Group Theory Notes

Brayden Letwin

Last Updated: September 21, 2025

Contents

1 Group Theory **2**
1.1 Definitions 2
1.2 Subgroups and Homomorphisms 4
1.3 Kernels, Images, and Cosets 5
1.4 Normal Subgroups and Quotient Groups 7
1.5 Structure and Isomorphism Theorems 8
1.6 Exact Sequences 12
1.7 Group Actions 13
1.8 Sylow Theorems 18
1.9 Solvable Groups 19

Chapter 1

Group Theory

1.1 Definitions

Definition 1. A group is a set G, equipped with a binary operation $G \times G \longrightarrow G$ such that

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$.
2. there exists $1 \in G$ text s.t. $1 \cdot g = g \cdot 1 = g$ for all $g \in G$.
3. for all $g \in G$ there exists $g^{-1} \in G$ s.t. $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

We will denote the binary operation of an additive group by $+$, 0 the identity and $-g$ the inverse of g. Otherwise, we will denote the binary operation using $\cdot$.

Lemma 1. *The identity of a group is unique.*

Proof. Let $1, 1'$ be two identity elements, then

$$1 = 1 \cdot 1' = 1'.$$

□

Lemma 2. *The inverse element is unique.*

Proof. Let $g \in G$ and $h_1, h_2 \in G$ be two inverses of g. Then

$$h_1 = h_1 \cdot 1 = h_1 \cdot (g \cdot h_2) = h_2.$$

□

Exercise 1. *Suppose every $g \in G$ has a left-inverse. Then every $g \in G$ has a right inverse.*

Proof. Let $g \in G$. Then

$$g^{-1} = g^{-1} \cdot g \cdot g^{-1}.$$

Let c be the left inverse to g^{-1}. Then we can write $1 = c \cdot g^{-1} = c \cdot g^{-1} \cdot g \cdot g^{-1} = g \cdot g^{-1}$. This implies that g has a right inverse. □

Definition 2. For $n \in \mathbb{Z}$ and $g \in G$ we define $g^n = g \cdot \ldots \cdot g$ (n-times multiplication) if $n \geq 1$. If $n \leq -1$ we define $g^n = (g^{-1})^{-n}$. If $n = 0$ we define $g^0 = 1$. The case for additive notation is similar.

Generally we will omit the multiplication symbol where not needed.

Definition 3. G is abelian if $gh = hg$ for all $g, h \in G$.

Here are some important examples of groups:

Example 1. Let S be a set. The symmetric group $G = \mathrm{Per}(S)$ is the set of all permutations of S to itself equipped with composition. A permutation is a bijection $\varphi : S \longrightarrow S$.

In the special case that $|S| = n$ we have S_n which is characterized by cycles. A nice formula to decompose a cycle is given by

$$(a_1 \ \ldots \ a_r) = (a_1 \, a_2)(a_2 \, a_3) \ldots (a_{r-1} \, a_r).$$

Later in the notes we will prove Cayley's theorem, which states that every group is isomorphic to a subgroup of $\mathrm{Per}(G)$. Here $\mathrm{Per}(G)$ carries absolutely no group structure from G, and so this is important because this means that all examples/counter-examples that are formulated can be formulated in terms of $\mathrm{Per}(S)$ for some set S. There are other important examples of groups (below), which are interesting in their own right.

Example 2. Let V be a vector space over a field F. The general linear group $GL(V)$ is the group of linear automorphisms $\varphi : V \longrightarrow V$. In particular with $V = F^n$ we write $GL(V)$ by $GL(n, F)$. For a general group G we define by $\mathrm{Aut}(G)$ is the group of all automorphisms from G to itself.

Example 3. For any field F we have the additive group F^+ and the multiplicative group $F^\times = F \setminus \{0\}$

Definition 4. Let G_1, G_2 be two groups. The direct product of G_1 and G_2 is defined as $G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$ with component-wise multiplication. The direct product $G_1 \times G_2$ is a group. More generally given an index set I and G_i a group for all $i \in I$ we define

$$\prod_{i \in I} G_i = \{(g_i)_{i \in I}, g_i \in G_i\},$$

called the direct product of each G_i, which is a group with component-wise multiplication.

1.2 Subgroups and Homomorphisms

Definition 5. Let G be a group. A subgroup $H \subset G$ is a subset such that

1. $gh \in H$ for all $g, h \in H$.
2. $g^{-1} \in H$ for all $g \in H$.
3. $1 \in H$.

Clearly a subgroup H forms a group. A simple way to verify whether a subset $H \subset G$ forms a subgroup is to check if H is not empty and $ab^{-1} \in H$ for all $a, b \in H$. Every group G has two subgroups $\{1\}$ and G, the so called trivial subgroups. Any other subgroup of G is called proper. If H_1, H_2 are subgroups of G, then so is $H_1 \cap H_2$.

Definition 6. Let $S \subset G$ be a set. The smallest subgroup containing S is denoted by $\langle S \rangle$. We define the smallest subgroup $\langle S \rangle$ to be the subgroup such that for any subgroup $S \subset H$, we have $\langle S \rangle \subset H$.

Lemma 3. $\langle S \rangle = \{s_1 \cdot s_2 \cdot \ldots \cdot s_n : s_i \in S \text{ or } s_i^{-1} \in S\}$.

The following one can prove by induction:

Lemma 4. *For all $g_1, \ldots, g_n \in G$ we have $(g_1 \cdot \ldots \cdot g_n)^{-1} = g_n^{-1} \cdot \ldots \cdot g_1^{-1}$.*

Definition 7. A cyclic group G is a group such that $G = \langle g \rangle$ for some $g \in G$.

We now begin the discussion of group homomorphisms, along with some properties:

Definition 8. A group homomorphism $\varphi : G \longrightarrow G'$ is a map such that $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in G$.

Lemma 5. *If $\varphi : G \longrightarrow G'$ is a group homomorphism then $\varphi(1) = 1$.*

Lemma 6. *If $\varphi : G \longrightarrow G'$ is a group homomorphism then $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.*

Definition 9. A group homomorphism $\varphi : G \longrightarrow G'$ that is bijective is called a group isomorphism. G and G' are said to be isomorphic. We write $G \cong G'$.

Definition 10. Group endomorphisms are group homomorphisms $\varphi : G \longrightarrow G$. Group automorphisms are group isomorphisms $\varphi : G \longrightarrow G$. The set of all automorphisms of a group G forms a group under composition. Group epimorphisms are surjective group homomorphisms $\varphi : G \longrightarrow G'$. Group monomorphisms are injective group homomorphisms $\varphi : G \longrightarrow G'$.

Here are some examples below of group homomorphisms:

Example 4. $\mathbb{Z}$ has exactly one homomorphism to any group G, which is determined by where $1 \in \mathbb{Z}$ maps to.

Proof. Let $\varphi : \mathbb{Z} \longrightarrow G$ be a homomorphism. Suppose $\varphi(1) = a \in G$. Then $\varphi(n) = \varphi(1)^n = a^n$ for any $n \in \mathbb{Z}$. □

More generally this shows that group homomorphisms preserves cylic properties of groups.

Example 5. Fix $n \in \mathbb{Z}$ and consider the map $\varphi : G \longrightarrow G$ defined by $\varphi(g) = g^n$. Then φ is a group homomorphism if G is abelian.

Proof. Suppose G is abelian. Then $(ab)^n = a^n b^n$ (by induction). □

One more example of a group homomorphism:

Example 6. Let I be an index set and $\varnothing \neq J \subset I$. Then the canonical map

$$\Pi_{j \in I} G_j \longrightarrow \Pi_{j \in J} G_j,$$

defined by $(g_j)_{j \in I} \longrightarrow (g_j)_{j \in J}$ is a group homomorphism.

Note that if $S \subset G$ then if we are given any map $f : S \subset G$, we can extend this map to at most one group homomorphism $f' : \langle S \rangle \longrightarrow G$. Such a homomorphism may not exist. This is the so called universal property of group homomorphisms. Note also that the composition of two homomorphisms is again a homomorphism.

1.3 Kernels, Images, and Cosets

We begin by defining some very important subgroups.

Definition 11. Let $\varphi : G \longrightarrow G'$ be a group homomorphism. Then the kernel of φ is $\ker \varphi = \{g \in G : \varphi(g) = 0\}$. The kernel is a subgroup of G.

Definition 12. Let $\varphi : G \longrightarrow G'$ be a group homomorphism. Then the image of φ is $\mathrm{im}\varphi = \{\varphi(g) : g \in G\}$. The image is a subgroup of G'.

Note that φ is a monomorphism iff $\ker \varphi = \{1\}$ and φ is an epimorphism iff $\mathrm{im}\, \varphi = G'$.

Now we will move onto cosets. Let $H \subset G$ be a subgroup. For fixed $g \in G$ the set $gH = \{gh : h \in H\}$ is called the left coset of H in G. A representative of gH is any element $b = gh \in gH$. In this case we have $gH = bH$ since H is a subgroup. We formuate this in the next Lemma:

Lemma 7. *Let $H \subset G$ be a subgroup. Then two cosets of H in G are either equal or disjoint.*

Proof. Take two cosets gH and $g'H$ and suppose $gH \cap g'H \neq \varnothing$. Let $x \in gH \cap g'H$. Then $x = gh = g'n$ for $h, n \in H$. Hence, $g = g'nh^{-1} \in g'H$. Thus, $gH = g'(nh^{-1})H \subset g'H$, since H is a subgroup. Conversely, we have $g' = ghn^{-1} \in gH$, so $g'H = g(hn^{-1})H \subset gH$. □

We denote by $G/H = \{gH : g \in G\}$ the set of all cosets of H in G. Using this, we can then define the rule $\sim$ on G by $g \sim h$ iff $gh^{-1} \in H$ (where we fix a subgroup H beforehand). This rule becomes an equivalence relation on G.

Lemma 8. *Given a subgroup H and two elements $g, n \in G$ we have $gH = nH$ iff $n^{-1}g \in H$.*

Proof. Let $g, n \in G$ and suppose $gH = nH$. This means that there is $h \in H$ such that $g = nh$ and so $n^{-1}g \in H$. Conversely if $n^{-1}g = h \in H$ then $g = nh \in nH$. Then $gH = nhH \subset nH$. With the same ideas we can write $nH = gh^{-1}H \subset gH$. □

Now we have another neat useful Lemma:

Lemma 9. *Let $g \in G$ and $H \subset G$ be a subgroup. Then $g^{-1} \in gH$ iff $g^2 \in gH$.*

Proof. Suppose $g^{-1} \in gH$. Then $g^{-1} = gh$ for some $h \in H$ and so $h = g^{-2}$, hence $g^2 \in H$ because H is a subgroup. On the other hand, suppose that $g^2 \in gH$. Then $g^2 = gh$ for some $h \in H$ implying that $h = g$. Thus, $g^{-1} \in H$ as H is a subgroup. □

Definition 13. The index of H in G, $[G : H]$ is the size of $G/H = \{gH : g \in G\}$. We define the order of G to be the index of $\{1\}$ in G.

Lemma 10. *For any chain $K \subset H \subset G$ of subgroups one has*

$$[G : K] = [G : H][H : K].$$

Proof. Let $\{h_i\}_{i=1}^n$ be a system of representatives for G/H, (recall that $G = \bigcup_{i=1}^n h_i H$, infact this union is disjoint). Let $\{k_i\}_{i=1}^m$ be a system of representatives of H/K ($G = \bigcup_{i=1}^m k_i K$). Then

$$G = \bigcup_{i,j} h_i k_j K$$

is a disjoint union of nm cosets. Thus $[G : K] = [G : H][H : K]$. □

Now we discuss Lagrange's theorem.

Theorem 11. *Let G be a group and $H \subset G$ be a subgroup. Then $|H|$ divides $|G|$ and $|H|\,[G : H] = |G|$.*

Proof. Take $K = \{1\}$ in Lemma 10. □

Recall, that if $|G| = p$ for some prime p, then G is cyclic. In fact, G is generated by any $1 \neq g \in G$. Let $1 \neq g \in G$. Then $|\langle g \rangle|$ divides $|G|$ so this implies either $\langle g \rangle = \{1\}$ or $|g| = G$, but the former is not possible since $g \in \langle g \rangle$.

1.4 Normal Subgroups and Quotient Groups

First, consider a group homomorphism $\varphi : G \longrightarrow G'$, it follows that if $H = \ker\varphi$ then $xHx^{-1} \subset H$ for all $x \in G$. Since this also holds for x^{-1} we obtain $x^{-1}Hx \subset H$ and thus $H \subset xHx^{-1}$, so we conclude that $xHx^{-1} = H$. This prompts the definition of a normal subgroup:

Definition 14. A subgroup H of G is called normal if $xHx^{-1} = H$ for all $x \in G$.

Definition 15. Let A be a non-empty set. The normalizer of A in G is defined as

$$N_G(A) = \{g \in G : gAg^{-1} \subset A\},$$

and is a subgroup of G.

Definition 16. Let A be a non-empty set. The centralizer of A in G is defined as

$$C_G(A) = \{g \in G : ga = ag \text{ for all } a \in A\},$$

and is a subgroup of G.

We define the center of G to be $Z(G) = C_G(G)$. If H is a subgroup of G then H is normal in $N_G(H)$. In fact, $N_G(H)$ is the largest such subgroup of G for which H is normal. This is immediate from the definition of $N_G(H)$.

Note that the centralizer of a subgroup H in a group G is not necessarily abelian. Indeed, take $G = S_3$, then G is not abelian and $C_{S_3}(\{1\}) = S_3$. On the other hand, note that $Z(G)$ is always abelian. Indeed, if $g_1, g_2 \in Z(G)$ then $g_1g_2 = g_2g_1$, simply by the definition of $Z(G)$. Indeed also, $Z(G)$ is normal in G since if $g \in G$ and $z \in Z(G)$ then $gzg^{-1} = zgg^{-1} = z \in Z(G)$. In general, not every abelian subgroup is normal in a group G. It is also important to note that $Z(G) = \bigcap_{g\in G} N_G(\{g\})$

Lemma 12. *The following are equivalent for a subgroup $H \subset G$.* 1. *The operation $(gH, g'H) \longrightarrow gg'H$ is well defined.* 2. *For all $g \in G$ one has $gHg^{-1} \subset H$.* 3. *For all $g \in G$ one has $gHg^{-1} = H$.* 4. *For all $g \in G$ one has $gH = Hg$.* 5. *$N_G(H) = G$. All of these are equivalent definitions of a normal subgroup.*

We will leave this Lemma as an exercise because it really is not too difficult to figure out if you have been following along until now.

Now, given a normal subgroup $H \subset G$ of a group G. We can endow a group structure on G/H by the multiplication $(g_1H, g_2H) \longrightarrow g_1g_2H$. Under this operation we have the following very important lemma. For one, it suffices to note that if one has a group homomorphism $\varphi : G \longrightarrow G'$ then any subgroup K of $H = \ker\varphi$ is normal in G (as explained above, but one can deal with subgroups of $\ker\varphi$ rather easily). On the other hand one has the following lemma:

Lemma 13. *Let H be a normal subgroup of G. Then H is the kernel of a group homomorphism.*

Proof. Define the map $\varphi : G \longrightarrow G/H$ by $g \longrightarrow gH$. Then $\ker \varphi = \{g \in G : gH = H\} = \{g \in G : g \in H\} = H \cap G = H$. □

Hence, there is a one to one correspondence between normal subgroups and kernels of group homomorphisms. It is important to note also that the intersection of normal subgroups is also normal.

1.5 Structure and Isomorphism Theorems

The structure (isomorphism) theorems are theorems chosen so that the structure of a group is understood more.

Lemma 14. *Let G be a group and H be a subset of G. Then H is a subgroup iff $H^2 = H, H^{-1} = H$ and $H \neq \varnothing$.*

This above Lemma is immediate and not hard to show.

Lemma 15. *Let G be a group and H, K be two subgroups of G. Then HK is a subgroup of G iff $HK = KH$.*

Proof. Suppose that HK is a subgroup. Indeed then $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. On the other hand if $HK = KH$ then $HKHK = HHKK = HK$, and also $(HK)^{-1} = (KH)^{-1} = H^{-1}K^{-1} = HK$. Indeed also HK is non-empty, so we are done. □

Lemma 16. *Let G be a group and $H, K \subset G$ be subgroups. Suppose that $H \cap K = \{1\}$ and $KH = HK = G$. Then the map $H \times K \longrightarrow G$ defined by $(h, k) \longrightarrow hk$ is an isomorphism.*

Proof. Verifying that the map is a homomorphism is easy, since $HK = KH$. Then $HK = G$ means that the map is surjective. If the map is f, then if $(h, k) \in \ker f$ then $f((h, k)) = hk = 1$, so $h = k^{-1}$, the left element is in H and the right element is in K so we conclude $h \in H \cap K$. Same with $k \in H \cap K$. Then $hk \in H \cap K$ because $H \cap K$ is a subgroup. Thus $(h, k) = \{(1, 1)\} \subset H \times K$. □

Lemma 17. *Suppose that H, K are subgroups of a group G. If H is a subgroup of $N_G(K)$ (that is, for all $h \in H$, $hKh^{-1} \subset K$, i.e. we say that H normalizes K), then HK is a subgroup of G. In particular, if K is a normal subgroup of G then HK is a subgroup for any H.*

Proof. We want to show that $HK = KH$. We have $HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH$, where we used that H normalizes K. □

Lemma 18. *Suppose H and K are subgroups of a group G and that HK is a subgroup. Then $HK = \langle H, K \rangle$.*

Proof. We have that $\langle H, K \rangle$ is the smallest subgroup that contains both H and K. In particular this means that $\langle H, K \rangle \subset HK$. One the other hand, since $\langle H, K \rangle$ is the intersection of all subgroups that contain H and K we have that $\langle H, K \rangle \subset HK$ because HK is a part of this intersection. □

Now we discuss the isomorphism theorems. These theorems are essentially the bread and butter of this text. First we begin with some motivation. Suppose that G is a group and N is normal in G, and we have a homomorphism $\varphi : G \longrightarrow H$. Consider the canonical projection $G \longrightarrow G/N$, we ask whether there is a homomorphism $\overline{\varphi} : G/N \longrightarrow H$ such that $\overline{\varphi} \circ \pi = \varphi$. If such a $\overline{\varphi}$ exists then we would have and $n \in N$ is given then $\varphi(n) = \overline{\varphi}(\pi(n)) = \overline{\varphi}(N) = 1$, so this implies that $N \subset \ker \varphi$. Conversely if $N \subset \ker \varphi$ then define the function $\overline{\varphi} : G/N \longrightarrow H$ by $\overline{\varphi}(gN) = \varphi(g)$. Indeed then this map is well defined. Suppose that $g_1 N = g_2 N$, then $g_2^{-1} g_1 \in N \subset \ker \varphi$, so $\varphi(g_2^{-1} g_1) = 1$, which implies that $\varphi(g_1) = \varphi(g_2)$. Then it is easy to see that $\overline{\varphi}$ is a homomorphism since

$$\overline{\varphi}(g_1 H g_2 N) = \overline{\varphi}(g_1 g_2 N) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1 N)\overline{\varphi}(g_2 N).$$

It is also not too hard to see by this definition that $\overline{\varphi} \circ \pi = \varphi$. Therefore we have a direct correspondence between the set of all subgroups of $\ker \varphi$ and homomorphisms of the form $\overline{\varphi} : G/N \longrightarrow H$. such that $\overline{\varphi} \circ \pi = \varphi$. More formally, this is encapsulated in the following theorem:

Theorem 19 (The Factorization Theorem)**.** *Let G and H be subgroups with $\varphi : G \longrightarrow H$ a homomorphism. Let $N \subset G$ be a subgroup. Then $N \subset \ker \varphi$ iff there exists a homomorphism $\overline{\varphi} : G/N \longrightarrow H$, satisfying $\overline{\varphi} \circ \pi = \varphi$. Furthermore, $\operatorname{im} \varphi = \operatorname{im} \overline{\varphi}$ and $\overline{\varphi}$ is uniquely determined by these properties.*

Proof. One has

$$\operatorname{im} \varphi = \{\varphi(x) : x \in G\} = \{\overline{\varphi}(xN) : x \in G\} = \{\overline{\varphi}(xN) : xN \in G/N\} = \operatorname{im} \overline{\varphi},$$

where we used the surjectivity of the projection π. Suppose that ψ is another homomorphism satisfying the above conditions. Then $\psi(gN) = \psi(\pi(g)) = \varphi(g) = \overline{\varphi}(gN)$, so we are done. □

Now we present the isomorphism theorems:

Theorem 20 (First Isomorphism Theorem)**.** *Let $\varphi : G \longrightarrow H$ be a homomorphism of groups. Then the map*

$$\overline{\varphi} : G/\ker \varphi \longrightarrow H$$

is an injective homomorphism of groups, inducing an isomorphism $G/\ker \varphi \cong \operatorname{im} \varphi$.

Proof. The latter part is just a technicality since the images of $\overline{\varphi}$ and φ agree, so we will prove the first part which is not immediate. We want to show that $\ker \overline{\varphi} = \{\ker \varphi\}$, which is the element 1 in $G/\ker \varphi$. Let $x \ker \varphi \in \ker \overline{\varphi}$. Then $\overline{\varphi}(x \ker \varphi) = \varphi(x) = 1$, so $x \in \ker \varphi$ and thus $x \ker \varphi = \ker \varphi$, so $\ker \overline{\varphi} = \{\ker \varphi\}$. It is important to note that one can not replace $\ker \varphi$ with any subgroup $N \subset \ker \varphi$, since the proof falls apart when we state that $x \in \ker \varphi$ (we can not conclude that $xN = \ker \varphi$). □

Theorem 21 (Second Isomorphism Theorem)**.** *Let G be a group and A, B be two subgroups of G so that $A \subset N_G(B)$ (A normalizes B). Then*

AB is a subgroup of G and B is a normal subgroup of AB.

$A \cap B$ is a normal subgroup of A.

The map $A/(A \cap B) \longrightarrow AB/B$ given by $a(A \cap B) \longrightarrow aB$ is an isomorphism.

Proof. Recall that AB is a subgroup of G because we can use the union trick as in Lemma 17. Now let $ab \in AB$. Then $abB(ab)^{-1} = abBb^{-1}a^{-1} = aBa^{-1} \subset B$ because $A \subset N_G(B)$ (A normalizes B). Now let $a \in A$. Then

$$a(A \cap B)a^{-1} = aAa^{-1} \cap aBa^{-1} \subset A \cap B,$$

again because A normalizes B. The trick of distributing over intersection is just standard set theory, write it all out if you are confused. Now consider the map $\varphi : A \longrightarrow AB/B$ defined by $a \longrightarrow aB$. φ is surjective because for all $abB \in AB/B$ one has $abB = aB = \varphi(a)$. One verifies very easily that φ is a homomorphism and that $\ker \varphi = \{a \in A : aB = B\} = \{a \in A : a \in B\} = A \cap B$, hence we conlude the result by the First Isomorphism Theorem. □

Theorem 22 (Third Isomorphism Theorem)**.** *Suppose that $K \subset H \subset G$ are a chain of subgroups with H, K normal in G. Then H/K is normal in G/K and the map $G/H \longrightarrow (G/K)/(H/K)$ given by $gH \longrightarrow gK(H/K)$ is an isomorphism.*

Proof. Let $gK \in G/K$ and $hK \in H/K$. Then

$$gK(hK)(gK)^{-1} = gK(hK)K^{-1}g^{-1} = gKhKg^{-1} = ghKKg^{-1} = ghKg^{-1}$$
$$= ghg^{-1}gKg^{-1} = ghg^{-1}K \in H/K.$$

because ghg^{-1} is an element of H. Hence, we can consider the composition of projections $G \longrightarrow G/K \longrightarrow (G/K)/(H/K)$ which is a well defined homomorphism because H/K is normal in G/K. Then what is the kernel of this map? Denote this map by φ and let $h \in H$. Then $hK(H/K) = H/K$ because $hK \in H/K$, so $H \subset \ker \varphi$. On the other hand if $g \in \ker \varphi$ then $gK(H/K) = H/K$ then we have that $gK \in H/K$, hence there is $h \in H$ such that $gK = hK$, so $h^{-1}g \in K \subset H$. This means that there is $c \in H$ such that $h^{-1}g = c$ and thus $g = hc \in H$. Hence, $\ker \varphi = H$ and so we can apply the First Isomorphism Theorem to conclude. □

This concludes the main three isomorphism theorems, but there is still one more isomorphism theorem to talk about. We present simple Lemmas to begin.

Lemma 23. *For any homomorphism of groups $\varphi : G \longrightarrow H$ and any subgroups $A \subset G$ and $B \subset H$ one has $\varphi(A)$ is a subgroup and $\varphi^{-1}(B)$ is a subgroup. Furthermore, taking images preserves cyclic properties, abelianness, and normalness (normalness if φ is surjective).*

Proof. Let $g, h \in \varphi(A)$ then $g = \varphi(a)$ and $h = \varphi(b)$ for some $a, b \in A$. Then $gh^{-1} = \varphi(ab^{-1}) \in \varphi(A)$. Moreover $\varphi(1) = 1$ so $\varphi(A) \neq \varnothing$.

Now let $g, h \in \varphi^{-1}(B)$. Then $\varphi(g) = a$, $\varphi(h) = b$ for some $a, b \in B$. Then $\varphi(gh^{-1}) = ab^{-1} \in B$, so $gh^{-1} \in \varphi^{-1}(B)$. Furthermore $\varphi^{-1}(B)$ is non-empty because $1 \in B$ and $1 = \varphi(1)$.

Now suppose that A is cyclic. Then $A = \langle a \rangle$ for some $a \in G$. Let $b \in \varphi(A)$. Then $b = \varphi(c) = \varphi(a^k) = \varphi(a)^k$, so we conclude that $\varphi(A) = \langle \varphi(a) \rangle$.

Suppose now A is abelian. Let $a, b \in \varphi(A)$. Then $ab = \varphi(g)\varphi(h) = \varphi(h)\varphi(g) = ba$ for some $g, h \in A$.

The case where φ is surjective and A is normal in G implies $\varphi(A)$ is normal in H is similar. □

Theorem 24 (Fourth Isomorphism Theorem)**.** *Let G be a group and H be a normal subgroup of G. Then for any subgroup $H \subset A \subset G$ one has $A/H \subset G/H$ is a subgroup of G/H and the map $A \longrightarrow A/H$ defines a bijection between the set of all subgroups of G containing H and the set of subgroups of G/H.*

Proof. Since $H \subset A \subset G$ and H is normal in G, it follows that H is normal in A, so A/H is indeed a group, and a subgroup of G/H because $A \subset G$. Denote by X the set of subgroups of G/H and Y the set of subgroups of G containing H. Indeed then, consider the map $\varphi : X \longrightarrow Y$ given by $K \longrightarrow \pi_H^{-1}(K)$. This map is well defined by Lemma 23, we see that the inverse image is indeed a subgroup containing H.

We check that $\pi_H^{-1}(A/H) = A$. Indeed, $A \subset \pi_H^{-1}(A/H)$ is obvious. On the other hand if $g \in \pi_H^{-1}(A/H)$ then $\pi_H(g) = gH \in A/H$ and thus $gH = aH$ for some $a \in A$, so $a^{-1}g \in H$, since $H \subset A$ it follows that $a^{-1}g \in A$ and thus $g \in A$.

Now if A/H is a subgroup of G/H we check that $A/H = \pi_H^{-1}(A/H)/H$. The containment $\pi_H^{-1}(A/H)/H \subset A/H$ is clear. On the other hand if $aH \in A/H$ then $aH \in G/H$ and so there is some $g \in G$ such that $aH = gH$, hence $g \in \pi_H^{-1}(A/H)$, implying $aH = gH \in \pi_H^{-1}(A/H)/H$.

Using these two checks we conclude that φ is indeed an inverse to our map sending $A \longrightarrow A/H$. □

This concludes the isomorphism theorems. We now give a couple lemmas related to the fourth isomorphism theorem.

Lemma 25. *Let G be a group and H be a normal subgroup of G. Then the projection map $G \longrightarrow G/H$ preserves the partial order of subgroups. That is, for any two subgroups A, B s.t. $H \subset A, B$, one has $A \subset B$ iff $A/H \subset B/H$.*

Proof. Suppose $A \subset B$. Then $A/H = \{aH : a \in A\} \subset \{bH : b \in B\} = B/H$. On the other hand if $A/H \subset B/H$, let $a \in A$. Then $aH \in A/H \subset B/H$ and so there is $b \in B$ such that $aH = bH$, hence $b^{-1}a \in H$ but $H \subset B$ so this finally implies $a \in B$. □

Lemma 26. *Let G be a group and H be a normal subgroup of G. Let $H \subset K \subset G$ be another subgroup of G containing H. Then K is normal in G iff K/H is normal in G/H.*

Proof. Suppose K is normal in G. Let $gH \in G/H$ and $kH \in K/H$. Then

$$gH(kH)(gH)^{-1} = gH(kH)H^{-1}g^{-1} = gHkHg^{-1} = gkHHg^{-1}$$
$$= gkHg^{-1} = gkg^{-1}gHg^{-1},$$

but then $gkg^{-1} \in K$ because K is normal in G, and also $gHg^{-1} \subset H$ because H is normal in G, hence $gkg^{-1}gHg^{-1} \in kH$. On the other hand, suppose that K/H is normal in G/H. Let $k \in K$ and $g \in G$. Then we have $gHkH(gH)^{-1} = gHkHHg^{-1} = gHkHg^{-1}H = Hgkg^{-1}H = gk^{-1}g^{-1}HH = gk^{-1}g^{-1}H \in K/H$. Hence $gk^{-1}g^{-1}H = k_1H$ for some $k_1 \in K$ and therefore we have $gk^{-1}g^{-1} = k_1h$ for some $h \in H$. But then $h \in K$ because $H \subset K$ and so $gk^{-1}g^{-1} \in K$. Applying inverses yields the result. □

One last structure theorem, note that the following theorem holds. We will omit the proof. It follows by going through the definitions:

Theorem 27. *Let G be a group. Then G is abelian iff $G/Z(G)$ is cyclic.*

1.6 Exact Sequences

Definition 17. Let $G \longrightarrow^f G' \longrightarrow^g G''$ be a sequence of homomorphisms. We say that this sequence is exact if $\operatorname{im} f = \ker g$.

Some examples of exact sequences, we start with $H \subset G$ a normal subgroup. Then the mappings $H \longrightarrow G \longrightarrow G/H$ is exact, since $\operatorname{im} f = H = \ker g$. Another example, the homomorphism $\{1\} \longrightarrow H \longrightarrow G$ is exact, since $\operatorname{im} f = \{1\} = \ker g$. Furthermore, $G \longrightarrow G/H \longrightarrow \{1\}$ exact, since $\operatorname{im} f = G/H = \ker g$.

Lemma 28. *Given a sequence of homomorphisms $\{1\} \longrightarrow G \longrightarrow^f G'$, this sequence is exact iff f is a monomorphism. Similarly the sequence $G \longrightarrow^f G' \longrightarrow \{1\}$ is exact iff f is an epimorphism.*

Proof. Trivial. □

More generally, a sequence

$$G_1 \longrightarrow^{f_1} \ldots \longrightarrow^{f_{i-1}} G_i \longrightarrow^{f_i} G_{i+1} \longrightarrow^{f_{i+1}} \ldots \longrightarrow^{f_{n-1}} G_n$$

is exact if $\operatorname{im} f_i = \ker f_{i+1}$ for all $1 \leq i \leq n-2$, i.e. it is exact at every part of the sequence.

For some examples, note that $\{1\} \longrightarrow G \longrightarrow^f G' \longrightarrow \{1\}$ is exact iff f is an isomorphism.

Definition 18. A short exact seqeuence is an exact sequence of the form

$$\{1\} \longrightarrow G \longrightarrow^f G' \longrightarrow^g G'' \longrightarrow \{1\}.$$

In this case all one needs to check is that $\operatorname{im} f = \ker g$.

Some examples of a short exact sequence. The standard short exact sequence is given by

$$\{1\} \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow \{1\},$$

for $H \subset G$ a normal subgroup.

In general, every short exact sequence is essentially given by the standard one. If one has a short exact sequence

$$\{1\} \longrightarrow G \longrightarrow^{f} G' \longrightarrow^{g} G'' \longrightarrow \{1\}$$

then one can define $H = \operatorname{im} f$ and consider the sequence

$$\{1\} \longrightarrow H \longrightarrow G' \longrightarrow G'/H \longrightarrow \{1\},$$

where every group in each respective sequence spots are isomorphic, and we have an induced commutative diagram under these isomorphisms. Note also that any group homomorphism $\varphi : G \longrightarrow H$ is the composition of an epimorphism followed by an isomorphism, followed by a monomorphism. Indeed we have the homomorphisms $G \longrightarrow G/\ker\varphi \longrightarrow \operatorname{im}\varphi \longrightarrow H$ by the First Isomorphism Theorem.

1.7 Group Actions

Suppose that G is a group and S is a set. We say that G acts on S if a homomorphism $G \longrightarrow \mathrm{Per}(S)$ is given. Alternatively, we can say there is a map $G \times S \longrightarrow S$ defined by $(x, s) \longrightarrow \psi_x(s)$ where $\psi_x \in \mathrm{Per}(S)$. We define $x \cdot s = \phi_x(s)$. Some properties: First is that $(xy) \cdot s = x \cdot (y \cdot s)$, and also $1 \cdot s = s$, since the map given above must be a homomorphism.

Below are some examples of group actions:

Example 7. First we have the trivial action. Given a set S we define for all $g \in G$ and $s \in S$ $g \cdot s = s$. Furthermore, any group acts on the empty set.

Some more important examples:

Example 8. Take any group G and let $H \subset G$ be a normal subgroup of G. Then G acts on H by conjugation through the map $G \longrightarrow \mathrm{Aut}(H)$ defined by $g \longrightarrow \psi_g$ where $\psi_g(x) = gxg^{-1}$.

It is not too difficult to see that conjugation is an automorphism on every normal subgroup H. In particular, the set of all maps arising as a conjugation forms a subgroup of $\mathrm{Aut}(G)$.

Definition 19. The Inner automorphisms of a group G are defined as $\mathrm{Inn}(G) = \{\psi_g \in \mathrm{Aut}(G) : g \in G \text{ and } \varphi_g(x) = gxg^{-1}\}$. Indeed also it is not too difficult to work out that $\mathrm{Inn}(G)$ is normal in G. We define the Outer automorphisms of a group G to be $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

This prompts a new definition of a normal subgroup. Note that a set A is stable under f if one has the inclusion $f(A) \subset A$.

Definition 20. A normal subgroup is a subgroup of G which is stable under inner automorphisms in G. A characteristic subgroup $N \subset G$ is a subgroup which is stable under all automorphisms of G.

Note that if H is characteristic in N and N is characteristic in G then H is characteristic in G. There is also this variant, if H is characteristic in N and N is normal in G then H is normal in G. Being characteristic is stronger than being normal.

We return to some examples of group actions. Let G be a group and X be the set of all subsets of G (when this makes sense). Then G acts on X through mapping a set S by left-muliplication or conjugation (or right multiplication).

Example 9. Let X be the set of all subgroups of a group G. G acts on X by $x \cdot H = xHx^{-1}$ (note that xHx^{-1} is a subgroup because $1 \in xHx^{-1}$, xHx^{-1} is closed under multiplication, and inverses (because H is).

G also acts on itself by left-multiplication. G acts on itself by right-mutliplcation through $g \cdot x = xg^{-1}$ (note that the inverse is needed, otherwise it is not an action).

Definition 21. Let V be a vector space over a field F. A linear representation of a group G is a group homomorphism $G \longrightarrow GL(V)$, where again $GL(V) \subset \mathrm{Per}(V)$ is the group of linear automorphisms of V. In particular a linear representation is an action.

Definition 22. Let S and S' be equipped with a G action. A morphism of G-sets, is a map $S \longrightarrow^f S'$ s.t. $f(x \cdot s) = x \cdot f(s)$ for all $x \in G$ and $s \in S$.

Definition 23. The isotropy subgroup of an element $s \in S$, denoted by $G_s = \{g \in G : gs = s\}$ is a subgroup of G. The orbit of an element $s \in S$, denoted by $Gs = \{gs : g \in G\} \subset S$. An element $s \in S$ is called fixed if $G_s = G$, or in other words $gs = s$ for all $g \in G$, or in other words that the orbit $Gs = \{s\}$.

Definition 24. If G acts on a set S then the kernel of the action is defined to be the kernel of $G \longrightarrow \mathrm{Per}(S)$. The action is said to be faithful if the kernel is trivial. Note that the kernel is equal to $\bigcap_{s \in S} G_s = \{g \in G : gs = s \text{ for all } s \in S\}$.

An action is said to be transitive if for all $s_1, s_2 \in S$ there is $g \in G$ such that $gs_1 = s_2$. Alternatively an action is transitive iff there is $s \in S$ such that $Gs = S$. Note that a transitive action has no fixed points unless S is empty or of size 1, since if $s \in S$ then $gs = s$ for all $g \in G$ implies that if $s^* \neq s$ then there is no $g \in G$ such that $gs^* = s$.

We say also that $s \in S$ is a fixed point for an element $g \in G$ if $gs = s$. The notion of a fixed point will be clear on the occasion.

Some more examples of actions are as follows:

Example 10. If G acts on a normal subgroup H by conjugation then we have $G_s = C_G(\{s\}) = N_G(\{s\})$. If G acts on itself by translation then we have $G_s = \{1\}$, since if $gs = s$ then applying s^{-1} yields that $g = 1$.

Suppose S is a G-set and $s' = xs$ for some $x \in G$ where s' and s are fixed. If $g \in G_s$ then we have $gs = s$ and therefore $gx^{-1}s' = x^{-1}s'$, which implies that $xgx^{-1}s' = s'$ so $xgx^{-1} \in G_{s'}$. Hence we have $xG_sx^{-1} \subset G_{s'}$. On the other hand, we have that the same holds when x is replaced by x^{-1}, so this immediately gives us equality.

Definition 25. A morphism of G-sets S and S' is a map $S \longrightarrow^f S'$ such that $f(gs) = gf(s)$ for all $s \in S$ and $g \in G$.

Under this definition a composition of morphisms is again a morphism and the identity is a morphism, hence we have the notion of an isomorphism, which is just a bijective morphism. The set of all G-set isomorphisms of the form $f : S \longrightarrow S$ forms a subgroup of $\mathrm{Per}(S)$.

It is important to note that the orbit and isotropy subgroup of an element s seem to be inversely proportional in size. See below for the start of the discussion:

Lemma 29. *Suppose that G acts on a set S. Then the orbits of the action form a partition of S with the associated equivalence relation $x \sim y$ iff there is $g \in G$ such that $gx = y$.*

This above lemma is trivial, just prove that the rule above is indeed an equivalence relation. If C is a system of representatives of the orbits, then the above implies that $S = \bigcup_{s \in C} Gs$ is a disjoint union equal to S. Note as well this means that if G acts on S transitively then there is only one orbit.

Theorem 30 (Orbit Stabilizer Theorem)**.** *Let G act on a set X and $x \in X$ be given. Then there is a well defined bijection $Gx \longrightarrow G/G_x$ given by $gx \longrightarrow gG_x$.*

Proof. This map is well defined. Indeed, if $gx = hx$ then $h^{-1}gx = x$ so $h^{-1}g \in G_x$ which implies $gG_x = hG_x$. Indeed also these implications can be read in reverse to show that the corresponding map $G/G_x \longrightarrow Gx$ is also well defined, and then these maps are inverses of each other. □

Corollary 1. *Let $H \subset G$ be a subgroup of a group G. Then the number of subgroups conjugate to H is $[G : N_G(H)]$.*

Proof. G acts on the set of all subgroups by conjugation. For a given subgroup H we have $GH = \{gHg^{-1} : g \in G\}$ and $G_H = \{g \in G : gHg^{-1} = H\} = N_G(H)$. The result now follows from the Orbit Stabilizer theorem. □

Now we will discuss some important actions in more detail. First we begin with the action of left multiplication of a group on itself.

Theorem 31 (Cayleys Theorem)**.** *Let G be a group and let G act on itself by left-multiplication. Then the action is faithful, transitive, and has no fixed points (unless $G = \{1\}$). In particular, G is isomorphic to a subgroup of* $\mathrm{Per}(G)$.

Proof. Let $g \in G$ and suppose $gh = h$ for all $h \in G$. Applying h^{-1} yields $g = 1$, so the kernel is trivial. Now we want to show that this action is transitive. Let $g_1, g_2 \in G$. Then we have $g_1(g_1^{-1}g_2) = g_2$ and so this action is transitive. Finally let $h \in G$ and suppose that $gh = h$ for all $g \in G$. Applying h^{-1} yields $g = 1$ for all $g \in G$, so $G = \{1\}$.

Since the action is faithful, the kernel of the permutation representation is trivial and therefore we conclude that G is isomorphic to a subgroup of $\mathrm{Per}(G)$ by the First Isomorphism Theorem. □

The following Lemma is also super useful. It generalizes the well known case of $p = 2$.

Lemma 32. *Suppose that G is a finite group and H is a subgroup of G such that $[G : H] = p$ is the smallest prime factor of $|G|$. Then H is normal.*

Proof. Let G act on G/H via. the rule $g(aH) = (ga)H$. This is well defined because $aH = bH$ iff $b^{-1}a \in H$ iff $b^{-1}g^{-1}ga \in H$ iff $(ga)H = (gb)H$. Let K be the kernel of this action $K = \{g \in G : gaH = aH \text{ for all } aH \in G/H\}$. Then K is normal in G because it is the kernel of the permutation representation. If $k \in K$ then we have $kH = H$ and therefore $k \in H$ so we now have the following chain $K \subset H \subset G$. Write $[G : H] = p$ and $[H : K] = m$. Then we have that $[G : K] = mp$ and G/K is isomorphic to a subgroup of $\mathrm{Per}(G/H)$ which has size $p!$. Therefore $mp \mid p!$ which implies that $m \mid (p-1)!$, but $m \mid |G|$ and p is the smallest prime factor of $|G|$ so this forces $m = 1$ and therefore $H = K$. □

Let C be a system of representatives for the orbits for an action of G on S. Since $S = \bigcup_{s \in C} Gs$ is a disjoint union of orbits one has that $|S| = \sum_{s \in C} |Gs|$, but then the Orbit Stabilizer Theorem tells us that this sum is precisely $|S| = \sum_{s \in C} |Gs| = \sum_{s \in C} [G : G_s]$. In the particular case where $S = G$ and G acts on itself by G by conjugation we have the class equation:

Theorem 33 (The Class Equation)**.** *Let $C \subset G$ be a set of representatives of conjugate elements (that is, $g \sim h$ if there is $x \in G$ such that $g = xhx^{-1}$). One has the formula*

$$|G| = \sum_{s \in C} |Gs| = \sum_{s \in C} [G : G_s] = \sum_{s \in C} [G : C_G(\{s\})] = |Z(G)| + \sum_{s \in C \setminus Z(G)} [G : C_G(\{s\}].$$

Proof. It suffices to note that $[G : C_G(\{s\})] = 1$ if and only if $C_G(\{s\}) = G$ if and only if $s \in Z(G)$. □

Now we move onto p-groups. Before this, we simply define the order of an element $x \in G$ to be the order of the (cyclic) subgroup generated by x.

Definition 26. Let p be a prime. A finite group G is called a $p-$group provided that $|G| = p^k$ for some k

Lemma 34. *Let G be a non-trivial p-group. Then $Z(G) \neq \{1\}$.*

Proof. The class equation tells us that p divides $|G|$ and p divides $[G : C_G(\{g\}]$ as long as $C_G(\{g\}) \neq Z(G)$, so in particular we get that p divides $|Z(G)|$, so $Z(G)$ is non-trivial. □

Theorem 35. *Let G be a group of size p^2 where p is a prime. Then G is abelian.*

Proof. The center of G is non trivial, so either the center is G or it is of order p. If the center is G then we are done. If not, then $G/Z(G)$ is a group of prime order, so it is cyclic and therefore G is abelian. □

We discuss cycles a little bit here, since they will be very useful in the future. We stated earlier that any cycle can be decomposed into a product of transpositions:

$$(a_1 \ \dots \ a_r) = (a_1 \, a_2)(a_2 \, a_3) \dots (a_{r-1} \, a_r).$$

It is also not too hard to see then that the set of all transpositions generate S_n. For conjugation in S_n we have the nice formula

$$\sigma(a_1 \ \dots \ a_r)\sigma^{-1} = (\sigma a_1 \ \dots \ \sigma a_r).$$

We define the sign of a permuation $\sigma \in S_n$ to be the sign change of its action on $\mathbb{Z}[x_1, \dots, x_n]$ through the polynomial

$$\sigma \cdot \Pi_{i \neq j}^n (x_i - x_j) = \Pi_{i \neq j}^n (x_{\sigma_{(i)}} - x_{\sigma_{(j)}}),$$

which is either invariant or leaving the polynomial as its negative. This induces a map $\varepsilon : S_n \longrightarrow \{\pm 1\}$ which is a homomorphism and we define A_n to be the kernel of this map. Note through this definition we have that A_n is normal in S_n. $A_n = \{\sigma \in S_n : \sigma$ decomposes into an even amount of transpositions$\}$.

Lemma 36. $|A_n| = n!/2$

Proof. This follows from the first isomorphism theorem. □

Now we discuss Cauchy's theorem, which shows the existence of a subgroup of order p if $p \mid |G|$.

Theorem 37 (Cauchy's theorem)**.** *Suppose that G is a finite abelian group and p is a prime number dividing the order of G. Then there is a subgroup $H \subset G$ of order p.*

Proof. Every finite abelian group is finitely generated and therefore of the form $\mathbb{Z}^k \times \mathbb{Z}/p_1^{k_1} \times \ldots \times \mathbb{Z}/p_n^{k_n}$, but $\mathbb{Z}$ is infinite so $k = 0$. Whence now it is easy to see that there is a cyclic subgroup N with orer p^k for some $k \geq 1$. Take a generator $x \in N$, then $x^{p^{n-1}}$ is an element of order p. □

1.8 Sylow Theorems

Now we begin the Sylow Theorems. Let G be a finite group and p a prime number. We can write the order of G uniquely as $p^k m$ where p does not divide m. In other words k is as large as possible. If a p-subgroup of G, say H has order p^k as above then H is called a Sylow-p subgroup of G.

Theorem 38 (Sylow 1)**.** *Let G be a finite group and p a prime number. Then G has a Sylow-p subgroup.*

Proof. We induct on $|G| = n$. The base case is trivial. Now for a general group G, if we can find a proper subgroup $H \subset G$ so that p doesn't divide $[G : H] = |G| / |H| > 1$, then we can find a p-sylow subgroup of H and therefore it will be a p-sylow subgroup of G.

Hence, we may assume for every proper subgroup $H \subset G$ we have $p \mid [G : H] = |G| / |H|$, so therefore $p \mid |G|$. Then $|G| = |Z(G)| + \sum_{s \in C \setminus Z(G)} [G : C_G(\{s\})]$. Then in the sum recall that $G \neq C_G(\{s\})$, so we can say that p divides each term of the sum, and therefore the entire sum. Therefore p divides $Z(G)$ so by Cauchy's theorem there is a subgroup $H \subset Z(G)$ of order p. Note that H is a normal subgroup of G because H is contained in the center and so if we consider the quotient G/H we can find a p-Sylow subgroup $S \subset G/H$. Then the lattice theorem tells us that there is a subgroup containing H of order $|H||S| = p^k$ for some k and it follows then that this subgroup is a Sylow-p subgroup. □

Theorem 39 (Sylow 2)**.** *Let P be a $p-$Sylow subgroup of a finite group G and Q a $p-$subgroup of G. Then there is a $g \in G$ such that Q is a subgroup of gPg^{-1}. In particular any two p-Sylow subgroups are conjugate.*

Theorem 40 (Sylow 3)**.** *The number of p-Sylow subgroups (denoted by n_p) of G are congruent to $1 \mod p$. If $|G| = p^k m$ so that p doesn't divide m then $n_p \mid m$. If P is any Sylow-p subgroup of G, then $n_p = [G : N(P)]$.*

Proof. Look at the orbit stabilizer theorem and the action of conjugation on the set of p-Sylow subgroups. □

We omit these two above theorems.

Lemma 41. *The following are equivalent. P is the unique sylow p-subgroup of G. P is normal in G. P is characteristic in G (invariant under any $\varphi \in \mathrm{Aut}(G)$).*

Now we begin some applications of the Sylow theorems. First note that for any two subgroups H, K if $|H|$ and $|K|$ are co-prime then their intersection is trivial since any element in the intersection must have order dividing the group.

Example 11. Groups of order pq where $p < q$ and p doesn't divide $q - 1$ are cyclic. Indeed, the number of q-Sylow subgroups divides p and is congruent to 1 mod q so we conclude there is only one. Same with p-Sylow subgroups (where

we use that p doesn't divide $q-1$). Denote these by H and K. Then their intersection is trivial (because they are coprime) and thus $|HK| = |H|\,|K| = pq$. It follows that HK is a subgroup because H is normal in G and thus $H \times K \cong HK$ by Lemma 16. Thus $H \times K$ is cyclic because both are cyclic and co-prime in order. This generalizes to groups of order pq.

Example 12. Groups of order pqr where $p < q < r$ are primes are not simple (have a proper normal-subgroup). Indeed, we have $n_r \equiv 1 \mod r$ and $n_r \mid pq$ implies that $n_r \in \{1, p, q, pq\}$, but the choices of p and q aren't possible since $p < q < r < n_r$, (because $n_r \equiv 1 \mod r$). If $n_r = 1$ then we are done, so now suppose that $n_r = pq$. Then there are $pq(r-1)$ elements of order r. Now $n_q \mid pr$ but $n_q > p$ so it follows that $n_q = r$ or $n_q = pr$. If $n_q = pr$ then there are $pr(q-1)$ elements of order q. In total there are then $prq - pr + pqr - pq = pqr + p(qr - r - q) > pqr$ elements of order either r or q which is bigger than the order of G, hence $n_q = r$ so there are $r(q-1)$ elements of order q. Now if $n_p = 1$ we are done. Otherwise we have $n_p \mid qr$ so that $n_p \geq q$. Hence there are at least $q(p-1)$ elements of order p. In total then there are at least $pq(r-1)+r(q-1)+q(p-1) = pqr-pq+rq-r+pq-q = pqr-rq-r-q > pqr$ elements of order p, q or r, again a contradiction.

Now because of this we have that one of $n_r, n_p, n_r = 1$. Let H be the unique Sylow-subgroup for one of these primes. Consider the chain $1 \subset H \subset G$. It follows that this is a normal chain and G/H is of order either pq, qr, or rp, hence Example 11 tells us that G/H is cyclic, and therefore abelian. Furthermore H is of prime order, so cyclic, and therefore G is solvable (which we will define what that is right now).

1.9 Solvable Groups

Here we will only be working with finite groups. A tower of subgroups in a group G is a finite chain of subgroups $G = G_0 \supset G_1 \supset \ldots \supset G_m$. A tower is normal if G_i is normal in G_{i-1} for all i. A normal tower is abelian if G_{i-1}/G_i is abelian for all i. A normal tower is cyclic if G_{i-1}/G_i is cyclic for all i.

Lemma 42. *A normal (resp. abelian, cyclic) tower $G' = H'_0 \supset H'_1 \supset \ldots \supset H'_m$ yields tower under a homomorphism $G \longrightarrow^f G'$ by letting $H_i = f^{-1}(H'_i)$.*

Proof. Indeed H' being normal in G' means that H is the kernel of the well defined map $G \longrightarrow^f G' \longrightarrow G'/H'$ and therefore H is normal in G. Indeed also G/H embeds into G'/H' so if G'/H' is abelian (resp. cyclic) then so is G/H. □

On the other hand if $f : G \longrightarrow G'$ is a surjective homomorphism then taking images under a tower (normal, abelian, cyclic) yields another tower (normal, abelian, cyclic).

Definition 27. Let $G = G_0 \supset G_1 \supset \ldots \supset G_m$ be a tower. Its refinement is another tower on G obtained by adding intermediate terms.

Definition 28. A finite group G is solvable if it has an abelian tower ending with 1.

Note that all abelian groups are solvable, indeed we have $1 \subset G$ is an abelian tower.

Lemma 43. *Let G be a finite abelian group. Then G admits a cyclic tower ending with* 1.

Proof. We induct on $|G| = n$. If $n = 1$ then we are done. Now if $1 \neq x \in |G|$ then $|G/H| < |G|$ where $H = \langle x \rangle$. Indeed also every subgroup of an abelian group is normal so we have that G/H admits a cyclic tower ending with 1. Then we can move this tower to G via the projection map $G \longrightarrow G/H$. It follows that we have a cyclic tower $G = G^0 \supset G^1 \supset \ldots \supset G^m = H$ where we computed $G^m = \pi^{-1}(1) = \{g \in G : gH = H\} = \{g \in G : g \in H\} = H$. Adding 1 to the end of the tower yields a cyclic tower. □

Lemma 44. *Any abelian tower admits a cyclic refinement.*

Proof. Let $G = G^0 \supset G^1 \supset \ldots \supset G^m$ be an abelian tower. Take some quotient G^i/G^{i+1}. Then G^i/G^{i+1} is finite and abelian and so admits a cyclic tower ending in 1. Then moving everything back we get a refinement of the part $G^i \supset G^{i+1}$ and repeating this to every quotient yields a cyclic refinement. □

Corollary 2. *Any solvable group G admits a cyclic tower ending with* 1.

Proof. Repeating the above Lemma, we obtain a cyclic tower, but since the tower ends in 1 already we get what we want. □

Theorem 45. *If G is a finite group and H is a normal subgroup then G is solvable iff H and G/H are both solvable.*

Proof. In the forward direction if G is solvable then we get a solvable tower through the inclusion $H \longrightarrow G$. Similarly we get a solvable tower in G/H through the map $G \longrightarrow G/H$ because it is a surjection. On the other hand if G/H and H are solvable then we have a solvable tower $G/H = G^0 \supset \ldots \supset G^m = 1$ and a tower $H = H^0 \supset \ldots \supset 1$. Take the tower back under the map $G \longrightarrow G/H$ and attach it to the tower that H induces. □

Now we begin our discussion of the commutator subgroup. A commutator on a group G is a product $[x, y] = x^{-1}y^{-1}xy$.

Definition 29. The commutator subgroup $G^{(1)} \subset G$ is the subgroup generated by all commuators on G, i.e. the subgroup where all products are commuatators.

Lemma 46. *$G^{(1)} \subset G$ is normal and $G/G^{(1)}$ is abelian. Furthermore $G^{(1)}$ is the smallest subgroup in G with the above two properties. That is, if H is any normal subgroup such that G/H is abelian then $G^{(1)} \subset H$.*

Proof. If we conjugate a commuator we have

$$gx^{-1}y^{-1}xyg^{-1} = gx^{-1}g^{-1}gy^{-1}g^{-1}gxg^{-1}gyg^{-1} = [gxg^{-1}, gyg^{-1}] \in G^{(1)}.$$

To show abelianness for $\overline{x}, \overline{y} \in G/G^{(1)}$ one has $\overline{x}^{-1}\overline{y}^{-1}\overline{xy} = \overline{x^{-1}y^{-1}xy} = 1 \in G/G^{(1)}$, so then we have $\overline{xy} = \overline{yx}$. □

Lemma 47. *Let $G \longrightarrow^f A$ be a homomorphism to an abelian group A. Then* $\ker f$ *contains $G^{(1)}$.*

Corollary 3. *If a non-trivial finite group G is solvable then its commutator subgroup is a proper subgroup.*

Proof. If G is solvable then it admits a cyclic tower ending in 1. This implies there is some $H \subset G$ such that $H \neq G$ and G/H is cyclic, and therefore abelian, so $G^{(1)} \subset H$. □

For any group G we can construct an abelian tower

$$G = G^{(0)} \supset G^{(1)} \subset \dots$$

where $G^{(1)}$ is the commutator subgroup of G and $G^{(i+1)} = G^{(i)^{(1)}}$. $G^{(i)}$ is called the i-th commutator subgroup of G. This tower can be infinite, and it may happen that $G^{(i)} = G^{(i+1)} = \dots$. If it does not end in 1, then G can not be solvable. See the below theorem:

Theorem 48. *If G is solvable, then $G^{(m)} = 1$ for some $m \geq 0$. In particular the commuatator series gives an abelian tower ending in* 1.

Proof. We claim that $G^{(i)} \subset G^i$ (therefore $G^{(n)} \subset G^n = 1$). Since G/G^1 is abelian, by the definition of the commutator subgroup we have the following relation $G^{(i)} \subset G^i$. □

Lemma 49. *Every p-group is solvable.*

Proof. The base case $n = 1$ is trivial. Now if G is a $p-$group then $Z(G)$ is non-trivial, so $G/Z(G)$ is again a p-group of smaller order. Thus $G/Z(G)$ admits an abelain tower ending in 1. Pulling back from the projection we get an abelian tower in G ending with $Z(G)$. Adding 1 at the end of this tower yields the Lemma. □

Now we discuss the solvability of S_n. Note that S_1 and S_2 is solvable since they are abelian. S_3 is solvable because the number of 3 Sylow subgroups divides 2 and is congruent to 1 mod 3 and therefore must be equal to 1. Denote this subgroup by P. It follows then that P is normal in S_3 and $|S_3/P| = 2$ which implies that S_3/P is abelian. Hence we have the abelian tower $S_3 \supset P \supset 1$. Similarly S_4 is solvable. Look at the subgroup H of all disjoint transpositions of even order. This subgroup is abelian and normal in S_4. Thus we get the chain $S_4 \subset H \subset 1$. Then H is solvable because H is abelian, and S_4/H is solvable because $|S_4/H| = 6$ (where we use the same argument for S_3). Therefore since H is normal in S_4 we conclude that S_4 is solvable.

Theorem 50. *For all $n \geq 5$, S_n is not solvable.*

Corollary 4. *A_n is solvable for $n = 1, 2, 3, 4$ but not solvable for $n \geq 5$.*

Proof. For $n \geq 5$ A_n is normal in S_n and S_n/A_n is abelian because it is of order 2, so if A_n was solvable we would have that S_n is solvable. Apply the same argument for $n = 1, 2, 3, 4$. □

Definition 30. A group G is called simple if it contains no proper normal subgroups.

Note that a non-abelian simple group is never solvable.

Theorem 51. *A_n is simple for $n \geq 5$.*