The Classification of Finite Groups of Order 16

Kyle Whitcomb Department of Mathematics University of Puget Sound

May 3, 2015

© 2015 Kyle Whitcomb. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license can be found at https://www.gnu.org/copyleft/fdl.html.

1 Introduction

The classification of the finite groups of order 16 is more difficult than it first appears. The legwork comes not from finding the groups, but from proving that there are no more.

This proof primarily follows the example of Marcel Wild's proof via cyclic extensions in [4], in which we limit the number of possible groups by examining the restrictions on the possible extension types realized by these groups, then match groups to these extension types to create a full list of the finite groups of order 16.

2 Definitions and Notation

This paper assumes a certain level of familiarity with Abstract Algebra, particularly as it is introduced in Thomas Judson's *Abstract Algebra: Theory and Applications* ([3]). Some concepts are restated here with brief definitions and, if applicable, the notation used. See [3] or any other introductory textbook on group theory for more information.

- A group G is abelian if xy = yx for all $x, y \in G$.
- If H is a subgroup of G, then $H \subseteq G$. If H is a proper subgroup of G, that is $H \subseteq G, \ H \neq G$ then $H \subset G$.
- Normal subgroups will play an important role in this paper, and the notation $H \triangleleft G$ will be used to denote that H is a normal subgroup of G.
- A group G generated by elements $\{x_1, x_2, \ldots, x_k\}$ will be written as $G = \langle x_1, x_2, \ldots, x_k \rangle$, and a group generated by a single element is a cyclic group.

- The order of a group G, or more generally the size of a set G, is |G|, and for some $x \in G$, |x| is understood to be the order of the cyclic group generated by x, or $|x| = |\langle x \rangle|$.
- The centralizer of an element $x \in G$ is $C(x) = \{g \in G \mid gx = xg\}$.
- The *center* of a group G is defined to be $Z(G) \equiv \{g \in G \mid gx = xg \text{ for all } y \in G\}$. The center is a normal subgroup, and it is abelian.
- An *automorphism* of a group G is an isomorphism $\phi : G \to G$.
- An inner automorphism t_a of G is $t_a: G \to G, t_a(x) = axa^{-1}$.
- The automorphism group of G, Aut(G), is the group of all automorphisms of G.
- Two elements $g_1, g_2 \in G$ are *conjugate* if there exists $a \in G$ such that $t_a(g_1) = g_2$. The set of all elements that are conjugate to g is [g], the *conjugacy class* of g.
- If N is a normal subgroup of G and H is a subgroup of G such that $NH = \{nh \mid n \in N, h \in H\}$ and $N \cap H = \{e_G\}$, then G is the *inner semidirect product* of N and H, or $G = N \rtimes H$.
- As with direct products, if G is the inne semidirect product of N and H, then G is isomorphic to an outer semidirect product of N and H. To do construct an outer semidirect product, you must specify an automorphism $\phi : H \to \operatorname{Aut}(N), \phi(h) = \phi_h$ for $h \in H$, and $\phi_h(n) = hnh^{-1}$ for $n \in N$. Then $G \cong N \rtimes_{\phi} H$ is the semidirect product of N and H with respect to ϕ . The operation in this group is $* : (N \times H) \times (N \times H) \to$ $N \rtimes_{\phi} H$, where $(n_1, h_1) * (n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2)$.

In addition to these two additional definitions are of critical importance to the classification of all groups of order 16, neither of which appear in [3]. These concepts are used in Marcel Wild's classification of groups of order 16 [4].

2.1 Cyclic Extensions and Extension Types

Definition 2.1 (Cyclic Extension). Let $N \triangleleft G$. If $G/N \cong \mathbb{Z}_n$, then G is a cyclic extension of N.

To motivate the next definition, we will examine some properties of cyclic extensions. Suppose G is a cyclic extension of N such that $G/N \cong \mathbb{Z}_n$. Consider $a \in G$ such that |Na| = n in G/N, then $v = a^n \in N$. Consider $\tau \in \operatorname{Aut}(N)$ such that τ is the restriction to N of the inner automorphism t_a of G. Then

$$\tau(v) = ava^{-1} = aa^na^{-1} = a^{1+n-1} = a^n = v.$$

Now further consider

$$\tau^{n}(x) = aa \cdots a(x)a^{-1} \cdots a^{-1}a^{-1} = a^{n}xa^{-n} = vxv^{-1} = t_{v}(x).$$

This is true for all $x \in N$, therefore $\tau^n = t_v$.

In order to move away from relying on an element $a \in G$ to discuss these cyclic extensions, we will define the extension *type*.

Definition 2.2. For a group N, a quadruple (N, n, τ, v) is an extension type if $v \in N$, $\tau \in Aut(N)$, $\tau(v) = v$, and $\tau^n = t_v$.

Not only does this definition eliminate the dependence on the element $a \in G$, it also eliminates the requirement of the group G. However, one can always work the other direction and from a group G with a normal subgroup N write down an extension type which G realizes. That is, if G is a cyclic extension of N, then there exists $v \in N$ and $\tau \in Aut(N)$ such that (N, n, τ, v) is an extension type. A group G with normal subgroup N may realize more than one extension type (which will differ in the last two entries of the quadruple). This leads us to the first major theorem of this paper.

3 Preliminary Theorems and Calculations

The following are a series of theorems that will aid in the classification of all groups of order 16. We will first explore the properties of extension types, then the implications of those properties for groups which realize extension types, and then finally move into concrete calculations of the properties of groups of order 16.

Theorem 3.1. Two extension types, (N, n, τ, v) and (N', n, σ, w) are *equivalent* if there exists an isomorphism $\varphi : N \to N'$ such that $\sigma = \varphi \tau \varphi^{-1}$ and $w = \varphi(v)$.

Proof. Reflexivity is obvious if you consider $\varphi = id$.

Similarly, this equivalence relation is clearly symmetric since φ is an isomorphism, so if $(N, n, \tau, v) \sim (N', n, \sigma, w)$ by φ , then $(N', n, \sigma, w) \sim (N, n, \tau, v)$ by φ^{-1} .

Finally, if $(N, n, \tau, v) \sim (N', n, \sigma, w)$ by φ_1 and $(N', n, \sigma, w) \sim (N'', n, \rho, u)$ by φ_2 , then $\varphi_2 \varphi_1 : N \to N''$ and

$$(\varphi_2\varphi_1)\tau(\varphi_2\varphi_1)^{-1} = (\varphi_2\varphi_1)\tau(\varphi_1^{-1}\varphi_2^{-1})$$
$$= \varphi_2(\varphi_1\tau\varphi_1^{-1})\varphi_2^{-1}$$
$$= \varphi_2\sigma\varphi_2^{-1}$$
$$= \rho.$$

Finally, $(\varphi_2\varphi_1)(v) = \varphi_2(\varphi_1(v)) = \varphi_2(w) = u$. So $(N, n, \tau, v) \sim (N'', n, \rho, u)$.

Now that we understand how to discuss equivalent extension types, we need to know the implications for groups that realize equivalent extension types. The following theorem should not be too surprising.

Theorem 3.2. G realizes (N, n, τ, v) and H realizes (M, n, σ, w) . If $(N, n, \tau, v) \sim (M, n, \sigma, w)$, then $G \cong H$.

Proof. $(N, n, \tau, v) \sim (M, n, \sigma, w)$. Therefore there exists $\varphi : N \to M$ such that $\sigma = \varphi \tau \varphi^{-1}$ and $w = \varphi(v)$. Furthermore, from Definition 2.1, G realizes (N, n, τ, v) so there exists $a \in G/N$ such that $a^n = v$. Similarly, there exists $b \in H/M$ such that $b^n = w$. Define $\Phi: G \to H$, such that for $x, y \in G$,

$$\Phi\left((xa^{i})(ya^{j})\right) = \Phi\left(x(a^{i}ya^{-i})a^{i+j}\right) = \Phi\left(x\tau^{i}(y)va^{i+j-n}\right)$$
$$= \varphi\left(x\tau^{i}(y)v)b^{i+j-n}\right) = \varphi(x)\varphi\left(\tau^{i}(y)\right)\phi(v)b^{i+j-n}$$
$$= \varphi(x)\sigma^{i}\left(\varphi(y)\right)wb^{i+j-n} = \varphi(x)\left(b^{i}\phi(y)b^{-i}\right)b^{i+j}$$
$$= \varphi(x)b^{i}\varphi(y)b^{j} = \Phi(xa^{i})\Phi(ya^{j}).$$

Now that we understand extension types, let us examine groups of order 16. A group G that realizes a normal extension (N, n, τ, v) must contain N as a normal subgroup, so we will examine some possible normal subgroups of groups of order 16 in order to push this discussion towards the final theorem classifying all groups of order 16. We will find that the group \mathbb{Z}_2^4 is an outlier in this discussion, so it will be considered separate from the other groups of order 16. Furthermore, the group $\mathbb{Z}_4 \times \mathbb{Z}_2$ will appear frequently, so for notational brevity we will define $K_8 \equiv \mathbb{Z}_4 \times \mathbb{Z}_2$.

Theorem 3.3. If |G| = 16 and $G \ncong \mathbb{Z}_2^4$, then either $\mathbb{Z}_8 \triangleleft G$ or $K_8 \triangleleft G$.

Proof. Since $[G : \mathbb{Z}_8] = [G : K_8] = 2$, it will be sufficient to show that either $K_8 \subset G$ or $\mathbb{Z}_8 \subset G$, since index 2 will guarantee normality. Orders of non-identity elements must be greater than 1 and divide 16, so they can only be 2, 4, 8, or 16.

Case 1. $|x| \leq 2$ for all $x \in G$, so $G \cong \mathbb{Z}_2^4$, but we assumed $G \ncong \mathbb{Z}_2^4$ so we have a contradiction.

Case 2. There exists $x \in G$ such that |x| = 8 Therefore $\langle x \rangle \cong \mathbb{Z}_8 \subset G$.

Case 3. There exists $x \in G$ such that |x| = 16, so $|x^2| = 8$ and we are back in Case 2.

We now know some more about G. Namely, G contains at least one element of order 4, since if G contains an element g such that |g| = 8 then $|g^2| = |\langle g^2 \rangle| = 4$. Furthermore, since $|G| = 2^4$, $|Z(G)| = 2^k$ for some $k \in \{1, 2, 3, 4\}$. By Cauchy's Theorem, there exists $z \in Z(G), |z| = 2$ and $\langle z \rangle = \{e, z\} \cong \mathbb{Z}_2$.

Case 4. There exists $x \in G$ such that |x| = 4 and $x^2 \neq z$. Then $\langle x \rangle \cong \mathbb{Z}_4$ and $\langle x \rangle \cap \langle z \rangle = \{e\}$, so the direct product of $\langle x \rangle$ and $\langle z \rangle$ is $\langle x, z \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2 = K_8 \subset G$.

Case 5. $x^2 = z$ for all $x \in G$ with |x| = 4. $G/\langle z \rangle$ is abelian since $|h| \leq 2$ for all $h \in G/\langle z \rangle$. Since |x| = 4, all conjugates of x are in the right coset $\langle z \rangle x$. $|\langle z \rangle| = 2$ and therefore $|C(x)| \geq 8$ where C(x) is the centralizer of x. Therefore, there must exist $y \in C(x), y \notin \langle x \rangle$.

- 1. |y| = 2 implies $\langle x, y \rangle = K_8$
- 2. |y| = 4 implies $y^2 = z$. So $(xy)^2 = x^2y^2 = zz = e$ and therefore $|xy| \le 2$. If |xy| = 1 then xy = e and $y = x^{-1} \in \langle x \rangle$, but $y \notin \langle x \rangle$ so |xy| = 2 and $xy \notin \langle x \rangle$ since then $xy = x^2$, or y = x which is another contradiction.

So now we know that every group of order 16 (except the outlier \mathbb{Z}_2^4) contains either K_8 or \mathbb{Z}_8 as a normal subgroup. Let us then consider all possible cyclic extensions of K_8 and \mathbb{Z}_8 . These two groups are small enough that we can reason through the possible automorphisms fairly easily. We will begin with \mathbb{Z}_8 .

If we let $\mathbb{Z}_8 = \langle \alpha \rangle$, then the automorphisms can easily be described by what they do to α . Namely, they raise α to odd powers, since a homomorphism that raised α to an even power would not have all of \mathbb{Z}_8 as a codomain. In fact, the codomain would be isomorphic to \mathbb{Z}_4 . So we can list the automorphisms of \mathbb{Z}_8 simply as

Automorphism $\phi_i \in \operatorname{Aut}(\mathbb{Z}_8)$	$\phi_i(\alpha)$
ϕ_1	α
ϕ_2	α^3
ϕ_3	α^5
ϕ_4	α^7

The automorphisms of K_8 are a little more involved, but follow similar principles. If we recall that $K_8 = \mathbb{Z}_4 \times \mathbb{Z}_2$ and let $\mathbb{Z}_4 = \langle \beta \rangle$ and $\mathbb{Z}_2 = \langle \gamma \rangle$ and the group $K_8 = \langle \beta, \gamma \rangle =$ $\{e, \beta, \beta^2, \beta^3, \gamma, \beta\gamma, \beta^2\gamma, \beta^3\gamma\}$, then we can just consider the effect of any particular automorphism on the generators β and γ . $|\gamma| = 2$, so γ can only be taken to elements of order 2. Only two of these exist in K_8 , namely γ and $\beta^2\gamma$. Similarly, $|\beta| = 4$ so β can only be taken to other order 4 elements, $\beta, \beta^3, \beta\gamma$, and $\beta^3\gamma$. So there are $4 \times 2 = 8$ possible automorphisms.

Automorphism $\psi_i \in \operatorname{Aut}(K_8)$	$\psi_i(\beta)$	$\psi_i(\gamma)$
ψ_1	β	γ
ψ_2	$eta^3\gamma$	$eta^2\gamma$
ψ_3	eta^3	γ
ψ_4	$eta\gamma$	$eta^2\gamma$
ψ_5	$eta\gamma$	γ
ψ_6	eta^3	$eta^2\gamma$
ψ_7	$eta^3\gamma$	γ
ψ_8	β	$eta^2\gamma$

Finally, recall that in Definition 2.1 we obtained the element n by noting that $G/N \cong \mathbb{Z}_n$ which implies that n = |G/N|. For our groups of order 16 with $N = K_8$ or \mathbb{Z}_8 , n will always be 2.

We can now begin to hone in on the possible groups of order 16. We have already established that every group of order 16 is either \mathbb{Z}_2^4 or contains a normal subgroup \mathbb{Z}_8 or K_8 , as well as every possible automorphism of \mathbb{Z}_8 (4 total) and K_8 (8 total). Since we are guaranteed that at most every possible extension type will be realized by a group, we have now an upper bound on the number of groups of order 16. In principle, for a group N and n = 2, there are $|\operatorname{Aut}(N)| \cdot |N|$ possible extensions. This puts our maximum number of groups of order 16 at $1 + 4 \cdot 8 + 8 \cdot 8 = 97$. Not a particularly low number, but this upper bound does not even account for the requirement $\tau(v) = v$. Furthermore, we can lower this bound considerably by examining which extension types can be realized at all and if there are any equivalent extension types in the list.

4 Restrictions on Possible Extension Types

Now that we have the normal subgroups and automorphisms of our extension types calculated, and the restriction n = 2, we can begin to narrow to list by considering which of our extension types are realizable, and which of those are equivalent. We will attempt to prove the following, our main theorem.

Theorem 4.1. Every group G of order 16 that is not isomorphic to \mathbb{Z}_2^4 realizes one of the following extension types, where $\mathbb{Z}_8 = \langle \alpha \rangle$ and $K_8 = \langle \beta, \gamma \rangle$:

Proof. This proof is split into several cases, but we will group them by the normal subgroup in question. In all cases, however, we will appeal to Definition 2.1 to frame the cases in terms of the order of the inducing element $g \in G$. Note that, since n = 2 for all cyclic extensions, we can write $v = g^2$, then consider which automorphisms fix v. Any $(N, 2, \tau, v)$ for which $\tau(v) \neq v$ will not be realizable.

First we will consider extension types with $N = \mathbb{Z}_8$.

Case 1. |g| = 2. Then $|v| = |g^2| = 1$, so v = e. Since $\tau(e) = e$ for all $\tau \in \operatorname{Aut}(\mathbb{Z}_8)$, all $(\mathbb{Z}_8, 2, \phi_i, e)$ are realizable. Furthermore, for all future cases, we can assume that $|x| \ge 4$ for all $x \in G/\langle z \rangle$, since otherwise we could return to this case.

Case 2. |g| = 4. Then $|v| = |g^2| = 2$, so $v = \alpha^4$.

1. $\tau = \phi_1$. Consider $(\alpha^2 g)^2$.

$$(\alpha^2 g)(\alpha^2 g) = \alpha^2 (g\alpha^2 g^{-1})g^2$$
$$= \alpha^2 \phi_1(\alpha^2)g^2 = \alpha^4 g^2$$
$$= v^2 = e,$$

so $|\alpha^2 g| = 2$, and we are back in case 1.

2. $\tau = \phi_2$. Consider $(\alpha g)^2$.

$$(\alpha g)(\alpha g) = \alpha (g\alpha g^{-1})g^2$$

= $\alpha \phi_2(\alpha)g^2 = \alpha \alpha^3 g^2$
= $\alpha^4 g^2 = v^2 = e,$

so $|\alpha g| = 2$, case 1.

3. $\tau = \phi_3$. Consider $(\alpha^2 g)^2$.

$$(\alpha^2 g)(\alpha^2 g) = \alpha^2 (g\alpha^2 g^{-1})g^2$$
$$= \alpha^2 \phi_3(\alpha^2)g^2 = \alpha^1 2g^2$$
$$= v^4 = e,$$

so $|\alpha^2 g| = 2$, case 1.

So at most $(\mathbb{Z}_8, 2, \phi_4, \alpha^4)$ is allowed, and we will see soon that it is a realized extension type.

Case 3. |g| = 8. Then |v| = 4, so $v = \alpha^2$ or $v = \alpha^6$. For $\tau = \phi_2$, $\phi_2(\alpha^2) = \alpha^6 \neq \alpha^2$ and $\phi_2(\alpha^6) = \alpha^{18} = (\alpha^8)^2 \alpha^2 = \alpha^2 \neq \alpha^6$. Similarly, $\phi_4(\alpha^2) = \alpha^6$ and $\phi_4(\alpha^6) = \alpha^2$, so only $\tau \in \{\phi_1, \phi_3\}$ are allowed.

However, for $\tau = \phi_1$, $|\alpha^3 g| = 2$ and for $\tau = \phi_3$, $|\alpha g| = 2$, so no $(\mathbb{Z}_8, 2, \phi_i, \alpha^2)$ or $(\mathbb{Z}_8, 2, \phi_i, \alpha^6)$ are allowed.

Case 4. |g| = 16. Then $G \cong \mathbb{Z}_{16}$ and G realizes $(\mathbb{Z}_8, 2, \phi_1, \alpha)$. Any other extension types must either fall into case 1 or be equivalent to this extension type.

We will now consider extension types of K_8 . Note that we can now assume that |x| < 8for all $x \in G$ since otherwise $\mathbb{Z}_8 \subset G$ and one of the extension types in the previous cases will be realized by G. So we only have two orders to consider, |g| = 2 and |g| = 4. Note that for $\tau^2 = id$ the automorphisms ψ_5 and ψ_7 are automorphic, as well as ψ_6 and ψ_8 . Additionally neither $\psi_2^2 = id$ nor $\psi_4^2 = id$, so no extension types of ψ_2 or ψ_4 can be realized for n = 2. So instead of considering all 8 automorphisms of K_8 , we need only consider 4, say $\{\psi_1, \psi_3, \psi_5, \psi_6\}$.

Case 5. |g| = 2. Then v = e. e is fixed by all automorphisms, so all $(K_8, 2, \psi_i, e)$, $i \in \{1, 3, 5, 6\}$ are allowed.

Case 6. |g| = 4. Then |v| = 2. So $v \in \{\beta^2, \gamma, \beta^2\gamma\}$.

1. $v = \beta^2$. For $\tau = \psi_1, |\beta g| = 2$, case 1.

For $\tau = \psi_6$, $|\beta \gamma g| = 2$, case 1. This holds true for all ψ_n with *n* even, but we already eliminated ψ_2, ψ_4 , and ψ_8 from the list.

So we are left with $(K_8, 2, \psi_3, \beta^2)$ and $(K_8, 2, \psi_5, \beta^2)$.

2. $v = \gamma$. $\tau(v) = v$ implies that we cannot have ψ_6 since $\psi_6(\gamma) = e \neq \gamma$.

For $\tau = \psi_7$, $|\beta g| = 2$, and we are back to case 1.

 $\tau = \psi_5$ results in $(\beta g)^2 = \beta^2$ which can be reduced to the previous subcase if we substitute $\bar{g} = \beta g$ as our inducing element. Similarly, ψ_3 reduces to the previous subcase. So we are left with $(K_8, 2, \psi_1, y)$.

3. $v = \beta^2 \gamma$. Again we cannot have ψ_n with even *n*. *v* is automorphic to *y* via ψ_8 . That is, $\psi_8(v) = \psi_8(x^2y) = x^2(x^2y) = x^4y = y$. So we will end up with the same groups as in the previous subcase.

5 The Groups of Order 16

Finally, here are the 13 groups which realize each of the extension types in Theorem 4.1, plus the outlier \mathbb{Z}_2^4 . Having just one group for each extension type is sufficient in light of Theorem 3.2.

Group Label	Construction	Extension Type
G_0	\mathbb{Z}_2^4	N/A
G_1	$\mathbb{Z}_8 imes \mathbb{Z}_2$	$(\mathbb{Z}_8, 2, \phi_1, e)$
G_2	$SD_{16} = \mathbb{Z}_8 \rtimes_{\phi_2} \mathbb{Z}_2$	$(\mathbb{Z}_8, 2, \phi_2, e)$
G_3	$\mathbb{Z}_8\rtimes_{\phi_3}\mathbb{Z}_2$	$(\mathbb{Z}_8, 2, \phi_3, e)$
G_4	$D_{16} = \mathbb{Z}_8 \rtimes_{\phi_4} \mathbb{Z}_2$	$(\mathbb{Z}_8, 2, \phi_4, e)$
G_5	Q_{16}	$(\mathbb{Z}_8, 2, \phi_4, \alpha^4)$
G_6	\mathbb{Z}_{16}	$(\mathbb{Z}_8, 2, \phi_1, \alpha)$
G_7	$\mathbb{Z}_4 imes \mathbb{Z}_2^2$	$(K_8, 2, \psi_1, e)$
G_8	$D_8 \times \mathbb{Z}_2$	$(K_8, 2, \psi_3, e)$
G_9	$\mathbb{Z}_4 \rtimes \mathbb{Z}_2^2$	$(K_8,2,\psi_5,e)$
G_{10}	$Q_8 \rtimes \mathbb{Z}_2$	$(K_8, 2, \psi_6, e)$
G_{11}	$Q_8 \times \mathbb{Z}_2$	$(K_8,2,\psi_3,\beta^2)$
G_{12}	$\mathbb{Z}_4 \rtimes \mathbb{Z}_4$	$(K_8,2,\psi_5,\beta^2)$
G_{13}	$\mathbb{Z}_4 imes \mathbb{Z}_4$	$(K_8,2,\psi_1,\gamma)$

References

- [1] Jeffrey D. Adler, Michael Garlow, and Ethel R. Wheland. Groups of order p⁴ made less difficult, 2006.
- [2] Daniel Gorenstein. Finite Groups. Chelsea Pub. Co., New York, second edition, 1980.
- [3] Thomas W. Judson. *Abstract Algebra: Theory and Application*. Orthogonal Publishing L3C, Ann Arbor, 2013.
- [4] Marcel Wild. The groups of order sixteen made easy. The American Mathematical Monthly, 112.1:20–31, 2005.