Interim Report

Daniel Laing

January 20, 2023

Contents

1 Theorems and Lemmas

1.1 Sylow Theorems

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

Theorem 1.1 (1st Sylow Theorem)**.** *G has a Sylow p-subgroup, i.e. a subgroup of order p^n.*

Theorem 1.2 (2nd Sylow Theorem)**.** *All Sylow p-subgroups of G are conjugate to each other.*

Corollary 1.2.1. *If $n_p = 1$ then the Sylow p-subgroup is normal in G.*

Theorem 1.3 (3rd Sylow Theorem)**.** *Let n_p denote the number of Sylow p-subgroups of G. Then:*

i) $n_p \mid m$

ii) $n_p \equiv 1 \pmod p$

Lemma 1.4. *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 1.5. *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. Any automorphism, φ of C_n has the property:

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

Hence φ is determined by it's effect on the generator, x, and preserves element order. In particular, φ sends generators to generators.

So for a generator, x, $x\varphi = x^k$ is surjective if x^k generates C_n. x^k generates C_n if $o(x^k) = n$ which is when $\gcd(n, k) = 1$.

Denote $\varphi_k : x \mapsto x^k$.

Consider:

$$x\varphi_k\varphi_l = (x^k)\varphi_l = (x^k)^l = x^{kl} = x^{lk} = (x^l)^k = x\varphi_l\varphi_k$$

So we see that $\operatorname{Aut} C_n$ is abelian. Moreover, $x\varphi_k\varphi_l = x\varphi_{kl}$.

Now consider $\theta : \operatorname{Aut} C_n \to \mathbb{Z}/n\mathbb{Z}^*$ defined by $\varphi_k\theta \mapsto k$. We will show θ is an isomorphism.

θ is surjective because every $k \in \mathbb{Z}/n\mathbb{Z}^*$ is coprime to n and so x^k is a generator of C_n, hence $\exists\, \varphi_k \in \operatorname{Aut} C_n$ such that $\varphi_k\theta = k$.

θ is also injective because if $\varphi_k, \varphi_l \in \operatorname{Aut} C_n$ such that $\varphi_k\theta = \varphi_l\theta$ then $k = l$.

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.

□

2 Groups of order 6

The prime factorisation of $6 = 2 \cdot 3$, so we can construct groups with products of C_2 and C_3. The automorphism groups of C_2, $\operatorname{Aut} C_2 = \{id\}$, containing just the identity map. So any meaningful products will look like $C_3 \rtimes C_2$.

$\operatorname{Aut} C_3 = \{\mathrm{id}, \psi\}$ where $x\psi = x^{-1}$. So we have two possible products: $C_3 \rtimes_{\mathrm{id}} C_2$ and $C_3 \rtimes_\varphi C_2$ where φ is the homomorphism $\varphi : C_2 \to \operatorname{Aut} C_3$ mapping $1 \mapsto \mathrm{id}$ and $x \mapsto \psi$.

2.1 $C_3 \rtimes_{\mathbf{id}} C_2$

By the Fundamental Theorem of Finite Abelian Groups, we know $C_3 \rtimes_{\mathrm{id}} C_2 \cong C_3 \times C_2 \cong C_6$.

2.2 $C_3 \rtimes_\varphi C_2$

So the group operation is

$$(a_1, b_1)(a_2, b_2) = (a_1 \cdot a_2\varphi_{b_1}, b_1 \cdot b_2)$$

Investigating elements:

$$(1, x)(1, x) = (1 \cdot 1\varphi_x, x \cdot x) = (1 \cdot 1^{-1}, x^2) = (1, 1)$$

So $(1, x)$ is of order 2.

$$(x, 1)(x, 1) = (x \cdot x\varphi_1, 1 \cdot 1) = (x \cdot x, 1) = (x^2, 1)$$
$$(x^2, 1)(x, 1) = (x^2 \cdot x\varphi_1, 1 \cdot 1) = (x^3, 1) = (1, 1)$$

So $(x, 1)$ is of order 3.

$$(x, 1)(x, x) = (x \cdot x\varphi_1, 1 \cdot x) = (x, x)$$
$$(x, x)(x, 1) = (x \cdot x\varphi_x, x \cdot 1) = (xx^{-1}, x) = (1, x)$$

Hence, $C_3 \rtimes_\varphi C_2$ is non-abelian.

3 Groups of Order 6 (Attempt 2)

Let G be a group of order 6, and n_3 denote the number of Sylow 3-subgroups of G. Then by Theorem 1.3:

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

So G has one Sylow 3-subgroup, and because 3 is prime, it is isomorphic to C_3, i.e.

$$C_3 \trianglelefteq G$$

Any Sylow 2-subgroup of G will have order 2, and so $C_2 \leqslant G$.

Lagrange's Theorem tells us that C_3 has elements of orders 1 and 3, and C_2 has elements of order 1 and 2 hence:

$$C_3 \cap C_2 = \mathbf{1}$$

By Lemma 1.4:

$$|C_3C_2| = \frac{|C_3| \cdot |C_2|}{|C_3 \cap C_2|} = \frac{3 \cdot 2}{1} = 6$$

So $G = C_3C_2$, $C_3 \trianglelefteq G$ and $C_3 \cap C_2 = \mathbf{1} \implies G = C_3 \rtimes C_2$

Now we need to determine $\operatorname{Aut} C_3$. $C_3 = \{1, x, x^2 = x^{-1}\}$ and so $\operatorname{Aut} C_3 = \{\mathrm{id}, \psi : x \mapsto x^{-1}\} \cong C_2$. So if $C_3 = \langle x \rangle$ and $C_2 = \langle y \rangle$, then we have two 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:

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

Hence G is isomorphic to either C_6 or D_6.

4 Generalisation to Groups of Order $2p$

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 1.3:

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

So G has one Sylow p-subgroup, it is isomorphic to $C_p = \langle x \rangle$ hence:

$$C_p \trianglelefteq G$$

A Sylow 2-subgroup of G will have order 2 so $C_2 = \langle y \rangle \leqslant G$.

Lagrange's Theorem tells us that C_p has elements of orders 1 and p, and C_2 has elements of order 1 and 2 hence:

$$C_p \cap C_2 = \mathbf{1}$$

By Lemma 1.4:

$$|C_pC_2| = \frac{|C_p| \cdot |C_2|}{|C_p \cap C_2|} = \frac{p \cdot 2}{1} = 2p$$

So $G = C_pC_2$, $C_p \trianglelefteq G$ and $C_p \cap C_2 = \mathbf{1} \implies G = C_p \rtimes C_2$

We want a homomorphism $\varphi : \operatorname{Aut} C_p \to C_2$. By Lemma 1.5, $\operatorname{Aut} C_p \cong \mathbb{Z}/p\mathbb{Z}^*$, so now we need to find elements of order 2 in Znp^*.

An element $x \in \mathbb{Z}/p\mathbb{Z}^*$ of order 2 satisfies:

$$x^2 = 1 \implies x^2 - 1 = 0 \implies (x-1)(x+1) = 0$$

Hence $x = 1$ or -1. But 1 has order 1 so x can only be -1.

So $C_2\varphi$ could be $\mathbf{1}$ or $\langle \beta : x \mapsto x{-}1 \rangle$. This gives us two possibilities:

$$y\varphi = x \mapsto x \quad \text{or} \quad y\varphi = x \mapsto x^{-1}$$

Case 1:

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

Case 2:

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

Hence a group of order $2p$ is isomorphic to C_{2p} or D_{2p}.

5 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, i.e. a group of order 4 must be abelian.

The Sylow theorems are not so helpful here, because $4 = 2^2$ so any Sylow 2-subgroup will be of order 4, which is just G.

6 Groups of order 9 (Might skip)

7 Generalisation to Groups of Order p^2

8 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 1.3:

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

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

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 $C_3 \leqslant G$.

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 1.4 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: $H = C_4$.

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: $H = V_4$.

$\operatorname{Aut} V_4 \cong S_3$ has 2 elements of order 3, giving us 3 posibilities for a homomorphism $\psi : C_3 \to \operatorname{Aut} V_4$:

$$C_3\psi = \mathbf{1}, \quad C_3\psi = (a, b, c) \quad \text{and} \quad C_3\psi = (a, c, b)$$

If $C_3\psi = \mathbf{1}$, then $G \cong C_2 \times C_2 \times C_3 \cong C_2 \times C_6$.

I don't how to do the other two cases. Something like:

$$G = \langle\, a, b, x \mid x^3 = a^2 = b^2 = (ab)^2 = 1,\ x^{-1}ax = b,\ x^{-1}bx = c,\ x^{-1}cx = a \,\rangle$$

$$G = \langle\, a, b, x \mid x^3 = a^2 = b^2 = (ab)^2 = 1,\ x^{-1}ax = c,\ x^{-1}bx = a,\ x^{-1}cx = b \,\rangle$$