Classification of Finite Groups

Daniel Laing

February 2, 2023

Contents

Part I
Done

1 Groups of Order 6

Let G be a group of order 6, and n_3 denote the number of Sylow 3-subgroups of G. Then by Theorem 5.3:

$$n_3 \equiv 1 \pmod 3 \quad \text{and} \quad n_3 \mid 2 \implies n_3 = 1$$

So G has one Sylow 3-subgroup, N, and because 3 is prime, it is isomorphic to C_3. Let $N = \langle x \rangle$. Any Sylow 2-subgroup, $H \leqslant G$, will have order 2, and so $H \cong C_2$. Let $H = \langle y \rangle$. Lagrange's Theorem tells us that N has elements of orders 1 and 3, and H has elements of order 1 and 2 hence:

$$N \cap H = \mathbf{1}$$

By Lemma 5.7:

$$|NH| = \frac{|N| \cdot |H|}{|N \cap H|} = \frac{3 \cdot 2}{1} = 6$$

So $G = NH$, $N \trianglelefteq G$ and $N \cap H = \mathbf{1}$, which means $G = N \rtimes H$, the semidirect product of N by H.

Now we need to determine $\operatorname{Aut} N$. An automorphism, φ of N preserves element order. In particular, φ maps generators to generators. Hence, $x\varphi = x$ or x^2 because they are the generators of N. So $\operatorname{Aut} N \cong C_2$.

Now we want a homomorphism $\psi : H \to \operatorname{Aut} N$. If ψ is trivial, then it maps H to the trivial group, so every element of H gets sent to the trivial automorphism. If ψ is not trivial, then at least one element of H is not sent to the trivial automorphism. It cannot be 1 because then element order is not preserved, so it must be the generator, y. Hence we obtain 2 possibilities for G:

Case 1:

$$\begin{aligned} G &= \langle\, x, y \mid x^3 = y^2 = 1,\ y^{-1}xy = x \,\rangle \\ &= \langle\, x, y \mid x^3 = y^2 = 1,\ xy = yx \,\rangle \\ &= C_3 \times C_2 \cong C_6 \end{aligned}$$

Case 2:

$$\begin{aligned} G &= \langle\, x, y \mid x^3 = y^2 = 1,\ y^{-1}xy = x^{-1} \,\rangle \\ &\cong D_6 \end{aligned}$$

These are clearly not isomorphic, because C_6 is abelian, and D_6 is not.

Hence G is isomorphic one of:

$$C_6 \quad \text{or} \quad D_6$$

2 Generalisation to Groups of Order $2p$

Now that we have seen groups of order 6, let's try and work towards a more general case: groups of order 2 times a prime number. So let G be a group of order $2p$ where p is a prime number, and n_p denote the number of Sylow p-subgroups of G. Then by Theorem 5.3:

$$n_p \equiv 1 \pmod p \quad \text{and} \quad n_p \mid 2 \implies n_p = 1$$

So G has one Sylow p-subgroup, say N, and it is isomorphic to C_p. Let $N = \langle x \rangle$. A Sylow 2-subgroup, $H \leqslant G$ will have order 2 so $H \cong C_2$. Let $H = \langle y \rangle$. Lagrange's Theorem tells us that N has elements of orders 1 and p, and H has elements of order 1 and 2 hence:

$$N \cap H = \mathbf{1}$$

By Lemma 5.7:

$$|NH| = \frac{|N| \cdot |H|}{|N \cap H|} = \frac{p \cdot 2}{1} = 2p$$

So $G = N \rtimes H$ as before.

We know by Lemma 5.8 that $\operatorname{Aut} N \cong \mathbb{Z}/p\mathbb{Z}^*$, so let's look for the elements of order 2. An element $x \in \mathbb{Z}/p\mathbb{Z}^*$ of order 2 satisfies $x^2 = 1$, hence $x = 1$ or -1. But 1 has order 1, so x can only be -1. From the proof of Lemma 5.8, this corresponds to the inverse map $\beta : x \mapsto x^{-1}$.

Now we want a homomorphism $\psi : H \to \operatorname{Aut} N$. By the same argument as for groups of order 6, we have two possibilities for G:

Case 1:

$$\begin{aligned} G &= \langle\, x, y \mid x^p = y^2 = 1,\ y^{-1}xy = x \,\rangle \\ &= C_p \times C_2 \cong C_{2p} \end{aligned}$$

Case 2:

$$\begin{aligned} G &= \langle\, x, y \mid x^p = y^2 = 1,\ y^{-1}xy = x^{-1} \,\rangle \\ &\cong D_{2p} \end{aligned}$$

Again, these are clearly not isomorphic, because C_{2p} is abelian, and D_{2p} is not.

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

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

3 Groups of order 4

From the Fundamental Theorem of Finite Abelian Groups, we know that a group G of order 4 could be isomorphic to one of C_4 and $C_2 \times C_2$. Now to show that these are the only possibilities. The Sylow theorems are not so helpful here, because any Sylow 2-subgroup will be of order 4, which is just G. Lagrange's Theorem tells us every element of G has order 1, 2 or 4.

If $x \in G$ has order 4, then x generates G so $G \cong C_4$.

If instead there is no element of order 4 in G, then every $x \in G$ except the identity is of order 2. Consider $a, b \in G$ with $a \neq b$, and their product, ab. It must be that ab is the third element of order 2, otherwise we reach a contradiction. So it is easy to see that $G \cong C_2 \times C_2$.

So any group of order 4 is isomorphic to one of:

$$C_4 \quad \text{or} \quad C_2 \times C_2$$

4 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 Theorem 5.3:

$$n_p \equiv 1 \pmod p \quad \text{and} \quad n_p \mid q \implies n_p = 1$$

$$n_q \equiv 1 \pmod q \implies n_q = 1,\ q+1,\ 2q+1,\ \ldots \quad \text{and} \quad n_q \mid p$$

So $C_p \trianglelefteq G$ and we have 2 possibilities for C_q: $p-1$ is a multiple of q or 1.

Let $\langle x \rangle = C_p$ and $\langle y \rangle = C_q$.

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

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

$$G = C_p \times C_q \cong C_{pq}$$

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

If $p-1$ *is* a multiple of q then $n_q = p$ and so $C_q \leqslant G$. By Lagrange's Theorem, $C_p \cap C_q = \mathbf{1}$ and by Lemma 5.7, $|C_pC_q| = pq$, hence, as well as the direct product, we have $G = C_p \rtimes C_q$.

By Lemma 5.8, $\operatorname{Aut} C_p \cong \mathbb{Z}/p\mathbb{Z}^* \cong C_{p-1}$, so if $\nu \in \mathbb{Z}/p\mathbb{Z}^*$, 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:

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

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

Notice that picking different generators are equivalent up to isomorphism.

So any group of order pq is isomorphic to either:

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

Part II
In Progress

5 Theorems and Lemmas

5.1 Sylow Theorems

Let G be a group of order $p^n m$ where p is a prime and $p \nmid m$.

Theorem 5.1 (1st Sylow Theorem)**.** *G has a Sylow p-subgroup, i.e. a subgroup of order p^n.*

Theorem 5.2 (2nd Sylow Theorem)**.** *All Sylow p-subgroups of G are conjugate to each other.*

Corollary 5.2.1. *If $n_p = 1$ then the Sylow p-subgroup is normal in G.*

Theorem 5.3 (3rd Sylow Theorem)**.** *Let n_p denote the number of Sylow p-subgroups of G. Then:*

(i) $n_p \mid m$

(ii) $n_p \equiv 1 \pmod p$

5.2 Isomorphism Theorems

Theorem 5.4.

Theorem 5.5.

Theorem 5.6.

Lemma 5.7. *For a group G with $N \leqslant G$ and $H \leqslant G$, then*

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

Lemma 5.8. *The automorphism group of C_n is isomorphic to the multiplicative group of integers mod n.*

i.e. $\operatorname{Aut} C_n \cong \mathbb{Z}/n\mathbb{Z}^*$

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. Consider:

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

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

Now consider $\theta : \operatorname{Aut} C_n \to \mathbb{Z}/n\mathbb{Z}^*$ defined by $\varphi_k\theta = k$. We will show θ is an isomorphism. Every $k \in \mathbb{Z}/n\mathbb{Z}^*$ is co-prime to n and so x^k is a generator of C_n, hence there is some $\varphi_k \in \operatorname{Aut} C_n$ such that $\varphi_k\theta = k$. So θ is surjective. If $\varphi_k, \varphi_l \in \operatorname{Aut} C_n$ such that $\varphi_k\theta = \varphi_l\theta$ 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 $\theta : \operatorname{Aut} C_n \to \mathbb{Z}/n\mathbb{Z}^*$ is an isomorphism.

□

6 Generalisation to Groups of Order p^2

Let G be a group of order p^2 and consider $\mathrm{Z}(G) \trianglelefteq G$. By Lagrange's Theorem, $\mathrm{Z}(G)$ has order 1, p or p^2.

If $|\mathrm{Z}(G)| = p^2$ then G is abelian.

Assume $|\mathrm{Z}(G)| \neq p^2$ and consider an element $x \in G$ but $x \notin \mathrm{Z}(G)$, and it's centraliser, $\mathrm{C}_G(x)$. We know $\mathrm{C}_G(x) \leqslant G$ and that $x \in \mathrm{C}_G(x)$, so $|\mathrm{C}_G(x)| \neq 1$, and so by Lagrange's Theorem, it must be that $|\mathrm{C}_G(x)| = p$. So:

$$|x^G| = |G : \mathrm{C}_G(x)| = \frac{p^2}{p} = p$$

The Class Equation, $|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{k} |x_i^G|$, tells us $|\mathrm{Z}(G)|$ must be a multiple of p because both $|G|$ and $|x^G|$ are multiples of p. Hence $|\mathrm{Z}(G)| = p$.

So then $|G : \mathrm{Z}(G)| = p$, which means $G/\mathrm{Z}(G) \cong C_p$.

Sketch

- Show G must be abelian. Result follows from FTFAB.
- $\mathrm{Z}(G)$ has order 1, p, or p^2 by Lagrange.
- If p^2 then done.
- Size of congruencty classies is multiple of p.
- Class eqn => order of centre is multiple of p. (and so is not 1)
- Quotient with G is cyclic.
- MT4003 showed then G must be abelian.

7 Groups of order 12

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 Theorem 5.3:

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

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

G has a unique Sylow 2-subgroup of order $2^2 = 4$, say $H \trianglelefteq G$, and we have already classified groups of order 4, so either C_4 or $V_4 \trianglelefteq G$. A Sylow 3-subgroup of G will have order 3, so $C_3 \leqslant G$, and for some groups, $C_3 \trianglelefteq G$.

Lagrange's Theorem tells us H has elements of order 1, 2, and 4, and C_3 has elements of order 1 and 3. Hence $H \cap C_3 = \mathbf{1}$.

Lemma 5.7 tells us:

$$|HC_3| = \frac{|H| \cdot |C_3|}{|H \cap C_3|} = 12$$

Hence $G = HC_3$, $C_3 \leqslant G$, $H \trianglelefteq G$, and $H \cap C_3 = \mathbf{1} \implies G = H \rtimes C_3$.

Since an automorphism, φ, must map generators to generators, $\operatorname{Aut} C_4 \cong C_2$ because the generators of C_4 are x and x^{-1}. An automorphism of V_4 corresponds to a permutation of the three non-identity elements, hence $\operatorname{Aut} V_4 \cong S_3$.

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

A homomorphism $\psi : C_3 \to \operatorname{Aut} C_4 \cong C_2$, preserves order and together with Lagrange's Theorem means that the only possibility for ψ is trivial, i.e. $C_3\psi = \mathbf{1}$.

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

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

A trivial homomorphism $C_3\psi = \mathbf{1}$ yields the direct product $G \cong C_2 \times C_2 \times C_3 \cong C_2 \times C_6$.

S_3 has one subgroup of order 3, hence there is essentially only one homomorphism $\psi : C_3 \to \operatorname{Aut} V_4$.

Still need to show this is A_4.

If we instead consider G where $C_3 \trianglelefteq G$, i.e. $G = C_3 \rtimes H$, then we again have two cases:

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

Say $C_3 = \langle x \rangle$ and $C_4 = \langle y \rangle$. We know $\operatorname{Aut} C_3 \cong C_2$ so a homomorphism ψ maps C_4 to the trivial group, $\mathbf{1}$ or to $\langle \beta : x \mapsto x^{-1} \rangle$.

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

If $C_4\psi = \langle \beta \rangle$ then we have:

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

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

If $\psi : (C_2 \times C_2) \to \operatorname{Aut} C_3$ is trivial then we obtain $G = C_3 \times C_2 \times C_2 \cong C_2 \times C_6$ which we have seen before.

The image of a non-trivial homomorphism $\psi : (C_2 \times C_2) \to \operatorname{Aut} C_3$ is C_2, so by Theorem 5.4: $\ker \theta = C_2$.

Choose $a, b \in C_2 \times C_2$ with $a, b \neq 1$ such that $a\theta = \beta : x \mapsto x^{-1}$ and $b\theta = \mathrm{id} : x \mapsto x$. Then:

$$G = \langle\, x, a, b \mid x^3 = a^2 = b^2 = 1,\ ab = ba,\ a^{-1}xa = x^{-1},\ b^{-1}xb = x \,\rangle$$

Let $y = xb$. The order of $y = \mathrm{lcm}\,(\mathrm{o}\,(x), \mathrm{o}\,(b)) = \mathrm{lcm}\,(2,3) = 6$ because x and b commute. $y^3 = x^3 b^3 = b$ so:

$$a^{-1}ya = a^{-1}xba = a^{-1}xab = x^{-1}b = x^2b = y^2y^3 = y^{-1}$$

Hence:

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

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

$$C_{12}, \quad C_2 \times C_6, \quad A_4, \quad D_{12}, \quad \text{or} \quad \langle\, x, y \mid x^3 = y^4 = 1,\ y^{-1}xy = x^{-1} \,\rangle$$

8 Generalisation to Groups of order $4p$

Suppose G is a group of order $4p$ where p is a prime number. Let n_2 denote the number of Sylow 2-subgroups.

9 Groups of Order 30

Let G be a group of order $30 = 2 \cdot 3 \cdot 5$, and let n_3 and n_5 denote the number of Sylow 3-subgroups and Sylow 5-subgroups of G respectively. Then by Theorem 5.3:

$$n_3 = 1 \text{ or } 10 \quad \text{and} \quad n_5 = 1 \text{ or } 6$$

If $n_3 = 10$, then there are 20 elements of order 3, and if $n_5 = 6$ then there are 24 elements of order 5 in G. G only has 30 elements, so then either:

$$n_3 = 1 \text{ and } n_5 = 6, \quad n_3 = 10 \text{ and } n_5 = 1 \quad \text{or} \quad n_3 = n_5 = 1$$

Hence either $C_3 \trianglelefteq G$ or $C_5 \trianglelefteq G$.

Let $H = C_3C_5$ and by Lagrange's Theorem, $C_3 \cap C_5 = \mathbf{1}$, hence $|H| = 15$ by Lemma 5.7. We know from our classification of groups of order pq that $H \cong C_{15}$. Notice that C_2 is a Sylow 2-subgroup of G, and by the same argument, $C_2 \cap C_{15} = \mathbf{1}$ and $|C_2C_{15}| = 30$. Hence $G = C_2C_{15}$.

Because $|C_{15}| = 15 = \frac{30}{2}$, the index of C_{15} in G is 2, and we know a subgroup of index 2 is normal, so $C_{15} \trianglelefteq G$. Moreover, $G = C_{15} \rtimes C_2$.

By Lemma 5.8:

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

A homomorphism, $\psi : C_2 \to C_2 \times C_4$ preserves element order, and there are 3 elements of order 2 in $C_2 \times C_4$: $(x, 1)$, $(1, y^2)$ and (x, y^2) where $\langle x, y \rangle = C_2 \times C_4$. We know ψ is determined by it's effect on a generator, so if $\langle z \rangle = C_2$ then $z\psi$ has four possibilities:

Case 1: $z\psi = (1, 1)$.

When $z\psi = (1, 1)$, then ψ is the trivial homomorphism, and so we obtain:

$$G \cong C_2 \times C_{15} \cong C_{30}$$

Case 2: $z\psi = (x, 1)$.

Case 3: $z\psi = (1, y^2)$.

Case 4: $z\psi = (x, y^2)$.

Part III
To Do

10 Semi-Direct Product

11 Groups of order 9 (Might skip)

12 Groups of Order 18

12.1 Groups of Order p^2q

13 Groups of Order p^3

13.1 Groups of Order 8

13.2 Groups of Order 27

13.3 General Case?

14 Groups of Order 24

15 Groups of Order 16