_6)}(\alpha) = \{\theta : \ \theta(a) = a, \theta(b) = ba^j, \theta(c) = ca^t, \ 2j + t(r-1) \equiv 0 \ (mod\ p)\}$$

is a subgroup of order p and so it is isomorphic to $\mathbb{Z}_p$. Let also

$$K = C_{Aut(R_6)}(\beta) = \{\theta : \ \theta(a) = a^i, \theta(b) = b, \theta(c) = c, \ 1 \leq i \leq p-1\}.$$

Clearly, $|K| = p-1$ and one can prove that K is the cyclic subgroup $K = \langle\gamma\rangle$, where

$$\gamma : \begin{cases} a \to a^s \\ b \to b \\ c \to c \end{cases}$$

and s is $(p-1)$-th primitive root of unity. Finally, $Aut(R_6) = K \times_\varphi H$, since $(p, p-1) = 1$ and this completes the proof.

2.2. **Automorphism group of groups of order $3pq$.** In this section, by continuing our method in section 2.1, the full automorphism group of a group of order $3pq$ is computed.

Lemma 2.6. *Consider the presentation of group S_6 of order $3pq$. For $1 \leq i \leq q-1$, $1 \leq j \leq p-1$, $0 \leq i' \leq q-1$, $0 \leq j' \leq p-1$ and $1 \leq k \leq 2$, the order of elements of S_6 is as reported in Table 1.*

Proof. The proof is straightforward.

Elements	a^j	b^i	$b^i a^j$	$c^k b^{i'} a^{j'}$
Orders	p	q	pq	3

Table 1. The order of elements S_6.

By a similar way, one can prove that the order of elements of group S_7 is as given in Table 1.

Theorem 2.7. *The automorphism group of groups of order $3pq$ is as follows:*

(1) $Aut(S_1) = \mathbb{Z}^*_{3pq}$,
(2) $Aut(S_2) = \mathbb{Z}_2 \times F_{p,p-1}$,
(3) $Aut(S_3) = \mathbb{Z}_{q-1} \times F_{p,p-1}$,
(4) $Aut(S_4) = F_{p,p-1}$,
(5) $Aut(S_5) = \mathbb{Z}_{p-1} \times F_{q,q-1}$,
(6) $Aut(S_6) = F_{p,p-1} \times F_{q,q-1}$,
(7) $Aut(S_7) = F_{p,p-1} \times F_{q,q-1}$.

Proof. According to Theorems 1,2 the proofs of parts $(1)-(5)$ are clear. To compute $Aut(S_6)$, at first we show $|Aut(S_6)| = pq(p-1)(q-1)$. Let us α be an automorphism of S_6, thus necessarily $\alpha(a) = a^j$ and $\alpha(b) = b^i$ for $1 \leq i \leq q-1$ and $1 \leq j \leq p-1$. We must consider two following cases:

- $k = 1$, then for $0 \leq i_1 \leq q-1$ and $0 \leq j_1 \leq p-1$, the map $\alpha(c) = cb^{i_1}a^{j_1}$ is an automorphism of S_6.
- $k = 2$, then for $0 \leq i_1 \leq q-1$ and $0 \leq j_1 \leq p-1$, we have $\alpha(c) = c^2 b^{i_1} a^{j_1}$. Consequently, we have $b^{iw^2} = b^{iw}$ and so $q | iw(w-1)$, a contradiction. This implies that $\alpha(c) \neq c^2 b^{i_1} a^{j_1}$.

One can prove that all automorphisms of S_6 are as above and hence $|Aut(S_6)| = pq(p-1)(q-1)$. In continuing, we show that $Aut(S_6) \cong F_{p,p-1} \times F_{q,q-1}$. To do this, without loss of generality, we can assume that

$$Aut(S_6) = \{\alpha : \alpha(a) = a^j, \alpha(b) = b^i, \alpha(c) = cb^{i_1}a^{j_1}\},$$

where $1 \leq i \leq q-1, 0 \leq j_1 \leq p-1, 0 \leq i_1 \leq q-1, 1 \leq j \leq p-1$ and $u^{p-2} + \cdots + u + 1 = 0 \ (mod\ p)$. Consider the following maps:

$$\alpha : \begin{cases} a \to a^{u^{-1}} \\ b \to b \\ c \to c \end{cases}, \beta : \begin{cases} a \to a \\ b \to b^{v^{-1}} \\ c \to c \end{cases}, \mu : \begin{cases} a \to a \\ b \to b \\ c \to ca^u \end{cases}, \gamma : \begin{cases} a \to a \\ b \to b \\ c \to cb^v \end{cases} \quad (2)$$

where $v^{q-2} + \cdots + v + 1 = 0 \ (mod\ q)$. One can prove that $\alpha^{p-1} = \beta^{q-1} = \mu^p = \gamma^q = id$ and $\alpha^{-1}\mu\alpha = \mu^u$, $\beta^{-1}\gamma\beta = \gamma^v$. This implies that $\langle \alpha, \mu \rangle \cong F_{p,p-1}$ and $\langle \beta, \gamma \rangle \cong F_{q,q-1}$. It is not difficult to prove that $F_{p,p-1}$ and $F_{q,q-1}$ are normal subgroups of $Aut(S_6)$ where $|F_{p,p-1}F_{q,q-1}| = pq(p-1)(q-1)$. On the other hand, $F_{p,p-1} \cap F_{q,q-1} = 1$. This means that $Aut(S_6)$ is a direct product as claimed. Finally, by a similar method, we can prove that $Aut(S_6) \cong Aut(S_7)$ and the proof is completed.

2.3. **Automorphism group of groups of order** pqr**.** Here we focus on groups of order pqr where $p > q > r > 2$. Computing the full automorphism group of a group of order pqr is similar to that of a group of order $3pq$. For $1 \le t \le q-1$, $1 \le j \le p-1$, $0 \le i^{'} \le q-1$, $0 \le j^{'} \le p-1$ and $1 \le k \le r-1$, the order of elements of $G_{5+i} (1 \le i \le r-1)$ is as given in Table 2.

Elements	a^j	b^t	$b^t a^j$	$c^k b^{i^{'}} a^{j^{'}}$
Orders	p	q	pq	r

Table 2. The order of elements G_{5+i}.

Theorem 2.8. *The automorphism group of groups of order* pqr *where* $p > q > r > 2$ *are as follows:*

(1) $Aut(G_1) = \mathbb{Z}^*_{pqr}$,
(2) $Aut(G_2) = \mathbb{Z}_{r-1} \times F_{p,p-1}$,
(3) $Aut(G_3) = \mathbb{Z}_{q-1} \times F_{p,p-1}$,
(4) $Aut(G_4) = F_{p,p-1}$,
(5) $Aut(G_5) = \mathbb{Z}_{p-1} \times F_{q,q-1}$,
(6) $Aut(G_{5+i}) = F_{p,p-1} \times F_{q,q-1}$.

Proof. According to the last discussion, we should compute the automorphism group of G_{5+i}. We compute the automorphism group of G_6 and the others can be computed similarly. At first we show $|Aut(G_6)| = pq(p-1)(q-1)$. Let us α be an automorphism of G_6, thus necessarily $\alpha(a) = a^j$ and $\alpha(b) = b^i$ for $1 \le i \le q-1, 1 \le j \le p-1$. Similar to Theorem 3, we can consider two following cases:

- $k = 1$, then for $0 \le i_1 \le q-1$ and $0 \le j_1 \le p-1$, the map $\alpha(c) = cb^{i_1}a^{j_1}$ is an automorphism of G_7.
- $k \ne 1$, then for $0 \le i_1 \le q-1$ and $0 \le j_1 \le p-1$, we have $\alpha(c) = c^k b^{i_1} a^{j_1}$. Consequently, $b^{iu^k} = b^{iu}$ and so $q | iu(u^{k-1} - 1)$, a contradiction. This implies that $\alpha(c) \ne c^k b^{i_1} a^{j_1}$.

On the other hand, by considering α, β, γ in equation (2), one can prove that $\langle \alpha, \mu \rangle \cong F_{p,p-1}$, $\langle \beta, \gamma \rangle \cong F_{q,q-1}$ and so $Aut(G_6) \cong F_{p,p-1} \times F_{q,q-1}$. Finally, one can prove that $Aut(G_6) \cong Aut(G_i)$ for $1 \le i \le r-1$ and this completes the proof.

References

[1] J. E. Adney, T. Yen, Automorphisms of a p-group, *Illinois J. Math.* **9** (1965) 137-143.

[2] B. E. Earn ley, On finite groups whose group of automorphisms is abelian, PhD thesis, Wayne State University, Detroit, Michigan, 1975.

[3] H. Christopher, R. Darren, Automorphisms of finite abelian groups, *Amer. Math. Month.* **114(10)** (2007) 917-923.

[4] M. J. Curran, Semidirect product groups with abelian automorphism groups, *J. Austral. Math. Soc. Ser. A* **42** (1987) 84–91.

[5] D. Dummit, David, S. Foote, M. Richard, Abstract Algebra (3rd ed.), John Wiley, Sons, 2004.

[6] H. Hölder, Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4, *Math. Ann.* **xliii** (1893) 371–410.

[7] T. W. Hungerford , Algebra, Springer-Verlag, New York, 1980.

[8] V. K. Jain, P. K. Rai, M. K. Yadav, On Finite p-groups with abelian automorphism group, *Inter. J. Alg. Compu.* in press.

[9] A. Jamali, Some new non-abelian 2-groups with abelian automorphism groups, *J. Group Theory* **5** (2002) 53–57.

[10] D. Jonah, M. Konvisser, Some non-abelian p-groups with abelian automorphism groups, *Arch. Math. (Basel)* **26** (1975) 131–133.

[11] E. I. Khukhro, V. D. Mazurov, Finite groups with an automorphism of prime order whose centralizer has small rank, *J. Algebra* **301** (2006) 474-492.

[12] G. A. Miller, A non-abelian group whose group of automorphisms is abelian, *Messenger Math.* **43** (1913) 124–125.

[13] M. Morigi, On p-groups with abelian automorphism group, *Rend. Sem. Mat. Univ. Padova* **92** (1994) 47–58.

[14] A. Ranum, The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group, *Trans. Amer. Math. Soc.* **8** (1907) 71–91.

[15] J. Thompson, Automorphisms of solvable groups, *J. Algebra* **1** (1964) 259-267.

[16] H. Wielandt, Finite Permutation Groups, Academic Press, New York, 1964.

M. Ghorbani

Department of Mathematics, Faculty of Science,

Shahid Rajaee Teacher Training University,

Tehran, 16785-136, I. R. Iran

`Email: mghorbani@srttu.edu`

F. Nowroozi Larki

Department of Mathematics, Faculty of Science,

Shahid Rajaee Teacher Training University,

Tehran, 16785-136, I. R. Iran