The Classification of Finite Groups of Order 16

Kyle Whitcomb

Department of Mathematics and Computer Science
University of Puget Sound
Tacoma, Washington

May 5, 2015

Outline

Introduction

There are significantly more groups of order 16 than of groups with lesser order. To put it more precisely, here is a table with the number of groups with orders 2 to 16:

Order n	1	2	3	4	5	6	7	8
# groups with order n	1	1	1	2	1	2	1	5
Order n	9	10	11	12	13	14	15	16
# groups with order n	2	2	1	5	1	2	1	14

We seek to classify all 14 of these groups of order 16 by utilizing extension types.

Table of Contents

Familiar Concepts

We will rely on the previous knowledge of the following concepts in abstract algebra, which we should be familiar with from Judson's *Abstract Algebra*.

- Abelian groups
- Normal subgroups, $N \lhd G$
- Generators, and groups generated by multiple elements, $G = \langle g_1, g_2, \ldots \rangle$
- Centers, $Z(G)$
- Automorphisms, and the automorphism group $\mathrm{Aut}(G)$

Familiar Concepts (cont.)

- The inner automorphism
  - For $a \in G$, there is an inner automorphism of G, $t_a : G \to G$, $t_a(x) = axa^{-1}$
- Conjugate elements
  - Two elements, $g_1, g_2 \in G$, are conjugate if there exists an inner automorphism t_a of G such that $t_a(g_1) = g_2$.

Inner Semidirect Products

The inner semidirect product is a very easy construction if you recall the inner direct product.

Definition

Given a group G, if $N \lhd G$ and $H \subseteq G$ such that

1. $G = NH = \{nh \mid n \in N,\ h \in H\}$, and
2. $N \cap H = \{e_G\}$,

then G is the **inner semidirect product** of N and H.

Outer Semidirect Products

If G is an inner semidirect product of N and H, then G is isomorphic to an outer semidirect product of N and H, $G \cong N \rtimes_{\varphi} H$.

Outer Semidirect Products

If G is an inner semidirect product of N and H, then G is isomorphic to an outer semidirect product of N and H, $G \cong N \rtimes_\varphi H$.

Definition

N and H are groups, and φ is a homomorphism $\varphi : H \to \text{Aut}(N)$, $\varphi(h) = \varphi_h$ where $\varphi_h(n) = hnh^{-1}$ for $h \in H, n \in N$. The **outer semidirect product** of N and H with respect to φ is $N \rtimes_\varphi H$, where the operation is

$$* : (N \times H) \times (N \times H) \to N \rtimes_\varphi H,$$

$$(n_1, h_1) * (n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2).$$

Cyclic Extensions

Definition (Cyclic Extension)

Let $N \lhd G$. If $G/N \cong \mathbb{Z}_n$, then G is a **cyclic extension** of N.

Some Properties of Cyclic Extensions

Suppose G is a cyclic extension of N, $G/N \cong \mathbb{Z}_n$.

Some Properties of Cyclic Extensions

Suppose G is a cyclic extension of N, $G/N \cong \mathbb{Z}_n$.
Consider $a \in G$ such that $|Na| = n$ in G/N, then $v = a^n \in N$.

Some Properties of Cyclic Extensions

Suppose G is a cyclic extension of N, $G/N \cong \mathbb{Z}_n$.
Consider $a \in G$ such that $|Na| = n$ in G/N, then $v = a^n \in N$.
Consider $\tau \in \mathrm{Aut}(N)$ such that τ is the restriction to N of the inner automorphism t_a of G.

Some Properties of Cyclic Extensions

Suppose G is a cyclic extension of N, $G/N \cong \mathbb{Z}_n$.
Consider $a \in G$ such that $|Na| = n$ in G/N, then $v = a^n \in N$.
Consider $\tau \in \mathrm{Aut}(N)$ such that τ is the restriction to N of the inner automorphism t_a of G.
Then

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

and

$$\tau^n(x) = aa \cdots a(x)a^{-1} \cdots a^{-1}a^{-1} = a^n x a^{-n} = vxv^{-1} = t_v(x)$$

for all $x \in N$. Therefore $\tau^n = t_v$.

Extension Types

Definition

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

Extension Types

Definition

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

Definition

Given a group G, if

1. $N \lhd G$,
2. $G/N \cong \mathbb{Z}_n$,
3. there exists $a \in G$ such that $v = a^n$,
4. and there exists $\tau \in \mathrm{Aut}(G)$ such that $\tau^n = t_v$ and $\tau(v) = v$,

then G **realizes** the extension type (N, n, τ, v).

Table of Contents

Equivalence of Extension Types

Theorem

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 $w = \varphi(v)$.

Isomorphic Groups Realize Equivalent Extension Types

Theorem

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

Important Subgroups of Groups of Order 16

Outlier group:

- $\mathbb{Z}_2^4$

Theorem

If $|G| = 16$ *and* $G \ncong \mathbb{Z}_2^4$*, then either* $\mathbb{Z}_8 \lhd G$ *or* $K_8 \lhd G$*, where* $K_8 \equiv \mathbb{Z}_4 \times \mathbb{Z}_2$.

Automorphisms of $\mathbb{Z}_8$

If α is a generator of $\mathbb{Z}_8$, $\mathbb{Z}_8 = \langle \alpha \rangle$, then all of the automorphisms of $\mathbb{Z}_8$ can be expressed as follows.

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

Automorphisms of K_8

Similarly, if $\mathbb{Z}_4 = \langle\beta\rangle$ and $\mathbb{Z}_2 = \langle\gamma\rangle$, then $K_8 = \langle\beta, \gamma\rangle$. The automorphisms of K_8 are then:

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

Table of Contents

The Big Theorem

Theorem

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 $K_8 = \langle\beta, \gamma\rangle$:

$$\begin{array}{cccc} (\mathbb{Z}_8, 2, \phi_1, e), & (\mathbb{Z}_8, 2, \phi_2, e) & (\mathbb{Z}_8, 2, \phi_3, e), & (\mathbb{Z}_8, 2, \phi_4, e), \\ (\mathbb{Z}_8, 2, \phi_4, \alpha^4), & (\mathbb{Z}_8, 2, \phi_1, \alpha), & (K_8, 2, \psi_1, e), & (K_8, 2, \psi_3, e), \\ (K_8, 2, \psi_5, e), & (K_8, 2, \psi_6, e), & (K_8, 2, \psi_3, \beta^2), & (K_8, 2, \psi_5, \beta^2), \\ (K_8, 2, \psi_1, \gamma). & & & \end{array}$$

The Big Proof

Proof Skeleton:
Preliminary details

- *Case 1.*
- *Case 2.* {Subcases *i*, *ii*, *iii*}
- *Case 3.*
- *Case 4.*
- *Case 5.*
- *Case 6.* {Subcases *i*, *ii*, *iii*}

Excerpts from The Big Proof

Preliminary setup:

- For $G \ncong \mathbb{Z}_2^4$, $K_8 \lhd G$ or $\mathbb{Z}_8 \lhd G$

Excerpts from The Big Proof

Preliminary setup:

- For $G \ncong \mathbb{Z}_2^4$, $K_8 \lhd G$ or $\mathbb{Z}_8 \lhd G$
- $[G : \mathbb{Z}_8] = [G : K_8] = 2$, so $n = 2$

Excerpts from The Big Proof

Preliminary setup:

- For $G \ncong \mathbb{Z}_2^4$, $K_8 \lhd G$ or $\mathbb{Z}_8 \lhd G$
- $[G : \mathbb{Z}_8] = [G : K_8] = 2$, so $n = 2$
- All possible extension types (up to isomorphism) take the form $(K_8, 2, \psi_i, v)$ and $(\mathbb{Z}_8, 2, \phi_j, v)$

Excerpts from The Big Proof

Preliminary setup:

- For $G \ncong \mathbb{Z}_2^4$, $K_8 \lhd G$ or $\mathbb{Z}_8 \lhd G$
- $[G : \mathbb{Z}_8] = [G : K_8] = 2$, so $n = 2$
- All possible extension types (up to isomorphism) take the form $(K_8, 2, \psi_i, v)$ and $(\mathbb{Z}_8, 2, \phi_j, v)$
- $v = g^2$ for some inducing element $g \in G$

Excerpts from The Big Proof

Outline of cases:

- First look through extension types of $\mathbb{Z}_8$, then K_8

Excerpts from The Big Proof

Outline of cases:

- First look through extension types of $\mathbb{Z}_8$, then K_8
- Consider all possibilities for $|g|$, where $g \in G$ is the (non-identity) inducing element.

Excerpts from The Big Proof

Outline of cases:

- First look through extension types of $\mathbb{Z}_8$, then K_8
- Consider all possibilities for $|g|$, where $g \in G$ is the (non-identity) inducing element.
- Consider each automorphism τ of the current group

Excerpts from The Big Proof

Outline of cases:

- First look through extension types of $\mathbb{Z}_8$, then K_8
- Consider all possibilities for $|g|$, where $g \in G$ is the (non-identity) inducing element.
- Consider each automorphism τ of the current group
- Search for contradictions with $\tau(v) = v$, or look for ways to reduce them to previous cases.

Excerpts from The Big Proof

Example 1: Case 1 (the easiest case)

- $N = \mathbb{Z}_8$, $|g| = 2$

Excerpts from The Big Proof

Example 1: Case 1 (the easiest case)

- $N = \mathbb{Z}_8$, $|g| = 2$
- Therefore $v = g^2 = e$

Excerpts from The Big Proof

Example 1: Case 1 (the easiest case)

- $N = \mathbb{Z}_8$, $|g| = 2$
- Therefore $v = g^2 = e$
- $\tau(e) = e$ for all $\tau \in \mathrm{Aut}(\mathbb{Z}_8)$

Excerpts from The Big Proof

Example 1: Case 1 (the easiest case)

- $N = \mathbb{Z}_8$, $|g| = 2$
- Therefore $v = g^2 = e$
- $\tau(e) = e$ for all $\tau \in \text{Aut}(\mathbb{Z}_8)$
- All $(\mathbb{Z}_8, 2, \phi_i, e)$ allowed

Excerpts from The Big Proof

Example 2: Case 3 (a more illuminating example)

- $N = \mathbb{Z}_8$, $|g| = 8$

Excerpts from The Big Proof

Example 2: Case 3 (a more illuminating example)

- $N = \mathbb{Z}_8$, $|g| = 8$
- Therefore $|v| = 4$ so $v \in \{\alpha^2 or \alpha^6\}$

Excerpts from The Big Proof

Example 2: Case 3 (a more illuminating example)

- $N = \mathbb{Z}_8$, $|g| = 8$
- Therefore $|v| = 4$ so $v \in \{\alpha^2 or \alpha^6\}$
- Consider $v = \alpha^2$

Excerpts from The Big Proof

Example 2: Case 3 (a more illuminating example)

- $N = \mathbb{Z}_8$, $|g| = 8$
- Therefore $|v| = 4$ so $v \in \{\alpha^2 or \alpha^6\}$
- Consider $v = \alpha^2$
  - Let $\tau = \phi_2$, then $\phi_2(v) = \phi_2(\alpha^2) = (\alpha^2)^3 = \alpha^6 \neq v$

Excerpts from The Big Proof

Example 2: Case 3 (a more illuminating example)

- $N = \mathbb{Z}_8$, $|g| = 8$
- Therefore $|v| = 4$ so $v \in \{\alpha^2 or \alpha^6\}$
- Consider $v = \alpha^2$
  - Let $\tau = \phi_2$, then $\phi_2(v) = \phi_2(\alpha^2) = (\alpha^2)^3 = \alpha^6 \neq v$
  - Let $\tau = \phi_4$, then then $\phi_4(v) = \phi_4(\alpha^2) = (\alpha^2)^7 = \alpha^14 = \alpha^6 \neq v$.

Excerpts from The Big Proof

Example 2: Case 3 (a more illuminating example)

- $N = \mathbb{Z}_8$, $|g| = 8$
- Therefore $|v| = 4$ so $v \in \{\alpha^2 or \alpha^6\}$
- Consider $v = \alpha^2$
  - Let $\tau = \phi_2$, then $\phi_2(v) = \phi_2(\alpha^2) = (\alpha^2)^3 = \alpha^6 \neq v$
  - Let $\tau = \phi_4$, then then $\phi_4(v) = \phi_4(\alpha^2) = (\alpha^2)^7 = \alpha^1 4 = \alpha^6 \neq v$.
- Similarly, for $v = \alpha^6$, $\phi_2(\alpha^6) = \phi_4(\alpha^6) = \alpha^2 \neq v$.

Excerpts from The Big Proof

Example 2: Case 3 (a more illuminating example)

- $N = \mathbb{Z}_8$, $|g| = 8$
- Therefore $|v| = 4$ so $v \in \{\alpha^2 or \alpha^6\}$

Excerpts from The Big Proof

Example 2: Case 3 (a more illuminating example)

- $N = \mathbb{Z}_8$, $|g| = 8$
- Therefore $|v| = 4$ so $v \in \{\alpha^2 or \alpha^6\}$
- Let $v = g^2 = \alpha^2$ and $\tau = \phi_1$

Excerpts from The Big Proof

Example 2: Case 3 (a more illuminating example)

- $N = \mathbb{Z}_8$, $|g| = 8$
- Therefore $|v| = 4$ so $v \in \{\alpha^2 or \alpha^6\}$
- Let $v = g^2 = \alpha^2$ and $\tau = \phi_1$
- Consider $(\alpha^3 g)$.

$$\begin{aligned}(\alpha^3 g)^2 &= \alpha^3 g \alpha^3 g = \alpha^3 g \alpha^3 g^{-1} g^2 \\ &= \alpha^3 \phi_1(\alpha^3)\alpha^2 = \alpha^3\alpha^3\alpha^2 \\ &= \alpha^8 = e.\end{aligned}$$

So $|\alpha^3 g| = 2$ and we are back in Case 1.

Excerpts from The Big Proof

Example 2: Case 3 (a more illuminating example)

- $N = \mathbb{Z}_8$, $|g| = 8$
- Therefore $|v| = 4$ so $v \in \{\alpha^2 or \alpha^6\}$
- Let $v = g^2 = \alpha^2$ and $\tau = \phi_1$
- Consider $(\alpha^3 g)$.

$$
\begin{aligned}
(\alpha^3 g)^2 &= \alpha^3 g \alpha^3 g = \alpha^3 g \alpha^3 g^{-1} g^2 \\
&= \alpha^3 \phi_1(\alpha^3)\alpha^2 = \alpha^3 \alpha^3 \alpha^2 \\
&= \alpha^8 = e.
\end{aligned}
$$

So $|\alpha^3 g| = 2$ and we are back in Case 1.

- Similar proofs for $\tau = \phi_3$ and the $v = \alpha^6$ subcases.

Excerpts from The Big Proof

Example 2: Case 3 (a more illuminating example)

- $N = \mathbb{Z}_8$, $|g| = 8$
- Therefore $|v| = 4$ so $v \in \{\alpha^2 or \alpha^6\}$
- Let $v = g^2 = \alpha^2$ and $\tau = \phi_1$
- Consider $(\alpha^3 g)$.

$$\begin{aligned}(\alpha^3 g)^2 &= \alpha^3 g \alpha^3 g = \alpha^3 g \alpha^3 g^{-1} g^2 \\ &= \alpha^3 \phi_1(\alpha^3)\alpha^2 = \alpha^3 \alpha^3 \alpha^2 \\ &= \alpha^8 = e.\end{aligned}$$

So $|\alpha^3 g| = 2$ and we are back in Case 1.

- Similar proofs for $\tau = \phi_3$ and the $v = \alpha^6$ subcases.
- No $(\mathbb{Z}_8, 2, \phi_i, \alpha^2)$ or $(\mathbb{Z}_8, 2, \phi_i, \alpha^6)$ are allowed.

Table of Contents

The 14 Groups of Order 16 (Part 1)

Group Label	Construction	Extension Type
G_0	$\mathbb{Z}_2^4$	N/A
G_1	$\mathbb{Z}_8 \times \mathbb{Z}_2$	$(\mathbb{Z}_8, 2, \phi_1, e)$
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	$\mathbb{Z}_{16}$	$(\mathbb{Z}_8, 2, \phi_1, \alpha)$

The 14 Groups of Order 16 (Part 2)

Group Label	Construction	Extension Type
G_7	$\mathbb{Z}_4 \times \mathbb{Z}_2^2$	$(K_8, 2, \psi_1, e)$
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}	$\mathbb{Z}_4 \times \mathbb{Z}_4$	$(K_8, 2, \psi_1, \gamma)$