

Classification of Finite Groups

Daniel Laing

February 27, 2023

Contents

| | | |
|------------|---|-----------|
| 1 | Introduction | 2 |
| 2 | Preliminaries | 2 |
| 2.1 | Semidirect Product | 3 |
| 2.2 | Group Actions | 6 |
| I | Prime Power Orders | 6 |
| 3 | First Classifications | 7 |
| 4 | Groups of Order p^2 | 8 |
| 5 | Groups of Order p^3 | 8 |
| II | Composite Orders | 11 |
| 6 | Groups of Order pq | 11 |
| 6.1 | Groups of Order $2p$ | 12 |
| 7 | Some Groups of Order p^2q | 12 |
| 7.1 | $4q$ | 12 |
| 7.2 | $2p^2$ | 13 |
| III | Special Cases | 14 |
| 8 | Groups of order 12 | 14 |
| 9 | Groups of Order 24 | 17 |
| 10 | Groups of Order 30 | 21 |
| 11 | Groups of Order 16 | 22 |
| | References | 23 |

1 Introduction

2 Preliminaries

To start, let's solidify the notation used in this report.

We shall denote groups and sets with capital letters, like G , H , and elements of those groups with lower case letters, like g , h . Greek letters shall denote mappings, generally ϕ , ψ , etc. with ι reserved for the identity map, and we will write mappings on the right.

We will use \mathbb{N} to denote the natural numbers (not including 0), \mathbb{Z} to denote the integers, and \mathbb{R} to denote the real numbers.

To denote the cyclic group of order n we will use C_n , D_{2n} to denote the cyclic group of order $2n$, A_n to denote the alternating group over n elements, S_n to denote the symmetric group over n elements, and Q_8 to denote the quaternion group. The trivial group, $\{1\}$ is denoted by $\mathbf{1}$.

Let's move on to review some facts and theorems which will be valuable later on, as well as introduce some new concepts and prove some new results!

Definition 1. If G and H are groups with elements $g_1, g_2 \in G$, then a map:

$$\phi : G \rightarrow H$$

is a homomorphism if:

$$(g_1 g_2) \phi = (g_1 \phi) (g_2 \phi)$$

If ϕ is bijective, then we call it an isomorphism, with $G \cong H$ denoting that G is isomorphic to H . And if ϕ is an isomorphism from G to itself, then we call it an automorphism of G .

Lemma 1. *The set of all automorphisms of a group G form a group under composition. Indeed, this is called the automorphism group of G , denoted $\text{Aut } G$.*

Proof. Let $A = \text{Aut } G = \{ \phi : G \rightarrow G \mid \phi \text{ is an isomorphism} \}$, and let $\phi \in A$. Denote an element of G by g .

We know already that the composition of two isomorphisms is an isomorphism, so A is closed under composition.

The identity map, $\iota : g \mapsto g$, is certainly an automorphism of G and so $A \neq \emptyset$.

Indeed, $\iota : g \mapsto g$ is the identity of A , since:

$$g \phi \iota = (g \phi) \iota = g \phi \quad \text{and} \quad g \iota \phi = (g \iota) \phi = g \phi$$

And inverses clearly exists, because automorphisms are bijections, and bijections are invertible. Hence $A = \text{Aut } G$ is a group. \square

Lemma 2. *The automorphism group of C_n is isomorphic to the multiplicative group of integers mod n .*

$$\text{i.e. } \text{Aut } C_n \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

Proof. Let $C_n = \langle x \rangle$. Any automorphism, φ of C_n has the property:

$$(x^i) \varphi = (x \varphi)^i$$

Hence φ is determined by it's effect on a generator, x , and preserves element order. In particular, φ sends generators to generators. So for φ to be an automorphism, it must send x to another generator, say x^k . An element x^k generates C_n if x^k has order n , i.e. when k and n are co-prime. Denote the automorphism sending x to x^k by φ_k .

Let's now investigate how these automorphisms behave. Let $\varphi_k, \varphi_l \in \text{Aut } C_n$, and consider:

$$x\varphi_k\varphi_l = (x^k)\varphi_l = (x^k)^l = x^{(kl)} = x\varphi_{kl} \quad \text{mod } n$$

Because multiplication modulo n is commutative, $x^{kl} = x^{lk}$, so $\text{Aut } C_n$ is abelian.

Now consider $\theta : \text{Aut } C_n \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ defined by $\varphi_k\theta = k$. We will show θ is an isomorphism. Every $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ is co-prime to n and so x^k is a generator of C_n , hence there is some $\varphi_k \in \text{Aut } C_n$ such that $\varphi_k\theta = k$. So θ is surjective. If $\varphi_k\theta = \varphi_l\theta$ then $k = l$, so θ is also injective. Finally, θ is a homomorphism because:

$$(\varphi_k\varphi_l)\theta = \varphi_{kl}\theta = kl = (\varphi_k\theta)(\varphi_l\theta)$$

So $\theta : \text{Aut } C_n \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism. □

Definition 2. A subgroup H of a group G is called characteristic if it is fixed by all automorphisms of G .

i.e. for an automorphism ϕ of G , $H\phi = H$.

Lemma 3. Let G be a group with normal subgroup H , and let K be characteristic in H . Then K is a normal subgroup of G .

Proof. Consider the map $\varphi_g : G \rightarrow G$ defined by $\varphi_g : x \mapsto g^{-1}xg$ for elements $x, g \in G$. We will show that this is an automorphism of G . For $x, y \in G$:

$$x\varphi_g y\varphi_g = (g^{-1}xg)(g^{-1}yg) = g^{-1}(xy)g = (xy)\varphi_g$$

Hence φ_g is a homomorphism. Moreover, φ_g is invertible with inverse $\varphi_{g^{-1}}$. So φ_g is indeed an automorphism of G .

Because H is normal, $H\varphi_g = H$. So φ_g is an automorphism of H too. And so φ_g maps K to itself, because it is characteristic. Hence:

$$\{g^{-1}kg \mid k \in K\} = K$$

So K is normal in G . □

2.1 Semidirect Product

We already know about the direct product:

Definition 3 (Direct Product). For groups N and H , the direct product, $G = N \times H$ is a group of ordered pairs of elements (n, h) where $n \in N$ and $h \in H$ with the operation:

$$(n_1, h_1)(n_2, h_2) = (n_1n_2, h_1h_2)$$

Moreover, if $\bar{N} = N \times \mathbf{1}$ and $\bar{H} = \mathbf{1} \times H$, then:

- (i) $\bar{N} \trianglelefteq G$ and $\bar{H} \trianglelefteq G$
- (ii) $\bar{N} \cap \bar{H} = \mathbf{1}$
- (iii) $\bar{N}\bar{H} = \{nh \mid n \in N, h \in H\} = G$

Now let's seek a slightly more general way to combine groups, by relaxing that H must be normal. So we have:

$$N \trianglelefteq G, H \leq G, NH = G, \quad \text{and} \quad N \cap H = \mathbf{1}$$

Consider the set, (not the direct product):

$$N \times H = \{ (n, h) \mid n \in N, h \in H \}$$

and a map

$$\phi : N \times H \rightarrow G \quad \text{defined by} \quad (n, h) \mapsto nh$$

We want ϕ to be an isomorphism.

To show ϕ is injective, take $n_1, n_2 \in N$ and $h_1, h_2 \in H$, and assume $n_1 h_1 = n_2 h_2$. Then multiplying on the left by n_2^{-1} and on the right by h_1^{-1} gives:

$$n_2^{-1} n_1 = h_2 h_1^{-1}$$

On the left we have an element of N and on the right, an element of H , so $n_2^{-1} n_1 = h_2 h_1^{-1} \in N \cap H$. But $N \cap H = \mathbf{1}$ so then $n_2^{-1} n_1 = h_2 h_1^{-1} = 1$. Hence:

$$n_1 = n_2 \quad \text{and} \quad h_1 = h_2$$

To show ϕ is surjective, consider the image, $\text{im } \phi = \{ nh \mid n \in N, h \in H \}$. This is by definition $NH = G$, so ϕ is surjective, and hence a bijection.

For ϕ to be a homomorphism, we need:

$$\begin{aligned} [(n_1, h_1)(n_2, h_2)]\phi &= (n_1, h_1)\phi (n_2, h_2)\phi \\ &= n_1 h_1 n_2 h_2 \\ &= n_1 h_1 n_2 h_1^{-1} h_1 h_2 \\ &= (n_1 h_1 n_2 h_1^{-1})(h_1 h_2) \end{aligned}$$

But N is normal in G so $h_1 n_2 h_1^{-1}$ is just another element in N , say n_3 . So:

$$[(n_1, h_1)(n_2, h_2)]\phi = (n_1 n_3)(h_1 h_2) = (n_1 n_3, h_1 h_2)\phi$$

We know that ϕ is injective, so then:

$$(n_1, h_1)(n_2, h_2) = (n_1 n_3, h_1 h_2)$$

This tells us the multiplication that will make NH a group. Because $N \trianglelefteq G$, the map

$$\varphi_{h_1} : n_2 \mapsto h_1 n_2 h_1^{-1} = n_3$$

is an automorphism of N . This gives rise to the definition:

Definition 4 (Semidirect Product).

- (i) For a group G with normal subgroup N and subgroup H with $NH = G$ and $N \cap H = \mathbf{1}$, G is the internal semidirect product of N by H , written $G = N \rtimes H$.

- (ii) For groups N and H , and a homomorphism $\psi : H \rightarrow \text{Aut } N$, the external semidirect product of N by H via ψ is the set:

$$N \times H = \{ (n, h) \mid n \in N, h \in H \}$$

with multiplication:

$$(n_1, h_1)(n_2, h_2) = (n_1(n_2^{h_1\psi}), h_1h_2)$$

denoted:

$$N \rtimes_{\psi} H$$

We use the notation $n_2^{h_1\psi}$ both because it indicates conjugation, and is clearer.

Lemma 4. For a group G with $N \leq G$ and $H \leq G$, with $N \cap H = \mathbf{1}$ then:

$$|NH| = |\{nh \mid n \in N, h \in H\}| = |N| \cdot |H|$$

Proof. We just saw above that for elements $n \in N$ and $h \in H$, the map:

$$\phi : N \times H \rightarrow NH \quad \text{defined by} \quad (n, h) \mapsto nh$$

is a bijection. The result follows immediately from this. \square

Lemma 5. Let N and H be groups, and $\alpha \in \text{Aut } H$. Then the semidirect products via the homomorphism ϕ , $N \rtimes_{\phi} H$, and via the homomorphism ψ , $N \rtimes_{\psi} H$, are isomorphic if $h\beta\psi = \alpha^{-1}h\phi\alpha$ for all $h \in H$, $\alpha \in \text{Aut } N$ and $\beta \in \text{Aut } H$.

That is, we can apply any automorphism to H and conjugate N , and the resulting semidirect product remains in the same isomorphism class.

Proof. Let $G = N \rtimes_{\phi} H$ and $\bar{G} = N \rtimes_{\psi} H$, and define:

$$\vartheta : G \rightarrow \bar{G} \quad \text{by} \quad \vartheta : (n, h) \mapsto (n\alpha, h\beta)$$

We will show that ϑ is an isomorphism.

First, ϑ^{-1} exists because both α^{-1} and β^{-1} exist, and is given by:

$$\vartheta^{-1} : (n, h) \mapsto (n\alpha^{-1}, h\beta^{-1})$$

Hence ϑ is a bijection.

We also have that:

$$h\beta\psi = \alpha^{-1}h\phi\alpha$$

implies:

$$\alpha h\beta\psi = h\phi\alpha$$

Now for two elements, $(n_1, h_1), (n_2, h_2) \in G$, consider:

$$\begin{aligned} (n_1, h_1)\vartheta (n_2, h_2)\vartheta &= (n_1\alpha, h_1\beta)(n_2\alpha, h_2\beta) \\ &= (n_1\alpha n_2\alpha^{(h_1\beta)\psi}, h_1\beta h_2\beta) \\ &= (n_1\alpha n_2^{(\alpha h_1\beta\psi)}, h_1\beta h_2\beta) \\ &= (n_1\alpha n_2^{(h_1\beta\phi\alpha)}, h_1\beta h_2\beta) \\ &= (n_1\alpha (n_2^{(h_1\beta\phi)})^{\alpha}, h_1\beta h_2\beta) \\ &= ((n_1 n_2^{(h_1\beta\phi)})^{\alpha}, (h_1 h_2)\beta) \\ &= (n_1 n_2^{(h_1\beta\phi)}, h_1 h_2)\vartheta \\ &= ((n_1, h_1)(n_2, h_2))\vartheta \end{aligned}$$

So ϑ is an isomorphism. \square

2.2 Group Actions

Some snazzy introduction.

Definition 5. Let G be a group, and Ω be a set, with elements $g \in G$ and $\omega \in \Omega$. Consider a map $\mu : \Omega \times G \rightarrow \Omega$, and write ω^g for the image of (ω, g) under μ . So we have:

$$\mu : \Omega \times G \rightarrow \Omega \quad \text{defined by} \quad (\omega, g) \mapsto \omega^g$$

We say G acts on Ω if for all $g_1, g_2 \in G$ and all $\omega \in \Omega$:

$$(i) \quad (\omega^{g_1})^{g_2} = \omega^{(g_1 g_2)}$$

$$(ii) \quad \omega^1 = \omega$$

We call μ the group action of G on Ω .

This might remind you of a homomorphism. Indeed we have a result:

Lemma 6. *A group action induces a homomorphism. Specifically, let G be a group which acts on a set Ω , with $g \in G$ and $\omega \in \Omega$, and define:*

$$\rho_g : \Omega \rightarrow \Omega \quad \text{by} \quad \omega \mapsto \omega^g$$

Then:

$$\rho : G \rightarrow \text{Sym } \Omega \quad \text{defined by} \quad g \mapsto \rho_g$$

is a homomorphism.

Proof. Firstly, ρ_g is indeed a permutation of Ω because it is invertible (and therefore a bijection), with:

$$(\rho_g)^{-1} = \rho_{g^{-1}}$$

Consider $g, h \in G$ and their corresponding maps, $\rho_g, \rho_h \in \text{Sym } \Omega$. Then:

$$\omega(g\rho)(h\rho) = \omega\rho_g\rho_h = (\omega^g)^h = \omega^{(gh)} = \omega\rho_{gh} = \omega(gh)\rho$$

Thus ρ is a homomorphism. □

A group acting on the set its cosets will be very useful:

Definition 6. For a group G with $H \leq G$, let $\Omega = \{Hg \mid g \in G\}$, i.e. the set of cosets of H in G . If $x \in G$, define a group action:

$$\Omega \times G \rightarrow \Omega \quad \text{by} \quad (Hg, x) \mapsto Hgx$$

Lemma 7. *The action above is well defined, meaning the action is independent of our choice of representative g .*

Proof. □

Part I

Prime Power Orders

First, we will prove a few useful lemmas:

Lemma 8. *If G is a p -group (i.e. a group of prime power order), then every subgroup of index p is normal.*

Proof. Let H be a subgroup of G , with index p . We know kernels are normal subgroups, so we will show that H is the kernel of some homomorphism. Let Ω be the set of all cosets of H . So by definition, $|\Omega| = p$. By Lemma 6, there is a homomorphism:

$$\rho : G \rightarrow S_p$$

Let's investigate the kernel of ρ . If we have $x \in \ker \rho$, then:

$$(H1)x = H1 = H$$

which means $x \in H$. So the kernel of ρ is H . Hence, $H \trianglelefteq G$. □

Lemma 9. *If G is a group of prime power order, the centre of G is non-trivial. In particular, p divides the order of the centre.*

Proof. Let Z denote the centre of G , and consider the action of G on itself by conjugation. The orbit of an element, $g \in G$ is:

$$g^G = \{ x^{-1}gx \mid x \in G \}$$

which is the conjugacy class of g . So the size of each orbit divides some power of p . In particular, the size of each orbit is divisible by p . So then the sum of the sizes of all of the conjugacy classes is also divisible by p . Looking at the class equation:

$$|G| = |Z| + \sum_{i=1}^k |g_i^G|$$

Then reducing mod p gives:

$$|G| \equiv |Z| \pmod{p}$$

Because G is non-trivial, it follows that $|Z| \neq 1$. □

Lemma 10. *For a group G with centre $Z(G)$. Then if $G/Z(G)$ is cyclic, G is abelian.*

Proof. Let $x \in G$ be the element such that $xZ(G)$ generates $G/Z(G)$. Then $\langle x, Z(G) \rangle$ contains $Z(G)$. Because G is the union of cosets of $Z(G)$, then indeed $\langle x, Z(G) \rangle = G$. The centraliser of x certainly contains x , and every element of $Z(G)$ also commutes with x . Hence the centre of G is a subgroup of the centraliser of x . The result follows by concluding:

$$G = \langle x, Z(G) \rangle = \langle Z(G) \rangle = Z(G)$$

□

Now onto the classification!

3 First Classifications

Let's start with the easiest case: groups of order 1. Any group G must have an identity element, and so that's all our possible elements used up! All groups of order 1 are isomorphic to the trivial group, $\mathbf{1}$.

What about groups of prime order? Let G be a group of order p , where p is a prime number. Then Lagrange's Theorem tell us all elements must have order 1 or p . Pick some $x \in G$ with x having order p . Then $\langle x \rangle = G$ so G is cyclic and $G \cong C_p$.

4 Groups of Order p^2

Let G be a group of order p^2 . By Lagrange's Theorem, the elements of G have order 1, p or p^2 . If $x \in G$ has order p^2 , then x generates G so $G \cong C_{p^2}$.

If G does not have an element of order p^2 then all elements, except the identity, have order p . We know that G must have a subgroup of order p , P , and because p is prime, $P \cong C_p$. Pick a generator for P , say x and an element $y \in G$ such that $y \notin P$. Then $y \neq x^i$ for any i .

If $y^j = x^i$ for some i and j , then:

$$(y^j)^{1-j} = (x^i)^{1-j} = y^{j-j+1} = y = x^{i(1-j)} = x^k \quad \text{for some } k, \text{ a contradiction.}$$

So no power of y is equal to any power of x . Because y has order p , it generates a subgroup of order p , \bar{P} , with $P \cap \bar{P} = \mathbf{1}$. Lemma 8 tells us that both P and \bar{P} are normal, and by Lemma 4, $|P\bar{P}| = p^2 = |G|$, so:

$$G = P \times \bar{P} \cong C_p \times C_p$$

If G has no elements of order p or p^2 , then it only has elements of order 1, which is the trivial group.

Hence any group of order p^2 is isomorphic to one of:

$$C_{p^2} \quad \text{or} \quad C_p \times C_p$$

5 Groups of Order p^3

This classification is based on the one found on the Groupprops subwiki¹. Let G be a group of order p^3 , where p is a prime number. We will first gain a handle on G by describing its centre, and quotient by it. If G is abelian, we know by the Fundamental Theorem of Finite Abelian Groups that it is isomorphic to one of:

$$C_{p^3}, \quad C_{p^2} \times C_p \quad \text{or} \quad C_p \times C_p \times C_p$$

So from now on, we will focus on the non-abelian groups.

Denote the centre of G by Z and consider its order. Lagrange's Theorem tells us Z must have order dividing p^3 . It cannot be p^3 because G is non-abelian, and Lemma 9 tells us that it cannot be 1. If $|Z| = p^2$, then $|G/Z| = p$, so $G/Z \cong C_p$. However Lemma 10 says that then G must be abelian, so then $|Z|$ must be p . Then by our previous classification, G/Z is isomorphic to either C_{p^2} or $C_p \times C_p$. Lemma 10 tells us that it must be the latter.

This gives us a handle to start investigating the structure of G . Another useful tool will be commutators, which we will denote by $[a, b] = a^{-1}b^{-1}ab$. The derived subgroup of G , $G' = \langle [x, y] \mid x, y \in G \rangle$, is the smallest normal subgroup such that G/G' is abelian. We saw that G/Z is abelian, so $G' \leq Z$, but because G' is non-trivial, we must have equality.

So far, we know $G/Z \cong C_p \times C_p$, and that $G' = Z$. Now pick two elements, a and b so that aZ and bZ generate G/Z . So then $G = \langle Z, a, b \rangle$.

Let $z = [a, b]$. If $z = 1$ then that means a and b commute. And by definition, a commutes with Z , so $a \in Z$, which contradicts our choice of a as a generator of G/Z . Hence $z \neq 1$, and in particular, a and b do not commute. Now we know $G' = Z$ which has order p , so $Z \cong C_p$. Moreover, $z \in Z$, and $z \neq 1$ so we can conclude that $\langle z \rangle = Z$. We can see that although a and b are not in Z , a^p and b^p are, because aZ and bZ have order p in G/Z . Considering the orders of a and b we have 3 cases:

1. Groupprops, "Classification of groups of prime-cube order," February 24, 2016, accessed February 23, 2023, https://groupprops.subwiki.org/wiki/Classification_of_groups_of_prime-cube_order.

Case 1: Both a and b have order p .

The above descriptions give the presentation:

$$G = \langle z, a, b \mid z^p = a^p = b^p = 1, az = za, bz = zb, [a, b] = z \rangle$$

We can write an arbitrary $g \in G$ as $a^i b^j z^k$ for integers i, j and k taken mod p . Hence this presentation has order at most p^3 .

Now consider the set:

$$\left\{ \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix} \mid \alpha, \beta, \gamma \in \mathbb{F}_p \right\}$$

It can be shown that this is a group under the usual matrix multiplication, and is known as the unitriangular group², denoted $UT_3(p)$. Taking:

$$z = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

we can see that $UT_3(p)$ satisfies this presentation for $p > 2$. (Indeed, the above presentation is the standard presentation definition for $UT_3(p)$). Thus there is a single isomorphism class for this case.

The group behaves differently when $p = 2$ because we know that a group whose elements all have order either 1 or 2 is abelian. So the elements cannot have order only 1 or 2. In particular:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

have order 4. We can check that all other non-identity elements have order 2. Thus $UT_2(2) \cong D_8$.

Case 2: One element of each order p and p^2 .

The roles of a and b are interchangeable, so we can take a to have order p^2 and b to have order p without loss of generality. So $\langle a \rangle \cong C_{p^2}$, and has index p , so by Lemma 8 is normal. We noted that $a^p \neq 1$ is in Z , and so a^p is some power of z , say $a^p = z^r$, with r taken mod p .

We know that $0 < r < p$ and I claim that we can take $r = 1$ without loss of generality. This is because z^r is not 1, so must be some element of order p in Z . Hence z^r generates Z . Because p is prime, $Z \cong C_p$ is a finite field. Hence there exists some integer s , with $0 < s < p$ such that $sr \equiv 1 \pmod{p}$. Then say $\bar{a} = a^s$ so:

$$\bar{a}^p = (a^s)^p = (a^p)^s = (z^r)^s = z \pmod{p}$$

Indeed we can take \bar{a}^p to be any power of z we want using a similar substitution. This is actually a sneaky application of Lemma 5, because it will turn out that G can be written as a semidirect product.

2. Groupprops, “Unitriangular matrix group:UT(3,p),” August 22, 2014, accessed February 23, 2023, [https://groupprops.subwiki.org/wiki/Unitriangular_matrix_group:UT\(3,%20p\)](https://groupprops.subwiki.org/wiki/Unitriangular_matrix_group:UT(3,%20p)).

Take $a^p = z$. Now because $G = \langle z, a, b \rangle$, $\langle a \rangle \cap \langle b \rangle = \mathbf{1}$. So we can conclude that $G = \langle a \rangle \rtimes \langle b \rangle$. How does b conjugate a ? Consider:

$$a^{-1}b^{-1}ab = [a, b] = z = a^p$$

So:

$$b^{-1}ab = a^{p+1}$$

Thus:

$$G \cong C_{p^2} \rtimes C_p$$

With presentation:

$$\langle a, b \mid a^{p^2} = b^p = 1, b^{-1}ab = a^{p+1} \rangle$$

When $p = 2$, this reduces to the dihedral group, D_8 . However, we can see that for $p > 2$, this is not isomorphic to the previous case, because $\text{UT}_3(p)$ has no element of order p^2 .

Case 3: Both a and b have order p^2 .

We will show that by substitutions, this is equivalent to the above case when $p > 2$. In the previous case, we saw that we can take a^p and b^p to be arbitrary powers of z using substitutions (which is Lemma 5 behind the scenes). So take $a^p = z$ and $b^p = z^{-1}$. Let $d = ab$, and consider:

$$d^p = (ab)^p = abab \dots ab$$

We will collect together the a 's and b 's, maintaining equality with the commutator, $[a, b] = z$:

$$\begin{aligned} d^p &= ababab \dots ab \\ &= zaabbab \dots ab \\ &= z^2aababb \dots ab \\ &= z^3aaabbb \dots ab \\ &\vdots \\ &= z^{\frac{p(p-1)}{2}} a^p b^p \end{aligned} \tag{\dagger}$$

However, $z^p = 1$ so:

$$d^p = a^p b^p = zz^{-1} = 1$$

So d has order p , and we are back in the previous case.

If $p = 2$, (\dagger) does not hold, and the exponent of z is 1 in that case. So we have the relations:

$$a^4 = b^4 = z^2 = 1, \quad a^2 = z, \quad b^2 = z^{-1} \quad \text{and} \quad [a, b] = z$$

Therefore:

$$b^{-1}ab = az = a^3 = a^{-1}$$

So we obtain the presentation:

$$G = \langle a, b \mid a^4 = b^4 = 1, a^2 = b^2, b^{-1}ab = a^{-1} \rangle$$

Which we recognise as the quaternion group, Q_8 .

Hence any group of order p^3 is isomorphic to one of:

$$\begin{aligned} C_{p^3}, \quad C_{p^2} \times C_p, \quad C_p \times C_p \times C_p \\ D_8, \quad \text{or} \quad Q_8 \quad \quad \quad (\text{when } p = 2) \\ \text{UT}_3(p), \quad \text{or} \quad C_{p^2} \rtimes C_p \quad \quad \quad (\text{when } p \geq 3) \end{aligned}$$

Part II

Composite Orders

6 Groups of Order pq

Let G be a group of order pq where p, q are prime numbers with $p > q$, and let n_p and n_q denote the number of Sylow p -subgroups and Sylow q -subgroups of G respectively. Then by Sylow's Theorems:

$$\begin{aligned} n_p &\equiv 1 \pmod{p} \quad \text{and} \quad n_p \mid q \implies n_p = 1 \\ n_q &\equiv 1 \pmod{q} \implies n_q = 1, q+1, 2q+1, \dots \quad \text{and} \quad n_q \mid p \end{aligned}$$

So G has a unique Sylow p -subgroup, say $P \trianglelefteq G$, and a Sylow q -subgroup, $Q \leq G$. Because p and q are prime numbers, $P \cong C_p$ and $Q \cong C_q$. Pick generators for each, say $\langle x \rangle = P$ and $\langle y \rangle = Q$. We have 2 possibilities for n_q : $p-1$ is a multiple of q or 1.

Case 1: $q \nmid p-1$.

If $p-1$ is not a multiple of q then $n_q = 1$ and $Q \trianglelefteq G$, hence:

$$G = P \times Q \cong C_{pq}$$

Case 2: $q \mid p-1$.

If $p-1$ is a multiple of q then $n_q = p$ and so Q is not normal in G . By Lagrange's Theorem, $P \cap Q = 1$ and by Lemma 4, $|PQ| = pq$. Hence, as well as the direct product, we have $G = P \rtimes Q$, some non-trivial semidirect product.

By Lemma 2, $\text{Aut } C_p \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$. So if $\nu \in (\mathbb{Z}/p\mathbb{Z})^\times$, then $x \mapsto x^\nu$ is an automorphism. We know also that C_{p-1} has a unique subgroup of order q , hence G has the presentation:

$$G = \langle x, y \mid x^p = y^q = 1, y^{-1}xy = x^a \rangle$$

where a is a generator for the subgroup of order q in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Notice that picking different generators are equivalent up to isomorphism because the composition of two isomorphisms is an isomorphism.

So any group of order pq is isomorphic to either:

$$\begin{aligned} C_{pq} \quad \text{or} \quad \langle x, y \mid x^p = y^q = 1, y^{-1}xy = x^a \rangle \quad & \text{if } q \mid p-1 \\ C_{pq} \quad & \text{if } q \nmid p-1 \end{aligned}$$

6.1 Groups of Order $2p$

To illustrate an example of groups of order pq , let's take $q = 2$. Because every prime greater than 2 is odd, $p - 1$ is an even number, and so $2 \mid p - 1$.

An element $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order 2 satisfies $\alpha^2 = 1$, hence $\alpha = 1$ or -1 . But 1 has order 1, so α can only be -1 . Side-note: from the proof of Lemma 2, this corresponds to the inverse map.

So, in addition to C_{2p} , we have:

$$G \cong \langle x, y \mid x^p = y^2 = 1, y^{-1}xy = x^{-1} \rangle$$

Which is the presentation for the dihedral group of order $2p$, D_{2p} .

Hence a group of order $2p$ is isomorphic to one of:

$$C_{2p} \quad \text{or} \quad D_{2p}$$

7 Some Groups of Order p^2q

Let p and q be distinct prime numbers, and G be a group of order p^2q . To classify G in full generality is beyond this report, so we will focus on the cases when $p = 2$ and when $q = 2$.

7.1 $4q$

Let G be a group of order $4p$, and require $p > 3$. And let n_q denote the number of Sylow q -subgroups. The n_q must divide 4, so could be 1, 2 or 4, and must be congruent to 1 mod q . If $q = 3$, then G could have 4 Sylow q -subgroups, so we will classify groups of order 12 later. If $q = 2$, then we have a group of order p^3 , which we have already classified. This is why we took $q > 3$. So G has a normal Sylow q -subgroup, $Q \cong C_q$. Let x generate Q .

Lagrange's Theorem, together with Lemma 4, tell us that a Sylow 2-subgroup, T , intersects trivially with Q , and $|QT| = |G|$. Hence, $G = Q \rtimes T$.

We know by Lemma 2, that $\text{Aut } Q \cong C_{q-1}$. So we have two cases:

Case 1: $T \cong V_4$ i.e. $G \cong C_q \rtimes V_4$.

We saw in our classification of groups of order $2p$, that $(\mathbb{Z}/q\mathbb{Z})^\times$ has a unique element of order 2, corresponding to the inversion map. So Lemma 5 tells us that there is only a single non-trivial homomorphism $\psi : T \rightarrow \text{Aut } Q$.

If ψ is trivial, then we obtain the product:

$$G \cong C_q \times V_4 \cong C_{2q} \times C_2$$

If ψ is non-trivial, it maps T to the subgroup generated by the inversion map, isomorphic to C_2 . Therefore the kernel is isomorphic to C_2 , so pick z such that it generates the kernel. Denote the other generator of T by y , then we obtain the following presentation:

$$G = \langle x, y, z \mid x^q = y^2 = z^2 = 1, yz = zy, xz = zx, y^{-1}xy = x^{-1} \rangle$$

Now let $a = xz$, and in a similar calculation to when we classified groups of order 12, we will show that $G \cong D_{4p}$.

Firstly, notice that the order of a is $4q$, and:

$$a^q = x^q z^q = z \quad \text{and} \quad a^{q-1} = x^{q-1} z^{q-1} = x^{q-1}$$

Now consider:

$$y^{-1}ay = y^{-1}xzy = y^{-1}xyz = x^{-1}z = a^{q-1}a^q = a^{2q-1} = a^{-1}$$

Hence:

$$G = \langle a, y \mid a^{2q} = y^2 = 1, y^{-1}ay = a^{-1} \rangle$$

which we recognise as D_{4p} .

Case 2: $T \cong C_4$ i.e. $G \cong C_q \rtimes C_4$.

Let t generate T . Assume $4 \nmid q-1$, which means $q \equiv 3 \pmod{4}$. So then $\text{Aut } Q$ has no subgroup of order 4, and a homomorphism, ψ must map T to either the trivial group, or the group generated by the inverse automorphism.

If $T\psi$ is trivial, then we recover the direct product, $C_q \times C_4 \cong C_{4q}$.

If $T\psi$ is non-trivial, then G has the presentation:

$$G = \langle x, t \mid x^q = t^4 = 1, t^{-1}xt = x^{-1} \rangle$$

Let $a = xt^2$. Then:

$$a^q = xt^2 \dots xt^2 = x^qt^{2q} = t^{2q}$$

We know $q \equiv 3 \pmod{4}$, so for some n , $q = 4n + 3$. Thus $2q = 8n + 6 = 4(2n + 1) + 2$. So then:

$$a^q = t^{4(2n+1)+2} = t^2$$

Additionally:

$$t^{-1}at = t^{-1}xt^2t = (t^{-1}xt)t^2 = x^{-1}t^2 = t^2x^{-1} = a^{-1}$$

Hence:

$$G = \langle a, t \mid a^{2q} = 1, a^q = t^2, t^{-1}at = a^{-1} \rangle$$

This is known as the binary dihedral or dicyclic group, denoted Dic_{4q} ³.

If $4 \mid q-1$, i.e. $q \equiv 1 \pmod{4}$, then $\text{Aut } Q$ contains a unique element of order 4, and so has a unique subgroup generated by it. We know by Lemma 2, that $\text{Aut } Q \cong (\mathbb{Z}/q\mathbb{Z})^\times$, so say α is the generator of the subgroup of order 4 in $(\mathbb{Z}/q\mathbb{Z})^\times$. Our homomorphism can map T to this subgroup, and we get a group with the presentation:

$$G = \langle x, t \mid x^q = t^4 = 1, t^{-1}xt = x^\alpha \rangle$$

7.2 $2p^2$

Let G be a group of order $2p^2$, with $p > 2$. Denote the number of Sylow p -subgroups by n_p . By Sylow's Theorems, n_p divides 2, and is congruent to 1 mod p , so must be 1. Hence, G has a normal Sylow p -subgroup, P of order p^2 .

If T is a Sylow 2-subgroup, then by applying Lagrange's Theorem, and Lemma 4, we can conclude that $G = P \rtimes T$. From our classification of groups of order p^2 , we have 2 choices for P :

³. Groupprops, "Dicyclic Groups," October 21, 2017, accessed January 19, 2023, https://groupprops.subwiki.org/wiki/Dicyclic_group.

Case 1: $P \cong C_{p^2}$ i.e. $G \cong C_{p^2} \rtimes C_2$.

From Lemma 2, we know $|\text{Aut } P| = p^2 - p = p(p - 1)$. Because p is prime, $2 \nmid p$, but $2 \mid p - 1$, so $\text{Aut } P$ has a unique element of order 2. Hence, in addition to the direct product, $G \cong C_{2p^2}$, we have $G \cong C_{p^2} \rtimes C_2$, with C_2 acting by inversion. If x generates P , and y generates T , we have the presentation:

$$G = \langle x, y \mid x^{p^2} = y^2 = 1, y^{-1}xy = x^{-1} \rangle$$

which we recognise as D_{2p^2} , the dihedral group of order $2p^2$.

Case 2: $P \cong C_p \times C_p$ i.e. $G \cong C_p \times C_p \rtimes C_2$.

Consider P as the product of the subgroups generated by a and b , i.e. $P = \langle a \rangle \times \langle b \rangle$. Then the action of T on P can either be trivial on both subgroups, invert one, or invert both.

If the action is trivial on both subgroups, then we recover the direct product $G \cong C_p \times C_{2p}$.

If the action is non-trivial on just one of the subgroups, then we can consider only one case. This is because they are equivalent up to an isomorphism of T , and Lemma 5 tells us the resulting semidirect products are isomorphic. So we have:

$$G = \langle a \rangle \times (\langle b \rangle \rtimes T) \cong C_p \times D_{2p}$$

Finally, if we choose to invert both subgroups, then we act on all of P by inversion. So if a and b generate P , then:

$$G = \langle a, b, x \mid a^p = b^p = x^2 = 1, ab = ba, x^{-1}ax = a^{-1}, x^{-1}bx = b^{-1} \rangle$$

Because C_p has all elements of order p , excluding 1, and they are all automorphic to each other (meaning that some automorphism maps one to the other), $x^{-1}gx = g^{-1}$ for all $g \in P$. Hence:

$$G = \langle P, x \mid x^2 = 1, x^{-1}gx = g^{-1} \forall g \in P \rangle$$

which is known as the generalised dihedral group for C_p , denoted $\text{Dih}(C_p)$.

Part III

Special Cases

8 Groups of order 12

We have seen that groups of order 12 have slightly different behaviour to groups of order $4q$ in general, and we will need this classification in order to classify groups of order 24.

Let G be a group of order $12 = 2^2 \cdot 3$, and n_3 and n_2 denote the number of Sylow 3-subgroups and Sylow 2-subgroups of G respectively. By Sylow's Theorems:

$$n_2 \equiv 1 \pmod{2} \quad \text{and} \quad n_2 \mid 3 \implies n_2 = 1 \text{ or } 3$$

$$n_3 \equiv 1 \pmod{3} \quad \text{and} \quad n_3 \mid 4 \implies n_3 = 1 \text{ or } 4$$

Let H be a Sylow 2-subgroup and K be a Sylow 3-subgroup of G .

Lagrange's Theorem tells us H has elements of order 1, 2, and 4, and K has elements of order 1 and 3. Hence $H \cap K = \mathbf{1}$. Lemma 4 tells us:

$$|HK| = |H| \cdot |K| = 12$$

Hence $G = HK$, $H \trianglelefteq G$, and $H \cap K = \mathbf{1}$.

Since an automorphism, φ , must map generators to generators, $\text{Aut } C_4 \cong C_2$ because C_4 has two generators. An automorphism of V_4 corresponds to a permutation of the three non-identity elements, hence $\text{Aut } V_4 \cong S_3$.

If we consider G where $K \trianglelefteq G$, i.e. $G = K \rtimes H$, then we have two cases:

Case 1: $H \cong C_4$ i.e. $G \cong C_3 \rtimes C_4$.

Let $H = \langle y \rangle$.

We know $\text{Aut } C_3 \cong C_2$ so a homomorphism ψ maps H to the trivial group or to $\langle \beta : x \mapsto x^{-1} \rangle$.

If $H\psi = \mathbf{1}$ then $G = K \times H \cong C_4 \times C_3$, which we have already seen.

If $H\psi = \langle \beta \rangle$ then we have:

$$G = \langle x, y \mid x^3 = y^4 = 1, y^{-1}xy = x^{-1} \rangle$$

Now let $a = xy^2$. And remember, $y^{-1}xy = x^{-1}$ means x commutes with y^2 . So now:

$$a^3 = xy^2xy^2xy^2 = x^3y^6 = y^2$$

and

$$y^{-1}ay = y^{-1}xy^2y = (y^{-1}xy)y^2 = x^{-1}y^2 = y^2x^{-1} = a^{-1}$$

So:

$$G = \langle a, y \mid a^6 = 1, a^3 = y^2, y^{-1}ay = a^{-1} \rangle$$

which we recognise as Dic_{12} . This group is also sometimes denoted by T .

Case 2: $H \cong V_4$ i.e. $G \cong C_3 \rtimes (C_2 \times C_2)$.

If $\psi : H \rightarrow \text{Aut } K$ is trivial then we obtain the direct product again. We saw in our classification of groups of order $2p$, that $\text{Aut } K$ only has a single element of order 2, corresponding to the inverse map. So we have 3 choices of elements in H to send to it, but they are all equivalent up to isomorphism, by Lemma 5.

We know that $H/\text{im } \psi \cong \ker \psi$, so $\ker \psi$ must be isomorphic to C_2 . Pick z so that it generates the kernel, and so the remaining generator, y is not in the kernel. Then:

$$G = \langle x, y, z \mid x^3 = y^2 = z^2 = 1, yz = zy, xz = zx, y^{-1}xy = x \rangle$$

Let $a = xz$. The order of $a = \text{lcm}(\text{o}(x), \text{o}(z)) = \text{lcm}(2, 3) = 6$ because x and z commute. So:

$$a^3 = x^3z^3 = z$$

and

$$y^{-1}ay = y^{-1}xzy = y^{-1}xyz = x^{-1}z = x^2z = a^2a^3 = a^{-1}$$

Hence:

$$G = \langle y, a \mid a^6 = y^2 = 1, a^{-1}ay = a^{-1} \rangle \cong D_{12}$$

Instead, if G has 4 Sylow 3-subgroups, then there are 8 elements of order 3 in G . So the remaining 4 must form the Sylow 2-subgroup, hence it is normal.

Case 1: $H \cong C_4$ i.e. $G \cong C_4 \rtimes C_3$.

Let $H = \langle y \rangle$.

A homomorphism $\psi : K \rightarrow \text{Aut } H \cong C_2$, preserves order and together with Lagrange's Theorem means that the only possibility for ψ is trivial, i.e. $K\psi = \mathbf{1}$.

Hence $G \cong C_4 \times C_3 \cong C_{12}$.

Case 2: $H \cong V_4$ i.e. $G \cong (C_2 \times C_2) \rtimes C_3$.

Let $H = \langle y, z \rangle$.

A trivial homomorphism $K\psi = \mathbf{1}$ yields the direct product. What non-trivial homomorphisms are there? The automorphism group, $\text{Aut } H \cong S_3$ is of order 6, and so has a unique subgroup of order 3, by Sylow's Theorems. We know that a homomorphism $\psi : K \rightarrow \text{Aut } H$ is determined by where it sends the generator x , so for ψ to be non-trivial, it must send x to an element of order 3 in $\text{Aut } H$.

There are 2 such elements. Because $\text{Aut } H \cong S_3$, we will think of them as the permutations of order 3 of the set $\{1, 2, 3\}$. Denote them $a = (1\ 2\ 3)$ and $b = (1\ 3\ 2)$. Notice that $b = a^{-1}$, so we have homomorphisms:

$$\psi_1 : x \mapsto a \quad \text{and} \quad \psi_2 : x \mapsto a^{-1}$$

It appears we have 2 choices, but this is not the case. The inverse map, $\beta : x \mapsto x^{-1}$, is an automorphism of K , and so by Lemma 5, the corresponding semidirect products of ψ_1 and ψ_2 are isomorphic. Hence (up to isomorphism) there is one non-trivial homomorphism $\psi : K \rightarrow \text{Aut } H$. So $x \in K$ acts by permuting the 3 non-identity elements of H .

We will show that in this case, $G \cong A_4$. First, let's check A_4 has the same subgroup structure as G . There is a subgroup isomorphic to C_3 in A_4 , generated by the 3-cycle $(1\ 2\ 3)$:

$$\bar{K} = \langle (1\ 2\ 3) \rangle$$

We can also find a subgroup isomorphic to V_4 :

$$\bar{H} = \{ 1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \}$$

Indeed, we can check that \bar{H} is normal in A_4 . We can see that $\bar{H} \cap \bar{K} = \mathbf{1}$ because \bar{H} contains no 3-cycles, and that $\bar{H}\bar{K} = A_4$. So we can conclude that $A_4 = \bar{H} \rtimes \bar{K}$.

Let's investigate how conjugation behaves. If we let $\alpha = (1\ 2)(3\ 4)$, $\beta = (1\ 4)(2\ 3)$ and $\gamma = (1\ 2\ 3)$, then we can write an element of A_4 as $\alpha^i \beta^j \gamma^k$ for some i, j and k . Define $\phi : A_4 \rightarrow G$ by $\phi : \alpha^i \beta^j \gamma^k \mapsto x^i y^j z^k$. Then:

$$\beta\phi = (\gamma^{-1}\alpha\gamma)\phi = c^{-1}ac = b$$

So conjugation acts in the same way. Hence we can conclude that $G \cong A_4$.

So a group G of order 12 is isomorphic to one of:

$$C_{12}, \quad C_2 \times C_6, \quad A_4, \quad D_{12}, \quad \text{or} \quad \text{Dic}_{12}$$

9 Groups of Order 24

Let G be a group of order 24, and let H be a Sylow 3-subgroup of G , so $H \cong C_3$, and let h generate H . Let T be a Sylow 2-subgroup of G , so T has order 8. By Lagrange's Theorem, $H \cap T = \mathbf{1}$ and then applying Lemma 4, $|HT| = 24$. Now let n_3 denote the number of Sylow 3-subgroups, and by Sylow's Theorems:

$$n_3 \equiv 1 \pmod{3} \quad \text{and} \quad n_3 \mid 8$$

Hence n_3 is either 1 or 4.

If $n_3 = 1$, then H is normal in G . Thus $G = H \rtimes T$. We'll want a homomorphism $\psi : T \rightarrow \text{Aut } H$. We know $\text{Aut } H \cong C_2$, and from our classification of groups of order 8, we have 5 possibilities. An action of T on H will have image isomorphic to C_2 , and a kernel isomorphic to a group of order 4. We can classify the possible actions by considering the kernel.

Case 1: $T \cong C_8$ i.e. $G \cong C_3 \rtimes C_8$.

Let t generate T , and so its unique subgroup of order 4 is generated by t^2 . Hence $\langle t^2 \rangle$ is the kernel of ψ , so ψ must send t to the identity or inversion map. Hence a non-trivial action of T on H is unique. If the action is trivial, then:

$$G = T \times H \cong C_{24}$$

Otherwise we obtain:

$$G = \langle h, t \mid h^3 = t^8 = 1, h^{-1}th = t^{-1} \rangle \cong C_3 \rtimes C_8$$

Case 2: $T \cong (C_4 \times C_2)$ i.e. $G \cong C_3 \rtimes (C_4 \times C_2)$.

In this case, T has subgroups isomorphic to both C_4 and $C_2 \times C_2$, so we have more possibilities for ψ . Firstly, if ψ is trivial, then we obtain the direct product:

$$G \cong C_3 \times C_4 \times C_2$$

Let T be generated by x and y , where $x^4 = y^2 = 1$, and consider non-trivial ψ . Say the kernel of ψ is isomorphic to $C_2 \times C_2$. So it must be generated by the elements of order 2 in T : x^2 and y . Then ψ must map x to the non-identity element in $\text{Aut } H$, inversion. Hence $\langle x \rangle$ acts by inversion on H , giving:

$$\begin{aligned} G &= (H \rtimes \langle x \rangle) \times \langle y \rangle \\ &\cong (C_3 \rtimes C_4) \times C_2 \\ &\cong \text{Dic}_{12} \times C_2 \end{aligned}$$

If instead the kernel is isomorphic to C_4 , then it must be generated by an element of order 4 from T . However, all elements of order 4 are automorphic, and so by Lemma 5, we can pick x to generate the kernel, without loss of generality. So then ψ must map y to inversion. Hence $\langle x \rangle$ acts trivially on H , and $\langle y \rangle$ acts by inversion. Thus:

$$\begin{aligned} G &= (H \rtimes \langle y \rangle) \times \langle x \rangle \\ &\cong (C_3 \rtimes C_2) \times C_4 \\ &\cong S_3 \times C_4 \end{aligned}$$

Case 3: $T \cong (C_2 \times C_2 \times C_2)$ i.e. $G \cong C_3 \rtimes (C_2 \times C_2 \times C_2)$.

Let $\langle a, b, c \rangle = T$. All elements in T have order 1 or 2, so cannot have subgroups isomorphic to C_4 . However, T does have subgroups isomorphic to $C_2 \times C_2$, which can be generated by 2 of the three generators of T . This gives us 3 subgroups, but permuting the generators a, b and c is an automorphism of T , so Lemma 5 tells us the resulting semidirect products are isomorphic. So choose ψ such that b and c are in the kernel. Then $a\psi$ is either the identity map or the inversion map. If ψ is trivial, then we obtain the direct product:

$$G \cong C_3 \times C_2 \times C_2 \times C_2$$

If $a\psi$ is inversion, then:

$$G = (C_3 \rtimes \langle a \rangle) \times \langle b \rangle \times \langle c \rangle \cong S_3 \times C_2 \times C_2$$

Case 4: $T \cong D_8$ i.e. $G \cong C_3 \rtimes D_8$.

Let r and s generate T with $r^4 = s^2 = 1$. A trivial homomorphism will yield the direct product:

$$G \cong C_3 \times D_8$$

So for a non trivial homomorphism, firstly assume $\ker \psi \cong C_4$. There is a unique subgroup in T isomorphic to C_4 , so it's generated by an element of order 4. However the choice of generator is the same up to an isomorphism of T , so Lemma 5 lets us pick r to be the generator, without loss of generality. Hence s cannot be in the kernel, and so $s\psi$ is the inversion map. We obtain the presentation:

$$G = \langle x, r, s \mid x^3 = r^4 = s^2 = 1, xr = rx, s^{-1}rs = r^{-1}, s^{-1}xs = x^{-1} \rangle$$

Let $a = xr$, and consider:

$$s^{-1}as = s^{-1}xrs = s^{-1}xrs^2s^{-1} = (s^{-1}xs)(srs^{-1}) = x^{-1}r^{-1} = r^{-1}x^{-1} = a^{-1}$$

So we have:

$$G = \langle a, s \mid a^{12} = s^2 = 1, s^{-1}as = a^{-1} \rangle$$

Which we recognise as D_{24} , the dihedral group of order 24.

If instead we consider ψ with kernel isomorphic to $C_2 \times C_2$, then the kernel is generated by two elements of order 2. However, T only has two elements of order 2, r^2 and s , so they must generate the kernel. So then ψ must map r to inversion. Hence this action is fully specified. So:

$$G \cong C_3 \rtimes_{V_4} D_8$$

We will use the above notation to mean the unique action with kernel isomorphic to V_4 .

Case 5: $T \cong Q_8$ i.e. $G \cong C_3 \rtimes Q_8$.

Let T be generated by i and j , with the product denoted by k . That is:

$$T = \langle i, j \mid i^4 = j^4 = 1, i^2 = j^2, j^{-1}ij = i^{-1} \rangle$$

There is a single element of order 2 in T , hence T has no subgroup isomorphic to $C_2 \times C_2$. The elements i, j and k each generate a cyclic subgroup in T . So ψ will

send one of them to the kernel. We know that permuting these is an automorphism of T , so Lemma 5 tells us the choice results in isomorphic semidirect products.

So take $i \in \ker \psi$. Indeed $\langle i \rangle = \ker \psi$. Then for a non-trivial homomorphism, we must have $j \notin \ker \psi$. Otherwise:

$$i\psi \ j\psi = (ij)\psi = k\psi \in \ker \psi$$

making ψ trivial.

Thus either ψ is trivial and we obtain:

$$G \cong C_3 \times Q_8$$

or ψ maps j to the inversion map and we obtain the presentation:

$$G = \langle x, i, j \mid x^3 = i^4 = j^4 = 1, \ xi = ix, \ i^2 = j^2, \ j^{-1}xj = x^{-1}, \ j^{-1}ij = i^{-1} \rangle$$

Now let $a = xi$. So:

$$a^6 = x^6 i^6 = i^2 = j^2$$

And:

$$j^{-1}aj = j^{-1}xij = j^{-1}xji^{-1} = x^{-1}i^{-1} = i^{-1}x^{-1} = a^{-1}$$

Hence:

$$G = \langle a, j \mid a^{12} = 1, \ a^6 = j^2, \ j^{-1}aj = a^{-1} \rangle$$

We recognise this as the dicyclic group of order 24, Dic_{24} .

If $n_3 = 4$ then H is not normal. We will proceed to show that G must have a normal Sylow 2-subgroup in a similar way to Borchers⁴.

The normaliser of H , $N_G(H)$ has index 4. Now let G act on the set of the cosets of $N_G(H)$ by conjugation. Hence we obtain a homomorphism $\rho : G \rightarrow S_4$. The kernel is a subgroup of $N_G(H)$ so must have order dividing 6 by Lagrange's Theorem.

The kernel cannot be of order 3, because G has no normal subgroup of order 3 (because kernels of homomorphism are normal in the domain group). Likewise the kernel cannot be of order 6 because every group of order 6 has a unique Sylow 3-subgroup, which is characteristic. So by Lemma 3, it would be normal in G . Hence the kernel must have order 1 or 2.

If the kernel is of order 1, then ρ is an isomorphism, so $G \cong S_4$.

If the kernel is of order 2, then we know that $G/\ker \rho \cong \text{im } \rho$, so then $\text{im } \rho$ must have order 12. It also cannot have a normal Sylow 3-subgroup, so looking at our classification of groups of order 12, this must be isomorphic to A_4 . We know that A_4 has a normal subgroup of order 4, and so by the Correspondence Theorem, G must contain a normal subgroup of order 8, say T . By Lagrange's Theorem and Lemma 4, we can conclude that $G = T \rtimes H$. Again, we have 5 cases, but this time we'll exclude the trivial homomorphism, because that will just give us the direct product which we have already seen:

Case 1: $T \cong C_8$ i.e. $G \cong C_8 \rtimes C_3$.

An automorphism of T , φ , maps generators to generators, so say $\langle x \rangle = T$. Then $x\varphi$ could be x, x^3, x^5 or x^7 . Notice that each of these, apart from $\varphi : x \mapsto x$, has order 2. Hence, and Lagrange's Theorem tells us that there are no non-trivial homomorphisms $\psi : H \rightarrow \text{Aut } T$. As a bonus: $\text{Aut } C_8 \cong V_4$.

4. Richard E. Borchers, "Group theory 21: Groups of order 24," June 30, 2020, accessed February 9, 2023, <https://www.youtube.com/watch?v=6TWuo2NO8vg>.

Case 2: $T \cong (C_4 \times C_2)$ i.e. $G \cong (C_4 \times C_2) \rtimes C_3$.

An automorphism of T , ψ preserves element order, so if $\langle x, y \mid x^4 = y^2 = 1, xy = yx \rangle = T$, then $x\psi$ must be of order 4, and $y\psi$ must be of order 2. Moreover, $y\psi$ cannot be in $\langle x\psi \rangle$ because ψ is injective.

So we are reduced to 2 possible choices for $y\psi$, and 4 possible choices for $x\psi$. Because an automorphism is determined by its effect on generators, this gives us 8 possible automorphisms. Hence $|\text{Aut } T| = 8$, and Lagrange's Theorem tells us that there are no non-trivial homomorphisms $\psi : H \rightarrow \text{Aut } T$.

Case 3: $T \cong (C_2 \times C_2 \times C_2)$ i.e. $G \cong (C_2 \times C_2 \times C_2) \rtimes C_3$.

To determine $\text{Aut } T$ it is helpful to think of C_2 as the finite field with two elements. Then T is isomorphic a 3 dimensional vector space over two elements. So an automorphism of that vector space is just any linear map, with non-zero determinant. Thus, $\text{Aut } T \cong \text{GL}_3(2)$.

We can determine that $|\text{GL}_3(2)| = 168 = 2^3 \cdot 3 \cdot 7$, so $\text{Aut } T$ has a Sylow 3-subgroup of order 3, isomorphic to C_3 .

Sylow's Theorems tells us that all subgroups of order 3 are conjugate, so Lemma 5 tells us there is only one unique action (up to isomorphism) of H on T . As before, pick a homomorphism, ψ , which will let us easily classify the resulting semidirect product.

Write $T = A \times B$ where $A \cong C_2$ and $B \cong C_2 \times C_2$. Then let ψ map H to the subgroup generated by the automorphism which fixes A and permutes the non-identity elements of B in a 3-cycle. This automorphism has order 3 by construction, so we can write:

$$G \cong C_2 \times (V_4 \rtimes C_3)$$

We know already that $V_4 \rtimes C_3 \cong A_4$, so $G \cong C_2 \times A_4$.

Case 4: $T \cong D_8$ i.e. $G \cong D_8 \rtimes C_3$.

Let $\langle s, r \mid s^2 = r^4 = 1, s^{-1}rs = r^{-1} \rangle = T$. An automorphism, ψ , of T preserves element order, so for $r\psi$ we have two choices, r or r^{-1} . We can send $s\psi$ to any element of order 2 which is not in $\langle r\psi \rangle$. This leaves only reflections, of which there are 4: s, rs, r^2s and r^3s . Hence there are 8 possible automorphisms of D_8 , so $|\text{Aut } D_8| = 8$. Lagrange's Theorem tells us that there are no non-trivial homomorphisms $\psi : H \rightarrow \text{Aut } T$.

Case 5: $T \cong Q_8$ i.e. $G \cong Q_8 \rtimes C_3$.

Firstly, because of the multiplication structure of the quaternions, the image of k is determined by the images of i and j ; it is forced. This reduces the possibilities for an automorphism. Additionally, ± 1 are fixed by an automorphism, because they are the only elements of their order. So an automorphism could send i to any of the remaining 6 elements of order 4. The image of j cannot be in the subgroup generated by the image of i , otherwise we wouldn't have an automorphism. Thus there are 4 choices for the image of j , giving us 24 possible automorphisms altogether.

So $\text{Aut } T$ will have a Sylow subgroup of order 3.

Somehow show this is $\text{SL}_2(\mathbb{F}_3)$.

10 Groups of Order 30

This classification is based on the one given in the cited Stack Exchange post⁵. Let G be a group of order $30 = 2 \cdot 3 \cdot 5$. So then G has a Sylow 3-subgroup, T , and a Sylow 5-subgroup, F . Let $H = TF$ and by Lagrange's Theorem, $T \cap F = \mathbf{1}$, hence $|H| = 15$ by Lemma 4. We know from our classification of groups of order pq that $H \cong C_{15}$. Because $|H| = 15 = \frac{30}{2}$, the index of H in G is 2, and we know a subgroup of index 2 is normal, so $H \trianglelefteq G$.

Notice that a Sylow 2-subgroup $K \leq G$ has order 2, so $K \cong C_2$. Let $\langle k \rangle = K$ and $\langle h \rangle = H$. By the same argument as above, $H \cap K = \mathbf{1}$ and $|HK| = 30$. Hence $G = HK$. Moreover, $G = H \rtimes K$.

By Lemma 2:

$$\text{Aut } C_{15} = (\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \cong C_2 \times C_4$$

A homomorphism, $\psi : C_2 \rightarrow C_2 \times C_4$ preserves element order and we know ψ is determined by it's effect on a generator. So then $k\psi$ has four possibilities: either the identity, or one of the three elements of order 2.

Additionally, ψ preserves the Sylow subgroups of H . So write $H = \langle h^3 \rangle \times \langle h^5 \rangle$, the direct product of its Sylow subgroups.

So the action of K on H is either trivial or by inversion on each of the Sylow subgroups of H , giving us 4 possibilities:

Case 1: Trivial action on both Sylow subgroups.

In this case, because the action is trivial on all of H , we recover the direct product, $G = H \times K \cong C_{30}$.

Case 2: Inversion on both Sylow subgroups.

Here, K acts on all of H , so we obtain:

$$G = \langle h, k \mid h^{15} = k^2 = 1, k^{-1}hk = h^{-1} \rangle$$

which we recognise as D_{30} .

Case 3: Inversion on $\langle h^5 \rangle$.

We know already, from our classification of groups of order $2p$, that $C_3 \rtimes C_2 \cong D_6$. So then because the action on $\langle h^3 \rangle$ is trivial:

$$G = \langle h^3 \rangle \times (\langle h^5 \rangle \rtimes K) \cong C_5 \times D_6$$

Case 4: Inversion on $\langle h^3 \rangle$.

Similar to above, we obtain:

$$G = \langle h^5 \rangle \times (\langle h^3 \rangle \rtimes K) \cong C_3 \times D_{10}$$

Hence any group of order 30 is isomorphic to one of:

$$C_{30}, \quad D_{15}, \quad C_5 \times D_6, \quad \text{or} \quad C_3 \times D_{10}$$

5. Stack Exchange (user azimut), "Classification of groups of order 30 (duplicate)," December 10, 2020, accessed January 24, 2023, <https://math.stackexchange.com/questions/569226/classification-of-groups-of-order-30>.

11 Groups of Order 16

The following classification is based of the one by Wild⁶. We begin by proving a lemma:

Lemma 11. *For a group, G , with order 16, not isomorphic to $C_2 \times C_2 \times C_2 \times C_2$, then G has a normal subgroup isomorphic to either C_8 or $C_4 \times C_2$.*

Proof. Firstly, we know that a subgroup with index 2 is normal, so any subgroup of order 8 in G is normal. So it remains to show G possesses such subgroups. If some $x \in G$ has order 8, then $\langle x \rangle \cong C_8$ and we are done. So assume G has no element of order 8.

Because $G \not\cong (C_2)^4$, there is at least one element of order 4 in G , say y . By Lemma 9, there is some element $z \in Z(G)$ which has order 2. Let $H = \langle z \rangle$. Moreover, $H \trianglelefteq G$ because z is in the centre.

If $y^2 \neq z$, then $\langle y \rangle \cap H = \mathbf{1}$, so $\langle y, z \rangle \cong C_4 \times C_2$.

If then all elements of order 4 in G have $y^2 = z$, all elements in G/H have order 2. Thus $G/H \cong (C_2)^3$, and in particular, is abelian. So the conjugacy class of y , y^G is a subgroup of yH . Hence the centraliser of y , $C_G(y)$, has order 8.

Let $g \in C_G(y) \setminus \langle y \rangle$. If g has order 2, then $\langle y, g \rangle \cong C_4 \times C_2$. If g has order 4, then:

$$g^2 = z \quad \text{and} \quad (yg)^2 = y^2 g^2 = z^2 = 1$$

We can see that $yg \notin \langle y \rangle$ because then, $yg = y^2$ which gives the contradiction $y = g$. So $\langle y, yg \rangle \cong C_4 \times C_2$. □

6. Marcel Wild, "The Groups of Order Sixteen Made Easy," The American Mathematical Monthly 112, no. 1 (2005): 20–31, ISSN: 00029890, 19300972, accessed February 27, 2023, <http://www.jstor.org/stable/30037381>.

References

- Borcherds, Richard E. “Group theory 21: Groups of order 24,” June 30, 2020. Accessed February 9, 2023. <https://www.youtube.com/watch?v=6TWuo2NO8vg>.
- Groupprops. “Classification of groups of prime-cube order,” February 24, 2016. Accessed February 23, 2023. https://groupprops.subwiki.org/wiki/Classification_of_groups_of_prime-cube_order.
- . “Dicyclic Groups,” October 21, 2017. Accessed January 19, 2023. https://groupprops.subwiki.org/wiki/Dicyclic_group.
- . “Unitriangular matrix group:UT(3,p),” August 22, 2014. Accessed February 23, 2023. [https://groupprops.subwiki.org/wiki/Unitriangular_matrix_group:UT\(3,%20p\)](https://groupprops.subwiki.org/wiki/Unitriangular_matrix_group:UT(3,%20p)).
- Stack Exchange (user azimuth). “Classification of groups of order 30 (duplicate),” December 10, 2020. Accessed January 24, 2023. <https://math.stackexchange.com/questions/569226/classification-of-groups-of-order-30>.
- Wild, Marcel. “The Groups of Order Sixteen Made Easy.” *The American Mathematical Monthly* 112, no. 1 (2005): 20–31. ISSN: 00029890, 19300972, accessed February 27, 2023. <http://www.jstor.org/stable/30037381>.