GROUPS OF ORDER $p^4$ MADE LESS DIFFICULT

JEFFREY D. ADLER, MICHAEL GARLOW, AND ETHEL R. WHELAND

Abstract. Using only undergraduate-level methods, we classify all groups of order $p^4$, where $p$ is an odd prime.

0. Introduction

Marcel Wild recently provided a simple classification [7] of the 14 groups of order 16. The virtue of his presentation is that it relies only on elementary methods, except for his use of the Cyclic Extension Theorem (see Theorem 2 below), for which Wild suggested that there should be an elementary proof. The present article has two purposes: to provide such a proof, thus putting all of Wild’s machinery onto an elementary footing; and to extend this machinery enough that one could use it to classify the groups of order $p^4$ for any prime $p$ without a lot of effort. We perform this classification when $p$ is odd. (There are 15 such groups.) For completeness, we also comment on the $p = 2$ case, though of course it is already covered by Wild. Our methods and results lead to several interesting projects and problems for students.

The cost of the generality of $p$ is that we must depend on some basic linear algebra in order to avoid an explosion of ad hoc calculations. More specifically, of all the results and tools that we use, the following are the most advanced:

- exactly half of the nonzero elements of a prime field of odd order are squares;
- every nontrivial finite $p$-group has a normal subgroup of index $p$;
- every nontrivial finite $p$-group has a nontrivial center;
- basic manipulation of matrices;
- theory of Jordan canonical forms (Lemma 14);
- Fundamental Theorem of Finite Abelian Groups.

Some of these could be dispensed with, but at the cost of more computation.

In §1 we recall the notion of an extension type (which we learned from [7]); show that every extension type determines a group (this is the Cyclic Extension Theorem); and explore (in §1.3) when two extension types determine isomorphic groups. In §2 we first discuss the abelian case, and then begin the construction of all nonabelian groups of order $p^4$ by cooking up a collection of extension types that together must describe all such groups. To keep this collection small, we make heavy use of the results of §1.3. In §3 we complete the classification by determining precisely which extension types from §2 yield isomorphic groups. Finally, in §4 we comment on the $p = 2$ case.

The classification of the groups of order $p^4$, and much else, was known to Hölder [5] and Young [8], and is covered in §§112–118 of the textbook of Burnside [2]. One can go much farther with the help of computers. See [1] for a history of the classification of small groups, and [6] for an example of recent progress.

Date: 20 July, 2006. We inserted, deleted, or changed about 30 words in October, 2016.
Notation: Let \( p \) denote an odd prime. For a natural number \( n \in \mathbb{N} \), \( C_n \) will denote the cyclic group with \( n \) elements. If \( x \) is an element of a group \( G \), then \( \text{Int}(x) \) will denote the automorphism of \( G \) that sends each element \( g \in G \) to \( xgx^{-1} \). If \( \tau \) is in the group \( \text{Aut}(G) \) of automorphisms of \( G \), then \( G^\tau \) will denote the set of fixed points of \( \tau \) in \( G \): \( G^\tau = \{ g \in G : \tau(g) = g \} \). We let \( |G| \) denote the order of \( G \). Let \( \mathbb{F}_p \) denote the field with \( p \) elements, and \( \text{GL}_m(\mathbb{F}_p) \) the group of invertible \( m \)-by-\( m \) matrices with entries in \( \mathbb{F}_p \). Fix a nonsquare \( \varepsilon \) modulo \( p \).

Acknowledgements: This paper is a refinement and generalization of the second-named author’s master’s thesis [4], written under the supervision of the other two authors. It is a pleasure to thank Jeffrey Riedl for his careful reading of the thesis; Marcel Wild for encouragement; and the Department of Theoretical and Applied Mathematics at The University of Akron for financial support.

1. Cyclic Extensions

1.1. Motivation. Let \( G \) be a finite group. Consider a normal subgroup \( N \triangleleft G \), where \( G/N \) is cyclic of order \( n \). Choose any \( a \in G \setminus N \) such that the coset \( aN \) generates \( G/N \). Let \( v = a^n \in N \), and let \( \tau \in \text{Aut}(N) \) act via conjugation by \( a \). Thus,
\[
\tau(v) = aa^n a^{-1} = a^n = v.
\]
In other words, \( \tau \) fixes \( v \). Also, for \( x \in N \),
\[
\tau^n(x) = a^nxa^{-n} = vxv^{-1}.
\]
That is, \( \tau^n = \text{Int}(v) \). In particular, if \( N \) is an abelian group, then \( \tau^n \) is the identity automorphism.

Definition 1. An extension type for a group \( N \) is a quadruple \((N, n, \tau, v)\), where \( n \in \mathbb{N}, v \in N \), and \( \tau \in \text{Aut}(N) \) is such that \( \tau^n = \text{Int}(v) \).

Following [7], notice that this definition is stated without mention of a group \( G \). However, starting with a group \( G \), choices of normal subgroup \( N \) (having cyclic factor group of order \( n \)) and element \( a \in G \setminus N \) (such that \( aN \) generates \( G/N \)) will determine an extension type \((N, n, \tau, v)\) as above. Moreover, the extension type determines \( G \) up to isomorphism. To see this, note that since \( N \) and \( a \) generate \( G \), every element of \( G \) has the form \( xa^i \) for some \( x \in N \) and \( 0 \leq i < n \). Thus, in order to determine the operation table of \( G \), we only need to know how to multiply two such elements \( xa^i \) and \( ya^j \) to obtain a third element in the same form. Now note that
\[
(xa^i)(ya^j) = x(a^iya^{-i})a^i a^j = (x\tau^i(y))a^{i+j},
\]
which we will rewrite as \((x\tau^i(y)v)a^{i+j-n}\) if \( i + j \geq n \).

1.2. Using extension types to construct groups. We have just seen that each extension type determines at most one group up to isomorphism. The next result guarantees that each extension type does indeed determine a group.

Theorem 2 (Cyclic Extension Theorem). Each extension type \((N, n, \tau, v)\) determines a group.
Proof. Following [7], let $G$ be the set of ordered pairs $(x, a^i)$ for $x \in N$ and $i \in \{0, 1, ..., n-1\}$, and define a binary operation $*$ on $G$ by

$$(x, a^i) * (y, a^j) = \begin{cases} (xτ^i(y), a^{i+j}) & \text{if } i + j < n, \\ (xτ^i(y)v, a^{i+j-n}) & \text{if } i + j \geq n. \end{cases}$$

We will find it convenient to use the following equivalent definition:

$$(x, a^i) * (y, a^j) = (xτ^i(y)v^{\frac{i+j}{n}}, a^{i+j-n}v^{\frac{i+j}{n}}).$$

We must show that $*$ satisfies the three axioms of a group operation. If associativity is known, then it is easy enough to check that $(e, a^0)$ is the identity (where $e$ is the identity in $N$) and that $(τ^{-i}\left[(vx)^{-1}\right], a^{n-i})$ is the inverse of $(x, a^i)$. Therefore, it only remains to show that $*$ is associative. We will use the elementary fact that for all integers $m$ and $r$, $v^rτ^m-nr(z) = τ^m(z)v^r$. Consider

$$[(x, a^i) * (y, a^j)] * (z, a^k) = (xτ^i(y)v^{\frac{i+j}{n}}, a^{i+j-n}v^{\frac{i+j}{n}}) * (z, a^k)$$

$$= (xτ^i(y)v^{\frac{i+j}{n}}τ^{i+j-n}\left[(vz)^{-1}\right], a^{i+j-n}v^{\frac{i+j}{n}}+k-n)v^{\frac{i+j+n}{n}})$$

$$= (xτ^i(y)v^{\frac{i+j}{n}}v^{\frac{i+j+n}{n}}v^{\frac{i+j+n}{n}}, a^{i+j+n}v^{\frac{i+j+n}{n}})$$

$$= (xτ^i(y)v^{\frac{i+j+n}{n}}, a^{i+j+n}v^{\frac{i+j+n}{n}})$$

$$= (xτ^i(y)v^{\frac{i+j+n}{n}}, a^{i+j+n}v^{\frac{i+j+n}{n}}),$$

which is equal to $(x, a^i) * [(y, a^j) * (z, a^k)]$ by similar reasoning. \qed

We will often write $a$ for $(e, a)$ and $x$ for $(x, a^0)$.

1.3. Equivalence of extension types. Recall (from the introduction) that every group of order $p^4$ has a normal subgroup of order $p^3$. Thus, in order to construct all groups of order $p^4$, it would be sufficient to construct all extension types $(N, p, τ, v)$, where $N$ is a group of order $p^3$. However, the number of such extension types is huge. We present some techniques for identifying when two extension types determine isomorphic groups.

**Definition 3.** Two extension types are equivalent if they determine isomorphic groups.

Note that in [7], equivalence has the following meaning.

**Definition 4.** The extension types $(N, n, τ, v)$ and $(N', n, σ, ω)$ are conjugate if there is an isomorphism $ϕ : N → N'$ such that $σ = ϕ ◦ τ ◦ φ^{-1}$ and $ω = ϕ(v)$.

**Lemma 5.** Conjugate extension types are equivalent.

**Proof.** This is Lemma 1(a) of [7]. \qed

**Lemma 6.** Let $N$ be finite abelian, let $n ∈ N$, and let $i ∈ Z$ be prime to $|N|$. Then the extension types $(N, n, τ, v)$ and $(N, n, τ, v')$ are conjugate.
Proof. By hypothesis, the map \( \phi : N \to N \) defined by \( \phi(x) = x^i \) has trivial kernel, and is thus an automorphism. For all \( x \in N \),
\[
\phi(\tau(x)) = (\tau(x))^i = \tau(x^i) = \tau(\phi(x)).
\]
That is, \( \phi \tau = \tau \phi \), so \( \phi \tau \phi^{-1} = \tau \). Since \( \phi(v) = v^i \), the result follows. \( \square \)

**Notation 7.** Given \( \tau \in \text{Aut}(N) \) and \( n \in \mathbb{N} \), define a function \( \mathcal{N}_{\tau,n} : N \to N \) by
\[
\mathcal{N}_{\tau,n}(x) = x\tau(x)\tau^2(x) \cdots \tau^{n-1}(x).
\]
We will elide the subscripts \( \tau \) and \( n \) when they are understood from the context.

The usefulness of the function \( \mathcal{N}_{\tau,n} \) comes from the following lemma.

**Lemma 8.** Suppose \( N \triangleleft G \) and \( \tau \in \text{Aut}(N) \) acts via conjugation by \( a \in G \). Then for all \( x \in N \), \( (xa)^n = \mathcal{N}_{\tau,n}(x)a^n \).

**Proof.** We have
\[
(xa)^n = (xa)(xa^{-1}a^2)(xa^{-2}a^3) \cdots (xa)^{-(n-1)}a^n
= x(axa^{-1})(a^2axa^{-2}) \cdots (a^{n-1}axa^{-n+1})a^n
= x\tau(x)\tau^2(x) \cdots \tau^{n-1}(x)a^n
= \mathcal{N}_{\tau,n}(x)a^n. \square
\]

Several remaining results (Lemmata 9, 11, and 17, and Proposition 13) assert that one extension type is equivalent to another. Their proofs all follow the same outline. Given an extension type \((N, n, \tau, v)\), construct a group \( G \) as in the proof of Theorem 2. Choose a normal subgroup \( N' \) of \( G \) (often but not always equal to \( N \)), and an element \( a' \in G \setminus N' \) such that \( a'N' \) generates \( G/N' \). As in Theorem 11, we obtain an extension type \((N', n, \tau', v')\). Since this type is realized by \( G \), it must be equivalent to \((N, n, \tau, v)\).

**Lemma 9.** For \( x \in N \), the extension types \((N, n, \tau, v)\) and \((N, n, \text{Int}(x)\tau, \mathcal{N}_{\tau,n}(x)v)\) are equivalent.

**Proof.** Let \( G \) be a group that realizes \((N, n, \tau, v)\) and constructed as in the proof of Theorem 2. We will show that \( G \) also realizes \((N, n, \tau, \mathcal{N}(x)v)\). Let \( a' = xa \), and let \( \tau' \in \text{Aut}(N) \) act via conjugation by \( a' \). For \( y \in N \), consider
\[
\tau'(y) = a'y(a')^{-1} = (xa)y(a^{-1}x^{-1}) = x(aya^{-1})x^{-1} = x\tau(y)x^{-1} = (\text{Int}(x)\tau)(y),
\]
so \( \tau' = \text{Int}(x)\tau \). From Lemma 8 \( (a')^n = \mathcal{N}(x)v \). \( \square \)

**Corollary 10.** If \( N \) is abelian and \( x \in N \), then the extension types \((N, n, \tau, v)\) and \((N, n, \tau, \mathcal{N}_{\tau,n}(x)v)\) are equivalent.

**Lemma 11.** If \( i \in \mathbb{Z} \) is prime to \( n \), then the extension types \((N, n, \tau, v)\) and \((N, n, \tau^i, v^i)\) are equivalent.

**Proof.** Let \( G \) be a group that realizes \((N, n, \tau, v)\). This extension type is determined by choices of \( N \) and \( a \in G \setminus N \). One could just as easily choose \( a^i \in G \setminus N \) and the resulting extension type would be \((N, n, \tau^i, v^i)\). \( \square \)
2. Construction of all groups of order $p^4$

2.1. Dispensing with the abelian case. In order to construct the groups of order $p^4$, we could construct, up to equivalence, all extension types $(N, p, \tau, v)$, where $N$ is a group of order $p^3$. However, from the Fundamental Theorem of Finite Abelian Groups (which follows easily from Theorem 5.3 of [3]), up to isomorphism the abelian groups are given by the following list:

$$C_{p^4}, C_{p^3} \times C_p, C_{p^2} \times C_{p^2}, C_{p^2} \times C_p \times C_p, C_p \times C_p \times C_p \times C_p.$$  

Therefore, we may concentrate on the nonabelian case. This allows us to assume that the automorphism $\tau$ is nontrivial.

2.2. Subgroups $N$. A corollary of Sylow’s Theorem ensures that a group of order $p^4$ has a subgroup of order $p^3$. Moreover, all subgroups of order $p^3$ are normal. There are five groups of order $p^3$, three of which are abelian and two of which are nonabelian. When constructing extension types, $N$ must come from this list of five groups. It is desirable to cut this list down.

Proposition 12. Every group $G$ of order $p^4$ has an abelian subgroup of order at least $p^3$.

Proof. Let $Z$ denote the center of $G$. If $|Z| \geq p^3$, then we are done. Since $p$-groups have nontrivial centers, we may assume that $|Z| = p$ or $|Z| = p^2$.

We claim that $G$ has a normal subgroup $H$ of order $p^2$. If $|Z| = p^2$, then this is obvious, so suppose that $|Z| = p$. By the Lattice Isomorphism Theorem (Theorem 3.20 in [3]), it is enough to find a normal subgroup of $G/Z$ of order $p$. Since $G/Z$ is a $p$-group, its center has order at least $p$, and thus contains a normal (in $G/Z$) subgroup of order $p$, so the claim is proved.

Now define a homomorphism $\Phi : G \rightarrow \text{Aut}(H)$ by

$$[\Phi(g)](h) = ghg^{-1}.$$  

If $g, h \in H$, then $[\Phi(g)](h) = h$. This implies $H \subseteq \ker(\Phi)$.

We wish to show that this containment is strict. Suppose for a contradiction that $\ker(\Phi) = H$. Then $|\ker(\Phi)| = |H| = p^2$, which gives $|G/\ker(\Phi)| = p^2$. By the First Isomorphism Theorem (Theorem 3.16 in [3]), $\Phi$ corresponds to a one-to-one map from $G/\ker(\Phi)$ to $\text{Aut}(H)$. Therefore, $|G/\ker(\Phi)|$ must divide $|\text{Aut}(H)|$. However, since $H = \ker(\Phi)$ is isomorphic to either $C_{p^2}$ or $C_p \times C_p$, we have that $|\text{Aut}(H)| = p^2 - p$ or $(p^2 - 1)(p^2 - p)$, neither of which is divisible by $p^2$, and so we have a contradiction.

Thus, we may pick an element $g \in \ker(\Phi) \setminus H$. Since $g$ must commute with all elements of $H$, the group generated by $H$ and $g$ is an abelian subgroup of $G$ of order at least $p^3$.

Therefore, in constructing extension types, we may assume that $N$ is one of the three abelian groups of order $p^3$. However, the following result shows that we need not consider the case where $N$ is cyclic.

Proposition 13. If a nonabelian group $G$ of order $p^4$ contains a subgroup isomorphic to $C_{p^3}$, then $G$ also contains a subgroup isomorphic to $C_{p^2} \times C_p$.

Proof. Let $H = \langle h \rangle$ be a cyclic subgroup of $G$ of order $p^3$. Choose $a \in G \setminus H$, define $v = a^3$ and let $\tau \in \text{Aut}(H)$ act via conjugation by $a$. Then $G = \langle h, a \rangle$. It remains to show that $G$ contains a subgroup isomorphic to $C_{p^2} \times C_p$. Since $H$ is
cyclic and has order \( p^3 \), every automorphism of \( H \) will be of the form \( x \mapsto x^m \), where \( m \) and \( p^3 \) are relatively prime. Thus, \( \text{Aut}(H) \) is cyclic of order \( \phi(p^3) \), where \( \phi \) is the Euler function. Since \( p \) divides \( \phi(p^3) = p^2(p-1) \), \( \text{Aut}(H) \) has \( \phi(p) = p-1 \) elements of order \( p \). By Lemma 6 we only need to consider one of them. Since \( p^2 + 1 \not\equiv 1 \mod p^3 \) but 
\[(p^2 + 1)^p = p^{2p} + \cdots + \binom{p}{1}p^2 + 1 \equiv 1 \mod p^3,
\]
we have that \( x \mapsto x^{p^2+1} \) is an automorphism of order \( p \). So assume without loss of generality that \( \tau(x) = x^{p^2+1} \). Let \( H' \) be the subgroup of \( H \) generated by \( h^p \). This is a cyclic subgroup of order \( p^2 \), and it commutes with \( a \) since \( \tau \) fixes \( h^p \). To see this, first notice that
\[\tau(h^p) = h^{(p^2+1)p} = h^p.\]
Also, \( \tau(h^p) = ah^pa^{-1} \), which gives that \( ah^p = h^pa \). Thus, it suffices to show the existence of an element \( x \in G \) of order \( p \) such that \( x \notin H' \) and \( xh^p = h^px \), since then \( (h^p, x) \cong C_{p^2} \times C_p \). Let \( a' = ah^r \), where \( r \) is to be determined. Clearly, \( ah^r \in G \setminus H \). So, for \( n \in H \), consider
\[a'n(a')^{-1} = (ah^r)n(h^{-r}a^{-1}) = a(h^rnh^{-r})a^{-1} = a(nh^r)h^{-r})a^{-1} = ana^{-1} = \tau(n).\]
Thus, \( a' \) commutes with \( H' \), just as \( a \) does. Lastly, it suffices to show that we can choose \( r \) such that \( a' \) has order \( p \). From Lemma 8
\[(a')^p = N(h^r)v.\]
Thus, we must show that \( N(h^r) = v^{-1} \) for an appropriate choice of \( r \). Consider
\[N(h^r) = \prod_{i=0}^{p-1} \tau^i(h^r) = h^r \sum_i (p^2+1)^i.\]
Reducing the exponent modulo \( p^2 \), we obtain
\[r \sum_{i=0}^{p-1} (p^2 + 1)^i = r \frac{(p^2 + 1)^p - 1}{(p^2 + 1) - 1} \equiv rp \mod p^3.\]
That is, \( N(h^r) = h^{rp} \). Thus, we must show that \( v = h^{-rp} \) for some \( r \). Equivalently, \( v \in H' \). However, \( v \) is fixed by \( \tau \), and \( H' \) is the set of all fixed points of \( \tau \). \( \square \)

Together, Propositions 12 and 13 produce a powerful result: Every nonabelian group of order \( p^4 \) contains a subgroup isomorphic to either \( C_{p^2} \times C_p \) or \( C_p \times C_p \times C_p \). In particular, it is sufficient to consider only these two choices of \( N \) when constructing extension types. Conveniently, much is known about the automorphism groups of both of these groups.
2.3. Automorphisms $\tau$ of $N$. For $N = C_{p^2} \times C_p$ and $N = C_p \times C_p \times C_p$, we must find enough automorphisms $\tau$ of $N$ to construct, up to equivalence, all extension types of the form $(N, p, \tau, v)$. The following lemma will be useful.

Lemma 14. Let $m$ be a positive integer. Every element of $\text{GL}_m(F_p)$ of order $p$ is conjugate over $F_p$ to a matrix in Jordan canonical form with ones along the diagonal.

Proof. Such an element $A$ is a root of the $F_p$-polynomial $X^p - 1$, which equals $(X - 1)^p$, and thus splits over $F_p$. Now apply Theorem 12.23 in [3]. □

Note that one could use Sylow theory to produce a more elementary proof in the cases where $m = 2$ or 3, which are the only ones we will need.

Exercise. Do it.

Now we begin our study of the automorphisms of order $p$ of $N = C_{p^2} \times C_p$. Let $x$ be a generator of $C_{p^2}$ and $y$ be a generator of $C_p$. Then every automorphism of $N$ has the form

$$
\begin{align*}
x &\mapsto x^a y^b \\
y &\mapsto x^c y^d
\end{align*}
$$

for $a$ and $c$ integers modulo $p^2$, and $b$ and $d$ integers modulo $p$. This automorphism can conveniently be represented as the matrix $(a \ c \ b \ d)$. Note that composition of automorphisms is compatible with matrix multiplication. By Lemma 5, we only need to consider automorphisms up to conjugacy in $\text{Aut}(C_{p^2} \times C_p)$. Consider the homomorphism from $\text{Aut}(C_{p^2} \times C_p)$ into $\text{GL}_2(F_p)$ that maps the matrix representation of an automorphism in $\text{Aut}(C_{p^2} \times C_p)$ to a matrix in $\text{GL}_2(F_p)$ by reducing the top row modulo $p$. By Lemma 14 the image in $\text{GL}_2(F_p)$ of an automorphism of order $p$ in $\text{Aut}(C_{p^2} \times C_p)$ is conjugate to either $(1 \ 0 \ 0 \ 1)$ or $(1 \ 0 \ 1 \ 1)$. Therefore, we may assume our matrix has the form $(1 + ps \ 0 \ 0 \ 1)$ or $(1 + sp \ 1 \ 1)$, where $r, s \in \{0, \ldots, p - 1\}$. Moreover, since $\tau$ is not the identity automorphism, we may assume in a matrix of the former type that $r$ and $s$ are not both zero.

Lemma 15. If $N = C_{p^2} \times C_p$, then we only need to consider the automorphisms of $N$ represented by the following matrices:

$$
\begin{align*}
(1 \ p \ 0 \ 1), (1 + p \ 0 \ 1), (1 \ 0 \ 1 \ 1), (1 \ p \ 1 \ 1), (1 \ v p \ 1 \ 1).
\end{align*}
$$

Proof. Recall that in our matrix computations, the first row of each matrix is taken modulo $p^2$ and the second is taken modulo $p$. We will use the following straightforward calculations:

(0-conj) \quad \left( \begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right) \left( \begin{array}{cc} \alpha & \beta \\ 0 & 1 \end{array} \right) \left( \begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right)^{-1} = \left( \begin{array}{cc} \alpha - \beta & \beta \\ 0 & 1 \end{array} \right)

(0-pow) \quad \left( 1 + p \ 0 \ 1 \right)^s = \left( 1 + sp \ 0 \ 1 \right)

(1-conj) \quad \left( \begin{array}{cc} 1 & -p \\ 0 & 1 \end{array} \right) \left( \begin{array}{cc} \alpha & \beta \\ 1 & 1 \end{array} \right) \left( \begin{array}{cc} 1 & -p \\ 0 & 1 \end{array} \right)^{-1} = \left( \begin{array}{cc} \alpha - p & \beta \\ 1 & 1 \end{array} \right)

(1-pow) \quad \left( \begin{array}{cc} 1 & rp \\ 0 & 1 \end{array} \right)^q = \left( \begin{array}{cc} 1 + \left( \frac{q}{2} \right) rp & \frac{q rp}{1} \end{array} \right).
First, consider a matrix of the form \( \begin{pmatrix} 1 + sp & rp \\ 0 & 1 \end{pmatrix} \) for \( r, s \in \{0, \ldots, p - 1\} \). If \( r \neq 0 \), then we may pick \( 0 < t < p \) so that \( rt \equiv 1 \mod p \). Apply \((0\text{-}\text{con})\) \( ts \) times to see that our matrix is conjugate to \( \begin{pmatrix} 1 & rp \\ 0 & 1 \end{pmatrix} \), which equals \( \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}^r \). By Lemmata \([5]\) and \([11]\) we can replace our original matrix by \( \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \). On the other hand, if \( r = 0 \), then \( s \neq 0 \), and so by \((0\text{-}\text{pow})\) and Lemma \([11]\) we may replace our matrix by \( \begin{pmatrix} 1+sp & 0 \\ 0 & 1 \end{pmatrix} \).

Now consider a matrix of the form \( \begin{pmatrix} 1 + sp & rp \\ 0 & 1 \end{pmatrix} \). Applying \((1\text{-}\text{con})\) \( s \) times, we see that our matrix is conjugate to \( \begin{pmatrix} 1 & rp \\ 0 & 1 \end{pmatrix} \). From \((1\text{-}\text{pow})\), we see that for all \( 0 < q < p \), the \( q \)th power of this latter matrix is \( \begin{pmatrix} 1 & (q + sp)rp \\ 0 & 1 \end{pmatrix} \). Applying \((1\text{-}\text{con})\) \( (qrp) \) \( r \) times, we see that this third matrix is conjugate to \( \begin{pmatrix} 1 & qrp \\ 0 & 1 \end{pmatrix} \). Now note that

\[
\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & qrp \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & q^2rp \\ 0 & 1 \end{pmatrix}.
\]

By Lemmata \([5]\) and \([11]\) we may thus replace our original matrix by \( \begin{pmatrix} 1 & r'p \\ 0 & 1 \end{pmatrix} \), where \( r' \) is any number that is in the same class as \( r \) modulo squares \( \mod p \). Thus, we may assume that \( r' \) is 0, 1, or \( \varepsilon \).

Next, assume \( N = C_p \times C_p \times C_p \). We will view \( N \) as a three-dimensional vector space over \( F_p \). By Proposition 4.17(3) in \([3]\), \( \text{Aut}(N) \cong \text{GL}_3(F_p) \).

**Lemma 16.** If \( N = C_p \times C_p \times C_p \), then every automorphism of \( N \) of order \( p \) is conjugate to one of the following:

\[
\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.
\]

**Proof.** This follows from Lemma \([14]\) \( \square \)

### 2.4. Choices for \( v \)

For each of the seven choices of \( \tau \) that we have identified in Lemmata \([15]\) and \([16]\) we wish to identify a set of choices for \( v \) so that all pairs \( (\tau, v) \) taken together will be sufficient to construct all nonabelian groups of order \( p^3 \).

Recall that \( v \) must belong to the set \( N^\tau \) of fixed points of \( \tau \) in \( N \). For each \( \tau \), finding \( N^\tau \) is a straightforward matrix calculation, equivalent to finding \( \ker(\tau - I) \), where \( I \) is the identity map on \( N \). From Corollary \([16]\) two choices of \( v \in N^\tau \) give equivalent extension types if they differ by an element of the image of \( N_{\tau, p} \). Since \( N_{\tau, p} \) has the matrix representation \( I + \tau + \cdots + \tau^{p-1} \), it is a straightforward matrix computation to find its image. Note that since \( N \) is abelian, \( N^\tau \) and \( \text{im}(N_{\tau, p}) \) are groups, and we are thus interested in choosing \( v \) from a set of coset representatives of \( N^\tau / \text{im}(N_{\tau, p}) \). From Lemma \([6]\) two such representatives give equivalent extension types if there is a power of the other (of order prime to \( p \)); or, equivalently, if they generate the same subgroup of \( N^\tau \).

For all but one of our choices for \( \tau \), this reasoning alone is enough to show that we only need to consider one or two choices for \( v \). The results are presented in Table \([2]\) \( 1 \). The remaining case is the one where \( N = C_p \times C_p \times C_p \) and \( \tau = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \), presented in the table on the line marked \((\xi)\). In this case the table reflects our claim that it is sufficient to take \( v \) to be trivial.

To prove this claim, we will show that for any nontrivial \( v \), a group \( G \) with extension type \((N, p, \tau, v)\) must contain a group isomorphic to \( C_{p^2} \times C_{p^2} \), and thus has already been constructed. It is enough to find commuting elements \( x, y \in G \) such that \( x \) has order \( p^2 \), \( y \) has order \( p \), and \( y \notin \langle x \rangle \).
Let \( a \in G \) be an element such that \( \tau \) acts via conjugation by \( a \). Since \( v \) has order \( p \), \( a \) has order \( p^2 \). The set \( N^\tau \) of fixed points of \( \tau \) can be viewed as a 2-dimensional subspace of the \( \mathbb{F}_p \)-vector space \( N \). Meanwhile, \( \langle v \rangle \) is a 1-dimensional subspace of \( N^\tau \), so \( N^\tau \setminus \langle v \rangle \) is nonempty. Pick \( x = a \) and \( y \in N^\tau \setminus \langle v \rangle \). This proves the claim, and finishes the justification of Table 1.

3. Classification

From now on, in writing an extension type \( (N, p, \tau, v) \) we will feel free to omit \( p \), since it is the same for all types we are considering. We will also omit \( N \), since we can infer it from \( \tau \). That is, \( N \) is either \( C_{p^2} \times C_p \) or \( C_p \times C_p \times C_p \) according as \( \tau \) is a 2-by-2 or 3-by-3 matrix. Thus, we will refer to a pair \( (\tau, v) \) as an extension type.

**Main Theorem.** Every nonabelian group of order \( p^4 \) realizes precisely one of the extension types \( (\tau, v) \) given in Table 2.

It is understood that if \( p = 3 \), then we ignore the row in Table 2 containing “N/A” in the “\( p = 3 \)” column, and similarly if \( p > 3 \). Thus, either way we only consider 10 rows of the table, and the theorem is asserting that there are exactly 10 nonabelian groups of order \( p^4 \).

**Proof.** Considering all choices for \( v \) that appear in Table 1 we obtain eleven pairs \( (\tau, v) \), which are sufficient for constructing all nonabelian groups of order \( p^4 \). All of these pairs appear in Table 2 except for \( ((1, 0), (0, 1)) \). However, in Lemma 17 we will see that this is equivalent to \( ((1+p, 0), (0, 1)) \). Thus, it only remains to show that the listed extension types are all pairwise inequivalent.
For each of the groups arising from the pairs \((\tau, v)\) in Table 2, we compute the isomorphism class of the center, and we count the elements of order up to \(p\). This alone will distinguish most of these groups from each other.

Suppose \(G\) realizes an extension type \((\tau, v)\) from Table 2. Then the center of \(G\) is precisely the group \(N_\tau\) of fixed points of \(\tau\), whose isomorphism class can be obtained from Table 1.

Counting the elements of \(G\) of order up to \(p\) is also straightforward. First, note that \(G\) is the union of the \(p\) cosets \(N, Na, \ldots, Na^{p-1}\). The number of elements of order up to \(p\) in \(N\) is easy to compute. If \(N = C_{p^2} \times C_p\), then there are \(p^2\) such elements. If \(N = C_p \times C_p \times C_p\), then there are \(p^3\) such elements. Moreover, for \(0 < i < p\), the map \(y \mapsto y^i\) induces a bijection between the cosets \(Na\) and \(Na^i\) that remains a bijection when restricted to elements of order \(p\). Thus, it’s enough to count the elements of order \(p\) in the coset \(Na\). For \(x \in N\), by Lemma 8 we know that \((xa)^p = N(x)v\). If \(v \notin \text{im}(N)\), then this cannot be the identity, and so \(Na\) has no elements of order \(p\). If \(v \in \text{im}(N)\), then the elements of order \(p\) in \(Na\) are in bijection with \(\ker(N)\). Thus, the number of elements of order up to \(p\) in \(G\) is

\[
\text{(the number of elements of order } \leq p \text{ in } N) + (p - 1) \begin{cases} 
|\ker(N)| & \text{if } v \in \text{im}(N), \\
0 & \text{otherwise.}\end{cases}
\]

Note that \(|\ker(N)| = p^3/|\text{im}(N)|\). Since \(\text{im}(N)\) is given in Table 1, we can now count the elements of \(G\) of order up to \(p\). The results are presented in Table 2.

---

**Table 2.** Extension types for all nonabelian groups of order \(p^4\)

| \(\tau\) | \(v\) | center | \(p = 3\) | \(p > 3\) |
|---|---|---|---|---|
| \(\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}\) | \(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\) | \(C_{p^2}\) | \(p^3\) | |
| \(\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}\) | \(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\) | \(C_{p^2}\) | \(p^2\) | |
| \(\begin{pmatrix} 1 + p & 0 \\ 0 & 1 \end{pmatrix}\) | \(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\) | \(C_p \times C_p\) | \(p^3\) | |
| \(\begin{pmatrix} 1 + p & 0 \\ 0 & 1 \end{pmatrix}\) | \(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\) | \(C_p \times C_p\) | \(p^2\) | |
| \(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\) | \(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\) | \(C_p \times C_p\) | \(p^3\) | |
| \(\begin{pmatrix} 1 & p \\ 1 & 1 \end{pmatrix}\) | \(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\) | \(C_p\) | \(p^3\) | |
| \(\begin{pmatrix} 1 & \varepsilon_p \\ 1 & 1 \end{pmatrix}\) | \(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\) | \(C_p\) | \(p^4 - p^3 + p^2\) | \(p^3\) |
| \(\begin{pmatrix} 1 & \varepsilon_p \\ 1 & 1 \end{pmatrix}\) | \(\begin{pmatrix} p \\ 0 \end{pmatrix}\) | \(C_p\) | \(p^2\) | \(\text{N/A}\) |
| \(\begin{pmatrix} 1 & 1 \varepsilon_p \\ 0 & 0 \end{pmatrix}\) | \(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\) | \(C_p \times C_p\) | \(p^4\) | |
| \(\begin{pmatrix} 1 & 1 \varepsilon_p \\ 0 & 0 \end{pmatrix}\) | \(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\) | \(C_p \times C_p\) | \(2p^3 - p^2\) | \(p^4\) |
| \(\begin{pmatrix} 1 & 1 \varepsilon_p \\ 0 & 0 \end{pmatrix}\) | \(\begin{pmatrix} 0 \varepsilon_p \\ 0 \end{pmatrix}\) | \(C_p\) | \(\text{N/A}\) | \(p^3\) |
Inspecting Table \[2\] we see that the only possible equivalences are between the two rows labeled \((\ast\ast)\); and \((p > 3)\) among the three rows labeled \((\ast\ast\ast)\). In Lemma \[18\] we will see that the former equivalence fails.

Consider the three rows labeled \((\ast\ast\ast)\). Each determines a group that has precisely \(p^3\) elements of order up to \(p\). In the third group, these must therefore be the elements of \(N\), all of which commute with each other. However, in the first two groups, it is easy to find examples of elements of order \(p^3\) that do not commute. Therefore, the third group is distinct from the other two. In Lemma \[19\] we will see that the first two groups are also distinct.

Thus, once we have proved Lemmata \[17\] \[18\] and \[19\] the theorem will be established.

We now take care of unfinished business from the proof. From now on, let \(N = C_{p^2} \times C_p\).

**Lemma 17.** The extension types \(((\frac{1+p}{0}, \frac{0}{1}), (\frac{1}{1}, \frac{0}{0}))\) and \(((\frac{1}{1}, \frac{0}{0}))\) are equivalent.

*Proof.* Assume that \(G\) realizes the extension type \((N, p, (\frac{1+p}{0}, \frac{0}{1}), (\frac{1}{1}, \frac{0}{0}))\) and is constructed as in the proof of Theorem \[2\]. Let \(x\) and \(y\) denote generators of \(C_{p^2}\) and \(C_p\) (respectively) in \(N\). To construct a subgroup \(N'\) that is isomorphic to \(N\), let \(x' = a^{p-1}, y' = x^p\), and \(N' = \langle x', y' \rangle\). Define \(a' = x\) so that \((a')^p = v' = y'\). Let \(\tau' \in \text{Aut}(N')\) be the automorphism that acts via conjugation by \(a'\). Consider

\[
\tau'(x') = a'x'(a')^{-1} = xa^{p-1}x^{-1} = x\tau^{p-1}(x^{-1})a^{p-1} = x(x^{-1})^{1+p/(p-1)}a^{p-1} = x(x^{-1})^{(1+p)}a^{p-1} = y'x' = y',
\]

and

\[
\tau'(y') = a'x'(a')^{-1} = xx^{p}x^{-1} = x^p = y'.
\]

With respect to the generators \(x'\) and \(y'\), \(\tau'\) thus has matrix representation \((\frac{1}{1})\), and \(v'\) has vector representation \((\frac{0}{0})\). Therefore, \(G\) realizes the extension type \(\langle N', p, (\frac{1}{1}, \frac{0}{0}) \rangle\). \hfill \(\blacksquare\)

**Lemma 18.** The extension types \(((\frac{1+p}{0}, \frac{0}{1}), (\frac{1}{1}, \frac{0}{0}))\) and \(((\frac{1}{1}, \frac{0}{0}))\) are inequivalent.

*Proof.* Let \(G_1\) and \(G_2\), respectively, realize the given extension types. For \(i = 1, 2\), define \(H_i = \langle g^p : g \in G_i \rangle\). Using Lemma \[8\] one can compute that \(H_1 = H_2 = \langle (\frac{0}{0}) \rangle\). It follows that each \(H_i\) is a subgroup of the center of \(G_i\), and is thus a normal subgroup of \(G_i\). We will be done if we can show that \(G_1/H_1\) is abelian and \(G_2/H_2\) is not. To do so, we will consider the image of each automorphism \(\tau\) in \(\text{Aut}(N/H_i) \cong \text{Aut}(C_p \times C_p) = \text{GL}_2(F_p)\), obtained by reducing modulo \(p\) the first row of the matrix for \(\tau\). Since the image of \(\tau = \left(\frac{1+p}{0}, \frac{0}{1}\right)\) in \(\text{GL}_2(F_p)\) is the identity, \(\tau\) acts trivially on \(N/H_1\). Hence, \(G_1/H_1\) is abelian. However, \(G_2/H_2\) is nonabelian since the image of \((\frac{1}{1}, \frac{0}{0})\) in \(\text{GL}_2(F_p)\) is not the identity. \hfill \(\blacksquare\)

If \(p = 3\), then we are done. Otherwise, we still need the following result.

**Lemma 19.** The extension types \(((\frac{1+p}{0}, \frac{0}{1}), (\frac{1}{1}, \frac{0}{0}))\) are inequivalent.

*Proof.* Let \(G\) be a group determined by the first extension type. As in the proof of Lemma \[17\] we have generators \(x, y\), and \(a\) for \(G\), where \(x\) and \(y\) generate \(N\), and the conjugation action \(\tau\) of \(a\) on \(N\) is represented by the matrix \((\frac{1}{1}, \frac{p}{0})\) with respect to our given generators for \(N\). In order for \(G\) to also realize the second extension type, we must have generators \(x', y', a'\) that satisfy the same relations as \(x, y, a\).
and $a$, except that the conjugation action $\tau'$ of $a'$ on $N' := \langle x', y' \rangle$ should now be represented by the matrix $\begin{pmatrix} 1 & \tau' \\ \tau' & 1 \end{pmatrix}$ with respect to our given generators for $N'$.

For a contradiction, suppose that there exist such $x'$, $y'$, and $a'$.

Let $Z$ and $H$ denote the center and commutator subgroup, respectively, of $G$. It is straightforward to compute that $Z = \langle \left( \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right) \rangle$, and $H = \langle \left( \begin{smallmatrix} p \\ 0 \\ 0 \end{smallmatrix} \right), \left( \begin{smallmatrix} 0 \\ 1 \\ 1 \end{smallmatrix} \right) \rangle$. Since $y$ is an element of order $p$ that lies in $H$ but not in $Z$, the same must be true for $y'$. Since $x$ commutes with $y$, $x'$ must commute with $y'$. It is straightforward to compute that for $n \in N$ and $k \not\equiv 0 \mod p$, $(na^k)y'(na^k)^{-1} \neq y'$ for $y' \in H \setminus Z$. Therefore, $x' \in N$, and so $N' = N$.

For any $n \in N$, $na'$ and $a'$ induce the same conjugation action on $N$. Therefore, we may assume that $a' = a^k$ for some $0 < k < p$.

For any homomorphism $\varphi : N \rightarrow N$, consider the homomorphism $\varphi - I$ that takes an element $n$ to $\varphi(n)n^{-1}$. To obtain the matrix representation of $\varphi - I$ with respect to some set of generators, take the matrix representation of $\varphi$ and subtract the identity matrix. For example, with respect to the generators $x$ and $y$, we see from (1-pow) that $(\tau^k - I)$ is represented by the matrix $\begin{pmatrix} (k^2p) & k \\ 0 & 0 \end{pmatrix}$. Thus, the composition $(\tau^k - I)^2$ of this map with itself is represented by the matrix $\begin{pmatrix} (k^2p) & 0 \\ 0 & 0 \end{pmatrix}$. Similarly, with respect to the generators $x'$ and $y'$, $(\tau' - I)$ is represented by the matrix $\begin{pmatrix} 0 & \tau' \\ \tau' & 0 \end{pmatrix}$.

Since $x'$ has order $p^2$, we must have $x' = x^cy^d$ for some $c$ and $d$, with $c \not\equiv 0 \mod p$. Note that $(x')^p = (x^p)^c$.

For any two group elements $g$ and $h$, let $[g, h]$ denote $ghg^{-1}h^{-1}$. For example, if $n \in N$, then $[a, n] = \tau(n)n^{-1} = (\tau - I)(n)$.

We now compute $[a', [a', x']]$ in two ways. First,$$[a', [a', x']] = (\tau' - I)^2(x') = x^{cp} = x^{c^p}.$$Second,$$[a', [a', x']] = [a'^k, [a^k, x']] = (\tau^k - I)^2(x^cy^d) = x^{k^2cp}.$$But the results of these two computations cannot be equal, since $k^2 \not\equiv c \mod p$, the latter being a nonsquare. □

From the information we have accumulated, it is possible to determine which nonabelian groups of order $p^4$ can be decomposed into semidirect products of smaller groups, and which cannot.

**Exercise.** Do it.

### 4. Comments on the $p = 2$ case

The Main Theorem is only valid for $p$ odd. Of course, one can find the classification of groups of order $2^4$ in [7]. However, if the reader wants to adapt the machinery we have used, here is what is required.

The first of our results that depends on $p$ being odd is Proposition 13 which says that it is enough to consider cyclic extensions of just two abelian groups of order $p^3$. When $p = 2$, then one can prove (or find in [7]) an analogous result, but the two groups in question are now $C_{p^3}$ and $C_{p^2} \times C_p$. Our analysis of the nonabelian cyclic extensions of $C_p \times C_p \times C_p$ is thus unnecessary when $p = 2$. Instead, one needs to study the nonabelian extensions of $C_{p^3}$, imitating the arguments of Proposition 13.
The method of analysis of the extensions of $C_{p^2} \times C_p$ remains valid. However, some of the calculations that go into Table 1 yield different answers, and Lemma 15 needs to take into account the fact that $F_2$ contains no nonsquare element, so there are no analogues of the extension types involving $\varepsilon$.

In light of the above comments, it is interesting to classify the groups of order 16 using as little effort as possible.

Exercise. Do it.

References

1. Hans Ulrich Besche, Bettina Eick, and Eamonn A. O'Brien, A millennium project: constructing small groups, Internat. J. Algebra Comput. 12 (2002), no. 5, 623–644. MR MR1935567 (2003h:20042)
2. William Burnside, Theory of groups of finite order, 2nd ed., Dover Publications Inc., New York, 1955. MR MR0069818 (16,1086c)
3. David S. Dummit and Richard M. Foote, Abstract algebra, 3rd ed., Wiley, New York, 2004.
4. Michael Garlow, An elementary classification of the groups of order 81, Master’s thesis, The University of Akron, 2006.
5. Otto Hölder, Die Gruppen der Ordnungen $p^3$, $pq^2$, $pqr$, $p^4$, Math. Ann. 43 (1893), no. 2-3, 301–412. MR MR1510814
6. Eamonn A. O’Brien and Michael R. Vaughan-Lee, The groups with order $p^7$ for odd prime $p$, J. Algebra 292 (2005), no. 1, 243–258. MR MR2166803 (2006d:20038)
7. Marcel Wild, The groups of order sixteen made easy, Amer. Math. Monthly 112 (2005), no. 1, 20–31. MR MR2110109
8. J. W. A. Young, On the determination of groups whose order is a power of a prime, Amer. J. Math. 15 (1893), no. 2, 124–178.