Classification of Finite Groups

Daniel Laing

February 13, 2023

Contents

Part I
Doing

1 Introduction

2 Preliminaries

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

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

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

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

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

Definition 2.1. A <u>permutation</u> of a set X is a bijection from X to X. The <u>symmetric group</u> X is the set of all permutations of X under composition. We write $\operatorname{Sym} X$ to denote this. It is easy to show $\operatorname{Sym} X$ is a group.

Definition 2.2. If G is a group, and $H \subseteq G$, then H is a <u>subgroup</u> of G if it is a group in its own right with the multiplication from G. We write $H \leqslant G$ to mean H is a subgroup of G.

If H is closed under <u>conjugation</u>, i.e. for all $g \in G$ and $h \in H$, $g^{-1}hg \in H$, then we say H is a <u>normal subgroup</u> of G. We write $H \trianglelefteq G$ to mean H is a normal subgroup of G.

Definition 2.3. If G is a group and $X \subseteq G$, then the <u>subgroup generated by X</u> is the intersection of all subgroups of G containing X. This in denoted $\langle X \rangle$. The proof that $\langle X \rangle$ is a subgroup of G is omitted. The elements of X are called <u>generators</u> of G.

Definition 2.4. If G is a group with subgroup H then the <u>right coset</u> of H in G with representative $g \in G$ is:

$$Hg = \{ hg \mid h \in H \}$$

Definition 2.5. The <u>order</u> of a group, G, is the number of elements in G, denoted $|G|$. The <u>order</u> of an element $g \in G$ is the smallest $i \in \mathbb{N}$ such that $g^i = 1$.

Definition 2.6. If G and H are groups with elements g_1, $g_2 \in G$, then a map:

$$\phi : G \to H$$

is a <u>homomorphism</u> if:

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

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

Lemma 2.7. *The set of all automorphisms of a group G form a group under composition. Indeed, this is called the <u>automorphism group</u> of G, denoted* $\operatorname{Aut} G$.

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

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

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

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

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

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

Lemma 2.8. *The automorphism group of C_n is isomorphic to the multiplicative group of integers mod n.*

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

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

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

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

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

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

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

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

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

So $\theta : \operatorname{Aut} C_n \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism. $\square$

This collection of theorems is extremely useful for describing group structures. Hopefully these ring some bells. We will use them without proof.

Theorem 2.9 (Lagrange's Theorem for Finite Groups)**.** *Let G be a finite group with subgroup H. Then $|H|$ divides $|G|$. In particular, the order of an element of G must divide $|G|$.*

For the Sylow Theorems, let G be a group of order $p^n m$ where p is a prime and $p \nmid m$.

Theorem 2.10 (1st Sylow Theorem)**.** *G has a Sylow p-subgroup, i.e. a subgroup of order p^n.*

Theorem 2.11 (2nd Sylow Theorem)**.** *All Sylow p-subgroups of G are conjugate to each other. In particular, if G has a unique Sylow p-subgroup, then it is a normal subgroup.*

Theorem 2.12 (3rd Sylow Theorem)**.** *Let n_p denote the number of Sylow p-subgroups of G. Then:*

(i) $n_p \mid m$

(ii) $n_p \equiv 1$ *(mod p)*

Theorem 2.13 (1st Isomorphism Theorem)**.** *For groups G and H, and a homomorphism $\psi : G \to H$:*

$$G/\ker\psi \cong \operatorname{im}\psi$$

Theorem 2.14 (2nd Isomorphism Theorem)**.** *Let G be a group, with subgroup H and normal subgroup N. Then:*

(i) $H \cap N$ is a normal subgroup of G

(ii) HN is a subgroup of G

(iii) $H/(H \cap N) \cong (HN)/N$

Theorem 2.15 (3rd Isomorphism Theorem)**.** *Let G be a group, with normal subgroups H and N, such that $H \leqslant N \leqslant G$. Then:*

(i) (N/H) is a normal subgroup of G/H

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

2.1 Semidirect Product

We already know about the direct product:

Definition 2.16 (Direct Product)**.** For groups N and H, the direct product, $G = N \times H$ is a group of ordered pairs of elements (n, h) where $n \in N$ and $h \in H$ with the operation:

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

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

(i) $\bar{N} \trianglelefteq G$ and $\bar{H} \trianglelefteq G$

(ii) $\bar{N} \cap \bar{H} = \mathbf{1}$

(iii) $\bar{N}\bar{H} = \{\, nh \mid n \in N,\ h \in H \,\} = G$

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

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

Consider the set, (not the direct product):

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

and a map

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

We want ϕ to be an isomorphism.

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

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

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

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

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

For ϕ to be a homomorphism, we need:

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

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

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

We know that ϕ is injective, so then:

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

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

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

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

Definition 2.17 (Semidirect Product)**.**

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

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

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

with multiplication:

$$(n_1,\, h_1)(n_2,\, h_2) = (n_1(n_2\phi_{h_1}),\, h_1 h_2)$$

denoted:

$$N \rtimes_\psi H$$

Lemma 2.18. *For a group G with $N \leqslant G$ and $H \leqslant G$, with $N \cap H = \mathbf{1}$ then:*

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

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

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

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

2.2 Group Actions

Some snazzy introduction.

Definition 2.19. Let G be a group, and Ω be a set, with elements $g \in G$ and $\omega \in \Omega$. Consider a map $\mu : \Omega \times G \to \Omega$, and write ω^g for the image of $(\omega,\, g)$ under μ. So we have:

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

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

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

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

We call μ the group action of G on Ω.

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

Lemma 2.20. *A group action induces a homomorphism. Specifically, let G be a group which acts on a set Ω, with $g \in G$ and $\omega \in \Omega$, and define:*

$$\rho_g : \Omega \to \Omega \quad \textit{by} \quad \omega \mapsto \omega^g$$

Then:

$$\rho : G \to \operatorname{Sym}\Omega \quad \textit{defined by} \quad g \mapsto \rho_g$$

is a homomorphism.

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

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

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

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

Thus ρ is a homomorphism. □

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

Definition 2.21. For a group G with $H \leqslant G$, let $\Omega = \{\, Hg \mid g \in G \,\}$, i.e. the set of cosets of H in G. If $x \in G$, define a group action:

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

Lemma 2.22. *The action above is well defined, meaning the action is independent of our choice of representative g.*

Proof. □

3 First Classifications

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

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

4 Groups of Order pq

Let G be a group of order pq where p, q are prime numbers with $p > q$, and let n_p and n_q denote the number of Sylow p-subgroups and Sylow q-subgroups of G respectively. Then by Theorem 2.12:

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

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

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

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

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

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

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

If $p-1$ is a multiple of q then $n_q = p$ and so Q is not normal in G. By Lagrange's Theorem, $P \cap Q = \mathbf{1}$ and by Lemma 2.18, $|PQ| = pq$. Hence, as well as the direct product, we have $G = P \rtimes Q$, some non-trivial semidirect product.

By Lemma 2.8, $\operatorname{Aut} C_p \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$. So if $\nu \in (\mathbb{Z}/p\mathbb{Z})^\times$, then $x \mapsto x^\nu$ is an automorphism. We know also that C_{p-1} has a unique subgroup of order q, hence G has the presentation:

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

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

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

So any group of order pq is isomorphic to either:

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

4.1 Groups of Order $2p$

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

An element $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order 2 satisfies $\alpha^2 = 1$, hence $\alpha = 1$ or -1. But 1 has order 1, so α can only be -1. Side-note: from the proof of Lemma 2.8, this corresponds to the inverse map $\beta : x \mapsto x^{-1}$.

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

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

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

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

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

5 Groups of Order p^2

Let G be a group of order p^2. First, we will prove a useful lemma:

Lemma 5.1. *If G is a p-group (i.e. a group of prime power order), then every subgroup of index p is normal.*

Proof. Let H be a subgroup of G, with index p. We know kernels are normal subgroups, so we will show that H is the kernel of some homomorphism. Let Ω be the set of all cosets of H. So by definition, $|\Omega| = p$. By Lemma 2.20, there is a homomorphism:

$$\rho : G \to S_p$$

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

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

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

By Lagrange's Theorem, the elements of G have order 1, p or p^2.

If $x \in G$ has order p^2, then x generates G so $G \cong C_{p^2}$.

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

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

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

So no power of y is equal to any power of x. Because y has order p, it generates a subgroup of order p, $\bar{P}$, with $P \cap \bar{P} = \mathbf{1}$. The lemma tells us that both P and $\bar{P}$ are normal, and by Lemma 2.18, $|P\bar{P}| = p^2 = |G|$, so:

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

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

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

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

6 Groups of order 12

We will see later, that we need groups of order 12 as a special case for groups of order p^2q for prime numbers p and q.

Let G be a group of order $12 = 2^2 \cdot 3$, and n_3 and n_2 denote the number of Sylow 3-subgroups and Sylow 2-subgroups of G respectively. By Theorem 2.12:

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

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

So G has a unique Sylow 2-subgroup of order 4, say $H \trianglelefteq G$, and we have already classified groups of order 4, so H is isomorphic to either V_4 (the Klein 4 group) or C_4. A Sylow 3-subgroup, $K \leqslant G$ will have order 3, so $K \cong C_3$. Say $K = \langle x \rangle$.

Lagrange's Theorem tells us H has elements of order 1, 2, and 4, and K has elements of order 1 and 3. Hence $H \cap K = \mathbf{1}$. Lemma 2.18 tells us:

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

Hence $G = HK$, $H \trianglelefteq G$, and $H \cap K = \mathbf{1}$. If we consider groups with 4 Sylow 3-subgroups then we can conclude that they are some semidirect product, $G = H \rtimes K$.

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

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

Let $H = \langle y \rangle$.

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

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

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

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

A trivial homomorphism $K\psi = \mathbf{1}$ yields the direct product. What non-trivial homomorphisms are there? The automorphism group, $\operatorname{Aut} H \cong S_3$ is of order 6, and so has a unique subgroup of order 3, by Theorem 2.12. We know already that a homomorphism $\psi : K \to \operatorname{Aut} H$ is determined by where it sends the generator x, so for ψ to be non-trivial, it must send x to an element of order 3 in $\operatorname{Aut} H$.

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

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

It appears we have 2 choices, but this is not the case. If we define $\theta : K \to K$ by $x\theta = x^{-1}$ then $\theta\psi_1 = \psi_2$. And notice that θ is an automorphism of K, so the semidirect products with ψ_1 and ψ_2 are isomorphic. Hence (up to isomorphism) there is one non-trivial homomorphism $\psi : K \to \operatorname{Aut} H$. So $x \in K$ acts by permuting the 3 non-identity elements of H.

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

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

We can also find a subgroup isomorphic to V_4:

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

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

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

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

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

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

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

Let $H = \langle y \rangle$.

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

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

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

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

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

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

If $\psi : H \to \operatorname{Aut} K$ is trivial then we obtain the direct product again.

The image of a non-trivial homomorphism $\psi : H \to \operatorname{Aut} K$ is isomorphic to C_2, so by Theorem 2.13: $\ker \psi \cong C_2$.

We can choose ψ such that $y\psi = \beta : x \mapsto x^{-1}$ and $z\psi = \iota : x \mapsto x$. Then:

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

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

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

and

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

Hence:

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

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

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

7 Groups of Order p^2q

Let p and q be distinct prime numbers, and G be a group of order p^2q. We shall consider the cases $p < q$ and $p > q$ separately.

7.1 $p < q$

Let $p < q$, and let n_q denote the number of Sylow q-subgroups. Then by Theorem 2.12:

$$n_q \mid p^2$$

so n_q could be 1, p or p^2. Also:

$$n_q \equiv 1 \bmod q$$

If $n_q = p$ then p must be congruent to 1 mod q, which is a contradiction since $p < q$. If $n_q = p^2$ then we must have:

$$q \mid (p^2 - 1)$$

Factorising gives:
$$q \mid (p+1)(p-1)$$
So either:
$$q \mid (p+1) \quad \text{or} \quad q \mid (p-1) \quad \text{or both}$$
However, q cannot divide $p-1$ because $p < q$ so q must divide $p+1$. This is only the case when $p = 2$ and $q = 3$, so $|G| = 12$ which we have already classified.

Hence if $|G| = p^2 q \neq 12$ with $p < q$, then G possesses a unique Sylow q-subgroup, $Q \cong C_q$, which is normal in G. A Sylow p-subgroup, $P \leqslant G$, will have order p^2 and by Lagrange's Theorem, intersects trivially with Q. And by applying Lemma 2.18:
$$|PQ| = |P| \cdot |Q| = p^2 q$$
So we can conclude that $G = Q \rtimes P$.

We know, by Lemma 2.8, that $\operatorname{Aut} Q \cong (\mathbb{Z}/q\mathbb{Z})^\times$, and we want a homomorphism, $\psi : P \to \operatorname{Aut} Q$. We have two possibilities for a group of order p^2:

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

Element order is preserved by ψ so let's consider what possibilities we have. Elements in P have order 1, p and p^2. Lagrange's Theorem tell us that $\operatorname{Aut} Q$ will have elements of order p if $p \mid q-1$, and p^2 if $p^2 \mid q-1$. Notice that if $p \mid q-1$ then so will p^2.

Expecting 2 non-trivial semidirect products, one with trivial centre requiring $p^2 \mid q-1$, and one with centre of order p requiring $p \mid q-1$.

Case 2: $P \cong C_p \times C_p$ i.e. $G \cong C_q \rtimes (C_p \times C_p)$.

This time, P only has elements of order 1 and p. If $p \nmid q-1$ then the only possibility is the trivial homomorphism and we recover the direct product again. So we can assume that $p \mid q-1$.

Expecting only one semidirect product.

7.2 $p > q$

Let $p > q$, and let n_p denote the number of Sylow p-subgroups. Then by Theorem 2.12:
$$n_p \mid q$$
so n_p could be 1 or q. Also:
$$n_p \equiv 1 \bmod p$$
and because $p > q$, this forces $n_p = 1$. Hence G has a unique Sylow p-subgroup, P, of order p^2, and $P \trianglelefteq G$. A Sylow q-subgroup of G, Q, will have order q, and so will be isomorphic to C_q. So by Lagrange's Theorem, $P \cap Q = \mathbf{1}$. Lemma 2.18 gives us that:
$$|PQ| = p^2 q$$
Hence, $G = P \rtimes Q$.

For this report, we will narrow our focus to groups of order less than 31, i.e. $p \leqslant 3$ and $q \leqslant 7$.

8 Groups of Order 24

Let G be a group of order 24, and let H be a Sylow 3-subgroup of G, so $H \cong C_3$. Let T by a Sylow 2-subgroup of G, so T has order 8. By Lagrange's Theorem, $H \cap T = \mathbf{1}$ and then applying Lemma 2.18, $|HT| = 24$. Now let n_3 denote the number of Sylow 3-subgroups, and by Theorem 2.12:

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

Hence n_3 is either 1 or 4.

If $n_3 = 1$, then H is normal in G. Thus $G = H \rtimes T$. We'll want a homomorphism $\psi : \operatorname{Aut} T \to H$ From our classification of groups of order 8, we have 5 possibilities:

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

1 group

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

2 groups

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

1 group

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

2 groups

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

1 group — binary dihedral

If $n_3 = 4$ then H is not normal. Now let G act by conjugation on the set of its Sylow 3-subgroups, $\Omega = \{\, H \mid H \text{ is a Sylow 3-subgroup of } G \,\}$:

$$H^x = x^{-1}Hx = \{\, x^{-1}hx \mid h \in H \,\} \quad \text{for } x \in G$$

This is indeed a group action because for x, $y \in G$:

$$(H^x)^y = (x^{-1}Hx)^y = (y^{-1}x^{-1})H(xy) = (xy)^{-1}H(xy) = H^{(xy)}$$

and:

$$H^1 = 1^{-1}H1 = H$$

Hence we obtain a homomorphism $\rho : G \to S_4$. The kernel of ρ must have order dividing $\frac{|G|}{|\Omega|} = 6$ so can be either 1, 2, 3 or 6. CHECK!

The kernel cannot be of order 3, because G has no normal subgroup of order 3 (because kernels of homomorphism are normal in the domain group). Likewise the kernel cannot be of order 6 because every group of order 6 has a normal subgroup of order 3, which would be normal in G as well. Hence the kernel must have order 1 or 2.

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

If the kernel is of order 2, then the image must be a subgroup of order 12, with no normal subgroup of order 3. Looking at our classification of groups of order 12, this must be isomorphic to A_4. We know that A_4 has a normal subgroup of order 4, and so by the Correspondence Theorem, G must contain a normal subgroup of order 8, say T. By Lagrange's Theorem and Lemma 2.18, we can conclude that $G = T \rtimes H$. Again, we have 5 cases, but this time we'll exclude the trivial homomorphism, because that will just give us the direct product which we have already seen:

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

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

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

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

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

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

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

Theorem 2.11 tells us that all subgroups of order 3 are conjugate, so there is only one unique action (up to isomorphism) of H on T.

1 group — $A_4 \times C_2$

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

If we say $\langle\, s,\, r \mid s^2 = r^4 = 1,\ s^{-1}rs = r^{-1} \,\rangle = T$, then consider two automorphisms, $\varphi_s,\, \varphi_r \in \operatorname{Aut} T$, given by:

$$x\varphi_s = xs \quad \text{and} \quad x\varphi_r = xr \quad \text{for } x \in T$$

We see that φ_s has order 2, and φ_r has order 4. Additionally:

$${\varphi_s}^{-1} = \varphi_{s^{-1}} \quad \text{and} \quad {\varphi_r}^{-1} = \varphi_{r^{-1}}$$

Now consider:

$$x{\varphi_s}^{-1}\varphi_r\varphi_s = xs^{-1}rs = xr^{-1} = x{\varphi_r}^{-1}$$

Hence:

$$\operatorname{Aut} T = \langle\, \varphi_s,\, \varphi_r \mid {\varphi_s}^2 = {\varphi_r}^4 = \iota,\ {\varphi_s}^{-1}\varphi_r\varphi_s = {\varphi_r}^{-1} \,\rangle \cong D_8$$

Lagrange's Theorem tells us that there are no non-trivial homomorphisms $\psi : H \to \operatorname{Aut} T$.

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

1 group — binary tetrahedral

9 Groups of Order 30

Let G be a group of order $30 = 2 \cdot 3 \cdot 5$, and let n_3 and n_5 denote the number of Sylow 3-subgroups and Sylow 5-subgroups of G respectively. Then by Theorem 2.12:

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

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

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

So if T is a Sylow 3-subgroup of G and F is a Sylow 5-subgroup, then at least one must be normal in G. So $T \trianglelefteq G$ or $F \trianglelefteq G$ or both.

Let $H = TF$ and by Lagrange's Theorem, $T \cap F = \mathbf{1}$, hence $|H| = 15$ by Lemma 2.18. We know from our classification of groups of order pq that $H \cong C_{15}$. Notice that a Sylow 2-subgroup $K \leqslant G$ has order 2, so $K \cong C_2$. Let $\langle t \rangle = K$ and $\langle v \rangle = H$. By the same argument as above, $H \cap K = \mathbf{1}$ and $|HK| = 30$. Hence $G = HK$.

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

By Lemma 2.8:

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

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

$$z\psi = (1,\, 1),\ (x,\, 1),\ (1,\, y^2) \quad \text{or} \quad (x,\, x^2)$$

So we know there are 4 groups of order 30 up to isomorphism, but which 4?

If $z\psi = (1,\, 1)$ then the action of K on H is trivial, so we obtain the direct product:

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

All other possibilities for $z\psi$ have order 2, and we have seen before that the only possible action of order 2 is inversion.

Notice that $(x,\, y^2)$ has both non-trivial elements of order 2, thus K acts on all of H:

$$G \cong \langle\, v, t \mid v^{15} = t^2 = 1,\ t^{-1}vt = v^{-1} \,\rangle$$

which we recognise as D_{15}.

For the final two cases, it is helpful to consider H as a direct product. Without loss of generality, take $H \cong C_5 \times C_3$.

If $z\psi = (1,\, y^2)$, then it acts trivially on C_5, and with inversion on C_3. So we can write:

$$G \cong C_5 \times (C_3 \rtimes C_2)$$

We have seen already that this semidirect product $C_3 \rtimes C_2$, is isomorphic to D_6, so we can conclude:

$$G \cong C_5 \times D_6$$

If $z\psi = (x,\, 1)$, then it acts with inversion on C_5, and trivially on C_3. Hence:

$$G \cong C_3 \times (C_5 \rtimes C_2)$$

Once again, this semidirect product is isomorphic to D_{10}, so we have:

$$G \cong C_3 \times D_{10}$$

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

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

Part II

To Do

10 Groups of Order p^3

10.1 Groups of Order 8

10.2 Groups of Order 27

10.3 General Case?

11 Groups of Order 16