Advanced Group Theory

Labix

May 2, 2024

Abstract

Leading off from Groups and Rings, these notes deal with the more advanced objects of study in the theory of groups. In particular, we will focus on finite group theory. However, in the first half we present useful result on other topics of mathematics that rely on group theory such as algebraic topology and representation theory.

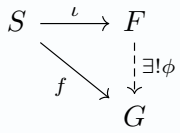
Contents

1 Free Groups and Free Product of Groups

1.1 Free Groups

Definition 1.1.1: Free Groups

Let F be a group and $S \subseteq F$ be a subset. We say that F is free on S if the following universal property holds. For any maps of sets $f : S \to G$, there exists a unique homomorphism $\phi : F \to G$ such that the following diagram commutes:



where $\iota : S \to F_S$ is the inclusion map.

Proposition 1.1.2

Let F_1 be free on S_1 and F_2 be free on S_2. Then $F_1 \cong F_2$ if and only if $|S_1| = |S_2|$.

Theorem 1.1.3

For any set S, there is a free group on S.

Definition 1.1.4: Free Group on a Set

Let S be a set. Define the free group constructed above to be the free group on S, denoted F_S.

Proposition 1.1.5

Any group G is isomorphic to a quotient group of a free group.

1.2 Free Products of Groups

Definition 1.2.1: Word

Let $\{G_i | i \in I\}$ be a collection of groups. A word on these groups is a finite sequence $g_1 \cdots g_m$ where $g_k \in G_i$ for some $i \in I$ and $k \in \{1, \ldots, m\}$. m is said to be the word length. The product of two words is defined to be

$$(g_1 \cdots g_m) \cdot (h_1 \cdots h_n) = g_1 \cdots g_m h_1 \cdots h_n$$

Definition 1.2.2: Reduced Words

A word $g_1 \cdots g_m$ is said to be reduced if

- $g_k \neq 1_i$ for any $i \in I$ and for $k \in \{1, \ldots, m\}$
- For any two consecutive letters g_i and g_{i+1}, they are not in the same group

The set of all reduced words of $\{G_i | i \in I\}$ is denoted

$$*_i G_i = \{ \text{ reduced words on } \{G_i | i \in I\}\}$$

The motrivation for reduced words is to allow us to work with less amount of words since every word can be reduced by removing the identities and replacing two consecutive elements in the same group

with their product in that group.

Proposition 1.2.3: Free Product

Let $\{G_i | i \in I\}$ be a collection of groups. Define a product on the set of reduced words as follows.

$$g * h = \begin{cases} g \cdot h & \text{if } g_m, h_1 \text{ are not in the same group} \\ g \cdots g_{m-1} * g_{m+1} * h_2 \cdots h_n & \text{if } g_m, h_1 \in G_i \text{ for some } i \in I \text{ and } g_m h_1 = g_{m+1} \neq 1 \\ g_1 \cdots g_{m-1} * h_2, \cdots h_n & \text{if } g_m h_1 \in G_i \text{ for some } i \in I \text{ and } g_m h_1 = 1 \end{cases}$$

Then $*_i G_i$ is a group.

Proof. We clearly have the identity 1 and the inverse of $g = g_1 \cdots g_n$ to be $g_n^{-1} \cdots g_1^{-1}$. We just have to check associativity and closure. By definition of the free product, the free product of reduced words is again a reduced word by definition and finiteness of the length of a reduced word.

For any $g \in G_i$, define the action of left multiplication by $L_g(h) = g * h$ for any $h \in *_i G_i$. We clearly have $L_{g_1} \circ L_{g_2} = L_{g_1 g_2}$ and $L_{g^{-1}} = L_g^{-1}$ and thus $L_g \in \text{Sym}(*_i G_i)$. For any word $g = g_1 \cdots g_m$, the map $L : *_i G_i \to \text{Sym}(*_i G_i)$ is injective since for any $g \in *_i G_i$, we have $L_g(1) = g$ which means that $g \neq h$ implies $L_g \neq L_h$. Thus we have embedded the set into the group $\text{Sym}(*_i G_i)$ so that associativity follows. □

Note: If $\{G_i\}$ is just a collection of two groups then we write the free product as $G_1 * G_2$.
The motivation is that we want to continue reducing the product of the word so that it could be fully reduced again.

Proposition 1.2.4

Let $\{G_i | i \in I\}$ be a collection of groups. Then $G_i \leq *_i G_i$ for any $i \in I$.

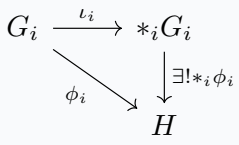
Proof. Clearly every element of G_i is in $*_i G_i$ since we can just treat each element as a word. □

Lemma 1.2.5

Let $\{G_i | i \in I\}$ be a collection of groups. Let $\{\phi_i : G_i \to H\}$ be a collection of group homomorphisms to some group G. Let $\iota_i : G_i \to *_i G_i$ be the inclusion map. Then there exists a unique map

$$*_i \phi_i : *_i G_i \to H$$

such that $(*_i \phi_i) \circ j_i = \phi_i$. In other words, the following diagram commutes:



Proof. Define $*_i \phi_i : *_i G_i \to H$ by $*_i \phi_i(g_1 \cdots g_m) = \phi_{i_1}(g_1) \cdots \phi_{i_m}(g_m)$ where we assume that each $g_k \in G_{i_k}$. Then clearly we have that $(*_i \phi_i) \circ j_i = \phi_i$. Moreover, since ϕ_i are group homomorphisms, we have that $\phi_i(g_k)\phi_i(g_{k+1}) = \phi_i(g_k g_{k+1})$ and $\phi_i(1) = 1$ and thus ϕ_i is compatible with reduced words. This means that $*_i \phi_i$ is a group homomorphism. □

1.3 Presentations of a Group

Definition 1.3.1: Presentations on a Free Group

Let S be a set and $F(S)$ be the free group on S. Let R be a set of words on S. Let N be the smallest normal subgroup that contains R. Define the group with presentations $\langle S|R\rangle$ to be

$$\langle S|R\rangle = \frac{F(S)}{N}$$

Elements of S are called generators and elements of R are called relations.

A group G is said to have a presentation if $G \cong \langle S|R\rangle$ for some S and R.

Theorem 1.3.2

Every group has a presentation.

Proof. This follows from the fact that every group is the quotient of a free group. □

Theorem 1.3.3

Let $G = \langle S|R\rangle$ for $S = \{s_1, \ldots, s_n\}$ a finite set of generators and R is a set of relations. Let H be a group and let $h_1, \ldots, h_n$ be elements of H. Then there exists a homomorphism $\phi : G \to H$ satisfying $\phi(s_i) = h_i$ for $1 \leq i \leq n$ if and only if every relation $r \in R$ holds with each s_i replaced by h_i.

In this case, the homomorphism ϕ is unique.

1.4 Amalgamated Products

2 Groups and Generators

2.1 Generated Groups

Generated Subgroups generalizes the notion of cyclic subgroups in the sense that there are now more than one generators for constructing the group.

Definition 2.1.1: Subgroups Generated by a Set

Let G be a group and A a subset of G. Define the subgroup generated by A to be

$$\langle A\rangle = \{a_1^{e_1}\cdots a_n^{e_n} | n \in \mathbb{N}^+, a_1, \ldots, a_n \in A, e_1, \ldots, e_n \in \{\pm 1\}\}$$

the subgroup of all elements of G that can be expressed as the finite product of elements in S and their inverses.

If $A = \{a_1, \ldots, a_r\}$, we often write the generated subgroup as $\langle A\rangle = \langle a_1, \ldots, a_r\rangle$, omitting the brackets.

Recall that the cyclic subgroup is the smallest subgroup containing the generator. Then generated subgroups also generalizes this particular property. In particular, we have the following identity.

Proposition 2.1.2

Let G be a group and A a subset of G. Then we have that

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

which means that the generated subgroup is the smallest subgroup of G containing A.

Definition 2.1.3: Generating Set of a Group

Let G be a group and S a subset of G. We say that S is a generating set of G if $G = \langle S\rangle$.

2.2 Finitely Generated Groups

Definition 2.2.1: Finitely Generated Groups

A group G is finitely generated if there is a finite subset $A = \{g_1, \ldots, g_n\}$ of G such that $G = \langle A\rangle$.

Lemma 2.2.2

Every finitely generated group is a free group.

Proposition 2.2.3

Every quotient of a finitely generated group is finitely generated.

2.3 Free Abelian Groups

Definition 2.3.1: Basis of a Group

Let G be an abelian group. Let $B \subset G$.

- We say that elements of B are linearly independent if $\sum_{b\in B} n_b \cdot b = 0$ implies $n_b = 0$ for each $b \in B$

- We say that B is a basis of G if it is linearly independent and generate G.

Definition 2.3.2: Free Abelian Group

A free abelian group is an abelian group G that has a basis.

Notice that $k_1, \ldots, k_n$ are unique for each element $g \in G$. This contrasts the fact that in finitely generated abelian groups, $k_1, \ldots, k_n$ are not necessarily unique.

Another comparison, every free group is not finite, but again there is none of this restriction on finitely generated abelian groups.

Definition 2.3.3: Free Abelian Group Generated by a Set

Let X be a countable set. Define the free abelian group on X to be

$$G(X) = \left\{ \sum_{x \in X} n_x \cdot x | n_x \in \mathbb{Z} \right\}$$

If $|X|$ is not finite we require that each element is sum of a finite number of nonzero n_x.

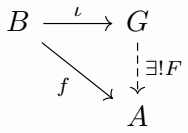
The following proposition shows that they are essentially the same construction.

Proposition 2.3.4

Let G be a free group with basis B. Then $G = G(B)$. Let X be a set. Then $G(X)$ is a free group with basis X.

Theorem 2.3.5: The Universal Property

Let G be a free abelian group with basis B. Let A be an arbitrary abelian group. Let $f : B \to A$ be a function (of sets). Then there exists a unique group homomorphism F from G to A such $F|_B = f$. In other words, the following diagram commutes:



Proposition 2.3.6

Let G be an abelian group and $g_1, \ldots, g_n \in G$. Denote e_k the element of $\mathbb{Z}^n$ with 1 at the kth position and 0 at all others. Define a function $\phi : \mathbb{Z}^n \to G$ by $\phi(e_k) = g_k$. Then

- by defining $\phi(a_1, \ldots, a_n) = \sum_{k=1}^{n} a_k g_k$, ϕ is a group homomorphism
- $g_1, \ldots, g_n$ are linearly independent if and only if ϕ is injective
- $g_1, \ldots, g_n$ generate G if and only if ϕ is surjective
- $g_1, \ldots, g_n$ form a basis of G if and only if ϕ is an isomorphism

Proposition 2.3.7

Let G be a free abelian group with finite basis B of cardinality n. Then

$$G \cong \mathbb{Z}^n$$

In this case, we say that the free group G is free of rank n.

2.4 Unimodular Smith Normal Form

Definition 2.4.1: Unimodular Elementary Operations

We define unimodular elementary operations on $A \in M_{m\times n}(\mathbb{Z})$ as follows:

- (UR1): Replace row r_i with $r_i + tr_j$ where $j \neq i$ and $t \in \mathbb{Z}$
- (UR2): Interchange two rows r_i and r_j
- (UR3): Replace row r_i by $-r_i$
- (UC1): Replace column c_i with $c_i + tc_j$ where $j \neq i$ and $t \in \mathbb{Z}$
- (UC2): Interchange two columns c_i and c_j
- (UC3): Replace columns r_i by $-r_i$

Definition 2.4.2: Unimodular Elementary Matrices

Define three elementary matrices as follows:

- Recombine Matrix: The $n \times n$ recombine matrix $R_{i,j,a}$ is given the zero matrix except the diagonal is all 1 and the ith row and jth column has the value $a \in \mathbb{Z}$.
- Scale Matrix: The $n \times n$ scale matrix $R_i(-1)$ is given by the zero matrix except the diagonal is all 1, and the i, ith element is -1.
- Transposition Matrix: The $n \times n$ transposition matrix $R_{i,j}$ is given by the zero matrix except the diagonal is all 1, the i, ith element and j, jth element is 0 and the i, jth and j, ith element is 1

Proposition 2.4.3

The unimodular elementary operations are exactly equivalent to performing left and right matrix multiplications with unimodular elementary matrices.

In particular, left multiplication corresponds to row operations and right multiplication corresponds to column operations.

Theorem 2.4.4

Let $A \in \mathbb{Z}_{m\times n}$ with rank r. Then there exists a sequence of unimodular elementary row and column operations such that A is reduced to

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

where the d_r is the last non zero diagonal entry. The diagonal also satisfies $d_i > 0$ for $1 \leq i \leq r$ and $d_i | d_{i+1}$ for $1 \leq i < r$. The $d_1, \ldots, d_r$ are also uniquely determined by A.

Proof. □

Definition 2.4.5: Unimodular Smith Normal Form

Let $A \in M_{n\times n}(\mathbb{Z})$ be a matrix with coefficients in $\mathbb{Z}$. Define the smith normal form of A to be the unique matrix above, denoted $\text{SNF}(A)$.

Lemma 2.4.6

Let $A \in \mathbb{Z}_{m\times n}$ has unimodular smith normal form S with rank r. Then the greatest common divisor of all entries of A is equal to d_1 where we require $\gcd(r, 0) = r$ for $r \geq 1$.

3 More Types of Groups

3.1 Torsion Groups

Definition 3.1.1: Torsion Group

A group G is said to be a torsion group if every element of G has finite order. A group G is called torsion free if every element of G except the identity has infinite order.

Definition 3.1.2: Torsion Subgroup

Let G be an abelian group. The torsion subgroup of G is the subgroup of G consisting of all elements of finite order.

Proposition 3.1.3

Let A be an abelian group and B a subgroup of A. If A/B is a free abelian group, then

$$A \cong B \times A/B$$

Proof. Denote the quotient map $f : A \to A/B$. Since A/B is free abelian, there exists $K = \{a_1 + B, \dots, a_n + B, \dots\}$ such that K is a basis of A/B. Now consider $L = \langle a_1, \dots, a_n, \dots \rangle$. I claim that this is isomorphic to A/B. In fact, this is given by $f|_L$. Clearly $f|_K(a_i) = a_i + B$ for each i. Suppose that $a \in \ker(f|_K)$. Write $a = \sum_{i=1}^{n} k_i a_i$. Then we have

$$f|_L\left(\sum_{i=1}^{n} k_i a_i\right) = B$$
$$\sum_{i=1}^{n} k_i f|_L(a_i) = B$$
$$\sum_{i=1}^{n} k_i(a_i + B) = B$$

By property of the basis, we have that $k_1 = \cdots = k_n = 0$. This generalizes well to the countable case since every element is written in a finite sum. Thus we have that $\ker(f|_L) = 0$. For surjectivity, if $\sum k_i(a_i + B)$ is a finite sum in A/B then just choose $\sum k_i a_i \in L$. Thus we have shown bijectivity.

Finally, we show that $A \cong B \times L$. Define $\phi : B \times L \to A$ by

$$\phi\left(b, \sum k_i a_i\right) = \sum k_i a_i + b$$

We first show injectivity. We have that

$$\sum k_i a_i + b = 0$$
$$\sum k_i a_i = -b$$
$$\sum k_i f|_L(a_i) = 0$$
$$\sum k_i(a_i + B) = 0$$

This implies that $k_i = 0$ and thus $b = 0$. Thus $\ker(\phi) = 0$. Now suppose that $a \in A$. Consider the element $a + B \in A/B$. Since A/B has the basis K, we have that

$$a + B = \sum k_i(a_i + B) = \left(\sum k_i a_i\right) + B$$

This implies that $a - \sum k_i a_i \in B$ Then choosing $b = a - \sum k_i a_i$ and $\sum k_i a_i \in L$, we are done with surjectivity. This makes sense even if $\sum k_i a_i \in B$ because in this case, $\sum k_i a_i = 0$ and we can choose $b = a \in B$. □

3.2 p-groups

Definition 3.2.1: p-groups

A group of order p^k for some $k > 0$ is called a p-group. Subgroups of any group that is a p-group are called p-subgroups.

3.3 Simple Groups

Definition 3.3.1: Simple Groups

We say that a group G is simple if its only normal subgroups are the trivial group and G.

3.4 Abelianization and Commutators

Commutators are useful for checking whether a given group is cyclic or not.

Definition 3.4.1: Commutators

Let $g, h \in G$. Define the commutator of g and h to be

$$[g, h] = ghg^{-1}h^{-1}$$

Definition 3.4.2: Commutator Subgroup

Let G be a group. Define the commutator subgroup of G to be

$$[G, G] = \langle [g, h] | g, h \in G \rangle$$

Note that in general, elements of $[G, G]$ are products of several commutators because we are taking the group generated by all the commutators. In general, the set of all commutators $\{[g, h] \mid g \in G, h \in H\}$ is not a group.

Proposition 3.4.3

Let G be a group. Then the following hold for the commutator subgroup of G.

- $[G, G] \trianglelefteq G$
- $G/[G, G]$ is abelian
- If $N \trianglelefteq G$ and G/N are abelian, then $[G, G] \leq N$.

Proof.

- Let $g, h, k \in G$. Then we have

$$\begin{aligned} k[g, h]k^{-1} &= kghg^{-1}h^{-1}k^{-1} \\ &= \left(kgk^{-1}\right)\left(khk^{-1}\right)\left(kg^{-1}k^{-1}\right)\left(kh^{-1}k^{-1}\right) \\ &= [kgk^{-1}, khk^{-1}] \in [G, G] \end{aligned}$$

So for $[g_1, h_1], \ldots, [g_n, h_n] \in [G, G]$, we have

$$k[g_1, h_1] \cdots [g_n, h_n]k^{-1} = \left(k[g_1, h_1]k^{-1}\right) \cdots \left(k[g_n, h_n]k^{-1}\right) \in [G, G]$$

- Let $g, h \in G$. Then we have

$$\begin{aligned} ghg^{-1}h^{-1} \in [G, G] &\implies [G, G]ghg^{-1}h^{-1} = [G, G] \\ &\implies [G, G]gh = [G, G]hg \\ &\implies [G, G]g \cdot [G, G]h = [G, G]h \cdot [G, G]g \end{aligned}$$

So $G/[G, G]$ is abelian.

- Suppose that G/N is abelian. Then $Ng \cdot Nh = Nh \cdot Ng$ for all $g, h \in G$. Thus

$$N(ghg^{-1}h^{-1}) = N$$

and so $[g, h] \in N$. Since N is a subgroup of G, we must have that $[G, G] \leq N$.

And so we conclude. □

Definition 3.4.4: Abelianization

Let G be a group. Define the abelianization of G to be the abelian group

$$G^{\text{ab}} = \frac{G}{[G, G]}$$

Proposition 3.4.5

A group G is abelian if and only if $G = G^{\text{ab}}$.

Proof. It suffices to show that G is abelian if and only if $[G, G] = 1$. We know that if G is abelian, then every commutator reduces to

$$[g, h] = ghg^{-1}h^{-1} = ghh^{-1}g^{-1} = 1$$

so $[G, G] = 1$. Now suppose that $[G, G] = 1$. Then this implies that $[g, h] = ghg^{-1}h^{-1} = 1$ which shows that $gh = hg$ for any $g, h \in G$. Thus G is abelian. □

Definition 3.4.6: Perfect Groups

A group is perfect if $G = [G, G]$.

4 The Theory of Abelian Groups

4.1 Finite Abelian Groups

Definition 4.1.1: Finite Abelian Groups

A group G is said to be a finite abelian group if it is finite and abelian.

Lemma 4.1.2

Let G be a finite abelian group of order n. If p is a prime that divides n, then G contains an element of order p.

Lemma 4.1.3

A finite abelian group is a p group if and only if the order of every element is a power of p.

Lemma 4.1.4

Let G be a finite abelian group. Let H be a subgroup of G. Then there exists a complement K such that $G = H \times K$.

Lemma 4.1.5

Let G be a finite abelian p group and suppose that $g \in G$ is an element in G with the highest order. Then G is isomorphic to $\langle g \rangle \times H$ for some subgroup H of G.

Theorem 4.1.6: The Fundamental Theorem for Finite Abelian Group

Let G be a finite abelian group. Then G can be decomposed into

$$G \cong \mathbb{Z}/k_1\mathbb{Z} \times \cdots \times \mathbb{Z}/k_u\mathbb{Z}$$

in one of the following canonical forms:

- $k_{i+1}|k_i$ for $1 \leq i \leq u-1$
- $k_1, \ldots, k_u$ are powers of primes that are not necessarily distinct

4.2 Finitely Generated Abelian Groups

Definition 4.2.1: Finitely Generated Abelian Groups

A group G is said to be finitely generated abelian if it is finitely generated and abelian.

Lemma 4.2.2

Let A be a subset of an abelian group $(G, +)$. Then

$$\langle A \rangle = \left\{ \sum_{g \in A} k_g \cdot g | k \in \mathbb{Z} \right\}$$

Proof. Using the above proposition and the fact that G is abelian means that we only need one copy of g in the sum (compare this to the nonabelian case). □

Lemma 4.2.3

Every finite abelian group is finitely generated.

Proposition 4.2.4

Subgroups of a finitely generated abelian group is finitely generated.

Proof. Let $H \leq G$. We prove by induction on n that H can be generated by at most n elements. If $n = 1$, then G is cyclic. Then $G = \{kx | k \in \mathbb{Z}\}$. Let m be the smallest positive number such that $mx \in H$. If m does not exists then $K = \{0\}$ and we are done. Otherwise, $\{k(mx) | k \in \mathbb{Z}\} \subseteq H$. We now prove the reverse inclusion. Write $tx = (qm + r)x \in G$ with $0 \leq r < m$. Then $tx \in H$ if and only if $rx = (t - qm)x \in H$. But this is true if and only if $r = 0$ since m is already the smallest number such that $mx \in H$. Thus $H \subseteq \{k(mx) | k \in \mathbb{Z}\}$ and H is cyclic.

Now suppose that the induction hypothesis is true for $n - 1$. Let K be the subgroup generated by $x_1, \ldots, x_{n-1}$. By induction, $H \cap K$ is generated by $y_1, \ldots, y_{m-1}$ with $m \leq n$. If $H \leq K$, then $H = H \cap K$ and we are done.

Suppose that H is not a subgroup of K. Then there exists elements of the form $k + tx_n \in H$ with $k \in K$ and $t > 0$. Choose $y_m = h + tx_n$ with t minimal. I claim that H is generated by $y_1, \ldots, y_m$. Let $h \in H$. Then $h = k' + ux_n$ with $k' \in K$ and $u \in \mathbb{Z}$. If t does not divied u then we can write $u = tq + r$ with $q, r \in \mathbb{Z}$ and $0, r < t$. Then $k - qy_m = (h' - qh) + rx_n \in H$ thus contradicting minimality of t. Thus $t|u$ and hence $u = tq$ and $k - qy_m \in H \cap K$. But $H \cap K$ is generated by $y_1, \ldots, y_{m-1}$ thus we are done. □

4.3 Relation of with Free Abelian Groups

Lemma 4.3.1

Every free abelian group of finite rank is a finitely generated abelian group.

Theorem 4.3.2

A finitely generated abelian group is a free abelian group if and only if it is torison free.

In the case that a finitely generated abelian group G is a free abelian group of rank n, we say that G is free of rank n.

Recall that any subgroup of a finitely generated abelian group is finitely generated.

Theorem 4.3.3

Every finitely generated abelian group is the quotient group of a free abelian group.

Proof. If G is a finitely generated abelian group, it has a surjective homomorphism $\phi : \mathbb{Z}^n \to G$. Using the first isomorphism theorem, we have that

$$G = \text{im}(\phi) \cong \frac{\mathbb{Z}^n}{\ker(\phi)}$$

□

Definition 4.3.4: Presentations

Let G be a finitely generated abelian group given by the quotient of a free abelian group $\mathbb{Z}^n$ with $\ker(\phi) = \langle v_1, \dots, v_m \in \mathbb{Z}^m \rangle$. We represent G in the form

$$G = \frac{\mathbb{Z}^n}{\ker(\phi)} = \langle x_1, \dots, x_n | v_1, \dots, v_m \rangle$$

following the conventions of presentations on a general free group.

In particular, this representation means that $v_1 = 0, \dots, v_m = 0$ in $\mathbb{Z}^n$. The question remaining is to how to transform the kernel $\ker(\phi)$ into the generators $v_1, \dots, v_m \in \mathbb{Z}^n$.

Proposition 4.3.5

Let H be a subgroup of $\mathbb{Z}^n$. Then there exists a basis $B = \{b_1, \dots, b_n\}$ of $\mathbb{Z}^n$ such that

$$H = \langle d_1 b_1, \dots, d_m b_m \rangle$$

where $d_1, \dots, d_n \in \mathbb{N}$ and $d_i | d_{i+1}$ for $1 \leq i \leq m-1$.

Proposition 4.3.6

Let $\langle x_1, \dots, x_n | v_1, \dots, v_m \rangle$ be a finitely generated abelian group. Then there exists a set of relations such that this group can be rewritten into

$$\langle b_1, \dots, b_n | d_1 x_1, \dots, d_m x_m \rangle$$

where $d_1, \dots, d_n > 0$ and $d_i | d_{i+1}$ for $1 \leq i \leq m-1$.

Proof. Suppose that $G = \langle x_1, \dots, x_n | v_1, \dots, v_m \rangle = \frac{\mathbb{Z}^n}{K}$. Since K is a subgroup of $\mathbb{Z}^n$, we know that it is also a free group. □

4.4 Fundamental Theorem for Finitely Generated Abelian Groups

Theorem 4.4.1: Invariant Factor Decomposition

Let G be a finitely generated abelian group. Then G can be decomposed into

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z} \times \mathbb{Z}^r$$

where

- (free rank / Betti number) $r \geq 0$ and $n_j \geq 2$ for all j
- (invariant factors) $n_{i+1} | n_i$ for $1 \leq i \leq s-1$
- $|G| = n_1 \cdots n_s$

This expression is unqiue up to reordering of the external product.

Proof. Let G be a finitely generated abelian group. Denote the torsion subgroup of G by tG. Then G/tG is a torsion free abelian group and thus is free abelian. Thus we have that $G \cong tG \times G/tG$. Since tG is a finite abelian group, we can invoke the the fundamental theorem for finite abelian groups to get $tG \cong \mathbb{Z}/k_1\mathbb{Z} \times \cdots \times \mathbb{Z}/k_s\mathbb{Z}$. Since G/tG is free abelian, it is isomorphic to $\mathbb{Z}^r$ for some r. Combining the results gives our proof. □

Below is the Primary Decomposition of finite abelian groups.

Theorem 4.4.2: Primary Decomposition

Let G be a finitely generated abelian group. Then G can be decomposed into

$$G \cong \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_t\mathbb{Z} \times \mathbb{Z}^r$$

where

- $r \geq 0$ is the free rank of G
- $q_1, \ldots, q_t$ are powers of primes numbers that may not be unique.

This expression is unique up to reordering of the indices.

Theorem 4.4.3

Let G be a finitely generated abelian group represented by

$$\langle b_1, \ldots, b_n | d_1 b_1, \ldots, d_m b_m \rangle$$

Further suppose that G has invariant decomposition

$$\left(\bigoplus_{i=1}^{m} \mathbb{Z}/d_i'\mathbb{Z} \right) \oplus \mathbb{Z}^{n'-m'}$$

Then these two representations of G match up through their numbers. In particular,

- Up to reordering, we have $d_i = d_i'$
- $n = n'$ and $m = m'$

5 The Sylow Theorems and its Consequences

Lagrange's theorem leads to a natural question. Does the converse hold? That is, given a number k dividing $|G|$, is there a subgroup of G with order k? This is true for cyclic groups but in general it is not true. For example, if $|G|$ is a non-abelian finite simple group, then G has no subgroup of order $|G|/2$ because otherwise, this subgroup would be normal.

We then want sufficient criterion for the converse to hold. This leads to the Sylow theorems and its relation to p-groups.

5.1 The Four Sylow Theorems

We introduce a notation for subgroups of order a power of a prime.

Definition 5.1.1: Sylow p-groups

Let G be a group of order $p^k m$ where $\gcd(p, m) = 1$, then subgroups of G of order p^k is called a Sylow p-subgroup of G. The set of all Sylow p-subgroups of G is denoted

$$\text{Syl}_p(G) = \{H \leq G \mid H \text{ is a Sylow } p\text{-subgroup } \}$$

and the number of Sylow p-subgroups is denoted

$$n_p(G) = \left|\text{Syl}_p(G)\right|$$

The maximal power of the prime p that divides $|G|$ is also called the p-part of G. This is denoted as $|G|_p$. Before we prove the main theorems of the section, we need a lemma.

Lemma 5.1.2

Let p be prime. Let $n, m \in \mathbb{N}$ such that $\gcd(m, p) = 1$. Then the following are true.

- p divides $\binom{p}{i}$ for all $1 \leq i \leq p-1$
- $\binom{p^n m}{p^n} \equiv m \pmod{p}$

Proof.

- By definition, we have that

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-(i-1))}{i(i-1)\cdots 2 \cdot 1}$$

  Let $a = (p-1)\cdots(p-(i-1))$ and $b = i!$ so that $\binom{p}{i} = \frac{pa}{b}$. Since b is the product of integers less than p, all prime divisors of b are less than p. Thus p does not divide a. We have that $b\binom{p}{i} = pa$. Since $\binom{p}{i}$ is an integer, and p does not divide b, p must divide $\binom{p}{i}$.

- Denote $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Consider the polynomial ring $\mathbb{F}_p[x]$ and $(1+x)^p \in \mathbb{F}_p[x]$. By the binomial theorem, we have that

$$\begin{aligned}(1+x)^p &= \sum_{i=0}^{p} \binom{p}{i} x^i \\ &= \binom{p}{0} + \binom{p}{p} x^p \\ &= 1 + x^p\end{aligned}$$

A similar calculation also shows that $(1+x)^{p^n} = 1 + x^{p^n}$. Thus

$$(1+x)^{p^n m} = (1+x^{p^n})^m$$

Using the binomial theorem on both sides, we get

$$\sum_{i=0}^{p^n m} \binom{p^n m}{i} x^i = \sum_{j=0}^{m} \binom{m}{j} x^{p^{n^j}}$$

Comparing coefficients give

$$\binom{p^n m}{p^n j} \equiv \binom{m}{j} \pmod{p}$$

Applying the result with $j = 1$ proves the lemma.

Thus we are done. □

The four Sylow theorems is due to Ludwig Sylow. It is an important corner stone in finite group theory.

Theorem 5.1.3: The First and Second Sylow Theorems

Let G be a finite group and $|G| = p^k m$ where $\gcd(p, m) = 1$. Then the following are true.

- There exists at least one Sylow p-subgroup of G.
- $n_p(G) \equiv 1 \pmod{p}$

Proof. We first prove that $n_p(G) \equiv 1 \pmod{p}$. Let G be a finite group and $|G| = p^k m$ where $\gcd(p, m) = 1$. Define

$$X = \{S \subset G \mid |S| = p^n\}$$

Then $|X| = \binom{p^n m}{p^n}$ and thus $|X| \equiv m \pmod{p}$ by the above lemma. Notice that p does not divide $|X|$.

Consider the action of G on X by left multiplication. If $S \in X$, define

$$g \cdot S = gS = \{gs \mid s \in S\}$$

Clearly this is a group action. We know that $\{\text{Orb}_G(S) | S \in X\}$ partitions X. In other words, there exists $S_1, \ldots, S_r \in X$ such that

$$X = \coprod_{i=1}^{r} \text{Orb}_G(S_i)$$

and thus $|X| = \sum_{k=1}^{r} |\text{Orb}_G(S_i)|$.

Since we know that p does not divide $|X|$, there must exists at least one of the orbits with $|\text{Orb}_G(S_i)|$ is not divisible by p. Let t be the number of orbits that have order indivisible by p. Without loss of generality, reorder the orbits such that $|\text{Orb}_G(S_i)|$ is not divisible by p for $1 \leq i \leq t$ and $p \mid |\text{Orb}_G(S_i)|$ for $t+1 \leq i \leq r$.

We now prove two claims.
Claim 1: Fix $1 \leq i \leq t$. Then there exists $x_i \in G$ such that $\text{Stab}_G(x_i S_i) = x_i S_i$. In particular, $\text{Stab}_G(x_i S_i) \in \text{Syl}_p(G)$ for each $1 \leq i \leq r$.
Take $1 \leq i \leq t$. Let $s_i \in S_i$ and take $x_i = s_i^{-1}$. Let $T_i = x_i S_i$. Then $1_G \in T_i$. By definition of orbits, we have $\text{Orb}_G(T_i) = \text{Orb}_G(S_i)$. By the orbit stabilizer theorem, we have that p does

not divide $|O_{T_i}| = [G : \text{Stab}_G(T_i)]$. Since $|G| = p^n m = [G : \text{Stab}_G(T_i)]|\text{Stab}_G(T_i)|$, we have that $p^n || \text{Stab}_G(T_i)|$. On the other hand, if $g \in \text{Stab}_G(T_i)$, then $gT_i = T_i$ by definition. Since $1_G \in T_i$, we have that $g \in gT_i = T_i$ and thus $\text{Stab}_G(T_i) \subseteq T_i$. Since $|T_i| = p^n \leq |\text{Stab}_G(T_i)|$, we deduce that $\text{Stab}_G(T_i) = T_i$ as required.

Claim 2: $t = \left|\text{Syl}_p(G)\right|$.
Define a map $f : \{\text{Orb}_G(T_i) | 1 \leq i \leq t\} \to \text{Syl}_p(G)$ by $f(\text{Orb}_G(T_i)) = T_i$. By claim 1, we know that T_i is a subgroup of G of order p^n since $T_i = \text{Stab}_G(T_i)$, so this map is well defined. We prove that f is a bijection.
Injectivity: Let $1 \leq i, j \leq t$. Suppose that $T_i = T_j$. Then

$$\text{Orb}_G(S_i) = \text{Orb}_G(T_i) = \text{Orb}_G(T_j) = \text{Orb}_G(S_j)$$

so $S_i = S_j$ since we have chosen $S_1, \leq, S_r$ so that their orbits are distinct.
Surjectivity: Let $p \in \text{Syl}_p(G)$. Then $P \in X$, and $\text{Stab}_G(P) = P$. It follows that p does not divide $m = [G : P] = [G : \text{Stab}_G(P)] = |\text{Orb}_G(P)|$, so $\text{Orb}_G(P) = \text{Orb}_G(T_i)$ for some i. Since $1_G \in T_i$, and $\text{Orb}_G(T_i) = \{xS_i \mid x \in G\}$, T_i is the unique element of $\text{Orb}_G(T_i)$ containing 1_G. Thus we must have $P = T_i = f(\text{Orb}_G(T_i))$ as required.

We resume the proof of the second Sylow theorem. Since we know that $|X| \equiv m \pmod p$, and that

$$|X| \equiv \sum_{i=1}^{r} |\text{Orb}_G(T_i)| \pmod p$$

Since $|\text{Orb}_G(T_i)| = [G : \text{Stab}_G(T_i)] = |G|/|T_i| = m$ by claim 1, and $t = \left|\text{Syl}_p(G)\right|$ by claim 2. From the above sum we deduce that

$$m \equiv m n_p(G) \pmod p$$

Since we also have that $\gcd(m, p) = 1$, we can cancel m on both sides to get $n_p(G) \equiv 1 \pmod p$. This also proves the first Sylow theorem. □

Proposition 5.1.4

Let G be a group and p a prime divisor of $|G|$. Let $H \leq G$ and let P be a Sylow p-subgroup of G. Then there exists some $g \in G$ such that $H \cap gPg^{-1}$ is a Sylow p-subgroup of H.

Proof. Consider the set $X = \{xP | x \in G\}$ of left cosets of P in G. Then G acts on X by left multiplication and thus H acts on X. For any $xP \in X$, we have that

$$\begin{aligned}
\text{Stab}_H(xP) &= \{h \in H | hxP = xP\} \\
&= \{h \in H | x^{-1}hxP = xP\} \\
&= \{h \in H | h \in xPx^{-1}\} \\
&= H \cap xPx^{-1}
\end{aligned}$$

Since P is a Sylow p-subgroup of G, $|X| = [G : P]$ is coprime to p. Let $\text{Orb}_H(x_1P), \ldots, \text{Orb}_H(x_sP)$ denote the distinct orbits of H in its action on X. We know that $|X| = \sum_{i=1}^{s} |\text{Orb}_H(x_iP)|$ If every such orbit has size divisible by p, then $|X|$ would be divisible by p, which is a contradiction. Thus there exists $x_i \in G$ such that p does not divide $|\text{Orb}_H(x_iP)|$.

We know that $\text{Stab}_H(x_iP) = H \cap x_iPx_i^{-1}$ is a p-subgroup since it is a subgroup of $x_iPx_i^{-1}$. We also have $[H : \text{Stab}_H(x_iP)] = |\text{Orb}_H(x_iP)|$ is not divisible by p. Thus $H \cap x_iPx_i^{-1}$ is a Sylow p-subgroups of H. Thus we are done. □

Theorem 5.1.5: The Third and Fourth Sylow Theorems

Let G be a finite group and $|G| = p^k m$ where $\gcd(p, m) = 1$. Then the following are true.

- Every Sylow p-subgroup is conjugate to each other
- Any p-subgroup of G is contained in a Sylow p-subgroup of G

Proof.

- Let P and Q be Sylow p-subgroups of G. By the above proposition, there exists $g \in G$ such that $Q \cap gPg^{-1}$ is a Sylow p-subgroup of Q. But $|Q|$ is a power of p and thus $\text{Syl}_p(Q) = \{Q\}$. Thus $Q = Q \cap gPg^{-1}$. Since also $|Q| = \left|gPg^{-1}\right|$ we have $Q = gPg^{-1}$.
- Let H be a Sylow p-subgroup of G and P a Sylow p-subgroup of G. By the above proposition, there exists $g \in G$ such that $H \cap gPg^{-1}$ is a Sylow p-subgroup of H. But $|H|$ is a power of p and thus $\text{Syl}_p(H) = \{H\}$. Thus $H = H \cap gPg^{-1} \leq gPg^{-1}$.

Thus we are done. □

5.2 Consequences of the Sylow Theorems

Corollary 5.2.1

Let G be a finite group. Let p be prime such that $|G| = p^k m$ with $\gcd(p, m) = 1$. Let $P \in \text{Syl}_p(G)$ be a Sylow p-subgroup. Then the following are true with respect to $n_p(G)$.

- $n_p(G) = [G : N_G(P)]$
- $n_p(G)|m$
- $P \trianglelefteq G$ if and only if $n_p(G) = 1$

Proof.

- By the third Sylow theorem, we know that G acts on $\text{Syl}_p(G)$ by conjugation and that $\text{Orb}_G(P) = \text{Syl}_p(G)$. The stabilizer $\text{Stab}_G(P)$ is thus equal to the normalizer $N_G(P)$. Using the orbit stabilizer theorem, we have that
$$\left|\text{Syl}_p(G)\right| = |\text{Orb}_G(P)| = [G : \text{Stab}_G(P)] = [G : N_G(P)]$$
- We know that P is a subgroup of $N_G(P)$. This means that we can apply Lagrange's theorem to get $|N_G(P)| = |P| \cdot [N_G(P) : P]$. Thus we have that
$$\begin{aligned}\left|\text{Syl}_p(G)\right| &= [G : N_G(P)] \\ &= \frac{|G|}{|N_G(P)|} \\ &= \frac{|G|}{|P| \cdot [N_G(P) : P]}\end{aligned}$$
Thus $\left|\text{Syl}_p(G)\right|$ divides $\frac{|G|}{|P|} = m$
- We have that P is a normal subgroup of G if and only if $N_G(P) = G$. And this is true if and only if $\left|\text{Syl}_p(G)\right| = 1$ by the first item.

Thus we are done. □

Proposition 5.2.2

There are no simple groups of order 20.

Proof. Let G be a group of order 20. Then $|G| = 2^2 \cdot 5$. By Sylow theorem 2, we know that $n_5(G) \equiv 1 \pmod 5$. By corollary 5.2.1, we have that $n_5(G)$ divides $\frac{|G|}{|P|} = \frac{20}{5} = 4$ and thus $n_5(G) = 1$. By the same corollary, we know that the unique Sylow 5-subgroup is normal. Thus G cannot be simple. □

Proposition 5.2.3

There are no simple groups of order 48.

Proof. Let G be a group of order 48. Then $|G| = 2^4 \cdot 3$. Consider $n_2(G)$. By the second Sylow theorem, we have that $n_2(G) \cong 1 \pmod 2$. By corollary 5.2.1, we have that $n_2(G)|3$ and thus $n_2(G) = 1$ or 3.

Suppose that $n_2(G) = 1$. Then by the same corollary, we have a unique Sylow 2-subgroup

that is normal to G. Thus G is not simple.

Suppose that $n_2(G) = 3$. Then G acts on $\text{Syl}_2(G)$ non-trivially. Then we know that there is a homomorphism $\phi : G \to S_3$. The first isomorphism theorem and Lagrange's theorem tells us that $\frac{|G|}{|\ker(\phi)|} = |\text{im}(\phi)|$. $\text{im}(\phi)$ is a subgroup of S_3 whose order is greater than 1 since ϕ is non-trivial. Thus $1 \leq |\text{im}(\phi)| \leq 6$ and thus $48/6 \leq |\ker(\phi)| < 48$. Thus $\ker(\phi)$ is a non-trivial normal subgroup of G and thus G is not simple. □

5.3 Simplicity of A_n for $n \geq 5$

Using the Sylow theorems, we can also analyzes the number of elements that possess a power of prime order. For a finite group G, define

$$F_p(G) = \{x \in G \mid x \neq 1 \text{ and } |x| = p^n \text{ for some } n\}$$

to be the number of elements in G that has its order the power of a prime p. We can deduce a number of information from the Sylow theorems, so that we can eventually some sort of contradiction in our proof of simplicity.

Corollary 5.3.1

Let G be a finite group such that $|G| = p^k m$ where p is a prime and $\gcd(p, m) = 1$. Let

$$F_p(G) = \{x \in G \mid x \neq 1 \text{ and } |x| = p^n \text{ for some } n\}$$

Then the following are true.

- $F_p(G) = \bigcup_{P \in \text{Syl}_p(G)} (P \setminus \{1\})$
- $|F_p(G)| \geq p^k - 1$ with equality if and only if $\left|\text{Syl}_p(G)\right| = 1$
- If $k = 1$ then $|F_p(G)| = \left|\text{Syl}_p(G)\right| \cdot (p - 1)$

Proof.

- First let $x \in F_p(G)$. Then $\langle x \rangle$ has a prime power order and so is a p-subgroup of G. Any p-subgroup is contained in a Sylow p-subgroup and so x lies in $\bigcup_{P \in \text{Syl}_p(G)} (P \setminus \{1\})$. Now if y lies in the union of the Sylow p-subgroups, then $\langle y \rangle$ is a subgroup of some Sylow p-subgroup. By Lagrange's theorem, the order of y must be a power of p since any Sylow p-subgroup has prime power order. Thus $y \in F_p(G)$.
- From the above characterization of $F_p(G)$, we have that $F_p(G) \supseteq (P \setminus \{1\})$ for any Sylow p-subgroup. Thus $|F_p(G)| \geq p^k - 1$. Now suppose that equality holds. Suppose for a contradiction that there are two distinct Sylow p-subgroups P and Q. This means that there exists an element in Q not contained in P. Hence $|F_p(G)| \geq |P \setminus \{1\}| + 1 = p^k$, this contradicts the assumption of equality. It is also clear that if $n_p(G) = 1$ then $|F_p(G)| = p^k - 1$.
- Firstly notice that when $k = 1$, we have that the first property in this corollary is a disjoint union. Indeed, if P_i and P_j are Sylow p-subgroups that intersect with element $x \in P_i \cap P_j$, then $\langle x \rangle$ has order p so that $P_i = \langle x \rangle = P_j$.

  We will now show that

$$F_p(G) = \coprod_{P \in \text{Syl}_p(G)} (P \setminus \{1\})$$

If $x \in F_p(G)$, then x has order p so that $\langle x \rangle$ is a Sylow p-subgroup and $x \in \langle x \rangle \subseteq \coprod_{P \in \text{Syl}_p(G)} (P \setminus \{1\})$. Now suppose that y is an element that lies in the coproduct. Then y lies in some Sylow p-subgroup. Any Sylow p-subgroup is cyclic and isomorphic to C_p since $k = 1$. Thus y has order p and $y \in F_p(G)$. Now $|F_p(G)| = \left|\text{Syl}_p(G)\right|(p-1)$ and so we conclude.

This completes the proof. □

Lemma 5.3.2

Let G be a finite group such that $|G| = p^k m$ where p is a prime and $\gcd(p, m) = 1$. Let

$$F_p(G) = \{x \in G | x \neq 1 \text{ and } |x| = p^n \text{ for some } n\}$$

Let N be a normal subgroup of G. Then the following are true.

- If $x \in N$, then $\{gxg^{-1} \mid g \in G\} \subseteq N$
- If p does not divide n, then $\text{Syl}_p(G) = \text{Syl}_p(N)$ and $F_p(G) = F_p(N)$.

Proposition 5.3.3

The alternating group A_5 is simple.

Proof. Suppose that there exists N a non-trivial normal subgroup of A_5. By Lagrange's theorem, $|N|$ divides $|A_5| = 60$ and thus at least one of the prime divisors are either $2, 3$ or 5.

The 5-cycles of A_5 are precisely elements of A_5 with order 5. Since each 5-cycle is of the form $(a_1 \quad \cdots \quad a_5)$, there are 5 possible choices for a_1, 4 for a_2 and so on. Since also that moving elements transitively along the cycle gives another presentation of the same cycle, we divide by 5 to obtain that there are precisely 24 elements of order 5 of A_5. A similar argument show that A_5 has 20 elements of order 3.

The only elements of order 2 are products of two disjoint transpositions. A similar argument shows that there are 15 of them. We know that they are part of the same conjugacy class in A_5.

Case 1: Either 3 divides $|N|$ or 5 divides $|N|$.
Let $p = 3$ or 5 such that p divides $|N|$. Then we know that p does not divide $[G : N]$ so by the above theorem we deduce that $F_p(G) = F_p(N)$. If $p = 5$ then $F_p(N) = 24$ and thus $|N| \geq 25$. Since $|N| \mid 60$ this implies that $|N| = 30$. If $p = 3$ then $F_p(N) = 20$ and thus $|N| \geq 21$. Since $|N| \mid 60$ we thus have $|N| = 30$. If either 3 divides $|N|$ or 5 divides $|N|$ then both 3 and 5 divides $|N|$. But $F_3(N) + F_5(N) > |N|$, a contradiction.

Case 2: Neither 3 or 5 divides $|N|$.
Then $|N|$ divides 4 by Lagrange's theorem. By Cauchy's theorem, there exists $x \in N$ of order 2. Thus using the above corollary, we have that $4 = |N| \geq \text{Cl}(x) = 15$ which is a contradiction. □

Lemma 5.3.4

Let $n \geq 3$. Let X be the set of 3-cycles in S_n. Then $A_n = \langle X \rangle$.

Proof. By definition, we know that A_n is consists of elements of an even number of

transpositions. We just have to show that every product of a pair of transpositions can be written as a product of 3-cycles. Let $(a \quad b)$ and $(c \quad d)$ be a pair of transpositions for $a, b, c, d \in \{1, \ldots, n\}$ with $a \neq b$ and $c \neq d$. There are three cases.

Case 1: $\{a, b\} \cap \{c, d\} = \emptyset$.
Then the two cycles are disjoint. By direct calculation, we have that

$$(a \quad b)(c \quad d) = (a \quad b \quad c)(b \quad c \quad d)$$

and so we are done.

Case 2: $|\{a, b\} \cap \{c, d\}| = 1$.
Without loss of generality assume that $a = c$. Then

$$(a \quad b)(a \quad d) = (a \quad d \quad b)$$

and so we are done.

Case 3: $|\{a, b\} \cap \{c, d\}| = 2$.
Then $(a \quad b)^2 = () = (a, b, e)^3$ for any $e \in \{1, \ldots, n\} \setminus \{a, b, c, d\}$ and so we conclude. □

Lemma 5.3.5

Let $n \geq 5$. Then any two 3-cycles are conjugate in A_n.

Proof. We know that gfg^{-1} has the same cycle type as f for $f, g \in S_n$. Let X be the set of 3-cycles in S_n. Then A_n acts on X by conjugation. By the above lemma, the group action is transitive so that it has only one orbit. □

Lemma 5.3.6

Let $n \geq 5$. Let $\sigma \in A_n$ be a non-trivial element. Then for any conjugate τ of σ, there exists $si \in \{1, \ldots, n\}$ such that $\tau(i) = \sigma(i)$.

Proof. Let r be the longest length of a disjoint cycle in σ. Relabelling if necessary, we have that

$$\sigma = (1 \quad 2 \quad \cdots \quad r)\,\pi$$

where π and $(1 \quad 2 \quad \cdots \quad r)$ are disjoint permutations. If $r \geq 3$. Let $\gamma = (3 \quad 4 \quad 5)$ and $\tau = \gamma\sigma\gamma^{-1}$. Clearly $\tau \neq \sigma$ since $\sigma(3) = 4$ and $\tau(3) = 6$. But $\sigma(1) = 2 = \tau(1)$ and so we are done.

If $r = 2$, then σ is a product of two disjoint transpositions. If there are at least 3 disjoint transpositions, then $n \geq 6$ and after relabelling we can write $\sigma = (1 \quad 2)(3 \quad 4)(5 \quad 6)\cdots$. Let $\gamma = (1 \quad 3 \quad 2)$ and set $\tau = \gamma\sigma\gamma^{-1}$. Clearly $\tau \neq \sigma$. We also have $\sigma(5) = 5 = \tau(5)$ and so we conclude. □

Theorem 5.3.7

The alternating group A_n for $n \geq 5$ is simple.

Proof. We know that A_5 is simple. So suppose that $n \geq 6$. Recall that A_n acts on $X_n = \{1, \ldots, n\}$, inherited by the action of S_n. For each $i \in X_n$, we have that $\mathrm{Stab}_{A_n}(i) \cong A_{n-1}$. We proceed by induction. The case $n = 5$ is clear. So suppose that A_{n-1}

is simply. By induction, $\text{Stab}_{A_n}(i)$ is a simple group. Notice that it also contains a 3-cycle.

Assume there exists a non-trivial proper normal group N of A_n. Let $\sigma \in N$ be a non-trivial element of N. By the above lemma, there exists a conjugate $\tau \in A_n$ of σ such that $\tau \neq \sigma$ but $\sigma(i) = \tau(i)$ for some $i \in X_n$. Since $N \trianglelefteq A_n$, $\tau \in N$. Hence $\sigma^{-1}\tau \in N$ and $\sigma^{-1}\tau \neq 1_{A_n}$ and $\sigma^{-1}\tau(i) = i$. Thus $\sigma^{-1}\tau \in \text{Stab}_{A_n}(i)$ and so $N \cap \text{Stab}_{A_n}(i) \neq \{1_{A_n}\}$. N being normal to A_n implies that

$$N \cap \text{Stab}_{A_n}(i) \trianglelefteq \text{Stab}_{A_n}(i)$$

Since $\text{Stab}_{A_n}(i)$ is simple, we have $N \cap \text{Stab}_{A_n}(i) = \text{Stab}_{A_n}(i)$ so that $\text{Stab}_{A_n}(i) \leq N$. But $\text{Stab}_{A_n}(i)$ contains a 3-cycle and thus so does N. By lemma 5.3.4, N contains all 3-cycles of A_n. By lemma 5.3.3, $N = A_n$ which is a contradiction. Thus we conclude. □

In fact, we can show that A_5 is the unique simple group of order 60. We will prove this once we classified small groups.

6 Classification of Groups of Order up to 16

6.1 Collection of Useful Results

Lemma 6.1.1

Let G be a group such that $g^2 = 1$ for all $g \in G$. Then G is abelian.

Proof. For $g, h \in G$, we have that

$$gh = g^{-1}h^{-1} = (hg)^{-1} = hg$$

and so we conclude. □

Recall the following result from groups and rings.

Proposition 6.1.2

Let G be a group and $a, b \in G$ such that a, b commutes. If furthermore $\langle a \rangle \cap \langle b \rangle = \{1\}$, then

$$|ab| = \operatorname{lcm}(|a|, |b|)$$

Proof. Let $n = |ab|$. Since a and b commute, we have that

$$1 = (ab)^n = a^n b^n$$

so that $a^n = b^{-n}$. Thus $a^n \in \langle b \rangle$. But $a^n \in \langle a \rangle \cap \langle b \rangle = \{1\}$ implies that $a^n = 1$. Similarly, we have that $b^n = 1$. This means that we have $|a|, |b|$ divides n. and thus $\operatorname{lcm}(|a|, |b|)$. We know from groups and rings that $|ab|$ divides $\operatorname{lcm}(|a|, |b|)$ and so we conclude. □

Definition 6.1.3: Inversion Homomorphism

The inversion homomorphism between two subgroups H and K of G is the homomorphism

$$\phi : H \to \operatorname{Aut}(K)$$

defined by $\phi_1(k) = k$ and $\phi_h(k) = k^{-1}$ for $h \neq 1$.

Lemma 6.1.4: Fitting's Lemma

Let G be a finite group. Suppose that $K \trianglelefteq G$ is abelian with odd order $\frac{|G|}{2}$. Let $H = \langle x \rangle \in \operatorname{Syl}_2(G)$. Define

$$[K, x] = \langle [v, x] \mid v \in K \rangle$$

Then the following are true.

- $xax^{-1} = a^{-1}$ for all $a \in [K, x]$
- $K = C_K(x) \times [K, x]$
- $G \cong (H \ltimes_\phi [K, x]) \times C_K(x)$ where $\phi : H \to \operatorname{Aut}(K)$ is the inversion homomorphism.

Proof.

- Since K is normal, $[K, x]$ is contained in K. Moreover, since K is abelian, we have that $xax^{-1} = a^{-1}$ for $a \in [K, x]$ if and only if $xax^{-1} = a^{-1}$ for all a in the generating set of

$[K,x]$. So it suffices to prove that $x[v,x]x^{-1} = [v,x]^{-1}$ for all $v \in K$. But we have

$$x(vxv^{-1}x^{-1})x = xvxv^{-1} = [v,x]^{-1}$$

since $x = x^{-1}$ and so we are done.

- Define $f : K \to [K,x]$ by $f(k) = [k,x]$ for $k \in K$. Then

$$\begin{aligned} f(k_1k_2) &= k_1k_2xk_2^{-1}k_1^{-1}x^{-1} \\ &= k_1k_2xk_2^{-1}x^{-1}xk_1^{-1}x^{-1} \\ &= k_1k_2(xk_2^{-1}x^{-1})(xk_1^{-1}x^{-1}) \\ &= k_1(xk_2^{-1}x^{-1})k_2(xk_1^{-1}x^{-1}) && (K \text{ is abelian}) \\ &= [k_1,x][k_2,x] \\ &= f(k_1)f(k_2) \end{aligned}$$

Thus f is a homomorphism. Clearly $\ker(f) = C_K(x)$. Also since $\mathrm{im}(f)$ is a subgroup of $[K,x]$ and contains a generating set for $[K,x]$, we have $\mathrm{im}(f) = [K,x]$. Thus by the first isomorphism theorem, we have that

$$|K| = |\ker(f)||\mathrm{im}(f)| = |C_K(x)||[K,x]|$$

Thus $K = C_K(x)[K,x]$. Since K is abelian, we have that $K = C_K(x) \times [K,x]$ and so we conclude.

- Step 1: $[K,x] \trianglelefteq G$.
Notice that $G = \langle x \cup K \rangle$. We just have to show that every element in the generating set normalizes $[K,x]$. By the first part of this lemma, it is easy to see that x normalizes $[K,x]$. Since K is abelian, K also normalizes $[K,x]$. Thus we are done.

□

6.2 The Dihedral Groups

Definition 6.2.1: The Dihedral Group

Let $X = \{1, \dots, n\}$ for $n \geq 3$. Define

$$\sigma = \begin{pmatrix} 1 & \cdots & n \end{pmatrix} \in \mathrm{Sym}(X) \quad \text{and} \quad \tau = \prod_{i=1}^{\lfloor n/2 \rfloor} \begin{pmatrix} i & n-i+1 \end{pmatrix} \in \mathrm{Sym}(X)$$

Define the dihedral group to be

$$D_{2n} \cong \langle \sigma, \tau \rangle$$

In particular, D_{2n} is a subgroup of $\mathrm{Sym}(X)$.

Proposition 6.2.2

Let $n \geq 3$. Then $D_{2n} \cong \langle a, b \mid a^n, b^2, ab = ba^{-1} \rangle$

Proposition 6.2.3

Let $n \geq 3$. Then $|D_{2n}| = 2n$.

Proposition 6.2.4

Let $n \geq 3$. Write $D_{2n} = \langle \sigma, \tau \rangle$. Then $\langle \sigma \rangle$ is a normal subgroup of D_{2n}.

With the inversion homomorphism, the following proposition shows that D_{2n} can be decomposed into a semidirect product.

Proposition 6.2.5

Let $\sigma = \begin{pmatrix} 1 & \cdots & n \end{pmatrix} \in S_n$ and $\tau = \prod_{i=1}^{\lfloor n/2 \rfloor} \begin{pmatrix} i & n-i+1 \end{pmatrix} \in S_n$. Write $K = \langle \sigma \rangle$ and $H = \langle \tau \rangle$. Then

$$D_{2n} \cong H \ltimes_\phi K$$

where $\phi : H \to \text{Aut}(K)$ is the inversion homomorphism.

Proof. It is clear that $|\tau| = 2$ and $|\sigma| = n$ and $D_{2n} = K \amalg \tau K$. This implies that $G = HK$ and $H \cap K = \{1\}$. Hence $G \cong H \ltimes_\phi K$ where $\phi : \{1, \tau\} \to \text{Aut}(K)$ is given by $\phi_1(k) = k$ and $\phi_\tau(k) = k^{-1}$. □

Theorem 6.2.6

Let G be a nonabelian finite group. Further suppose that

- G has a cyclic subgroup of K of order $n = \frac{|G|}{2}$
- $G \setminus K$ contains an element of G of order 2
- If $i \in \{0, \ldots, n-1\}$ satisfies $i^2 \equiv 1 \pmod{n}$ implies $i \equiv \pm 1 \pmod{n}$

Then $G \cong D_{2n}$.

Proof. Let G be a group satisfying the above requirements. Then K is a normal subgroup of G. Let x be an element of $G \setminus K$ of order 2. Let $H = \langle x \rangle$. Then $H \cap K = \{1_G\}$. This implies that $|HK| = |H||K| = 2p = |G|$. Thus have that $G = HK$. Let $\phi : H \to \text{Aut}(K)$ be the homomorphism defined by $\phi_h(k) = hkh^{-1}$ for each $h \in H$. Then from groups and rings theorem 5.3.5 we have that

$$G \cong H \ltimes_\phi K$$

The next step is to show that $\phi_h(k) = k^{-1}$ for all $k \in K$. Write $K = \langle y \rangle$ where $|y| = n$. Then $xyx^{-1} = y^i$ for some $0 \leq i < n$. This means that

$$\begin{aligned} y &= x^2 y x^{-2} && (x^2 = 1) \\ &= x y^i x^{-1} \\ &= (xyx^{-1})^i \\ &= y^{i^2} \end{aligned}$$

It follows that $y^{i^2-1} = 1_G$. Since $n = |y|$ we have that $i \equiv \pm 1 \pmod{n}$. Since $0 \leq i < n$, we have that $i = 1$ or $n-1$. If $i = 1$, then $xyx^{-1} = y$ means that G is abelian, which is a contradiction. So we must have $xyx^{-1} = y^{-1}$. Thus the homomorphism ϕ_h is given by $\phi_1(k) = k$ and $\phi_h(k) = k^{-1}$ for all $k \in K$.

By the above proposition, we must have $G \cong H \ltimes_\phi K \cong D_{2n}$. □

Some particular integers satisfying the third condition above include

- If $n = 6$, then by inspection it is easy to see that $i^2 \equiv 1 \pmod{6}$ if and only if $i = 1$ or 5

- If $n = p$ a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field and has no zero divisor. We can then factorize the expression into $(i-1)(i+1) \equiv 0 \pmod{p}$ so that $i = 1$ or $p-1$.
- If $n = p^2$ a square of prime, the case $p = 2$ is obvious by inspection. Namely $i = 1$ or 3. If p is odd, p^2 divides $(i-1)(i+1)$. Notice that p cannot divide both $i+1$ and $i-1$ else p divides $i+1+i-1 = 2i$, which is a contradiction. So p divides either $i-1$ or $i+1$. Thus $i = 1$ or p^2-1.

These are examples of quadratic residues in number theory. Notice that the above examples all have two solutions. This is similar to the case where a quadratic can have at most two solutions.

6.3 Groups of Order p, p^2, $2p$, $2p^2$

In this section we classify all groups of order p, p^2, $2p$, $2p^2$, pq for p a prime. We also give some result on the case pq where p and q are distinct.

Proposition 6.3.1

If $|G| = p$ is prime, then $G \cong C_p$.

Proof. Let $1 \neq g \in G$. By Lagrange's theorem, $|g| | p$ and thus $|g| = p$ and $G = \langle g \rangle$. □

Proposition 6.3.2

If $|G| = p^2$ where p is prime, then $G \cong C_{p^2}$ or $G \cong C_p \times C_p$.

Proof. We know by proposition 6.1.1 that all groups of order p^2 are abelian. The results then follows by the fundamental theorem of finite abelian groups. □

Proposition 6.3.3

If $|G| = 2p$ with p an odd prime, then either $G \cong C_{2p}$ or $G \cong D_{2p}$.

Proof. Let G be a group of order $2p$. If G is abelian, then we must have $G \cong C_{2p}$ by the fundamental theorem of finite abelian groups. Now assume that G is non-abelian. Let $P \in \text{Syl}_p(G)$. Since $\left|\text{Syl}_p(G)\right|$ divides $\frac{|G|}{|P|} = 2$ by corollary 5.2.1, together with $\left|\text{Syl}_p(G)\right| \equiv 1 \pmod{p}$, we must have that $\left|\text{Syl}_p(G)\right| = 1$. This means that P is a normal subgroup of G. Since p is odd, all elements of G of order 2 lies in $G \setminus P$. Now since $\mathbb{Z}/p\mathbb{Z}$ is a field, the only solutions to the equation $x^2 - 1$ in $\mathbb{Z}/p\mathbb{Z}$ are congruent to 1 modulo p. It then follows from theorem 6.2.3 that $G \cong D_{2p}$ as required. □

Definition 6.3.4: Generalized Dihedral Group

Let p be an odd prime. Let $H = C_2 = \langle x \rangle$ and let $K = C_p \times C_p$. Let $\phi : H \to \text{Aut}(K)$ be the inversion homomorphism. Define the generalized dihedral group of order $2p^2$ to be the semidirect product

$$\text{GD}_{2p^2} = H \ltimes_\phi K$$

Proposition 6.3.5

Let G be a group of order $2p^2$ where p is odd. Then G is isomorphic to one of the following groups:

- The cyclic group C_{2p^2}

- $C_p \times C_{2p}$
- $C_p \times D_{2p}$
- The dihedral group D_{2p^2}
- The generalized dihedral group GD_{2p^2}

Proof. Suppose that G is abelian. Then by the fundamental theorem of finite abelian groups, G is isomorphic to either C_{2p^2} or $C_{2p} \times C_p$. So suppose that G is not abelian. Let $K \in \mathrm{Syl}_p(G)$ and $H = \langle x \rangle \in \mathrm{Syl}_2(H)$ with $|x| = 2$. Then $|K| = p^2$, so $[G : K] = 2$ and that $K \trianglelefteq G$. By by proposition 6.2.2, we have that K is isomorphic to either C_{p^2} or $C_p \times C_p$.

Case 1: $K \cong C_{p^2}$.
It is clear that G now satisfies the first two conditions of theorem 6.1.3. It remains to show the last. Suppose that $i \in \{0, \ldots, p^2 - 1\}$ is such that $i^2 \equiv 1 \pmod{p^2}$. Then p^2 divides $(i-1)(i+1)$. Since p is odd, either p does not divide $i-1$ or p does not divide $i+1$. This means that either p^2 divides $i-1$ or p^2 divides $i+1$. Since $0 \leq i < p^2$, the only possibilities are either $i = 1$ or $i = p^2 - 1$, and so we conclude that

$$G \cong D_{2p^2}$$

in this case.

Case 2: $K \cong C_p \times C_p$.
In this case, G, satisfies all the conditions of Fitting's lemma so that

$$G \cong (H \ltimes_\phi K) \times C_K(x)$$

where ϕ is the inversion homomorphism. By Lagrange's theorem, we must have $|C_K(x)| = 1$ or p or p^2. However, since $G = \langle K \cup \{x\} \rangle$, we see that $C_K(x)$ cannot have order p^2. Otherwise, G would be abelian since K is abelian. Note that $|[K, x]| = \frac{|K|}{|C_K(x)|}$ by Fitting's lemma. There are now two cases.

Case 2(a): $|C_k(x)| = 1$.
We then have that $G \cong H \ltimes_\phi K$ since $[K, x] = K$ and $C_K(x) = \{1\}$. Combining the fact that $K \cong C_p \times C_p$, we have that

$$G \cong \mathrm{GD}_{2p^2}$$

Case 2(b): $|C_K(x)| = p$.
In this case, we have $|C_K(x)| = p = [K, x]$. Thus $H \ltimes_\phi [K, x]$ is a non-abelian group of order $2p$. Hence $H \ltimes_\phi [K, x] \cong D_{2p}$ by proposition 6.2.3. Since $C_K(x) \cong C_p$ by proposition 6.2.1, we deduce that

$$G \cong D_{2p} \times C_p$$

which completes the proof. □

Proposition 6.3.6

Let p and q be distinct primes with $p < q$ and p does not divide $q - 1$. Let G be a group of order pq. Then $G \cong C_{pq}$.

Proof. By corollary 5.2.1, we know that $n_p(G) | q$. By Sylow's theorem, we have that $n_p(G) \equiv 1 \pmod{p}$. If $n_p(G) = q$, then p divides $q - 1$ which is a contradiction. So $n_p(G) = 1$. By a similar argument and the fact that $q > p$, we have that $n_q(G) = 1$. Therefore we have

that G has a normal p-subgroup, say H and a normal q-subgroup, say K. By Lagrange's theorem, we must have that $H \cap K = \{1\}$. This means that $|HK| = |H||K|$. By proposition 5.2.5 in Groups and Rings, we have that $G = HK$. Hence we have that $G \cong H \times K$ by proposition 5.2.5 in Groups and Rings. Let x and y be generators of H and K respectively. Then x and y commute since $H \cap K = \{1\}$. So $|xy| = |x||y| = pq$ by proposition 1.1.9 in Groups and Rings. Thus $G = \langle x, y \rangle$. □

6.4 Groups of Order 4

The Klein Four Group is the only other group of order 4 that is not isomorphic to the cyclic group.

Definition 6.4.1: The Klein Four Group K_4

The Klein four group of order 4 is defined to be the group

$$K_4 = \{1, a, b, c\}$$

where multiplication is defined by $a^2 = b^2 = c^2 = 1$, $ab = ba = c$, $ac = ca = b$ and $bc = cb = a$.

Treating c in the definition as ab makes it easy to see that K_4 is in fact D_4 in disguise.

Lemma 6.4.2

The Klein four group K_4 is isomorphic to D_4 but not isomorphic to C_4.

6.5 Groups of Order 8

Definition 6.5.1: Quaternion Group

Let i, j, k be indeterminates and consider the set

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

together with a binary operation $\cdot : Q_8 \times Q_8 \to Q_8$ defined by

- $1 \cdot g = g \cdot 1 = 1$ and $(-1) \cdot g = g \cdot (-1) = -g$ for all $g \in Q_8$
- $i \cdot j = k$, $j \cdot k = i$ and $k \cdot i = j$
- $j \cdot i = -k$, $k \cdot j = -i$ and $i \cdot k = -j$
- $(\pm 1)^2 = 1$, $(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1$

Then $(Q_8, \cdot)$ is called the Quaternion group.

Proposition 6.5.2

The following are properties of the quaternion group Q_8.

- $Z(Q_8) = \{\pm 1\}$
- Q_8 has precisely 1 element of order 2, which is -1
- Q_8 has precisely 6 elements of order 4, which is $\pm i$, $\pm j$ and $\pm k$
- $Q_8 = \langle i, j \rangle = \langle j, k \rangle = \langle k, i \rangle$

Theorem 6.5.3

Any group of order 8 is isomorphic to one of the following groups:

- The Dihedral group D_8
- The Quaternion group Q_8
- The Cyclic group C_8
- $C_4 \times C_2$
- $C_2 \times C_2 \times C_2$

Proof. Let G be a group of order 8. Suppose that G is abelian. Then G is isomorphic to one of $C_2 \times C_2 \times C_2$ or $C_4 \times C_2$ or C_8 by the fundamental theorem of finitely generated abelian groups.

So suppose that G is nonabelian. Then G has no element of order 8 else $G \cong C_8$. Moreover G must have at least one nontrivial element of order not equal to 2 else G is abelian. So say $u \in G$ has order larger than 2. By Lagrange's theorem we must have $|u| = 4$. Let $H = \langle u \rangle$. Let $v \in G \setminus H$ with $|v|$ minimal. Then either $|v| = 2$ or 4. There are two cases.

Case 1: $|v| = 2$
Suppose that $|v| = 2$. Then G satisfies the three hypotheses for the Dihedral group by proposition 4.1.2 and thus $G \cong D_8$.

Case 2: $|v| = 4$
Suppose that $|v| = 4$. Then since $v \notin H$ and $[G : H] = 2$, we must have $G/H = \{H, vH\}$. Since $v \in H$ has minimal order, this means that all elements in vH has order 4. Since furthermore $u, u^{-1} \in H$ both has order 4, there are precisely 6 elements of order 4 and one element of order 2 (u^2 has order 2). It follows that for x an element of order 6, $x^2 = u^2$ since u^2 has order 2. Some algebra shows that $u^2 x = xu^2$ which means that $u^2 \in Z(G)$. We also have $u^2 x = x^3 = x^{-1}$ for all x with order 6.

Side claim: $vuv^{-1} = u^{-1}$
Clearly $G = \langle u, v \rangle$ since $v \notin H = \langle u \rangle$, and $|H| = 4$. Moreover, $H \trianglelefteq G$ since $[G : H] = 2$. Thus $vuv^{-1} \in H$. If $vuv^{-1} = u$, the v and u commute, thus G is abelian which is a contradiction. u^3 is then the only element of order 4 in H and we know that $\left|vuv^{-1}\right| = |u|$. This means that $vuv^{-1} = u^{-1}$.

Continuing the proof, let $w = uv$. We have that

$$\begin{aligned} w &= uv \\ &= vvuv^{-1} \\ &= vu^{-1} \in vH && (vuv^{-1} = u^{-1}) \end{aligned}$$

We already know that u, u^{-1}, v, v^{-1} are distinct elements since they lie in different cosets. But also now w, w^{-1} is not any of the four. Indeed $w \in vH$ thus w, w^{-1} will not be equal to u, u^{-1}. But if $w = v$, then this implies $u = 1$, a contradiction. Similarly, if $w = v^{-1}$, then $v^2 = u$ which is also a contradiction since $\left|v^2\right| = 2$ while $|u| = 4$.

Thus we must have that

$$G = \{1, u^2, u^{\pm 1}, v^{\pm 1}, w^{\pm 1}\} = \{1, u, u^2, u^3, v, u^2 v, w, u^2 w\}$$

Notice that

$$\begin{aligned} uv &= vv^{-1}uv \\ &= vu^{-1} \\ &= vu^3 \\ &= (vu)(u^2) \\ &= (u^2)(vu) \end{aligned}$$

A similar argument show that $gh = u^2hg$ for all $g, h \in \{u, v, w\}$. Using the fact that $v^2 = w^2 = u^2 \in Z(G)$, we see that

- $u^2g = gu^2$ for all $g \in G$
- $uv = w$, $vw = vuv = u^2v^2u = u$ and $wu = uvu = u^2vu^2 = v$
- $vu = u^2w$, $wv = u^3$, $uw = u^2v$
- $(\pm 1)^2 = 1$ and $(\pm g)^2 = u^2$ for all $g \in \{u, u^3, v, u^2v, w, u^2w\}$

It is easy to see that the Cayley diagram can be formed from these relations which shows that this group is isomorphic to Q_8. □

6.6 Groups of Order 12

Definition 6.6.1: Dicyclic Group of Order 12

Let $C_4 = \langle h \rangle$. Define $\phi : C_4 \to \text{Aut}(C_3)$ to be the inversion homomorphism for. Define the dicyclic group of order 12 to be

$$\text{Dic}_{12} = C_4 \rtimes_\phi C_3$$

Theorem 6.6.2

Let G be a group of order 12. Then G is isomorphic to one of the following groups:

- The cyclic group C_{12}
- $C_6 \times C_2$
- Dic_{12}
- The dihedral group D_{12}
- The alternating group A_4

Proof. When G is abelian, the fundamental theorem of finite abelian group tells us that G is isomorphic to either C_{12} or $C_6 \times C_2$. So suppose that G is non-abelian. We split into two cases.

Case 1: G contains an element of order 6.
Let $|a| = 6$ and $K = \langle a \rangle$.

Case 1(a): $G \setminus K\rangle$ has an element of order 2.
Then G satisfies the first two hypothesis of theorem 6.1.3. It remains to show that the final condition is satisfied. But it is clear that $2^2, 3^2, 4^2$ is congruent to $4, 3, 4$ respectively modulo 6. So i^2 modulo 6 is 1 if and only if $i = 1$ or 5. So we can conclude that in this case, $G \cong D_{12}$.

Case 1(b): No element of $G \setminus K$ is of order 2.
Let $H \in \text{Syl}_2(G)$. Then H is not a subgroup of K since K has two elements of order 2 and $|H| = 4$. If every non-identity element of H has order 2, then $H \setminus K$ would consist of elements of order 2, contrary of our assumption that $G \setminus K$ has no elements of order 2. Thus H must have an element of order 4 and thus $H \cong C_4$. Now let $K_1 = \langle a^2 \rangle$. Then $|K_1| = 3$. Thus $K_1 \in \text{Syl}_3(G)$.

Claim: K_1 is normal. We want to show that $ga^2g^{-1} \in K_1$ and $ga^4g^{-1} \in K_1$. Since K is normal, we have that $ga^2g^{-1} = a^i$ for $i \in \{0, \dots, 5\}$. But $(ga^2g^{-1})^3 = 1$ implies that $a^{3i} = 1$. This means that $3i$ is a multiple of 6. This means that i is a multiple of 2. Thus $ga^2g^{-1} \in K_1$. A similar method shows that $ga^4g^{-1} \in K_1$. Thus K_1 is normal.

We now have that $H \leq G$, $K_1 \trianglelefteq G$, $H \cap K_1 = \{1\}$ by Lagrange's theorem and $|HK_1| = |H| = |K_1| = |G|$ implies that $HK_1 = G$ by proposition 5.2.5 in Groups and Rings. Using proposition 5.3.5 in Groups and Rings, we have that $G \cong H \ltimes_\phi K$ where $\phi : H\text{Aut}(K)$ is given by $\phi_h(k) = hkh^{-1}$. Suppose that $H \cong C_4 = \langle h \rangle$ and $k \in K \setminus \{1_G\}$. Then $G = \langle h, k \rangle$ so $hkh^{-1} \neq k$ since G is non-abelian. Since $hkh^{-1} \in K_1$ and $\left|hkh^{-1}\right| = |k|$, we must have that $hkh^{-1} = k^{-1}$. This means ϕ is the inversion homomorphism and that G is just the dicyclic group of order 12 by definition.

Case 2: G has no element of order 6.
By Cauchy's theorem, we may choose an element of order 3. Since $x \in C_G(x)$ and G has no element of order 6, we see that 2 does not divide $|C_G(x)|$. Indeed if it did, then we could choose an element of order 2 in $C_G(x)$ by Cauchy's theorem. But then $|xy| = 6$ by proposition 1.3.6 in Groups and Rings. Thus we must have that $|C_G(x)| = 3$ by Lagrange's theorem. By the orbit stabilizer theorem, we have that $|\text{Cl}(x)| = [G : C_G(x)] = 4$. Since G has precisely $n_3(G) \times (3-1)$ elements of order 3 by corollary 5.3.1, we deduce that $n_3(G) > 1$. In particular, H is not a normal subgroup of G.

Finally, let $H \in \text{Syl}_3(G)$ and consider the action of G on $\frac{G}{H}$ by left multiplication. Let K be the kernel of this action. Then $K \leq H$ by ???. But H is not normal in G. So we must have $|K| = 1$ since $|H| = 3$. Thus $G \cong \frac{G}{K}$ is isomorphic to a subgroup of S_4. But the only subgroup of S_4 of order 12 is A_4. Thus $G \cong A_4$. □

6.7 Unique Simple Group of Order 60

As an application of the classification of small groups, together with the Sylow theorems, we prove that the unique group of order 60 is A_5.

Theorem 6.7.1

Let G be a simple group of order 60. Then $G \cong A_5$.

Proof.
Step 1: G does not contain a proper subgroup of index $n \leq 4$. Assume the contrary. Let $H \leq G$ with $1 \neq [G : H] \leq 4$. Then G acts non-trivially by left multiplication on the set of left cosets G/H of H in G, and $|G/H| = n$ for some $2 \leq n \leq 4$. Since G is simple, the kernel of this action is trivial. Thus G is isomorphic to a subgroup of S_n. Since $2 \leq n \leq 4$, we have that $|S_n| \leq 4! = 24$. But $|G| = 60$ so that this contradicts Lagrange's theorem.

Step 2: G contains a subgroup of index 5.
Assume the contrary. Let $P \in \text{Syl}_2(G)$. By Sylow's theorem, we have that $n_2(G)$ is odd and $n_2(G)$ divides 15. Moreover $n_2(G) \neq 1$ since G is simple. We also know that $n_2(G) = \frac{|G|}{|N_G(P)|}$ so by step 1, $n_2(G) = 5$ or 15. If $n_2(G) = 5$ then $\frac{|G|}{|N_G(P)|} = 5$, a contradiction.

So suppose $n_2(G) = 15$. Let $g \in G \setminus N_G(P)$. Let $H = \langle P \cup gPg^{-1} \rangle$. Then H contains at least two Sylow 2-subgroups namely P and gPg^{-1}. So $n_2(H)$ being an odd number, is at least 3. Since 4 divides $|H|$, we deduce that $|H|$ is divisible by $4n_2(H)$. By step 1, we have either $H = G$ or $|H| < \frac{|G|}{4} = 15$. Thus we must have either $H \neq G$ and $n_2(H) = 3$ or $H = G$. If $H \neq G$ and $n_2(H) = 3$, then 12 divides $|H|$ so we must have $|H| = 12$ by step 1. Thus $[G : H] = 5$ as needed.

Now assume that for all $g \in G \setminus N_G(P)$, we then have $G = \langle P \cup gPg^{-1} \rangle$. Assume that $x \in P \cap gPg^{-1}$, then x is centralized by both P and gPg^{-1}, since groups of order 4 are abelian. Thus x is centralized in G since $G = \langle P \cup gPg^{-1} \rangle$. Then $x \in Z(G)$. Since G is simple, we have $Z(G) = \{1\}$ and so $x = 1$ and we conclude that $P \cap gPg^{-1} = \{1\}$ for all $g \in G$. Now

$$F_2(G) = \bigcup_{P \in \text{Syl}_2(G)} P \setminus \{1_G\}$$

by consequences of the Sylow theorems. By the above work, this is a disjoint union. Thus $|F_2(G)| = n_2(G) \times 3 = 45$. By Sylow's theorem, we have that $n_5(G) \equiv 1 \pmod 5$ and $n_5(G)$ divides 12. Since G is simple, we have $n_5(G) > 1$ so that $n_5(G) = 6$. But then $|F_5(G)| = 6 \times 4 = 24$. This means that $|G| > |F_2(G)| + |F_5(G)| = 69$, a contradiction. This completes the proof of step 2.

Step 3: Final result.
Let $H \leq G$ be a subgroup of index 5. Then G acts non-trivially by left multiplication on the set of left cosets G/H of H in G. Since G is simple, the kernel of this action is trivial, and thus G is isomorphic to a subgroup of S_5. But the only subgroup of S_5 of order 60 is A_5, which completes the proof. □

7 Series of Subgroups

7.1 Series of Subgroups

Definition 7.1.1: Subnormal Series

Let G be a group. A subnormal series of a group G is a sequence of subgroups, each a normal subgroup of the next one. This is written as

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

In this case we say that the series has length n.

Definition 7.1.2: Types of Subnormal Series

Let G be a group and

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

a subnormal series of G. Then the subnormal series can have additional properties.

- The series is normal if each $G_i \triangleleft G$ for $0 \leq i \leq r$
- The series is a composition series if G_{i+1}/G_i is simple for $0 \leq i \leq r-1$
- The series is a central series if it is a normal series in which $G_{i+1}/G_i \leq Z(G/G_i)$ for $0 \leq i \leq r-1$

7.2 Composition Series

Lemma 7.2.1

Let G be a finite group. Let N be a normal subgroup of G. Suppose that

$$\{1_G\} = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r = N$$

and

$$\{1_{G/N}\} = \frac{X_0}{N} \triangleleft \frac{X_1}{N} \triangleleft \cdots \triangleleft \frac{X_s}{N} = \frac{G}{N}$$

are composition series for N and $\frac{G}{N}$ respectively. Set $G_i = N_i$ for $0 \leq i \leq r$ and $G_i = X_i$ for $r+1 \leq i \leq r+s$. Then

$$G_0 \triangleleft \cdots \triangleleft G_s$$

is a composition series of G.

Proof. It is clear that we can write the composition series of $\frac{G}{N}$ as as quotient groups by the correspondence theorem: Suppose we write $\overline{G}_i$ for the composition series of $\frac{G}{N}$. Fix $0 \leq i \leq s$. By the correspondence theorem, there exists a subgroup X_i of G containing N such that $\overline{G}_i = \frac{X_i}{N}$.

Since $\overline{G}_i$ is a normal subgroup of $\overline{G}_{i+1}$, it follows that X_i is a normal subgroup of X_{i+1}. By the third isomorphism theorem, we have

$$\frac{\overline{G}_{i+1}}{\overline{G}_i} = \frac{X_{i+1}/N}{X_i/N} \cong \frac{X_{i+1}}{X_i}$$

so that $\frac{X_{i+1}}{X_i}$ is simple. Now notice that $X_s = G$ and $N_r = N = X_0$. Set $G_i = N_i$ for $0 \leq i \leq r$ and set $G_i = X_{i-r}$ for $r+1 \leq i \leq r+s$. Then $G_0 \triangleleft \cdots \triangleleft G_{r+s}$ is a composition series for G. □

Proposition 7.2.2

Every finite group has a composition series.

Proof. We induct on $|G|$. If $|G| = 1$, there is a trivial composition series. So assume that $|G| > 1$, and that every group of order less than $|G|$ has a composition series. If G is simple, we are done. So assume G is not simple. Then G has a normal subgroup N with $\{1_G\} \neq N \neq G$. Then $|N| < |G|$ and $\frac{G}{N} < |G|$, so our inductive hypothesis implies that N has a composition series $N_0 \triangleleft \cdots \triangleleft N_r$ and $\frac{G}{N}$ has a composition series $\overline{G}_0 \triangleleft \cdots \triangleleft \overline{G}_{r+s}$. The results follow by the above lemma. □

Definition 7.2.3: Equivalent Composition Series

Let G be a group. Two composition series of G, namely $A_0 \triangleleft \cdots \triangleleft A_r$ and $B_0 \triangleleft \cdots \triangleleft B_s$ is said to be equivalent if $r = s$ and there exists a bijection

$$f : \{A_i/A_{i-1} | 1 \leq i \leq r\} \to \{B_j/B_{j-1} | 1 \leq j \leq s\}$$

such that $A_i/A_{i-1} \cong f(A_i/A_{i-1})$ for $1 \leq i \leq r$.

Theorem 7.2.4: The Jordan–Hölder Theorem

Let $A_0 \triangleleft \cdots \triangleleft A_r$ and $B_0 \triangleleft \cdots \triangleleft B_s$ be two compositions series of a finite group G. Then they are equivalent.

Proof. Without loss of generality, let $r \leq s$. We induct on r. If $r = 0$, then $G = \{1_G\}$ and the result is clear. Assume that $r > 0$. There are two cases.

Case 1: $A_{r-1} = B_{s-1}$.
Then $A_0 \triangleleft \cdots \triangleleft A_{r-1}$ and $B_0 \triangleleft \cdots \triangleleft B_{s-1}$ are two composition series of $A_{r-1} = B_{s-1}$ of lengths $r-1$ and $s-1$. By induction hypothesis, they are equivalent and hence so are the two composition series of G.

Case 2: $A_{r-1} \neq B_{s-1}$.
Consider $A_{r-1}B_{s-1}$. Since A_r and B_s are proper normal subgroups of G, we have $B_{s-1} < A_{r-1}B_{s-1} \trianglelefteq G$. It follows from the third isomorphism theorem that $A_{r-1}B_{s-1}/B_{s-1}$ is a normal subgroup of G/B_{s-1}. Since $B_{s-1} < A_{r-1}B_{s-1}$, it is in fact a non-trivial normal subgroup by the correspondence theorem. Since G/B_{s-1} is simple, we have $A_{r-1}B_{s-1}/B_{s-1} = G/B_{s-1}$ so that $A_{r-1}B_{s-1} = G$ by the correspondence theorem. Let $D = A_{r-1} \cap B_{s-1}$. By the second isomorphism theorem, we have

$$\frac{G}{A_{r-1}} = \frac{A_{r-1}B_{s-1}}{A_{r-1}} \cong \frac{B_{s-1}}{A_{r-1} \cap B_{s-1}} = \frac{B_{s-1}}{D}$$

and as G/A_{r-1} is simple, so is B_{s-1}/D. Similarly, by applying the second isomorphism theorem again, we have

$$\frac{G}{B_{s-1}} = \frac{A_{r-1}B_{s-1}}{B_{s-1}} \cong \frac{A_{r-1}}{A_{r-1} \cap B_{s-1}} = \frac{A_{r-1}}{D}$$

and as G/B_{s-1} is simple, so is A_{r-1}/D. Now let

$$\{1_G\} = D_0 \triangleleft \cdots \triangleleft D_t = D$$

be a composition series for D. Then

$$\{1_G\} = D_0 \triangleleft \cdots \triangleleft D_t = D \triangleleft A_{r-1} \triangleleft G$$

and

$$\{1_G\} = D_0 \triangleleft \cdots \triangleleft D_t = D \triangleleft B_{s-1} \triangleleft G$$

are both composition series of G.

Since $r \leq s$, we can apply the first case to the get that

$$A_0 \triangleleft \cdots \triangleleft A_r \quad \text{and} \quad D_0 \triangleleft \cdots \triangleleft D_t = D \triangleleft A_{r-1} \triangleleft G$$

are equivalent. In particular, we have that $r = t + 2$ and hence $D_0 \triangleleft \cdots \triangleleft D_t = D \triangleleft B_{s-1} \triangleleft G$ has length $t + 2 = r$. Thus we can apply case 1 again to conclude that

$$B_0 \triangleleft \cdots \triangleleft B_s \quad \text{and} \quad D_0 \triangleleft \cdots \triangleleft D_t = D \triangleleft B_{s-1} \triangleleft G$$

are equivalent. Finally, we have seen that $G/A_{r-1} \cong B_{s-1}/D$ and $A_{r-1}/D \cong G/B_{s-1}$. Thus

$$D_0 \triangleleft \cdots \triangleleft D_t = D \triangleleft A_{r-1} \triangleleft G \quad \text{and} \quad D_0 \triangleleft \cdots \triangleleft D_t = D \triangleleft B_{s-1} \triangleleft G$$

are equivalent so that we conclude. □

We have thus proved that the following definition of is an invariant of a group.

Definition 7.2.5: Composition Factors

Let G be a group and

$$\{1_G\} = G_0 \triangleleft \cdots \triangleleft G_r = G$$

be a composition series of G. We say that the simple groups $\frac{G_{i+1}}{G_i}$ for $0 \leq i < r$ are called the composition factors of G.

7.3 Soluble Groups and Derived Series

Soluble group, while interesting in its own right, has two main applications: To the study of Galois theory and to the study of composition series. We will focus on its relations with composition series and leave the relation to Galois theory in Fields and Galois Theory.

Definition 7.3.1: Soluble Groups

A group G is said to be soluble if it is either trivial, or its composition factors are all cyclic groups of prime order.

Notice that all abelian groups are soluble. Indeed every quotient group of G is abelian and so every composition factors of G are abelian simple groups, which must be cyclic groups of prime order.

Lemma 7.3.2

Let G be a finite group. Let N be a normal subgroup of G. Then G is soluble if and only if both N and $\frac{G}{N}$ are soluble.

Proof. Write $\mathrm{CF}(G)$ the composition factors of G. By the Jordan–Hölder theorem and lemma 7.2.1, we have

$$\mathrm{CF}(G) = \mathrm{CF}(N) \cup \mathrm{CF}(G/N)$$

Thus G is soluble if and only if both N and G/N are soluble. □

Definition 7.3.3: Derived Series

Let G be a group. Define $G^{(1)} = [G, G]$ and inductively, $G^{(n+1)} = [G^{(n)}, G^{(n)}]$ for integers $n > 0$. We call the descending series

$$G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(n)} \geq \cdots$$

the derived series of G.

Lemma 7.3.4

Let G be a group and $G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(n)} \geq \cdots$ its derived series. Then the following are true:

- $(G^{(n)})^{(m)} = G^{(n+m)}$
- $H^{(n)} \leq G^{(n)}$ if $H \leq G$

Proof.

- We proceed by induction on m. When $m = 0$ the results are clear. If $(G^{(n)})^{(m-1)} = G^{(n+m-1)}$, then we have

$$\begin{aligned}(G^{(n)})^{(m)} &= [(G^{(n)})^{m-1}, (G^{(n)})^{m-1}] \\ &= [G^{(n+m-1)}, G^{(n+m-1)}] \\ &= G^{(n+m)}\end{aligned}$$

  and so we are done.

- Similarly by induction, we have

$$\begin{aligned}H^{(n)} &= [H^{(n-1)}, H^{(n-1)}] \\ &\leq [G^{(n-1)}, G^{(n-1)}] \\ &= G^{(n)}\end{aligned}$$

And so we conclude. □

We focus the rest of the chapter to the case where G is finite.

Theorem 7.3.5

Let G be a finite group. The following are equivalent characterizations for solubility.

- G is soluble.
- $G^{(n)} = 1$ for some $n \geq 0$ in the derived series of G
- G has a normal series with abelian factors.

Proof.

- (1) $\implies$ (2): Suppose that G is soluble. We proceed by induction on the order of G. When $|G| = 1$ the results are clear. Suppose that $|G| > 1$. Let $N = [G, G]$. Since N is normal and G is soluble, N is soluble by lemma 7.2.1. By definition of solubility, G has all composition factors cyclic groups of prime order. In particular, G_{r-1} is a normal subgroup of G with

$$G_r/G_{r-1} = G/G_{r-1}$$

being cyclic of prime order. By proposition 3.4.3, we have that $N \leq G_{r-1}$. In particular, $|N| < |G|$. So $N^{(m)} = 1$ by induction hypothesis. Since $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$ by definition, it follows that $G^{(m+1)} = 1$ and so we are done.

- (2) $\implies$ (1): Suppose that $G^{(n)} = 1$ for some $n \in \mathbb{N}$. We will again induct on the order of G. This is clearly true if $|G| = 1$. So suppose that $|G| > 1$. Let $N = [G, G]$. If $N = G$ then we have that
$$G^{(n)} = [G, G]^{(n-1)} = G^{(n-1)} = \cdots = G$$
which is a contradiction. So we must have $N < G$. Since $N^{(n-1)} = G^{(n)} = 1$, we have that N is soluble by induction hypothesis. Also $G/N = G/[G, G]$ is abelian so that both N and G/N is soluble. Hence G is soluble by lemma 7.4.2. Thus we are done.

□

Corollary 7.3.6

Let G be a finite soluble group and $H \leq G$. Then H is soluble.

Proof. Suppose that G is soluble. Then $G^{(n)} = 1$ for some $n \in \mathbb{N}$. Then since $H^{(n)} \leq G^{(n)}$, we have $H^{(n)} = 1$ and so H is soluble. □

Theorem 7.3.7

Let p be prime and $n \in \mathbb{N}$. Let G be a finite group of order p^n. Then G is soluble, and all composition factors of G are isomorphic to C_p.

Proof. We prove the theorem by induction on $|G|$. If $|G| = p$ then G is cyclic of prime order, so G is soluble of composition length 1, and its composition factors are C_p.

Assume that $|G| > p$. The normal subgroup $Z(G)$ is non-trivial in this case. Since $Z(G)$ is abelian, $Z(G)$ is soluble. By induction hypothesis, $G/Z(G)$ is soluble. Thus G is soluble by lemma 7.4.2. By the same lemma, we have that the composition factors of G is the union of the composition factors of $Z(G)$ and $G/Z(G)$. By induction hypothesis all their composition factors are isomorphic to C_p and so we conclude. □

Theorem 7.3.8

Let G_1, G_2 be soluble groups. Then $G_1 \times G_2$ is soluble.

Proof. Recall that $G_1 \times G_2 \cong G_1 \rtimes_\phi G_2$ where $\phi : G_2 \to \text{Aut}(G_1)$ is the trivial homomorphism. Also since $G_1 \trianglelefteq G_1 \times G_2$, and $G_1 \times G_2/G_1 \cong G_2$, together with G_1, G_2 being soluble implies that $G_1 \times G_2$ is soluble. □

As usual, this theorem can be applied inductively to see that $G_1 \times \cdots \times G_n$ is soluble given that $G_1, \ldots, G_n$ are soluble.

7.4 Nilpotent Groups

Definition 7.4.1: Nilpotent Groups

Let G be a group. We say that G is nilpotent if G has a central series of finite length.

Definition 7.4.2: Lower Central Series

Let G be a group. Define the lower central series of G to be the descending series of subgroups

$$G = G_1 \trianglerighteq G_2 \triangleright \cdots \triangleright G_n \triangleright$$

where $G_{n+1} = [G_n, G]$. We often write $\gamma_n(G) = G_n = [G_{n-1}, G]$ for the nth term in the lower central series of G.

Proposition 7.4.3

Let G be a group. Then G is nilpotent if and only if the lower central series terminates at the trivial subgroup after finitely many steps.

Definition 7.4.4: Nilpotency Class

Let G be a nilpotent group. Define the nilpotentcy class of G to be the smallest $n \in \mathbb{N}$ such that G has a central series of length n. Equivalently, the nilpotency class is the maximal of $n \in \mathbb{N}$ such that $\gamma_n(G) \neq 1$.

Proposition 7.4.5

Let G be a nilpotent group. Let $H \leq G$ and $N \trianglelefteq G$. Then the following are true.

- H is nilpotent
- $\gamma\left(\frac{G}{N}\right) = \frac{\gamma_n(G)N}{N}$ for all $n \in \mathbb{N}$. In particular, G/N is nilpotent.

Proposition 7.4.6

Let G be a finite nilpotent group. Then G is soluble.

Proposition 7.4.7

Let G be a finite group of prime power order. Then G is nilpotent.