Chapter 2

Finite $p$-Groups with Abelian Automorphism Group

In this chapter we construct various types of specific non-special finite $p$-groups having abelian automorphism group. We also find some structural information about the groups whose automorphism groups are elementary abelian. Throughout the chapter, any unexplained $p$ always denotes an odd prime.

2.1 Abelian Automorphism Groups: Literature

Study of groups having abelian automorphism groups is an old problem in group theory. Though a lot of work has been done by many on the subject, not very significant is known about such groups. In this section we review the literature about such groups and give motivation behind theorems presented in this chapter. The story began in 1908 with the following question of Hilton [33]: Whether a non-abelian group can have an abelian group of isomorphisms (automorphisms). In 1913, Miller [51] constructed a non-abelian group $G$ of order 64 such that $\text{Aut}(G)$ is an elementary abelian group of order 128. More examples of such 2-
groups were constructed in [13, 38, 68]. For an odd prime $p$, the first example of a finite $p$-group $G$ such that $\text{Aut}(G)$ is abelian was constructed by Heineken and Liebeck [28] in 1974. In 1975, Jonah and Konvisser [40] constructed 4-generated groups of order $p^8$ such that $\text{Aut}(G)$ is an elementary abelian group of order $p^{16}$, where $p$ is any prime. In 1975, by generalizing the constructions of Jonah and Konvisser, Earnley [17, Section 4.2] constructed $n$-generated special $p$-groups $G$ such that $\text{Aut}(G)$ is abelian, where $n \geq 4$ is an integer and $p$ is any prime number. Among other things, Earnley also proved that there is no $p$-group $G$ of order $p^5$ or less such that $\text{Aut}(G)$ is abelian. On the way to constructing finite $p$-groups of class 2 such that all normal subgroups of $G$ are characteristic, in 1979 Heineken [29] produced groups $G$ such that $\text{Aut}(G)$ is abelian. In 1994, Morigi [54] proved that there exists no group of order $p^6$ whose group of automorphisms is abelian and constructed groups $G$ of order $p^{n^2 + 3n + 3}$ such that $\text{Aut}(G)$ is abelian, where $n$ is a positive integer. In particular, for $n = 1$, it provides a group of order $p^7$ having an abelian automorphism group.

There have also been attempts to get structural information of finite groups having abelian automorphism group. In 1927, Hopkins [34], among other things, proved that a finite $p$-group $G$ such that $\text{Aut}(G)$ is abelian, can not have a non-trivial abelian direct factor. In 1995, Morigi [55] proved that the minimal number of generators for a $p$-group with abelian automorphism group is 4. In 1995, Hegarty [27] proved that if $G$ is a non-abelian $p$-group such that $\text{Aut}(G)$ is abelian, then $|\text{Aut}(G)| \geq p^{12}$, and the minimum is obtained by the group of order $p^7$ constructed by Morigi. Moreover, in 1998, Ban and Yu [3] obtained independently the same result and proved that if $G$ is a group of order $p^7$ such that $\text{Aut}(G)$ is abelian, then $|\text{Aut}(G)| = p^{12}$.

We remark here that all the examples (for an odd prime $p$) mentioned above
are special $p$-groups. In 2008, Mahalanobis [48] published the following conjecture: *For an odd prime $p$, any finite $p$-group having abelian automorphism group is special.* Jain and Yadav [37] provided counter examples to this conjecture by constructing a class of non-special finite $p$-groups $G$ such that $\text{Aut}(G)$ is abelian. These counter examples, constructed in [37], enjoy the following properties: (i) $|G| = p^{n+5}$, where $p$ is an odd prime and $n$ is an integer $\geq 3$; (ii) $\gamma_2(G)$ is a proper subgroup of $Z(G) = \Phi(G)$; (iii) exponents of $Z(G)$ and $G/\gamma_2(G)$ are same and it is equal to $p^{n-1}$; (iv) $\text{Aut}(G)$ is abelian of exponent $p^{n-1}$.

Now we review non-special 2-groups having abelian automorphism group. In contrast to $p$-groups for odd primes, there do exist finite 2-groups $G$ with $\text{Aut}(G)$ abelian and $G$ satisfies either of the following two properties: (P1) $G$ is 3-generated; (P2) $G$ has a non-trivial abelian direct factor. The first 2-group having abelian automorphism group was constructed by Miller [51] in 1913. This is a 3-generated group and, as mentioned above, it has order 64 with elementary abelian automorphism group of order 128. Earnley [17] showed that there are two more groups of order 64 having elementary abelian automorphism group. These groups are also 3-generated. Further Earnley gave a complete description of 2-groups satisfying (P2) and having abelian automorphism group and established the existence of such groups (see 1.2.8).

### 2.2 Groups $G$ with $\text{Aut}(G)$ abelian

Though the conjecture of Mahalanobis has been proved false, one might expect that some weaker form of the conjecture still holds true. Two obvious weaker forms of the conjecture are: (WC1) For a finite $p$-group $G$ with $\text{Aut}(G)$ abelian, $Z(G) = \Phi(G)$ always holds true; (WC2) For a finite $p$-group $G$ with $\text{Aut}(G)$ abelian and $Z(G) \neq \Phi(G)$, $\gamma_2(G) = Z(G)$ always holds true. So, on the way to
exploring some general structure on the class of such groups $G$, it is natural to ask the following question:

**Question.** Does there exist a finite $p$-group $G$ such that $\gamma_2(G) \leq Z(G) < \Phi(G)$ and $\text{Aut}(G)$ is abelian?

At the end of this section we will be able to answer this question.

Let $G$ be a finite $p$-group of nilpotency class 2 generated by $x_1, x_2, \ldots, x_d$, where $d$ is a positive integer. Let $e_{x_i} = x_1^{a_{i1}} x_2^{a_{i2}} \cdots x_d^{a_{id}} = \prod_{j=1}^{d} x_j^{a_{ij}}$, where $x_i \in G$ and $a_{ij}$ are non-negative integers for $1 \leq i, j \leq d$. Since the nilpotency class of $G$ is 2, we have

$$[x_k, e_{x_i}] = [x_k, \prod_{j=1}^{d} x_j^{a_{ij}}] = \prod_{j=1}^{d} [x_k, x_j^{a_{ij}}] = \prod_{j=1}^{d} [x_k, x_j]^{a_{ij}} \quad (2.1)$$

and

$$[e_{x_k}, e_{x_i}] = [\prod_{l=1}^{d} x_l^{a_{kl}}, \prod_{j=1}^{d} x_j^{a_{ij}}] = \prod_{j=1}^{d} \prod_{l=1}^{d} [x_l^{a_{kl}}, x_j^{a_{ij}}] = \prod_{j=1}^{d} \prod_{l=1}^{d} [x_l, x_j]^{a_{kl}a_{ij}}. \quad (2.2)$$

Equations (2.1) and (2.2) will be used for our calculations without any further reference.

Let $n \geq 4$ be a positive integer and $p$ be an odd prime. Consider the following group:

$$G = \left\langle x_1, x_2, x_3, x_4 \mid x_1^{p^n} = x_2^{p^4} = x_3^{p^4} = x_4^{p^2} = 1, [x_1, x_2] = x_2^{p^2}, [x_1, x_3] = x_2^{p^2}, [x_1, x_4] = x_3^{p^2}, [x_2, x_3] = x_1^{p^{n-2}}, [x_2, x_4] = x_3^{p^2}, [x_3, x_4] = x_2^{p^2} \right\rangle. \quad (2.3)$$
It is easy to see that $G$ enjoys the properties given in the following lemma.

**Lemma 2.2.1** The group $G$ is a regular $p$-group of nilpotency class 2 having order $p^{n+10}$ and exponent $p^n$. For $n = 4$, $\gamma_2(G) = Z(G) < \Phi(G)$ and for $n \geq 5$, $\gamma_2(G) < Z(G) < \Phi(G)$.

Let $e_{ix} = x_1^{a_{i1}}x_2^{a_{i2}}x_3^{a_{i3}}x_4^{a_{i4}} = \prod_{j=1}^4 x_j^{a_{ij}}$, where $x_i \in G$ and $a_{ij}$ are non-negative integers for $1 \leq i, j \leq 4$. Let $\alpha$ be an automorphism of $G$. Since the nilpotency class of $G$ is 2 and $\gamma_2(G)$ is generated by $x_1^{p^{n-2}}$, $x_2^{p^2}$, $x_3^{p^2}$, we can write $\alpha(x_i) = x_i e_{ix} = x_i \prod_{j=1}^4 x_j^{a_{ij}}$ for some non-negative integers $a_{ij}$ for $1 \leq i, j \leq 4$.

**Proposition 2.2.2** Let $G$ be the group defined in (2.3) and $\alpha$ be an automorphism of $G$ such that $\alpha(x_i) = x_i e_{ix} = x_i \prod_{j=1}^4 x_j^{a_{ij}}$, where $a_{ij}$ are some non-negative integers for $1 \leq i, j \leq 4$. Then the following equations hold:

\[
\begin{align*}
    a_{31} &\equiv 0 \mod p^{n-2}, \quad (2.4) \\
    -a_{32} + a_{13} + a_{13} a_{44} &\equiv 0 \mod p^2, \quad (2.5) \\
    -a_{33} + a_{44} + a_{11} + a_{11} a_{44} + a_{12} + a_{12} a_{44} &\equiv 0 \mod p^2, \quad (2.6) \\
    a_{21} &\equiv 0 \mod p^{n-2}, \quad (2.7) \\
    a_{44} - a_{22} + a_{33} + a_{33} a_{44} &\equiv 0 \mod p^2, \quad (2.8) \\
    a_{32} - a_{23} + a_{32} a_{44} &\equiv 0 \mod p^2, \quad (2.9) \\
    -a_{13} + a_{12} a_{23} - a_{13} a_{22} &\equiv 0 \mod p^2, \quad (2.10) \\
    a_{23} + a_{11} + a_{11} a_{22} + a_{11} a_{23} + a_{13} a_{24} - a_{14} a_{23} &\equiv 0 \mod p^2, \quad (2.11) \\
    -a_{23} + a_{24} + a_{11} a_{24} - a_{14} + a_{12} a_{24} - a_{14} a_{22} &\equiv 0 \mod p^2, \quad (2.12) \\
    a_{12} + a_{12} a_{33} - a_{13} a_{32} &\equiv 0 \mod p^2, \quad (2.13) \\
    a_{32} + a_{33} + a_{11} - a_{22} - a_{14} + a_{11} a_{32} + a_{11} a_{33} + a_{13} a_{34} - a_{14} a_{33} &\equiv 0 \mod p^2, \quad (2.14)
\end{align*}
\]
\[ a_{34} + a_{11}a_{34} + a_{12}a_{34} - a_{14}a_{32} - a_{23} \equiv 0 \mod p^2, \]  
(2.15)

\[ a_{23} - a_{32} + a_{23}a_{44} \equiv 0 \mod p^2, \]  
(2.16)

\[-a_{33} + a_{44} + a_{22} + a_{22}a_{44} \equiv 0 \mod p^2, \]  
(2.17)

\[-a_{11} + a_{33} + a_{22} + a_{22}a_{33} - a_{23}a_{32} \equiv 0 \mod p^2. \]  
(2.18)

**Proof.** Let \( \alpha \) be the automorphism of \( G \) such that \( \alpha(x_i) = x_i e_{x_i}, 1 \leq i \leq 4 \) as defined above. Since \( G_{p^2} = \langle x_1^{p^{n-2}}, x_2^{p^2}, x_3^{p^2}, x_4 \rangle \) is a characteristic subgroup of \( G \), \( \alpha(x_4) \in G_{p^2} \). Thus we get the following set of equations:

\[ a_{41} \equiv 0 \mod p^{n-2}, \]  
(2.19)

\[ a_{4i} \equiv 0 \mod p^2, \text{ for } i = 2, 3. \]  
(2.20)

We prove equations (2.4) - (2.6) by comparing the powers of \( x_i \)'s in \( \alpha([x_1, x_4]) = \alpha(x_3^{p^2}) \).

\[
\alpha([x_1, x_4]) = [\alpha(x_1), \alpha(x_4)] = [x_1 e_{x_1}, x_4 e_{x_4}]
\]

\[
= [x_1, x_4][x_1, e_{x_4}][e_{x_1}, x_4]
\]

\[
= [x_1, x_4]\Pi_{j=1}^4 [x_1, x_j]^{a_{4j}}\Pi_{j=1}^4 [x_4, x_j]^{-a_{1j}}\Pi_{j=1}^4 [x_1, x_j]^{a_{1j}a_{4j}}
\]

\[
= [x_1, x_2]^{a_{42}+a_{11}a_{42}-a_{12}a_{41}}[x_1, x_3]^{a_{43}+a_{11}a_{43}-a_{13}a_{41}}
\]

\[
[x_1, x_4]^{1+a_{44}+a_{11}a_{44}-a_{14}a_{41}}[x_2, x_3]^{a_{12}a_{43}-a_{13}a_{42}}
\]

\[
[x_2, x_4]^{a_{12}+a_{12}a_{44}-a_{14}a_{42}}[x_3, x_4]^{a_{13}+a_{13}a_{44}-a_{14}a_{43}}
\]

\[
= x_1^{p^{n-2}(a_{12}a_{43}-a_{13}a_{42})}
\]

\[
x_2^{p^2(a_{42}+a_{43}+a_{11}a_{42}-a_{12}a_{41}+a_{11}a_{43}-a_{13}a_{41}+a_{13}a_{44}-a_{14}a_{43})}
\]

\[
x_3^{p^2(1+a_{44}+a_{11}+a_{12}a_{44}-a_{14}a_{41}+a_{12}a_{44}-a_{14}a_{42})}
\]
On the other hand

\[ \alpha([x_1, x_4]) = \alpha(x_3^{p^2}) = x_3^{p^2} x_1^{p^2 a_{31}} x_2^{p^2 a_{32}} x_3^{p^2 a_{33}} x_4^{p^2 a_{34}} = x_1^{p^2 a_{31}} x_2^{p^2 a_{32}} x_3^{p^2 (1 + a_{33})}. \]

Comparing the powers of \( x_1 \) and using (2.20), we get \( a_{31} \equiv 0 \mod p^{n-2} \).

Comparing the powers of \( x_2 \) and \( x_3 \), and using (2.19) - (2.20), we get

\[
\begin{align*}
-a_{32} + a_{13} + a_{13} a_{44} & \equiv 0 \mod p^2, \\
-a_{33} + a_{44} + a_{11} + a_{11} a_{44} + a_{12} + a_{12} a_{44} & \equiv 0 \mod p^2.
\end{align*}
\]

Hence equations (2.4) - (2.6) hold.

Equations (2.7) - (2.9) are obtained by comparing the powers of \( x_1, x_2 \) and \( x_3 \) in \( \alpha([x_3, x_4]) = \alpha(x_2^{p^2}) \) and using equations (2.4), (2.19) and (2.20). Equations (2.10) - (2.12) are obtained by comparing the powers of \( x_1, x_2 \) and \( x_3 \) in \( \alpha([x_1, x_2]) = \alpha(x_2^{p^2}) \) and using equation (2.7). Equations (2.13) - (2.15) are obtained by comparing the powers of \( x_1, x_2 \) and \( x_3 \) in \( \alpha([x_1, x_3]) = \alpha(x_2^{p^2}) \) and using equations (2.4) and (2.7). Equations (2.16) - (2.17) are obtained by comparing the powers of \( x_2 \) and \( x_3 \) in \( \alpha([x_2, x_4]) = \alpha(x_3^{p^2}) \) and using equations (2.7), (2.19) and (2.20). The last equation (2.18) is obtained by comparing the powers of \( x_1 \) in \( \alpha([x_2, x_3]) = \alpha(x_1^{p^{n-2}}) \).

**Theorem 2.2.3** Let \( G \) be the group defined in (2.3). Then all automorphisms of \( G \) are central.

**Proof.** We start with the claim that \( 1 + a_{44} \neq 0 \mod p \). For, let us assume the contrary, i.e., \( p \) divides \( 1 + a_{44} \). Then

\[
\alpha(x_4^{p^2}) = \alpha(x_4)^p = x_4^{p(1+a_{44})}(x_1^{a_{44}} x_2^{a_{42}} x_3^{a_{43}})^p \in Z(G),
\]
since $a_{4j} \equiv 0 \mod p^2$ for $1 \leq j \leq 3$ by equations (2.19) and (2.20). But this is not possible as $x_4^n \not\in \mathbb{Z}(G)$. This proves our claim. Subtracting (2.16) from (2.5), we get $(1 + a_{44})(a_{13} - a_{23}) \equiv 0 \mod p^2$. Since $p$ does not divide $1 + a_{44}$, we get

$$a_{13} \equiv a_{23} \mod p^2. \quad (2.21)$$

By equations (2.10) and (2.21) we have

$$a_{13}(1 - a_{12} + a_{22}) \equiv 0 \mod p^2. \quad (2.22)$$

Here we have three possibilities, namely (i) $a_{13} \equiv 0 \mod p^2$, (ii) $a_{13} \equiv 0 \mod p$, but $a_{13} \not\equiv 0 \mod p^2$, (iii) $a_{13} \not\equiv 0 \mod p$. We are going to show that cases (ii) and (iii) do not occur and in the case (i) $a_{ij} \equiv 0 \mod p^2, 1 \leq i, j \leq 4$.

**Case (i).** Assume that $a_{13} \equiv 0 \mod p^2$. Equations (2.9) and (2.21), together with the fact that $p$ does not divide $1 + a_{44}$, gives $a_{32} \equiv 0 \mod p^2$. We claim that $1 + a_{33} \not\equiv 0 \mod p$. Suppose $p$ divides $1 + a_{33}$. Since $a_{32} \equiv 0 \mod p^2$ and $a_{31} \equiv 0 \mod p^{n-2}$ (equation (2.4)), we get $\alpha(x_3^p) = x_1^{p^3a_{31}}x_2^{p^3a_{32}}x_3^{p^3(1+a_{33})}x_4^{p^3a_{34}} = 1$, which is not possible. This proves our claim. So by equation (2.13), we get $a_{12} \equiv 0 \mod p^2$.

Subtracting (2.17) from (2.6), we get $(a_{11} - a_{22})(1 + a_{44}) \equiv 0 \mod p^2$. This implies that $a_{11} - a_{22} \equiv 0 \mod p^2$. Since $a_{i3} \equiv 0 \mod p^2$ for $i = 1, 2, 3$, by equation (2.11) we get $a_{11} + a_{33} \equiv 0 \mod p^2$. Thus $p^2$ divides $a_{11}$ or $1 + a_{11}$. We claim that $p^2$ can not divide $1 + a_{11}$. For, suppose the contrary, i.e., $a_{11} \equiv -1 \mod p^2$. Since $n - 2 \geq 2$ and $a_{12} \equiv a_{13} \equiv 0 \mod p^2$, we get

$$\alpha(x_1)^{p^{n-2}} = x_1^{p^{n-2}(1+a_{11})}x_2^{p^{n-2}a_{12}}x_3^{p^{n-2}a_{13}}x_4^{p^{n-2}a_{14}} = 1.$$
This contradiction, to the fact that order of $x_1$ is $p^n$, proves our claim. Hence $p^2$ divides $a_{11}$. Since $a_{11} - a_{22} \equiv 0 \pmod{p^2}$, by equation (2.17), it follows that $a_{33} \equiv a_{44} \pmod{p^2}$. Putting the values $a_{23}, a_{11}$ and $a_{22}$ in (2.18), we get $a_{33} \equiv 0 \pmod{p^2}$. Thus $a_{44} \equiv 0 \pmod{p^2}$. Putting values of $a_{32}, a_{33}, a_{11}, a_{22}$ and $a_{13}$ in (2.14), we get $a_{14} \equiv 0 \pmod{p^2}$. Putting values of $a_{12}, a_{14}, a_{11}$ and $a_{23}$ in (2.15), we get $a_{34} \equiv 0 \pmod{p^2}$. Putting above values in (2.12), we get $a_{24} \equiv 0 \pmod{p^2}$.

Hence $a_{ij} \equiv 0 \pmod{p^2}$ for $1 \leq i, j \leq 4$.

**Case (ii).** Assume that $a_{13} \equiv 0 \pmod{p}$, but $a_{13} \not\equiv 0 \pmod{p^2}$. Equation (2.22) implies that $(1-a_{12}+a_{22}) \equiv 0 \pmod{p}$. Now consider all the equations (2.7)-(2.18) mod $p$. Repeating the arguments of Case (i) after replacing $p^2$ by $p$, we get the following facts: (a) $a_{32} \equiv 0 \pmod{p}$ (by (2.9)); (b) $a_{12} \equiv 0 \pmod{p}$ (by (2.13)); (c) $a_{11} - a_{22} \equiv 0 \pmod{p}$ (subtracting (2.17) from (2.6)); (d) $a_{11}(1 + a_{11}) \equiv 0 \pmod{p}$ (by (2.11)). We claim that $a_{11} \equiv 0 \pmod{p}$. For, suppose that $a_{11} + 1 \equiv 0 \pmod{p}$. Since $n - 1 \geq 3$ and $a_{12} \equiv a_{13} \equiv 0 \pmod{p}$, it follows that $\alpha(x_1)^{p^n-1} = x_1^{p^n-1(1+a_{11})} x_2^{p^n-1} x_3^{p^n-1} x_4^{p^n-1} = 1$, which is a contradiction. This proves that $p$ can not divide $a_{11} + 1$. Hence $p$ divides $a_{11}$, and therefore by fact (c), we have $a_{22} \equiv 0 \pmod{p}$. This gives a contradiction to the fact that $(1 - a_{12} + a_{22}) \equiv 0 \pmod{p}$. Thus Case (ii) does not occur.

**Case (iii).** Finally assume that $a_{13} \not\equiv 0 \pmod{p}$. Thus $(1 - a_{12} + a_{22}) \equiv 0 \pmod{p^2}$, i.e., $1 + a_{22} \equiv a_{12} \pmod{p^2}$ (we’ll use this information throughout the remaining proof without referring). Notice that $(\alpha(x_2x_1^{-1}))^{p^2} = x_1^{-p^2(1+a_{11})}$. Since the order of $(\alpha(x_2x_1^{-1}))^{p^2}$ is $p^{n-2}$, $p$ does not divide $(1 + a_{11})$. Putting the value of $a_{32}$ from (2.16) into (2.9), we have $a_{23} = a_{23}(1 + a_{44})^2 \pmod{p^2}$. Since $a_{23} \equiv a_{13} \pmod{p^2}$ (equation (2.21)) and $a_{13} \not\equiv 0 \pmod{p}$, it follows that $a_{23} \not\equiv 0 \pmod{p}$. Hence $(1 + a_{44})^2 \equiv 1 \pmod{p^2}$. This gives $a_{44}(a_{44} + 2) \equiv 0 \pmod{p^2}$. Thus we have three cases (iii)(a) $a_{44} \equiv 0 \pmod{p^2}$, (iii)(b) $a_{44} \equiv 0 \pmod{p}$, but $a_{44} \not\equiv 0 \pmod{p^2}$.
and (iii)(c) \( a_{44} \neq 0 \mod p \). We are going to consider these cases one by one.

**Case (iii)(a).** Suppose that \( a_{44} \equiv 0 \mod p^2 \). Using this in (2.16) and (2.17), we get \( a_{32} \equiv a_{23} \mod p^2 \) and \( a_{22} \equiv a_{33} \mod p^2 \) respectively. Putting the value of \( a_{44} \) in (2.6), we have \( a_{12} + a_{11} \equiv a_{33} \mod p^2 \). Further, replacing \( a_{12} \) by \( 1 + a_{22} \) and \( a_{22} \) by \( a_{33} \), we have \( 1 + a_{11} \equiv 0 \mod p^2 \), which is a contradiction.

**Case (iii)(b).** Suppose that \( a_{44} \equiv 0 \mod p \), but \( a_{44} \neq 0 \mod p^2 \). Notice that by reading the equations \( \mod p \), arguments of Case (iii)(a) show that \( 1 + a_{11} \equiv 0 \mod p \), which is again a contradiction.

**Case (iii)(c).** Suppose that \( a_{44} \neq 0 \mod p \). This implies that \( a_{44} \equiv -2 \mod p^2 \). Putting this value of \( a_{44} \) in the difference of (2.8) and (2.6), we get \( a_{11} + a_{12} - a_{22} \equiv 0 \mod p^2 \). Since \( 1 + a_{22} \equiv a_{12} \mod p^2 \), this equation contradicts the fact that \( 1 + a_{11} \neq 0 \mod p \).

Thus Case (iii) cannot occur. This completes the proof of the theorem.

The following theorem gives the answer to the question raised at the beginning of this section.

**Theorem 2.2.4** For every positive integer \( n \geq 4 \) and every odd prime \( p \), there exists a group \( G \) of order \( p^{n+10} \) and exponent \( p^n \) such that

1. for \( n = 4 \), \( \gamma_2(G) = Z(G) < \Phi(G) \) and \( \text{Aut}(G) \) is abelian;

2. for \( n \geq 5 \), \( \gamma_2(G) < Z(G) < \Phi(G) \) and \( \text{Aut}(G) \) is abelian.

Moreover, the order of \( \text{Aut}(G) \) is \( p^{n+20} \).

**Proof.** Let \( G \) be the group defined in (2.3). By Lemma 2.2.1, we have \( |G| = p^{n+10} \), \( \gamma_2(G) = Z(G) < \Phi(G) \) for \( n = 4 \) and \( \gamma_2(G) < Z(G) < \Phi(G) \) for \( n \geq 5 \).

By Theorem 2.2.3, we have \( \text{Aut}(G) = \text{Autcent}(G) \). Thus to complete the proof of the theorem, it is sufficient to prove that \( \text{Autcent}(G) \) is an abelian group.
Since \( Z(G) < \Phi(G) \), \( G \) is purely non-abelian. The exponents of \( Z(G) \), \( \gamma_2(G) \) and \( G/\gamma_2(G) \) are \( p^{n-2} \), \( p^2 \) and \( p^{n-2} \) respectively. Thus we get

\[
R = \{ z \in Z(G) \ | \ |z| \leq p^{n-2} \} = Z(G)
\]

and

\[
K = \{ x \in G \ | \ \text{ht}(x\gamma_2(G)) \geq p^2 \} = G^{p^2}\gamma_2(G) = Z(G).
\]

This shows that \( R = K \). Also \( R/\gamma_2(G) = Z(G)/\gamma_2(G) = \langle x_1^{p^2}\gamma_2(G) \rangle \). Thus all the conditions of Theorem 1.2.6 are now satisfied. Hence Autcent\((G)\) is abelian.

That the order of Aut\((G)\) is \( p^{n+20} \) can be easily proved by using Lemmas 1.1.2, 1.1.3, Theorem 1.2.5 and the structures of \( G/\gamma_2(G) \) and \( Z(G) \). This completes the proof of the theorem.

### 2.3 Groups \( G \) with Aut\((G)\) elementary abelian

As mentioned in the Section 2.1, all \( p \)-groups \( G \) (except the ones in [37]) available in the literature and having abelian automorphism group are special \( p \)-groups. Thus it follows that Aut\((G)\), for all such groups \( G \), is elementary abelian. One more weaker form of the conjecture of Mahalanobis is: (WC3) If Aut\((G)\) is an elementary abelian \( p \)-group, then \( G \) is special. Berkovich and Janko [5, Problem 722] published the following long standing problem: (Old problem) Study the \( p \)-groups \( G \) with elementary abelian Aut\((G)\).

The following theorem provides some structural information about a group \( G \) for which Aut\((G)\) is elementary abelian.

**Theorem 2.3.1** Let \( G \) be a finite \( p \)-group such that Aut\((G)\) is elementary abelian, where \( p \) is an odd prime. Then one of the following two conditions holds true:
1. $Z(G) = \Phi(G)$ is elementary abelian;

2. $\gamma_2(G) = \Phi(G)$ is elementary abelian.

Moreover, the exponent of $G$ is $p^2$.

**Proof.** Since $\text{Aut}(G)$ is elementary abelian, $G/Z(G)$ is elementary abelian and so $\Phi(G) \leq Z(G)$. Also from Theorem 1.2.8 $G$ is purely non-abelian. It follows from Theorem 1.2.9 that either $Z(G)$ or $G/\gamma_2(G)$ is of exponent $p$. If the exponent of $Z(G)$ is $p$, then by Lemma 1.1.7 $Z(G) \leq \Phi(G)$. Hence $Z(G) = \Phi(G)$ is elementary abelian. If the exponent of $G/\gamma_2(G)$ is $p$, then obviously $\gamma_2(G) = \Phi(G)$. Thus the exponent of $G$ is at most $p^2$. That the exponent of $G$ can not be $p$, follows from Theorem 1.2.7. Hence the exponent of $G$ is $p^2$. This completes the proof of the theorem.

Let $G$ be an arbitrary finite $p$-group such that $\text{Aut}(G)$ is elementary abelian. Then it follows from the previous theorem that one of the following two conditions necessarily holds true: (C1) $Z(G) = \Phi(G)$ is elementary abelian; (C2) $\gamma_2(G) = \Phi(G)$ is elementary abelian. So one might expect that for such groups $G$ both of the conditions (C1) and (C2) hold true, i.e., WC(3) holds true, or, a little less ambitiously, (C1) always holds true or (C2) always holds true. In the following two theorems we show that none of the statements in the preceding sentence holds true.

**Theorem 2.3.2** There exists a group $G$ of order $p^9$ such that $\text{Aut}(G)$ is elementary abelian of order $p^{20}$, $\Phi(G) < Z(G)$ and $\gamma_2(G) = \Phi(G)$ is elementary abelian.
Theorem 2.3.3 There exists a group $G$ of order $p^8$ such that $\text{Aut}(G)$ is elementary abelian of order $p^{16}$, $\gamma_2(G) < \Phi(G)$ and $Z(G) = \Phi(G)$ is elementary abelian.

First we proceed to construct $p$-group $G$ as in Theorem 2.3.2

Let $p$ be any prime, even or odd. Consider the group

$$
G_1 = \langle x_1, x_2, x_3, x_4, x_5 \mid x_1^{p^2} = x_2^{p^2} = x_3^{p^2} = x_4^{p^2} = x_5^p = 1, [x_1, x_2] = x_1^p, [x_1, x_3] = x_3^p, [x_1, x_4] = 1, [x_1, x_5] = x_1^p, [x_2, x_3] = x_2^p, [x_2, x_4] = 1, [x_2, x_5] = x_2^p, [x_3, x_4] = x_3^p, [x_3, x_5] = 1, [x_4, x_5] = 1 \rangle.
$$

(2.23)

It is easy to see the following properties of $G_1$.

Lemma 2.3.4 The group $G_1$ is a $p$-group having order $p^9$, $\gamma_2(G_1) = \Phi(G_1) < Z(G_1)$, $\Phi(G_1)$ is elementary abelian and the exponent of $Z(G_1)$ is $p^2$, where $p$ is any prime. Moreover, if $p$ is odd, then $G_1$ is regular.

It can be checked by using GAP [23] that for $p = 2$, $\text{Aut}(G_1)$ is elementary abelian. So we assume that $p$ is odd. Let $\alpha$ be an arbitrary automorphism of $G_1$. Since the nilpotency class of $G_1$ is 2 and $\gamma_2(G_1)$ is generated by the set $\{x_i^p \mid 1 \leq i \leq 4\}$, we can write

$$
\alpha(x_i) = x_i \prod_{j=1}^{5} x_j^{a_{ij}}
$$

(2.24)

for some non-negative integers $a_{ij}$ for $1 \leq i, j \leq 5$.

Lemma 2.3.5 Let $\alpha$ be the automorphism of $G_1$ defined in (2.24). Then

$$
a_{4j} \equiv 0 \pmod{p} \text{ for } j = 1, 2, 3, 5.
$$

(2.25)
Proof. Since $x_4 \in Z(G_1)$, it follows that $\alpha(x_4) = x_4^{1+a_{44}}x_1^{a_{41}}x_2^{a_{42}}x_3^{a_{43}}x_5^{a_{45}} \in Z(G_1)$. This is possible only when $a_{4j} \equiv 0 \mod p$ for $j = 1, 2, 3, 5$, which completes the proof of the lemma.

We’ll make use of the following table in the proof of Theorem 2.3.2, which is produced in the following way. The equation in the $k$th row is obtained by applying $\alpha$ on the relation in $k$th row, then comparing the powers of $x_i$ in the same row, and using preceding equations in the table and equations (2.25). For example, equation in 5th row is obtained by applying $\alpha$ on $[x_1, x_3] = x_3^p$, then comparing the powers of $x_2$ and using equations in 2nd and 3rd row.

Table 2.1: Table for the group $G_1$

<table>
<thead>
<tr>
<th>No.</th>
<th>equations (read $\equiv 0 \mod p$)</th>
<th>relations</th>
<th>$x_i$'s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$a_{5j}, 1 \leq j \leq 4$</td>
<td>$x_5^p = 1$</td>
<td>$x_1, \ldots, x_4$</td>
</tr>
<tr>
<td>2</td>
<td>$a_{12}$</td>
<td>$[x_1, x_5] = x_1^p$</td>
<td>$x_2$</td>
</tr>
<tr>
<td>3</td>
<td>$a_{13}$</td>
<td>$[x_1, x_5] = x_1^p$</td>
<td>$x_3$</td>
</tr>
<tr>
<td>4</td>
<td>$a_{14}$</td>
<td>$x_1, x_5 = x_1^p$</td>
<td>$x_4$</td>
</tr>
<tr>
<td>5</td>
<td>$a_{32}$</td>
<td>$[x_1, x_3] = x_3^p$</td>
<td>$x_2$</td>
</tr>
<tr>
<td>6</td>
<td>$a_{55}(1 + a_{11})$</td>
<td>$[x_1, x_5] = x_1^p$</td>
<td>$x_1$</td>
</tr>
<tr>
<td>7</td>
<td>$a_{23}(1 + a_{11})$</td>
<td>$[x_1, x_2] = x_1^p$</td>
<td>$x_3$</td>
</tr>
<tr>
<td>8</td>
<td>$a_{21} + a_{21}a_{55}$</td>
<td>$x_2, x_5 = x_4^p$</td>
<td>$x_1$</td>
</tr>
<tr>
<td>9</td>
<td>$a_{31} + a_{31}a_{55}$</td>
<td>$[x_3, x_5] = x_4^p$</td>
<td>$x_1$</td>
</tr>
<tr>
<td>10</td>
<td>$a_{35} + a_{11}a_{55} - a_{15}a_{31} - a_{31}$</td>
<td>$[x_1, x_3] = x_3^p$</td>
<td>$x_1$</td>
</tr>
<tr>
<td>11</td>
<td>$a_{11}(1 + a_{33})$</td>
<td>$[x_1, x_3] = x_3^p$</td>
<td>$x_3$</td>
</tr>
<tr>
<td>12</td>
<td>$a_{33}(1 + a_{22})$</td>
<td>$[x_2, x_3] = x_2^p$</td>
<td>$x_2$</td>
</tr>
<tr>
<td>13</td>
<td>$a_{55} + a_{43} + a_{33}a_{55} - a_{44}$</td>
<td>$[x_3, x_5] = x_4^p$</td>
<td>$x_4$</td>
</tr>
<tr>
<td>14</td>
<td>$a_{55} + a_{22} + a_{22}a_{55} + a_{23}(1 + a_{55}) - a_{44}$</td>
<td>$x_2, x_5 = x_4^p$</td>
<td>$x_4$</td>
</tr>
<tr>
<td>15</td>
<td>$(a_{22} + a_{25})(1 + a_{11}) - a_{15}a_{21}$</td>
<td>$[x_1, x_2] = x_1^p$</td>
<td>$x_1$</td>
</tr>
<tr>
<td>16</td>
<td>$a_{35}(1 + a_{23} + a_{22}) - a_{25}(1 + a_{23}) - a_{24}$</td>
<td>$[x_2, x_3] = x_2^p$</td>
<td>$x_4$</td>
</tr>
<tr>
<td>17</td>
<td>$a_{15} - a_{15}a_{22} - a_{15}a_{23}$</td>
<td>$[x_1, x_2] = x_1^p$</td>
<td>$x_4$</td>
</tr>
<tr>
<td>18</td>
<td>$a_{15} - a_{15}a_{33} - a_{34}$</td>
<td>$[x_1, x_3] = x_3^p$</td>
<td>$x_4$</td>
</tr>
</tbody>
</table>

Now we are ready to prove Theorem 2.3.2. In the following proof, by (k) we mean the equation in the $k$th row of Table 2.1.

Proof of Theorem 2.3.2. Consider the group $G_1$ defined in 2.23. It follows
from Lemma 2.3.4 that $G_1$ is of order $p^9$, $\Phi(G_1) < Z(G_1)$ and $\gamma_2(G_1) = \Phi(G_1)$ is elementary abelian. It is easy to show that the order of Autcent($G_1$) is $p^{20}$. As mentioned earlier, it can be checked using GAP that Aut($G_1$) is elementary abelian for $p = 2$. We therefore assume that $p$ is odd. We now prove that all automorphisms of $G_1$ are central. Let $\alpha$ be the automorphism of $G_1$ defined in (2.24), i.e., $\alpha(x_i) = x_i \prod_{j=1}^{5} x_i^{a_{ij}}$, where $a_{ij}$ are non-negative integers for $1 \leq i, j \leq 5$. Since $G_1/Z(G_1)$ is elementary abelian, it is sufficient to prove that $a_{ij} \equiv 0 \mod p$ for $1 \leq i, j \leq 5$. Since $\alpha(x_1^p) = x_1^{p(1+a_{11})} \prod_{j=2}^{5} x_j^{p a_{1j}} \neq 1$, $x_5^p = 1$ and $a_{1j} \equiv 0 \mod p$ for $2 \leq j \leq 4$, it follows that $1 + a_{11}$ is not divisible by $p$. Therefore (6) and (7) give $a_{55} \equiv 0 \mod p$ and $a_{23} \equiv 0 \mod p$ respectively. Thus by (8) and (9) respectively, we get $a_{21} \equiv 0 \mod p$ and $a_{31} \equiv 0 \mod p$. Using the fact that $a_{31} \equiv 0 \mod p$, (10) reduces to the equation $a_{35}(1 + a_{11}) \equiv 0 \mod p$. Since $1 + a_{11}$ is not divisible by $p$, we get $a_{35} \equiv 0 \mod p$. Observe that $1 + a_{33}$ is not divisible by $p$. For, suppose $p$ divides $1 + a_{33}$. Since $a_{31}, a_{32}, a_{35}$ are divisible by $p$ and $x_4 \in Z(G_1)$, it follows that $\alpha(x_3) \not\in Z(G_1)$, which is not true. Using this fact, it follows from (11) that $a_{11} \equiv 0 \mod p$. Using above information, (13), (14) and (15) reduce, respectively, to the following equations.

$$a_{33} - a_{44} \equiv 0 \mod p,$$  \tag{2.26}  

$$a_{22} - a_{44} \equiv 0 \mod p,$$  \tag{2.27}  

$$a_{22} + a_{25} \equiv 0 \mod p.$$  \tag{2.28}  

Subtracting equation (2.27) from equation (2.26), we get $a_{33} - a_{22} \equiv 0 \mod p$. Adding this to equation (2.28) gives $a_{33} + a_{25} \equiv 0 \mod p$. Using this fact after adding (12) to equation (2.28), we get $a_{22}(1 + a_{33}) \equiv 0 \mod p$. Since $1 + a_{33}$ is
not divisible by $p$, $a_{22} \equiv 0 \mod p$. Thus equations (2.27) and (2.28) give $a_{44} \equiv 0 \mod p$ and $a_{25} \equiv 0 \mod p$ respectively. So $a_{33} \equiv 0 \mod p$ from equation 2.26. Now (16) and (17) give $a_{24} \equiv 0 \mod p$ and $a_{15} \equiv 0 \mod p$ respectively. Finally, from (18) we get $a_{34} \equiv 0 \mod p$. Hence all $a_{i_j}$'s are divisible by $p$, which shows that $\alpha$ is a central automorphism of $G_1$. Since $\alpha$ was an arbitrary automorphism of $G_1$, we get $\text{Aut}(G_1) = \text{Autcent}(G_1)$.

It now remains to prove that $\text{Aut}(G_1)$ is elementary abelian. Notice that $G_1$ is purely non-abelian. Since $\gamma_2(G_1) = \Phi(G_1)$, the exponent of $G_1/\gamma_2(G_1)$ is $p$. That $\text{Aut}(G_1) = \text{Autcent}(G_1)$ is elementary abelian now follows from Theorem 1.2.9. This completes the proof of the theorem.

Now we proceed to construct a finite $p$-group $G$ such that $\text{Aut}(G)$ is elementary abelian, $\gamma_2(G) < \Phi(G)$ and $\Phi(G) = Z(G)$ is elementary abelian. Let $p$ be any prime, even or odd. Define the group

\[ G_2 = \langle x_1, x_2, x_3, x_4 \mid x_1^{p^2} = x_2^{p^2} = x_3^{p^2} = x_4^{p^2} = 1, [x_1, x_2] = 1, [x_1, x_3] = x_4^p, [x_1, x_4] = x_4^p, [x_2, x_3] = x_1^p, [x_2, x_4] = x_2^p, [x_3, x_4] = x_3^p \rangle. \]  

(2.29)

It is easy to prove the following lemma.

**Lemma 2.3.6** The group $G_2$ is a $p$-group of order $p^8$, $\gamma_2(G_2) < \Phi(G_2)$ and $Z(G_2) = \Phi(G_2)$ is elementary abelian, where $p$ is any prime. Moreover, if $p$ is odd, then $G_2$ is regular.

Again, it can be checked by using GAP that for $p = 2$, $\text{Aut}(G_2)$ is elementary abelian. So from now onwards, we assume that $p$ is odd. Let $\alpha$ be an arbitrary automorphism of $G_2$. Since the nilpotency class of $G_2$ is 2 and $\gamma_2(G_2)$ is generated
by the set \( \{ x_1^p, x_2^p, x_4^p \} \), we can write

\[
\alpha(x_i) = x_i \prod_{j=1}^{4} x_j^{a_{ij}}
\]

(2.30)

for some non-negative integers \( a_{ij} \) for \( 1 \leq i, j \leq 4 \).

The following table, which will be used in the proof of Theorem 2.3.3 below, is produced in a similar fashion as Table 1.

<table>
<thead>
<tr>
<th>No.</th>
<th>equations</th>
<th>relations</th>
<th>( x_i )'s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( a_{13} \equiv 0 \mod p )</td>
<td>( x_2, x_3 = x_1^p )</td>
<td>( x_3 )</td>
</tr>
<tr>
<td>2</td>
<td>( a_{23} \equiv 0 \mod p )</td>
<td>( x_2, x_4 = x_2^p )</td>
<td>( x_3 )</td>
</tr>
<tr>
<td>3</td>
<td>( a_{43} \equiv 0 \mod p )</td>
<td>( x_1, x_3 = x_4^p )</td>
<td>( x_3 )</td>
</tr>
<tr>
<td>4</td>
<td>( a_{41} \equiv 0 \mod p )</td>
<td>( x_1, x_4 = x_4^p )</td>
<td>( x_1 )</td>
</tr>
<tr>
<td>5</td>
<td>( a_{21} \equiv 0 \mod p )</td>
<td>( x_2, x_4 = x_2^p )</td>
<td>( x_1 )</td>
</tr>
<tr>
<td>6</td>
<td>( a_{24} \equiv 0 \mod p )</td>
<td>( x_2, x_4 = x_2^p )</td>
<td>( x_4 )</td>
</tr>
<tr>
<td>7</td>
<td>( a_{14} \equiv 0 \mod p )</td>
<td>( x_2, x_3 = x_1^p )</td>
<td>( x_4 )</td>
</tr>
<tr>
<td>8</td>
<td>( a_{44}(1 + a_{22}) \equiv 0 \mod p )</td>
<td>( x_2, x_4 = x_2^p )</td>
<td>( x_2 )</td>
</tr>
<tr>
<td>9</td>
<td>( a_{11} + a_{11}a_{44} \equiv 0 \mod p )</td>
<td>( x_1, x_4 = x_4^p )</td>
<td>( x_4 )</td>
</tr>
<tr>
<td>10</td>
<td>( a_{22} + a_{22}a_{33} + a_{33} - a_{11} \equiv 0 \mod p )</td>
<td>( x_2, x_3 = x_1^p )</td>
<td>( x_1 )</td>
</tr>
<tr>
<td>11</td>
<td>(-a_{12}(1 + a_{33}) \equiv 0 \mod p )</td>
<td>( x_3, x_4 = x_4^p )</td>
<td>( x_1 )</td>
</tr>
<tr>
<td>12</td>
<td>( a_{12} + a_{12}a_{44} - a_{42} \equiv 0 \mod p )</td>
<td>( x_1, x_4 = x_4^p )</td>
<td>( x_2 )</td>
</tr>
<tr>
<td>13</td>
<td>( a_{32} + a_{32}a_{44} - a_{34}a_{42} - a_{42} \equiv 0 \mod p )</td>
<td>( x_3, x_4 = x_4^p )</td>
<td>( x_2 )</td>
</tr>
<tr>
<td>14</td>
<td>( a_{34}(1 + a_{22}) - a_{12} \equiv 0 \mod p )</td>
<td>( x_2, x_3 = x_1^p )</td>
<td>( x_2 )</td>
</tr>
<tr>
<td>15</td>
<td>( a_{11}(1 + a_{33} + a_{34}) + a_{33} + a_{34} - a_{44} \equiv 0 \mod p )</td>
<td>( x_1, x_3 = x_4^p )</td>
<td>( x_4 )</td>
</tr>
<tr>
<td>16</td>
<td>( a_{31} + a_{31}a_{44} + a_{33} + a_{33}a_{44} \equiv 0 \mod p )</td>
<td>( x_3, x_4 = x_4^p )</td>
<td>( x_4 )</td>
</tr>
</tbody>
</table>

Now we are ready to prove Theorem 2.3.3. By (k), in the following proof, we mean the equation in the \( k \)th row of Table 2.2.

**Proof of Theorem 2.3.3.** Consider the group \( G_2 \) defined in 2.29. It follows from Lemma 2.3.6 that \( G_2 \) is of order \( p^8 \), \( \gamma_2(G_2) < \Phi(G_2) \) and \( Z(G_2) = \Phi(G_2) \) is elementary abelian. It is again easy to show that the order of \( \text{Aut}(G_2) \) is \( p^{16} \). Since \( \text{Aut}(G_2) \) is elementary abelian for \( p = 2 \), assume that \( p \) is odd. As in the proof of Theorem 2.3.2, to show that all automorphisms of \( G_2 \) are central, it
is sufficient to show that \( a_{ij} \equiv 0 \mod p \) for \( 1 \leq i, j \leq 4 \).

Since \( a_{21}, a_{23}, a_{24} \) are divisible by \( p \), it follows that \( (1 + a_{22}) \) is not divisible by \( p \). For, if \( p \) divides \( (1 + a_{22}) \), then \( \alpha(x_2) \in Z(G_2) \), which is not possible. Using this fact, (8) gives \( a_{44} \equiv 0 \mod p \). Thus from (9) we get \( a_{11} \equiv 0 \mod p \). Now we observe from (10) that \( (1 + a_{33}) \) is not divisible by \( p \). For, suppose, \( (1 + a_{33}) \) is divisible by \( p \), then using the fact that \( a_{11} \equiv 0 \mod p \), (10) gives \( a_{33} \equiv 0 \mod p \), which is not possible. Thus (11) gives \( a_{42} \equiv 0 \mod p \). Now using that \( a_{42} \) and \( a_{44} \) are divisible by \( p \), (12) and (13) give \( a_{12} \equiv 0 \mod p \) and \( a_{32} \equiv 0 \mod p \) respectively. Since \( a_{12} \equiv 0 \mod p \) and \( (1 + a_{22}) \) is not divisible by \( p \), (14) gives \( a_{34} \equiv 0 \mod p \). Using that \( a_{11}, a_{34} \) and \( a_{44} \) are divisible by \( p \), (15) gives \( a_{33} \equiv 0 \mod p \). Now using that \( a_{33} \) and \( a_{44} \) are divisible by \( p \), equation (16) gives \( a_{31} \equiv 0 \mod p \). Since \( a_{11} \) and \( a_{33} \) are divisible by \( p \), equation (10) gives \( a_{22} \equiv 0 \mod p \).

Hence \( a_{ij} \equiv 0 \mod p \) for \( 1 \leq i, j \leq 4 \).

Since \( Z(G_2) \) is elementary abelian, \( \text{Aut}(G_2) = \text{Autcent}(G_2) \) is elementary abelian by Theorem 1.2.9. This completes the proof of the theorem.

Let \( G \) be a purely non-abelian finite 2-group such that \( \text{Aut}(G) \) is elementary abelian. Thus \( \text{Aut}(G) = \text{Autcent}(G) \). Then \( G \) satisfies one of the three conditions of Theorem 1.2.10. We here record that there exist groups \( G \) which satisfy exactly one condition of this theorem. It is easy to show that the 2-group \( G_1 \) constructed in (2.23) satisfies only the first condition of Theorem 1.2.10 and the 2-group \( G_2 \) constructed in (2.29) satisfies only the second condition of Theorem 1.2.10. That \( \text{Aut}(G_1) \) and \( \text{Aut}(G_2) \) are elementary abelian, can be checked using GAP. The examples of 2-groups \( G \) satisfying only the third condition of Theorem 1.2.10 with \( \text{Aut}(G) \) elementary abelian were constructed by Miller [51] and Curran [13].

The examples constructed in Theorems 2.2.4, 2.3.2 and 2.3.3 indicate that it
is difficult to put an obvious structure on the class of groups $G$ such that $\text{Aut}(G)$ is abelian or even elementary abelian. We remark that many non-isomorphic groups, satisfying the conditions of the above theorems, can be obtained by making suitable changes in the presentations given in (2.3), (2.23) and (2.29). We conclude this chapter with a further remark that the kind of examples constructed in this chapter may be useful in cryptography (see [48] for more details).