PMATH 336: Introductory Group Theory Notes

Sumeet Khatri

Table of Contents

Preface . . . . . **iv**

I Review of Prerequisites **1**

1 Mappings **2**

1.1 Properties of Mappings 3

1.2 Cyclic Notation 6

1.3 Examples of Bijections 9

1.3.1 Permutations 9

1.3.2 Symmetry Transformations in $\mathbb{R}^n$ 10

1.4 Factoring into Disjoint Cycles 13

2 Basic Algebra (MATH 135) **14**

3 Modular Arithmetic (MATH 135) **18**

3.1 Integer Congruence 18

3.2 Motivating Modular Arithmetic 19

3.3 The Integers Modulo m 21

II The Course Material **26**

4 Groups **27**

4.1 Basic Concepts 27

4.2 The Definition of a Group and Examples 28

4.3 Special Groups 35

4.3.1 Permutation Groups 36

4.3.2 Dihedral Groups 39

4.3.3 The General Linear Group 44

4.3.4 The Special Linear Group 45

4.3.5 The Klein 4-Group 45

4.3.6 The Quaternion Group 47

4.4 Subgroups and Cyclic Groups 48

4.4.1 Cyclic Subgroups and Cyclic Groups 50
4.4.2 Centralisers and Normalisers, Stabilisers and Kernels 61

5 Cosets and Lagrange's Theorem 63

5.1 Equivalence Relations on a Group 63
5.2 Cosets 64
5.3 Lagrange's Theorem 68
5.4 Examples 69

6 Isomorphisms and Quotient Groups 74

6.1 Homomorphisms 74
6.2 Isomorphisms 79
6.3 The Direct Product 84
6.4 Normal Subgroups 88
6.5 The Subset Product and the Internal Direct Products 93
6.6 Quotient Groups and the First Isomorphism Theorem 99
6.7 The Second and Third Isomorphism Theorems 108
6.8 Automorphisms 116

7 The Permutation Group S_n 119

7.1 Disjoint Permutations 119
7.2 Cycle Structures 122
7.3 Conjugacy Classes 128
7.4 Even and Odd Permutations 132
7.5 The Alternating Group A_n 135
7.6 The Simplicity of A_n 138

8 Finite Abelian Groups 141

8.1 p-Groups 144
8.2 The Fundamental Theorem of Finite Abelian Groups 152
8.3 Examples 154

9 Group Actions 159

9.1 Stabilisers and Orbits in a Group Action 165

9.2 The Number of Orbits and Polya-Burnside Problems 171
9.3 The Class Equation 176
9.4 Conjugation in the Permutation Group S_n 183
9.5 Cauchy's Theorem 184
9.6 The Classification of Small Groups 190
9.6.1 Groups of Order 8 191
9.6.2 Groups of Order 12 193
9.7 The Sylow Theorems 195
9.8 Applications of Sylow's Theorems 201
10 Group Solvability and the Semi-Direct Product 204
10.1 The Commutator and Commutator Subgroup 204
10.2 Solvable Group 207
10.3 The Semi-Direct Product 209

Preface

[Insert preface material here.]

Part I

Review of Prerequisites

1 Mappings

We are all familiar with the concept of a mapping: a (non-empty) set, call it X, of objects, which are called points, are changed to some points in another set Y.

Definition 1.0.1 Mappings

Given two sets X and Y, a **mapping**, or **function**, from X to Y is a recipe that assigns to each element of X exactly one element of Y. We write $\alpha : X \to Y$ to indicate that α is a map from X to Y. We write $y = \alpha(x)$ for the element of Y assigned to the element x of X, which is called the **image** of x under the mapping α. If X' is a subset of X, then we write $\alpha(A') = \{\alpha(x) \mid x \in X'\}$, which is also called the image of X' under α.

A mapping must be well-defined, which means that if α is specified by a rule assigning to each element of X and element of Y, then the rule must unambiguously assign to each element of X one and only on element of Y.

If X is a finite set of n points, then we can enumerate the points in X as, say, $p_1, \ldots, p_n$. X could also be an infinite set, for example, the set of positive integers, 1, 2, 3, etc, or a continuum, like all the points in the xy plane.

For a finite set of points, the description of a mapping can be done by enumeration. For example, for a set of three points, $X = \{a, b, c\}$, we can describe a mapping by saying: the mapping $\alpha : X \to X$ takes the point a into its image b, the point b into a, and the point c into c; symbolically,

$$\alpha = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}. \tag{1.1}$$

Another possible mapping $\beta : X \to X$ might be

$$\beta = \begin{pmatrix} a & b & c \\ a & a & a \end{pmatrix}, \tag{1.2}$$

where in both cases we have used the notation

$$\alpha = \begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ \alpha(p_n) & \alpha(p_2) & \cdots & \alpha(p_n) \end{pmatrix}. \tag{1.3}$$

For an infinite set of points, enumeration is not possible. Instead, we give a *functional law* (or *recipe*) for the mapping α. For example, we may consider the set of points on the x axis, and a mapping α such that $x' = \alpha(x) = x + 2$, i.e., each point is to be shifted two units to the right to arrive at its image.

Definition 1.0.2 Injective (One-to-One Mapping)

A mapping $\alpha : X \to Y$ is an **injective** mapping, or is **one-to-one** if $x_1 \neq x_2$ in X always implies $\alpha(x_1) \neq \alpha(x_2)$ in Y. Equivalently, α is injective if $\alpha(x_1) = \alpha(x_2)$ in Y always implies $x_1 = x_2$ in X.

Definition 1.0.3 Surjective (Onto Mapping)

A mapping $\alpha : X \to Y$ is an **surjective** mapping, or is **onto** if for every $y \in Y$ there is an $x \in X$ such that $\alpha(x) = y$. In this case, $\alpha(X) = Y$.

We will be working only with mappings that are *one-to-one* (*injective*) and *onto* (*surjective*), mappings which are also called *transformations* or *bijections*. These are mappings in which no two points of the set have the same image, and every point p' of the set is the image of one, and only one, point p. The mapping α in (1.1) was a bijection, while (1.2) was not (it was neither one-to-one nor onto).

1.1 Properties of Mappings

Definition 1.1.1 Identical Mappings

Two mappings α and β of a set of points X are **identical** if $\alpha(p) = \beta(p)$ for all $p \in X$. Conversely, $\alpha = \beta$ means that $\alpha(p) = \beta(p)$.

Definition 1.1.2 Composition of Mappings

If $x' = \alpha(x)$ and $x'' = \beta(x')$ for $\alpha, \beta : X \to X$, and $x, x', x'' \in X$, then we denote the **composition**, or **succession**, of the mappings α and β (i.e., β then α) by $\alpha \circ \beta$, so that

$$p'' = (\alpha \circ \beta)(x) = \alpha(\beta(x)) = \beta\left(x'\right).$$

In other words, there is a single mapping, denoted $\beta \circ \alpha$, which produce the same effect as the successive application of β then α.

REMARK (Powers of Mappings): The result of applying a mapping α r times in succession is represented by α^r. Since composition of mappings are associative, we have that, for some μ, $\nu \in \mathbb{Z}$,

$$\alpha^\mu \alpha^\nu = \alpha^{\mu+\nu} = \alpha^\nu \alpha^\mu. \tag{1.4}$$

Now, since there are only a finite number of operations that can be performed on a bijection over a finite set, the series of compositions $\alpha, \alpha^2, \alpha^3, \ldots$ cannot all be distinct. Suppose that α^{m+1} is the first of the series that is the same as α, so that

$$\alpha^{m+1} = \alpha.$$

Then,

$$\alpha^m \alpha \alpha^{-1} = \alpha \alpha^{-1},$$

or

$$\alpha^m = \mathcal{I}.$$

There is no power $\mu < m$ for which this relation holds, for if $\alpha^\mu = \mathcal{I}$, then $\alpha^{\mu+1} = \alpha\mathcal{I} = \alpha$, contrary to the assumption that α^{m+1} is the first of the series that is the same as α.

Moreover, the $m-1$ substitutions $\alpha, \alpha^2, \ldots, \alpha^{m-1}$ must be all distinct. For if $\alpha^\mu = \alpha^\nu$, $\nu < \mu < m$, then

$$\alpha^{\mu-\nu}\left(\alpha^\nu\right)^{-1} = \alpha^\nu\left(\alpha^\nu\right)^{-1} \Rightarrow \alpha^{\mu-\nu} = \mathcal{I},$$

which has just been shown to be impossible.

The number m is called the **order** of the mapping α. Note that if $\alpha^n = \mathcal{I}$, then n is a multiple of m; also, if $\alpha^a = \alpha^b$, then $a - b = 0 \pmod{m}$.

If now the equation $\alpha^{\mu+\nu}$ is assumed to hold, when either or both of the integers ν and μ is a negative integer, a definite meaning is obtained for α^{-r}, the negative power of a mapping; and a definite meaning is also obtained for α^0, for

$$\alpha^\mu\alpha^{-\nu} = \alpha^{\mu-\nu} = \alpha^{\mu-\nu}\alpha^\nu\left(\alpha^\nu\right)^{-1} = \alpha^\mu\left(\alpha^\nu\right)^{-1},$$

so that

$$\alpha^{-\nu} = \left(\alpha^\nu\right)^{-1},$$

as one might expect. Similarly, it can be shown that $\alpha^0 = \mathcal{I}$, also as one would expect.

Theorem 1.1.1

Let $\alpha : X \to Y$, $\beta : U \to V$, and $\gamma : W \to Z$ be three mappings. Then,

1. If we successively apply the mappings α, β, γ, then

$$\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma,$$

   i.e., mappings are **associative**.
2. If α and β are both one-to-one, then so is $\beta \circ \alpha$.
3. If α and β are both onto, then so is $\beta \circ \alpha$.

PROOF: We prove each in turn.

1. For any $x \in X$, we have $\gamma \circ (\beta \circ \alpha)(x) = \gamma((\beta \circ \alpha)(x)) = \gamma(\beta(\alpha(x))) = (\gamma \circ \beta)(\alpha(x)) = (\gamma \circ \beta) \circ \alpha(x)$.
2. Suppose that α and β are both one-to-one and consider any $x, y \in X$ for which we have $(\beta \circ \alpha)(x) = (\beta \circ \gamma)(y)$. Then, $\beta(\alpha(x)) = \beta(\alpha(y))$, and since β is one-to-one, we must have $\alpha(x) = \alpha(y)$. But then, since α is one-to-one, we must have $x = y$. Hence, $\beta \circ \alpha$ is one-to-one.
3. Suppose that α and β are both onto and consider any $z \in Z$. Since β is onto, there must be some $y \in Y$ such that $\beta(y) = z$. And since α is onto, there must be some $x \in X$ such that $\alpha(x) = y$. But then $\beta(\alpha(x)) = \beta(y) = z$, and since $(\beta \circ \alpha)(x) = \beta(\alpha(x))$, we have found an element $x \in X$ with $(\beta \circ \alpha)(x) = z$, so $\beta \circ \alpha$ is onto. ■

Using our example mappings α and β from (1.1) and (1.2), we have

$$\beta \circ \alpha = \begin{pmatrix} a & b & c \\ a & a & a \end{pmatrix}\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & a & a \end{pmatrix}.$$

However,

$$\alpha \circ \beta = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \begin{pmatrix} a & b & c \\ a & a & a \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & b & b \end{pmatrix},$$

indicating that $\alpha \circ \beta \neq \beta \circ \alpha$, so that mappings are generally **not commutative**.

Definition 1.1.3 The Identity Mapping

The **Identity mapping**, denoted $\mathcal{I} : X \to X$, maps all points $p \in X$ to themselves, i.e., for all $x \in X$, $\mathcal{I}(x) = x$.

Theorem 1.1.2

Let X be any set and $\mathcal{I} : X \to X$ be the identity mapping. Then,

1. $\mathcal{I}$ is one-to-one and onto.
2. For any set Y and any mapping $\alpha : X \to Y$, we have $\alpha \circ \mathcal{I}$.
3. For any set Y and any map $\alpha : Y \to X$, we have $\mathcal{I} \circ \alpha = \alpha$.

Definition 1.1.4 Inverse Mapping

The **inverse** of a mapping $\alpha : X \to Y$, denoted $\alpha^{-1} : Y \to X$ is a mapping such that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \mathcal{I}$, the identity mapping. In other words, if $\alpha(x) = y$, then $\alpha^{-1}(y) = x$. α is said to be **invertible** is such a mapping α^{-1} exists.

For example, the inverse of

$$\alpha = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

is

$$\alpha^{-1} = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}.$$

Hence, α is its own inverse. The inverse of a composition of mappings α and β is

$$(\alpha \circ \beta)^{-1} = \beta^{-1}\alpha^{-1}, \tag{1.5}$$

i.e., the inverse of the composition is obtained by carrying out the inverse tranformations in reverse order.

Theorem 1.1.3

Let $\alpha : X \to Y$ be invertible. Then,

1. There is a *unique* inverse α^{-1} for α.
2. $\left(\alpha^{-1}\right)^{-1} = \alpha$, that is, α is the inverse of α^{-1}.

PROOF: We prove each statement in turn.

1. Suppose there are two inverse mappings $\beta : Y \to X$ and $\gamma : Y \to X$ with $\beta \circ \alpha = \gamma \circ \alpha = \mathcal{I}_X$, the identity map on X, and $\alpha \circ \beta = \alpha \circ \gamma = \mathcal{I}_Y$, the identity map on Y. Then, $\beta = \beta \circ \mathcal{I}_Y = \beta \circ (\alpha \circ \gamma) = (\beta \circ \alpha) \circ \gamma = \mathcal{I}_X \circ \gamma = \gamma$. So the inverse mapping is unique.

2. This follows immediately from the definition of the inverse mapping. ■

Theorem 1.1.4

Let $\alpha : X \to Y$ and $\beta : Y \to Z$ be two maps. Then,

1. α is invertble if and only if α is one-to-one and onto.
2. If α and β are invertible, then $\beta \circ \alpha$ is invertible, and $(\beta \circ \alpha)^{-1} = \alpha^{-1} \circ \beta^{-1}$. (Note that $\alpha \circ \beta$ is also invertible, and that $(\alpha \circ \beta)^{-1} = \beta^{-1} \circ \alpha^{-1}$.)

PROOF: We again prove each statement in turn.

1. ($\Rightarrow$): Suppose $\alpha^{-1} : Y \to X$ exists. Then, for any x and y in X, $\alpha(x) = \alpha(y)$ implies $x = \alpha^{-1}(\alpha(x)) = \alpha^{-1}(\alpha(y)) = y$. So α is one-to-one. And, given any $u \in Y$, $\alpha\left(\alpha^{-1}(u)\right) = u$, so letting $x = \alpha^{-1}(u)$, we have found an element $x \in X$ with $\alpha(x) = u$, so α is onto. ($\Leftarrow$): Suppose α is one-to-one and onto. Define $\tau : Y \to X$ as follows. For any $u \in Y$, let $\tau(u)$ by the $x \in X$ such that $\alpha(x) = u$. Since α is onto, there will be some such x. And since α is one-to-one, there will be only one, since if $\alpha(x) = \alpha(y) = u$, then $x = y = u$. So the specification just gives a well-defined function τ. Furthermore, $\alpha(\tau(u)) = u$ for any $u \in Y$ by definition of τ, and also $\tau(\alpha(x)) = x$. Hence, $\tau = \alpha^{-1}$, so α is invertible (since we found an inverse).

2. Assume that both α and β are invertible. Then, by 1., they are both one-to-one and onto. So $\beta \circ \alpha$ is one-to-one and onto by an above theorem, and so $\beta \circ \alpha$ is invertible by 1. Also, we have

$$\left(\alpha^{-1} \circ \beta^{-1}\right) \circ (\beta \circ \alpha) = \alpha^{-1} \circ \left(\beta^{-1} \circ \beta\right) \circ \alpha = \alpha^{-1} \circ \mathcal{I}_Y \circ \alpha = \alpha^{-1} \circ \alpha = \mathcal{I}_X,$$

and therefore $(\beta \circ \alpha)^{-1} = \alpha^{-1} \circ \beta^{-1}$. ■

Definition 1.1.5

Two sets X and Y have the **same cardinality**, and we write $|X| = |Y|$, if there exists a one-to-one and onto mapping $\alpha : X \to Y$.

1.2 Cyclic Notation

We can also improve the notation shown above for a mapping $\alpha : X \to X$. Let $X = \{p_1, p_2, \ldots, p_n\}$ be a set of n distinct points and $p_1', p_2', \ldots, p_n'$ the images of the points $p_1, p_2, \ldots, p_n$ under α. The mapping α replaces each point in X by another point in X, which could be the same point or a different one, under the condition that no two points are replaced by one and

the same letter. The mapping is thus taking the points $p_1, p_2, \ldots, p_n$ and simply *rearranging* them to the new set of points $p'_1, p'_2, \ldots, p'_n$ (note that all of these image points are still in X, even though they have been labelled differently). The notation shown above,

$$\begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ p'_1 & p'_2 & \cdots & p'_n \end{pmatrix}, \tag{1.6}$$

thus indicates that each point in the upper line is to be replaced by the point standing under it in the lower line.

Definition 1.2.1

If $x \in X$, then α **fixes** x if $\alpha(x) = x$ and α **moves** x if $\alpha(x) \neq x$.

Definition 1.2.2

Let $p_1, p_2, \ldots, p_r \in X$ be r distinct points from a set X of n points. If $\alpha : X \to X$ fixes the remaining $n - r$ points, and if

$$\alpha(p_1) = p_2,\ \alpha(p_2) = p_3,\ \ldots,\ \alpha(p_{r-1}) = p_r,\ \alpha(p_r) = p_1, \tag{1.7}$$

then α is an r**-cycle**, or α is a **cycle of length** r. We then write $\alpha = (p_1, p_2, \ldots, p_r)$.

REMARK: Every 1-cycle (i.e., cycles with only one point) fixes every element of X, and so all 1-cycles are equal to the identity $\mathcal{I}$.

A 2-cycle, which merely interchanges a pair of elements, is called a **transposition**.

Below are three examples:

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} &= (1\,2\,3\,4) \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix} &= (1\,5\,3\,4\,2) \\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} &= (1\,2\,3)\,(4)\,(5) = (1\,2\,3)\,. \end{aligned} \tag{1.8}$$

Composition of functions is easy with one uses the cycle notation. For example, let us compute $\gamma = \alpha \circ \beta$, where $\alpha = (1\,2)$ and $\beta = (1\,3\,4\,2\,5)$. We have

$$\begin{aligned} \gamma(1) = \alpha \circ \beta(1) = \alpha(\beta(1)) = \alpha(3) = 3 \\ \gamma(3) = \alpha(4) = 4 \\ \gamma(4) = \alpha(2) = 1. \end{aligned}$$

Having returned to 1, we now seed $\gamma(2)$, because 2 is the smallest integer for which γ has not yet been evaluated. We have $\gamma(2) = \alpha(5) = 5$, so that

$$\gamma = \alpha \circ \beta = (1\,2)\,(1\,3\,4\,2\,5) = (1\,3\,4)\,(2\,5)\,. \tag{1.9}$$

REMARK: The cyclic notation for a mapping is not unique. The mapping $(q\,r\,\cdots\,s\,p)$ represents the same mapping as $(p\,q\,r\,\cdots\,s)$ as long as the letters that occur between r and s in the two mappings are the same and occur in the same order so that, as regards the letters inside the braket, any one may be chosen to stand first so long as the cyclic order is preserved.

Moreover, the order in which the brakets are arranged, for example, in (1.9), is immaterial, since the operation denoted by any one braket has no effect on the letters contained in the other brakets. This latter property is characteristic of the particular expression that has been obtained for a mapping–it depends on the fact that the expression contains each of the points only once.

Definition 1.2.3 Disjoint Mappings

Two mappings $\alpha, \beta : X \to X$ are **disjoint** if every x moved by one is fixed by the other, i.e., if $\alpha(x) \neq x$, then $\beta(x) = x$, and if $\beta(y) \neq y$, then $\alpha(y) = y$. Note that it is possible that there is a $z \in X$ with $\alpha(z) = z = \beta(z)$.

The cycles on the right-hand side of (1.9) are thus disjoint.

Theorem 1.2.1 Facts about Disjoint Bijections

For α and β both disjoint bijections:

1. If $\alpha = (p_1\,p_2\,\cdots\,p_r)$ and $\beta = (j_1\,j_2\,\cdots\,j_s)$, then α and β are disjoint bijections if and only if $\{p_1, p_2, \cdots, p_r\} \cap \{j_1, j_2, \cdots, j_s\}$.
2. $\alpha \circ \beta = \beta \circ \alpha$, i.e., α and β *commute*.
3. If $\alpha \circ \beta = \mathcal{I}$, then $\alpha = \mathcal{I} = \beta$.
4. $(\alpha \circ \beta)^k = \alpha^k \circ \beta^k$ for all $k \geq 0$. Is this true if α and β are not disjoint?
5.

PROOF: **complete this!!** ■

Theorem 1.2.2

We have:

1. Let $\alpha = \beta \circ \gamma$, where β and γ are disjoint. If β moves i, then $\alpha^k(i) = \beta^k(i)$ for all $k \geq 0$.
2. Let α and β be cycles. If there is an p_1 moved by both α and β, and if $\alpha^k(p_1) = \beta^k(p_1)$ for all positive integers k, then $\alpha = \beta$.

PROOF: **complete this!!** ■

REMARK (Circular Mappings): If the cycles of a bijection

$$\alpha = (p\,q\,r\,\cdots\,s)\,(p'\,q'\,\cdots\,s')\,(p''\,q''\,\cdots\,s'')\,\cdots$$

contain $m, m', m'', \ldots$ points respectively, and if $\alpha^\mu = \mathcal{I}$, then μ must be a common multiple of $m, m', m'', \ldots$. This is why: **figure it out!!**. Hence, the order of α is the least common multiple of

m, m', m'', ... In particular, when a bijection consists of a single cycle, its order is equal to the number of letters that is interchanges. Such a bijection is called a **circular bijection**.

A bijection, all of whose cycles contain the same number of points, is called **regular**. The order of a regular bijection is equal to the number of points in one of its cycles.

REMARK (Similar Bijections): Two bijections that contain the same number of cycles and the same number of points on corresponding cycles are called **similar**. If α and β are similar bijections, then so are α^r and β^r, and the orders of α and β are the same. Let now

$$\alpha = (a_p a_q \cdots a_s)\,(a_{p'} a_{q'} \cdots a_{s'}) \cdots$$

and

$$\beta = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$$

be any two bijections. Then,

$$\begin{aligned} \beta^{-1}\alpha\beta &= \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} (a_p a_q \cdots a_s)\,(a_{p'} a_{q'} \cdots a_{s'}) \cdots \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} \\ &= (b_p b_q \cdots b_s)\,(b_{p'} b_{q'} \cdots b_{s'}) \cdots . \end{aligned}$$

Hence, α and $\beta^{-1}\alpha\beta$ are similar bijections.

1.3 Examples of Bijections

We now go through some special bijections.

1.3.1 Permutations

Definition 1.3.1 Permutations

If X is a non-empty set, a **permutation** of X is a bijection $\alpha : X \to X$. We denote the set of all permutations of X by S_X. In the important special case of $X = \{1, 2, \ldots, n\}$, we write S_n instead of S_X. Note that $|S_n| = n!$, as you may recall from basic combinatorics.

In Lagrange's day, a permutations of $X = \{1, 2, \ldots, n\}$ was viewed as a rearrangement of the numbers in X, i.e., as a list $i_1, i_2, \ldots, i_n$ with no repetitions of the elements of X. Now, given a rearrangement $i_1, i_2, \ldots, i_n$, defined a mapping $\alpha : X \to X$ by $\alpha(j) = i_j$ for all $j \in X$. This function α is an injection because the list as no repetitions; it is a surjection because all of the elements of X appear on the list. Thus, every rearrangement gives a bijection, i.e., each permutation of the list is a bijection. This is why $|S_n| = n!$, since this is simply a statement of the fact that there are $n!$ ways of arranging a sequence of n *distinct* objects, as you should recall from basic combinatorics. So the two viewpoints of permutations, as rearrangements and bijections, are equivalent.

Properties of Permutations

- The product, i.e., the composition, of two permutations is again a permutation. For example, if $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3)\,(2)$ and $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3)$, both of which are permutations of $X = \{1, 2, 3\}$, then $\alpha \circ \beta = (1\,2)\,(3)$, which is another permutation of $\{1, 2, 3\}$.
- Permutations are generally not commutative, i.e., $\alpha \circ \beta \neq \beta \circ \alpha$. Using the example from the previous point, we have $\beta \circ \alpha = (1)\,(2\,3) \neq \alpha \circ \beta$.
- The identity $\mathcal{I}_X$ on a set X is a permutation such that $\alpha \circ \mathcal{I}_X = \alpha = \mathcal{I}_X \circ \alpha$ for every permutation $\alpha \in S_X$. In other words, $\mathcal{I}_X$ leaves the permutation unchanged.
- Permutations are associative, i.e., if $\alpha, \beta, \gamma \in S_X$, then $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$.
- For each $\alpha \in S_X$, there is a $\beta \in S_X$ such that $\alpha \circ \beta = \mathcal{I}_X = \beta \circ \alpha$, i.e., there exists an inverse $\beta = \alpha^{-1}$. Note that for α as above, $\alpha^{-1} = (1\,3)\,(2) = \alpha$, since $\alpha \circ \alpha^{-1} = \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathcal{I}$, i.e., α is its own inverse.

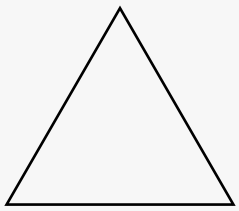
1.3.2 Symmetry Transformations in $\mathbb{R}^n$

Definition 1.3.2 Symmetry Transformation

Given an object in $\mathbb{R}^n$, a **symmetry transformation** of the object is a bijection from the object to itself.

Example 1.3.1 How many symmetry transformations are there for an equilaterial triangle in $\mathbb{R}^2$?

Solution: Here is our triangle:



We can label the vertices of the triangle as shown. Note that a symmetry transformation is a bijection from the object *to itself*. What this implies here is that, after the transformation, the triangle should have the *same orientation*, since a triangle that is tilted slightly to the right, for example, is *not* the same as the triangle shown above. With this in mind, we see that 120-degree counter-clockwise rotations will return the triangle to the same orientation. As well, reflections about the three bisectors will return the triangle to the original orientation. These are the only types of symmetry transformations possible in $\mathbb{R}^2$. Using the

vertices to indicate the transformation, we can write:

$$\alpha_{\frac{2\pi}{3}} = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3\,2)$$
$$\alpha_{\frac{4\pi}{3}} = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix} = (1\,2\,3)$$
$$\alpha_{\frac{6\pi}{3}} = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 3 & 2 \end{pmatrix} = (1)\,(3)\,(2) = \mathcal{I}$$

as the three rotations. Not suprisingly, since $\frac{6\pi}{3} = 2\pi$, $\alpha_{\frac{6\pi}{3}}$ merely returns the triangle to its original state, which is exacly what the identity transformation does. So in this case, the identity transformation corresponds to a rotation by 360 degrees. The remaining three transformations, the reflections about the bisectors, are

$$\alpha_3 = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2)\,(3)$$
$$\alpha_1 = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix} = (1)\,(3\,2)$$
$$\alpha_2 = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3)\,(2)\,.$$

So there are six symmetry transformations of the equilateral triangle in $\mathbb{R}^2$.

REMARK: Observe that the symmetry transformations of the equilaterial triangle in $\mathbb{R}^2$ are the same as the permutations of the set $\{1, 2, 3\}$. Try to recall a term that you may have encountered in Linear Algebra for this type of correspondence.

Example 1.3.2 How many symmetry transformations are there of the hexagonal pyramid in $\mathbb{R}^3$?

SOLUTION: Like the equilateral triangle in $\mathbb{R}^2$, note that the orientation of the pyramid must be preserved in order to have a symmetry transformation. So, for example, we cannot flip the pyramid upside down, or rotate it in any way about a horizontal axis. All we can do is rotate it about a straight vertical axis going through the top of the pyramid, specifically, by multiples of 60 degrees. We again label the vertices of the hexagon from 1 to 6 to get

$$\alpha_{\frac{\pi}{3}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix} = (1\,2\,3\,4\,5\,6)$$
$$\alpha_{\frac{2\pi}{3}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (1\,3\,5)\,(2\,4\,6)$$
$$\alpha_{\pi} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix} = (1\,4)\,(2\,5)\,(3\,6)$$
$$\alpha_{\frac{4\pi}{3}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix} = (1\,5\,3)\,(2\,6\,4)$$
$$\alpha_{\frac{5\pi}{3}} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1\,6\,5\,4\,3\,2)$$
$$\alpha_{2\pi} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \mathcal{I}.$$

Again, we have six symmetry transformations, and again notice that the identity transformation corresponds to a rotation by 360 degrees.

Properties of the Symmetry Transformation

- Composing two symmetry transformations gives another symmetry transformation. For instance, using the transformations of Example 1.3.2, we have

$$\alpha_{\frac{2\pi}{3}} \circ \alpha_{\frac{\pi}{3}} = (1\,3\,5)\,(2\,4\,6)\,(1\,2\,3\,4\,5\,6) = (1\,4)\,(2\,5)\,(3\,6) = \alpha_{\pi},$$

  i.e., a rotation by 180 degrees is the same as rotating first by 60 degees then by 120 degrees, as one would expect. In fact, for general symmetric rotation transformations by angles θ_1 and θ_2,

$$\alpha_{\theta_1} \circ \alpha_{\theta_2} = \alpha_{\theta_1+\theta_2} = \alpha_{\theta_2} \circ \alpha_{\theta_1}.$$

- Symmetry transformations are generally not commutative. Notice in Example 1.3.2 for the hexagonal pyramid that for all symmetry transformations γ, δ, $\gamma \circ \delta = \delta \circ \gamma$, i.e., all the symmetry transformations of the hexagonal pyramid are mutually commutative. However, for the equilateral triangle in Example 1.3.2, this is not the case. For instance,

$$\alpha_{\frac{4\pi}{3}} \circ \alpha_3 = (1\,2\,3)\,(1\,2) = (1\,3)\,,$$

  but

$$\alpha_3 \circ \alpha_{\frac{4\pi}{3}} = (1\,2)\,(1\,2\,3) = (2\,3) \neq \alpha_{\frac{4\pi}{3}} \circ \alpha_3.$$

  However,

$$\alpha_{\frac{2\pi}{3}} \circ \alpha_{\frac{4\pi}{3}} = (1\,3\,2)\,(1\,2\,3) = \alpha_{2\pi} = \alpha_{\frac{4\pi}{3}} \circ \alpha_{\frac{2\pi}{3}}.$$

  In fact, all of the *rotation* transformations are mutually commutative, though this does not apply to any of the reflection transformations. So, although all the symmetry transformations of the equilateral triangle do not mutually commute, *some* of them do.

- There is an identity symmetry transformation $\mathcal{I}$ such that for all symmetry transformations α, $\alpha \circ \mathcal{I} = \mathcal{I} \circ \alpha = \alpha$. We have already seen that the identity symmetry transformation in both of the above examples corresponds to a rotation by 360 degrees, or equivalently, a rotation by 0 degrees.

- Symmetry transformations are associative, i.e., if α, β, γ are symmetry transformations, then $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$.

- Given a symmetry transformation α, there exists a symmetry transformation β such that $\alpha \circ \beta = \mathcal{I} = \beta \circ \alpha$. As we know already, $\beta = \alpha^{-1}$, the inverse transformation. In the two examples above, the inverse transformation simply undoes either the rotation or the reflection, and hence has the same effect as a rotation by 360 degrees. Using Example 1.3.2, notice that we can write $\alpha_{\frac{5\pi}{3}}$ as $\alpha_{-\frac{\pi}{3}}$. It is then clear that $\alpha_{-\frac{\pi}{3}} \circ \alpha_{\frac{\pi}{3}} = \alpha_0 = \alpha_{2\pi} = \mathcal{I}$, so that $\alpha_{\frac{5\pi}{3}}$ is the inverse of $\alpha_{\frac{\pi}{3}}$.

1.4 Factoring into Disjoint Cycles

Let us "factor" the bijection

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix}$$

into a product (i.e., composition) of disjoint cycles. Now, $\alpha(1) = 6$, and so α begins as $(1\,6$; $\alpha(6) = 3$, so α continues as $(1\,6\,3$; $\alpha(3) = 1$, and so the first cycle closes and α is so far $(1\,6\,3)$. The smallest integer not having appeared is 2, so we write $\alpha = (1\,6\,3)\,(2$, and then, since $\alpha(2) = 4$, we get $\alpha = (1\,6\,3)\,(2\,4$; $\alpha(4) = 2$, so this cycle closes, and we get so far $\alpha = (1\,6\,3)\,(2\,4)$. Since $\alpha(5) = 5$, and observing the cycle on the right-most points 7, 8 and 9, we get

$$\alpha = (1\,6\,3)\,(2\,4)\,(5)\,(7\,8\,9)\,.$$

One often suppresses all 1-cycles, such as (5) in the above factorisation, since all 1-cycles are equal to the identity $\mathcal{I}$. Though sometimes it is convenient to display all the cycles.

Definition 1.4.1 Complete Factorisation

A **complete factorisation** of a bijection α is a factorisation of α as a composition of disjoint cycles that contains one 1-cycle (i) for every i fixed by α. In a complete factorisation, every point in α occurs in exactly one of the cycles.

Theorem 1.4.1

Let $\alpha = \beta_1 \circ \beta_2 \circ \cdots \circ \beta_t$ be a complete factorisation of the bijection α into disjoint cycles $\beta_1, \ldots, \beta_t$. This factorisation is unique except for the order in which the factors occur.

PROOF: Disjoint cycles commute by Theorem 1.2.1, so that the order of the factors in a complete factorisation is not uniquely determined. However, we shall see that the factors themselves are uniquely determined. Since there is exactly one 1-cycle (i) for every i fixed by α, it suffices to prove uniqueness of the cycles of length at least 2. Suppose $\alpha = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$ is a second complete factorisation into disjoint cycles. If β_t moves i_1, then $\beta_t^k(i_1) = \alpha^k(i_1)$ for all k by Theorem 1.2.2-1. Now, some γ_j must move i_1; since disjoint cycles commute, we may assume that $\gamma_j = \gamma_s$. But $\gamma_s^k(i_1) = \alpha^k(i_1)$ for all k, and so Theorem 1.2.2-2 gives $\beta_t = \gamma_s$. We thus have $\beta_1 \circ \beta_2 \circ \cdots \circ \beta_{t-1} = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{s-1}$, and the pf is complete by induction on $\max\{s, t\}$. ■

2 Basic Algebra (MATH 135)

We now review some of the most important concepts learnt in MATH 135.

Definition 2.0.2 Divisibility

An integer m **divides** an integer n, and we write $m \mid n$, if there exists an integer k such that $n = km$. m is called the **divisor**.

Theorem 2.0.2 Divisibility Theorems

Here is a summary of facts about divisibilty.

1. (Transitivity) Let a, b, and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.
2. (Divisibility of Integer Combinations) If a, b, and c are integers such that $a \mid b$ and $a \mid c$, and x and y are any integers, then $a \mid (bx + cy)$.
3. (Bounds by Divisibility) Let a and b be integers. If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

Theorem 2.0.3 Division Algorithm

If a and b are integers, and $b > 0$, then there exist *unique* integers q and r such that

$$a = qb + r, \quad 0 \leq r < b.$$

q is called the **quotient** and r is called the **remainder**.

REMARK: Note that the integer r is always strictly less than b. As well, the integer r is always positive or zero. Finally, observe that $b \mid a$ if and only if $r = 0$.

Definition 2.0.3 Prime and Composite Number

An integer $p > 1$ is called a **prime number** if its only positive divisors (i.e., divisors strictly greater than zero) are 1 and p. If this is not the case, the p is called a **composite number**.

Definition 2.0.4 Greatest Common Divisor (gcd)

Let a and b be integers not both zero. An integer $d > 0$ is the **greatest common divisor** (gcd) of a and b, written $\gcd(a, b)$ if and only if

1. $d \mid a$ and $d \mid b$ (this captures the *common* part of the definition), and
2. if $c \mid a$ and $c \mid b$, then $c \leq d$ (this captures the *greatest* part of the definition).

An equivalent definition is as follows: the greatest common divisor of two integer a and b is smallest positive integer d that can be written in the form $d = ap + bq$ where p and q are integers. Any other such integers must be multiples of d.

Example 2.0.1 Here are some examples of gcds:

- $\gcd(24, 30) = 6$
- $\gcd(17, 25) = 1$
- $\gcd(-12, 0) = 12$
- $\gcd(-12, -12) = 12$
- $\gcd(0, 0) = 0$ (by convention)

Theorem 2.0.4

Here are some important properties of the greatest common divisor.

1. $\gcd(a, 0) = |a|$
2. If m is a non-negative integer, then $\gcd(ma, mb) = m\gcd(a, b)$.
3. If m is any integer, then $\gcd(a + mb, b) = \gcd(a, b)$.
4. If m is a non-zero common divisor of a and b, then $\gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a,b)}{m}$.
5. $\gcd(a, b) = \gcd(b, a)$, i.e., the gcd is commutative.
6. $\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$, i.e., the gcd is associative.
7. The greates common divisor of three numbers can be computed as $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$, or in some different way by applying commutativity and associativity. This can be extended to the gcd of any number of numbers.

Theorem 2.0.5 GCD with Remainders

If a and b are integers not both zero, and q and r are integers such that $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Theorem 2.0.6 GCD Characterisation Theorem

If d is a positive common divisor of the integers a and b, i.e., $d \mid a$ and $d \mid b$, and there exists integers x and y such that $ax + by = d$, then $d = \gcd(a, b)$.

Theorem 2.0.7 Extended Euclidean Algorithm

If $a > b > 0$ are positive integers, then $d = \gcd(a, b)$ can be computed, and there exist integers x and y such that $ax + by = d$.

Definition 2.0.5 Coprime Numbers

Two integers a and b are **coprime** if $\gcd(a, b) = 1$.

Theorem 2.0.8 Coprimeness and Divisibility

If a, b, and c are integers and $c \mid ab$ and $\gcd(a, c) = 1$, i.e., a and c are coprime, then $c \mid b$.

Theorem 2.0.9 Coprimeness and Divisibility 2

If a_1 and a_2 are coprime, then $\gcd(a_1 a_2, b) = \gcd(a_1, b)\gcd(a_2, b)$.

Theorem 2.0.10 Primeness and Divisbility

If p is a prime number and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Theorem 2.0.11

Let a and b be integers. Then $\gcd(a, b) = 1$ if and only if there are integers x and y such that $ax + by = 1$.

Theorem 2.0.12 Division by the GCD

Let a and b be integers. If $\gcd(a, b) = d \neq 0$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Theorem 2.0.13

Let $g = \gcd(a, b)$ for two integers a and b. Then $g \mid a$ and $g \mid b$.

PROOF: Suppose $g = \gcd(a, b)$. This means that there exist integers s and t such that $g = as + bt$ is the smallest linear combination of a and b. Assume for a contradiction that $g \nmid a$. This means that $a = gu + r$ for some integers u and r, $0 \leq r < g$, or $r = a - ug = a - u(as + bt) =$

$a(1-us)-utb$. Since $r < g$, we have found a smaller integer that is a linear combination of a and b, a contradiction, since we assumed $g = \gcd(a,b)$, which implies that g is the smallest such integer. Hence $g \mid a$. A similar argument for b proves $g \mid b$. ■

Theorem 2.0.14

Let $n, k \in \mathbb{Z}$. Then

$$\gcd\left(\frac{n}{\gcd(n,k)}, \frac{k}{\gcd(n,k)}\right) = 1$$

PROOF: By definition of the gcd, there exist integers p and q such that d is the smallest integer satisfying

$$d = \frac{n}{\gcd(k,n)}p + \frac{k}{\gcd(k,n)}q = \frac{1}{\gcd(k,n)}(np+kq).$$

But $g = \gcd(k,n)$ is the smallest integer satisfying $g = nu + kv$ for integers u and v. Now, since we are looking for the smallest d, we must have that $np+kq$ is in fact $\gcd(k,n)$, i.e., that $u, v = p, q$, so that

$$\gcd\left(\frac{n}{\gcd(n,k)}, \frac{k}{\gcd(n,k)}\right) = \frac{1}{\gcd(k,n)}\gcd(k,n) = 1,$$

as required. ■

3 Modular Arithmetic (MATH 135)

We now take some time to review modular arithmetic, which was studied in MATH 135.

Modular arithmetic is the arithmetic of congruences, specifically, the arithmetic of congruent integers. Modular arithmetic is also informally known as "clock arithmetic". In modular arithmetic, numbers wrap around upon reaching a given fixed quantity, called the **modulus**, which would be 12 in the case of hours on a clock, or 60 in the case of minutes or seconds on a clock.

3.1 Integer Congruence

Definition 3.1.1 Congruent Integers

Let m be a fixed positive integer, the modulus. If $a, b \in \mathbb{Z}$, we say that a is **congruent** to b **modulo** m and write

$$a \equiv b \mod m \tag{3.1}$$

if $m \mid (a - b)$, i.e., if m divides $(a - b)$ If m does not divide $(a - b)$, then we write $a \neq b \mod m$.

Example 3.1.1 Let's now go through some examples of these congruences:

- $38 \equiv 14 \mod 12$ because $38 - 14 = 24$, which is a multiple of 12, i.e., $12 \mid 24$.
- We can also write congruences for negative integers; for example, $-8 \equiv 7 \mod 5$.
- $2 \equiv -3 \mod 5$.
- $5 \neq 3 \mod 7$.

REMARK: Observe that congruence relations for integers are not unique. For instance, in the above example, instead of $38 \equiv 14 \mod 12$, we could have written $38 \equiv 24 \mod 12$. This second representation may seem more intuitive to you, because it more closely resembles the way we keep track of time on a 12-hour clock. For instance, we know that instead of saying that the time is 13 o'clock we say that it is 1 o'clock in the afternoon. We can say this because $13 \equiv 1 \mod 12$, i.e., 1 is the number of hours by which we must increase 12 to get the current time. Similarly, we have $14 \equiv 2 \mod 12$, which is why 14 o'clock is equivalent to 2 o'clock in the afternoon, etc.

Back to $38 \equiv 24 \mod 12$, a "better" representation would be $38 \equiv 2 \mod 12$. We will see why this third representation is better shortly.

Theorem 3.1.1 Conguence is an Equivalence Relation

Let $a, b, c \in \mathbb{Z}$. Then,

1. $a \equiv a \bmod m$. (Reflexivity)
2. If $a \equiv b \bmod m$, then $b \equiv a \bmod m$. (Symmetry)
3. If $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $a \equiv c \bmod m$. (Transitivity)

In other words, the congruence relation satisfies the three properties of an *equivalence relation.*

Theorem 3.1.2

$a \equiv b \bmod m$ if and only if a and b have the same remainder when divided by m.

Theorem 3.1.3 Congruences and Division

If $ac \equiv bc \bmod m$, and $\gcd(c, m) = 1$, then $a \equiv b \bmod m$.

3.2 Motivating Modular Arithmetic

Now, we all know that the set of integers can be broken up into the following two classes:

- The *even numbers* $\{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$.
- The *odd numbers* $\{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$.

There are certain generalisations we can make about the arithmetic of numbers based on which of these two classes they come from. For example, we know that the sum of two even numbers is even; the sum of an even number and an odd number is odd; the sum of two odd numbers is even; the product of two even numbers is even; and the product of two odd numbers is odd.

Modular arithmetic lets us state these results quite precisely, and it also provides a convenient language for similar but slightly more complex statements. Now, notice that $-4 \equiv 0 \bmod 2$, $2 \equiv 0 \bmod 2$, $1 \equiv 1 \bmod 2$, etc., i.e., all of the even numbers are conguent to each other *modulo 2* and all the odd numbers are congruent to each other *modulo 2.* So we can think of the modulus as the number of classes into which we have broken the integers. Note that it is also the difference between any two "consecutive" numbers in a given class. Even better, we have that *all of the even numbers are congruent to 0 modulo 2*, and *all of the odd numbers are congruent ot 1 modulo 2.*

Let us thus represent each of our two classes by a single symbol. Let [0] mean "the class of all even numbers" and the symbol [1] mean "the class of all odd numbers". In the same way that congruence relations of integers are not unique, there is no great reason for choosing [0] and [1] for our symbols–we could have chosen [2] and [1], or [-32] or [177], but [0] and [1] are the conventional choices.

The statement "the sum of two even numbers is even" can then be expressed by

$$[0] + [0] \equiv [0],$$

since we just said that all even numbers are congruent to 0 modulo 2. Similarly, the statement "the sum of an even number and an odd number is odd" is represented by

$$[0] + [1] \equiv [1],$$

since we just said that all odd numbers are congruent to 1 modulo 2. We can also write "the sum of two odd numbers is even" as

$$[1] + [1] \equiv [1].$$

We have analogous statements for multipliction of even and odd numbers:

$$[0] \times [0] \equiv [0]$$
$$[1] \times [1] \equiv [0]$$
$$[1] \times [1] \equiv [1].$$

In a sense, we have created a number system with addition and multiplication in which the only "numbers" that exist are [0] and [1]. This number system is called the system of *integers modulo 2*, and because of the previous six properties shown above, *any arithmetic done in the integers translates to arithmetic done in the integers modulo 2.*

Now, suppose we want to know which integers might solve the *diophantine equation*

$$3a - 3 = 12.$$

Since, for any integer a, $3a$ will be an odd number, we can reduce this equation modulo 2 to write

$$[1]a + [1] = [0] \Rightarrow a = [0] - [1] = [-1] \equiv [1],$$

so any integer a satisfying the equation $3a - 3 = 12$ must be odd.

> Remark: We have not quite justified or fully explained yet what it means to add or subtract these classes of even and odd numbers labelled [0] and [1], though hopefully at this point it seems plausible that they work similarly to regular integers, which is why they are being used as such.

Since any integer solution of an equation reduces to a solution modulo 2, it follows that if there is not solution modulo 2, then there is no solution in integers. For example, assume that a is an integer solution to

$$2a - 3 = 12,$$

which reduces to

$$[0]a + [1] = [0] \Rightarrow [1] = [0],$$

which is a contradiction, since [0] and [1] are different numbers modulo 2 (no even number is an odd number, and vice versa). So a cannot be an integer. Let's now consider the system of equations

$$6a - 5b = 4$$
$$2a + 3b = 3.$$

Modulo 2, these equations reduce to

$$[0]a - [1]b = [0]$$
$$[0]a + [1]b = [1].$$

This says that b is both even and odd, which is a contradiction. Therefore, we know that the original system of equations has no integer solution, and to prove this we didn't even need to know anything about a.

3.3 The Integers Modulo m

We now formalise and generalise everything about modular arithmetic that we have just seen.

Definition 3.3.1 Congruence Class

The **congruence class modulo** m of the integer a is the set of integers $[a] = \{x \in \mathbb{Z} \,|\, x \equiv a \bmod m\}$.

Example 3.3.1 We have that when $m = 2$,

$$[0] = \{x \in \mathbb{Z} \,|\, x \equiv 0 \bmod 2\} = \{\ldots, -8, -4, -6, -2, 0, 2, 4, 6, 8, \ldots\},$$

which are indeed all the even integers, as we knew from before. And

$$[1] = \{x \in \mathbb{Z} \,|\, x \equiv 1 \bmod 2\} = \{\ldots, -7, -5, -3, -1, 1, 3, 5, 7, 9, \ldots\},$$

which are indeed all the odd numbers, as we knew from before. Recall that we mentioned that the classes [0] and [1] are not unique representations of the even and odd numbers. We can see this quite clearly now. Notice that

$$[2] = \{x \in \mathbb{Z} \,|\, x \equiv 2 \bmod 2\} = \{\ldots, -4, -6, -2, 0, 2, 4, 6, 8, 10, \ldots\},$$

which is just the set of even integers, and

$$[3] = \{x \in \mathbb{Z} \,|\, x \equiv 3 \bmod 2\} = \{\ldots, -5, -3, -1, 1, 3, 5, 7, 9, 11, \ldots\},$$

which is just the set of odd numbers. So $[0] = [2]$ and $[1] = [3]$.

Remark: In fact, $\cdots = [-4] = [-2] = [0] = [2] = [4] = \cdots$ and $\cdots = [-5] = [-3] = [-1] = [1] = [3] = [5] = \cdots$, so that each congruence class has an infinite number of representations.

Example 3.3.2 When $m = 4$, we have

$$[0] = \{x \in \mathbb{Z} \,|\, x \equiv 0 \bmod 4\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\} = \{4k \,|\, k \in \mathbb{Z}\}$$
$$[1] = \{x \in \mathbb{Z} \,|\, x \equiv 1 \bmod 4\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\} = \{4k + 1 \,|\, k \in \mathbb{Z}\}$$
$$[2] = \{x \in \mathbb{Z} \,|\, x \equiv 2 \bmod 4\} = \{\ldots, -6, -2, 2, 6, 10, \ldots\} = \{4k + 2 \,|\, k \in \mathbb{Z}\}$$
$$[3] = \{x \in \mathbb{Z} \,|\, x \equiv 3 \bmod 4\} = \{\ldots, -5, -1, 3, 7, 11, \ldots\} = \{4k + 3 \,|\, k \in \mathbb{Z}\}.$$

And again, we have $\cdots = [-8] = [-4] = [0] = [4] = [8] = \cdots$, $\cdots = [-7] = [-3] = [1] = [5] = [9] = \cdots$, $\cdots = [-6] = [-2] = [2] = [6] = [10] = \cdots$, and $\cdots = [-5] = [-1] = [3] = [7] = [11] = \cdots$.

Definition 3.3.2 The Integers Modulo m

We define $\mathbb{Z}_m$, the **integers modulo** m to be the set of m congruence classes,

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}, \tag{3.2}$$

and we define two operations on $\mathbb{Z}_m$ for $[a], [b] \in \mathbb{Z}_m$,

$$\begin{aligned} [a] + [b] &= [a + b] \qquad \text{(Addition modulo } m\text{)} \\ [a] \cdot [b] &= [a \cdot b] \qquad \text{(Multiplication modulo } m\text{)}, \end{aligned} \tag{3.3}$$

which are the definitions of addition and multiplication in $\mathbb{Z}_m$.

Remark: Notice that $\mathbb{Z}_m$ only include the equivalence classes up to $[m-1]$. As we have already seen, the reason for this is that $[m] = [0]$, $[m+1] = [1]$, etc.

Remark: Though the definition of addition and mulplication may seem obvious, especially since we have already used them, there is a fair amount going on here:

1. Sets are being treated as individual "numbers". Modular addition and multiplication are being performed on congruence classes, which, remember, are sets.
2. The addition and multiplication symbols and the left-hand side of the equal sign in Equation (3.3) are in $\mathbb{Z}_m$ and those on the right-hand side are operations in $\mathbb{Z}$.
3. We are assuming that the operations are *well-defined*. That is, we are assuming that these operations make sense even when there are multiple representations of a congruence class.

Remark: Since $[a] = \{x \in \mathbb{Z} \mid x \equiv a \bmod m\}$, we have that

$$[a] = [b] \Rightarrow a \equiv b \bmod m \tag{3.4}$$

for any $[a], [b] \in \mathbb{Z}_m$.

Theorem 3.3.1

For any $[a], [b], [c] \in \mathbb{Z}_m$, we have

- The Commutative Laws:

$$[a] + [b] = [b] + [a] \qquad [a] \cdot [b] = [b] \cdot [a]$$

- The Associative Laws:

$$[a] + ([b] + [c]) = ([a] + [b]) + [c] \qquad [a] \cdot ([b] \cdot [c]) = ([a] \cdot [b]) \cdot [c]$$

- The Distributive Law:

$$[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$$

PROOF: These can be easily proven using the definition of addition and multiplication modulo m and the properties of $\mathbb{Z}$. ■

Theorem 3.3.2 Addition Identity in $\mathbb{Z}_m$

The identity under addition in $\mathbb{Z}_m$ is $[0]$, just like 0 is the identity under addition in $\mathbb{Z}$.

PROOF: This follows immediately from the definition:

$$\begin{gathered} \forall [a] \in \mathbb{Z}_m,\ [a] + [0] = [a + 0] = [a] \\ \forall [a] \in \mathbb{Z}_m,\ [a] \cdot [0] = [a \cdot 0] = [0]. \end{gathered} \tag{3.5}$$

In other words, $[0]$ behaves just like 0. ■

Theorem 3.3.3 Additive Inverse in $\mathbb{Z}_m$

For any $[a] \in \mathbb{Z}_m$, its additive inverse is $[a]^{-1} = [-a]$.

PROOF: We have

$$[a] + [-a] = [a - a] = [0],$$

by the definition of addition in $\mathbb{Z}_m$. Since $[0]$ is the additive identity in $\mathbb{Z}_m$ by the above theorem, by the definition of the inverse, $[a]^{-1} = [-a]$ is the additive inverse of [a]. ■

Theorem 3.3.4 Multiplication Identity in $\mathbb{Z}_m$

The identity under multiplication in $\mathbb{Z}_m$ is $[1]$, just like 1 is the identity under multiplication in $\mathbb{Z}$.

PROOF: Again, this follows immediately from the definition:

$$\forall [a] \in \mathbb{Z}_m,\ [a] \cdot [1] = [a \cdot 1] = [a]. \tag{3.6}$$

In other words, [1] behaves just like 1. ■

Unlike the additive inverse, there does not exist a specific form for the multiplicative inverse of a number $[a] \in \mathbb{Z}_m$. By definition, the multiplicative inverse of any $[a] \in \mathbb{Z}_m$ is a number $[a]^{-1}$ such that $[a] \cdot [a]^{-1} = [1]$, since [1] is the multiplicative identity in $\mathbb{Z}_m$. Unlike addition in $\mathbb{Z}_m$, in which every element has an additive inverse, it is not always the case that a non-zero element in $\mathbb{Z}_m$ has a multiplicative inverse.

Definition 3.3.3 Coprime

To integers a and b are **coprime**, or **relatively prime** or **mutually prime**, if the only positive integer that divides both of them is one. This is equivalent to stating that the greatest common divisor of a and b is one, denoted $\gcd(a, b) = 1$.

Theorem 3.3.5 Multiplicative Inverse in $\mathbb{Z}_m$

The multiplicative inverse of $[a] \in \mathbb{Z}_m$ exists if and only if a and m are coprime, i.e., if and only if $\gcd(a, m) = 1$.

With these theorems, we can now define subtraction and division in $\mathbb{Z}_m$. These definitions are just like those in $\mathbb{Z}$: subtraction is addition of the inverse, and division is multiplication by the inverse (if the inverse exists!).

Definition 3.3.4 Subtraction in $\mathbb{Z}_m$

Subtraction of any two elements $[a], [b] \in \mathbb{Z}_m$ is defined as the addition of [a] with the (additive) inverse $[b]^{-1} = [-b]$ of $[b]$, i.e.,

$$[a] - [b] = [a] + [-b] = [a - b]. \tag{3.7}$$

Definition 3.3.5 Division in $\mathbb{Z}_m$

Division of any two elements $[a], [b] \in \mathbb{Z}_m$ is defined as multiplication by the (multiplicative) inverse $[a]^{-1}$ of $[a]$, assuming that this inverse exists.

Example 3.3.3 The modulus $m = 12$ comes up quite frequently in everyday life, and its application illustrates a good way to think about modular arithmetic. With $m = 12$, we there are only twelve numbers we every need to think about: $\mathbb{Z}_{12} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\}$ by definition of $\mathbb{Z}_m$, although for this example we may also equivalently take $\mathbb{Z}_{12} = \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]\}$ since we know that [0]=[12]. These numbers represent the twelve equivalence classes modulo 12. So

every integer is congruent to *exactly one* of the numbers 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, just as the hour on the clock always reads exactly one of $1, 2, \ldots, 12$.

Now, if its 7 o'clock currently, what time will it be in 25 hours?

SOLUTION: Since $25 \equiv 1 \bmod 12$, we have, using (3.4),

$$[7] + [25] = [7] + [1] = [7 + 1] = [8],$$

so the clock will read 8 o'clock. Note that this gives no indication of the time of day we are in (day or night).

REMARK: It is customary to drop the square brakets from the modular numbers when the context is clear, so that we could have written $7 + 25 = 7 + 1 = 8$. Or, we may write

$$7 + 25 \equiv 7 + 1 \equiv 8 \pmod{12}$$

REMARK: The minutes and seconds on a clock are also modular. In these cases the modulus is $m = 60$. If we think of the days of the week as labelled by the numbers $[0], [1], [2], [3], [4], [5], [6], [7]$, then the modulus is $m = 7$. The point is that we measure many things, both in mathematics and in daily life, that are periodic in some sense, and this can usually be thought of as an application of modular arithmetic.

Part II

The Course Material

4 Groups

We now start learning about the concept of a group. Several sources contributed to the emergence of the *abstract group* concent. First, understanding the different deep properties of the intergers was one of the most ancient preoccupations of mathematicians. Further, finding solutions to polynomial equations was for many centuries another important source of mathematical problems. Finally, the study of transformations of geometric objects gave rise to new ideas in the development of mathematics in modern times. These three mathematical disciplines–number theory, the theory of algebraic equations, and the theory of geometric transformations–all contributed to the development of what in present-day mathematics is called the concept of an abstract group, or simply of a *group*.

4.1 Basic Concepts

Definition 4.1.1

A binary **operation** on a nonempty set S is a function $\mu : S \times S \to S$, denoted $*$, such that for all $\alpha, \beta \in S$, $\alpha * \beta \in S$.

REMARK: The composition operation between mappings, $\circ$, seen in Chapter 1, was an example of a binary operation.

The operation $*$ assigns to each ordered pair (a, b) of elements of S a third element of S, $\mu(a, b) = a * b$. We regard this operations as a "multiplication" of the elements of G.

As we have already seen with permutations, it is quite possible that $a * b$ and $b * a$ are distnct elements of S.

Definition 4.1.2 Commutatitvity of $*$

Let $*$ be a binary operation on a set S. $*$ is said to be **commutative** if $\alpha * \beta = \beta * \alpha$ for all $\alpha, \beta \in S$.

How can we multiply three elements of S? Given (not necessarily distinct) elements $a_1, a_2, a_3 \in S$, the expression $a_1 * a_2 * a_3$ is ambiguous: since we can $*$ only two element of S at a time, we have the option of doing first $a_1 * a_2$ then multiplying the result of this with a_3, to get $(a_1 * a_2) * a_3$, or first doing $a_2 * a_3$ then multiplying a_1 by its result, so that we get $a_1 * (a_2 * a_3)$. In general, $a_1 * (a_2 * a_3)$ and $(a_1 * a_2) * a_3$ may be different. If S is the set of all integers (positive, negative, and zero), and we let $*$ be subtraction $-$, then any choice of integers a, b, c with $c \neq 0$ results in $(a - b) - c \neq a - (b - c)$.

Definition 4.1.3 Associativity of $*$

An operation $*$ on a set S is **associative** if

$$(a * b) * c = a * (b * c)$$

for every $a, b, c \in S$.

REMARK: We have seen that the composition operation on both permutations and symmetry transformations is associative.

Theorem 4.1.1 Generalised Associativity

If $*$ is an associative operation on a set S, then every expression $a_1 * a_2 * \cdots * a_n$ needs to parenthesis, i.e., no matter what choices of multipliation of adjacent factors are made, the resulting elements of S are all equal.

4.2 The Definition of a Group and Examples

Definition 4.2.1 Group

A **group** $G = (S, *)$ is a set S along with a binary operation $*$, which satisfies the **group axioms**:

- For all $\alpha, \beta \in S$, $\alpha * \beta \in S$. (Closure under $*$)
- For all $\alpha, \beta, \gamma \in S$, $\alpha * (\beta * \gamma) = (\alpha * \beta) * \gamma$. (Associativity)
- There exists an element $\mathcal{I}_S \in S$ such that for all $\alpha \in S$ $\alpha * \mathcal{I}_S = \mathcal{I}_S * \alpha = \alpha$. (Identity)
- For all $\alpha \in S$ there exists a $\beta \in S$ such that $\alpha * \beta = \mathcal{I}_S$. β is the inverse of α, and is denoted $\beta = \alpha^{-1}$. (Inverse)

Definition 4.2.2 Abelian Group

Let $G = (S, *)$ be a group. If for every $\alpha, \beta \in S$ $\alpha * \beta = \beta * \alpha$, i.e., $*$ is commutative, then G is said to be an **Abelian group** or simply **Abelian**.

Definition 4.2.3 Powers of Group Elements

If $G = (S, *)$ is a group and $a \in S$, then the nth **power** of a is $a^n = a * a * \cdots * a$. a^{-n} is the inverse of a^n. We also let $a^0 = a^{-1} * a = \mathcal{I}_S$, the identity element of S, and $a^1 = a$.

Theorem 4.2.1 Powers of Group Elements

Let $G = (S, *)$ be a group and let $a \in S$ be an element of G. Then,

1. $a^{-n} = \left(a^{-1}\right)^n = a^{-1} * a^{-1} \cdots a^{-1}$.
2. $a^m * a^n = a^{m+n} = a^n * a^m$.
3. $(a^m)^n = a^{mn} = (a^n)^m$.

PROOF: We prove each statement in turn.

1. We have $a^n * \left(a^{-1}\right)^k = a*a*\cdots*a*a^{-1}*a^{-1}*\cdots*a^{-1} = a*a*\cdots*a*\mathcal{I}_S*a^{-1}*a^{-1}*\cdots*a^{-1} = \cdots = \mathcal{I}_S$ by the associativity of $*$.
2.
3. ■

Definition 4.2.4 Group Order

Let $G = (S, *)$ be a group with operation $*$. The **order** of G is the cardinality of the set S, denoted $o(G)$ or $|G|$. If $|G|$ is finite, then G is said to be a **finite group**; otherwise, G is an **infinite group**.

Definition 4.2.5 Order of a Group Element

The element a of the group G is of **order** m, denoted $o(a) = m$ if m is the smallest positive integer such that $a^m = \mathcal{I}_S$. If no such m exists, then a is said to have **infinite order**. In other words, all of the powers of a are distinct.

REMARK: If a is of order m, then all the elements

$$a^0, a, a^2, \ldots, a^{m-1}$$

are distinct. Thus, every other power of a will be equal to one of these elements. Since any integer k can be written as $k = sm + t$, for $0 \leq t < m$, we have

$$a^k = a^{sm+t} = a^{sm}a^t = (a^m)^s\, a^t = \mathcal{I}^s a^t = a^t.$$

From this, we see that if $a^k = \mathcal{I}$, then k is a multiple of m.

REMARK: Note that for any element $a \in G$, $a^n = \mathcal{I} \not\Rightarrow o(a)$ but $a^n = \mathcal{I} \Rightarrow o(a) \leq n$. However $o(a) = n \Rightarrow a^n = \mathcal{I}$.

REMARK: The group $G = (S, *)$ of order one contains one element, the identity $\mathcal{I}_S$ (remember that all groups, by definition, have to contain the identity).

If G is of order two, then S contains two distinct elements, one of which, by definition, must be the identity. Call the second element a. Then $a * a = a^2$ cannot be a since $a^2 = a \Rightarrow a = \mathcal{I}_S$, which would mean that S

contains only one element, a contradiction. So we must have $a^2 = \mathcal{I}_S$, which implies that $a = a^{-1}$, i.e., a is its own inverse.

If G is of order three, then S contains three distinct element, one of which, by definition, is the identity. Call the other two elements a and b. Then $a * b$ cannot equal a or b since this would imply $b = \mathcal{I}_S$ or $a = \mathcal{I}_S$, which is a contradiction. So $a * b$ must equal $\mathcal{I}_S$. Similarly, we have $a^2 = b$, so that $a^3 = \mathcal{I}_S$, i.e., a is of order three. So a group of order three consists of the elements $a, a^2, a^3 = \mathcal{I}_S$. This is an example of a **cyclic** group, one which consists of the powers of a single element.

REMARK: It can be shown that if G is a finite group, then there exists a positive integer m such that $a^m = 1$ for all $a \in G$.

Example 4.2.1 Below are several examples of groups.

- $(\mathbb{Z}, +)$, the set of all integers under the operation of addition, is a group since addition of integers give other integers, $0 \in \mathbb{Z}$ is the identity element, and for every element $a \in \mathbb{Z}$, $a^{-1} = -a$ is the inverse of a. Addition is also clearly associative. $|(\mathbb{Z}, +)| = \infty$. In addition, every non-zero element of this group has infinite order.
- $(2\mathbb{Z}, +)$, the set of all even integers under addition, is also a group because the sum of two even integers is again even. More generally, $(n\mathbb{Z}, +)$ is a group for any n. (Notice that the set all odd integers under addition is *not* a group since the sum of two odd numbers is *even* (e.g., $1 + 3 = 4$)). $|(2\mathbb{Z}, +)| = \infty$. Again, every element of the group has infinite order.
- $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, the rational, real, and complex numbers under addition, are all groups. $|(\mathbb{Q}, +)| = |(\mathbb{R}, +)| = |(\mathbb{C}, +)| = \infty$, with each element of each group having infinite order.
- $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ under addition modulo n is a group. $[0]$ is the identity element, and for each $[a] \in \mathbb{Z}_n$, its inverse element in $[a]^{-1} = [-a]$, as we saw in Chapter 2. $|(\mathbb{Z}_n, +)| = n$. For every element $[a]$ in the group, its order is $o([a]) = \frac{n}{\gcd(a,n)}$. For example, for $n = 20$, $o([5]) = 4$, $o([2]) = 10$, and $o([30]) = 2$.
- Let $M(2, \mathbb{R})$ be the set of all 2×2 matrices with real entries. Then $(M(2, \mathbb{R}), +)$ is a group under addition of matrices. $|(M(2, \mathbb{R}), +)| = \infty$.

Note that all of these groups are Abelian, as can be verified by using the commutativity of addition in $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}$.

Example 4.2.2 Below are some examples of *non groups*.

- $(\mathbb{Z}, \times)$, the set of integers under multiplication, is not a group because there is no inverse element, i.e., for any $a, b \neq \pm 1$ there is no *integer* such that $a \times b = 1$. Indeed,

the multiplicative inverse of an integer a is $\frac{1}{a}$, which is not an integer except for when $a = \pm 1$.

- $(\mathbb{Q}, \times)$, the set of rational numbers under multiplication, is not a group. For though the rational numbers are closed under multiplication, multiplication is associative, there is a multiplivative identity, 1, and every *non-zero* rational number a has the multiplicative inverse $\frac{1}{a}$, the rational number 0 has no multiplicative inverse. The same goes for $(\mathbb{R}, \times)$ and $(\mathbb{C}, \times)$.
- $(\mathbb{Z}_n, \times)$, the set of integers modulo n under multiplication modulo n, is not a group. The reason for this is that elements in $\mathbb{Z}_n$ generally do *not* have an inverse (see Chapter 2).

REMARK: The example above shows that a set may form a group under one operation and not another, which is why we consider a group as a pair, the set and the operation. Often, however, when it is understood what operation we have in mind, we speak simply of the group G.

Example 4.2.3 If we consider the set

$$\mathbb{Q}^* = \mathbb{Q} - \{0\}$$

of all nonzero rational numbers, then $\mathbb{Q}^*$ is closed under multiplication. Similarly, the sets

$$\mathbb{R}^* = \mathbb{R} - \{0\} \qquad \text{and} \qquad \mathbb{C}^* = \mathbb{C} - \{0\}$$

are closed under multiplication. Therefore, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, and $(\mathbb{C}^*, \times)$ are all groups, in particular, Abelian groups. $|(\mathbb{Q}^*, \times)| = |(\mathbb{R}^*, \times)| = |(\mathbb{C}, \times)| = \infty$.

Example 4.2.4 Recall Theorem 3.3.5, which says that two elements $[a], [b] \in \mathbb{Z}_n$ have a multiplicative inverse if and only if a and b are coprime. Now, consider the set

$$\mathbb{Z}_n^* = \{[a] \,|\, \gcd(a, b) = 1\}.$$

For example,

$$\begin{aligned}
\mathbb{Z}_6^* &= \{[1], [5]\} \\
\mathbb{Z}_7^* &= \{[1], [2], [3], [4], [5], [6]\} \\
\mathbb{Z}_8^* &= \{[1], [3], [5], [7]\}
\end{aligned}$$

Now, let $U(n) = (\mathbb{Z}_n^*, \times)$, where $\times$ represents multiplication modulo n. Now, notice that for any elements $[a], [b] \in \mathbb{Z}_7^*$ $[a] \times [b] \in \mathbb{Z}_7^*$. For example, $[1] \times [2] = [1 \times 2] = [2] \in \mathbb{Z}_7^*$, and $[3] \times [4] = [3 \times 4] = [12] = [5] \in \mathbb{Z}_7^*$. Also, since 1 is coprime with all integers, $[1] \in \mathbb{Z}_n^*$ is the identity element. Also, every element in $\mathbb{Z}_n^*$ has an inverse in $\mathbb{Z}_n^*$. For

example, consider $\mathbb{Z}_7^*$ again. Observe that $[2] \times [4] = [8] = [1]$, so that $[2]^{-1} = [4] \in \mathbb{Z}_7^*$ and $[3] \times [5] = [15] = [1]$, so that $[3]^{-1} = [5] \in \mathbb{Z}_7^*$. Finally, since multiplication modulo n is associative and commutative, we have that $U(n) = (\mathbb{Z}_n^*, \times)$ is an Abelian group under multiplication modulo n. $|U(n)| = \phi(n)$, where ϕ is the *Euler phi function*.

Definition 4.2.6 The Euler Phi Function

Euler's Phi Function, or **Euler's Totient Function**, is an arithmetic function that counts the number of positive integers less than or equal to n that are coprime to n. For a prime number p, $\phi(p) = p-1$. For example, $\phi(7) = 7-1 = 6$.

Example 4.2.5 Consider the group $U(16) = (\mathbb{Z}_{16}^*, \times)$ where $\times$ represents multiplication modulo 16. We have

$$\mathbb{Z}_{16}^* = \{[1], [3], [5], [7], [9], [11], [13], [15]\},$$

so that $|U(16)| = 8$. Let us construct the multiplication table for $\mathbb{Z}_{16}^*$:

$\times$	[1]	[3]	[5]	[7]	[9]	[11]	[13]	[15]
[1]	[1]	[3]	[5]	[7]	[9]	[11]	[13]	[15]
[3]	[3]	[9]	[15]	[5]	[11]	[1]	[7]	[13]
[5]	[5]	[15]	[9]	[3]	[13]	[7]	[1]	[11]
[7]	[7]	[5]	[3]	[1]	[15]	[13]	[11]	[15]
[9]	[9]	[11]	[13]	[15]	[1]	[3]	[5]	[7]
[11]	[11]	[1]	[7]	[13]	[3]	[9]	[15]	[5]
[13]	[13]	[7]	[1]	[11]	[5]	[15]	[9]	[3]
[15]	[15]	[13]	[11]	[9]	[7]	[5]	[3]	[1]

We can see that $o([1]) = 1$ and $o([7]) = o([9]) = o([15]) = 2$. And since $[3]^2 = [5]^2 = [11]^2 = [13]^2 = [9]$, we get that $o([3]) = o([5]) = ([11]) = o([13]) = 4$. So there is one element of order one, three elements of order two, and four elements of order four. ◀

Example 4.2.6 The 3rd and 4th Roots of Unity Let us find the roots of the polynomial $f(x) = x^3 - 1$ in $\mathbb{C}$. Note that $f(x)$ can be factored as $f(x) = (x-1)\left(x^2 + x + 1\right)$. Then, if we use the quadratic formula, we find that $\omega = \frac{1}{2}\left(-1 + i\sqrt{3}\right)$ and $\omega^2 = \frac{1}{2}\left(-1 - i\sqrt{3}\right)$ are the two complex roots of $x^2 + x + 1$ (note that they are *complex conjugates* of one another. Hence, the roots of $f(x)$, the third roots of unity, are $\sqrt[3]{1} = \left\{1, \omega, \omega^2\right\}$. If we use the usual multiplication of complex numbers, we obtain the following multiplication table.

$\sqrt[3]{1}$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Let us also find the roots of $f(x) = x^4 - 1$ in $\mathbb{C}$. Note that $f(x)$ can be factored as $\left(x^2-1\right)\left(x^2+1\right) = (x-1)(x+1)(x-i)(x+i)$. So the four roots of $f(x)$, the fourth roots of unity, are $\sqrt[4]{1} = \{1, -1, i, -i\}$ (again, note that the two complex roots are complex conjugates of one another). Again, using the usual multiplication of complex numbers, we obtain the following multiplication table for the roots.

$\sqrt[4]{1}$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

In both cases, notice that the product of any two roots gives another root. Additionally, multiplication by the root 1 does not change the root, and that multiplication of a root by its complex conjugate gives 1. And multiplication, as we know, is an associative operation. Hence, the identity element in the sets $\sqrt[3]{1}$ and $\sqrt[4]{1}$ is 1 and the inverse of a root a in $\sqrt[3]{1}$ and $\sqrt[4]{1}$ is $\overline{a}$, the complex conjugate of a. So under $\times$, multiplication in $\mathbb{C}$, $\left(\sqrt[3]{1}, \times\right)$ and $\left(\sqrt[4]{1}, \times\right)$ are Abelian groups. ◀

REMARK: In fact, $\left(\sqrt[n]{1}, \times\right)$, the group consisting of the set of the nth roots of unity, is also an Abelian group, where $\sqrt[n]{1} = \left\{1, \omega, \omega^2, \ldots, \omega^{n-1}\right\}$ and $\omega = e^{i\frac{2\pi}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$.

Theorem 4.2.2 Basic Group Properties

For any group $G = (S, *)$:

1. The identity element $\mathcal{I}_S$ is unique.
2. For every $a \in S$, the inverse a^{-1} is unique.
3. For every $a \in S$, $\left(a^{-1}\right)^{-1} = a$.
4. For every $a, b \in S$, $(a * b)^{-1} = b^{-1} * a^{-1}$.
5. For every $a, b \in S$, the equations $a*x = b$ and $y*a = b$ have unique solutions. These are the **right** and **left cancellation laws**. In general, the right and left cancellation laws are $a * b = c * b \Rightarrow a = c$ and $b * a = b * c \Rightarrow a = c$, respectively.

PROOF: We prove each in turn.

1. Let $\mathcal{I}_S$ and $\mathcal{I}'_S$ be identity elements in S. Then $\mathcal{I}_S * \mathcal{I}'_S = \mathcal{I}'_S$ because $\mathcal{I}_S$ is an identity, but also $\mathcal{I}_S * \mathcal{I}'_S = \mathcal{I}_S$ because $\mathcal{I}'_S$ is an identity. Hence, $\mathcal{I}_S = \mathcal{I}'_S$.

2. Let a' and a'' be two inverses in S. Then, using the associativity of $*$, $a' = a' * \mathcal{I}_S = a' * (a * a'') = (a' * a) * a'' = \mathcal{I}_S * a'' = a''$. So the inverse is unique.

3. Since $a^{-1} * a = a * a^{-1} = \mathcal{I}_S$, and since by 2. the inverse of an element in unique, it follows that a is the inverse of a^{-1}, or $\left(a^{-1}\right)^{-1} = a$.

4. Since $\left(b^{-1} * a^{-1}\right) * (a * b) = b^{-1} * \left(a^{-1} * a\right) * b = b^{-1} * \mathcal{I}_S * b = b^{-1} * b = \mathcal{I}_S$ and similarly $(a * b) * \left(b^{-1} * a^{-1}\right) = \mathcal{I}_S$, and since the inverse of an element is unique, it follows that $b^{-1} * a^{-1}$ is the inverse of $a * b$, or $(a * b)^{-1} = b^{-1} * a^{-1}$.

5. For $a, b \in S$, the equation $a * x = b$ implies $a^{-1} * (a * x) = a^{-1} * b$ after multiplying both sides on the left by a^{-1}. Since $a^{-1} * (a * x) = \left(a^{-1} * a\right) * x = \mathcal{I}_S * x = x$, the equation implies $x = a^{-1} * b$. Therefore, x is unique, since a^{-1} is unique. Similarly, the equation $a * y = b$ implies $y = b * a^{-1}$, and y is unique. ■

REMARK: With regards to 5., note that $b * a = c * b \nRightarrow a = c$. In other words, the cancellation has to, in general, be on the same side, since groups are generally not Abelian, i.e., $b * a \neq a * b$.

REMARK (Notation): To ease notation, for a group $G = (S, *)$, is is conventional to write $a * b$ for $a, b \in S$ as simply ab or $a \cdot b$. Additionally, we usually use e or 1 for identity element $\mathcal{I}_S$ of S.

As well, if the group being dealt with is Abelian, then we generally write the inverse of an element a of the group as $-a$ instead of a^{-1} and na instead of a^n.

We now present three very important theorems that will be useful later in the course.

Theorem 4.2.3

Let G be a group and $a \in G$. Suppose $o(a) = n < \infty$. Then the elements $a^0 = 1, a^1, a^2, \ldots, a^{n-1}$ are distinct. (We asserted this in a remark above.)

PROOF: Let $o(a) = n$. Assume for a contradiction that $a^i = a^j$, for $0 \leq i < j < n$. Then $a^{j-i} = a^j a^{-i} = a^i a^{-i} = 1$, which implies that $o(a) \leq j - i < n$, contrary to the assumption that n is the smallest integer such that $a^n = 1$, i.e., contrary to the assumption that $o(a) = n$. Hence $a^i \neq a^j$, and all the elements $1, a^1, a^2, \ldots, a^{n-1}$ are distinct. ■

Theorem 4.2.4

Let G be a group and $a \in G$. Then, for all $i, j \in \mathbb{Z}$, we have:

1. If a has infinite order, i.e., $o(a) = \infty$, then $a^i = a^j$ if and only if $i = j$.
2. If a has finite order, i.e., $o(a) = n < \infty$, then $a^i = a^j$ if and only if n divides $i - j$.

PROOF: We prove each in turn.

1. Suppose a has infinite order. ($\Leftarrow$) If $i = j$, then clearly $a^i = a^j$. ($\Rightarrow$) if $a^i = a^j$, then $a^{i-j} = a^i a^{-j} = a^j a^{-j} = 1$. But since a has infinite order, $a^n = 1$ if and only if $n = 0$, so we have $i - j = 0 \Rightarrow i = j$.
2. Suppose a has finite order $o(a) = n$. ($\Leftarrow$) if n divides $i-j$, so that $i - j = nk \Rightarrow i = nk + j$ for some $k \in \mathbb{Z}$, then we have $a^i = a^{nk+j} = a^{nk}a^j = (a^n)^k a^j = 1^k a^j = ea^j = a^j$. ($\Rightarrow$) Suppose $a^i = a^j$, or, equivalently, $a^{i-j} = 1$. By the division algorithm, we can write $i - j = qn + r$, where $0 \leq r < n$. Then, $1 = a^{i-j} = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = 1^q a^r = 1a^r = a^r$. Since $0 \leq r < n$ and n is, by definition of order, the least positive integer such that $a^n = 1$, we must have $r = 0$, so $i - j = qn$ and $i - j$ is divisible by n. ■

Theorem 4.2.5

Let G be an arbitrary group and $a, b \in G$ and $o(a), o(b) < \infty$ (so we are dealing with finite groups). For any $m, n \in \mathbb{Z}$, if $a^n = 1$ and $a^m = 1$, then $a^d = 1$, where $d = \gcd(m, n)$. In particular, if $a^k = 1$ for some $k \in \mathbb{Z}$, then $o(a) \mid k$.

PROOF: By the Euclidean Algorithm, there exist integers r and s such that $d = mr + ns$, where d is the gcd of n and m. Thus,

$$a^d = a^{mr+ns} = (a^m)^r (a^n)^s = 1^r 1^s = 1.$$

This proves the first assertion.

We have actually already seen the second assertion in one of the remarks above (and is in a sense simply a corollary to the previous theorem). Let us now show it more formally. By the Division Algorithm, there exists $q, r \in \mathbb{Z}$, with $0 \leq r < o(a)$, such that $k = q \cdot o(a) + r$. Therefore,

$$1 = a^k = a^{q \cdot o(a)+r} = \left(a^{o(a)}\right)^q a^r = 1^q a^r = a^r.$$

Now $1 = a^r \Rightarrow r = 0$, so that there exists and integer q such that $k = q \cdot o(a)$, i.e., $o(a) \mid k$ by definition of divisibility. ■

4.3 Special Groups

We now look at some special groups. It turns out that many of the special groups (i.e., groups that are used explicitly in applications) are non-Abelian.

The first example is the group of permutations of n distinct objects, which we have already seen in Chapter 1. The second example is is the dihedral group, which uses the symmetry transformations seen in Chapter 1.

4.3.1 Permutation Groups

We have already discussed these in detail. Recall that we let S_n be the set of permutations of the set $O_n = \{1, 2, 3, \ldots, n\}$. We know that permutations are bijections from O_n to O_n, and so if we let the binary operation $*$ be the composition of the bijections $\circ$, then $(S_n, \circ)$ is a group since, as we have already seen, the composition of mappings is associative. The identity element in S_n is

$$\mathcal{I}_{S_n} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

Now, let $\alpha \in S_n$ be a permutation. As we have seen, we can write in general

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \cdots & \alpha(n) \end{pmatrix},$$

so that the inverse α^{-1} is

$$\alpha^{-1} = \begin{pmatrix} \alpha(1) & \alpha(2) & \alpha(3) & \cdots & \alpha(n) \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

For example,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \Rightarrow \alpha^{-1} = \begin{pmatrix} 3 & 1 & 4 & 2 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

We have also seen that the composition of permutations is not commutative, so that $(S_n, \circ)$ is non-Abelian.

Now, what is $|(S_n, \circ)| = |S_n|$? In other words, how many permutations are there of n *distinct* objects? We have already seen that $|S_n| = n!$, so that $|(S_n, \circ)| = n!$. Also, observe that

$$\begin{aligned} \alpha^2 = \alpha \circ \alpha \circ \alpha \circ \alpha &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \mathcal{I}_{S_5}, \end{aligned}$$

so that α is of order 4, or $o(\alpha) = 4$. However, if we let

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix},$$

then

$$\beta^2 = \beta \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \mathcal{I}_{S_5},$$

so that $o(\beta) = 2$. If $\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$, then

$$\gamma^3 = \gamma \circ \gamma \circ \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \mathcal{I}_{S_5},$$

so that $o(\gamma) = 3$. Now let $\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$, then we get

$$\delta^2 = \delta \circ \delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \mathcal{I}_{S_5},$$

so that $o(\delta) = 2$. Now, let $\epsilon = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$, so that

$$\epsilon^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \mathcal{I}_{S_5},$$

so that $o(\epsilon) = 5$. Finally, let $\zeta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$. Then,

$$\zeta^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}^6 = \mathcal{I}_{S_5},$$

so that $o(\zeta) = 6$. To see what is going on here, it is useful to write all of these permutations in cyclic notation:

$$\alpha = (1\,3\,4\,2)\,(5) \Rightarrow o(\alpha) = 4$$
$$\beta = (1\,2)\,(3)\,(4\,5) \Rightarrow o(\beta) = 2$$
$$\gamma = (1\,2\,3)\,(4)\,(5) \Rightarrow o(\gamma) = 3$$
$$\delta = (1\,2)\,(3)\,(4)\,(5) \Rightarrow o(\delta) = 2$$
$$\epsilon = (1\,3\,4\,2\,5) \Rightarrow o(\epsilon) = 5$$
$$\zeta = (1\,2\,3)\,(4\,5) \Rightarrow o(\zeta) = 6.$$

What we have done is split all of the possible permutations into, including the identity permutation, seven different *cycle types*. With the exception of the cycle type represented by ζ, we see that the order of the permutation is equal to the number of points moved by the permutation. This allows us to compute the number of elements of each order in S_5, then S_n, in general.

Calculating the Number of Elements of a Cycle Type

First, observe that, in the cyclic notation for n=5 shown above, we have *partitioned* the five elements into cycles. For example, β has two 2-cycles and one 1-cycle. Observe that $2\times2+1\times1 = 5 = n$. Let us write this cycle type as

$$(a_1\,a_2)\,(a_3)\,(a_4\,a_5)\,.$$

We can arrange these numbers 1 to 5 in any of 5! ways and then just set them down into the cycles to get a permutation of this cycle type–but then we've overcounted. For instance, since the cycle $(a_1\, a_2)$ is the same as $(a_2\, a_1)$, we've overcounted by a factor of two. In general, each k-cycle will be overcounted by a factor of k. The two 2-cycles cause us to overcount by 4 (each 2-cycle contributes a factor of two).

Since disjoint cycles commute (see Chapter 1), we can switch the 2-cycles above and get the same permutation: $(a_1\, a_2)\,(a_4\, a_5)$ is the same as $(a_4\, a_5)\,(a_1\, a_2)$. There are 2! ways to arrange these cycles, therefore, and so we have overcounted by 2! in this case. So we have

$$\frac{5!}{2 \times 2 \times 2! \times 1} = 15$$

permutations of this cycle type. In general, let's say the cycle type has c_1 1-cycles, c_2 2-cycles, up to c_k k-cycles, where $1c_1 + 2c_2 + \cdots + kc_k = n$. The above case had $c_1 = 1$ and $c_2 = 2$, with $k = 2$. There are $n!$ ways of filling arranging the numbers and placing them in the cycles. We then correct for our overcounting as we did above:

- Each of the c_j j-cycles can be rotated around j ways and be the same cycle, so we divide by j^{c_j} for $j = 1, 2, \ldots, k$.
- There are c_j j-cycles that can be permuted in $c_j!$ ways, so we divide by $c_j!$ for $j = 1, 2, \ldots, k$. (We don't change the position of the cycles.)

Therefore, the number of permutations per cycle type is

$$\frac{n!}{\prod_{i=1}^{k} i^{c_i} \prod_{i=1}^{k} c_i!}. \tag{4.1}$$

The sum of the number of permutations of each cycle type should be $n!$. Let us check to see if this is true for S_5:

$$\begin{aligned}
\text{Identity:} \quad & \frac{5!}{(1)^5\, 5!} = 1 \\
\text{Type } \alpha: \quad & \frac{5!}{[4^1 1!]\,[1^1 1!]} = 30 \\
\text{Type } \beta: \quad & \frac{5!}{[2^2 2!]\,[1^1 1!]} = 15 \\
\text{Type } \gamma: \quad & \frac{5!}{[3^1 1!]\,[1^2 2!]} = 20 \\
\text{Type } \delta: \quad & \frac{5!}{[2^1 1!]\,[1^3 3!]} = 10 \\
\text{Type } \epsilon: \quad & \frac{5!}{5^1 1!} = 24 \\
\text{Type } \zeta: \quad & \frac{5!}{[3^1 1!]\,[2^1 1!]} = 20
\end{aligned}$$

So, indeed, $1 + 30 + 15 + 20 + 10 + 24 + 20 = 120 = 5!$.

Let us now examine a more abstract way of looking at permutation groups, which will help us later on when studying more advanced groups. Consider S_3, the permuation group of three distinct objects $\{1, 2, 3\}$. We know that $|S_3| = 6$–specifically,

$$S_3 = \{(1\,2)\,,\,(2\,3)\,,\,(1\,3)\,,\,(1\,2\,3)\,,\,(3\,2\,1)\,,\,e\}\,.$$

Now, let $a = (1\,2)$ and $b = (1\,2\,3)$. Then $a^2 = e$, so that $o(a) = 2$. We also have $b^2 = (1\,2\,3)\,(1\,2\,3) = (1\,3\,2)\,(3\,2\,1)$ and $b^3 = (3\,2\,1)\,(1\,2\,3) = e$. As well, $ab = (1\,2)\,(1\,2\,3) = (2\,3)$ and $ab^2 = (1\,2)\,(3\,2\,1) = (1\,3)$. So we can write

$$S_3 = \left\{a, b, b^2, ab, ab^2 \,|\, a^2 = 1, b^3 = 1\right\}.$$

However, we can do better. Observe that $ba = (1\,2\,3)\,(1\,2) = (1\,3) = ab^2$, so that

$$\boxed{S_3 = \left\{a^2 = 1,\, b^3 = 1,\, ba = ab^2\right\}}\,. \tag{4.2}$$

$ba = ab^2$ gives us the rule for "multiplying" elements of S_3 without knowing anything about the elements of the set which are being permuted. This makes it easy to write up the multiplication table for this group (which would contain 36 cells). For instance,

$$b\,(ab) = (ba)\,b = \left(ab^2\right)b = a\left(b^2b\right) = ab^3 = a1 = a,$$

and we perfomed this multiplication without knowing anything about the elements 1, 2, and 3, i.e., without having to write out the cycles.

Writing S_3 in the form (4.2) is known as writing a group as a **generator relation**, with the elements a and b being the **generators**. All we need are the three facts expressed in (4.2) to know all the elements of the group, and whatever follows from that.

4.3.2 Dihedral Groups

Let D_n be the set of symmetry transformations of a regular n-gon in $\mathbb{R}^2$. Place the n-gon in the xy plane with its centre at the origin. We have already seen that there are only two types of symmetry transformations possible when we looked at the equilateral triangle (whose symmetry transformations belong in D_3):

- *Rotations* by $\theta = \frac{2\pi}{n}, \frac{4\pi}{n}, \ldots, \frac{2\pi k}{n}, \ldots$. Denote these transformations by γ_k, $0 \leq k \leq n-1$.
- *Reflections* along the axis through the ray $\theta = \frac{\pi l}{n}$, $1 \leq l \leq n$. Denote these transformations by f_l. (Note that for n odd, these lines simply become the lines through each of the vertices.)

So

$$D_n = \{\gamma_k, f_l \,|\, 0 \leq k \leq n-1,\, 1 \leq l \leq n\}\,.$$

If we let the operations on these transformations (the elements of D_n) be the composition of mappings $\circ$, then we have that $(D_n, \circ)$ is a group. (Again, composition of mappings is associative.)

Now, let us label the vertices 1 through n. The identity transformation is the one that leaves the n-gon in its original position, so that

$$\mathcal{I}_{D_n} = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

The inverse transformation reverses the transformation previously performed, so that if $\alpha \in D_n$ is defined as

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix},$$

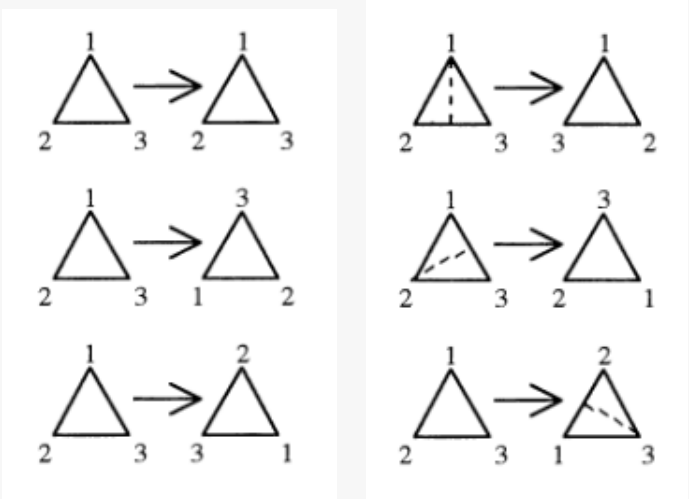
then

$$\alpha^{-1} = \begin{pmatrix} \alpha(1) & \alpha(2) & \cdots & \alpha(n) \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

As with the symmetry transformations of the equilaterial triangle in $\mathbb{R}^2$ and the permutations of $\{1, 2, 3\}$, the specification of the transformations is exactly the same. In fact, every symmetry transformation is just a permutation of the labels assigned to the vertices. Try to recall a term from Linear Algebra used for this type of correspondence.

What is $|(D_n, \circ)|$? We know that there are n rotations possible. There are also n reflections possible. Hence, there are $n + n = 2n$ elements in D_n, and so $|(D_n, \circ)| = 2n$, which agrees with the number we got for the equilateral triangle, $2 \times 3 = 6$. And as with the equilateral triangle, since in general the symmetry transformations do not commute, we have that the dihedral groups are non-Abelian.

Example 4.3.1 Let us reexamine the equilateral triangle example, the D_3 dihedral group. Recall that we have six symmetry transformations, three rotations and three reflections, as shown below.



Let the 120-degree counter-clockwise rotation be

$$\gamma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

recalling that we defined γ_k to be rotation by $\frac{2\pi k}{n}$. Recall that the composition of two rotations, each of angles θ_1 and θ_2, was equivalent to the rotation by $\theta_1 + \theta_2$, regardless of the order (i.e., the rotations were commutative). Hence, we can write

$$\gamma_2 = \gamma_1^2, \qquad \gamma_0 = \gamma_1^3 = \mathcal{I}.$$

Since $\gamma_1^3 = \mathcal{I}$, we have that γ_1 is of order three, i.e., $o(\gamma_1) = 3$. The same goes for γ_2. This can be easily explained geometrically: since the triangle has three sides, rotating it three times by 120 degrees each will necessarily return the triangle to its original state, no matter what the original state is. And since returning to the original state corresponds to the identity transformation $\mathcal{I}$, the order of each rotation must be 3.

Now, the three reflections are:

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

What should the order of a reflection be? It should be clear that applying the same reflection *twice* will return the triangle to its original state, so that $o(f_1) = o(f_2) = o(f_3) = 2$. Now, observe that

$$\gamma_1 \circ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_2$$

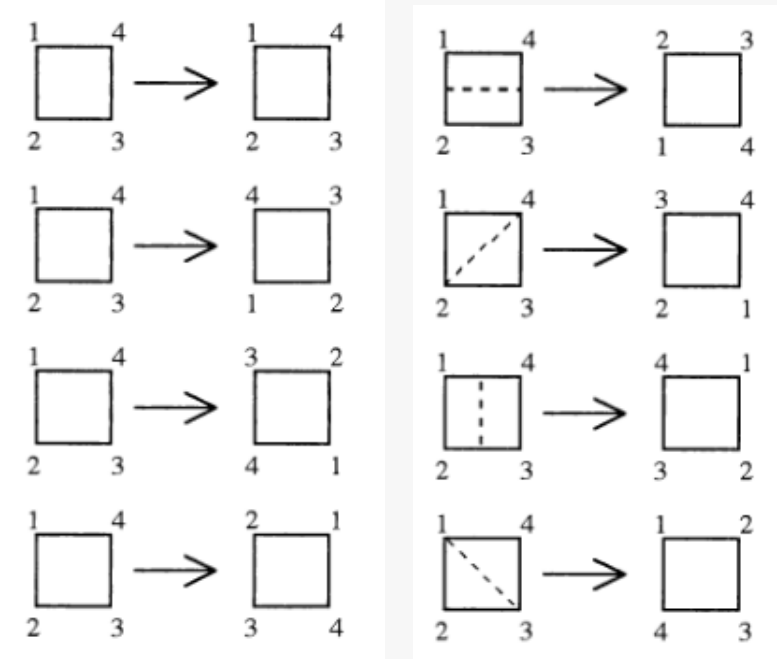
$$\gamma_2 \circ f_1 = \gamma_1^2 \circ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_3,$$

so that all the reflections can be written as the product of a rotation and a reflection about *one* axis. So let's let $\gamma_1 \equiv \gamma$ and $f_1 \equiv f$. Then,

$$D_3 = \{\gamma, \gamma^2, \gamma^3 = \mathcal{I}, f, \gamma f, \gamma^2 f\}$$

is our group. ◀

Example 4.3.2 Let's now look at the symmetry transformations of the square, which are part of the dihedral group D_4. We know that there must be $2 \times 4 = 8$ transformations, and that four of these will be rotations and the remaining four will be reflections. Notice this time, however, that the reflections won't just be about the axes through vertices, as shown below.



Let $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ be the counter-clockwise rotation by 90 degrees and let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ be the reflection about the horizontal axis shown in the top-right-hand panel in the above figure. We then have

$$\gamma^2 = \gamma_2, \quad \gamma^3 = \gamma_3, \quad \gamma^4 = \gamma_4 = \gamma_0 = \mathcal{I},$$

so that, again, all the rotations can be described as the powers of just one rotation, and $o(\gamma) = 4$ since rotating the square by 90 degrees four times sequentially will return it to its original position. And just like for the equilateral triangle, we can write all the reflections as a composition of the reflection f and the rotation γ (verify these explicitly):

$$\begin{aligned} f &= \text{flip around horizontal axis} \\ \gamma f &= \text{flip around diagonal } 2-4 \\ \gamma^2 f &= \text{flip around vertical axis} \\ \gamma^3 f &= \text{flip around diagonal } 1-3 \end{aligned}$$

Again, all of the reflections must be of order two (verify this explicitly). So we have

$$D_4 = \left\{\gamma,\, \gamma^2,\, \gamma^3,\, \gamma^4 = \mathcal{I},\, f,\, \gamma f,\, \gamma^2 f,\, \gamma^3 f\right\},$$

which indeed has eight elements. ◀

We now summarise generalise the results of dihedral groups from these two examples in the following theorem.

Theorem 4.3.1

Let $(D_n, \circ)$, $n \geq 3$ be a group with the set D_n and the composition operation $\circ$ on D_n. D_n is the set of symmetry transformations of the regular n-gon centred at the origin of the xy plane. Then:

1. $D_n = \left\{\gamma^k, \gamma^k f \,|\, 0 \leq k \leq n-1\right\}$, where γ is the rotation by $\frac{2\pi}{n}$ and f is the reflection about the axis coinciding with the ray $\frac{\pi}{n}$.
2. $|D_n| = 2n$.
3. If n is odd, then the n rotations are of order n and the n reflections are of order 2.
4. If n is even, then the rotation by π is given by $\gamma^{n/2}$ and is of order 2. The remaining $n-1$ rotations, which are of the form γ^a, $a \neq \frac{n}{2}$ and $a \neq 0$, are of order $o\left(\gamma^a\right) = \frac{n}{\gcd(a,n)}$. The n reflections are of order 2.
5. $\gamma f = f\gamma^{-1} \Rightarrow f^{-1}\gamma f = \gamma^{-1}$.

Using 1., 3., 4. and 5., we can write D_n as a generator relation:

$$\boxed{D_n = \left\{\gamma^n = 1,\, f^2 = 1,\, \gamma f = f\gamma^{-1}\right\}} \tag{4.3}$$

This allows us to easily see why the order of every reflection is two. For instance,

$$\begin{aligned}
(\gamma f)^2 &= \gamma f \gamma f \\
&= f\gamma^{-1}\gamma f \quad (4.4) \\
&= f1f \\
&= f\,(1f) \quad \text{(associativity)} \\
&= ff = f^2 \\
&= 1 \quad (4.4)
\end{aligned}$$

Example 4.3.3 For each dihedral group listed below, state the number of elements in each group of each possible order (i.e., how many elements of order one, how many elements of order two, etc.).

1. D_{10}
2. D_{11}
3. D_{14}

Solution: We solve each in turn.

1. This is the dihedral group of order 20, and so has 10 rotations and 10 reflections. By the previous theorem, all of the 10 reflections are of order two. In addition since 10 is even, we have that the rotation by π will be of order two (the rotation by π is given by γ^5, where γ is the rotation by $\frac{2\pi}{10} = \frac{\pi}{5}$). So there are 11 elements of order two. In addition there are four elements of order five $(\gamma^2, \gamma^4, \gamma^6, \gamma^8)$, and four elements of order ten $(\gamma, \gamma^3, \gamma^7, \gamma^9)$. So,

n	1	2	5	10
# of elements of order n	1	11	4	4

2.

3. This is the dihedral group of order 28, and so has 14 rotations and 14 reflections. Again, all of the 14 reflections are of order two, and the rotation by π, which is γ^7 where γ is rotation by $\frac{2\pi}{14} = \frac{\pi}{7}$, is also of order two. So there are 15 elements of order two. There are six elements of order seven $(\gamma^2, \gamma^4, \gamma^6, \gamma^8, \gamma^{10}, \gamma^{12})$ and six elements of order fourteen $(\gamma, \gamma^3, \gamma^5, \gamma^9, \gamma^{11}, \gamma^{13})$. So,

n	1	2	7	14
# of elements of order n	1	15	6	6

4.3.3 The General Linear Group

Definition 4.3.1 Field

A **field** is a set $\mathbb{F}$ together with two binary operations $+$ and $\cdot$ on $\mathbb{F}$ such that $(F, +)$ is an Abelian group (call its identity 0) and $(\mathbb{F} - \{0\}, \cdot)$ is also an Abelian group.

For example, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{Z}_n$ are fields. If p is a prime number, then we write $\mathbb{Z}_p$, which is a finite field.

Now, for each $n \in \mathbb{Z}^+$, let $GL_n(\mathbb{F})$ be the set of all $n \times n$ matrices whose entries come from $\mathbb{F}$ and whose determinant is non-zero, i.e.,

$$GL_n(\mathbb{F}) = \{A \mid A \text{ is an } n \times n \text{ matrix with entries from } \mathbb{F} \text{ and } \det(A) \neq 0\}, \tag{4.4}$$

where the determinant of any matrix A with entries from $\mathbb{F}$ can be computed by the same formulas used when $\mathbb{F} = \mathbb{R}$. For arbitrary $n \times n$ matrices A and B, let AB denote their product as computed by the same rules as when $\mathbb{F} = \mathbb{R}$. We note the following facts about this product.

- This product is associative.

- Since $\det(AB) = \det(A)\det(B)$, it follows that if $\det(A) \neq 0$ and $\det(B) \neq 0$, i.e., if $A, B \in GL_n(\mathbb{F})$, then $\det(AB) \neq 0$, so that $AB \in GL_n(\mathbb{F})$, i.e., $GL_n(\mathbb{F})$ is closed under matrix multiplication.
- $\det(A) \neq 0$ if and only if A has a matrix inverse (this inverse can be computed using the same formulas as when $\mathbb{F} = \mathbb{R}$), so every $A \in GL_n(\mathbb{F})$ has an inverse $A^{-1} \in GL_n(\mathbb{F})$ such that $AA^{-1} = A^{-1}A = \mathbb{1}$, where $\mathbb{1}$ is the $n \times n$ identity matrix.
- Since $\det(\mathbb{1}) \neq 0$ (in fact, $\det(\mathbb{1}) = 1$ for any n), we have that there exists an identity element in $GL_n(\mathbb{F})$.

Since all four group axioms have been satisfied, we have that $GL_n(\mathbb{F})$ is a group under matrix multiplication. It is called the **general linear group**. For example, if $n = 2$, then we have

$$\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Also, since matrix multiplication is not in general commutative, the general linear group is an example of a non-Abelian group.

Theorem 4.3.2

We have the following important results:

1. If $\mathbb{F}$ is a field and $|\mathbb{F}| < \infty$, then $|\mathbb{F}| = p^m$ for some prime p and integer m.
2. If $|\mathbb{F}| = q < \infty$, then $|GL_n(\mathbb{F})| = (q^n - 1)(q^n - q)\left(q^n - q^2\right) \cdots \left(q^n - q^{n-1}\right)$.

4.3.4 The Special Linear Group

The **special linear group** is a special case of the general linear group in which the matrices have determinant one:

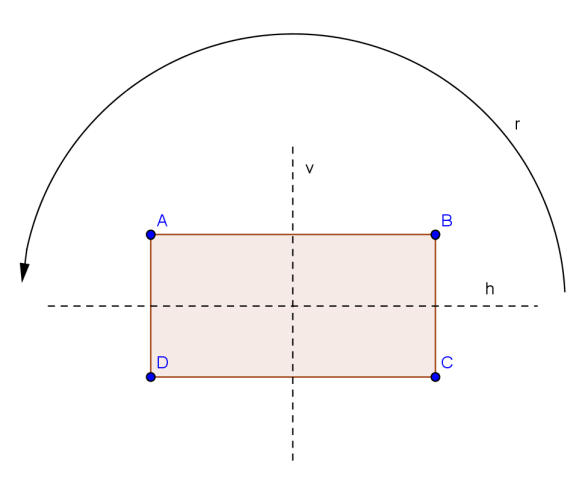
$$SL_n(\mathbb{F}) = \{A \mid A \text{ is an } n \times n \text{ matrix with entries from } \mathbb{F} \text{ and } \det(A) = 1\} \tag{4.5}$$

This group is also non-Abelian.

4.3.5 The Klein 4-Group

Example 4.3.4 [

Symmetry Transformations of a Non-Square Rectangle] Let us examine the symmetry transformations of a non-square rectangle.



From this diagram, we can see that there are four possible symmetry transformations: the identity, rotation by 180 degrees, and two reflections about the axes h and v. Observe that each of these transformations is of order two, i.e., each transformation is its own inverse, and that these transformations constitute the dihedral group D_2 of order four:

$$\boxed{D_2 = \left\{\gamma^2 = f^2 = 1,\, \gamma f = f\gamma^{-1}\right\}},$$

if we let γ be the rotation by π and f the rotation about the h axis. So the four elements are $1, \gamma, f, \gamma f$. We also get these same elements if we consider the symmetry transformations of the rhombus that is not a square.

The multiplication table for D_2 is:

D_2	1	γ	f	γf
1	1	γ	f	γf
γ	γ	1	γf	f
f	f	γf	1	γ
γf	γf	f	γ	1

Now, observe that if we let

$$\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \gamma = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, f = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \gamma f = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$

then these matrices will exbihit the same multiplication table as the one above. In fact, because each of the matries is of determinant one, we have that the elements of D_2 are elements of $SL_2(\mathbb{R})$. This group is called the **Klein four-group**. It is non-Abelian.

REMARK: Another construction of the Klein four-group is $\mathbb{Z}_8^* = \{[1],[3],[5],[7]\}$ under multiplication modulo 8. You can verify that $\gamma = [3]$, $f = [5]$, and $\gamma f = [3] \times [5] = [15] = [7]$.

4.3.6 The Quaternion Group

The **quaternion group** is a non-Abelian group of order eight under multiplication in $\mathbb{C}$. It is often denoted Q_8,

$$\boxed{Q_8 = \left\{-1, i, j, k \,|\, (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1\right\}} = \{1, -1, i, -i, j, -j, k, -k\}\,. \quad (4.6)$$

Observe, however, that each element is of order four, and that any two of the elements in the group will generate the entire group, so we can write

$$\boxed{Q_8 = \left\{x, y \,|\, x^4 = y^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1}\right\}}\,. \quad (4.7)$$

Using either of these forms, we can write down the multiplication table for Q_8:

Q_8	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Now, observe that if we let

$$\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix},$$

then these matrices will have the same multiplication table as the one above. In fact, since each of these matrices has determinant one, we have that Q_8 is a subset of $SL_2(\mathbb{C})$. And since $ij = k$ but $ji = -k$, this confirms that Q_8 is non-Abelian.

REMARK: Notice that the multiplication of pairs of elements from the subset $\{\pm i, \pm j, \pm k\}$,

$$\begin{aligned} ij &= k, \quad ji = -k, \\ jk &= i, \quad kj = -i, \\ ki &= j, \quad ik = -j, \end{aligned}$$

works like the cross product of the unit vectors in three-dimensional Cartesian coordinates of Euclidean space

4.4 Subgroups and Cyclic Groups

One basic method for unravelling the structure of any mathematical object that is defined by a set of axioms is to study *subsets* of that objects that also satisfy the same axioms.

Definition 4.4.1 Subgroup

A non-empty subset H of a group G is a **subgroup** of G is H is a group (i.e., satisfies all the group axioms) under the same operation as G. We use the notation $H \subseteq G$ to mean that H is a subset of G, and $H \leq G$ to means that H is a subgroup of G .

REMARK: In general, it is possible that the subset H has the structure of a group with respect to some operation other than the operation on G that makes G a group. This is why we emphasise that H must be a group under the same operation as G.

REMARK: If $H \subseteq G$ and $H \neq G$, then, as we know, we can write $H \subset G$ to emphasise that H is a *proper subset* of G. In the same way, for groups, if $H \leq G$ and $H \neq G$, then we can write $H < G$ and say that H is a proper subgroup of G.

Definition 4.4.2 Trivial and Non-Trivial Subgroups

For any group G under operation $*$ with identity element e, $(\{e\}, *)$ is a subgroup of G and is called the **trivial subgroup** of G. G is itself a subgroup of G, called the **improper subgroup**. Any group of G other than these two is called a **non-trivial proper subgroup** of G.

We now state the subgroup test, which is almost exacly like the subspace test from Linear Algebra (in fact, the concept of the subgroup itself may have reminded you of subspaces from Linear Algebra). Like the name suggests, we use to test whether a subset of a group is indeed a subgroup.

Theorem 4.4.1 The Subgroup Test

Let G be a group and $H \subset G$ a subset. Then H is a subgroup of G, i.e., $H \leq G$ if and only if

1. $H \neq \varnothing$, i.e., H is non-empty.
2. For all $a, b \in H$, $ab \in H$.
3. For all $a, b \in H$, $a^{-1} \in H$.

PROOF: We prove each direction in turn.

- ($\Rightarrow$): If H is a subgroup of G, then certainly all of 1., 2., and 3. hold because H contains the identity of G and the inverse of each its elements, and because H is closed under multiplication by definition of a group.

- ($\Leftarrow$): Now we show that if 1., 2., and 3. are satisfied, then $H \leq G$, i.e., H is a subgroup of G. By 2., we have that H is closed under multiplication. Also, since $H \subset G$, and G is associative, being a group, then H must also be associative. Now, by 1., since H is not empty, consider an arbitrary element $a \in H$. By 3., $a^{-1} \in H$, so by 2., $aa^{-1} = 1 \in H$, so the H contains the identity element. Finally, by 3., every element of H has an inverse. Therefore, since H satisfies all of the group axioms, it is a group, by definition, a subgroup. ■

Example 4.4.1 Below are several examples of subgroups.

- The set of even integers $2\mathbb{Z}$ is a subste of the set of integers $\mathbb{Z}$ and, as we have seen, are both groups under addition. So $(2\mathbb{Z}, +) < (\mathbb{Z}, +)$.
- The set of fourth roots of unity $\{1, -1, i, -i\}$ is a subset of the set of nonzero complex numbers $\mathbb{C}^* = \mathbb{C} - \{0\}$, and since both are groups under multiplication, the fourth roots of unity are a subgroup of the non-zero complex numbers.
- Consider $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$ and the subset $H = \{[0], [2], [4], [6]\}$. Then H is a subgroup of G under addition modulo 8 with the following addition table:

$\mathbb{Z}_8$	[0]	[2]	[4]	[6]
[0]	[0]	[2]	[4]	[6]
[2]	[2]	[4]	[6]	[0]
[4]	[4]	[6]	[0]	[2]
[6]	[6]	[0]	[2]	[4]

- $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.
- $(\mathbb{Q}^*, \times) \leq (\mathbb{R}^*, \times) \leq (\mathbb{C}^*, \times)$.
- $\{1, -1\} \leq \{1, -1, i, -i\}$ under multiplication of complex numbers.
- $\left\{b, b^2, b^3 = 1\right\} \leq S_3$ under composition of mappings (recall (4.2)).
- $\left\{\gamma, \gamma^2, \ldots, \gamma^n = 1\right\} \leq D_n$, i.e., the subset of rotations in the dihedral group of order $2n$ is a subgroup under composition of mappings since, as we have seen, the composition of two rotations is another rotation and the inverse of a rotation is another rotation.
- $SL(2, \mathbb{F})$ is a subgroup of $GL(2, \mathbb{F})$. For if $A \in SL(2, \mathbb{F})$, then $\det A = 1$, so $\det\left(A^{-1}\right) = \frac{1}{\det A} = 1$, and $A^{-1} \in SL(2, \mathbb{F})$. Further, if $A, B \in SL(2, \mathbb{F})$, then $\det A = \det B = 1$, so $textdet(AB) = \det A \det B = 1$ and $AB \in SL(2, \mathbb{F})$.

Example 4.4.2 Below are some examples of *non subgroups*.

- $(\mathbb{N}, +) \not\leq (\mathbb{Z}, +)$ because $(\mathbb{N}, +)$ fails criterion 3 of the subgroup test since the additive inverse of a natural number is negative, and negative numbers are not part of $\mathbb{N}$.
- $\mathbb{Q} - \{0\}$ under multiplication is not a subgroup of R under addition even though both are groups and $\mathbb{Q} - \{0\}$ is a subset of $\mathbb{R}$ because both subsets have to be groups under the *same operation*.
- $(\mathbb{Z}^+, +) \not\leq (\mathbb{Z}, +)$: although $\mathbb{Z}^+$, the positive integers, is closed under $+$, it does not contain the identity element $0 \in \mathbb{Z}$. In addition, the additive inverse of any non-zero integer is negative, which by definition is not in $\mathbb{Z}^+$. In fact $(\mathbb{Z}^+, +)$ is not even a group.
- D_3 is not a subgroup of D_4 such the former is not even a subset of the latter.

4.4.1 Cyclic Subgroups and Cyclic Groups

We now examine the important class of groups called cyclic groups, which we first introduced in a remark at the beginning of this chapter. In it, we saw that all groups of order three are cyclic. In this section, we will formally define a cyclic group.

Definition 4.4.3

Let G be a group and $a \in G$. Define a subset $\langle a \rangle$ as

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}, \tag{4.8}$$

called the **subset generated by** a (it could be finite or infinite).

Theorem 4.4.2

Let G be a group under binary operation $*$ and $a \in G$. Then $(\langle a \rangle, *)$ is a group under the same binary operation as G.

Proof: We check that $(\langle a \rangle, *)$ satisfies the group axioms.

- For all $n, m \in \mathbb{Z}$, $a^n a^m = a^{n+m} = a^{m+n} \in \langle a \rangle$ since $n + m \in \mathbb{Z}$.
- Since G is associative, and $\langle a \rangle \subset G$, $\langle a \rangle$ must also be associative.
- $1 = a^0 \in \langle a \rangle$, so the identity element is in $\langle a \rangle$.
- For all $n \in \mathbb{Z}$ $(a^n)^{-1} = a^{-n} \in \langle a \rangle$ since $-n \in \mathbb{Z}$. So all elements in $\langle a \rangle$ contain their inverse.

Since $(\langle a\rangle, *)$ satisfie the group axioms, it is a group. ■

Theorem 4.4.3 Cyclic Subgroup

Let G be a group and $a \in G$. Then $\langle a\rangle$ is a subgroup of G, called the **cyclic subgroup generated by** a (it could be of finite or infinite order). In other words, every element of a group generates a cyclic subgroup.

PROOF: We must check that $\langle a\rangle$ under the same operation as G passes the subgroup test. Clearly, $\langle a\rangle$ is not empty. Let $x, y \in \langle a\rangle$, i.e., $x = a^m$ and $y = a^n$ for some $m, n \in \mathbb{Z}$. Then, $xy = (a^m)(a^n) = a^{m+n} \in \langle a\rangle$ since $m + n \in \mathbb{Z}$. Furthermore, $x^{-1} = (a^m)^{-1} = a^{-m} \in \langle a\rangle$ since $-m \in \mathbb{Z}$. Since all three criteria have been satisfied, $\langle a\rangle$ under the same operation as G passes the subspace test, and so is a subgroup of G, i.e., $\langle a\rangle \leq G$. ■

Example 4.4.3 Below are some examples of cyclic subgroups.

- In $(\mathbb{Z}, +)$, the cyclic subgroup generated by 3 is $\langle 3\rangle = 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = \{\ldots, 3^{-3}, 3^{-2}, 3^{-1}, 3^0, 3^1, 3^2, 3^3, \ldots\}$.
- In $(\mathbb{C}^*, \times)$, the cyclic subgroup generated by i is $\langle i\rangle = \{i, -1, -i, 1\} = \{i, i^2, i^3, i^4\}$.
- In S_3, the cyclic subgroup generated by b is $\langle b\rangle = \{b^0 = b^3 = 1, b^1, b^2\}$.
- For the dihedral group of order n, which is defined, remember, by $D_n = \{\gamma, f \,|\, \gamma^n = f^2 = 1, \gamma f = f\gamma^{-1}\}$, we have that the rotations $\langle\gamma\rangle = \{1, \gamma, \gamma^2, \ldots, \gamma^{n-1}\}$ form a cyclic subgroup generated by γ. Note that $|\langle\gamma\rangle| = o(\gamma) = n$.
- All of the subgroups of $(\mathbb{Z}_6, +)$ are:
  - $\{[0]\}$, the trivial subgroup.
  - $\{[0], [1], [2], [3], [4], [5]\} = \mathbb{Z}_6$, the improper subgroup.
  - $\langle 2\rangle = \langle 4\rangle = \{[0], [2], [4]\}$, two cyclic subgroups.
  - $\langle 3\rangle = \{[0], [3]\}$, a cyclic subgroup.

  Note that if H is a subgroup and $[5] \in H$, then $[-5] = [1] \in H$, and that if $[2], [3] \in H$, then $[3] - [2] = [1] \in H$, and in either case $H = \mathbb{Z}_6$, so the subgroups listed are all there are.

Definition 4.4.4 Cyclic Group

Let G be a group. If there exists an $a \in G$ such that $G = \langle a\rangle$, then we say that G is a **cyclic group** and a is called a **generator** of G.

REMARK: Note that we said a is *a* generator of G, not *the* generator. Indeed, a cyclic group may have more than one generator, as we'll see in the examples below.

Example 4.4.4 Here are some examples of cyclic groups.

- $(\mathbb{Z}_5, +) = \{[0], [1], [2], [3], [4]\}$ is cyclic and is generated by all of [1], [2], [3], and [4], i.e., $\mathbb{Z}_5 = \langle [1] \rangle = \langle [2] \rangle = \langle [3] \rangle = \langle [4] \rangle$. So see why, note that

$$\begin{aligned} \langle [1] \rangle &= \left\{ \ldots, [1]^{-3}, [1]^{-2}, [1]^{-1}, [1]^0, [1]^1, [1]^2, [1]^3, \ldots \right\} \\ &= \{ \ldots, [-3], [-2], [-1], [0], [1], [2], [3], \ldots \}. \end{aligned}$$

  But, modulo 5, $-3 \equiv 2 \Rightarrow [-3] = [2]$, $-2 \equiv 3 \Rightarrow [-2] = [3]$, and $-1 \equiv 4 \Rightarrow [-1] = [4]$, so that

$$\langle [1] \rangle = \{[0], [1], [2], [3], [4]\} = \mathbb{Z}_5.$$

  Similar arguments can be applied for $\langle [2] \rangle$, $\langle [3] \rangle$, and $\langle [4] \rangle$.

- Likewise, $\mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$.
- In fact, for any $n > 1$, $\mathbb{Z}_n = \langle 1 \rangle = \langle n - 1 \rangle$. So $\mathbb{Z}_n$ is a cyclic group of order n.
- $(\mathbb{Z}, +) = \{ \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \}$ is cyclic and is generated by both 1 and -1, i.e., $\mathbb{Z} = \langle -1 \rangle = \langle 1 \rangle$. But, for example, $\mathbb{Z} \neq \langle 2 \rangle$, since $\langle 2 \rangle = \left\{ \ldots, 2^{-3}, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, 2^3, \ldots \right\} = \{-6, -4, -2, 0, 2, 4, 6, \ldots\} \neq \mathbb{Z}$. However, note that $(\langle 2 \rangle, +)$ is a *subgroup* of $(\mathbb{Z}, +)$.
- $U(10) = \{[1], [3], [7], [9]\} = \left\{3^0, 3^1, 3^2, 3^3\right\} = \langle 3 \rangle$.
- We have $2\mathbb{Z} = \langle 2 \rangle$ and, in general, for any $n \geq 1$, $n\mathbb{Z} = \langle n \rangle$. These are all infinite cyclic groups.

Example 4.4.5 Here are some examples of *non-cyclic groups*.

- In S_3, $\langle b \rangle = \left\langle b^2 \right\rangle = \left\{1, b, b^2\right\}$, while $\langle \mu_i \rangle = \{1, \mu_i\}$ for $i = 1, 2, 3$. Hence, none of the elements of S_3 generates the whole group, and so S_3 is not cyclic.
- $\mathbb{Z}_{10} \neq \{[0], [2], [4]\}$.

Theorem 4.4.4

Let G be a cyclic (sub)group generated by $a \in G$. Then G is Abelian.

PROOF: Let $x, y \in G$ be arbitrary. Since G is cyclic, we have that there exists two integers m

and n such that $x = a^m$ and $y = a^n$. So

$$xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx,$$

Since x, y are arbitrary, we have that $xy = yx$ for all $x, y \in G$, i.e., G is Abelian by definition. ■

Theorem 4.4.5

Let G be a group and $a \in G$, an element of finite order, i.e., $o(a) = n < \infty$. Then $\langle a \rangle = \left\{a^0 = 1, a, a^2, \ldots, a^{n-1}\right\}$.

PROOF: Prove this!!! (We already know that if $o(a) = n$, then the elements $a^0 = 1, a^1, \ldots, a^{n-1}$ are distinct) ■

Theorem 4.4.6

Let G be a group and $a \in G$. Then $o(a) = |\langle a \rangle|$.

PROOF: We examine three cases to complete the pf.

Case 1

Suppose $o(a) = \infty$. Assume for a contradiction that $|\langle a \rangle| < \infty$, i.e., that $\langle a \rangle$ is finite. Then the set $\left\{a^0, a^1, a^2, \ldots, a^{|\langle a \rangle|}\right\}$ must have duplicate elements, i.e., there must exist two element a^i, a^j, $i \neq j$, $0 \leq i < j \leq |\langle a \rangle|$ such that $a^i = a^j$, which implies $a^{i-j} = 1$, which implies $o(a) \leq i - j < \infty$, a contradiction to the assumption that $o(a) = \infty$. So $o(a) = |\langle a \rangle|$.

Case 2

Suppose $o(a) = 1$. Then $\langle a \rangle = \left\{a^k \,|\, k \in \mathbb{Z}\right\} = \{1\}$, the identity element. Thus, $o(a) = 1 = |\langle a \rangle|$.

Case 3

Let $o(a) = n < \infty$, $n \neq 1$ and $|\langle a \rangle| = m \neq \infty$. We will prove that $m \leq n$ and $m \geq n$, from which we will establish that $m = n$, and hence, the result.

- Let $a^k \in \langle a \rangle$. By the division algorithm, there exists integers p and q such that $k = qn + r$, $0 \leq r < n - 1$. Then,

  $$a^k = a^{qn+r} = (a^n)^q a^r = 1^q q^r = q^r,$$

  which implies that $\langle a \rangle = \left\{a^k \,|\, k \in \mathbb{Z}\right\} = \{a^r \,|\, 0 \leq r < n - 1\}$, which implies that $|\langle a \rangle| = m \leq o(a) = n$, i.e., $m \leq n$.
- Consider the elements $a^0, a^1, \ldots, a^m$. Since $|\langle a \rangle| = m$, there exists $0 \leq i < j \leq m$ such that $a^i = a^j \Rightarrow a^{i-j} = 1$, which implies that $o(a) = n \leq i - j \leq m - 0 = m$, i.e., $n \leq m$.

So we have shown that $n \leq m$ and $m \leq n$, which means that $m = n \Rightarrow o(a) = |\langle a \rangle|$, as required. ■

Corollary 4.4.1

Theorem 4.4.7

Let G be an arbitrary group and $a, b \in G$ and $o(a), o(b) < \infty$ (so we are dealing with finite groups).

1. If $o(a) = \infty$, then $o\left(a^k\right) = \infty$ for $a \in \mathbb{Z} - \{0\}$.
2. If $o(a) = n < \infty$, then $o\left(a^k\right) = \frac{n}{\gcd(k,n)}$.
3. In particular, if $k \geq 1$ and $k \mid n$, then $o\left(a^k\right) = \frac{n}{k}$.

PROOF: We prove each in turn.

1. Assume for a contradiction that $o(a) = \infty$ by $o\left(a^k\right) = m < \infty$. By definition of order,

$$1 = \left(a^k\right)^m = a^{km}.$$

Also,

$$a^{-km} = \left(a^{km}\right)^{-1} = 1^{-1} = 1.$$

Now, one of km or $-km$ is positive, since neither k nor m is zero, so some positive power of a is the identity, which contradicts the assumption that $o(a) = \infty$. So the assumption $o\left(a^k\right) < \infty$ must be false, i.e., $o\left(a^k\right) = \infty$.

2. Let

$$y = a^k, \quad (k,n) = d, \quad \text{and write} \quad n = db,\ k = dc,$$

for suitable $b, c \in \mathbb{Z}$ with $b > 0$ (why can we do this?). Since d is the greatest common divisor of k and n, the integers b and c must be coprime (by which theorem?), i.e., $\gcd(b,c) = 1$. We must now show that $o(y) = b$. First, note that

$$y^b = a^{kb} = a^{dcb} = \left(a^{db}\right)^c = (a^n)^c = 1^c = 1,$$

so, applying Theorem 4.2.5, we see that $o(y)$ divides b. Let $m = o(y)$. Then

$$a^{km} = y^m = 1,$$

so applying Theorem 4.2.5 again, we get $n \mid km$, i.e., $db \mid dcm$. Thus, $b \mid cm$. Since b and c have no factors in common (being coprime), b must divide m. Since b and m are positive integers that divide each other, $b = m = o(y)$. So the pf is complete.

Alternate pf: To prove the result, we will show that $o\left(a^k\right) \mid \frac{n}{\gcd(k,n)}$ and $\frac{n}{\gcd(k,n)} \mid o\left(a^k\right)$. We first show the former. We have

$$\left(a^k\right)^{\frac{n}{\gcd(k,n)}} = (a^n)^{\frac{k}{\gcd(k,n)}}.$$

Now, by Theorem 2.0.13, we have that $\frac{k}{\gcd(k,n)}$ is an integer, so that

$$(a^n)^{\frac{k}{\gcd(k,n)}} = 1^{\frac{k}{\gcd(k,n)}} = 1.$$

So, by 1., $o\left(a^k\right) \mid \frac{n}{\gcd(k,n)}$. Let us now show that $\frac{n}{\gcd(k,n)} \mid o\left(a^k\right)$. We have

$$1 = \left(a^k\right)^o \left(a^k\right) = a^{k \cdot o\left(a^k\right)},$$

so by 1., $n \mid ko\left(a^k\right)$. Dividing both sides by $\gcd(k,n)$, we get

$$\frac{n}{\gcd(k,n)} \mid \frac{k}{\gcd(k,n)} o\left(a^k\right).$$

Now, by Theorem 2.0.14, we have that

$$\gcd\left(\frac{n}{\gcd(n,k)}, \frac{k}{\gcd(k,n)}\right) = 1,$$

so that by Theorem 2.0.8 we get

$$\frac{n}{\gcd(k,n)} \mid o\left(a^k\right).$$

Therefore, $o\left(a^k\right) = \frac{n}{\gcd(k,n)}$.

3. This is just a special case of 2: since $k \mid n$, there exists $x \in \mathbb{Z}$ such that $n = xk$. Therefore, $\gcd(k,n) = \gcd(k,xk) = k\gcd(1,x) = k(1) = k$.

   Alternate pf: Suppose $d \mid n$, i.e., d divides n, i.e., there exists an $m \in \mathbb{Z}$ such that $m = \frac{n}{d} \Rightarrow n = md$. Then, $\left(g^d\right)^m = g^{dm} = g^{md} = g^n = 1$, so $o\left(g^d\right) \leq m = \frac{n}{d}$. We must now prove that there is no $k < m$ such that $\left(g^d\right)^k = 1$. Suppose $o\left(g^d\right) = k < m$. Then $\left(g^d\right)^k = 1$, so $g^{kd} = 1$. Moreover, since $d \geq 1$, we have $1 \leq kd < md = n$, which is a contradiction since n, by hypothesis, is the smallest positive integer satisfying $g^n = 1$. So we must have $g^{kd} \neq 1$. Thus, it cannot be that $o\left(g^d\right) < m$, and hence $o\left(g^d\right) = m$.

4. This can be proved directly or it can be deduced from 2. as follows: Let $G = (\mathbb{Z}_n, +)$ and $g = 1$, so $o(g) = n$. For any $a \in \mathbb{Z}_n$, observe that, thinking of a as an integer and letting $d = \gcd(a,n)$, the notations g^a and g^d denote for this group

   $$1 + 1 + \cdots + 1 \quad (a \text{ times}) \qquad \text{and} \qquad 1 + 1 + \cdots + 1 \quad (d \text{ times}),$$

   respectively, i.e., the elements $a, d \in \mathbb{Z}_n$. Because $d \mid n$, 1. gives $o(d) = \frac{n}{d}$. We also get $o(a) = \frac{n}{d} = \frac{n}{\gcd(a,n)}$, as required. ■

Example 4.4.6 Prove that if $a \in \mathbb{Z}$ and $d = \gcd(a,n)$, then $o\left(g^a\right) = o\left(g^d\right)$. Hint: show that for any $k \in \mathbb{Z}$, we have $\left(g^a\right)^k = 1$ if and only if $\left(g^d\right)^k = 1$.

SOLUTION: Let $t = \frac{a}{d} \Rightarrow a = td$. Let us follow the hint. Suppose $k \in \mathbb{Z}$. Certainly, if $\left(g^d\right)^k = 1$, i.e., $g^{dk} = 1$, then $\left(g^a\right)^k = \left(g^{td}\right)^k = \left(g^{dk}\right)^t = 1^t = 1$. Conversely, suppose $\left(g^a\right)^k = 1$. Since $d = \gcd(a, n)$, we can pick $u, v \in \mathbb{Z}$ such that $au + nv = d$. Then,

$$\left(a^d\right)^k = \left(g^{au+nv}\right)^k = \left(g^{au}\right)^k \left(g^{nv}\right)^k = \left(g^{ak}\right)^u \left(g^n\right)^{vk} = 1^u 1^{vk} = 1.$$

This proves the hint. It follows that g^a and g^d have the same order since the same powers give the identity.

Theorem 4.4.8

Let G be a group and $a, b \in G$, with $o(a), o(b) < \infty$. Then, if $\gcd(o(a), o(b)) = 1$ (i.e., $o(a)$ and $o(b)$ are coprime), and $ab = ba$ (i.e., G is Abelian), then $o(ab) = o(a)\, o(b)$.

PROOF: We have

$$\begin{aligned}(ab)^{o(a)o(b)} &= a^{o(a)o(b)} b^{o(a)o(b)} \quad \text{because } ab = ba \\ &= \left(a^o(a)\right)^o(b) \left(b^o(b)\right)^o(a) \\ &= 1^o(b)\, 1^o(a) = 1.\end{aligned}$$

So by Theorem 4.4.7 Part 1. $o(ab) \mid o(a)\, o(b)$.

Now

$$\begin{aligned}1 = 1^o(a) = \left((ab)^o(ab)\right)^o(a) &= a^{o(ab)o(a)} b^{o(ab)o(a)} \\ &= 1^o(ab)\, b^{o(ab)o(a)} \\ &= b^{o(ab)o(a)}.\end{aligned}$$

Therefore, by Theorem 4.4.7 Part 1. again, we have $o(b) \mid o(ab)\, o(a)$. But since $\gcd(o(a), o(b)) = 1$, by Theorem 2.0.8, we have $o(b) \mid o(ab)$. Similarly, $o(a) \mid o(ab)$. However, since $\gcd(o(a), o(b)) = 1$, $o(a)\, o(b) \mid o(ab)$. Hence, $o(ab) = o(a)\, o(b)$. ■

Example 4.4.7 Let G be a cyclic group of order six, $G = \left\{1, a, a^2, a^3, a^4, a^5\right\}$. Find $o\left(a^4\right)$.

SOLUTION: We have $\left(a^4\right)^2 = a^8 = a^{6+2} = a^6 a^2 = 1a^2 = a^2 \neq 1$, while $\left(a^4\right)^3 = a^{12} = a^{6+6} = a^{6\cdot 2} = \left(a^6\right)^2 = 1^2 = 1$. Hence, $o\left(a^4\right) = 4$. However, we can solve this much more easily by using Theorem 4.4.7 Part 2. Since $o(a) = |\langle a \rangle|$, we have that $o(a) = 6$. Hence, $o\left(a^4\right) = \frac{6}{\gcd(4,6)} = \frac{6}{2} = 3$.

Example 4.4.8 Here are some examples of finding the orders of powers of elements in cyclic groups.

- In a cyclic group $G = \langle a \rangle$ of order 210, the order of a^{80} is $o\left(a^{80}\right) = \frac{210}{\gcd(210,80)} = \frac{210}{10} = 21$.
- In $\mathbb{Z}_{105}$, the order of 84 is $o\left(84\right) = \frac{105}{\gcd(105,84)} = \frac{105}{21} = 5$.

Example 4.4.9 Consider $\mathbb{Z}_{12}$ and let us find all of its generators, which is to say all elements $s \in \mathbb{Z}_{12}$ such that $o\left(s\right) = 12$. By Theorem 4.4.7 Part 2., we have $o\left(s\right) = \frac{12}{\gcd(12,s)}$, so $o\left(s\right) = 12$ if and only if $\gcd\left(12, s\right) = 1$. Thus, the generators of $\mathbb{Z}_{12}$ are the elements $s \in \mathbb{Z}_{12}$ such that $\gcd\left(12, s\right) = 1$, namely, the elements $s = 1, 5, 7, 11$.

Corollary 4.4.2

Let $G = \langle a \rangle$ be a cyclic group with generator a, of order $|G| = o\left(a\right) = n$. Then,

1. If $n = \infty$, then $G = \left\langle a^k \right\rangle$ if and only if $k = \pm 1$.
2. For any element $a^s \in G$, a^s is a generator of G, i.e., $G = \langle a^s \rangle$, if and only if $\gcd\left(n, s\right) = 1$.

PROOF: We have, by definition, a^s is a generator of $G \Leftrightarrow G = \langle a^s \rangle \Leftrightarrow o\left(a^s\right) = n$. But $o\left(a^s\right) = |\langle a^s \rangle|$, and $o\left(a^s\right) = \frac{n}{\gcd(n,s)}$. So a^s is a generator of G if and only if $\frac{n}{\gcd(n,s)} = n \Rightarrow \gcd\left(n, s\right) = 1$. ■

Corollary 4.4.3

Let G be a cyclic group of order n. Then the number of generators of G is the Euler Phi Function $\phi\left(n\right)$.

PROOF: This is immediate from the previous corollary, since by definition $\phi\left(n\right)$ is the number of integers s, with $1 \leq s < n$, such that $\gcd\left(n, s\right) = 1$. ■

The next example illustrates a property of cyclic groups that makes them especially easy to understand.

Example 4.4.10 Determine all of the subgroups of
$\mathbb{Z}_{15} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14]\}$.

SOLUTION: To begin with, we have the trivial subgroup $\langle[0]\rangle$. We also have the non-trivial subgroup $\langle[1]\rangle$. Now, let H be any non-trivial subgroup other than $\langle[1]\rangle$. If H contains any of the elements 2, 4, 7, 8, 11, 13, 14 (i.e., the numbers coprime with 15), then H will be the improper subgroup $\langle[2]\rangle$, $\langle[4]\rangle$, $\langle[7]\rangle$, $\langle[8]\rangle$, $\langle[11]\rangle$, $\langle[13]\rangle$, $\langle[14]\rangle$, i.e., $\mathbb{Z}_{15} = \langle[2]\rangle = \langle[4]\rangle = \langle[7]\rangle = \langle[8]\rangle = \langle[11]\rangle = \langle[13]\rangle = \langle[14]\rangle$ (recall the difference between improper and proper subgroups!). Now, let H be a non-trivial *proper* subgroup. First, suppose $[3] \in H$. Then, for any $y \in H$, using the division algorithm, we can write $y = q[3]+r$ for some r with $0 \leq r < [3]$. Since $[3], y \in H$, we have $r = y - q[3] \in H$. But since H is proper, $[1], [2] \in H$. So we must have $r = 0$, and so y is a multiple of $[3]$. Thus, $H = \langle[3]\rangle = \{0, 3, 6, 9, 12\} = 3\mathbb{Z}_{15}$. Now, since $[6]+[6]+[6] = [9]+[9] = [12]+[12]+[12]+[12] = [3]$, any non-trivial proper subgroup containing any of [6], [9], or [12] will also contain [3] and be equal to $3\mathbb{Z}_{15} = \langle[3]\rangle = \langle[6]\rangle = \langle[9]\rangle = \langle[12]\rangle$. Now, suppose H is a non-trivial proper subgroup and $[5] \in H$. A similar argument to the previous shows that $H = \langle[5]\rangle = \{0, 5, 10\} = 5\mathbb{Z}_{15}$, and that any proper subgroup containing [10] will also be equal to $5\mathbb{Z}_{15} = \langle[5]\rangle = \langle[10]\rangle$. Since we have accounted for all possible elements in $\mathbb{Z}_{15}$, we have found all possible subgroups.

You may have noticed that this cyclic group $\mathbb{Z}_{15}$ had the property that all of its subgroups, proper and improper, were all themselves cyclic. This is no coincidence.

Theorem 4.4.9

Let $G = \langle a\rangle$ be a cyclic group. Then, every subgroup H of G is cyclic–either $H = \{1\}$ or $H = \langle a^k\rangle$, where k is the smallest positive integer such that $a^k \in H$.

PROOF: Let $G = \langle a\rangle$ be a cyclic group and H a subgroup of G. If H is the trivial subgroup $\{1\}$, then $H = \langle 1\rangle$ and is cyclic. Now, assume that H is non-trivial, so there exists an element $b \in H$ with $b \neq 1$. Since $b \in G = \langle a\rangle$, we have $b = a^s$ for some integer s, and since $b \neq 1$, we have $s \neq 0$. Also, since $b \in H$, we have $a^{-s} = (a^s)^{-1} = b^{-1} \in H$. Since one or the other of s or $-s$ is positive, H contains some positive power of a. Now, let m be the least positive integer such that $a^m \in H$. Consider any other element $y \in H$. Then, $y = a^n$ for some integer n. Applying the division algorithm to m and n, we can write $n = qm + r$ for some integers q and r with $0 \leq r < m$. Then, $y = a^n = a^{qm+r} = a^{qm}a^r = (a^m)^q\, a^r$, and $a^r = y\,(a^m)^{-q}$. Since $y, a^m \in H$, it follows that $a^r \in H$. But since $0 \leq r < m$ and m is the least positive integer with $a^m \in H$, we must have $r = 0$, and so $y = (a^m)^q$. Thus, every element of H is a power of a^m and $H = \langle a^m\rangle$ is cyclic. *Alternate pf:* Let $H \leq G$. If $G = \{1\}$, the theorem is true for this subgroup, so we assume $H \neq \{1\}$. Thus, there exists some $x \neq 0$ such that $a^x \in H$. If $x < 0$, then since H is a group, we must have $a^{-x} = (a^x)^{-1} \in H$. Hence, H always contains some positive power of a. Now, let

$$\mathcal{P} = \left\{ b \,|\, b \in \mathbb{Z}^+ \quad \text{and} \quad a^b \in H \right\}.$$

By the above $\mathcal{P}$ is a non-empty set of positive integers. By the Well-Ordering Principle, $\mathcal{P}$ has a minimum element–call it d. Since H is a subgroup and $a^d \in H$, $\langle a^d\rangle \leq H$. Since H is a subgroup of G, any element of H is of the form a^x for some integer x. By the division algorithm, write

$$x = qd + r, \quad 0 \leq r < d.$$

Then, $a^x = a^{x-qd} = a^x \left(a^d\right)^{-q}$ is an element of H since both a^x and a^d are elements of H. By the minimality of d, it follows that $r = 0$, i.e., $x = qd$ and so $a^x = \left(a^d\right)^q \in \left\langle a^d \right\rangle$. This gives $K \leq \left\langle a^d \right\rangle$, which completes the pf. ■

Example 4.4.11 Consider the group $(\mathbb{Z}, +)$. Find all the subgroups H of $(\mathbb{Z}, +)$.

SOLUTION: To determine all the subgroups of $\mathbb{Z}$ under addition, consider the set

$$n = \min \{k \in H \mid k \geq 1\}.$$

We now consider three cases.

Case 1

n does not exist, i.e., there is no element in H that is positive. Now, for all $k \in H$, we must have $-k \in H$, since $-k$ is the inverse of k and H is a subgroup. But k is not positive since n is empty, so we must have $k = 0 \Rightarrow H = \{0\}$, i.e., the trivial subgroup.

Case 2

n does exist, and $H' = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. We now show that $H' = H$, i.e., that H' is a subgroup (and, in fact, all the non-trivial subgroups). To show this, we show that $H' \subseteq H$ and $H \subseteq H'$. First, by definition, $n \in H$. Then, $n + n + \cdots + n = nk \in H$ and so we have shown that $H' \subseteq H$. Now, for all $i \in H$, by the division algorithm there exists integers q and r, $0 \leq r < n$ such that $i = qn + r \Rightarrow i - qn = r \in H$. So, by the minimality of n, we must have $r = 0 \Rightarrow i = qn \in H$. Therefore $H \subseteq H'$, and so $H' = H$. Therefore, all the subgroups of $(\mathbb{Z}, +)$ are $n\mathbb{Z} = \langle n \rangle$ for all $n \geq 0$, i.e., all the subgroups of $\mathbb{Z}$ under addition are cyclic.

Alternate Solution: The fact that the subgroups of $\mathbb{Z}$ under addition are cyclic should not be surprising after understanding that $(\mathbb{Z}, +)$ is cyclic and using the previous theorem. To see that $\mathbb{Z}$ under addition is cyclic, notice that $\mathbb{Z} = \langle 1 \rangle$. So, by the previous theorem, all of the subgroups of $\mathbb{Z}$ are cclic and of the form $H = \langle m \rangle$ for some integer m. Since $\langle -m \rangle = \langle m \rangle$, and either $m \geq 0$ or $-m \geq 0$, $H = \langle n \rangle = n\mathbb{Z}$ for some $n \geq 0$.

Example 4.4.12 Since $\mathbb{Z}_{12}$ is cyclic, all the subgroups of $\mathbb{Z}_{12}$ are cyclic, and if $H = \langle s \rangle$ is a subgroup, then $|H| = o(s) = \frac{12}{\gcd(12,s)}$ and is a divisor of 12. Let us consider a divisor of 12, say 4, and find all the subgroups H with order four. We know that $o([3]) = \frac{12}{\gcd(12,3)} = \frac{12}{3} = 4$, and hence $H = \langle [3] \rangle = \{[0], [3], [6], [9]\}$ is one subgroup of order four. It is in fact the *only* subgroup of order four since the only other element of order four in $\mathbb{Z}_{12}$ is [9], and $\langle [9] \rangle = \langle [3] \rangle$.

Theorem 4.4.10

Let $G = \langle a \rangle$ be a cyclic group of order n. Then,

1. If $n = \infty$, then for any distinct non-negative integers x and y, $\langle a^x \rangle \neq \langle a^y \rangle$. Furthermore, for every integer m, $\langle a^m \rangle = \left\langle a^{|m|} \right\rangle$, where $|m|$ denotes the absolute value of m, so that the non-trivial subgroups of G correspond bijectively with the integers 1, 2, 3, ...
2. (If $n < \infty$) The order $|H|$ of any subgroup H of G is a divisor of $n = |G|$.
3. (If $n < \infty$) For each positive integer d that divides n, there exists a unique subgroup of order d, the subgroup $H = \left\langle a^{n/d} \right\rangle$ (is this all the subgroups of G?). Furthermore, for every integer m, $\langle a^m \rangle = \left\langle a^{\gcd(n,m)} \right\rangle$, so that the subgroups of G correspond bijectively with (i.e., there is a one-to-one correspondence between the subgroups of G and) the positive divisors of n.

PROOF: We prove each in turn.

1. Pending...
2. Let H be a subgroup of $G = \langle a \rangle$. Since all the subgroups of a cyclic group are cyclic, we have that $H = \langle a^m \rangle$ for some integer $m \geq 0$, and so $|H| = o\left(a^m\right) = \frac{n}{\gcd(n,m)}$, which is a divisor of n.
3. Since $1 \in H$ for any subgroup H of G, the only subgroup of G of order one is the trivial subgroup $\{1\} = \langle 1 \rangle$. Let d be a divisor of n, with $d > 1$. Then, $o\left(a^{n/d}\right) = \frac{n}{\gcd(n,n/d)} = d$. Hence, $\left\langle a^{n/d} \right\rangle$ is a subgroup of G of order d. What remains to be shown is that this is the only subgroup of G of order d. So let G be a subgroup of G of order $|H| = d$. Let $H = \langle a^s \rangle$, where s is the smallest positive integer such that $a^s \in H$. We know that there are integers u, v such that $\gcd(n, s) = un + vs$. Therefore, $a^{\gcd(n,s)} a^{un+vs} = \left(a^n\right)^u \left(a^s\right)^v \in H$. Since $1 \leq \gcd(n, s) \leq s$ and s was the least positive integer with $a^s \in H$, we must have $\gcd(n, s) = s$. Then, $d = |H| = o\left(a^s\right) = \frac{n}{\gcd(n,s)} = \frac{n}{s}$, so that $s = \frac{n}{d}$ and $H = \langle a^s \rangle = \left\langle a^{n/d} \right\rangle$, as desired.

   To prove the final assertion of 3., we note that $\langle a^m \rangle$ is a subgroup of $\left\langle a^{\gcd(n,m)} \right\rangle$, and it follows that they have the same order. Since $\gcd(n, m)$ is a divisor of n, we have that every subgroup of G arises from a divisor of n. ■

Example 4.4.13 $G = (\mathbb{Z}_{10}, +)$ is a cyclic group generated by [1], i.e., $\mathbb{Z}_{10} = \langle [1] \rangle$, and $o(1) = 10$. By Part 3 of the above theorem, there are four subgroups of G, $\left\langle [1]^{10/1} \right\rangle = \langle [10] \rangle = \langle [0] \rangle$, $\left\langle [1]^{10/2} \right\rangle = \left\langle [1]^5 \right\rangle = \langle [5] \rangle$, $\left\langle [1]^{10/5} \right\rangle = \left\langle [1]^2 \right\rangle = \langle [2] \rangle$, and $\left\langle [1]^{10/10} \right\rangle = \langle [1] \rangle$. In summary, these are the subgroups of $(\mathbb{Z}_{10}, +)$:

$$\begin{aligned}
&\langle [0] \rangle = \langle [10] \rangle \qquad \text{(trivial)} \\
&\langle [1] \rangle = \mathbb{Z}_{10} \qquad \text{(improper)} \\
&\langle [2] \rangle = \{[2], [4], [6], [8], [10]\} \\
&\langle [5] \rangle = \{[5], [10]\}
\end{aligned}$$

Observe that Part 2 of the previous theorem is also verified: $|\mathbb{Z}_{10}| = 10$, and $|\langle[1]\rangle| = 10$, $|\langle[2]\rangle| = 5$, $|\langle[5]\rangle| = 2$ and $|\langle[10]\rangle| = 1$, which are all divisors of 10.

4.4.2 Centralisers and Normalisers, Stabilisers and Kernels

We now introduce some important families of subgroups of an arbitrary group G that in particular provide many examples of subgroups.

Definition 4.4.5 Group Center

Let G be any group. Then the **center** of G, denoted $Z(G)$, consists of the elements of G that commute with every element of G. In other words,

$$\boxed{Z(G) = \{x \in G \,|\, xy = yx \text{ for all } y \in G\}}. \tag{4.9}$$

Note that $1y = y = y1$ for all $y \in G$, so $i \in Z(G)$, and so the center is a non-empty subset of G.

So the center of a group is all those elements of the group that commute with each other. Note that the center of the group does not necessarily contain all the elements of G, *unless the group is Abelian.*

Theorem 4.4.11

The center $Z(G)$ of a group G is a subgroup of G.

Proof: We use the subgroup test. We have already noted that $Z(G)$ is not empty because it contains the identity element. Now, let $a, b \in Z(G)$. By definition, then, $ay = ya$ and $by = yb$ for any $y \in G$. It follows that $(ab)\,y = a\,(by) = a\,(yb) = (ay)\,b = (ya)\,b = y\,(ab)$ using associativity, for any $y \in G$, which means that $ab \in Z(G)$. Now, let $a \in Z(G)$. By definition, then, $ay = ya$ for all $y \in G$. It follows that $a^{-1}y = a^{-1}\left(y^{-1}\right)^{-1} = \left(y^{-1}a\right)^{-1} = \left(ay^{-1}\right)^{-1} = \left(y^{-1}\right)^{-1}a^{-1} = ya^{-1}$, which means that $a^{-1} \in Z(G)$. So by the subgroup test, $Z(G) \leq G$. ■

Example 4.4.14 Let us find the center of the non-Abelian group $D_4 = \left\{1, \gamma, \gamma^2, \gamma^3, f, \gamma f, \gamma^2 f, \gamma^3 f\right\}$. We have $f\gamma = \gamma^3 f$, so $f \notin Z(D_4)$ and $\gamma \notin Z(D_4)$ and $\gamma^3 \notin Z(D_4)$. On the other hand, we have $f\gamma^2 = (f\gamma)\,\gamma = \left(\gamma^3 f\right)\gamma = \gamma^3\,(f\gamma) = \gamma^3\left(\gamma^3 f\right) = \left(\gamma^3\gamma^3\right) f = \gamma^6 f = \gamma^2 f$, and it is then easy to see that γ^2 commutes with all other elements of D_4, so that $\gamma^2 \in Z(D_4)$. Finally,

$$\begin{aligned}
(\gamma f)\,\gamma &= \gamma\left(\gamma^3 f\right) = f \neq \gamma^2 f = \gamma\,(\gamma f) \\
\left(\gamma^2 f\right)\gamma &= \gamma^2\left(\gamma^3 f\right) = \gamma f =\neq \gamma^3 f = \gamma\left(\gamma^2 f\right) \\
\left(\gamma^3 f\right)\gamma &= \gamma^3\left(\gamma^3 f\right) = \gamma^2 f \neq f = \gamma\left(\gamma^3 f\right).
\end{aligned}$$

Hence, $Z(D_4) = \{1, \gamma^2\}$.

Definition 4.4.6 Centraliser

Let G be a group and $a \in G$. Then, the **centraliser** of a in G, denoted $C_G(a)$, is

$$C_G(a) = \{y \in G \mid ay = ya\}, \tag{4.10}$$

i.e., the set of all elements of G that commute with a.

REMARK: Note that for any $a \in G$, we have $Z(G) \subseteq C_G(a)$. In other words, the center is contained in the centraliser of any element. Also, when it is understood what group G is involved, we usually just write $C(a)$ instead of $C_G(a)$.

There is an alternative definition of centraliser. If $A \subseteq G$ is non-empty, then the centraliser of A in G is $C_G(A) = \{y \in G \mid ay = ya, \text{ for all } a \in A\}$.

Example 4.4.15 Let us find the centraliser of γ in the group S_3. Obviously, since rotations mutually commute, $1, \gamma, \gamma^2 \in C(\gamma)$. We know that $\gamma f \neq f\gamma$. We can calculate that $\gamma f = ...$ (complete this!!). Hence, $C(\gamma) = \{1, \gamma, \gamma^2\}$.

It can be shown that both $C_G(a)$ and $C_G(A)$ are subgroups of G. (show this!!!)

Definition 4.4.7 Normaliser

Let A be a non-empty subset of a group G and let $y \in G$. Define $yAy^{-1} = \{yay^{-1} \mid y \in A\}$. The **normaliser** of A in G is the set $N_G(A) = \{y \in G \mid yAy^{-1} = A\}$.

Notice that if $y \in C_G(A)$, then $yay^{-1} = a \in A$ for all $a \in A$, which implies that $ay = ya$, i.e., $C_G(A) \leq N_G(A)$. We can also show that $N_G(A) \leq G$. (show this!!!)

5 Cosets and Lagrange's Theorem

We have seen in Theorem 4.4.10 that if G is a finite *cyclic* group and $H \leq G$, then the order of H divides the order of G. We will now prove a more general fact, called Lagrange's Theorem, which says that if G is *any* finite group and $H \leq G$, then $|H|$ divides $|G|$.

5.1 Equivalence Relations on a Group

Recall the definition of congruent integers. We write $a \equiv b \pmod{m}$ if $m \mid (a-b) \Rightarrow a - b = km$, $k \in \mathbb{Z}$. We also proved that $\equiv$ was an equivalence relation on the integers modulo m. We will now generalise this notion of congruence to groups and subgroups.

Definition 5.1.1 Congruence Group Elements

Let G be a group and $H \leq G$. For any $a, b \in G$, define $a \equiv b \pmod{H}$, or $a \equiv_H b$, if $ab^{-1} \in H$.

REMARK: Observe that this definition truly is a generalisation of the definition of congruent integers. For if we let $G = (\mathbb{Z}, +)$ and $H = m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\}$, then we get, for $a, b \in \mathbb{Z}$, $a \equiv_{m\mathbb{Z}} b \Leftrightarrow a - b = km$, $k \in \mathbb{Z} \Leftrightarrow a - b \in H$, since "multiplication" in this groups is addition and hence $b^{-1} = -b$.

REMARK: We can define this relation $\equiv_H$ slighly differently by saying that $a \equiv_H b$ if $a^{-1}b \in H$.

We call $\equiv_H$ the **equivalence relation on the group** G. We now prove that $\equiv_H$ is an equivalence relation.

Theorem 5.1.1

Let G be a group and $H \leq G$. Then $\equiv_H$, as defined above, is an equivalence relation.

PROOF: We prove that the relation $\equiv_H$ is reflexive, symmetric, and transitive.

1. Reflexive: For all $a \in G$, $aa^{-1} = 1 \in H$, since H is a (sub)group. So by definition $a \equiv_H a$.
2. Symmetric: For all $a, b \in G$, let $a \equiv_H b$. Then, by definition $ab^{-1} \in H$. Also, since H is a (sub)group, we must have $\left(ab^{-1}\right)^{-1} \in H$. But $\left(ab^{-1}\right)^{-1} = \left(b^{-1}\right)^{-1} a^{-1} = ba^{-1}$. So, by definition, $b \equiv_H a$.
3. Transitive: For all $a, b, c \in G$, suppose $a \equiv_H b$ and $b \equiv_H c$. Then, by definition, $ab^{-1} \in H$ and $bc^{-1} \in H$. Now, $\left(ab^{-1}\right)\left(bc^{-1}\right) = a\left(bb^{-1}\right)c^{-1} = a1c^{-1} = ac^{-1} \in H$, since the product

of two elements in H must also be in H since H is a (sub)group. Hence, by definition, $a \equiv_H c$.

So we have shown that $\equiv_H$ satisfies all the properties of an equivalence relation, and so $\equiv_H$ is an equivalence relation. ■

Recall that for the integers modulo m, we also defined something called a congruence class of an integer, which was the set of all integers that were congruent to that integer. The congruence class is a specific name for what is generally called an **equivalence class**. Given a set X and in equivalence relation on X, an equivalence class of an element $n \in X$ is the subset of all elements in X that are equivalent to n. This makes sense in the context of congruent integers. We now formally define the equivalence class of an element a in a group G.

Definition 5.1.2 Equivalence Class of a Group Element

Let G be a group and $H \leq G$. For any $a \in G$, the equivalence class $[a]$ of a is the set

$$[a] = \{x \in G \,|\, a \equiv_H x\} \subseteq G, \tag{5.1}$$

i.e., $[a]$ is the set of all elements of G that are equivalent to a under $\equiv_H$. We thus also call $[a]$ *an* equivalence class under $\equiv_H$, for there could certainly be other elements of G that that are equivalent to a subset of other elements in G under $\equiv_H$.

5.2 Cosets

Having defined an equivalence relation on a group G with a subgroup H, let us now go further. For example, when we looked at the integers modulo 2, we found that the equivalence classes of 0 and 1, [0] and [1], collectively contained all of the integers, i.e., $\mathbb{Z} = [0] \cup [1]$, with $[0] \cap [1] = \varnothing$. So the equivalence relation "mod 2" gave rise to two equivalence classes, which allowed us to *partition* the integers into two disjoint sets. If we look at the integers modulo 3, [0], [1], and [2], then

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} \,|\, x \equiv 0 \pmod 3\} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} \\
[1] &= \{x \in \mathbb{Z} \,|\, x \equiv 1 \pmod 3\} = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\} \\
[2] &= \{x \in \mathbb{Z} \,|\, x \equiv 2 \pmod 3\} = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}
\end{aligned}$$

So we see that the equivalence relation "mod 3" partitions the integers into three sets, $\mathbb{Z} = [0] \cup [1] \cup [2]$, with each of [0], [1], and [2] being mutually disjoint.

In general: *defining an equivalence relation on a set allows us to partition the set into disjoint equivalence classes under the equivalence relation.*

In the context of a group G with a subgroup H, this means that we can write the set G as a disjoint union of the equivalence classes of $\equiv_H$,

$$G = \bigsqcup_i H_i,$$

where $\bigsqcup$ means that $H_i \cap H_j = \varnothing$, $i \neq j$, and for all $a, b \in H_i$, if $a \equiv_H b$ and $c \in G$ with $c \equiv_H a$, then $c \in H_i$. (The H_i are the equivalence classes.) If G is finite, then

$$|G| = \sum_i |H_i| \,,$$

where $|H_i|$ is the cardinality of the set H_i.

Let us know determine the actual form of these equivalence classes. Let us fix an equivalence class H_i and let $a \in H_i$. By definition, then

$$b \in H_i \Leftrightarrow a \equiv_H b \Leftrightarrow ab^{-1} = h \in H \Leftrightarrow b = h^{-1}a \Rightarrow b = \tilde{h}a,\ \tilde{h} \in H.$$

Now, let

$$Ha = \{ha \,|\, h \in H\} \,.$$

Since by definition all elements of H_i are congruent under $\equiv_H$ to a, and since, from above, $a \equiv_H b \Leftrightarrow b = \tilde{h}a$ for some arbitrary element $\tilde{h} \in H$, we have that $H_i = Ha$.

REMARK: If we instead use the alternate definition of $\equiv_H$ given in a previous remark, and if we define $aH = \{ah \,|\, h \in H\}$, then we have that $H_i = aH$.

Definition 5.2.1 Left and Right Cosets

Let G be a group and $H \leq G$. For any $a \in G$, the set

$$aH = \{ah \,|\, h \in H\} \tag{5.2}$$

is a subset called a **left coset** of H in G, and the set

$$Ha = \{ha \,|\, h \in H\} \tag{5.3}$$

is a subset called a **right coset** of H in G. We call a a **representative** of Ha and aH.

Definition 5.2.2 Representative Set

The **representative set** of right (left) cosets of H in G is a subset R of H (i.e., the elements of R are some elements of H) such that for every coset C of G $|C \cap R| = 1$.

REMARK: The set of representatives of right (left) cosets is not unique, as we'll see later in examples.

We thus see that *every equivalence class under* $\equiv_H$ *is a right coset.*

REMARK: If we instead use the alternate definition of $\equiv_H$, then every equivalence class under $\equiv_H$ is a left coset.

Theorem 5.2.1

All equivalence classes under $\equiv_H$ are of the same size, and therefore, from above, $|G| = n\,|H| \Rightarrow |H| \mid |G|$.

PROOF: We will see the pf of this as a direct consequence of an upcoming theorem. ■

Theorem 5.2.2

Let G be a group and $H \leq G$. Given any $b \in G$ and $c \in Hb$, $Hb = Hc$.

PROOF: Let $c = hb$ for some $h \in H$. To show that $Hb = Hc$, we have to show that $Hb \subseteq Hc$ and $Hc \subseteq Hb$. Now, for any $g \in Hb$, there exists a $\tilde{h} \in H$ such that $g = \tilde{h}b$. Now, let $h' = \tilde{h}h^{-1} \in H$. Then, $h'c = \tilde{h}h^{-1}c = \tilde{h}h^{-1}hb = \tilde{h}1b = \tilde{h}b = g$. Thus, $g \in Hc$, so we have shown that $Hb \subseteq Hc$. Now, for any $g \in Hc$, there exists an $\tilde{h} \in H$ such that $g = \tilde{h}c$. Then, $g = \tilde{h}c = \tilde{h}hb = h'b$, where $h' = \tilde{h}h \in H$, because H is closed under multiplication, being a (sub)group. Thus, $g \in Hb$, and we have shown that $Hc \subseteq Hb$. Therefore, $Hb = Hc$. ■

Theorem 5.2.3

Let G be a group and $H \leq G$. Then $Ha = Hb$ if and only if $ab^{-1} \in H$. (or $aH = bH$ if and only if $b^{-1}a \in S$).

PROOF: If $Ha = Hb$, then $a = 1a \in Ha = Hb$, and so there is an $h \in H$ with $a = hb$; hence, $ab^{-1} = h \in H$. Conversely, assume that $ab^{-1} = \sigma \in H$; hence, $a = \sigma b$. To prove that $Ha = Hb$, we prove two inclusions. If $x \in Ha$, then $x = ha$ for some $h \in H$, and so $x = h\sigma b \in Hb$; similarly, if $y \in Hb$, then $y = \tilde{h}b$ for some $\tilde{h} \in H$ and $y = \tilde{h}\sigma^{-1}a \in Ha$. Therefore, $Ha = Hb$. ■

The following corollary proves that distinct equivalence classes under $\equiv_H$ are indeed disjoint, as we have been asserting all along.

Corollary 5.2.1

Let G be a group and $H \leq G$. Then any two right (or any two left) cosets of H in G are either identical or disjoint.

PROOF: We show that if there exists an element $x \in Ha \cap Hb$, then $Ha = Hb$. Such an x has the form $x = ha = a\tilde{h}$ for some $h, \tilde{h} \in H$. Hence, $ab^{-1} = \tilde{h}h \in H$, and so the theorem above gives $Ha = Hb$. ■

We now show and prove, in the next theorem, that the right cosets (and left cosets) of a subgroup H of G comprise a *partition* of G; in particular, G is a disjoint union of the right cosets of H in G.

Theorem 5.2.4

Let G be a group and $H \leq G$. Then,

1. We can pick a set R of represenatives in each (right or left) coset of H. If there are n right cosets of H in G, then there exist representatives $a_1, \ldots, a_n \in G$ such that $a_1H, \ldots, a_nH$ is the family of all left cosets and $Ha_1, \ldots, Ha_n$ is the family of all right cosets (and $|R| = n$). In fact,
$$G = \bigsqcup_{a \in R} Ha = \bigsqcup_{a \in R} aH.$$
2. For all $a, b \in G$, there is a bijection between the two cosets Ha and Hb given by $f : Ha \to Hb$, with $f(g) = ga^{-1}b$ for some $g \in Ha$.
3. For all $a, b \in G$, there is a bijection between a right coset Ha and a left coset bH.

PROOF: We prove only the second and third statements.

2. We must first check that the bijection f is well-defined, that is, we must check that $f(g) \in Hb$, i.e., we need to check that $g^{-1}ab \in Hb$. Let $g = ha$ for some $h \in H$ (we write this because we have that $g \in Ha$ by definition of the bijection). Then, $f(g)\, b^{-1} = \left(ga^{-1}b\right) b^{-1} = haa^{-1}bb^{-1} = h \in H$, so by definition of $\equiv_H$, we have $f(g) \equiv_H b$, which means that $f(g) \in Hb$ by definition of equivalence class.

   Next, we prove that f is indeed a bijection, i.e., that it is one-to-one and onto.

   One-to-One: Let $g_1, g_2 \in G$ and $f(g_1) = f(g_2)$. By definition of f, this gives $g_1a^{-1}b = g_2a^{-1}b \Rightarrow g_1 = g_2$ by the cancellation law. So f is one-to-one.

   Onto: Let $\tilde{g} = hb \in Hb$ for some $h \in H$. Let $g = ha \in Ha$. Then, $f(g) = ga^{-1}b = haa^{-1}b = hb = \tilde{g}$. So we have shown that for every element $\tilde{g}$ in the codomain Hb there exists an element g in the domain Ha such that $f(g) = \tilde{g}$, and so f is onto.

   So f is a bijection.

3. Let Ha be a right coset and bH a left coset. Then define $f : Ha \to bH$ such that $f(g) = bga^{-1}$. We can easily prove that this is a bijection (do it!). ■

Corollary 5.2.2

Let G be a group and $H \leq G$. Then the size of each right coset of H in G is the same.

PROOF: This follows immediately from the second statement of the previous theorem since there exists a bijection between two right cosets. ■

Corollary 5.2.3

Let G be a group and $H \leq G$. Then the number of right cosets of H in G is equal to the number of left cosets of H in G.

PROOF: This follows immediately from the third statement of the previous theorem since there exists a bijection from a right coset to a left coset. ■

Theorem 5.2.5

Let G be a group and $H \leq G$. Then $Ha = aH$ for all $a \in G$ if and only if G is Abelian.

PROOF: This follows immediately from the definition of Abelian and the definitions of the left and right cosets,

$$Ha = \{ha \,|\, h \in \mathbb{H}\} = \{ah \,|\, h \in \mathbb{H}\} = aH,$$

for all $a \in G$. ■

5.3 Lagrange's Theorem

The purpose of this section is to present and prove Lagrange's theorem as simply a result of the theory of cosets we have just developed.

Definition 5.3.1 Index of a Subgroup

Let G be a group and $H \leq G$. The **index** of H in G, denoted $[G : H]$ is the number of right cosets of H in G.

REMARK: Intuitively, the index of a subgroup H of G is the "relative size" of H in G; equivalently, it is the number of "copies" (cosets) of H that fill up G. For example, if H has index 2 in G, then "half" of the elements of G lie in H.

Lemma 5.3.1 Let G be a group and $H \leq G$. Then for any $a \in G$, $|H| = |aH| = |Ha|$.

PROOF: To show that the two sets H and aH have the same number of elements, we need to construct a map from H to aH that is one-to-one and onto. Let $f : H \to aH$ be the map defined by $f(h) = ah$. Then, f is one-to-one because if $f(h_1) = f(h_2)$, then $ah_1 = ah_2 \Rightarrow h_1 = h_2$ by the cancellation law. As well, f is onto because for any $y \in aH$, we have $y = ah$ for some $h \in H$, hence $y = f(h)$. We can similarly show that any right coset Ha of H has the same number of elements as H. ■

Theorem 5.3.1 Lagrange

If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$ and $[G : H] = \frac{|G|}{|H|}$.

PROOF: By Theorem 5.2.4 Part 1,

$$G = \bigsqcup_{a \in R} Ha = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_n,$$

and so $|G| = \sum_{i=1}^{n} |Ha_i|$. But each right coset of H in G is the same size, so $|G| = |R|\,|H|$ (how does $|Ha| = |H|$?). But $|R|$ is simply the number of right cosets, i.e., $|R| = n$, and so $|G| = n\,|H|$, i.e., $|H|$ divides $|G|$. Furtherfore, since n is the number of right cosets, by definition, $[G : H] = n$, hence $n = [G : H] = \frac{|G|}{|H|}$. ■

REMARK: If G is an infinite group, the quotient $\frac{|G|}{|H|}$ does not make sense. Infinite groups may have subgroups of finite or infinite index.

Corollary 5.3.1

If G is a finite group and $a \in G$, then the order of a divides the order of G. In particular, $a^{|G|} = 1$ for all $a \in G$.

PROOF: We have that $o(a) = |\langle a \rangle|$, and so the result follows from Lagrange's Theorem. The second statement is then clear since $|G|$ is a multiple of the order of a. ■

Example 5.3.1 Let G be a group of order seven. Then, by Lagrange's theorem, G has no non-trivial proper subgroups, since no number other than 7 and 1 divides 7 (i.e., 7 is a prime number). If we let $a \in G$ with $a \neq 1$, then $|a| \neq 1$. Hence, $|a| = 7 = |\langle a \rangle|$, which means that $\langle a \rangle$ is the whole group, i.e., $G = \langle a \rangle$, so G is cyclic.

Corollary 5.3.2

If p is a prime number and $|G| = p$, then G is a cyclic group.

PROOF: Take $a \in G$ with $a \neq 1$. Then the cyclic subgroup $\langle a \rangle$ has more than one element (since it contains a and 1), and its order $|\langle a \rangle| > 1$ is a divisor of p by Lagrange's theorem. Since p is a prime number, $|\langle a \rangle| = p = |G|$, and so $\langle a \rangle = G$. ■

5.4 Examples

We now go through some examples of cosets and illustrate Lagrange's theorem.

Example 5.4.1 In $\mathbb{Z}$, consider the subgroups $3\mathbb{Z} \subseteq 6\mathbb{Z}$. The cosets of $6\mathbb{Z}$ are:

$$\begin{aligned} &6\mathbb{Z} \\ &1 + 6\mathbb{Z} = 6\mathbb{Z} + 1 \\ &2 + 6\mathbb{Z} = 6\mathbb{Z} + 2 \\ &3 + 6\mathbb{Z} = 6\mathbb{Z} + 3 \\ &4 + 6\mathbb{Z} = 6\mathbb{Z} + 4 \\ &5 + 6\mathbb{Z} = 6\mathbb{Z} + 5 \end{aligned}$$

The coset of $6\mathbb{Z}$ that is in $3\mathbb{Z}$ is $3 + 6\mathbb{Z}$.

Example 5.4.2 Recall that permutation group of three distinct objects S_3, which was also the dihedral group D_3 of order six,

$$S_3 = \left\{a, b \,|\, a^2 = b^3 = 1,\, ba = ab^2\right\} = \left\{1, b, b^2, a, ab, ab^2\right\}.$$

Consider the subgroups

$$\begin{aligned} H = \langle a \rangle = \{1, a\} &\Rightarrow |H| = 2 \\ C = \langle b \rangle = \left\{1, b, b^2\right\} &\Rightarrow |C| = 3. \end{aligned}$$

Now, $|S_3| = 6$, and we see that $2 \,|\, 6$ and $3 \,|\, 6$, so that Lagrange's theorem is verified.

Now, let us look at the right cosets of H:

$$\begin{aligned} H1 &= \{1 \cdot 1, a1\} = \{1, a\} = H \\ Ha &= \{1a, a \cdot a\} = \{a, 1\} = H \\ Hb &= \{1b, ab\} = \{b, ab\} \\ Hab &= \{1ab, a \cdot ab\} = \left\{ab, a^2b\right\} = \{ab, b\} = Hb \\ Hb^2 &= \left\{1b^2, ab^2\right\} = \left\{b^2, ab^2\right\} \\ Hab^2 &= \left\{1ab^2, a \cdot ab^2\right\} = \left\{ab^2, b^2\right\} = Hb^2. \end{aligned}$$

Notice that since we have duplication in the right cosets of H, there are only three cosets of H, $\left\{H1, Hb, Hb^2\right\}$, i.e., $[S_3 : H] = 3$. The representative set of this coset can be taken as $R = \left\{1, b, b^2\right\}$. Observe that $|R| = 3$, as it should be by Lagrange's theorem. However, we could also take as the cosets of H $\left\{Ha, Hab, Hb^2\right\}$ and the corresponding representative set $R = \left\{a, ab, b^2\right\}$.

Now let's look at the left cosets of H:

$$\begin{aligned} 1H &= \{1 \cdot 1, 1a\} = H \\ aH &= \{a1, a \cdot a\} = H \\ bH &= \{b1, ba\} = \left\{b, ab^2\right\} \\ abH &= \{ab1, aba\} = \left\{ab, a \cdot ab^2\right\} = \left\{ab, b^2\right\} \\ b^2H &= \left\{b^21, b^2a\right\} = \left\{b^2, bba\right\} = \left\{b^2, bab^2\right\} = \left\{b^2, ab^2b^2\right\} = \left\{b^2, ab\right\} \\ ab^2H &= \left\{ab^21, ab^2a\right\} = \left\{ab^2, aab\right\} = \left\{ab^2, b\right\}. \end{aligned}$$

So we also have three left cosets of H. Observe that for all $c \in G$, $cH \neq Hc$, i.e., the left and right cosets are not equal. This is to be expected since, unlike $\mathbb{Z}$, S_3 is a non-Abelian group. We can also find the left and right cosets of C (do it!).

Example 5.4.3 Let us look back at our integers modulo m. Specifically, let $G = (\mathbb{Z}, +)$ and $H = 2\mathbb{Z} = \{2n \,|\, n \in \mathbb{Z}\}$, the set of even integers. Now, for any $a, b \in \mathbb{Z}$, $a \equiv_H b$ means, by definition, that $ab^{-1} \in H$, i.e., that $a - b \in 2\mathbb{Z}$. Note carefully what $a - b \in 2\mathbb{Z}$ means—it does *not* mean that a and b are necessarily even. It just means that a and b have the same *parity*, i.e., that a and b are either odd or even. With this in mind, let us look at some right cosets Ha, where $a \in \mathbb{Z}$:

$$\begin{aligned} H0 &= 2\mathbb{Z} + 0 = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\} \\ H1 &= 2\mathbb{Z} + 1 = \{\dots, -7, -5, -3, -1, 1, 3, 5, 7, \dots\} \\ H2 &= 2\mathbb{Z} + 2 = \{\dots, -4, -2, 0, 2, 4, 6, 8, \dots\} \\ H3 &= 2\mathbb{Z} + 3 = \{\dots, -5, -3, -1, 1, 3, 5, 7, 9, \dots\} \\ &\vdots \end{aligned}$$

First of all, notice that these cosets do constitute equivalence classes, since, for example, all elements in $H0$ are congruent to one another under $\equiv_H$, or $\equiv_{2\mathbb{Z}}$. Secondly, notice that $H0 = H2 = H4 = \dots$ and $H1 = H3 = H5 = \dots$. We see that there are only *two* right cosets of $2\mathbb{Z}$ in G, and that these constitute, as expected, the even and odd integers. We could take as these two cosets any of $H0, H2, H4, \dots$ or $H1, H3, H5, \dots$ for the even and odd integers, respectively. The representative set of these right cosets contains only two elements, since there are only two right cosets. We could take as these two representatives either $\{0, 1\}$, $\{4, 9\}$, or any pair of even and odd integers. This is why the representative set is not unique. Let us take $R = \{0, 1\}$. By Theorem 5.2.4, therefore, we get

$$G = \mathbb{Z} = \bigsqcup_{a \in \{0,1\}} Ha = \bigsqcup_{a \in \{0,1\}} (2\mathbb{Z} + a) = (2\mathbb{Z} + 0) \cup (2\mathbb{Z} + 1)\,,$$

as expected: the odd and even integers together consitute all the integers. Or, if we let $R = \{42, 7\}$, we get

$$\mathbb{Z} = \bigsqcup_{a \in \{42,7\}} = (2\mathbb{Z} + 42) \cup (2\mathbb{Z} + 7)\,.$$

Finally, since $(\mathbb{Z}, +)$ is an Abelian group, we have by Theorem 5.2.5 that the right cosets are equal to the left cosets. For instance,

$$\begin{aligned} 0H &= 0 + 2\mathbb{Z} = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\} = H0 \\ 1H &= 1 + 2\mathbb{Z} = \{\dots, -7, -5, -3, -1, 1, 3, 5, 7, \dots\} = H1. \end{aligned}$$

So we can also write

$$G = \mathbb{Z} = \bigsqcup_{a \in \{0,1\}} aH = \bigsqcup_{a \in \{0,1\}} (a + 2\mathbb{Z}) = (0 + 2\mathbb{Z}) \cup (1 + 2\mathbb{Z})\,.$$

Though this example has not showed us anything we didn't already know (indeed, we didn't need the theory of cosets to determine what we have just shown), the theory of cosets allows us to make analogous statements about *any* group and its subgroups.

Example 5.4.4 Still using the group $G = (\mathbb{Z}, +)$, let us now take the subgroup $H = 3\mathbb{Z} = \langle 3 \rangle = \{3n \,|\, n \in \mathbb{Z}\}$. Based on the previous example, we have that the left and right cosets, which coincide, are

$$\begin{aligned} H0 = 0H = 3\mathbb{Z} &= \{\dots, -6, -3, 0, 3, 6, \dots\} \\ H1 = 1H = 1 + 3\mathbb{Z} &= \{\dots, -5, -2, 1, 4, 7, \dots\} \\ H2 = 2H = 2 + 3\mathbb{Z} &= \{\dots, -4, -1, 2, 5, 8, \}\end{aligned}$$

The representative set is then $R = \{0, 1, 2\}$, and hence

$$\begin{aligned} \mathbb{Z} &= \bigsqcup_{a \in \{0,1,2\}} Ha = \bigsqcup_{a \in \{0,1,2\}} aH \\ &= \bigsqcup_{a \in \{0,1,2\}} (a + 3\mathbb{Z}) = \bigsqcup_{a \in \{0,1,2\}} (3\mathbb{Z} + a) \\ &= (0 + 3\mathbb{Z}) \cup (1 + 3\mathbb{Z}) \cup (2 + 3\mathbb{Z}) \\ &= (3\mathbb{Z} + 0) \cup (3\mathbb{Z} + 1) \cup (3\mathbb{Z} + 2)\,, \end{aligned}$$

is the partitioning of $\mathbb{Z}$ under $3\mathbb{Z}$.

From the two above integer group examples, we see the following result: if G is the the set of integers under addition, and H the subgroup $n\mathbb{Z}$, then the number of cosets of H in G is n. More concisely,

$$\boxed{\text{If } G = (\mathbb{Z}, +) \text{ and } H = n\mathbb{Z}, \text{ then } [\mathbb{Z} : n\mathbb{Z}] = n} \,. \tag{5.4}$$

Also observe one other thing in both of the examples above. When we looked at the subgroup $H = 2\mathbb{Z}$ of the integers $\mathbb{Z}$ under addition, the cosets were nothing but the *integer congruence class* modulo 2, i.e., $H0 = 0H = [0]$ and $H1 = 1H = [1]$. In particular the *set of cosets* of $2\mathbb{Z}$ in $\mathbb{Z}$ is $\{H0, H1\} = \{[0], [1]\} = \mathbb{Z}_2$! The same applies for the subgroup $3\mathbb{Z}$: the set of cosets is simply $\mathbb{Z}_3$ the integers modulo 3. And as we know, the integers modulo n, $\mathbb{Z}_n$, form a group under addition modulo n. So it appears that the set of cosets of a subgroup H in a group G is itself a group. We will come back to this important point later.

Example 5.4.5 Let us now consider the group $G = (\mathbb{Z}_{15}, +)$ and the subgroup $H = \langle [3] \rangle =$

$\{[0],[3],[6],[9],[12]\}$. Then H partitions $\mathbb{Z}_{15}$ as follows:

$$\begin{aligned}
[0]H &= [0] + \langle[3]\rangle = \{[0],[3],[6],[9],[12]\} = H = H[0] \\
[1]H &= [1] + \langle[3]\rangle = \{[1],[4],[7],[10],[13]\} = H[1] \\
[2]H &= [2] + \langle[3]\rangle = \{[2],[5],[8],[11],[14]\} = H[2] \\
[3]H &= [3] + \langle[3]\rangle = \{[3],[6],[9],[12],[15] = [0]\} = H[3] = [0]H = H[0] \\
&\vdots
\end{aligned}$$

So we see that there are only three left and right cosets of H in G, and so the representative set can be taken as $R = \{[0],[1],[2]\}$. Therefore,

$$\mathbb{Z} = \bigsqcup_{a\in\{[0],[1],[2]\}} (a + \langle[3]\rangle) = ([0] + \langle[3]\rangle) \cup ([1] + \langle[3]\rangle) \cup ([2] + \langle[3]\rangle)$$

is the partitioning of $\mathbb{Z}_{15}$ under $\langle[3]\rangle$.

Example 5.4.6 Let H be a subgroup of a group G, where $|G| = 10$. Then, by Lagrange's theorem, $|H| = 1, 2, 5, 10$, since these are the divisors of 10. For example, if $G = D_5 = \{1, \gamma, \gamma^2, \gamma^3, \gamma^4, f, f\gamma, f\gamma^2, f\gamma^3, f\gamma^4\}$. Then, $|\langle 1\rangle| = 1$, $\left|\langle\gamma^i\rangle\right| = 5$, $|\langle f\rangle| = \left|\langle f\gamma^i\rangle\right| = 2$, for $1 \leq i \leq 4$, and, of course, $|D_5| = 10$.

6 Isomorphisms and Quotient Groups

In this section we make precise the notion of when two groups "look the same", that is, have exactly the same group-theoretic structure. This is the notion of an *isomorphism* between two groups. We first define the notion of a *homomorphism.*

First, some notation: we will use C_n to denote a general cyclic group of order n, or write $\langle g,\, o(g) = n\rangle$. And we'll denote a general infinite cyclic group by C_∞.

6.1 Homomorphisms

Definition 6.1.1 Group Homomorphism

Let G be a group under $*$ and K a group under $\Diamond$. A mapping $f : G \to K$ is a **group homomorphism** if for any $a, b \in G$ $f(a * b) = f(a) \Diamond f(b)$.

Observe the emphasis placed on the operation under which G and K are groups. Specifically, note that the right-hand side of the above equation is multiplication by $\Diamond$, i.e., multiplication of elements in K, and the left-hand side is multiplication by $*$, i.e., muliplication of elements in G. From now on, we will simply write $f(ab) = f(a) f(b)$. Intuitively, a mapping f is a homomorphism if it respects the group structures of its domain and codomain.

Example 6.1.1 Below are some examples of homomorphisms.

1. The mapping $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = 5x$ is a homomorphism (with group $(\mathbb{Z}, +)$) since $f(x + y) = 5(x + y) = 5x + 5y = f(x) = f(y)$.

2. The mapping $f : \mathbb{R}^* \to \mathbb{Z}_2$ given by

$$f(x) = \begin{cases} 0 & \text{if } x > 0 \\ 1 & \text{if } x < 0 \end{cases}$$

   is a homomorphism. To check this, note that if x and y are both positive, then xy is positive and $f(xy) = 0 = 0 + 0 = f(x) + f(y)$. Also, if x and y are both negative, then xy is positive and $f(xy) = 0 = 1 + 1 = f(x) + f(y)$. Also, if x is positive and y is negative, then xy is negative and $f(xy) = 1 = 0 + 1 = f(x) + f(y)$ and similarly in the opposite case in which x is negative and y is positive.

3. Let $f : \mathbb{Z} \to \mathbb{Z}_5$ be defined by

$$f(n) = \text{the remainder of } n \text{ mod } 5.$$

So, for instance, we have $f(7) = [2]$, $f(8) = [3]$, $f(7+8) = f(15) = [0]$, and $f(7) + f(8) = [2] + [3] = [0]$ in $\mathbb{Z}_5$. For any $n, m \in \mathbb{Z}$, we can apply the division algorithm to write $n = q[5] + f(n)$ and $n = p[5] + f(m)$. We then have $n + m = (q+p)[5] + (f(n) + f(m))$, and $f(n+m)$ is the sum of $f(n)$ and $f(m)$ in $\mathbb{Z}_5$, so f is a homomorphism.

Definition 6.1.2 Kernel

Let $f : G \to K$ be a homomorphism from G to K and let 1_K denote the identity element in K. Then the **kernel** of f is the set $\{x \in G \mid f(x) = 1_K\}$, denoted $\text{Kern}(f)$.

Definition 6.1.3 Image

Let $f : G \to K$ be a homomorphism from G to K. The **image** of G under f, denoted $Im(f)$, is the set $\text{Im}(f) = \{f(x) \mid x \in G\}$.

Definition 6.1.4 Identity Homomorphism

For any group G, the **identity mapping** $f : G \to G$ such that $f(x) = x$ is always a homomorphism since $f(xy) = xy = f(x) f(y)$. (Obviously, the identity mapping is not in general the *only* homomorphism from G to itself.)

Definition 6.1.5 Trivial Homomorphism

For any groups G and K, the mapping $f : G \to K$, given by $f(x) = 1_K$, where 1_K denotes the identity element of K, is a homomorphism. It is called the **trivial homomorphism** between G and K. Indeed, $f(xy) = 1_K = 1_K 1_K = f(x) f(y)$ for any $x, y \in G$. In this case $\text{Im}(f) = \{1_K\}$ and $\text{Kern}(f) = G$.

Definition 6.1.6 Exponential Homomorphism

For any group G and any $a \in G$, the mapping $f : \mathbb{Z} \to \langle a \rangle$ is called the *exponential mapping* and is given by $f(n) = a^n$. f is a homomorphism between $\mathbb{Z}$ and $\langle a \rangle$ since $f(n+m) = a^{n+m} = a^n a^m = f(n) f(m)$ for any $n, m \in \mathbb{Z}$.

Theorem 6.1.1

For any groups G, H, and K, suppose $f : G \to H$ and $g : H \to K$ are both homomorphisms. Then the composite mapping $g \circ f(x) = g(f(x))$ is a homomorphism from G to K.

PROOF: Consider any $x, y \in G$. We have $g \circ f(xy) = g(f(xy)) = g(f(x) f(y)) = g(f(x)) g(f(y)) = g \circ f(x) g \circ f(y)$. ■

Example 6.1.2 The kernels of the examples shown in Example 6.1.1 are, in order (also do the images!):

1. Figure it out!
2. The kernel of $f : \mathbb{R}^* \to \mathbb{Z}_2$ is $\text{Kern}(f) = \{x \in \mathbb{R}^* \mid x \text{ is positive}\}$.
3. The kernel of $f : \mathbb{Z} \to \mathbb{Z}_5$ is $\text{Kern}(f) = 5\mathbb{Z}$.

Example 6.1.3 The kernel of $f : \mathbb{Z} \to \langle a \rangle$ is $\text{Kern}(f) = \{n \mid o(a) \text{ divides } n\}$.

Theorem 6.1.2 Basic Group Homomorphism Properties

Let $f : G \to K$ be a homomorphism from G to K. Then,

1. $f(1_G) = 1_K$, where 1_G and 1_K are the identity elements in G and K, respectively.
2. $f\left(a^{-1}\right) = (f(a))^{-1}$ for any $a \in G$.
3. $f(a^n) = f(a)^n$ for any $n \in \mathbb{Z}$ and $a \in G$.
4. If $o(a)$ is finite, then $|f(a)|$ divides $o(a)$.
5. If H is a subgroup of G, then $f(H) = \{f(x) \mid x \in H\}$ is a subgroup of K.
6. If J is a subgroup of K, then $f^{-1}(J) = \{x \in G \mid f(x) \in J\}$ is a subgroup of G.

PROOF: We prove each in turn.

1. Since $f(1_G) f(1_G) = f(1_G 1_G) = f(1_G) = 1_K f(1_G)$, we have $f(1_G) = 1_K$ by the cancellation law.
2. Since $f(a) f\left(a^{-1}\right) = f\left(aa^{-1}\right) = f(1_G) = 1_K = f(a)(f(a))^{-1}$, we have $f\left(a^{-1}\right) = (f(a))^{-1}$ by the cancellation law.
3. We prove this by induction on n. Let A be the set of all $n > 0$ (i.e., natural numbers) for which $f(a^n) = f(a)^n$.
   (a) Clearly, for $n = 1$, $f\left(a^1\right) = f(a)^1$, so that 1 is in A.
   (b) Assume n is in A, i.e., assume $f(a^n) = f(a)^n$. Then $f\left(a^{n+1}\right) = f(a^n a) = f(a^n) f(a) = f(a)^n f(a) = f(a)^{n+1}$, so $n + 1$ is in A.

So by induction, the result holds for $n > 0$. For $n = 0$, the result follows from 1., and for $n < 0$, the result follows from induction on $-n$.

4. Let $o(a) = n < \infty$. Then, by 3., we have $f(a)^n = f(a^n) = f(1_G) = 1_K$. So $f(a)^n = 1_K$, which implies that $|f(a)|$ divides n by Theorem 4.2.5.

5. We use the subgroup test. Let $u, v \in f(H) = \{u \in K \mid u = f(x) \text{ for some } x \in H\}$, and let $x, y \in H$ be such that $u = f(x)$ and $v = f(y)$. Then, $xy^{-1} \in H$ since H is a subgroup and $uv^{-1} = f(x) f(y)^{-1} = f\left(xy^{-1}\right) \in f(H)$. Hence, by the subgroup test, $f(H)$ is a subgroup of G.

6. We again use the subgroup test. Let $x, y \in f^{-1}(J)$. We have $f\left(xy^{-1}\right) = f(x) f(y)^{-1} \in J$. Hence, $xy^{-1} \in f^{-1}(J)$ and $f^{-1}(J)$ is a subgroup of G. ■

Theorem 6.1.3

Let $f : G \to K$ be a homomorphism from G to K. Then,

1. $\text{Kern}(f)$ is a subgroup of G.
2. $\text{Im}(f)$ is a subgroup of K.

PROOF: We prove each in turn.

1. Since $1_G \in \text{Kern}(f)$, the kernel of f is not empty. Let $x, y \in \text{Kern}(f)$, that is $f(x) = f(y) = 1_K$. Then,

$$f\left(xy^{-1}\right) = f(x) f\left(y^{-1}\right) = f(x) f(y)^{-1} = 1_H 1_H^{-1} = 1_H,$$

   i.e., $xy^{-1} \in \text{Kern}(f)$. So by the subgroup test, $\text{Kern}(f) \leq G$.

2. Since $f(1_G) = 1_K$, the identity of K lies in the image if f, so $\text{Im}(f)$ is non-empty. If x and y are in $\text{Im}(f)$, say $x = f(a)$ and $y = f(b)$, then $y^{-1} = f(b)^{-1} = f\left(b^{-1}\right)$, so that $xy^{-1} = f(a) f\left(b^{-1}\right) = f\left(ab^{-1}\right)$ since f is a homorphism. Hence also xy^{-1} is an image of f, so $\text{Im}(f)$ is a subgroup of K by the subgroup test. ■

Theorem 6.1.4

Let $f : G \to K$ be a homomorphism from G to K. Then f is one-to-one if and only if the kernel of f is trivial, i.e., $\text{Kern}(f) = \{1_G\}$.

PROOF: ($\Rightarrow$): Suppose f is one-to-one and suppose $x \in \text{Kern}(f)$. Then, $f(x) = 1_K = f(1_G) \Rightarrow x = 1_G$ since f is one-to-one, and so $\text{Kern}(f) = \{1_G\}$. ($\Leftarrow$): Suppose $\text{Kern}(f) = \{1_G\}$ and suppose for some $x, y \in G$ that we have $f(x) = f(y)$. Then, $f\left(xy^{-1}\right) = f(x) f\left(y^{-1}\right) = f(x) f(y)^{-1} = f(y) f(y)^{-1} = 1_K$. It follows that $xy^{-1} \in \text{Kern}(f) = \{1_G\}$, i.e., we must have $xy^{-1} = 1_G \Rightarrow x = y$, so f is one-to-one. ■

Theorem 6.1.5

Let $f : G \to K$ be a mapping from the group G to the group K. If G can be presented as a generator relation, to show that f is a homomorphism it is enough to show that f is a mapping satisfying the generator relation of G.

We use the above theorem in the next example.

Example 6.1.4 Find all the homomorphisms from the group S_3 to $\mathbb{Z}_6$, and state their kernels and images.

SOLUTION: Recall that we may write S_3 as a generator relation: $S_3 = \langle a, b \,|\, a^2 = b^3 = 1, ba = ab^2 \rangle$. Specifically, $S_3 = \{1, b, b^2, a, ab, ab^2\}$. Now, since f must map the identity of S_3 to the identity of $\mathbb{Z}_6$, we must have $f(1) = [0]_6$. Now, observe that all elements of S_3 are of the form $a^i b^j$ for $0 \leq i \leq 1$ and $0 \leq j \leq 2$. Then, $f\left(a^i b^j\right) = f\left(a^i\right) f\left(b^j\right) = (f(a))^i (f(b))^j$.

Now,

$$[0]_6 = f(1) = f\left(a^2\right) = (f(a))^2 \Rightarrow o(f(a)) \mid 2 \Rightarrow o(f(a)) = 1 \text{ or } 2$$
$$[0]_6 = f(1) = f\left(b^3\right) = (f(b))^3 \Rightarrow o(f(b)) \mid 3 \Rightarrow o(f(b)) = 1, 2 \text{ or } 3.$$

f must also satsify the relation $ba = ab^2$, so that

$$f(ba) = f(b) f(a) = f\left(ab^2\right) = f(a) (f(b))^2,$$

but since $\mathbb{Z}_6$ is Abelian, we may write

$$f(a) f(b) = f(a) (f(b))^2 \Rightarrow f(b) = (f(b))^2 \Rightarrow f(b) = [0]_6.$$

So we have fixed $f(b)$. Therefore, we have two cases:

Case 1 $o(f(a)) = 2$

Since $[3]_6$ is the only element of $\mathbb{Z}_6$ of order 2, we must have $f(a) = [3]_6$. Therefore, the homomorphism is

$$f = \begin{pmatrix} 1 & b & b^2 & a & ab & ab^2 \\ [0]_6 & [0]_6 & [0]_6 & [3]_6 & [3]_6 & [3]_6 \end{pmatrix}$$

Hence,

$$\text{Kern}(f) = \{1, b, b^2\} = \langle b \rangle$$
$$\text{Im}(f) = \{[0]_6, [3]_6\} = \langle [3]_6 \rangle \leq \mathbb{Z}_6$$

Case 2 $o(f(a)) = 1$

The only element of order 1 is the identity (always!), i.e., $f(a) = [0]_6$. So the homomorphism is the trivial homomorphism,

$$f = \begin{pmatrix} 1 & b & b^2 & a & ab & ab^2 \\ [0]_6 & [0]_6 & [0]_6 & [0]_6 & [0]_6 & [0]_6 \end{pmatrix}.$$

Therefore,

$$\begin{aligned} \text{Kern}\,(f) &= S_3 \\ \text{Im}\,(f) &= \{[0]_6\} = \langle [0]_6 \rangle \leq \mathbb{Z}_6 \end{aligned}$$

are the kernel and image.

So there are two homomorphisms between S_3 and $\mathbb{Z}_6$. (is there always a trivial homomorphism between any two groups?)

6.2 Isomorphisms

Definition 6.2.1 Isomorphism

A bijective homomorphism $f : G \to K$ from G to K (i.e., a homomorphism that is one-to-one and onto) is called an **isomorphism**. The groups G and K are called **isomorphic**, and we write $G \cong K$, if there exists an isomorphism $f : G \to K$.

We also have some additional terminology for two groups G and K:

- An injective (one-to-one) homomorphism $f : G \to K$ is called a **monomorphism** from G to K.
- A surjective (onto) homomorphism $f : G \to K$ is called an **epimorphism** from G to K.
- An isomorphism from G to itself is called an **automorphism**.

To show that two groups G and K are isomorphic, we need to four things:

1. Define a mapping $f : G \to K$, and *show that it is well defined.*
2. Show that f is a homomorphism.
3. Show that f is one-to-one.
4. Show that f is onto.

Example 6.2.1 Let us show that $\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphic groups (under addition). We carry out the four steps outlined above:

1. Define $f : \mathbb{Z} \to 3\mathbb{Z}$ by $f(x) = 3x$. Show that this is well defined!
2. We have $f(x + y) = 3(x + y) = 3x + 3y = f(x) + f(y)$, so f is a homomorphism.
3. $f(x) = 0$ if and only if $3x = 0$, hence if and only if $x = 0$, which, rememeber, is the identity element. So $\text{Kern}\,(f) = \{0\}$, and so by the theorem above f is one-to-one.

4. Given some $u \in 3\mathbb{Z}$, $u = 3x$ for some $x \in \mathbb{Z}$, i.e., $u = f(x)$, so f is onto.

So we have shown all four steps, and so $\mathbb{Z}$ and $3\mathbb{Z}$ are indeed isomorphic.

Example 6.2.2 $\mathbb{R}$, the real numbers under addition, is isomorphic to $\mathbb{R}^+$, the positive real numbers under multiplication. To show this, we again carry out our four steps.

1. Let $f : \mathbb{R} \to \mathbb{R}^+$ be the exponential function $f(x) = e^x$. Show that this is well defined!
2. $f(x+y) = e^{x+y} = e^x e^y = f(x) f(y)$, so f is a homomorphism.
3. The identity element in $\mathbb{R}^+$ is 1. Hence, if $x \in \text{Kern}(f)$, then $f(x) = 1$, which is to say $e^x = 1$, which implies that $x = 0$. So $\text{Kern}(f) = \{0\}$, where 0 is the identity element of $\mathbb{R}$ under addition, so that f is one-to-one.
4. For $u \in \mathbb{R}^+$, let $x = \ln(u)$, the natural logarithm of u. Then $f(x) = e^x = e^{\ln(u)} = u$, and so f is onto.

Example 6.2.3 From the two examples above, we can show that the inverse mappings are both isomorphisms. First, the mapping $f^{-1} : 3\mathbb{Z} \to \mathbb{Z}$, with $f^{-1}(u) = \frac{u}{3}$, is an isomorphism from $3\mathbb{Z}$ to $\mathbb{Z}$. As well, the mapping $f^{-1} : \mathbb{R}^+ \to \mathbb{R}$, with $f^{-1}(u) = \ln(u)$, is an isomorphism from $\mathbb{R}^+$ and $\mathbb{R}$.

Theorem 6.2.1

Let $f : G \to H$ and $g : H \to K$ be isomorphisms. Then

1. The composition $f \circ g : G \to K$ is an isomorphism.
2. The identity mapping $f : G \to G$ is an isomorphism.
3. The inverse $f^{-1} : H \to G$ is an isomorphism.

PROOF: We prove each in turn.

1. $f \circ g$ is a homomorphism by a previous theorem. Additionally, we know that a composition of one-to-one maps is one-to-one, and a composition of onto maps is onto (see Chapter 1).
2. Do this!!
3. Do this!! ■

REMARK: Note carefully what we have just shown. Let us restate the theorem using the notation $G \cong H$ and $H \cong K$ since G and H and H and K are isomorphic. Then, the statements of the theorem are

1. If $G \cong H$ and $H \cong K$, then $G \cong K$.
2. $G \cong G$.
3. If $G \cong H$, then $H \cong G$.

Indeed, the three statements of this theorem are nothing other than the statements of transitivity, reflexivity, and symmetry, respectively, for the binary relation "$\cong$". So "$\cong$" defines an equivalence relation on groups.

Lemma 6.2.1 Let f be an isomorphism from a group G to a group K and let $a \in G$. Then $o(a) = o(f(a))$.

PROOF: Suppose $a \in G$ and let $o(a) = n$ and let m be the order of $f(a)$ in K. We know from Theorem 6.1.2 Part 4 that m divides n. But since $f(a^m) = f(a)^m = 1_K$, and since f is one-to-one, we must have $a^m = 1_G$, and so n divides m. m divides n and n divides m can only be simulatneously possible if $n = m$. This proves the result. ■

Theorem 6.2.2

Let groups G and K be isomorphic, i.e., $G \cong K$. Then,

1. $|G| = |K|$.
2. G is Abelian if and only if K is Abelian.
3. G is cyclic if and only if K is cyclic.
4. G has k elements of order n if and only if K has k elements of order n.

PROOF: Let $f : G \to K$ be an isomorphism.

1. Since f is one-to-one and onto by definition, we must have $|G| = |K|$.
2. Suppose G is Abelian and let $u, v \in K$. Since f is onto, there are $x, y \in G$ with $f(x) = u$ and $f(y) = v$. Then,
$$uv = f(x) f(y) = f(xy) = f(yx) = f(y) f(x) = vu,$$
since G is Abelian. So $uv = vu$ and K is Abelian. If K is Abelian, then $f(xy) = f(x) f(y) = f(y) f(x) = f(xy) = f(yx)$, and since f is one-to-one, we have $xy = yx$, i.e., G is Abelian.
3. If $G = \langle a \rangle$ is cyclic with generator a, then by the lemma above $|f(a)| = o(a) = |G| = |K|$, so that $K = \langle f(a) \rangle$ is cyclic. Conversely, if $K = \langle b \rangle$ is cyclic with generator b, then since f is onto there is an $a \in G$ with $f(a) = b$. But then $o(a) = |f(a)| = o(b) = |K| = |G|$, and so $G = \langle a \rangle$ is cyclic.
4. Suppose $a_1, a_2, \ldots, a_k$ are k distinct element of order n in G. Then since f is one-to-one, $f(a_1), f(a_2), \ldots, f(a_k)$ are all distinct, and by the lemma above, are all of order n. If

$a_1, a_2, \ldots, a_k$ are *all* the elements of G of order n, then $f(a_1), f(a_2), \ldots, f(a_k)$ will be *all* the elements of K of order n. For consider any other element u of K. Since f is onto, $u = f(x)$ for some $x \in G$, and u is distinct from all the $f(a_i)$, x is distinct from all the a_i. Since the a_i were all the elements of G of order n, we have $o(u) = |f(x)| = o(x) \neq n$. ■

Lemma 6.2.2 Let G and H be cyclic groups of the same finite order n, and let a be any generator of G and b any generator of H. Then there is an isomorphism $f : G \to H$ with $f(a) = b$. (Note that the last sentence says "*an* isomorphism"—there could be others!)

PROOF: We have $G = \langle a \rangle$, where $|G| = n$. We know that we can then write

$$G = \left\{1_G, a, a^2, \ldots, a^{n-1}\right\},$$

where these elements are all distinct. Define a mapping $f : G \to H$ by $f\left(a^i\right) = b^i$ for $0 \leq i < n$. We then show that f is an isomorphism. As usual, we go through the four steps.

1. We have just defined the mapping. Is it well defined?
2. Consider two elements a^i and a^j in G, $0 \leq i, j < n$. Then,
$$f\left(a^i a^j\right) = f\left(a^{i+j}\right) = b^{i+j} = b^i b^j = f\left(a^i\right) f\left(a^j\right),$$
so that f is a homomorphism.
3. Denote the identity element of H as 1_H, and let a^i be an element in G. Then $f\left(a^i\right) = b^i = 1_H \Rightarrow i = 0$. So we have $a^i = a^0 = 1_G$, so that $\text{Kern}(f) = \{1_G\}$, and so f is one-to-one.
4. Finally, we show that f is onto. However, notice that since $|G| = |H| = n$, and f is one-to-one, f must necessarily be onto.

So we have shown that an isomorphism f exists, and so the pf is exists. ■

Theorem 6.2.3

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

1. If $|G| = \infty$, then $G \cong \mathbb{Z}$.
2. If $|G| = n < \infty$, then $G \cong \mathbb{Z}_n$.

REMARK: Take note of what this theorem is saying: *all* cyclic groups of infinite order are isomorphic to the integers under addition, while *all* finite cyclic groups are isomorphic to the integers modulo n under addition modulo n. So there is really only *one* finite cyclic group, and only *one* infinite cyclic group!

PROOF: We prove each in turn.

1. If $G = \langle a \rangle$, where $o(a) = \infty$, let $f : \mathbb{Z} \to G$ be the exponential homomorphism defined by $f(k) = a^k$. Since $o(a) = \infty$, $a^k = 1$ if and only if $k = 0$ (we have seen this before!). Hence, $\text{Kern}(f) = \{0\}$, and so f is one-to-one. Since G is cyclic, every $u \in G$ is of the form $u = a^k$ for some $k \in \mathbb{Z}$. Hence $u = f(k)$ and f is onto. So f is an isomorphism from $\mathbb{Z}$ to G, but also f^{-1} is an isomorphism from G to $\mathbb{Z}$.

2. This is immediate from the previous lemma, but we also prove this directly. Let $G = \langle a \rangle$. Define a mapping $f : \mathbb{G} \to \mathbb{Z}_n$ by $f\left(a^k\right) = [k]_n$. We then prove that f is a bijective homomorphism:

   (a) For all $k_1, k_2 \in \mathbb{Z}$, $f\left(a^{k_1} g^{k_2}\right) = f\left(a^{k_1+k_2}\right) = [k_1+k_2]_n = [k_1]_n + [k_2]_n = f\left(a^{k_1}\right) f\left(a^{k_2}\right)$. So f is a homomorphism.

   (b) Let $k_1, k_2 \in \mathbb{Z}$ such that $f\left(a^{k_1}\right) = f\left(a^{k_2}\right)$. Then, $[k_1]_n = [k_2]_n$, which implies that $k_1 \equiv k_2 \pmod{n} \Leftrightarrow n \,|\, k_1 - k_2$, which implies that there exists an $m \in \mathbb{Z}$ such that $k_1 - k_2 = mn \Rightarrow k_1 = k_2 + mn$. But $a^{k_1} = a^{k_2+mn} = a^{k_2} a^{mn} = a^{k_2} \left(a^n\right)^m = a^{k_2} 1^m = a^{k_2}$. So f is one-to-one.

   (c) Since $|G| = n = |\mathbb{Z}_n|$ and f is one-to-one, we must have that f is onto.

   So we have f is an isomorphism, and that every cyclic group of order n is isomorphic to $\mathbb{Z}_n$. ■

REMARK: To reiterate, this theorem above shows that *all cyclic groups of order n are unique up to isomorphism*. Now, recall Corollary 8.2.1, which stated that if $|G| = p$, a prime number, then G must be a cyclic group. But we now have that all cyclic groups are isomorphic to $\mathbb{Z}_n$—so if the size of a group is p, then we can immediately conclude that it is isomorphic to $\mathbb{Z}_p$ (since the group is cyclic).

REMARK: When we study different structures (such as fields, rings, vectors spaces, etc.), we shall formulate corresponding notions of isomorphisms between respective structures. One of the central problems in mathematics is to determine what properties of a structure specify its isomorphism type (i.e., to prove that if G is an object with some structure, such as a group, and G has property $\mathcal{P}$, then any other similarly-structured object, or group, X with property $\mathcal{P}$ is isomorphic to G). Theorems of this type are referred to as *classification theorems*.

For example, we have that *any non-Abelian group of order 6 is isomorphic to* S_3. Using this, we immediately get $D_3 \cong S_3$ and $GL_2(\mathbb{F}_2) \cong S_3$ without having to find explicit mappings between the groups. Note that it is not true hat any group of order six is isomorphic to S_3. In fact, as we have seen the previous example above, up to isomorphism (i.e., which isomorphism we choose), there are only *two groups of order six*, S_3 and $\mathbb{Z}_6$. In other words, *any* group of order six is isomorphic to one of these two groups, with S_3 not isomorphic to $\mathbb{Z}_6$.

We end this section with a couple of more examples.

Example 6.2.4 D_4 and $\mathbb{Z}_8$ are not isomorphic because D_4 is non-Abelian and $\mathbb{Z}_8$ is Abelian. Remember that if $G \cong K$, then G is Abelian if and only if K is Abelian.

Example 6.2.5 $U(10) = \mathbb{Z}_{10}^* = \{[1], [3], [7], [9]\}$ and $U(12) = \mathbb{Z}_{12}^* = \{[1], [5], [7], [11]\}$ are not isomorphic because $U(10)$ is cyclic while $U(12)$ is not (verify this!).

Example 6.2.6 $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{Q}^*, \times)$ under multiplication. For suppose there is an isomorphism $f : \mathbb{Q} \to \mathbb{Q}^*$. Since f is onto, there exists some $a \in \mathbb{Q}$ such that

$f(a) = 2$. Consider the rational number $r = f\left(\frac{a}{2}\right)$. We have $r^2 = f\left(\frac{a}{2}\right) f\left(\frac{a}{2}\right) = f\left(\frac{a}{2} + \frac{a}{2}\right) = f(a) = 2$, which is impossible since no rational number solves $r^2 = 2$.

Example 6.2.7 Recall that $D_n = \left\{r, s \,|\, r^n = s^2 = 1, sr = r^{-1}s\right\}$. Suppose K is a group containing elements a and b with $a^n = 1$, $b^2 = 1$ and $ba = a^{-1}b$. Then there is a homomorphism from D_n to K mapping r to a and s to b. For instance, let k be an integer dividing n with $k \geq 3$ and let $D_k = \left\{r_1, s_1 \,|\, r_1^k = s_1^2 = 1, s_1 r_1 = r_1^{-1} s_1\right\}$. Define

$$f : D_n \to D_k \quad \text{by} \quad f(r) = r_1 \quad \text{and} \quad f(s) = s_1.$$

If we write $n = km$ (since k divides n), then since $r_1^k = 1$ $r_1^n = \left(r_1^k\right)^m = 1^m = 1$. Thus, the three relations satisfied by r, s in D_n are satisfied by r_1, s_1 in D_k. Thus, f extends (uniquely) to a homomorphism from D_n to D_k. Since r_1, s_1 generates D_k, f is onto. This homomorphism is not an isomorphism if $k < n$.

Example 6.2.8 Following up on the previous example, let $G = D_3$ as presented above. Check that in $K = S_3$, the elements $a = (1\,2\,3)$ and $b = (1\,2)$ satisfy the relations $a^3 = 1$, $b^2 = 1$ and $ba = ab^{-1}$. Thus, there is a homomorphism from D_3 to S_3 that sends r to a and s to b. One may further check that S_3 is generated by a and b, so this homomorphism is onto. Since D_3 and S_3 both have order six, we have that the homomorphism is one-to-one, so that the homomorphism is an isomorphism, i.e., $D_3 \cong S_3$.

REMARK: Note that the element a in the two examples above need not have *order* n, i.e., n need not be the *smallest* power of a giving the identity in K, and similarly b need to have order two (for example, b could well be the identity if $a = a^{-1}$). This allows us to more easily construct homomorphisms and is in keeping with the idea that the generators and relations for a group G constitute a complete set of data for the group structure of G.

Any group of order four is isomorphic to either $\mathbb{Z}_4$ or to the Klein 4-Group.

Any group of order six is isomorphic to either $\mathbb{Z}_6$ or to the group S_3.

6.3 The Direct Product

In this section we introuce the notion of a *product* of two groups G and K.

Definition 6.3.1 Direct Product of Groups

We distinguish between the direct product of a finite number of a groups and an infinite number of groups.

- The direct product of n groups $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$, denoted $G_1 \times G_2 \times \ldots \times G_n$, is the set of n-tuples $(g_1, g_2, \ldots, g_n)$ where $g_i \in G_i$ with the operation $*$ on two elements of the product, $(g_1, g_2, \ldots, g_n)$ and $(h_1, h_2, \ldots, h_n)$, defined component-wise:

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n).$$

- The direct product of an *infinite* number of groups $(G_1, *_1), (G_2, *_2), \ldots$, denoted $G_1 \times G_2 \times \ldots$ is the set of sequences $(g_1, g_2, \ldots)$ where $g_i \in G_i$ with the operation $*$ between two elements of the proudct, $(g_1, g_2, \ldots)$ and $(h_1, h_2, \ldots)$, defined component-wise:

$$(g_1, g_2, \ldots) * (h_1, h_2 \ldots) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots).$$

Although the operations may be different in each of the factors of a direct product, like with homomorphisms, we shall omit the operation symbol, so that we have simply

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, g_n) = (g_1 h_1, g_2 h_2, \ldots, g_n h_n).$$

Theorem 6.3.1

If $G_1, G_2, \ldots, G_n$ are groups, their direct proudct $G_1 \times G_2 \times \ldots \times G_n$ is a group of order $|G_1 \times G_2 \times \ldots \times G_n| = |G_1|\,|G_2| \cdots |G_n|$. If any G_i is infinite, then so is the direct product.

PROOF: Let G denote the direct product. We must show that G satisfies the group axioms. This is straightforward since each axiom is a consequence of the fact that the same axiom holds in each factor G_i and the operation on G is defined component-wise. For example, the associative law is verfied as follows. Let $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n), (c_1, c_2, \ldots, c_n) \in G$. Then,

$$\begin{aligned}
&(a_1, a_2, \ldots, a_n)\,[(b_1, b_2, \ldots, b_n)(c_1, c_2, \ldots, c_n)] \\
&= (a_1, a_2, \ldots, a_n)(b_1 c_1, b_2 c_2, \ldots, b_n c_n) \\
&= (a_1 (b_1 c_1), a_2 (b_2 c_2), \ldots, a_n (b_n c_n)) \\
&= ((a_1 b_1) c_1, (a_2 b_2) c_2, \ldots, (a_n b_n) c_n) \\
&= [(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)](c_1, c_2, \ldots, c_n),
\end{aligned}$$

where in the third step we have used the associative law in each component. The remaining axioms are easy to check:

- The identity element in G is the n-tuple $(1_{G_1}, 1_{G_2}, \ldots, 1_{G_n})$.
- The inverse element of an element $(g_1, g_2, \ldots, g_n) \in G$ is $\left(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}\right)$, where each g_i^{-1} is the inverse of g_i in G_i. ■

REMARK: If the factors of the direct product are rearranged, then the resulting direct product is isomorphic to the original one.

We will deal mostly with the direct product of two groups.

Theorem 6.3.2

Let G and K be finite groups. Then there exists a monomorphisms $f_1 : G \to G \times K$ and $f_2 : K \to G \times K$ given by $f(g) = (g, 1_K)$ and $f(k) = (1_G, k)$, respectively.

PROOF: For all $g_1, g_2 \in G$, $f(g_1 g_2) = (g_1 g_2, 1_K)$ and $f(g_1) f(g_2) = (g_1, 1_k)(g_2, 1_K) = (g_1 g_2, 1_K)$ by the definition of the product of elements of the direct product. So $f(g_1) f(g_2) = f(g_1 g_2)$, and so f_1 is a homomorphism. The pf for f_2 is almost exacly the same. ■

Example 6.3.1 Here are some examples of direct product groups.

- Consider the set $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(a, b) \mid a \in \mathbb{Z}_2, b \in \mathbb{Z}_3\}$. So the elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$ are $\{([0]_2, [0]_3), ([0]_2, [1]_3), ([0]_2, [2]_3), ([1]_2, [0]_3), ([1]_2, [1]_3), ([1]_2, [2]_3)\}$. For any two elements $([a]_2, [b]_3), ([c]_2, [d]_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$, we define the product by $([a]_2, [b]_3)([c]_2, [d]_3) = ([a]_2 + [c]_2, [b]_3 + [d]_3) = ([a + c]_2, [b + d]_3)$. Also, $([0]_2, [0]_3)$ is the identity element, and the inverse element of $([a]_2, [b]_3)$ is $([-a]_2, [-b]_3)$.
- Consider the direct product $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = \{(a, b) \mid a, b \in \mathbb{Z}\}$. In this case, the direct product is infinite, and for any $(a, b), (c, d) \in \mathbb{Z}^2$, we let $(a, b) + (c, d) = (a + c, b + d)$. The identity element is $(0, 0)$ and the inverse of $(a, b) \in \mathbb{Z}^2$ is $(-a, -b)$. In the same way can define the group $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ under addition.
- Consider the set $\mathbb{Z}_2 \times S_3 = \{(a, \sigma) \mid a \in \mathbb{Z}_2, \sigma \in S_3\}$. For any (a, σ) and (b, τ) in $\mathbb{Z}_2 \times S_3$, let $(a, \sigma)(b, \tau) = ([a + b]_2, \sigma \circ \tau)$, where $\sigma \circ \tau$ is the composition of permutations. The identity element is $([0]_2, 1)$ and the inverse element of $(a, \sigma) = \left(-a, \sigma^{-1}\right)$.

Theorem 6.3.3

Let G_1 and G_2 be groups. Then $G_1 \times G_2 \cong G_2 \times G_1$.

PROOF: To prove this, we simply go through the four steps of showing two groups are isomorphic.

1. Let $f : G_1 \times G_2 \to G_2 \times G_1$ be defined by $f((a, b)) = (b, a)$. Is it well defined?
2. f is a homomorphism since for any $(a, b), (c, d) \in G_1 \times G_2$, we have $f((a, b)(c, d)) = f((ac, bd)) = (bd, ac) = (b, a)(d, c) = f((a, b)) f((c, d))$.

3. f is one-to-one since $(a,b) \in \text{Kern}(f)$ if and only if $(b,a) = (1_{G_2}, 1_{G_1})$, hence $\text{Kern}(f) = \{(1_{G_1}, 1_{G_2})\}$.

4. Since the size of $G_1 \times G_2$ and $G_2 \times G_1$ are the same and f is one-to-one, f is necessarily onto. ■

REMARK: The above theorem tells us that the order in which we take the direct product does not matter. This is also true when we construct the direct product of more than two groups, as was mentioned in a remark above.

Theorem 6.3.4

Let G_1 and G_2 be groups. Then $G_1 \times G_2$ is Abelian if and only if both G_1 and G_2 are Abelian.

PROOF: Given $(a,b), (c,d) \in G_1 \times G_2$, $(a,b)(c,d) = (ac, bd)$ and $(c,d)(a,b) = (ca, db)$. Thus, $(a,b)(c,d) = (c,d)(a,b)$ for all pairs of elements in $G_1 \times G_2$ if and only if $ac = ca$ for all pairs of elements in G_1 and $bd = db$ for pairs of elements in G_2 since both G_1 and G_2 are Abelian. ■

The next example requires the use of the Chinese Remainder Theorem, so we state it here without pf.

Theorem 6.3.5 Chinese Remainder Theorem

If $m_1, m_2, \ldots, m_k \in \mathbb{Z}$ and $\gcd(m_i, m_j) = 1$ whenever $i \neq j$, then for any choice of integers $a_1, a_2, \ldots, a_k$, there exists a solution to the simultaneous congruences

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \\ &\vdots \\ n &\equiv a_k \pmod{m_k}. \end{aligned}$$

All solutions n of this system are congruent modulo $m_1 m_2 \cdots m_k$. Moreover, if $n = n_0$ is one integer solution, then the complete solution is $n \equiv n_0 \pmod{m_1 m_2 \cdots m_k}$.

Example 6.3.2 Show that $\mathbb{Z}_{20}$ is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_5$.

SOLUTION: Let us define a mapping $f : \mathbb{Z}_{20} \to \mathbb{Z}_4 \times \mathbb{Z}_5$ by

$$f([a]_{20}) = ([a]_4, [a]_5).$$

Let us now go through our usual process.

1. We have just defined the mapping. We now show that it is well defined, i.e., we need to show that for all $a, b \in \mathbb{Z}$ such that $[a]_{20} = [b]_{20}$, $f([a]_{20}) = f([b]_{20})$. Now,

$$\begin{aligned}[a]_{20} = [b]_{20} &\Leftrightarrow \exists k \in \mathbb{Z} a = b + 20k \Leftrightarrow 20k = a - b \\ &\Rightarrow 4 \mid (a-b) \text{ and } 5 \mid (a-b) \Leftrightarrow [a]_4 = [b]_4 \text{ and } [a]_5 = [b]_5 \\ &\Rightarrow f([a]_{20}) = ([a]_4, [a]_5) = ([b]_4, [b]_5) = f([b]_{20}).\end{aligned}$$

   The third step above (second line) follows because 4 and 5 are both divisors of 20 (i.e., we used the fact that if $(ab) \mid c$ then $a \mid c$ and $b \mid c$). So the mapping is well defined.

2. We now show that f is a homomorphism. For all $a, b \in \mathbb{Z}$,

$$\begin{aligned}f([a]_{20} + [b]_{20}) &= f([a+b]_{20}) = ([a+b]_4, [a+b]_5) = ([a]_4 + [b]_4, [a]_5 + [b]_5) \\ &= ([a]_4, [a]_5) + ([b]_4, [b]_5) = f([a]_{20}) + f([b]_{20}).\end{aligned}$$

   So f is a homomorphism. We then show that f is a bijection. Note that since $|\mathbb{Z}_{20}| = |\mathbb{Z}_4 \times \mathbb{Z}_5|$, we need only show one of one-to-one and onto.

3. Let us show that the homomorphism f is one-to-one. We have that for all $a, b \in \mathbb{Z}$,

$$\begin{aligned}f([a]_{20}) = f([b]_{20}) &\Leftrightarrow ([a]_4, [a]_5) = ([b]_4, [b]_5) \\ &\Leftrightarrow a \equiv b \pmod 4 \text{ and } a \equiv b \pmod 5 \\ &\Leftrightarrow a \equiv b \pmod{20} \quad \text{(Chinese Remainder Theorem, since } \gcd(4,5) = 1) \\ &\Leftrightarrow [a]_{20} = [b]_{20}.\end{aligned}$$

4. As mentioned, f is necessarily onto since f maps sets of the same size and is one-to-one.

So f is an isomorphism, and hence $\mathbb{Z}_{20} \cong \mathbb{Z}_4 \times \mathbb{Z}_5$.

In general,

$$\boxed{\text{if } n = m_1 m_2 \cdots m_k \text{ and } \gcd(m_i, m_j) = 1,\ i \neq j, \text{ then } \mathbb{Z}_n \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}.} \quad (6.1)$$

6.4 Normal Subgroups

Definition 6.4.1 Conjugate Group Element

Let G be a group and $H \leq G$, with $a \in G$ and $h \in H$. The element aha^{-1} of G is called the **conjugate** of h by a. The set $aHa^{-1} = \left\{aha^{-1} \mid h \in H\right\}$ is called the **conjugate** of H by a.

REMARK: We will show later that conjugatiion is an equivalence relation, so that we may partition a group into disjoint sets of elements that are conjugates of one another. The equivalence classes will be called *conjugacy classes*.

Theorem 6.4.1

Let H be a subgroup of a group G. Then for any $a \in G$:

1. aHa^{-1} is a subgroup of G.
2. $\left|aHa^{-1}\right| = |H|$.

PROOF: We prove each in turn.

1. Let $x, y \in aHa^{-1}$. Then, $x = ah_1a^{-1}$ and $y = ah_2a^{-1}$ for some $h_1, h_2 \in H$. Therefore, $xy^{-1} = ah_1a^{-1}\left(ah_2a^{-1}\right)^{-1} = ah_1a^{-1}ah_2^{-1}a^{-1} = ah_1h_2^{-1}a^{-1}$, and since H is a (sub)group, $h = h_1h_2^{-1} \in H$, and so $xy^{-1} = aha^{-1} \in aHa^{-1}$, and so by the subgroup test aHa^{-1} is a subgroup.
2. Do this!! ■

Using this definition, we restate the definition of the normaliser.

Definition 6.4.2 Normaliser

Let G be a group and $H \leq G$. The **normaliser** of H in G, denoted $N_G(H)$, is the set of all $a \in G$ such that the conjugate of H by a is equal to H, i.e., $N_G(H) = \left\{a \in G \,|\, aHa^{-1} = H\right\}$. Such elements a are said to **normalise** H.

Theorem 6.4.2

Let H be a subgroup of a group G. Then the normaliser $N_G(H)$ is a subgroup of G.

PROOF: Do it!! ■

So, if an element $a \in G$ normalises H, we have $aHa^{-1} = H$, but multiplying both sides on the right by a gives the equivalent condition that a normalises H if $Ha = aH$, i.e., the left and right cosets of H in G are equal! A subgroup $H \leq G$ with the property that for all $a \in G$ the left and right cosets of H are equal is called a *normal subgroup*.

Definition 6.4.3 Normal Subgroup

Let G be a group and $H \leq G$. If all $a \in G$ normalises H, i.e., if $aHa^{-1} = H \Rightarrow aH = Ha$ (or, for all $a \in G$ and $h \in H$ $aha^{-1} \in H$), i.e., if the left and right cosets of H in G are equal, then H is said to be a **normal** subgroup of G and we write $H \trianglelefteq G$ or $H \lhd G$.

So a normal subgroup is a group that is closed under *conjugation*.

Theorem 6.4.3

Let $f : G \to J$ be a homomorphism, and let $K = \text{Kern}(f)$. Then $K \trianglelefteq G$, i.e., K is a normal subgroup of G.

PROOF: Let $x \in aK$, so $x = ak_1$ for some $k_1 \in K$. Then, $f(x) = f(ak_1) = f(a) f(k_1) = f(a) 1_J = f(a)$. It follows that $1_J = f(x) f(a)^{-1} = f\left(xa^{-1}\right)$ and $xa^{-1} \in K$. Letting $k_2 = xa^{-1} \in K$, we have that $x = k_2 a \in Ka$. Thus, $aK \subseteq Ka$. The pf that $aK \subseteq Ka$ is similar (do it!!).

Alternate pf: We have already shown that K is a subgroup of G. We must now show that for any $a \in G$ and $k \in K$ $a^{-1}ka \in K$, i.e., that K is closed under conjugation. Now, $f\left(a^{-1}ka\right) = f\left(a^{-1}\right) f(k) f(a) = (f(a))^{-1} 1_J f(a) = 1_J$. Therefore, $a^{-1}ka \in K$, and hence $K \trianglelefteq G$. ■

Corollary 6.4.1

A subgroup H of the group G is normal if and only if it is the kernel of some homomorphism.

PROOF: Think about this! ■

Theorem 6.4.4

Here are some basic facts about normal subgroups of a group G. These are quite trivial.

1. The identity subgroup $\{1_G\} \trianglelefteq G$ for any group G (finite or infinite).
2. $G \trianglelefteq G$.

So all groups have at least two normal subgroups!

Example 6.4.1 Consider the mapping $f : S_3 \to \mathbb{Z}_2$, where

$$f(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is an even permutation} \\ 1 & \text{if } \sigma \text{ is an odd permutation} \end{cases}.$$

Then, $\text{Kern}(f) = A_3 = \{1, b, b^2\}$. The left cosets of A_3 are

$$A_3 = \{1, b, b^2\} \quad \text{and} \quad aA_3 = \{a, ab, ab^2\},$$

and the right cosets of A_3 are

$$A_3 = \{1, b, b^2\} \quad \text{and} \quad A_3a = \{a, ba, b^2a\} = \{a, ab^2, bab^2\} = \{a, ab^2, ab^4\} = \{a, ab, ab^2\} = aA_3,$$

so the left and right cosets are equal. Therefore, A_3 is a normal subgroup of S_3, i.e., $A_3 \trianglelefteq S_3$.

Example 6.4.2 Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group. Let $f : Q_8 \to \mathbb{Z}_2$ be defined by

$$f(\pm 1) = f(\pm i) = 0 \quad \text{and} \quad f(\pm j) = f(\pm k) = 1.$$

Then f is a homomorphism with $\text{Kern}(f) = \{\pm 1, \pm i\}$. The left cosets of $K = \text{Kern}(f)$ are

$$K = \{1, -1, i, -i\} \quad \text{and} \quad jK = \{j, -j, ji = -k, j(-i) = k\},$$

and the right cosets of K are

$$K = \{1, -1, i, -i\} \quad \text{and} \quad Kj = \{j, -j, ij = k, -ij = -k\} = jK,$$

so again the left and right cosets are equal. Hence $K \trianglelefteq Q_8$, verifying the above theorem.

Example 6.4.3 Consider the group $S_3 = \{1, b, b^2, a, ab, ab^2\}$ and the subgroup $H = \langle b \rangle = \{1, b, b^2\}$. Consider the element $g = ab^2$. Then, the left and right cosets of H in S_3 are:

$$gH = \{ab^2, ab^2b, ab^2b^2\} = \{ab^2, a, ab\} \quad \text{and}$$
$$Hg = \{ab^2, bab^2, b^2ab^2\} = \{ab^2, ab, a\} = gH$$

So we have $Hg = gH$, i.e., g normalises H. We may check all other elements of S_3 to see that they all normalise H, which means that $H = \langle b \rangle = \{1, b, b^2\}$ is a normal subgroup of S_3.

Theorem 6.4.5

If G is an Abelian group, then every subgroup of G is a normal subgroup of G.

PROOF: Complete this!! ■

Now, because $\mathbb{Z}$ under addition is an Abelian group and all subgroups of $\mathbb{Z}$ are $n\mathbb{Z}$ (which are

cyclic), we have the following result:

$n\mathbb{Z} \trianglelefteq \mathbb{Z}$ i.e., every subgroup of $\mathbb{Z}$ is normal.

$\mathbb{Z}_n$ under addition modulo n is also an Abelian group. So we also have

Every subgroup of $\mathbb{Z}_n$ is normal.

Theorem 6.4.6

Let G be a group and H a subgroup of G with index $[G : H] = 2$. Then H is a normal subgroup of G.

PROOF: Since $[G : H] = 2$, H has just two left cosets and just two right cosets. Since $H = 1H = H1$ is itself both a left and right coset, for any $g \in G$ with $g \notin H$, the two distinct left cosets are H and gH and the two distinct right cosets are H and Hg. Since the cosets determine a partition of G, as we have seen, we must have $gH = \{k \in G \mid k \notin H\} = Hg$, and hence $H \trianglelefteq G$. ■

Example 6.4.4 The subgroup $H = \langle \gamma \rangle$ in the dihedral group D_4 generated by the rotation γ has order four and hence has index $[D_4 : H] = 2$, so $H \trianglelefteq D_4$.

Example 6.4.5 Let $G = GL_2(\mathbb{R})$ and $H = SL_2(\mathbb{R})$ be the general and special linear groups of 2×2 matrices with entries from $\mathbb{R}$. Then $H \trianglelefteq G$ because if $A \in G$ and $B \in H$ we have $\det\left(ABA^{-1}\right) = \det(A)\det(B)\left(\det(A)\right)^{-1} = \det\left(A^{-1}\right)\left(\det(A)\right)^{-1} = 1$, hence $ABA^{-1} \in H$.

Example 6.4.6 $Z(G)$, the center of a group G, is a normal subgroup of G since the elements of $Z(G)$ commute with every element of G.

Theorem 6.4.7

Let H be a subgroup of a group G. If H is the only subgroup of G of order $|H|$, then $H \trianglelefteq G$.

PROOF: Follows from the theorem presented at the beginning of this section. ■

Theorem 6.4.8

Let H be a subgroup of a group G. Then:

1. $H \trianglelefteq N_G(H)$.
2. If K is a subgroup of G and $H \trianglelefteq K$, then K is a subgroup of $N_G(H)$.
3. $H \trianglelefteq G$ if and only if $N_G(H) = G$.

PROOF: Do it!! ■

Theorem 6.4.9 Characterisation of Normal Subgroups

Let H be a subgroup of a group G. Then the following are equivalent:

1. For all $a \in G$ and $h \in H$, $a^{-1}ha \in H$.
2. Every left coset is a right coset, i.e., for all $a \in G$ there exists an $a' \in G$ such that $aH = Ha'$.
3. Every right coset is a left coset, i.e., for all $a \in G$ there exists an $a' \in G$ such that $Ha' = aH$.
4. For all $a \in G$, the left coset aH is equal to the right coset Ha.
5. For any $a, b \in G$, if $ab \in H$, then $ba \in H$.

Theorem 6.4.10

Let G be a group with subgroups N and H such that $N \leq H \leq G$. If $N \trianglelefteq G$, then $N \trianglelefteq H$.

PROOF: Let $N \leq H \leq G$ such that $N \trianglelefteq G$. Since $N \trianglelefteq G$, we have $gng^{-1} \in N$ for all $n \in N$ and all $g \in G$. Now, let $h \in H$. Then, since $H \leq H$, we have $h \in G$, and since $N \trianglelefteq G$, we have $hnh^{-1} \in N$, so that $N \trianglelefteq H$, as required. ■

6.5 The Subset Product and the Internal Direct Products

Definition 6.5.1 Subset Product

Let G be a group and $\{H_k\}_{k=1}^n$ be a set of subsets of G. Then,

$$H_1H_2\cdots H_n = \{h_1h_2\cdots h_n \mid h_1 \in H_1, h_2 \in H_2, \ldots, h_n \in H_n\} \subseteq G$$

is called the **subset product** of G.

It it certainly possible for H and K to be *subgroups* but for HK or KH to not be subgroups. It is also possible that H and K are merely subsets but for HK to be a subgroup.

Example 6.5.1 Find a group G and subgroups H and K such that HK is not a subgroup of G.

SOLUTION: Let $G = S_3$, $H = \langle a \rangle = \{1, a\} \leq G$ and $K \langle ab \rangle = \{1, ab\} \leq G$. Then,

$$HK = \left\{1, ab, a, a^2b\right\} \text{ and } KH = \left\{1, ab, a, b^2\right\}.$$

Now, since $|HK| = |KH| = 4 \nmid 6$, we have that neither HK nor KH are subgroups of G.

Theorem 6.5.1

Let H and K be subgroups of a group G, and assume $H \trianglelefteq G$. Then $HK \leq G$.

REMARK: Technically, it is not necessary for H to be a normal subgroup of G as long as K is a subgroup of the *normaliser* of N.

PROOF: Let $x, y \in HK$, so $x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then, $xy^{-1} = h_1k_1 (h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1kh_2^{-1}$, where $k = k_1k_2^{-1} \in K$ since K is a (sub)group. We have $kh_2 \in kH$, and since $H \trianglelefteq G$, $kH = Hk$, and so $kh_2^{-1} \in Hk$. So $kh_2^{-1} = h_3k$ for some $h_3 \in H$, and $xy^{-1} = h_1kh_2^{-1} = h_1h_3k = hk$, where $h = h_1h_3 \in H$. Thus, $xy^{-1} \in HK$, and so HK is a subgroup by the subgroup test. ■

Theorem 6.5.2

Let G be an Abelian group and $H, K \leq G$. Then $HK \leq G$.

Theorem 6.5.3

Let G be a finite group and $H, K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.

PROOF: ($\Rightarrow$): Assume that HK is a subgroup of G and let $x \in HK$ be arbitrary. We must show that $HK \subseteq KH$ and $KH \subseteq HK$. Now, $x^{-1} \in HK$, where we may write $x^{-1} = hk$ for some $h \in H$ and $k \in K$. But then $x = \left(x^{-1}\right)^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$, so $HK \subseteq KH$ since x is arbitrary. Similarly, we may show that if $y \in KH$, then $y \in HK$, establishing that $KH \subseteq HK$. Therefore, $HK = KH$.

($\Leftarrow$): Assume that $HK = KH$. We want to show that HK is a subgroup of G.

1. Since H and K are subgroups, we have $1_G \in H$ and $1_G \in K$, so $1_G \in HK$.
2. Let $x, y \in HK$, so that $x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2, \in K$. Hence, since $HK = KH$, we have $k_1h_2 = h_2'k_1'$ for some $k_1' \in K$ and $h_2' \in H$. Therefore, $xy = h_1k_1h_2k_2 = h_1h_2'k_1'k_2$. But then $h_1h_2' = h_3 \in H$ and $k_1'k_2 = k_3 \in K$. So $xy = h_3k_3$, i.e., $xy \in HK$.

3. For all $x \in HK$, we have $x = hk$ for some $h \in H$ and $k \in K$. Then $x^{-1} = k^{-1}h^{-1}$; but again, since $HK = KH$, we have $k^{-1}h^{-1} = h'k'$ for some other $h' \in H$ and $k' \in K$. Therefore, $x^{-1} = h'k'$, i.e., $x^{-1} \in HK$.

So, by the subgroup test, we have established that $HK \leq G$, and so the pf is complete. ■

Theorem 6.5.4

If H and K are (normal) subgroups of G, then so is $H \cap K$.

PROOF: Assume $H, K \leq G$.

1. Then $1_G \in H$ and $1_G \in K$, so $1_G \in H \cap K$, so $H \cap K$ is not empty.
2. Let $g_1, g_2 \in H \cap K$, i.e., $g_1, g_2 \in H$ and $g_1, g_2 \in K$. Since H and K are subgroups, we have $g_1 g_2 \in H$ and $g_1 g_2 \in K$. Therefore, $g_1 g_2 \in H \cap K$.
3. Finally, for all $g \in H \cap K$, since H and K are subgroups, we have $g^{-1} \in H$ and $g^{-1} \in K$, so $g^{-1} \in H \cap K$.

So by the subgroup test, we have $H \cap K \leq G$.

Now, assume that $H, K \trianglelefteq G$, and let $g \in H \cap K$. For all $f \in G$, we have $fgf^{-1} \in H$ since H is normal, and $fgf^{-1} \in K$ since K is normal. So $fgf^{-1} \in H \cap K$ for all $f \in G$ and all $g \in H \cap K$. So $H \cap K \trianglelefteq G$. ■

Theorem 6.5.5

Suppose G is a finite group and $H, K \leq G$. Then

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

PROOF: Observe first that in HK, it is possible to have $h_1k_1 = h_2k_2$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Also, recall that

$$H \times K = \{(h, k) \mid h \in H, k \in K\}.$$

Now, define an equivalence relation on $H \times K$ by $(h_1, k_1) \sim (h_2, k_2) \Leftrightarrow h_1k_1 = h_2k_2$ (it is easy to show that this is in fact an equivalence relation). So "$\sim$" partitions $H \times K$ into disjoint subsets, which are the equivalence classes. Since every element in HK is of the form hk for $h \in H$ and $k \in K$, we have that the number of equivalence classes of the equivalence relation "$\sim$" is $|HK|$.

Now, let C be one of these equivalence classes. So we have that for all $(h_1, k_1), (h_2, k_2) \in C$ $(h_1, k_1) \sim (h_2, k_2) \Rightarrow h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} = l$, where $l \in H$ and $l \in K$ (since l has been written as both a product of elements in H and as a product of elements in K). In other

words, $l \in H \cap K$. Now, given any $l \in H \cap K$, for any $(h_1, k_2) \in C$, we have $\left(h_1 l^{-1}, l k_1\right) \in C$. Thus, there is a one-to-one correspondence between every element in C and every element in $H \cap K$.

Using this, let us define the mappings

$$f : H \cap K \to C \text{ by } f(l) = \left(h_1 l^{-1}, l k_1\right)$$
$$g : C \to H \cap K \text{ by } g(h_2, k_2) = h_2^{-1} h_1 = k_2 k_1^{-1}$$

Using this, we see that f is an invertible function (and so is g), which means that f (and g) must be bijections, so that $|C| = |H \cap K|$, i.e., the size of each equivalence class is $|H \cap K|$.

Finally, then, since there are $|HK|$ equivalence classes, each of size $|H \cap K|$, and since the equivalence relation partitions the subset $H \times K$, we have

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

as required. ■

Lemma 6.5.1 Let H and K be finite subgroups of a group G. Then $|HK| = |H|\,s$, where $s = [K : H \cap K]$.

Proof: Consider $Hk_1, \ldots, Hk_s$. They are distinct cosets of H because if $Hk_i = Hk_j$, then $k_i k_j^{-1} \in H \cap K$, contrary to the choice of $k_1, \ldots, k_s$. Also, every element of HK belongs to one of them, since given any $hk \in HK$, we know that $k \in (H \cap K)\,k_i$ for some $1 \leq i \leq s$, and it follows that $hk \in Hk_i$. Thus, the Hk_i partition HK, and each has $|H|$ elements, ans so $|HK| = |H|\,s$. ■

Theorem 6.5.6

If H and K are finite subgroups of a group G, then $|HK| = \frac{|H||K|}{|H \cap K|}$.

Proof: Let s be the index $[K : H \cap K]$, and let $(H \cap K)\,k_1, \ldots, (H \cap K)\,k_s$ be the s distinct cosets of $H \cap K$ in K. These cosets form a partition of K and every element of K belongs to exactly one of them. Since $s = [K : H \cap K] = \frac{|K|}{|H \cap K|}$ by Lagrange's Theorem, and since by the lemma $|HK| = |H|\,s$, we have

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

as required. ■

We can generalise the above theorem to any number of subgroups. We state the result without pf.

Theorem 6.5.7

Let G be a finite group with $\{H_k\}_{i=1}^n$ a sequence of subgroups of G. Then

$$|H_1 H_2 \cdots H_n| = ?$$

Definition 6.5.2 Internal and External Direct Product

The direct product that was introduced in section 3.3 is sometimes called the **external direct product** in order to distinguish it from the internal direct product. An **internal direct product** is a direct product of two normal subgroups H and K of some group G such that $HK \leq G$ and $H \cap K = \{1_G\}$.

Theorem 6.5.8 Characterisation of the Internal Direct Product

Let G, be a group and $H, K \leq G$. Then $G \cong H \times K$ if and only if there exist normal subgroups H^* and K^* of G such that

1. $H \cong H^*$ and $K \cong K^*$;
2. $H^* \cap K^* = \{1_G\}$;
3. $H^* K^* = G$.

PROOF: ($\Leftarrow$): Assume that the three conditions above are satisfied. Without loss of generality, we may take H and K as normal subgroups of G, i.e., $H^* = H$ and $K^* = K$. Define a mapping

$$f : H \times K \to G \text{ by } f(h,k) = hk.$$

Then, for all $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$f((h_1,k_1)(h_2,k_2)) = f(h_1h_2, k_1k_2) = h_1h_2k_1k_2.$$

But by the lemma above, $hk = kh$, so we get

$$f((h_1,k_1)(h_2,k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = f(h_1,k_1)\, f(h_2,k_2),$$

so f is a homomorphism. Additionally, since $\text{Im}(f) = HK = G$, we have that f is onto. Finally,

$$\begin{aligned}
\text{Kern}(f) &= \{(h,k) \in H \times K \mid f(h,k) = 1_G\} \\
&= \{(h,k) \in H \times K \mid hk = 1_G\} \\
&= \left\{(h,k) \in H \times K \mid h = k^{-1} = l\right\} \\
&= \{(h,k) \in H \times K \mid l \in H, l \in K\} \\
&= \{(h,k) \in H \times K \mid l \in H \cap K = \{1_G\}\} \\
&= \{(h,k) \in H \times K \mid l = 1_G \Rightarrow h = k = 1_G\} \\
&= \{(1_G, 1_G)\} \\
&= 1_{H \times K}.
\end{aligned}$$

So f is one-to-one, and therefore f is an isomorphism.

($\Rightarrow$): Assume that $G \cong H \times K$, where H and K are some groups. Let

$$H^* = H \times \{1_K\} \text{ and } K^* = \{1_H\} \times K.$$

Now, consider the mapping defined in the first part of the pf above. By the first lemma above, we have that every element of H commutes with every element of K (note that this follows only because f is a homomorphism and does not assume that H and K are normal subgroups as the second lemma above does). Additionally, since we proved that f is onto, we may write any element in $a \in G$ in the form $a = hk$, where $h \in H$ and $k \in K$. Therefore, for all $a \in G$ and all $\tilde{h} \in H$

$$\begin{aligned} a\tilde{h}a^{-1} &= (hk)\,\tilde{h}\,(hk)^{-1} \\ &= hk\tilde{h}k^{-1}h^{-1} \\ &= h\tilde{h}kk^{-1}h^{-1} \quad \text{since } k \text{ commutes with } \tilde{h} \\ &= h\tilde{h}h^{-1} \in H. \end{aligned}$$

So $H \trianglelefteq G$. Similarly, for all $a \in G$ and all $\tilde{k} \in K$,

$$\begin{aligned} a\tilde{k}a^{-1} &= (hk)\,\tilde{k}\,(hk)^{-1} \\ &= hk\tilde{k}k^{-1}h^{-1} \\ &= hk'h^{-1} \quad \text{since } k' = k\tilde{k}k^{-1} \in K \\ &= k'hh^{-1} \quad \text{since } k' \text{ commutes with } h \\ &= k' \in K. \end{aligned}$$

Therefore, $K \trianglelefteq G$ as well.

Then, since $\{1_H\} \trianglelefteq H$ and $\{1_K\} \trianglelefteq K$, and all identity elements of any group are isomorphic to each other, we get that $H^* \trianglelefteq G$ and $K^* \trianglelefteq G$.

Now, it is clear that $H^* \cong H$ and $K^* \cong K$, so that the first requirement is satisfied. As well,

$$H^* \cap K^* = \{(1_H, 1_K)\} = \{1_G\}$$

since $G \cong H \times K$. So the second requirement is satisfied. Finally,

$$\begin{aligned} H^*K^* &= \{(h, 1_K)\,(1_H, k) \mid h \in H, k \in K\} \\ &= \{(h, k) \mid h \in H, k \in K\} \\ &= H \times K = G, \end{aligned}$$

again, since $G \cong H \times K$. So the third requirement is satisfied as well, and so the pf is complete. ■

REMARK: Observe that under the conditions of this theorem, we get $|H^*K^*| = |G|$.

The theorem above can be generalised to any number of subgroups. We state this generalisation without pf.

Theorem 6.5.9 Characterisation of the Internal Direct Product–General Case

Let G be a group and $\{H_k\}_{k=1}^n$ a set of subgroups of G. Then $G \cong H_1 \times H_2 \times \cdots \times H_n$ if and only if there exist normal subgroups $\{H_k^*\}_{k=1}^n$ such that

1. $H_k^* \cong H_k$ for all $1 \leq k \leq n$;
2. for all $k \in \{2, \ldots, n\}$ $(H_1 H_2 \cdots H_{k-1}) \cap H_k = \{1_G\}$;
3. $H_1 H_2 \cdots H_n = G$.

REMARK: Observe that under the conditions of this theorem, we immediately get $|H_1 H_2 \cdots H_n| = |G|$.

6.6 Quotient Groups and the First Isomorphism Theorem

Recall that all the subroups of $\mathbb{Z}$ are $n\mathbb{Z}$ for $n \in \mathbb{Z}$, and that all of these subgroups are cyclic. Also recall that the cosets of H in G were nothing but the integers modulo n, which, as we know, forms a group under addition modulo n. We now ask: does the set of (left or right) cosets of any subgroup $H \leq G$ always form a group? The answer to this question will lead to the important notion of a *quotient group*.

Now, in the preceding section we showed that if K is the kernel $\text{Kern}(f) = \{a \in G \mid f(a) = 1\}$ of a homomorphism $f : G \to K$, then $aK = Ka$ for all $a \in G$, i.e., K was a normal subgroup. In this section, we will also study the images of homomorphisms. We will see that if K is a normal subgroup of a group G, then K is the kernel of some homomorphism f from G to H. We actually show how to construct the group H and the homomorphism f starting from G and K. This construction, which will be called the *quotient group construction*, is very important in understanding the structure of groups.

Definition 6.6.1 Quotient Group

Let H be a normal subgroup of a group G. Then the set of right cosets of H in G,

$$\{Ha\}_{a \in R} = \{Hg \mid g \in G\},$$

where R is the set of representatives, is a group under the operation $(Ha)(Hb) = Hab$ and is called the **quotient group**, or **factor group**, of G by H, denoted G/H and read "G modulo H" or "G mod H".

REMARK: Note that we could also define the quotient group in terms of the set of the left cosets $\{aH\}_{a \in R}$ of H in G, in which case the operation becomes $(aH)(bH) = abH$.

We have not yet actually proved that G/H is indeed a group, nor that the group operation is well defined. We do that now.

Lemma 6.6.1 Let H be a subgroup of a group G. Then $H \trianglelefteq H$ if and only if $(Ha)(Hb) = Hab$ is a well-defined operation on the right cosets of H.

PROOF: ($\Rightarrow$) Assume $H \trianglelefteq G$. To show that the product $(Ha)(Hb) = Hab$ is well defined, we need to show that if Ha_1 and Ha_2 are the same coset and if Hb_1 and Hb_2 are the same coset, then Ha_1b_1 and Ha_2b_2 are the same coset, i.e., that $(a_2b_2)(a_1b_1)^{-1} \in H$. In other words, we need to know that the result of the operation does not depend on which element a_1 or a_2 we choose to represent the first coset, or on which element b_1 or b_2 we choose to represent the second coset.

Now, then, assume

$$\left.\begin{array}{l} Ha_1 = Ha_2 \Rightarrow a_1 \equiv_H a_2 \Rightarrow a_2a_1^{-1} = h \in H \\ Hb_1 = Hb_2 \Rightarrow b_1 \equiv_H b_2 \Rightarrow b_2b_1^{-1} = h' \in H \end{array}\right\} \quad \text{for some } h, h' \in H.$$

Then, $a_2 = ha_1$ and $b_2 = h'b_1$. Therefore,

$$(a_2b_2)(a_1b_1)^{-1} = a_2b_2b_1^{-1}a_1^{-1} = (ha_1)\left(h'b_1\right)b_1^{-1}a_1^{-1} = ha_1h'a_1^{-1}.$$

But $a_1h'a_1^{-1} \in H$ since H is a normal subgroup of G. And since $h \in H$, we have that $ha_1h'a_1^{-1} \in H$ since H is closed under multiplication (being a (sub)group). So the product is well defined.

($\Leftarrow$). Now assume that the operation is well defined and let $a \in G$ and $h \in H$. Since $Ha = Hah$ and the operation is well defined, we must have $H\left(aha^{-1}\right) = H(ah)Ha^{-1} = HaHa^{-1} = H\left(aa^{-1}\right) = H1 = H$. Therefore, $aha^{-1} \in H$ for all $a \in G$ and $h \in H$, and so by definition H is a normal subgroup. ■

Theorem 6.6.1

Let H be a normal subgroup of G. Then the set of right (or left) cosets of H in G, G/H, forms a group under the operation $(Ha)(Hb) = Hab$.

PROOF: We have just shown that the operation is well defined. We then proceed to show that the four group axioms are satisfied.

1. For all $a, b \in G$, $(Ha)(Hb) = Hab \in G/H$ since Hab is a coset of H in G. So we have closure.
2. For all $a, b \in G$, $Ha * (Hb * Hc) = Ha * Hbc = Ha(bc) = H(ab)c = (Ha * Hb) * Hc$. So the operation is associative.
3. For all $a \in G$, $Ha * H = Ha * H1 = Ha = H1 * Ha$. So the identity element in G/H is H. (Remember that H is itself a left *and* right coset of H.)
4. For all $a \in G$, $Ha * Ha^{-1} = Haa^{-1} = H1 = H = Ha^{-1} * Ha$. So the inverse element of an element $Ha \in G/H$ is $(Ha)^{-1} = Ha^{-1}$.

Having shown that all the group axioms are satisfied, we have that G/H is indeed a group. ■

Example 6.6.1 We can now write that $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$. In fact the groups are exactly the same, we we might want to write $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$. As well, $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$.

In general we have

$$\boxed{\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n}. \tag{6.2}$$

To prove this formally, let us make use of Lemma 6.2.2, but first we must show that $\mathbb{Z}/n\mathbb{Z}$ is a cyclic group. Now, the right cosets of $n\mathbb{Z}$, which are the elements of $\mathbb{Z}/n\mathbb{Z}$, can be written generally as

$$\begin{aligned}
&n\mathbb{Z} + 0 = n\mathbb{Z}\\
&n\mathbb{Z} + 1\\
&n\mathbb{Z} + 2\\
&\quad\vdots\\
&n\mathbb{Z} + (n-1)\\
&n\mathbb{Z} + n = \{\ldots, -2n+n, -n+n, 0+n, n+n, 2n+n, 3n+n, \ldots\} = n\mathbb{Z}
\end{aligned}$$

So we see that there are n unique right cosets. Now, observe that

$$\begin{aligned}
(n\mathbb{Z}+1)^0 &= 1_{\mathbb{Z}/n\mathbb{Z}} = n\mathbb{Z}\\
(n\mathbb{Z}+1)^1 &= n\mathbb{Z}+1\\
(n\mathbb{Z}+1)^2 &= (n\mathbb{Z}+1)(n\mathbb{Z}+1) = n\mathbb{Z}+(1+1) = n\mathbb{Z}+2\\
&\vdots\\
(n\mathbb{Z}+1)^{n-1} &= n\mathbb{Z}+(n-1)\\
(n\mathbb{Z}+1)^n &= n\mathbb{Z}+n = n\mathbb{Z},
\end{aligned}$$

so that $\mathbb{Z}/n\mathbb{Z}$ is indeed a cyclic group with generator $n\mathbb{Z}+1$, i.e.,

$$\boxed{\mathbb{Z}/n\mathbb{Z} = \langle n\mathbb{Z}+1\rangle}.$$

And, as we already know $\mathbb{Z}_n = \langle [1]_n \rangle$. Then, according to Lemma 6.2.2, the mapping $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ defined by

$$f(n\mathbb{Z}+1) = [1]_n$$

is an isomorphism. So $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}_n$ are indeed isomorphic.

Example 6.6.2 In $\mathbb{Z}_6$, consider the subgroup $\langle [3] \rangle = \{[0], [3]\}$. How many right cosets are there? Remember that this is equal to the *index* of $\langle [3] \rangle$ in $\mathbb{Z}_6$, $[\mathbb{Z}_6 : \langle [3] \rangle] = \frac{|\mathbb{Z}_6|}{|\langle [3] \rangle|} = \frac{6}{2} = 3$.

Let us confirm this by writing all the cosets and seeing that there are only three unique ones:

$$\begin{aligned}
\langle[3]\rangle[0] &= \langle[3]\rangle + [0] = \{[0],[3]\} \\
\langle[3]\rangle[1] &= \langle[3]\rangle + [1] = \{[1],[4]\} \\
\langle[3]\rangle[2] &= \langle[3]\rangle + [2] = \{[2],[5]\} \\
\langle[3]\rangle[3] &= \langle[3]\rangle + [3] = \{[3],[6]\} = \{[3],[0]\} = \langle[3]\rangle[0] \\
\langle[3]\rangle[4] &= \langle[3]\rangle + [4] = \{[4],[7]\} = \{[4],[1]\} = \langle[3]\rangle[1] \\
\langle[3]\rangle[5] &= \langle[3]\rangle + [5] = \{[5],[8]\} = \{[5],[2]\} = \langle[3]\rangle[5]
\end{aligned}$$

Indeed, there are three cosets. Now, then, the set

$$\mathbb{Z}_6/_{\langle[3]\rangle} = \{\langle[3]\rangle[0], \langle[3]\rangle[1], \langle[3]\rangle[2]\}$$

is a group of order three (the identity element is $\langle[3]\rangle$). Observe that

$$\begin{aligned}
(\langle[3]\rangle[1])^0 &= \langle[3]\rangle \\
(\langle[3]\rangle[1])^1 &= \langle[3]\rangle[1] \\
(\langle[3]\rangle[1])^2 &= (\langle[3]\rangle[1])(\langle[3]\rangle[1]) \\
&= \langle[3]\rangle[1][1] = \langle[3]\rangle[2] \\
(\langle[3]\rangle[1])^3 &= \langle[3]\rangle[3] = \langle[3]\rangle[0] = \langle[3]\rangle \\
(\langle[3]\rangle[1])^4 &= \langle[3]\rangle[4] = \langle[3]\rangle[1],
\end{aligned}$$

so that we may write

$$\mathbb{Z}_6/_{\langle[3]\rangle} = \langle\langle[3]\rangle[1]\rangle,$$

i.e., the quotient group $\mathbb{Z}_6/_{\langle[3]\rangle}$ is a cyclic group of order three generated by $\langle[3]\rangle[1]$. And since, as we know, all finite cyclic groups of order n are isomorphic to $\mathbb{Z}_n$, we have that $\mathbb{Z}_6/_{\langle[3]\rangle} \cong \mathbb{Z}_3$. Find an isomorphism!

Example 6.6.3 In $\mathbb{Z}_{12}$, consider the subgroup $\langle[8]\rangle = \{[0],[4],[8]\}$. The order of the quotient group $\mathbb{Z}_{12}/_{\langle[8]\rangle}$ is the number of right cosets of $\langle[8]\rangle$, or the index of $\langle[8]\rangle$ in $\mathbb{Z}_{12}$, which is $[\mathbb{Z}_{12} : \langle[8]\rangle] = \frac{|\mathbb{Z}_{12}|}{|\langle[8]\rangle|} = \frac{12}{3} = 4$. Now, every group of order four is isomorphic to either $\mathbb{Z}_4$ or to the Klein 4-group. And since every finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$, if $\mathbb{Z}_{12}/_{\langle[8]\rangle}$ is cyclic then it is isomorphic to $\mathbb{Z}_4$. Indeed,

$$\begin{aligned}
(\langle[8]\rangle[1])^0 &= \langle[8]\rangle \quad \text{(the identity)} \\
(\langle[8]\rangle[1])^1 &= \langle[8]\rangle[1] \\
(\langle[8]\rangle[1])^2 &= \langle[8]\rangle[2] \\
(\langle[8]\rangle[1])^3 &= \langle[8]\rangle[3] \\
(\langle[8]\rangle[1])^4 &= \langle[8]\rangle[4] = \langle[8]\rangle \\
(\langle[8]\rangle[1])^5 &= \langle[8]\rangle[5] = \langle[8]\rangle[1],
\end{aligned}$$

so $\mathbb{Z}_{12}/\langle[8]\rangle$ is a cyclic group of order four, so that $\mathbb{Z}_{12}/\langle[8]\rangle \cong \mathbb{Z}_4$.

Example 6.6.4 In the dihedral group D_4, consder the subgroup $\langle b^2\rangle = \{1, b^2\}$. Since $b^2 \in Z(D_4)$, the center of D_4, $\langle b^2\rangle$ is a normal subgroup. The index is $[D_4 : \langle b^2\rangle] = \frac{8}{2} = 4$, so the quotient group $D_4/\langle b^2\rangle$ has order 4. Let us see to which of the two groups of order four, $\mathbb{Z}_4$ or the Klein 4-group, this quotient group is isomorphic. We have $D_4/\langle b^2\rangle = \{\langle b^2\rangle, b\langle b^2\rangle, a\langle b^2\rangle, ab\langle b^2\rangle\}$, and all the non-identity elements have order two. So the group is not cyclic; hence, $D_4/\langle b^2\rangle \cong D_2$.

Theorem 6.6.2

Let H be a normal subgroup of a group G. Then

1. The order of an element Ha in the quotient group G/H is the least positive integer k such that $a^k \in H$.
2. If G is finite, then $|G/H| = \frac{|G|}{|H|}$, i.e., the size of the quotient group is the quotient of the sizes of the group and the subgroup.
3. If G is an Abelian group, the G/H is an Abelian group.
4. If G is a cyclic group, then G/H is a cyclic group.

PROOF:

1. Let $Ha \in G/H$. Since H is the identity element in G/H, $o(Ha)$ is the least positive integer k such that $(Ha)^k = H$. But $(Ha)^k = Ha^k$, so the order is the least positive integer such that $Ha^k = H$. And $Ha^k = H$ if and only if $a^k(1)^{-1} \in H$, i.e., if and only if $a^k \in H$. So the pf is complete.
2. Complete this!
3. Complete this!
4. Complete this! ■

Note that the converses of Parts 3 and 4 of the above theorem are *not* in general true.

Theorem 6.6.3

Let $f : G \to H$ be a homomorphism with $\text{Kern}(f) = K$. Then, for any $g \in G$, we have $f^{-1}(f(g)) = gK$.

PROOF: Since for any $y \in H$ we have $f^{-1}(y) = \{x \in G \mid f(x) = y\}$ by definition, it follows that $x \in f^{-1}(f(g))$ if and only if $f(x) = f(g)$. This condition is equivalent to the condition

that $(f(g))^{-1} f(x) = 1_H$, the identity of H. Since $(f(g))^{-1} f(x) - f\left(g^{-1}x\right)$, it follows that $x \in f^{-1}(f(g))$ if and only if $f\left(g^{-1}x\right) = 1_H$ or, in other words, if and only if $g^{-1}x \in \text{Kern}(f)$. This condition is equivalent to the condition that $x \in gK$. ■

Corollary 6.6.1

Let $f : G \to H$ by a homomorphism. Then $f^{-1}(f(1_G)) = \text{Kern}(f)$.

PROOF: This is immediate from the preceding theorem since $1K = K1 = K = \text{Kern}(f)$. ■

Theorem 6.6.4

Let $f : G \to K$ be a homomorphism. The image $\text{Im}(f) = \{f(x) \mid x \in G\}$, as we know, is always a subset (indeed, a subgroup) of K. It will be equal to K if and only if f is onto.

PROOF: (Show this explicitly! It makes sense because if the homomorphism is onto, then all points in K get mapped to by a point in G, so the set of all $f(x)$ must be equal to K, i.e., the image and K are the same.) ■

Definition 6.6.2 Homomorphic Image

Let $f : G \to K$ be a surjective (onto) homomorphism. Then K is said to be a **homomorphic image** of G.

REMARK: For any isomorphism $f : G \to K$ between two groups, since f is onto by definition, K is always a homomorphic image of G.

The next theorem (a very important one!) shows that there is a correspondence between normal subgroups and homomorphic images of a group.

Theorem 6.6.5 First Isomorphism Theorem

For any two groups G and K, let $f : G \to K$ be a homomorphism. Then,

$$G/\text{Kern}(f) \cong \text{Im}(f).$$

REMARK: Using this theorem, we may restate the definition of homomorphic image as follows: a group K is called a homomorphic image of a group G if there exists an onto homomorphism $f : G \to K$, i.e., if $K \cong G/\text{Kern}(f)$.

PROOF: We follow our four basic steps for proving two groups are isomorphic, constructing a map (and showing that it is well defined), showing that the mapping is a homomorphism, is

one-to-one, and is onto. First, recall that the quotient group $G/\text{Kern}(f)$ is

$$G/\text{Kern}(f) = \{(\text{Kern}(f))\, g \mid g \in G\} = \{g\,(\text{Kern}(f))\}.$$

1. Let us define a mapping $\tilde{f} : G/\text{Kern}(f) \to \text{Im}(f)$ by

$$\tilde{f}\,((\text{Kern}(f))\, g) = f(g),$$

where f is the homomorphism $f : G \to K$. We must show that this definition of $\tilde{f}$ is well defined, i.e., we must show that if $(\text{Kern}(f))\, g_1 = (\text{Kern}(f))\, g_2$ for some $g_1, g_2 \in G$, then $\tilde{f}\,((\text{Kern}(f))\, g_1) = \tilde{f}\,((\text{Kern}(f))\, g_2)$. Now, by definition of equal cosets,

$$(\text{Kern}(f))\, g_1 = (\text{Kern}(f))\, g_2 \Leftrightarrow g_1 g_2^{-1} = k \in \text{Kern}(f) \Rightarrow g_1 = k g_2.$$

Now, since $k \in \text{Kern}(f)$, we must have $f(k) = 1_K$. Therefore,

$$\begin{aligned}\tilde{f}\,((\text{Kern}(f))\, g_1) &= f(g_1) = f(k g_2)\\ &= f(k)\, f(g_2)\\ &= 1_K f(g_2)\\ &= f(g_2)\\ &= \tilde{f}\,((\text{Kern}(f))\, g_2).\end{aligned}$$

So $\tilde{f}$ is well defined.

2. We now show that $\tilde{f}$ is a homomorphism. For all $g_1, g_2 \in G$, we have

$$\begin{aligned}\tilde{f}\,((\text{Kern}(f))\, g_1\, (\text{Kern}(f))\, g_2) &= \tilde{f}\,((\text{Kern}(f))\, g_1 g_2)\\ &= f(g_1 g_2)\\ &= f(g_1)\, f(g_2)\\ &= \tilde{f}\,((\text{Kern}(f))\, g_1)\, \tilde{f}\,((\text{Kern}(f))\, g_2).\end{aligned}$$

So $\tilde{f}$ is a homomorphism.

3. We now show that $\tilde{f}$ is onto. Let $k \in \text{Im}(f)$, i.e., there exists a $g \in G$ such that $k = f(g)$. We must find an element in $G/\text{Kern}(f)$ that maps to k. We have

$$\tilde{f}\,((\text{Kern}(f))\, g) = f(g) = k,$$

which means that $\tilde{f}$ is onto.

4. Finally, we show that $\tilde{f}$ is one-to-one. Recall that to show a homomorphism it suffices to show that its kernel is trivial, i.e., we must show that $\text{Kern}\left(\tilde{f}\right) = \left\{1_{G/\text{Kern}(f)}\right\}$. Now,

$$\begin{aligned}\text{Kern}\left(\tilde{f}\right) &= \left\{(\text{Kern}(f))\, g \mid \tilde{f}\,((\text{Kern}(f))\, g) = 1_{\text{Im}(f)}\right\}\\ &= \{(\text{Kern}(f))\, g \mid f(g) = 1_K\} \quad (\text{since } 1_K = 1_{\text{Im}(f)})\\ &= \{(\text{Kern}(f))\, g \mid g \in \text{Kern}(f)\}\\ &= \{\text{Kern}(f)\}\\ &= \left\{1_{G/\text{Kern}(f)}\right\},\end{aligned}$$

(The last step follows from the fact that if H is a subgroup and $a \in H$, then $Ha = H$.) so that the kernel of $\tilde{f}$ is indeed the identity of $G/\text{Kern}(f)$. So $\tilde{f}$ is one-to-one.

Therefore, $\tilde{f}$ is an isomorphism, and the pf is complete. ■

Example 6.6.5 In $\mathbb{Z}$ consider the subgroup $5\mathbb{Z}$ and the set whose elements are the cosets of $5\mathbb{Z}$ in $\mathbb{Z}$, namely, $\mathbb{Z}/5\mathbb{Z}$. Since $m + 5\mathbb{Z} = n + 5\mathbb{Z}$ if and only if $m \equiv n \bmod 5$, we have

$$\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z} + 0 = 5\mathbb{Z}, 5\mathbb{Z} + 1, 5\mathbb{Z} + 2, 5\mathbb{Z} + 3, 5\mathbb{Z} + 4\}.$$

By using addition modulo 5 on this set, we have that $\mathbb{Z}/5\mathbb{Z}$ is a group that is isomorphic to $\mathbb{Z}_5$. We can define the isomorphism $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}_5$ by $f(5\mathbb{Z} + 1) = [1]_5$ using Lemma 6.2.2, which is enough to define the isomorphism on all other elements in each group. Let us explicitly write the isomorphism anyway:

$$f = \begin{pmatrix} 5\mathbb{Z} + 0 & 5\mathbb{Z}_1 & 5\mathbb{Z} + 2 & 5\mathbb{Z} + 3 & 5\mathbb{Z} + 4 \\ [0]_5 & [1]_5 & [2]_5 & [3]_5 & [4]_5 \end{pmatrix}$$

Now, let $f : \mathbb{Z} \to \mathbb{Z}_5$ be the homomorphism with

$$f(m) = (n\mathbb{Z})\, m = n\mathbb{Z} + m.$$

What is the kernel of this homomorphism? First, note that that the identity element in $\mathbb{Z}_5$ is $[0]_5$. Therefore, what we are looking for is the set of all integers $K = \text{Kern}(f)$ such that $f(K) = [0]_5$. Since any multiple of five is congruent to zero modulo five, we have that $\text{Kern}(f) = 5\mathbb{Z}$.

Also, what is the image $\text{Im}(f)$ of f? In this case, it is clear that $\text{Im}(f) = \mathbb{Z}_5$. So, using the terms of the first isomorphism theorem, we can let $G = \mathbb{Z}$ and $K = \mathbb{Z}_5$. Then, since $\text{Kern}(f) = 5\mathbb{Z}$, we get

$$G/\text{Kern}(f) = \mathbb{Z}/5\mathbb{Z} \cong \text{Im}(f) = \mathbb{Z}_5, \quad \text{i.e.,} \quad \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}_5,$$

confirming what we had already discovered.

Example 6.6.6 The General and Special Linear Groups

Recall the general linear group, $GL_n(\mathbb{F})$, the set of $n \times n$ matrices with entries from $\mathbb{F}$ and with non-zero determinant. Also recall the special linear group, $SL_n(\mathbb{F})$, the set of $n \times n$ matrices with entries from $\mathbb{F}$ and with determinant equal to unity. The field $\mathbb{F}$ will be one of $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_n$, and the operation on both groups is matrix multiplication. We first prove that

$$\boxed{SL_n(\mathbb{F}) \trianglelefteq GL_n(\mathbb{F})}.$$

To prove this, we must show that for all $A \in GL_n(\mathbb{F})$ and all $B \in SL_n(\mathbb{F})$ $ABA^{-1} \in SL_n(\mathbb{F})$, or $A^{-1}BA \in SL_n(\mathbb{F})$ (both are equivalent). We have

$$\det\left(A^{-1}BA\right) = \det\left(A^{-1}\right)\det(B)\det(A) = \frac{1}{\det(A)} \cdot 1 \cdot \det(A) = 1,$$

so, indeed $A^{-1}BA \in SL_n(\mathbb{F})$, and similarly, we have $ABA^{-1} \in SL_n(\mathbb{F})$. So the special linear group is indeed a normal subgroup in the general linear group. Now, because $SL_n(\mathbb{F})$ is a normal subgroup, we may consider the quotient group ${}^{GL_n(\mathbb{F})}/_{SL_n(\mathbb{F})}$. What does this group look like? To answer this question, we'll use the first isomorphism theorem. Consider the mapping

$$\det : GL_n(\mathbb{F}) \to \mathbb{F}^*,$$

where $\mathbb{F}^* = \mathbb{F} - \{0\}$, analogous to $\mathbb{R}^*$ and $\mathbb{C}^*$ that we saw at the beginning of the course. We use this mapping as our homomorphism f from the statement of the theorem. Indeed, it is a homomorphism since for any two matrices $A, B \in GL_n(\mathbb{F})$, $\det(AB) = \det(A)\det(B)$, as you should have seen from Linear Algebra (and since neither $\det(A)$ nor $\det(B)$ equals zero, we have that $\det(AB)$). What is the kernel of this homomorphism? In any of the four choices of $\mathbb{F}$, the (multiplicative) identity is 1, so

$$\text{Kern}(\det) = \{A \in GL_n(\mathbb{F}) \mid \det(A) = 1\},$$

which is nothing other than $SL_n(\mathbb{F})$! So by the first isomorphism theorem,

$${}^{GL_n(\mathbb{F})}/_{SL_n(\mathbb{F})} \cong \text{Im}(\det),$$

but what is $\text{Im}(\det)$? Let us posit that $\text{Im}(\det) = \mathbb{F}^*$. To show this, it suffices to show, by Theorem 6.6.4, that det is onto. We must show that every number $\lambda \in \mathbb{F}^*$ gets mapped to by some point (i.e., matrix) in $GL_n(\mathbb{F})$. Now, consider the matrix

$$A_\lambda = \begin{bmatrix} \lambda & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

Because A_λ is diagonal, $\det(A_\lambda) = \lambda \neq 0$, and so there exists an element in $GL_n(\mathbb{F})$ such that its determinant is non-zero. Therefore, det is onto, and $\text{Im}(\det) = \mathbb{F}^*$. In conclusion, then,

$$\boxed{{}^{GL_n(\mathbb{F})}/_{SL_n(\mathbb{F})} \cong \mathbb{F}^*}.$$

Theorem 6.6.6

Let G and K be finite groups, and let $f : G \to K$ be a homomorphism. Then $|\text{Im}(f)|$ divides both $|G|$ and $|K|$.

PROOF: We already know that $\text{Im}(f)$ is a subgroup of K, hence $|\text{Im}(f)|$ divides $|K|$ by Lagrange's Theorem. But $|\text{Im}(f)| = |{}^{G}/_{\text{Kern}(f)}|$ by the first isomorphism theorem, i.e.,

$$|\text{Im}(f)| = \frac{|G|}{|\text{Kern}(f)|} \Rightarrow |\text{Kern}(f)| = \frac{|G|}{|\text{Im}(f)|},$$

i.e., $|\text{Im}(f)|$ divides $|G|$ as well. ■

Theorem 6.6.7

Given a group K and a normal subgroup K, there exists an onto homomorphism $f : G \to {}^{G}/_{K}$ with $\text{Kern}\,(f) = K$.

PROOF: We define f by letting $f\,(g) = Kg$ for any $g \in G$. Since $K \trianglelefteq G$, then we know that the set of cosets ${}^{G}/_{K}$ is a group under the operation $(Kg_1)\,(Kg_2) = Kg_1g_2$ for all $g_1, g_2 \in G$. Then f is a homomorphism because $f\,(g_1g_2) = Kg_1g_2 = (Kg_1)\,(Kg_2) = f\,(g_1)\,f\,(g_2)$. In the group ${}^{G}/_{K}$, the identity element is K, as we know. So we have $x \in \text{Kern}\,(f)$ if and only if $f\,(x) = K$, and since $f\,(x) = Kx$, we have $x \in \text{Kern}\,(f)$ if and only if $Kx = K$, which is equivalent to $x \in K$. Thus, $\text{Kern}\,(f) = K$. Finally, f is onto since every element of ${}^{G}/_{K}$ is of the form Kg for some $g \in G$. ■

6.7 The Second and Third Isomorphism Theorems

In this section, we present the second and third isomorphism theorems. Before that, we present the correspondence theorem.

Theorem 6.7.1 Correspondence Theorem

Let G be a group and $N \trianglelefteq G$ be a normal subgroup of G. Then:

1. If K is a subgroup of the quotient group ${}^{G}/_{N}$, then K is of the form ${}^{H}/_{N}$, where H is a subgroup of G such that $N \leq H \leq G$, and $N \subseteq H$. Conversely, if $N \leq H \leq G$ and $N \subseteq H$, then ${}^{H}/_{N} \leq {}^{G}/_{N}$ for some $H \leq G$.
2. The correspondence between subgroups of ${}^{G}/_{N}$ and subgroups of G containing N is a bijection. This bijection maps normal subgroups of ${}^{G}/_{N}$ on to normal subgroups of G that contain N.

REMARK: Let us try to deconstruct the elements of the first part of the above theorem. Remember that the quotient group ${}^{G}/_{N} = \{Ng \,|\, g \in G\}$, where $N \trianglelefteq G$. Now, suppose for the sake of argument that ${}^{G}/_{N} = \{Ng_1, Ng_2, \ldots, Ng_n\}$. As we have seen in examples, $g_1, g_2, \ldots, g_n$ is not necessarily all of the elements of G since generally not all the cosets are unique. In fact $\{g_1, g_2, \ldots, g_n\} = R$, the set of representatives for the cosets such that $R \subseteq G$.

Now, let $K \leq {}^{G}/_{N}$. Then K contains some, but perhaps not all, of the elements of ${}^{G}/_{N}$. So we may write $K = \{Nk \,|\, k \in R = \{g_1, g_2, \ldots, g_n\}\}$. Lets say that $K = \{Ng_1, Ng_2, Ng_{10}, Ng_7\}$. Now, let us define a the set $H = \{g \in G \,|\, Ng \in K\}$. Observe that in general $H \subseteq R$, i.e., H is the set of those representatives that are used in the cosets that make up K. So, using our example, we have $H = \{g_1, g_3, g_{10}, g_7\}$. Now, K is a subgroup, so we must have that, for example, $(Ng_1)\,(Ng_3) = Ng_1g_3 \in K$. For Ng_1g_3 to be in K, we must have $g_1g_3 \in H$. This is the idea that will be used in the pf that H is a subgroup.

PROOF:

1. ($\Rightarrow$) Suppose $K \leq {}^{G}/_{N}$, i.e., K is a subgroup of the quotient group ${}^{G}/_{N}$. Remember that the quotient group ${}^{G}/_{N}$ is the set of all cosets of N in G, i.e., ${}^{G}/_{N} = \{Ng \,|\, g \in G\}$. Therefore, since K is a subgroup of ${}^{G}/_{N}$, the elements of K will be a set of the right cosets

of N in G. Now, define

$$H = \{g \in G \,|\, Ng \in K\}.$$

We first prove that H is a subgroup of G.

(a) Since K is a subgroup of G/N, it must contain the identity of G/N, namely, N. But $N = N1$, so by definition $1 \in H$, i.e., H is not empty.

(b) For all $h_1, h_2 \in H$ $Nh_1Nh_2 = Nh_1h_2$, and since K is a (sub)group, we must have $Nh_1h_2 \in K$, which is possible if and only if $h_1h_2 \in H$. So H is closed under multiplication.

(c) For all $h \in H$, $(Nh)^{-1} = Nh^{-1}$. Now, since K is a (sub)group, every element must have an inverse, i.e., $Nh^{-1} \in K$, which is possible if and only if $h^{-1} \in H$. So every element of H has an inverse in H.

So by the subgroup test $H \leq G$. In particular, then $N \leq H$. Now, define a mapping $f : H \to K$ by $f(h) = Nh$. Now, by definition of H, for any $Nh \in K$, there exists a $h \in H$, so f is onto, and hence $K = \text{Im}(f)$. Now, $\text{Kern}(f) = \{h \in H \,|\, Nh = N\}$. But $Nh = N$ implies that $h \equiv_N 1$, which implies that $h1^{-1} \in N \Rightarrow h \in N$. So $\text{Kern}(f) = \{h \in H \,|\, h \in N\} = H \cap N$. But since $N \leq H$, we must have $N \cap H = N$, so that $\text{Kern}(f) = \{h \in H \,|\, h \in N\} = N$. So the first isomorphism theorem gives

$$H/\text{Kern}(f) = H/N \cong \text{Im}(f) = K,$$

i.e., K is the of the form H/N, as required.

($\Leftarrow$) Suppose $N \leq H \leq G$ and $N \subseteq H$ and consider the quotient group $H/N = \{Nh \,|\, h \in H\}$ (we can consider this subgroup since $N \leq H$—in fact, $N \trianglelefteq H$). We must show that H/N is a group.

(a) Since H is a (sub)group, it must contain the identity element $1_H = 1_G$. Hence, $N1_H = N \in H/N$, so H/N is not empty.

(b) If $Nh_1, Nh_2 \in H/N$, then $Nh_1Nh_2 = Nh_1h_2 \in H/N$ since H is a (sub)group and so is closed under multiplication.

(c) If $Nh \in H/N$, then $(Nh)^{-1} = Nh^{-1}$. Since H is a (sub)group, any element $h \in H$ must contain an inverse h^{-1}, so that $Nh^{-1} \in H/N$.

So by the subgroup test H/N is a subgroup of G/N since $H/N \subseteq G/N$.

2. Not covered in lectures. ■

Before we go to the Second Isomorphism Theorem, it is useful to recall Theorems **??** and 6.5.6. In particular, in Theorem **??**, we showed that if K is a subgroup of a group G and H is a normal subgroup of G, then the group HK is a subgroup of G. We now prove another result here, which ties into Theorem 6.5.6 and the second isomorphism theorem.

Theorem 6.7.2

Let G be a group and H and N subgroups such that $N \trianglelefteq G$. Then $H \cap N$ is a normal subgroup of H.

PROOF: Because $N \trianglelefteq G$, we have that for all $n \in N$ and all $g \in G$ $gng^{-1} \in N$.

1. Because H and N are both (sub)groups of G, they both contain the identity element of G, namely 1_G. Therefore, $1_G \in H \cap N$, and so $H \cap N$ is not empty.
2. For all elements $x \in H \cap N$ and $h \in H$, we must have $hxh^{-1} \in H \cap N$. Indeed, since H is closed under multiplication and $x \in H$ (since x is in the intersection of H and N, it is necessarily in *both* H and N), we have $hxh^{-1} \in H$ for all $h \in H$. Additionally, since $x \in N$ and $N \trianglelefteq G$, certainly $gxg^{-1} \in N$ for all $g \in G$, which means this is true for all $h \in H$. Hence $hxh^{-1} \in H \cap N$ for all $h \in H$, and the pf is complete. ■

Theorem 6.7.3

Let G be a group and H and N subgroups such that $N \trianglelefteq G$. Then $N \trianglelefteq NH = HN \leq G$.

PROOF: Get this!! ■

Theorem 6.7.4 Second Isomorphism Theorem

Let G be a group and H and N subgroups such that $N \trianglelefteq G$. Then,

$$\boxed{{}^{H}\!/_{H \cap N} \cong {}^{HN}\!/_{N}}.$$

REMARK: What does the quotient group ${}^{HN}\!/_{N}$ even look like? First of all, can we even construct such a quotient group? Yes, since the previous theorem says that if H and N are subgroups and $N \trianglelefteq G$, then N is a normal subgroup in NH, which itself is a subgroup of G. Now, then, we have $HN = \{hn \mid h \in H,\, n \in N\}$. We then take this subgroup of G (remember that HN is indeed a subgroup!) and partition it using the equivalence classes mod N, so that

$${}^{HN}\!/_{N} = \{aN \mid a \in HN\}.$$

Additionally, as we know, ${}^{H}\!/_{N} = \{hN \mid h \in H\}$, but *this is only if N is a normal subgroup of H*!. The statement of the theorem only says that N is a normal subgroup of G, which does *not* necessarily imply that N is a normal subgroup of H. Certainly if N was a subset of H, then N would also be a normal subgroup of H—but this is not true in general. So, to which quotient group does the coset Nh, where $h \in H$, belong, to ${}^{H}\!/_{N}$ or ${}^{HN}\!/_{N}$? Let $n = 1_G$. Then $h = h1_G$ and so $h1_GN$ is of the form hnN, hence $hN \in {}^{HN}\!/_{N}$. If N was a subset of N, then hN would belong to both ${}^{HN}\!/_{N}$ and ${}^{H}\!/_{N}$.

PROOF: Let us define a mapping $f : H \to {}^{HN}\!/_{N}$ by $f(h) = hN$ (it *has* to be left coset!). From the above remark, hN is an element of ${}^{NH}\!/_{H}$. Then f is a homomorphism since

$$f(xy) = xyN = (xN)(yN) = f(x) f(y),$$

for all $x, y \in H$. Also,

$$\begin{aligned} \text{Kern}(f) &= \left\{h \in H \mid f(h) = 1_{{}^{HN}\!/_{N}}\right\} \\ &= \{h \in H \mid hN = N\} \\ &= \{h \in H \mid h \in N\} \\ &= H \cap N. \end{aligned}$$

It is also clear that f is onto, since for any element $hnN \in {}^{HN}/_{N}$, where $h \in H$ and $n \in N$, we have $hnN = hN$, so that $f(h) = hN$. Therefore, $\text{Im}(f) = {}^{HN}/_{N}$, so by the first isomorphism theorem, we get

$$ {}^{H}/_{\text{Kern}(f)} = {}^{H}/_{H \cap N} \cong \text{Im}(f) = {}^{HN}/_{N} \Rightarrow {}^{H}/_{H \cap N} \cong {}^{HN}/_{N}, $$

as required. ■

Theorem 6.7.5 Third Isomorphism Theorem

Let G be a group and H and N subgroups such that $N \leq H$ and $N \trianglelefteq G$. Then

1. From the correspondence theorem, if K is a normal subgroup of ${}^{G}/_{N}$, then it is of the form ${}^{H}/_{N}$, where $H \leq G$. If $H \trianglelefteq G$, then ${}^{H}/_{N} \trianglelefteq {}^{G}/_{N}$. Conversely, if ${}^{H}/_{N} \trianglelefteq {}^{G}/_{N}$, then $H \trianglelefteq G$.
2. If ${}^{H}/_{N} \trianglelefteq {}^{G}/_{N}$, then

$$ \boxed{ {}^{{}^{G}/_{N}}/_{{}^{H}/_{N}} \cong {}^{G}/_{H} } . $$

Proof:

1. Suppose H and N are normal subgroups of G such that $N \leq H$. In particular, then $N \trianglelefteq H$ (as we have shown). We must show that ${}^{H}/_{N} \trianglelefteq {}^{G}/_{N}$. Recall what these two quotient groups look like:

$$ {}^{H}/_{N} = \{Nh \,|\, h \in H\} $$
$$ {}^{G}/_{N} = \{Ng \,|\, g \in G\} $$

We must show that for all elements $a \in {}^{H}/_{N}$ and $b \in {}^{G}/_{N}$ $b^{-1}ab \in {}^{H}/_{N}$ (i.e., the conjugate of all elements in ${}^{H}/_{N}$ by all elements in ${}^{H}/_{N}$ is still in ${}^{H}/_{N}$). So,

$$ (Ng)^{-1}(Nh)(Ng) = \left(Ng^{-1}\right)(Nh)(Ng) = Ng^{-1}hg, $$

for all $g \in G$ and $h \in H$. But since $H \triangleleft G$, we have that $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$. So since $g^{-1}hg \in H$, as required, we have that ${}^{H}/_{N}$ is normal in ${}^{G}/_{N}$.

Conversely, suppose ${}^{H}/_{N} \trianglelefteq {}^{G}/_{N}$, i.e., for all elements $a \in {}^{H}/_{N}$ and $b \in {}^{G}/_{N}$ $b^{-1}ab \in {}^{H}/_{N}$. But then $(Ng)^{-1}(Nh)(Ng) = Ng^{-1}hg$, which implies that $g^{-1}hg \in H$ for all $g \in G$ and $h \in H$. So $H \trianglelefteq G$.

2. Suppose ${}^{H}/_{N} \trianglelefteq {}^{G}/_{N}$. Define a mapping

$$ f : G \to {}^{{}^{G}/_{N}}/_{{}^{H}/_{N}} \quad \text{by} \quad f(g) = ({}^{H}/_{N})\, g, $$

i.e., the right coset of the quotient group ${}^{H}/_{N}$, which is

$$ ({}^{H}/_{N})\, g = \{ag \,|\, a \in {}^{H}/_{N}\}, $$

which we can also write as

$$ ({}^{H}/_{N})\, g = \{Nh \,|\, h \in H\}\, g = \{Nhg \,|\, h \in H\}. $$

Now, let us first show that this coset $(H/N)\,g$ is indeed an element of the quotient group $G/N\big/H/N$. But what does $G/N\big/H/N$ even look like!? It is the set of cosets of H/N in G/N, so each element in the group is of the form $(H/N)\,b$, where $b \in G/N$, i.e.,

$$G/N\big/H/N = \{(H/N)\,b \,|\, b \in G/N\}\,.$$

But since b is an element of G/N, we have $b = Ng$ for some $g \in G$, i.e.,

$$(H/N)\,b = \{Nhb \,|\, h \in H\} = \{NhNg \,|\, h \in H\} = \{Nhg \,|\, h \in H\} = (H/N)\,g,$$

so $(H/N)\,g$ is indeed an element of $G/N\big/H/N$. Now, let us go through our four steps of proving an isomorphism.

(a) We have just defined the mapping. Show that it is well defined!

(b) We now show that f is a homomorphism. For any two $g_1, g_2 \in G$, we have

$$\begin{aligned} f(g_1g_2) &= (H/N)\,g_1g_2 = \{Nhg_1g_2 \,|\, h \in H\} = \{Nhg_1 \,|\, h \in H\}\,\{Nhg_2 \,|\, h \in H\} \\ &= (H/N)\,g_1\,(H/N)\,g_2 = f(g_1)\,f(g_2)\,, \end{aligned}$$

so f is a homomorphism.

(c) We just showed above that any element $(H/N)\,b \in G/N\big/H/N$ can be written as $\{Nhg \,|\, h \in H\}$ and that $f(g) = \{H/N)\,g = \{Nhg \,|\, h \in H\}$, so that f is onto, which means that

$$\mathrm{Im}\,(f) = G/N\big/H/N.$$

(d) Finally, let us consider the kernel of f—it consists of all elements $g \in G$ such that $f(g) = 1_{G/N\big/H/N} = H/N = \{Nh \,|\, h \in H\}$. In general, $f(g) = (H/N)\,g = \{Nhg \,|\, h \in H\}$. Now, for all elements $h' \in G$ that are also in H

$$f\left(h'\right) = \left\{Nhh' \,|\, h \in H\right\} = \left\{N\tilde{h} \,|\, \tilde{h} \in H\right\} = H/N,$$

since $hh' = \tilde{h} \in H$. But since $H \leq G$, all those elements of g that are in H are all the elements of H; therefore,

$$\mathrm{Kern}\,(f) = H,$$

i.e., since $\mathrm{Kern}\,(f) \neq 1_G$, we have that f is *not* one-to-one, so that f is *not* a homomorphism.

It's OK that f is not an isomorphism—we only need f to be a homomorphism since the first isomorphism theorem immediately gives

$$G/\mathrm{Kern}\,(f) = G/H \cong \mathrm{Im}\,(f) = G/N\big/H/N,$$

as required. This completes the pf. ■

Theorem 6.7.6

Let G and K be two groups and let $N \trianglelefteq G$ and $H \trianglelefteq K$. Then:

1. $N \times H \trianglelefteq G \times K$.
2. $G \times K\big/N \times H \cong (G/N) \times (K/H)$.

PROOF:

1. First of all, as a reminder, we have

$$N \times H = \{(n,h) \mid n \in N,\, h \in H\}$$
$$G \times K = \{(g,k) \mid g \in G,\, k \in K\}.$$

We must show that any element $(n,h) \in N \times H$ is closed under conjugation, i.e., $(n,h)^{-1}(g,k)(n,h) \in N \times H$. We have

$$(g,k)^{-1}(n,h)(g,k) = \left(g^{-1},k^{-1}\right)(n,h)(g,k) = \left(g^{-1}ng, k^{-1}hk\right).$$

Now, $N \trianglelefteq G$ and $H \trianglelefteq K$, so $g^{-1}ng \in N$ and $k^{-1}hk \in H$, so that $\left(g^{-1}ng, k^{-1}hk\right) \in N \times H$. So $N \times H \trianglelefteq G \times K$.

2. To show this, we simply construct a mapping and show that it is a homomorphism and use the first isomorphism theorem.

   (a) Let us define a mapping

$$f : G \times K \to (G/N) \times (K/H) \quad \text{by} \quad f(g,k) = (Ng, Hk).$$

   Show that it is well defined!

   (b) We now show that f is a homomorphism. For any two elements $(g_1,k_1),(g_2,k_2) \in G \times K$, we have

$$\begin{aligned} f((g_1,k_1)(g_2,k_2)) &= f(g_1g_2, k_1k_2) = (Ng_1g_2, Hk_1k_2) = (Ng_1Ng_2, Hk_1Hk_2) \\ &= (Ng_1, Hk_1)(Ng_2, Hk_2) = f(g_1,k_1)\,f(g_2,k_2), \end{aligned}$$

   so that f is a homomorphism.

   (c) It is quite clear from the definition of the mapping that f is onto, so that

$$\mathrm{Im}(f) = (G/N) \times (K/H).$$

   (d) Finally, let us consider $\mathrm{Kern}(f)$. We want those elements of $G \times K$ that get mapped to the identity element of $(G/N) \times (K/H)$, namely (N,H). We know that $(Nn, Hh) = (N,H)$ whenever $n \in N$ and $h \in H$. And since $N \leq G$ and $H \leq K$ (in fact $N \trianglelefteq G$ and $H \trianglelefteq K$ as per the statement of the theorem), all elements of H are in G and all elements of H are in K, so that the kernel consists of all those pairs $(n,h) \in G \times K$ that are also in $N \times H$. In other words,

$$\mathrm{Kern}(f) = N \times H.$$

So by the first isomorphism theorem

$$(G \times K)/\mathrm{Kern}(f) = (G \times K)/(N \times H) \cong \mathrm{Im}(f) = (G/N) \times (K/H),$$

as required. ■

Theorem 6.7.7

Let G_1 and G_2 be two groups. Then:

1. $G_1 \times \{1_{G_2}\} \trianglelefteq G_1 \times G_2$ and $\{1_{G_1}\} \times G_2 \trianglelefteq G_1 \times G_2$.
2. $^{G_1 \times G_2}/_{G_1 \times \{1_{G_2}\}} \cong G_2$ and $^{G_1 \times G_2}/_{\{1_{G_1}\} \times G_2} \cong G_1$.

PROOF:

1. Let $H = G_1 \times \{1_{G_2}\}$ and let $(a, 1_{G_2}), (b, 1_{G_2}) \in H$. Then
$$(a, 1_{G_2})(b, 1_{G_2})^{-1} = (a, 1_{G_2})\left(b^{-1}, 1_{G_2}\right) = \left(ab^{-1}, 1_{G_2}\right) \in H,$$
so that H is a subgroup of $G_1 \times G_2$. Now, let $(a_1, a_2) \in G_1 \times G_2$ and $(b, 1_{G_2}) \in H$. Then,
$$(a_1, a_2)(b, 1_{G_2})(a_1, a_2)^{-1} = (a_1, a_2)(b, 1_{G_2})\left(a_1^{-1}, a_2^{-1}\right) = \left(a_1 b a_1^{-1}, 1_{G_2}\right) \in H,$$
so that H is a normal subgroup of $G_1 \times G_2$. The second part is similar (do it!!).
2. Consider the mapping $f : G_1 \times G_2 \to G_2$ defined by $f(a_1, a_2) = a_2$. Then f is a homomorphism since we have
$$f((a_1, a_2)(b_1, b_2)) = f(a_1 b_1, a_2 b_2) = a_2 b_2 = f(a_1, a_2) f(b_1, b_2).$$
Also, f is onto since, given any $y \in G_2$, we have $y = f(x, y)$ for any $x \in G_1$. Finally, $(a_1, a_2) \in \text{Kern}(f)$ if and only if $a_2 = 1_{G_2}$, hence if and only if $(a_1, a_2) \in G_1 \times \{1_{G_2}\} = H$. Therefore, by the first isomorphism theore, we have the required isomorphism. The second part of the statement is similar (do it!!). ■

Example 6.7.1 Show that the Klein 4-Group, which we saw can be represented as D_2, is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

SOLUTION:

Example 6.7.2 Consider the group $S_3 = \left\{1, b, b^2, a, ab, ab^2\right\}$.

1. Determine all normal subgroups of S_3 and write down their corresponding quotient group.
2. Then consider the group $S_3 \times S_3$ (which has 36 elements). Determine all the normal subgroups of $S_3 \times S_3$ and write down their corresponding quotient group.

SOLUTION:

1. Let us first determine all the subgroups before going to normal subgroups. Recall Lagrange's Theore, which says that if H is a subgroup of a group G, then $|H|$ divides $|G|$. Now, $|S_3| = 6$, and the integers that divide 6 are 1,2,3,6, so there are four subgroups of S_3. These are

$$\begin{aligned}
\langle 1\rangle &= \{1\} \qquad |\langle 1\rangle| = 1 \text{ (trivial subgroup)} \\
\langle a\rangle &= \{1, a\} \qquad |\langle a\rangle| = 2 \\
\langle ab\rangle &= \{1, ab\} \qquad |\langle ab\rangle| = 2 \\
\left\langle ab^2\right\rangle &= \left\{1, ab^2\right\} \qquad \left|\left\langle ab^2\right\rangle\right| = 2 \\
\langle b\rangle &= \left\{1, b, b^2\right\} \qquad |\langle b\rangle| = 3 \\
S_3 &= \left\{1, b, b^2, a, ab, ab^2\right\} \qquad |S_3| = 6 \text{ (the whole group)}
\end{aligned}$$

   Now, to determine which of these subgroups is normal in S_3, it is easiest to simply see for which subgroups are the corresponding left and right cosets equal. We have already seen in a previous example that $\langle b\rangle \trianglelefteq S_3$, so we don't check that one. Also, it should be clear that $\{1\}$, being the trivial subgroup, has equal left and right cosets, so that $\{1\} \trianglelefteq S_3$. Also, $S_3 \trianglelefteq S_3$. So far we have three normal subgroups.

   The left and right cosets of $\langle a\rangle$ are

$$\begin{aligned}
1\langle a\rangle &= \{1, a\} \quad \langle a\rangle 1 = \{1, a\} \\
a\langle a\rangle &= \{a, 1\} \quad \langle a\rangle a = \{a, 1\} \\
b\langle a\rangle &= \left\{b, ab^2\right\} \quad \langle a\rangle b = \{b, ab\} \neq b\langle a\rangle,
\end{aligned}$$

   and we don't need to check the rest since we found an instance in which the left and right cosets are not equal. So $\langle a\rangle$ is not normal in S_3.

   Similarly, we can see that

$$b\langle ab\rangle = \{b, bab\} = \{b, a\} \quad \text{and} \quad \langle ab\rangle b = \{b, abb\} = \left\{b, ab^2\right\} \neq b\langle ab\rangle,$$

   so $\langle ab\rangle$ is not normal in S_3. Finally,

$$b\left\langle ab^2\right\rangle = \left\{b, bab^2\right\} = \{b, ab\} \quad \text{and} \quad \left\langle ab^2\right\rangle b = \left\{1, ab^2b\right\} = \{1, a\} \neq b\left\langle ab^2\right\rangle,$$

   so $\left\langle ab^2\right\rangle$ is also not normal in S_3. So there are only three normal subgroups of S_3,

$$\{1\}, \quad \langle b\rangle, \quad \text{and} \quad S_3.$$

   Let us focus on the normal subgroup $\langle b\rangle$. Its corresponding quotient group $S_3/\langle b\rangle$ has two elements,

$$S_3/\langle b\rangle = \left\{\left\{1, b, b^2\right\}, \left\{a, ab, ab^2\right\}\right\} = \{\langle b\rangle, \langle b\rangle a\}.$$

   Remember that the identity element of this group is $\langle b\rangle$. Now,

$$(\langle b\rangle a)^2 = \langle b\rangle a\langle b\rangle a = \langle b\rangle aa = \langle b\rangle a^2 = \langle b\rangle,$$

   so we have that $S_3/\langle b\rangle$ is a *cyclic group of order two.* And as we know, all cyclic groups of order two are isomorphic to $\mathbb{Z}_2$, which itself is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Hence,

$$S_3/\langle b\rangle \cong \mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z}.$$

2. We now want to find the normal subgroups of $S_3 \times S_3$. We have seen that S_3 has three normal subgroups, the trivial one, the improper one, and $\langle b \rangle$. Using the theorem above, then, we immediately get *nine* normal subgroups:

$$\begin{aligned}
\{1\} \times \langle b \rangle &= \left\{(1,1), (1,b), \left(1,b^2\right)\right\} \\
\langle b \rangle \times \{1\} &= \left\{(1,1), (b,1), \left(b^2,1\right)\right\} \\
\{1\} \times S_3 &= \left\{(1,1), (1,b), \left(1,b^2\right), (1,a), (1,ab), \left(1,ab^2\right)\right\} \\
S_3 \times \{1\} &= \left\{(1,1), (b,1), \left(b^2,1\right), (a,1), (ab,1), \left(ab^2,1\right)\right\} \\
\langle b \rangle \times S_3 & \\
S_3 \times \langle b \rangle & \\
\{1\} \times \{1\} &= \{(1,1))\} \qquad \text{(trivial)} \\
\langle b \rangle \times \langle b \rangle & \\
S_3 \times S_3 & \qquad \text{(whole group)}
\end{aligned}$$

Now, we discovered above that ${}^{S_3}/_{\langle b \rangle} \cong \mathbb{Z}_2$. This implies that

$$\left({}^{S_3}/_{\langle b \rangle}\right) \times \left({}^{S_3}/_{\langle b \rangle}\right) \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

(Remember that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to the Klein 4-Group.) But remember that $\mathbb{Z}_2$ is an Abelian group, and by Theorem 6.4.5, every subgroup of an Abelian groups is a normal subgroup. Therefore, using the theorem above, any subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a normal subgroup. On the other hand, using the theorem above with $G = K = S_3$ and $N = \langle b \rangle$, we get

$${}^{S_3 \times S_3}/_{\langle b \rangle \times \langle b \rangle} \cong \left({}^{S_3}/_{\langle b \rangle}\right) \times \left({}^{S_3}/_{\langle b \rangle}\right) \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

This means that any subgroup of ${}^{S_3 \times S_3}/_{\langle b \rangle \times \langle b \rangle}$ is a normal subgroup. Now, from the third isomorphism theorem part 1 (the converse), any normal subgroup of ${}^{S_3 \times S_3}/_{\langle b \rangle \times \langle b \rangle}$ is of the form ${}^{H}/_{\langle b \rangle \times \langle b \rangle}$ where $H \trianglelefteq S_3 \times S_3$. And these subgroups H will be isomorphic to the normal subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$. The subgroups (which are all normal) of $\mathbb{Z}_2 \times \mathbb{Z}_2$ are

$$\begin{aligned}
\{([0],[0])\} & \qquad \text{(trivial)} \\
\mathbb{Z}_2 \times \mathbb{Z}_2 & \qquad \text{(whole group)} \\
\langle([0],[1])\rangle &= \{([0],[0]), ([0],[1])\} = [0] \times \mathbb{Z}_2 \\
\langle([1],[0])\rangle &= \{([0],[0]), ([1],[0])\} = \mathbb{Z}_2 \times [0] \\
\langle([1],[1])\rangle &= \{([0],[0]), ([1],[1])\}.
\end{aligned}$$

6.8 Automorphisms

Recall that automorphisms are isomorphisms from a group to itself. In this section we will present some results about automorphisms. We will denote the set of all automorphisms of a group G by $\mathrm{Aut}(G)$.

Theorem 6.8.1

Let G be a group. Then $\mathrm{Aut}(G)$ is a group under composition of functions.

PROOF: We prove that the four group axioms hold.

1. Let $f_1, f_2 \in \mathrm{Aut}(G)$ be two automorphisms, and consider $f_1 \circ f_2$. We already know from Chapter 1 that a composition of injective functions is injective and a composition of surjective functions is surjective. So to show that $f_1 \circ f_2$ is also an automorphism, we must show that $f_1 \circ f_2$ is a homomorphism, but this follows from Theorem 6.1.1.
2. We have already seen in Chapter 1 that composition of functions is associative.
3. Let f_0 be the identity mapping on G, i.e., $f_0(a) = a$ for all $a \in G$. Indeed, f_0 is an automorphism and since $f \circ f_0 = f$ and $f_0 \circ f = f$, we see that f_0 is the appropriate identity element in $\mathrm{Aut}(G)$.
4. Let $f \in \mathrm{Aut}(G)$. Since f is a bijection (being an isomorphism), from Chapter 1 we have that f is invertible, i.e., f^{-1} exists and is also a bijection such that $f \circ f^{-1} = f_0 = f^{-1} \circ f$. Finally, we show that f^{-1} is a homomorphism. Indeed, let $a, b \in G$ and let $c = f^{-1}(a)$, $d = f^{-1}(b)$. We have $f(c) = a$, $f(d) = b$, and since f is a homomorphism, $f(cd) = f(c) f(d) = ab$, from which it follows that $f^{-1}(ab) = cd = f^{-1}(a) f^{-1}(b)$, so that f^{-1} is a homomorphism. In other words, for every $f \in \mathrm{Aut}(G)$ there exists an inverse $f^{-1} \in \mathrm{Aut}(G)$.

Having proved the four group axioms, we have that $\mathrm{Aut}(G)$ is a group. ■

Example 6.8.1 Let us find all possible isomorphisms $f : \mathbb{Z}_6 \to \mathbb{Z}_6$, i.e., let us determine $\mathrm{Aut}(\mathbb{Z}_6)$. We know that $\mathbb{Z}_6$ is cyclic and $[1]$ is a generator, i.e., $\mathbb{Z}_6 = \langle [1] \rangle$. From Lemma 6.2.1, $o(f(a)) = o(a)$ for all a. So if f is an isomorphism, we must have $o(f([1])) = o([1]) = 6$, so $f([1])$ must be a generator of $\mathbb{Z}_6$, and therefore $f([1]) = [1]$ or $f([1]) = [5]$. Also, once $f([1])$ is known, f is completely determined, since we must have $f([2]) = [2] f([1])$, $f([3]) = [3] f([1])$, and so on, and these maps are isomorphisms by Lemma 6.2.2. So there are exactly two isomorphisms (observe that the one with $f([1]) = [1]$ is nothing but the identity, mapping, i.e., the trivial isomorphism). Let f_0 be this mapping, and let f_1 be the isomorphism with $f([1]) = [5]$. Consider now the operation of composition of functions on the set $\{f_0, f_1\}$. We have

$$f_0 \circ f_0 = f_0$$
$$f_0 \circ f_1 = f_1 \circ f_0 = f_1.$$

What about $f_1 \circ f_1 = (f_1)^2$? We have

$$f_1 \circ f_1([1]) = f_1(f_1([1])) = f_1([5]) = [5][5] = [25] = [1] \Rightarrow f_1 \circ f_1 = (f_1)^2 = f_0.$$

Therefore, $\mathrm{Aut}(\mathbb{Z}_6) = \{f_0, f_1\}$ is thus a cyclic group of order two!

Example 6.8.2 Let us now determine $\mathrm{Aut}(\mathbb{Z}_8)$. Since $\mathbb{Z}_8$ is cyclic with generator $[1]$, if f is any automorphism, we must have $o(f([1])) = o([1]) = 8$, and $f([1])$ must also be a generator of $\mathbb{Z}_8$. That is, we must have either $f([1]) = [1]$ (trivial automorphism), $f([1]) = [3]$, $f([1]) = [5]$, or $f([1]) = [7]$. Again, once $f([1])$ is known, f is completely determined, since in general $f([n]) = [n]f([1])$. All of these maps are indeed isomorphisms. Therefore, we have four automorphisms.

Remember that all finite cyclic groups of order n are isomorphic to $\mathbb{Z}_n$.

Theorem 6.8.2

Let G be a finite cyclic group of order n. Then $\mathrm{Aut}(G) \cong U(n)$.

PROOF: We follow our four steps of proving two groups are isomorphic.

1. First we define a mapping $T : \mathrm{Aut}(G) \to U(n)$ as follows. Let $G = \langle a \rangle$, where $o(a) = n$. Consider $f \in \mathrm{Aut}(G)$. For any $g \in G$, we have $g = a^i$ for some integer i, $0 \leq i < n$, and then $f(g) = f(a^i) = f(a)^i$ (since f is a homomorphism), so f is completely determined once $f(a)$ is fixed. We must have $o(f(a)) = f(a) = n$, hence $f(a)$ is also a generator of G, and therefore $f(a) = a^r$ for some r with $\gcd(n, r) = 1$, and hence $a^r = a^s$, where s is the remainder of r mod n (what does this mean?). Thus, there is an $s \in \{q \mid \gcd(n, q) = 1, 0 \leq q < n\} = U(n)$ such that $f(a) = a^s$. So we define T by $T(f) = s$.

2. We now show that T is a homomorphism. If $f, g \in \mathrm{Aut}(G)$, with $f(a) = a^s$ and $g(a) = a^r$, where $r, s \in U(n)$, then $g \circ f(a) = g(f(a)) = g(a^s) = a^{st} = a^u$, where $u \equiv st \bmod n$. It follows that $T(g \circ f) = u = T(g)\,T(f) \bmod n$ (since the operation in $U(n)$ is *multiplication* modulo n).

3. T is one-to-one beause if $T(g) = T(f)$, then $f(a) = a^{T(f)} = a^{T(g)} = g(a)$, and hence $f = g$.

4. T is onto because if $s \in U(n)$, then a^s is a generator of G, and the mapping defined by $f(a^i) = a^{si}$ is an isomorphism by Lemma 6.2.2.

Therefore, we have found an isomorphism T, and hence $\mathrm{Aut}(G) \cong U(n)$. ■

Let G be a cyclic group of order n. Then $\mathrm{Aut}(G) \cong U(n)$.

7 The Permutation Group S_n

We looked at this in section 4.3.1, and we established that S_n, which is the set of permutations of n distinct objects, or simply the permutations of $O_n = \{1, 2, \ldots, n\}$, is a group under composition of functions. In fact, we saw that permutations are simply bijections from O_n to itself. We looked at some examples, and we also looked at the number of elements of S_n that have a particular type of cycle structure. We also developed the concept of cyclic notation for bijections in section 1.2, and looked at *disjoint* bijections.

We will now revisit all of these concepts and develop them more formally in the context of permutations. The permutation group is important because, as we will see later, *any* finite group can be viewed as a subgroup of a permutation group. This means that studying finite groups amounts to studying permutation groups and their subgroups. When we want to construct a finite group with specific properties, we look for permutations that generate a subgroup with these properties.

In general, any bijection from a set X to itself can be regarded as permutation, and in this case the bijection is called a **permutation of the set** X.

Example 7.0.3 Here are some examples of permutations.

1. The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n+1$ is one-to-one because if $f(n_1) = f(n_2)$, then $n_1+1 = n_2+1 \Rightarrow n_1 = n_2$. It is also onto, because for any $m \in \mathbb{Z}$, $f(m-1) = m$. So f is a bijection, and hence a permutation of the set $\mathbb{Z}$.
2. The function $f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$, defined by $f(1) = 3$, $f(2) = 4$, $f(3) = 1$, and $f(4) = 2$, is clearly one-to-one and onto, so it is a permutation of the set $\{1, 2, 3, 4\}$.

A more common name for S_n is the *symmetric group of order* n, for reasons we shall see later.

Definition 7.0.1 The Symmetric Group of Order n

The group consisting of the set S_n under the operation of composition of bijections, is called the **symmetric group of order** n.

7.1 Disjoint Permutations

The key concept in the factorisation of permutations is disjoint cycles. Indeed, we have already seen that every permutation can be written as a product of disjoint cycles. We will now prove

this result formally. First, let us restate some of the definitions from section 1.2.

Definition 7.1.1

Here is a summary of important definitions that we will need.

1. Let $\alpha \in S_n$. If $x \in O_n$, then α **fixes** x if $\alpha(x) = x$ and α **moves** x if $\alpha(x) \neq x$.
2. Let $p_1, p_2, \ldots, p_r \in O_n$ be r distinct points from O_n, with $r \leq n$. If $\alpha : O_n \to O_n$ fixes the remaining $n - r$ points, and if

$$\alpha(p_1) = p_2,\ \alpha(p_2) = p_3,\ \ldots,\ \alpha(p_{r-1}),\ \alpha(p_r) = p_1,$$

   then α is an r-**cycle**, or a **cycle of length** r. We then write $\alpha = (p_1\, p_2\, \cdots\, p_r)$.
3. A 2-cycle, i.e., a cycle of length two, merely interchanges a pair of elements. It is called a **transposition**.

Definition 7.1.2 Disjoint Permutations

Let $\alpha, \beta \in S_n$. We say that α and β are **disjoint** if for any $i \in \{1, 2, \ldots, n\}$

$$\alpha(i) \neq i \Rightarrow \beta(i) = i.$$

If α and β are disjoint, then so are β and α, i.e.,

$$\beta(i) \neq i \Rightarrow \alpha(i) = i,$$

since this is just the contrapositive of the first statement for α and β being disjoint.

REMARK: Be careful when using this definition. Note that is is perfectly possible that there exists an element $i \in O_n$ such that $\alpha(i) = i = \beta(i)$, i.e., it is perfectly possible that α and β both fix some element of O_n. All the defintion says is that if one of the permutations moves i, then the other must fix i.

Note that this is exactly the same definition as the one given in Definition 1.2.3.

Theorem 7.1.1 Commutativity of Disjoint Permutations

If $\alpha, \beta \in S_n$ are disjoint, then $\alpha\beta = \beta\alpha$.

PROOF: To prove this, we need to show that $\alpha\beta(i) = \beta\alpha(i)$ for all $i \in O_n = \{1, 2, \ldots, n\}$. Let $i \in O_n$ be arbitrary. Then there are two cases

Case 1 $\alpha(i) = i$, i.e., α fixes i.
Then $\beta\alpha(i) = \beta(i)$. Then, we have two cases

1. $\beta(i) = i$: In this case, we have $\beta\alpha(i) = \beta(i) = i$ and $\alpha\beta(i) = \alpha(i) = i = \beta\alpha(i)$, as required.
2. $\beta(i) = j \neq i$: Now, we must have $\beta(j) \neq j$, i.e., β must move j, otherwise we would have $\beta(i) = j$ and $\beta(j) = j$, i.e., that β is not one-to-one, contradicting the fact that β is a permutation, and hence a bijection. So $\beta(j) \neq j$, and since α and β are disjoint, we must have that $\alpha(j) = j$. Therefore, $\alpha\beta(i) = \alpha(j) = j$ and $\beta\alpha(i) = \beta(i) = j = \alpha\beta(i)$, as required.

Case 2 $\alpha(i) \neq i$, i.e., α moves i.

Since α and β are disjoint, we must then have $\beta(i) = i$. Again, we consider two subcases.

1. $\alpha(i) = i$: In this case, we get $\beta\alpha(i) = \beta(i) = i$ and $\alpha\beta(i) = \alpha(i) = i = \beta\alpha(i)$, as required.
2. $\alpha(i) = j \neq i$: Now, we must have $\alpha(j) \neq j$, otherwise $\alpha(j) = j$ and $\alpha(i) = j$, meaning that α is not one-to-one, contradicting the fact that α is a permutation, and hence a bijection. So $\alpha(j) \neq j$, which means that $\beta(j) = j$ since α and β are disjoint. Therefore, $\alpha\beta(i) = \alpha(j) = j$ and $\beta\alpha(i) = \beta(j) = j = \alpha\beta(i)$, as required. ■

Theorem 7.1.2

Let $\alpha, \beta \in S_n$ be two disjoint permutations. Then, for any $k \in \mathbb{Z}$, we have

$$(\alpha\beta)^k = \alpha^k\beta^k.$$

PROOF: By the previous theorem, since α and β are disjoint, $\alpha\beta = \beta\alpha$. Using this, we get

$$\begin{aligned}(\alpha\beta)^k &= (\alpha\beta)(\alpha\beta)\cdots(\alpha\beta)\\ &= (\alpha\alpha\ldots\alpha)(\beta\beta\cdots\beta)\\ &= \alpha^k\beta^k,\end{aligned}$$

as required. ■

Theorem 7.1.3

Let $\alpha, \beta \in S_n$ be disjoint permutations. Then, for any $l \in \mathbb{Z}$, we have that α^l and β^l are also disjoint.

PROOF: Since α and β are disjoint, we have that if $\alpha(i) \neq i$, then $\beta(i) = i$ for some $i \in \{1, 2, \ldots, n\}$. Now, since β fixes i, we must have that β^l also fixes i for any $l \in \mathbb{Z}$ (to see this, simply write down a general permutation and multiply it l times). Now, suppose α^l moves i, i.e., $\alpha^l(i) \neq i$. Then we must have $\alpha(i) \neq i$, for if $\alpha(i) = i$, then we would have $\alpha^l(i) = i$, a contradiction (note that the converse of this is generally false!). Therefore, we have

$$\alpha^l(i) \neq i \Rightarrow \alpha(i) \neq i \Rightarrow \beta(i) = i \Rightarrow \beta^l(i) = i,$$

i.e., $\alpha^l(i) \neq i \Rightarrow \beta(i) = i$, i.e., α^l and β^l are disjoint, as required. ■

Theorem 7.1.4

If α and β are disjoint cycles, then

$$o(\alpha\beta) = \text{lcm}(o(\alpha), o(\beta)).$$

PROOF: To prove this, we will show that $o(\alpha\beta) \mid \text{lcm}(o(\alpha), o(\beta))$ and $\text{lcm}(o(\alpha), o(\beta)) \mid o(\alpha\beta)$. Now, let $m = \text{lcm}(o(\alpha), o(\beta))$. Then,

$$(\alpha\beta)^m = \alpha^m\beta^m = 1 \times 1 = 1,$$

which, as we know, implies that

$$o(\alpha\beta) \mid m \Rightarrow o(\alpha\beta) \mid \text{lcm}(o(\alpha), o(\beta)).$$

Next, let $l = o(\alpha\beta)$ and suppose $(\alpha\beta)^l = \alpha^l\beta^l = 1$. In other words $\alpha^l\beta^l$ is the identity permutation and so $\alpha^l\beta^l(i) = i$ for all $i \in \{1, 2, \ldots, n\}$. Now, we must have $\beta^l(i) = i$ for all i, for if $\beta^l(i) = j \neq i$, then we must have $\alpha^l(j) = i$ in order to satisfy the assumption that $\alpha^l\beta^l = 1$ and hence that $\alpha^l\beta^l(i) = i$ for all $i \in \{1, 2, \ldots, n\}$. But, from the theorem above, we have that α^l and β^l are disjoint, which means that since $\beta^l(i) \neq i$ $\alpha^l(i) = i$. But then $\alpha^l(i) = i$ and $\alpha^l(j) = j$, so that α is not one-to-one, a contradiction to the fact that α is a permutation, and hence a bijection. Therefore $\beta^l(i) = i$ for all $i \in \{1, 2, \ldots, n\}$, that is, $\beta^l = 1$. A similar argument, using the fact that $\beta^l\alpha^1 = 1$ as well, and so $\beta^l\alpha^l(i) = i$ for all $i \in \{1, 2, \ldots, n\}$, leads to $\alpha^l = 1$.

Therefore, we have $\alpha^l = 1$ and $\beta^l = 1$, which implies that $o(\alpha) \mid o(\alpha\beta)$ and $o(\beta) \mid o(\alpha\beta)$, which implies that

$$\text{lcm}(o(\alpha), o(\beta)) \mid o(\alpha\beta).$$

Therefore, we have $o(\alpha\beta) = \text{lcm}(o(\alpha), o(\beta))$, as required. ■

7.2 Cycle Structures

In this section, we set out to formally define what cycles are and show that every permutation can not be factored into cycles, something we have seen quite a bit of, but that this factorisation is *unique* up to the order of the cycles.

Consider the set $O_9 = \{1, 2, 3, \ldots, 9\}$ and the permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 18 & 6 & 4 & 3 & 5 & 2 & \end{pmatrix} \in S_9.$$

Let is look at where repeated application of α takes various elements of the set O_9:

$$1 \to \alpha(1) = 7 \to \alpha^2(1) = \alpha(7) = 3 \to \alpha^3(1) = \alpha(3) = 1$$
$$2 \to \alpha(2) = 9 \to \alpha^2(2) = \alpha(9) = 2$$
$$4 \to \alpha(4) = 8 \to \alpha^2(4) = \alpha(8) = 5 \to \alpha^3(4) = \alpha(5) = 6 \to \alpha^4(4) = \alpha(6) = 4$$

Notice that we are taking certain elements of O_9, applying α and its powers to that element until we return to it. This may remind us of the cyclic notation for permutations. Indeed, we may write the first case as the permutation $(1\,7\,3)$, the second as $(2\,9)$, and the third as $(4\,8\,5\,6)$. The permutation α has, in a sense, given us three new permutations based on its powers. In particular, what we have just done is *factor* α, something that we have already looked at, albeit in a completely different way. So we may write

$$\alpha = (1\ 7\ 3)\,(2\ 9)\,(4\ 8\ 5\ 6)\,.$$

We now go a bit further in our interpretation of this factorisation. We can see that factoring α has *partitioned* the set O_9 into three disjoint subsets.

What have we seen already in relation to partitioning of sets. We have seen, for example, with cosets, that equivalence relations allow us to partition our set. The equivalence relation we may state for such a partition is as follows: two elements $i, j \in O_9$ are equivalent under α, written $i \sim_\alpha j$, if $\alpha^n(i) = j$ for some $n \in \mathbb{Z}$. Thus, $1 \sim_\alpha 3$ because $\alpha^2(1) = 3$, and $4 \sim_\alpha 6$ because $\alpha^3(4) = 6$. The equivalence classes are $\{1, 7, 3\}$, $\{2, 9\}$, and $\{4, 8, 5, 6\}$. We see that α moves elements of O_9 only within an equivalence class, but not between them.

Theorem 7.2.1

Every permutation $\alpha \in S_n$ determines an equivalence relation on the set O_n. This equivalence relation is defined by the condition that, for some $i, j \in O_n$, $i \sim_\alpha j$ if and only if there exists an $l \in \mathbb{Z}$ such that $\alpha^l(i) = j$.

PROOF: We simply prove that the three properties of an equivalence relation, reflexivity, symmetry, and transitivity, hold.

1. (Reflexivity) For all $i \in O_9$, $\alpha^0(i) = i$, so that $i \sim_\alpha i$.
2. (Symmetry) Suppose $i \sim_\alpha j$ for all $i, j \in O_n$. Then there exists an $l \in \mathbb{Z}$ such that $\alpha^l(i) = j$, which implies that $i = \alpha^{-l}(j)$ (α^{-1} exists because α is a bijection). But $-l \in \mathbb{Z}$, so by definition $j \sim_\alpha i$.
3. (Transitivity) Suppose $i \sim_\alpha j$ and $j \sim_\alpha k$ for all $i, j, k \in O_n$. Then there exist integers l_1 and l_2 such that $\alpha^{l_1}(i) = j$ and $\alpha^{l_2}(j) = k$. Then,

$$\alpha^{l_2}\left(\alpha^{l_1}(i)\right) = \alpha^{l_2}(j) = k = \alpha^{l_1+l_2}(i)\,,$$

so that by definition $i \sim_\alpha k$.

We have shown that $\sim_\alpha$ satisfies the properties of an equivalence relation, so the pf is complete. ■

The equivalence classes generated by $\sim_\alpha$ are the *cycles*, which we now formally define.

Definition 7.2.1 Cycle

Each equvalence class generated by $\sim_\alpha$ is a permutation called a **cycle**. A cycle $C = \{c_1, c_2, \ldots, c_l\}$ is a finite subset of $\{1, 2, \ldots, n\}$, written as the sequence $(c_1\ c_2\ \cdots c_l)$, such that for all $1 \leq i, j \leq l$ $c_i \neq c_j$. Additionally, for all $a \in \{1, 2, \ldots, n\}$, if $a \in C$, say $a = c_i$, and $\alpha = (c_1\ c_2\ \cdots\ c_l) \in S_n$, then

$$\alpha(c_i) = \begin{cases} c_{i+1} & \text{if } i \leq l \\ c_1 & \text{if } i = l \end{cases}.$$

If $a \notin C$, then $\alpha(a) = a$.

Definition 7.2.2 Cycle Structure

Suppose $C_1, C_2, \cdots, C_k$ are the equivalence classes generated by $\sim_\alpha$ for any $\alpha \in S_n$. We may order these so that $|C_1| \leq |C_2| \leq \cdots \leq |C_k|$. The **cycle structure** of α is

$$[|C_1|,\ |C_2|,\ \cdots,\ |C_n|],$$

such that

$$\sum_{i=1}^{k} |C_i| = n.$$

It is important to note that, as we have seen already, each cycle is itself a permutation. Of course, we may multiply several permutations to get other permutations.

Definition 7.2.3 Disjoint Cycles

Let $\alpha = (a_1\ a_2\ \cdots\ a_k) \in S_n$ and $\beta = (b_1\ b_2\ \cdots\ b_l) \in S_n$ be two cycles such that $k, l \leq n$ and $\{a_1, a_2, \ldots, a_k\}, \{b_1, b_2, \ldots, b_l\} \subseteq \{1, 2, \ldots, n\}$. α and β are **disjoint** if $\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_l\} = \varnothing$.

Example 7.2.1 Let $\alpha = (1\ 2\ 8)$ and $\beta = (5\ 6\ 7)$ in S_8. Then α and β are disjoint because $\{1, 2, 8\} \cap \{5, 6, 7\} = \varnothing$. However, if $\gamma = (1\ 5)$, then α and γ are not disjoint because $\{1, 2, 8\} \cap \{1, 5\} = \{1\} \neq \varnothing$.

Theorem 7.2.2

If $\alpha, \beta \in S_n$ are disjoint cycles, then α and β are disjoint permutations.

PROOF: Let $C = \{c_1, c_2, \ldots, c_l\}$ be the set associated to α, i.e., let $\alpha = (c_1\ c_2 \cdots\ c_l)$, and let $C' = \{c_1, c_2, \ldots, c_k\}$ be the set associated to β, i.e., let $\beta = (c_1\ c_2\ \cdots\ c_k)$. Suppose $a \in \{1, 2, \ldots, n\}$ and $\alpha(a) \neq a$. Since α is a cycle, by definition, we must have $a \in C$ since α moves a. Now, since α and β are disjoint, $C \cap C' = \varnothing$. In particular, then, $a \in C'$. But then, by

definition of cycle, we must have $\beta(a) = a$, i.e., we must have that β fixes a. So we have that if α moves a, then β fixes a, which is precisely the definition of disjoint permutations, so the pf is complete. ■

Theorem 7.2.3

Let $\alpha = \alpha_1\alpha_2\cdots\alpha_k$ be a product of the disjoint cycles $\alpha_1, \alpha_2, \ldots, \alpha_k$ (we know that such a disjoint cycle factorisation exists). Then,

$$o(\alpha) = \text{lcm}\left(o(\alpha_1), o(\alpha_2), \ldots, o(\alpha_k)\right).$$

PROOF: Since $\alpha_1, \alpha_2, \ldots, \alpha_k$ are disjoint disjoint cycles, by the theorem above, they are also disjoint permutations. Now, recall that we showed that $o(\alpha\beta) = \text{lcm}(o(\alpha), o(\beta))$ for two disjoint permutations α and β. We can extend this result, so that $o(\alpha_1\alpha_2\cdots\alpha_k) = \text{lcm}\left(o(\alpha_1), o(\alpha_2), \ldots, o(\alpha_k)\right) = o(\alpha)$, as required. ■

Theorem 7.2.4

Let $\alpha = (c_1\ c_2\ \cdots\ c_l) \in S_n$ be a cycle. Then $o(\alpha) = l$.

PROOF: Let $C = \{c_1, c_2, \ldots, c_l\}$ be the set associated with α and let $a \in C$. Then we must have $\alpha^l(a) = a$, i.e., we must have $\alpha^l = 1$, the identity permutation. Thus, $o(\alpha) \quad l$. But, by definition of a cycle, all elements in C are unique, hence it is not possible that $\alpha^k(a) = a$ for any $1 \leq k < l$. So we must have $o(\alpha) = l$. ■

Example 7.2.2 In S_8, let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 2 & 4 & 7 & 1 & 6 & 3 \end{pmatrix} = (1\ 5\ 7\ 6)(2\ 8\ 3)(4).$$

Then, $o(\alpha) = \text{lcm}(4, 3, 1) = 12$. The cycle of structure of α is $[4, 3, 1]$. Now, observe that we may write α as

$$\alpha = \left(1\ \alpha(1)\ \alpha^2(1)\ \alpha^3(1)\right)\left(2\ \alpha(2)\ \alpha^2(2)\right),$$

or equivalently as

$$\alpha = (5\ 7\ 6\ 1)(8\ 3\ 2) \Rightarrow \alpha = \left(5\ \alpha(5)\ \alpha^2(5)\ \alpha^3(5)\right)\left(8\ \alpha(8)\ \alpha^2(8)\right),$$

an so on for each different way of writing each cycle. (We may also write $1 = \alpha^0(1)$ and $5 = \alpha^0(5)$.) This way of writing the cycle looks more like the way we write cyclic (sub)groups, say, of D_n.

We have formally defined what a cycle is, and we have said that if $\alpha = (c_1\ c_2\ \cdots\ c_l)$ is a cycle,

then $\alpha(c_l) = c_1$. We now prove that this actually follows from the formalism of the equivalence relation $\sim_\alpha$. At the same time, we will prove that there exists a factorisation into disjoint cycles for each element $\alpha \in S_n$.

Theorem 7.2.5 **Existence of Disjoint Factorisation**

Given an element $\alpha \in S_n$ with cycle structure $[n_1, n_2, \ldots, n_k]$, then there exists disjoint cycles $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that $\alpha = \alpha_1\alpha_2\cdots\alpha_k$ with each α_i being an n_i-cycle, $1 \leq i \leq k$.

PROOF: Let $\alpha \in S_n$ and consider the equivalence class C_i of $\sim_\alpha$ for some $i \in \{1, 2, \ldots, n\}$. In particular, let

$$C_i = \left\{a_i^1, a_i^2, \ldots, a_i^{n_i}\right\}.$$

Remember that each equivalence class is a cycle. Without loss of generality, consider a_i^1. Then,

$$\alpha\left(a_i^1\right) = a_i^2, \alpha\left(a_i^2\right) = a_i^3, \ldots, \alpha\left(a_i^l\right) = a_i^k, \quad 1 \leq k \leq l,\ 1 \leq l \leq n_i.$$

Observe that this does not violate the fact that each element of C_i is equivalent to each other under $\sim_\alpha$ (remember that since C_i is an equivalence class of $\sim_\alpha$, each one of its elements must be equivalent to each other under $\sim_\alpha$), since there exists a $j \in \mathbb{Z}$, in this case 1, such that $\alpha\left(a_1^1\right) = a_i^2$, and so on.

Now, by definition of the cycle, we must have $\alpha\left(a_i^{n_i}\right) = a_i^1$. We now *prove* (by contradiction) that this must be the case, i.e., we prove that $l = n_i$ and $k = 1$. For if it is not, then let us define the set

$$\tilde{C}_i = \left\{a_i^1, a_i^2, \ldots, a_i^l\right\} \subset C_i.$$

We have $\alpha\left(a_i^l\right) = a_i^k$. Now, let $m \in \mathbb{Z}$ be arbitrary. By the Division Algorithm, we may write $m = q(l-k) + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r \leq l - k$. Then,

$$\alpha^m\left(a_i^k\right) = \alpha^{r+q(l-k)}\left(a_i^k\right) = \alpha^r\left(\alpha^{q(l-k)}\left(a_i^k\right)\right) = \alpha^r\left(a_i^k\right) = a_i^{k+r},$$

which implies, by definition of $\sim_\alpha$, that

$$\tilde{C_i}' = \left\{a_i^k, a_i^{k+1}, a_i^{k+2}, \ldots, a_i^l\right\}$$

is an equivalence class of $\sim_\alpha$, which contradicts the fact that C_i is an equivalence class of $\sim_\alpha$. This is a contradiction because $\tilde{C_i}' \subseteq \tilde{C}_i \subset C_i$ and C_i being an equivalence relation means that all elements in C_i are equivalent to i under $\sim_\alpha$; moreover, C_i contains *all* such elements. To say that there exists a subset of C_i that is an equivalence class is to say that ... . Thus, $k = 1$ and $l = n_i$, and

$$\left(a_i^1\ a_i^2\ \cdots\ a_i^{n_i}\right) = \left(a_i^1\ \alpha\left(a_i^1\right)\ \alpha^2\left(a_i^1\right)\ \cdots\ \alpha^{n_i-1}\left(a_i^1\right)\right) = \alpha_i$$

is a cycle of order n_i. Since all C_i are mutually disjoint, it follows that all α_i are disjoint.

We know prove that the product $\alpha = \prod_{i=1}^k \alpha_i = \alpha_1\alpha_2\cdots\alpha_k$ indeed holds. It suffices to show that

$$(\alpha_1\alpha_2\cdots\alpha_k)(j) = \alpha(j)$$

for all $j \in \{1, 2, \ldots, n\}$. Remember that all cycles in the product are mutually disjoint, and the equivalence class C_i corresponds to the cycle α_i. Now, without loss of generality, we may take the arbitrary element $j \in C_1$. Since all cycles are mutually disjoint, we have that $\alpha_i(j) = j$ for all $2 \leq i \leq k$, i.e., only α_1 moves j, which should be clear by definition of disjoint cycles. Then,

$$(\alpha_1 \alpha_2 \cdots \alpha_k)(j) = \alpha_1(j)$$

since, as mentioned, all cycles other than α_1 fix j. But by the above arguments, we have

$$\alpha_1 = \left(a_1^1 \ \alpha\left(a_1^1\right) \ \cdots \ \alpha^{n_1-1}\left(a_1^1\right)\right),$$

(where $a_1^1 \in C_1$), though due to the cyclic nature of cycle notation, we may just as easily take

$$\alpha_1 = \left(j \ \alpha(j) \ \cdots \ \alpha^{n_1-1}(j)\right),$$

so that $\alpha_1(j) = \alpha(j)$. Hence,

$$\alpha = \alpha_1 \alpha_2 \cdots \alpha_k,$$

and so we have shown that each equivalence class C_i corresponds to a cycle as per the definition state earlier, that these cycles are disjoint, and that the product of these cycles indeed gives us the desired element in S_n. So the pf is complete. ■

Lemma 7.2.1 Suppose $\alpha, \beta, \gamma \in S_n$.

1. Let $\alpha = \beta\gamma$, where β and γ are disjoint. If β moves i, then $\alpha^k(i) = \beta^k(i)$ for all $k \geq 0$.
2. Let α and β be cycles not necessarily of the same length. If there is an i_1 moved by both α and β and if $\alpha^n(i_1) = \beta^n(i_1)$ for all positive integers n, then $\alpha = \beta$.

Proof:

1. This follows from Theorem 7.1.3 since if β moves i, then by definition of disjoint cycles γ must fix i, i.e., $\gamma(i) = i$, which means that we must have $\gamma^k(i) = i$ for all $k \geq 0$.
2. Suppose
$$\alpha = (a_1 \ a_2 \ \cdots \ a_k) \quad \text{and} \quad \beta = (b_1 \ b_2 \ \cdots \ b_l).$$
which we may also write as
$$\alpha = \left(a_1 \ \alpha(a_1) \ \cdots \ \alpha^{k-1}(a_1)\right) \quad \text{and} \quad \beta = \left(b_1 \ \beta(b_1) \ \cdots \ \beta^{l-1}(a_1)\right).$$
Now, suppose $i_1 \in \{a_1, a_2, \ldots, a_k\}$ and $i_1 \in \{b_1, b_2, \ldots, b_l\}$. Then, we may write
$$\alpha = \left(i_1 \ \alpha(i_1) \ \cdots \ \alpha^{k-1}(i_1)\right) \quad \text{and} \quad \beta = \left(i_1 \ \beta(i_1) \ \cdots \ \beta^{l-1}(i_1)\right).$$
By hypothesis, $\alpha^n(i_1) = \beta^n(i_1)$ for all positive integers n. We now show that we must have $k = l$, i.e., α and β must be of the same size. For suppose $k \neq l$, and without loss of generality, assume $k > l$.

■

Theorem 7.2.6 Uniqueness of Disjoint Factorisation

For every element $\alpha \in S_n$, the disjoint cycle factorisation is unique up to the order of the cycles.

PROOF: Let

$$\alpha = \alpha_1\alpha_2\cdots\alpha_k \quad \text{and} \quad \alpha = \beta_1\beta_2\cdots\beta_l$$

be two factorisations of α into disjoint cycles. To show that the factorisation is unique, it suffices to show that ■

7.3 Conjugacy Classes

We first mentioned conjugate elements of a group G when we talked about normal subgroups. It was then mentioned in a remark that elements that mutually conjugate can be used to partition the group G. We now develop this theory. We first restate the definition of conjugate elements.

Definition 7.3.1 Conjugate Group Element

Let G be a group and $a, b \in G$. We say that a is **conjugate** to b by g if there exists a $g \in G$ such that the conjugate of a by g is equal to b, i.e., if $gag^{-1} = b$. Observe that if a is conjugate to b, then indeed b is conjugate to a since $gag^{-1} = b$ implies $a = g^{-1}bg$, which we can write as $a = g^{-1}b\left(g^{-1}\right)^{-1}$.

Theorem 7.3.1

Let G be a group and $a, b \in G$. The relation $\sim$, defined as $a \sim b \Leftrightarrow \exists g\ gag^{-1} = b$, i.e., $a \sim b$ if and only if a is conjugate to b by some $g \in G$, is an equivalence relation.

PROOF: As usual, we go through the three requirements of an equivalence relation.

1. (Reflexivity) Let $g = 1_G$. Then, since $1_G a 1_G^{-1} = a$ for all $a \in G$, so that $a \sim a$.
2. (Symmetry) Let $a \sim b$, i.e., $gag^{-1} = b$ for some $g \in G$. Then $a = g^{-1}bg = g^{-1}b\left(g^{-1}\right)^{-1}$, so that $b \sim a$ by definition.
3. (Transitivity) Let $a \sim b$ and $b \sim c$. Then there exists $g_1, g_2 \in G$ such that $g_1 a g_1^{-1} = b$ and $g_2 b g_2^{-1} = c$. But then $b = g_2^{-1}cg_2$, so that $g_1 a g_1^{-1} = g_2^{-1}cg_2 \Rightarrow g_2 g_1 a g_1^{-1} = cg_2 \Rightarrow g_2 g_1 a g_1^{-1} g_2^{-1} = c = g_2 g_1 a \left(g_2 g_1\right)^{-1}$, and since $g_2 g_1 \in G$, we have by definition $a \sim c$.

Having shown that $\sim$ satisfies the three properties of an equivalence relation, the pf is complete. ■

Definition 7.3.2 Conjugacy Class

The conjugation equivalence relation $\sim$ can be used to partition the group G into disjoint subsets, which we are called equivalence classes. In the case of conjugation, the equivalence classes are called **conjugacy classes**.

Let us now focus specifically on S_n. Recall that if $\alpha \in S_n$ is an l-cycle, then $o(\alpha) = l$. Also, if $\alpha = \alpha_1\alpha_2\cdots\alpha_k$, where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are disjoint cycles such that $o(\alpha_1) = n_1, o(\alpha_2) = n_2, \ldots, o(\alpha_k) = n_k$, then the cycle structure of α is $[n_1, n_2, \ldots, n_k]$ and $o(\alpha) = \text{lcm}(n_1, n_2, \ldots, n_k)$. Now consider the following two questions:

1. Given a cycle structure $[n_1, n_2, \ldots, n_k]$, how many elements in S_n have this cycle structure?
2. How many conjugacy classes are there in S_n and what is the size of each conjugacy class?

Recall that we actually have already answered the first question in section 4.3.1, with the formula given in 4.1. We restate it here, with different notation. We have the cycle structure $[n_1, n_2, \ldots, n_k]$, with the requirement that $\sum_{i=1}^{k} n_i = n$. Also, for all $1 \leq m \leq n$, let l_m denote the number of elements in the cycle structure equal to m, where m, remember, is the length of a cycle (and the maximum possible length of a cycle is of course n). Therefore:

The number of elements in S_n with cycle structure $[n_1, n_2, \ldots, n_k]$ is $\dfrac{n!}{\prod_{m=1}^{n} m^{l_m} l_m!}$.

Example 7.3.1 In S_9 how many elements have the cycle structure $[3, 3, 1, 1, 1]$?

SOLUTION: One possible permutation with this cycle structure is $(1\ 2\ 3)\,(4\ 5\ 6)\,(7)\,(8)\,(9)$, although we know, of course, that the last three 1-cycles do not need to be written. To answer the question, we simply use the formula above. We get

$$\frac{9!}{\prod_{m=1}^{9} m^{l_m} l_m!} = \frac{9!}{(1^3 3!)\,(2^0 0!)\,(3^2 2!)\,(4^0 0!)\,(5^0 0!)\,(6^0 0!)\,(7^0 0!)\,(8^0 0!)\,(9^0 0!)} = 3360.$$

So there are 3360 elements in S_9 with the cycle structure $[3, 3, 1, 1, 1]$.

Let us know answer the second question.

Example 7.3.2 In S_5, let $\alpha = (1\ 2\ 3)$ and $\beta = (1\ 2)\,(4\ 5)$. What is the conjugate of α by β, i.e., what is $\beta\alpha\beta^{-1}$?

SOLUTION: Let $\gamma = \beta\alpha\beta^{-1}$, and let $i \in \{1, 2, 3, 4, 5\}$. Then,

$$\gamma(\beta(i)) = \beta\alpha\beta^{-1}(\beta(i)) = \beta\left(\alpha\left(\beta^{-1}\beta(i)\right)\right) = \beta(\alpha(i)).$$

Now,

$$\begin{aligned}
\gamma(\beta(1)) &= \beta(\alpha(1)) = \beta(2)\\
\gamma(\beta(2)) &= \beta(\alpha(2)) = \beta(3)\\
\gamma(\beta(3)) &= \beta(\alpha(3)) = \beta(1)\\
\gamma(\beta(4)) &= \beta(\alpha(4)) = \beta(4)\\
\gamma(\beta(5)) &= \beta(\alpha(5)) = \beta(5).
\end{aligned}$$

so that

$$\gamma = \beta\alpha\beta^{-1} = (\beta(1)\ \ \beta(2)\ \ \beta(3))(\beta(4))(\beta(5)) = (2\ 1\ 3)(5)(4),$$

which has the same cycle structure as α!

The example above has illustrated the following theorem.

Theorem 7.3.2

If $\alpha = (a_1\ a_2\ \cdots\ a_l) \in S_n$ is an l-cycle, then is conjugate by any $\beta \in S_n$ is

$$\beta\alpha\beta^{-1} = (\beta(a_1)\ \ \beta(a_2)\ \ \cdots\ \beta(a_l)).$$

In particular, $\beta\alpha\beta^{-1}$ has the same cycle structure as α, i.e., *conjugation preserves cycle structure.*

The theorem says that if any two elements $\alpha, \beta \in S_n$ are conjugates, then they have the same cycle structure. The converse is true as well.

Theorem 7.3.3

If $\alpha, \beta \in S_n$ have the same cycle structure, then α and β are conjugates.

Proof: Let

$$\begin{aligned}
\alpha &= (a_1\ a_2\ \cdots\ a_l)(b_1\ b_2\ \cdots\ b_k)\cdots,\\
\beta &= \left(a'_1\ a'_2\ \cdots\ a'_l\right)\left(b'_1\ b'_2\ \cdots\ b'_k\right)\cdots.
\end{aligned}$$

Now, define $g \in S_n$ as

$$g = \begin{pmatrix} a_1 & a_2 & \cdots & a_l & b_1 & b_2 & \cdots & b_k & \cdots\\ a'_1 & a'_2 & \cdots & a'_l & b'_1 & b'_2 & \cdots & b'_k & \cdots \end{pmatrix}.$$

Then, using the above theorem, the conjugate of α by g is

$$\begin{aligned}
g\alpha g^{-1} &= (g(a_1)\ \ g(a_2)\cdots g(a_l))(g(b_1)\ \ g(b_2)\ \ \cdots g(b_k))\\
&= \left(a'_1\ a'_2\ \cdots\ a'_l\right)\left(b'_1\ b'_2\ \cdots\ b'_k\right)\\
&= \beta,
\end{aligned}$$

i.e., we have found a $g \in S_n$ such that $g\alpha g^{-1} = \beta$, so $\alpha \sim \beta$, as required. ■

So all elements of a particular cycle structure are conjugate to each other, and if two elements are known to be conjugate to one another, then we may immediately conclude that they have the same cycle structure. In other words, there is a one-to-one correspondence betweeen conjugate elements of S_n and their cycle structures, so that every cycle structure acts as a "label" for a conjugacy class. This immediately answers the second question:

> The number of conjugacy classes in S_n is equal to the number of its cycle structures. The size of each conjugacy class is equal to the number of elements with the corresponding cycle structure.

But how can we determine the number of cycle structures, and hence the number of conjugacy classes, of S_n?

Example 7.3.3 How many cycle structures are possible in S_6?

SOLUTION: We simply solve this by listing all of them:

$$[6]\,,\ \ [5,1]\,,\ [4,2]\,,\ \ [4,1,1]\,,\ \ [3,3]$$
$$[3,2,1]\,,\ \ [3,1,1,1]\,,\ \ [2,2,2]\,,\ [2,2,1]\,,\ \ [2,1,1,1,1]\,,\ \ [1,1,1,1,1,1]$$

So there are eleven possible cycle structures, which means that there are eleven conjugacy classes in S_6.

You may have noticed that the number of cycle structures in the previous example was simply the number of *partitions* of the natural number 6. This illustrates the following theorem.

Theorem 7.3.4

The number of conjugacy classes of S_n is equal to the number of paritions of the natural number n.

REMARK: In number theory, the number of partitions of the natural number n is denoted $p\,(n)$, where p is called the **partition function**. No closed form formula exists for p. The table below displays some of its values.

n	1	2	3	4	5	6	7	8	9	10
$p\,(n)$	1	2	3	5	7	11	15	22	30	42

There is also the recursion formula attributed to Euler,

$$p\,(n) = p\,(n-1) + p\,(n-2) - p\,(n-5) - p\,(n-7) + \cdots\,,$$

with the convention that $p\,(m) = 0$ for all $m \leq 0$.

7.4 Even and Odd Permutations

We begin with the following observation. Recall that any permutation may be written as a product of disjoint cycles, where each cycle is itself a permutation. Also, a transposition is a cycle of length two, i.e., a 2-cycle.

Lemma 7.4.1 Every cycle $\alpha \in S_n$ can be written as a product of transpositions.

PROOF: Let $\{a_1, a_2, \ldots, a_k\} \in \{1, 2, \ldots, n\}$ such that the cycle $(a_1\ a_2\ \cdots\ a_k) \in S_n$. Then we have simply

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k)\,(a_1\ a_{k-1}) \cdots (a_1\ a_3)\,(a_1\ a_2)$$

as **one** possibility of a factorisation into a product of two cycles. So we are done. ■

Therefore, if $\alpha = (1\ 2\ \cdots\ m)$, then we may write α as a product of $m-1$ transpositions,

$$\alpha = (1\ m)\,(1\ m-1) \cdots (1\ 2)\,.$$

Theorem 7.4.1

Every permutation $\alpha \in S_n$ can be written as a product of transpositions.

PROOF: We already know that any permutation $\alpha \in S_n$ can be written as a product of disjoint cycles, say $\alpha = \alpha_1\alpha_2 \cdots \alpha_k$. By the lemma, each cycle can be written as a product of two cycles, and so the product of all the cycles will result in a product of transpositions. ■

Note that, unlike the decomposition of a permutation into disjoint cycles, the decompositions into transpositions is in general *NOT* unique, neither in terms of the factors themselves or the number of factors; for example,

$$\begin{aligned}(1\ 2\ 3) &= (1\ 3)\,(1\ 2) = (2\ 3)\,(1\ 3)\\ &= (1\ 3)\,(4\ 2)\,(1\ 2)\,(1\ 4)\\ &= (1\ 3)\,(4\ 2)\,(1\ 2)\,(1\ 4)\,(2\ 3)\,(2\ 3)\,.\end{aligned}$$

Definition 7.4.1 Even and Odd Permutations

A permutation $\alpha \in S_n$ is called an **even permutation** if it is a product of an even number of transpositions; otherwise (i.e., if α is a product of an odd number of transpositions), α is called an **odd permutation**.

Theorem 7.4.2

Let $\alpha \in S_n$ be an m-cycle.

1. If m is odd, then α is an even permutation.
2. If m is even, then α is an odd permutation.

PROOF: Since the decomposition of α results in $m-1$ transpositions, as shown above, it is clear that if m is odd, then $m-1$ is even, and if m is even, then $m-1$ is odd. ■

Example 7.4.1 Consider the permutation

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 1 & 7 & 8 & 2 & 6 & 4 & 3 \end{pmatrix} \in S_9.$$

We can write $\alpha = (1\ 9\ 3)\,(2\ 5\ 8\ 4\ 7\ 6)$, which is a decomposition into disjoint cycles. The first cycle is of length three, and so by the previous theorem, it is an even permutation, i.e., it may be written as a product of an even number of permutations. The second is a 6-cycle, which means that it is an odd permutation, i.e., it may be written as a product of an odd number of permutations. Since the sum of an odd and an even number is an odd number, we have that α can be written as an odd number of permutations, and so α is an odd permutation.

Example 7.4.2 Let $\alpha \in S_{16}$ have the cycle structure $[4, 3, 3, 2, 2, 1, 1]$. Then since each m-cycle can be written as a product of $m-1$ transpositions, we get that α can be written as a product of $3+2+2+1+1+0+0 = 9$, which is an odd number. So α is an odd permutation.

Theorem 7.4.3

Let $\alpha \in S_n$ have the cycle structure $[n_1, n_2, \ldots, n_k]$. Then α can be written as a product of $n-k$ transpositions, and hence the parity of α is the same as the parity of $n-k$.

PROOF: Let $\alpha \in S_n$ with cycle structure $[n_1, n_2, \ldots, n_k]$. We know that each m-cycle can be written as a product of $m-1$ transpositions, so we get that α may be written as a product of

$$(n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1) = \sum_{i=1}^{n} n_i - k = n - k$$

transpositions. Therefore, the parity of α (i.e., whether α is an even or an odd permutation) depends on the parity of $n-k$. ■

Since every permutation can be written as a product of disjoint cycles, and since every non-zero integer is either odd or even, it follows that every integer can be odd or even—but can a permutation be both odd and even? We now set out answering this question.

Lemma 7.4.2 Let $a,\ b,\ c,\ d \in \{1, 2, \ldots, n\}$, for arbitrary n, be distinct elements. Then,

1. $(a\ b)\,(c\ d) = (c\ d)\,(a\ b)$;
2. $(a\ b)\,(b\ c) = (b\ c)\,(a\ c)$;
3. $(a\ b)\,(a\ c) = (b\ c)\,(a\ b)$;
4. $(a\ b)\,(a\ b) = () = 1$, where 1 represents the identity permutation (the identity mapping).

PROOF: Verify these. It's easy! ■

Lemma 7.4.3 Suppose $\alpha \in S_n$ is a product of k transpositions. Assume that $a \in \{1, 2, \ldots, n\}$ occurs in at least one transposition. Then either $\alpha\,(a) \neq a$ or α can be written as a product of $k-2$ transpositions.

PROOF: Let $l > 1$ be the number of occurrences of a in α. We use induction of l. Let A be the set of all l such that the result holds.

1. Let $l = 1$, i.e., there is only one occurrence of a in α, so α looks something like

   $$\alpha = \cdots (a\ b) \cdots,$$

   with $a \neq b$ (otherwise we don't have a transposition!). Clearly, then $\alpha\,(a) = b \neq a$, so α moves a, so the result holds. So $1 \in A$.

2. Assume the result holds for $l \leq m$, i.e., $l \in A$ for all $l \leq m$, and suppose $l = m + 1$. Then α looks something like

   $$\alpha = \cdots (a\ b) \cdots (a\ c) \cdots,$$

   where all $a,\ b,\ c,\ d$ are distinct. Now, observe that in Part 3 of the lemma above, the left-hand side contains two occurrences of a while the right-hand side contains only one. We will exploit this fact. Now, using Parts 1 and 2 of the above lemma, we move every transposition containing a to the right until it meets another transposition containing a. Once we have done this, there are two options:

   (a) If the adjacent transpositions are of the form in Part 3 of the lemma, then the number of occurrences of a is decreased by 1, i.e., $l = m$. But since the result holds for m, we have that $m + 1 \in A$, so the result holds by induction and the pf is complete.

   (b) If the adjacent transpositions are of the form in Part 4 of the lemma, then those two transpositions disappear completely, so that we are left with only $k-2$ transpositions. So $m + 1 \in A$, and by induction the result holds, completing the pf. ■

Theorem 7.4.4

Let $\alpha = \alpha_1\alpha_2 \cdots \alpha_k \in S_n$ be a permutation written as a product of k transpositions. The parity of m is unique. In other words, m is only one of odd and even, i.e., α cannot be both odd and even.

REMARK: Hence, no matter how many ways one decomposes α into a product of transpositions, the parity of the number of transpositions will always be the same, i.e., if α is even in one representation, then it will be even in all representations.

PROOF: Let

$$\begin{aligned}\alpha &= \alpha_1\alpha_2\cdots\alpha_l \\ &= \alpha_1'\alpha_2'\cdots\alpha_m',\end{aligned}$$

be two decompositions of α into a product of transpositions such that k is odd and m is even. Then, since all transpositions are self-inverses (verify this for yourself!),

$$\alpha_1\alpha_2\cdots\alpha_k = \alpha_1'\alpha_2'\cdots\alpha_m' \Rightarrow \alpha_1'\alpha_2'\cdots\alpha_m'\alpha_k\alpha_{k-1}\cdots\alpha_1 = (),$$

where () is the identity permutation. Now, since the sum of an odd and even number is odd, we have written the identity element as a product of an odd number of transpositions. Call this number $k = l + m$, and suppose that k is the smallest such number (i.e., the smallest number number of odd permutations whose product is the identity element). Since k is odd, there is at least one transposition in the product. Now, since the identity permutation fixes any element in $\{1, 2, \ldots, n\}$, we must have that $()(i) = i$ for any $i \in \{1, 2, \ldots, n\}$, including any i that occur in the transpositions. By the lemma, then, since i is not moved by the identity, we must have that the identity can be written as a product of $k - 2$ transpositions, a contradiction to the minimality of k. So k must not be odd, hence it must be even, and since $k = l + m$, either l and m are both odd or they are both even. So the pf is complete. ■

7.5 The Alternating Group A_n

Theorem 7.5.1

Let $\alpha = \alpha_1\alpha_2\cdots\alpha_k$ be a decomposition of α into k transpositions. Define a mapping

$$\text{sgn} : S_n \to \mathbb{Z}_2 \quad \text{by} \quad \text{sgn}(\alpha) = [k]_2.$$

sgn (read "signum") is a well-defined function and a surjective (onto) homomorphism.

PROOF: We first prove that sgn is a well-defined mapping. Let $\alpha = \alpha_1\alpha_2\cdots\alpha_k$ and $\alpha_1'\alpha_2'\cdots\alpha_m'$ be two ways of writing $\alpha \in S_n$ as a product of transpositions. Then, since the parity of k and m must be the same, we have

$$\text{sgn}(\alpha_1\alpha_2\cdots\alpha_k) = [k]_2 = [m]_2 = \text{sgn}\left(\alpha_1'\alpha_2'\cdots\alpha_m'\right),$$

so sgn is well defined.

Now, let $\beta = \beta_1\beta_2\cdots\beta_l \in S_n$. Then,

$$\text{sgn}(\alpha\beta) = \text{sgn}(\alpha_1\alpha_2\cdots\alpha_k\beta_1\beta_2\cdots\beta_l) = [k+l]_2 = [k]_2 + [l]_2 = \text{sgn}(\alpha)\,\text{sgn}(\beta),$$

so that sgn is indeed a homomorphism.

Finally, sgn is quite clearly onto since sgn is simply counting the number of transpositions in the decomposition of α, and hence must be either even or odd (but not both, as we have seen). ■

Let us know determine the kernel of sgn. We have

$$\begin{aligned}\text{Kern}\,(\text{sgn}) &= \{\alpha \in S_n \mid \text{sgn}\,(\alpha) = [0]_2\} \\ &= \{\alpha \in S_n \mid \alpha \text{ is an even permutation}\}\,.\end{aligned}$$

So the kernel of sgn is the set of all even permutations in S_n. We also know that the kernel is a subgroup of the domain, so that $\text{Kern}\,(\text{sgn}) \trianglelefteq S_n$, and hence we may consider the quotient group ${}^{S_n}\!/_{\text{Kern}\,(\text{sgn})}$. In particular, the first isomorphism theorem gives

$${}^{S_n}\!/_{\text{Kern}\,(\text{sgn})} \cong \mathbb{Z}_2 \Rightarrow \left|{}^{S_n}\!/_{\text{Kern}\,(\text{sgn})}\right| = \frac{|S_n|}{|\text{Kern}\,(\text{sgn})|} = |\mathbb{Z}_2| = 2.$$

Definition 7.5.1 **The Alternating Group A_n**

The kernel of sgn, which consists of all the even permutations of S_n, is called the **alternating group of degree** n, and is denoted A_n.

So we have

$$\boxed{A_n \trianglelefteq S_n \text{ and } [S_n : A_n] = 2.}$$

Lemma 7.5.1 Let $\alpha \in S_n$ be an even permutation. If α commutes with an odd permutation, then all permutations with the cycle structure as α are conjugate in A_n.

PROOF: We know that all permutations with the same cycle structure as α are conjugates in S_n. Let β be an odd permutation that commutes with α. For any odd permutation γ, the product $\gamma\beta$ is an even permutation (since the sum of two odd numbers is even), and hence

$$(\gamma\beta)\,\alpha\,(\gamma\beta)^{-1} = \gamma\beta\alpha\beta^{-1}\gamma^{-1} = \gamma\alpha\beta\beta^{-1}\gamma^{-1} = \gamma\alpha\gamma^{-1},$$

so any conjugate of α by an odd permutation is also a conjugate of α by an even permutation. Therefore, the permutations with the same cycle structure as α remain conjugate in A_n. ■

Lemma 7.5.2 Any even permutation can be written as a product of 3-cycles.

PROOF: Start by writing an even permutation as a product of transpositions. Consider the first pair of transpositions $(a\ b)\,(c\ d)$ in this product. If $b = c$, then $(a\ b)\,(c\ d) = (a\ d\ b)$ is a 3-cycle. Otherwise,

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

is a product of 3-cycles. Continuing with the remaining pairs, we can express the even permutation as a product of 3-cycles. ■

Now, we have that all 3-cycles are even permutations because they may be written as a product of two transpositions. Therefore, all the 3-cycles in S_n will be elements of A_n. We now show that these 3-cycles are enough to *generate* A_n.

Theorem 7.5.2

For $n \geq 3$, A_n is generated by the 3-cycles of S_n. (We assume that $n \geq 3$ simply to ensure that A_n is non-trivial. When $n \leq 2$, A_n is the trivial group.)

PROOF: We have that A_n is the subgroup of S_n consisting of all the even permutations, which means that any element in A_n may be written as a product of an even number of transpositions. We also have that all 3-cycles are even because they may be written as a product of two transpositions. From the lemma above, we have that any even permutation, i.e., any product of 2-cycles, can be written as a product of 3-cycles. Therefore, all the elements of A_n are some product of 3-cycles, which means that A_n is generated by the set of 3-cycles of S_n. This completes the pf. ■

REMARK: We can also show that A_n is generated by the 5-cycles of S_n.

Theorem 7.5.3

If $n \geq 4$ and $N \trianglelefteq A_n$, with $N \neq \{()\}$, and if N contains a 3-cycle, then $N = A_n$.

REMARK: Again, we ignore all $n \leq 2$ because the corresponding A_n is trivial. We don't include $n = 3$ for the following reason: recall that

$$S_3 = \{(), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (3\ 2\ 1)\},$$

and that $A_3 = \langle(1\ 2\ 3)\rangle = \{(), (1\ 2\ 3), (3\ 2\ 1)\}$. Now, $|A_3| = 3$, and since all groups of order three are Abelian, we have that A_3 is Abelian, and hence all of its subgroups are normal. In particular, $N = \{(), (1\ 2\ 3)\} \trianglelefteq A_3$. So we have $N \trianglelefteq A_3$ with $N \neq \{()\}$ containing a 3-cycle—yet $N \neq A_3$! So the theorem does not apply for $n = 3$.

PROOF: Let $n \geq 4$ and $N \trianglelefteq A_n$ such that $N \leq \{()\}$ and N contains a 3-cycle. We have just shown that for all $n \geq 3$, A_n is generated by 3-cycles—in particular, that A_n contains all 3-cycles, since all 3-cycles are even. So to show that $N = A_n$, it suffices to show that all 3-cycles of S_n are contained in N. Without loss of generality, assume $\alpha = (1\ 2\ 3) \in N$ is the 3-cycle in N. Since N is a group, we must have $\alpha^2 = (1\ 3\ 2) \in N$. Also, since N is normal in A_n, all of the elements of N must be even permutations, hence writable as an even product of transpositions. Suppose, then, that

$$\beta = \cdots (1\ i)\,(2\ j)\,(3\ k) \cdots \in A_n,$$

for any $i, j, k \in \{1, 2, \ldots, n\}$ with $i, j, k \neq 1, 2, 3$. Then,

$$\beta\alpha^2\beta^{-1} = (\beta\,(1)\ \ \beta\,(3)\ \ \beta\,(2)) = (i\ k\ j) \in N.$$

(Observe that by our construction of α and β it does not matter what elements are contained in the other transpositions that make up β since they do not contribute to the evaluation of β at 1,

2 and 3. In other words, for any element $\beta \in A_n$ that is expressed a product of transpositions, only those transpositions in the product that contain the elements of α matter in computing the conjugate.) So we see that the conjugate of the 3-cycle $\alpha \in N$ by any element $\beta \in A_n$ gives rise to a 3-cycle completely distinct from α. Therefore, N contains all 3-cycles, and hence $N = A_n$. ■

7.6 The Simplicity of A_n

The purpose of this section is to prove that for all $n \geq 5$, the alternating group A_n is simple, with the definition of a simple group given below.

Definition 7.6.1 Simple Group

A group G with no non-trivial normal subgroups, i.e., a group with only the trivial groups $\{1_G\}$ and G as the normal subgroups, is called a **simple group**.

Theorem 7.6.1

Any cyclic group of prime order, which we know is isomorphic to $\mathbb{Z}_p$ for p a prime number, is a simple group.

PROOF: Let G be a cyclic group of order p, where p is a prime number. If H is any subgroup of G, then by Lagrange's theorem, since $|H|$ must divide $|G| = p$, we must have either $|H| = 1$ or $|H|$. So the only subgroups, and certainly then the only normal subgroups, of G are the trivial subgroup $\{1_G\}$ and G itself. So G is a simple group. ■

Theorem 7.6.2

An Abelian group is simple if and only it is isomorphic to $\mathbb{Z}_p$. In other words, $\mathbb{Z}_p$ is the only simple Abelian group.

PROOF: Let G be an Abelian group.

($\Rightarrow$): Assume G is simple. Then its only normal subgroups are $\{1_G\}$ and G.

($\Leftarrow$): Assume G is cyclic of prime order. Then the above theorem has already shown that G is simple. ■

Example 7.6.1 Note that the group A_4 is not a simple group, since the subgroup $H = \{(), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \trianglelefteq A_4$. A_3 is also not a simple group, since we have already seen that $A_3 = \langle b \rangle \trianglelefteq A_3$. A_2 is also not simple since it only has two elements, the permutation (1 2) and (), the identity, and hence are its only normal subgroups. Finally, A_1 is the trivial group, so it has no normal subgroups.

Theorem 7.6.3

For $n \geq 5$, A_n is a simple group.

PROOF: Let $H \trianglelefteq A_n$, with $H \neq \{()\}$. We have already seen in Theorem 7.5.3 , if H contains a 3-cycle, then $H = A_n$. And since we are assuming that $H \neq \{()\}$, then to show that $H = A_n$ it suffices to show that H contains a 3-cycle. Let some $\alpha \in H$ have the cycle structure $[n_1, n_2, \dots]$. By convention, we write the cycle structure in decreasing order. We split up the pf into cases for the number of elements in the longest cycle of α.

Case 1 $n_1 \geq 4$

Without loss of generality, assume that $\alpha = (1\ 2\ 3\ \cdots\ m)\cdots$, $m \geq 4$. Let $\beta = (1\ 2\ 3)$. Therefore,

$$\begin{aligned}\gamma = \beta\alpha\beta^{-1} &= (1\ 2\ 3)\,[(1\ 2\ 3\ \cdots\ m)\cdots]\,(1\ 2\ 3)^{-1} \\ &= (1\ 2\ 3)\,(1\ 2\ 3\ \cdots\ m)\,(1\ 3\ 2) \\ &= (2\ 3\ 1\ \cdots\ m)\cdots \in H,\end{aligned}$$

since H is a normal subgroup. Then, since γ and α are in H, in particular since $\alpha^{-1} \in H$, we have $\gamma\alpha^{-1} \in H$, where

$$\gamma\alpha^{-1} = (2\ 3\ 1\ \cdots\ m)\cdots(1\ m\ m-1\ \cdots\ 3\ 2)\cdots = (1\ 2\ 4) \in H.$$

So H contains a 3-cycle, hence by Theorem 7.5.3, $H = A_n$.

Case 2 $n_1 = 3$

In this case, the cycle structure of α is something like

$$[3, 3, \dots, 2, 2, 2, \dots, 1, 1, \dots].$$

Since all two cycles are of order two, we may square α to get rid of all the two cycles (the square of α is of course still in H). So we may assume that α has no 2-cycles, so that the cycle structure is $[3, 3, \dots, 1, 1 \dots]$. We also assume, without loss of generality, that α contains more than one 3-cycle, otherwise α would itself be a 3-cycle, and we would be done by Theorem 7.5.3. Suppose without loss of generality that

$$\alpha = (1\ 2\ 3)\,(4\ 5\ 6)\cdots.$$

Let $\beta = (1\ 2\ 4)$. Then

$$\gamma = \beta\alpha\beta^{-1} = (1\ 2\ 4)\,[(1\ 2\ 3)\,(4\ 5\ 6)\cdots]\,(1\ 4\ 2) = (2\ 4\ 3)\,(1\ 5\ 6)\cdots \in H.$$

Then,

$$\gamma\alpha^{-1} = [(2\ 4\ 3)\,(1\ 5\ 6)\cdots]\,[(3\ 2\ 1)\,(6\ 5\ 4)\cdots] = (1\ 2\ 5\ 3\ 4) \in H,$$

which is a 5-cycle, a cycle of the type considered in Case 1. Therefore, the result holds.

Case 3 $n_1 = 2$

In this case, the cycle structure of α is something like

$$[2, 2, \dots, 2, 1, 1, \dots].$$

We consider two subcases here:

1. Without loss of generality, assume $\alpha = (1\ 2)\,(3\ 4)$. Then, let $\beta = (1\ 3)\,(2\ 5)$. Then

$$\gamma = \beta\alpha\beta^{-1} = (1\ 3)\,(2\ 5)\,(1\ 2)\,(3\ 4)\,(1\ 3)\,(2\ 5) = (3\ 5)\,(1\ 4) \in H.$$

   Then $\gamma\alpha^{-1} = (3\ 5)\,(1\ 4)\,(1\ 2)\,(3\ 4) = (1\ 2\ 4\ 5\ 3) \in H$, a 5-cycle, so we are again back to Case 1, and the result holds.

2. Without loss of generality, assume $\alpha = (1\ 2)\,(3\ 4)\,(5\ 6)\,(7\ 8)\ldots$. Then, let $\beta = (1\ 3)\,(2\ 5)$. Then,

$$\gamma = \beta\alpha\beta^{-1} = (3\ 5)\,(1\ 4)\,(2\ 6)\,(7\ 8)\ldots$$

   and hence

$$\gamma\alpha^{-1} = [(3\ 5)\,(1\ 4)\,(2\ 6)\,(7\ 8)\ldots]\,[(1\ 2)\,(3\ 4)\,(5\ 6)\,(7\ 8)\ldots] = (1\ 6\ 3)\,(2\ 4\ 5)\,,$$

   which is a product of 3-cycles, a permutation of the kind considered in Case 2. So the result holds here as well. ■

Theorem 7.6.4

$\{()\}$, A_n, and S_n are the only normal subgroups of S_n for $n \geq 5$.

PROOF: The identity $\{()\}$ and S_n are always normal subgroups of S_n. Now, let $N \trianglelefteq S_n$. Then $N \cap A_n \trianglelefteq A_n$, and so $N \cap A_n$ is either A_n or $\{()\}$ because A_n is simple for $n \geq 5$. In the case $N \cap A_n = A_n$, we find that $A_n \subseteq N \subseteq S_n$ and, by considering the indices of the subgroups in one another, we conclude that $N = A_n$ or $N = S_n$, since $2 = [S_n : A_n] = [S_n : N]\,[N : A_n]$. In the second case, assume for a contradiction that $N \neq \{()\}$. Then, because

$$n! = |S_n| \geq |A_n N| = \frac{|A_n|\,|N|}{|A_n \cap N|},$$

we get that $|N| = 2$. Thus, $N = \{1, \alpha = \alpha_1\alpha_2\cdots\alpha_r\}$, where each α_i are mutually disjoint. Since N is of order two, we must have $\alpha^2 = 1$, which means that each α_i is a transposition. Let us write $\alpha_i = (a_i\ b_i)$. Now, it is easy to see that we can find a different permutation $\beta = \beta_1\beta_2\cdots\beta_r \neq \alpha$, which is a product of disjoint transpositions $\beta_i = (c_i\ d_i)$. Now, if we take γ to be the permutation taking a_i to c_i, b_i to d_i, and fixing any other element of $\{1, 2, \ldots, n\}$, then $\gamma\alpha\gamma^{-1} = \beta \notin N$. So N cannot be normal, a contradiction. So $N = \{()\}$. This completes the pf. ■

8 Finite Abelian Groups

In this chapter, we show how finite Abelian groups can be completely described in terms of direct products of some cyclic groups. We will be able to list all Abelian groups of a given finite order. Since we know how to construct subgroups of cyclic groups and how to calculate the order of an element in cyclic groups, we will be able to do the same for any finite Abelian group.

Theorem 8.0.5 Cauchy's Theorem, Abelian Case

Let G be a finite Abelian group and p a prime number such that p divides $|G|$. Then there exists an element $g \in G$ such that $o(g) = p$.

PROOF: We perform induction on $|G|$. Note that if $|G| = p$, then by Lagrange's theorem, G is cyclic and necessarily has an element of order p, namely, the generator, and so we are done.

Now, let $|G| = n$ and suppose that the result holds for all Abelian groups of order less than or equal to n. Let $h \in G$ be some non-identity element. Then, by the unique prime factorisation theorem, $q \mid o(h)$ for some prime number q. In particular, $o(h) = kq$ for some $k \in \mathbb{Z}$. Then,

$$o\left(h^k\right) = \frac{kq}{\gcd(k, kq)} = q.$$

If $q = p$, then the element $h^k \in G$ has order p, and we are done.

Suppose, then, that $p \neq q$. Consider the cyclic subgroup $\left\langle h^k \right\rangle$, which is normal since G is normal, and the quotient group $G/\langle h^k \rangle$. Then,

$$|G/\langle h^k \rangle| = \frac{|G|}{|\langle h^k \rangle|} = \frac{n}{q} \leq n.$$

Since G is Abelian, so is $G/\langle h^k \rangle$, which means that $G/\langle h^k \rangle$ is an Abelian group of order less than n; hence, by the induction hypothesis, the result holds for $G/\langle h^k \rangle$, and there exists an element $g' = \left\langle h^k \right\rangle g \in G/\langle h^k \rangle$ such that $o(g') = p$, i.e.,

$$(g')^p = \left(\left\langle h^k \right\rangle g\right)^p = \left\langle h^k \right\rangle g^p = \left\langle h^k \right\rangle \Rightarrow g^p \in \left\langle h^k \right\rangle.$$

Then, as a result of Lagrange's theorem,

$$(g^p)^{\left|\langle h^k \rangle\right|} = (g^p)^{o\left(h^k\right)} = (g^p)^q = g^{pq} = 1_G \Rightarrow o(g) \mid pq \Rightarrow pq = mo(g),\ m \in \mathbb{Z}.$$

Now, we must have $m \neq p$ since $o(g) = q \Rightarrow \left(\left\langle h^k \right\rangle g\right)^q = \left\langle h^k \right\rangle g^q = \left\langle h^k \right\rangle \Rightarrow p \mid q \Rightarrow p = q$, a contradiction to the assumption that $p \neq q$. On the other hand, if $m = q$, then $o(g) = p$, and we are done.

If $m \neq q$, consider the element $g^q \in G$. Then, from above, $(g^q)^p = 1_G \Rightarrow o(g^q) \mid p$, which implies that $o(g^q) = 1$ or $o(g^q) = p$. Suppose $o(g^q) = 1 \Rightarrow g^q = 1_G \Rightarrow \left(\left\langle h^k \right\rangle g\right)^q = \left\langle h^k \right\rangle g^q = \left\langle h^k \right\rangle \Rightarrow p \mid q \Rightarrow p = q$, again, a contradiction. So we have $o(g^q) = p$, and we are done. ■

Recall that at the end of section 3.4 we introduced the set HK, where H and K were two *subsets* of the group G. Let us restate some of the result from there.

Definition 8.0.2

Let H and K be two subsets of a group G. Define

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

We may similarly define the subset KH.

It it certainly possible for H and K to be *subgroups* but for HK or KH to not be subgroups. It is also possible that H and K are merely subsets but for HK to be a subgroup.

Example 8.0.2 Find a group G and subgroups H and K such that HK is not a subgroup of G.

Solution: Let $G = S_3$, $H = \langle a \rangle = \{1, a\} \leq G$ and $K \langle ab \rangle = \{1, ab\} \leq G$. Then,

$$HK = \left\{1, ab, a, a^2b\right\} \text{ and } KH = \left\{1, ab, a, b^2\right\}.$$

Now, since $|HK| = |KH| = 4 \nmid 6$, we have that neither HK nor KH are subgroups of G.

Theorem 8.0.6

Let H and K be subgroups of a group G, and assume $H \trianglelefteq G$. Then $HK \leq G$.

Proof: See section 3.5. ■

Theorem 8.0.7

Let G be an Abelian group and $H, K \leq G$. Then $HK \leq G$.

Proof: See section 3.5. ■

Theorem 8.0.8

Let G be a finite group and $H, K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.

Proof: ($\Rightarrow$): Assume that HK is a subgroup of G and let $x \in HK$ be arbitrary. We must

show that $HK \subseteq KH$ and $KH \subseteq HK$. Now, $x^{-1} \in HK$, where we may write $x^{-1} = hk$ for some $h \in H$ and $k \in K$. But then $x = \left(x^{-1}\right)^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$, so $HK \subseteq KH$ since x is arbitrary. Similarly, we may show that if $y \in KH$, then $y \in HK$, establishing that $KH \subseteq HK$. Therefore, $HK = KH$.

($\Leftarrow$): Assume that $HK = KH$. We want to show that HK is a subgroup of G.

1. Since H and K are subgroups, we have $1_G \in H$ and $1_G \in K$, so $1_G \in HK$.
2. Let $x, y \in HK$, so that $x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2, \in K$. Hence, since $HK = KH$, we have $k_1h_2 = h_2'k_1'$ for some $k_1' \in K$ and $h_2' \in H$. Therefore, $xy = h_1k_1h_2k_2 = h_1h_2'k_1'k_2$. But then $h_1h_2' = h_3 \in H$ and $k_1'k_2 = k_3 \in K$. So $xy = h_3k_3$, i.e., $xy \in HK$.
3. For all $x \in HK$, we have $x = hk$ for some $h \in H$ and $k \in K$. Then $x^{-1} = k^{-1}h^{-1}$; but again, since $HK = KH$, we have $k^{-1}h^{-1} = h'k'$ for some other $h' \in H$ and $k' \in K$. Therefore, $x^{-1} = h'k'$, i.e., $x^{-1} \in HK$.

So, by the subgroup test, we have established that $HK \leq G$, and so the pf is complete. ■

Theorem 8.0.9

If H and K are (normal) subgroups of G, then so is $H \cap K$.

PROOF: Assume $H, K \leq G$.

1. Then $1_G \in H$ and $1_G \in K$, so $1_G \in H \cap K$, so $H \cap K$ is not empty.
2. Let $g_1, g_2 \in H \cap K$, i.e., $g_1, g_2 \in H$ and $g_1, g_2 \in K$. Since H and K are subgroups, we have $g_1g_2 \in H$ and $g_1g_2 \in K$. Therefore, $g_1g_2 \in H \cap K$.
3. Finally, for all $g \in H \cap K$, since H and K are subgroups, we have $g^{-1} \in H$ and $g^{-1} \in K$, so $g^{-1} \in H \cap K$.

So by the subgroup test, we have $H \cap K \leq G$.

Now, assume that $H, K \trianglelefteq G$, and let $g \in H \cap K$. For all $f \in G$, we have $fgf^{-1} \in H$ since H is normal, and $fgf^{-1} \in K$ since K is normal. So $fgf^{-1} \in H \cap K$ for all $f \in G$ and all $g \in H \cap K$. So $H \cap K \trianglelefteq G$. ■

Theorem 8.0.10

Suppose G is a finite group and $H, K \leq G$. Then

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

PROOF: Observe first that in HK, it is possible to have $h_1k_1 = h_2k_2$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Also, recall that

$$H \times K = \{(h, k) \mid h \in H, k \in K\}.$$

Now, define an equivalence relation on $H \times K$ by $(h_1, k_1) \sim (h_2, k_2) \Leftrightarrow h_1k_1 = h_2k_2$ (it is easy to show that this is in fact an equivalence relation). So "$\sim$" partitions $H \times K$ into disjoint subsets, which are the equivalence classes. Since every element in HK is of the form hk for $h \in H$ and $k \in K$, we have that the number of equivalence classes of the equivalence relation "$\sim$" is $|HK|$.

Now, let C be one of these equivalence classes. So we have that for all $(h_1, k_1), (h_2, k_2) \in C$ $(h_1, k_1) \sim (h_2, k_2) \Rightarrow h_1k_1 = h_2k_2 \Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} = l$, where $l \in H$ and $l \in K$ (since l has been written as both a product of elements in H and as a product of elements in K). In other words, $l \in H \cap K$. Now, given any $l \in H \cap K$, for any $(h_1, k_2) \in C$, we have $\left(h_1l^{-1}, lk_1\right) \in C$. Thus, there is a one-to-one correspondence between every element in C and every element in $H \cap K$.

Using this, let us define the mappings

$$f : H \cap K \to C \text{ by } f(l) = \left(h_1l^{-1}, lk_1\right)$$
$$g : C \to H \cap K \text{ by } g(h_2, k_2) = h_2^{-1}h_1 = k_2k_1^{-1}$$

Using this, we see that f is an invertible function (and so is g), which means that f (and g) must be bijections, so that $|C| = |H \cap K|$, i.e., the size of each equivalence class is $|H \cap K|$.

Finally, then, since there are $|HK|$ equivalence classes, each of size $|H \cap K|$, and since the equivalence relation partitions the subset $H \times K$, we have

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

as required. ■

We can generalise the above theorem to any number of subgroups. We state the result without pf.

Theorem 8.0.11

Let G be a finite group with $\{H_k\}_{i=1}^n$ a sequence of subgroups of G. Then

$$|H_1H_2 \cdots H_n| = ?$$

8.1 p-Groups

This section is devoted to understanding p-groups (as will be defined below), with the ultimate goal of begin able to classify all finite Abelian p-groups by "isomorphism class".

Definition 8.1.1 ***p*-Group**

Let p be a prime number. If G is a finite group such that $|G| = p^k$ for some $k \in \mathbb{Z}$ with $k \geq 1$, then G is called a **p-group**. If G is an Abelian p-group, then it is also sometimes called a **p-primary group**. We usually denote a p-group by H_p.

REMARK: In case G is infinite, an equivalent defnintion (the equivalence will be established in the following theorem) is that G is a p-group if every element of G has order a power of p.

Theorem 8.1.1

Let G be a finite group and p a prime number. Then G is a p-group if and only if all the elements of G have order a power of p.

PROOF: ($\Rightarrow$): Let G be a p-group. Then, by definition, $|G| = p^k$ for some $k \geq 1$ and $k \in \mathbb{Z}$. Then, for any $g \in G$, and since G is finite, Lagrange's theorem gives that the order of g must divide $|G|$, i.e., $o(g) \mid |G| \Rightarrow o(g) \mid p^k$. In other words, for all $g \in G$, we must have $o(g) = p^j$ for $j \leq k$.

($\Leftarrow$): Suppose

$$G = \left\{ g \in G \mid o(g) = p^j, j \in \mathbb{Z}, \right\},$$

i.e., suppose that G is a group such that all of its elements have order a power of p. Assume for a contradiction that $|G| \neq p^k$, say $|G| = mp^k$ for some $m \in \mathbb{Z}$. So $|G|$ is not divisible by p, but it is divisible still (by the unique prime factorisation theorem) by some other prime number q. Then, by Cauchy's theorem (which has yet to be proved for the non-Abelian case), there exists an order of element q in G. Since $q \nmid p$, we have that there exists an element in G with an order that is not some power of p, a contradiction. So $|G| = p^k$. ■

Theorem 8.1.2

Let G be a finite Abelian group and let p be a prime number such that $|G| = p^k m$, where $m \in \mathbb{Z}$, $\gcd(p, m) = 1$, and $k \geq 1$. Then there exists a unique p-subgroup H_p such that $|H_p| = p^k$.

PROOF: We first establish that H_p is a subgroup of G using the subgroup test. By the previous theorem, let

$$H_p = \{ g \in G \mid o(g) = p^n, n \in \mathbb{Z}, n \geq 0 \}.$$

1. By taking $n = 0$, we see that H contains the identity element, so H_p is not empty.
2. Let $a, b \in H$ and let $o(a) = p^s$ and $o(b) = p^t$ for some $s, t \in \mathbb{Z}$ and $s, t \geq 0$. Then $o(ab) = p^{\max\{s,t\}}$, and so $ab \in H$.

3. It is clear that an element and its inverse have the same order, so for all elements $a \in H$, we have $a^{-1} \in H$.

So by the subgroup test, $H_p \leq G$.

We now establish that $|H| = p^k$. Assume for a contradiction that $|H| \neq p^k$. Then G/H has order divisible by p, and hence there exists an element $Hb \in G/H$ of order p by Cauchy's theorem (Abelian case). Since $o(Hb) = p$, we have $(Hb)^p = 1_G = Hb^p$, which implies that p is the smallest power of b such that $b^p \in H$. In particular, then, $b \notin H$. However, $b^p \in H$ implies that $o(b) = p^s$ for some $s \in \mathbb{Z}$, which implies that $b \in H$, a contradiction to the previous sentence. So we must have $|H| = p^k$.

It remains to be shown that the p-subgroup H_p is unique. It suffices to show that H_p is the only subgroup of G of order p^k. ■

Theorem 8.1.3

Let G be a finite Abelian group and p and q prime numbers such that $p \mid |G|$ and $q \mid |G|$. Then $H_p \cap H_q = \{1_G\}$, where H_p and H_q are p- and q-subgroups of G, respectively, i.e., $|H_p| = p^k$ and $|H_q| = q^n$ for some $k, n \in \mathbb{Z}$.

PROOF: Let $g \in H_p \cap H_q$. Now, $o(g) = p^l$ for some $l \in \mathbb{Z}$ and $l \geq 0$ since $g \in H_p$. But also $o(g) = q^m$ for some $m \in \mathbb{Z}$ and $m \geq 0$ since $g \in H_q$. So we must have

$$p^l = q^m \Rightarrow l = m = 0 \Rightarrow o(g) = 1 \Rightarrow g = 1_G,$$

so $H_p \cap H_q = \{1_G\}$, as required. ■

Lemma 8.1.1 Let G be a group and $H, K \leq G$. Define $f : H \times K \to G$ by $f(h,k) = hk$ for all $(h,k) \in H \times K$. Then f is a homomorphism if and only if every element of H commutes with every element of K.

PROOF: ($\Rightarrow$): Suppose f is a homomorphism. Then, for all $h_1, h_2 \in H$ and all $k_1, k_2 \in K$,

$$h_1h_2k_1k_2 = f(h_1h_2, k_1k_2) = f((h_1,k_1))\, f((h_2,k_2)) = h_1k_1h_2k_2.$$

Then, multiplying on the left by h_1^{-1} and on the right by k_2^{-1}, we get $k_1h_2 = h_2k_1$. So every element of H commutes with every element of K.

($\Leftarrow$): Now, suppose that every element of H commutes with every element of K. For all $(h_1,k_1), (h_2,k_2) \in H \times K$

$$\begin{aligned} f((h_1,k_1)(h_2,k_2)) &= f(h_1h_2, k_1k_2) \\ &= h_1h_2k_1k_2 \\ &= h_1k_1h_2k_2 \qquad \text{since } h_2 \text{ commutes with } k_1 \\ &= f(h_1,k_1)\, f(h_2,k_2). \end{aligned}$$

Therefore, f is a homomorphism. ■

Corollary 8.1.1

Let G be a group and define a mapping $f : G \times G \to G$ such that $f(a, b) = ab$ for all $a, b \in G$. Then f is a homomorphism if and only if G is Abelian.

We can prove a slighly stronger version of the above lemma, which does not require a homomorphism, but does require H and K to be *normal* subgroups.

Lemma 8.1.2 Let G be a group and $H, K \trianglelefteq G$ with $H \cap K = \{1_G\}$. Then $hk = kh$ for all $h \in H$ and all $k \in K$ (i.e., every element of H commutes with every element of K).

PROOF: Let $H, K \trianglelefteq G$. Then, for all $h \in H$ and $k \in K$, $hkh^{-1} \in K$ and $khk^{-1} \in H$. But, since H and K are (sub)groups, we have $hkh^{-1}k^{-1} = \left(hkh^{-1}\right)k^{-1} \in K$, but also $hkh^{-1}k^{-1} = h\left(kh^{-1}k^{-1}\right) \in H$, so that $hkh^{-1}k^{-1} \in H \cap K = \{1_G\}$, so that $hkh^{-1}k^{-1} = 1_G \Rightarrow hk = kh$. ■

(This material should be moved to the end of section 3.5.)

Definition 8.1.2 Internal and External Direct Product

The direct product that was introduced in section 3.3 is sometimes called the **external direct product** in order to distinguish it from the internal direct product. An **internal direct product** is a direct product of two normal subgroups H and K of some group G such that $HK \leq G$ and $H \cap K = \{1_G\}$.

Theorem 8.1.4 Characterisation of the Internal Direct Product

Let G, be a group and $H, K \leq G$. Then $G \cong H \times K$ if and only if there exist normal subgroups H^* and K^* of G such that

1. $H \cong H^*$ and $K \cong K^*$;
2. $H^* \cap K^* = \{1_G\}$;
3. $H^*K^* = G$.

PROOF: ($\Leftarrow$): Assume that the three conditions above are satisfied. Without loss of generality, we may take H and K as normal subgroups of G, i.e., $H^* = H$ and $K^* = K$. Define a mapping

$$f : H \times K \to G \text{ by } f(h, k) = hk.$$

Then, for all $(h_1, k_1), (h_2, k_2) \in H \times K$, we have

$$f((h_1, k_1)(h_2, k_2)) = f(h_1h_2, k_1k_2) = h_1h_2k_1k_2.$$

But by the lemma above, $hk = kh$, so we get

$$f((h_1, k_1)(h_2, k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = f(h_1, k_1)\, f(h_2, k_2),$$

so f is a homomorphism. Additionally, since $\text{Im}(f) = HK = G$, we have that f is onto. Finally,

$$\begin{aligned}
\text{Kern}(f) &= \{(h,k) \in H \times K \mid f(h,k) = 1_G\} \\
&= \{(h,k) \in H \times K \mid hk = 1_G\} \\
&= \left\{(h,k) \in H \times K \mid h = k^{-1} = l\right\} \\
&= \{(h,k) \in H \times K \mid l \in H, l \in K\} \\
&= \{(h,k) \in H \times K \mid l \in H \cap K = \{1_G\}\} \\
&= \{(h,k) \in H \times K \mid l = 1_G \Rightarrow h = k = 1_G\} \\
&= \{(1_G, 1_G)\} \\
&= 1_{H \times K}.
\end{aligned}$$

So f is one-to-one, and therefore f is an isomorphism.

($\Rightarrow$): Assume that $G \cong H \times K$, where H and K are some groups. Let

$$H^* = H \times \{1_K\} \text{ and } K^* = \{1_H\} \times K.$$

Now, consider the mapping defined in the first part of the pf above. By the first lemma above, we have that every element of H commutes with every element of K (note that this follows only because f is a homomorphism and does not assume that H and K are normal subgroups as the second lemma above does). Additionally, since we proved that f is onto, we may write any element in $a \in G$ in the form $a = hk$, where $h \in H$ and $k \in K$. Therefore, for all $a \in G$ and all $\tilde{h} \in H$

$$\begin{aligned}
a\tilde{h}a^{-1} &= (hk)\,\tilde{h}\,(hk)^{-1} \\
&= hk\tilde{h}k^{-1}h^{-1} \\
&= h\tilde{h}kk^{-1}h^{-1} \quad \text{since } k \text{ commutes with } \tilde{h} \\
&= h\tilde{h}h^{-1} \in H.
\end{aligned}$$

So $H \trianglelefteq G$. Similarly, for all $a \in G$ and all $\tilde{k} \in K$,

$$\begin{aligned}
a\tilde{k}a^{-1} &= (hk)\,\tilde{k}\,(hk)^{-1} \\
&= hk\tilde{k}k^{-1}h^{-1} \\
&= hk'h^{-1} \quad \text{since } k' = k\tilde{k}k^{-1} \in K \\
&= k'hh^{-1} \quad \text{since } k' \text{ commutes with } h \\
&= k' \in K.
\end{aligned}$$

Therefore, $K \trianglelefteq G$ as well.

Then, since $\{1_H\} \trianglelefteq H$ and $\{1_K\} \trianglelefteq K$, and all identity elements of any group are isomorphic to each other, we get that $H^* \trianglelefteq G$ and $K^* \trianglelefteq G$.

Now, it is clear that $H^* \cong H$ and $K^* \cong K$, so that the first requirement is satisfied. As well,

$$H^* \cap K^* = \{(1_H, 1_K)\} = \{1_G\}$$

since $G \cong H \times K$. So the second requirement is satisfied. Finally,

$$\begin{aligned} H^*K^* &= \{(h, 1_K)\,(1_H, k) \mid h \in H, k \in K\} \\ &= \{(h, k) \mid h \in H, k \in K\} \\ &= H \times K = G, \end{aligned}$$

again, since $G \cong H \times K$. So the third requirement is satisfied as well, and so the pf is complete. ■

REMARK: Observe that under the conditions of this theorem, we get $|H^*K^*| = |G|$.

The theorem above can be generalised to any number of subgroups. We state this generalisation without pf.

Theorem 8.1.5 Characterisation of the Internal Direct Product–General Case

Let G be a group and $\{H_k\}_{k=1}^n$ a set of subgroups of G. Then $G \cong H_1 \times H_2 \times \cdots \times H_n$ if and only if there exist normal subgroups $\{H_k^*\}_{k=1}^n$ such that

1. $H_k^* \cong H_k$ for all $1 \leq k \leq n$;
2. for all $k \in \{2, \ldots, n\}$ $(H_1 H_2 \cdots H_{k-1}) \cap H_k = \{1_G\}$;
3. $H_1 H_2 \cdots H_n = G$.

REMARK: Observe that under the conditions of this theorem, we immediately get $|H_1 H_2 \cdots H_n| = |G|$.

Lemma 8.1.3 Let G be a finite Abelian p-group with at most $p-1$ elements of order p. Then G is cyclic.

PROOF: Let $|G| = p^k$ for some $k \geq 1$ and $k \in \mathbb{Z}$, and let $a \in G$ be an element of maximum order. Since the order of each element divdes the order of G, the maximum possible order of an element is p^k, so let $o(a) = |G| = p^k$. Note that

$$a^{p^{k-1}},\ a^{2p^{k-1}},\ \ldots,\ a^{(p-1)p^{k-1}}$$

are all elements of order p, and there are $p-1$ of them. In fact, these are *all* the elements of order p (why?). Therefore, there are at most $p-1$ elements of order p, satisfying the second hypothesis of the theorem.

Now, we want to show that $\langle a \rangle = G$. Assume for a contradiction that G is not cyclic, i.e., that $G \neq \langle a \rangle$. Therefore, there must exist an element b such that $b^{p^l} \in \langle a \rangle$ but $b^{p^{l-1}} \notin \langle a \rangle$. Without loss of generality, let us take $l = 1$, so that $b^p \in \langle a \rangle$ but $b \notin \langle a \rangle$. Since $b^p \in \langle a \rangle$, there must exist an $s \in \mathbb{Z}$ such that $b^p = a^s$. Now,

$$o(a^s) = \frac{o(a)}{\gcd(o(a), s)} = \frac{p^k}{\gcd(p^k, s)}.$$

Now, if $\gcd(p,s)=1$, then $\gcd\left(p^k,s\right)=1$ and so $o(a^s)=o(a)$, which implies that

$$o(b)>o\left(b^p\right)=o\left(a^s\right)=o(a)\Rightarrow o(a)<o(b),$$

which is a contradiction to the maximality of $o(a)$. Since either $\gcd(p,s)=1$ or $\gcd(p,s)=p$, we must have then $\gcd(p,s)=p$, i.e., $s=mp$ for some $m\in\mathbb{Z}$. Therefore,

$$\begin{aligned} b^p=a^{mp}&\Rightarrow b^pa^{-mp}=1_G\\ &\Rightarrow \left(ba^{-m}\right)^p=1_G\\ &\Rightarrow ba^{-m}=a^{jp^{k-1}},\quad 1\le j\le p-1\\ &\Rightarrow b=a^{jp^{k-1}+m}\in\langle a\rangle \end{aligned}$$

Since b was arbitrary, we have that $\langle a\rangle=G$, i.e., G is cyclic. ■

Lemma 8.1.4 Let G be a finite Abelian p-group and $a\in G$ an element with maximum order (a might not be unique). Then,

1. There exists a surjective homomorphism $\alpha: G\to\langle a\rangle$;
2. $G\cong \mathrm{Kern}(\alpha)\times\langle a\rangle$.

PROOF: Let $|G|=p^n$. We will prove the result by (strong) induction on n.

If $n=0$, then G is necessarily cyclic ($G=\{1_G\}$), so the result holds—simply define $\alpha: G\to\langle 1_G\rangle$ by $\alpha(1_G)=1_G$ and since $\mathrm{Kern}(\alpha)=\{1_G\}=G$, it is certainly true that $G\cong G\times\langle 1_G\rangle\Rightarrow G\cong G\times\{1_G\}$.

Now, assume that the result holds for all $n\le k$, and consider $n=k+1$, i.e., let $|G|=p^{k+1}$. Let $a\in G$ be an element with maximum order, and suppose that G is not cyclic, so that there exists an element $b\in G$ such that $b\notin\langle a\rangle$ and $o(b)=p$, say. Note that since $o(b)=p$, we must have $\langle b\rangle\cap\langle a\rangle=\{1_G\}$, for if this were not so, we would have that $b^k=a^l$ for some $l\in\mathbb{Z}$ and $1\le k\le p-1$, which would mean that there exists an $m\in\mathbb{Z}$ such that $mk=qp+1$, and therefore

$$\left(b^k\right)^m=a^{ml}=b^{qp+1}=\left(b^p\right)^q b=b\Rightarrow b\in\langle a\rangle,$$

a contradiction.

Now, look at the quotient group $G/\langle b\rangle$ and let $\overline{a}=\langle b\rangle a$. Assume that $o(a)=p^r$, which is maximal. We claim that $o(\overline{a})=p^r$ also. Suppose not, in particular, suppose $\overline{a}^{p^{r-1}}=\overline{1}\in G/\langle b\rangle$. Then $a^{p^{r-1}}\in\langle b\rangle$. But $a^{p^{r-1}}\in\langle a\rangle$ also, so $a^{p^{r-1}}\in\langle b\rangle\cap\langle a\rangle=\{1_G\}\Rightarrow a^{p^{r-1}}=1_G$, an contradiction to the assumption that $o(a)=p^r$. So we must have $o(\overline{a})=p^r$, and therefore $\overline{a}$ has maximal order in $G/\langle b\rangle$. Clearly $|G/\langle b\rangle|<|G|=p^n$, and so by the induction hypothesis there exists a surjective homomorphism

$$\overline{\alpha}: G/\langle b\rangle\to\langle\overline{a}\rangle.$$

Now, define

$$\alpha: G\to\langle a\rangle\quad\text{by}\quad\alpha=h\circ\overline{\alpha}\circ f,$$

where

$$f: G\to G/\langle b\rangle\quad\text{and}\quad h:\langle\overline{a}\rangle\to\langle a\rangle.$$

In fact, we have that $\langle \overline{a} \rangle \cong \langle a \rangle$, so h is certainly surjective, and we have seen the mapping f before and know that it is surjective. Therefore, α is a surjective homomorphism.

Now, without loss of generality, we may assume that $\alpha(a) = a$ (why?). By the internal direct product theorem, to show that $G \cong \text{Kern}(\alpha) \times \langle a \rangle$, it suffices to show that $G = (\text{Kern}(\alpha)) \langle a \rangle$ (indeed, since $\text{Kern}(\alpha), \langle a \rangle \trianglelefteq G$ on account of G being Abelian, and certainly $\text{Kern}(\alpha) \cap \langle a \rangle = \{1_G\}$ by definition of α).

Let $g \in G$. Then

$$\alpha\left(\alpha(g) g^{-1}\right) = \alpha(g)\alpha\left(g^{-1}\right) = \alpha\left(gg^{-1}\right) = \alpha(1_G) = 1_G \Rightarrow \alpha(g) g^{-1} \in \text{Kern}(\alpha).$$

Then, let $s = \alpha(g) g^{-1} \in \text{Kern}(\alpha)$. In other words,

$$g = s^{-1}\alpha(g) \in \text{Kern}(\alpha) \langle a \rangle,$$

i.e., every element in G may be expressed as the product of an element in $\text{Kern}(\alpha)$ and an element in $\langle a \rangle$, i.e., $G = \text{Kern}(\alpha) \langle a \rangle$, i.e., $G \cong \text{Kern}(\alpha) \times \langle a \rangle$, as required. This completes the pf. ■

Theorem 8.1.6 Classification of Finite Abelian p-Groups

Let G be a finite Abelian p-group such that $|G| = p^n$. Let $[n_1, n_2, \ldots, n_l]$ be a partition of n with $n_1 \geq n_2 \geq \cdots \geq n_l$. Then we have

$$G \cong \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_l}}.$$

In other words, every finite Abelian p-group may be *uniquely* (up to the order of the factors, of course) written as a direct product of cyclic p-groups.

PROOF: We first prove that every finite Abelian p-group can be written as a direct product of of cyclic p-groups. Pick an element $g \in G$ with maximal order. By the lemma above, $G \cong \text{Kern}(\alpha) \times \langle g \rangle$, where α is the appropriate homomorphism as defined in that lemma. By (strong) induction on $|G|$, since $\text{Kern}(\alpha) \leq G$ and $|\text{Kern}(\alpha)| < |G|$, and $\text{Kern}(\alpha)$ is itself a p-group, we have that $\text{Kern}(\alpha)$ is a product of cyclic p-groups. Therefore, G is a product of cyclic p-groups. (Another way of looking at it is this: since $\text{Kern}(\alpha)$ is itself a p-group, we may apply the previous lemma to it to write $\text{Kern}(\alpha) \cong \text{Kern}(\alpha') \times \langle g' \rangle$. Since G is finite, this process will eventually end and consequently we will have expressed G as a product of cyclic p-groups.)

We now show that each finite Abelian p-group of order p^n can be uniquely written as the direct product of cyclic p-groups using the paritions of n. Let

$$|G| = p^n.$$

Using the first part of the pf of the theorem, we may write

$$G \cong \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_l}},$$

which gives

$$\begin{aligned} p^n &= |G| \\ &= |\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_l}}| \\ &= |\mathbb{Z}_{p^{n_1}}|\,|\mathbb{Z}_{p^{n_2}}| \cdots |\mathbb{Z}_{p^{n_l}}| \\ &= p^{n_1} p^{n_2} \cdots p^{n_l} \\ &= p^{n_1+n_2+\cdots+n_l}, \end{aligned}$$

i.e., we have $n = n_1 + n_2 + \cdots + n_l$. Without loss of generality, we may let $n_1 \geq n_2 \geq \cdots \geq n_l$. Then, it is clear that each unique decomposition of G into cyclic p-groups will come from each unique *partition* of n, i.e., each different way of summing at most l integers to obtain n. This completes the pf. ■

Corollary 8.1.2

Up to isomorphism, there are exactly $P(n)$ Abelian p-groups of order p^n, where $P(n)$ is the partition function.

PROOF: This is clear since each partition of n produces a *unique decomposition* into cyclic p-groups, and there are $P(n)$ partitions. ■

8.2 The Fundamental Theorem of Finite Abelian Groups

In this section we present the funamental theorem of finite Abelian groups, a theorem that will allow us to classify all finite Abelian groups of arbirary order into "isomorphism classes".

Lemma 8.2.1 Let G be a finite Abelian group. By the unique prime factorisation theorem, we may write

$$G = \prod_{i=1}^{l} p_i^{m_i},$$

where each p_i is a prime number. let $H_{p_i^{m_i}}$ be a p-subgroup such that $\left|H_{p_i^{m_i}}\right| = p_i^{m_i}$. Since G is Abelian, we necessarily have $H_{p_i^{m_i}} \trianglelefteq G$. Then,

$$H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_l^{m_l}} = G \quad \text{and} \quad \left|H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_l^{m_l}}\right| = |G|.$$

PROOF: First of all, the p-subgroups $H_{p_i^{m_i}}$, $1 \leq i \leq l$ exist due to Theorem 8.1.2. Then, it is clear that $H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_l^{m_l}} \subseteq G$ since each p-group in the product is a subgroup of G. Now, we show that $\left|H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_l^{m_l}}\right| = |G|$, and we do this by induction on l.

When $l = 1$, then $|G| = p^m$. By Theorem 8.1.2, there exists a unique p-subgroup of order p^m, so the result holds.

Now, assume that the result holds for $l = k$, so that $\left|H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_l^{m_l}}\right| = \prod_{i=1}^{k} p_i^{m_i}$. Then, let $g \in H_{p_1} H_{p_2} \cdots H_{p_k} \cap H_{p_{k+1}}$. Since $g \in H_{p_{k+1}}$, we have $o(g) = p^{k+1} \Rightarrow g^{p^{k+1}} = 1_G$ for

some $k \geq 0$. On the other hand, since $g \in H_{p_1} H_{p_2} \cdots H_{p_k}$ we have $g = h_1 h_2 \cdots h_k$, where $o(h_i) = p^i \Rightarrow h_i^{p^j} = 1_G$ for some prime exponents p^j, $1 \leq i \leq k$ and $j \geq 0$. Let $m = \prod_{i=1}^{k} p^j$. Then m and p^{k+1} are coprime (how?), i.e., $\gcd\left(m, p^{k+1}\right) = 1$, so that there are integers r and s such that $rm + sp^{k+1} = 1$. Therefore,

$$g = g^1 = g^{rm+sp^{k+1}} = (g^m)^r \left(g^{p^{k+1}}\right)^s = 1_G,$$

which means that $H_{p_1} H_{p_2} \cdots H_{p_k} \cap H_{p_{k+1}} = \{1_G\}$, i.e., $\left|H_{p_1} H_{p_2} \cdots H_{p_k} \cap H_{p_{k+1}}\right| = 1$. Therefore, by the induction hypothesis,

$$\left|H_{p_1} H_{p_2} \cdots H_{p_k} H_{p_{k+1}}\right| = \frac{\left|H_{p_1} H_{p_2} \cdots H_{p_k}\right| \left|H_{p_{k+1}}\right|}{\left|H_{p_1} H_{p_2} \cdots H_{p_k} \cap H_{p_{k+1}}\right|} = \prod_{i=1}^{k} p_i^{m_i} \cdot p_{k+1}^{m_{k+1}} = \prod_{i=1}^{k+1} p_i^{m_i},$$

so the result holds for $l = k + 1$. By induction, therefore, the result holds for all l.

Finally, since $H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_l^{m_l}} \subseteq G$ and $\left|H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_l^{m_l}}\right| = |G|$, we must have $G = H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_l^{m_l}}$, and thus the pf is complete. ■

Corollary 8.2.1

Let G be a finite Abelian group with $|G| = \prod_{i=1}^{l} p_i^{m_i}$. Let $H_{p_i^{m_i}}$ be a p-subgroup such that $\left|H_{p_i^{m_i}}\right| = p_i^{m_i}$ (such a p-subgroup exists by Theorem 8.1.2). Then

$$G \cong H_{p_1^{m_1}} \times H_{p_2^{m_2}} \times \cdots \times H_{p_l^{m_l}}.$$

In other words, every finite Abelian group is isomorphic to the direct product of its p-subgroups.

PROOF: The result follows from the previous theorem and the generalisation of internal direct product theorem if we can show that for all $k \in \{2, \ldots, l\}$

$$H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_{k-1}^{m_{k-1}}} \cap H_{p_k^{m_k}} = \{1_G\}.$$

Now, fix a $k \in (2, \ldots, l\}$ and write the order of G as $|G| = p_k^{m_k} a$, where $\gcd(p_k, a) = 1$. By the previous theorem, we get that $\left|H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_{k-1}^{m_{k-1}}}\right| = a$, with $\left|H_{p_k^{m_k}}\right| = p_k^{m_k}$. Therefore,

$$\gcd\left(\left|H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_{k-1}^{m_{k-1}}}\right|, \left|H_{p_k^{m_k}}\right|\right) = 1,$$

and thus $H_{p_1^{m_1}} H_{p_2^{m_2}} \cdots H_{p_{k-1}^{m_{k-1}}} \cap H_{p_k^{m_k}} = \{1_G\}$ for all $k \in \{2, \ldots, l\}$. Therefore, by the general internal direct product theorem, we get

$$G \cong H_{p_1^{m_1}} \times H_{p_2^{m_2}} \times \cdots \times H_{p_l^{m_l}},$$

as required. (Also show pf from class.) ■

So we see that every finite Abelian group can be written as a direct product of p-groups. However, we have seen that every p-group is isomorphic to a direct product of cyclic p-groups. This finally leads to the important fundamental theorem of finite Abelian groups, also called the *Classification Theorem for Finite Abelian Groups*.

Theorem 8.2.1 Fundamental Theorem of Finite Abelian Groups

Every finite Abelian group is isomorphic to the direct product of a unique collection of cyclic p-groups.

REMARK: By "collection" we mean a multiset, i.e., a set in which repetition of elements is allowed but the ordering, as with regular sets, is not important.

PROOF: Let G be a finite Abelian group. We have just seen in the previous corollary that G is isomorphic to the direct product of p-subgroups such that the product of their orders satisfy the prime factorisation of $|G|$. Then, by the classifiction of finite Abelian p-groups, every p-subgroup in that decomposition is isomorphic (uniquely) to a direct product of cyclic p-groups. Therefore, G is isomorphic to a direct product of a unique collection of cyclic p-groups. ■

Corollary 8.2.2

Let n be a positive integer and let $n = \prod_{i=1}^{l} p_i^{m_i}$ be the prime factorisation of n. Then, up to isomorphism, there are exactly $\prod_{i=1}^{l} P(m_i)$ distinct (finite) Abelian groups of order n where P is the partition function.

PROOF: We know that every finite Abelian group of order n may be written as the direct product of l p-subgroups, where l is the number of primes in the prime factorisation of n. Each of these p-subgroups, of order p^{m_i}, is itself a direct product of cyclic p-groups. In fact, we have seen that there are $P(m_i)$ groups of order p^{m_i} up to isomorphism. It thus follows that there are $\prod_{i=1}^{l} P(m_i)$ unique ways of writing the group as a direct product of cyclic p-groups. ■

8.3 Examples

In this section, we go through several examples of the use of the classification of finite Abelian p-groups theorem and the fundamental theorem of finite Abelian groups.

Example 8.3.1 Prove that $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ if and only if $\gcd(n, m) = 1$. Deduce that $\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic if and only if $\gcd(n, m) = 1$.

SOLUTION:

Example 8.3.2 Determine all Abelian groups, up to isomorphism, of order 16.

SOLUTION: We begin with the prime factorisation of 16. Notice that $16 = 2^4$, so that any group of order 16 is a p-group, with $p = 2$. So, using the classification of finite Abelian p-groups, the number of Abelian groups of order 16 is equal to the number of partitions of 4. The partitions are, with their corresponding group,

$$\begin{aligned}
[4] &\longrightarrow \mathbb{Z}_{2_4} = \mathbb{Z}_{16}, \\
[3,1] &\longrightarrow \mathbb{Z}_{2^3} \times \mathbb{Z}_{2_1} = \mathbb{Z}_8 \times \mathbb{Z}_2, \\
[2,2] &\longrightarrow \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} = \mathbb{Z}_4 \times \mathbb{Z}_4, \\
[2,1,1] &\longrightarrow \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \\
[1,1,1,1] &\longrightarrow \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.
\end{aligned}$$

So there are five Abelian groups, up to isomorphism, of order 16, as listed above. So if G is an Abelian group of order 16, then it must be isomorphic to one of the groups above.

Example 8.3.3 Up to isomorphism, list all the Abelian groups of order 32.

SOLUTION: We begin with the prime factorisation of 32. Notice that $32 = 2^5$, so in fact any group of order 32 is a p-group, with $p = 2$. So our answer comes directly from the classification theorem of finite Abelian p-groups, which means we must look for the partition of 5. Remember that each partition of 5 corresponds to a unique direct product, and hence unique Abelian group, of order 32. The partitions of 5 are

$$\begin{aligned}
[5] &\longrightarrow \mathbb{Z}_{2^5} = \mathbb{Z}_{32}, \\
[4,1] &\longrightarrow \mathbb{Z}_{2^4} \times \mathbb{Z}_{2^1} = \mathbb{Z}_{16} \times \mathbb{Z}_2, \\
[3,1,1] &\longrightarrow \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} = \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \\
[3,2] &\longrightarrow \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^2} = \mathbb{Z}_8 \times \mathbb{Z}_4, \\
[2,2,1] &\longrightarrow \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1} = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2, \\
[2,1,1,1] &\longrightarrow \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \\
[1,1,1,1,1] &\longrightarrow \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.
\end{aligned}$$

So we see that there are seven Abelian groups of order 32, as listed above. This tells us that if G is an Abelian group of order 32, then it must be isomorphic to one of the groups above.

Example 8.3.4 Determine all Abelian groups of order 56.

SOLUTION: The prime factorisation of 56 is $56 = 2^3 \cdot 7^1$. So, by the funamental theorem of finite Abelian groups, the Abelian groups of order 56 are given by the combinations of the direct products of the decompositions of the p-groups of orders 8 and 7. In other words, every combination (without regard for order, of course) of the partitions of 3 and 1 will give rise to an Abelian group of order 56. There is only one partition of 1, and that is [1], and

there are three partitions of 3, namely

$$[3]\,, \quad [2,1]\,, \quad \text{and} \quad [1,1,1]\,.$$

Therefore, there are three Abelian groups, up to isomorphism, of order 56:

$$\begin{aligned}
[3]\,,[1] &\longrightarrow \mathbb{Z}_{2^3} \times \mathbb{Z}_{7^1} = \mathbb{Z}_8 \times \mathbb{Z}_7 \cong \mathbb{Z}_{56}, \quad \text{since } \gcd(7,8) = 1, \\
[2,1]\,,[1] &\longrightarrow \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{7^1} = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_7 \cong \mathbb{Z}_4 \times \mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_{28}, \quad \text{since } \gcd(2,7) = \gcd(4,7) = 1, \\
[1,1,1]\,,[1] &\longrightarrow \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{7^1} = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{14}, \quad \text{since } \gcd(2,7) = 1.
\end{aligned}$$

Again, any Abelian group of order 56 will be isomorphic to one of these groups.

Example 8.3.5 Determine all Abelian groups of order 400.

SOLUTION: The prime factorisation of 400 is $400 = 5^2 \cdot 2^4$. We have

Partitions of 2	Partitions of 4
$[2]$	$[4]$
$[1,1]$	$[3,1]$
	$[2,2]$
	$[2,1,1]$
	$[1,1,1,1]\,.$

Therefore, there are $5 \times 2 = 10$ Abelian groups of order 400. They are

$$\begin{aligned}
\mathbb{Z}_{5^2} \times \mathbb{Z}_{2^4} &= \mathbb{Z}_{25} \times \mathbb{Z}_{16} \\
\mathbb{Z}_{5^2} \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_{25} \times \mathbb{Z}_8 \times \mathbb{Z}_2 \\
\mathbb{Z}_{5^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} &= \mathbb{Z}_{25} \times \mathbb{Z}_4 \times \mathbb{Z}_4 \\
\mathbb{Z}_{5^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_{25} \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
\mathbb{Z}_{5^2} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_{25} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{2^4} &= \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{16} \\
\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_8 \times \mathbb{Z}_2 \\
\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{2^2} &= \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \\
\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.
\end{aligned}$$

Recall much earlier that we proved the isomorphism relation "$\cong$" to be an equivalence relation (in a remark), and we mentioned that the equivalence classes, or "isomorphism classes", consisted of all groups of a particular order that were isomorphic to some representative of those classes. In the four examples above, we have split all *Abelian* groups of a particular order into isomorphism classes, with the representatives of each class being the groups listed. Keep in mind that we

have only done this for *Abelian* groups of that order. Determining the non-Abelian isomorphism classes for groups of a particular order is a much harder problem!

Example 8.3.6 Show that there are only two Abelian groups of order four, and describe them. To which of these isomorphism classes does $U(12)$ belong?

SOLUTION: We have that $4 = 2^2$, so there are only two Abelian groups of order four. In fact, we have seen that all groups of order four are Abelian, so we can say that *any* group of order four is isomorphic to either one of two groups. We've seen already that these two groups are $\mathbb{Z}_4$ and the Klein 4-Group, which may be represented as the dihedral group D_2, or, in terms of the classification of p-groups, as $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Now, $U(12) = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$. It can be shown that $U(12)$ is not cyclic; and since $\gcd(2,2) = 2 \neq 1$, we have that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic, and clearly $\mathbb{Z}_4$ is cyclic, so $U(12)$ belongs to the isomorphism class containing $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 8.3.7 To which isomorphism class does $U(60)$ belong?

SOLUTION:

Example 8.3.8 To which isomorphism class does $U(63)$ belong?

SOLUTION:

Example 8.3.9 For each n below, identify the group $U(n)$ by writing it as the direct product of cyclic p-groups.

(a) $n = 27$

(b) $n = 32$

(c) $n = 45$

(d) $n = 72$

SOLUTION:

Example 8.3.10 Count how many distinct Abelian groups there are for each n.

(a) $n = 1024$

(b) $n = 27000$

(c) $n = 30030$

(d) $n = 31104$

SOLUTION:

Example 8.3.11 Let $G = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_9$.

(a) How many elements in G are of order 9?

(b) How many elements in G are of order 6?

SOLUTION:

9 Group Actions

In this chapter, we study the concept of a group *acting* on a set. Group actions are a powerful tool that we shall use both for proving theorems for abstract groups and for unravelling the structure of specific examples. We will eventually see that the theory of group actions generalises the theory of cycles and cycle structures seen in the chapter on S_n. The concept of an "action" turns out to be an important tool for studying objects in general abstract algebra.

Recall that any bijection from a set X to itself can be regarded as a permutation, as all it does is is "rearrange" the elements of X. (Does X have to be a finite set?) The set of these permutations, S_X, is a group.

Definition 9.0.1 Group Action

A **group action** of a group G on a set X is a function $\varphi : G \times X \to X$ satisfying the following properties:

1. $\varphi(gh, x) = \varphi(g, \varphi(h, x))$ for all $g, h \in G$ and all $x \in X$.
2. $\varphi(1_G, x) = x$ for all $x \in X$.

Example 9.0.12 Let $G = \mathbb{R}$ (under addition) and $X = \mathbb{R}^2$. Define a group action

$$\varphi_1 : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2 \quad \text{by} \quad \varphi_1(a, (x, y)) = (x + a, y),$$

and define

$$\varphi_2 : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2 \quad \text{by} \quad \varphi_2(b, (x, y)) \to (x, y + b).$$

(You may verify that φ_1 and φ_2 are group actions.) Observe that φ_1 is merely a horizontal translation in $\mathbb{R}^2$ and φ_2 a vertical translation.

Example 9.0.13 Let $G = \{1_G, a\}$ and $X = \mathbb{C}$. Then G acts on X by the action

$$\varphi : G \times \mathbb{C} \to \mathbb{C}, \quad \text{defined by} \quad \varphi(1_G, x + yi) = x + yi \quad \text{and} \quad \varphi(a, x + yi) = x - yi,$$

for all complex numbers $x + yi \in \mathbb{C}$. Again, verify that this is a group action.

Example 9.0.14 Every subgroup H of a group G (including the group G itself) acts on G by *left multiplication* if we define the mapping $\varphi : H \times G \to G$ by $\varphi(h, g) = hg$ for all $h \in H$

and all $g \in G$. Again, verify that φ is indeed a group action (the set X here is actually the group G!). We may similarly define the mapping $\varphi : H \times G \to G$ by $\varphi(h, g) = gh$ for all $h \in H$ and all $g \in G$, in which case H acts on G by *right multiplication.*

Example 9.0.15 Every subgroup H of a group G (again, including the group G itself) acts on G by *conjugation* if we define the mapping $\varphi : H \times G \to G$ by $\varphi(h, g) = hgh^{-1}$ for all $h \in H$ and $g \in G$. Again, verify that φ is indeed a group action (the set X here is actually the group G!).

Example 9.0.16 Let $X = \{1, 2, \ldots, n\}$ and let $G = S_n$, the group of permutations of n elements. Then S_n acts on X using the mapping $\varphi : \S_n \times X \to X$ defined by $\varphi(\alpha, i) = \alpha(i)$ for all $\alpha \in S_n$ and all $i \in X$. In particular, for any $\alpha \in S_n$ let us define the action of $\langle \alpha \rangle$ (i.e., the cyclic subgroup of S_n generated by α) on X, $\varphi : \langle \alpha \rangle \times X \to X$, by

$$\varphi\left(\alpha^l, i\right) = \alpha^l(i)$$

for all $l \in \mathbb{Z}$ and $i \in X$. Let us show that this mapping is actually a group mapping by showing that it satisfies the two defining properties.

1. For all $k, l \in \mathbb{Z}$ and all $i \in X$, we have

$$\varphi\left(\alpha^{k+l}, i\right) = \alpha^{k+l}(i) = \alpha^k\left(\alpha^l(i)\right) = \varphi\left(\alpha^k, \alpha^l(i)\right) = \varphi\left(\alpha^k, \varphi\left(\alpha^l, i\right)\right),$$

   so the first condition is satisfied.

2. For all $i \in X$, $\varphi\left(\alpha^0, i\right) = \alpha^0(i) = i$ since α^0 is the identity mapping. So the second condition is satisfied as well.

So φ is indeed a group action.

Theorem 9.0.1

Let G be a group acting on the set X. Then

1. For every $g \in G$, the mapping $\varphi_g : X \to X$ defined by $\varphi_g(x) = \varphi(g, x)$ for all $x \in X$ is a permutation of X, i.e., $\varphi_g \in S_X$.
2. The mapping $\overline{\varphi} : G \to S_X$ defined by $\overline{\varphi}(g) = \varphi_g$ is a group homomorphism.

REMARK: The first part of the theorem shows us that the set consisting of all φ_g for all $g \in G$, i.e., the set consisting of all permutations of X, which we denote S_X, is a group under composition of functions. This makes the notion of the homomorphism in the second part of the theorem valid.

PROOF:

1. To say that φ_g is a permutation is to say that φ_g is a bijection. To show that φ_g is a bijection, it suffices to show that it has an inverse. Note that if $g = 1_G$, then by property 2 of group actions, we must have $\varphi_1(x) = x$ for all $x \in X$. In other words, φ_1 is the identity mapping on X. Now, consider the mapping $\varphi_{g^{-1}} : X \to X$. We have

$$\begin{aligned}\varphi_g \circ \varphi_{g^{-1}}(x) &= \varphi_g\left(\varphi_{g^{-1}}(x)\right) \\ &= \varphi_g\left(\varphi\left(g^{-1}, x\right)\right) \\ &= \varphi\left(g, \varphi\left(g^{-1}, x\right)\right) \\ &= \varphi\left(gg^{-1}, x\right) = \varphi(1_G, x) \\ &= x.\end{aligned}$$

   Similarly, we can show that $\varphi_{g^{-1}} \circ \varphi_g(x) = x$. In other words, both $\varphi_{g^{-1}} \circ \varphi_g$ and $\varphi_g \circ \varphi_{g^{-1}}$ do not move x, i.e., they corresponding to φ_1, the identity mapping. So

$$\varphi_g \circ \varphi_{g^{-1}} = \varphi_{g^{-1}} \circ \varphi_g = \varphi_1,$$

   i.e., $\varphi_g^{-1} = \varphi_{g^{-1}}$. So we have found an inverse; hence, φ_g is a bijection, hence a permutation on X.

2. We now show that $\overline{\varphi} : G \to S_X$ is a group homomorphism. We have for all $g, h \in G$ and all $x \in X$

$$\begin{aligned}\overline{\varphi}(gh) &= \varphi_{gh}(x) \\ &= \varphi(gh, x) = \varphi(g, \varphi(h, x)) \\ &= \varphi(g, \varphi_h(x)) \\ &= \varphi_g(\varphi_h(x)) \\ &= \varphi_g \circ \varphi_h(x) \\ &= \overline{\varphi}(g) \circ \overline{\varphi}(h).\end{aligned}$$

   So $\overline{\varphi}$ is indeed a homomorphism. ■

We can easily show that the converse of the preceding proposition is also true.

Theorem 9.0.2

Given a group homomorphism $\overline{\varphi} : G \to S_X$ from a group G to the group S_X, the mapping $\varphi : G \times X \to X$ defined by $\varphi(g, x) = \varphi_g(x)$ for all $g \in G$ is a group action of G on X.

PROOF: We need to show that the two defining conditions of a group action are satisfied.

1. We have $\varphi(g, \varphi(h, x)) = \varphi_g(\varphi_h(x)) = \varphi_g \circ \varphi_h(x) = \varphi_{gh}(x) = \varphi(gh, x)$, the second-last step following because $\overline{\varphi}$ is a homomorphism.

2. We have $\varphi(1_G, x) = \varphi_1(x) = x$, where, as established before, φ_1 is the identity mapping, i.e., the identity element of S_X.

So φ is a group action. ■

A word on notation: we will sometimes use $\overline{g}$ to denote $\varphi_g = \overline{\varphi}(g)$. Remember that φ_g is a permutation of X (i.e., $\varphi_g : X \to X$) and $\overline{\varphi}$ is a homomorphism that gives, for each $g \in G$, a permutation φ_g (i.e., $\overline{\varphi} : G \to S_X$).

Lemma 9.0.1 Let G be any group acting on itself. Define the mapping $\varphi : G \times G \to G$ by $\varphi(g, h) = gh$ for all $g, h \in G$. Then φ is a group action.

PROOF: We simply show that the defining properties of group actions are satisfied.

1. For all $g, h, k \in G$,

$$\varphi(gh, k) = ghk = g(hk) = g\varphi(h, k) = \varphi(g, \varphi(h, k)),$$

so the first condition is satisfied.

2. For all $g \in G$,

$$\varphi(1_G, g) = 1 \cdot g = g,$$

so the second property is satisfied.

Therefore, φ is a group action. ■

Definition 9.0.2 Permutation Representation

The homomorphism $\overline{\varphi} : G \to S_X$ associated with an action of a group G on a set X is called the **permutation representation** of G.

We now present the important theorem, due to Cayley, that establishes all finite groups as subgroups of the permutation group S_n.

Theorem 9.0.3 Cayley's Theorem

Every finite group of order n is isomorphic to a subgroup of S_n.

PROOF: Let G be any finite group of order n, and let it act on itself by multiplication as in the previous lemma, i.e., let

$$\varphi : G \times G \to G \quad \text{such that} \quad \varphi(g, h) = gh, \ \forall g, h \in G.$$

We know from Theorem 9.0.1 that there exists a group homomorphism $\overline{\varphi} : G \to S_G$ defined by $\overline{\varphi}(g) = \varphi_g(x)$ for $x \in G$ (S_G is the set of permutations on G) (remember that φ_g is *one*

permutation, i.e., one member of S_G!). Now,

$$\begin{aligned}\text{Kern}(\overline{\varphi}) &= \{g \in G \mid \overline{\varphi}(g) = 1_{S_G} = \varphi_1\} \\ &= \{g \in G \mid \varphi_g = \varphi_1\} \\ &= \{g \in G \mid \varphi(g,x) = gx = \varphi(1_G, x) = x \text{ for all } x \in G\} \quad \text{since } \varphi_g = \varphi(g,x) \\ &= \{g \in G \mid g = 1_G\} \quad \text{by cancellation law} \\ &= \{1_G\} \quad \text{since identity element is unique.}\end{aligned}$$

So $\text{Kern}(\overline{\varphi}) = \{1_G\}$, which means that $\overline{\varphi}$ is one-to-one. More importantly, however, the first isomorphism theorem gives

$$G/\text{Kern}(\overline{\varphi}) \cong \text{Im}(\overline{\varphi}) \leq S_G.$$

But $\text{Kern}(\overline{\varphi}) = \{1_G\}$, and

$$G/\{1_G\} \cong G,$$

which means that

$$G \cong \text{Im}(\overline{\varphi}) \leq S_G,$$

i.e., G is isomorphic to a subgroup of S_G, as required. ■

Example 9.0.17 We have already given a permutation representation of the dihedral group D_3, which was the symmetry transformations of the equilateral triangle. We have seen that this group is isomorphic to the group S_3, and have used this fact many times already. So we have unknowingly used Cayley's theorem many times already. We have also seen the permutation representation of the group D_4, which was the symmetry transformations of the square..

More generally,

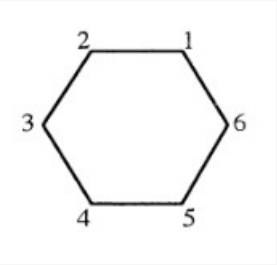
T

he action of the dihedral group D_n on a regular n-gon (i.e., on the set of points constituting the n-gon) gives a representation of D_n as a subgroup of the permutation group S_n.

Definition 9.0.3 Faithful Action

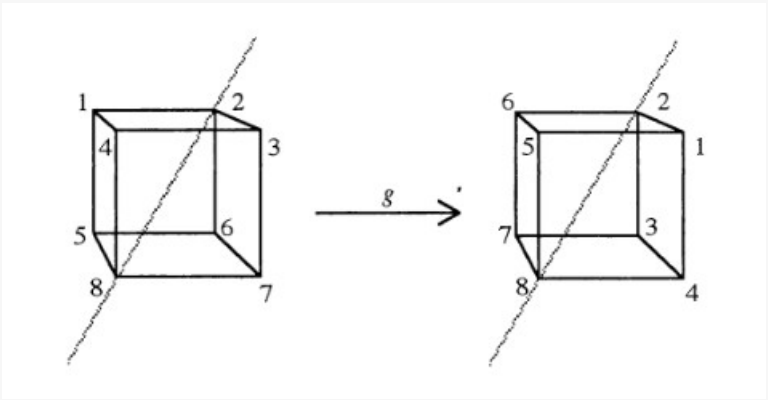
The group G is said to act **faithfully** on the set X if $\text{Kern}(\overline{\varphi}) = \{1_G\}$, where $\overline{\varphi} : G \to S_X$, defined as usual by $\overline{\varphi}(g) = \varphi_g(x) = \varphi(g,x)$ for all $g \in G$ and all $x \in X$ (φ is the corresponding group action). In other words, G is faithful to X if the only element of G that fixes every element of X is the identity (since all elements of G that fix x, by definition of $\overline{\varphi}$, are part of $\text{Kern}(\overline{\varphi})$). So G is faithful to X if and only if $\overline{\varphi}$ is one-to-one.

Example 9.0.18 The action of the dihedral group $D_n = \left\{1, b, b^2, \ldots, b^{n-1}, a, ab, ab^2, \ldots, ab^{n-1}\right\}$ on a regular n-gon is faithful. So is the action of any subgroup of D_n.



For example, let $G = \left\{1, b^2, b^4\right\}$, a subgroup of the dihedral group D_6, and let $X = \{1, 2, 3, 4, 5, 6\}$ be the six vertices of a regular hexagon, as shown in the figure above. Let G act on X by having b rotate the hexagon counterclockwise by 60°. Then G acts faithfully on X and can be represented as the subgroup $\{(), (1\ 3\ 5)\,(2\ 4\ 6), (1\ 5\ 3)\,(2\ 6\ 4)\}$ of S_6, where the generator of the subgroup G is $b = (1\ 3\ 5)\,(2\ 4\ 6)$.

Example 9.0.19 Let $G = \left\{1, g, g^2\right\}$ be the cyclic group of order three, let $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ be the eight vertices of a cube, as shown below, and let G act on X by having g rotate the cube around the axis through vertices 2 and 8, so that $\varphi(g, 1) = 6$, $\varphi(g, 3) = 1$, and $\varphi(g, 6) = 3$, as shown in the figure below.

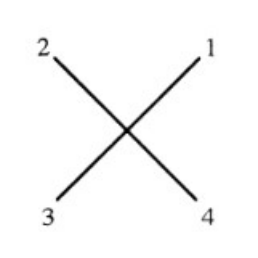


Then again the action is faithful and G may be represented as the subgroup

$$\{(), (1\ 6\ 3)\,(4\ 5\ 7), (1\ 3\ 6)\,(4\ 7\ 5)\}$$

of S_8. In this case, the generator g of G is represented by the permutation $g = (1\ 6\ 3)\,(4\ 7\ 5)$.

Example 9.0.20 Since D_4, which corresponds to the symmetry transformations of a square, may be represnted as a subgroup of S_4, we know that that action of D_4 on $\{1, 2, 3, 4\}$ (corresponding to the vertices of the square) is faithful. But we may consider D_4 instead acting on the set $\{d_{13}, d_{24}\}$ of the two diagonals of the square.



In this case, the action is not faithful, since $\varphi\left(b^2, d_{13}\right) = d_{13}$ and $\varphi\left(b^2, d_{24}\right) = d_{24}$, where b is the group element representable by (1 2 3 4) $\in S_4$. (i.e., we have that elements other than the identity fix d_{13} and d_{24}.)

9.1 Stabilisers and Orbits in a Group Action

Definition 9.1.1 Stabiliser

Let G be a group, X a set, and $\varphi : G \times X \to X$ a group action. Define the set

$$\boxed{\text{Stab}_G(x) = \{g \in G \mid \varphi(g, x) = \varphi_g(x) = x\} \subseteq G},$$

called the **stabiliser** of x in G. Remember that x is an element of X. So the stabiliser of an element $x \in X$ is the collection of those $g \in G$ that fix x under the action φ. Complementarily, we define the set

$$\boxed{\text{Stab}_X(g) = \{x \in X \mid \varphi(g, x) = x\} \subseteq X}$$

as the stabiliser of g in X, i.e., the set of elements in X that are fixed by G.

Theorem 9.1.1

Let G be a group, X a set, and $\varphi : G \times X \to X$ a group action. For any $x \in X$, $\text{Stab}_G(x) \leq G$.

PROOF: We use the subgroup test. For any element $x \in X$:

1. Since by definition $\varphi(1_G, x) = x$ for all $x \in X$, we have that $1_G \in \text{Stab}_G(x)$, so $\text{Stab}_G(x)$

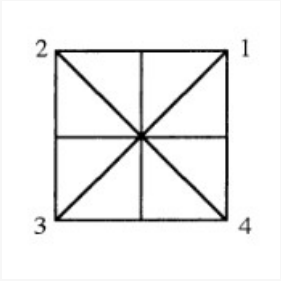
is not empty.

2. Consider two elements $g, h \in \mathrm{Stab}_G(x)$, i.e., $\varphi(g,x) = x$ and $\varphi(h,x) = x$. Then,
$$\varphi(gh,x) = \varphi(g,\varphi(h,x)) = \varphi(g,x) = x,$$
so that $gh \in \mathrm{Stab}_G(x)$.

3. Consider an element $g \in \mathrm{Stab}_G(x)$, so that $\varphi(g,x) = x$. Since $1_G = g^{-1}g \in \mathrm{Stab}_G(x)$, we have
$$\varphi\left(g^{-1},x\right) = \varphi\left(g^{-1},\varphi(g,x)\right) = \varphi\left(g^{-1}g,x\right) = \varphi(1_G,x) = x,$$
so that $g^{-1} \in \mathrm{Stab}_G(x)$.

So by the subgroup test, $\mathrm{Stab}_G(x) \leq G$. ■

Example 9.1.1 Consider the dihedral group D_4. It acts in a natural way on the set consisting of the four vertices $1,2,3,4$ of the square, together with the sides $t_{12}, t_{23}, t_{34}, t_{41}$ and the diagonals d_{13} and d_{24}.



The table below describes the action.

	1	2	3	4	t_{12}	t_{23}	t_{34}	t_{41}	d_{13}	d_{24}
id	1	2	3	4	t_{12}	t_{23}	t_{34}	t_{41}	d_{13}	d_{24}
b	2	3	4	1	t_{23}	t_{34}	t_{41}	t_{12}	d_{24}	d_{13}
b^2	3	4	1	2	t_{34}	t_{41}	t_{12}	t_{23}	d_{13}	d_{24}
b^3	4	1	2	3	t_{41}	t_{12}	t_{23}	t_{34}	d_{24}	d_{13}
a	2	1	4	3	t_{12}	t_{41}	t_{34}	t_{23}	d_{24}	d_{13}
ab	3	2	1	4	t_{23}	t_{13}	t_{41}	t_{34}	d_{13}	d_{24}
ab^2	4	3	2	1	t_{34}	t_{23}	t_{12}	t_{41}	d_{24}	d_{13}
ab^3	1	4	3	2	t_{41}	t_{34}	t_{23}	t_{12}	d_{13}	d_{24}

From this table, we can see that, for example, $\varphi(g,2) = 2$ exactly when $g = \mathrm{id}$ or $g = ab$, that $\varphi(g,d_{13}) = d_{13}$ exactly when $g = \mathrm{id}, b^2, ab, ab^3$, and that $\varphi(g,t_{41}) = t_{41}$ exactly when $g = \mathrm{id}, ab^2$. Therefore, we have

$$\mathrm{Stab}_G(2) = \{\mathrm{id}, ab\}, \quad \mathrm{Stab}_G(d_{13}) = \left\{\mathrm{id}, b^2, ab, ab^3\right\}, \quad \mathrm{Stab}_G(t_{41}) = \left\{\mathrm{id}, ab^2\right\}$$

as some stablisers.

Theorem 9.1.2

Let G be a group, X a set, and $\varphi : G \times X \to X$ a group action. Define a relation $\sim_\varphi$ on X by the following: for all $x_1, x_2 \in X$, $x_1 \sim_\varphi x_2$ if and only if there exists a $g \in G$ such that $\varphi(g, x_1) = x_2$. The relation $\sim_\varphi$ is then an equivalence relation.

PROOF: We simply verify the properties of reflexivity, symmetry, and transitivity.

1. (Reflexivity) For all $x \in X$, we have $\varphi(1_G, x) = x$ by definition of a group action. So $x \sim_\varphi x$.
2. (Symmetry) For all $x_1, x_2 \in X$, suppose $x_1 \sim_\varphi x_2$, so that $\varphi(g, x_1) = x_2$ for some $g \in G$. We have seen that $\varphi^{-1}(g, x_1) = \varphi_g^{-1} = \varphi_{g^{-1}} = \varphi\left(g^{-1}, x_2\right) = x_1$, which means that $x_2 \sim_\varphi x_1$.
3. (Transitivity) For all $x_1, x_2, x_3 \in X$, suppose $x_1 \sim_\varphi x_2$ and $x_2 \sim_\varphi x_3$, i.e., there exist $g, h \in H$ such that $\varphi(g, x_1) = x_2$ and $\varphi(h, x_2) = x_3$. Then,

$$\varphi(hg, x_1) = \varphi(h, \varphi(g, x_1)) = \varphi(h, x_2) = x_3.$$

Therefore, $x_1 \sim_\varphi x_3$. ■

Definition 9.1.2 Orbit

Let G be a group, X a set, and $\varphi : G \times X \to X$ a group action. The equivalence class under $\sim_\varphi$ containing the element $x \in X$, denoted $[x]$ and defined as

$$[x] = \{y \in X \mid x \sim_\varphi y\} = \{\overline{g}(x) \mid g \in G\},$$

is called the **orbit** of x.

REMARK: Notice that we have defined the orbit of an element $x \in X$ in two ways. The first is the familar way of defining equivalence classes in general. The second is $[x] = \{\overline{g}(x) \mid g \in G\}$, which is completely equivalent to the first. To see why, note that $x \sim_\varphi y \Leftrightarrow \varphi(g, x) = y$ for some $g \in G$. Hence, as long as $g \in G$ any element of X of the form $\varphi(g, x)$ will be equivalent to x under $\sim_\varphi$, hence an element of $[x]$. Since, for a fixed g, $\varphi(g, x) = \varphi_g(x) = \overline{\varphi}(g) = \overline{g}(x)$, the second defnition follows.

Example 9.1.2 Consider the preceding example of the action on D_4. From the table, we can see that there are three orbits, the sets of vertices, of edges, and of diagonals. So, for instance, $[2] = \{1, 2, 3, 4\}$ and $[d_{13}] = \{d_{13}, d_{24}\}$ and $[t_{41}] = \{t_{12}, t_{23}, t_{34}, t_{41}\}$. We have seen that $\text{Stab}_G(2)$ is a group of order two, while $[2]$ has four elements; also, $\text{Stab}_G(d_{13})$ is a group of order four, while $[d_{13}]$ has two elements; finally, $\text{Stab}_G(t_{41})$ is a group of order two, while $[t_{41}]$ has four elements.

Theorem 9.1.3 The Orbit-Stabiliser Theorem

Let G be a group, X a set, and $\varphi : G \times X \to X$ a group action. For any $x \in X$, we have

$$|[x]| = [G : \mathrm{Stab}_G(x)],$$

i.e., the size of the orbit of x is equal to the index of its stabiliser. If G is finite, then

$$|[x]| = \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

PROOF: (Only for finite G) First note that if $g, h \in G$, then

$$\begin{aligned} \varphi_g(x) = \varphi_h(x) &\Leftrightarrow \varphi_{h^{-1}}(x) \circ \varphi_g(x) = \varphi_{h^{-1}}(x) \circ \varphi_h(x) = x \\ &\Leftrightarrow \varphi_{h^{-1}g}(x) = x \\ &\Leftrightarrow h^{-1}g \in \mathrm{Stab}_G(x). \end{aligned}$$

Now, let us write $\overline{g} = \varphi_g$, and define a mapping

$$\tilde{\varphi} : [x] \to {}^{G}\!/_{\mathrm{Stab}(x)} \quad \text{by} \quad \tilde{\varphi}(\overline{g}) = g\mathrm{Stab}_G(x).$$

We want to show that $\tilde{\varphi}$ is a bijection, from which the result will follow.

1. We first show that $\tilde{\varphi}$ is well-defined. For all $g_1, g_2 \in G$, suppose $\overline{g_1} = \overline{g_2}$. From above, we get that $g_2^{-1}g_1 \in \mathrm{Stab}_G(x)$, which, by definition of equivalent *left* cosets, gives $g_1\mathrm{Stab}_G(x) = g_2\mathrm{Stab}_G(x)$, which implies that $\tilde{\varphi}(\overline{g_1}) = \tilde{\varphi}(\overline{g_2})$. So $\tilde{\varphi}$ is well defined.

2. It is clear from the definition of $\tilde{\varphi}$ that it is surjective.

3. We now show that $\tilde{\varphi}$ is injective. For all $g_1, g_2 \in G$,

$$\begin{aligned} g_1\mathrm{Stab}_G(x) = g_2\mathrm{Stab}(x) &\\ &\Leftrightarrow g_2^{-1}g_1 \in \mathrm{Stab}_G(x) \\ &\Leftrightarrow \overline{g_1}(x) = \overline{g_2}(x). \end{aligned}$$

   Therefore, $\tilde{\varphi}$ is injective.

Therefore, $\tilde{\varphi}$ is a bijection, which means that

$$|[x]| = |{}^{G}\!/_{\mathrm{Stab}_G(x)}| = \frac{|G|}{|\mathrm{Stab}_G(x)|},$$

as required. ■

Definition 9.1.3

Let G be a group, X a set, and $\varphi : G \times X \to X$ a group action. We have that $\text{Stab}_X(g) = \{x \in X \mid \varphi(g,x) = x\}$, i.e., the set of those elements in x that are fixed by a particular $g \in G$. Let us now consider those elements $x \in X$ that are fixed by *every* element in G, i.e., define the set

$$\boxed{\text{Fix}(X) = \{x \in X \mid \varphi(g,x) = x \text{ for all } g \in G\}}.$$

Complementarily, we can also define the set

$$\boxed{\text{Fix}(G) = \{g \in G \mid \varphi(g,x) = x \text{ for all } x \in X\}},$$

which is the set of those elements $g \in G$ that fix *every* element in X.

Theorem 9.1.4

Let G be a group, X a set, and $\varphi : G \times X \to X$ a group action. Then,

$$\text{Fix}(X) = \bigcap_{g \in G} \text{Stab}_X(g) \quad \text{and} \quad \text{Fix}(G) = \bigcap_{x \in X} \text{Stab}_G(x).$$

In addition, $\text{Fix}(G) = \text{Kern}(\overline{\varphi})$, where recall $\overline{\varphi} : G \to S_G$ is defined by $\overline{\varphi}(g) = \varphi_g$.

Theorem 9.1.5

Let G be a group, X a set, and $\varphi : G \times X \to X$ a group action. Then $|[x]| = 1$ if and only if $x \in \text{Fix}(X)$.

PROOF: Consider an element $a \in \text{Fix}(X)$, which, by definition, is fixed by all $g \in G$. Its orbit is therefore

$$[a] = \{\varphi(g,a) \mid g \in G\} = \{a\},$$

since, as mentioned, all $g \in G$ fix a. So any element in $\text{Fix}(X)$ has an orbit of size one. Conversely, suppose $|[a]| = 1$ for some $a \in X$. Because every element in X is equivalent to itself under the equivalence relation $\sim_\varphi$, we must then have $[a] = \{a\}$, which by definition of orbits means that $\varphi(g,a) = a$ for all $g \in G$, which by definition of $\text{Fix}(X)$ means that $a \in \text{Fix}(X)$. So any element of X with an orbit of size one belongs to $\text{Fix}(X)$, completing the pf. ■

Now, we know that if a and b are in the same orbit, then $a, b \in [a]$ (or $a, b \in [b]$), i.e., there exists an $h \in G$ such that $\varphi(h,b) = a$ (or $\varphi\left(h^{-1}, a\right) = b$); in particular, then, $[a] = [b]$. Therefore,

$$|\text{Stab}_G(x)| = \frac{|G|}{|[a]|} = \frac{|G|}{|[b]|} = |\text{Stab}_G(y)|,$$

In fact, we can say more. If a and b are in the same orbit, then

$$\begin{aligned}
h^{-1}\mathrm{Stab}_G(a)\,h &= \left\{h^{-1}xh \mid x \in \mathrm{Stab}_G(a)\right\} = \left\{h^{-1}xh \mid \varphi(x,a) = a\right\} \\
&= \left\{h^{-1}xh \mid \varphi(x,\varphi(h,b)) = \varphi(h,b)\right\} \quad \text{(since } \varphi(h,b) = a \text{ from above)} \\
&= \left\{h^{-1}xh \mid \varphi(xh,b) = \varphi(h,b)\right\} \quad \text{(by definition of group action)} \\
&= \left\{h^{-1}xh \mid \varphi_{xh}(b) = \varphi_h(b)\right\} \quad \text{(alternate notation)} \\
&= \left\{h^{-1}xh \mid \varphi_h^{-1} \circ \varphi_{xh}(b) = b\right\} \\
&= \left\{h^{-1}xh \mid \varphi_{h^{-1}} \circ \varphi_{xh}(b) = b\right\} \\
&= \left\{h^{-1}xh \mid \varphi\left(h^{-1}xh, b\right) = b\right\} \\
&= \mathrm{Stab}_G(b)\,.
\end{aligned}$$

Theorem 9.1.6 The Equivalence Class Equation

Let G be a finite group, X a set, and $\varphi : G \times X \to X$ a group action. Let N be the number of orbits in the action, and let $a_1, a_2, \ldots, a_r$ be those representatives of the orbits of X such that none of them are in $\mathrm{Fix}(X)$ and none of $[a_1], [a_2], \ldots, [a_r]$ are contained in $\mathrm{Fix}(X)$ (meaning that no two of the a_i are conjugate to each other, but every element not in $\mathrm{Fix}(X)$ is equivalent to one of them). Then

$$|X| = \sum_{i=1}^{N} \frac{|G|}{|\mathrm{Stab}_G(a_i)|} = |\mathrm{Fix}(X)| + \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}_G(a_i)|}.$$

PROOF: We know that the action of G on X determines an equivalence relation $\sim_\varphi$ with the orbits $[a_i]$ as the equivalence classes. As we know, the equivalence classes partition the underlying set. Therefore,

$$|X| = \sum_{i=1}^{N} |[a_i]|\,,$$

which, by the orbit-stabiliser theorem, gives

$$|X| = \sum_{i=1}^{N} \frac{|G|}{|\mathrm{Stab}_G(a_i)|}.$$

Now, let $|\mathrm{Fix}(X)| = s$ and $b_1, b_2, \ldots, b_s$ all of the elements of $\mathrm{Fix}(X)$. Then, since each b_i is equivalent under $\sim_\varphi$ only to itself (we saw this in the paragraph above the statement of this theorem, which stated that $[b_i] = \{b_i\}$), the b_j and a_i are together the complete set of representaties of *all* the orbits, i.e., $N = r + s$. Now, since $b_i \in \mathrm{Fix}(X)$, it is fixed by all $g \in G$, which means that

$$\mathrm{Stab}_G(b_i) = \{g \in G \mid \varphi(g, b_i) = b_i\} = G,$$

i.e., $|\mathrm{Stab}_G(b_i)| = |G|$. Therefore,

$$\begin{aligned}|X| &= \sum_{i=1}^{N} \frac{|G|}{|\mathrm{Stab}_G(a_i)|} = \sum_{i=1}^{s} \frac{|G|}{|\mathrm{Stab}_G(b_i)|} + \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}_G(a_i)|} \\ &= \sum_{i=1}^{s} 1 + \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}_G(a_i)|} = s + \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}_G(a_i)|} \\ &= |\mathrm{Fix}(X)| + \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}_G(a_i)|},\end{aligned}$$

as required. ■

REMARK: Remember that by the orbit-stabiliser theorem, $\frac{|G|}{|\mathrm{Stab}_G(a_i)|} = |[a_i]|$, so that the size of X is simply the sum of the sizes of each orbit. The equivalence class equation splits the sum of sizes of each orbit into orbits of size one and orbits of size greater than one.

9.2 The Number of Orbits and Polya-Burnside Problems

In this section, we apply the orbit-stabiliser theorem above to prove Burnside's theorem, which gives a method of counting the number of orbits of a set under the action of a group of symmetries. We also illustrate how this theorem can be applied to various counting problems.

Example 9.2.1 You want to construct a string of four beads. You have a bunch of black and white beads (at least four of each, say) to choose from. How many distinct strings can you make?

SOLUTION: Before we start counting, let us think about what is meant by *distinct* strings of beads. We must keep in mind that flipping the string about its centre may change the colour scheme as read from left to right, but it will still be the same string. So we will want to avoid doubly-counting such apparently-different strings. Therefore, distinct means that our collection of strings should not contain pairs that differ only by a flip.

Now, since there are two possibilities for each bead, there are at most $2^4 = 16$ possible bead strings, each labelled by a particular colour scheme as read from left to right. Let X be the set of these colour schemes. We will use "B" to denote a black bead and "W" to denote a white bead. So we have

$$\begin{aligned}X = \{&WWWW, BWWW, WBWW, WWBW, WWWB, \\ &BBBB, WBBB, BWBB, BBWB, BBBW, \\ &BWBW, WBWB, BWWB, WBBW, BBWW, WWBB\}.\end{aligned}$$

If we don't care about flippling the strings and only care about distinctness as read from left to right, then are 16 possibilities. If we take the flipping into account, then observe that there are only four "invariant" strings that remain, i.e., only four strings that stay the same when flipped about the centre, $WWWW, BBBB, BWWB, WBBW$. The remaining

twelve come in pairs that are equivalent to each other under flipping, so that these twelve strings only give six unique ones. Therefore, there are $4 + 6 = 10$ distinct strings that we can construct. We may also write this result as $\frac{1}{2}\left(2^4 + 2^{\frac{4}{2}}\right)$.

Theorem 9.2.1 Cauchy-Frobenius-Burnside (CFB Theorem)

Let G be a finite group, X a finite set, and $\varphi : G \times X \to X$ a group action. Let N be the number of orbits in X under φ. Then

$$N = \frac{1}{|G|} \sum_{g \in G} F(g),$$

where $F(g) = |\mathrm{Stab}_X(g)|$.

REMARK: Think of $F(g)$ as the number of elements in X that are "invariant" under g in the action.

PROOF: In $G \times X$, consider all pairs (g, x), where $\varphi(g, x) = x$. Let n be the number of such pairs. We count them in two different ways. First, for a fixed $g \in G$, the number of such pairs that are of the form $(g, *)$ is exactly $F(g)$. Hence, we get the following expression for n:

$$n = \sum_{g \in G} F(g).$$

Secondly, for a fixed $x \in X$, the number of such pairs that are of the form $(*, x)$ is exactly $\mathrm{Stab}_G(x)$. Hence, also

$$n = \sum_{x \in X} |\mathrm{Stab}_G(x)|.$$

Now, by the orbit-stabiliser theorem, we know that $|\mathrm{Stab}_G(x)| = \frac{|G|}{|[x]|}$. Hence, we get the following expression for n:

$$n = |G| \sum_{x \in X} \frac{1}{|[x]|}.$$

Now, let $R = \{a_1, a_2, \ldots, a_N\}$ be the set of representatives of all the orbits of X. Then, observe that

$$\sum_{x \in X} \frac{1}{|[a]|} = \sum_{a \in R} \sum_{b \in [a]} \frac{1}{|[a]|} = \sum_{a \in R} \frac{1}{|[a]|} \sum_{b \in [a]} 1 = \sum_{a \in R} \frac{1}{|[a]|} |[a]| = \sum_{a \in R} 1 = N.$$

Therefore, we have

$$n = \sum_{g \in G} F(g) \quad \text{and} \quad n = |G| N \Rightarrow N = \frac{1}{|G|} \sum_{g \in G} F(g),$$

as required. ■

We now illustrate how to apply Burnside's theorem to specific counting problems. In all these problems, we are counting the number of orbits in some action. We first need to specify the set X and the group G acting on it, and then determine $F(g)$ for all $g \in G$.

In particular, placing the previous example in the language of this theorem, we can see that the group G is the group of symmetry transformations of the string of beads. Since there are only two such transformations, namely keeping the string in its place and flipping it about the centre, they can be represented using the group $G = \mathbb{Z}_2$, where $[0]_2$ represents keeping the string in its place and $[1]_2$ represents flipping it about its centre. Then G acts on X, which was the set of all possible colour schemes, by flipping, and we can see that $F([0]_2)$ represents the number of colour schemes that are invariant under no flipping, i.e., $F([0]_2) = 16$, and $F([1]_2)$ is the number of colour schemes that are invariant under a flip about the centre, i.e., $F([1]_2) = 4$. The CFB theorem then gives $\frac{1}{2}(16 + 4) = 10$, as before.

We now generalise this example for any number of beads and any number of possible colours.

Example 9.2.2 Consider a string of n beads (in the sense of the previous example). Each bead comes in t colours. How many distinct strings of beads of size n can be made?

SOLUTION: Like the previous example, we assume that we have as many beads of each colour as we need. There are only two symmetry transformations for the string—either we keep it in its place, or we flip it about its centre. So the group of symmetries is isomorphic to $\mathbb{Z}_2$, where $[0]_2$ represents keeping the object in its place, and $[1]_2$ represents flipping it about its centre. So let $G = \mathbb{Z}_2$. Like before, we also let X be the set of all colour schemes of the string. Then $|X| = t^n$. By the CFB theorem, the number of strings N is

$$N = \frac{1}{2} \sum_{g \in \mathbb{Z}_2} F(g).$$

Now,

$$F([0]_2) = t^n$$

since all possible colour schemes are invariant when we don't perform a flip on them. Now, as mentioned, $F([1]_2)$ is the number of colour schemes that are invariant under a flip about the centre, which means that both sides of the string must look the same. We can thus focus our attention only on one half of the string. The problem is then equivalent to determining the number of colour schemes on a half-string when no flipping is taken into account. If n is even, then there are $\frac{n}{2}$ beads on each half of the string, and if n is odd, then there are $\frac{n+1}{2}$ beads on each half, so we get

$$F([1]_2) = \begin{cases} t^{\frac{n}{2}} & \text{if } n \text{ is even;} \\ t^{\frac{n+1}{2}} & \text{if } n \text{ is odd.} \end{cases}$$

Therefore, by the CFB theorem, we get

$$N = \begin{cases} \frac{1}{2}\left(t^n + t^{\frac{n}{2}}\right) & \text{if } n \text{ is even;} \\ \frac{1}{2}\left(t^n + t^{\frac{n+1}{2}}\right) & \text{if } n \text{ is odd,} \end{cases}$$

which is the answer to our problem. You can check that this agrees with our result from the previous example in which $n = 4$ and $t = 2$.

Example 9.2.3 Consider a rigid rectangle with a bead at each corner. Each bead can be either black or white, and we have as many of each colour as we wish. How many unique rectangles can we make?

SOLUTION: We have seen before that the symmetry transformations of a rectangle are described by the Klein 4-group D_2, so we use this as our group G. Again, the set X consists of all colour schemes, and again there are 2^4 colour schemes. Starting from the top-left corner and moving counter-clockwise, they are

$$\begin{aligned} X = \{&WWWW, BWWW, WBWW, WWBW, WWWB, \\ &BBBB, WBBB, BWBB, BBWB, BBBW, \\ &BWBW, WBWB, BWWB, WBBW, BBWW, WWBB\}. \end{aligned}$$

Also, $D_2 = \{1, b, a, ab\}$, where 1 represents the rotation by 2π, or zero, b represents rotation by π, a represents a reflection about the horizontal symmetry axis, and ab represents a reflection about the vertical symmetry axis. We now determine all the colour schemes that are invariant under each symmetry transformation (remember that $WWWW$ and $BBBB$ are invariant under each one!).

$$\begin{aligned} F(1) &= 16 \quad \text{(all invariant under no rotation)} \\ F(b) &= 4 \quad \text{(pattern } ABAB\text{)} \\ F(a) &= 4 \quad \text{(pattern } AABB\text{)} \\ F(ab) &= 4 \quad \text{(pattern } ABBA \end{aligned}$$

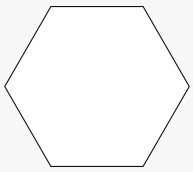
Therefore, by the CFB theorem, $N = \frac{1}{4}(16 + 4 + 4 + 4) = \frac{28}{4} = 7$ rectangles are possible.

Example 9.2.4 Consider a rigid regular hexagon with a bead at each vertex. Each bead comes in t colours, and we have as many of them as we like. How many distinct hexagons are possible?

SOLUTION: We can think of the hexagon as a necklace or a bracelet. So we want to know how many necklaces with six beads are possible when there are t choices of bead to choose from for each spot. The group describing the symmetry transformations of a regular hexagon is

$$D_6 = \left\{1, b, b^2, b^3, b^4, b^5, a, ab, ab^2, ab^3, ab^4, ab^5\right\},$$

where b represents counter-clockwise rotation by $\frac{2\pi}{6} = \frac{\pi}{3}$ and a represents a reflection about an axis of symmetry.



We will label the vertices starting from the top-left corner and moving counter-clockwise. We'll take the reflection a along the axis joining vertices 1 and 4. Now, since we have as many beads of each colour as we like, $|X| = t^6$, where X is the set of all colour schemes. Then,

$$\begin{aligned}
F(1) &= t^6 && \text{(all invariant under no rotation)}\\
F\left(b^5\right) = F(b) &= t && \text{(pattern } AAAAAA\text{)}\\
F\left(b^4\right) = F\left(b^2\right) &= t^2 && \text{(only two points free, pattern } ABABAB\text{)}\\
F\left(b^3\right) &= t^3 && \text{(only three points free, pattern } ABCABC\text{)}\\
F(a) &= t^4 && \text{(only four points free, pattern } ABCDCB\text{)}\\
F(ab) &= t^3 && \text{(only three points free, pattern } ABCCBA\text{)}\\
F\left(ab^2\right) &= t^4 && \text{(only four points free, pattern } ABCABD\text{)}\\
F\left(ab^3\right) &= t^3 && \text{(only three points free, pattern } ABBACC\text{)}\\
F\left(ab^4\right) &= t^4 && \text{(only four points free, pattern } ABACDC\text{)}\\
F\left(ab^5\right) &= t^3 && \text{(only three points free, pattern } AABCCB\text{)}
\end{aligned}$$

Therefore, by the CFB theorem,

$$N = \frac{1}{12}\left(2t + 2t^2 + 4t^3 + 3t^4 + t^6\right),$$

which is our answer. Note that we get the expected answer of 1 when $t = 1$, since there is only one way to make a necklace in which all the beads have the same colour (assuming beads of the same colour are indistinguishable, of course).

Example 9.2.5 Three black and three white beads are strung together to form a necklace, which can be rotated and turned over. Assuming that beads of the same colour are indistinguishable, how many different kinds of necklaces can be made?

SOLUTION: Again, we will be consdering the symmetry transformations of a regular hexagon, and hence the group D_6. The set X is again the set of all colour schemes, but because we are limited to three white and three black beads, $|X| \neq 2^6$. In fact, $|X| = \frac{6!}{3!3!} = 20$, and

$$\begin{aligned}
X = \{&BBBWWW, BBWBWW, BWBBWW, WBBBWW, WBBWBW,\\
&WBWBBW, WWBBBW, WWBBWB, WWBWBB, WWWBBB,\\
&BBWWBW, BWBWBW, BWWWBB, WBWWBB, BWBWWB,\\
&WBBWWB, BBWWWB, BWWBBW, WBWBWB, BWWBWB\}
\end{aligned}$$

We already have all the patterns corresponding to each rotation from the previous example, so to determine invariant colour schemes we will simply match the schemes with the patterns.

$$\begin{aligned} F(1) &= 20 \quad \text{(all invariant under no rotation)} \\ F\left(b^5\right) = F(b) &= 0 \quad \text{(pattern } AAAAAA\text{)} \\ F\left(b^4\right) = F\left(b^2\right) &= 2 \quad \text{(pattern } ABABAB\text{)} \\ F\left(b^3\right) &= 0 \quad \text{(pattern } ABCABC\text{)} \\ F(a) &= 4 \quad \text{(pattern } ABCDCB\text{)} \\ F(ab) &= 0 \quad \text{(pattern } ABCCBA\text{)} \\ F\left(ab^2\right) &= 4 \quad \text{(pattern } ABCABD\text{)} \\ F\left(ab^3\right) &= 0 \quad \text{(pattern } ABBACC\text{)} \\ F\left(ab^4\right) &= 4 \quad \text{(pattern } ABACDC\text{)} \\ F\left(ab^5\right) &= 0 \quad \text{(pattern } AABCCB\text{)} \end{aligned}$$

Therefore, the CFB theorem gives

$$N = \frac{1}{12}(20 + 2 \cdot 2 + 4 + 4 + 4) = 3,$$

so there are three necklaces possible.

9.3 The Class Equation

In this section, we study an important group action, which we already saw in an example, the action of a group G on itself by conjugation, i.e., the action $\varphi : G \times G \to G$ defined by $\varphi(g, h) = ghg^{-1}$ for all $g, h \in G$. We will derive another important counting formula concerning the orbits in this particular action. This formula will be important in understanding the structure of finite groups, and we will apply it to the study of groups whose order is a power of a prime number p.

Definition 9.3.1 Conjugate Group Elements

Let G be a group acting on itself by conjugation, i.e., define the action $\varphi : G \times G \to G$ by $\varphi(g, a) = gag^{-1}$ for all $g, a \in G$. If there exists a $g \in G$ such that $\varphi(g, a) = gag^{-1} = b$, then a and b are said to be **conjugate** in G. In other words, a and b are conjugate in G if they are in the same orbit under the action φ, i.e., if $[a] = [b]$.

As before, we define the conjugacy class as the equivalence class under conjugation. In terms of the action φ corresponding to conjugation, the conjugacy classes are simply the orbits.

Theorem 9.3.1

Let G be a group acting on itself by conjugation, i.e., define the action $\varphi : G \times G \to G$ by $\varphi(g, a) = gag^{-1}$ for all $g, a \in G$. Then the centraliser $C_G(a)$ is equal to the stabiliser $\text{Stab}_G(a)$ for all $a \in G$.

PROOF: Recall that the centraliser of a group element $a \in G$ is the set of all elements in G that commute with a, i.e.,

$$C_G(a) = \{g \in G \mid ga = ag\}.$$

However, $ga = ag \Rightarrow gag^{-1} = a \Rightarrow \varphi(g, a) = a$. In other words,

$$C_G(a) = \{g \in G \mid \varphi(g, a) = a\} = \text{Stab}_G(a)$$

by definition of the stabiliser. ■

Theorem 9.3.2

Let G be a group acting on itself by conjugation, i.e., define the action $\varphi : G \times G \to G$ by $\varphi(g, a) = gag^{-1}$ for all $g, a \in G$. Then $|[a]| = [G : C_G(a)]$ for all $a \in G$, i.e., the size of the conjugacy class of any $a \in G$ is equal to the index of $C_G(a)$ in G. If G is finite, then $|[a]| = \frac{|G|}{|C_G(a)|}$.

PROOF: By the orbit-stabiliser theorem,

$$|[a]| = [G : \text{Stab}_G(a)] = \frac{|G|}{|\text{Stab}_G(a)|}$$

when G is finite. But we have just seen that $C_G(a) = \text{Stab}_G(a)$ when G acts on itself by conjgation. Therefore,

$$|[a]| = [G : C_G(a)] = \frac{|G|}{|C_G(a)|}$$

when G is finite, as required. ■

REMARK: Note that $[a]$, for some $a \in G$, on top of being the conjugacy class containing a, can also be thought of as the set consisting of all the conjugates of a. As such $|[a]|$ can be thought of as the number of conjugates of a in G.

If a and b are in the same orbit, we have seen in general that $h^{-1}\text{Stab}_G(a)\, h = \text{Stab}_G(b)$. In this particular case, a and b in the same orbit means that a and b are in the same conjugacy class, which means that a and b are conjugates ($a = hbh^{-1}$ for some $h \in G$), and since $\text{Stab}_G(a) \equiv C_G(a)$ for all $a \in G$ when the action is conjugation, we have that

$$\text{if } h^{-1}ah = b, \text{ then } h^{-1}C_G(a)\, h = C_G(b),$$

and hence $|C_G(a)| = |C_G(b)|$, i.e., conjugate elements have the same number of elements in their centralisers. (It does not mean that the centralisers are equal!)

Theorem 9.3.3 The Conjugacy Class Equation

Let G be a finite group acting on itself by conjugation, i.e., define the action $\varphi : G \times G \to G$ by $\varphi(g, a) = gag^{-1}$ for all $g, a \in G$. Let $Z(G)$ the centre of G, and let $a_1, a_2, \ldots, a_r$ be those representatives of the conjugacy classes of G such that none of $a_1, a_2, \ldots, a_r$ are in $Z(G)$ and none of $[a_1], [a_2], \ldots, [a_r]$ are contained in $Z(G)$ (meaning that no two of the a_i are conjugate to each other, but every element not in the centre is conjugate to one of them). Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(a_i)|},$$

which is the **conjugacy class equation**, often just called the **class equation**.

PROOF: Let $|Z(G)| = s$ and $b_1, b_2, \ldots, b_s$ all of the elements of $Z(G)$. Then, since each b_i is conjugate only to itself, the b_j and a_i are together the complete set of representatives of *all* the conjugacy classes. Then, using Theorem 9.1.6, we have

$$|G| = \sum_{i=1}^{s} [G : \mathrm{Stab}_G(b_i)] + \sum_{i=1}^{r} [G : \mathrm{Stab}_G(a_i)] = \sum_{i=1}^{s} [G : C_G(b_i)] + \sum_{i=1}^{r} [G : C_G(a_i)]$$

since, as we have seen, $\mathrm{Stab}_G(a) = C_G(a)$ for all $a \in G$ when we consider the action of G on itself by conjugation. Now, since each $b_i \in Z(G)$ it commutes with every element in G, by definition. This means that $C_G(b_i) = G$, so that $[G : C_G(b_i)] = 1$. Therefore,

$$|G| = \sum_{i=1}^{s} 1 + \sum_{i=1}^{r} \frac{|G|}{|C_G(a_i)|} = s + \sum_{i=1}^{r} \frac{|G|}{|C_G(a_i)|} = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(a_i)|},$$

where we have written the index $[G : C_G(a_i)]$ as shown because G is finite. This completes the pf. ■

REMARK: Observe that in the second term of the class equation (the summation), the summand is the size of the orbit $[a_i]$, and that, based on how the representatives of these orbits were split, $|[a_i]| > 1$. Remember that the orbits of size one correspond to the elements of the centre of G since the conjugate of any element $b_i \in Z(G)$ is itself, i.e., for any $g \in G$, $gb_ig^{-1} = gg^{-1}b_i = b_i$, with the second-last step following from the fact that b_i is in the centre, and hence commutes with every element in G. Hence $[b_i] = \{b_i\}$, and so $|[b_i]| = 1$. So the size of the centre of a group is equal to the number of orbits of size one.

REMARK: Notice that the pf above is almost identical to that of the equivalence class equation. In fact, as you might have noticed, the conjugacy class equation is merely the equivalence class equation for the special case of $X = G$ and φ the action of conjugation. Therefore, $Z(G) \equiv \mathrm{Fix}(G)$ and, as we have seen already, $\mathrm{Stab}_G(a) \equiv C_G(a)$. Note that these two equivalences apply only when G acts on itself and the action is conjugation.

Example 9.3.1 Find the conjugacy classes and verify the class equation for the dihedral group D_4.

SOLUTION: We have that

$$D_4 = \left\{1, b, b^2, b^3, a, ba, b^2a, b^3a \mid ba = ab^{-1}\right\}.$$

Now,

$$\begin{aligned} aba^{-1} &= (ab)\,a = \left(b^3a\right)a = b^3a^2 = b^3 \\ bab^{-1} &= b\left(ab^3\right) = b\,(ba) = b^2a \\ b\,(ba)\,b^{-1} &= b\,(ba)\,b^3 = b^2\left(ab^3\right) = b^2\,(ba) = b^3a. \end{aligned}$$

When we say conjugacy classes, we mean the orbits of each element of D_4 when considering the action of G on itself by conjugation. Now, let $g \in D_4$. By definition of orbit, we have $[g] = \left\{hgh^{-1} \mid h \in D_4\right\}$. Therefore,

$$\begin{aligned} [1] &= \{1\} \\ \left[b^2\right] &= \left\{b^2\right\} \\ [b] &= \left\{b, b^3\right\} \\ [a] &= \left\{a, b^2a\right\} \\ [ba] &= \left\{ba, b^3a\right\}. \end{aligned}$$

Since there are two orbits of size one, we have that $|Z(D_4)| = 1$. Therefore,

$$|G| = |Z(G)| + |[b]| + |[a]| + |[ba]| = 2 + 2 + 2 + 2 = 8,$$

which verifies the class equation.

Lemma 9.3.1 Let G be a finite group. Then $[G : Z(G)] = |{}^{G}/_{Z(G)}|$ is not a prime number.

PROOF: Suppose first that G is Abelian. Then $G = Z(G)$ and $[G : Z(G)] = \frac{|G|}{|Z(G)|} = 1$, which is not prime. So the result holds for Abelian groups.

Now suppose that G is not Abelian. Assume for a contradiction that $[G : Z(G)] = p$, for p a prime number. Then ${}^{G}/_{Z(G)}$ is cyclic, so it can be generated by some element, say $gZ(G)$ of ${}^{G}/_{Z(G)}$. Then, any two distinct elements of G can be written as g^ix and g^jy for $i \neq j$, $x, y \in Z(G)$ and $g \in G - Z(G)$. But then

$$\begin{aligned} g^ixg^jy &= g^ig^jxy \quad (\text{since } x \in Z(G)) \\ &= g^{i+j}xy = g^{j+i}xy = g^jg^ixy = g^jg^iyx \quad (\text{since } x \in Z(G)) \\ &= g^jyg^ix \quad (\text{since } y \in Z(G)), \end{aligned}$$

so that any two elements in G commute, i.e., G is Abelian, a contradiction. So $[G : Z(G)]$ cannot be a prime number. ■

Theorem 9.3.4

Let G be a p-group. Then $Z(G) \neq \{1_G\}$.

PROOF: The class equation gives us

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(a_i)|},$$

where the a_i are a complete set of representatives of the orbits (conjugacy classes) not contained in $Z(G)$. Therefore, $C_G(a_i) \neq G$, and so $\frac{|G|}{|C_G(a_i)|} \neq 1$, so we must have

$$p \mid \frac{|G|}{|C_G(a_i)|}$$

But since $p \mid |G|$ (G is a p-group), it follows that $|Z(G)|$ is divisible by p, i.e.,

$$p \mid |Z(G)|.$$

Since $|Z(G)|$ is divisible by a prime, we can't have $|Z(G)| = 1$, i.e., we must have $|Z(G)| \neq 1 \Rightarrow Z(G) \neq \{1_G\}$. In particular, since $Z(G) \leq G$, $|Z(G)| \mid |G| = p^n$, and so must be p^k for some $1 \leq k \leq n$. ■

Corollary 9.3.1

If $|G| = p^2$, for p a prime number, then G is Abelian. In particular, then G is isomorphic to $\mathbb{Z}_{p^2} \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

PROOF: Let $Z(G)$ be the centre of G. Since $Z(G) \leq G$, by Lagrange's theorem, $|Z(G)|$ divides $|G|$, and hence $|Z(G)| = 1, p, p^2$ are the only possibilities since p is prime. From the previous theorem, we already know that $|Z(G)| \neq 1$. Additionally, from the lemma above, $|Z(G)| \neq p$ since this would imply that $[G : Z(G)] = \frac{p^2}{p} = p$, which that lemma shows is not possible. Hence $|Z(G)| = p^2 = |G| \Rightarrow Z(G) = G$, which means that G is Abelian. ■

Theorem 9.3.5

Let G be a finite group and $H < G$ (i.e., H is a proper subgroup). If $|G| \nmid [G : H]!$, then G is not simple.

PROOF: Let X be the set of all left cosets of H in G, i.e.,

$$X = \{aH \mid a \in G - H\}.$$

Then, $|X| = [G : H]$. Note that we thus have $|S_X| = [G : H]!$. Now, define the action

$$\varphi : G \times X \to X \quad \text{by} \quad \varphi(g, aH) = gaH$$

for all $g \in G$. We first show that φ is indeed a group action.

1. We have $\varphi(gh, aH) = ghaH = g(haH) = \varphi(g, \varphi(h, ah))$, so that the first property is satisfied.
2. We have $\varphi(1_G, aH) = 1_G aH = aH = 1_X$, so that the second property is also satisfied.

So φ is a group action, which means that $\overline{\varphi} : G \to S_X$ is a homomorphism.

We now show that $\text{Kern}(\overline{\varphi}) \neq G$. Assume for a contradiction that $\text{Kern}(\overline{\varphi}) = G$. Then $\varphi_g(aH) = gaH = aH$ for all $g, a \in G$. In particular, if $a = 1$, then $gH = H \Rightarrow g \in H$. But then also $g \in \text{Kern}(\overline{\varphi}) = G$, which implies that $H = G$, a contradiction to the assumption that H is a proper subgroup. So $\text{Kern}(\overline{\varphi}) \neq G$.

Let us also show that $\text{Kern}(\overline{\varphi}) \neq \{1_G\}$. Again, assume for a contradiction that $\text{Kern}(\overline{\varphi}) = \{1_G\}$. The first isomorphism theorem then gives

$$G/_{\{1_G\}} \cong G \cong \text{Im}(\overline{\varphi}) \leq S_X,$$

so G is isomorphic to a subgroup of S_X, which means that $|G| \mid |S_X| = [G : H]!$ (since the order of every subgroup of a group divides the order of the group), a contradiction to the assumption that $|G| \nmid [G : H]!$. Therefore, $\text{Kern}(\overline{\varphi}) \neq \{1_G\}$.

Therefore, $\text{Kern}(\overline{\varphi})$ is a non-trivial proper normal subgroup of G, and hence G is not simple. ■

Example 9.3.2 Prove that every group of order 15 is Abelian. Deduce that each such group is cyclic.

SOLUTION: Let G be a group of order 15. The positive divisors of 15 are 1, 3, 5, and 15. By the lemma above, $[G : Z(G)]$ cannot be a prime number. This rules out $[G : Z(G)] = 3$ and $[G : Z(G)] = 5$. So the index of the centre is either equal to 1 or 15. If $[G : Z(G)] = 1$, we get that $|Z(G)| = 15 \Rightarrow Z(G) = G$, and G is Abelian.

Now, suppose $[G : Z(G)] = 15 \Rightarrow |Z(G)| = 1$, i.e., that G is not Abelian. Since the centre is a subgroup, we must have $Z(G) = \{1_G\}$. Now, the class equation is

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(a_i)|},$$

where the summation is over all elements of G that represent its conjugacy classes (the orbits) of size greater than one. Remember that $Z(G)$ contains all those elements of G whose conjugacy class has size one. Since $|Z(G)| = 1$, there is only one conjugacy class of size one. Now, it is not possible to have an orbit of size 15 (why, exactly?), so we must have $\frac{|G|}{|C_G(a_i)|}$ either 3 or 5. Since $|G| = 15$, the summation must give us 14, and the only way of summing 3s and 5s to give 15 is $3 + 3 + 3 + 5$, so that

$$|G| = 15 = 1 + 3 + 3 + 3 + 5.$$

So we have three centralisers of order five, and since the centraliser is a subgroup, there are at least three subgroups of order five. Call these subgroups H_1, H_2, H_3. Now,

$$|H_1 H_2| = \frac{|H_1|\,|H_2|}{|H_1 \cap H_2|}.$$

But $|H_1 \cap H_2| = 1$ (why?), so that $|H_1 H_2| = 25$, a contradiction since $H_1 H_2 \subseteq G$ and $|G| = 15$ (a subset cannot be larger than its containing set!). So $|Z(G)| \neq 1$, and so Z is Abelian. Now, the prime factorisation of 15 is $15 = 3 \cdot 5$. By Cauchy's theorem (Abelian case), there exists p-subgroups of order 3 and 5, and by Corollary 8.2.1 G is ismorphic to these p-subgroups. We also know that each of these p-subgroups are themselves isomorphic to a direct product of cyclic p-groups based on the partitions of, in this case, one ($3 = 3^1$ and $5 = 5^1$), so $G \cong \mathbb{Z}_3 \times \mathbb{Z}_5$, and since $\gcd(3, 5) = 1$, we have $G \cong \mathbb{Z}_{15}$, which means that G is cyclic.

We now recall the definition of the normaliser of a subgroup H of a group G. (Stricly speaking, H only needs to be a *subset*.)

Definition 9.3.2 Normaliser

Let G be a group and $H \leq G$. The **normaliser** of H in G is defined as the set $N_G(H) = \left\{g \in G \mid gHg^{-1} = H\right\}$.

Recall also that $N_G(H)$ is a subgroup of G that contains H, and that $H \trianglelefteq N_G(H)$. In particular, $N_G(H)$ is the largest subgroup of G that has H as a normal subgroup.

Also recall the action of conjugation that we defined between a group G and itself as $\varphi(g, h) = ghg^{-1}$, which was the conjugate of the element $h \in G$ by another element $g \in G$. The orbit of h, denoted $[h]$, was then all the conjugates of h.

We now consider the action $\varphi : G \times X \to X$ of a group G on a set X, where X is the *set of all subgroups of* G. We define this action by

$$\varphi(g, H) = gHg^{-1} = \left\{ghg^{-1} \mid h \in H\right\}.$$

(Note that $H \leq G$.) This action can be considered as the conjugation of a subgroup. The orbit of H, denoted $[H]$, is then all of the conjugates of H, by definition. Two subgroups $H, K \leq G$ are then said to be conjugate in G if $[H] = [K]$, or equivalently, if there exists a $g \in G$ such that $K = \varphi(g, H)$. The stabiliser of this action is then

$$\mathrm{Stab}_G(H) = \{g \in G \mid \varphi(g, H) = H\} = \left\{g \in G \mid gHg^{-1} = H\right\} = N_G(H),$$

i.e., the stabiliser of $H \in X$ is simply the normaliser $N_G(H)$.

Now, the orbit of some some subgroup H of G is $[H] = \{\varphi(g, H) \mid g \in G\} = \left\{ghg^{-1} \mid g \in G\right\}$, i.e., it is the set of all the conjugates of H in G. Hence, by the orbit-stabiliser theorem, the size of the orbit of H, hence the number of conjugates of H in G, is

$$[H] = \frac{|G|}{|N_G(P)|}.$$

9.4 Conjugation in the Permutation Group S_n

Let us now consider the action of conjugation on the group $G = S_n$, i.e., let us define the action $\varphi : S_n \times S_n \to S_n$ by $\varphi(\alpha, \beta) = \alpha\beta\alpha^{-1}$. We know already that in this case $\mathrm{Stab}_G(\alpha) \equiv C_G(\alpha)$ for all $\alpha \in S_n$, so that the size of each orbit $[\alpha]$, which is the size of the conjugacy class containing α (equivalently, the number of conjugates of α, equivalently the number of elements that commute with α) is

$$|[\alpha]| = \frac{|S_n|}{|C_G(\alpha)|} = \frac{n!}{|C_G(\alpha)|}.$$

But recall that the size of each conjugacy class $[\alpha]$ is equal to the number of elements in S_n that have the same cycle structure as α since conjugate elements in S_n must have the same cycle structure. Let the cycle structure of α be $[n_1, n_2, \ldots, n_k]$. Also, for all $1 \leq m \leq n$, let l_m denote the number of elements in the cycle structure equal to m, where m, remember, is the length of a cycle in α (and the maximum possible length of a cycle is of course n). Therefore, we have

$$\boxed{|[\alpha]| = \frac{n!}{\prod_{m=1}^{n} m^{l_m} l_m!}}.$$

Using this and the expression for $|[\alpha]|$ that we get using the orbit-stabiliser theorem, we may write down the formula for the number of elements in the centraliser of α:

$$\boxed{|C_G(\alpha)| = \prod_{m=1}^{n} m^{l_m} l_m!}.$$

In fact, we know that if α and β belong to the same conjugacy class, then they are conjugate to one another, i.e., there exists a $\gamma \in S_n$ such that $\alpha = \gamma\beta\gamma^{-1}$. Also, then, $[\alpha] = [\beta]$. Therefore, as we have seen in general already, $\gamma^{-1} C_G(\alpha)\, \gamma = C_G(\beta)$, and $|C_G(\alpha)| = |C_G(\beta)|$.

Example 9.4.1 What is the order of the centraliser of $\alpha = (1\ 2\ 3) \in S_4$?

SOLUTION: The cycle structure of α is $[3, 1]$, so using the formula above gives

$$|C_G(\alpha)| = \prod_{m=1}^{4} m^{l_m} l_m! = \left(1^1 1!\right)\left(3^1 1!\right) = 3.$$

Additionally, since we know that $C_G(\alpha) \leq S_4$, and since we require $\alpha \in C_G(\alpha)$ and that any group of order three must be cyclic, we have that $C_G(\alpha) = \langle\alpha\rangle = \left\{(), \alpha, \alpha^2\right\}$.

Example 9.4.2 What is the order of the centraliser of $\alpha = (1\ 2\ 3) \in S_5$?

SOLUTION: Again, since the cycle structure of α is $[3, 1, 1]$, we get

$$|C_G(\alpha)| = \prod_{m=1}^{5} m^{l_m} l_m! = \left(1^2 2!\right)\left(3^1 1!\right) = 2 \cdot 3 = 6$$

as the order of the centraliser of $\alpha \in S_5$, i.e., there are 6 conjugates of α in S_5, i.e., there are 6 elements in S_5 that commute with α.

Example 9.4.3 Determine the number of conjugates of $\alpha = (1\ 2\ 3\ 4\ 5)$ and $\beta = (1\ 2)\,(3\ 4)$ in S_5.

SOLUTION: The cycle structure of α is $[5]$ and the cycle structure of β is $[2, 2, 1]$. Therefore,

$$|C_G(\alpha)| = 5^1 1! = 5 \quad \text{and} \quad |C_G(\beta)| = \left(1^1 1!\right)\left(2^2 2!\right) = 8,$$

so there are 5 conjugates of α and 8 conjugates of β in S_5.

9.5 Cauchy's Theorem

We now present and prove the general Cauchy theorem. First, recall that one result of Lagrange's theorem is that the order of any subgroup of a finite group is a divisor of the order of the group. Note that the converse to this result is false, i.e., just because one number divides another does not mean that there is a subgroup of that order. For example, let $G = A_5$, so that $|G| = \frac{5!}{2} = 60$. Now, 30 divides 60, so let's suppose $H \leq A_5$ such that $|H| = 30$. Then $[A_5 : H] = 2$, which means that H is a normal subgroup of A_5, a contradiction to simplicity of A_5. So there does not exist a subgroup of order 30 in A_5. Note, however, that the converse of Lagrange's theorem *does* hold for all finite Abelian groups: if a number divides the order of a group, there is a subgroup of that order. This follows from the fundamental theorem of finite Abelian groups.

Theorem 9.5.1

Let G be a finite cyclic group. For all non-negative integers n that divide $|G|$, i.e., $n \mid |G|$, there exists a subgroup of G of order n.

PROOF: Let g be a generator of G, so that $o(g) = |\langle g \rangle| = |G|$. Because $n \mid |G|$, we have $|G| = nk$ for some $k \in \mathbb{Z}$. Consider the cyclic subgroup $\langle g^k \rangle$ (since $g \in G$, we have $g^k \in G$). Then,

$$\left|\left\langle g^k \right\rangle\right| = o\left(g^k\right) = \frac{o(g)}{\gcd(k, nk)} = \frac{nk}{k} = n,$$

so that $\langle g^k \rangle$ is a subgroup of G of order n. ■

This establishes that Lagrange's theorem has a converse for all finite cyclic group, which we know are Abelian. In fact, as mentioned, we now show that the converse for Lagrange's theorem is true for all finite Abelian groups.

Theorem 9.5.2

Let G be a finite Abelian group. For all non-negative integers n that divide $|G|$ there exists a subgroup of G of order n.

PROOF: To prove this, we will use the fundamental theorem of finite Abelian groups. Now, perform a prime factorisation of $|G|$, so that

$$|G| = p_1^{m_1} p_2^{m_2} \cdots p_l^{m_l}.$$

From Corollary 8.2.1, we have that G is isomorphic to a direct product of p-subgroups, i.e.,

$$G \cong H_{p_1^{m_1}} \times H_{p_2^{m_2}} \times \cdots \times H_{p_l^{m_l}},$$

where $\left|H_{p_i^{m_i}}\right| = p^{m_i}$ for $1 \leq i \leq l$. But the classification of finite Abelian p-groups says that each $H_{p_i^{m_i}}$ is isomorphic to a direct product of cyclic p-groups, i.e.,

$$H_{p_i^{m_i}} \cong \mathbb{Z}_{p_i^{k_1}} \times \mathbb{Z}_{p_i^{k_2}} \times \cdots \times \mathbb{Z}_{p_i^{k_s}}, \quad \text{for all } 1 \leq i \leq l, \quad \text{where } k_1 + k_2 + \cdots + k_s = m_i.$$

Now, if n divides $|G|$, then we must have

$$n = p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l}$$

for some $r_1, r_2, \ldots, r_l$ with $0 \leq r_i \leq m_i$.

We now show that each $H_{p_i^{m_i}}$ has a subgroup of order $p_i^{r_i}$. Since $0 \leq r_i \leq m_i$, let us write $r_i = c_1 + c_2 + \cdots + c_s$, where $0 \leq c_j \leq k_j$ for $1 \leq j \leq s$. Then $p_i^{c_j} \mid p_i^{k_j}$ for each $1 \leq j \leq s$, so that each factor $\mathbb{Z}_{p_i^{k_j}}$ has a subgroup of order $p_i^{c_j}$, $1 \leq j \leq s$ since we have just shown that the converse of Lagrange's theorem holds for finite cyclic groups. Taking the direct product of each of these subgroups gives us a new subgroup $H'_{p_i^{m_i}}$ of $H_{p_i^{m_i}}$:

$$H'_{p_i^{m_i}} \cong \mathbb{Z}_{p_i^{c_1}} \times \mathbb{Z}_{p_i^{c_2}} \times \cdots \times \mathbb{Z}_{p_i^{c_s}}.$$

The order of this subgroup is $p_i^{c_1} \cdot p_i^{c_2} \cdots p_i^{c_s} = p_i^{c_1 + c_2 + \cdots + c_s} = p_i^{r_i}$, so that each $H_{p_i^{m_i}}$ has a subgroup of order $p_i^{r_i}$, as claimed.

Therefore, G has the subgroup H, defined as

$$H \cong H'_{p_1^{m_1}} \times H_{p_2^{m_2}} \times \cdots \times H_{p_l^{m_l}},$$

whose order is $p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l} = n$, which completes the pf. ■

Though the converse of Lagrange's theorem is generally false, there is a *partial* converse, true for *all* groups (i.e., Abelian or non-Abelian), which states that if the divisor of the order of the group is a *prime number*, then there is a subgroup of that prime order. This is the essence of Cauchy's theorem.

Theorem 9.5.3 Cauchy's Theorem, General Case

Let G be a finite group and $p \mid |G|$, where p is a prime number. Then there exists a $g \in G$ such that $o(g) = p$.

REMARK: Note that since there exists an element of order p, then certainly there exists a subgroup of order p since every element generates a cyclic subgroup.

PROOF: We have proved the case in which G is Abelian, so we only show that the result holds for G non-Abelian, and we do this by induction on $|G|$.

If a proper subgroup H of G has order divisible by p, then by (strong) induction, there is an element of order p in H, which gives us an element of order p in G. Thus, we assume for a contradictin that no proper subgroup of G has order divisible by G. For any proper subgroup H, $|G| = |H|[G:H]$, and since $|H|$ is not divisble by p, we get $p \mid [G:H]$ for every proper subgroup H of G.

Now, let $a_1, a_2, \ldots, a_k$ represent the conjugacy classes in G with size greater than one. Remember that the conjugacy classes of size one are the elements in $Z(G)$. The class equation gives

$$|G| = |Z(G)| + \sum_{i=1}^{k} \frac{|G|}{|C_G(a_i)|}.$$

Since the size of each conjugacy class represented by a_i has size greater than one, we have $C_G(a_i) \neq G$. Therefore, $p \mid [G : C_G(a)]$. Now, $p \mid |G|$ by hypothesis, and, as mentioned in the previous sentence, each element in the summand in the class equation above is divisible by p; therefore, $|Z(G)|$ is divisible by p. Now, since $|H|$ is not divisble by p, and H is a proper subgroup, we must have $G = Z(G)$, i.e., G is Abelian, a contradiction. So the order H divides p, and H contains an element of order p, which means that G contains and element of order p, which completes the pf. ■

There are many interesting results that may now be proved using Cauchy's theorem and other important theorems from this chapter and the previous one involving group orders and prime numbers.

Lemma 9.5.1 Let G be a group and $h, g \in G$ such that $o(h) = p$ and $o(g) = q$ for prime numbers p and q, which are not necessarily distinct. Then, either $\langle h \rangle = \langle g \rangle$ or $\langle h \rangle \cap \langle g \rangle = \{1_G\}$, in which case $|\langle h \rangle \langle g \rangle| = pq$.

PROOF: We split our pf into two cases.

Case 1 $p \neq q$

In this case, $\langle h \rangle = \langle g \rangle$ is not possible, so we must only prove that $\langle h \rangle \cap \langle g \rangle = \{1_G\}$. Let $k \in \langle h \rangle \cap \langle g \rangle$. Since $k \in \langle h \rangle$, we have $o(k) \mid p$ and since $k \in \langle g \rangle$ we have $o(k) \mid q$, which implies that $o(k) \mid \gcd(p, q)$. But since $p \neq q$ and p and q are primes, we must have $\gcd(p, q) = 1$. Therefore, $o(k) \mid 1 \Rightarrow o(k) = 1 \Rightarrow k = 1_G$. So the result holds, and it follows that $|\langle h \rangle \langle g \rangle| = pq$.

Case 2 $p = q$

Let $k \in \langle h \rangle \cap \langle g \rangle$ with $k \neq 1_G$. Since $p = q$, there exists $1 \leq i, j \leq p-1$ such that $k = h^i = g^j$. Now, $\gcd(i, p) = 1$, so by the extended Euclidean algorithm, there exists integers x_0, y_0 such that $ix_0 + py_0 = 1 \Rightarrow ix_0 = 1 - py_0$. Therefore,

$$\left(h^i\right)^{x_0} = \left(g^j\right)^{x_0} \Rightarrow h^{ix_0} = h^{1-py_0} = h\left(h^p\right)^{-y_0} = h \cdot 1 = h = g^{jx_0} \Rightarrow h \in \langle g \rangle \Rightarrow \langle h \rangle \subseteq \langle g \rangle .$$

Similarly, since $\gcd(j, p) = 1$, we may write $jx_0 + py_0 = 1 \Rightarrow jx_0 = 1 - py_0$ for some $x_0, y_0 \in \mathbb{Z}$. Then,

$$\left(h^i\right)^{x_0} = \left(g^j\right)^{x_0} \Rightarrow g^{jx_0} = g^{1-py_0} = g\left(g^p\right)^{-y_0} = g \cdot 1 = g = h^{ix_0} \Rightarrow g \in \langle h \rangle \Rightarrow \langle g \rangle \subseteq \langle h \rangle .$$

Therefore, $\langle h \rangle = \langle g \rangle$, as required. ■

Theorem 9.5.4

Let $|G| = np$, where $n \leq p$ and p is a prime number. Then a subgroup of order p must be a normal subgroup.

PROOF: First of all, since $|G|$ divides p, we have from Cauchy's theorem that a subgroup of order p exists.

Now, if $n = p$, then $|G| = p^2$, and we have seen that any group of prime power order is Abelian. Additionally, all subgroups of Abelian groups are normal, hence the subgroup of order p is normal, and we are done.

Assume $n < p$, and let H_p denote the subgroup of order p. We have seen that any group of prime order must be cyclic, hence H_p is cyclic, and we let $H_p = \langle h \rangle$ for some generator $h \in G$ such that $o(h) = p$. Now, for all $g \in G$, $o\left(ghg^{-1}\right) = o(g)$ (verify this general result if you are unsure), and hence by the previous lemma above, there are two possibilities: either $\left\langle ghg^{-1} \right\rangle \cap \langle h \rangle = \{1_G\}$ or $\left\langle ghg^{-1} \right\rangle = \langle h \rangle$. Suppose $\left\langle ghg^{-1} \right\rangle \cap \langle h \rangle = \{1_G\}$. Then

$$\left|\left\langle ghg^{-1} \right\rangle \langle h \rangle\right| = \frac{\left|\left\langle ghg^{-1} \right\rangle\right| |\langle h \rangle|}{\left|\left\langle ghg^{-1} \right\rangle \cap \langle h \rangle\right|} = \frac{p^2}{1} = p^2,$$

a contradiction, since $\left\langle ghg^{-1} \right\rangle \langle h \rangle \subseteq G$, and it is impossible for the size of a subgroup to be greater than the size of the set that contains it. Hence we must have $\left\langle ghg^{-1} \right\rangle = \langle h \rangle$, so that $\left\langle ghg^{-1} \right\rangle = H_p$, i.e., $ghg^{-1} \in H_p$ for all $g \in G$. Now, because H_p is cyclic, any element in it is of the form h^k for some $k \in \mathbb{Z}$. Now, since $\left(gh^k g^{-1}\right) = \left(ghg^{-1}\right)^k$, and since $ghg^{-1} \in H_p$ and H_p is a subgroup, then certainly $gh^k g^{-1} \in H_p$, for all $g \in G$ and all elements $h^k \in H_p$. Therefore, H_p is normal in G. ■

Theorem 9.5.5 Euler's Theorem

Let $n \geq 2$ and a be two coprime integers. Then $a^{\phi(n)} \equiv 1 \pmod{n}$, where ϕ is the Euler totient function.

PROOF: Recall that the order of the group $U(n)$ is $|U(n)| = \phi(n)$. Now, since a and n are coprime, we have $\gcd(a, n) = 1$, and hence by definition of $U(n)$, we have $[a]_n \in U(n)$. Therefore, since the identity element in $U(n)$ is $[1]_n$, we get $[a]_n^{\phi(n)} = [1]_n$, or, in other words, $a^{\phi(n)} \equiv 1 \pmod{n}$. ■

Corollary 9.5.1 Fermat's Little Theorem

If p is a prime number, then for any integer a, we have $a^{p-1} \equiv 1(\bmod p)$.

PROOF: We know that if p is a prime number, then $\phi(p) = p - 1$. If $\gcd(p, a) = 1$, then by Euler's theorem, we get immediately $a^{p-1} \equiv 1 \pmod{p}$, and we are done.

If $\gcd(p, a) \neq 1$, i.e., if $[a]_n \notin U(n)$, then... ■

Theorem 9.5.6

Let $|G| = pq$, where $q \leq p$ and p and q are prime numbers. If $q \nmid (p - 1)$, then G is Abelian.

PROOF: If $p = q$, then we have $|G| = p^2$, and we know already that such a group is Abelian, so we are done.

If $q < p$, then let H_p be a subgroup of order p and H_q a subgroup of order q, the existence of which is guaranteed by Cauchy's theorem. Additionally, since q and p are primes, both H_q and H_p are cyclic.

Now, let $H_p = \langle b \rangle$ such that $o(b) = p$ and $\langle a \rangle = H_q$ such that $o(a) = q$. By the above theorem, we have that H_p is a normal subgroup. Therefore, we must have $aba^{-1} \in H_p$, in particular, $aba^{-1} = b^k$ for some $1 \leq k \leq p - 1$. Observe that, in general,

$$ab^k a^{-1} = \left(aba^{-1}\right)^k$$

for all $k \in \mathbb{N}$. Since $aba^{-1} = b^k$, we get

$$ab^k a^{-1} = \left(aba^{-1}\right)^k = \left(b^k\right)^k = b^{k^2}.$$

Therefore, for all $m \in \mathbb{N}$, we have

$$\begin{aligned} a^m b a^{-m} &= a^{m-1} a b a^{-1} a^{-m+1} \\ &= a^{m-1} b^k a^{-m+1} \\ &= a^{m-2} a b^k a^{-1} a^{-m+2} \\ &= a^{m-2} b^{k^2} a^{-m+2} \\ &= a^{m-3} a b^{k^2} a^{-m+3} \\ &= a^{m-2} b^{k^3} a^{-m+3} \\ &\vdots \\ &= b^{k^m}. \end{aligned}$$

Now, set $m = q$. Since $o(a) = q$, we get

$$\begin{aligned} &a^q b a^{-q} = b = b^{k^q} \Rightarrow b^{k^q - 1} = 1_G \Rightarrow o(b) = p \mid (k^q - 1) \\ &\Rightarrow k^q - 1 = mp, \ m \in \mathbb{Z} \Rightarrow k^q = 1 + mp \Rightarrow k^q \equiv 1 \pmod{p}. \end{aligned}$$

Moreover, by Fermat's Little Theorem, $k^{p-1} \equiv 1 \pmod{p}$. Since $q \nmid (p-1)$, we have $\gcd(q, p-1) = 1$. Now, by the extended Euclidean algorithm, since $\gcd(q, p-1) = 1$, there exist integers x_0, y_0 such that

$$q x_0 + (p-1) y_0 = 1.$$

Now,

$$\begin{aligned} k^q \equiv 1 \pmod{p} &\Rightarrow [k^q - 1]_p = [1]_p \quad \text{and} \\ k^{p-1} \equiv 1 \pmod{p} &\Rightarrow \left[k^{p-1}\right]_p = [1]_p . \end{aligned}$$

Therefore,

$$\left[k^{p-1}\right]_p^{y_0} \cdot [k^q]_p^{x_0} = \left[k^{y_0(p-1)}\right]_p \cdot [k^{qx_0}] = \left[k^{qx_0 + y_0(p-1)}\right]_p = [k]_p = [1]_p ,$$

which means that $k \equiv 1 \pmod{p}$, which means that $k = 1$, since $1 \leq k \leq p-1$. Therefore, $aba^{-1} = b^k = b \Rightarrow ab = ba$, so a and b commute. Now, by Lemma 9.5.1, we must have $\langle b \rangle \cap \langle a \rangle = \{1_G\}$ since $p \neq q$, so that

$$|\langle b \rangle \langle a \rangle| = pq = |G| \Rightarrow \langle b \rangle \langle a \rangle = G,$$

since $\langle b \rangle \langle a \rangle \subseteq G$. Therefore, all $g_1, g_2 \in G$ may be written as a product of an element in $\langle a \rangle$ and an element in $\langle b \rangle$, i.e.,

$$g_1 = a^{n_1} b^{n_1'} \quad \text{and} \quad g_2 = a^{n_2} b^{n_2'}, \quad n_1, n_1', n_2, n_2' \in \mathbb{Z}.$$

Therefore,

$$\begin{aligned} g_1 g_2 &= \left(a^{n_1} b^{n_1'}\right)\left(a^{n_2} b^{n_2'}\right) \\ &= a^{n_1} a^{n_2} b^{n_1'} b^{n_2'} \quad (\text{since } ab = ba) \\ &= a^{n_1 + n_2} b^{n_1' + n_2'}, \end{aligned}$$

and similarly $g_2 g_1 = a^{n_2 + n_1} b^{n_2' n_1'} = a^{n_1 + n_2} b^{n_1' + n_2'} = g_1 g_2$. So any two elements in G commute, so that G is Abelian. ■

So we have dealt with groups whose order are a product of primes p and q such that $q \leq p$ and $q \nmid (p-1)$. Observe that this makes it much easier to prove that any group of order 15 is Abelian, since $15 = 3 \cdot 5$, 3 and 5 are primes, and $3 \nmid 4$.

We now want to consider what happens when $|G| = pq$, with $q \leq p$, but $q \mid (p-1)$. Specifically, we will consider below that case $q = 2$ and p an odd prime.

Theorem 9.5.7

Let $|G| = 2p$, for p an odd prime number. Then, either $G \cong \mathbb{Z}_2 \times \mathbb{Z}_p \cong \mathbb{Z}_{2p}$ (and hence G is cyclic), or $G \cong D_p$.

PROOF: From Cauchy's theorem, there exists a subgroup of G of order p, call it H_p, and a subgroup of order two, call it H_2. Additionally, from Theorem 9.5.4, this subgroup is a normal subgroup. Since both H_p and H_2 are of prime order, they are cyclic, so we let $H_2 = \langle a \rangle$, where $o(s) = 2$, and $H_p = \langle r \rangle$, where $o(r) = p$. Now, recall that

$$D_p = \left\langle r^p = s^2 = 1 \mid rs = sr^{-1} \right\rangle.$$

Now, $rs = sr^{-1} \Rightarrow srs = r^{-1} \Rightarrow srs^{-1} = r^{-1}s^{-2} = r^{-1}$. Now, since H_p is a normal subgroup, we have $srs^{-1} \in H_p$, which means that $srs^{-1} = r^k$ for $1 \leq k \leq p_1$. We now follow exactly the same reasoning as in the pf of Theorem 9.5.6 to conclude that

$$s^m r s^{-m} = r^{k^m} \quad \text{for all} \quad m \in \mathbb{N}.$$

Set $m = 2$, which gives

$$\begin{aligned} &s^2 r s^{-2} = r = r^{k^2} \Rightarrow r^{k^2-1} = 1_G \Rightarrow p \mid \left(k^2 - 1\right) \\ &\Rightarrow k^2 - 1 = mp, \ m \in \mathbb{Z} \Rightarrow k^2 = 1 + mp \Rightarrow k^2 \equiv 1 \pmod{p}. \end{aligned}$$

Now, the solution to $k^2 \equiv 1 \pmod{p}$ is $k = \pm 1$ since $1 \leq k \leq p-1$.

If $k = 1$, then we get $srs^{-1} = r \Rightarrow sr = rs$. Then, following the last part of the pf to Theorem 9.5.6, we get that G is Abelian, and thus by the fundamental theorem of finite Abelian groups, we get $G \cong H_2 \times H_p$, but by the classification of finite Abelian p-groups, we get $H_2 \cong \mathbb{Z}_2$ (only one partition of 2) and $H_p \cong \mathbb{Z}_p$ (possibly with others). So $G \cong \mathbb{Z}_2 \times \mathbb{Z}_p \cong \mathbb{Z}_{2p}$, since $\gcd(2, p) = 1$.

If $k = -1$, then we have $srs^{-1} = r^{-1}$, and therefore G satisfies the generator relation for D_p, hence $G \cong D_p$. ■

9.6 The Classification of Small Groups

We have looked at the classification of groups of orders involving prime numbers, and this, along with the fundamental theorem of finite Abelian groups, allows us to classify *all* groups of a particular order, at least ones of small order. In this section we will state all (up to isomorphism, of course—in other words, the isomorphism classes) of groups of order less than or equal to 25.

Now, in the preceding sections we have looked at

- Groups with order p^2;
- Groups with order pq; and
- Groups with order $2p$.

This covers most of the groups of order less than 25. Unfortunately, this does not cover groups of order 8, 12, 16, 20, and 24. Below we will work out the groups of order 8 and 12, but will leave the rest, as these involve groups that have not been covered in the course.

9.6.1 Groups of Order 8

Definition 9.6.1 **Boolean Group**

A group G is called a **Boolean group** if and only if all non-identity elements have order two.

Theorem 9.6.1

The Boolean group is Abelian.

PROOF: (Omitted for now...) ■

We have that any group of order 8 is a p-group since $8 = 2^3$. And since there are three partitions of 3, namely $[3], [2,1], [1,1,1]$, by the classification theorem for finite Abelian p-groups, there are three Abelian groups of order 8:

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \text{and} \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

More importantly, let us focus on non-Abelian groups of order 8, call it G. You may try to think right now if there are any groups, other than those above, that we have seen with order eight. Perhaps D_4? What about Q_8? Certainly, these are groups of order eight, and we should include them in our list. But are there any more?

By Lagrange's theorem, elements in G have elements of order 1, 2, 4, or 8. There can only be one element of order one, and that is the identity element. If G contains an element of order eight, then $G \cong \mathbb{Z}_8$, so G is Abelian. If $o(x) = 2$ for all $x \in G$ that are not the identity, i.e., if G is the Boolean group of order eight, then from the above theorem G is Abelian; in particular $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Hence, G contains at least one element of order four.

There are two possibilities if G contains an element of order four, and we go through these in turn. Let $o(a) = G$ for $a \in G$.

Case 1 There exists an element $b \in G - \langle a \rangle$.

In this case, either $o(b) = 2$ or $o(4) = 4$ (we implicitly rule out $o(b) = 8$ because that would immediately give $G = \langle b \rangle \cong \mathbb{Z}_8$). Observe that since $[G : \langle a \rangle] = 2$, we must have $\langle a \rangle \trianglelefteq G$.

If $o(b) = 2$, then $\langle b\rangle \cap \langle a\rangle = \{1_G\}$, and hence

$$|\langle b\rangle \langle a\rangle| = |\langle b\rangle|\,|\langle a\rangle| = 2 \cdot 4 = 8 = |G|\,.$$

Since $\langle b\rangle \langle a\rangle \subseteq G$, we must have $\langle b\rangle \langle a\rangle = G$, so every element in G may be written as a product of a power of b and a power of a, so our problem has been reduced to determining how a and b are related. Now, since $\langle a\rangle \trianglelefteq G$, $bab^{-1} = bab = a^k$ for $1 \leq k \leq 3$. Then, following the same reasoning as in the pf of Theorem 9.5.6, we have

$$b\left(bab^{-1}\right)b^{-1} = ba^kb^{-1} \Rightarrow a = a^{k^2} \Rightarrow a^{k^2-1} = 1 \Rightarrow o(a) = 4 \mid k^2 - 1 \Rightarrow k = 1 \text{ or } k = 3.$$

If $k = 1$, then we get $bab^{-1} = a \Rightarrow ba = ab$, so that G is Abelian by following the same reasoning as in the last part of the pf of Theorem 9.5.6. In particular, we must have $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ (since all the other Abelian options have already been accounted for). If instead $k = 3$, then we get $bab^{-1} = b^3 = b^{-1}$, which is nothing but the generator relation for the dihedral group, i.e., we must have $G \cong D_4$.

If $o(b) = 4$, then we must have that all elements in $G - \langle a\rangle$ are of order four (why?), and this is the second case we consider.

Case 2 All elements in $G - \langle a\rangle$ are of order four.

Let $c \in G - \langle a\rangle$, with $o(c) = 4$. Again, since $\langle a\rangle \trianglelefteq G$, we must have $cac^{-1} = a^k$ for $1 \leq k \leq 3$. Then,

$$c\left(cac^{-1}\right)c^{-1} = ca^kc^{-1} = a^{k^2} \Rightarrow c^2ac^{-2} = a^{k^2}.$$

Now, note that

$$o\left(c^2\right) = \frac{o(c)}{\gcd(o(c), 2)} = \frac{4}{\gcd(4, 2)} = \frac{4}{2} = 2,$$

which implies that $c^2 \in \langle a\rangle$ since all elements in $G - \langle a\rangle$ are of order four. In fact, since all the powers of a in $\langle a\rangle$ are distinct, and $|\langle a\rangle| = 4$, there is only one element of order two in $\langle a\rangle$, and that is a^2, which means that $c^2 = a^2$. Therefore, using this in the above equation, we get

$$a^2aa^{-2} = a = a^{k^2} \Rightarrow a^{k^2-1} = 1 \Rightarrow 4 \mid k^2 - 1 \Rightarrow k = 1 \text{ or } k = 3.$$

If $k = 1$, we get $cac^{-1} = a \Rightarrow ca = ac$, which again leads to G being Abelian since $\langle c\rangle \cap \langle a\rangle = \left\langle c^2\right\rangle = \{1_G\}$, i.e., $\langle c\rangle \langle a\rangle = G$.

If $k = 3$, then we get $cac^{-1} = c^3 = a^{-1}$, which, though it looks the same, is *not* the same generator relation as the one for the dihedral group because $o(c) = 4$, and for the dihedral group we would have required $o(c) = 2$. So we have some group that can be described as $G = \left\langle a, c \mid a^4 = c^4 = 1, c^2 = a^2, cac^{-1} = a^{-1}\right\rangle$, which is indeed the generator relation for the *quaternion group* Q_8.

Since we have exhausted all possible cases, we conclude that D_4 and Q_8 are the only non-Abelian groups of order 8, and hence there are only five groups of order eight, and they are

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad D_4, \quad \text{and} \quad Q_8.$$

9.6.2 Groups of Order 12

Definition 9.6.2 Dicyclic Group

The **dicyclic group** of degree n, denoted Dic_n, is a non-Abelian group of order with generator relation

$$\mathrm{Dic}_n = \left\langle a, x \mid a^{2n} = x^4 = 1, x^2 = a^n, xax^{-1} = a^{-1} \right\rangle.$$

For $n > 1$, $|\mathrm{Dic}_n| = 4n$.

Observe that for $n = 2$ we get

$$\mathrm{Dic}_2 = \left\langle a, x \mid a^4 = x^4 = 1, x^2 = a^2, xax^{-1} = a^{-1} \right\rangle = Q_8,$$

so the dicyclic group provides, in a sense, a generalisation to groups that are similar in structure to the quaternion group.

We are now ready to present our table of all group of order up to 25. The two main characteristics of a group are whether or not it is Abelian and whether or not it is cyclic. Of course, a group may be some combination of both. The possible combinations are

- Abelian and not cyclic (for example, the Klein 4-Group);
- Abelian and cyclic (for example, $\mathbb{Z}_n$);
- non-Abelian and not cyclic (for example, S_n for $n \geq 3$).

Note that it is not possible for a group to be non-Abelian and cyclic, since a non-Abelian group implies that the group is not cyclic (remember that all cyclic groups are Abelian!).

Order	Groups	Properties	Notes
1	$\{1_G\}$	Trivial group; Abelian, cyclic	
2	$\{1_G, a\}$	Abelian, cyclic	
3	$\{1_G, a, a^2\}$	Abelian, cyclic	
4	$\mathbb{Z}_4$	Abelian, cyclic	Theorem 9.5.7
	$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong D_2$	Abelian; not cyclic	Klein 4-Group
5	$\mathbb{Z}_5$	Prime order, so cyclic, so Abelian	
6	$\mathbb{Z}_6$	Abelian, cyclic	Theorem 9.5.7
	$S_3 \cong D_3$	non-Abelian, not cyclic	
7	$\mathbb{Z}_7$	Prime order, so cyclic, so Abelian	
8	$\mathbb{Z}_8$	Abelian, cyclic	
	$\mathbb{Z}_2 \times \mathbb{Z}_4$	Abelian, not cyclic	
	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	Abelian, not cyclic	
	D_4	not Abelian, not cyclic	
	Q_8	not Abelian, not cyclic	Quaternion Group
9	$\mathbb{Z}_9$	Abelian, cyclic	Theorem 9.5.6 or Corollary 9.3.1
	$\mathbb{Z}_3 \times \mathbb{Z}_3$	Abelian, not cyclic	
10	$\mathbb{Z}_{10}$	Abelian, cyclic	Theorem 9.5.7
	D_5	non-Abelian, not cyclic	
11	$\mathbb{Z}_{11}$	Prime order, so cyclic, so Abelian	
12	$\mathbb{Z}_{12}$	Abelian, cyclic	
	A_4	non-Abelian, not cyclic	
	D_{12}	non-Abelian, not cyclic	
	$\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \times \mathbb{Z}_2$	Abelian, not cyclic	
	Dic_4	non-Abelian, not cyclic	Dicyclic Group
13	$\mathbb{Z}_{13}$	Prime order, so cyclic, so Abelian	
14	$\mathbb{Z}_{12}$	Abelian, cyclic	Theorem 9.5.7
	D_7	non-Abelian, not cyclic	
15	$\mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$	Abelian, cyclic	
17	$\mathbb{Z}_{17}$	Prime order, so cyclic, so Abelian	
19	$\mathbb{Z}_{19}$	Prime order, so cyclic, so Abelian	

9.7 The Sylow Theorems

In this section we state and prove the very important Sylow theorems. Recall Theorem 8.1.2, which stated that for finite *Abelian* groups whose orders are divisible by p^k there exists a unique p-subgroup of order p^k (confirm the unique part!!). In this section we will generalise this assertion to *all* groups, which will be *Sylow's First Theorem*.

Theorem 9.7.1

Let G be a p-group, i.e., let $|G| = p^n$ for some $n \in \mathbb{Z}$. Then, for every divisor p^k of p^n, where $k \in \mathbb{Z}$ such that $0 \leq k \leq n$, there is a subgroup of order p^k.

PROOF: If G is Abelian, then the result follows from Theorem 9.5.2.

Assume, then, that G is non-Abelian. We will perform induction on n. Assume that for $1 \leq j \leq n-1$ the statement is true, i.e., that for all $1 \leq j \leq n-1$ such that $i \neq j$, $|G| = p^j$ and hence there exists a subgroup of G of order p^i. Then, for $|G| = p^n$, we know that $Z(G) \neq \{1_G\}$, so since $Z(G) \leq G$, we must have $|Z(G)| = p^l$ for some $l \leq 1$. Note that since $Z(G)$ is an Abelian group, the results holds for it. Now, for any $1 \leq k \leq n$, if $k \leq l$, then the result holds simply by taking a subgroup of $Z(G)$, which will have prime power order that divides p^n and will also necessarily be a subgroup of G.

So assume that $k > l$, and consider the quotient group $G/Z(G)$. Observe that

$$|G/Z(G)| = p^{n-l} < p^n.$$

Therefore, by (strong) induction, the result holds for $G/Z(G)$, so that there is a subgroup, call it $\tilde{H}_k$, of $G/Z(G)$ such that $\left|\tilde{H}_k\right| = p^{k-l}$. Now, by the correspondence theorem, the subgroup $\tilde{H}_k$ is of the form $\frac{H_k}{Z(G)}$ for some $H_k \leq G$. Therefore,

$$|H_k/Z(G)| = \frac{|H_k|}{|Z(G)|} = \left|\tilde{H}_k\right| = p^{k-l} \Rightarrow |H_k| = p^{k-l}|Z(G)| = p^{k-l}p^l = p^k,$$

so we have found a subgroup $H_k \leq G$ with order p^k, as required. ■

Definition 9.7.1 Sylow p-Subgroup

Let G be a finite group and p a prime number. A **Sylow p-Subgroup** of G is a maximal p-subgroup of G. In other words, if H is a Sylow p-subgroup of G, then

1. $|H| = p^k$ for some $k \in \mathbb{Z}$ (this captures the p-subgroup part); and
2. if $H \leq L \leq G$ and L is a p-subgroup of G, then $H = L$ (this captures the maximal part).

Sylow p-subgroups are sometimes called p-Sylow subgroups, or just Sylow subgroups.

Example 9.7.1 Let $G = S_3$, so that $|G| = 3! = 2 \cdot 3$. For $p = 3$, there is the Sylow 3-subgroup $A_3 \langle (1\ 2\ 3) \rangle$. Since $(1\ 2\ 3)$ and its inverse $(1\ 3\ 2)$ are the only elements of order three, this is the only Sylow 3-subgroup. For $p = 2$, there are three Sylow 2-subgroups of S_3, namely $\langle (1\ 2) \rangle$, $\langle (1\ 3) \rangle$, and $\langle (2\ 3) \rangle$. Since $(1\ 3)(1\ 2)(1\ 3) = (2\ 3)$ and $(2\ 3)(1\ 2)(2\ 3) = (1\ 3)$, the three sylow 2-subgroups are all conjugate to each other.

Example 9.7.2 Let $G = A_4$, so that $|G| = 2^2 \cdot 3$. For $p = 2$, G has the Sylow 2-subgroup (of order four) $\{1_G, (1\ 2)(2\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Since its three non-identity elements are all the elements of order two in G, this is the only Sylow 2-subgroup. For $p = 3$, G also has at least four Sylow 3-subgroups (of order 3), namely $P = \langle (1\ 2\ 3) \rangle$, $\langle (1\ 2\ 4) \rangle$, $\langle (1\ 3\ 4) \rangle$, and $\langle (2\ 3\ 4) \rangle$. Since the four elements displayed and their inverses are all the elements of order three, these are all the Sylow 3-subgroups. We can verify that

$$\begin{aligned}(1\ 2)(3\ 4)P(1\ 2)(3\ 4) &= \langle (1\ 2\ 4) \rangle \\ (1\ 3)(2\ 4)P(1\ 3)(2\ 4) &= \langle (1\ 3\ 4) \rangle \\ (1\ 4)(2\ 3)P(1\ 4)(2\ 3) &= \langle (2\ 3\ 4) \rangle,\end{aligned}$$

so that all the Sylow 3-subgroups are conjugate to one another.

Example 9.7.3 Let $G = D_6 = \left(1, b, b^2, \ldots, a, ba, b^2a, \ldots, b^5a\right\}$, where as usual b is a rotation by $\frac{2\pi}{6} = \frac{\pi}{3}$ and a is a reflection about some axis of symmetry. Now, $|G| = 2^2 \cdot 3$, so that for $p = 3$ there is just one Sylow 3-subgroup (of order three), $\left\{1, b^2, b^4\right\}$, since b^2 and b^4 are the only elements of order three. For $p = 2$, G has at least three Sylow 2-subgroups (of order four), namely $Q = \left\{1, a, b^3, b^3a\right\}$, $\left\{1, ba, b^3, b^4a\right\}$ and $\left\{1, b^2a, b^3, b^5a\right\}$. The seven non-identity elements displayed are all the elements of order two, and there are no elements of order four, so any Sylow 2-subgroup would have to be made up of the identity and three of these seven elements. It follows that there are no other Sylow 2-subgroups than the three just shown because any group of order four is Abelian and no two of b^3a, b^4a, b^5a commute with each other. We can verify that

$$\begin{aligned}b^2Qb^4 &= \left\{1, b^2a, b^3, b^5a\right\} \\ bQb^5 &= \left\{1, ba, b^3, b^4a\right\},\end{aligned}$$

so that the three Sylow 2-subgroups are conjugate to each other.

Lemma 9.7.1 Let G be a finite group and P a Sylow p-subgroup. If $g \in G$ satisfies the following requirements, then $g \in P$:

1. $o(g) = p^l$ for some l (i.e., $\langle g \rangle$ is a p-subgroup) (really only need $g^{p^l} = 1_G$); and
2. $gPg^{-1} = P$, i.e., $g \in N_G(P)$.

PROOF: Remember that $P \trianglelefteq N_G(P)$. We therefore consider the quotient group ${}^{N_G(P)}/_P$, and an element $gP \in {}^{N_G(P)}/_P$, where $g \in N_G(P)$ and $o(g) = p^l$ for some $l \in \mathbb{Z}$, as per the requirements. Let $\overline{g} = gP$. Since $o(g) = p^l$, we must have $o(\overline{g}) \mid p^l$, so let $o(\overline{g}) = p^k$ for some $k \in \mathbb{Z}$. Now, by the correspondence theorem, the subgroup $\langle \overline{g} \rangle$ of ${}^{N_G(P)}/_P$ corresponds to a subgroup $\overline{P}$ of P, i.e., $\langle \overline{g} \rangle$ is of the form ${}^{\overline{P}}/_P$. Therefore, $\left|\overline{P}\right| = |P|\,|\langle \overline{g} \rangle| = |P|\,p^k$. Since P is a Sylow p-subgroup, we must have that $\overline{P}$ is also a p-group. However, by the maximality of P, we must have $\overline{P} = P$, which means that $k = 0$; therefore, $o(\overline{g}) = 1$, which means that $\overline{g}$ is the identity in ${}^{N_G(P)}/_P$, i.e., $gP = P \Rightarrow g \in P$. ■

Corollary 9.7.1

Let G be a finite group and P a Sylow p-subgroup. Then $p \nmid \frac{|N_G(P)|}{|P|}$.

PROOF: Let G be a finite group and P a Sylow p-subgroup. Assume for a contradiction that p does divide $\frac{|N_G(P)|}{|P|}$. Then, by Cauchy's theorem, there exists a $g \in N_G(P)$ such that $o(gP) = p$ in ${}^{N_G(P)}/_P$, i.e., $(gP)^p = g^p P = P \Rightarrow g^p \in P \Rightarrow (g^p)^{|P|} = 1$ by Lagrange's theorem, which implies that $(g^p)^{p^k} = 1$ for some k, where $|P| = p^k$. Therefore, $g^{p^{k+1}} = 1$, and since $g \in N_G(P)$, we have by the lemma above that $g \in P$, a contradiction to the fact that $o(gP) = p$ in ${}^{N_G(P)}/_P$. ■

Corollary 9.7.2

If Q is another p-subgroup in $N_G(P)$, where P is a Sylow p-subgroup of G, then $Q \leq P$.

PROOF: Since $Q \leq N_G(P)$ and Q is a p-subgroup, for all $g \in Q$, $o(g) = p^k$ for some $k \in \mathbb{Z}$ and $g \in N_G(P)$. Therefore, by the lemma above $g \in P$, which means that $Q \subseteq P$, which means that $Q \leq P$. ■

Theorem 9.7.2 Sylow's Theorems

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

1. Every Sylow p-subgroup of G has order p^k (*Sylow's First Theorem*);
2. All Sylow p-subgroups of G are conjugate to each other (*Sylow's Second Theorem*); and
3. If n_p is the number of Sylow p-subgroups of G, then $n_p \equiv 1 \pmod{p}$ and $n_p \mid m$ (*Sylow's Third Theorem*).

PROOF: The pf will establish the results in reverse order, i.e., we will first prove 3 and 2, and this will lead to 1.

Now, let P be a Sylow p-subgroup and X be the set of conjugates of P in G, i.e., $X =$

$\left\{gPg^{-1} \mid g \in G\right\}$. Suppose that $X = \{P, P_2, P_3, \ldots, P_l\}$. Let H be a p-subgroup of G (the existence of which is guaranteed by Cauchy's theorem since p divides $|G|$), and consider of action of H on X by conjugation, i.e., define $\varphi : H \times X \to X$ by $\varphi(h, P_i) = hP_ih^{-1}$ for all $h \in H$ and all $P_i \in X$. Note that $hP_ih^{-1} \in X$ because $H \leq G$. Then, recall that the orbit of an element of X, in this case $[P_i]$, is defined as

$$[P_i] = \{\varphi(h, P_i) \mid h \in H\}.$$

Based on what we have seen before with group actions and their orbits, the size of the orbit $[P_i]$ will be equal to one when all $h \in H$ fix P_i, i.e., when $\varphi(h, P_i) = hP_ih^{-1} = P_i$ for all $h \in H$. In other words, $|[P_i]| = 1 \Leftrightarrow P_i \in \text{Fix}(X)$. But $hP_ih^{-1} = P_i$ also means that $h \in N_G(P_i)$. In fact, when $hP_iH^{-1} = P_i$ for all $h \in H$, we have $N_H(P_i) = H \subseteq N_G(P_i)$. Therefore, by the second corollary above, $H \leq P_i$. So, under this action, $|[P_i]| = 1$ when $H \leq P_i$. In other words, H is a subgroup of one of the conjugates of P. We now have two cases to consider. First, we let H be one of the conjugates P_i of P, and second, we let $H = Q$, where Q is some Sylow p-subgroup not in X.

Case 1 $H = P_i$ for some $i \in \{1, 2, \ldots, l\}$

The action thus becomes $\varphi : P_i \times X \to X$. By maximality of the Sylow p-subgroups in X, $P_i \nsubseteq P_j$ for $i \neq j$. Thus, in this action, there is only one orbit with size one, and that is $[P_i]$. Therefore, $|\text{Fix}(X)| = 1$, and the equivalence class equation gives

$$|X| = l = 1 + \sum \frac{|P_i|}{\text{Stab}_{P_i}(a)},$$

where the summation is over all representatives of the orbits of size greater than one. Now, being a Sylow p-subgroup, $|P_i|$ is some power of p. Hence, by Theorem 9.7.1, all subgroups of P_i, in particlar $|\text{Stab}_{P_i}(a)|$ is some power of p less than that of $|P_i|$ for all $a \in X$. The sum in the above equivalence class equation is thus a sum of powers of p, say $p^{x_1} + p^{x_2} + \cdots$, where every p_{x_i} is less than (or equal to) the order of P_i. We may remove a factor of p from the sum to write $p\left(p^{x_1-1} + p^{x_2-1} + \cdots\right) = pn$, where $n \in \mathbb{Z}$. Therefore, the equivalence class equation becomes

$$l = 1 + np \Rightarrow l \equiv 1 \pmod{p}.$$

Case 2 $H = Q$, where $Q \notin X$ is a Sylow p-subgroup of G.

Assume for a contradiction that $Q \neq X$. Since $H \nleq P_i$, we have that $|[P_i]| \neq 1$ for any $P_i \in X$, i.e., there are no orbits of size one in this action, i.e., $|\text{Fix}(X)| = 1$. Therefore, the equivalence class equation gives

$$|X| = l = 0 + \sum \frac{|Q|}{|\text{Stab}_Q(a)|} = pr, \ r \in \mathbb{Z},$$

where we again rewrite the sum as before. So we have $l \equiv 0 \pmod{p}$, a contradiction to the fact that $l \equiv 1 \pmod{p}$. Therefore, we must have $Q \in X$, which means that all Sylow p-subgroups are conjugate to one another. This completes the pf of the second theorem, and establishes that each Sylow p-subgroup should be of the same size, since $|P_i| = \left|gP_ig^{-1}\right|$ for any $g \in G$. The pf of the third theorem is also complete since all the Sylow p-subgroups in G are contained in X and $|X| = l$; therefore, $l = n_p \equiv 1 \pmod{p}$.

All that remains is to show that each Sylow p-subgroup has size p^k and that $n_p \mid m$. Consider the action $\varphi : G \times X \to X$. Observe that in this case

$$[P] = \{\varphi(g, P) \mid g \in G\} = \left\{gPg^{-1} \mid g \in G\right\} = X,$$

and that

$$\text{Stab}_G(P) = \{g \in G \mid \varphi(g, P) = P\} = \left\{g \in G \mid gPg^{-1} = P\right\} = N_G(P).$$

Therefore, by the orbit-stabiliser theorem, we get

$$|[P]| = |X| = n_p = \frac{|G|}{|\text{Stab}_G(P)|} = \frac{|G|}{|N_G(P)|},$$

which implies that

$$|G| = [G : N_G(P)]\,[N_G(P) : P]\,|P| = n_p \frac{|N_G(P)|}{|P|}\,|P| = p^k m.$$

Now, by the first corollary above, since P is a Sylow p-subgroup, $p \nmid \frac{|N_G(P)|}{|P|}$, which means that $\frac{|N_G(P)|}{|P|}$ must not contain any factors of p; and we have that since $n_p \equiv 1 \pmod{p}$ $p \nmid n_p$, i.e., n_p does not contain any factors of p. Therefore, we must have $|P| = p^k$ and $m = n_p \frac{|N_G(P)|}{|P|} \Rightarrow n_p \mid m$, which completes the pf. ■

Observe that Sylow's first theorem immediately implies Cauchy's theorem in the general case.

Corollary 9.7.3

[Cauchy's Theorem, General Case] Let G be a finite group. For every prime divisor p of $|G|$ there is an element $g \in G$ with $o(g) = p$.

PROOF: Letting $|G| = pm$, where $\gcd(p, m) = 1$, we get from Sylow's first theorem that there exists a Sylow p-subgroup of G, call it P. Since p divides the order of G, P is non-trivial. Pick a non-identity element $x \in P$. By Lagrange's theorem, $o(x)$ divides $|P|$, and since P is a p-group, we must have that $o(x)$ is a prime power, say p^r where $r \geq 1$. Now,

$$o\left(x^{p^{r-1}}\right) = \frac{o(x)}{\gcd\left(o(x), p^{r-1}\right)} = \frac{p^r}{\gcd\left(p^r, p^{r-1}\right)} = \frac{p^r}{p^{r-1}} = p,$$

so that we have found an element of order p in G. ■

Corollary 9.7.4

Let G be a finite group and p a prime divisor of $|G|$. Then $n_p = 1$ (i.e., the Sylow p-subgroup is unique) if and only if the Sylow p-subgroup P is a normal subgroup of G. Hence, if the number of Sylow p-subgroups of G is one, then G is not simple.

PROOF: Recall from the pf of Sylow's theorems that if we let X be the set of conjugates of P, then G acting on X by conjugation has the orbit $[P] = X$, and since X contains all the Sylow p-subroups of G, we have $n_p = 1 = |[P]| \Rightarrow P \in \text{Fix}(X) \Rightarrow gPg^{-1} = P \ \forall g \in G \Rightarrow gP = Pg \ \forall g \in G$, which means by definition that P is a normal subgroup of G. ■

Corollary 9.7.5

Let G be a finite group with $|G| = p^k m$, where $k \geq 1$, $\gcd(p, m) = 1$, and p is a prime number. Then, for every divisor p^l of p^k, where $l \in \mathbb{Z}$ and $0 \leq l \leq k$, there exists a subgroup of order p^l.

PROOF: By Sylow's first theorem, there exists a Sylow p-subgroup of G, call it P, such that $|P| = p^k$. Then, by Theorem 9.7.1, there exists a subgroup of P of order p^l for every divisor p^l of p^k, which is certainly also a subgroup of G. ■

Example 9.7.4 Consider $G = S_4$, so that $|G| = 4! = 24 = 2^3 \cdot 3$. So a Sylow 2-subgroup of G exists and has order eight by Sylow's first theorem. Indeed, we know that the dihedral group D_4 has a permutation representation as a subgroup of S_4, so that D_4 is a Sylow 2-subgroup of S_4.

Example 9.7.5 Consider $G = A_5$, so that $|G| = \frac{5!}{2} = 60 = 2^2 \cdot 15$. So a Sylow 2-subgroup of G exists and has order four by Sylow's first theorem. The following are two Sylow 2-subgroups:

$$P = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$
$$Q = \{1, (1\ 2)(3\ 5), (1\ 3)(2\ 5), (1\ 5)(2\ 3)\}.$$

According to Sylow's second theorem, these should be conjugate in A_5. Indeed, letting $a = (2\ 3)(4\ 5)$, then $a(1\ 2)(3\ 4)b^{-1} = (1\ 3)(2\ 5)$ and $a(1\ 3)(2\ 4)a^{-1} = (1\ 2)(3\ 5)$ and $a(1\ 4)(2\ 3)a^{-1} = (1\ 5)(2\ 3)$, so that $aPa^{-1} = Q$.

Example 9.7.6 Consider again $G = A_5$. We may write $|G| = 2^2 \cdot 3 \cdot 5$, so that by Sylow's first theorem there exist Sylow 2-, 3-, and 5-subgroups of order four, three, and five, respectively. There are no elements of order four in A_5 (since these would have to be 4-cycles, which are odd permutations), and the only elements of order two are products of disjoint 2-cycles of the form $(x\ y)(u\ v)$. Each such permutation belongs to a subgroup $\{(), (x\ y)(u\ v), (x\ u)(y\ v), (x\ v)(u\ y)\}$ as in the previous example, and each such subgroup contains three such permutations. The number of such permutations turns out to be 15 (do this!). Therefore, the number of Sylow 2-subgroups is $\frac{15}{3} = 5$. As for Sylow 3- and 5-subgroups, these will be generated by 3-cycles and 5-cycles, respectively. It can be shown that the number of 3-cycles in A_5 is 20 and the number of 5-cycles in A_5 is 24. Since each

subgroup of order three contains two 3-cycles and each subgroup of order five contains four 5-cycles, the total numbers of such groups are $\frac{20}{2} = 10$ and $\frac{24}{4} = 6$, respectively. Note that

$$\begin{aligned} 5 &\equiv 1 \pmod 2 \quad \text{and} \quad 5 \mid 3 \cdot 5 \\ 10 &\equiv 1 \pmod 3 \quad \text{and} \quad 10 \mid 2^2 \cdot 5 \\ 6 &\equiv 1 \pmod 5 \quad \text{and} \quad 6 \mid 2^2 \cdot 3, \end{aligned}$$

which agrees with Sylow's third theorem.

Example 9.7.7 Let $P = \left\{ (), a = (1\ 2\ 3), a^2 = (1\ 3\ 2) \right\}$ be a Sylow 3-subgroup of A_5. Let us find the normaliser $N_G(P)$ of P in A_5. From the previous example, we know that P has 10 conjugates, so that by the orbit-stabliser theorem, $\frac{|A_5|}{|N_G(P)|} = 10$, and so we should have $|N_G(P)| = \frac{|A_5|}{10} = 6$. Since $P \subseteq N_G(P)$, we need only find an element x of order two in $N_G(P)$. We can verify that if $x = (2\ 3)(4\ 5)$, then $xax^{-1} = a^2$ and $xa^2x^{-1} = a$. So $x \in N_G(P)$, and hence $N_G(P) = \left\{ (), a, a^2, x, xa, xa^2 \right\}$.

9.8 Applications of Sylow's Theorems

In this section we go through several examples of how Sylow's theorems can be used to prove several results about Abelian and non-Abelian groups.

Example 9.8.1 Show that every group G of order 45 is Abelian.

SOLUTION: We have that $45 = 3^2 \cdot 5$. Let P_5 and P_3 be a Sylow 5-subgroup and a Sylow 3-subgroup, respectively. These groups are of orders 5 and 9, respectively, by Sylow's first theorem, and since 5 is a prime we know that P_5 is cyclic, hence Abelian; since $9 = 3^2$, we know that P_3 is Abelian. By Sylow's third theorem, n_3, which is the number of Sylow 3-subgroups in G, is of the form $1 + 3k$ for $k \in \mathbb{Z}$ (since $n_3 \equiv 1 \pmod p$); as well, $n_3 \mid 5$. The only number n_3 satisfying both requirements is $n_3 = 1$, which means that there is only one Sylow 3-subgroup in G, which by Corollary 9.7.4 means that P_3 is normal in G. Similarly, n_5 is of the form $1 + 5k$ for $k \in \mathbb{Z}$ and it divides 9. Again, the only possibility is $n_5 = 1$ so there is only one Sylow 5-subgroup, namely P_5, and we know that it is normal in G. Since P_3 contains elements whose orders divide 9 and P_5 contains elements whose orders divide 5 (in fact, since 5 is a prime, all non-identity elements must be of order five), we must have $P_3 \cap P_5 = \{1_G\}$, which means that $|P_3P_5| = |G| = 45 \Rightarrow P_3P_5 = G$. Now, recall the internal direct product theorem. In that theorem, we require two normal subgroups of G such that their subset product is equal to G and such that their intersection is trivial. P_3 and P_5 satisfy all three requirements, and so we conclude that $G \cong P_3 \times P_5$. Now, since P_3 is Abelian; we have from the fundamental theorem of finite Abelian groups that $P_3 \cong \mathbb{Z}_9$ or $P_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Since P_5 is cyclic, we know immediately that $P_5 \cong \mathbb{Z}_5$. So $G \cong \mathbb{Z}_9 \times \mathbb{Z}_5$ or

$G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. Since the direct product of Abelian groups is Abelian, we have that G is Abelian.

Example 9.8.2 Show that every group G of order 99 is Abelian.

SOLUTION: We follow the same reasoning as in the previous example. We have $99 = 3^2 \cdot 11$, so we let P_3 and P_{11} be a Sylow 3-subgroup and a Sylow 11-subgroup of G, respectively. We have that P_3 is Abelian since its order is a prime power, and since 11 is a prime we have that P_{11} is cyclic, hence Abelian. By Sylow's third theorem, $n_3 = 1+3k$, $k \in \mathbb{Z}$ and $n_3 \mid 11$, which implies that $n_3 = 1$, so P_3 is normal in G. Similarly, $n_{11} = 1+11k$, $k \in \mathbb{Z}$, and $n_{11} \mid 9$, which means that $n_{11} = 1$, i.e., P_{11} is normal in G as well. Now, since P_3 contains elements whose orders divide 9 and since all non-identity elements of P_{11} must be of order 11 (since 11 is a prime), we have that $P_3 \cap P_{11} = \{1_G\}$, which means that $|P_3P_{11}| = |G| = 99 \Rightarrow P_3P_{11} = G$. Thus, by the internal direct product theorem, $G \cong P_3 \times P_{11}$. Now, we have that $P_3 \cong \mathbb{Z}_9$ or $P_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ and $P_{11} \cong \mathbb{Z}_{11}$, so either $G \cong \mathbb{Z}_9 \times \mathbb{Z}_{11}$ or $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}$, both of which are Abelian. So G is Abelian.

Example 9.8.3 Show that every group G of order 175 is Abelian.

SOLUTION: We have $175 = 5^2 \cdot 7$. Therefore, let P_5 and P_7 be a Sylow 5-subgroup and a Sylow 7-subgroup of G, respectively. We know that since $|P_5| = 5^2$ P_5 must be Abelian, and since 7 is a prime we must have that P_7 is cyclic, hence Abelian. Now, by Sylow's third theorem, we must have $n_5 = 1 + 5k$, $k \in \mathbb{Z}$, and $n_5 \mid 7$, which means that $n_5 = 1$, which means that P_5 is normal in G. Additionally, we must have $n_7 = 1 + 7k$, $k \in \mathbb{Z}$ and $n_7 \mid 25$. Again, the only possibility is $n_7 = 1$, so that P_7 is also normal in G. Then, since 7 is a prime, all non-identity elements of P_7 must have order 7, which implies that $P_5 \cap P_7 = \{1_G\}$, which means that $|P_5P_7| = |G| = 175 \Rightarrow G = P_5P_7$. Then the internal direct product theorem gives $G \cong P_5 \times P_7$. Now, $P_5 \cong \mathbb{Z}_{25}$ or $P_5 \cong \mathbb{Z}_5 \times \mathbb{Z}_5$ by the fundamental theorem of finite Abelian groups. As well, $P_7 \cong \mathbb{Z}_7$ only since P_7 is cyclic. Therefore, either $G \cong \mathbb{Z}_{25} \times \mathbb{Z}_7$ or $G \cong \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7$, both of which are Abelian, so that G is Abelian.

These three examples illustrate the following theorem.

Theorem 9.8.1

Let G be a group of order p^2q, where p and q are distinct prime numbers such that $p \nmid q - 1$ and $q \nmid p^2 - 1$. Then G is Abelian.

The next few examples illustrate how Sylow's theorem can be used to show that groups of certain order cannot be simple.

Example 9.8.4 Prove that no group of order 30 is simple.

SOLUTION: Assume G is a simple group of order $30 = 2 \cdot 3 \cdot 5$. Consider the numbers n_5 and n_3 of Sylow 5-subgroups and Sylow 3-subgroups. We must have $n_5 > 1$ and $n_3 > 1$ or else the corresponding Sylow p-subgroup would be normal and the group not simple. But since $n_5 = 1 + 5k$, $k \in \mathbb{Z}$, and $n_5 \mid 6$, we must have $n_5 = 6$. Similarly, since $n_3 = 1 + 3k$, $k \in \mathbb{Z}$, and $n_3 \mid 10$, we must have $n_3 = 10$. (In both cases, we used the assumption that G is simple and hence that $n_5, n_3 > 1$.) Now, since any Sylow 5-subgroup is of order 5 and since any Sylow 3-subgroup is of order 3, the intersection of any two of these groups must be trivial, which means that there are $6 \cdot (5 - 1) = 24$ elements of order five in G and $10 \cdot (3 - 1) = 20$ elements of order three in G, giving a total of 44 elements of orders five and three, a contradiction to the fact that $|G| = 30$. Therefore, $n_5 = 1$ or $n_3 = 1$ and in either case this means that G is not simple.

Example 9.8.5 Prove that no group G of order 56 is simple.

SOLUTION: We have $56 = 7 \cdot 2^3$, so by Sylow's first theorem there exist Sylow 2-subgroups and Sylow 7-subgroups of G. Assuming G is simple, we must then have $n_2 > 1$ and $n_7 > 1$, where n_2 and n_7 are the numbers of Sylow 2- and 7-subgroups, respectively. Since $n_7 = 1+7k$, $k \in \mathbb{Z}$, and $n_7 \mid 8$, we must have $n_7 = 8$; similarly, $n_2 = 1+2k$ and $n_2 \mid 7$ implies that $n_2 = 7$. Each Sylow 7-subgroup must have 6 elements of order seven, and hence 8 of these groups will give 48 elements of order seven. Also, even just two Sylow 2-subgroups will give more than seven elements of even order. Including also the identity, we have too many elements, and so G cannot be simple.

Example 9.8.6 Prove that no group of order 36 is simple.

SOLUTION:

Example 9.8.7 Show that any group G of order 255 is Abelian and cyclic.

SOLUTION:

10 Group Solvability and the Semi-Direct Product

In this chapter we give a very brief account of solvable groups, and we will introduce the semi-direct product, which we will see gives rise to the dicyclic group of order 3, a group of order 12.

10.1 The Commutator and Commutator Subgroup

Definition 10.1.1 Commutator

Let G be a group and $a, b \in G$. The **commutator** of a and b, denoted $[a, b]$ is the element $[a, b] = aba^{-1}b^{-1} \in G$.

Theorem 10.1.1 Properties of the Commutator

Let G be a group, $a, b \in G$, and $[a, b]$ the commutator of a and b. Then,

1. $[a, b] = 1_G \Leftrightarrow ab = ba$. Hence G is Abelian $\Leftrightarrow [a, b] = 1_G$ for all $a, b \in G$.
2. $[a, b]^{-1} = \left(aba^{-1}b^{-1}\right)^{-1} = bab^{-1}a^{-1} = [b, a]$.
3. For any $g \in G$,

$$\begin{aligned} g\,[a, b]\,g^{-1} &= g\left(aba^{-1}b^{-1}\right)g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} \\ &= \left(gag^{-1}\right)\left(gbg^{-1}\right)\left(ga^{-1}g^{-1}\right)\left(gb^{-1}g^{-1}\right) \\ &= \left(gag^{-1}\right)\left(gbg^{-1}\right)\left(gag^{-1}\right)^{-1}\left(gbg^{-1}\right)^{-1} \\ &= \left[gag^{-1}, gbg^{-1}\right]. \end{aligned}$$

   "The conjugate of a commutator is the commutator of the conjugates".
4. The product of commutators is not necessarily another commutator.
5. If $\alpha : G \to H$ is a group homomorphism, then for all $a, b \in G$, $\alpha([a, b]) = [\alpha(a), \alpha(b)]$.

Definition 10.1.2 Commutator Subgroup

Let G be a group. The **commutator subgroup** of G, denoted G', is the set of products of the commutators in G, i.e.,

$$G' = \{c_1 c_2 \cdots c_l \mid l \in \mathbb{Z}, l \geq 0\},$$

where the c_i are the commutators in G.

REMARK: Note that, as mentioned, since the product of commutators is not necessarily another commutator, the commutator subgroup contains more than just the commutators in G.

REMARK: We may also easily verify that G' is indeed a subgroup by performing the subgroup test.

1. We have that $[1_G, 1_G] = 1_G$, so G' is not empty and contains the identity.
2. Suppose $x, y \in G'$. Then we may write x and y as a product of commutators, say $x = c_1 c_2 \cdots c_m$ and $y = d_1 d_2 \cdots d_n$. Then,
$$xy = c_1 c_2 \cdots c_m d_1 d_2 \cdots d_n,$$
which is in G' because xy is again just a product of commutators. So G' is closed.
3. Finally, let $x \in G'$. Write x as a product of commutators, say $x = c_1 c_2 \cdots c_m$. Then $x^{-1} = (c_1 c_2 \cdots c_m)^{-1} = c_m^{-1} \cdots c_2^{-1} c_1^{-1}$, and since the inverse of a commutator is again a commutator, we have that x^{-1} is a product of commutators, and hence $x^{-1} \in G'$.

Theorem 10.1.2

Let G be a group and G' its commutator subgroup. Then,

1. $G' \trianglelefteq G$;
2. G/G' is Abelian.

PROOF:

1. To prove that G' is normal, we must show that for all $x \in G'$ and all $g \in G$ $gxg^{-1} \in G'$. Let $x = c_1 c_2 \cdots c_m$, where remember $c_1, c_2, \ldots, c_m$ are all commutators in G. Then, for all $g \in G$,
$$gxg^{-1} = gc_1 c_2 \cdots c_m g^{-1} = \left(gc_1 g^{-1}\right)\left(gc_2 g^{-1}\right) \cdots \left(gc_m g^{-1}\right),$$
where we have inserted $gg^{-1} = 1_G$ in between each c_i and c_{i+1}. We have already seen that the conjugate of a commutator is also a commutator. So gxg^{-1} is nothing but a product of commutators, and hence $gxg^{-1} \in G'$, so G' is normal in G.

2. The first property of the commutator stated above, we have that a group is Abelian if and only if the commutator of all pairs of elements in the group is trivial. Now, let $1_G, g_1, \ldots, g_n$ be the representatives of the cosets of G' in G, i.e., let $G', g_1 G', \ldots, g_n G'$ be the elements of G/G'. Remember that the identity element in G/G' is G'. Now, for any two elements $g_i G'$ and $g_j G'$ in G/G', we have
$$\left[g_i G', g_j G'\right] = \left(g_i G'\right)\left(g_j G'\right)\left(g_i G'\right)^{-1}\left(g_j G'\right)^{-1} = \left(g_i g_j G'\right)\left(g_i^{-1} g_j^{-1} G'\right) = g_i g_j g_i^{-1} g_j^{-1} G' = [g_i, g_j]\, G'.$$

But $[g_i, g_j]$ is a commutator, hence it belongs in G'; therefore, $[g_iG', g_jG'] = G'$, which means that G/G' is an Abelian group. ■

Theorem 10.1.3

Let G be a group and G' its commutator subgroup. Then G is Abelian if and only if $G' = \{1_G\}$.

REMARK: Therfore, in a way, the commutator subgroup can be used as one measure how how far a group is from being Abelian. The larger the commutator, the "farther" the group is from being Abelian.

PROOF: Suppose G is Abelian. Then, from the first property of the commutator, $[a, b] = 1_G$ for all $a, b \in G$. Now, G' contains every product of commutators in G, but all of these products will be equal to 1_G since every commutator is trivial. Hence $G' = \{1_G\}$.

Conversely, suppose $G' = \{1_G\}$. Then all the products of commutators in G are equal to the identity. Now, let $x = c_1c_2 \cdots c_m \in G'$. We must have $c_1c_2 \cdots c_m = 1_G$, which will happen if and only if all of $c_1, c_2, \ldots, c_m = 1_G$ or if and only if n is even and every pair of adjacent commutators consists of a commutator and its inverse. Since every element of G' must be equal to the identity, let us consider an element $c_1c_2 \cdots c_m$ such that the product does not contain the inverse of any of the factors. Then $c_1c_2 \cdots c_m = 1_G \Leftrightarrow c_1, c_2, \ldots, c_m = 1_G$. This means that all the commutators in G must be equal to the identity, which means that G must be Abelian. ■

Example 10.1.1 Show that every commutator in S_n is an even permutation.

SOLUTION: Take any elements $\alpha, \beta \in S_n$. Their commutator is

$$[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}.$$

Remember that the function sgn is a homomorphism and returns an element in $\mathbb{Z}_2$ (which indicates whether the permutation is even or odd). Since a permutation and its inverse must have the same number of transpositions, we get

$$\begin{aligned} \operatorname{sgn}\left(\alpha\beta\alpha^{-1}\beta^{-1}\right) &= \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)\operatorname{sgn}(\alpha)\operatorname{sgn}(\beta) \\ &= (\operatorname{sgn}(\alpha))^2 (\operatorname{sgn}(\beta))^2 \\ &= [0]_2 + [0]_2 = [0]_2, \end{aligned}$$

which means that $[\alpha, \beta]$ is an even permutation. So all commutators in S_n are even permutations.

Theorem 10.1.4

The commutator subgroup S_n' of S_n is A_n for all n.

PROOF: We have seen in Theorem 7.6.4 that for $n \geq 5$ the only normal subgroups of S_n are $\{()\}$, A_n, and S_n itself. Now, for any $a, b, d \in \{1, 2, \ldots, n\}$,

$$\begin{aligned}[(a\ b)\,(b\ d)] &= (a\ b)\,(b\ d)\,(a\ b)^{-1}\,(b\ d)^{-1} \\ &= (a\ b)\,(b\ d)\,(a\ b)\,(b\ d) \\ &= (a\ d\ b)\,,\end{aligned}$$

which means that we cannot have $S_n' = \{()\}$. Also, since every commutator is an even permutation (above example) and the product of even permutations is also an even permutation, we also cannot have $S_n' = S_n$. Therefore, the only possibility must be $S_n' = A_n$. Indeed, since all commutators are even, and the product of even permutations is even, we have $S_n' \subseteq A_n$. Also, we know that A_n is generated by the 3-cycles of S_n for $n \geq 3$. Therefore, every element in A_n is the product of 3-cycles. But each 3-cycle can be written as a commutator using the above calculation, hence any element in A_n can be written as a product of commutators (if not as a single commutator). Therefore, $A_n \subseteq S_n'$, and so $S_n' = A_n$. ■

10.2 Solvable Group

Definition 10.2.1 Solvable Group

A group G is said to be **solvable** if it has a series of subgroups

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_n = \{1_G\}$$

in which the quotient groups ${}^{G_i}/_{G_{i+1}}$ are Abelian for all $0 \leq i \leq n-1$. n is called the **derived length** of G. If no n exists such that $G_n = \{1_G\}$, then G is said to be **not solvable**.

Definition 10.2.2

Given a group G, we construct a **series** of subgroups inductively as follows: (let $i \in \mathbb{Z}$)

$$\begin{aligned}&G^{(0)} = G \\ &G^{(1)} = G' \quad \text{(the commutator subgroup)} \\ &G^{(i)} = \left(G^{(i-1)}\right)',\ i \geq 2 \quad \text{(i.e., the commutator subgroup of } G^{(i)}\text{)}.\end{aligned}$$

By Theorem 10.1.2, we have

$$G^{(i)} \trianglelefteq G^{(i-1)} \quad \text{and} \quad {}^{G^{(i-1)}}/_{G^{(i)}} \text{ is Abelian,}$$

for all $i \geq 2$.

Theorem 10.2.1

Let G be a group and $G^{(i)}$ the subgroups of G as defined above. Then G is solvable if and only if $G^{(n)} = \{1_G\}$ for some positive integer n.

Theorem 10.2.2

Let G be a solvable group and $H \trianglelefteq G$. Then:

1. Every subgroup of G is solvable.
2. Every homomorphic image of G is solvable.
3. H and G/H are both solvable. (The converse is also true.)
4. $G/Z(G)$ is solvable. (The converse is also true.)

Also, if G_1 and G_2 are solvable groups, then so is $G_1 \times G_2$.

Theorem 10.2.3

Let G be a group. If G is not Abelian and G is simple, then G is not solvable.

REMARK: Note that contrapositive of this statement: if G is solvable, then G is either simple or Abelian (but not both).

PROOF: Since G is not Abelian, we must have $G' \neq \{1_G\}$ by Theorem 10.1.3. Moreover, because G is simple, and $G' \trianglelefteq G$ by Theorem 10.1.2, we must have $G' = G$. Thus, $G^{(i)} = G^{(i-1)} = G \neq \{1_G\}$ for all $i \geq 1$, and so G is not solvable. ■

Theorem 10.2.4 Summary of Facts about Solvable Groups

1. Every Abelian group is solvable (finite or infinite).
2. Every p-group is solvable.
3. Every group of order $2p$, where p is an odd prime number, is solvable.
4. Every group of order pq, where p and q are distinct prime numbers, is solvable.
5. Every group of order p^2q is solvable.
6. S_n is not solvable for any $n \geq 5$.
7. D_n is solvable for all $n \geq 3$.

PROOF:

1. We have shown in Theorem 10.1.3 that if a group G is Abelian, then its commutator

subgroup is $G' = \{1_G\}$. But $G' = G^{(1)} = \{1_G\}$, so by Theorem 10.2.1 G is solvable. ■

Example 10.2.1 Show that every group G of order 42 is solvable.

SOLUTION: We have that $42 = 7 \cdot 6$. Hence, by Sylow's first theorem there exists a Sylow 7-subgroup of G of order seven. By Sylow's third theorem, the number of Sylow 7-subgroups n_7 must satisfy $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 6$. The only possible value is $n_7 = 1$, which means that the Sylow 7-subgroup is unique and normal in G—call it P_7. Since 7 is prime, P_7 is cyclic, hence Abelian, hence solvable. Also, $|{}^G/_{P_7}| = 6$, so that either ${}^G/_{P_7} \cong \mathbb{Z}_6$ or ${}^G/_{P_7} \cong S_3$. If ${}^G/_{P_7} \cong \mathbb{Z}_6$ then since $\mathbb{Z}_6$ is Abelian, it is solvable, so by Theorem 10.2.2 part 3 we have that G is solvable. Now consider ${}^G/_{P_7} \cong S_3$. The commutator subgroup of S_3 is A_3 by Theorem 10.1.4, and since $|A_3| = \frac{6}{2} = 3$, we must have A_3 is cyclic, hence Abelian, so that the commutator subgroup of A_3 is $\{1_G\}$. So S_3 is solvable, and again by Theorem 10.2.2 part 3 we get that G is solvable.

Example 10.2.2 Show that every group G of order 20 is solvable.

SOLUTION: We have $20 = 4 \cdot 5$, which means that there exist Sylow 5-subgroups of G of order 5 such that the number n_5 of such subgroups satisfies $n_5 \equiv \pmod 5$ and $n_5 \mid 4$. The only possibility is $n_5 = 1$, which means that there is only one Sylow 5-subgroup, call it P_5, and it is normal in G. Additionally, since 5 is prime, P_5 is cyclic, hence Abelian. Now, then, $|{}^G/_{P_5}| = 4$, and since every group of order four must be Abelian, we have that ${}^G/_{P_5}$ is Abelian, hence solvable. So by Theorem 10.2.2 part 3, G must be solvable.

10.3 The Semi-Direct Product

Recall the internal direct product theorem, which stated that $G \cong H \times K$ if and only if there existed normal subgroups H^* and K^* of G such that $H^* \cong H$, $K^* \cong K$, $G = H^*K^*$, and $H^* \cap K^* = \{1_G\}$.

In this section, we study the "semi-direct product" of two groups H and K, which is a generalisation to this notion of the internal direct product and is obtained by relaxing the requirement that both H^* and K^* be normal in G, i.e., we will require only *one* of them to be normal. One reason the semi-direct product is useful is that it allows us to construct non-Abelian groups even when the groups in the product are Abelian (remember that if H and K are Abelian groups, then the regular direct product $H \times K$ is also Abelian).

Definition 10.3.1 Semi-Direct Product

Let H and K be groups and let $\overline{\varphi}$ be a homomorphism from K to $\mathrm{Aut}(H)$. The **semi-direct product** of H and K, denoted $H \rtimes K$, is the set of ordered-pairs (h, k) with a binary operation $*$ on any two elements in $H \rtimes K$ defined by

$$(h_1, k_1) * (h_2, k_2) = (h_1 \varphi(k_1, h_2), k_1 k_2)$$

for all $h_1, h_2 \in H$ and all $k_1, k_2 \in K$, where φ is the action of K on H that determines $\overline{\varphi}$. (The $*$ will be omitted from now on.)

Now, let us assume that H and K are subgroups of G such that $H \trianglelefteq G$ and $K \leq G$. Remember that we still have $HK \leq G$. Let us define the action $\varphi : K \times H \to H$ of K on H by conjugation, i.e., let $\varphi(k, h) = khk^{-1}$ for all $h \in H$ and all $k \in K$ (note that since H is normal in G, khk^{-1} is indeed still in H). Then, as we have seen when we first introduced group actions, the mapping $\varphi_k : H \to H$ defined by $\varphi_k(h) = \varphi(k, h)$ is a permutation of H, and the mapping $\overline{\varphi} : K \to S_H$ defined by $\overline{\varphi}(k) = \varphi_k$ is a group homomorphism (S_H is the set of permutations on H). Now, φ_k, being a permutation, is a bijection, and since H is a group it is clear that φ_k is also a homomorphism (from H to H); therefore, φ_k is an *isomorphism* from H to H, which we have seen is also called an *automorphism*, and hence $\varphi_k \in \mathrm{Aut}(H)$. Therefore, S_H is nothing but $\mathrm{Aut}(H)$ itself (remember that $\mathrm{Aut}(H)$ is itself a group).

Theorem 10.3.1

Let G, H, and K be groups and let $\overline{\varphi}$ be a homomorphism from K to $\mathrm{Aut}(H)$. Let φ denote the action of K on H that determines $\overline{\varphi}$. Then:

1. The sets $H^* = \{(h, 1_G) \mid h \in H\}$ and $K^* = \{(1_G, k) \mid k \in K\}$ are subgroups of G and the maps $f : H \to H^*$ and $g : K \to K^*$ defined by $f(h) = (h, 1_G)$ and $g(k) = (1_G, K)$ for all $h \in H$ and all $k \in K$ are isomorphisms, i.e., $H \cong H^*$ and $K \cong K^*$.
2. $H^* \trianglelefteq G$.
3. $H^* \cap K^* = \{1_G\}$.
4. The action of K on H is defined by conjugation, i.e., $\varphi(k, h) = khk^{-1}$ for all $k \in K$ and all $h \in H$.
5. $G = H \rtimes K$ is a group of order $|G| = |H|\,|K|$ under the binary operation $(h_1, k_1) * (h_2, k_2) = (h_1 \varphi(k_1, h_2), k_1 k_2)$ for all $h_1, h_2 \in H$ and all $k_1, k_2 \in K$.

We now state the theorem analogous to the internal direct product theorem.

Theorem 10.3.2 Characterisation of the Semi-Direct Product

Let G, H, and K be groups and let $\overline{\varphi}$ be a homomorphism from K to $\mathrm{Aut}(H)$. Let φ denote the action of K on H by conjugation that determines $\overline{\varphi}$. Then, $G \cong H \rtimes K$ if and only if there exists subgroups H^* and K^* of G such that

1. $H \cong H^*$, $K \cong K^*$ and $H^* \trianglelefteq G$;
2. $H^* \cap K^* = \{1_G\}$;
3. $H^*K^* = G$.