Group Theory

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

May 2022

Contents

0 Preliminaries

0.1 Basics and Notations (and to ~~test~~ develop my LaTeX math knowledge)

- The order or cardinality of a set A is denoted by $|A|$.
- A subset of a set A is represented as
  $B = \{\, a \in A \mid \ldots \text{ (conditions on } a\text{) } \ldots \}$

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

Definition 0.2. 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 0.3. 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 0.4. 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 0.5. 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 0.1. 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 0.2. *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 $A_i, i \in I$.*

0.2 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

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

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

0.3 $\mathbb{Z}/n\mathbb{Z}$: 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 $a \equiv b(modn)$ (Congruence) if $a \sim b$.

Definition 0.6. 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 0.3. $(\mathbb{Z}/n\mathbb{Z})^\times = \{\, \overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a,n) = 1 \,\}$.

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 $\mathbb{Z}/n\mathbb{Z}$.

1 Introduction to Groups

1.1 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 1.1. 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 1.2. 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 1.3. 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 1.4. 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 1.5. 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 1.4 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 0.6)

  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 :

[1] Beyond the scope of this paper

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

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.

Proposition 1.1. *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 1.4, $a \star b = a$ 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}.
5.

□

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 1.2. *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 1.6. 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 infnite 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 1.7. 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 $g_i g_j$

1.2 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
$$D_{2n} = \{ 1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1} \}$$
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 $n = 10$,

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

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 1.8 (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 1.9 (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.

1.3 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 *symmetric 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

[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

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 :

- 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.*

1.4 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 1.10 (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 :

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

Definition 1.11. 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 $|GL_n(F)| = (q^n-1)(q^n-q)(q^n-q^2)(q^n-q^3)\dots(q^n-q^{n-1})$.

1.5 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.

1.6 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 1.12. 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 1.13. 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 1.14. *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 properties. 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 $G \cong H$.

1.7 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 1.15. 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 0.1

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.

Based on the above example, if G acts on a set A such that distinct elements of G induce distinct permutations of A, the action is called *faithful*. This also means that the associated permutation representation is injective.

Definition 1.16 (Kernel)**.** The *kernel* of the action of G on B is defined to be $\{ g \in G \mid gb = b \text{ for all } b \in B \}$, 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* :

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

2 Subgroups

2.1 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 2.1 (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).

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 2.1 (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. □

2.2 Centralizers, Normalizers, Stabilizers and Kernels

Let A be a non-empty subset of G.

Definition 2.2 (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 2.3 (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 2.4 (Normalizer)**.** Define $gAg^{-1} = \left\{ gag^{-1} \mid a \in A \right\}$. Define the *normalizer* of A to be the set $N_G(A) = \left\{ g \in G \mid gAg^{-1} = A \right\}$.

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 $gbg^{-1} \neq b$.

Modified PoA

So far, I haven't even come close to reaching my original PoA, which was to do upto Chapter 4, I've since realised that it isn't a realistic target for me, given the arrival on campus and all the tests, quizzes and *procrastination* I do, so my modified PoA is to stop with Section 2.2 for my midterm report, and do until Chapter 4 (and even chapter 5 if time permits) for the endsem report. I will have time after my endsems, so that is when I'll be picking up.

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 LaTeXknowledge he's imparted to me, and all the other cool modifications such as the colouring, etc.