FINITE GROUPS WITH AUTOMORPHISM GROUP OF ORDER $2PQ^2 (P > Q > 2)$

By

Xianggui Zhong*
Department of Mathematics, Guangxi Normal University, Guilin, Guangxi 541004, P. R. China

and

Shirong Li
Department of Mathematics, Guangxi University, Nanning, Guangxi 530004, P. R. China

(Communicated by T.D. Spearman, M.R.I.A.)

[Accepted 18 August 2005. Published 25 October 2006.]

Abstract

We classify all finite groups G for which $\mathrm{Aut}(G)$ is of order $2pq^2$, where p and q with $p > q > 2$ are primes, and $\mathrm{Aut}(G)$ denotes the full automorphism group of G.

1. Introduction

For a given finite group X, the problem of solving the equation $\mathrm{Aut}(G) = X$, generally speaking, is tantalizing, and its difficulty is such that powerful general theorems and techniques are rare.

In 1983, MacHale began the study of finite groups that can occur as the automorphism group of a finite group, and his result states that all finite groups G with $|\mathrm{Aut}(G)| = 2^n, n \leq 4$ (see [9]). His study has attracted many experts, and a long series of papers can now be found dealing with the problem in some special cases. Some samples are given below. For any odd prime p, Curran [2] shows that there is no group G such that $|\mathrm{Aut}(G)| = p^n, n \leq 5$. Chen [1] determines all finite groups G with $|\mathrm{Aut}(G)| = p_1 p_2 \dots p_n$ or pq^2, where $p, q, p_1, \dots, p_n$ are distinct primes. In Hegarty [5], finite groups G such that $|\mathrm{Aut}(G)| = p^2 q^2$ are classified. Li [6; 7] gives all finite groups G such that $|\mathrm{Aut}(G)| = p^3 q$, where p and q are distinct primes. The assertion, for p, q, r distinct odd primes, that $|\mathrm{Aut}(G)| = prq^2$ is impossible follows from a lemma of Li's, which is proven in [8 (see lemma 2.6)]. Du and Li [4] determine all finite groups G if $q = 2$. Our purpose in the present paper is to determine all finite groups G with $|\mathrm{Aut}(G)| = 2pq^2 (p > q > 2)$. Our results may be summarized as follows:

*Corresponding author; e-mail: xgzhong@mailbox.gxnu.edu.cn

Theorem 1.1. *A finite group G has automorphism group of order $2pq^2$, where p and q are distinct primes with $p > q > 2$, if and only if G is one of the following:*

(1) $1 + 2pq^2$ *is a prime:* $C_n, n = 1 + 2pq^2$ *or* $2(1 + 2pq^2)$;
(2) $q = 3$ *and* $p = 19$: C_{p^2} *or* C_{2p^2} *or* $D_p =< a, b|a^p = b^2 = 1, a^b = a^{-1} >$ *or* $G_1 =< a, b|a^p = b^q = 1, a^b = a^7 >$;
(3) $G_2 =< a, b|a^p = b^{q^2} = 1, a^b = a^r >$, *where r mod p has a index q if* $p - 1 = 2q$ *or* q^2 *if* $(p, q, r) = (19, 3, -2)$;
(4) $G_3 =< a, b, c|a^p = b^{q^i} = c^2 = 1 = [b, c], a^b = a^r, a^c = a^{-1} >$, *where* $i = 1$ *if* $(p, q, r) = (19, 3, 7)$ *or* $i = 2$ *if* $p - 1 = 2q$ *and* $r^q \equiv 1(mod\ p)$ *or* $i = 2$ *if* $(p, q, r) = (19, 3, -2)$;
(5) $G_1 \times C_2, G_2 \times C_2$.

2. Notation and Preliminary Remarks

All groups considered in this paper are finite. Let G be a finite group. $Z(G)$ denotes the center of G; G' the commutator subgroup of G; $\varphi(m)$ the Euler function and $\delta_p(r) = k$ means $r^k \equiv 1(mod\ p)$, but $r^i \equiv 1$ cannot occur for all $i < k$.

Inn(G): Inner automorphism group of G.

Aut(G): Full automorphism group of G.

$Cen(G)$: Group of central automorphism of G, i.e.

$$Cen(G) = \{\alpha \in Aut(G)|g^{-1}\alpha(g) \in Z(G), \forall g \in G\}.$$

Out(G): Group of outer automorphism of G.

If H and K are subgroups of G, then $[H]K$ denotes a split extension of a normal subgroup H by a complement K; $H < G$ denotes that H is a proper subgroup of G. Moreover, C_n is the cyclic group of order n and D_m is the dihedral group of order $2m$.

Lemma 2.1.

(i) $Inn(G) \cong \frac{G}{Z(G)}$. *Furthermore, if* $\frac{G}{N}$ *is cyclic and* $N \leq Z(G)$, *then G is abelian.*
(ii) $Cen(G) = C_{Aut(G)}(Inn(G))$.

We take the primary decomposition of $\frac{G}{G'}$ and $Z(G)$ as

$$\frac{G}{G'} = \frac{G_{p_1}}{G'} \times \ldots \times \frac{G_{p_r}}{G'},$$
$$Z(G) = Z_{p_1} \times \ldots \times Z_{p_r},$$

where $p_i(i = 1, \ldots, r)$ are the prime factors of $|G|$.

Lemma 2.2. *Let G be a group with no non-trivial abelian direct factor. Then*

(i) $|Cen(G)| = \prod_{i=1}^{r} \prod_{j=1}^{k_i} |Z_{p_i,j}|^{r_{i,j}}$,

where $Z_{p_i,j} = \{x \in Z_{p_i}|o(x) = p_i^j\}, p_i^{k_i}$ *is the exponent of* $\frac{G_{p_i}}{G'}$ *and* $r_{i,j}(j = 1, \ldots, k_i)$ *are the invariants of* $\frac{G}{G'}$.

(ii) *If* p *is a prime and* $p|\left(|\frac{G}{G'}|, |Z(G)|\right)$, *then* G *has a central automorphism of order* p *(see [7]).*

Lemma 2.3. *If* $G = [A]B$ *and* A *is Abelian, then, for every integer* k *such that* $(k, |A|) = 1$, *the map* $\sigma_k : ab \mapsto a^k b, \forall a \in A, b \in B$ *is an automorphism of* G *(see [6, lemma 3]).*

The following two lemmas have already been proven by Guiyun Chen [1]. For the convenience of the reader, we include the proofs.

Lemma 2.4. *Let* G *be non-nilpotent with* $|G| = 2p^2$, *then either* 4 *divides* $|Aut(G)|$ *or* p^3 *divides* $|Aut(G)|$.

PROOF. The assumption of this lemma implies that G is isomorphic to one of the following groups:
(i) $< a, b|a^{p^2} = b^2 = 1, a^b = a^{-1} >$,
(ii) $< a, b|a^p = b^p = c^2 = 1, a^c = a^{-1}, b^c = b^{-1} >$,
(iii) $< a, b|a^p = b^p = c^2 = 1, b^c = b^{-1} >$.
By direct calculation, we have that $|\text{Aut}(G)|$ is $p^3(p-1), p^3(p^2-1)(p-1), p(p-1)^2$, respectively. This completes the proof. ■

Lemma 2.5. *Let* m *be a positive integer, and let* n *be a prime,* $G =< a, b|a^m = b^n = 1, b^a = b^t >$, *where* $\delta_n(t) = k$. *If* $m = kl_1l_2, \prod(l_1) \subseteq \prod(k)$, $(l_2, k) = 1$, *then* $|Aut(G)| = nl_1\varphi(n)\varphi(l_2)$.

PROOF. For an arbitrary automorphism σ of G, we may assume that $\sigma(a) = a^ib^j, \sigma(b) = b^v$. By the defining relations of G, we have

$$|a^ib^j| = m, |b^v| = n, (a^ib^j)^{-1}b^v(a^ib^j) = (b^v)^t.$$

It follows that $(v, n) = 1$ and $b^{vt^i} = b^{vt}$. Thus, $t^{i-1} \equiv 1(mod\ n)$, and so $i \equiv 1(mod\ k)$. This implies that

$$i \in X = \{1, k+1, 2k+1, \cdots, (l_1l_2-1)k+1\}.$$

Now we claim that $(i, m) = 1$. In fact, if we write $(i, m) = d$ and $s = \frac{m}{d}$, then we see that

$$(a^ib^j)^s = a^{is}b^{j(t^{i(s-1)}+t^{i(s-2)}+\cdots+1)} = 1.$$

Clearly, $|a^ib^j|$ divides s, and so $d = 1$. This verifies our claim. On the other hand, $|a^ib^j| = m$ if and only if $(i, m) = 1$. It is easy to see that there are the $l_1\varphi(l_2)$ various possibilities for $i \in X$, such that $(i, m) = 1$. It follows, since $1 \le j \le n$ and $(v, n) = 1$, that $|\text{Aut}(G)| = nl_1\varphi(n)\varphi(l_2)$. ■

Lemma 2.6. *Let* n *be an integer and let* $n = p_1^{n_1}p_2^{n_2}\dots p_r^{n_r}$ *be the primary decom-*

position of n. Write

$$\omega(n) = \sum_{i=1}^{r} n_i.$$

Then there is no group G such that $|Aut(G)|$ is odd and $\omega(|Aut(G)|) \leq 4$ (see [8]).

Lemma 2.7. *Let G be a non-cyclic p-group, $|G| > p^2$, and $|\frac{G}{Z(G)}| \leq p^4$. Then $|G|$ divides $|Aut(G)|$ (see [3]).*

Lemma 2.8. *Let $G = Z(G)K$, where $K < G$, and G has no Abelian direct factor. Then G has an outer automorphism (see [6]).*

Lemma 2.9. *Let p and q be distinct primes, and let*

$$G \cong < a, b, c, g | a^p = b^q = c^q = g^2 = 1 = [c, g] = [a, b] = [b, c], a^g = a^{-1}, b^g = b^{-1}, a^c = a^t, \delta_p(t) = q > .$$

Then $|Aut(G)| = pq(p-1)(q-1)$.

Proof. For an arbitrary automorphism σ of G, we may assume that $\sigma(a) = a^{i_1}$, $\sigma(b) = a^{i_2}b^{j_1}c^{k_1}$, $\sigma(c) = a^{i_3}b^{j_2}c^{k_2}$ and $\sigma(g) = a^{i_4}b^{j_3}c^{k_3}g$. By the defining relations of G, we have:

(1) $[\sigma(a), \sigma(b)] = 1$. It follows that $k_1 = q$, since $\delta_p(t) = q$;
(2) $(\sigma(a))^{\sigma(c)} = (\sigma(a))^t$, which yields $k_2 = 1$;
(3) $[\sigma(b), \sigma(c)] = 1$ implies $i_2 t \equiv i_2 (mod\ p)$, and so $a^{i_2} = 1$;
(4) $(\sigma(a))^{\sigma(g)} = (\sigma(a))^{-1}$ gives $k_3 = q$;
(5) $[\sigma(c), \sigma(g)] = 1$ implies $b^{2j_2} = a^{i_4(1-t^{q-1})-2i_3}$, and so $b^{j_2} = 1, i_4(1-t^{q-1}) \equiv 2i_3 (mod\ p)$.

Now we see

$$\sigma = \begin{pmatrix} a & b & c & g \\ a^{i_1} & b^{j_1} & a^{i_3}c & a^{i_4}b^{j_3}g \end{pmatrix}$$

extends to an automorphism of G for suitable i_1, i_3, i_4, j_1, j_3, where

$$1 \leq i_1 < p, 1 \leq i_3, i_4 \leq p, 1 \leq j_1 < q, 1 \leq j_3 \leq q.$$

Thus $|\text{Aut}(G)| = pq(p-1)(q-1)$. ■

3. Main results

From now on we always assume that (*) denotes the condition: $|\text{Aut}(G)| = 2pq^2$, where p and q are distinct primes with $p > q > 2$. The argument for Theorem 1.1 above consists of the following theorems.

Theorem 3.1. *Let G be nilpotent and satisfy (*), then G is one of the following:*

(i) $1+2pq^2$ *is a prime:* $C_n, n=1+2pq^2$ *or* $2(1+2pq^2)$.
(ii) $q=3$ *and* $p=19$*:* C_{361} *or* C_{722}.

PROOF. Let G be such a group. Then G is the direct product of its Sylow subgroups, i.e. $G=P_1\times\ldots\times P_r$, where P_i is Sylow p_i-subgroup with order $p_i^{n_i}(i=1,2,\ldots,r)$, and

$$\mathrm{Aut}(G)\cong\mathrm{Aut}(P_1)\times\ldots\times\mathrm{Aut}(P_r).$$

By Lemma 2.6, we may assume $|\mathrm{Aut}(P_1)|=2pq^2$ and $|\mathrm{Aut}(P_i)|=1(i>1)$, which implies that $P_i=1$ or C_2, and then we have $G=P_1$ or $C_2\times P_1$.

So we only need to determine P_1. If P_1 is non-cyclic, then $\frac{P_1}{Z(P_1)}\cong\mathrm{Inn}(P_1)\le\mathrm{Aut}(P_1)$ implies $|\frac{P_1}{Z(P_1)}|\le p_1^2$. In this case, suppose that $|P|\ge p_1^3$, it follows that p_1^3 divides $|\mathrm{Aut}(P_1)|=2pq^2$, from Lemma 2.7, which is a contradiction. Thus, $P_1\cong C_{p_1}\times C_{p_1}$, and so $|\mathrm{Aut}(P_1)|=|GL(2,p_1)|=p_1(p_1-1)^2(p_1+1)$, which yields 8 divides $|\mathrm{Aut}(P_1)|$ or $P_1=C_2\times C_2$, and so $|\mathrm{Aut}(P_1)|=6$, which is also a contradiction.

Next, assume that P_1 is cyclic. We have

$$2pq^2=|\mathrm{Aut}(P_1)|=p_1^{n_1-1}(p_1-1),$$

which implies that either $p_1=2pq^2+1$ and $P_1\cong C_{p_1}$, or $p_1=p$ and $P_1\cong C_{p^2}$, with $p=1+2q^2$. Further, we have $q=3$. Recall that $G=P_1$ or $C_2\times P_1$, thus we obtain (i) and (ii) of the theorem, as desired. ■

Theorem 3.2. *Let G be non-nilpotent with no nontrivial Abelian direct factor and let it satisfy (*), then $Out(G)>1$ if and only if G is one of the following:*
(i) D_{19};
(ii) $G_1=<a,b|a^{19}=b^3=1,a^b=a^7>$;
(iii) $G_2=<a,b|a^p=b^{q^2}=1,a^b=a^r>$, *where* $\delta_p(r)=q$ *if* $p-1=2q$ *or* q^2 *if* $p-1=2q^2$,*i.e.* $p=19,q=3$ *and* $r=-2$;
(iv) $G_3=<a,b,c|a^p=b^{q^i}=c^2=1=[b,c],a^b=a^r,a^c=a^{-1},\delta_p(r)=q>$, *where* $i=1$ *if* $p-1=2q^2$*, i.e.* $(p,q,r)=(19,3,7)$ *or* $i=2$ *if* $p-1=2q$.

PROOF. Let $T\in\mathrm{Syl}_2(G),P\in\mathrm{Syl}_p(G)$ and $Q\in\mathrm{Syl}_q(G)$. Since G is non-nilpotent, we have that $\mathrm{Inn}(G)\cong\frac{G}{Z(G)}$ is non-nilpotent and so $|\mathrm{Inn}(G)|=2p$, $2q,pq,2q^2,pq^2$ or $2pq$. It is clear that P is a normal subgroup of G.

We first show the following:
(1) $|Cen(G)|_q\le q$ and $|Cen(G)|_{\{2,p\}}=1$. This is immediate, by a combination of the assumptions of the theorem and Lemma 2.1(ii).
(2) $|P|\le p,|T|\le 2$ and $Z(G)$ is a q-group.

Let $G=TPQ,H=TQ\le G$, where $P\trianglelefteq G$ and both T and P are Abelian by Lemma 2.1(i). If $P>1$, then the p'-group H acts non-trivially on the Abelian p-group P, which implies $P=C_P(H)\times[P,H]$. Thus $G=H[P,H]\times C_P(H)$, so $C_P(H)=1$ since G has no non-trivial, Abelian, direct factor, and so $|P|=p$. On the other hand, $G'=[P,H]H'$, $H'=Q'[Q,T]\le Q$. It is obvious that $[P,H]=P$. Now, if $T\cap Z(G)>1$, then $G'\le PQ$ implies $|\frac{G}{G'}|_2>1$, $|Cen(G)|_2=2$ by Lemma

2.2(ii); this contradicts (1), however, so $T \cap Z(G) = 1$, i.e. $|T| \leq 2$, so $Z(G)$ is a q-group and so (2) is proved.

Now we complete our proof by the following six cases:

Case I. $|\mathrm{Inn}(G)| = 2p, G = [P]T$. In this case, $Z(G) = 1$ by (2), so $|G| = 2p$, and so $G \cong D_p$. By direct calculation, we see that $|\mathrm{Aut}(G)| = p(p-1)$. Thus $p-1 = 2q^2$ and $G \cong D_p$. Further, we have $p = 19$ and $q = 3$, as desired.

Case II. $|\mathrm{Inn}(G)| = 2q$. In this case, $Q \trianglelefteq G$. Hence $Q = C_Q(T) \times [Q,T]$ and $G = C_Q(T)[Q,T]T$, so $C_Q(T) = 1$, since G has no nontrivial, Abelian, direct factor. Further, we have $Z(G) = 1$ and $|\mathrm{Aut}(G)| = q(q-1) \neq 2pq^2$. Hence Case II is eliminated.

Case III. $|\mathrm{Inn}(G)| = 2q^2$. In this case, $G = [Q]T$. First, Lemma 2.4 gives $Z(G) > 1$. Second, if Q is Abelian, then $Q = C_Q(T) \times [T,Q]$, so $G = T[T,Q] \times C_Q(T)$, hence $C_Q(T) = 1$, since G has no non-trivial, Abelian, direct factor. This implies $Z(G) = 1$, since $Z(G) \leq Q$ by (2), which is a contradiction. Thus we may assume that Q is non-Abelian, and so $Z(Q) = Z(G) \cap Q = Z(G)$. Thus $\frac{Q}{Z(Q)}$ is an elementary Abelian q-group of order q^2. Apply Maschke's theorem to see

$$\frac{Q}{Z(Q)} = \frac{Q_1}{Z(Q)} \times \frac{Q_2}{Z(Q)},$$

where both the direct factors have order q and are T-invariant. From this we obtain $[Q_i,T] \neq 1 (i = 1,2)$, and T acts on an Abelian group Q_i. It follows that $Q_i = C_{Q_i}(T) \times [Q_i,T]$, and so $[Q_i,T]$ has order q, since $C_{Q_i}(T) = Z(Q)$. Letting $[Q_1,T] = < x >$, $[Q_2,T] = < y >$ and $K = < y > T$, we have $G = [Q_1]K$. If $Z(Q)$ has an element a_0 of order q^2, then by defining:

$$\alpha_{q+1} : ga \mapsto ga^{q+1}, \forall g \in K, a \in Q_1,$$

we see that α_{q+1} provides an automorphism of G from Lemma 2.3. However, $a_0^{\alpha_{q+1}} = a_0^{q+1} \neq a_0$, it follows α_{q+1} is an outer automorphism of order q^n, where n is some integer. This contradicts $|\mathrm{Out}(G)|_q = 1$. Thus, $Z(G)$ is an elementary Abelian q-group.

Now, $Q = < x,y > Z(Q) = < x,y > \times Z$. From the hypothesis on G we have $Z = 1$, and so $Q = < x,y >$, it follows $\Phi(Q) = Z(Q)$, and so Q is a minimal non-Abelian q-group. Hence Q' is of order q and so $|Q| = q^3$. Recall that $< x >$ and $< y >$ are T-invariant, so G has the following defining relations:

$$G = < x,y,z,a | x^q = y^q = z^q = a^2 = 1, [x,y] = z \in Z(G), x^a = x^i, y^a = y^j >,$$

where i and j are suitable integers. In this case, define $\alpha \in \mathrm{Aut}(G)$ by

$$\alpha = \begin{pmatrix} a & x & y & z \\ a & x^{-1} & y & z^{-1} \end{pmatrix}.$$

It is easy to check that α is an outer automorphism of order 2. This contradicts $|\mathrm{Out}(G)|_2 = 1$. That is to say, Case III cannot occur.

Case IV. $|\mathrm{Inn}(G)| = pq$. It is well known that

$$\frac{G}{Z(G)} \cong < a,b | a^p = b^q = 1, a^b = a^r, \delta_p(r) = q > .$$

If $Z(G) = 1$, then $|\mathrm{Aut}(G)| = p(p-1)$ by Lemma 2.5. For this, we have $p-1 = 2q^2$ and $G \cong G_1$, further, $p = 19, q = 3, \delta_{19}(r) = 3$ implies $r = 7$ or 11, but in this case, the two groups for $r = 7$ and 11 are isomorphic. This gives conclusion (ii) of the theorem. If $Z(G) > 1$, obviously we have $G' = P$. By (2), $|P| = p$, $1 < Z(G) \leq Q$, and by Lemma 2.3, every automorphism of P can be extended to G, i.e. $\mathrm{Aut}(P) \leq \mathrm{Aut}(G)$, and so $p-1 = 2q$ or $2q^2$. On the other hand, $|Cen(G)| = q$ by (1). Since $\frac{G_q}{G'} \cong \frac{Q}{Q \cap G'} = Q$, from Lemma 2.2(i), we obtain $|Z(G)| = q$ and $Q \cong C_{q^2}$. Hence $|G| = pq^2$; by Lemma 2.5 we have $|\mathrm{Aut}(G)| = 2pq^2$ and $G \cong G_2$, with $|Z(G)| = q$ and $p-1 = 2q$.

Case V. $|\mathrm{Inn}(G)| = pq^2 (p > q)$. From a complete classification of G of order pq^2, supposing that $Z(G) = 1$, we have $G \cong G_2$ with $|Z(G)| = 1$. In this case, G satisfies that $|\mathrm{Aut}(G)| = 2pq^2$ by Lemma 2.5. This conclusion, together with the latter part of Case IV, gives conclusion (iii) of the theorem.

Next, assume that $Z(G) > 1$. At first, we claim that $\frac{G}{Z(G)} \cong G_2$ is false. Suppose that this is not so, then Q is Abelian and so $G' = P$, since $G' = PQ'[Q,T]$ and $T = 1$, this yields that $G' \cap Z(G) = 1$. Since

$$\mathrm{Aut}(G) \geq Cen(G)\mathrm{Inn}(G),$$

if $1 = Z(\mathrm{Inn}(G)) = Cen(G) \cap \mathrm{Inn}(G)$ by Lemma 2.1(ii), then $|Cen(G)||\mathrm{Inn}(G)|$ divides $|\mathrm{Aut}(G)|$, i.e.$|Cen(G)|pq^2$ divides $2pq^2$, and this yields $|Cen(G)| = 1$ by (1). Obviously, $G' = P$, $\frac{G_q}{G'} \cong Q$. Lemma 2.2(ii) implies $|Q| = q^2$ and $Z(G) = 1$ by (2), which is a contradiction. Thus we may assume that $|Z(\mathrm{Inn}(G))| = q$. In this case, we see $|Cen(G)| = q$. This yields, by Lemma 2.2(i), $|Z(G)| = q$, since $G' = P$ and $\frac{QG'}{G'} \cong Q$. At the same time we obtain that Q is cyclic and $Q \cong C_{q^3}$. Thus we have $G \cong < a, b | a^p = b^{q^3} = 1, a^b = a^r, \delta_p(r) = q^2 >$. This contradicts the assumption that $Z(\mathrm{Inn}(G))$ is non-trivial. We may now assume that

$$\frac{G}{Z(G)} \cong < a, b, c | a^p = b^q = c^q = 1 = [b, c] = [a, b], a^c = a^r, \delta_p(r) = q > .$$

In this case, from Lemma 2.2(ii) and (1), it is clear that $|Cen(G)| = q$. If Q is Abelian, then we see easily that $\frac{QG'}{G'} \cong Q$ and $|Z(G)| = q$ by Lemma 2.2(i); further, we have $Q \cong C_{q^3}$ and so $\frac{Q}{Z(G)}$ is cyclic, which is a contradiction. If Q is non-Abelian, we see that $Z(Q) = Z(G)$, $\frac{G}{G'} \cong \frac{Q}{Q'}$. So $Q' \leq Z(Q)$, since $\frac{Q}{Z(Q)} \cong C_q \times C_q$, and so $\frac{Q}{Q'}$ is non-cyclic. But this yields that $|Cen(G)| \geq q^2$ by Lemma 2.2(i), which, again, is a contradiction.

Case VI. $|\mathrm{Inn}(G)| = 2pq$. By a classification of G of order $2pq (p > q)$, $\frac{G}{Z(G)} \cong H_i (i = 1, 2, 3)$, where:

$H_1 = < a, b | a^{pq} = b^2 = 1, a^b = a^r, r^2 \equiv 1 (mod\ pq) >$,

$H_2 = < a, b > \times < c >$ with $a^p = b^q = c^2 = 1$,

$H_3 = < a, b, c | a^p = b^q = c^2 = 1 = [b, c], a^b = a^r, a^c = a^{-1}, r^q \equiv 1 (mod\ p) >$.

If $\frac{G}{Z(G)} \cong H_1$, then since $Z(G) \leq Q$ by (2), we have:

$$G \cong < a, b, Z(G) | a^{pq} = z_1, b^2 = 1, a^b = a^r z_2 >, z_1, z_2 \in Z(G).$$

Define α by

$$\alpha = \begin{pmatrix} a & b & z \\ a^{-1} & b & z^{-1} \end{pmatrix}.$$

Then $Z(G) > 1$ implies $\alpha \in \mathrm{Out}(G)$ with $\alpha^2 = 1$, which is a contradiction. Hence, $Z(G) = 1$ and $G \cong [< a >] < b >$. Lemma 2.3 implies that $|\mathrm{Aut}(< a >)|$ divides $|\mathrm{Aut}(G)|$, i.e. $\varphi(pq)$ divides $2pq^2$, which is also a contradiction. If $\frac{G}{Z(G)} \cong H_2$, then since T acts trivially on $\frac{PQ}{Z_p Z_q}$, we have that T acts trivially on PQ, also. This implies $G = T \times PQ$, which, again, is a contradiction.

Now consider the case when $\frac{G}{Z(G)} \cong H_3 = [< a >] < bc >$, where $a^p = (bc)^{2q} = 1, a^{bc} = a^{-r}, \delta_p(-r) = 2q$. Substituting bc for b, if $Z(G) = 1$, by Lemma 2.5 we have $|\mathrm{Aut}(G)| = p(p-1)$. Hence, $p - 1 = 2q^2, G \cong G_3$ with $i = 1$, as desired.

Next assume that $Z(G) > 1$. If $|\frac{G}{G'}|_q = 1$, then $Q \leq G'$. This yields that $Z(G) = Z(G) \cap Q \leq Z(G) \cap G' = 1$, since every Sylow subgroup of G is Abelian, which is a contradiction. Hence, $q| \left(|\frac{G}{G'}|, |Z(G)|\right)$ and $|Cen(G)| = q$ by (1) and Lemma 2.2(ii). By (1) we have $|P| = p$. In addition, that $G' = \left(\frac{G}{Z(G)}\right)' \cong H_3' \in \mathrm{Syl}_p(H_3)$ implies $G' = P$, and so $\frac{G_q}{G'} \cong Q$. By Lemma 2.2(i) we give $Q \cong C_{q^2}$ and $Z(G) \cong C_q$. Hence we obtain $G \cong G_3$ with $i = 2$. Lemma 2.5 implies $|\mathrm{Aut}(G)| = 2pq^2$ and $p - 1 = 2q$, as desired.

The proof of the theorem now is complete. ∎

Theorem 3.3. *Let G be non-nilpotent with no non-trivial direct factor and let it satisfy (*), then Out(G) = 1 if and only if G is the following:*

$$G_4 \cong < a, b, c | a^{19} = b^{18} = 1, a^b = a^2 > .$$

Proof. First, we may similarly derive the following (1) and (2) from the proof of Theorem 3.2.

(1) $G = [P]QT, |Cen(G)| = 1$ or q or q^2.

(2) $|P| = p, |T| = 2, G' = PQ'[Q, T], Z(G) \leq Q$, where $P \in \mathrm{Syl}_p(G)$, $T \in \mathrm{Syl}_2(G)$, $Q \in \mathrm{Syl}_q(G)$.

Second, from Lemma 2.3 we have $p - 1 = 2q$ or $2q^2$. Finally, we can complete our proof in the following three parts:

(a) $|Cen(G)| = q^2$. Lemma 2.1 implies $|Z(\frac{G}{Z(G)})| = q^2$, obviously, $G = Q \times TP$. Since G has no non-trivial, Abelian, direct factor, we have that Q is non-Abelian and $|Q| > q^2$. Hence, $Z(Q) = Q \cap Z(G) = Z(G)$ and $|\frac{Q}{Z(Q)}| = q^2$, which yields that $|Q|$ divides $|\mathrm{Aut}(Q)|$. Now, since $\mathrm{Aut}(G) = \mathrm{Aut}(Q) \times \mathrm{Aut}(TP)$, we have q^3 divides $|\mathrm{Aut}(G)|$, which is a contradiction.

(b) $|Cen(G)| = q$, i.e. $|Z(\frac{G}{Z(G)})| = q, Z(G) > 1$. $\frac{G}{Z(G)}$ may be isomorphic to one of the following groups:

(i) $H_1 = < a, b, c, g | a^q = b^q = c^p = g^2 = 1 = [a, b] = [a, c] = [b, c], a^g = b, b^g = a, c^g = c^{-1} >$.

(ii) $H_2 = < a, b, g | a^p = b^{q^2} = g^2 = 1 = [b, g], a^g = a^{-1}, a^b = a^r, \delta_p(r) = q >$.

(iii) $H_3 =< a,b,c,g|a^p = b^q = c^q = g^2 = 1 = [a,c] = [b,c] = [c,g], a^g = a^{-1}, a^b = a^r, b^g = b^i >, i = 1,-1$.

Case I. $\frac{G}{Z(G)} \cong H_1$. Since $Z(G) \leq Q$, we have $G \cong < a,b,c,g,Z(G)|a^q = z_1, b^q = z_2, c^p = g^2 = 1, [a,b] = z_3, a^g = bz_4, b^g = az_5, c^g = c^{-1} >$, where $z_i \in Z(G), i = 1,2,3,4,5$. But, $z_3 = [a,b]^g = [bz_4, az_5] = z_3^{-1}$, hence $z_3 = 1$. Letting

$$\alpha = \begin{pmatrix} a & b & c & g & z \\ a^{-1} & b^{-1} & c & g & z^{-1} \end{pmatrix}, \forall z \in Z(G),$$

we see that α extends to an automorphism of G. Thus $z_i = 1 (i = 1, 2, 4, 5)$ since $\mathrm{Out}(G) = 1$, and so $Z(G) = 1$, which is a contradiction.

Case II. $\frac{G}{Z(G)} \cong H_2$. In this case, Q is Abelian and since $[Q,T] \leq Z(G)$, we have

$$1 = G' \cap Z(G) = P[Q,T] \cap Z(G) = [Q,T](P \cap Z(G)) = [Q,T].$$

On the other hand, $\frac{G_q}{G'} = \frac{QG'}{G'} \cong Q$. So $|Z(G)| = q$ by Lemma 2.2(i) and $|Cen(G)| = q$, which implies that Q is cyclic. This is a contradiction, since b^q will then lie in $Z(G)$ and not just $Z(H_2)$.

Case III. $\frac{G}{Z(G)} \cong H_3$ with $i = -1$. In this case, $|Cen(G)| = q$ implies $[a,b] = 1$ and so $G = [PQ]T$. By Lemma 2.3,

$$\alpha = \begin{pmatrix} x & g \\ x^{-1} & g \end{pmatrix}, \forall x \in PQ, g \in T.$$

Obviously, α provides an automorphism of G of order 2, so G has an outer automorphism. This contradicts $\mathrm{Out}(G) = 1$.

Case IV. $\frac{G}{Z(G)} \cong H_3$ with $i = 1$. We may take:

$$G =< a,b,c,g,Z(G)|a^p = g^2 = 1, [b,g] = z_1, [c,g] = z_2, b^q = z_3, c^q = z_4, [b,c] = z_5, a^g = a^{-1}, a^b = a^r > .$$

In this case, $z_1^2 = 1 = z_2^2$ implies $z_1 = 1 = z_2$, since $Z(G) < Q$. Hence $[Q,T] = 1$. Furthermore, $G' = PQ'$ by (2) and so $G' \leq PZ(G)$. On the other hand, $|Cen(G)| = q$ implies that $\frac{G}{G'}$ has a cyclic Sylow subgroup $\frac{G_q}{G'}$. It follows that $\frac{G}{PZ(G)}$ has a cyclic Sylow subgroup $\frac{Q}{Q} \cap PZ(G)$, i.e. $\frac{Q}{Z(G)}$ is cyclic. This contradicts the assumption that $\frac{G}{Z(G)} \cong H_3$, as this would imply that $\frac{Q}{Z(Q)} \cong C_q \times C_q$.

(c) $|Cen(G)| = 1$ i.e. $|Z(\frac{G}{Z(G)})| = 1$. $\frac{G}{Z(G)}$ may be isomorphic to one of the following groups:

(i) $H_1 =< a,b|a^{pq^2} = b^2 = 1, a^b = a^{-1} >$;

(ii) $H_2 =< a,b,c,g|a^q = b^q = c^p = g^2 = 1, a^g = a^{-1}, b^g = b^{-1}, c^g = c^{-1} >$;

(iii) $H_3 =< a,b,g|a^p = b^{q^2} = g^2 = 1, a^g = a^{-1}, a^b = a^r >$;

(iv) $H_4 =< a,b,c,g|a^p = b^q = c^q = g^2 = 1, a^g = a^i, b^g = b^{-1}, a^c = a^r >$, where $i = 1$ or -1.

We first assume that $Z(G) > 1$. Thus $|\frac{G}{G'}|_q = 1$ by Lemma 2.2(ii), which yields $Q \leq G'$. Assume Q is Abelian, it follows that $Q \cap Z(G) \leq G' \cap Z(G) = 1$. This contradicts $Z(G) > 1$. Hence Q is non-Abelian and $\frac{G}{Z(G)} \cong H_1$, or H_3 or H_4 cannot occur.

Suppose $\frac{G}{Z(G)} \cong H_4$. In this case, we have $[c, g] = z_1$ and $[b, c] = z_2$, with $z_1, z_2 \in Z(G)$. Obviously, $z_1^2 = [c, g^2] = 1$, and so $z_1 = 1$. In addition, $z_2^{-1} = [c, b]^g = [c, b^g] = [c, b^{-1}] = z_2$, and it follows that $z_2 = 1$, so Q is Abelian, which is a contradiction. If $\frac{G}{Z(G)} \cong H_2$, then we have

$G = < a, b, c, g, Z(G) | a^q = z_1, b^q = z_2, c^p = g^2 = 1 = [a, c] = [b, c], a^g = a^{-1}z_3, b^g = b^{-1}z_4, c^g = c^{-1}, [a, b] = z_5 >$,

where $z_i \in Z(G), i =$1, 2, 3, 4, 5. Now Lemma 2.8 implies $G \cong < a, b, c, g, z_1, z_2, z_3, z_4, z_5 >$, since $\mathrm{Out}(G) = 1$. In addition,

$$1 = [a^q, g](= [z_1, g]) = a^{-q}(a^q)^g = a^{-q}(a^{-1}z_3)^q,$$

so we have $1 = z_1^{-2}z_3^q$. Similarly, we have $1 = z_2^{-2}z_4^q$. Noting that

$$\alpha = \begin{pmatrix} a & b & c & g & z \\ a^t & b^t & c & g & z^t \end{pmatrix}$$

defines an automorphism of G for any t such that $t \equiv 1 (mod\ q)$. In particular, if we take $t = q + 1$, then the requirement that α be inner gives that $z^q = 1$ for all $z \in Z(G)$. Hence, we have always $z_i^q = 1, i = 1, 2, 3, 4, 5$. So $z_1 = z_2 = 1$.

If $< z_3 > \cap < z_5 > = 1$ and $< z_4 > \cap < z_5 > \neq 1$, then we see that

$$\alpha_1 = \begin{pmatrix} a & b & c & g & z_3 & z_4 & z_5 \\ a & b^{-1} & c & g & z_3 & z_4^{-1} & z_5^{-1} \end{pmatrix}$$

defines an outer automorphism of G, which is a contradiction.

A similar argument shows that $< z_3 > \cap < z_5 > \neq 1$ and $< z_4 > \cap < z_5 > = 1$ cannot occur.

If $< z_3 > \cap < z_5 > = 1 =< z_4 > \cap < z_5 >$, then

$$\alpha_2 = \begin{pmatrix} a & b & c & g & z_3 & z_4 & z_5 \\ a^{-1} & b^{-1} & c & g & z_3^{-1} & z_4^{-1} & z_5 \end{pmatrix}$$

defines an automorphism of G. So $z_3 = z_4 = 1$, since $\mathrm{Out}(G) = 1$. In this case, since Q is non-Abelian, we see that

$$\alpha_3 = \begin{pmatrix} a & b & c & g & z_5 \\ a^{-1} & b & c & g & z_5^{-1} \end{pmatrix}$$

provides an outer automorphism of G, which is, again, a contradiction.

If $< z_3 > \cap < z_5 > \neq 1 \neq < z_4 > \cap < z_5 >$, then $< z_3 > = < z_4 > = < z_5 >$. We have

$G = < a, b, c, g, z | a^q = b^q = c^p = g^2 = 1 = [b, c] = [a, c], c^g = c^{-1}, [a, b] = z \in Z(G), a^g = a^{-1}z^i, b^g = b^{-1}z^j >$

for suitable i, j. Choose i_1 and i_2 such that $2i_1 \equiv 1 - i(\ mod\ q)$ and $2i_2 \equiv 1 - j(\ mod\ q)$ and, replacing a and b by az^{i_1}, bz^{i_2}, respectively, we have

$G = < a, b, c, g, z | a^q = b^q = c^p = g^2 = 1 = [a, c] = [b, c], c^g = c^{-1}, [a, b] = z \in Z(G), a^g = a^{-1}z, b^g = b^{-1}z >$.

In this case, define α_4 by

$$\alpha_4 = \begin{pmatrix} a & b & c & g & z \\ az^{-1} & ab^{-1} & c & g & z^{-1} \end{pmatrix}.$$

Then α_4 determines an outer automorphism of G, since Q is non-Abelian. This contradicts $\mathrm{Out}(G) = 1$.

Next, we may assume that $Z(G) = 1$. Thus $G \cong H_i (i = 1, 2, 3, 4)$. If $G \cong H_1$, then by Lemma 2.3 we have that $|\mathrm{Aut}(PQ)|$ divides $|\mathrm{Aut}(G)|$. However, $|\mathrm{Aut}(PQ)| = \varphi(pq^2)$, this implies that 4 divides $|\mathrm{Aut}(G)|$, which is a contradiction. If $G \cong H_2$, then we can use the same argument as when $G \cong H_1$. PQ is still Abelian and this time $|\mathrm{Aut}(PQ)|$ is even divisible by 32, since $|GL(2, q)|$ is divisible by 16.

When $G \cong H_3$, if we write $G = < a, b | a^p = b^{2q^2} = 1, a^b = a^r >$, then $\delta_p(r) = 2q^2$, since $Z(\mathrm{Inn}(G)) = 1$. Now Lemma 2.5 implies that $|\mathrm{Aut}(G)| = p(p-1) = 2pq^2$, as desired. Further, $p - 1 = 2q^2$ implies $p = 19$ and $q = 3$. In addition, $r = 2, 3, -4, -5, -6, -9$, since $\delta_p(r) = 18$. For the various possibilities for r, choose suitable i such that $r^i \equiv 2(mod\ 19)$, we then have $G \cong < a, b | a^{19} = b^{18} = 1, a^b = a^2 >$, as desired.

If $G \cong H_4$ with $i = 1$ and $Z(G) = 1$, then $G \cong < b, g > \times < a, c >$.

$$|\mathrm{Aut}(< a, c >)||\mathrm{Aut}(< b, g >)| \text{ divides } |\mathrm{Aut}(G)|.$$

But, from Lemma 2.3 we have $\mathrm{Aut}(< a >) \leq \mathrm{Aut}(< a, c >)$ and $\mathrm{Aut}(< b >) \leq \mathrm{Aut}(< b, g >)$. It follows that $(p - 1)(q - 1)$ divides $|\mathrm{Aut}(G)|$, which contradicts $|\mathrm{Aut}(G)|_2 = 2$.

If $G \cong H_4$ with $i = -1$, then $\delta_p(r) = q$ since $Z(G) = 1$. From Lemma 2.9, we have that 4 divides $|\mathrm{Aut}(G)|$, which is a contradiction. Therefore $G \cong H_4$ cannot occur.

This completes the proof of the theorem. ■

Theorem 3.4. *Let G be non-nilpotent with an Abelian direct factor and let it satisfy (*), then one of the following holds:*

(i) $G \cong G_1 \times C_2$,

(ii) $G \cong G_2 \times C_2$,

where G_1 and G_2 are the same as in Theorem 3.2.

PROOF. Assume that $G = H \times A$, where $A \neq 1$ is Abelian and H has no Abelian direct factor. Then

$$|\mathrm{Aut}(H)||\mathrm{Aut}(A)| \text{ divides } |\mathrm{Aut}(G)|,$$

and Lemma 2.6 implies that $|\mathrm{Aut}(H)|_2 = 2$ and $A \cong C_2$.

(1) Clearly, 4 divides $|\mathrm{Aut}(H)|$ when $H \cong D_p$, since, if we write $G = < z > \times < a, b | a^p = b^2 = 1, a^b = a^{-1} >$, then the map $a \longmapsto a, b \longmapsto zb$ extends to an automorphism of order 2 of G, and hence $\mathrm{Aut}(D_p)$ has even index in $\mathrm{Aut}(G)$. If $H \cong G_1$ or G_2, then $\mathrm{Aut}(G) = \mathrm{Aut}(H) \times \mathrm{Aut}(A)$ and $|\mathrm{Aut}(G)| = 2pq^2$, as desired. If $H \cong G_3$ or G_4, a similar argument as when $H \cong D_p$, shows that this case cannot occur.

(2) For $|\mathrm{Aut}(H)| = 2pq$, we have

$$H \cong < a, b | a^m = b^p = 1, b^a = b^t, \delta_p(t) = m, m | 2q, p - 1 = 2q > .$$

In this case, we may assume that $m = 2q$. By direct calculation, we see that $|\mathrm{Aut}(G)| = 4pq$, which is a contradiction.

(3) $|\mathrm{Aut}(H)| = 2p$ or $2q$. By [6, lemma 6] we have that $H \cong S_3$. However, 4 divides $|\mathrm{Aut}(S_3 \times C_2)|$, which is also a contradiction.

(4) By [6, lemma 7], the case when $|\mathrm{Aut}(H)| = 2q^2$ cannot arise.

The proof of the theorem is therefore completed. ■

Acknowledgements

This research is supported by the Natural Science Foundation of China N10161001. The authors are greatly indebted to the referee for pointing out to us the work of P.V. Hegarty [5], for detecting and correcting some errors and omissions in the original version of this paper, and for a most comprehensive and well-informed report, which helped us to improve the presentation of this paper considerably.

References

[1] Guiyun Chen, Finite group with automorphism group having an order of $p_1 p_2 \dots p_n$ or pq^2, *Journal of the Southwest China Teachers' University* **15** (1990), 21–8 (In Chinese).

[2] M.J. Curran, Automorphisms of certain p-groups(p odd), *Bulletin of the Australian Mathematical Society* **38** (1988), 299–305.

[3] R.M. Davitt, On the automorphism group of a finite p-group with a small central quotient, *Canadian Journal of Mathematics* **32**(1980), 1168–76.

[4] Ni Du and Shirong Li, Finite groups with automorphism group of order $4pq$, *Acta Mathematica Sinica* **47** (2004), 181–8.

[5] P.V. Hegarty, Automorphism groups of order p^2q^2, *Proceedings of the Royal Irish Academy* **95**A (1995), 149–52.

[6] Shirong Li, Finite groups with automorphism group of order 2^3p, *Proceedings of the Royal Irish Academy* **94**A (1994), 193–205.

[7] Shirong Li, Finite groups with automorphism group of order p^3q(p odd), *Proceedings of the Royal Irish Academy* **94**A (1994), 207–18.

[8] Shirong Li, Automorphism groups of some finite groups, *Science in China* (Series A) **37** (1994), 295–303.

[9] D. MacHale, Some finite groups which are rarely automorphism groups II, *Proceedings of the Royal Irish Academy* **83**A (1983), 189–96.