Group Theory-test

Anand Narasimhan
210051001
Undergraduate, Department of Computer Science
Indian Institute of Technology Bombay

May 2022

Contents

1 Preliminaries

1.1 Basics and Notations (and to develop my LaTeXmath knowledge)

- The order or cardinality of a set A is denoted by $|A|$.
- A subset of a set A is represented as
  $B = \{\, a \in A \mid \ldots \text{ (conditions on } a) \ \ldots \}$
- Standard definitions apply for the Cartesian product, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}^+$, $\mathbb{Q}$, $\mathbb{Q}^+$, $\mathbb{R}$, $\mathbb{R}^+$, $\mathbb{C}$.
- A function from A to B is denoted by $f : A \to B$ or $A \xrightarrow{f} B$
- $f : a \mapsto b$ indicates that $f(a) = b$

Remark

If the function f is not specified on elements it is important in general to check that f is well defined, i.e., is unambiguously determined. For example, if the set A is the union of two subsets A_1 and A_2 then one can try to specify a function from A to the set $\{\, 0, 1 \,\}$ by declaring that f is to map everything in A_1 to 0 and is to map everything in A_2 to 1. This unambiguously defines f unless A_1 and A_2 have elements in common (in which case it is not clear whether these elements should map to 0 or to 1). Checking that this f is well defined therefore amounts to checking that A_1 and A_2 have no intersection.

Some important definitions :

Let $f : A \to B$.

Definition 1.1: Injective

f is **injective** or is an **injection** if whenever $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.

Definition 1.2: Surjective

f is **surjective** or is a **surjection** if for all $b \in B$ there is some $a \in A$ such that $f(a) = b$, i.e., the range of f is **all** of B.
Note that the codomain must be specified for the question of surjectivity to be meaningful.

Definition 1.3: Bijective

f is **bijective** or is a **bijection** if it is both injective and surjective. If there exists at least one such bijection from A to B, then A and B are said to be in **bijective correspondence**.

Definition 1.4: Left Inverse

f has a **left inverse** if there is a function $g : B \to A$ such that $g \circ f : A \to A$ is the identity map on A, i.e., $(g \circ f)(a) = a$, for all $a \in A$.

Definition 1.5: Right Inverse

f has a **right inverse** if there is a function $h : B \to A$ such that $f \circ h : B \to B$ is the identity map on B.

Proposition 1.6: Bijectiveness

Let $f : A \to B$.

1. *The map f is injective if and only if f has a left inverse*
2. *The map f is surjective if and only if f has a right inverse*
3. *The map f is a bijection if and only if there exists $g : B \to A$ such that $f \circ g$ is the identity map on B and $g \circ f$ is the identity map on A.*

A **permutation** of a set A is simply a bijection from A to itself.

If $A \subseteq B$ and $f : B \to C$, the **restriction** of f to A is denoted by $f|_A$ Similarly the reverse is called an **extension**.

A **binary relation** on a set A is a subset R of $A \times A$ and we write $a \sim b$ if $(a, b) \in R$.

If $\sim$ defines an equivalence relation on A, then the equivalence class of $a \in A$ is defined to be $\{ x \in A \mid x \sim a \}$. Elements of the equivalence class of a are said to be equivalent to a. If C is an equivalence class, any element of C is called a representative of the class C.

A **partition** of A is any collection $\{ A_i \mid i \in I \}$ of non-empty subsets of A (where I is some indexing set) such that A is the disjoint union of the sets in the partition.

Proposition 1.7: Partition

Let A be a non-empty set.

1. *If $\sim$ defines an equivalence relation on A, then the set of equivalence classes of $\sim$ form a partition of A.*
2. *If $\{ A_i \mid i \in I \}$ is a partition of A then there is an equivalence relation on A whose equivalence classes are precisely the sets $A_i, i \in I$.*

1.2 Properties of the Integers

1. **Well Ordering of $\mathbb{Z}^+$** : If A is any nonempty subset of $\mathbb{Z}^+$, there is some element $m \in A$ such that $m \leq a$ for all $a \in A$ (m is called a **minimal element** of A).

Remark

It is more appropriate to call m the minimum element of A.

2. **Division** : If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say **a divides b** if there is an element $c \in \mathbb{Z}$ such that $b = ac$. In this case we write $a \mid b$; if a does not divide b we write $a \nmid b$.
3. **GCD** : If $a, b \in \mathbb{Z} \setminus \{0\}$, There is a unique positive integer d called the GCD of a and b, whose properties are known. It is denoted by (a, b)
4. **LCM** : Similarly, there is a unique positive integer l called the LCM of a and b, again, whose properties are known.
5. **The Division Algorithm** : if $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$, then there exists unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < |b|$$

   where q is the **quotient** and r is the **remainder**.
6. **The Euclidean Algorithm** To find the GCD of two numbers by iterating the **Division Algorithm**
7. **Consequence of the Euclidean algorithm** If $a, b \in \mathbb{Z} \setminus \{0\}$, then there exists $x, y \in \mathbb{Z}$ such that

$$(a, b) = ax + by$$

   that is, **the g.c.d of a and b is a $\mathbb{Z}$-linear combination of a and b**.
8. **Prime Numbers** Belonging to $\mathbb{Z}^+$, usual definition.

   An important property (which can be used to define the primes) : if p is a prime and $p \mid ab$, for some $a, b \in \mathbb{Z}$, then either $p \mid a$ or $p \mid b$.

9. **The Fundamental Theorem of Arithmetic** : if $n \in \mathbb{Z}, n > 1$, then n can be factored uniquely into the product of primes, i.e., there are distinct primes $p_1, p_2, \ldots, p_s$ and positive integers $\alpha_1, \alpha_2, \ldots, \alpha_s$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}.$$

This provides a way to express the g.c.d and l.c.m of two numbers : After writing them as a product of powers of primes, the g.c.d (and l.c.m) can be expressed as the product of the min (max) of the corresponding powers of the primes.

Suppose the positive integers a and b are expressed as products of prime powers:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$$

where $p_1, p_2, \ldots, p_s$ are distinct and the exponents are ≥ 0 (To allow the products to be taken over the same set of primes, the exponent will be 0 if the prime is not actually a divisor). Then the g.c.d of a and b is :

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_s^{\min(\alpha_s, \beta_s)} \quad a = p_1 p_2 \cdots p_n$$

and the l.c.m is obtained by taking the maximum instead of the minimum.

10. The **Euler φ-function** is defined as follows : for $n \in \mathbb{Z}^+$ let $\varphi(n)$ be the number of positive integers $a \leq n$ with a relatively prime to n, i.e., $(a, n) = 1$. For example, $\varphi(12) = 4$ since $1, 5, 7$ and 11 have no common factors with 12.

For primes p, $\varphi(p) = p - 1$, and, more generally, for all $a \geq 1$ we have the formula

$$\psi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1).$$

The function is multiplicative in certain cases (only when a and b are relatively prime). :

$$\varphi(ab) = \varphi(a)\varphi(b) \qquad \text{if } (a, b) = 1$$

So these two formulas above give a general formula for the values of φ : if $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, then :

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_s^{\alpha_s - 1}(p_s - 1) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_s}) \end{aligned}$$

Remark

Note that the letter φ will be used for many different functions throughout this paper, so when it is used to denote Euler's function, it will be indicated explicitly.

1.3 The Integers Modulo n

Let n be a fixed positive integer. Define a relation on $\mathbb{Z}$ by

$$a \sim b \text{ if and only if } n \mid (b-a).$$

One can clearly show that it is an equivalence relation. Write $a \equiv b(mod n)$ (Congruence) if $a \sim b$.

Definition 1.8: Equivalence Class

The equivalence class of a is denoted by $\overline{a}$. This is called the **congruence class** or **residue class** of a mod n and consists of the integers which differ from a by an integral multiple of n.

There are precisely n distinct equivalence classes mod n, namely

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$$

determined by the possible remainders after division by n and these residue classes partition the integers $\mathbb{Z}$. **The set of equivalence classes under this equivalence relation will be denoted by $\mathbb{Z}/n\mathbb{Z}$ and called the integers modulo n.**

Note that for different n's the equivalence relation and equivalence classes are different so n must be fixed before using the bar notation. The process of finding the equivalence class mod n of some integer a is often referred to as **reducing a mod n**

An addition and a multiplication can be defined for the elements of $\mathbb{Z}/n\mathbb{Z}$, defining **modular arithmetic** as follows : for $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$

$$\overline{a} + \overline{b} = \overline{a+b} \qquad \text{and} \qquad \overline{a} \cdot \overline{b} = \overline{ab}$$

It is easy to see that these operations are well defined, i.e., they don't depend on the choices of a and b for the classes involved.

We shall see later that the process of adding equivalence classes by adding their representatives is a special case of a more general construction (the construction of a **quotient**)

It is important to be able to think of the equivalence classes of some equivalence relation as **elements** which can be manipulated (as we do, for example, with fractions) rather than as sets.

An important subset of $\mathbb{Z}/n\mathbb{Z}$ consists of the collection of residue classes which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\, \overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{there exists } \overline{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \overline{a} \cdot \overline{c} = \overline{1} \,\}$$

Proposition 1.9: Condition for Multiplicative Inverse

$(\mathbb{Z}/n\mathbb{Z})^\times = \{\, \overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1 \,\}$.
In other words, only those elements which are ***coprime*** *with n have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$*

It is easy to see that if any representative of $\overline{a}$ is relatively prime to n then all representatives are relatively prime to n so that the set on the right in the proposition is well defined.

If a is an integer relatively prime to n then the Euclidean Algorithm produces integers x and y satisfying $ax + ny = 1$, hence $ax = 1 \pmod{n}$, so that x is the multiplicative inverse of a in $\mathbb{Z}/n\mathbb{Z}$. This gives an efficient method for computing multiplicative inverses in $\mathbb{Z}/n\mathbb{Z}$.

2 Introduction to Groups

2.1 Basic Axioms and some Examples

In this section the basic algebraic structure to be studied in Group Theory is introduced and some examples are given.

Definition 2.1: Binary Operation

A **binary operation** $*$ on a set G is a function $* : G \times G \to G$. For any $a, b \in G$ we shall write $a * b$ for $*(a, b)$.

Definition 2.2: Associativity

A binary operation $*$ on a set G is **associative** if for all $a, b, c \in G$ we have $a * (b * c) = (a * b) * c$.

Definition 2.3: Commutativity

If $*$ is a binary operation on a set G we say elements a and b of G **commute** if $a*b = b*a$ We say $*$ (or G) is **commutative** if for all $a, b \in G, a*b = b*a$.

Example

$+$ (usual addition) and $\times$ (usual multiplication) are both commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ respectively.

Example

$-$ (usual subtraction) is a non-commutative binary operation on $\mathbb{Z}$. The map $a \mapsto -a$ is not a binary operation (not binary).
Also, $-$ is not a binary operation on $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ since sometimes the difference of two numbers in $\mathbb{Z}^+$ can be negative.

Example

Taking the vector cross product of two vectors in $\mathbb{R}^3$ is a binary operation which is neither associative nor commutative.

Suppose that $*$ is a binary operation on a set G and H is a subset of G. If the restriction of $*$ to H is a binary operation on H, i.e., for all $a, b \in H$, $a * b \in H$, then H is said to be **closed** under $*$. If $*$ is associative or commutative on G, they get carried over onto H as well.

Definition 2.4: Groups

A **group** is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following axioms :

1. $(a * b) * c = a * (b * c)$, for all $a, b, c \in G$, i.e., $*$ is **associative**,
2. There exists an element $e \in G$, called an identity of G such that for all $a \in G$ we have $a * e = e * a = a$,
3. For each $a \in G$ there is an element $a^{-1} \in G$, called an **inverse** of a, such that $a * a^{-1} = a^{-1} * a = e$.

Definition 2.5: Abelian Groups

The group $(G, *)$ is called **abelian** (or **commutative**) if $a * b = b * a$ for all $a, b \in G$.

Alternatively, a less formal way to convey the information is to say G is a group under $*$ if $(G, *)$ is a group (or just G is a group when the operation $*$ is clear

from the context). Also, G is a **finite group** if in addition G is a finite set. Note that axiom 2 in Definition 2.1 ensures that a group is never empty.

Example

$\mathbb{Z} \setminus \{0\}$ is not a group under $\times$ because some elements like 2 don't have inverses.
However examples like $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ etc. are groups under $\times$

We haven't really talked about the associativity part of groups yet, and kind of assumed that associativity holds. The associativity of $\mathbb{Z}$ under $+$ holds due to the axiom of associativity of natural numbers. The associative law for $\mathbb{Q}$, $\mathbb{R}$ etc. follow from this basic associative axiom. [1]

A similar procedure is followed for the associativity of $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ under $\times$.

So in the following sections we will take the associativity laws over all these sets as given.

Some examples :

- A vector space, by definition, requires commutativity with respect to $+$, in addition to all the properties required for a normal group. Therefore it is an abelian additive group.
- For $n \in \mathbb{Z}^+$f, $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the operation $+$ of addition of residue classes (Definition 1.3)

  The identity is $\bar{0}$ and the inverse of $\bar{a}$ is $\overline{-a}$ for each $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$.

  Henceforth when this group is talked about, it is understood that the group operation is addition of classes mod n.
- If $(A, *)$ and $(B, \diamond)$ are two groups, then a new group can be formed, whose elements are in the cartesian product $A \times B$ and whose operation is defined componentwise as :

$$(a_1, b_1)(a_2, b_2) = (a_1 * a_2)(b_1 \diamond b_2)$$

  This group is called their direct product. Examples would be the group $\mathbb{R} \times \mathbb{R}$ over addition, as $\mathbb{R}$ itself is a group over addition. The former is the familiar euclidean plane.

Remark

There should be no confusion between the groups $\mathbb{Z}/n\mathbb{Z}$ (under addition) and $(\mathbb{Z}/n\mathbb{Z})^\times$ (under multiplication) even though the second is a subset of the first.

[1] Beyond the scope of this paper

Proposition 2.6: Properties of a Group

If G is a group under the operation $\star$, then

1. *The identity of G is unique*
2. *For each $a \in G$, a^{-1} is uniquely determined*
3. *$(a^{-1})^{-1} = a$*
4. *$(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$*
5. *for any $a_1, a_2, \ldots, a_n \in G$, the value of $a_1 \star a_2 \star \cdots \star a_n$ is independent of how the expression is bracketed (This is called the general associative law)*

Proof. Proving the above propositions :

1. If a and b are both identities, then by axiom 2 of 2.1, $a \star b = a$ and $a \star b = b$, which means equating the RHS of both, we get that $a = b$, and that the identity is unique
2. Let's assume b, c are both inverses of a and e be the identity of G. So, $a \star b = e$ and $c \star a = e$. Then :

$$\begin{aligned} c &= c \star e \\ &= c \star (a \star b) \\ &= (c \star a) \star b \\ &= e \star b \\ &= b \end{aligned}$$

3. This is just the same as showing that the inverse of a^{-1} is a, which is the same as interchanging the roles of a and a^{-1} in the definition of a^{-1}.
4. This can be proved by taking the definition of $(a \star b)^{-1}$, using the associative law, and premultiplying with a^{-1} and b^{-1}.

□

To make our work easier, the operation for an abstract group will almost always be assumed as $\cdot$ and $a \cdot b$ would be written as ab. Also, because of the general associative law, products of 3 or more group elements will not be bracketed since the placement of brackets doesn't matter. Also, the identity element will be denoted by 1.

We shall also start using terms like x^n to denote $xx \cdots x$ (n terms) and x^0 to denote 1, the identity.

Of course, if we're dealing with specific groups, we would use the given operation, like + ,etc.

Proposition 2.7: Cancellation Laws

Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, left and right cancellation laws hold in G, i.e.

1. *If $au = av$, then $u = v$*
2. *If $ub = vb$, then $u = v$*

These can be proved by multiplying on both sides to the left (right) with the inverse of a (b) respectively

A consequence of the above proposition is that if either $ab = 1$ or $ba = 1$, then $b = a^-1$ without needing the other equation. A similar consequence holds for the identity element for a particular element in a group.

Definition 2.8: Order of a element of a Group

For G a group and $x \in G$, define the **order** of x to be the smallest positive integer such that $x^n = 1$, and denote this integer by $\mid x \mid$. x is said to have order n. If there is no positive finite n, then the order of x is defined to be infinity and x is said to be of infinite order.

Example

Some examples :

1. An element of a group can have order 1 iff it is the identity.
2. In the additive groups $\mathbb{R}$, $\mathbb{Q}$, etc. every non-zero element has infinite order.

Definition 2.9: Multiplication Table

Let $G = \{ g_1, g_2, \ldots, g_n \}$ be a finite group with $g_1 = 1$. The **multiplication table** or **group table** of G is the $n \times n$ matrix whose entry at the cell in the i^{th} row and j^{th} column is the group element $g_i g_j$

Problem 2.1 Think of some operations that are closed on a set and are

1. Associative but not Commutative
2. Commutative but not Associative

Can you think of examples for finite sets as well?

Solution For an infinite set, say $\mathbb{R}$,

1. The set of all non-singular $n \times n$ matrices which take their entries

from $\mathbb{R}$ will suffice. The identity element is I_n, the inverse exists since each element is non-singular, and matrix multiplication is inherently associative. Also, the operation is not commutative for all possible elements.

2. There are some interesting ones here, such as $(a+b)/2$ and more generally $k(a+b)$. Also, another example is $ab+1$, or even $ab+k$ for any k.

For finite sets, all that needs to be done is to take the remainder mod n, if you take the set $\mathbb{Z}/n\mathbb{Z}$. This ensures that the operation is closed. And also, $(a+b)/2$ won't work for all n and it's safer to take $k(a+b)$ for $k \in \mathbb{N}$

Problem 2.2 Let G be a finite group and let x be an element of G of order n. Prove that if n is odd, then $x = (x^2)^k$ for some k.

Solution We know from the order that $x^n = 1$ and multiplying by x on both sides gives $x = x^{n+1}$. We know that n is odd, which means that you can write $n = 2k-1$ for some $k \in \mathbb{N}$. The equation then becomes $x = x^{2k}$, which can be written as x^2 multiplied k times, which means that it is $(x^2)^k$.

Problem 2.3 Let G be a finite group and let $a, b \in G$. Show that $|ab| = |ba|$.

Solution Let me take two cases, one where a, b commute and the other when they do not.

If a, b commute, then $ab = ba$ and therefore $|ab| = |ba|$.

If they do not commute, then let us assume that the order of ab is n. Then $(ab)^n = 1$ or $a(ba)^{n-1}b = 1$. Premultiplying a^{-1} and postmultiplying a gives us $(ba)^{n-1}ba = 1$, or $(ba)^n = 1$, which means the order of ba divides ab. The same can be done reversing ab and ba, which means both their orders are equal.

Problem 2.4 Prove that if $x^2 = 1$ for all $g \in G$ then G is abelian.

Solution Our task is to prove that $ab = ba$ for all $a, b \in G$. Starting off with $x^2 = 1$, we get that $x = x^{-1}$ after multiplying both sides by x^{-1}, and this holds for all $x \in G$. Now, take the expression ab and see that since

$a = a^{-1}$ and $b = b^{-1}$,

$$ab = a^{-1}b^{-1} = (ba)^{-1} = ba$$

The last step deserves some more attention. We know that since the operation is closed on G, ba must also be an element in G. We also know that for $x \in G$, $x = x^{-1}$, therefore, $(ba)^{-1} = ba$, and the proof is complete.

Problem 2.5 Prove that any finite group of even order contains an element of order 2.

Solution Let us consider the elements $g \in G$ such that $g \neq g^{-1}$. For every such g, the group contains a different g^{-1}. Therefore the total number of elements g such that $g \neq g^{-1}$ is a multiple of 2, since they all come in pairs.

Excluding them from the main set (since their orders are not 2), we know that the identity is going to be part of the remaining set, and as that remaining set is bound to have an even order (since the difference of two even numbers is also even), there must be at least one element such that $g = g^{-1}, g \neq 1$, which means that $g^2 = 1$ and it has an order of 2. Also, an odd number of elements have an order of 2, which is another takeaway.

Problem 2.6 Let $G = \{1, a, b, c\}$ be a group of order 4 with identity 1. Assume G has no elements of order 4 (which means the order of all elements is ≤ 3). Show that there exists a unique multiplication table for G and also show that G is abelian.

Solution By the above problem, we see that there must be either 1 or 3 elements with order 2. Let us try both the possibilities.

Case 1 : Let a, b, c all have order 2. This means $a^2 = b^2 = c^2 = 1$. It also means that the elements are equal to their inverses.

Let's try to form the multiplication table. $ab \neq 1$, since then that would mean they are inverses of each other and that wouldn't be possible as they would be identical. $ab = a$ or $ab = b$ would also not be possible, since that would mean that either a or b would be the identity, which is obviously incorrect (since they're distinct elements). Therefore ab has to be c (since ab has to be an element of the group and by the process of elimination, it is c).

Similarly, you can work out that $ab = ba = c$, $bc = cb = a$ and $ac = ca = b$, which completes the multiplication timetable. You can also see that in

this case, the group is abelian as the group table is symmetric.

Case 2 : This is the case where only 1 element has order 2 (The rest have order 3). Without loss of generality, let that element be a. This implies that $a^2 = 1$, $b^3 = c^3 = 1$ and also that $a^{-1} = a$, $b^{-1} = c$ and $c^{-1} = b$. (The latter two relations are because b^{-1} must exist in the set, and since it can't be 1, a or b, it must be c.

Let's try to form the group table. What can the element ab be? It can't be 1, a, or b, for the same reasons as the previous case. Therefore, ab must be c, since ab must be present in the group.

However, unlike in the last case, we have some extra material to work with in this case, namely $c = b^{-1}$. Substituting that, we see that $ab = b^{-1}$, which means $ab^2 = 1$. Post multiplying b on both sides gives $ab^3 = b$. However, the order of b is 3, which means $b^3 = 1$. This leads to the equation $a = b$, which clearly isn't possible. Therefore, this case isn't realistically possible, and the only possible solution to the problem is the first case.

2.2 Dihedral Groups

Class of groups whose elements are symmetries of geometrical objects

Simplest form is with regular planar figures.

For each $n \in \mathbb{Z}^+$, $n \geq 3$, let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigid motion of the n-gon which can be be affected by taking a copy, moving it in any fashion in 3-space and then placing the copy back on the original so that it exactly covers the original.

We can describe the symmetry by a set of labels of the n-vertices. Each of them can be described uniquely by a permutation σ of $\{1, 2, 3, \ldots, n\}$ where if the symmetry puts vertex i in the place where vertex j was in originally, that means σ is the permutation sending $i \to j$.

To find the order $|D_{2n}|$, for any given i, there is a symmetry that sends vertex i to vertex i. Vertex 2, which is adjacent to 1, can either be sent to the $i + 1$ or $i - 1$ vertices, where the vertices are integers $\pmod n$. Once the position of these two vertices become fixed, everything else becomes fixed as well, so we have $n * 2$ choices for the symmetry. Therefore, the order of the group is $2n$, explaining the notation behind D_{2n}.

These symmetries can also be thought of as n rotations and n reflections about the n lines of symmetry.

We need a way to bring this discussion out of a geometric point of view and more into an abstract group. Therefore, we introduce some notation.

Fix the regular n-gon with the centre at the origin and label the vertices $1, 2, 3, \ldots, n$ clockwise. Let r be the rotation of the figure by $\frac{2\pi}{n}$ radians clockwise about the origin, and s be the reflection about the line of symmetry passing through the vertex 1 and the origin.

Some points to note :

1. $1, r, r^2, r^3, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$
2. $|s| = 2$
3. $s \neq r^i$ for any i
4. $sr^i \neq sr^j$, for all $0 \leq i, j \leq n-1$ with $i \neq j$, so

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

5. $rs = sr^{-1}$, which implies the group is not abelian.
6. $r^i s = sr^{-i}$. (Induction based proof combined with the previous point)

All the elements in D_{2n} can be written uniquely in the form $s^k r^i$, $k = 0$ or 1 and $0 \leq i \leq n-1$. Any product of two elements can be reduced to another in the same form using the above points. For example, if $n = 10$,

$$(sr^5)(sr^9) = s(r^5 s)r^9 = s(sr^{-5})r^9 = s^2 r^4 = r^4$$

In the above example, r and s were elements of the group which could be used to **generate** any other element in the group. They are called generators, the exact definition being as follows :

Definition 2.10: Generators

A subset S of elements of a group G with the property that every element of G can be written as a (finite) product of elements of S and their inverses is called a set of **generators** of G

This shall be indicated by the notation $G = \langle S \rangle$.

Example

In the additive group of $\mathbb{Z}$, each and every element can be written in terms of a finite sum of 1's and -1's, which leads to the notation $\mathbb{Z} = \langle 1 \rangle$

It can also be proven that in a finite group G, the condition of inverses of elements of S being used to generate the elements of G can be removed, i.e., it is not necessary.

Definition 2.11: Relations

Any equations in a general group G that the generators satisfy are called **relations** in G

In D_{2n} for example, we had three relations: $r^n = 1, s^2 = 1$ and $rs = sr{-}1$. Also, these three relations have the property that any other general relation between the elements of the group can be derived from these.

A **presentation** of the group D_{2n} is as follows :

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

A presentation gives an easy way of describing a group, however, extracting all the information about the group just from the given relations is difficult, such as telling when two elements of a group, specified in terms of the given generators, are equal. This leads to doubt over the order of the group, or whether it even is finite or infinite!

Also, for some presentations (could be simple), there could be some implicit and hidden relations as consequences of the specified ones, so the relations given could ensure that a group is a trivial group containing only 1 element, as an example.

So although it is necessary to be extremely careful in describing new groups by presentations, for known groups, it is a powerful tool.

Some problems :

Problem 2.7 Let $Y = \langle\, u, v \mid u^4 = v^3 = 1,\, uv = v^2u^2 \,\rangle$. Find the elements of the group.

Solution This group looks like it has an order of 12 at first glance, but let's see if we can manipulate our way into a relation that gives us more info.

$$\begin{aligned} uv = v^2u^2 &\implies u^2v = (uv)vu^2 \\ u^2v = v^2u(uv)u^2 &= v^2uv^2u^4 = v^2uv^2 \\ u^2 = v^2(uv) &= v^4u^2 = vu^2 \\ v &= 1 \end{aligned}$$

Putting this into the last relation, you get $u = u^2$, which means u is also equal to 1. So a group which looked like it might have order 12 turned out to have order 1, with the only element being the identity.

Problem 2.8 Let G be the group of rigid motions in $\mathbb{R}^3$ of the following solids : Tetrahedron, Cube, Dodecahedron. Find the orders of all these groups.

Solution The essence of this is to first calculate the number of vertices and see how many possibilities the adjacent vertices have of going to (keep in mind they still have to be connected). For a tetrahedron, it has 4 vertices and since each vertex is directly connected to 3 other vertices (basically all other vertices), the total number of rigid rotations is $4 * 3 = 12$.

Similarly, for a cube, 8 vertices, each vertex has 3 connections, so it's 24. For a dodecahedron, it has 12 pentagonal faces, and each vertex is in 3 faces, so the number of vertices is $12 * 5/3 = 20$, and since each vertex is again connected to 3 vertices, so the total is $20 * 3 = 60$.

Problem 2.9 Show that the group $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1 y_1)^2 = 1 \rangle$ is actually the dihedral group D_4.

Solution Let's show that the last relation is the same as $x_1 y_1 = y_1 x_1^{-1}$.

$$x_1 y_1 x_1 y_1 = 1 \implies x_1 y_1 = y_1^{-1} x_1^{-1}$$
$$x_1 y_1 = y_1 x_1^{-1} \qquad \text{since } y_1 = y_1^{-1}$$

Now it fits the presentation of the group D_4, hence it is the dihedral group D_4.

2.3 Symmetric Groups

Let Ω be any non-empty set and let S_Ω be the set of all bijections from Ω to itself (permutations). Then the set S_Ω is a group under function composition: $\circ$. Note that $\circ$ is a binary operation on S_Ω, and like function composition, is also associative. The identity is the permutation that takes a set to itself, i.e., $1(a) = a$ for all $a \in \Omega$. For every permutation σ there is also a two sided inverse function σ^{-1} satisfying $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$. This group is called the **symmetric group on the set** Ω.

Remark

It is very important to note that the elements of the group aren't the elements of the set, they are the **permutations** of the set.

When the set Ω is $\{ 1, 2, 3, \cdots, n \}$, the symmetric group is denoted S_n, the **sym-**

metric group of degree n[1]. We will use this group as a means of illustrating general theory.

It is fairly straightforward to see that the order of S_n is $n!$.

A **cycle** is a string of integers which cyclically permutes those integers and leaves the rest alone. The cycle (a_1, a_2, a_3) sends $a_1 \to a_2$, $a_2 \to a_3$ and $a_3 \to a_1$.

Remark

It is easily seen that the members of the cycle can themselves be cyclically permuted without altering the cycle itself, for example, $(1, 2, 3) = (2, 3, 1) = (3, 1, 2)$

In general, any permutation σ can be decomposed into a product of k cycles of the form :

$$(a_1 a_2 \dots a_{m_1})(a_{m_1+1} a_{m_1+2} \dots a_{m_2}) \dots (a_{m_{k-1}+1} a_{m_{k-1}+2} \dots a_{m_k})$$

This is called the **cycle decomposition** of σ and can be used to determine where any element goes in the permutation, by the rules of the cycle. Cycle decompositions are efficient ways to write elements σ of S_n.

The algorithm to find the cycle decomposition is fairly intuitive, and will be demonstrated with an example.

Let $n = 7$ and $\sigma \in S_7$ be defined as :

$$(1\,2\,3\,4\,5\,6\,7) \to (5\,2\,4\,6\,7\,3\,1)$$

Start with 1. As it goes to 5, the first cycle now has (1 5 so far. Find out where 5 goes. If it went back to 1, end the cycle and start a new cycle from the next smallest integer that hasn't appeared, i.e., in this case, 2. In this case, 5 goes to 7, so include 7 in the first cycle. 7 goes back to 1 now, so the cycle stops there as (1 5 7).

Now start the next cycle with 2 and follow the same procedure. In this case, 2 maps to itself, and by convention, cycles with one element can be omitted, as it is understood that it maps to itself. For example, the identity permutation maps everything to itself, so it's cycle decomposition can be simply written as 1

Next, 3 maps to 4, which maps to 6, which maps back to 3. So this cycle must be included as well.

Since we've exhausted all our elements, the final cycle decomposition is :

$$\sigma = (1\,5\,7)(3\,4\,6)$$

Some intuitive terms regarding cycles :

[1] The structure of S_Ω depends only on the cardinality of Ω, so it "looks like" S_n where n is the cardinality of Ω

- The **length** of a cycle is the number of integers which appear in it, and if the length is t, it is called a t-**cycle**
- Two cycles are called **disjoint** if they have no numbers in common

Remark

The convention not to include 1-cycles means that you can use the same cycle decomposition for sets with higher cardinality, with all the extra elements being fixed.

To find the cycle decomposition of the inverse permutation, just write the numbers in each cycle of the cycle decomposition in reverse order. For example, in the above cycle decomposition,

$$\sigma^{-1} = (7\,5\,1)(6\,4\,3)$$

Products in S_n are of the form $\sigma \circ \tau$, where σ and τ are both elements of S_n. The important thing is that like function composition, it goes from right to left, and it's sufficient to track where the elements go after successive permutations.

Example

In the product $(1\,2\,3\,4) \circ (1\,2)(3\,4\,5)$, in the first permutation, $1 \to 2$ and in the second, $2 \to 3$, so the whole thing maps $1 \to 3$. Similarly the composite maps $2 \to 2$, $3 \to 1$, $4 \to 5$ and $5 \to 4$, so $(1\,2\,3\,4) \circ (1\,2)(3\,4\,5) = (1\,3)(4\,5)$.

Example

Also, for example $(1\,2) \circ (1\,3) = (1\,3\,2)$ and $(1\,3) \circ (1\,2) = (1\,2\,3)$.

The above example shows that S_n **is a non-abelian group for all** $n \geq 3$

Another interesting fact is that **disjoint cycles commute**, since they only permute the elements in their cycles and not in the other ones.

Remark

A permutation may be written in many ways as an arbitrary product of cycles, for example, in S_3, $(1\,2\,3) = (1\,2)(2\,3) = (1\,3)(1\,3\,2)(1\,3)$, etc. However, the cycle decomposition of each permutation is the **unique** way of expressing a permutation as a product of **disjoint** cycles. Once you convert an arbitrary product into a disjoint product of cycles, you can determine easily whether the two permutations are the same.
Also, it can be proven that **the order of a permutation is the l.c.m of the lengths of the cycles in its cycle decomposition**.

Problem 2.10 Let σ be the 12-cycle (1 2 3 4 5 6 7 8 9 10 11 12). For which positive integers i is σ^i also a 12 cycle?

Solution It can be seen that *sigma* maps each element of the set to the element to the right of it, while mapping the last element to the first. This means σ^i maps each element to the element i places to the right, and cycles back to the first after the end.

We will look at where 1 goes. If 1 maps to 1 without going through all the other elements, then the permutation will not be a 12-cycle. This comes down to whether the number i is coprime with 12 or not. If it is coprime with 12, then the number 1 will be mapped with $1+ki \mod 12$ as the kth element in the cycle containing 1. So if i doesn't have any common factors with 12, then $1 + ki \mod 12$ will take all values from 1 to 12, but if not, it will go back to 1 for $k = \text{l.c.m}(12, i)/i$, which is a number between 1 and 12, which means the cycle containing 1 will be a k-cycle.
The final result is : σ^i will be a 12 cycle if and only if $\gcd(12, i) = 1$.

Problem 2.11 If $\tau = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)$ determine whether there is a n-cycle σ $(n \geq 10)$ such that $\tau = \sigma^k$ for some integer k.

Solution We observe that the order of τ is 2 (LCM of the lengths of the cycles). Therefore, if we're trying to find a 10-cycle (which is reasonable since there are 10 elements), k must be 5, since $(\sigma^k)^2$ must be the identity and that happens when $k = 5$.

We then see that in a 10-cycle (σ for example), if $k = 5$, then σ^5 will just map cycle through the elements which are 5 apart. So in this case, a possible σ is just (1 3 5 7 9 2 4 6 8 10), where σ^5 basically maps elements which are 5 apart (notice how they cycle around, for example, $1 \mapsto 2 \mapsto 1$, which completes a cycle.

Problem 2.12

Solution

2.4 Matrix Groups

The co-efficients of Matrix Groups come from fields. A **field** is the smallest mathematical structure in which we can perform all the arithmetic operations $+, -, \times, \div$ (by non-zero elements), so every non-zero element must have a multiplicative inverse.

In this section the only fields we will see are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{Z}/p\mathbb{Z}$, where p is a prime. The last example above is a finite field, and note that we chose a prime since only then would multiplicative inverses exist for every non-zero element in the group. We denote $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$.

Definition 2.12: Field

A **field** is a triple $(F, +, \cdot)$ such that $(F, +)$ is an abelian group (identity 0) and $(F \setminus \{0\}, \cdot)$ is also an abelian group, and the following **distributive** law holds :

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \qquad \text{for all } a, b, c \in F$$

For any field F let $F^x = F \setminus \{0\}$.

All the theory on vector spaces, matrices, linear transformations, etc. when the scalars come from R is true when the scalars come from a field F.

For each $n \in \mathbb{Z}^+$ let $GL_n(F)$ be the set of all $n \times n$ matrices whose entries come from F and whose $\det(A) \neq 0$. The determinant and product can be computed by the same formulas when $F = \mathbb{R}$.

The product of these matrices is still associative and since $\det(AB) = \det(A) \cdot \det(B)$, it follows that if $\det(A), \det(B) \neq 0$, then $\det(AB) \neq 0$, so $GL_n(F)$ is closed under matrix multiplication. Also, the fact that $\det(A) \neq 0$ means that every $A \in GL_n(F)$ has a (two sided) inverse. Also, the identity element is the $n \times n$ identity matrix.

Thus $GL_n(F)$ is a group under matrix multiplication, called the **general linear group of degree n**.

The following results are out of the scope of the paper, but are stated here and are to be accepted as a fact :

1. if F is a field and it's order is finite, then the order can be written as p^m for some prime p and integer m
2. if $|F| = q < \infty$, then $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2)(q^n - q^3) \dots (q^n - q^{n-1})$.

2.5 The Quaternion Group

The **quaternion group**, Q_8 s defined by

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

with product $\cdot$ as follows :

$$1 \cdot a = a \cdot 1 = a \qquad \text{for all } a \in Q_8$$

$$(-1)\cdot(-1)=1 \qquad (-1)\cdot a = a\cdot(-1) = -a, \qquad \text{for all } a \in Q_8$$

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

$$\begin{aligned} i\cdot j &= k, & j\cdot i &= -k \\ j\cdot k &= i, & k\cdot j &= -i \\ k\cdot i &= j, & i\cdot k &= -j \end{aligned}$$

We will interchangeably use both $a\cdot b$ and ab. Also, it is very long to check associativity, however, the other axioms are evident.

Q_8 is a non-abelian group of order 8.

2.6 Homomorphisms and Isomorphisms

The notion of an **isomorphism** between two groups, is a way to precisely define when two groups 'look the same', i.e., have the same group-theoretic structure.

Let's start with **homomorphisms**, which we will explore later.

Definition 2.13: Homomorphism

Let $(G,\star)$ and $(H,\diamond)$ be groups. A map $\phi : G \to H$ such that

$$\phi(x\star y) = \phi(x)\diamond\phi(y), \qquad \text{for all } x,y\in G$$

is called a **homomorphism**.

Sometimes the group operations are not explicitly written, in which case it is important to keep in mind that there are two different operations taking place, one in G and one in H.

Remark

Intuitively, a map ϕ is a homomorphism if it respects the group structures of its domain and codomain.

Definition 2.14: Isomorphism

The map $\phi : G \to H$ is called an **isomorphism** and G and H are said to be **isomorphic** or of the same **isomorphism type**, written $G \cong H$, if

- ϕ is a homomorphism (i.e., $\phi(xy) = \phi(x)\phi(y)$), and
- ϕ is a bijection.

Two groups are isomorphic if there is a bijection between them which preserves the group operations.

In other words, they are essentially the same group, except the elements and the operations may be written differently. Any property which one groups has, which depends only on the group structure (i.e., can be derived from it's group axioms, like commutativity), also holds in the other group. This justifies the writing of group operations as $\cdot$ since changing the symbol of the operation doesn't change the isomorphism type.

Remark

For any group, the identity map is an obvious isomorphism between itself, however it need not be the only one.
Also, if G is a nonempty collection of groups, the relation $\cong$ is actually an equivalence relation on G, since it is reflexive (G is isomorphic to itself), symmetric (The map is a bijection, so if $G \cong H$ through a map ϕ, then $H \cong G$ through the inverse map ϕ^{-1}) and transitive (the composition of the two maps will also satisfy all the properties that the two maps satisfied individually).

Example

$\exp(x) = e^x$, from $\mathbb{R} \to \mathbb{R}^+$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$, since the group operation is preserved ($e^{x+y} = e^x e^y$), and it has an inverse function $\log_e$. So even though the groups and the operations are different, as groups, they have identical structures.

The isomorphism type of a symmetric group depends only on the cardinality of the underlying set being permuted, i.e.

Theorem 2.15: Isomorphism of Symmetric Groups

Let Δ and Ω be non-empty sets. Then the symmetric groups S_Δ and S_Ω are isomorphic if and only if $|\Delta| = |\Omega|$.

Isomorphisms aren't only between groups. When different structures are studied (rings, fields, vector spaces, etc.), isomorphisms can be formulated across these different structures. An example of this is n isomorphism between two vector spaces V and W by mapping any basis set of V to a basis set of W. The transformation is invertible, and the operations of the vector space remain well defined.

A central problem in Mathematics is to determine which properties of a group specify its isomorphic type, such theorems are called **classification theorems**. For example

any non-abelian group of order 6 is isomorphic to S_3

It is easy to see when two groups are **not** isomorphic, by checking a few proper-

ties. If $\phi : G \to H$ is an isomorphism, then the following are necessary, but not sufficient conditions, meaning that if even one of them are wrong, it is equivalent to showing that they are not isomorphic.

- $|G| = |H|$
- G is abelian if and only if H is abelian
- for all $x \in G$, $|x| = |\phi(x)|$.

This can be used to show that $\mathbb{Z}/6\mathbb{Z}$ and S_3 are not isomorphic, since the former is abelian whereas the latter isn't. $(\mathbb{R} \setminus 0, +)$ and $(\mathbb{R}, +)$ aren't isomorphic, since in the former, -1 has an order of 2 whereas in the latter, there is no element which has the order 2.

Another useful fact that helps us use generators and relations to deal with homomorphisms and isomorphisms. Let G be a finite group of order n, containing a presentation and let $S = \{ s_1, s_2, \ldots, s_n \}$ be the generators. Let H be another group and $\{ r_1, r_2, \ldots, r_m \}$ be m elements of H. If we can choose the set $\{ r_1, r_2, \ldots, r_m \}$ from H such that any relation satisfied in G by the generators is also satisfied in $\{ r_1, r_2, \ldots, r_m \}$, this means that there is a unique homomorphism $\phi : G \to H$ which maps s_i to r_i.

If H is also generated by $\{ r_1, r_2, \ldots, r_m \}$ and has the same order as G (which makes the map both surjective and injective respectively), then $G \cong H$.

2.7 Group Actions

Group actions explain the precise way that a group acts on a set. It will be used to prove theorems for abstract groups and also to gain more info about its structure. The concept of an action is a method for studying an algebraic object by seeing how it can act on other structures.

Definition 2.16: Group Action

A **group action** of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$ for all $g \in G$ and $a \in A$) satisfying the following properties

- $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$.
- $1 \cdot a = a, \quad$ for all $a \in A$.

Less formally, G is a group acting on a set A.

Remark

Note that in the first property, $(g_2 \cdot a)$ is an element of A (since the group action maps $G \times A \to A$) and acting on it by g_1 makes sense, and gives the final result as an element in A. On the right hand side, $(g_1 g_2)$ is a product in G itself, which gives you an element in G again, which acts on

a as a group action to give an element in A.

Let the group G act on the set A. Then for an element $g \in G$ we get a map σ_g defined by :

$$\sigma_g : A \to A$$
$$\sigma_g(a) = g \cdot a$$

It can be proved that :

- for each fixed $g \in G$, σ_g is a **permutation** of A
- The map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism

To prove the first, it's enough if we show that σ_g, as a set map from A to A it has a 2-sided inverse, namely $\sigma_{g^{-1}}$, and now σ_g is a bijection from A to A, which means it's a permutation by Proposition 1.1

For the second, you must show that $\phi(g_1 g_2) = \phi(g_1) \circ \phi(g_2)$, since S_A is a group under function composition.

A group action of G on a set A means that every element g in G acts as a permutation on A in a manner consistent with the group operations in G. The homomorphism from G to S_A is called the **permutation representation** associated to the given action.

Example

Let G be a group and A be a non-empty set. Let $ga = a$, for all $g \in G$, $a \in A$. This is called the **trivial action** and G is said to act trivially on A. **Distinct** elements in G induce the same permutation in A, the identity. The permutation representation $G \to S_A$ is the trivial homomorphism which maps G as a whole to the identity.

Definition 2.17: Kernel

The **kernel** of the action of G on B is defined to be $\{ g \in G \mid gb = b$ for all $b \in B \}$, all the elements of G which fix **all** the elements of B.

For the trivial action, the kernel is all of G.

Let G be any group and let $A = G$. A map from $G \times A$ to A by $g \cdot a = ga$, where ga is the product in the group G. This is a group action of G on itself,

where each fixed $g \in G$ permutes the elements of G by **left multiplication** :

$$g : a \mapsto ga \qquad \text{for all } a \in G$$

Some interesting and insightful problems :

3 Subgroups

3.1 Definition and Examples

In general, when studying about a larger mathematical object that satisfies some set of axioms, it's easier to unravel it's structure by looking at **subsets** of the object, which also **satisfy** the same axioms. Another method for studying the structure of a group is to deal with a quotient group, which is for the next chapter.

Definition 3.1: Subgroup

Let G be a group. The subset H of G is a **subgroup** of G if H is nonempty and H is closed under products and inverses ($x, y \in H \implies x^{-1} \in H$ and $xy \in H$).

The notation, if H is a subgroup of G, is $H \leq G$, and if $H \neq G$ then it can be written as $H < G$, to emphasise the proper containment.

Basically, a subgroup of G is just a subset which is itself a group with respect to the operation of G. So in general, when it is said that H is a subgroup of G, it is implied that it is under the same operation as that of G, restricted to H of course (It is possible that H is a group under some other operation as well though).

Remark

As the operation is the same with respect to a group, any equation in the subgroup H is an equation in the group G. This implies that the **identity** of G must be, first of all, present in H, and furthermore, must be the identity also in H.

Also, the inverse of an element x in H is the same as the inverse of x in G (x^{-1} is the same in both places)

Example

$\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$, operation being $+$.

Example

Any group has atleast 2 subgroups : One being just the identity element and the other being itself. The former is called the **trivial subgroup** and is denoted by 1.

Example

In D_{2n}, the set of all rotations represented by $\{1, r, r^2, \ldots, r^{n-1}\}$ is a subgroup of D_{2n} of order n, since the product of two rotations is a rotation and the inverse of a rotation is also a rotation.

Example

In the group of quaternions, the set $\{1, -1\}$ is itself a subgroup, since multiplying any 2 elements gives an element in the set, and the inverses of $1, -1$ are $1, -1$ respectively.
Note that $\{1, -1, i, -i\}$ is also a subgroup, however, $\{1, i, -i\}$ is not a subgroup, since $i \cdot i = -1$, which isn't in the group.

Some examples of subsets which are not subgroups are :

Example

$\mathbb{Z}^+$ under addition is not a subgroup of $\mathbb{Z}$ under addition, since it doesn't have the identity, 1, and it isn't closed with respect to inverses.

Also, the relation "is a subgroup of" is transitive, i.e., if $F \leq G$ and $G \leq H$ then $F \leq H$.

Proposition 3.2: The Subgroup Criterion

A subset H of a group G is a subgroup if and only if
1. *$H \neq \emptyset$*
2. *for all $x, y \in H$, $xy^{-1} \in H$.*

Furthermore, if H is finite, it is enough to check that H is non-empty and closed under multiplication.

Proof. If H is a subgroup of G, then both the properties hold, since the identity and the inverses are all in the group, and the group is closed under multiplication.
Now, we need to show that if the two properties hold, then $H \leq G$. Take an element x in H (which is possible as H is non-empty by property 1). Now, by property 2, taking $y = x$, we get that $xx^{-1} = 1 \in H$.

Now that H contains the elements 1 and x, it must also contain $1x^{-1} = x^{-1}$ and H is closed under taking inverses. Finally, if x, y are two elements of H, then H contains y^{-1} also, and so H contains $x(y^{-1})^{-1} = xy$, meaning it is closed under multiplication, which proves that H is a subgroup of G.
Now, if H is finite and closed under multiplication, then if x is any element in H, there are only finitely many distinct elements among $x, x^2, x^3, \ldots$ and so $x^a = x^b$ for some integers a, b with $b > a$. By cancellation, $x^{b-a} = 1$, so every element in H is of finite order. Finally, from $x^{b-a} = 1$, we get the relation $x \cdot x^{b-a-1} = x^{b-a-1} \cdot x = 1$, and so there exists an inverse for every element x. □

3.2 Centralizers, Normalizers, Stabilizers and Kernels

Let A be a non-empty subset of G.

Definition 3.3: Centralizer

Define $C_G(A) = \{\, g \in G \mid gag^{-1} = a \text{ for all } a \in A \,\}$. This subset is called the **centralizer** of A in G.
This relation is equivalent to the fact that $ga = ag$, so $C_G(A)$ is the set of elements in G which commute with every element in A.

Let us prove that $C_G(A)$ is a subgroup of G.

Proof. Using the fact that $C_G(A)$ is a set of elements that commute with each and every element of A, the identity element must be a part of $C_G(A)$, since $1 \cdot a = a \cdot 1 = a$ for all $a \in A$.
To prove that the group is closed under inverses, let $x \in C_G(A)$, which means $xax^{-1} = a$ for all $a \in A$. By pre-multiplying both sides by x^{-1} and post-multiplying by x, we get that $x^{-1}ax = a$ for all $a \in A$, which means x^{-1} also belongs to $C_G(A)$.
Given $x, y \in C_G(A)$, let's prove that xy is also in $C_G(A)$.

$$\begin{aligned}(xy)a(xy)^{-1} &= (xy)ay^{-1}x^{-1} \\ &= x(yay^{-1})x^{-1} \\ &= x(a)x^{-1} \\ &= a\end{aligned}$$

Hence $C_G(A)$ is closed under both inverses and multiplication, therefore $C_G(A) \leq G$. □

If A is a singleton set, for example, $\{\, a \,\}$, it suffices to write $C_G(a)$ as the

centralizer of A. Also note that $a^n \in C_G(A)$ for all $n \in Z$.

Remark

It is pretty obvious, but for an abelian group G, $C_G(A) = G$, for all subsets A.

Definition 3.4: Center

Define $Z(G) = \{ g \in G \mid gx = xg \text{ for all } x \in G \}$, the set of elements commuting with all the elements of G. This set is called the **center** of G.

Note that $Z(G) = C_G(G)$, so $Z(G)$ is already a subgroup of G.

Definition 3.5: Normalizer

Define $gAg^{-1} = \{ gag^{-1} \mid a \in A \}$. Define the **normalizer** of A to be the set $N_G(A) = \{ g \in G \mid gAg^{-1} = A \}$.

If $g \in C_G(A)$, then $gag^{-1} = a \in A$ for all $a \in A$, so $C_G(A) \leq N_G(A)$. Proving that $N_G(A)$ is a subgroup is similar to proving likewise for $C_G(A)$.

Remark

Note that $C_G(A)$ need not be equal to $N_G(A)$, since the difference between them is that in $C_G(A)$, specifically, $gag^{-1} = a$, or $a \mapsto a$, whereas in $N_G(A)$, it does not require an element in A to map to itself, just that the entire set to be mapped to itself in the end.
Suppose $A = \{a, b\}$ and there is a $g \in G$ such that $gag^{-1} = b$ and $gbg^{-1} = a$. Then $gAg^{-1} = \{b, a\} = A$, although $gag^{-1} \neq a$ and $gbg^{-1} \neq b$.

Example

Let $A = \{ 1, r, r^2, \ldots, r^{n-1} \}$ be a subset of D_{2n}, r, s being the generators of D_{2n}, then $C_{D_{2n}}(A) = A$. We observe that r^m, for all m, commutes with every element of the set A. All the other elements of D_{2n} are of the form sr^i for $0 \leq i < n$. We also know that $r^i s = sr^{-i}$, so $r^m sr^i = sr^{-m}r^i \neq sr^i r^m$ for all allowed i, m. Hence only the elements of A commute with every element of A, which proves the statement.

Example

Related to the previous example, we try and find $N_{D_{2n}}(A)$. We know that the elements of A are part of the normalizer, since it's centralizer is a subset of the normalizer. Now let's try and see if s is part of the

normalizer.

$$\begin{aligned} sAs^{-1} &= \{\, s1s^{-1}, srs^{-1}sr^2s^{-1}, \ldots, sr^{n-1}s^{-1} \,\} \\ &= \{\, s1s^{-1}, sr^{n-1}s^{-1}, sr^{n-2}s^{-1}, \ldots, srs^{-1} \,\} \\ &= A \end{aligned}$$

This means s is a part of the normalizer. Also, since the normalizer is a subgroup, we see that since both s and A are present in the subgroup, their products must also be present. Therefore we get that the entire set D_{2n} is part of the normalizer, and since the normaliser is a subgroup of the original group, it cannot have any elements not part of the original group, hence $N_{D_{2n}}(A) = D_{2n}$

Example

Finally, an example for the **center** of a group : $\{\, 1, r^2 \,\}$ is the center for D_8.
The first observation is that the center of a group is contained in $C_G(A)$ for all $A \leq G$. So, the center is limited to a subset of A. r and r^3 are both not part of the center, since they don't commute with s ($rs = sr^{-1} = sr^3 and r^3 s = sr^{-3} = sr$). r^2 commutes both with r and s ($r^2 s = sr^{-2} = sr^2$), and as every element is generated by r and s, r^2 commutes with every element in D_8 and so the centre is $\{\, 1, r^2 \,\}$

The fact that the normalizer of A in G, the centralizer of A in G, and the center of G are all subgroups can be deduced as special cases of results on group actions, indicating that the structure of G is reflected by the sets on which it acts, as follows:

Definition 3.6: Stabilizer

If G is a group acting on a set S and s is some fixed element of S, the stabilizer of s in G is the set

$$G_s = \{\, g \in G \mid g \cdot s = s \,\}$$

It can be shown that G_s is a group under the group operation of G. (The steps are the same as showing that the centralizer was a subgroup, but the associative identity gets replaced by Axiom 1 of Definition 2.16)

Definition 3.7: Kernel

If G is a group acting on a set S, the kernel of the action of G on S is defined as :

$$G_s = \{\, g \in G \mid g \cdot s = s, \text{ for all } s \in S \,\}$$

Proving that the kernel is a subgroup of G is also straightforward.

Finally, we observe that the fact that centralizers, normalizers and kernels are subgroups is a special case of the facts that stabilizers and kernels of actions are subgroups.

Let $S = \mathcal{P}(G)$, the collection of all subsets of G , and let G act on S by conjugation, that is, for each $g \in G$ and each $B \subseteq G$ let

$$g : B \to gBg^{-1} \quad \text{where} \quad gBg^{-1} = \left\{\, gbg^{-1} \mid b \in B \,\right\}$$

. Under this action, it is easy to check that $N_G(A)$ is precisely the stabilizer of A in G, so $N_G(A)$ is a subgroup of G.

3.3 Cyclic Groups and Subgroups

Given a group G and a random element x in it, the easiest way to form a subgroup H is by letting H be the set of all the integer powers of x (guarantees closure under inverses and products)

Definition 3.8: Cyclic Group

A group H is **cyclic** if H can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{\, x^n \mid n \in \mathbb{Z} \,\}$ (where the operation is multiplication)

This means, we can write $H = \langle\, x \,\rangle$ and say H is **generated** by x. We shall see how to find out all possible generators of a given cyclic group H. Also, by exponent laws, **all cyclic groups are abelian.**

Example

Some examples of cyclic groups include the subgroup of all rotations in D_2n with r as the generator.
Another example is the group $H = \mathbb{Z}$ over $+$, which can be generated by the element 1, with 0 as the identity.

Proposition 3.9: Orders of sets and elements

If $H = \langle x \rangle$, then $|H| = |x|$ (assuming infinities can be considered equal). More specifically :

1. *If $|H| = n$, which is finite, then $x^n = 1$ and $1, x, \ldots, x^{n-1}$ are all the distinct elements of H.*
2. *If the order of H is infinite, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$*

This proposition is quite intuitive, but relates the order of a cyclic group to the order of the generator of the group.

This gives us a method to reduce arbitrary powers of a generator in a finite cyclic group into its least powers, and notice how they're being calculated using the elements in $\mathbb{Z}/n\mathbb{Z}$ (not a coincidence)

Proposition 3.10

Let G be an arbitrary group, $x \in G$ and let $x^m = 1$ and $x^n = 1$ both be valid, for $m, n \in \mathbb{Z}$ Then $x^d = 1$, where $d = \gcd(m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m.

The proof is pretty straightforward, using the Euclidean Algorithm to write d in terms of a sum of integer multiples of m and n is the key step. The second part can be proven using the first.

Theorem 3.11: Isomorphism of Cyclic Groups

Any two cyclic groups of the same order are isomorphic. Specifically :

1. *If $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map*

$$\varphi : \langle x \rangle \to \langle y \rangle$$
$$x^k \mapsto y^k$$

   is well defined and is a isomorphism.

2. *If $\langle x \rangle$ is an infinite cyclic group, then the map*

$$\varphi : \mathbb{Z} \to \langle y \rangle$$
$$k \mapsto y^k$$

   is well defined and is an isomorphism.

I'll leave the proof as an exercise (gives me some sadistic pleasure saying this), but it can be done just by the definition of an isomorphism.

Remark

Since $\mathbb{Z}/n\mathbb{Z}$ is also a cyclic group of order n under addition modulo n, any cyclic group with order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Let's introduce some notation for cyclic groups (since all of them having the same order are isomorphic to each other). Let's call the cyclic group with order $n \in \mathbb{Z}^+ Z_n$ (written multiplicatively) and it is unique upto isomorphism.

When we want to use additive notation, we will use $\mathbb{Z}/n\mathbb{Z}$ as our representative cyclic group of order n (for infinite order, it will be $\mathbb{Z}$).

A cyclic group may have many possible generators, the following propositions determine exactly which powers of x can be used to generate the cyclic group $\langle x \rangle$.

Proposition 3.12: Orders of Elements in Cyclic Groups

Let G be a group, let $x \in G$ and let $a \in \mathbb{Z} \setminus \{0\}$. Then :

1. *If $|x| = \infty$, then $|x^a| = \infty$*
2. *If $|x| = n < \infty$, then $|x^a| = \frac{n}{\gcd(n,a)}$.*
3. *In particular, if $|x| = n < \infty$ and a is a positive integer dividing n, then $|x^a| = \frac{n}{a}$.*

Proof. 1. Assume that $|x| = \infty$ whereas $|x^a| = m < \infty$. This means that $x^{am} = 1$, where $a, m \in \mathbb{Z} \setminus \{0\}$. Similarly, we can show that $x^{-am} = 1$. Therefore, since $a, m \neq 0$, some positive finite power of x is 1, which is a contradiction.

2. This proof is fairly intuitive, I hope it has sufficient mathematical rigor. Since the order of x is n, multiplying x n times will give you the identity. We also know that multiplying x with itself k number of times, where $k < n$, will not give you the identity (since the order is the least possible number). Similarly, if for some m, $x^m = 1$, this means n divides m, since if n didn't divide m, we could write $m = nq + r$, where $0 < r < n$, and the equation would reduce to $x^{nq}x^r = 1$, and since $x^{nq} = (x^n)^q = 1$, x^r would have to be 1, which is not possible, therefore, n must divide m.
   Now, let t be the order of x^a, which means x^a multiplied t times with itself will give you 1, or, x multiplied at times would give you 1. We must choose the smallest possible t such that this is possible. By the previous para, we know n must divide at, and the smallest at such that this is possible is the $\text{lcm}(a, n)$, since at must be both a multiple of n and a, and must be the least possible number.
   Therefore, if $at = \text{lcm}(n, a)$, then $t = \text{lcm}(n, a)/a$, which means

$t = \frac{n}{\gcd(n,a)}$

3. This part folows directly from the 2nd part, however, direct proofs are much easier to think of.

□

Proposition 3.13: Generators of Cyclic Groups

Let $H = \langle x \rangle$.

1. *If the order of x is infinite, then $H = \langle x^a \rangle$ if and only if $a = \pm 1$*
2. *If the order of $x = n < \infty$, then $H = \langle x^a \rangle$ if and only if $(a, n) = 1$. Also, the number of generators is $\varphi(n)$, where φ is Euler's $\varphi-$function.*

Proof.

1. If the order is infinite, then for every $a \in \mathbb{Z}$, x^a is unique. If x^a is a generator, where $a \in \mathbb{Z}$ but $\neq \pm 1$, then it is impossible to generate x with integer powers of x^a. Therefore, the only generators are x, x^{-1}.
2. By Proposition 3.9, we see that the order of the subgroup generated by x^a is $|x^a|$. This subgroup is H only when $|x^a| = |x|$, which by Proposition 3.12, only happens when $\gcd(n, a) = 1$.
   Also, x^a where a is not between 0 and $n - 1$ can be reduced to a unique residue power which satisfies the conditions, therefore, the number of generators is $\varphi(n)$, since we're only checking for positive integers $\leq n$

□

The above proposition also tells us which residue classes mod n can generate $\mathbb{Z}/n\mathbb{Z}$, $\bar{a}$ generates it only if $\gcd(a, n) = 1$

The next theorem specifies the complete subgroup structure of a cyclic group.

Theorem 3.14: Subgroups of Cyclic Groups

Let $H = \langle x \rangle$ be a cyclic group.

1. *Every subgroup of H is cyclic, and if $K \leq H$, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.*
2. *If $|H| = \infty$, then for any distinct non negative integers a and b, $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$, so the non-trivial subgroups of H correspond bijectively with the integers $1, 2, \ldots$.*
3. *If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of H of order a. This subgroup is the cyclic*

subgroup $\langle x^d \rangle$, *where* $d = \frac{n}{a}$. *Furthermore, for every integer* m, $\langle x^m \rangle = \langle x^{\gcd(m,n)} \rangle$, *so that the subgroups of* H *correspond bijectively with the positive divisors of* n.

Example

We can use the previous theorems and propositions to list all the possible subgroups of $\mathbb{Z}/n\mathbb{Z}$ for any given n. For example, for $n = 12$:

- $\mathbb{Z}/12\mathbb{Z} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \overline{11} \rangle$ (order 12)
- $\langle \bar{2} \rangle = \langle \overline{10} \rangle$ (order 6)
- $\langle \bar{3} \rangle = \langle \bar{9} \rangle$ (order 4)
- $\langle \bar{4} \rangle = \langle \bar{8} \rangle$ (order 3)
- $\langle \bar{6} \rangle$ (order 2)
- $\langle \bar{0} \rangle$ (order 1)

The inclusions between them are given by

$$\langle \bar{a} \rangle \leq \langle \bar{b} \rangle \quad \text{if and only if } \gcd(b, 12) \mid \gcd(a, 12)$$

3.4 Subgroups Generated by Subsets of a Group

Forming cyclic subgroups of a given group is a special case of the usual way of forming a subgroup generated from an arbitrary subset of a group. In cyclic subgroups, that subset was a singleton set, for example $\{x\}$ and the cyclic subgroup consisted of all powers of x, which indirectly is the same as closing the set under the group operation and the process of taking inverses.

This makes this subgroup the "smallest" subgroup that contains the set $\{x\}$ (smallest in the sense that any subgroup which has the element x must also contain $\langle x \rangle$, i.e., sorted by inclusion). Another way of saying this is that $\langle x \rangle$ is the unique minimal element of the set of subgroups of G containing x, where G is the parent group (The minimal element is assuming that the elements are ordered under inclusion). We try to look at how the subgroups look when the singleton set $\{x\}$ is replaced by an arbitrary subset of G.

This problem is analogous to a similar problem dealing with vector spaces : What is the smallest (again, by inclusion) vector subspace of $\mathbb{R}^n$ that contains a particular set of vectors $A = \{ v_1, v_2, \ldots, v_n \}$.

A quick recap of a vector space over reals :

1. Must not be empty.
2. If a vector space has an element, then any real scalar multiplied by the element must also be an element in the vector space. (Implies that the zero vector is always part of a vector space)

3. If a vector space has 2 elements, then their sum must also be part of the vector space.

The smallest vector subspace that contains the set A is said to be the **span** of A, that is, the set of all linear combinations of the elements of A (coefficients can be any real number).

Now, let's try to precisely define the notion of a subgroup G defined from A, where G is a group and A is any subset of the group.

Proposition 3.15: Intersection of Subgroups

If $\mathcal{A}$ is any non-empty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroup of G.

Proof. This can be proved using The Subgroup Criterion (Proposition 3.2). Let K be the set of intersection of all the elements of $\mathcal{A}$. Very clearly, 1 is an element of K, since it is present in all the subgroups of $\mathcal{A}$.

Secondly, if $a, b \in K$, that means a, b must be part of every element of $\mathcal{A}$. Since all elements of $\mathcal{A}$ are subgroups, by Proposition 3.2, they must also contain ab^{-1}, and if all elements of $\mathcal{A}$ contain ab^{-1}, then that means K also contains ab^{-1}, and this means that by Proposition 3.2, K is a subgroup of G. □

Definition 3.16: Subgroup Generated by a Subset

If A is any subset of the group G define

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

This is called the **subgroup of G generated by A.**

Thus $\langle A \rangle$ is the intersection of all subgroups of G containing A. It can be shown that it is a subgroup of G with $\mathcal{A} = \{ H \mid A \subseteq H, H \leq G \}$ by the previous proposition ($\mathcal{A}$ is non-empty since G itself is in it). $\langle A \rangle$ is the unique minimal element in $\mathcal{A}$ (ordered by inclusion) since firstly, it is part of $\mathcal{A}$ since it is a subgroup of G containing A, and it is the intersection of all the elements of $\mathcal{A}$, which means every element contains $\langle A \rangle$.

When A is the finite set $\{ a_1, a_2, \ldots, a_n \}$, we write $\langle A \rangle$ as $\langle a_1, a_2, \ldots, a_n \rangle$, and if A, B are two sets, instead of $\langle A \cup B \rangle$ we write $\langle A, B \rangle$

Let's now define the set which is the closure of A under the group operation

(and under the process of taking inverses) and prove that this set equals $\langle A \rangle$. Let

$$\overline{A} = \{ a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \mid n \in \mathbb{Z}, n \geq 0 \text{ and } a_i \in A, \epsilon_i = \pm 1 \text{ for each } i \}$$

where $\overline{A} = \{1\}$ if $A = \varnothing$ so that $\overline{A}$ is the set of all finite products (called **words**) of elements of A and their inverses. The a_is need not be distinct, so a^2, for example, can be written as aa in the notation defining $\overline{A}$. Also, A is not assumed to be a finite or even countable set.

Proposition 3.17: Subgroup Generated by a Subset

$$\overline{A} = \langle A \rangle$$

Proof. Note that $\overline{A}$ can never be empty, not even when $A = \varnothing$. Now, to prove that $\overline{A}$ is a subgroup, we just need to use Proposition 3.2. Let $a, b \in \overline{A}$ with $a = a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n}$ and $b = b_1^{\delta_1} b_2^{\delta_2} \dots b_m^{\delta_m}$, then

$$ab^{-1} = a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \cdot b_m^{-\delta_m} b_{m-1}^{-\delta_{m-1}} \dots b_1^{-\delta_1}$$

Thus, ab^{-1} is a product of elements of A raised to powers ± 1, hence $ab^{-1} \in \overline{A}$, therefore, $\overline{A}$ is a subgroup of G.
Each $a \in A$ could be written as a^1, hence, $A \subseteq \overline{A}$, hence $\langle A \rangle \subseteq \overline{A}$ (Since every subgroup containing A must contain $\langle A \rangle$, the subgroup generated by A). But since $\langle A \rangle$ is a group containing A, hence it must have all elements of the form $a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n}$ (closure under products and inverses). This means that $\overline{A} \subseteq \langle A \rangle$. The proof is done. □

Remark

Another neat way to write $\langle A \rangle$ is by noting that, in the previous definition of $\langle A \rangle$, terms like aa, aaa, aa^{-1} could be simplified further. So a better way to write it would be

$$\langle A \rangle = \{a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n} \mid n \in \mathbb{Z}^+ \text{ and } a_i \in A, a_i \neq a_{i+1}, \alpha_i \in \mathbb{Z} \text{ for each } i\}$$

Even better, when G is abelian, and A is the finite subset $\{a_1, a_2, \dots, a_k\}$ we can directly write

$$\langle A \rangle = \{ a_1^{\alpha_1} a_2^{\alpha_2} \dots a_k^{\alpha_k} \mid \alpha_i \in \mathbb{Z} \text{ for each } i \}$$

In the abelian case, we can put an upper bound on the order of the set, if we know the order of the individual elements. In the above example, let the orders of $\{a_1, a_2, \dots, a_k\}$ be $\{d_1, d_2, \dots, d_k\}$ respectively. Then $|\langle A \rangle| < d_1 d_2 \dots d_k$, since that is the maximum number of distinct products (there might be lesser but this is the worst case)

For non-abelian groups, let's just say, it's a lot more difficult, and that even if the order of the generator elements is known, we won't be able to find out the order of the subgroup.

3.5 The Lattice of Subgroups of a Group

We won't go too in depth with the idea here, but I'll just give you a brief intro to the idea and show some examples.

The lattice of subgroups of a group is a graph associated with the group that depicts the relation between its subgroups. It's a good way to visualise a group (better than a multiplication table)

It is constructed as follows : plot all subgroups of G starting at the bottom with 1 , ending at the top with G and, roughly speaking, with subgroups of larger order positioned higher on the page than those of smaller order. Draw paths upwards between subgroups using the rule that there will be a line upward from A to B if $A \leq B$ and if there are no other subgroups properly in between A and B.

So if $A \leq B$ there is a path connecting A to B which may or may not be filled with intermediate subgroups which are contained in B and themselves contain A.

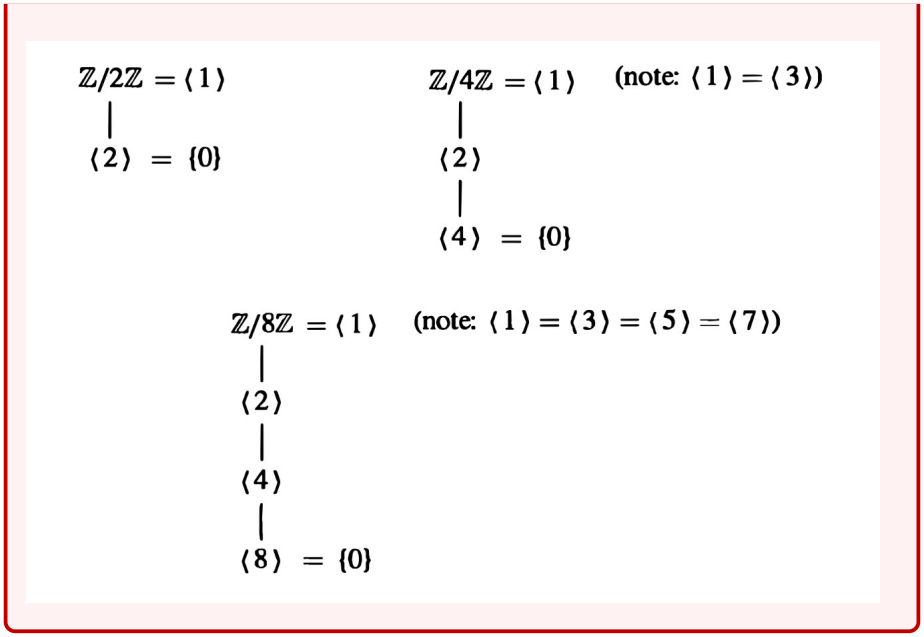
Some limitations : Cannot be carried out for infinite groups, and difficult for finite groups of larger order. There are some cases where it's extremely difficult even with a small order group.

Remark

Notice that isometric groups have the same lattice structure (the same directed graphs), however, it is possible for two non-isometric groups to also have the same lattice structure.

Example

For $G = Z_n = \mathbb{Z}/n\mathbb{Z}$, by Theorem 3.14, the lattice of subgroups of G is the lattice of divisors of n (that is, the divisors of n are written on a page with n at the bottom, 1 at the top and paths upwards from a to b if $b \mid a$. Some examples are :

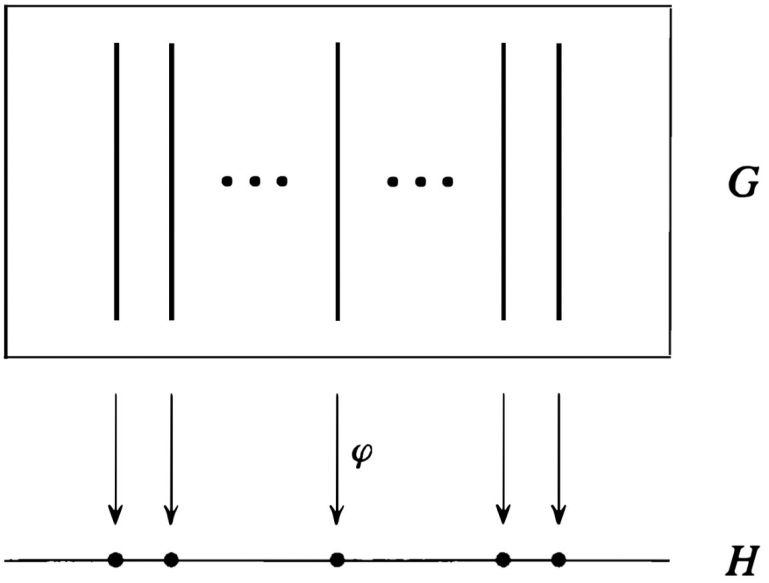


4 Quotient Groups and Homomorphisms

Quotient groups are another way of getting smaller groups from a bigger group and therefore can also be used in studying it's properties. The structure of the group G is reflected in the structure of the quotient groups and the subgroups of G.

The study of the quotient groups of G is essentially equivalent to the study of the homomorphisms of G, i.e., the maps of the group G to another group which respect the group structures.

If φ is a homomorphism from G to a group H recall that the **fibers** of φ are the sets of elements of G projecting to single elements of H , which we can represent pictorially as shown below :



where the vertical line in the box above a point a represents the fiber of φ over a.

Remark

Note, that if the mapping between G and H is an isomorphism (a bijective homomorphism), that means each filter consists of only 1 element in G.

Since the group operation allows us to multiply two elements in the image of φ, we should be able to multiply the **fibers** above them. This lends itself to the idea of **the set of fibers being a group**, since the group operation can be linked with the group operation of H.

Everything fits nicely, if X_a is the fiber above a and X_b is the fiber above b then the product of X_a with X_b is defined to be the fiber above the element ab in H, namely X_{ab}. Associativity of the multiplication of fibers follows from the associativity of the group operation in H, the identity is the fiber above the identity in H, and the inverse of the fiber over a is the fiber over a^{-1}.

Basically, the group G is partitioned into sub parts (fibers), which themselves have the structure of a group, called a **quotient** group of G. (Defined a bit later)

Remark

Since the multiplication of fibers is defined from the multiplication of elements in H, the quotient group with this multiplication is isomorphic to the group H (the image of G under the homomorphism φ) since the fiber X_a is identified by the element a in H.

Example

Let $G = \mathbb{Z}$ and $H = Z_n = \langle x \rangle$ be the cyclic group of order n and define $\varphi : \mathbb{Z} \to Z_n$ by $\varphi(a) = x^a$.

$$\varphi(a+b) = x^{a+b} = x^a x^b = \varphi(a)\varphi(b)$$

which shows that φ is a homomorphism (operation on $\mathbb{Z}$ is addition and Z_n is multiplication). φ is also surjective.
It can be seen that the fiber of φ over x^a is the equivalence class $\overline{a}$, since $x^n = 1$. Therefore, the fibers of φ are the residue classes **modulo** n

Some properties of homomorphisms and fibers are given below :

Definition 4.1: Kernel of a Homomorphism

If φ is a homomorphism $\varphi : G \to H$, the **kernel** of φ is the set

$$g \in G \mid \varphi(g) = 1$$

and will be denoted by $\ker(\varphi)$ (1 is the identity of H here)

The **kernel** of the map is just the fiber over the identity element of the image.

Proposition 4.2: Some Properties of Homomorphisms

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

1. $\varphi(1_G) = 1_H$
2. $\varphi(g^{-1}) = (\varphi(g))^{-1}$ *for all* $g \in G$
3. $\varphi(g^n) = (\varphi(g))^n$ *for all* $g \in G$, $n \in \mathbb{Z}$
4. *$\ker(\varphi)$ is a subgroup of G.*
5. *The image of G under φ is a subgroup of H.*

The proofs are fairly straightforward, so I'll leave them to you.

Let's define stuff!

Definition 4.3: Quotient Groups

Let $\varphi : G \to H$ be a homomorphism with kernel K. The **quotient group** of **factor group**, G/K (read G **modulo** K or simply G **mod** K is the group whose elements are the fibers of φ with group operation defined as : if X is the fiber above a and Y is the fiber above b then the product of X and Y is defined to be the fiber above the product ab.

The notation emphasizes the fact that the kernel K is a single element in the group G/K and we shall see below that, as in the case of $\mathbb{Z}/n\mathbb{Z}$ above, the other elements of G/K are just the "translates" of the kernel K. Hence we may think of G/K as being obtained by collapsing or "dividing out" by K (or more precisely, by equivalence modulo K). This explains why G/K is referred to as a **quotient** group.

The definition of the quotient group would ideally require the map φ explicitly, since multiplication of fibers involves projecting both the fibers using φ, multiplying in the image and then determining the fiber over the product.

However, it is also possible to define the multiplication of fibers directly in terms of representatives from the fibers. Here, the map doesn't enter explicitly and it's also computationally easier.

We first show that the fibers of a homomorphism can be expressed in terms of the kernel of the homomorphism just as in the example above (where the kernel was $n\mathbb{Z}$ and the fibers were translates of the form $a + n\mathbb{Z}$).

Proposition 4.4: Fibers in terms of the Kernel

Let $\varphi : G \to H$ be a homomorphism with kernel K. Let $X \in G/K$ be the fiber above a, i.e., $X = \varphi^{-1}(a)$. Then

1. *For any $u \in X$, $X = \{uk \mid k \in K\}$*
2. *For any $u \in X$, $X = \{ku \mid k \in K\}$*

Proof. The proof for 1. is as follows : Let $u \in X$ and let $U = \{uk \mid k \in K\}$. Our goal is to prove that $U = X$, and we try to prove containment both ways.
We know that $\varphi(u) = a$ (By the definition of fibers). Let us prove $U \subseteq X$. For any $k \in K$,

$$\begin{aligned} \varphi(uk) &= \varphi(u)\varphi(k) && \text{(Since } \varphi \text{ is a homomorphism)} \\ &= a \cdot 1 && \text{(Since } k \in \ker(\varphi) \\ &= a \end{aligned}$$

i.e., $uk \in X$, which proves $U \subseteq X$.

To prove the reverse containment : Let $g \in X$ and let $k = u^{-1}g$. Then :

$$\begin{aligned}\varphi(k) &= \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g) \qquad \text{(By the above proposition)} \\ &= a^{-1}a = 1\end{aligned}$$

which shows that $k \in \ker(\varphi)$. Since $k = u^{-1}g$, $g = uk \in U$, which proves $X \subseteq U$.
2. can be proved very similarly as well. □

The sets arising in the above Proposition are defined for any set K, not necessarily the kernel of the map, and are given names.

Definition 4.5: Cosets of a Subset of a Group

For any $N \leq G$ and any $g \in G$ let

$$gN = \{gn \mid n \in N\} \text{ and } Ng = \{ng \mid n \in N\}$$

called a **left coset** and a **right coset** respectively of N in G. Any element of the coset is called a **representative** for the coset.

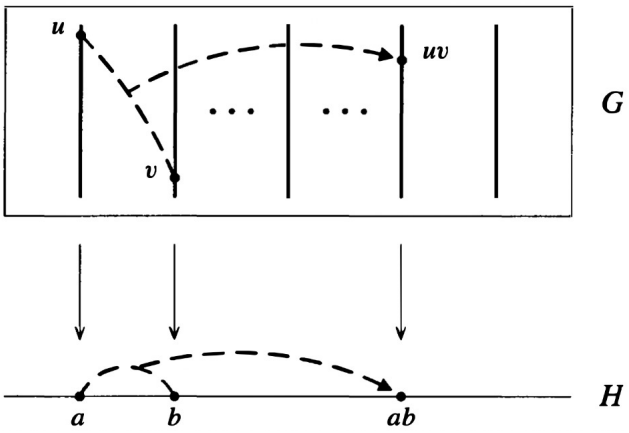
Theorem 4.6: Cosets and Quotient Groups

Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set whose elements are the left cosets of K in G with operation defined by

$$uK \circ vK = (uv)K$$

forms a group G/K. In particular, this operation is well defined in the sense that if u_1 is any element in uK and v_1 is any element in vK, then $u_1v_1 \in (uv)K$, furthermore, $u_1v_1 = (uv)K$ so that the multiplication is independent of the choice of representation of cosets. The same is true replacing left coset with right coset.

This figure gives a good pictorial representation for the multiplication in G/K via representatives



and it emphasises the fact that **multiplication is independent of the representatives chosen in the fiber**.

The concept of picking any representative element in the fiber, or reducing it mod K (since if you know one element in the fiber, every other element can be obtained by multiplying it with each element in the kernel) is the same as what is done in $\mathbb{Z}/n\mathbb{Z}$. As in $\mathbb{Z}/n\mathbb{Z}$, we can denote the fiber containing u (or the coset uK or Ku, they are the same) as $\bar{u}$, and the quotient group G/K itself as $\bar{G}$. Also, the cosets uK in G/K are **elements** $\bar{u}$ in G/K

Example

The first example in this section, the homomorphism from $\mathbb{Z} \to Z_n$ has fibers equivalent to the left cosets $a + n\mathbb{Z}$ of the kernel $n\mathbb{Z}$. (Also right cosets). Theorem 4.6 specifies that the cosets form a group under addition of representatives, which are $\mathbb{Z}/n\mathbb{Z}$, which is consistent with the notation G/K for quotient groups. This group is also isomorphic to its image under φ, so we get the known fact that $\mathbb{Z}/n\mathbb{Z} \cong Z_n$.

Example

If φ is a **isomorphism**, then the kernel (and any other fibre too) must only have 1 element (bijective) and so that element must be 1, the identity of G. The group G/K becomes $G/1$, which is essentially G, and $G \cong G$.

Example

Let G be any group and let $H = 1$ be the group of order 1 and define $\varphi : G \to H$ by $\varphi(g) = 1$, for all $g \in G$. It is immediate that φ is a homomorphism, and this map is called the **trivial homomorphism**. In this case, $\ker \varphi = G$ and G/G is a singleton group with the element G

and $G/G \cong Z_1 = \{1\}$

By Theorem 4.6, if we are given a subgroup K of a group G which we know is the kernel of some homomorphism, we may define the quotient G/K without recourse to the homomorphism by the multiplication $(uK)(vK) = (uv)K$. This raises the question of whether it is possible to define the quotient group G/N similarly for any subgroup N of G. The answer is no in general since this multiplication is not in general well defined (a later Proposition). In fact we shall see that it is possible to define the structure of a group on the cosets of N if and only if N is the kernel of some homomorphism (another later Proposition). We shall also give a criterion to determine when a subgroup N is such a kernel - this is the notion of a normal subgroup and we shall consider non-normal subgroups in subsequent sections.

We'll start by showing that the cosets of an arbitrary subgroup of G partition G (i.e., their union is all of G and distinct cosets have trivial intersection).

Proposition 4.7: Partitioning of a Group by Cosets

Let N be any subgroup of the group G. The sets of left cosets of N in G form a partition of G. Furthermore, for all $u, v \in G$, $uN = vN$ if and only if $v^{-1}u \in N$ and in particular, $uN = vN$ if and only if u and v are representatives of the same coset.

Proof. Firstly, since N is a subgroup of G, $1 \in N$. Thus $g = g \cdot 1 = gN$ for all $g \in G$, i.e.,

$$G = \bigcup_{g \in G} gN$$

To show that distinct left cosets have empty intersection, suppose $uN \cup vN \neq \varnothing$. We try to show that $uN = vN$. Let $x = un = vm$ be a common element for some $n, m \in N$. Multiplying both sides by n^{-1} on the right gives $u = vmn^{-1} = vm_1$ where $m_1 = mn^{-1} \in N$
Now, for any element $uy \in uN$ ($y \in N$), $uy = (vm_1)y = v(m_1 y) \in vN$, which means $uN \subseteq vN$. Interchanging u and v gives you the reverse relation, namely $vN \subseteq uN$, which completes the proof. Thus two cosets with non-empty intersection coincide. □

The takeaway is that $uN = vN$ if and only if u and v are representatives of the same coset (which is $uN = vN$)

Proposition 4.8: Operations on Cosets

Let G be a group and let N be a subgroup of G.

1. *The operation on the set of left cosets of N in G described by*

$$uN \cdot vN = (uv)N$$

   is well defined if and only if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.
2. *If the operation is well defined, then it makes the set of left cosets of N in G into a group. In particular the identity of this group is the coset $1N$ and the inverse of gN is the coset $g^{-1}N$, i.e., $(gN)^{-1} = g^{-1}N$.*

Proof.
Assume first that this operation is well defined, i.e., for all $u, v \in G$,

$$\text{if} u, u_1 \in uN \text{ and } v, v_1 \in vN \qquad \text{then} \qquad uvN = u_1v_1N.$$

Let g be an arbitrary element of G and let n be an arbitrary element of N. Letting $u = 1$, $u_1 = n$ and $v = v_1 = g^{-1}$ and applying the assumption above we deduce that

$$1g^{-1}N = ng^{-1}N \quad \text{i.e.,} \quad g^{-1}N = ng^{-1}N.$$

Since $1 \in N, ng^{-1} \cdot 1 \in ng^{-1}N$, which implies $ng^{-1} \in g^{-1}N$, hence $ng^{-1} = g^{-1}n_1$, for some $n_1 \in N$, which directly leads to $gng^{-1} \in N$, as claimed.
To prove the converse, assume $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. Let $u, u_1 \in uN$ and $v, v_1 \in vN$. We can write $u_1 = un$ and $v_1 = vm$ for some $n, m \in N$.
We must prove that $u_1v_1 \in uvN$

$$\begin{aligned} u_1v_1 &= (un)(vm) = u(vv^{-1})nvm \\ &= (uv)(v^{-1}nv)m = (uv)(n_1m) \end{aligned}$$

where $n_1 = v^{-1}nv = v^{-1}n(v^{-1})^{-1}$ is an element of n by the initial assumption. N is also closed under products, so $n_1m \in N$. Therefore :

$$u_1v_1 = (uv)n_2 \qquad \text{for some } n_2 \in N$$

Thus the cosets uvN and u_1v_1N have a common element u_1v_1. By the previous proposition they are equal, and the operation is well defined.
For 2., it's easy to check the group axioms if the operation is well defined. I'll leave it as an exercise to check the associative law (fairly trivial), the identity in G/N is the coset $1N$ and the inverse of gN is $g^{-1}N$ □

These subgroups N for which the above proposition is satisfied (natural group structure on the quotient G/K) are given a name:

Definition 4.9: Normal Subgroups and Conjugates

The element gng^{-1} is called the **conjugate** of $n \in N$ by g. The set $gNg^{-1} = \left\{ gng^{-1} \mid n \in N \right\}$ is called the **conjugate** of N by g. The element g is said to **normalize** N if $gNg^{-1} = N$. A subgroup N of a group G is called **normal** if every element of G normalizes N, i.e., if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we shall write $N \trianglelefteq G$.

The structure of G is reflected in the structure of the quotient G/N when N is a normal subgroup (for example, the associativity of the multiplication and the inverses of G/N correlate to the associativity and inverses in G)

The following theorem is a summary of our results :

Theorem 4.10: Summary of Results

Let N be a subgroup of the group G. The following are equivalent:

1. $N \trianglelefteq G$
2. $N_G(N) = G$ *($N_G(N)$ is the normalizer in G of N)*
3. $gN = Ng$ *for all* $g \in G$
4. *The operation on left cosets of N in G described in the above Proposition makes the set of left cosets into a group*
5. $gNg^{-1} \subseteq N$ *for all* $g \in G$.

We now prove that the normal subgroups are precisely the same as the kernels of homomorphisms considered earlier.

Proposition 4.11: Kernels and Normal Subgroups

A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.

Proof. If N is the kernel of a homomorphism, then the left cosets of N are the same as right cosets of N, so by the previous Theorem, N is a normal subgroup.
Conversely, if $N \trianglelefteq G$, let $H = G/N$ and let $\varphi : G \to G/N$ by

$$\varphi(g) = gN \quad \text{for all} g \in G.$$

By definition of the operation in G/N,

$$\varphi(g_1g_2) = (g_1g_2)N = g_1Ng_2N = \varphi(g_1)\varphi(g_2).$$

This implies φ is a homomorphism. Also,

$$\begin{aligned}\ker\varphi &= \{\, g \in G \mid \varphi(g) = 1N \,\} \\ &= \{\, g \in G \mid gN = 1N \,\} \\ &= \{\, g \in G \mid g \in N \,\} = N.\end{aligned}$$

Thus N is the kernel of the homomorphism φ. □

This homomorphism φ (Let's call it π from now) is given a name:

Definition 4.12: Natural Projection

Let $N \trianglelefteq G$ The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called the **natural projection(homomorphism)** of G onto G/N. If $\bar{H} \leq G/N$ is a subgroup of G/N, the **complete preimage** of $\bar{H}$ in G is the preimage of $\bar{H}$ under the natural projection homomorphism.

So the preimage of a subgroup of a subgroup of G/N is a subgroup of G, which has to contain the subgroup N (lots of subgroups!) since the elements in N map to the identity $\bar{1} \in \bar{H}$. We shall see later that there is a natural correspondence between the subgroups of G that contain N and the subgroups of the quotient G/N.

However, the most important takeaway is the criteria for when a subgroup N of a given group G is the kernel of some homomorphism, i.e.,

$$N_G(N) = G$$

We may thus think of the normalizer of a subgroup N of G as being a measure of "how close" N is to being a normal subgroup (this explains the choice of name for this subgroup). Keep in mind that the property of being normal is an **embedding** property, that is, it depends on the relation of N to G, not on the internal structure of N itself (the same group N may be a normal subgroup of G but not be normal in a larger group containing G.

Needless to say, we've come a long way since normalizers were introduced (had to prove a lot of stuff) but now we get to know why they're useful.

As always, some examples : Let G be a group

Example

The subgroups 1 and G are always normal in G, with $G/1$ mapping to G and G/G mapping to 1 (Just like division?)

Example

Abelian groups are special, since for any subgroup N of an abelian group G, N is normal in G, since for all $g \in G$ and all $n \in N$,

$$gng^{-1} = gg^{-1}n = n \in N.$$

It's important for G to be abelian and not just N, since it must be true for all $g \in G$.
Suppose that $G = Z_k$ is the cyclic group of order k. Let x be a generator of G and let $N \leq G$. By Proposition 3.14, $N = \langle x^d \rangle$, where d is the smallest power of x such that x^d lies in N. Then

$$G/N = \{ gN \mid g \in G \} = \{ x^\alpha N \mid \alpha \in \mathbb{Z} \}$$

and since $x^\alpha N = (xN)^\alpha$ (quite straightforward to prove, I'll prove it below)

$$G/N = \langle xN \rangle \quad \text{i.e.,} G/N \text{ is cyclic with } xN \text{ as a generator.}$$

One can show that the order of xN in G/N is d. Also, $d = \frac{|G|}{|N|}$
Summarising :

quotient groups of a cyclic group are cyclic

and the image of a generator g for G is a generator $\bar{g}$ for the quotient. If in addition G is a **finite** cyclic group and $N \leq G$, then $|G/N| = \frac{|G|}{|N|}$ is the order of the quotient group.

Example

If $N \leq Z(G)$, then $N \trianglelefteq G$ because for all $g \in G$ and all $n \in N$, $gng^{-1} = n \in N$. Hence, $Z(G) \trianglelefteq G$.

Some problems :

Problem 4.1 Prove that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

Solution We have that for any elements $u, v \in G$, $(uN)(vN) = (uv)N$,

therefore,

$$\begin{aligned} g^\alpha N = (g \cdot g^{\alpha-1})N &= (gN)(g^{\alpha-1}N) \\ &= (gN)(gN)(g^{\alpha-2}N) = (gN)^2(g^{\alpha-2}N)\dots \\ &= (gN)^\alpha \end{aligned}$$

Problem 4.2 Use the preceding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $gN \in N$ (and gN has infinite order if no such positive integer exists).

Solution We know that the coset $1N = N$ is the kernel for the quotient group, or more appropriately, the identity of the group. So the problem reduces to finding the smallest power a such that $(gN)^a = 1N = n_1N$ for any $n \in N$ (since any representative of the group $\bar{1} = N$ is fine.

From the previous problem , $(gN)^a = g^aN$, so we need to find the smallest a such that $g^a \in N$, which, by the question, is n.

4.1 Lagrange's Theorem

Lagrange's Theorem is one of the most important combinatorial results in finite group theory. Let's dive in!

Theorem 4.13: Lagrange's Theorem

If G is a finite group and H is a subgroup of G, then the order of H divides the order of G and the number of left cosets of H in G equals $\frac{|G|}{|H|}$

Proof. Let $|H| = n$ and let the number of left cosets of H in G be k. By an earlier proposition, the set of left cosets of H in G partition G. Also, by definition, the map : $H \to gH$ defined by $h \mapsto gh$ is a surjection from H to the left coset gH.
The left cancellation law implies that the map is injective, since $gh_1 = gh_2 \implies h_1 = h_2$. Therefore, H and gH have the same order n.
Since G is partitioned into k disjoint subsets, each of which has cardinality n, $|G| = kn$. Thus, $k = \frac{|G|}{n} = \frac{|G|}{|H|}$, and hence proved. □

Corollary 4.13.1 If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular $x^{|G|} = 1$ for all $x \in G$.

Proof. Using the fact that $|x| = |\langle x \rangle|$ and applying Lagrange's Theorem on $H = \langle x \rangle$, we get the first part. The second part follows since $|x|$ divides $|G|$ □

Corollary 4.13.2 If G is a group of prime order p, then G is cyclic and $G \cong Z_p$.

Proof. Let $x \in G$, $x \neq 1$, so $|\langle x \rangle| > 1$ and $|\langle x \rangle|$ divides $|G|$. Since $|G|$ is prime we must have $|\langle x \rangle| = |G|$, hence $G = \langle x \rangle$ is cyclic (if the generator isn't the identity element). □

Definition 4.14: Index of a Coset of a Group

If G is a group (maybe infinite) and $H \leq G$, then the number of left cosets of H in G is called the **index** of H in G and is denoted by $|G : H|$.

In the case of finite groups the index of H in G is $\frac{|G|}{|H|}$. For infinite groups there are subgroups of finite or infinite index.

Example

Let $H = \langle (1\,2\,3) \rangle \leq S_3$ and let $G = S_3$. We show that $H \trianglelefteq S_3$. Since H is a cyclic group, we have

$$H \leq N_G(H) \leq G$$

. Which means the order of H divides that or $N_G(H)$, which divides that of G. So we have only two possibilities for $N_G(H)$, either having order 3 (H) or order 6 (G).
Let's try to prove that it isn't H. Taking an element in G, let's say (1 2), let's see if it lies in the normalizer of H. The elements of H are (1,2,3), (1,3,2) and 1, the identity. The inverse of (1 2) in G is simply (1 2) itself, since it has order 2.
Performing the computations gHg^{-1}, we see that (1 2 3) gets mapped to (1 3 2) and vice versa, while 1 gets mapped to 1. Therefore, (1 2) $\in N_G(H)$ and therefore $N_G(H)$ cannot be H itself, therefore, it must be G.
Since $N_G(H) = G$, by Theorem 4.10, $H \trianglelefteq G$.

Example

Let G be any group containing a subgroup H of index 2. We prove $H \trianglelefteq G$. Let $g \in G \setminus H$, so the two left cosets have to be the identity $1H$ and the coset gH. Since the cosets partition G and the coset H exists, $gH = G \setminus H$. The same logic applies for the right cosets, so $Hg = G \setminus H$, which means that $gH = Hg$ for all $g \in G \setminus H$ and for $g \in H$, the equality is trivial, therefore, $gH = Hg$ for all $g \in G$, and by Theorem 4.10, we have that $H \trianglelefteq G$.
This results proves that $\langle -1 \rangle$ is a normal subgroup of $\mathbb{Z}$ and $\langle i \rangle, \langle j \rangle, \langle k \rangle$ are all normal subgroups of Q_8.

Remark

The property "is a normal subgroup of " is **not transitive**. An example :

$$\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$$

(each subgroup is of index 2 in the next) but $\langle s \rangle$ is not normal in D_8 since $rsr^{-1} = sr^2 \notin \langle s \rangle$

There are groups G where the only normal subgroups are the trivial ones, 1 and G. The search for normal subgroups of a given group is generally very non-trivial and difficult.

The **full converse** to Lagrange's Theorem is **not** true, so if G is a finite group and n divides $|G|$, then G need not have a subgroup of order n.

There are some partial converses though, for example, finite **abelian** groups show the full converse of Lagrange's Theorem. Also, there is this theorem :

Theorem 4.15: Cauchy's Theorem

If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

The strongest converse to Lagrange's Theorem which applies to **arbitrary** finite groups is the following:

Theorem 4.16: Sylow's Theorem

If G is a finite group of order $p^\alpha m$, where p is a prime and p does not divide m, then G has a subgroup of order p^α.

Let's conclude with some results involving cosets

Proposition 4.17: Orders of Unions and Intersections

If H and K are finite subgroups of a group and define

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

Then

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

Proof. HK is actually a union of left cosets of K, i.e.,

$$HK = \bigcup_{h \in H} hK.$$

Since each coset of K has $|K|$ elements we need to find the number of **distinct** left cosets of the form $hK, h \in H$. However, we know $h_1K = h_2K$ for $h_1, h_2 \in H$, if and only if $h_2^{-1}h_1 \in K$.
We can use this smartly to figure out that $h_2^{-1}h_1 \in H \cap K$ and therefore, this can happen if and only if $h_1(H \cap K) = h_2(H \cap K)$.
Thus the problem reduces to finding the number of distinct cosets $h(H \cap K), h \in H$. Now we can apply Lagrange's Theorem since $H \cap K$ is a subgroup of H. Therefore, HK consists of $\frac{|H|}{|H \cap K|}$ distinct cosets of K, which each have $|K|$ elements, justifying the formula. □

Remark

In the above proof, there was no assumption that HK be a subgroup. There are cases where HK cannot be a subgroup, and it can be shown by finding it's order and if it isn't a factor of the order of the group, by the contrapositive of Lagrange's Theorem, it cannot be a subgroup.

Proposition 4.18: More Properties

If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.

The proof of the above can just be done using The Subgroup Criterion.

Remark

$HK = KH$ doesn't imply that each element of H commutes with each element of K. It just means that every product hk, $h \in H, k \in K$ can be written as k_1h_1, $h \in H, k \in K$.

Corollary 4.18.1 If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.

Proof. By the previous proposition, we try to prove $HK = KH$. We know that $hkh^{-1} \in K$, so

$$hk = (hkh^{-1})h \in KH$$

which proves $HK \subseteq KH$. $kh = h(h^{-1}kh) \in HK$, proving the reverse containment. Thus since $HK = KH, HK$ is a subgroup of G. □

Remark

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

So the previous Corollary says that HK **is a subgroup if** H **normalizes** K.

In this discussion, we've only talked about left cosets of a subgroup. We could have talked only about right cosets as well, although they aren't necessarily the same as the left cosets.

Lagrange's Theorem gives that in a finite group G

the number of right cosets of the subgroup H **is** $\frac{|G|}{|H|}$

So in a finite group the **number** of left cosets of H in G is equal to the **number** of right cosets, even though the left cosets are not right cosets in general. So for purely combinatorial purposes one may use either left or right cosets (but not a mixture when a partition of G is needed).

4.2 Isomorphism Theorems

I'm just going to list some consequences of the relations between quotient groups and homomorphisms.

Theorem 4.19: The First Isomorphism Theorem

If $\varphi : G \to H$ is a homomorphism of groups, then $\ker \varphi \trianglelefteq G$ and $G/\ker\varphi \cong \varphi(G)$.

Corollary 4.19.1 Let $\varphi : G \to H$ is a homomorphism of groups.

1. φ is injective if and only if $\ker\varphi = 1$.
2. $|G : \ker\varphi| = |\varphi(G)|$.

Theorem 4.20: The Second or Diamond Isomorphism Theorem

Let G be a group and let A and B be subgroups of G and assume $A \leq N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \equiv A/A \cap B$

Theorem 4.21: The Third Isomorphism Theorem

Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and

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

Theorem 4.22: The Fourth of Lattice Isomorphism Theorem

Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\bar{A} = A/N$ of G/N. In particular, every subgroup of $\bar{G}$ is of the form A/N for some subgroup A of G containing N (namely, its pre-image in G under the natural projection homomorphism from G to G/N). This bijection has the following properties : for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

1. *$A \leq B$ if and only if $\bar{A} \leq \bar{B}$,*
2. *if $A \leq B$ then $|B : A| = |\bar{B} : \bar{A}|$*
3. *$\langle \bar{A}, \bar{B} \rangle = \langle \bar{A}, \bar{B} \rangle$*
4. *$A \cap B = \bar{A} \cap \bar{B}$*
5. *$A \trianglelefteq G$ if and only if $\bar{A} \trianglelefteq \bar{G}$*

Finally, to conclude, we look closer into the definition of homomorphisms on quotient group, specifically, **"the well-definedness"** of the map φ on the quotient group G/N, since the homomorphism was itself specified by giving the value of φ on the coset gN in terms of the representative g alone. We had to prove that φ was well defined (was independent of the choice of the representative g).

So basically, we are defining a homomorphism Φ on G itself by specifying the value of φ on g. This is directly linked to the fact that Φ must be trivial on N, so that

φ is well defined on G/N if and only if $N \leq \ker \Phi$

This gives a simple criterion for defining homomorphisms on quotients (namely, define a homomorphism on G and check that N is contained in its kernel). In this situation we shall say the homomorphism Φ factors through N and Φ is the induced homomorphism on G/N.

Acknowledgements

I'd like to thank my mentor, Aryaman Maithani, for mentoring me through this "course" (half-course, to be specific) and for the questions related to the reading material that he posed to me, I've really broken my head on some of the questions (still haven't gotten some of them). I'd also thank him for the LaTeX knowledge he's imparted to me, and all the other cool modifications such as the colouring, etc.