Classification of some groups of order pqr

Adam Burley

Contents

Preliminaries

0.1. Results from [**1**]

The following is the main result proved in [**1**]. There, it is numbered as Corollary 1.5, and proved in section 7.

Lemma 0.1.1. *There are no non-Abelian simple groups of order less than* 200.

Removing the last 3 sentences of the proof of Theorem 6.2 in [**1**], we obtain the following.

Theorem 0.1.2. *Let G be a group, G not a p-group, and suppose that G has a Sylow p-subgroup P (of order p^s, say) with $P \leqslant \mathrm{Z}(\mathrm{N}_G(P))$. Then G has a normal subgroup of index p^s.*

The following is the core argument of the proof of Corollary 7.1 in [**1**]. It can be extracted from the proof of this, by taking only paragraphs 2 and 3, and the first 4 sentences of paragraph 5, and making very minor modifications to the wording.

Lemma 0.1.3. *Let G be a group and P a Sylow p-subgroup. If there exists no prime q such that $q > p$ and $q \mid |\operatorname{Aut}(P)|$, then $P \leqslant \mathrm{Z}(\mathrm{N}_G(P))$.*

Combining the above two lemmas, we obtain:

Theorem 0.1.4. *Let G be a group, G not a p-group, and suppose that G has a Sylow p-subgroup P (of order p^s, say), such that there exists no prime q with $q > p$ and $q \mid |\operatorname{Aut}(P)|$. Then G has a normal subgroup of index p^s.*

The following is Proposition 3.2 of [**1**].

Lemma 0.1.5. *Let G be a group of order p, where p is a prime. Then*

$$|\operatorname{Aut}(G)| = p - 1.$$

0.2. Other Results

The following is from elementary Group Theory.

Lemma 0.2.1. *If X is a G-set, then the map*

$$\rho : G \mapsto \operatorname{Sym}(X); \rho(g)(x) = gx$$

is a homomorphism.

CHAPTER 1

Solvability results

1.1. Subgroups of quotient groups

The following lemma establishes the form of subgroups of a quotient group.

LEMMA 1.1.1. *Let G be a finite group and N a normal subgroup. If $K \leqslant G/N$ then $K = H/N$ for some $H \leqslant G$ with $N \trianglelefteq H$.*

PROOF. Let G be a finite group and N a normal subgroup. Also, let $K \leqslant G/N$. Let $H = \{g \in G : gN \in K\}$. Then if $x \in K$ then $x \in G/N$, so $x = gN$ for some $g \in G$, and so this $g \in H$. Therefore, $x = gN \in H/N$, so we have shown $K \subseteq H/N$. If $hN \in H/N$, then this $h \in H$, so $hN \in K$. So $H/N \subseteq K$, and so $K = H/N$.

Next we show that $H \leqslant G$. Clearly we have $H \subseteq G$. Now take $h_1, h_2 \in H$. Then $h_1N, h_2N \in K$, so $(h_1h_2)N = (h_1N)(h_2N) \in K$, so $h_1h_2 \in H$. Also if $h \in H$ then $hN \in K$, so $h^{-1}N = (hN)^{-1} \in K$, so $h^{-1} \in H$. Therefore, $H \leqslant G$.

Now, if $n \in N$ then $nN = N = id_{G/N} \in K$, so $n \in H$ (as $n \in G$ and $nN \in K$). So $N \subseteq H$. Now if $n \in N$, $h \in H$ then $h \in G$ so $nhn^{-1} \in N$ (as $N \trianglelefteq G$). So we have shown that $N \trianglelefteq H$. □

We can establish a stronger result if we have a normal subgroup of the quotient group. The following is the key step.

LEMMA 1.1.2. *Let G be a finite group with a subgroup H and a normal subgroup N. Suppose $H/N \leqslant G/N$. Then $H \trianglelefteq G$.*

PROOF. Assume $H/N \trianglelefteq G/N$. So for all $gN \in G/N$ (or in other words, for all $g \in G$), we have $(gN)(H/N)(gN)^{-1} = H/N$, so

$$\{(gN)(hN)(gN)^{-1} : h \in H\} = \{hN : h_1 \in H\} \text{ for all } g \in G$$

so

$$\{(ghg^{-1})N : h \in H\} = \{hN : h_1 \in H\} \text{ for all } g \in G$$

so for all $g \in G$, $h \in H$, we have that $(ghg^{-1})N = h_1N$ for some $h_1 \in H$, so that $(ghg^{-1}) = h_1$, so $ghg^{-1} \in H$. Therefore, we have proved that $H \trianglelefteq G$. □

This lemma corresponds to Lemma 1.1.1, in the case where we have a normal subgroup. The proof is immediate from our previous two lemmas, but we give it in any case.

LEMMA 1.1.3. *Let G be a finite group and N a normal subgroup. If $K \trianglelefteq G/N$ then $K = H/N$ for some $H \trianglelefteq G$ with $N \trianglelefteq H$.*

Proof. Let G be a finite group and N a normal subgroup. If $K \trianglelefteq G/N$ then $K = H/N$ for some $H \leqslant G$ with $N \trianglelefteq H$, by Lemma 1.1.1. But since $K = H/N$ we have $H/N \trianglelefteq G/N$, and we already have that $N \trianglelefteq G$ and $H \leqslant G$. So we can apply Lemma 1.1.2 to obtain that $H \trianglelefteq G$. □

We may use this powerful lemma to prove an important result about maximal normal subgroups.

Lemma 1.1.4. *Suppose G is a finite group and N is a maximal proper normal subgroup of G. Then G/N is simple.*

Proof. Suppose G is a finite group and N is a maximal proper normal subgroup of G. Suppose for a contradiction that G/N were not simple. Then there exists a proper non-trivial normal subgroup of G/N, say K. By Lemma 1.1.3, K has the form H/N for some $H \trianglelefteq G$, where also $N \trianglelefteq H$. However H is a proper subgroup of G, since if $H = G$ then $|H| = |G|$ so

$$|H/N| = \frac{|H|}{|N|} = \frac{|G|}{|N|} = |G/N|$$

and so $H/N = G/N$, a contradiction as H/N is proper. Since N is the **maximal** proper normal subgroup of G, we must have $N = H$. But then

$$|H/N| = \frac{|H|}{|N|} = 1$$

so H/N is a trivial subgroup, a contradiction. □

Finally, we shall prove a lemma concerning quotients of quotient groups.

Lemma 1.1.5. *Suppose G is a finite group, and N and H are finite with $N \trianglelefteq H$, $H \leqslant G$, $N \trianglelefteq G$, and $H/N \trianglelefteq G/N$ (so that $H \trianglelefteq G$ by Lemma 1.1.2). Then*

$$(G/N)/(H/N) \cong G/H.$$

Proof. Suppose G is a finite group, and N and H are finite with $N \trianglelefteq H$, $H \leqslant G$, $N \trianglelefteq G$, and $H/N \trianglelefteq G/N$ (so that $H \trianglelefteq G$ by Lemma 1.1.2). Take the function defined by:

$$\phi : (G/N)/(H/N) \mapsto G/H; (gN)(H/N) \mapsto gH$$

We must check that this function is well-defined. There are two things which could change: first of all, we could take a different representative of the coset gN, or in other words take a $g_1 \in gN$ and consider $\phi((g_1N)(H/N))$. This would equal g_1H. But since $g_1 = gn_1$ for some $n_1 \in N$, and $N \subseteq H$, we have that $g_1 = gn_1$ for $n_1 \in H$. So we have

$$\phi((g_1N)(H/N)) = g_1H = gH = \phi((gN)(H/N))$$

and the function is well-defined in that sense.

The other way is if we took a different representative for the coset $(gN)(H/N)$, or in other words take $(g_2N) \in (gN)(H/N)$ and consider $\phi((g_2N)(H/N))$. This equals g_2H. However $g_2N = (gN)(hN) = (gh)N$ for some $hN \in H/N$ (so $h \in H$), and so $g_2 = ghn_2$ for some $n_2 \in N$. But $n_2 \in H$ as $N \subseteq H$, so $hn_2 \in H$, and so

$$\phi((g_2N)(H/N)) = g_2H = gH = \phi((gN)(H/N))$$

and the function is well-defined in that sense too.

Since

$$|(G/N)/(H/N)| = \frac{|G/N|}{|H/N|} = \frac{\frac{|G|}{|N|}}{\frac{|H|}{|N|}} = \frac{|G|}{|H|} = |G/H|$$

the domain and codomain of ϕ have the same size, so to show it is a bijection we need only check it is onto. But this is clear, as for any $gH \in G/H$, the element $(gN)(H/N)$ maps onto gH. So ϕ is a bijection.

We shall check that ϕ is an homomorphism. Take

$$(g_1N)(H/N), (g_2N)(H/N) \in (G/N)/(H/N);.$$

Then:

$$\begin{aligned}\phi((g_1N)(H/N))\phi((g_2N)(H/N)) &= (g_1H)(g_2H)\\ &= (g_1g_2)H\\ &= \phi(((g_1g_2)N)(H/N))\\ &= \phi(((g_1N)(g_2N))(H/N))\\ &= \phi(((g_1N)(H/N))((g_2N)(H/N)))\end{aligned}$$

so that ϕ is a homomorphism. So ϕ is an isomorphism. □

1.2. Facts about derived subgroups

In this section we shall prove some lemmas about derived subgroups. Recall that the derived subgroup is the subgroup generated by all elements $xyx^{-1}y^{-1}$. The derived series is the sequence $G, G', G'', ...$ If this series terminates, the group is said to be solvable. For a more precise account, see my other document [**1**].

These elements $xyx^{-1}y^{-1}$ are called commutators. Throughout this section we shall denote $[x, y] = xyx^{-1}y^{-1}$. Note that the inverse of a commutator is a commutator.

LEMMA 1.2.1. *Let G be a group and $x, y \in G$. Then $[x, y]^{-1} = [y, x]$.*

PROOF.

$$[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x]$$

□

First of all, a general picture of what elements of G' look like is very easy to derive.

LEMMA 1.2.2. *Let G be a group and $x \in G'$. Then there exist $c_1, ..., c_n$ with $x = c_1c_2 \cdots c_n$, such that for all $0 \leq i \leq n$, $c_i = [u_i, v_i]$, where $u_i, v_i \in G$.*

Proof. If $x \in G'$ then $x = a_1^{r_1} \cdots a_m^{r_m}$ by definition. Let $c_1, ..., c_n$ be obtained by regarding $r_i = 0$ as the element id_G, $r_i < 0$ as a product $(a_i)^{-1} \cdots (a_i)^{-1}$, and $r_i > 0$ as a product $a_i \cdots a_i$. Note that the elements obtained in this method are all commutators, as $a_i{}^{-1}$ is a commutator from Lemma 1.2.1, and $id_G = [id_G, id_G]$. So $x = c_1 \cdots c_n$ where for all $0 \leq i \leq n$, c_i is a commutator, or in other words, $c_i = [u_i, v_i]$ where $u_i, v_i \in G$. □

We shall now prove, in three main parts, that the derived subgroup is the smallest normal subgroup N such that G/N is Abelian. The first of these parts is split into two lemmas, as we shall need a stronger result than simply $G' \trianglelefteq G$ later on.

Lemma 1.2.3. *Let G be a finite group and $N \trianglelefteq G$. Then $N' \trianglelefteq G$.*

Proof. First notice that if $u, v \in N$, and $g \in G$, then

$$\begin{aligned} g([u,v])g^{-1} &= g(uvu^{-1}v^{-1})g^{-1} \\ &= g(ug^{-1}gvg^{-1}gu^{-1}g^{-1}gv^{-1})g^{-1} \\ &= (gug^{-1})(gvg^{-1})(gug^{-1})^{-1}(gvg^{-1})^{-1} \\ &= [gug^{-1}, gvg^{-1}] \end{aligned}$$

which is itself a commutator (since N is normal, gug^{-1} and gvg^{-1} are in N), so $g([u,v])g^{-1} \in N'$. Now, if $x \in N'$ then $x = c_1 \cdots c_n$, where the c_i are all commutators, by Lemma 1.2.2. Now:

$$\begin{aligned} gxg^{-1} &= g(c_1 \cdots c_n)g^{-1} \\ &= g(c_1g^{-1}gc_2g^{-1} \cdots gc_{n-1}g^{-1}gc_n)g^{-1} \\ &= (gc_1g^{-1})(gc_2g^{-1}) \cdots (gc_{n-1}g^{-1})(gc_ng^{-1}) \end{aligned}$$

but the last term is a product of commutators, so $gxg^{-1} \in N'$, and the result is proved. □

Lemma 1.2.4. *Let G be a group. Then $G' \trianglelefteq G$.*

Proof. We know $G \trianglelefteq G$, so we apply Lemma 1.2.3 with N replaced by G, to obtain the result. □

Lemma 1.2.5. *If G is a group, then G/G' is Abelian.*

Proof. Let (xG') and (yG') be arbitrary elements of G/G'. Then $[x,y] \in G'$, as $x, y \in G$. So $[x,y]G' = G'$, and:

$$\begin{aligned} (xG')(yG')(xG')^{-1}(yG')^{-1} &= (xG')(yG')(x^{-1}G')(y^{-1}G') \\ &= (xyx^{-1}y^{-1})G' \\ &= [x,y]G' \\ &= G' \\ &= id_{G/G'} \end{aligned}$$

so that

$$(xG')(yG') = (yG')(xG')$$

as required. □

Lemma 1.2.6. *If N is a normal subgroup of a group G such that G/N is Abelian, then $G' \leqslant N$.*

Proof. Let $x, y \in G$, then $[x, y] \in G'$. Now,

$$\begin{aligned}[x,y]N &= (xyx^{-1}y^{-1})N \\ &= (xN)(yN)(x^{-1}N)(y^{-1}N) \\ &= (xN)(yN)(xN)^{-1}(yN)^{-1} \\ &= (xN)(xN)^{-1}(yN)(yN)^{-1} \\ &= id_{G/N} \\ &= N\end{aligned}$$

so that $[x, y] \in N$. Since N contains all commutators, it contains all products of commutators, and therefore $G' \leqslant N$. □

Finally, we present some results on derived subgroups of subgroups and of isomorphic groups. The first of these states that taking derived subgroups preserves the subgroup relation.

Lemma 1.2.7. *If G and H are groups with $G \leqslant H$, then $G' \leqslant H'$.*

Proof. Suppose $x \in G'$. Then, by Lemma 1.2.2

$$x = c_1 \cdots c_n$$

where the $c_i = [u_i, v_i]$ for $u_i, v_i \in G$. So $u_i, v_i \in H$, and so

$$c_i = u_i v_i u_i^{-1} v_i^{-1} \in H'$$

So we must have

$$x = c_1 \cdots c_n \in H'$$

which gives the result. □

We may extend this result by induction.

Lemma 1.2.8. *If G and H are groups with $G \leqslant H$, then $G^{(r)} \leqslant H^{(r)}$ for all integers $r \geq 0$.*

Proof. Let G and H be groups with $G \leqslant H$. We shall prove the statement "$G^{(r)} \leqslant H^{(r)}$" by induction, for all integers $r \geq 0$. First take the case $r = 0$. Then the statement reads $G^{(0)} \leqslant H^{(0)}$, i.e. $G \leqslant H$, which is one of our hypotheses. Now suppose the statement is true for $r = k$. Then $G^{(k)} \leqslant H^{(k)}$ by the inductive hypothesis, and we can apply Lemma 1.2.7 to obtain $(G^{(k)})' \leqslant (H^{(k)})'$. But this means $G^{(k+1)} \leqslant H^{(k+1)}$, so the statement is true for $r = k + 1$. Therefore, by the principle of induction, the statement holds for all integers $r \geq 0$. □

This enables us to get a result on solvability.

Lemma 1.2.9. *If G is a solvable group and $H \leqslant G$, then H is solvable.*

Proof. Let G be a solvable group and $H \leqslant G$. Then there exists N such that $G^{(N)} = \{id_G\}$. Therefore $H^{(N)} \leqslant G^{(N)} = \{id_G\}$, by Lemma 1.2.8. Therefore, $H^{(N)} = \{id_G\}$, and so H is solvable. □

Another, similar result on solvability may be obtained in a similar fashion.

LEMMA 1.2.10. *If G and H are groups such that $G \cong H$, then $G' \cong H'$.*

PROOF. Let G and H be groups such that $G \cong H$. Let $\phi : G \mapsto H$ be an isomorphism. We shall show that $\phi(G') = H'$. Therefore, the restriction of ϕ to G' is an onto map from G' to H'. We already know that this restriction is a 1-1 homomorphism, so this will give $G' \cong H'$ as required.

($\subseteq$) First suppose that $c \in G'$ is a commutator. Then $c = xyx^{-1}y^{-1}$ for some $x, y \in G$. Now

$$\phi(c) = \phi(x)\phi(y)\phi(x^{-1})\phi(y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} \in H'$$

as $\phi(x), \phi(y) \in H$.

Now suppose that $g \in G'$ is any element. Then, by Lemma 1.2.2,

$$g = c_1c_2 \cdots c_n$$

where $c_1, ..., c_n \in G'$ are commutators. Now

$$\phi(g) = \phi(c_1)\phi(c_2) \cdots \phi(c_n) \in H'$$

and so $\phi(G') \subseteq H'$.

($\supseteq$) First suppose that $c \in H'$ is a commutator. Then $c = xyx^{-1}y^{-1}$ for some $x, y \in H$. Since ϕ is onto, there exist $x_1, y_1 \in G$ such that $\phi(x_1) = x$ and $\phi(y_1) = y$. Let $c_1 = x_1y_1x_1^{-1}y_1^{-1}$. Then c_1 is a commutator, $c_1 \in G'$ and

$$\begin{aligned} \phi(c_1) &= \phi(x_1)\phi(y_1)\phi(x_1^{-1})\phi(y_1^{-1}) \\ &= \phi(x_1)\phi(y_1)\phi(x_1)^{-1}\phi(y_1)^{-1} \\ &= xyx^{-1}y^{-1} \\ &= c. \end{aligned}$$

Now suppose that $h \in H'$ is any element. Then, by Lemma 1.2.2,

$$h = c_1c_2 \cdots c_n$$

where $c_1, c_2, ..., c_n \in H'$ are commutators. Now there exist commutators $d_1, d_2, ..., d_n \in G'$ such that $\phi(d_i) = c_i$ for each i with $1 \leq i \leq n$. Let $g = d_1d_2 \cdots d_n \in G'$. Then $\phi(g) \in \phi(G')$, and

$$\phi(g) = \phi(d_1)\phi(d_2) \cdots \phi(d_n) = c_1c_2 \cdots c_n = h.$$

Thus $H' \subseteq \phi(G')$, i.e. $\phi(G') \supseteq H'$. □

LEMMA 1.2.11. *If G and H are groups such that $G \cong H$, then $G^{(r)} \cong H^{(r)}$ for all integers $r \geq 0$.*

PROOF. Let G and H be groups such that $G \cong H$. We shall prove the statement "$G^{(r)} \cong H^{(r)}$" by induction, for all integers $r \geq 0$. First take the case $r = 0$. Then the statement reads $G^{(0)} \cong H^{(0)}$, i.e. $G \cong H$, which is one of our hypotheses. Now suppose the statement is true for $r = k$. Then $G^{(k)} \cong H^{(k)}$ by the inductive hypothesis, and we can apply Lemma 1.2.10 to obtain $(G^{(k)})' \cong (H^{(k)})'$. But this means $G^{(k+1)} \cong H^{(k+1)}$, so the statement is true for $r = k+1$. Therefore, by the principle of induction, the statement holds for all integers $r \geq 0$. □

LEMMA 1.2.12. *If G is a solvable group and H is a group such that $G \cong H$, then H is solvable.*

PROOF. Let G be a solvable group and H be a group such that $G \cong H$. Since G is solvable, there exists N such that $G^{(N)} = \{id_G\}$. Therefore, $|G^{(N)}| = 1$. By Lemma 1.2.11, $G^{(N)} \cong H^{(N)}$, and so $|H^{(N)}| = 1$. Therefore, $H^{(N)} = \{id_H\}$, so H is solvable. □

1.3. Abelian series

We met solvability briefly in [**1**]. However, here it will be much more important. We start by providing a new equivalent definition of solvability. This starts with the definition of a normal series.

DEFINITION 1.3.1. Let G be a group. A **normal series of subgroups** for G is a sequence

$$H_0, H_1, ..., H_n$$

of subgroups of G such that $H_0 = \{id_G\}$, $H_n = G$, and $H_i \trianglelefteq H_{i+1}$ for all $0 \leq i < n$. n is the length of the normal series of subgroups.

DEFINITION 1.3.2. Let G be a group. A **normal series** for G is a sequence

$$G_0, G_1, ..., G_n$$

of groups such that there exists a normal series of subgroups

$$H_0, H_1, ..., H_n$$

for G with $G_i \cong H_i$ for all $0 \leq i \leq n$. n is the length of the normal series.

Now we define the idea of an Abelian series, which leads directly to our new definition of solvability.

DEFINITION 1.3.3. Let G be a group. An **Abelian series of subgroups** for G is a normal series of subgroups

$$H_0, H_1, ..., H_n$$

for G such that H_{i+1}/H_i is Abelian for all $0 \leq i < n$. n is the length of the Abelian series of subgroups.

DEFINITION 1.3.4. Let G be a group. An **Abelian series** for G is a sequence

$$G_0, G_1, ..., G_n$$

of groups such that there exists an Abelian series of subgroups

$$H_0, H_1, ..., H_n$$

for G with $G_i \cong H_i$ for all $0 \leq i \leq n$. n is the length of the Abelian series.

While our definitions of "normal series of subgroups" and "Abelian series of subgroups" are non-standard, it is clear that any normal series of subgroups is a normal series, and any Abelian series of subgroups is an Abelian series.

Our new definition of solvability is "having an Abelian series".

PROPOSITION 1.3.5. *Let G be a group. Then G is solvable iff it has an Abelian series.*

PROOF. ($\Longrightarrow$) If G is a solvable group then there exists some N with $G^{(N)} = \{id_G\}$. Let n be the smallest such N. Then let $G_n = G$ and $G_r = G^{(n-r)}$ for all $0 \leq r < n$. By construction we have $G_0 = G^{(n)} = \{id_G\}$ and $G_n = G$. By Lemma 1.2.4, $G_i \trianglelefteq G_{i+1}$. Also, for all $0 \leq i < n$:

$$G_{i+1}/G_i = G_{i+1}/(G_{i+1})'$$

which is Abelian by Lemma 1.2.5.

($\Longleftarrow$) If G has an Abelian series $G_0, G_1, ..., G_n$, then there is an Abelian series of subgroups $H_0, H_1, ..., H_n$. Now H_n/H_{n-1} is Abelian (by Lemma 1.2.6), so $G' = (H_n)' \leqslant H_{n-1}$. Next note that H_{n-1}/H_{n-2} is Abelian, so again by Lemma 1.2.6, $(H_{n-1})' \leqslant H_{n-2}$. But by Lemma 1.2.7, we have that

$$G'' \leqslant (H_{n-1})' \leqslant H_{n-2}.$$

Continuing in this way, we obtain that $G^{(r)} \leqslant H_{n-r}$ for all $0 < r \leq n$. In particular, $G^{(n)} \leqslant H_0 = \{id_G\}$, so $G^{(n)} = \{id_G\}$, and so G is solvable. □

1.4. An important condition for solvability

The new definition of solvability we have presented makes the following result immediate.

LEMMA 1.4.1. *If N is a solvable normal subgroup of a group G, and G/N is Abelian, then G is solvable.*

PROOF. If N is a solvable normal subgroup of a group G then N has an Abelian series, and therefore an Abelian series of subgroups, say $N_0, N_1, ..., N_r$. Let $n = r + 1$, and let $G_i = N_i$ for all $0 \leq i < n$, and $G_n = G$. Then $G_0 = \{id_N\} = \{id_G\}$ also. Furthermore, $N_i \trianglelefteq N_{i+1}$ for all $0 \leq i < n - 1 = r$, and $N_i = N \trianglelefteq G = G_{i+1}$ for $i = n - 1$. Finally, N_{i+1}/N_i is Abelian for all $0 \leq i < n - 1 = r$, and $N_{i+1}/N_i = G/N$ is Abelian for $i = n - 1$. So $G_0, ..., G_n$ is an Abelian series for G, and hence G is solvable. □

The apparent weakness of this result is deceptive; it may in fact be used in conjunction with induction to prove a much stronger result. We shall first require an easy lemma.

LEMMA 1.4.2. *Suppose G is a finite Abelian group and H is a finite group, with $G \cong H$. Then H is Abelian.*

PROOF. Suppose G is a finite Abelian group and H is a finite group, with $G \cong H$. Let

$$\phi : G \mapsto H$$

be an isomorphism.

Now take any $x, y \in H$. There are $x_1, y_1 \in G$ with $\phi(x_1) = x, \phi(y_1) = y$ (as ϕ is onto). Now,

$$xy = \phi(x_1)\phi(y_1) = \phi(x_1y_1) = \phi(y_1x_1) = \phi(y_1)\phi(x_1) = yx.$$

So H is Abelian. □

Now the stronger version of Proposition 1.4.1 can be proved.

Proposition 1.4.3. *If N is a solvable normal subgroup of a finite group G, and G/N is solvable, then G is solvable.*

Proof. Let G be a finite group. We shall use induction to prove the statement "If $N \trianglelefteq G$, N is solvable and G/N has an Abelian series of length k, then G is solvable" for all k.

First of all consider the case $k = 0$. So suppose that $N \trianglelefteq G$, N is solvable and G/N has an Abelian series of length 0. So G/N has an Abelian series of subgroups of length 0. This series contains exactly one element. This element is the first in the series and so must equal $\{id_{G/N}\}$, but is also the last in the series so must equal G/N. So $G/N = \{id_{G/N}\}$ and G/N is then Abelian. Therefore, G is solvable by Lemma 1.4.1.

Now assume truth for $k = m$ and suppose that $N \trianglelefteq G$, N is solvable and G/N has an Abelian series of length $m + 1$. Then G/N has an Abelian series of subgroups of length $m + 1$, say $K_0, ..., K_m, K_{m+1}$. By Lemma 1.1.3, we have that $K_m = H/N$, where $N \trianglelefteq H$ and $H \trianglelefteq G$. Now $H/N = K_m$ is clearly solvable (as it has an Abelian series $K_0, K_1, ..., K_m$), and N is solvable, so H is solvable (as we have assumed truth for $k = m$).

We have that $(G/N)/(H/N) = K_{m+1}/K_m$ is Abelian. By Lemma 1.1.5, $(G/N)/(H/N) \cong G/H$. By Lemma 1.4.2, G/H is Abelian. So we have $H \trianglelefteq G$, with H solvable and G/H is Abelian. Therefore, G is solvable by Lemma 1.4.1, and the statement is true for $k = m + 1$.

By the principle of induction, we have truth for all k, namely, the original statement of the proposition. □

1.5. Groups of squarefree order

The aim of this section is to show that all groups of squarefree order are solvable. The following is a cut down version of Corollary 7.1 from [**1**].

Proposition 1.5.1. *Let G be a group of order $p_1 \cdots p_r$, where $p_1, ..., p_r$ are primes. Then G has a normal subgroup of index p_1.*

Proof. Let G be a group of order $p_1 \cdots p_r$, where $p_1, ..., p_r$ are primes. Let P be a Sylow p_1-subgroup, which clearly has order p_1. We have that $|\operatorname{Aut}(P)| = p_1 - 1$, by Lemma 0.1.5. Suppose there were a prime q with $q > p_1$ and $q \mid |\operatorname{Aut}(P)|$. Then $q < |\operatorname{Aut}(P)| = p_1 - 1 < p_1$, a contradiction. Therefore, there is no such q, and so, by Theorem 0.1.4 (and G is clearly not a p-group), G has a normal subgroup of index p_1. □

We may now prove that all groups of squarefree order are solvable.

Corollary 1.5.2. *Let G be a group of order $p_1 \cdots p_r$, where $p_1 < ... < p_r$ are primes. Then G is solvable.*

Proof. Suppose for a contradiction that the statement of the result is false, and let r be the smallest positive integer such that there exists a non-solvable group of order $p_1 \cdots p_r$ ($p_1 < ... < p_r$ primes). Let G be such a group. By Proposition 1.5.1, G has a normal subgroup of index p_1, say N. Now N has order $p_2 \cdots p_r$ and hence is solvable, otherwise r would not be the smallest positive integer satisfying its defining property, as $r - 1$ would also satisfy it.

In addition, G/N is Abelian (having prime order p_1) and therefore solvable. So G is solvable by Lemma 1.4.3. This is a contradiction as G was assumed not to be solvable. Therefore, the statement of the result is true. □

CHAPTER 2

Hall Theory

2.1. π-numbers

The concept of a π-number is the foundation of the Hall Theory.

DEFINITION 2.1.1. Let π be a finite set of primes. A π-number is either 1, or an integer divisible by only those primes in π. A π'-number is either 1, or an integer divisible by none of the primes in π.

This leads to the idea of a π-group, a generalisation of the p-group, and the Hall subgroup, a generalisation of the Sylow subgroup.

DEFINITION 2.1.2. A π-group is a group G such that $|G|$ is a π-number. A π'-group is a group G such that $|G|$ is a π'-number.

DEFINITION 2.1.3. Let G be a finite group and π a finite set of primes. A π-subgroup of G is a subgroup H of G such that H is a π-group. A π'-subgroup of G is a subgroup H of G such that H is a π'-group.

DEFINITION 2.1.4. Let G be a finite group and π a finite set of primes. A Hall π-subgroup of G is a π-subgroup H such that $[G : H]$ is a π'-number. A Hall π'-subgroup of G is a π'-subgroup H such that $[G : H]$ is a π-number.

It can be seen that this is a generalisation of the Sylow subgroup.

LEMMA 2.1.5. *Let G be a finite group and π a finite set of primes. Then a Hall π-subgroup of G is a maximal π-subgroup, and a Hall π'-subgroup is a maximal π'-subgroup.*

PROOF. We shall show the π case; the π' case is similar. Suppose G is a finite group, π a finite set of primes, and H a Hall π-subgroup of G. Suppose for a contradiction that there existed a π-subgroup K with $|K| > |H|$. There are two cases. Firstly, we could have that there was some prime p dividing $|K|$ such that p does not divide $|H|$. However then $p \in \pi$, as p divides $|K|$, a π-number. Now p divides $|G| = |H|[G : H]$, but p does not divide $|H|$, so $p \mid [G : H]$. However this is a contradiction as $p \in \pi$, and $[G : H]$ is meant to be a π'-number.

The second case is if H and K are divisible by all the same primes. Then, we must have at least one prime p which divides $|K|$ to a higher power, say s, than it divides $|H|$ to (say r). We must have $p \in \pi$, as p divides $|K|$, a π-number. Now p^{s-r} does not divide $p^{-r}|H|$, as p divides $|H|$ to the rth power only. Also, p^s divides $|G| = |H|[G : H]$, so p^{s-r} divides $p^{-r}|G| = (p^{-r}|H|)[G : H]$. Thus p^{s-r} divides $[G : H]$, and as $s > r$, we have $p \mid [G : H]$. However this is a contradiction as $p \in \pi$, and $[G : H]$ is meant to be a π'-number. $\square$

Then, the following lemma, allowing us to calculate the orders of Hall π-subgroups, is immediate.

LEMMA 2.1.6. *Let G be a finite group and π a finite set of primes. Suppose $p_1, ..., p_r$ is an enumeration of the primes in π, and $q_1, ..., q_s$ are the primes dividing $|G|$ which are not in π. Suppose*

$$|G| = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}.$$

Then a Hall π-subgroup of G has order $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, and a Hall π'-subgroup has order $q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$.

We present some examples.

EXAMPLES 2.1.7.

(1) A Hall $\{5, 7\}$-subgroup of a group of order $4725 = 3^3 5^2 7$ would have order $5^2 7 = 175$.
(2) A Hall $\{3\}$-subgroup of a group of order $4725 = 3^3 5^2 7$ would have order $3^3 = 27$. This is the same order as a Sylow 3-subgroup would have. In fact, it is easy to see that a Hall $\{p\}$-subgroup is the same as a Sylow p-subgroup.
(3) A Hall $\{11, 13\}$-subgroup of a group of order $4725 = 3^3 5^2 7$ would have order 1.

Finally, the intersection of a π-subgroup and a π'-subgroup (whether Hall or not) must be trivial.

PROPOSITION 2.1.8. *Let G be a group with subgroups A and B, then $A \cap B \leqslant A$ and $A \cap B \leqslant B$. Furthermore, if $A \trianglelefteq G$ and $B \trianglelefteq G$ then $A \cap B \trianglelefteq G$.*

PROOF. Let G be a group with subgroups A and B. We have that $A \cap B$ is non-empty, as both A and B contain the identity of G. It is also clearly a subset of G (as e.g. $A \cap B \subseteq A \subseteq G$).

Now take $x, y \in A \cap B$. Then $x \in A$ and $y \in A$ so $xy \in A$. Also $x \in B$ and $y \in B$ so $xy \in B$. Therefore, $xy \in A \cap B$.

Take any $x \in A \cap B$. Then $x \in A$ so $x^{-1} \in A$, and $x \in B$ so $x^{-1} \in B$. Therefore, $x^{-1} \in A \cap B$.

Therefore, $A \cap B$ is a subgroup of G, hence a group. Since $A \cap B \subseteq A$ and $A \cap B \subseteq B$, we have that $A \cap B \leqslant A$ and $A \cap B \leqslant B$.

Suppose $A \trianglelefteq G$ and $B \trianglelefteq G$. Take $n \in A \cap B$, and $g \in G$. Then $n \in A$ so $gng^{-1} \in A$, and $n \in B$ so $gng^{-1} \in B$. Therefore, $gng^{-1} \in A \cap B$, and so $A \cap B \trianglelefteq G$. □

COROLLARY 2.1.9. *Let G be a group, let A be a π-subgroup and B a π'-subgroup. Then $A \cap B$ is trivial.*

PROOF. Let G be a group, let A be a π-subgroup and B a π'-subgroup. Then $A \cap B \leqslant A$ and $A \cap B \leqslant B$, by Proposition 2.1.8. Therefore, $|A \cap B|$ divides both $|A|$ and $|B|$, hence is both a π-number and a π'-number. Therefore, it must be 1, and so $A \cap B$ is trivial. □

2.2. Hall's Theorems

The object of this chapter is to prove the following theorems, known as Hall's First, Second and Third Theorems. The first and second of these are essentially generalisations of Sylow's First and Second Theorems.

THEOREM 2.2.1. *Let G be a finite **solvable** group, and π be a set of primes.*

(1) *G has a Hall π-subgroup.*
(2) *Any two Hall π-subgroups of G are conjugate.*
(3) *Any π-subgroup is contained within a Hall π-subgroup.*

In fact, for π-groups or π'-groups, the theorems are easy.

LEMMA 2.2.2. *Let G be a π-group or a π'-group. Then Theorem 2.2.1 holds for G.*

PROOF. Suppose first that G is a π-group. Then G is a π-subgroup of itself, and therefore any Hall π-subgroup of G must have order $|G|$, by Lemma 2.1.5. Hence, G is the only Hall π-subgroup of G. Clearly, Hall's First Theorem holds then. Also, G is conjugate to itself by the identity. Therefore, Hall's Second Theorem holds. Finally, Hall's Third Theorem holds (as any π-subgroup of G is contained in G, a Hall π-subgroup)

Suppose now that G is a π'-group. Then the order of any subgroup of G must be a π'-number, as it must divide the order of G. Therefore, every subgroup of G is a π'-subgroup, and so any π-subgroup of G must also be a π'-subgroup. The order of such a subgroup must be both a π and a π'-number, in other words, it must be 1. Therefore, $H = \{id_G\}$ is the only π-subgroup, and it is a Hall π-subgroup. Thus, Hall's First Theorem is proved. H is conjugate to itself by the identity and it is the only Hall π-subgroup, giving Hall's Second Theorem. Finally, any π-subgroup must equal H, therefore it is contained in H, which gives Hall's Third Theorem. □

2.3. Elementary Abelian p-groups

The following definition is perhaps at first interesting as it is the exact case to which we can generalise the arguments in Section 4 of [**1**] to. However this will not be the purpose we will require it for.

DEFINITION 2.3.1. Let p be a prime. An elementary Abelian p-group is an Abelian p-group in which all non-identity elements have order p.

We have a simpler condition for an elementary Abelian p-group.

LEMMA 2.3.2. *Let p be a prime, and G an Abelian p-group such that for all $x \in G$, we have $x^p = id_G$. Then G is an elementary Abelian p-group.*

PROOF. Let p be a prime, and G an Abelian p-group such that for all $x \in G$, we have $x^p = id_G$. Let x be in G. Then the order of x divides the order of G, a power of p, therefore the order of x is $1, p, p^2, ...$ However as $x^p = id_G$, then the order of x is 1 or p. If x is a non-identity element then its order is not 1, so it must be p. □

The following lemma states that (non-trivial) normal subgroups of smallest order are elementary Abelian.

Lemma 2.3.3. *Let G be a solvable group and A a non-trivial normal subgroup of G of smallest order. Then A is an elementary Abelian p-group, for some prime p.*

Proof. Let G be a solvable group and A a non-trivial normal subgroup of G of smallest order. A is solvable by Lemma 1.2.9. Therefore, $A' \neq A$ (so $|A'| < |A|$). If A' is non-trivial, then A' is a normal subgroup of G (by Lemma 1.2.3), non-trivial, and has smaller order than A. This contradicts the minimality of A. Therefore, A' must be trivial, i.e. A is Abelian.

Choose any prime p such that $p \mid |A|$. Let

$$B = \{x \in A : x^p = id_G\}$$

Then B is non-trivial, as by Cauchy's group theorem, A contains an element of order p; this element is not the identity, and is in B.

We shall show that $B \trianglelefteq G$. So take $b \in B$, $g \in G$. Then $b \in A$, so $gbg^{-1} \in A$, as $A \trianglelefteq G$. Also

$$(gbg^{-1})^p = gb^pg^{-1} = gid_Gg^{-1} = id_G$$

(noting for the first equality that the inner $g^{-1}g$ terms all cancel) so that $gbg^{-1} \in B$. Therefore, $B \trianglelefteq G$.

So B is a non-trivial normal subgroup of G, which is a subgroup of A. Therefore, we must have $A = B$, or else B would contradict the minimality of A. Suppose A were not a p-group. Then there exists some other prime q dividing the order of A. So by Cauchy's group theorem, there is an element a of A which has order q. Since $a^p = id_G$, we must have $q \mid p$, a contradiction. Therefore, A must be a p-group, and so we have all we need to apply Lemma 2.3.2, and obtain that A is an elementary Abelian p-group. □

2.4. Products of subgroups and The Frattini Argument

We can take the product of two subgroups simply by taking the products of their elements.

Definition 2.4.1. Let G be a group with subgroups H and K. We define

$$HK = \{hk : h \in H, k \in K\}$$

While this product will not be a group in general, it will be a group if one of the subgroups is normal.

Proposition 2.4.2. *Let G be a group with subgroups H and K, and either $H \trianglelefteq G$ or $K \trianglelefteq G$. Then HK is a group.*

Proof. Let G be a group with subgroups H and K. The set HK is non-empty as it contains $id_G = id_Gid_G$, as $id_G \in H, id_G \in K$. It is clearly a subset of G.

Firstly suppose $H \trianglelefteq G$. To show closure under the binary operation, take $h_1k_1, h_2k_2 \in HK$, and let $h_3 = k_1h_2k_1^{-1} \in H$. Then:

$$h_1k_1h_2k_2 = h_1k_1h_2k_1^{-1}k_1k_2 = h_1h_3k_1k_2 \in HK$$

so the set is closed under the binary operation. To show closure under inverses, take $hk \in HK$ and let $h_1 = k^{-1}h^{-1}k = k^{-1}h^{-1}(k^{-1})^{-1} \in H$. Then:

$$(hk)^{-1} = k^{-1}h^{-1} = k^{-1}h^{-1}kk^{-1} = h_1k^{-1} \in HK$$

so the set is closed under inverses. Therefore, HK is a group.

Secondly suppose $K \trianglelefteq G$. To show closure under the binary operation, take $h_1k_1, h_2k_2 \in HK$, and let $k_3 = h_2^{-1}k_1h_2 = h_2^{-1}k_1(h_2^{-1})^{-1} \in K$. Then:

$$h_1k_1h_2k_2 = h_1h_2h_2^{-1}k_1h_2k_2 = h_1h_2k_3k_2 \in HK$$

so the set is closed under the binary operation. To show closure under inverses, take $hk \in HK$ and let $k_1 = hk^{-1}h^{-1} \in K$. Then:

$$(hk)^{-1} = k^{-1}h^{-1} = h^{-1}hk^{-1}h^{-1} = h^{-1}k_1 \in HK$$

so the set is closed under inverses. Therefore, HK is a group. □

We can compute the order of this set.

Proposition 2.4.3. *Let G be a group with subgroups H and K. Then:*

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proof. Let G be a group with subgroups H and K. Let $S = H \times K$, $T = HK$ and $A = H \cap K$. A acts on S by

$$a * (h,k) = (ha^{-1}, ak)$$

and if $a * (h,k) = (h,k)$ then $a = \mathrm{id}_A$, so the stabilizer always consists only of the identity. Therefore, by the orbit-stabilizer theorem, every orbit has size $|A|$.

Consider the map

$$\phi : S \mapsto T; (h,k) \mapsto hk$$

which is onto, since if $t \in T$, then $t = hk$ for some $h \in H, k \in K$, so that $\phi(h,k) = t$.

We shall show that ϕ is 1-1 within its orbits: Suppose $\phi(s_1) = \phi(s_2)$ where $s_1 = h_1k_1$ and $s_2 = h_2k_2$. Then $h_1k_1 = h_2k_2$ so that $h_2^{-1}h_1 = k_2k_1^{-1}$. The left-hand side is in H and the right is in K, so both are in $H \cap K = A$ (being equal). Let $a = h_2^{-1}h_1 = k_2k_1^{-1} \in A$. Then

$$a * s_1 = a(h_1,k_1) = (h_1a^{-1}, ak_1) = (h_1h_1^{-1}h_2, k_2k_1^{-1}k_1) = (h_2,k_2) = s_2$$

and so s_1 and s_2 lie in the same orbit.

Converseley, suppose that $s_1 = (h,k)$ and s_2 lie in the same orbit. Then $s_2 = a * s_1$ for some $a \in A$. Now

$$\phi(s_1) = hk = \phi(ha, a^{-1}k) = \phi(a * s_1) = \phi(s_2)$$

and taking this together with the previous argument gives that $\phi(s_1) = \phi(s_2)$ if and only if s_1 and s_2 lie in the same orbit.

Enumerate the elements of $T = HK$ by $\{t_1, ..., t_n\}$ where $n = |T|$. Let $S_i = \phi^{-1}(t_i)$, for $1 \leq i \leq n$. Then the S_i are disjoint, and S is the union of them (as each s must map to a t_i and it cannot map to more than one).

Take any $s_i \in S_i$, and notice that

$$s \in S_i \iff \phi(s) = t_i \iff \phi(s) = \phi(s_i) \iff s \in \mathrm{Orb}(s_i)$$

and so each $S_i = \mathrm{Orb}(s_i)$, so $|S_i| = |A|$ for each i.

Now we get

$$\begin{aligned} |H| \cdot |K| &= |S| \\ &= |S_1| + |S_2| + ... + |S_n| \\ &= |A| + |A| + ... + |A| \\ &= n|A| \\ &= |HK| \cdot |H \cap K| \end{aligned}$$

and so

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

as required. □

The following chain of lemmas lead to the computation of the derived subgroup of such a product, under some (rather restrictive) conditions.

Lemma 2.4.4. *Let G be a group with subgroups H and K. Then $(HK)/K = H/K$.*

Proof. Let G be a group with subgroups H and K. Take $x \in H/K$. Then $x = hK$ for some $h \in H$, and so

$$x = (h\,\mathrm{id}_G)K = (h\,\mathrm{id}_K)K \in (HK)/K$$

so $H/K \subseteq (HK)/K$.

Now take $x \in (HK)/K$. Then $x = (hk)K = h(kK)$ for some $h \in H$, $k \in K$. Clearly $kK \subseteq K$ (as any element of kK is a product of two elements of K). But also $K \subseteq kK$, since if $y \in K$ then $y = k(k^{-1}x) \in kK$. Therefore, $kK = K$, and $x = h(kK) = hK \in H/K$. So $(HK)/K \subseteq H/K$, and the result follows. □

Lemma 2.4.5. *If G is a group with subgroups H and K. Then $(HK/K)' = (H'K)/K$.*

Proof. Let G be a group with subgroups H and K. By Lemma 2.4.4, $(HK/K)' = (H/K)'$ and $(H'K)/K = H'/K$. It remains to show that $(H/K)' = H'/K$

($\subseteq$) Let $x \in (H/K)'$ be a commutator. Then $x = [u, v]$ for some $u, v \in H/K$. We have $u = h_1K$ and $v = h_2K$ for some $h_1, h_2 \in H$. Then

$$\begin{aligned} x &= [h_1K, h_2K] \\ &= (h_1K)(h_2K)(h_1K)^{-1}(h_2K)^{-1} \\ &= (h_1h_2h_1^{-1}h_2^{-1})K \\ &= [h_1, h_2]K \in H'/K. \end{aligned}$$

Now let $x \in (H/K)'$ be any element. Then $x = c_1c_2 \cdots c_n$ for $c_1, c_2, ..., c_n \in H/K$ all commutators (by Lemma 1.2.2). Each $c_i \in H'/K$, so $x \in H'/K$. Therefore, $(H/K)' \subseteq H'/K$.

($\supseteq$) Let $x \in H'/K$ be such that $x = hK$ where $h = [u, v] \in H'$ is a commutator (where $u, v \in H$). Then

$$\begin{aligned} x &= [u, v]K \\ &= (uvu^{-1}v^{-1})K \\ &= (uK)(vK)(uK)^{-1}(vK)^{-1} \\ &= [uK, vK] \in (H/K)' \end{aligned}$$

Now let $x \in H'/K$ be any element. Then $x = hK$ for some $h \in H'$. Then, by Lemma 1.2.2, $h = c_1 \cdots c_n$ for $c_1, ..., c_n \in H$ all commutators. Then each $c_iK \in (H/K)'$, and

$$x = (c_1c_2 \cdots c_n)K = (c_1K)(c_2K)\cdots(c_nK) \in (H/K)'$$

so that $(H/K)' \supseteq H'/K$.

Therefore, $(H/K)' = H'/K$, as required. □

Lemma 2.4.6. *Suppose G is a group. Let H and K be subgroups of G, such that K is a normal subgroup of G of smallest order. Suppose further that if N_1, N_2 are normal subgroups of HK then $|N_1|$ cannot divide $|(HK)/N_2|$. Then $(HK)' = H'K$.*

Proof. Suppose G is a group such that if N_1, N_2 are normal subgroups of G then $|N_1|$ cannot divide $|G/N_2|$. Let H and K be subgroups of G, such that K is a normal subgroup of G of smallest order. We wish to show that $(HK)' = H'K$.

HK and $H'K$ are groups by Proposition 2.4.2. If $k \in K$ and $g \in HK$ then $g = hk_1$ for some $h \in H$ and $k_1 \in K$, and so

$$(hk_1)k(hk_1)^{-1} = h(k_1kk_1^{-1})h^{-1} \in K$$

as $K \trianglelefteq G$. Thus $K \trianglelefteq HK$. Therefore, $K \trianglelefteq H'K$, as $H'K \subseteq HK$ (since $H' \subseteq H$).

If $n \in H'K$ and $g \in HK$ then $n = h_1k_1$ and $g = hk$ for some $h_1 \in H'$, $h \in H$, $k_1, k \in K$. Let

$$\begin{aligned} h_2 &= hh_1h^{-1} \in H' \\ k_2 &= hkh^{-1} \in K \\ k_3 &= hk_1k^{-1}h^{-1} \in K \\ k_4 &= h_2^{-1}k_2h_2 \in K \end{aligned}$$

because $H' \trianglelefteq H$ and $K \trianglelefteq HK$ (note $H \subseteq HK$ so e.g. $h \in HK$ for the second equality here). We have:

$$\begin{aligned} gng^{-1} &= hkh_1k_1k^{-1}h^{-1} \\ &= hkh^{-1}hh_1k_1k^{-1}h^{-1} \\ &= k_2hh_1k_1k^{-1}h^{-1} \\ &= k_2hh_1h^{-1}hk_1k^{-1}h^{-1} \\ &= k_2h_2k_3 \\ &= h_2h_2^{-1}k_2h_2k_3 \\ &= h_2k_4k_3 \in H'K \end{aligned}$$

and so $H'K \trianglelefteq HK$.

($\subseteq$) We have that

$$(HK)/(H'K) \cong ((HK)/K)/((H'K)/K) = ((HK)/K)/(((HK)/K)')$$

the isomorphism being by Lemma 1.1.5, and the equality by Lemma 2.4.5. The last term is Abelian by Lemma 1.2.5, and hence the first term is Abelian by Lemma 1.4.2. Therefore, by Lemma 1.2.6, $(HK)' \subseteq H'K$.

($\supseteq$) Suppose $K \not\subseteq (HK)'$. Then $K \cap (HK)' \neq K$, and clearly $K \cap (HK)' \subseteq K$, so $|K \cap (HK)'| < |K|$. But $K \trianglelefteq (HK)$ and $(HK)' \trianglelefteq (HK)$, so $K \cap (HK)' \trianglelefteq (HK)$, by Proposition 2.1.8. Therefore, $K \cap (HK)'$ must be trivial, or it would contradict the minimality of K.

Define the map

$$\phi : (HK)' \mapsto (HK)/K; x \mapsto xK$$

which is a homomorphism since if $x, y \in (HK)'$ then

$$\phi(x)\phi(y) = (xK)(yK) = (xy)K = \phi(xy).$$

Also we have

$$\begin{aligned} \ker(\phi) &= \{x \in (HK)' : xK = K\} \\ &= \{x \in (HK)' : x \in K\} \\ &= (HK)' \cap K \\ &= \{\mathrm{id}_G\}. \end{aligned}$$

Therefore, by the First Isomorphism Theorem,

$$(HK)' \cong (HK)'/ker(\phi) \cong \mathrm{im}(\phi)$$

and so

$$|(HK)'| = |\operatorname{im}(\phi)| \mid |(HK)/K|.$$

However $(HK)' \trianglelefteq HK$ and $K \trianglelefteq HK$, so this is a contradiction. Therefore we must have $K \subseteq (HK)'$.

As $H \leqslant (HK)'$ then $H' \leqslant (HK)'$. If $x \in H'K$ then $x = hk$ for some $h \in H'$, $k \in K$. Thus $h \in (HK)'$, $k \in (HK)'$, so $x = hk \in (HK)'$, and so $(HK)' \supseteq H'K$. □

The following is known as The Frattini Argument. Since we will use a slightly modified version of it later, we shall "wrap up" the core of the argument in an initial lemma, with less restrictive conditions.

LEMMA 2.4.7. *If G is a finite group, K is a normal subgroup of G and P is a subgroup of K, such that for all $g \in G$, gPg^{-1} is conjugate to P in K, then $G = K\,\mathrm{N}_G(P)$.*

PROOF. Let G be a finite group, K be a normal subgroup of G and P be a subgroup of K, such that for all $g \in G$, gPg^{-1} is conjugate to P in K. Let $g \in G$. So for some $k \in K$ we have $kPk^{-1} = gPg^{-1}$. Let $x = k^{-1}g$, then $xPx^{-1} = (k^{-1}g)P(g^{-1}k) = k^{-1}(kPk^{-1})k = P$, and so $x \in \mathrm{N}_G\,P$. But $g = kx$, so $g \in K\,\mathrm{N}_G(P)$. Therefore $G \subseteq K\,\mathrm{N}_G(P)$. However it is clear that $K\,\mathrm{N}_G(P) \subseteq G$, so the result follows. □

PROPOSITION 2.4.8 (The Frattini Argument). *If G is a finite group, K is a normal subgroup of G and P is a Sylow p-subgroup of K, then $G = K\,\mathrm{N}_G(P)$.*

PROOF. Let G be a finite group, K be a normal subgroup of G and P be a Sylow p-subgroup of K. Take any $g \in G$, then P and gPg^{-1} are conjugate in K, by Sylow's Second Theorem. The result follows by Lemma 2.4.7. □

We state a useful lemma which sometimes works in unison with the Frattini Argument.

LEMMA 2.4.9. *If G is a finite group and H a subgroup, then $\mathrm{N}_G(H) = H\,\mathrm{N}_G(H)$.*

PROOF. Let G be a finite group and H a subgroup. Clearly

$$\mathrm{N}_G(H) \subseteq H\,\mathrm{N}_G(H).$$

Now if $h_1 \in H, h_2 \in \mathrm{N}_G(H)$, then

$$(h_1h_2)H(h_1h_2)^{-1} = h_1h_2Hh_2^{-1}h_1^{-1} = h_1Hh_1^{-1}$$

since h_2 is in the normalizer. But this last term is just $h_1Hh_1^{-1} = H$, as $h_1 \in H$. Therefore, $h_1h_2 \in \mathrm{N}_G(H)$, and so $\mathrm{N}_G(H) \supseteq H\,\mathrm{N}_G(H)$. □

2.5. An important special case of the Hall Theory

The following case will be dealt with separately.

LEMMA 2.5.1. *Let G be a finite solvable group and π a set of primes. Suppose that G has a non-trivial normal subgroup N such that G/N is not a π-group. Then Theorem 2.2.1 holds for G.*

PROOF. Suppose the statement of the result were false, and let G be a counterexample of minimum order. Let N be a non-trivial normal subgroup of G such that G/N is not a π-group. Since N is non-trivial, $|G/N| < |G|$, so Theorem 2.2.1 must hold for G/N, otherwise G/N would contradict the minimality of G.

(i) As Hall's First Theorem holds for G/N, G/N has a Hall π-subgroup, say K/N (here we are invoking Lemma 1.1.1, and we have that $K \leqslant G$ and $N \trianglelefteq K$). Since K/N is a π-group and G/N is not, then $K/N \neq G/N$, so $K \neq G$. Let

H be a Hall π-subgroup of K. Then $|H|$ is a π'-number, and $[K : H]$ is a π'-number. Note also that $[G : K] = [G/N : K/N]$ is a π'-number. Therefore, $[G : H] = [G : K][K : H]$ is a π'-number, and so H is a Hall π-subgroup of G. Therefore, Hall's First Theorem holds for G.

(ii) Let H_1, H_2 be two Hall π-subgroups of G. By Proposition 2.4.2, NH_1 is a group, and since $N \trianglelefteq G$, $N \trianglelefteq NH_1$. Therefore, $(NH_1)/N$ is a group, and furthermore it has order equal to that of H_1, therefore it is a π-group. Also $[G/N : (NH_1)/N] = [G : NH_1]$ and $[G : NH_1][NH_1 : H_1] = [G : H_1]$ so $[G/N : (NH_1)/N] \mid [G : H_1]$, a π'-number. Therefore $[G/N : (NH_1)/N]$ is itself a π'-number, and so $(NH_1)/N$ is a Hall π-subgroup of G/N. Similarly, $(NH_2)/N$ is a Hall π-subgroup of G/N.

As Hall's Second Theorem holds for G/N, $(NH_1)/N$ and $(NH_2)/N$ are conjugate in G/N. Therefore there exists $gN \in G/N$ with

$$(gN)((NH_1)/N)(gN)^{-1} = (NH_2)/N$$

. We have:

$$\begin{aligned}(NH_2)/N &= (gN)((NH_1)/N)(gN)^{-1} \\ &= \{(gN)(hN)(gN)^{-1} : hN \in (NH_1)/N\} \\ &= \{ghg^{-1}N : hN \in (NH_1)/N\} \\ &= \{ghg^{-1}N : h \in NH_1\} \\ &= \{xN : x \in g(NH_1)g^{-1}\} \\ &= (g(NH_1)g^{-1})/N\end{aligned}$$

so that $NH_2 = g(NH_1)g^{-1}$. Then:

$$\begin{aligned}NH_2 &= g(NH_1)g^{-1} \\ &= \{gnh_1g^{-1} : n \in N, h_1 \in H_1\} \\ &= \{gng^{-1}gh_1g^{-1} : n \in N, h_1 \in H_1\} \\ &= \{n'gh_1g^{-1} : n' \in N, h_1 \in H_1\} \\ &= N(gH_1g^{-1})\end{aligned}$$

the penultimate inequality being because $gNg^{-1} = N$, as N is normal. The group gH_1g^{-1} is a subgroup of $N(gH_1g^{-1})$ and hence of NH_2. Furthermore, it is a π-group (so is H_2). Also, $[G : (gH_1g^{-1})] = [G : H_2]$, a π'-number, and so $[NH_2 : (gH_1g^{-1})] = [NH_2 : H_2]$ is a π'-number, as it divides $[G : H_2]$ (the quotient is $[G : NH_2]$, which is an integer as NH_2 is a group by Proposition 2.4.2). Therefore, H_2 and (gH_1g^{-1}) are Hall π-subgroups of NH_2.

Suppose $G = NH_2$. Then, by Proposition 2.4.3,

$$|G| = \frac{|N||H_2|}{|N \cap H_2|}$$

so

$$|G/N| = \frac{|G|}{|N|} = \frac{|H_2|}{|N \cap H_2|}.$$

Now if $p \mid |G/N|$ then

$$p \mid \frac{|H_2|}{|N \cap H_2|}$$

so p divides $|H_2|$, so $p \in \pi$. Therefore, G/N is a π-group, a contradiction.

Therefore, $NH_2 \neq G$. So $|NH_2| < |G|$, and so Theorem 2.2.1 holds for NH_2. Therefore, H_2 and (gH_1g^{-1}) are conjugate in NH_2, i.e. there exists $k \in H_2$ with $k(gH_1g^{-1})k^{-1} = H_2$, and so H_1 and H_2 are conjugate in G (by kg). Therefore, Hall's Second Theorem holds for G.

(iii) Let J be a π-subgroup of G. Then NJ is a group, and since $N \trianglelefteq G$, then $N \trianglelefteq NJ$. So $(NJ)/N$ is a subgroup of G/N, and since Theorem 2.2.1 holds for the latter, then (NJ/N) is contained in a Hall π-subgroup of G/N. By Lemma 1.1.1, this π-subgroup can be written as L/N, where $N \trianglelefteq L$ and $L \leqslant G$. Then $J \subseteq NJ \subseteq L$ and so $J \leqslant L$. L is not equal to G, as otherwise $G/N = L/N$ would be a π-group. Therefore, $|L| < |G|$, and Theorem 2.2.1 holds for L. So there is a Hall π-subgroup of L, say H, which contains J. We have that

$$[G : H] = [G : L][L : H] = [G/N : L/N][L : H]$$

a product of two π'-numbers, hence a π'-number itself. Now H is a Hall π-subgroup of G and $J \leqslant H$. Therefore, Hall's Third Theorem holds for G. □

2.6. The Remaining Case

Before tackling the remaining cases, we shall give a preliminary lemma.

Lemma 2.6.1. *If G is a group, $A, B \leqslant G$ and $([G : A], [G : B]) = 1$ then $[G : A \cap B] = [G : A][G : B]$.*

Proof. Let G be a group, $A, B \leqslant G$ with $([G : A], [G : B]) = 1$. Then:

$$\begin{aligned}
[G : A \cap B] &= [G : A][G : A \cap B] \\
&= [G : A]\frac{|G|}{|A \cap B|} \\
&= [G : A]\frac{|AB|}{|B|} \\
&\leq [G : A]\frac{|G|}{|B|} \\
&= [G : A][G : B]
\end{aligned}$$

the third equality being from Proposition 2.4.3.

Also, since $[G : A], [G : B] \mid [G : A \cap B]$ (the quotients being $[A : A \cap B]$ and $[B : A \cap B]$, respectively). Therefore, $[G : A][G : B] \mid [G : A \cap B]$, and so $[G : A][G : B] \leq [G : A \cap B]$.

Taking these two inequalities together gives $[G : A \cap B] = [G : A][G : B]$. □

The following argument will be used more than once in the proof, so it is convenient to give it here.

LEMMA 2.6.2. *Let G be a group, π a set of primes, H a Hall π-subgroup of G, and K a Hall π'-subgroup of G. Then $G = KH = HK$.*

PROOF. Let G be a group, π a set of primes, H a Hall π-subgroup of G, and K a Hall π'-subgroup of G.

Suppose that H is trivial. Then none of the primes in π divide the order of G, and so G is a π'-group. Then K, being a maximal Hall π'-subgroup of G (by Lemma 2.1.5), has to equal G. We have that $G = \{id_G\}G = HK$ and $G = G\{id_G\} = KH$, and so we are done. For the rest of the proof therefore, we can assume that H is non-trivial.

First, as $[G : K]$ is a π-number, and divides $[G : K]|K| = |G|$, then we must have $[G : K] \leq |H|$, as $|H|$ is the maximal π-number dividing $|G|$, by Lemma 2.1.5.

Secondly, as H is a subgroup of G, $|H|$ divides $|G| = [G : K]|K|$, and so $|H|$ divides either $|K|$ or $[G : K]$. However $|H|$ is a π-number (and does not equal 1 as H is non-trivial), and $|K|$ is a π'-number, so we cannot have that $|H|$ divides $|K|$. Therefore, $|H|$ divides $[G : K]$, so $|H| \leq [G : K]$.

Taking these two inequalities together gives $[G : K] = |H|$, that is,

$$|G| = |K|[G : K] = |K| \cdot |H|.$$

However, as $|K|$ is a π'-number and $|H|$ is a π-number, then by Corollary 2.1.9, $|K \cap H| = 1$. Therefore, by Proposition 2.4.3,

$$|G| = |K| \cdot |H| = |KH| \cdot |K \cap H| = |KH|.$$

Similarly,

$$|G| = |H| \cdot |K| = |HK| \cdot |H \cap K| = |HK| \cdot |K \cap H| = |HK|.$$

Clearly $KH \subseteq G$ and $HK \subseteq G$, so the fact that they have the same order gives that $G = KH = HK$, as required. □

We can now deal with the remaining case.

PROOF OF THEOREM 2.2.1. Let G be a finite solvable group, and π be a set of primes. If G is a π-group or a π'-group then the theorem holds by Lemma 2.2.2, and if G has a non-trivial normal subgroup N with G/N not a π-group, then the theorem holds by Lemma 2.5.1. Therefore, we may assume that neither of these hold. That is, G is not a π-group or a π'-group, and every non-trivial normal subgroup N of G is a π-group.

We have that for any $p \in \pi$, and a non-trivial Sylow p-subgroup P of G, that Theorem 2.2.1 holds for $\mathrm{N}_G(P)$. To see this, suppose for a contradiction that $G = \mathrm{N}_G(P)$. Then P must be a normal subgroup, as any element of G normalizes P. Also, P is non-trivial. Therefore G/P is a π-group, and so $|G| = |G/P| \cdot |P|$ is a π-number (as also $p \in \pi$). Therefore, G is a π-group, contradiction. So we must have that $\mathrm{N}_G(P) \neq G$, and so $|\mathrm{N}_G(P)| < |G|$, so Theorem 2.2.1 holds for $\mathrm{N}_G(P)$.

Let A be a non-trivial normal subgroup of G of smallest order. Then G/A is a π-group. Also, A is an elementary Abelian p-group for some prime p, by Lemma 2.3.3. If $p \in \pi$, then $|G| = |G/A||A|$ would be a π-number, and so G

would be a π-group, which we have assumed it to not be. Therefore, $p \notin \pi$, and so A is a π'-group.

(i) Take a normal subgroup of G/A of smallest order, which by Lemma 1.1.3, we can write as B/A, where $A \trianglelefteq B$ and $B \trianglelefteq G$. Then, B/A is a q-group, by Lemma 2.3.3. Since $q \mid |G/A|$, we must have $q \in \pi$, and so $q \neq p$.

Let Q be a Sylow q-subgroup of B. Then Q is non-trivial, as

$$q \mid |B/A| \mid |B/A||A| = |B|.$$

We have that $B = AQ$, by Lemma 2.6.2. Therefore, by the Frattini Argument and then Lemma 2.4.9, we have:

$$G = B\,\mathrm{N}_G(Q) = AQ\,\mathrm{N}_G(Q) = A\,\mathrm{N}_G(Q).$$

Notice that

$$[G : \mathrm{N}_G(Q)] = \frac{|G|}{|\,\mathrm{N}_G(Q)|} = \frac{|A\,\mathrm{N}_G(Q)|}{|\,\mathrm{N}_G(Q)|} = \frac{|A|}{|A \cap \mathrm{N}_G(Q)|}$$

the last equality being because of Proposition 2.4.3. However, considering the last term on the right, the numerator is a power of p and the denominator is also a power of p (as it must divide $|A|$ by Proposition 2.1.8 and Lagrange's Theorem). Therefore, $[G : \mathrm{N}_G(Q)]$ is a power of p. By an argument at the start of this proof, Theorem 2.2.1 holds for $\mathrm{N}_G(Q)$.

By Hall's First Theorem in $\mathrm{N}_G(Q)$, there exists a Hall π-subgroup H of $\mathrm{N}_G(Q)$. H is a π-group, and

$$[G : H] = [G : \mathrm{N}_G(Q)][\mathrm{N}_G(Q) : H].$$

The first term in the product is π' as it is a power of p and $p \notin \pi$, and the second term is π' as H is a Hall π-subgroup of $\mathrm{N}_G(Q)$. Therefore, $[G : H]$ is π', and H is a Hall π-subgroup of G. Therefore, Hall's First Theorem holds for G.

(ii) We shall split this into two cases, depending on whether G/A is Abelian.

(ii.1) First consider the case where G/A is Abelian. Take any Hall π-subgroup of G, say H. Consider the map

$$\phi : H \mapsto G/A; x \mapsto xA.$$

This map is an homomorphism: take $x, y \in H$ and then

$$\phi(xy) = (xy)A = (xA)(yA) = \phi(x)\phi(y).$$

It is onto: take any $B \in G/A$, and some $x \in B$, then $\phi(x) = xA = B$, the last equality being as $x \in xA$. G/A has the same order as a Hall π-subgroup, as $|G/A|$ is a π-number, and

$$\frac{|G|}{|G/A|} = |A|$$

which is a power of p, hence a π'-number (since $p \notin \pi$). Therefore, ϕ is order-preserving, hence 1-1, hence an isomorphism. We shall use this to show that H is Abelian: take any $x, y \in H$. Then $\phi(xy) = \phi(x)\phi(y) = \phi(y)\phi(x) = \phi(yx)$, so taking inverses (which we can do since ϕ is a bijection) gives $xy = yx$.

Let q be any prime dividing the order of G/A. Let Q be a Sylow q-subgroup of G (then Q is non-trivial since q divides $|G/A|$, which divides $|G/A||A| = |G|$), and $\overline{Q}$ be a Sylow q-subgroup of H. By an argument at the start of this proof, Theorem 2.2.1 holds for $\mathrm{N}_G(Q)$.

The group $\overline{Q}$ is a Sylow q-subgroup of G, since $q \in \pi$ and so cannot divide $[G : H]$, a π'-number, hence q cannot divide $[G : H][H : \overline{Q}]$ (as $\overline{Q}$ is a Sylow q-subgroup of H, so q does not divide $[H : \overline{Q}]$). Therefore, by Sylow's Second Theorem, Q and $\overline{Q}$ are conjugate in G.

Take any $h \in H$. We wish to show that $h \in \mathrm{N}_G(\overline{Q})$. So take any $q \in \overline{Q}$. Then $q \in H$, and as H is Abelian, $qh = hq$ so $hqh^{-1} = q$. Therefore, as q was arbitrary, $h\overline{Q}h^{-1} = \overline{Q}$, and so $h \in \mathrm{N}_G(\overline{Q})$. Therefore, $H \leqslant \mathrm{N}_G(\overline{Q})$.

Now let $g \in G$ be such that Q and $\overline{Q}$ are conjugate by g. Then $Q = g\overline{Q}g^{-1}$, and so

$$\begin{aligned}
g\,\mathrm{N}_G(\overline{Q})g^{-1} &= \{gng^{-1} : n \in \mathrm{N}_G(\overline{Q})\} \\
&= \{gng^{-1} : n \in G, (\forall h \in \overline{Q})(hnh^{-1} = n)\} \\
&= \{m : g^{-1}mg \in G, (\forall h \in \overline{Q})(hg^{-1}mgh^{-1} = g^{-1}mg)\} \\
&= \{m : m \in G, (\forall h \in \overline{Q})(hg^{-1}mgh^{-1} = g^{-1}mg)\} \\
&= \{m : m \in G, (\forall h \in \overline{Q})(ghg^{-1}mgh^{-1}g^{-1} = m)\} \\
&= \{m : m \in G, (\forall q \in Q)(qmq^{-1} = m)\} \\
&= \mathrm{N}_G(Q)
\end{aligned}$$

therefore H is conjugate to a subgroup of $\mathrm{N}_G(Q)$, say K. K has the same order as H, and hence is a π-group; also $[\mathrm{N}_G(Q) : K]$ divides $[G : K] = [G : H]$ (the quotient is $[G : \mathrm{N}_G(K)]$) and therefore is a π'-number. Hence H is conjugate to a Hall π-subgroup of $\mathrm{N}_G(Q)$.

Now take any two Hall π-subgroups of G, say H_1 and H_2. H_1 is conjugate to some Hall π-subgroup of $\mathrm{N}_G(Q)$, say H_3, and H_2 is conjugate to some other Hall π-subgroup of $\mathrm{N}_G(Q)$, say H_4. By Hall's Second Theorem in $\mathrm{N}_G(Q)$, H_3 and H_4 are conjugate. Therefore, H_1 is conjugate to H_3, which is conjugate to H_4, which is conjugate to H_2. So H_1 and H_2 are conjugate, and Hall's Second Theorem is true for G.

(ii.2) Suppose G/A is non-Abelian and let H be a Hall π-subgroup of G. Then $G = HA$, by Lemma 2.6.2. We have that $A \trianglelefteq G$. If
$N_1, N_2 \trianglelefteq HA = G$ then $|G/N_2|$ is a π-number. If $|N_1|$ divides $|(HA)/N_2| = |G/N_2|$, then $|N_1|$ would also be a π-number. However, $|G/N_1|$ is a π-number, and so $|G| = |G/N_1||N_1|$ is a π-number, a contradiction. Therefore, we can apply Lemma 2.4.6 to obtain $G' = H'A$.

Now, $G' \trianglelefteq G$, $H' \leqslant G'$ by Lemmas 1.2.4 and 1.2.7. We have $G' \neq G$, since otherwise G would not be solvable. So $|G'| < |G|$, and Theorem 2.2.1 holds for G'. Now H' is a π-group, as if p divides $|H'|$ then p divides $|H|$ (as $H' \leqslant H$ and we can use Lagrange) and so $p \in \pi$. Furthermore ($[G' : H']$ is π', as if it wasn't, there would exist a prime in π dividing $[G' : H']$, but then this prime would also divide $[G' : H'][H' : H] = [G : H]$, a contradiction as H is a Hall π-subgroup of G). Therefore H' is a Hall π-subgroup of G'.

Since $H' \subseteq G'$ and $G' \trianglelefteq G$, then $gH'g^{-1} \leqslant G'$ for any $g \in G$. Therefore $gH'g^{-1}$, having the same order as H', is also a Hall π-subgroup of G', and Hall's

Second Theorem in G' gives that H is conjugate to gHg^{-1} in G'. Then the core Frattini Argument, Lemma 2.4.7, gives that $G = G' \operatorname{N}_G(H')$. This gives $G = AH' \operatorname{N}_G(H') = A \operatorname{N}_G(H')$, the second equality being from Lemma 2.4.9.

Now take any two Hall π-subgroups of G, say H_1 and H_2. From the above work, we have that H_1' and H_2' are Hall π-subgroups of G' and Theorem 2.2.1 holds for G', so that H_1' and H_2' are conjugate in G'. Let $h \in G'$ be an element they are conjugate by, so that $hH_1'h^{-1} = H_2'$.

Note that if $u, v \in H_1$ then

$$\begin{aligned} h[u,v]h^{-1} &= huvu^{-1}v^{-1}h^{-1} \\ &= huh^{-1}hvh^{-1}hu^{-1}h^{-1}hv^{-1}h^{-1} \\ &= (huh^{-1})(hvh^{-1})(huh^{-1})^{-1}(hvh^{-1})^{-1} \\ &= [huh^{-1}, hvh^{-1}] \end{aligned}$$

so that

$$\begin{aligned} &(hH_1h^{-1})' \\ &= \{[hu_1h^{-1}, hv_1h^{-1}][hu_2h^{-1}, hv_2h^{-1}] \cdots [hu_nh^{-1}, hv_nh^{-1}] : u_i, v_i \in H_1\} \\ &= \{(h[u_1,v_1]h^{-1})(h[u,v]h^{-1}) \cdots (h[u_n,v_n]h^{-1}) : u_i, v_i \in H_1\} \\ &= \{h[u_1,v_1][u_2,v_2] \cdots [u_n,v_n]h^{-1} : u_i, v_i \in H_1\} \\ &= hH_1'h^{-1} \end{aligned}$$

where the first and last equalities come from Lemma 1.2.2.

Now H_2 is a π-group and a subgroup of $\operatorname{N}_G(H_2')$ (as $H_2' \trianglelefteq H_2$), and $[\operatorname{N}_G(H_2') : H_2]$ divides $[G : H_2]$ (the quotient is $[G : \operatorname{N}_G(H_2')]$), a π'-number. Therefore, H_2 is a Hall π-subgroup of $\operatorname{N}_G(H_2')$. Since $|hH_1h^{-1}| = |H_1| = |H_2|$, and hH_1h^{-1} is also a subgroup of $\operatorname{N}_G((hH_1h^{-1})') = \operatorname{N}_G(hH_1'h^{-1}) = \operatorname{N}_G(H_2')$ (as $(hH_1h^{-1})' \trianglelefteq hH_1h^{-1}$), we have that hH_1h^{-1} is a Hall π-subgroup of $\operatorname{N}_G(H_2)$ as well.

Suppose $\operatorname{N}_G(H_2) = G$. Then H_2 is a normal subgroup of G. Furthermore, it is a π-group. We have that $[G : H_2]$ is a π-number, and so $|G| = [G : H_2]|H_2|$ is also a π-number, contradiction. Thus $\operatorname{N}_G(H_2) \neq G$, and since $\operatorname{N}_G(H_2) \subseteq G$, we have that $|\operatorname{N}_G(H_2)| < |G|$. Therefore, Hall's Second Theorem holds for $\operatorname{N}_G(H_2)$.

Thus hH_1h^{-1} and H_2 are conjugate in $\operatorname{N}_G(H_2)$, say by an element n, so that $n(hH_1h^{-1})n^{-1} = H_2$. Then

$$(nh)H_1(nh)^{-1} = nhH_1h^{-1}n^{-1} = H_2$$

so that H_1 and H_2 are conjugate in G (namely by nh). Therefore, Hall's Second Theorem holds for G.

(iii) Let J be a π-subgroup of G. Suppose $G = AJ$. Then

$$|G| = \frac{|A| \cdot |J|}{|A \cap J|} = |A| \cdot |J|$$

by Corollary 2.1.9. Therefore,

$$[G : J] = \frac{|G|}{|J|} = \frac{|A| \cdot |J|}{|J|} = |A|$$

which is a π'-number. So J is itself a Hall π-subgroup of G, and certainly $J \subseteq J$, so Hall's Third Theorem is true for G in this case.

Now suppose $G \neq AJ$. We have that $|AJ| = |A| \cdot |J|$, by Proposition 2.4.3 (as $|A \cap J| = 1$ by Corollary 2.1.9). So

$$[G : AJ] = \frac{|G|}{|AJ|} = \frac{|G|}{|A| \cdot |J|} = \frac{[G : A]}{|J|}$$

the quotient of two π-numbers, hence a π-number.

Let H be any Hall π-subgroup of G. Then $[G : H]$ is a π'-number. By Lemma 2.6.1, we have that $[G : H \cap AJ] = [G : H][G : AJ]$, and so $[G : H \cap AJ] = |A|[G : AJ] = [G : J]$ (as $[G : A]$, being a π number with $\frac{|G|}{[G:A]}$ a π'-number, is the order of a Hall π-subgroup, and hence $[G : A] = |H|$, so $[G : H] = |A|$). So $|H \cap AJ| = |J|$.

We know A is normal in G so AJ is a group, and $H \cap J \leqslant J \leqslant AJ$. Also note that $|H \cap AJ| = |J|$ is a π-number and $[AJ : H \cap J] = [AJ : J] = |A|$ is a π'-number, so J and $H \cap AJ$ are Hall π-subgroups of AJ. As $G \neq AJ$, $AJ \subseteq G$, we have $|AJ| < |G|$. Therefore, Theorem 2.2.1 holds for AJ, and so J and $H \cap AJ$ are conjugate in AJ, hence in G. Let g be an element which they are conjugate by. Then

$$J = g(H \cap AJ)g^{-1} \subseteq gHg^{-1}$$

and the latter term has the same order as H, so is a Hall π-subgroup of G. Therefore, Hall's Third Theorem holds for G. □

CHAPTER 3

The Extension Classification Schema

3.1. Isomorphism Classes

Recall that two groups are isomorphic if there exists a bijective homomorphism between them. We say that $G \cong H$ if the groups are isomorphic, and we say that the bijective homomorphism is an isomorphism.

LEMMA 3.1.1. $\cong$ *is an equivalence relation.*

SKETCH OF PROOF. For groups G, H, K, and isomorphisms $\phi_1 : G \mapsto H$, $\phi_2 : H \mapsto K$, the identity map $G \mapsto G$ is an isomorphism, the inverse map $(\phi_1)^{-1} : H \mapsto G$ is an isomorphism and the composition $(\phi_2 \circ \phi_1) : G \mapsto K$ is an isomorphism. □

Because of this, $\cong$ splits the class of all groups into "equivalence classes". However, these are not true equivalence classes, as the collection of all groups cannot ever form a set in the traditional sense. We can consider them to be equivalence classes, however, and certainly we can take a complete set of representatives from the equivalence classes. This set will in fact only be countably infinite, in light of the following result:

LEMMA 3.1.2. *If n is a positive integer, there exists a finite set π_n of groups such that if G is any group of order n, then G is isomorphic to one of the groups in π_n.*

PROOF. Define a magma as an arbitrary set X equipped with a binary operation $X \times X \mapsto X$. The idea of a group isomorphism is identical for magmas, and any group must itself be a magma. Now, any magma is completely described (up to isomorphism) by a Cayley table showing the result of applying the operation to any pair of elements, and each Cayley table corresponds to a magma (e.g by taking the set $\{1, ..., n\}$). There are n^2 elements in the table if $|X| = n$, and each element in the table can be chosen in n ways, so the number of possible tables is n multiplied by itself n^2 times, or n^{n^2} possible tables. Therefore, the set of all magmas of order n (say, T_n) has size n^{n^2}, and hence is finite. Now let π_n be the set of magmas in T_n which are also groups. This set is clearly finite. □

So therefore we have the existence of a finite complete set of representatives for the "isomorphism classes", because it is just equal to $\bigcup_n \pi_n$ above.

We call each set π_n a classification of the groups of order n, or an enumeration of them a list of groups of order n up to isomorphism:

Definition 3.1.3. Let $G_1, ..., G_n$ be a sequence of groups. We say that $G_1, ..., G_n$ is a list of groups with property P (for some property P) up to isomorphism, if:

(1) For each i with $1 \leq i \leq n$, G_i has property P.
(2) Every group which has property P is isomorphic to G_i for some i with $1 \leq i \leq n$.
(3) For each i, j with $1 \leq i \leq n$, $1 \leq j \leq n$ and $i \neq j$, G_i and G_j are not isomorphic.

Definition 3.1.4. Let S be a finite set of groups. We say that S is a classification of groups with property P (for some property P), if there is an enumeration $G_1, ..., G_n$ of the groups in S which is a list of groups with property P up to isomorphism.

We shall give some examples of this:

Examples 3.1.5.

(i) The sequence C_6, S_3 is a list of groups of order 6 up to isomorphism.
(ii) The set $\{C_4, C_2 \times C_2\}$ is a classification of groups of order 4.
(iii) The sequence $C_{10}, C_5 \times C_2, D_5$ is not a list of groups of order 10 up to isomorphism, as $C_{10} \cong C_5 \times C_2$.
(iv) The empty set is a classification of non-Abelian prime-order groups.

Our aim is to classify some groups of order pqr. In this chapter, we shall present The Extension Classification Schema, which is a much more powerful result than we need for the order pqr case. However, it shall give us all we need in order to present the classification of groups of order pqr.

3.2. Semidirect Products

We know the direct product well, both in its internal and external forms. If a group is the internal direct product of two of its subgroups, then both have to be normal. If we relax the condition so that only one of them has to be normal, we get something called the semidirect product, and this has a fairly simple external analog. (In fact, if we require neither to be normal, we get something called the Zappa-Szep Product (discovered independently by Zappa and Szep in the 1940s), but the external analog of this is much more complicated).

First we consider the internal semidirect product.

Definition 3.2.1. Let G be a group with subgroups N and H. Then G is said to be the **internal semidirect product** of N and H, if $N \trianglelefteq G$, $G = NH$, and $N \cap H$ is trivial.

The analog to this is the external semidirect product.

Definition 3.2.2. Let H, K be groups, and $\sigma \in \mathrm{Hom}(K, \mathrm{Aut}(H))$. Then the **external semidirect product** of H and K with respect to σ, is the magma whose underlying set is $H \times K$ (where $\times$ is the cartesian product of sets) and whose operation is defined by:

$$(h_1, k_1)(h_2, k_2) = (h_1\sigma(k_1)(h_2), k_1k_2).$$

We denote the external semidirect product of H and K with respect to σ by $H \rtimes_\sigma K$.

Proposition 3.2.3. *Let H, K be groups, and $\sigma \in \mathrm{Hom}(K, \mathrm{Aut}(H))$. Then $H \rtimes_\sigma K$ is a group.*

Proof. Let H, K be groups, and $\sigma \in \mathrm{Hom}(K, \mathrm{Aut}(H))$. Let $G = H \rtimes_\sigma K$. Since the underlying set of G is the set cartesian product of two non-empty sets, G is non-empty.

We shall check associativity for the group operation. Suppose $x_1, x_2, x_3 \in G$. Then $x_1 = (h_1, k_1), x_2 = (h_2, k_2) and x_3 = (h_3, k_3)$ for some $h_1, h_2, h_3 \in H$ and $k_1, k_2, k_3 \in K$. Now:

$$\begin{aligned}
(x_1x_2)x_3 &= ((h_1, k_1)(h_2, k_2))(h_3, k_3)\\
&= (h_1\sigma(k_1)(h_2), k_1k_2)(h_3, k_3)\\
&= (h_1\sigma(k_1)(h_2)\sigma(k_1k_2)(h_3), k_1k_2k_3)\\
&= (h_1\sigma(k_1)(h_2)(\sigma(k_1) \circ \sigma(k_2))(h_3), k_1k_2k_3)\\
&= (h_1\sigma(k_1)(h_2)\sigma(k_1)(\sigma(k_2)(h_3)), k_1k_2k_3)\\
&= (h_1\sigma(k_1)(h_2\sigma(k_2)(h_3)), k_1k_2k_3)\\
&= (h_1, k_1)(h_2\sigma(k_2)(h_3), k_2k_3)\\
&= (h_1, k_1)((h_2, k_2)(h_3, k_3))
\end{aligned}$$

and so the group operation is associative.

Let $x \in G$, then $x = (h, k)$ for some $h \in H$, $k \in K$. Now:

$$\begin{aligned}
x(\mathrm{id}_H, \mathrm{id}_K) &= (h, k)(\mathrm{id}_H, \mathrm{id}_K)\\
&= (h\sigma(k)(\mathrm{id}_H), k\,\mathrm{id}_K)\\
&= (h\,\mathrm{id}_H, k)\\
&= (h, k)\\
&= x
\end{aligned}$$

and

$$\begin{aligned}
(\mathrm{id}_H, \mathrm{id}_K)x &= (\mathrm{id}_H, \mathrm{id}_K)(h, k)\\
&= (\mathrm{id}_H\,\sigma(\mathrm{id}_K)(h), \mathrm{id}_K\,k)\\
&= (\mathrm{id}_H\,h, k) = (h, k)\\
&= x
\end{aligned}$$

so the element $(\mathrm{id}_H, \mathrm{id}_K)$ acts like an identity.

Finally, again let $x \in G$ so that $x = (h, k)$ for some $h \in H$, $k \in K$. Let $y = ((\sigma(k^{-1}))(h^{-1}), k^{-1})$. Then:

$$\begin{aligned} yx &= ((\sigma(k^{-1}))(h^{-1}), k^{-1})(h, k) \\ &= ((\sigma(k^{-1}))(h^{-1})\sigma(k^{-1})(h), k^{-1}k) \\ &= ((\sigma(k^{-1}))(h^{-1})\sigma(k^{-1})(h), \mathrm{id}_K) \\ &= (\sigma(k^{-1})(h^{-1}h), \mathrm{id}_K) \\ &= (\sigma(k^{-1})(\mathrm{id}_H), \mathrm{id}_K) \\ &= (\mathrm{id}_H, \mathrm{id}_K) \end{aligned}$$

and

$$\begin{aligned} xy &= (h, k)((\sigma(k^{-1}))(h^{-1}), k^{-1}) \\ &= (h\sigma(k)((\sigma(k^{-1}))(h^{-1})), kk^{-1}) \\ &= (h(\sigma(k) \circ \sigma(k^{-1}))(h^{-1}), \mathrm{id}_K) \\ &= (h\sigma(kk^{-1})(h^{-1}), \mathrm{id}_K) \\ &= (h\sigma(\mathrm{id}_K)(h^{-1}), \mathrm{id}_K) \\ &= (hh^{-1}, \mathrm{id}_K) \\ &= (\mathrm{id}_H, \mathrm{id}_K) \end{aligned}$$

so the element y acts like an inverse for x.

Therefore, all the group axioms are satisfied, and so G is a group. □

We can see that the external semidirect product is indeed an analog of the internal one by the following proposition and Proposition 3.2.6.

Proposition 3.2.4. *Let G be a group with subgroups N and H. Suppose G is the internal semidirect product of N and H. Then there exists $\sigma \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ with $G \cong N \rtimes_\sigma H$.*

Proof. Let G be a group with subgroups N and H. Suppose G is the internal semidirect product of N and H. For each $h \in H$ let λ_h be defined by

$$\lambda_h : N \mapsto N; n \mapsto hnh^{-1}.$$

Clearly $\lambda \in \mathrm{Aut}(N)$. Now define a map σ by:

$$\sigma : H \mapsto \mathrm{Aut}(N); h \mapsto \lambda_h.$$

Clearly $\sigma \in \mathrm{Hom}(H, \mathrm{Aut}(N))$. Define a map ϕ by:

$$\phi : N \rtimes_\sigma H \mapsto G; (n, h) \mapsto nh$$

Our goal is to show that ϕ is an isomorphism.

First of all ϕ is onto. Take any $g \in G$. Then as G is the internal semidirect product of N and H then $G = NH$ so $g = nh$ for some $n \in N$, $h \in H$. Now $(n, h) \in N \rtimes_\sigma H$, and $\phi(n, h) = nh$.

Also $|N \rtimes_\sigma H| = |N| \cdot |H| = \frac{|N|\cdot|H|}{|N\cap H|} = |NH| = |G|$ since $G = NH$ and $|N \cap H| = 1$. Therefore, taken with the fact that ϕ is onto, ϕ is a bijection and hence 1-1.

Finally we must show that ϕ is a homomorphism. Take $x_1, x_2 \in N \rtimes_\sigma H$. Then $x_1 = (n_1, h_1)$ and $x_2 = (n_2, h_2)$ for $n_1, n_2 \in N$ and $h_1, h_2 \in H$. Now

$$\begin{aligned}\phi(x_1x_2) &= \phi((n_1, h_1)(n_2, h_2))\\ &= \phi(n_1\sigma(h_1)(n_2), h_1h_2)\\ &= \phi(n_1(h_1n_2h_1^{-1}), h_1h_2)\\ &= n_1h_1n_2h_1^{-1}h_1h_2\\ &= n_1h_1n_2h_2\\ &= \phi(n_1, h_1)\phi(n_2, h_2)\\ &= \phi(x_1)\phi(x_2)\end{aligned}$$

so that ϕ is a homomorphism. Therefore, ϕ is an isomorphism, and hence we are done. □

We cannot have that an external semidirect product is an internal semidirect product of the two original groups, since these are not even subsets (note that an external semidirect product is a group of ordered pairs). However, it is an internal semidirect product of groups isomorphic to the original groups, given by the following definition.

Definition 3.2.5. Suppose H and K are groups. Then we define the **canonical semidirect product embeddings**:

$$(H, \mathrm{id}_K) = \{(h, \mathrm{id}_K) : h \in H\}$$

and

$$(\mathrm{id}_H, K) = \{(\mathrm{id}_H, k) : k \in K\}.$$

Proposition 3.2.6. *Let H and K be groups and $\sigma \in \mathrm{Hom}(K, \mathrm{Aut}(H))$. Let*

$$H_1 = (H, \mathrm{id}_K)$$

and

$$K_1 = (\mathrm{id}_H, K).$$

Then H_1 and K_1 are subgroups of $H \rtimes_\sigma K$, $H_1 \cong H$ and $K_1 \cong K$, and $H \rtimes_\sigma K$ is the internal semidirect product of H_1 and K_1.

Proof. Let H and K be groups and $\sigma \in \mathrm{Hom}(K, \mathrm{Aut}(H))$. Let

$$H_1 = \{(h, \mathrm{id}_K) : h \in H\}$$

and

$$K_1 = \{(\mathrm{id}_H, k) : k \in K\}.$$

First note that H_1 and K_1 are non-empty, as they both contain the element $(\mathrm{id}_H, \mathrm{id}_K)$.

Let $x_1, x_2 \in H_1$. Then $x_1 = (h_1, \mathrm{id}_K)$ and $x_2 = (h_2, \mathrm{id}_K)$. $\sigma(\mathrm{id}_K)$ is an automorphism, and so $\sigma(\mathrm{id}_K)(h_2) \in H$, and so

$$\begin{aligned}x_1x_2 &= (h_1, \mathrm{id}_K)(h_2, \mathrm{id}_K)\\ &= (h_1\sigma(\mathrm{id}_K)(h_2), \mathrm{id}_K\,\mathrm{id}_K)\\ &= (h_1\sigma(\mathrm{id}_K)(h_2), \mathrm{id}_K) \in H_1.\end{aligned}$$

Similarly, if $y_1, y_2 \in H_2$, then $y_1 = (\mathrm{id}_H, k_1)$ and $y_2 = (\mathrm{id}_H, k_2)$. $\sigma(k_2)$ is an automorphism, and so $\sigma(k_2)(\mathrm{id}_H) = \mathrm{id}_H$, and so

$$\begin{aligned} y_1 y_2 &= (\mathrm{id}_H, k_1)(\mathrm{id}_H, k_2) \\ &= (\mathrm{id}_H\, \sigma(k_2)(\mathrm{id}_H), k_1 k_2) \\ &= (\mathrm{id}_H\, \mathrm{id}_H, k_1 k_2) \\ &= (\mathrm{id}_H, k_1 k_2) \in K_1. \end{aligned}$$

Now let $x \in H_1$. Then $x = (h, \mathrm{id}_K)$. Let $a = (h^{-1}, \mathrm{id}_K)$. Since σ is a homomorphism, $\sigma(\mathrm{id}_K)$ is the identity automorphism, and

$$\begin{aligned} ax &= (h^{-1}, \mathrm{id}_K)(h, \mathrm{id}_K) \\ &= (h^{-1}\sigma(\mathrm{id}_K)(h), \mathrm{id}_K\, \mathrm{id}_K) \\ &= (h^{-1}h, \mathrm{id}_K) \\ &= (\mathrm{id}_H, \mathrm{id}_K) \end{aligned}$$

and also

$$\begin{aligned} xa &= (h, \mathrm{id}_K)(h^{-1}, \mathrm{id}_K) \\ &= (h\sigma(\mathrm{id}_K)(h^{-1}), \mathrm{id}_K\, \mathrm{id}_K) \\ &= (hh^{-1}, \mathrm{id}_K) \\ &= (\mathrm{id}_H, \mathrm{id}_K) \end{aligned}$$

so that a is the inverse of x. However clearly $a \in H_1$. This taken with previous arguments gives that H_1 is a subgroup of $H \rtimes_\sigma K$.

Let $y \in K_1$. Then $y = (\mathrm{id}_H, k)$. Let $b = (\mathrm{id}_H, k^{-1})$. Since $\sigma(k)$ and $\sigma(k^{-1})$ are a automorphisms, $\sigma(k)(\mathrm{id}_H) = \mathrm{id}_H$ and $\sigma(k^{-1})(\mathrm{id}_H) = \mathrm{id}_H$, and

$$\begin{aligned} by &= (\mathrm{id}_H, k^{-1})(\mathrm{id}_H, k) \\ &= (\mathrm{id}_H\, \sigma(k)(\mathrm{id}_H), k^{-1}k) \\ &= (\mathrm{id}_H\, \mathrm{id}_H, \mathrm{id}_K) \\ &= (\mathrm{id}_H, \mathrm{id}_K) \end{aligned}$$

and also

$$\begin{aligned} yb &= (\mathrm{id}_H, k)(\mathrm{id}_H, k^{-1}) \\ &= (\mathrm{id}_H\, \sigma(k^{-1})(\mathrm{id}_H), kk^{-1}) \\ &= (\mathrm{id}_H\, \mathrm{id}_H, \mathrm{id}_K) \\ &= (\mathrm{id}_H, \mathrm{id}_K) \end{aligned}$$

so that b is the inverse of y. However clearly $b \in K_1$. This taken with previous arguments gives that K_1 is a subgroup of $H \rtimes_\sigma K$.

Construct maps from H_1 to H and K_1 to K as follows:

$$\phi : H_1 \mapsto H; (h, \mathrm{id}_K) \mapsto h$$

$$\psi : K_1 \mapsto K; (\mathrm{id}_H, k) \mapsto k$$

Then ϕ and ψ are onto by definition. Suppose $\phi(x) = \phi(y)$. Then $x = (h_1, \mathrm{id}_K)$ and $y = (h_2, \mathrm{id}_K)$ for some $h_1, h_2 \in H$, so we get $h_1 = \phi(x) = \phi(y) = h_2$, so

$x = y$ and ϕ is 1-1, hence a bijection. Suppose $\psi(x) = \psi(y)$. Then $x = (\mathrm{id}_H, k_1)$ and $y = (\mathrm{id}_H, k_2)$ for some $k_1, k_2 \in K$, so we get $k_1 = \psi(x) = \psi(y) = k_2$, so $x = y$ and ψ is 1-1, hence a bijection. From this we get that $|H_1| = |H|$ and $|K_1| = |K|$.

In fact we have that ϕ and ψ are homomorphisms. First take $x, y \in H_1$. Then $x = (h_1, \mathrm{id}_K)$ and $y = (h_2, \mathrm{id}_K)$ for some $h_1, h_2 \in H$. Then

$$\begin{aligned}
\phi(xy) &= \phi((h_1, \mathrm{id}_K)(h_2, \mathrm{id}_K)) \\
&= \phi(h_1 \sigma(\mathrm{id}_K)(h_2), \mathrm{id}_K \, \mathrm{id}_K) \\
&= \phi(h_1 h_2, \mathrm{id}_K) \\
&= h_1 h_2 \\
&= \phi(h_1, \mathrm{id}_K)\phi(h_2, \mathrm{id}_K) \\
&= \phi(x)\phi(y)
\end{aligned}$$

as $\sigma(\mathrm{id}_K)$ is the identity automorphism. Therefore ϕ is a homomorphism. Secondly, take $x, y \in K_1$. Then $x = (\mathrm{id}_H, k_1)$ and $y = (\mathrm{id}_H, k_2)$ for some $k_1, k_2 \in K$. Then

$$\begin{aligned}
\psi(xy) &= \psi((\mathrm{id}_H, k_1)(\mathrm{id}_H, k_2)) \\
&= \psi(\mathrm{id}_H \, \sigma(k_1)(\mathrm{id}_H), k_1 k_2) \\
&= \psi(\mathrm{id}_H, k_1 k_2) \\
&= k_1 k_2 \\
&= \psi(\mathrm{id}_H, k_1)\psi(\mathrm{id}_H, k_2) \\
&= \psi(x)\psi(y)
\end{aligned}$$

as any automorphism must map the identity to the identity. Therefore ψ is a homomorphism. Since ϕ and ψ are also bijections, they are isomorphisms, and this gives $H_1 \cong H$ and $K_1 \cong K$.

It is clear that if $g \in H_1 \cap K_1$ then $g = (h, \mathrm{id}_K) = (\mathrm{id}_H, k)$, so $g = (\mathrm{id}_H, \mathrm{id}_K)$. Therefore, $H_1 \cap K_1$ is trivial. By Proposition 2.4.3, we have that $|H_1 K_1| = |H_1| \cdot |K_1| = |H| \cdot |K| = |H \rtimes_\sigma K|$, and so since $H_1 K_1 \subseteq H \rtimes_\sigma K$, we must have $H_1 K_1 = H \rtimes_\sigma K$.

Finally, we show that $H_1 \trianglelefteq H \rtimes_\sigma K$. We do this by showing that every left coset is equal to every right coset. Let $(s, t) \in H \rtimes_\sigma K$. Then

$$\begin{aligned}
H_1(s, t) &= \{(h, \mathrm{id}_H)(s, t) : h \in H\} \\
&= \{(h\sigma(\mathrm{id}_H)(s), \mathrm{id}_H \, t) : h \in H\} \\
&= \{(hs, t) : h \in H\} \\
&= \{(x, t) : x \in H\}
\end{aligned}$$

since every element of H can be written as $x = (xs^{-1})s = hs$ for $h = xs^{-1}$. Also

$$\begin{aligned}(s,t)H_1 &= \{(s,t)(h, \mathrm{id}_H) : h \in H\}\\ &= \{(s\sigma(t)(h), t\,\mathrm{id}_H) : h \in H\}\\ &= \{(s\sigma(t)(h), t) : h \in H\}\\ &= \{(x,t) : x \in H\}\end{aligned}$$

since every element of H can be written as

$$x = ss^{-1}x = s(\sigma(t)((\sigma(t))^{-1}(s^{-1}x))) = s\sigma(t)(h)$$

for $h = (\sigma(t))^{-1}(s^{-1}x)$. This is what we wanted.

Therefore, $H_1 \trianglelefteq H \rtimes_\sigma K$ is the internal semidirect product of H_1 and K_1. □

We would be questioning our definition of the semidirect product if semidirect products of isomorphic groups were not isomorphic. We wrap up the core of the proof in a preliminary lemma, which is slightly stronger than we require here.

Lemma 3.2.7. *Suppose H_1, K_1, H_2, K_2 are groups, such that $H_1 \cong H_2$ and $K_1 \cong K_2$. Let $\alpha : H_1 \mapsto H_2$ and $\beta : K_1 \mapsto K_2$ be isomorphisms. Define*

$$\lambda_\alpha : \mathrm{Aut}(H_1) \mapsto \mathrm{Aut}(H_2); f \mapsto \alpha \circ f \circ \alpha^{-1}.$$

Take $\sigma_1 \in \mathrm{Hom}(K_1, \mathrm{Aut}(H_1))$, $\sigma_2 \in \mathrm{Hom}(K_2, \mathrm{Aut}(H_2))$. Define

$$\phi : H_1 \rtimes_{\sigma_1} K_1 \mapsto H_2 \rtimes_{\sigma_2} K_2; (h_1, k_1) \mapsto (\alpha(h_1), \beta(k_1)).$$

Then ϕ is a homomorphism if and only if $\sigma_2 = \lambda_\alpha \circ \sigma_1 \circ \beta^{-1}$.

Proof. Suppose H_1, K_1, H_2, K_2 are groups, such that $H_1 \cong H_2$ and $K_1 \cong K_2$. Let $\alpha : H_1 \mapsto H_2$ and $\beta : K_1 \mapsto K_2$ be isomorphisms. Define

$$\lambda_\alpha : \mathrm{Aut}(H_1) \mapsto \mathrm{Aut}(H_2); f \mapsto \alpha \circ f \circ \alpha^{-1}.$$

Take $\sigma_1 \in \mathrm{Hom}(K_1, \mathrm{Aut}(H_1))$, $\sigma_2 \in \mathrm{Hom}(K_2, \mathrm{Aut}(H_2))$. Define

$$\phi : H_1 \rtimes_{\sigma_1} K_1 \mapsto H_2 \rtimes_{\sigma_2} K_2; (h_1, k_1) \mapsto (\alpha(h_1), \beta(k_1)).$$

Let $x_1, x_2 \in H_1$ be arbitrary. Then $x_1 = (h_1, k_1)$ and $x_2 = (h_2, k_2)$ for some $h_1, h_2 \in H_1$ and $k_1, k_2 \in K_1$. Note that:

$$\begin{aligned}\phi(x_1x_2) &= \phi((h_1,k_1)(h_2,k_2))\\ &= \phi(h_1\sigma_1(k_1)(h_2), k_1k_2)\\ &= (\alpha(h_1\sigma_1(k_1)(h_2)), \beta(k_1k_2))\\ &= (\alpha(h_1)\alpha(\sigma_1(k_1)(h_2)), \beta(k_1)\beta(k_2))\\ &= (\alpha(h_1)\alpha(\sigma_1(k_1)(\alpha^{-1}(\alpha(h_2)))), \beta(k_1)\beta(k_2))\\ &= (\alpha(h_1)\lambda_\alpha(\sigma_1(k_1))(\alpha(h_2)), \beta(k_1)\beta(k_2))\\ &= (\alpha(h_1)\lambda_\alpha(\sigma_1(\beta^{-1}(\beta(k_1))))(\alpha(h_2)), \beta(k_1)\beta(k_2))\end{aligned}$$

and

$$\begin{aligned}\phi(x_1)\phi(x_2) &= \phi(h_1,k_1)\phi(h_2,k_2)\\ &= (\alpha(h_1),\beta(k_1))(\alpha(h_2),\beta(k_2))\\ &= (\alpha(h_1)\sigma_2(\beta(k_1))(\alpha(h_2)),\beta(k_1)\beta(k_2))\end{aligned}$$

($\Longleftarrow$) Suppose $\sigma_2 = \lambda_\alpha \circ \sigma_1 \circ \beta^{-1}$. Then

$$\begin{aligned}\phi(x_1)\phi(x_2) &= (\alpha(h_1)\sigma_2(\beta(k_1))(\alpha(h_2)),\beta(k_1)\beta(k_2))\\ &= (\alpha(h_1)\lambda_\alpha(\sigma_1(\beta^{-1}(\beta(k_1))))(\alpha(h_2)),\beta(k_1)\beta(k_2))\\ &= \phi(x_1x_2)\end{aligned}$$

and so ϕ is a homomorphism.

($\Longrightarrow$) Suppose ϕ is a homomorphism. Then

$$\begin{aligned}&(\alpha(h_1)\lambda_\alpha(\sigma_1(\beta^{-1}(\beta(k_1))))(\alpha(h_2)),\beta(k_1)\beta(k_2))\\ &= \phi(x_1x_2)\\ &= \phi(x_1)\phi(x_2)\\ &= (\alpha(h_1)\sigma_2(\beta(k_1))(\alpha(h_2)),\beta(k_1)\beta(k_2))\end{aligned}$$

Now we have

$$\alpha(h_1)\lambda_\alpha(\sigma_1(\beta^{-1}(\beta(k_1))))(\alpha(h_2)) = \alpha(h_1)\sigma_2(\beta(k_1))(\alpha(h_2))$$

and so

$$\lambda_\alpha(\sigma_1(\beta^{-1}(\beta(k_1))))(\alpha(h_2)) = \sigma_2(\beta(k_1))(\alpha(h_2)).$$

This formula holds true for **all** $h_2 \in H_1$ and $k_1 \in K_1$. Let $h \in H_2$, $k \in K_2$. Then since α and β are onto, there exist some $h_2 \in H_1$ and $k_1 \in K_1$ such that $\alpha(h_2) = h$ and $\alpha(k_1) = k$. Now the above formula becomes:

$$\lambda_\alpha(\sigma_1(\beta^{-1}(k)))(h) = \sigma_2(k)(h)$$

for all $h \in H_2$, $k \in K_2$. We therefore have

$$(\lambda_\alpha \circ \sigma_1 \circ \beta^{-1})(k) = \sigma_2(k)$$

and so

$$\sigma_2 = \lambda_\alpha \circ \sigma_1 \circ \beta^{-1}$$

as required. □

PROPOSITION 3.2.8. *Suppose H_1, K_1, H_2, K_2 are groups, such that $H_1 \cong H_2$ and $K_1 \cong K_2$. Let $\alpha : H_1 \mapsto H_2$ and $\beta : K_1 \mapsto K_2$ be isomorphisms. Define*

$$\lambda_\alpha : \mathrm{Aut}(H_1) \mapsto \mathrm{Aut}(H_2); f \mapsto \alpha \circ f \circ \alpha^{-1}.$$

Take any $\sigma_1 \in \mathrm{Hom}(K_1, \mathrm{Aut}(H_1))$ and define

$$\sigma_2 : K_2 \mapsto \mathrm{Aut}(H_2)$$

by $\sigma_2 = \lambda_\alpha \circ \sigma_1 \circ \beta^{-1}$. Then $H_1 \rtimes_{\sigma_1} K_1 \cong H_2 \rtimes_{\sigma_2} K_2$.

PROOF. Suppose H_1, K_1, H_2, K_2 are groups, such that $H_1 \cong H_2$ and $K_1 \cong K_2$. Let $\alpha : H_1 \mapsto H_2$ and $\beta : K_1 \mapsto K_2$ be isomorphisms. Define

$$\lambda_\alpha : \mathrm{Aut}(H_1) \mapsto \mathrm{Aut}(H_2); f \mapsto \alpha \circ f \circ \alpha^{-1}.$$

Take any $\sigma_1 \in \mathrm{Hom}(K_1, \mathrm{Aut}(H_1))$ and define

$$\sigma_2 : K_2 \mapsto \mathrm{Aut}(H_2)$$

by $\sigma_2 = \lambda_\alpha \circ \sigma_1 \circ \beta^{-1}$. Define

$$\phi : H_1 \rtimes_{\sigma_1} K_1 \mapsto H_2 \rtimes_{\sigma_2} K_2; (h, k) \mapsto (\alpha(h), \beta(k)).$$

First let us show that ϕ is onto. Take any $x \in H_2 \rtimes_{\sigma_2} K_2$. Then $x = (h_2, k_2)$ for some $h_2 \in H_2$, $k_2 \in K_2$. Since α and β are onto, there exist $h_1 \in H_1$, $k_1 \in K_1$ such that $\alpha(h_1) = h_2$ and $\alpha(k_1) = k_2$. Now

$$\phi(h_1, k_1) = (\alpha(h_1), \beta(k_1)) = (h_2, k_2) = x$$

and so ϕ is onto.

Since α and β are isomorphisms, they are bijections and so $|H_1| = |H_2|$ and $|K_1| = |K_2|$. Therefore

$$|H_1 \rtimes_{\sigma_1} K_1| = |H_1| \cdot |H_2| = |K_1| \cdot |K_2| = |H_2 \rtimes_{\sigma_2} K_2|$$

and taking this with the fact that ϕ is onto gives that it is a bijection, hence 1-1.

Finally, ϕ is a homomorphism by Lemma 3.2.7. Therefore, ϕ is an isomorphism, and so $H_1 \rtimes_{\sigma_1} K_1 \cong H_2 \rtimes_{\sigma_2} K_2$. □

3.3. The Schema itself

The schema works by classifying groups of a particular type into semidirect products: however such groups are sometimes isomorphic to each other. Therefore we group the ones which are isomorphic into orbits under a particular action specific to this Schema. We shall therefore call this action the ECS Action:

PROPOSITION 3.3.1. *Let X and Y be groups, then the map*

$$\begin{aligned} * : (\mathrm{Aut}(X) \times \mathrm{Aut}(Y)) \times \mathrm{Hom}(Y, \mathrm{Aut}(X)) &\mapsto \mathrm{Hom}(Y, \mathrm{Aut}(X)); \\ ((\alpha, \phi), \rho) &\mapsto \lambda_\alpha \circ \rho \circ \phi^{-1} \end{aligned}$$

where

$$\lambda_\alpha : \mathrm{Aut}(X) \mapsto \mathrm{Aut}(X); f \mapsto \alpha f \alpha^{-1}$$

is an action.

PROOF. Let X and Y be groups, and define the map $*$ as in the statement of the proposition. First notice that for any $x \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$:

$$\begin{aligned} *(\mathrm{id}_{\mathrm{Aut}(X) \times \mathrm{Aut}(Y)}, x) &= *((\mathrm{id}_{\mathrm{Aut}(X)}, \mathrm{id}_{\mathrm{Aut}(Y)}), x) \\ &= \lambda_{\mathrm{id}_{\mathrm{Aut}(X)}} \circ x \circ (\mathrm{id}_{\mathrm{Aut}(Y)})^{-1} \\ &= \lambda_{\mathrm{id}_{\mathrm{Aut}(X)}} \circ x \\ &= x \end{aligned}$$

since

$$\lambda_{\mathrm{id}_{\mathrm{Aut}(X)}}(f) = \mathrm{id}_{\mathrm{Aut}(X)} \circ f \circ (\mathrm{id}_{\mathrm{Aut}(X)})^{-1} = f$$

Now take any $g, h \in \mathrm{Aut}(X) \times \mathrm{Aut}(Y)$. Let $g = (g_1, g_2)$ and $h = (h_1, h_2)$. Then $gh = (g_1 \circ h_1, g_2 \circ h_2)$. Again, take $x \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$, and $f \in \mathrm{Aut}(X)$. We have:

$$\begin{aligned}
\lambda_{g_1 \circ h_1}(f) &= (g_1 \circ h_1) \circ f \circ (g_1 \circ h_1)^{-1} \\
&= (g_1 \circ h_1) \circ f \circ ((h_1)^{-1} \circ (g_1)^{-1}) \\
&= g_1 \circ (h_1 \circ f \circ (h_1)^{-1}) \circ (g_1)^{-1} \\
&= g_1 \circ \lambda_{h_1}(f) \circ (g_1)^{-1} \\
&= (\lambda_{g_1} \circ \lambda_{h_1})(f)
\end{aligned}$$

so that $\lambda_{g_1 h_1} = \lambda_{g_1} \lambda_{h_1}$, and so

$$\begin{aligned}
*(gh, x) &= *((g_1 \circ h_1, g_2 \circ h_2), x) \\
&= \lambda_{g_1 \circ h_1} \circ x \circ (g_2 \circ h_2)^{-1} \\
&= \lambda_(g_1 \circ h_1) \circ x \circ h_2^{-1} \circ g_2^{-1} \\
&= \lambda_(g_1) \circ \lambda_{h_1} \circ x \circ h_2^{-1} \circ g_2^{-1} \\
&= \lambda_(g_1) \circ (\lambda_{h_1} \circ x \circ h_2^{-1}) \circ g_2^{-1} \\
&= \lambda_(g_1) \circ *((h_1, h_2), x) \circ g_2^{-1} \\
&= \lambda_(g_1) \circ *(h, x) \circ g_2^{-1} \\
&= *((g_1, g_2), *(h, x)) \\
&= *(g, *(h, x)).
\end{aligned}$$

Therefore, both the conditions for an axioms are satisfied, and so $*$ is an action. □

Definition 3.3.2. The action of the above proposition is called the **ECS Action**. We denote as usual $*((\alpha, \phi), \rho)$ by $(\alpha, \phi) * \rho$.

Remarks.

(i) Note that it is perhaps easier to see what is happening with the action by looking at the result of the action applied to an element of Y. Then we get:

$$((\alpha, \phi) * \rho)(y) = \lambda_\alpha(\rho(\phi^{-1}(y))) = \alpha \circ \rho(\phi^{-1}(y)) \circ \alpha^{-1}.$$

(ii) Note also how similar this action is to the function σ_2 defined in Proposition 3.2.8. This is no coincidence, as the proof of part (iii) of the below shows.

We are now in a position to state the actual schema.

Theorem 3.3.3 (The Extension Classification Schema). *Let X and Y be solvable groups of coprime orders. Then:*

(i) *For any $\rho \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$, the semidirect product $G = X \rtimes_\rho Y$ has a normal subgroup N isomorphic to X with G/N isomorphic to Y.*

(ii) *For any group G with a normal subgroup N isomorphic to X and G/N isomorphic to Y, there exists some $\rho \in \operatorname{Hom}(Y, \operatorname{Aut}(X))$ such that G is isomorphic to the semidirect product $X \rtimes_\rho Y$.*

(iii) *Let $\sigma, \rho \in \operatorname{Hom}(Y, \operatorname{Aut}(X))$. Then the semidirect products $X \rtimes_\sigma Y$ and $X \rtimes_\rho Y$ are isomorphic if and only if σ and ρ lie in the same orbit of the ECS Action for X and Y.*

Once we have proved this, we have classified all groups with a certain property.

Corollary 3.3.4. *Let X and Y be solvable groups of coprime orders. Let T be a complete set of representatives for the orbits of the ECS Action for X and Y. Then the set*

$$\{X \rtimes_\rho Y : \rho \in T\}$$

is a classification of the groups G with a normal subgroup N isomorphic to X, and G/N isomorphic to Y.

Proof. Let X and Y be solvable groups of coprime orders. Let T be a complete set of representatives for the orbits of the ECS Action for X and Y. Let $G_1, ..., G_n$ be an enumeration of the elements of the set

$$\{X \rtimes_\rho Y : \rho \in T\}$$

where n is the size of the above set. Take any G_i, then $G_i = X \rtimes_\rho Y$ for some $\rho \in T \subseteq \operatorname{Hom}(Y, \operatorname{Aut}(X))$, and so, by Theorem 3.3.3(i), G_i has a normal subgroup N isomorphic to X, and G/N isomorphic to Y.

Take any group G with a normal subgroup N isomorphic to X and G/N isomorphic to Y. By Theorem 3.3.3(ii), there is some $\rho \in \operatorname{Hom}(Y, \operatorname{Aut}(X))$ with $G \cong X \rtimes_\rho Y$. Since T is a complete set of representatives for the orbits of the ECS Action for X and Y, there is some $\sigma \in T$ such that $\sigma \in \operatorname{Orb}(\rho)$ under the ECS Action for X and Y. Therefore, σ and ρ lie in the same orbit of the ECS Action for X and Y, and so by the "if" part of Theorem 3.3.3(iii), $X \rtimes_\sigma Y \cong X \rtimes_\rho Y \cong G$. Also, since $\sigma \in T$, there is some i with $1 \leq i \leq n$ and $G_i = X \rtimes_\sigma Y$. For this i, we therefore have $G_i = X \rtimes_\sigma Y \cong G$.

Finally, take any G_i, G_j, with $1 \leq i \leq n$, $1 \leq j \leq n$ and $i \neq j$. The group $G_i = X \rtimes_\sigma Y$ for some $\sigma \in T$ and the group $G_j = X \rtimes_\rho Y$ for some $\rho \in T$. In fact, $\sigma \neq \rho$, otherwise $G_i = G_j$, so $i = j$. Therefore, σ and ρ lie in different orbits of the ECS Action. By the "only if" part of Theorem 3.3.3(iii), we cannot have that $X \rtimes_\sigma Y \cong X \rtimes_\rho Y$, that is, G_i is not isomorphic to G_j. □

Remark. As we shall see later, the above result allows us to classify all groups of squarefree order, in a very theoretical sense. This is because any such group (of order say $p_1 \cdots p_n$) has a normal subgroup of index p_1 (by Proposition 1.5.1), and we can take this for X, and C_{p_1} for Y (as there is only one group of order p_1 up to isomorphism). Proceeding inductively, we can go from a classification of groups of order $p_2 \cdots p_n$ to a classification of groups of order $p_1 \cdots p_n$ (taking X to be each possibility for a group of order $p_2 \cdots p_n$ in turn), and in this way classify all groups of squarefree order.

3.4. Proof of Theorem 3.3.3(i) and Theorem 3.3.3(ii)

Before proving parts (i) and (ii) of Theorem 3.3.3, we must first prove some initial lemmas.

LEMMA 3.4.1. *Suppose G is a group with subgroups N and H, such that G is the internal semidirect product of N and H. Then $NH = HN$.*

PROOF. Suppose G is a group with subgroups N and H, such that G is the internal semidirect product of N and H. Then $G = NH$, so that $|G| = |NH|$. Furthermore, $|N \cap H| = 1$, so that $|H \cap N| = 1$. Therefore, by Proposition 2.4.3,

$$|HN| = \frac{|H| \cdot |N|}{|H \cap N|} = \frac{|N| \cdot |H|}{|N \cap H|} = |NH| = |G|.$$

But also $HN \subseteq G$. Therefore, we must have $HN = G = NH$. □

LEMMA 3.4.2. *Suppose G is a group with subgroups N and H, such that G is the internal semidirect product of N and H. Then $H \cong G/N$.*

PROOF. Suppose G is a group with subgroups N and H, such that G is the internal semidirect product of N and H. Since $H \subseteq G$, if $h \in H$ then $h \in G$ and so $hN \in G/N$. Define the following map:

$$\phi : H \mapsto G/N; h \mapsto hN.$$

By the above, this is well-defined.

We shall first show that ϕ is onto. Take any $x \in G/N$, then $x = gN$ for some $g \in G$. Since $G = NH$, then by Lemma 3.4.1, $G = HN$. Therefore, $g = hn$ for some $h \in H$, $n \in N$. Now $gN = (hn)N = h(nN) = hN$ and so $\phi(h) = hN = gN = x$. Therefore, ϕ is onto.

Since $G = NH$, then by Proposition 2.4.3, $|G| = |NH| = \frac{|N| \cdot |H|}{|N \cap H|} = |N| \cdot |H|$, as $|N \cap H| = 1$. Therefore, $|H| = \frac{|G|}{|N|}$, and so since ϕ is also onto, it is a bijection, hence 1-1.

Finally let $h_1, h_2 \in H$. Then

$$\phi(h_1 h_2) = (h_1 h_2)N = (h_1 N)(h_2 N) = \phi(h_1)\phi(h_2)$$

so that ϕ is a homomorphism.

Therefore, ϕ is an isomorphism, and we are done. □

We are now in a position to prove Theorem 3.3.3, parts (i) and (ii).

PROOF OF THEOREM 3.3.3(i). Let X and Y be solvable groups of coprime orders, and let $\rho \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$. Let $G = X \rtimes_\rho Y$. Let $X_1 = (X, \mathrm{id}_Y)$ and $Y_1 = (\mathrm{id}_X, Y)$. Then, by Proposition 3.2.6, X_1 and Y_1 are subgroups of G, $X_1 \cong X$ and $Y_1 \cong Y$, and G is the internal semidirect product of X_1 and Y_1.

Let $N = X_1$. Then $N = X_1 \trianglelefteq G$, as G is the internal semidirect product of X_1 and Y_1. Also $N = X_1 \cong X$, and $Y \cong Y_1 \cong G/X_1 = G/N$, the second isomorphism being by Lemma 3.4.2. Therefore, we are done. □

PROOF OF THEOREM 3.3.3(ii). Let X and Y be solvable groups of coprime orders, and let G be a group with a normal subgroup N isomorphic to X and

G/N isomorphic to Y. N and G/N are solvable by Lemma 1.2.12, and hence G is solvable by Proposition 1.4.3.

Let π be the set of primes dividing both $|G|$ and $|Y|$. Note $|X| = |N|$ as N is isomorphic to X. Therefore, if p is a prime dividing the order of N then p divides the order of X. However since X and Y have coprime orders, p does not divide the order of Y, so p is not in π. The upshot is that N is actually a π'-group.

By Proposition 1.2.12, N and G/N are solvable. Therefore, by Proposition 1.4.3, G is solvable. By Theorem 2.2.1, G has a Hall π-subgroup, say H. By Lemma 2.6.2, $G = NH$. Since also $N \trianglelefteq G$ and $|N \cap H| = 1$ (by Corollary 2.1.9), we have that G is the internal semidirect product of N and H.

By Proposition 3.2.4, there is some $\sigma \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ such that $G \cong N \rtimes_\sigma H$. By Lemma 3.4.2, $H \cong G/N$, and so $Y \cong G/N \cong H$. Therefore, by Proposition 3.2.8, $G \cong X \rtimes_\rho Y$, where $\rho = \lambda_\alpha \circ \sigma \circ \beta^{-1}$. Here $\beta : G/N \mapsto Y$ is an isomorphism, and

$$\lambda_\alpha : \mathrm{Aut}(N) \mapsto \mathrm{Aut}(X); f \mapsto \alpha \circ f \circ \alpha^{-1}$$

where $\alpha : N \mapsto X$ is an isomorphism. □

3.5. Proof of Theorem 3.3.3(iii)

The core proof of this part of the theorem has already been done, in Lemma 3.2.7 and Lemma 3.2.8. We proved a stronger version of this than we required, and we may now reap the benefits of that.

Proof of Theorem 3.3.3(iii). Let X and Y be solvable groups of coprime orders. Let $\sigma, \rho \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$. Define $G_\sigma = X \rtimes_\sigma Y$, $G_\rho = X \rtimes_\rho Y$. Define $N_\sigma = N_\rho = (X, \mathrm{id}_Y)$ as sets, and $H_\sigma = H_\rho = (\mathrm{id}_X, Y)$ as sets. By Proposition 3.2.6, N_σ and H_σ are subgroups of G_σ, $N_\sigma \cong X$ and $H_\sigma \cong Y$, and G_σ is the internal semidirect product of N_σ and H_σ. By Proposition 3.2.6 again, N_ρ and H_ρ are subgroups of G_ρ, $N_\rho \cong X$ and $H_\rho \cong Y$, and G_ρ is the internal semidirect product of N_ρ and H_ρ.

($\Longleftarrow$) Suppose σ and ρ lie in the same orbit of the ECS Action for X and Y. Then in particular $\sigma \in \mathrm{Orb}(\rho)$, and so we have

$$\sigma = (\alpha, \beta) * \rho = \lambda_\alpha \circ \rho \circ \beta^{-1}$$

(where λ_α is defined as in the ECS Action, and $*$ denote the ECS Action itself), for some $(\alpha, \beta) \in \mathrm{Aut}(X) \times \mathrm{Aut}(Y)$. Therefore $\alpha \in \mathrm{Aut}(X)$ and $\beta \in \mathrm{Aut}(Y)$, and so by Proposition 3.2.8, we have that $G_\sigma \cong G_\rho$.

($\Longrightarrow$) Suppose $G_\sigma \cong G_\rho$. Then there exists some isomorphism $\psi : G_\sigma \mapsto G_\rho$. We know that ψ could be split into component functions ψ_1 and ψ_2, however in general these functions will depend on both inputs, i.e. $\psi_1 = \psi_1(x, y)$. We want to find an isomorphism such that that these component functions in fact only depend on one of the inputs, so they become like α and β above.

First of all, since G_ρ is the internal semidirect product of N_ρ and H_ρ, then $N_\rho \trianglelefteq G_\rho$. Also, N_ρ is solvable, since $N_\rho \cong X$, and we can apply

Lemma 1.2.12. The group G_ρ/N_ρ is solvable, because it is isomorphic to $H_\rho \cong Y$ (by Lemma 3.4.2), and we can again apply Lemma 1.2.12. Therefore, G_ρ is solvable by Proposition 1.4.3.

Now let π be the set of primes dividing H_σ. Then since $|\psi(H_\sigma)| = |H_\sigma|$, $\psi(H_\sigma)$ is also a π-group. Also,

$$[G_\rho : \psi(H_\sigma)] = \frac{|G_\rho|}{|\psi(H_\sigma)|} = \frac{|X| \cdot |Y|}{|H_\sigma|} = \frac{|X| \cdot |Y|}{|Y|} = |X|.$$

Suppose $p \mid [G_\rho : \psi(H_\sigma)]$. Then p divides the order of X, so it cannot divide the order of Y, since X and Y have coprime orders. Therefore, it does not divide $|H_\sigma| = |Y|$, and so is not in π. So $\psi(H_\sigma)$ is a Hall π-subgroup of G_ρ. Since $|\psi(H_\sigma)| = |H_\sigma| = |H_\rho|$, H_ρ is also a Hall π-subgroup of G_ρ. By Theorem 2.2.1, H_ρ and $\psi(H_\sigma)$ are conjugate by some element of G_ρ, say a.

Define a map

$$\phi : G_\sigma \mapsto G_\rho; t \mapsto a\psi(t)a^{-1}.$$

ϕ is a bijection as its inverse is

$$f : G_\rho \mapsto G_\sigma; t \mapsto a^{-1}\psi^{-1}(t)a$$

and is a homomorphism: take $t_1, t_2 \in G_\sigma$ and then

$$\phi(t_1t_2) = a\psi(t_1t_2)a^{-1} = a\psi(t_1)\psi(t_2)a^{-1} = a\psi(t_1)a^{-1}a\psi(t_2)a^{-1} = \phi(t_1)\phi(t_2).$$

Therefore, it is an isomorphism. We also have that $\phi(H_\sigma) = a\psi(H_\sigma)a^{-1} = H_\rho$.

Now let π be redefined as the set of primes dividing N_σ. Then since $|\phi(N_\sigma)| = |N_\sigma|$, $\phi(N_\sigma)$ is also a π-group. Also,

$$[G_\rho : \phi(N_\sigma)] = \frac{|G_\rho|}{|\phi(N_\sigma)|} = \frac{|X| \cdot |Y|}{|N_\sigma|} = \frac{|X| \cdot |Y|}{|X|} = |Y|.$$

Suppose $p \mid [G_\rho : \phi(N_\sigma)]$. Then p divides the order of Y, so it cannot divide the order of X, since X and Y have coprime orders. Therefore, it does not divide $|N_\sigma| = |X|$, and so is not in π. So $\phi(N_\sigma)$ is a Hall π-subgroup of G_ρ. Since $|\phi(N_\sigma)| = |N_\sigma| = |N_\rho|$, N_ρ is also a Hall π-subgroup of G_ρ. By Theorem 2.2.1, $\phi(N_\sigma)$ and N_ρ are conjugate by some element of G_ρ, say a. But as N_ρ is normal in G_ρ, $N_\rho = aN_\rho a^{-1} = \phi(N_\sigma)$.

We have that, for all $x \in X, y \in Y$, $\phi(x, y) = (\phi_1(x, y), \phi_2(x, y))$ for some $\phi_1 : X \rtimes_\sigma Y \mapsto X$ and $\phi_2 : X \rtimes_\sigma Y \mapsto Y$. Let

$$\alpha : X \mapsto X; x \mapsto \phi_1(x, id_Y)$$

and

$$\beta : Y \mapsto Y; y \mapsto \phi_2(id_X, y).$$

Since $\phi(N_\sigma) = N_\rho$ and $\phi(H_\sigma) = H_\rho$, we have that for all $x \in X$, $y \in Y$, $\phi_2(x, \mathrm{id}_Y) = \mathrm{id}_Y$ and $\phi_1(\mathrm{id}_X, y) = \mathrm{id}_X$ (the reader is advised to look at the definitions of N_σ, H_σ, etc if still unsure). Now we have that, for all $(x, y) \in G_\sigma$,

$$\begin{aligned}
\phi(x, y) &= \phi((x\sigma(\mathrm{id}_Y)(\mathrm{id}_X), \mathrm{id}_Y\, y)) \\
&= \phi((x, \mathrm{id}_Y)(\mathrm{id}_X, y)) \\
&= \phi(x, \mathrm{id}_Y)\phi(\mathrm{id}_X, y) \\
&= (\phi_1(x, \mathrm{id}_Y), \mathrm{id}_Y)(\mathrm{id}_X, \phi_2(\mathrm{id}_X, y)) \\
&= (\alpha(x), \mathrm{id}_Y)(\mathrm{id}_X, \beta(y)) \\
&= (\alpha(x)\sigma(\mathrm{id}_Y)(\mathrm{id}_X), \mathrm{id}_Y\, \beta(y)) \\
&= (\alpha(x)\, \mathrm{id}_X, \beta(y)) \\
&= (\alpha(x), \beta(y))
\end{aligned}$$

We would like to show that α and β are automorphisms. First, they are 1-1 since if $\alpha(x) = \alpha(y)$ for some $x, y \in X$, then

$$\begin{aligned}
\phi(x, \mathrm{id}_Y) &= (\phi_1(x, \mathrm{id}_Y), \phi_2(x, \mathrm{id}_Y)) \\
&= (\phi_1(y, \mathrm{id}_Y), \mathrm{id}_Y) \\
&= (\phi_1(y, \mathrm{id}_Y), \phi_2(y, \mathrm{id}_Y)) \\
&= \phi(y, \mathrm{id}_Y)
\end{aligned}$$

and so $(x, \mathrm{id}_Y) = (y, \mathrm{id}_Y)$ (since ϕ is 1-1), and so $x = y$. If $\beta(x) = \beta(y)$ for some $x, y \in Y$, then

$$\begin{aligned}
\phi(\mathrm{id}_X, x) &= (\phi_1(\mathrm{id}_X, x), \phi_2(\mathrm{id}_X, x)) \\
&= (\mathrm{id}_X, \phi_2(\mathrm{id}_X, y)) \\
&= (\phi_1(\mathrm{id}_X, y), \phi_2(\mathrm{id}_X, y)) \\
&= \phi(\mathrm{id}_X, y)
\end{aligned}$$

and so $(\mathrm{id}_X, x) = (\mathrm{id}_X, y)$ (since ϕ is 1-1), and so $x = y$. Hence α and β are 1-1. Since their domain and codomains are equal, they have the same size, and so α and β are bijections, hence onto.

We shall now show that α and β are homomorphisms. Take $x, y \in X$. Then:

$$\begin{aligned}
(\alpha(xy), \mathrm{id}_Y) &= (\phi_1(xy, \mathrm{id}_Y), \phi_2(xy, \mathrm{id}_Y)) \\
&= \phi(xy, \mathrm{id}_Y) \\
&= \phi(x\sigma(\mathrm{id}_Y)(y), \mathrm{id}_Y\, \mathrm{id}_Y) \\
&= \phi((x, \mathrm{id}_Y)(y, \mathrm{id}_Y)) \\
&= \phi(x, \mathrm{id}_Y)\phi(y, \mathrm{id}_Y) \\
&= (\phi_1(x, \mathrm{id}_Y), \phi_2(x, \mathrm{id}_Y))(\phi_1(y, \mathrm{id}_Y), \phi_2(y, \mathrm{id}_Y)) \\
&= (\alpha(x), \mathrm{id}_Y)(\alpha(y), \mathrm{id}_Y) \\
&= (\alpha(x)\rho(\mathrm{id}_Y)(\alpha(y)), \mathrm{id}_Y\, \mathrm{id}_Y) \\
&= (\alpha(x)\alpha(y), \mathrm{id}_Y)
\end{aligned}$$

and so $\alpha(xy) = \alpha(x)\alpha(y)$, thus α is a homomorphism, hence an isomorphism. Now take any $x, y \in Y$.

$$\begin{aligned}
(\mathrm{id}_X, \alpha(xy)) &= (\phi_1(\mathrm{id}_X, xy), \phi_2(\mathrm{id}_X, xy)) \\
&= \phi(\mathrm{id}_X, xy) \\
&= \phi(\mathrm{id}_X\, \sigma(x)(\mathrm{id}_X), xy) \\
&= \phi((\mathrm{id}_X, x)(\mathrm{id}_X, y)) \\
&= \phi(\mathrm{id}_X, x)\phi(\mathrm{id}_X, y) \\
&= (\phi_1(\mathrm{id}_X, x), \phi_2(\mathrm{id}_X, x))(\phi_1(\mathrm{id}_X, y), \phi_2(\mathrm{id}_X, y)) \\
&= (\mathrm{id}_X, \beta(x))(\mathrm{id}_X, \beta(y)) \\
&= (\mathrm{id}_X\, \rho(\beta(x))(\mathrm{id}_X), \beta(x)\beta(y)) \\
&= (\mathrm{id}_X\, \mathrm{id}_X, \beta(x)\beta(y)) \\
&= (\mathrm{id}_X, \beta(x)\beta(y))
\end{aligned}$$

and so $\beta(xy) = \beta(x)\beta(y)$, thus β is a homomorphism, hence an isomorphism.

Since ϕ is an isomorphism, it is a homomorphism, and so by Lemma 3.2.7, $\rho = \lambda_\alpha \circ \sigma \circ \beta^{-1}$, where λ_α is defined as in the ECS Action. Therefore, $\rho = (\alpha, \beta) * \sigma$, where $*$ denotes the ECS Action. Thus $\rho \in \mathrm{Orb}(\sigma)$, and so ρ and σ lie in the same orbit under the ECS Action. □

CHAPTER 4

Some groups of order *pqr*

4.1. Classification of automorphisms of the Cyclic Group

We wish to classify the automorphisms of the cyclic group of order n, C_n. The following result is a generalisation of our results in [**1**], Section 3.

Proposition 4.1.1. *Suppose G is a cyclic group of order n, say $G = \langle c\rangle$ where c has order n. Then*

$$\mathrm{Aut}(G) = \{(\beta : G \mapsto G) : (\exists i : \beta(c^r) = c^{ri}, 1 \leq i < n, (n, i) = 1)\}$$

Proof. Suppose G is a cyclic group of order n, say $G = \langle c\rangle$ where c has order n. Let

$$X = \{(\beta : G \mapsto G) : (\exists i : \beta(c^r) = c^{ri}, 1 \leq i < n, (n, i) = 1)\}$$

for brevity.

($\supseteq$) Let $\alpha \in X$. Then $\exists i : \alpha(c^r) = c^{ri}, (n, i) = 1$. α is a homomorphism, since

$$\alpha(c^r c^s) = c^{ri} c^{si} = c^{ri+si} = c^{(r+s)i} = \alpha(c^{r+s})$$

Now suppose $\alpha(c^r) = \alpha(c^s)$, then $c^{ri} = c^{si}$, so $ri = si + kn$ for some k, so $i \mid kn$, so $i \mid k$, as $(n, i) = 1$. Therefore,

$$c^r = c^{s+\frac{k}{i}n} = c^s$$

(noting here that $i \neq 0$) and so α is injective. Finally, if $y \in G$ then by Lemma 0.2 of [**1**], we have that $(c^i)^k = y$, so that if we set $x = c^k$ then $\alpha(x) = \alpha(c^k) = (c^k)^i = (c^i)^k = y$. So α is an automorphism of G and so $\alpha \in \mathrm{Aut}(G)$. As α was an arbitrary element of X, we have that $X \subseteq \mathrm{Aut}(G)$.

($\subseteq$) Let $\alpha \in \mathrm{Aut}(G)$. Then $\alpha(c) \in G$, so $\alpha(c) = c^i$ for some $0 \leq i < n$, as c generates the group. This $i \neq 0$, otherwise we would have

$$\alpha(c) = c^0 = \mathrm{id}_G = \alpha(\mathrm{id}_G)$$

and so α would not be 1-1. So $1 \leq i < n$. We have that $\alpha(c^r) = (\alpha(c))^r = (c^i)^r = c^{ri}$. It remains to show that $(n, i) = 1$. Suppose not, and let $a \mid n$, $a \mid i$, where $a > 1$. Now $i = am$, say, and $n = ar$. Note $r \mid n$ so $r < n$, and $r \neq 1$ otherwise $n = a$ so $n \mid i$, but this is a contradiction as $i < n$. So

$$\alpha(c^r) = c^{ri} = c^{ram} = c^{nm} = (c^n)^m = (id_G)^m = id_G = \alpha(id_G)$$

but since $1 < r < n$, we have $c^r \neq id_G$, so α is not injective and so cannot be an automorphism. □

4.2. The case where Y is cyclic of prime order

Computation of the set $\mathrm{Hom}(Y, \mathrm{Aut}(X))$ is crucial for any application of Theorem 3.3.3. However, in general this set is quite hard to compute. For our purposes, the case where Y is cyclic of prime order shall be quite important, as the remark immediately after Corollary 3.3.4 shows. In this case, the computation of the set is simplified a little.

Proposition 4.2.1. *Suppose X is a solvable group of order n, and Y is a cyclic (and therefore Abelian, therefore solvable) group of prime order p, such that p does not divide n (so that X and Y have coprime orders). Let c be a generator of Y. Then the map*

$$\phi : \mathrm{Hom}(Y, \mathrm{Aut}(X)) \mapsto \{f \in \mathrm{Aut}(X) : f^p = \mathrm{id}_{\mathrm{Aut}(X)}\}; g \mapsto g(c)$$

where f^p denotes f composed with itself p times, is a bijection.

Proof. Let X be a solvable group of order n, and Y a cyclic group of prime order p, such that p does not divide n. Let c be a generator of Y, and define

$$S = \{f \in \mathrm{Aut}(X) : f^p = \mathrm{id}_{\mathrm{Aut}(X)}\}$$

and

$$\phi : \mathrm{Hom}(Y, \mathrm{Aut}(X)) \mapsto S; g \mapsto g(c)$$

where f^p denotes f composed with itself p times.

This map is well-defined, since for any $g \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$, $g(c) \in \mathrm{Aut}(X)$, and also

$$(g(c))^p = g(c^p) = g(\mathrm{id}_Y) = \mathrm{id}_{\mathrm{Aut}(X)}$$

as a homomorphism must map the identity to the identity. Therefore, $\phi(g) = g(c)$ is in S.

We shall show that ϕ is 1-1. Let $g_1, g_2 \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$ be such that $\phi(g_1) = \phi(g_2)$. Then $g_1(c) = g_2(c)$. Take any $y \in Y$, then $y = c^i$ for some integer i. Now

$$g_1(y) = g_1(c^i) = (g_1(c))^i = (g_2(c))^i = g_2(c^i) = g_2(y)$$

so that $g_1 = g_2$ (since y was arbitrary). Therefore, ϕ is 1-1.

We show that ϕ is onto. Let $f \in S$. Define the map

$$g : Y \mapsto \mathrm{Aut}(X); c^i \mapsto f^i$$

where c^i denotes the unique such representation with i an integer and $0 \leq i < p$. Clearly $\phi(g) = g(c) = g(c^1) = f^1 = f$. We need to show that g is a homomorphism. Take $y_1, y_2 \in Y$, then $y_1 = c^i$ and $y_2 = c^j$ for some unique integers i, j with $0 \leq i < p, 0 \leq j < p$. Now if $i + j < p$ then

$$g(y_1 y_2) = g(c^i c^j) = g(c^{i+j}) = f^{i+j} = f^i f^j = g(y_1)g(y_2).$$

But if $i + j \geq p$ then certainly $i + j < 2p$, so $i + j = p + r$ for some r with $0 \leq r < p$. In this case,

$$\begin{aligned} g(y_1 y_2) &= g(c^i c^j) \\ &= g(c^{i+j}) \\ &= g(c^{p+r}) \\ &= g(c^p c^r) \\ &= g(c^r) \\ &= f^r \\ &= f^p f^r \\ &= f^{p+r} \\ &= f^{i+j} \\ &= f^i f^j \\ &= g(y_1) g(y_2). \end{aligned}$$

In either case, g is a homomorphism, and so ϕ is onto.

Therefore, ϕ is a bijection. □

Example 4.2.2 (Groups of order $2qr$). Let G be a group of order $2qr$. Let $X = C_{qr}$ and $Y = C_2$. Y is Abelian therefore solvable, and X is solvable by Proposition 1.5.2. Furthermore, $(2, qr) = 1$. Applying the Extension Classification Schema, G corresponds to a homomorphism from Y to $\mathrm{Aut}(X)$, and by Proposition 4.2.1, the set $\mathrm{Hom}(Y, \mathrm{Aut}(X))$ is in 1-1 correspondence with the set of automorphisms σ of X which have the property $\sigma^2 = \mathrm{id}_{\mathrm{Aut}(X)}$. Thus for any G we get an automorphism of X, and G is uniquely determined by this automorphism. However the automorphism does not uniquely determine G - if any two σ_1 and σ_2 produce isomorphic groups, then the corresponding homomorphisms ρ_1 and ρ_2 must be in the same orbit of the ECS Action. If this happens, then we must have $\rho_2 = \lambda_\alpha \circ \rho_1 \circ \beta^{-1}$ for some automorphisms $\alpha : X \mapsto X$ and $\beta : Y \mapsto Y$. However any automorphism of $Y = C_2$ must be the identity, so we get that $\rho_2 = \lambda_\alpha \circ \rho_1$, or in other words, $\rho_2 = \alpha \circ \rho_1 \circ \alpha^{-1}$. Since the ρ_i are homomorphisms, this property must translate to the automorphisms σ_i, in other words, σ_1 and σ_2 give rise to isomorphic groups iff they are conjugate by some element of $\mathrm{Aut}(X)$, i.e. if they are conjugate in $\mathrm{Aut}(X)$.

4.3. Classification of groups of order pq

We state an initial lemma concerning composition of automorphisms of cyclic groups.

Lemma 4.3.1. *Suppose that G is a cyclic group with order n and generator g, that $f \in \mathrm{Aut}(G)$, that i is an integer such that $0 \leq i < n$ and $f(g) = g^i$, and that m is a non-negative integer. Then*

$$f^m(x) = x^{i^m}$$

for all $x \in G$.

Proof. Suppose that G is a cyclic group with order n and generator g, that $f \in \mathrm{Aut}(G)$, and that i is an integer such that $0 \le i < n$ and $f(g) = g^i$.

We shall prove the statement "$f^m(x) = x^{i^m}$ for all $x \in G$" by induction, for all integers $m \ge 0$. The basis case is easy, since $f^0(x) = x = x^1 = x^{i^0}$.

Suppose the statement is true for $m = k$. Take any $x \in G$. Then $x = g^r$ for some r with $0 \le r < n$ and

$$\begin{aligned} f^{k+1}(x) &= f(f^k(x)) \\ &= f(x^{i^k}) \\ &= f((g^r)^{i^k}) \\ &= f(g^{ri^k}) \\ &= f(g)^{ri^k} \\ &= (g^i)^{ri^k} \\ &= g^{ri^{k+1}} \\ &= (g^r)^{i^{k+1}} \\ &= x^{i^{k+1}} \end{aligned}$$

so that the statement is true for $m = k + 1$.

By the principle of induction, the statement holds for all integers $m \ge 0$, i.e. the lemma is true. □

When we have a group of order pq, X is also cyclic, and so we have a much simpler situation again. However we shall prove the following results in the case where X is just cyclic, not necessarily of prime order. As we have done before, we shall split the proof into two results, so that we can use the core of the argument again later under different circumstances.

Lemma 4.3.2. *Suppose that X is a cyclic group (therefore Abelian, therefore solvable) of order n and with generator d. For any $x \in X$, let $\mathrm{I}(x)$ denote the unique i with $0 \le i < n$ such that $x = d^i$. Define*

$$\begin{aligned} S &= \{f \in \mathrm{Aut}(X) : f^p = \mathrm{id}_{\mathrm{Aut}(X)}\} \\ T &= \{i \in \mathbb{Z} : 1 \le i < n, (n, i) = 1, i^p \equiv 1 \pmod{n}\} \end{aligned}$$

where f^p denotes f composed with itself p times. Then the map

$$\phi : S \mapsto T; f \mapsto \mathrm{I}(f(d))$$

is a bijection.

Proof. Suppose that X is a cyclic group of order n and with generator d. For any $x \in X$, let $\mathrm{I}(x)$ denote the unique i with $0 \le i < n$ such that $x = d^i$. Define

$$\begin{aligned} S &= \{f \in \mathrm{Aut}(X) : f^p = \mathrm{id}_{\mathrm{Aut}(X)}\} \\ T &= \{i \in \mathbb{Z} : 1 \le i < n, (n, i) = 1, i^p \equiv 1 \pmod{n}\} \end{aligned}$$

where f^p denotes f composed with itself p times, and

$$\phi : S \mapsto T; f \mapsto \mathrm{I}(f(d)).$$

First of all ϕ is well-defined. Take any $f \in S$ and let $i = \mathrm{I}(f(d))$, clearly an integer with $0 \leq i < n$. By Proposition 4.1.1, we have $(n, i) = 1$ and $1 \leq i < n$ from the fact that $f \in \mathrm{Aut}(X)$. By Lemma 4.3.1, we have $f^p(d) = d^{i^p}$, but as $f \in S$ we also have $f^p(d) = d$. Therefore, $d^{i^p - 1}$ is equal to the identity, so $i^p - 1$ must be a multiple of n, the order of d. Therefore, $i \equiv 1 \pmod{n}$, and so $i \in T$.

Next ϕ is 1-1. Suppose $f, g \in S$ and $\phi(f) = \phi(g)$. Then $f(d) = g^i$ for some i with $0 \leq i < n$ and $g(d) = g^j$ for some j with $0 \leq j < n$. But $i = j$, so $f(d) = g(d)$. Now let $x \in X$ be arbitrary. Then $x = d^r$ for some r with $0 \leq r < n$. Now

$$f(x) = f(d^r) = f(d)^r = g(d)^r = g(d^r) = g(x)$$

and so $f = g$. Hence ϕ is 1-1.

Finally, we show ϕ is onto. Suppose $i \in T$. Define the map

$$f : X \mapsto X; d^r \mapsto d^{ir}.$$

As $i \in T$, Proposition 4.1.1 gives that f is an automorphism. Also, if x is any element of X then $x = d^r$ for some r with $0 \leq r < n$. Then, by Lemma 4.3.1, $f^p(x) = x^{i^p} = x$, since $i^p \equiv 1 \pmod{n}$. Therefore, $f \in S$, and so ϕ is onto.

Therefore, ϕ is a bijection. □

Proposition 4.3.3. *Suppose that X is a cyclic group (therefore Abelian, therefore solvable) of order n and with generator d, and Y is a cyclic group (therefore Abelian, therefore solvable) of prime order p and with generator c, such that p does not divide n (so that X and Y have coprime orders). For any $x \in X$, let $\mathrm{I}(x)$ denote the unique i with $0 \leq i < n$ such that $x = d^i$. Then the map*

$$\phi : \mathrm{Hom}(Y, \mathrm{Aut}(X)) \mapsto \{i \in \mathbb{Z} : 1 \leq i < n, (n, i) = 1, i^p \equiv 1 \pmod{n}\};$$
$$g \mapsto \mathrm{I}(g(c)(d))$$

is a bijection.

Proof. Suppose that X is a cyclic group of order n and with generator d, and Y is a cyclic group of prime order p and with generator c, such that p does not divide n. For any $x \in X$, let $\mathrm{I}(x)$ denote the unique i with $0 \leq i < n$ such that $x = d^i$. Define

$$S = \{f \in \mathrm{Aut}(X) : f^p = \mathrm{id}_{\mathrm{Aut}(X)}\}$$
$$T = \{i \in \mathbb{Z} : 1 \leq i < n, (n, i) = 1, i^p \equiv 1 \pmod{n}\}$$

where f^p denotes f composed with itself p times, and

$$\phi : \mathrm{Hom}(Y, \mathrm{Aut}(X)) \mapsto T; g \mapsto \mathrm{I}(g(c)(d)).$$

Now let

$$\phi_1 : \mathrm{Hom}(Y, \mathrm{Aut}(X)) \mapsto S; g \mapsto g(c)$$

and

$$\phi_2 : S \mapsto T; f \mapsto \mathrm{I}(f(d))$$

so that $\phi = \phi_2 \circ \phi_1$. Since X is a cyclic group, it is Abelian and therefore solvable, and so Proposition 4.2.1 gives that ϕ_1 is a bijection. By Lemma 4.3.2, ϕ_2 is a bijection. Therefore, $\phi = \phi_2 \circ \phi_1$ is a bijection. □

Remark. This proposition shows that any element $\sigma \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$ is uniquely determined by its value $\sigma(c)(d)$. For given some $x \in X$, we can construct an element of $\mathrm{Hom}(Y, \mathrm{Aut}(X))$ which has $\sigma(c)(d)$ is equal to x, as ϕ is onto. Furthermore, if σ_1 and σ_2 are two elements of $\mathrm{Hom}(Y, \mathrm{Aut}(X))$ with the same value $\sigma(c)(d)$, then they are in fact equal, as ϕ is 1-1.

The set constructed above is in fact rather special: it forms a group.

Lemma 4.3.4. *Let p, q be primes, $p < q$. Then the set*

$$G = \{i \in \mathbb{Z} : 1 \leq i < q, i^p \equiv 1 \pmod{q}\}$$

forms a group with respect to multiplication modulo q. Furthermore, this group is cyclic, and is either trivial or has order p.

Proof. Let p, q be primes, $p < q$, and

$$G = \{i \in \mathbb{Z} : 1 \leq i < q, i^p \equiv 1 \pmod{q}\}$$

under the operation of multiplication modulo q.

First, G is closed, as if $i, j \in G$ then $i^p \equiv 1 \pmod{q}$ and $j^p \equiv 1 \pmod{q}$, so $(ij)^p = i^p j^p \equiv 1 \pmod{q}$.

Secondly, the operation is associative on G, as modular multiplication is associative.

Thirdly, G contains an identity, namely 1, and $1i = i1 = i$ for $i \in G$ under normal multiplication, therefore this remains true under modular multiplication.

Finally, if $i \in G$ then $i^{q-1}i = ii^{q-1} = 1$ under normal multiplication, therefore also under modular multiplication, and so i has an inverse (namely i^{q-1}).

G is cyclic since it is a subgroup of $\mathbb{Z}_q^*$, a cyclic group.

If G is non-trivial then there is some non-identity $i \in G$ and $i^p \equiv 1 \pmod{q}$, that is, $i^p = 1$ in the group. The order of i must therefore divide p, so must be 1 or p. Since i is not the identity, it does not have order 1, so it has order p. The order of i divides the order of the group, so the order of the group is at least p.

Since i was arbitrary, we have shown that every non-identity element has order p. Since G is cyclic, it must contain an element with order equal to the order of the group. The maximum order of elements is p, so G must have order at most p. Therefore, $|G| = p$. □

We shall also need a result on cyclic groups of squarefree order.

Lemma 4.3.5. *Let $p_1, ..., p_r$ be primes, then*

$$C_{p_1} \times C_{p_2} \times \cdots \times C_{p_r} \cong C_{p_1 p_2 \cdots p_r}.$$

Proof. Let $p_1, ..., p_r$ be primes, and let

$$G = C_{p_1} \times C_{p_2} \times \cdots \times C_{p_r}$$

Further, let

$$n = |G| = p_1 p_2 \cdots p_r$$

We need only show that the group G is cyclic. Then it must be isomorphic to the unique (up to isomorphism) cyclic group of order n.

Suppose $a_i \in C_{p_i}$ are generators. Let

$$a = (a_1, a_2, ..., a_r) \in G.$$

Now we have that

$$\begin{aligned} a^n &= (a_1^n, a_2^n, ..., a_r^n) \\ &= ((a_1^{p_1})^{\frac{n}{p_1}}, (a_1^{p_2})^{\frac{n}{p_2}}, ..., (a_r^{p_r})^{\frac{n}{p_r}}) \\ &= (\mathrm{id}_{C_{p_1}}^{\frac{n}{p_1}}, \mathrm{id}_{C_{p_2}}^{\frac{n}{p_2}}, ..., \mathrm{id}_{C_{p_r}}^{\frac{n}{p_r}}) \\ &= (\mathrm{id}_{C_{p_1}}, \mathrm{id}_{C_{p_2}}, ..., \mathrm{id}_{C_{p_r}}) \\ &= \mathrm{id}_G \end{aligned}$$

and so the order of a must divide n. However divisors of n have the form $m = q_1 q_2 \cdots q_s$ where each $q_i = p_j$ for some j, and no two q_i are equal. We certainly have $m \leq n$. If $m < n$ then there must exist some k such that p_k does not divide m. Now if $a^m = \mathrm{id}_G$ then

$$\mathrm{id}_G = (\mathrm{id}_{C_{p_1}}, \mathrm{id}_{C_{p_2}}, ..., \mathrm{id}_{C_{p_r}}) = a^m = (a_1^m, a_2^m, ..., a_r^m)$$

and so $a_k^m = id_{C_{p_k}}$. However as a_k generates C_{p_k}, it has order p_k, so p_k must divide m, a contradiction. Therefore $n = |G|$ is the order of a, and so a generates G, hence G is cyclic. □

We are now in a position to apply the Extension Classification Schema to classify all groups of order pq.

Proposition 4.3.6. *Let p and q be primes with $p < q$.*

(i) *If there does not exist an integer i with $1 < i < q$ and $i^p \equiv 1 \pmod q$ then any group of order pq is isomorphic to the cyclic group C_{pq}.*

(ii) *If there exists an integer i with $1 < i < q$ and $i^p \equiv 1 \pmod q$ then define a map*

$$\sigma : C_p \mapsto \mathrm{Aut}(C_q); a^r \mapsto f_{i^r}$$

where a is a generator of C_p, and

$$f_j : C_q \mapsto C_q; b^s \mapsto b^{js}$$

where b is a generator of C_q. Then "C_{pq}, $C_q \rtimes_\sigma C_p$" is a list of groups of order pq up to isomorphism.

Proof. Let p and q be primes with $p < q$. Let G be any group of order pq. Then, by Proposition 1.5.1, G has a normal subgroup of index p, say N. Let $X = C_q$ (with generator b) and $Y = C_p$ (with generator a). X and Y are both cyclic, therefore Abelian, therefore solvable. They also have coprime orders, since p and q are primes with $p \neq q$. We have that

$$|N| = \frac{|G|}{\frac{|G|}{|N|}} = \frac{|G|}{[G:N]} = \frac{pq}{p} = q$$

and so $N \cong X$. Furthermore, $|G/N| = [G : N] = p$, and so $G/N \cong Y$.

Let

$$S = \{i \in \mathbb{Z} : 1 \leq i < q, i^p \equiv 1 \,(\operatorname{mod} q)\}.$$

By Proposition 4.3.3, $\operatorname{Hom}(Y, \operatorname{Aut}(X))$ has the same size as S (we have $(i, q) = 1$ for all $i \in S$, because q is prime and $i < q$).

(i) Suppose that there does not exist an integer i with $1 < i < q$ and $i^p \equiv 1 \,(\operatorname{mod} q)$. Then there cannot exist any elements in S which are not equal to 1. But in fact $1 \in S$, because $1 \leq 1 < q$, $(1, q) = 1$ and $1^p = 1 \equiv 1 \,(\operatorname{mod} q)$. Therefore, S contains only 1 element, namely 1. So

$$|\operatorname{Hom}(Y, \operatorname{Aut}(X))| = |S| = 1.$$

By Theorem 3.3.3(ii), $G \cong X \rtimes_\sigma Y$, for some $\sigma \in \operatorname{Hom}(Y, \operatorname{Aut}(X))$. However also $C_{pq} \cong X \rtimes_\rho Y$ for some $\rho \in \operatorname{Hom}(Y, \operatorname{Aut}(X))$. Since $\operatorname{Hom}(Y, \operatorname{Aut}(X))$ has only one element, we must have $\sigma = \rho$, and so $G \cong X \rtimes_\sigma Y = X \rtimes_\rho Y \cong C_{pq}$.

(ii) Suppose that there exists an integer i with $1 < i < q$ and $i^p \equiv 1 \,(\operatorname{mod} q)$. Define

$$f_j : X \mapsto X; x \mapsto x^j$$

for any j, as in the statement of the result, and let

$$\sigma_i : Y \mapsto \operatorname{Aut}(X); a^k \mapsto f_{i^k}$$

for any integer i.

Now take any r, s such that $1 < r < q$, $1 < s < q$ and $r^p \equiv 1 \,(\operatorname{mod} q)$, $s^p \equiv 1 \,(\operatorname{mod} q)$. By Theorem 3.3.3(iii), σ_r and σ_s give rise to isomorphic groups $X \rtimes_{\sigma_r} Y$ and $X \rtimes_{\sigma_s} Y$ if and only if

$$\sigma_s = \lambda_\alpha \circ \sigma_r \circ \beta^{-1} \,(\dagger)$$

for some $\alpha \in \operatorname{Aut}(X)$, $\beta \in \operatorname{Aut}(Y)$. By Proposition 4.3.3, σ_r, σ_s are completely determined by their values $\sigma(a)(b)$. By Proposition 4.1.1, α and β are completely determined by their values at b and a respectively. Therefore, let $\beta(a) = a^i$ and $\alpha(b) = b^j$ (by Proposition 4.1.1 we also have that $1 \leq i < p$, $1 \leq j < q$). The formula ($\dagger$) is then equivalent to:

$$\begin{aligned}
b^s &= \sigma_s(a)(b) \\
&= (\lambda_\alpha(\sigma_r(\beta^{-1}(a))))(b) \\
&= (\lambda_\alpha(\sigma_r(a^{p-i})))(b) \\
&= (\lambda_\alpha(f_{r^{p-i}}))(b) \\
&= \alpha(f_{r^{p-i}}(\alpha^{-1}(b))) \\
&= \alpha(f_{r^{p-i}}(b^{q-j})) \\
&= \alpha(b^{r^{p-i}(q-j)}) \\
&= ((b^{r^{p-i}})^{q-j})^j \\
&= b^{r^{p-i}}
\end{aligned}$$

which is in turn equivalent to $s = r^{p-i} \,(\operatorname{mod} q)$. So σ_r and σ_s give rise to isomorphic groups if and only if there exists some i with $1 \leq i < p$ such that $s = r^{p-i} \,(\operatorname{mod} q)$, in other words, if there exists some i with $0 < i \leq p - 1$

such that $s = r^i \pmod{q}$. However, by Lemma 4.3.4, this is true if $r, s \neq 1$, the identity of the group, as then r must generate the group. This is true by hypothesis, and so σ_r and σ_s give rise to isomorphic groups. Therefore, there is at most two groups of order pq in this case. However in fact, there are exactly two, as we cannot have i such that $s = 1^i$ for some $s \neq 1$. Therefore, the r, s above give rise to a different group from 1. Let $\sigma = \sigma_r$ as in the statement of the result, and $\theta = \sigma_1$, the trivial map corresponding to 1. By applying Theorem 3.3.3(i) and Theorem 3.3.3(ii), we obtain that "$X \rtimes_\theta Y$, $X \rtimes_\sigma Y$" is a complete list of groups of order pq up to isomorphism (because any such group must be isomorphic to some $X \rtimes_\rho Y$ for $\rho \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$, and this group is isomorphic to either $X \rtimes_\theta Y$, if $\rho = \theta$, or $X \rtimes_\sigma Y$, otherwise).

It remains to show that $X \rtimes_\theta Y$ is isomorphic to the cyclic group of order pq. First note that this group has underlying set $X \times Y$, and if we take (x_1, y_1) and (x_2, y_2) in the group, then the operation is

$$(x_1, y_1)(x_2, y_2) = (x_1\theta(y_1)(x_2), y_1y_2) = (x_1f_1(x_2), y_1y_2) = (x_1x_2, y_1y_2)$$

in other words, the group is isomorphic to the direct product $X \times Y = C_q \times C_p$. By Lemma 4.3.5, this group is cyclic of order $qp = pq$. □

We may indeed get a much easier condition for the previous result to hold. For the proof of the following I was helped by Bart Goddard ([**3**]).

LEMMA 4.3.7. *Suppose p and q are primes. Then there exists i with $1 < i < q$ and $i^p \equiv 1 \pmod{q}$ iff $p \mid q - 1$.*

PROOF. Suppose p and q are primes. Let $G = \{1, 2, ..., q-1\}$ under multiplication modulo q.

($\Longrightarrow$) Suppose there exists i with $1 < i < q$ and $i^p \equiv 1 \pmod{q}$. Then $i \in G$, and $i^p \equiv 1$ within the group. Therefore, the order of i is at most p. Suppose the order is m. Then $m \mid p$, but $m \neq 1$ otherwise $i = 1$. Therefore, $m = p$. Since the order of i divides the order of the group, we have that $p \mid q-1$.

($\Longleftarrow$) Suppose $p \mid q - 1$. Then G contains an element of order p by Cauchy's Group Theorem. This element, say i, has $i^p \equiv 1 \pmod{q}$. Also $i \neq 1$, since otherwise i would have order 1. □

The proof of the following involves an easy combination of the above two results, and so is omitted.

PROPOSITION 4.3.8. *Let p and q be primes with $p < q$.*

(i) *If $p \nmid q-1$ then any group of order pq is isomorphic to the cyclic group C_{pq}.*

(ii) *If $p \mid q-1$ then by Lemma 4.3.7, there exists an integer i with $1 < i < q$ and $i^p \equiv 1 \pmod{q}$. Define a map*

$$\sigma : C_p \mapsto \mathrm{Aut}(C_q); a^r \mapsto f_{i^r}$$

where a is a generator of C_p, and

$$f_j : C_q \mapsto C_q; b^s \mapsto b^{js}$$

where b is a generator of C_q. Then "C_{pq}, $C_q \rtimes_\sigma C_p$" is a list of groups of order pq up to isomorphism.

4.4. The case where X is cyclic of squarefree order

The initial lemmas of this section concern the automorphism group of a product. The first of these is simply an intermediate step of the second, which is convenient to give outside of the main body of the proof for notational purposes.

LEMMA 4.4.1. *Let $G_1, G_2, ..., G_r$ be groups of coprime orders $n_1, n_2, ..., n_r$, and $G = G_1 \times G_2 \times \cdots \times G_r$. For each i, let*

$$H_i = \{(\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, x, \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r}) : x \in G_i\}$$

and

$$J_i = \{x \in G : x^{n_i} = \mathrm{id}_G\}.$$

Then $H_i = J_i$.

PROOF. Let $G_1, G_2, ..., G_r$ be groups of coprime orders $n_1, n_2, ..., n_r$, and $G = G_1 \times G_2 \times \cdots \times G_r$. For each i, let

$$H_i = \{(\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, x, \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r}) : x \in G_i\}$$

and

$$J_i = \{x \in G : x^{n_i} = \mathrm{id}_G\}.$$

($\subseteq$) Let i be an integer and $h \in H_i$. Then $h_i^{n_i} = \mathrm{id}_{G_i}$, since $h_i \in G_i$ and $|G_i| = n_i$. Therefore,

$$\begin{aligned} h^{n_i} &= (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, x, \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r})^{n_i} \\ &= (\mathrm{id}_{G_1}^{n_i}, \mathrm{id}_{G_2}^{n_i}, ..., \mathrm{id}_{G_{i-1}}^{n_i}, x, \mathrm{id}_{G_{i+1}}^{n_i}, ..., \mathrm{id}_{G_r}^{n_i}) \\ &= (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, \mathrm{id}_{G_i}, \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r}) \\ &= \mathrm{id}_G \end{aligned}$$

so that $h \in J_i$.

($\supseteq$). Let i be an integer and $j \in J_i$. Then $j^{n_i} = \mathrm{id}_G$, so

$$\begin{aligned} (j_1^{n_i}, j_2^{n_i}, ..., j_r^{n_i}) &= (j_1, j_2, ..., j_r)^{n_i} \\ &= j^{n_i} \\ &= \mathrm{id}_G \\ &= (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_r}) \end{aligned}$$

and so $j_k^{n_i} = \mathrm{id}_{G_k}$ for each integer k.

Take an integer $k \neq i$. Now $j_k^{n_i} = \mathrm{id}_{G_k}$, so the order of j_k must divide n_i. However certainly the order of j_k divides $|G_k| = n_k$. But n_k and n_i are coprime (as $k \neq i$), therefore the order of j_k must be 1. Thus $j_k = \mathrm{id}_{G_k}$ for each $k \neq i$, that is, j has the form

$$j = (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, j_i, \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r})$$

or in other words, $j \in H_i$. □

LEMMA 4.4.2. *Let $G_1, G_2, ..., G_r$ be groups of coprime orders. Then*

$$\mathrm{Aut}(G_1 \times G_2 \times \cdots \times G_r) = \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \times \cdots \times \mathrm{Aut}(G_r).$$

Proof. Let $G_1, G_2, ..., G_r$ be groups of coprime orders $n_1, n_2, ..., n_r$, and $G = G_1 \times G_2 \times \cdots \times G_r$.

($\supseteq$) Let $f \in \text{Aut}(G_1) \times \text{Aut}(G_2) \times \cdots \times \text{Aut}(G_r)$. Then $f = (f_1, f_2, ..., f_r)$ where each $f_i \in \text{Aut}(G_i)$. We regard f as a function from G to G, by

$$f(g_1, g_2, ..., g_r) = (f_1(g_1), f_2(g_2), ..., f_r(g_r)).$$

We must check that f is an automorphism of G. Clearly its domain and codomain have the same order, so we need only check that it is onto to see it is a bijection. Take some $y \in G$, then

$$y = (y_1, y_2, ..., y_r)$$

for $y_i \in G_i$. Now each $y_i = f_i(x_i)$ for some $x_i \in G_i$, since f_i is onto. Let

$$x = (x_1, x_2, ..., x_r)$$

then

$$f(x) = f(x_1, x_2, ..., x_r) = (f_1(x_1), f_2(x_2), ..., f_r(x_r)) = (y_1, y_2, ..., y_r) = y$$

and so f is onto, hence a bijection.

Finally we show that f is a homomorphism. Take $x, y \in G$, then

$$x = (x_1, x_2, ..., x_r)$$

and

$$y = (y_1, y_2, ..., y_r).$$

Now

$$\begin{aligned} f(xy) &= f((x_1, x_2, ..., x_r)(y_1, y_2, ..., y_r)) \\ &= f(x_1y_1, x_2y_2, ..., x_ry_r) \\ &= (f_1(x_1y_1), f_2(x_2y_2), ..., f_r(x_ry_r)) \\ &= (f_1(x_1)f_1(y_1), f_2(x_2)f_2(y_2), ..., f_r(x_r)f_r(y_r)) \\ &= (f_1(x_1), f_2(x_2), ..., f_r(x_r))(f_1(y_1), f_2(y_2), ..., f_r(y_r)) \\ &= f(x_1, x_2, ..., x_r)f(y_1, y_2, ..., y_r) \\ &= f(x)f(y) \end{aligned}$$

so that f is a homomorphism.

Altogether, f is an automorphism of G.

($\subseteq$) Let $f \in \text{Aut}(G)$. For each i, let

$$H_i = \{(\text{id}_{G_1}, \text{id}_{G_2}, ..., \text{id}_{G_{i-1}}, x, \text{id}_{G_{i+1}}, ..., \text{id}_{G_r}) : x \in G_i\}$$

and

$$J_i = \{x \in G : x^{n_i} = \text{id}_G\}$$

Then $H_i = J_i$, by Lemma 4.4.1.

We may split f into components $f_i : G \mapsto G_i$, so that

$$f(x_1, x_2, ..., x_r) = (f_1(x_1, x_2, ..., x_r), f_2(x_1, x_2, ..., x_r), ..., f_r(x_1, x_2, ..., x_r)).$$

Take any $x \in G$. We have that

$$x = y_1y_2 \cdots y_r$$

where

$$y_i = (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, x_i, \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r}).$$

We can deduce $y_i \in H_i$, so $y_i \in J_i$, so $y_i^{n_i} = \mathrm{id}_G$. We have that

$$f(y_i)^{n_i} = f(y_i^{n_i}) = f(\mathrm{id}_G) = \mathrm{id}_G$$

so $f(y_i) \in J_i$, so $f(y_i) \in H_i$. Therefore, $f(y_i)$ has the form

$$(f_1(y_i), f_2(y_i), ..., f_r(y_i)) = f(y_i) = (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, z_i, \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r})$$

for some $z_i \in G_i$, so that $f_k(y_i) = \mathrm{id}_{G_k}$ for $k \neq i$. Now,

$$\begin{aligned}
&(f_1(x_1, x_2, ..., x_r), f_2(x_1, x_2, ..., x_r), ..., f_r(x_1, x_2, ..., x_r))\\
&= f(x_1, x_2, ..., x_r)\\
&= f(x)\\
&= f(y_1 y_2 \cdots y_r)\\
&= f(y_1) f(y_2) \cdots f(y_r)\\
&= (f_1(y_1), f_2(y_1), ..., f_r(y_1))\\
&\qquad (f_2(y_1), f_2(y_2), ..., f_r(y_2))\\
&\qquad \cdots\\
&\qquad (f_1(y_r), f_2(y_r), ..., f_r(y_r))\\
&= (f_1(y_1), \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_r})\\
&\qquad (\mathrm{id}_{G_1}, f_2(y_2), \mathrm{id}_{G_3}, ..., \mathrm{id}_{G_r})\\
&\qquad \cdots\\
&\qquad (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{r-1}}, f_r(y_r))\\
&= (f_1(y_1), f_2(y_2), ..., f_r(y_r))\\
&= (f_1(x_1, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_r}),\\
&\qquad f_2(\mathrm{id}_{G_1}, x_2, \mathrm{id}_{G_3}, ..., \mathrm{id}_{G_r}),\\
&\qquad ...,\\
&\qquad f_r(\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{r-1}}, f_r(y_r)))
\end{aligned}$$

so that for each i,

$$f_i(x_1, x_2, ..., x_r) = f_i(\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, x_i, \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r})$$

no matter what x_j equals for $i \neq j$. In other words, f_i does not depend on x_j for $j \neq i$, and we can simply write

$$f_i(x_1, x_2, ..., x_r) = f_i(x_i)$$

and regard f_i as a function $f_i : G_i \mapsto G_i$.

Now take $x_i, y_i \in G_i$ for each i and let $x = (x_1, x_2, ..., x_r)$ and $y = (y_1, y_2, ..., y_r)$. Then

$$\begin{aligned}(f_1(x_1y_1), f_2(x_2y_2), ..., f_r(x_ry_r)) &= (f_1((xy)_1), f_2((xy)_2), ..., f_r((xy)_r))\\ &= f(xy)\\ &= f(x)f(y)\\ &= (f_1(x_1), f_2(x_2), ..., f_r(x_r))\\ &\quad\ (f_1(y_1), f_2(y_2), ..., f_r(y_r))\\ &= (f_1(x_1)f_1(y_1), f_2(x_2)f_2(y_2), ..., f_r(x_r)f_r(y_r))\end{aligned}$$

and so for each i,

$$f_i(x_iy_i) = f_i(x_i)f_i(y_i)$$

therefore, the f_i are homomorphisms.

We have that

$$\begin{aligned}(f_1(\mathrm{id}_{G_1}), f_2(\mathrm{id}_{G_2}), ..., f_r(\mathrm{id}_{G_r})) &= f(\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_r})\\ &= f(\mathrm{id}_G)\\ &= \mathrm{id}_G\\ &= (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_r})\end{aligned}$$

so that $f_i(\mathrm{id}_{G_i}) = \mathrm{id}_{G_i}$ for each i.

Suppose that $f_i(x) = f_i(y)$ for some integer i and $x, y \in G_i$. Let

$$g = (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, x, \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r})$$

and

$$h = (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, y, \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r}).$$

Now it is certainly true that

$$\begin{aligned}&(\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, f_i(x), \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r})\\ &= (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, f_i(y), \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r})\end{aligned}$$

and so $f(g) = f(h)$. Therefore $g = h$, that is, $x = y$. Thus f_i is 1-1 for each i.

Let $y \in G_i$ for some integer i. Define

$$h = (\mathrm{id}_{G_1}, \mathrm{id}_{G_2}, ..., \mathrm{id}_{G_{i-1}}, y, \mathrm{id}_{G_{i+1}}, ..., \mathrm{id}_{G_r}).$$

There is some $g \in G$ with $f(g) = h$. Now let $x = g_i$, so that

$$(f_1(g_1), f_2(g_2), ..., f_{i-1}(g_{i-1}), f_i(x), f_{i+1}(g_{i+1}), ..., f_r(g_r)) = f(g) = h$$

that is, $f_i(x) = y$. Therefore f_i is onto for each i.

Altogether we have shown that for each i, f_i is an automorphism of G_i. But by definition $f = (f_1, f_2, ..., f_r)$, so

$$f \in \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2) \times \cdots \times \mathrm{Aut}(G_r)$$

as required. □

The following is a generalisation of Proposition 4.3.3, Lemma 4.3.4 and our results on two homomorphisms being in the same orbit, taken from the proof of Proposition 4.3.6. Because the pqr case is more notationally complicated, we split this off from the main theorem (which was not so necessary with the

pq case). However both directions of implication for part (iii) of the below proposition rely on the same algebraic lemma, which we shall state and prove before the main proposition.

LEMMA 4.4.3. *Let X be a cyclic group of squarefree order $n = p_1p_2\cdots p_r$ with generator d, and let Y be a cyclic group of prime order p with generator c. Let*

$$H = C_{p_1} \times C_{p_2} \times \cdots \times C_{p_r}.$$

Let h_i be a generator of C_{p_i} for each i, chosen such that

$$d = \psi^{-1}(h_1, h_2, ..., h_r).$$

Define for each i, j the function

$$f_{i,j} : C_{p_i} \mapsto C_{p_i}; x \mapsto x^j$$

Let $\alpha : X \mapsto X$ and $\beta : Y \mapsto Y$ be automorphisms, and let $\psi : X \mapsto H$ be an isomorphism. Let $\sigma_1, \sigma_2 \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$, and define r-tuples $(s_1, s_2, ..., s_r)$ and $(t_1, t_2, ..., t_r)$ such that

$$\sigma_1(c) = \psi \circ (f_{1,s_1}, f_{2,s_2}, ..., f_{r,s_r}) \circ \psi^{-1}$$

and

$$\sigma_2(c) = \psi \circ (f_{1,t_1}, f_{2,t_2}, ..., f_{r,t_r}) \circ \psi^{-1}$$

which we can do by Proposition 4.1.1, Lemma 4.4.2 and Lemma 4.3.5. Also let

$$\lambda_\alpha : \mathrm{Aut}(X) \mapsto \mathrm{Aut}(X); f \mapsto \alpha \circ f \circ \alpha^{-1}.$$

Let i be the unique integer such that $1 \le i < p$ and $\beta^{-1}(c) = c^i$. Then

(i)

$$(h_1^{t_1}, h_2^{t_2}, ..., h_r^{t_r}) = \psi(\sigma_2(c)(d))$$

(ii)

$$(h_1^{s_1^i}, h_2^{s_2^i}, ..., h_r^{s_r^i}) = \psi((\lambda_\alpha(\sigma_1(\beta^{-1}(c))))(d)).$$

PROOF. Let X be a cyclic group of squarefree order $n = p_1p_2\cdots p_r$ with generator d, and let Y be a cyclic group of prime order p with generator c. Let

$$H = C_{p_1} \times C_{p_2} \times \cdots \times C_{p_r}.$$

Let h_i be a generator of C_{p_i} for each i, chosen such that

$$d = \psi^{-1}(h_1, h_2, ..., h_r)$$

which we can do (for the details, see the proof of Lemma 4.3.5). Define for each i, j the function

$$f_{i,j} : C_{p_i} \mapsto C_{p_i}; x \mapsto x^j$$

Let $\alpha : X \mapsto X$ and $\beta : Y \mapsto Y$ be automorphisms, and let $\psi : X \mapsto H$ be an isomorphism. Let $\sigma_1, \sigma_2 \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$, and define r-tuples $(s_1, s_2, ..., s_r)$ and $(t_1, t_2, ..., t_r)$ such that

$$\sigma_1(c) = \psi \circ (f_{1,s_1}, f_{2,s_2}, ..., f_{r,s_r}) \circ \psi^{-1}$$

and

$$\sigma_2(c) = \psi \circ (f_{1,t_1}, f_{2,t_2}, ..., f_{r,t_r}) \circ \psi^{-1}$$

which we can do by Proposition 4.1.1, Lemma 4.4.2 and Lemma 4.3.5. Also let

$$\lambda_\alpha : \mathrm{Aut}(X) \mapsto \mathrm{Aut}(X); f \mapsto \alpha \circ f \circ \alpha^{-1}.$$

Finally, let i be the unique integer such that $1 \leq i < p$ and $\beta^{-1}(c) = c^i$.

(i)

$$\begin{aligned}
(h_1^{t_1}, h_2^{t_2}, ..., h_r^{t_r}) &= (f_{1,t_1}(h_1), f_{2,t_2}(h_2), ..., f_{r,t_r}(h_r)) \\
&= (f_{1,t_1}, f_{2,t_2}, ..., f_{r,t_r})(h_1, h_2, ..., h_r) \\
&= (\psi \circ \sigma_2(c) \circ \psi^{-1})(h_1, h_2, ..., h_r) \\
&= \psi(\sigma_2(c)(\psi^{-1}(h_1, h_2, ..., h_r))) \\
&= \psi(\sigma_2(c)(d))
\end{aligned}$$

(ii) Let j be the unique integer such that $\alpha(d) = d^j$ and k be the unique integer such that $\alpha^{-1}(d) = d^k$. Now $d^{jk} = \alpha(\alpha^{-1}(d)) = d$. This means that for any $x \in X$, which must be a power of d, we have that $x^{jk} = x$. By applying ψ to both sides, the same is true in H: raising elements of H to the power jk leaves them unchanged.

$$\begin{aligned}
(h_1^{s_1^i}, h_2^{s_2^i}, ..., h_r^{s_r^i}) &= (h_1^{s_1^i}, h_2^{s_2^i}, ..., h_r^{s_r^i})^{jk} \\
&= (h_1^{ks_1^i}, h_2^{ks_2^i}, ..., h_r^{ks_r^i})^j \\
&= \psi(\psi^{-1}((h_1^{ks_1^i}, h_2^{ks_2^i}, ..., h_r^{ks_r^i})^j)) \\
&= \psi((\psi^{-1}(h_1^{ks_1^i}, h_2^{ks_2^i}, ..., h_r^{ks_r^i}))^j) \\
&= \psi(\alpha(\psi^{-1}(h_1^{ks_1^i}, h_2^{ks_2^i}, ..., h_r^{ks_r^i}))) \\
&= \psi((\alpha \circ \psi^{-1})(h_1^{ks_1^i}, h_2^{ks_2^i}, ..., h_r^{ks_r^i})) \\
&= \psi((\alpha \circ \psi^{-1})(f_{1,s_1}^i(h_1^k), f_{2,s_2}^i(h_2^k), ..., f_{r,s_r}^i(h_r^k))) \\
&= \psi((\alpha \circ \psi^{-1})(f_{1,s_1}^i, f_{2,s_2}^i, ..., f_{r,s_r}^i)(h_1^k, h_2^k, ..., h_r^k)) \\
&= \psi((\alpha \circ \psi^{-1} \circ (f_{1,s_1}, f_{2,s_2}, ..., f_{r,s_r})^i)(h_1, h_2, ..., h_r)^k) \\
&= \psi((\alpha \circ \psi^{-1} \circ (f_{1,s_1}, f_{2,s_2}, ..., f_{r,s_r})^i)(\psi(d))^k) \\
&= \psi((\alpha \circ \psi^{-1} \circ (f_{1,s_1}, f_{2,s_2}, ..., f_{r,s_r})^i \circ \psi)(d^k)) \\
&= \psi((\alpha \circ (\psi^{-1} \circ (f_{1,s_1}, f_{2,s_2}, ..., f_{r,s_r}) \circ \psi)^i)(d^k)) \\
&= \psi((\alpha \circ (\psi^{-1} \circ (f_{1,s_1}, f_{2,s_2}, ..., f_{r,s_r}) \circ \psi)^i)(\alpha^{-1}(d))) \\
&= \psi((\alpha \circ (\psi^{-1} \circ (f_{1,s_1}, f_{2,s_2}, ..., f_{r,s_r}) \circ \psi)^i \circ \alpha^{-1})(d)) \\
&= \psi((\lambda_\alpha((\psi^{-1} \circ (f_{1,s_1}, f_{2,s_2}, ..., f_{r,s_r}) \circ \psi)^i))(d)) \\
&= \psi((\lambda_\alpha(\sigma_1(c))^i)(d)) \\
&= \psi((\lambda_\alpha(\sigma_1(c^i)))(d)) \\
&= \psi((\lambda_\alpha(\sigma_1(\beta^{-1}(c))))(d))
\end{aligned}$$

□

Proposition 4.4.4. *Suppose that X is a cyclic group of squarefree order $n = p_1 p_2 \cdots p_r$ with generator d, and that Y is a cyclic group of prime order p with generator c, such that $p \neq p_i$ for any i. Define*

$$S = S_1 \times S_2 \times \cdots \times S_r$$

where

$$S_i = \{j \in \mathbb{Z} : 1 \leq j < p_i, i^p \equiv 1 \pmod{p}\}.$$

Let

$$\psi : X \mapsto C_{p_1} \times C_{p_2} \times \cdots C_{p_r}$$

be an isomorphism. For each $x \in C_{p_1} \times C_{p_2} \times \cdots C_{p_r}$, denote by $\mathrm{I}(x)$ the unique r-tuple of integers

$$(i_1, i_2, ..., i_r)$$

such that $0 \leq i_j < p_j$ and $h_j^{i_j} = x_j$ for each j, where x_j is the jth component of x, and h_j is a generator for C_{p_j}, chosen such that

$$d = \psi^{-1}(h_1, h_2, ..., h_r).$$

Define also

$$\phi : \mathrm{Hom}(Y, \mathrm{Aut}(X)) \mapsto S; g \mapsto \mathrm{I}(\psi(g(c)(d))).$$

(i) *The function ϕ is a bijection.*

(ii) *The set S forms an elementary Abelian p-group under the operation*

$$(x_1, x_2, ..., x_r)(y_1, y_2, ..., y_r) = (x_1 y_1 \pmod{p_1}, x_2 y_2 \pmod{p_2}, ..., x_r y_r \pmod{p_r})$$

(iii) *Two homomorphisms σ_1 and σ_2 lie in the same orbit of the ECS Action for X and Y iff there exists i with $1 \leq i < p$ and*

$$\phi(\sigma_2) = (\phi(\sigma_1))^i$$

considering $\phi(\sigma_1)$ as a group element under the operation defined in (ii).

Proof. Suppose that X is a cyclic group of squarefree order $n = p_1 p_2 \cdots p_r$ with generator d, and that Y is a cyclic group of prime order p with generator c, such that $p \neq p_i$ for any i. Define

$$S = S_1 \times S_2 \times \cdots \times S_r$$

where

$$S_i = \{j \in \mathbb{Z} : 1 \leq j < p_i, i^p \equiv 1 \pmod{p}\}.$$

(i) X is cyclic, therefore Abelian, therefore solvable. Also, $p = |Y|$ does not divide the order of X, since otherwise p would have to equal p_i for some i. Let

$$T_1 = \{f \in \mathrm{Aut}(X) : f^p = \mathrm{id}_{\mathrm{Aut}(X)}\}.$$

By Proposition 4.2.1, there is a bijection

$$\phi_1 : \mathrm{Hom}(Y, \mathrm{Aut}(X)) \mapsto T_1; g \mapsto g(c).$$

Now, by Lemma 4.3.5, X is isomorphic to the group

$$H = C_{p_1} \times C_{p_2} \times \cdots \times C_{p_r}.$$

Let

$$\psi : X \mapsto H$$

be such an isomorphism, and let

$$T_2 = \{f \in \mathrm{Aut}(H) : f^p = \mathrm{id}_{\mathrm{Aut}(H)}\}.$$

For each $f \in T_1$, define

$$\phi_2 : T_1 \mapsto T_2; f \mapsto \psi \circ f \circ \psi^{-1}$$

noting that ψ^{-1} exists as ψ is an isomorphism, hence a bijection.

First ϕ_2 is well-defined. Given f in T_1, $\psi \circ f \circ \psi^{-1}$ is certainly an isomorphism as it is a composition of isomorphisms, and it is also an automorphism as clearly $\psi \circ f \circ \psi^{-1} : X \mapsto X$. Now

$$\begin{aligned}(\psi \circ f \circ \psi^{-1})^p &= \psi \circ (f \circ \psi^{-1} \circ \psi)^{p-1} \circ f \circ \psi^{-1} \\ &= \psi \circ f^{p-1} \circ f \circ \psi^{-1} \\ &= \psi \circ f^p \circ \psi^{-1} \\ &= \psi \circ \mathrm{id}_{\mathrm{Aut}(X)} \circ \psi^{-1} \\ &= \psi \circ \psi^{-1} \\ &= \mathrm{id}_{\mathrm{Aut}(H)}\end{aligned}$$

so that $\psi \circ f \circ \psi^{-1} \in T_2$.

We shall show that ϕ_2 is 1-1: take any $f, g \in T_1$ such that $\phi_2(f) = \phi_2(g)$. Let $x \in X$ be arbitrary, then

$$\begin{aligned}\psi(f(x)) &= (\psi \circ f \circ \psi^{-1} \circ \psi)(x) \\ &= (\phi_2(f))(\psi(x)) \\ &= (\phi_2(g))(\psi(x)) \\ &= (\psi \circ g \circ \psi^{-1} \circ \psi)(x) \\ &= \psi(g(x))\end{aligned}$$

so that $f(x) = g(x)$, since ψ is 1-1. Since x was arbitrary, we have $f = g$, and so ϕ_2 is 1-1.

We shall show that ϕ_2 is onto: take any $g \in T_2$. Let $f = \psi^{-1} \circ g\psi$. Now f is a composition of isomorphisms, hence an isomorphism. Clearly $f : X \mapsto X$, so f is an automorphism of X. Next note that

$$\begin{aligned}f^p &= (\psi^{-1} \circ g \circ \psi)^p \\ &= \psi^{-1} \circ (g \circ \psi \circ \psi^{-1})^{p-1} \circ g \circ \psi \\ &= \psi^{-1} \circ g^{p-1} \circ g \circ \psi \\ &= \psi^{-1} \circ g^p \circ \psi \\ &= \psi^{-1} \circ \mathrm{id}_{\mathrm{Aut}(H)} \circ \psi \\ &= \psi^{-1} \circ \psi \\ &= \mathrm{id}_{\mathrm{Aut}(X)}\end{aligned}$$

so $f \in T_1$. We have

$$\phi_2(f) = \psi \circ \psi^{-1} \circ g = g.$$

Thus ϕ_2 is onto, hence a bijection.

By Lemma 4.4.2,

$$\mathrm{Aut}(H) = \mathrm{Aut}(C_{p_1}) \times \mathrm{Aut}(C_{p_2}) \times \cdots \mathrm{Aut}(C_{p_r}).$$

Therefore,

$$\begin{aligned}
&T_2 \\
&= \{(f_1, f_2, ..., f_r) \in \mathrm{Aut}(C_{p_1}) \times \mathrm{Aut}(C_{p_2}) \times \cdots \mathrm{Aut}(C_{p_r}) \\
&\quad : (f_1, f_2, ..., f_r)^p = (\mathrm{id}_{\mathrm{Aut}(C_1)}, \mathrm{id}_{\mathrm{Aut}(C_2)}, ..., \mathrm{id}_{\mathrm{Aut}(C_r)})\} \\
&= \{(f_1, f_2, ..., f_r) \in \mathrm{Aut}(C_{p_1}) \times \mathrm{Aut}(C_{p_2}) \times \cdots \mathrm{Aut}(C_{p_r}) \\
&\quad : (f_1^p, f_2^p, ..., f_r^p) = (\mathrm{id}_{\mathrm{Aut}(C_1)}, \mathrm{id}_{\mathrm{Aut}(C_2)}, ..., \mathrm{id}_{\mathrm{Aut}(C_r)})\} \\
&= U_1 \times U_2 \times \cdots U_r
\end{aligned}$$

where

$$U_i = \{f \in \mathrm{Aut}(C_{p_i}) : f^p = \mathrm{id}_{\mathrm{Aut}(C_i)}\}.$$

If $j \in S_i$, then $j < p$ so $(j, p) = 1$. Let h_i be a generator of C_{p_i} for each i, chosen such that

$$d = \psi^{-1}(h_1, h_2, ..., h_r).$$

By Lemma 4.3.2, the maps

$$\mu_i : U_i \mapsto S_i; f \mapsto \mathrm{I}_i(f(h_i))$$

where I_i denotes the ith component of I, are bijections (note that I_i is just what we usually call the I function, but as a map from the cyclic group of order p_i to S_i). Let

$$\phi_3 : T_2 \mapsto S; (f_1, f_2, ..., f_r) \mapsto (\mu_1(f_1), \mu_2(f_2), ..., \mu_r(f_r)).$$

We show that ϕ_3 is onto. Let $(i_1, i_2, ..., i_r) \in S$. Then as the μ_j are bijections, therefore onto, and so there is always some $f_j \in U_j$ with $\mu_j(f_j) = i_j$. Now

$$\phi_3(f_1, f_2, ..., f_r) = (\mu_1(f_1), \mu_2(f_2), ..., \mu_r(f_r)) = (i_1, i_2, ..., i_r)$$

and so ϕ_3 is onto.

We shall now also show that ϕ_3 is 1-1. So let

$$(f_1, f_2, ..., f_r), (g_1, g_2, ..., g_r) \in T_2$$

and suppose that

$$\phi_3(f_1, f_2, ..., f_r) = \phi_3(g_1, g_2, ..., g_r).$$

Now

$$\phi_3(\mu_1(f_1), \mu_2(f_2), ..., \mu_r(f_r)) = (\mu_1(g_1), \mu_2(g_2), ..., \mu_r(g_r))$$

so that $\mu_j(f_j) = \mu_j(g_j)$ for each j. Now we have $f_j = g_j$ since μ_j is 1-1, and hence

$$(f_1, f_2, ..., f_r) = (g_1, g_2, ..., g_r)$$

so that ϕ_3 is 1-1. Therefore, ϕ_3 is a bijection.

Let $(f_1, f_2, ..., f_r) \in T_2$ be arbitrary. Now

$$\begin{aligned}
\phi_3(f_1, f_2, ..., f_r) &= (\mu_1(f_1), \mu_2(f_2), ..., \mu_r(f_r)) \\
&= (\mathrm{I}_1(f_1(h_1)), \mathrm{I}_2(f_2(h_2)), ..., \mathrm{I}_r(f_r(h_r))) \\
&= \mathrm{I}(f_1(h_1), f_2(h_2), ..., f_r(h_r))
\end{aligned}$$

since the I_i are the components of I. Now, by Lemma 4.4.2,

$$\begin{aligned}(f_1, ..., f_r) &\in \mathrm{Aut}(C_{p_1}) \times \mathrm{Aut}(C_{p_2}) \times \cdots \mathrm{Aut}(C_{p_r})\\ &= \mathrm{Aut}(C_{p_1} \times C_{p_2} \times \cdots \times C_{p_r})\\ &= \mathrm{Aut}(H)\end{aligned}$$

so

$$(f_1, ..., f_r) = f$$

for some $f \in \mathrm{Aut}(H)$, and the f_i are the components of f. This means that

$$f(h_1, h_2, ..., h_r) = (f_1(h_1), f_2(h_2), ..., f_r(h_r))$$

so that

$$\phi_3(f) = \mathrm{I}(f(h))$$

where

$$h = (h_1, h_2, ..., h_r).$$

Now h generates H (for more details, see the proof of Lemma 4.3.5). We have that $d = \psi^{-1}(h)$, thus d has order equal to that of h (since ψ^{-1} is an isomorphism as ψ is), namely $|H|$ (as h generates H), which is equal to $|X|$. Now $d = \psi(h)$, and so

$$\phi_3(f) = \mathrm{I}(f(h)) = \mathrm{I}(f(\psi(d)))$$

Now we may define $\phi = \phi_3 \circ \phi_2 \circ \phi_1$. This is a bijection, as it is a composition of bijections. Clearly $\phi : \mathrm{Hom}(Y, \mathrm{Aut}(X)) \mapsto S$. Also

$$\phi(\sigma) = \mathrm{I}(\psi(\sigma(c)(\psi^{-1}(\psi(d))))) = \mathrm{I}(\psi(\sigma(c)(d)))$$

so that ϕ is indeed the same function given in the statement of the result.

(ii) Each S_i is a group with respect to multiplication modulo p_i, by Lemma 4.3.4. The set S therefore forms a group under the operation

$$(x_1, x_2, ..., x_r)(y_1, y_2, ..., y_r) = (x_1y_1 \pmod{p_1}, x_2y_2 \pmod{p_2}, ..., x_ry_r \pmod{p_r})$$

as it is then the direct product of the S_i.

Each of the groups S_i are cyclic by Lemma 4.3.4, therefore they are all Abelian. Any elements x and y in S have the form $x = (x_1, x_2, ..., x_r)$ and $y = (y_1, y_2, ..., y_r)$. Now within the group S,

$$\begin{aligned}xy &= (x_1, x_2, ..., x_r)(y_1, y_2, ..., y_r)\\ &= (x_1y_1, x_2y_2, ..., x_ry_r)\\ &= (y_1x_1, y_2x_2, ..., y_rx_r)\\ &= (y_1, y_2, ..., y_r)(x_1, x_2, ..., x_r)\\ &= yx\end{aligned}$$

so that S is an Abelian group.

Again by Lemma 4.3.4, the groups S_i all have order 1 or p. Hence for any $x \in S_i$, x the order of x must divide the order of S_i, thus x has order 1 or p. If x has order 1, then it is the identity and $\mathrm{id}_{S_i}^p = \mathrm{id}_{S_i}$. If x has order p then $x^p = \mathrm{id}_{S_i}$ by definition. Now take any $x \in S$. We know $x = (x_1, x_2, ..., x_r)$, and so

$$x^p = (x_1, x_2, ..., x_r)^p = (x_1^p, x_2^p, ..., x_r^p) = (\mathrm{id}_{S_1}, \mathrm{id}_{S_2}, ..., \mathrm{id}_{S_r}) = \mathrm{id}_S$$

and so the order of x must divide p, hence be 1 or p. If x is a non-identity element, its order cannot be 1, so must be p. Therefore, every non-identity element of S has order p.

Suppose S were not a p-group. Then there must be some prime q dividing the order of S, with $q \neq p$. Now by Cayley's Group Theorem, there is an element of S of order q. This element is not the identity as if so it would have order 1 and $q \neq 1$ as it is a prime. However we have just seen that every non-identity element of S has order p. This is a contradiction, so S is a p-group.

Therefore, S is an elementary Abelian p-group.

(iii) Suppose that σ_1 and σ_2 are elements of $\mathrm{Hom}(Y, \mathrm{Aut}(X))$. Define r-tuples $(s_1, s_2, ..., s_r)$ and $(t_1, t_2, ..., t_r)$ such that

$$\sigma_1(c) = \psi \circ (f_{1,s_1}, f_{2,s_2}, ..., f_{r,s_r}) \circ \psi^{-1}$$

and

$$\sigma_2(c) = \psi \circ (f_{1,t_1}, f_{2,t_2}, ..., f_{r,t_r}) \circ \psi^{-1}$$

which we can do by Proposition 4.1.1, Lemma 4.4.2 and Lemma 4.3.5.

Define also for each i, j the function

$$f_{i,j} : C_{p_i} \mapsto C_{p_i}; x \mapsto x^j$$

($\Longrightarrow$) Suppose that σ_1 and σ_2 lie in the same orbit of the ECS Action. Then there exists some $\alpha \in \mathrm{Aut}(X)$ and $\beta \in \mathrm{Aut}(Y)$ such that

$$\sigma_2 = (\alpha, \beta) * \sigma_1$$

or in other words

$$\sigma_2 = \lambda_\alpha \circ \sigma_1 \circ \beta^{-1}.$$

Let i be the unique integer such that $1 \leq i < p$ and $\beta^{-1}(c) = c^i$. Then, by Lemma 4.4.3, we have

$$(h_1^{t_1}, h_2^{t_2}, ..., h_r^{t_r}) = \psi(\sigma_2(c)(d)) = \psi((\lambda_\alpha(\sigma_1(\beta^{-1}(c))))(d)) = (h_1^{s_1^i}, h_2^{s_2^i}, ..., h_r^{s_r^i}).$$

Therefore, for each j, we have $h_j^{t_j} = h_j^{s_j^i}$. Since h_j has order p_j, this implies $t_j \equiv s_j^i \pmod{p_j}$, which gives

$$(t_1, t_2, ..., t_r) = (s_1^i, s_2^i, ..., s_r^i) = (s_1, s_2, ..., s_r)^i$$

regarded as elements of S. However it is clear that $\phi(\sigma_1) = (s_1, s_2, ..., s_r)$ and $\phi(\sigma_2) = (t_1, t_2, ..., t_r)$, so we have

$$\phi(\sigma_2) = (\phi(\sigma_1))^i$$

and $1 \leq i < p$, as required.

($\Longleftarrow$) Suppose there exists an integer i with

$$\phi(\sigma_2) = (\phi(\sigma_1))^i$$

and $1 \leq i < p$. Let α be any automorphism of X, and define

$$\gamma : Y \mapsto Y; y \mapsto y^i$$

and $\beta = \gamma^{-1}$. Now $\beta^{-1}(c) = \gamma(c) = c^i$. By Lemma 4.4.3, we have

$$\psi(\sigma_2(c)(d)) = (h_1^{t_1}, h_2^{t_2}, ..., h_r^{t_r}) = (h_1^{s_1^i}, h_2^{s_2^i}, ..., h_r^{s_r^i}) = \psi((\lambda_\alpha(\sigma_1(\beta^{-1}(c))))(d)).$$

Therefore, as ψ is 1-1,

$$\sigma_2(c)(d) = (\lambda_\alpha(\sigma_1(\beta^{-1}(c))))(d).$$

Let x be any element of X. Then $x = d^k$ for some integer k, and

$$\begin{aligned}
\sigma_2(c)(x) &= \sigma_2(c)(d^k) \\
&= (\sigma_2(c)(d))^k \\
&= ((\lambda_\alpha(\sigma_1(\beta^{-1}(c))))(d))^k \\
&= (\lambda_\alpha(\sigma_1(\beta^{-1}(c))))(d^k) \\
&= (\lambda_\alpha(\sigma_1(\beta^{-1}(c))))(x) \\
&= ((\lambda_\alpha \circ \sigma_1 \circ \beta^{-1})(c))(x)
\end{aligned}$$

and so $\sigma_2(c) = (\lambda_\alpha \circ \sigma_1 \circ \beta^{-1})(c)$. Now let y be any element of Y. Then $y = c^k$ for some integer k, and

$$\begin{aligned}
\sigma_2(y) &= \sigma_2(c^k) \\
&= (\sigma_2(c))^k \\
&= ((\lambda_\alpha \circ \sigma_1 \circ \beta^{-1})(c))^k \\
&= (\lambda_\alpha \circ \sigma_1 \circ \beta^{-1})(c^k) \\
&= (\lambda_\alpha \circ \sigma_1 \circ \beta^{-1})(y)
\end{aligned}$$

and so $\sigma_2 = \lambda_\alpha \circ \sigma_1 \circ \beta^{-1}$. Therefore, $\sigma_2 = (\alpha, \beta) * \sigma_1$, and so σ_1 and σ_2 lie in the same orbit of the ECS Action. □

Finally, we shall give an algorithm to generate a particular set from an elementary Abelian group; this will turn out to be in correspondence with the set of homomorphisms for one of the cases of the main theorem.

ALGORITHM 4.4.5. *Suppose that G is an elementary Abelian p-group. Produce a finite sequence of a_i as follows:*

(1) *Let $i = 0$.*
(2) *Let $a_0 = \mathrm{id}_G$.*
(3) *(LABEL 1)*
(4) *If*

$$\bigcup_{r=0}^{i} \langle a_r \rangle = G$$

then END.
(5) *Let $i = i + 1$.*
(6) *Choose*

$$a_i \in G \ \bigcup_{r=0}^{i} \langle a_r \rangle.$$

(7) *GOTO LABEL 1.*

LEMMA 4.4.6. *Let G be an elementary Abelian p-group of order p^n. The number of elements constructed by Algorithm 4.4.5 is equal to*

$$p^{n-1} + p^{n-2} + ... + p^2 + p + 2.$$

PROOF. Let G be an elementary Abelian p-group of order p^n. Suppose Algorithm 4.4.5 constructs the $m + 1$ elements $a_0, a_1, a_2, ..., a_m$. After each "GOTO LABEL 1" of the algorithm, we have removed $p - 1$ elements from the choices for the next a (these are the $p - 1$ non-identity elements of $\langle a_i \rangle$, which has order p since we are working in an elementary Abelian p-group. None of these have already been removed, as if one had, say b, then b is in $\langle a_j \rangle$ for some $j < i$, so a_i is a power of this a_j, hence in $\langle a_j \rangle$, a contradiction. We do not remove the identity, as this was never a choice, being in $\langle a_0 \rangle$). After all the a_i have been constructed, we have removed a total of $m(p-1)+1$ elements (where the 1 comes from the identity, which we dealt with separately), and this must equal $|G| = p^n$, since the condition to end the algorithm was that there are no elements left to choose from. We have

$$p^n - 1 = m(p - 1)$$

and this gives that

$$m = p^{n-1} + p^{n-2} + ... + p^2 + p + 1.$$

Therefore, the number of elements constructed is

$$m + 1 = p^{n-1} + p^{n-2} + ... + p^2 + p + 2.$$

□

4.5. Classification of groups of order pqr where $q \nmid r-1$

Theorem 4.5.1 (Classification of groups of order pqr where $q \nmid r-1$). *Let p, q, r be primes with $p < q < r$ and $q \nmid r-1$. Let $Y = C_p$ with generator c, $A = C_q$ with generator a and $B = C_r$ with generator b. Further, define maps*

$$f_i : A \mapsto A; x \mapsto x^i$$

and

$$g_i : B \mapsto B; x \mapsto x^i.$$

Also define

$$H = A \times B$$

and let

$$\psi : X \mapsto H$$

be an isomorphism.

(i) *Suppose $p \nmid q-1$ and $p \nmid r-1$. Then any group of order pqr is isomorphic to the cyclic group C_{pqr}.*

(ii) *Suppose $p \nmid q-1$ and $p \mid r-1$. There exists an integer i with $1 < i < r$ and $i^p \equiv 1 \pmod r$. Define a map*

$$\sigma : Y \mapsto \operatorname{Aut}(X); c^s \mapsto \psi^{-1} \circ (\mathrm{id}_{\operatorname{Aut}(A)}, g_{j^s}).$$

Then "C_{pqr}, $C_p \rtimes_\sigma (C_q \times C_r)$" is a list of groups of order pqr up to isomorphism.

(iii) *Suppose $p \mid q-1$ and $p \nmid r-1$. There exists an integer i with $1 < i < q$ and $i^p \equiv 1 \pmod q$. Define a map*

$$\sigma : Y \mapsto \operatorname{Aut}(X); c^s \mapsto \psi^{-1} \circ (f_{i^s}, \mathrm{id}_{\operatorname{Aut}(B)}).$$

Then "C_{pqr}, $C_p \rtimes_\sigma (C_q \times C_r)$" is a list of groups of order pqr up to isomorphism.

(iv) *Suppose $p \mid q-1$ and $p \mid r-1$. Let*

$$S = \{(i,j) : i, j \in \mathbb{Z}, j \in \mathbb{Z}, 1 \le i < q, 1 \le j < r, i^p \equiv 1 \pmod q), j^p \equiv 1 \pmod r).$$

Then we can apply Algorithm 4.4.5 to obtain a sequence of $p+2$ elements

$$(i_0, j_0), (i_1, j_1) ..., (i_{p+1}, j_{p+1}).$$

Define maps

$$\sigma_m : Y \mapsto \operatorname{Aut}(X); c^s \mapsto \psi^{-1} \circ (f_{i_m^s}, g_{j_m^s}).$$

Then "C_{pqr}, $C_p \rtimes_{\sigma_1} (C_q \times C_r)$, $C_p \rtimes_{\sigma_2} (C_q \times C_r)$, ..., $C_p \rtimes_{\sigma_{p+1}} (C_q \times C_r)$" is a list of groups of order pqr up to isomorphism.

Proof. Let p, q, r be primes with $p < q < r$ and $q \nmid r-1$. Let $Y = C_p$ with generator c, $A = C_q$ with generator a and $B = C_r$ with generator b. Further, define maps

$$f_i : A \mapsto A; x \mapsto x^i$$

and

$$g_i : B \mapsto B; x \mapsto x^i.$$

Also define

$$H = A \times B$$

and let

$$\psi : X \mapsto H$$

be an isomorphism. Note that $\mathrm{Aut}(H) = \mathrm{Aut}(A) \times \mathrm{Aut}(B)$, by Lemma 4.4.2.

Let

$$S = \{(i, j) : i, j \in \mathbb{Z}, j \in \mathbb{Z}, 1 \leq i < q, 1 \leq j < r, i^p \equiv 1 \,(\mathrm{mod}\, q), j^p \equiv 1 \,(\mathrm{mod}\, r).$$

It is clear that S contains the element $(1, 1)$, since $1^p = 1 \equiv 1$ under any modulus bigger than 1. Let

$$S_1 = \{i : i \in \mathbb{Z}, 1 \leq i < q, i^p \equiv 1 \,(\mathrm{mod}\, q)\}$$

and

$$S_2 = \{i : i \in \mathbb{Z}, 1 \leq i < r, i^p \equiv 1 \,(\mathrm{mod}\, r)\}$$

so that clearly

$$S = S_1 \times S_2.$$

Let $X = C_{qr}$ with generator d. Let G be a group of order pqr. Then G has a subgroup of index p, by Proposition 1.5.1. For any such subgroup N, we have that

$$|N| = \frac{|G|}{\frac{|G|}{|N|}} = \frac{|G|}{[G : N]} = \frac{pqr}{p} = qr.$$

Therefore N is a group of order qr, and hence is isomorphic to the cyclic group of order qr, by Proposition 4.3.8. Thus $N \cong X$. We have that G/N has order $[G : N] = p$, and so G/N is isomorphic to the cyclic group of order p, i.e. $G/N \cong Y$. This group has order p, and hence $(|X|, |Y|) = (qr, p) = 1$. Furthermore, X and Y are solvable by Proposition 1.5.2. Since G was arbitrary, we have shown that any group of order pqr with a normal cyclic subgroup of order qr, has a normal subgroup N isomorphic to X and G/N isomorphic to Y.

Define

$$\phi : \mathrm{Hom}(Y, \mathrm{Aut}(X)) \mapsto S; g \mapsto \mathrm{I}(\psi(g(c)(d)))$$

which is a bijection by Proposition 4.4.4(i). Let the homomorphism θ be defined by

$$\theta : Y \mapsto \mathrm{Aut}(X); y \mapsto \psi^{-1} \circ (\mathrm{id}_{\mathrm{Aut}(A)}, \mathrm{id}_{\mathrm{Aut}(B)}).$$

Note that this group has underlying set $X \times Y$ and if $x_1, x_2 \in X$, $y_1, y_2 \in Y$ then

$$\begin{aligned}(x_1, y_1)(x_2, y_2) &= (x_1\theta(y_1)(x_2), y_1y_2)\\ &= (x_1\psi^{-1}(id_{\mathrm{Aut}(A)}, \mathrm{id}_{\mathrm{Aut}(B)})(x_2), y_1y_2)\\ &= (x_1\psi^{-1}(\mathrm{id}_{\mathrm{Aut}(H)})(x_2), y_1y_2)\\ &= (x_1\, \mathrm{id}_{\mathrm{Aut}(X)}(x_2), y_1y_2)\\ &= (x_1x_2, y_1y_2)\end{aligned}$$

so $X \rtimes_\theta Y$ is in fact the direct product of X and Y, or $C_{qr} \times C_p$. However, C_{qr} is isomorphic to $C_q \times C_r$ by Lemma 4.3.5, and hence

$$X \rtimes_\theta Y = X \times Y \cong (C_q \times C_r) \times C_p \cong C_q \times C_r \times C_p \cong C_{qrp} = C_{pqr}$$

the last isomorphism being again by Lemma 4.3.5. Note that $\phi(\theta) = (1,1)$ (since $\theta(c)(d) = (\mathrm{id}_A, \mathrm{id}_B)$). We also have that

$$|X \rtimes_\theta Y| = |C_{pqr}| = pqr.$$

(i) Suppose $p \nmid q-1$ and $p \nmid r-1$. By Lemma 4.3.7, there do not exist i, j with $1 < i < q$, $1 < j < r$ and $i^p \equiv 1 \pmod q$, $j^p \equiv 1 \pmod r$. Therefore, S can only contain the element $(1,1)$. Thus $|S| = 1$. By Proposition 4.4.4(i), $|\operatorname{Hom}(Y, \operatorname{Aut}(X))| = |S| = 1$, and so $\operatorname{Hom}(Y, \operatorname{Aut}(X))$ contains only one element, say σ.

Now the group C_{pqr} is of order pqr, hence has a normal subgroup N isomorphic to X with G/N isomorphic to Y. By Theorem 3.3.3(ii), we have that the cyclic group C_{pqr} is isomorphic to $X \rtimes_\sigma Y$.

Take any group G of order pqr. Then G has a normal subgroup N isomorphic to X with G/N isomorphic to Y. By Theorem 3.3.3(ii), we have that G is isomorphic to $X \rtimes_\sigma Y$, and hence to C_{pqr}.

(ii) Suppose $p \nmid q-1$ and $p \mid r-1$. By Lemma 4.3.7, there does not exist i with $1 < i < q$ and $i^p \equiv 1 \pmod q$ but there does exist j with $1 < j < r$ and $j^p \equiv 1 \pmod r$. The set S_1 has only one element, and the set S_2 has more than one element and hence has p elements by Lemma 4.3.4. Therefore $|S| = |S_1||S_2| = p$. Also, S is a group under the operation

$$(1, y_1)(1, y_2) = (1, y_1 y_2 \pmod r)$$

by Proposition 4.4.4(ii).

Let the homomorphism σ be defined by

$$\sigma : Y \mapsto \operatorname{Aut}(X); c^s \mapsto \psi^{-1} \circ (\mathrm{id}_{\operatorname{Aut}(A)}, g_{j^s}).$$

First of all note that $\phi(\sigma) \neq (1,1)$ (since $\sigma(c)(d) = (\mathrm{id}_A, b^j)$). Since $(1,1)^k = (1,1)$ for any k, we have that

$$X \rtimes_\theta Y \ncong X \rtimes_\sigma Y$$

by Proposition 4.4.4(iii).

We have that

$$|X \rtimes_\sigma Y| = |X| \cdot |Y| = (|C_q| \cdot |C_r|) \cdot |C_p| = pqr.$$

Now take any group G of order pqr. Then G has a normal subgroup N isomorphic to X with G/N isomorphic to Y. Therefore, by Theorem 3.3.3(ii), G is isomorphic to $X \rtimes_\rho Y$ for some $\rho \in \operatorname{Hom}(Y, \operatorname{Aut}(X))$. Now if $\rho = \theta$ then $G \cong X \rtimes_\theta Y$. If $\rho \neq \theta$ then $\phi(\rho) = \phi(\sigma)^k$ for some integer k (since $\phi(\sigma)$ is a non-identity element and hence generates the group). Now as $\phi(\rho)$ is not the identity (as otherwise we could deduce $\rho = \theta$), this k is not 0, and so $1 \leq k < p$ (S has order p). By Proposition 4.4.4(iii), ρ and σ lie in the same orbit of the ECS Action, and then by Theorem 3.3.3(iii)

$$G \cong X \rtimes_\rho Y \cong X \rtimes_\sigma Y.$$

Therefore $X \rtimes_\sigma Y$ and $X \rtimes_\theta Y$ are non-isomorphic groups, and every group of order pqr is isomorphic to one of them, so "$X \rtimes_\theta Y$, $X \rtimes_\sigma Y$" is a list of groups of order pqr up to isomorphism. However $X \rtimes_\theta Y \cong C_{pqr}$, so "$C_{pqr}$, $X \rtimes_\sigma Y$" is a list of groups of order pqr up to isomorphism.

(iii) Suppose $p \mid q-1$ and $p \nmid r-1$. By Lemma 4.3.7, there does exist i with $1 < i < q$ and $i^p \equiv 1 \pmod{q}$ but there does not exist j with $1 < j < r$ and $j^p \equiv 1 \pmod{r}$. The set S_1 has more than one element and hence has p elements by Lemma 4.3.4, and the set S_2 has only one element. Therefore $|S| = |S_1||S_2| = p$. Also, S is a group under the operation

$$(x_1, 1)(x_2, 1) = (x_1x_2 \pmod{q}, 1)$$

by Proposition 4.4.4(ii).

Let the homomorphism σ be defined by

$$\sigma : Y \mapsto \mathrm{Aut}(X); c^s \mapsto \psi^{-1} \circ (f_{i^s}, \mathrm{id}_{\mathrm{Aut}(B)}).$$

First of all note that $\phi(\sigma) \neq (1,1)$ (since $\sigma(c)(d) = (a^i, \mathrm{id}_B)$). Since $(1,1)^k = (1,1)$ for any k, we have that

$$X \rtimes_\theta Y \ncong X \rtimes_\sigma Y$$

by Proposition 4.4.4(iii).

We have that

$$|X \rtimes_\sigma Y| = |X| \cdot |Y| = (|C_q| \cdot |C_r|) \cdot |C_p| = pqr.$$

Now take any group G of order pqr. Then G has a normal subgroup N isomorphic to X with G/N isomorphic to Y. Therefore, by Theorem 3.3.3(ii), G is isomorphic to $X \rtimes_\rho Y$ for some $\rho \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$. Now if $\rho = \theta$ then $G \cong X \rtimes_\theta Y$. If $\rho \neq \theta$ then $\phi(\rho) = \phi(\sigma)^k$ for some integer k (since $\phi(\sigma)$ is a non-identity element and hence generates the group). Now as $\phi(\rho)$ is not the identity (as otherwise we could deduce $\rho = \theta$), this k is not 0, and so $1 \leq k < p$ (S has order p). By Proposition 4.4.4(iii), ρ and σ lie in the same orbit of the ECS Action, and then by Theorem 3.3.3(iii)

$$G \cong X \rtimes_\rho Y \cong X \rtimes_\sigma Y.$$

Therefore $X \rtimes_\sigma Y$ and $X \rtimes_\theta Y$ are non-isomorphic groups, and every group of order pqr is isomorphic to one of them, so "$X \rtimes_\theta Y$, $X \rtimes_\sigma Y$" is a list of groups of order pqr up to isomorphism. However $X \rtimes_\theta Y \cong C_{pqr}$, so "$C_{pqr}$, $X \rtimes_\sigma Y$" is a list of groups of order pqr up to isomorphism.

(iv) Suppose $p \mid q-1$ and $p \mid r-1$. By Lemma 4.3.7, there exists i with $1 < i < q$ and $i^p \equiv 1 \pmod{q}$ and j with $1 < j < r$ and $j^p \equiv 1 \pmod{r}$. The set S_1 has more than one element and hence has p elements by Lemma 4.3.4, and the set S_2 has more than one element and hence has p elements by Lemma 4.3.4. Therefore $|S| = |S_1||S_2| = p^2$. Also, S is an elementary Abelian p-group under the operation

$$(x_1, y_1)(x_2, y_2) = (x_1x_2 \pmod{q}, y_1y_2 \pmod{r})$$

by Proposition 4.4.4(ii).

Define a sequence $a_0, a_1, ..., a_{p+1}$ by Algorithm 4.4.5; this sequence is full and complete by Lemma 4.4.6 with $n = 2$. For each integer m with $0 \leq m \leq p+1$, let $a_m = (i_m, j_m)$ and define homomorphisms

$$\sigma_m : Y \mapsto \mathrm{Aut}(X); c^s \mapsto \psi^{-1} \circ (f_{i_m^s}, g_{j_m^s}).$$

We have that

$$|X \rtimes_{\sigma_m} Y| = |X| \cdot |Y| = (|C_q| \cdot |C_r|) \cdot |C_p| = pqr.$$

Note that as $a_0 = \mathrm{id}_S = (1, 1)$, then if $y = c^s$,

$$\begin{aligned}
\sigma_0(y) &= \sigma_0(c^s) \\
&= \psi^{-1} \circ (f_{i_0^s}, g_{j_0^s}) \\
&= \psi^{-1} \circ (f_{1^s}, g_{1^s}) \\
&= \psi^{-1} \circ (f_1, g_1) \\
&= \psi^{-1} \circ (\mathrm{id}_{\mathrm{Aut}(A)}, \mathrm{id}_{\mathrm{Aut}(B)}) \\
&= \theta(y)
\end{aligned}$$

and so $\sigma_0 = \theta$, so $X \rtimes_{\sigma_0} Y \cong C_{pqr}$.

Let $r < s$ and suppose $\phi(\sigma_s) = \phi(\sigma(r))^k$ for some k with $1 \leq k < p$. Then $a_s = a_r^k$. Therefore, $a_s \in \langle a_r \rangle$, but this is impossible in the algorithm. This is a contradiction, so $\phi(\sigma_s) \neq \phi(\sigma(r))^k$ for any k, and so by Proposition 4.4.4(iii),

$$X \rtimes_{\sigma_r} Y \ncong X \rtimes_{\sigma_s} Y.$$

Let G be any group of order pqr. Then G has a normal subgroup N isomorphic to X with G/N isomorphic to Y. So G is isomorphic to $X \rtimes_\rho Y$ for some $\rho \in \mathrm{Hom}(Y, \mathrm{Aut}(X))$, by Theorem 3.3.3(ii). Suppose $\rho = \theta$, then $G \cong C_{pqr}$. If $\rho \neq \theta$ then $\phi(\rho) \neq \phi(theta) = (1, 1) = \mathrm{id}_S$. Let $s = \phi(\rho) \in S$. Then since

$$S = \bigcup_{k=0}^{p+1} \langle a_k \rangle$$

then we must have $s \in \langle a_k \rangle$ for some integer k. Now $s = a_k^t$ for some integer t with $t \neq 0$ (since $s \neq (1, 1)$) and $0 \leq t < p$, or in other words, $\phi(\rho) = \phi(\sigma_k)^t$ for some integer t with $1 \leq t < p$. Thus, by Proposition 4.4.4(iii),

$$X \rtimes_\rho Y \cong X \rtimes_{\sigma_k} Y.$$

Now we have shown that "$X \rtimes_{\sigma_0} Y$, $X \rtimes_{\sigma_1} Y$, $X \rtimes_{\sigma_2} Y$, ..., $X \rtimes_{\sigma_r} Y$", and hence "C_{pqr}, $X \rtimes_{\sigma_1} Y$, $X \rtimes_{\sigma_2} Y$, ..., $X \rtimes_{\sigma_r} Y$", is a list of groups of order pqr up to isomorphism. □

4.6. Examples of the classification

This section serves to apply Theorem 4.5.1, in some special cases.

Remark. We know how to classify groups of order pqr ($q \nmid r - 1$) for a general prime p, from Theorem 4.5.1. Therefore, we can classify groups of order $2qr$, and $3qr$, specifically. In the case of groups of order $2qr$, things are slightly simplified as for any such order, we must have $p \mid q - 1$ and $p \mid r - 1$, since q and r, being primes greater than 2, must be odd.

Example 4.6.1 (Groups of order 105). Let G be a group of order 105. We have $105 = 3 \cdot 5 \cdot 7$ so let $p = 3$, $q = 5$ and $r = 7$. We have that $q \nmid r - 1$, $p \nmid q - 1$ and $p \mid r - 1$. Therefore, applying Theorem 4.5.1(ii), we obtain that there are two groups of order 105 up to isomorphism. One of these is the cyclic group of order 105. To get the other, note that there must be some integer i with $1 < i < 7$ and $i^3 \equiv 1 \pmod 7$. For example, we can take $i = 2$. Now define

$$\sigma : Y \mapsto \mathrm{Aut}(X); y^r \mapsto f_{2^r}$$

where y is a generator of Y and

$$f_j : X \mapsto X; x \mapsto x^j.$$

We may calculate the values of this homomorphism. For example,

$$\sigma(\mathrm{id}_Y) = f_{2^0} = f_1 = \mathrm{id}_{\mathrm{Aut}(X)}$$

and

$$\sigma(y) = f_{2^1} = f_2$$

which is the map which squares every element of X.

We know that any non-cyclic group of order 105 must be isomorphic to $X \rtimes_\sigma Y$, by Theorem 4.5.1.

Example 4.6.2 (Groups of order 273). Let G be a group of order 273.

(1) We have $273 = 3 \cdot 7 \cdot 13$, so let $p = 3$, $q = 7$ and $r = 13$. We have that $q \nmid r - 1$, $p \mid q - 1$ and $q \mid r - 1$.

(2) We may compute the S_1 and S_2 of Proposition 4.4.4. Each will have size p, by Lemma 4.3.7. We have that

$$S_1 = \{1, 2, 4\}$$

and

$$S_2 = \{1, 3, 9\}.$$

Now the S from Theorem 4.5.1, namely

$$S = \{(i, j) : i, j \in \mathbb{Z}, j \in \mathbb{Z}, 1 \le i < q, 1 \le j < r, i^p \equiv 1 \pmod q), j^p \equiv 1 \pmod r)$$

has

$$S = S_1 \times S_2 = \{(1,1), (1,3), (1,9), (2,1), (2,3), (2,9), (4,1), (4,3), (4,9)\}.$$

We may apply Algorithm 4.4.5 to S, which is an elementary Abelian p-group by Proposition 4.4.4. We have $a_0 = (1, 1)$. Choose a_1 not in $\langle a_0 \rangle = \{(1, 1)\}$, so choose $a_1 = (2, 1)$. Choose a_2 not in

$$\begin{aligned} &\langle a_0 \rangle \cup \langle a_1 \rangle \\ &= \{(1,1)\} \cup \{(1,1), (2,1), (4,1)\} \\ &= \{(1,1), (2,1), (4,1)\} \end{aligned}$$

so choose $a_2 = (1, 3)$. Choose a_3 not in

$$\begin{aligned} &\langle a_0 \rangle \cup \langle a_1 \rangle \cup \langle a_2 \rangle \\ &= \{(1,1)\} \cup \{(1,1), (2,1), (4,1)\} \cup \{(1,1), (1,3), (1,9)\} \\ &= \{(1,1), (2,1), (4,1), (1,3), (1,9)\} \end{aligned}$$

so choose $a_3 = (2, 3)$. Choose a_4 not in

$$\begin{aligned}&\langle a_0\rangle \cup \langle a_1\rangle \cup \langle a_2\rangle \cup \langle a_3\rangle\\&= \{(1,1)\} \cup \{(1,1),(2,1),(4,1)\} \cup \{(1,1),(1,3),(1,9)\} \cup \{(1,1),(2,3),(4,9)\}\\&= \{(1,1),(2,1),(4,1),(1,3),(1,9),(2,3),(4,9)\}\end{aligned}$$

so choose $a_4 = (2, 9)$. But now $\langle a_4\rangle = \{(1,1),(2,9),(4,3)\}$ and so

$$\begin{aligned}&\langle a_0\rangle \cup \langle a_1\rangle \cup \langle a_2\rangle \cup \langle a_3\rangle \cup \langle a_4\rangle\\&= \{(1,1),(2,1),(4,1),(1,3),(1,9),(2,3),(4,9),(2,9),(4,3)\}\\&= S\end{aligned}$$

so the algorithm is over.

(3) As predicted, the algorithm has produced $p+2 = 5$ elements, and each corresponds to a group of order 273, by Theorem 4.5.1. There are 5 such, and each has the form $C_p \rtimes_{\sigma_k} (C_q \times C_r)$, where

$$\sigma_k : C_p \mapsto \mathrm{Aut}(C_q) \times \mathrm{Aut}(C_r); c^s \mapsto (f_{i_k^s}, g_{j_k^s})$$

where c is a generator of C_p, we define $(i_k, j_k) = a_k$, and

$$\begin{aligned}f_i &: C_q \mapsto C_q; x \mapsto x^i\\g_i &: C_r \mapsto C_r; x \mapsto x^i.\end{aligned}$$

The group $C_p \rtimes_\sigma (C_q \times C_r)$ corresponds to the cyclic group of order 273.

(4) Any group of order 273 is isomorphic to one of those constructed above, and no two of the above are isomorphic. Thus they form a list of groups of order 273 up to isomorphism, and there are 5 such.

4.7. Conclusion

We have presented a general method which can be applied to classification of groups of any squarefree order. Whereever possible, we have tried to present our results in the case where G has any squarefree order, not necessarily the product of three primes. Theoretically, we could continue to classify groups of order pqr in the case where $q \mid r-1$, by constructing the automorphism group of the non-cyclic group of order qr, and then putting this back into the Extension Classification Schema, along with Proposition 4.2.1 and other tools. We could also try to classify groups of order $pqrs$, as was done in 1939 by D T Sigley ([**2**]). However the theorem we have proved (Theorem 4.5.1) is very general and can be used to classify groups of many orders. For example, there are 9 groups of order $232, 401, 421$.

Index

Bibliography

[1] Burley, A. Application of the transfer homomorphism to prove a famous corollary of the Feit-Thompson theorem for groups of order less than or equal to 200. 2006, Unpublished.

[2] Sigley, D T. An Enumeration of the Groups of Order $pqrs$. American Journal of Mathematics, Vol. 61, No. 1. (Jan., 1939), pp. 102-106.

[3] Goddard, Bart. Re: Number-theoretic question (congruency). sci.math posting, accessible at http://mathforum.org/kb/message.jspa?messageID=5474319 (retrieved 24th Jan 2007).

APPENDIX A

Solvability without the transfer

A.1. The full Feit-Thompson Theorem

In the previous document, [**1**], we saw that any non-Abelian group of odd order less than 200 is not simple. We now can extend this result to prove the full Feit-Thompson theorem for groups of order less than 200; namely, that any group of odd order less than 200 is solvable.

Theorem A.1.1 (The Feit-Thompson Theorem). *Suppose G is a group with odd order less than 200. Then G is solvable.*

Proof. Suppose for a contradiction that there exists a group with odd order less than 200 which is not solvable. Let $n < 200$ be the smallest integer such that there exists a non-solvable group with odd order n. Let G be a group with order n. Then $G \neq \{id_G\}$, since the trivial group is solvable (for such a group G we have $G^{(1)} = G' = 1$). So G has a proper normal subgroup, namely $\{id_G\}$. Let N be a maximal proper normal subgroup of G. Now, G/N has smaller order than G and therefore its order is also less than 200. However, as N is maximal normal in G, we must have that G/N is simple by Lemma 1.1.4. So G/N must be Abelian (as otherwise it could not be simple, by Lemma 0.1.1). Also, N is solvable as it has odd order less than n (its order is odd since it divides the order of the group G, which is odd), and n is the smallest integer such that there exists a non-solvable group with odd order n. So we have found $N \trianglelefteq G$, G/N Abelian, N solvable, and so G is solvable by Lemma 1.4.1. □

A.2. Solvability of groups of order pqr, without the transfer

Since we already know quite a lot about groups of odd order, the proof in this case will be much easier. We are most interested, therefore, in the case of even orders. In this case, suppose we have a group of order pqr. We may assume without loss of generality that $p < q < r$. So if pqr is even then $p = 2$, since 2 must divide the group order. Furthermore, $q, r \neq 2$ as the primes must be distinct. So 2 divides the group order and $2^2 = 4$ does not. Therefore the theorems in this section can be proved in the more general case where the size of G is simply twice an odd number. The disadvantage of not employing the transfer results, is that we are now restricted to groups of order less than 200.

Proposition A.2.1. *Let G be a finite group and suppose $|G| = 2m$ where m is an odd integer. Then G contains a normal subgroup of index 2.*

Proof. Let G be a finite group with $|G| = 2m$ where m is an odd integer. Since 2 divides $|G|$, then G contains an element of order 2 (as 2 is a prime, and by Cauchy's Group Theorem). Let h be an element of order 2 in G. Choose any $x_1 \in G$ and let $x_2 = hx_1$. Now repeat this until the elements of G are exhausted, at each stage picking $x_{2i-1} \in G \ \{x_1, ..., x_{2i-2}\}$ and letting $x_{2i} = hx_{2i-1}$. Since the order of G is even, there will be an exact number of repetitions of this step until the process ends.

Now let $X = G$ with the action of left multiplication. Define

$$\rho : G \mapsto \mathrm{Sym}(X); \rho(g)(x) = gx$$

This is a homomorphism by Lemma 0.2.1. Then

$$\rho(h)(x_{2i-1}) = hx_{2i-1} = x_{2i}$$

and

$$\rho(h)(x_{2i}) = hx_{2i} = h^2 x_{2i-1} = x_{2i-1}$$

as h has order 2. Now, $\rho(h)$ swaps consecutive (when indexed by x_i) elements of G. Or another way of saying this is:

$$\rho(h) = (x_1\ x_2)(x_3\ x_4) \cdots (x_{2m-3}\ x_{2m-2})(x_{2m-1}\ x_{2m})$$

$\rho(h)$ is a product of m transpositions, where m is odd, hence $\rho(h)$ is an odd permutation. Because of this, it has sign -1. Or more technically, let ϵ denote the sign homomorphism, which maps even permutations to $+1$ and odd permutations to -1. Then $\epsilon(\rho(h)) = -1$, so $(\epsilon \circ \rho)(h) = -1$. Also $(\epsilon \circ \rho)(id_G) = 1$, since a homomorphism must map the identity of one group to the identity of the other group (and $\epsilon \circ \rho$ is the composition of two homomorphisms so must be a homomorphism itself). So $\epsilon \circ \rho : G \mapsto \{+1, -1\}$ is onto.

Let $N = \ker(\epsilon \circ \rho)$. Then N is a normal subgroup of G. Also, by the First Isomorphism Theorem,

$$[G : N] = |G/N| = |G/\ker(\epsilon \circ \rho)| = |\operatorname{im}(\epsilon \circ \rho)| = 2$$

as $\epsilon \circ \rho$ is onto with a codomain of size 2. Therefore, G has a normal subgroup of index 2 (namely, N). □

The previous result is much more general than our Proposition 1.5.1. It leads to an alternative proof that all groups of order pqr are solvable.

Corollary A.2.2. *Suppose G is a group of order $pqr < 200$, where p, q, r are distinct primes. Then G is solvable.*

Proof. Suppose G is a group of order $pqr < 200$, where p, q, r are distinct primes. We may assume without loss of generality that $p < q < r$. Now if G has odd order, we are done by Theorem A.1.1. So suppose G has even order. Therefore, we must have $p = 2$, since if q or r was 2, then as 2 divides the group order, p would have to be a prime less than 2, a contradiction. Now q and r are primes which are not 2, so they are both odd. So the group order is $2m$ where $m = qr$ is odd. By Proposition A.2.1, G contains a normal subgroup of index 2, say N. N has order $m < |G| < 200$, which is odd, and so N is solvable by Theorem A.1.1. G/N has order 2 also, and so is Abelian (as it has prime order). So we have $N \trianglelefteq G$, N solvable, G/N Abelian, and so G is solvable by Theorem 1.4.1. □

A.3. Solvability of groups of order p^2q

In this section, we shall prove that all groups of order p^2q are solvable, using earlier results in the document. There is only one case which has not been already proved, and we shall prove this here, after the following initial lemma.

Lemma A.3.1. *Suppose G is a group of order 6. Then G is solvable.*

Proof. Let G be a group of order 6. By Proposition A.2.1, G has a normal subgroup of index 2, say N. Then G/N has prime order 2 and so is Abelian, and N has prime order 3 and so is Abelian, so is solvable. So G is solvable by Lemma 1.4.1. □

Now we may deal with the remaining case.

Proposition A.3.2. *Suppose G is a group of order $4q$ where q is an odd prime. Then G is solvable.*

Proof. Suppose G is a group of order $4q$ where q is an odd prime. Then n_q, the number of Sylow q-subgroups, divides 4, so is 1, 2 or 4. If $n_q = 2$, then as $n_q \equiv 1 \pmod{q}$, we must have $2 \equiv 1 \pmod{q}$, so $1 \equiv 0 \pmod{q}$. However as $q > 1$ (as it is prime), $1 \not\equiv 0 \pmod{q}$. This is a contradiction, so $n_q \neq 2$. If $n_q = 1$ then let Q be a Sylow q-subgroup. Then Q is normal, also $|G/Q| = 4 = 2^2$, so G/Q is Abelian (as its order is the square of a prime). Finally, Q is Abelian as it has order q, a prime, therefore it is solvable (as every commutator is the identity). Hence by Lemma 1.4.1, G is solvable. For the rest of this proof we shall assume the last case, namely that $n_q = 4$. Then, as $4 = n_q \equiv 1 \pmod{q}$, we must have that $q = 3$ (as certainly $q \neq p = 2$, and if $q > 3$ then $q \geq 5$ (as q is prime) but then we do not have $4 \equiv 1 \pmod{q}$). So $|G| = 4q = 12$.

Then n_2, the number of Sylow 2-subgroups, divides 3, so is either 1 or 3. If it's 1, then we get a normal Sylow 2-subgroup P. Also G/P is Abelian as its order is q, a prime. P is solvable as it has order $2^2 = 4$ and therefore is Abelian, therefore solvable. So G is solvable by Lemma 1.4.1.

Now we shall assume that $n_2 = 3$. Let the Sylow 2-subgroups be P_1, P_2 and P_3, and let $X = \{P_1, P_2, P_3\}$. Define an action $*$ by:

$$g * P = gPg^{-1}$$

for all $g \in G$, $P \in X$. Now we get a homomorphism

$$\rho : G \mapsto \mathrm{Sym}(X); \rho(g)(P_r) = g * P_r$$

Since all Sylow 2-subgroups are conjugate, there exists $g \in G$ such that $gP_1g^{-1} = P_2$. So $g * P_1 = P_2$. Therefore, $\rho(g)(P_1) = g * P_1 = P_2$, so $\rho(g)$ is not the identity map. So ρ is not a trivial homomorphism. This means that its kernel is not equal to the whole group, so $|\ker(\rho)| < |G| = 12$. However $|\ker(\rho)|$ must divide the order of the group, so we must have $|ker(\rho)| \leq 6$. Also $|\mathrm{im}(\rho)|$ must divide the order of $\mathrm{Sym}(X)$, which is $3! = 6$, so $|\mathrm{im}(\rho)| \leq 6$. So $|G/\ker(\rho)| = |\mathrm{im}(\rho)| \leq 6$. This means that $|\ker(\rho)| \geq 2$.

Now, $2 \leq |\ker(\rho)| \leq 6$. We will show that $\ker(\rho)$ is solvable. First note that $\ker(\rho)$ has order dividing the order of G, so along with the constraint

$2 \leq |\ker(\rho)| \leq 6$, we have that $|\ker(\rho)|$ is 2, 3 or 6. If $|\ker(\rho)| = 2$ or $|\ker(\rho)| = 3$ then it has prime order and therefore is Abelian, therefore solvable. If $|\ker(\rho)| = 6$, then we can apply Lemma A.3.1 to determine that $\ker(\rho)$ is solvable.

Since $|\ker(\rho)|$ is 2, 3 or 6, we also have $|G/\ker(\rho)|$ is equal to 2, 3 or 6. If $|G/\ker(\rho)| = 2, 3$ then $G/\ker(\rho)$ has prime order and therefore is Abelian. So $\ker(\rho)$ is a solvable normal subgroup with $G/\ker(\rho)$ Abelian, so G is solvable by Lemma 1.4.1, and we are done.

So we turn to the case $|G/\ker(\rho)| = 6$. Then $|\ker(\rho)| = 2$. By Proposition A.2.1, there is a normal subgroup N of $G/\ker(\rho)$ with index 2. By Lemma 1.1.1, $N = H/\ker(\rho)$ for some $H \trianglelefteq G$ (normal as $N \trianglelefteq G/\ker(\rho)$) and $\ker(\rho) \trianglelefteq H$. So $|H| \geq 2$ (as $\ker(\rho) \trianglelefteq H$, $|\ker(\rho)| = 2$). In fact, $|H| \neq 2$, since if $|H| = 2$ then

$$|N| = \frac{|H|}{|\ker(\rho)|} = \frac{2}{2} = 1$$

so $[G/\ker(\rho) : N] = |G/\ker(\rho)| = 6$, but the index should equal 2. This is a contradiction, therefore $|H| \neq 2$, so $|H| > 2$. So $|H| = 3, 6$. If $|H| = 3$ then H has prime order, therefore is Abelian, therefore solvable. If $|H| = 6$ then H is solvable by Lemma A.3.1. Note also that $|G/H| = 2, 4$, and so G/H is Abelian (as it has order either equal to a prime or a prime squared). So G is solvable, by Lemma 1.4.1. □

Now we simply tie all our results together.

PROPOSITION A.3.3. *Suppose G is a group of order $p^2q < 200$, where p and q are distinct primes. Then G is solvable.*

PROOF. Suppose G is a group of order $p^2q < 200$, where p and q are distinct primes. If G has odd order then we are done, by Theorem A.1.1. So suppose G has even order. Then 2 divides the order of G, so either $p = 2$ or $q = 2$, but not both (as they are distinct). If $q = 2$ then p must be odd (as it is a prime not equal to 2), so the group order has the form $2m$ where $m = p^2$ is odd. Then G is solvable by Proposition A.2.1. If $p = 2$ then the order of G is equal to $4q$, where q is odd (as it is a prime not equal to 2). Then G is solvable by Proposition A.3.2. □