Rice University
Department of Mathematics

Group Theory

A deep introduction to groups

Author
Gabriel Gress

June 11, 2021

Contents

Chapter 1

Groups

1.1 Fundamentals of Groups

Definition 1.1.1: Group

A **group** is a set G that has an associative operation with an identity e and inverses for all elements. If the operation is commutative, then we say G is **abelian**.

Definition 1.1.2: Order

Let $g \in G$. The **order of** g, denoted by $o(g)$, is the smallest positive integer k satisfying $g^k = e$. If there is no such k, then we say that $o(g) = \infty$.

In the finite case, the powers of g are periodic, and so the order is the smallest period.

Definition 1.1.3: Subgroup

A set $H \subset G$ is a **subgroup** of G if it is a group under the operation of G. We denote this by $H \leq G$.

$H \leq G$ if and only if it contains the identity of G and is closed under the operation in G, and for inverses. We can reduce these conditions to requiring that H satisfies the criterion

$$xy^{-1} \in H \quad \forall x, y \in H$$

Proposition 1.1.1

Let $\mathcal{A}$ be a nonempty collection of subgroups of G. Then their intersection is a subgroup:

$$K = \bigcap_{H \in \mathcal{A}} H \leq G.$$

This leads us to the following definition.

Definition 1.1.4: Generated Subgroup

Let $A \subset G$ be a subset of the group G. We define

$$\langle A \rangle = \bigcap_{A \subset H \leq G} H$$

to be the **subgroup of** G **generated by** A.

Alternatively, we define $\overline{A}$ to be the (finite product) closure of A under the group operation of G. One should check that $\langle A \rangle = \overline{A}$.

In short, we can generate a subgroup on a set by looking for the smallest subgroup that contains the set. This is a unique minimal element. This will also be the exact same subgroup formed by taking the closure of A under the group operations of G.

Definition 1.1.5: Coset

Let $H \leq G$ and $g \in G$. Then $gH = \{gh \mid h \in H\}$ is a **left coset**, and $Hg = \{hg \mid h \in H\}$ is a **right coset**.

Two left cosets are either disjoint or equal, and every coset is of the same size.

Proposition 1.1.2

Let $H \leq G$ be a subgroup of G. Then the set of left cosets of H form a partition of G. That is,

$$G = \bigcup_{g \in G} gH.$$

Furthermore, for all $g, g' \in G$, $gH = g'H$ if and only if $g'^{-1}g \in H$. In other words, g and g' are representatives of the same coset.

The set of left cosets form a group by the operation

$$gH \cdot g'H = (gg')H$$

provided that $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. We will soon give this property a name. But first, we will state and prove a fundamental theorem for groups.

Theorem 1.1.1: Lagrange's Theorem

Let H be a subgroup of a finite group G. Then $|H| \mid |G|$, and te number of left cosets of H in G is $\dfrac{|G|}{|H|}$.

This gives a new perspective on subgroups– we can view subgroups as a means of partitioning a group.

Definition 1.1.6: Index

If G is a group and $H \leq G$, the number of left cosets of H in G is called the **index** of H in G. We denote this by $|G : H|$.

Lagrange's Theorem gives us a lot of really nice results. For example, we can immediately see that $|g| \mid |G|$ for $g \in G$ in a finite group, and moreover $g^{|G|} = 1$ for all $g \in G$.

We will define a way to compose two subgroups of a group that can sometimes be convenient.

Definition 1.1.7

Let $H, K \leq G$ be subgroups of G. We define

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

Proposition 1.1.3

If $H, K \leq G$ are finite subgroups of G, then

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

This equation becomes nicer when H, K are disjoint (with the exception of identity of course), as it implies that $|HK| = |H|\,|K|$. However, one needs to be careful– this product isn't necessarily a subgroup, as it may not contain inverses.

Proposition 1.1.4

Let $H, K \leq G$ be subgroups of G. HK is a subgroup if and only if

$$HK = KH.$$

If this holds, then inverses will be contained within HK, and hence it will be closed under group operations.

Normal Subgroups

Cosets are such a vital construction to visualize subgroups, as they will become key to understanding quotient groups. However, we notice one flaw that makes this characterization difficult– left and right cosets of a subgroup are not necessarily equivalent. This property is important enough to earn itself a name.

Definition 1.1.8: Normal Subgroup

A subgroup N of G is **normal** if the left and right cosets are the same; i.e.

$$N \leq G \text{ and } gN = Ng$$

for every $g \in G$. We denote this by $N \triangleleft G$.

We can also think of this as $Ng \subset gN$ and $gN \subset Ng$, or in other words, $g^{-1}ng \in N$ and $gng^{-1} \in N$.

$$N \triangleleft G \iff N \leq G \text{ and } g^{-1}ng \in N \text{for every } g \in G, n \in N$$

We call $g^{-1}ng$ a **conjugate** of n.

Observe that, because the trivial subgroups are trivially normal, then all subgroups H of index 2 are normal.

Theorem 1.1.2

Let $N \leq G$ be a subgroup of a group G. The following are equivalent:

- $N \triangleleft G$
- $gN = Ng$ for all $g \in G$
- The left cosets of N in G form a group by the natural group operation

$$gN \cdot g'N = (gg')N$$

- $gNg^{-1} \subset N$ for all $g \in G$

Every group also has a special normal subgroup called the **center**.

Definition 1.1.9: Center

The **center** of a group is the normal subgroup given by

$$Z(G) = \{g \in G \mid xg = gx \text{ for every } x \in G\}.$$

Every subgroup of the center is normal.

Quotient Groups

Definition 1.1.10: Group Homomorphism

We call a map $\varphi : G_1 \to G_2$ a **group homomorphism** if it preserves the operation; $\varphi(gh) = \varphi(g)\varphi(h)$ for every $g, h \in G_1$.

If the homomorphism is bijective, then it is an **isomorphism**. A homomorphism φ is an isomorphism if and only if $\mathrm{Ker}\varphi = e_1$ and $\mathrm{Im}\varphi = G_2$.

Proposition 1.1.5

Let G and H be groups and let $\varphi : G \to H$ be a homomorphism.

- $\varphi(1_G) = 1_H$
- $\varphi(g^{-1}) = \varphi(g)^{-1}$
- $\varphi(g^n) = \varphi(g)^n$
- $\mathrm{Ker}\varphi \triangleleft G$
- $\mathrm{Im}\varphi \leq H$

In fact, a subgroup $N \triangleleft G$ is normal if and only if it is the kernel of a group homomorphism.

Definition 1.1.11: Quotient Group

We denote by G/N the **quotient group**, whose elements are the cosets of the normal subgroup N, with operations defined by $(aN)(bN) = (abN)$

Theorem 1.1.3: First Isomorphism Theorem

If $\varphi : G_1 \to G_2$ is a homomorphism, then

$$\mathrm{Im}\varphi \cong G_1/\mathrm{Ker}\varphi.$$

This tells us that φ is injective if and only if the kernel is trivial, and we can also see that $|G : \mathrm{Ker}\varphi| = |\varphi(G)|$.

This key theorem allows us to fully connect the notion of normal subgroups partitioning a group.

Definition 1.1.12: Natural Homomorphism

If $N \triangleleft G$, then $\psi : G \to G/N$ defined by $\psi(g) = gN$ is the natural homomorphism with $\mathrm{Ker}\psi = N$ and $\mathrm{Im}\psi = G/N$.

Theorem 1.1.4: Third Isomorphism Theorem

Let G be a group, and let $H, K \triangleleft G$ with $H \leq K$. Then $K/H \triangleleft G/H$ and

$$(G/H)/(K/H) \cong G/K$$

The point of this theorem is that quotients of quotient groups provide little additional information.

Theorem 1.1.5: Fourth Isomorphism Theorem

Let $N \triangleleft G$ be a normal subgroup of G. There is a bijection from the set of subgroups A satisfying $N \leq A \leq G$ onto the set of subgroups $A/N \leq G/N$.

That is, every subgroup of G/N can be viewed as some A/N for some subgroup A containing N. Furthermore, for all $A, B \leq G$ with $N \leq A, B$,

(i). $A \leq B \iff A/N \leq B/N$

(i). $A \leq B \implies |B : A| = |B/N : A/N|$

(i). $\langle A, B\rangle/N = \langle A/N, B/N\rangle$

(i). $A \triangleleft G \iff A/N \triangleleft G/N$

This theorem really just tells us that we can get isomorphisms beween structures via lattices– if two group structures have a certain lattice structure, there is a natural isomorphism between each other.

Direct Product of Groups

Definition 1.1.13: Direct Product

The **direct product** $G_1 \times G_2$ of groups G_1, G_2 is the group of all ordered pairs (g_1, g_2) where $g_i \in G_i$, with the usual definition of multiplication:

$$(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2).$$

It is clearly a group, and the projection subsets $G_1^* = \{(g_1, e_2) \mid g_1 \in G_1\}$ and $G_2^* = \{(e_1, g_2) \mid g_2 \in G_2\}$ are isomorphic to their respective groups. This in turn tells us that $|G_1 \times G_2| = |G_1|\,|G_2|$.

Proposition 1.1.6

$G_1^*, G_2^* \triangleleft G_1 \times G_2$ are normal subgroups, and every $u \in G_1 \times G_2$ can be decomposed as $u = u_1u_2$, $u_i \in G_i^*$.

The converse holds as well; if N, M are normal subgroups of a group G, and every $g \in G$ can be written as $g = nm$, $n \in N, m \in M$, then $G \cong N \times M$.

Of course, $(G_1 \times G_2)/G_1^* \cong G_2$ and vice versa.

We can even take the direct product of more than two groups:

$$g = (g_1, g_2, \ldots, g_n) \in G_1 \times G_2 \times \ldots \times G_n$$
$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n).$$

We will later see that direct products provide us a means of characterizing all finitely generated abelian groups.

1.2 Cyclic Groups

One particular important class of groups are cyclic groups.

Definition 1.2.1: Cyclic Group

A group G is **cyclic** if G can be generated by a single element. That is, there is some element $g \in G$ such that

$$G = \{g^n \mid n \in \mathbb{Z}\}.$$

We write a cyclic group by $G = \langle g \rangle$.

It is not necessarily true that all powers of g are distinct (to see this, observe that in a finite group, if $g^n = 1$, then $g^{n+k} = g^k$). However, it is true that all cyclic groups are abelian (due to the law of exponents).

Proposition 1.2.1

Let $G = \langle g \rangle$. Then $|G| = |g|$. That is, the order of the group is the order of the generator– if the order is infinite, then the group must also be infinite.

Ideas from cyclic groups are useful in the general case for groups as well. For example, if G is any group, and $g^n = g^m = 1$ for some $m, n \in \mathbb{Z}$, then $g^{(m,n)} = 1$. This actually gives us the following theorem:

Theorem 1.2.1

Any two cyclic groups of the same order are isomorphic. In particular, if $\langle g \rangle$ and $\langle h \rangle$ are finite cyclic groups of order n, we have an isomorphism

$$\begin{aligned} \varphi : \langle g \rangle &\to \langle h \rangle \\ x^k &\mapsto h^k \end{aligned}$$

and if $\langle g \rangle$ has infinite order, then

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle g \rangle \\ k &\mapsto g^k \end{aligned}$$

is an isomorphism.

A finite group G is cyclic if and only if $|G| = o(g)$ for some $g \in G$. Lagrange's theorem implies that $o(g) \mid |G|$ for $|G| < \infty$.

Of course, a generator for a cyclic group is not necessarily unique. For example, if g generates a group with order n, then g^a will also generate the group provided that $(n, a) = 1$. Combining this with previous results allow us to completely classify cyclic groups.

Theorem 1.2.2: Classification of cyclic groups

Let $G = \langle g \rangle$ be a cyclic group.

(i). Every subgroup $H \leq G$ is cyclic. In particular, $H = \{1\}$ or $H = \langle g^d \rangle$, where d is the smallest positive integer such that $g^d \in K$.

(ii). If $|G| = \infty$, then $\langle g^a \rangle \neq \langle g^b \rangle$ for distinct nonnegative integers a, b. Equality only holds if $|a| = |b|$. This implies that subgroups of infinite cyclic groups are in bijection with $\mathbb{Z}_+$.

(iii). If $|G| = n < \infty$, then for each $a \mid n$ with $a > 0$, there is a unique subgroup $H \leq G$ with $|H| = a$. This subgroups is exactly the cyclic group

$$H = \langle x^{n/a} \rangle.$$

In general, for every integer m,

$$\langle x^m \rangle = \langle x^{(n,m)} \rangle.$$

1.3 Groups of Symmetries

While the abstract definition of groups seems very natural, the construction of groups actually originated as a way to capture certain notions of physical systems. One important natural group arises from symmetries of geometric objects.

Let $n \in \mathbb{Z}_+$ be a positive integer with $n \geq 3$, and denote by D_{2n} the set of symmetries of a regular n-gon (the **dihedral group**). We consider a symmetry to be any rigid motion that maintains the same locations of nodes of the n-gon (but the ordering of the nodes might differ).

We can uniquely describe a symmetry s by defining the permutation σ on $\{1, 2, \ldots, n\}$ that permutes the nodes. Notice, however, that not every permutation is allowed– rotations do not change the relative ordering of the nodes, and reflections merely reverse the ordering of the nodes. In short, instead of the $n!$ possible permutations, we are actually restricting ourselves to $2n$ permutations– the n permutations obtained by cycling the list, and the n permutations obtained by reversing each of those permutations.

We can make D_{2n} into a group by defining the oberation st for $s, t \in D_{2n}$, which is the symmetry obtained by first applying the transformations of t, and then the transformations of s. This is associative because it is the composition of functions; the identity is given by the identity permutation (fixing all vertices in place), and the inverse symmetry is the transformations that undoes the symmetries.

In fact, for any n-gon, all symmetries can be described as an element of D_{2n}, and hence we will show some properties of D_{2n} that will allow us to utilize it better as group. We denote by r the transformation given by the rotation clockwise about the origin by $2\pi/n$ radians, and s to be the reflection about the line of symmetry from the first index through the origin. Then D_{2n} has the following properties:

- $1, r, r^2, \ldots, r^{n-1}$ are all distinct, $r^n = 1$ and so $|r| = n$
- $|s| = 2$
- $s \neq r^i$ for any i
- $sr^i \neq sr^j$ for all $i \neq j$, $i, j < n$

These properties allow us to explicitly view the symmetry group by

$$D_{2n} = \left\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\right\}$$

Furthermore, we have that $rs = sr^{-1}$, and $r^i s = sr^{-i}$. These properties allow us to combine elements and simplify quickly, and hence are good to be familiar with.

Example 1.3.1

Consider $n = 12$, and hence D_{24}. To compose the symmetries given by (sr^9) and (sr^6), we get

$$(sr^9)(sr^6) = s(r^9s)r^6 = s(sr^{-9})r^6 = s^2(r^{-3}) = r^{-3} = r^9$$

1.4 Groups of Permutations

When considering the construction of the dihedral group, one might be curious what occurs if one allows all permutations of nodes within the set. This in fact results in a group as well– the permutaton group.

Definition 1.4.1: Permutation Group

Let Ω be a nonempty set and let S_Ω denote the set of all bijections from Ω to itself. S_Ω is a group under the operation of composition, and is referred to as the **symmetric group on the set** Ω.

If $\Omega = \{1, 2, 3, \ldots, n\}$, the **symmetric group of degree** n is denoted S_n.

One learns in combinatorics that the number of permutations of a set of size n is $n!$, and so $|S_n| = n!$.

Now we will describe a clever notation that can be used to write elements σ of S_n referred to as cycle decomposition.

Definition 1.4.2: Cycle Decomposition

A **cycle** is a string of integers representing the elements of S_n which cyclically permutes these integers (and fixes all other integers). For example, the cycle $(a_1a_2 \ldots a_m)$ sends a_1 to a_2, a_2 to a_3, and so on, finally sending a_m to a_1. Every element $\sigma \in S_n$ can be described by following the rearrangement of integers until a cycle forms– and then looking for the cycles in the remaining numbers. Thus, we can write a permutation in the form

$$(a_1a_2 \ldots a_{m_1})(a_{m_1+1}a_{m_1+2} \ldots a_{m_2}) \ldots (a_{m_{k-1}+1}a_{m_{k-1}+2} \ldots a_{m_k})$$

which represents k different cycles that σ partitions Ω into.

This allows us to quickly see how σ acts on elements in S_n. To calculate $\sigma(x)$, find x in the list, and if there is an integer to the right of it, then $\sigma(x)$ equals that integer. Otherwise, it is the end of the cycle and hence $\sigma(x)$ is the first element in the list.

The product of all the cycles is called the **cycle decomposition** of σ.

The **length** of a given cycle is the number of integers that appears in it. A cycle of length t is called a t-cycle. Finally, two cycles are called **disjoint** if they have no numbers in common (in a symmetric group, all cycles are disjoint).

This also makes it simple to find inverses, as the cycle decomposition of σ^{-1} is obtained by reversing the order of elements within each cycle. To compute compositions, first follow the cycle given in the first permutation, then the cycle in the second permutation.

As one works with more examples, they will quickly see that S_n is non-abelian for all $n \geq 3$. But of course, disjoint cycles commute, and so one can rearrange the cycles in any product of disjoint cycles without changing the permutation.

Exercise caution– one will see that a permutation can be written via many different decompositions of cycles. However, there is only one unique decomposition into *disjoint* cycles.

Corollary 1.4.1

With the combinatorial construction of a permutation, we say a permutation is even or odd based on the number of inversions. With this definition, we say that a permutation is even if and only if the permutation is the product of an even number of transpositions.

Thus we can check if a permutation is even or odd by counting the number of even cycles. An odd cycle does not change parity, but an even cycle will. Thus, if a permutation has an even number of even cycles, it is even (parity of one). If instead the number of even cycles is odd, then it is an odd permutation (parity of negative one).

Definition 1.4.3: Permutation Groups

Permutation groups are subgroups of S_n.

For example, the dihedral group is merely one of many permutation groups.

Let A_n denote the set of even permutations. This is clearly a subgroup of S_n.

Proposition 1.4.1

$$|S_n : A_n| = 2.$$

Proof. Observe that there is a bijection from the even permutations to the odd permutations by simply transposing the first two elements. ■

We will discuss the alternating group A_n momentarily.

Exercise 1.4.1

The order of an element $g \in S_n$ is the LCM of the lengths of disjoint cycles.

Matrix Groups

For each $n \in \mathbb{Z}^+$, let $GL_n(F)$ be the set of all $n \times n$ matrices whose entries are from a field F and whose determinant is nonzero, i.e.

$$GL_n(F) = \{A \mid A \text{ is an } n \times n \text{ matrix with entries from } F \text{ and } \det(A) \neq 0\}$$

The definitions of fields, matrices, and determinants can be read from a standard linear algebra resource. The product and sum of matrices forms a group operation, and because

$$\det(AB) = \det(A)\det(B)$$

it follows that the set is closed under the grouo operation. Hence, $GL_n(F)$ forms a group called the **general linear group of degree** n.

Quaternion Group

The **quaternion group** Q_8 is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with the group operation computed as follows:

$$1 \cdot a = a \cdot 1 = a$$
$$(-1) \cdot (-1) = 1, \quad (-1) \cdot a = a \cdot (-1) = -a$$

for all $a \in Q_8$, and

$$i \cdot i = j \cdot j = k \cdot k = -1$$
$$i \cdot j = k \quad j \cdot i = -k$$
$$j \cdot k = i \quad k \cdot j = -i$$
$$k \cdot i = j \quad i \cdot k = -j$$

One can check as an exercise that this in fact satisfies the group axioms. Notice that Q_8 is non-abelian of order 8.

Generators and Relations

First, we will give an initial perspective of groups via generators and relations, and then revisit the symmetric group under this light.

Definition 1.4.4: Generator

A subset S of elements of a group G is called a **generator** if every element can be written as a finite product of elements (and their inverses) of S. We denote this by $\langle S \rangle = G$ and when this holds say that G is **generated by** S.

Of course, we need to know exactly what happens to these products of elements in order to get a structure for G.

Definition 1.4.5: Relations and Presentations

Let $G = \langle S \rangle$ be a group generated by S. Any equations R_i that elements in the generator satisfy are called **relations**. If there is some collection of relations $R_1, \ldots, R_m$ such that any relation among elements of S can be deduced from, we call these generators and relations a **presentation** of G, denoted by

$$G = \langle S \mid R_1, R_2, \ldots, R_m \rangle.$$

Example 1.4.1: Dihedral Group

The dihedral group D_{2n} can be viewed as a presentation given by

$$D_{2n} = \langle r, s \mid r^n =^2= 1,\ rs = sr^{-1} \rangle.$$

Showing that a presentation is equivalent to a group structure is non-trivial. Relations can often be tricky, in that there are often "hidden" relations that arise from combining two relations in different ways. As a result, often the best way to show that a presentation indeed corresponds to our group is to show bounds on the order of the presentation, and show that it has the same order as the group desired. Then provided your group satisfies the relations, it is likely that it is the only group (of that order) that does so.

Alternating Group

Our initial description of even and odd permutations was left intentionally vague. A careful reader might question the robustness of our definition, and the correspondence between the combinatiorial definition of even/odd permutations and the group definition.

This section will answer these questions in better detail.

Recall that every element of S_n can be written uniquely as a product of disjoint cycles. However, if we remove the requirement that the cycles are disjoint, we are launched into disarray, as we find multitudes of various ways to write the same product of cycles. We will find that one thing remains constant between these variations– if we write our element as a product of 2-cycles, then the quantity of 2-cycles maintains a parity.

Definition 1.4.6: Transposition

A 2-cycle is called a **transposition**.

Exercise 1.4.2

Prove that every permutation of $\{1, 2, \ldots, n\}$ can be written by a succession of transpositions.

Conclude from this that every element of S_n can be written as a product of transpositions.

While there are many different ways to represent the product of transpositions, one will notice that the number of terms remains the same. We will now show this more formally.

Let Δ be the polynomial on variables $\{x_i\}_i^n$ given by

$$\Delta(x_1, x_2, \ldots, x_n) = \prod_{i<j}(x_i - x_j).$$

Now let $\sigma \in S_n$ be a permutation. We say that σ acts on Δ by

$$\sigma(\Delta) = \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)})$$

Proposition 1.4.2: Even and odd permutations

Let σ, τ be two permutations with $\rho = \sigma\tau$. Then

- $\sigma(\Delta) = \pm\Delta$
- $\rho(\Delta) = \sigma(\tau(\Delta))$
- $\sigma(\Delta) = -\Delta$ whenever σ is a transposition.

This allows us to formally define even and odd permutations.

Definition 1.4.7

Let σ be a permutation so that $\sigma(\Delta) = (-1)^k\Delta$ for some $\in \mathbb{N}$. If k is even, we say that σ is an **even permutation**, and if k is odd, we say that σ is an **odd permutation**.

In general, $(-1)^k$ is the **sign** of a permutation.

Proposition 1.4.3

There is a surjective homomorphism given by

$$\varphi : S_n \to \mathbb{Z}_2$$
$$\varphi(\sigma) = \operatorname{sign}(\sigma)$$

The kernel of the surjective homomorphism is the **alternating group** A_n and consists of the even transpositions.

The alternating group has a fascinating property that it only has non-trivial normal subgroups for $n = 4$. Otherwise, any proper normal subgroups are trivial.

Definition 1.4.8: Simple

A group G is **simple** if the only normal subgroups are the trivial ones.

Theorem 1.4.1

Suppose that $n \neq 4$. Then A_n is a simple group.

1.5 Group Actions

By this point, the reader should have a solid foundation in the basic ideas of group theory. There are richer details to follow, but some of them rely on more advanced ideas in algebra. In particular, group actions are fundamentally connected to permutation groups and group presentations. More details on these topics can be found elsewhere, but one can also get a basic understanding of group actions without this prerequisite knowledge.

Definition 1.5.1: (Left) Action

A (left) **action** of a group G on a set Ω is a function $\mu : G \times \Omega \to \Omega$ with the following two properties:

- $\mu(g_1, \mu(g_2, x)) = \mu(g_1 g_2, x)$ for all $x \in \Omega$, $g_1, g_2 \in G$.
- $\mu(e, x) = x$ for all $x \in \Omega$.

It immediately follows that $\mu(g^{-1}, \mu(g, x)) = \mu(g, \mu(g^{-1}, x)) = x$ for all $x \in \Omega, g \in G$.

While $\mu(e, x) = x$, it doesn't have to be the only element which does so. The **kernel** of the action is the set of elements of G that act trivially on Ω:

$$\mathrm{Ker}\mu = \{g \in G \mid g \cdot x = x \quad \forall x \in \Omega\}$$

If this set is trivial, then we say the action is **faithful**. Regardless, the kernel forms a normal subgroup, as we will see later.

Proposition 1.5.1

- For any $g \in G$, the map $\sigma_g : \Omega \to \Omega$ defined by $\sigma_g x = \mu(g, x)$ is a permutation.
- The map $\theta : G \to S_n$ defined by $\theta(g) = \sigma_g$ is a homomorphism (where S_n is the set of permutations of Ω, so $n = |\Omega|$)
- Conversely, given a homomorphism $\theta : G \to S_n$, there is an action μ of G on Ω given by $\mu(g, x) = \theta(g)x$.

Viewing group actions via permutations is a good way to get a grasp of group actions. One can view group actions of G on Ω as each element $g \in G$ permuting the set Ω. We call the homomorphism $G \to S_\Omega$ given by $\theta(g) = \sigma_g$ to be the **permutation representation** associated to the given action.

Example 1.5.1

- Let H be a subgroup of G. Let Ω be the set of all left cosets of H in G (written as gH for some $g \in G$). Define an action by $\mu(g, g'H) = (gg')H$. This is the action of **left multiplication**.
- Define an action of G on itself ($\Omega = G$) by the rule $\mu(g, x) = gxg^{-1}$. This is the action of **conjugation**.
- Let Ω be the set of all subgroups of G. Then G acts on Ω by **conjugation**: $\mu(g, H) = gHg^{-1}$.

An equivalence relation on Ω is formed by a group action via the rule that $x \sim y$ if there exists $g \in G$ with $\mu(g, x) = y$. The equivalence classes are called **orbits**. The set Ω decomposes into a disjoint union of orbits.

Definition 1.5.2: Transitivity

We say that an action is **transitive** if there is just one orbit, and **intransitive** otherwise.

Left multiplication is transitive, but conjugation is in general not. The orbits for conjugation of G onto itself are the **conjugacy classes** of G.

Definition 1.5.3: Stabilizer

The **stabilizer** of an element $x \in \Omega$ is the set

$$\{g \in G \mid \mu(g, x) = x\}$$

of elements of G for which the corresponding permutation fixes x. It is denoted G_x.

Notice that the union of all stabilizers on Ω is exactly the kernel of the action.

Example 1.5.2

Let A be a subset of G. Consider the action of G on A by conjugation, i.e. $\mu(g, a) = gag^{-1}$. Then the stabilizer of an element $a \in A$ is called the **centralizer of** a denoted by $C_G(a)$. Considering the entire subset A, we define

$$C_G(A) = \left\{g \in G \mid gag^{-1} = a \forall a\right\}$$

to be the **centralizer of** A.

It turns out that $C_G(A) \leq G$ is a subgroup.

One will find that abelian groups prove not to be good examples for centralizers, as one will quickly see that in an abelian group G, $C_G(A) = G$ for all subsets A. However, one can check that

$$C_{Q_8}(i) = \{\pm 1, \pm i\}.$$

There are some similar subgroups that will be of interest soon.

Recall the center subgroup of G denoted by

$$Z(G) = \{g \in G \mid gx = xg \; x \in G\}.$$

The center plays an important role with these new ideas, as one can see that $Z(G) = C_G(G)$ (and hence we already know that $Z(G)$ is a subgroup).

One might recall that we also defined conjugation by subgroups earlier. This also corresponds to a variation of a centralizer.

Definition 1.5.4: Normalizer

Let A be a subset of G, and consider the action of G on A by coset conjugation, i.e. $\mu(g, A) = gAg^{-1} = \left\{gag^{-1} \mid a \in A\right\}$. Then the set of elements which fix A is called the **normalizer** of A in G, denoted by

$$N_G(A) = \left\{g \in G \mid gAg^{-1} = A\right\}.$$

This is actually a larger subgroup containing the centralizer– if $g \in C_G(A)$, then $gag^{-1} = a \in A$, and so $C_G(A) \leq N_G(A)$. One can show that $N_G(A)$ is a subgroup as well.

Proposition 1.5.2

Let $N \leq G$ be a subgroup of G. Then $N \triangleleft G$ is a normal subgroup of G if and only if $N_G(N) = G$.

There are some other nice properties of subgroups that come about from the normalizer.

Proposition 1.5.3

If $H, K \leq G$ are subgroups of G, and $H \leq N_G(K)$, then $HK \leq G$.

Thus, if $K \triangleleft G$ then $HK \leq G$ for any $H \leq G$.

Definition 1.5.5

If A is any subset of $N_G(K)$, we say A **normalizes** K.

Example 1.5.3

Consider $G = S_4$ and $H = D_8$. Let $K = \langle (123) \rangle$. We can view D_8 as a subgroup of S_4 by identifying each symmetry by its permutation on the four vertices. Lagrange's Theorem tells us that $H \cap K = 1$ (as their orders are relatively prime), and hence $|HK| = 24$ and hence $HK = S_4$.

Furthermore, H nor K normalizes the other.

It is worthwhile to notice that if we take $S = \mathcal{P}(G)$, then the action of G on S by coset conjugation admits a stabilizer on its elements A by $N_G(A)$.

Finally, we can also let $N_G(A)$ act on A by conjugation $a \mapsto gag^{-1}$. Then the centralizer $C_G(A)$ is precisely the kernel of this action, and so we have now conceptualized these main definitions via group actions.

Now we will state some theorems that formalize these ideas.

Theorem 1.5.1: Second Isomorphism Theorem

Let G be a group with $A, B \leq G$. Assume $A \leq N_G(B)$. Then

- $AB \leq G$
- $B \triangleleft AB$
- $A \cap B \triangleleft A$
- $AB/B \cong A/(A \cap B)$

Note that AB/A is not necessarily a group, i.e. A is not necessarily normal in AB.

Theorem 1.5.2: Orbit-Stabilizer Theorem

Given an action of G onto Ω, and $x \in \Omega$, the stabilizers G_x form a subgroup of G. Furthermore, there is a bijection between the orbit of x and the set of left cosets of G_x in G given by

$$\mu^i x \mapsto \mu^i G_x.$$

If G is finite, the size of the orbit of x is equal to $|G : G_x| = |G| / |G_x|$.

Corollary 1.5.1

Every transitive action is isomorphic to an action by left multiplication on the left cosets of a subgroup. Furthermore, the actions on the left cosets of two subgroups H, K are isomorphic if and only if H, K are conjugate.

Note: Let $\mathrm{fix}(g)$ denote the number of elements in Ω that are mapped to themselves when g is applied to them as an action.

Theorem 1.5.3: Orbit-Counting Lemma

The number of orbits of G on Ω is given by

$$\frac{1}{|G|} \sum_{g \in G} \mathrm{fix}(g).$$

Lemma 1.5.1: Burnside's Lemma

The number of orbits is equal to the average number of fixed points. We can write this by

$$|G| \cdot (\text{number of orbits}) = \sum_{g \in G} |S^g|$$

We can get some interesting results by considering the action of G on itself, or subsets of itself. This corresponds to the notion of permutations of a group.

Theorem 1.5.4

Let $H \leq G$ be a subgroup and let G act by left multiplication on the set A of left cosets of H in G. We denote this action by σ_H, the associated permutation representation. Then

- G acts transitively on A
- The stabilizer in G of $eH \in A$ is the subgroup H
- The kernel of σ_H is $\bigcap_{x \in G} xHx^{-1}$, and $\mathrm{Ker}\sigma_H$ is the largest normal subgroup of G contained in H

Corollary 1.5.2: Jordan's Theorem

- Let G act transitively on the finite set Ω, where $|\Omega| > 1$. Then there is an element of G which fixes no point of Ω.
- Let H be a proper subgroup of a finite group G. Then

$$\bigcup_{g \in G} g^{-1} H g \neq G.$$

Theorem 1.5.5: Cayley's Theorem

Every group of size n is isomorphic to a subgroup of S_n.

Proof. Let S_n be all permutations of the group $G = \{e, g_2, \ldots, g_n\}$ and define $\varphi : G \to S_n$ by $\binom{g \mapsto g_i}{g g_i}$. In other words, we assign to $g \in G$ the permutation of G onto itself; we multiply every g_i by the given g from the left. One can check that φ is an injective homomorphism, and so $G \cong \mathrm{Image}(\varphi) \leq S_n$. ■

Cayley's theorem can also be seen as a consequence of the above theorem, as one can simply take H to be trivial to get the result.

Proposition 1.5.4

If G is a finite group with $|G| = n$, and p is the smallest prime that satisfies $p \mid n$, then any subgroup of index p is normal.

This can be proven via Cayley's Theorem.

Conjugacy Classes

Earlier, we obtained interesting results such as Cayley's theorem by having G act on itself via left multiplication. We can also get some interesting results by letting G act on itself by conjugation:

$$g \cdot a = gag^{-1} \quad \forall g, a \in G.$$

Definition 1.5.6: Conjugates

Two elements $a, b \in G$ are said to be **conjugate in** G if there is some $g \in G$ such that $b = gag^{-1}$. The orbits of G acting on itself by conjugation are called the **conjugacy classes of** G.

One can clearly see that a, b are conjugate in G if they are contained in the same orbit.

Example 1.5.4

Observe that if G is abelian, then the action of G on itself by conjugation is trivial, and hence not interesting.

If G is non-trivial, then G will never act transitively on itself by conjugation. This is because the identity will always have its own orbit.

As an example, the conjugacy classes of S_3 are

$$\{1\}, \{(12), (13), (23)\}, \{(123), (132)\}$$

G can act on subsets of itself by conjugation, as well. We define this for $S \subset G$ by:

$$gSg^{-1} = \left\{gsg^{-1} \mid s \in S\right\}.$$

We can even use this to define a group action on a higher level– that is, we can define an action of G on $\mathcal{P}(G)$ by $g \cdot S$.

Definition 1.5.7: Set Conjugates

Two subsets $S, T \subset G$ are said to be **conjugate in** G if there is some $g \in G$ such that $T = gSg^{-1}$, i.e. they are in the same orbit of G acting on its subsets by conjugation.

Our previous propositions give us the index of these conjugates within the group:

Proposition 1.5.5

The number of conjugates of $S \subset G$ is the index of the normalizer of S

$$|G : N_G(S)|.$$

The number of conjugates of an element s of G is hence

$$|G : C_G(s)|.$$

Theorem 1.5.6

Let G be a finite group and let $g_1, \ldots, g_n$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G) \leq G$. Then

$$|Z(G)| + \sum_{i=1}^{n} |G : C_G(g_i)| = |G|.$$

This essentially partitions the order of G into its abelian and non-abelian parts.

This has a lot of useful consequences naturally. For example, we can use this to help classify groups of prime power order.

Corollary 1.5.3

Let G be a group with $|G| = p^\alpha$ for some p prime, $\alpha \geq 1$. Then G has a nontrivial center.

Proof. The class equation tells us that

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(g_i)|$$

Because $C_G(g_i)$ are non-central conjugacy classes they cannot be the full group G. Thus, $p \mid |G : C_G(g_i)|$, and hence divides the sum. Thus $p \mid |Z(G)|$, proving the result desired. ■

Corollary 1.5.4

If $|G| = p^2$ for some prime p, then G is abelian and isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Now we will look at the specific case of S_n.

Proposition 1.5.6

Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decomposition

$$(a_1 a_2 \dots a_{k_1})(b_1 b_2 \dots b_{k_2}) \dots$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1)\tau(a_2)\dots\tau(a_{k_1}))\dots(\tau(b_1)\tau(b_2)\dots\tau(b_{k_2})).$$

This provides an easy means of computing conjugation in S_n of course, but moreover it tells us that conjugation doesn't change the general structure of cycles.

Definition 1.5.8: Cycle lengths and partitions

If $\sigma \in S_n$ is the product of disjoint cycles of length $n_1, n_2, \dots, n_r$ with

$$n_1 \leq n_2 \leq \dots \leq n_r,$$

then the integers $\{n_i\}_{i=1}^{r}$ are called the **cycle type of** σ.

If $n \in \mathbb{Z}_+$, a **partition of** n is any nondecreasing sequence of positive integers whose sum is n.

The previous proposition tells us that the cycle type of a permutation is unique.

Proposition 1.5.7

Two elements of S_n are conjugate in S_n if and only if they have the same cycle type.

The number of conjugacy classes of S_n is the number of partitions of n.

We can use these results to prove important ideas– for example, one can give a combinatorial proof that A_5 is a simple group.

1.6 Automorphisms

Definition 1.6.1: Automorphism

Let G be a group. An isomorphism from G onto itself is called an **automorphism** of G. The set of all automorphisms of G is denoted $\mathrm{Aut}(G)$.

One can check that the set of automorphisms of a group forms a group under composition. Furthermore, it is easy to see that automorphisms of G are permutations of G, and hence a subgroup of S_G.

Proposition 1.6.1

Let $H \triangleleft G$ be a normal subgroup. Then G acts by conjugation on H as automorphisms of H. That is, the action defined by

$$h \mapsto ghg^{-1}$$

is an automorphism of H. If $g \in C_G(H)$, then the automorphism will be the trivial automorphism– and hence $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

This shows us that conjugation on normal subgroups are structure preserving permutations. Notice that because G is normal in itself, then for any $K \leq G$ and $g \in G$ then $K \cong gKg^{-1}$. Furthermore, conjugate elements and conjugate subgroups have the same order.

Corollary 1.6.1

For any subgroup $H \leq G$, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. It follows that $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$.

Definition 1.6.2

Let G be a group. Then conjugation by $g \in G$ is called an **inner automorphism** of G, and the subgroup of $\mathrm{Aut}(G)$ consisting of all inner automorphisms is denoted $\mathrm{Inn}(G)$.

Of course, it holds then that $\mathrm{Inn}(G) \cong G/Z(G)$. In some sense, the inner automorphisms capture the non-abelianity of a group, as there are more inner automorphisms the smaller the center is.

This gives us really helpful properties to characterize normal subgroups. We can quickly see how G acts by conjugation on $H \triangleleft G$ by looking at the automorphism group of H, which in turn gives us information on G.

Definition 1.6.3

A subgroup $H \leq G$ is called **characteristic in** G, denoted $H\mathrm{char}G$, if every automorphism of G maps H to itself; that is, $\sigma(H) = H$ for all $\sigma \in \mathrm{Aut}(G)$.

Exercise 1.6.1

Show that

- Characteristic subgroups are normal
- If H is the unique subgroup of G of a given order, then $H\mathrm{char}G$
- If $K\mathrm{char}H$ and $H \triangleleft G$, then $K \triangleleft G$.

The third part shows that while normality is not transitive, it is in the case that the smaller subgroup is characteristic in the larger subgroup.

Proposition 1.6.2

The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, which is an abelian group of order $\varphi(n)$.

Proposition 1.6.3

- If p is an odd prime and $n \in \mathbb{Z}_+$, then the automorphism group of the cyclic group of order p is cyclic of order $p-1$. Moreover, the automorphism group of the cyclic group of order p^n is cyclic of order $p^{n-1}(p-1)$.
- For all $n \geq 3$, the automorphism group of the cyclic group of order 2^n is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$, and hence is not cyclic (but has cyclic subgroup of index 2)
- Let p be a prime and let V be an abelian group with the property that $pv = 0$ for all $v \in V$ (where $pv = (v+v+\ldots^p+v)$). If $|V| = p^n$, then V is an n-dimensional vector space over the bielf $\mathbb{F}_p$. The automorphisms of V are then
$$\mathrm{Aut}(V) \cong GL(V) \cong GL_N(\mathbb{F}_p).$$
- For all $n \neq 6$ we have $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \cong S_n$. For $n = 6$, $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| = 2$.
- $\mathrm{Aut}(D_8) \cong D_8$ and $\mathrm{Aut}(Q_8) \cong S_4$.

1.7 Group Representations and Free Groups

We revisit group representations by introducing some new concepts to incorporate, and see how that allows us to expand our theory.

Definition 1.7.1: Commutator

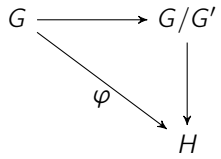
Let $x, y \in G$ be elements of a group, and let $A, B \subset G$ be nonempty subsetf of G. The **commutator of** x **and** y is denoted by
$$[x, y] = x^{-1}y^{-1}xy$$
and the group generated by commutators of elements from A, B is denoted by
$$[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle.$$
We can also define a subgroup of G by the group generated by commutators of elements of G:
$$G' = \langle [x, y] \mid x, y \in G \rangle$$
We call this the **commutator subgroup** of G.

This terminology arises because the commutator of x, y is 1 if and only if x and y commute.

Proposition 1.7.1: Properties of commutators

Let $x, y \in G$ be elements of a group and let $H \leq G$. Then

- $xy = yx[x, y]$
- $H \triangleleft G$ if and only if $[H, G] \leq H$
- $\sigma[x, y] = [\sigma(x), \sigma(y)]$ for any automorphism σ of G. Hence, $G' \mathrm{char} G$, and G/G' is abelian.
- If $H \triangleleft G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \triangleleft G$ and G/H is abelian.
- If $\varphi : G \to H$ is a homomorphism of G into H and H is abelian, then $G' \leq \mathrm{Ker}\varphi$ and the following diagram commutes:



The way to think about this is that by passing to the quotient by the commutator subgroup of G, we collapse all commutators to identity. Hence, all elements in the quotient group commute. This is why we have such a strong property in that, if $G' \leq H$, then G/H must be abelian.

One word of caution– there can be elements of the commutator subgroup that *cannot* be written as a single commutator $[x, y]$ for any x, y. In other words, G' is not just the set of single commutators, but is the group generated by elements of that form.

Proposition 1.7.2

Let $H, K \leq G$ be subgroups. The number of distinct ways of writing each element of the set HK in the form hk, for some $h \in H$, $k \in K$, is $|H \cap K|$.

If $H \cap K = 1$, then each element of HK can be written uniquely as a product hk for some $h \in H$, $k \in K$.

Theorem 1.7.1

Let $H, K \leq G$ be subgroups of G such that $H, K \triangleleft G$ and $H \cap K = 1$. Then

$$HK \cong H \times K$$

Free Groups

The idea of the free group is to define a group $F(S)$ to be generated by some set S with no relations on any of the elements of S. For example, if $S = \{a, b\}$, then some elements of $F(S)$ would be of the form a, aa, ab, $abab$, bab, as well as the inverses of these elements. We call elements of a free group **words**. Then we can multiply elements in the free group simply by concatenation. Our goal will be to define this formally and show it indeed satisfies the necessary properties.

Construction of Free Groups

Let S be a set, and let S^{-1} be a set disjoint from S such that there is a bijection from S to S^{-1}. We denote the corresponding element for $s \in S$ to be $s \mapsto s^{-1} \in S^{-1}$, and furthermore we denote $(s^{-1})^{-1} = s$. Finally, we add a third singleton set disjoint from S, S^{-1} and call it $\{1\}$, and define it so $1^{-1} = 1$. We also define that for any $x \in S \cup S^{-1} \cup \{1\}$, $x^1 = x$.

A **word** on S is a sequence $(s_1, s_2, s_3, \ldots)$ where $s_i \in S \cup S^{-1} \cup \{1\}$, and $s_i = 1$ for all $i \geq N$ for some arbitrarily large N (so that words are "infinite", but not in practice). In order to get uniqueness of words, we say a word is **reduced** if

$$s_{i+1} \neq s_i^{-1} \quad \forall i, s_i \neq 1$$
$$s_k = 1 \implies s_i = 1 \, \forall i \geq k$$

We refer to the special word given by

$$(1, 1, 1, \ldots)$$

to be the **empty word** and denote it by 1. Let $F(S)$ be the set of reduced words on S, and embed mKS into $F(S)$ by

$$s \mapsto (s, 1, 1, 1, \ldots)$$

Hence we identify S with its image and consider $S \subset F(S)$. Notie that if $S = \emptyset$, $F(S) = \{1\}$.

Now we simply introduce a binary operation on $F(S)$, so that two words in $F(S)$ are concatenated, then reduced to their reduced word form. We leave the details of defining this binary operation to the reader, but one can check that this operation is well-defined and satisfies all the properties of a group operation.

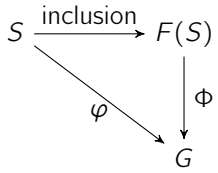
Theorem 1.7.2

$F(S)$ is a group by the binary operation of word concatenation with reduction.

Furthermore, free groups satisfy a special kind of universal property.

Theorem 1.7.3

Let G be a group, S a set, and $\varphi : S \to G$ a set map. There is a unique group homomorphism $\Phi : F(S) \to G$ such that the following diagram commutes:



This further shows that $F(S)$ is unique up to a unique isomorphism, which is the identity map on the set S.

Definition 1.7.2: Free Group

The group $F(S)$ is called the **free group** on the set S. A group F is a **free group** if there is some set S such that $F = F(S)$, in which case we call S a set of **free generators** of F. The cardinality of S is called the **rank** of the free group.

Theorem 1.7.4

Subgroups of a free group are free.

Furthermore, if $G \leq F$ are free and $[F : G] = m$, then

$$\text{rank}(G) = 1 + m(\text{rank}(F) - 1)$$

Proving this requires a lot of other tools, such as covering spaces.

Presentations

Notice that if we take $S = G$, then we can view G as a homomorphic image of the free group $F(G)$ onto G. Moreover, if $G = \langle S \rangle$, there is a unique surjective homomorphism from $F(S)$ onto G which is the identity on S. This allows us to construct a more powerful construction of presentations, generators, and relations.

Definition 1.7.3

A subset $S \subset G$ **generates** G by $G = \langle S \rangle$ if and only if the map $\pi : F(S) \to G$ which extends the identity map of S to G is surjective.

This is distinct but equivalent to our earlier notion for subsets generating a group. However, it is more flexible, so we will use this from here on out.

Definition 1.7.4: Presentations, Generators, and Relations

Let $S \subset G$ be a subset of G such that $G = \langle S \rangle$. A **presentation** for G is a pair (S, R), where R is a set of words in $F(S)$ such that

$$\text{ncl}_{F(S)}(\langle R \rangle) = \text{Ker}(\pi)$$

where ncl denotes the normal closure (the smallest normal subgroup containing $\langle R \rangle$). The elements of S are called **generators**, and the elements of R are called **relations** of G.

We say G is **finitely generated** if there is a presentation (S, R) such that S is finite. Furthermore, G is **finitely presented** if R is also finite.

A word of caution– the kernel of the map $F(S) \to G$ is *not* $\langle R \rangle$, but instead the union of all subsets conjugate to $\langle R \rangle$ (including $\langle R \rangle$ itself). Furthermore, even if S is fixed, a group will have many different presentations.

Finally, often when writing relations, if we have $w_1 w_2^{-1} = 1$, we might instead write $w_1 = w_2$, or vice versa.

Applying presentations to find homomorphisms and automorphisms

Suppose G is presented by $(\langle a, b \rangle, \langle r_1, \ldots, r_k \rangle)$. Then if $a', b' \in H$ are elements that satisfy $r_1, \ldots, r_k$, then there is a homomorphism from G into H. If $\pi : F(\{a, b\}) \to G$ is the presentation homomorphism, we can define

$$\pi' : F(\{a, b\}) \to H$$
$$\pi'(a) = a', \ \pi'(b) = b'.$$

This works because $\text{Ker}\pi \leq \text{Ker}\pi'$, and so π' factors through $\text{Ker}\pi$ and we get

$$G \cong F(\{a, b\})/\text{Ker}\pi \to H$$

Moreover, if $\langle a', b' \rangle = H = G$, then this homomorphism is an automorphism of G(!!). In the other direction, any automorphism on a presentation must send a set of generators to another set of generators satisfying the same relations.

Example 1.7.1: Dihedral presentation

Consider $D_8 = \langle a, b \mid a^2 = b^4 = 1, aba = b^{-1} \rangle$. Any pair of elements a', b' that are of order 2 and 4 (and a' is noncentral) must satisfy the same relations. There are four noncentral elements of order 2, and two elements of order 4, so D_8 has 8 automorphisms.

Similarly, any distinct pair of elements of order 4 in Q_8 that are not inverses of each other necessarily generate Q_8 and satisfy its relations. There are 24 such pairs, so $|\mathrm{Aut}(Q_8)| = 24$. As one can see, free groups are an incredibly useful tool to classify these maps.

Definition 1.7.5

Let G be a group and p prime. If $|G| = p^\alpha$ for $\alpha \geq 1$ then G is called a p-**group**. Even if G has different order, if a subgroup has order p^α, then we call the subgroups p-**subgroups**.

In the specific case where $|G| = p^\alpha m$ for $p \not| m$, then a subgroup of G of order p^α is called a **Sylow** p-**subgroup of** G.

We denote the set of Sylow p-subgroups of G by $\mathrm{Syl}_p(G)$, and the number of Sylow p-subgroups of G by $n_p(G)$.

Theorem 1.7.5: Sylow's Theorem

Let G be a group of order $n = p^a m$, where p is prime and $p \not| m$. Then

- G contains a Sylow p-subgroup.
- The number of Sylow p-subgroups of order p^a is congruent to 1 (mod p) and all these subgroups are conjugate. Furthermore, $n_p \mid m$ as n_p is the index in G of the normalizer of any Sylow p-subgroup.
- Any p-subgroup is a subgroup of a Sylow p-subgroup.

Moreover, Sylow p-subgroups are not only conjugate, but isomorphic.

Corollary 1.7.1

Let P be a Sylow p-subgroup of G. The following are equivalent:

- P is the unique Sylow p-subgroup of G ; $n_p = 1$
- $P \triangleleft G$
- $P \mathrm{char} G$
- If $X \subset G$ such that $|x| = p^{k_x}$ for all $x \in X$, then $\langle X \rangle$ is a p-group.

Example 1.7.2

Let G be finite and p prime.

- If $p \not| |G|$, the Sylow p-subgroup of G is trivial. If $|G| = p^\alpha$, then G is the unique Sylow p-subgroup of G.
- A finite abelian group has a unique Sylow p-subgroup for each prime p called the p-**primary component** of the abelian group. It consists of all elements g such that $|g| = p^{k_g}$.
- S_3 has three Sylow 2-subgroups:

  $$\langle (12) \rangle, \langle (23) \rangle, \langle (13) \rangle.$$

  It has a unique (hence normal) Sylow 3-subgroup $\langle (123) \rangle = A_3$.
- A_4 has a unique Sylow 2-subgroup $\langle (12)(34), (13)(24) \rangle \cong V_4$. It has four Sylow 3-subgroups:

  $$\langle (123) \rangle, \langle (124) \rangle, \langle (134) \rangle, \langle (234) \rangle.$$

- S_4 has $n_2 = 3$ and $n_3 = 4$. Furthermore, S_4 has a subgroup isomorphic to D_8, and hence by conjugacy properties every 2-subgroup of S_4 is isomorphic to D_8.

Sylow's theorem is incredibly useful for showing that groups of a particular order cannot be simple. For example, it can be used to show that if a group is of order 60 and has more than one Sylow 5-subgroup, it must be simple, and hence proves easier that A_5 is simple (and its uniqueness as a simple group of order 60).

Before we get into some nice applications of Sylow's theorem, we will construct some properties for p-groups that will be useful later.

Definition 1.7.6: Maximal Subgroup

A **maximal subgroup** of a group G is a proper subgroup $M < G$ such that there ar eno subgroups $H < G$ that satisfy

$$M < H < G.$$

We can easily see that every proper subgroup of a finite group is contained in a maximal subgroup, but infinite groups need not have maximal subgroups.

Theorem 1.7.6: Properties of p-groups

Let p be a prime and let P be a group of order p^a for $a \geq 1$. Then

- $Z(P) \neq 1$
- If $H \triangleleft P$ is nontrivial, then $H \cap Z(P) \neq 1$. Furthermore, every normal subgroup of order p is contained in $Z(P)$.
- If $H \triangleleft P$ then H contains a subgroup H' of order p^b so that $H' \triangleleft P$ for each divisor $p^b \mid |H|$.
- If $H < P$ then $H < N_P(H)$ (every proper subgroup of P is a proper subgroup of its normalizer in P)
- Every maximal subgroup $M < P$ is of index p and $M \triangleleft P$.

Theorem 1.7.7: Cauchy's Theorem

If a prime number p divides the order of a group G, then G contains an element of order p.

A group of p-power order, acting on a set of size divisible by p, has the property that the number of fixed points is divisible by p. Hence, if there is at least one fixed point, then there are at least p.

Theorem 1.7.8

Let G be a group of order $p^a m$, where p is prime not dividing m. Then, for $0 \leq i \leq a$,

- G contains a subgroup of order p^i
- if $i < m$, then any subgroup of order p^i is contained normally in a subgroup of order p^{i+1}.

Theorem 1.7.9

The center of a non-trivial p-group is non-trivial. Furthermore, if $|P| = p^a$, then P has a chain

$$P_0 < P_1 < \ldots < P_a = P$$

of subgroups, where $|P_i| = p^i$ and each is a normal subgroup of P. Moreover, $P_{i+1}/P_i \cong C_p$.

1.8 Characterization of Finitely Generated Groups

(Note: One can read this section without having seen Sylow's theorem and simply ignore any statement about Sylow p-groups. However, the content here should be revisited once the reader encounters Sylow's theorem elsewhere)

We have already begun classifying groups via Sylow's theorem, but once we utilize the tools of direct products, we can more generally classify groups. Hence the theorems in this section are an extension of the tools given via Sylow's theorem.

A group G is **finitely generated** if there is a finite subset $A \subset G$ such that $G = \langle A \rangle$.

Definition 1.8.1: Free Abelian Group

Let $r \in \mathbb{N}$ be given. We define the **free abelian group of rank** r to be the group

$$\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \ldots^r \times \mathbb{Z}.$$

If $r = 0$, then $\mathbb{Z}^0 = 1$.

Theorem 1.8.1: Fundamental Theorem of Finitely Generated Abelian Groups

Let G be a finitely generated abelian group. Then

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_s}$$

for some integers $r, n_1, n_2, \ldots, n_s$ such that $r \geq 0$, $n_i \geq 2$, and $n_{i+1} \mid n_i$. Furthermore, this factorization of G is unique.

We call r the **free rank** or **Betti number** of G, and the integers $n_1, n_2, \ldots, n_s$ the **invariant factors of** G. The factorization above is hence referred to as the **invariant factor decomposition of** G**.**

A finitely generated abelian group is a finite group if and only if its free rank is zero. Furthermore, if G is a finite abelian group, then its order is the product of its invariant factors, and we say that G is of **type** $(n_1, \ldots, n_s)$.

Observe that because n_1 is the largest invariant factor, and each $n_i \mid n$, if p is a prime divisor of $|G| = n$, then $p \mid n_1$.

Corollary 1.8.1

If n is the product of distinct primes, then up to isomorphism the only abelian group of order n is $\mathbb{Z}_n$.

The fact that $n_{i+1} \mid n_i$ really puts a strong restriction on the structure of finite abelian groups. When n is finite, we will see that the types of abelian groups of order n correspond to the factorization of n.

Theorem 1.8.2: Primary Decomposition Theorem for Finite Abelian Groups

Let G be an abelian group with $|G| = n > 1$, and let the unique factorization of n into distinct prime powers be given by

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Then

$$G \cong A_1 \times A_2 \times \ldots \times A_k$$

where $|A_i| = p_i^{\alpha_i}$, and

$$A_i \cong \mathbb{Z}_{p_i^{\beta_1}} \times \mathbb{Z}_{p_i^{\beta_2}} \times \ldots \times \mathbb{Z}_{p_i^{\beta_t}}$$

where

$$\beta_1 + \beta_2 + \ldots + \beta_t = \alpha_i$$
$$\beta_1 \geq \beta_2 \geq \ldots \geq \beta_t \geq 1.$$

Furthermore, this decomposition is unique.

We call the integers $p_i^{\beta_j}$ the **elementary divisors of** G. Thhis decomposition is called the **elementary divisor decomposition of** G.

The subgroups A_i are the Sylow p_i-subgroups of G, and hence the theorem essentially states that G is isomorphic to the direct product of its Sylow subgroups (which are normal and hence unique, because G is abelian).

Notice that the decomposition in A is the invariant factor decomposition of A with the divisibility condition in the fundamental theorem of finitely generated abelian groups, and hence the elementary divisors of G are the invariant factors of the Sylow p_i-subgroups.

The advantage of this representation is that it lets us easier determine all possible abelian groups of a certain order. Because the β_i are all uniquely determined and satisfy the above properties, it forms a partition of α, and hence we simply look at all combinations of partitions of α_i.

Example 1.8.1: Abelian groups of order p^5

Consider an abelian group G with $|G| = p^5$ for some p prime. Then this technique allows us to distinguish all unique groups like so:

Invariant Factors	Abelian Groups
5	$\mathbb{Z}_{p^5}$
4, 1	$\mathbb{Z}_{p^4} \times \mathbb{Z}_p$
3, 2	$\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$
3, 1, 1	$\mathbb{Z}_{p^3} \times \mathbb{Z}_p \times \mathbb{Z}_p$
2, 2, 1	$\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p$
2, 1, 1, 1	$\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$
1, 1, 1, 1, 1	$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

Hence, there are exactly 7 distinct (up to isomorphism) groups of order p^5.

Of course, it would be more helpful if we had a nice way to pass between the two representations of a factorization of a finite abelian group...

Proposition 1.8.1

Let $m, n \in \mathbb{Z}_+$. Then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $(m, n) = 1$.

If $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1}^{\alpha_1} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}.$$

Then we can go back and forth between the two representations by: factoring out our n_i's into their prime decomposition, in which case collecting each p_j factor gives you each of the Sylow p_j subgroups.

For the reverse direction, we group the elementary divisors by their p_i value, then take the product across different p_i in decreasing order. For example, if the elementary divisors of G are $2, 3, 2, 25, 3, 2$, then $|G| = 2^3 \cdot 3^2 \cdot 5^2$, so the invariant factors of G are $(2_1^1 \cdot 3_1^1 \cdot 5_1^2)$, $(2_2^1 \cdot 3_2^1 \cdot 5_2^0)$, and $(2_3^1 \cdot 3_3^0 \cdot 5_3^0)$, so that

$$G \cong \mathbb{Z}_{150} \times \mathbb{Z}_6 \times \mathbb{Z}_2.$$

This makes it very easy to compare groups of the same order, because if their elementary divisors differ, they cannot be isomorphic.

Definition 1.8.2: Rank

If G is a finite abelian group of type $(n_1, \dots, n_t)$, the integer t is called the **rank** of G.

Proposition 1.8.2

- If $|G| = p$, then $G \cong Z_p$
- If $|G| = p^2$, then G is Abelian and $G \cong Z_{p^2}$ OR $Z_p \times Z_p$
- Let $p > 2$, if $|G| = 2p$, then $G \cong Z_{2p}$ OR D_p.

The first two we have already seen from automorphisms. We will see the latter one after developing more group theory.

1.9 Nilpotent and Solvable Groups

Definition 1.9.1: Nilpotence

For any group G, define the following subgroups inductively:

$$Z_0(G) = 1, \quad Z_1(G) = Z(G),$$
$$Z_i(G) \subset Z_{i+1}(G) < G \quad Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

That is, $Z_{i+1}(G)$ is a subgroup of G containing $Z_i(G)$ that is the complete preimage in G of the center of $G/Z_i(G)$ under the natural projection. We call the chain of subgroups

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \dots$$

the **upper central series** of G.

A group G is called **nilpotent** if $Z_c(G) = G$ for some $c \in \mathbb{Z}$; the smallest such c is called the **nilpotence class of** G.

Nilpotence is a more general form of being abelian– a group may not be abelian, but when one quotients out abelian elements, the quotient might have abelian elements within itself– if we can iterate this process until all elements are abelian under some quotient of centers, then our group is nilpotent.

Remark 1.9.1

If G is abelian, then G is nilpotent with nilpotence class 1. This holds because $Z(G) = G$. Furthermore, we will show the following hierarchy:

$$\text{cyclic groups} \subset \text{abelian groups} \subset \text{nilpotent groups} \subset \text{solvable groups} \subset \text{all groups}$$

If G is finite, there must be an integer N so that for all $n \geq N$,

$$Z_n(G) = Z_{n+1}(G) = \dots$$

If there is a point such that $Z_n(G) = Z_{n+1}(G)$, then the upper limit has been reached.

Infinite groups act a little bit differently with nilpotency; for example, $Z_i(G) < G$ might all be proper subgroups of G (i.e G is not nilpotent), yet

$$G = \bigcup_{i=0}^{\infty} Z_i(G).$$

We call these groups **hypernilpotent**.

Proposition 1.9.1

Let p be a prime and let P be a group of order p^a. Then P is nilpotent of nilpotence class at most $a - 1$.

Proof. Observe that for $i \geq 0$, $P/Z_i(P)$ is a p-group. Hence, if $|P/Z_i(P)| > 1$, then $Z(P/Z_i(P)) \neq 1$.

Assume that $Z_i(P) \neq G$. Then

$$|Z_{i+1}(P)| \geq p\,|Z_i(P)|$$

and so $|Z_{i+1}(P)| \geq p^{i+1}$. Thus,

$$|Z_a(P)| \geq p^a \implies P = Z_a(P)$$

This is just an upper bound however– P is only nilpotence of class a if $|Z_i(P)| = p^i$. This cannot occur, however, as $Z_{a-2}(P)$ would have index p^2 in P, and hence be abelian (in which case $Z_{a-1}(P) = P$). Hence, the class of P is at most $a - 1$. ■

Example 1.9.1

Both D_8 and Q_8 are nilpotent of class 2. Moreover, D_{2^n} is nilpotent of class $n - 1$. This can be proven inductively by showing $|Z(D_{2^n})| = 2$ and $D_{2^n}/Z(D_{2^n}) \cong D_{2^{n-1}}$ for $n \geq 3$.

If n is not a power of 2, then D_{2n} is not nilpotent.

Theorem 1.9.1

Let G be a finite group, and let $p_1, p_2, \dots, p_s \mid |G|$ be distinct primes that divide its order. Let $P_i \in \mathrm{Syl}_{p_i}(G)$. The following are equivalent:

- G is nilpotent
- if $H < G$, then $H < N_G(H)$
- $P_i \triangleleft G$ for all $1 \leq i \leq s$
- $G \cong P_1 \times P_2 \times \dots \times P_s$

This theorem proves part of the fundamental theorem of finite abelian groups.

Corollary 1.9.1

A finite abelian group is the direct product of its Sylow subgroups.

Proposition 1.9.2

If G is a finite group such that, for all $n \mid |G|$ positive, G has at most n elements that satisfy $x^n = 1$, then G is cyclic.

Proposition 1.9.3: Frattini's Argument

Let G be a finite group and $H \triangleleft G$, and let P be a Sylow p-subgroup of H. Then

$$G = HN_G(P)$$
$$|G : H| \mid |N_G(P)|.$$

Proposition 1.9.4

A finite group is nilpotent if and only if every maximal subgroup is normal.

Proof. Let G be a finite nilpotent group and let M be the maximal subgroup of G. Because $M < N_G(M)$, by maximality, $N_G(M) = G$ and hence $M \triangleleft G$.

For the reverse direction, assume every maximal subgroup of the finite group G is normal. Let P be a Sylow p-subgroup of G. For the sake of contradiction, assume that $P \not\triangleleft G$, and let M be a maximal subgroup of G containing $N_G(P)$. Frattini's argument tells us that $G = MN_G(P)$. But $N_G(P) \leq M$ and so $MN_G(P) = M$ giving us a contradiction. Hence $P \triangleleft G$ which is equivalent to nilpotency. ■

Definition 1.9.2: Lower central series

Let G be a group, and define the following subgroups inductively:

$$G^0 = G, \quad G^1 = [G, G],$$
$$G^{i+1} = [G, G^i].$$

Then the chain of groups

$$G^0 \geq G^1 \geq G^2 \geq \dots$$

is called the **lower central series** of G.

Exercise 1.9.1

Prove that G^i is a characteristic subgroup of G for all i.

Theorem 1.9.2

A group G is nilpotent of class c if and only if c is the smallest nonnegative integer such that $G^c = 1$. If G is nilpotent of class c then

$$Z_i(G) \leq G^{c-i-1} \leq Z_{i+1}(G) \quad \forall i \in \{0, 1, \dots, c-1\}.$$

The terms in the upper and lower central series do not necessarily coincide (although this does happen sometimes).

Remark 1.9.2

If G is abelian, then $G' = G^1 = 1$ and so the lower central series is identity after one term. Similar to the upper central series, for any finite group there is some integer N so that for all $n \geq N$,

$$G^n = G^{n+1} = G^{n+2} = \dots$$

For non-nilpotent groups, G^n is a nontrivial subgroup of G. Once equality holds for some $G^n = G^{n+1}$, it holds for all terms after.

Theorem 1.9.3: Krull-Schmidt Theorem

We say that a group G satisfies the **ascending chain condition** on subgroups if every sequence of subgroups of G

$$1 = G_0 \leq G_1 \leq G_2 \leq \dots$$

is eventually constant. Likewise, we say that G satisfies the **descending chain condition** on subgroups if

$$G = G_0 \geq G_1 \geq G_2 \geq \dots$$

is eventually constant.

Assume G is a group that satisfies one of these chain conditions on normal subgroups. Then there is a unique way to write G by

$$G \cong G_1 \times G_2 \times \dots \times G_k$$

where G_k are indecomposable (i.e. cannot be written as a direct product of two proper subgroups).

Note that the decomposition could be non-trivial– all the theorem gives is uniqueness.

Solvable Groups

Definition 1.9.3

Let G be a group. A **subnormal series** is a sequence of subgroups satisfying:

$$1 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_s = G$$

If moreover $H_i \triangleleft G$ for all i, then we say it is a **normal series**.

A **solvable group** is a group with a subnormal series such that H_{i+1}/H_i is abelian.

We will see that in fact the subnormal series of a solvable group is actually a normal series.
We will shortly see that this is related to the notions described above.

Definition 1.9.4

Let G be a group. We define the following sequence of subgroups inductively:

$$G^{(0)} = G, \quad G^{(1)} = [G, G]$$
$$G^{(i+1)} = [G^{(i)}, G^{(i)}]$$

This series of subgroups is called the **derived** or **commutator** series of G.

Note that sometimes we notate $G^{(1)} = G'$, $G^{(2)} = G''$, and so on. One can show that $G^{(i)}$ is characteristic in G.

Caution must be used here– $G^{(0)} = G^0$, $G^{(1)} = G^1$, but this does not hold necessarily for all i. The terms are noticably smaller, so $G^{(i)} \leq G^i$.

Theorem 1.9.4

A group G is solvable if and only if $G^{(n)} = 1$ for some $n \geq 0$.

If G is solvable, the smallest nonnegative n for which $G^{(n)} = 1$ is called the **solvable length** of G.

Proposition 1.9.5

Let G, K be groups, let $H \leq G$, and let $\varphi : G \to K$ be a surjective homomorphism. Then

- $H^{(i)} \leq G^{(i)}$– thus if G is solvable, then H is solvable
- $\varphi(G^{(i)} = K^{(i)}$– homomorphic images and quotient groups of solvable groups are solvable
- If $N \triangleleft G$ and N, G/N are solvable, then so is G.

Theorem 1.9.5

Let G be a finite group.

- If $|G| = p^a q^b$ for some primes p, q, then G is solvable (Burnside)
- If for every prime $p \mid |G|$ we factor the order of G as $|G| = p^a m$ where $(p, m) = 1$, and G has a subgroup of order m, then G is solvable (Philip Hall)
- If $|G|$ is odd then G is solvable (Feit-Thompson)
- If for every pair of elements $x, y \in G$, $\langle x, y \rangle$ is a solvable group, then G is solvable.

Let A and C be arbitrary groups.. One question worth exploring is if there exists a group B such that $A/B \cong C$– that is, B is an extension of C by A. The tools we develop to understand this question are exact sequences. If A is isomorphic to a subgroup of B, there is an injective homomorphism from A to B. And if C is isomorphic to the quotient, then there is a surjective homomorphism from B to C. This will give us a chain

$$A \to B \to C$$

where the homomorphisms are compatible with. We formalize this idea via exact sequences.

Definition 1.9.5: Exact Sequences

Let α, β be homomorphisms so that

$$X \to^{\alpha} Y \to^{\beta} Z.$$

If $\mathrm{Im}(\alpha) = \mathrm{Ker}(\beta)$, then we say the pair of homomorphisms are **exact**.

A sequence of homomorphisms

$$\ldots \to X_{n-1} \to X_n \to X_{n+1} \to \ldots$$

is said to be an **exact sequence** if it is exact at every X_n between a pair of homomorphisms.

Hence, our goal is to see whether we can form an exact sequence $A \to B \to C$. Our notions of injectivity and surjectivity correspond exactly to the notions of exactness.

Proposition 1.9.6

Let A, B, C be groups. Then the sequence

$$0 \to A \to^{\psi} B$$

is exact at A if and only if ψ is injective. Likewise, the sequence

$$B \to^{\varphi} \to C \to 0$$

is exact at C if and only if φ is surjective.

Combining the two ideas, the sequence

$$0 \to A \to^{\psi} B \to^{\varphi} C \to 0$$

is exact if and only if ψ is injective, φ is surjective, and $\mathrm{Im}(\psi) = \mathrm{Ker}(\varphi)$.

Definition 1.9.6

An exact sequence of the form

$$0 \to A \to^{\psi} B \to^{\varphi} C \to 0$$

is called an **short exact sequence**.

Our goal then is to determine if two groups admit a short exact sequence, and if so, how many.

Notice that any exact sequence can be written as a succession of short exact sequences. For example, if

$$X \to^{\alpha} Y \to^{\beta} Z$$

is exact at Y, then equivalently

$$0 \to \alpha(X) \to Y \to Y/\mathrm{Ker}(\beta) \to 0$$

is a short exact sequence.

Example 1.9.2

For fixed A, C, there can be many extensions of C by A. Hence, we need to determine a notion of a homomorphism to distinguish exact sequences.

Definition 1.9.7: Homomorphism of Short Exact Sequences

Let

$$0 \to A \to B \to C \to 0$$
$$0 \to A' \to B' \to C' \to 0$$

be two short exact sequences of groups. A **homomorphism of short exact sequences** is a collection of group homomorphisms α, β, γ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

This is an **isomorphism of short exact sequences** if α, β, γ are isomorphisms in which case the extensions B, B' are **isomorphic extensions**.

The two exact sequences are called **equivalent** if $A = A'$, $C = C'$, and there is an isomorphism between them where α, γ are identity. In this case B and B' are **equivalent extensions**.

Equivalency by extensions is strongesomorphisms between B and B'– it tells us that there is an isomorphism between B and B' that restricts to an isomorphism from A to A' and induces an isomorphism on the quotients by C and C'.

Example 1.9.3

Proposition 1.9.7: Short Five Lemma

Let α, β, γ be a homomorphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

- If α, γ are injective then so is β
- If α, γ are surjective then so is β
- If α, γ are isomorphisms then so is β

Proof of Short Five Lemma. ■

There is always at least one extension of a group C by A given by $B = A \rtimes C$.

Definition 1.9.8

If

$$1 \to A \to^{\psi} B \to^{\varphi} C \to 1$$

is a short exact sequence of groups, then the sequence is **split** if there is a sugroup complement to $\psi(A)$ in B. Then up to isomorphism $B = A \rtimes C$ up to isomorphism by

$$B = \psi(A) \rtimes C'$$

for some subgroup C', which satisfies $\varphi(C') \cong C$.

We say B is a **split extension of** C **by** A.

This is really just the question of existence of a complement to $\psi(A)$ in B that is isomorphic by φ to C.

Proposition 1.9.8

The short exact sequence of groups

$$1 \to A \to^{\psi} B \to^{\varphi} C \to 0$$

of groups is split if and only if there is a group homomorphism $\mu : C \to B$ such that $\varphi \circ \mu \cong \mathrm{Id}_C$.

Any set map $\mu : C \to B$ such that $\varphi \circ \mu = \mathrm{Id}_C$ is called a **section** of φ. If μ is a homomorphism, then μ is called a **splitting homomorphism** for the sequence.

A section of φ is merely a choice of coset representative in B for $B/\mathrm{Ker}\varphi \cong C$. A section is a splitting homomorphism if this set of coset representatives forms a subgroup, in which case this subgroup gives a complement to $\psi(A)$ in B.

Example 1.9.4

Proposition 1.9.9

Let

$$0 \to A \to^{\psi} B \to^{\varphi} C \to 0$$

be a short exact sequence of groups. Then $B = \psi(A) \rtimes C'$ for some subgroup C' of B with $\varphi(C') \cong C$ if and only if there is a homomorphism $\lambda : B \to A$ such that $\lambda \circ \psi = \mathrm{Id}_A$.

This is stronger than the previous proposition. The existence of a splitting homomorphism on the left end of the sequence gives that the extension group is a direct product (instead of a semidirect product).