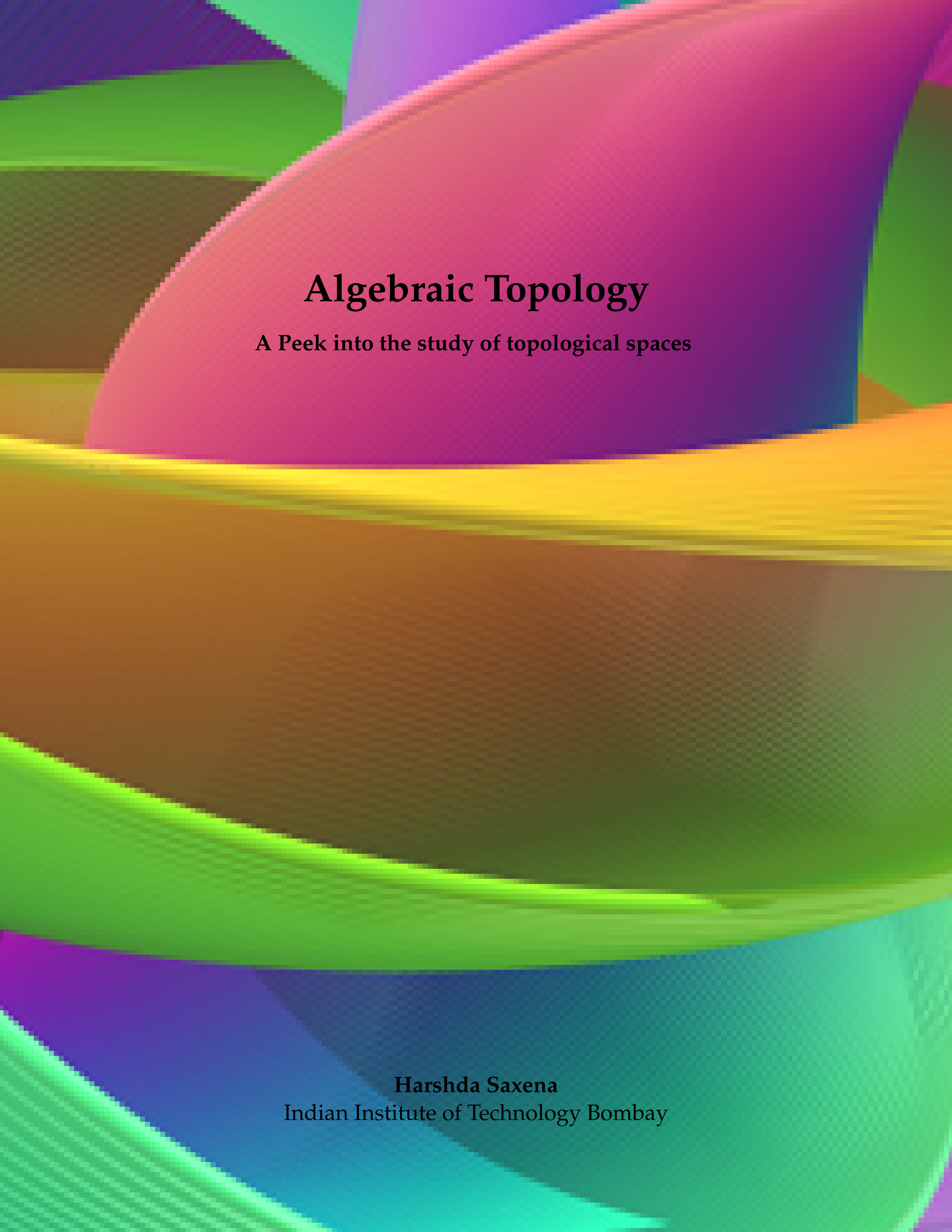

Algebraic Topology

A Peek into the study of topological spaces

Harshda Saxena
Indian Institute of Technology Bombay

Contents

§1. Preliminaries

§§1.1. Basics of sets and functions

Subsets of a set are denoted by $B = \{a \in A|(\text{conditions})\}$, cardinality of a set by $|A|$ and cartesian product of 2 sets as $A \times B = \{(a, b)|a \in A, b \in B\}$. A function from A to B is denoted as $f : A \to B$ where A is domain of f and B is codomain. $f : a \mapsto b$ indicates that $f(a) = b$.
Range or Image of A under f defined as -

$$f(A) = \{b \in B \,|\, b = f(a), \text{for some a} \in A\}$$

Preimage or inverse image of C under f defined as -

$$f^{-1}(C) = \{a \in A \,|\, f(a) \in C\}$$

For each $\{b\} \in B$, the preimage of {b} under f is called fibers of f over b (can contain one or more elements). If $f : A \mapsto B$ and $g : B \mapsto C$ then the composite map $g \circ f : A \mapsto C$ is defined as $(g \circ f)(a) = g(f(a))$. A function f is injective if whenever $a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$, surjective if for all $b \in B$, there is some $a \in A$ such that $f(a) = b$, and is bijective if it is both injective and surjective. A left inverse of $f : A \mapsto B$ is a function $g : B \mapsto A$ such that $g \circ f : A \mapsto A$ is the identity map, and a similar definiton for the right inverse. Important proofs considering $f : A \to B$

- f is injective if and only if f has left inverse
- f is surjective if and only if f has a right inverse
- f is a bijection iff there is a $g : B \mapsto A$ such that $f \circ g$ and $g \circ f$ are the identity maps on their respective domains (the map here is unique)
- if A and B have same cardinality, then f is bijective if and only if f is injective if and only if f is surjective

A permutation of set A is a bijection from A to itself. $f|_A$ is used to denote a restriction on domain A, if defined over a superset of A, and if $f|_A = g$, then f is an extention of g. For a non empty set A -

- A binary relation on set A is written as a $a \sim b$ if (a,b)$\in A \times A$
- A relation is an equivalence relation if it is reflexive, symmetric and transitive
- Equivalence class of some $a \in A$ is $\{x \in A|x \sim a\}$, elements of this set are equivalent to a and any one element of this class is called its representative
- A partition is any collection such that $A = \cup_i A_i$ and $A_i \cap A_j = \emptyset$ for all $i \neq j$ and in the indexing set.

Hence, for an equivalence relation on A, the set of all equivalence classes of A forms a partition of A and conversely, given a partition of A we can define an equivalence relation on A with the same equivalence classes as given.

§§1.2. Properties of Integers

There exists a minimal element in a non empty subset of $\mathbb{Z}^+$ (well-ordering property of $\mathbb{Z}$). If a, b $\in \mathbb{Z}$ with a $\neq 0$, a divides b if there is an element $c \in \mathbb{Z}$ such that $b = ac$ and is written by $a|b$. If

$a, b \in \mathbb{Z}/0$, there is a unique positive integer d (greatest common divisor of a and b) satisfying: (a) $d|a$ and $d|b$ and (b) if $e|a$ and $e|b$, then $e|d$. The gcd of a and b will be denoted by (a, b). If $(a, b) = 1$, we say that a and b are relatively prime.
If $a, b \in \mathbb{Z} - 0$, there is a unique positive integer l, called the least common multiple of a and b (or l.c.m. of a and b), satisfying: (a) $a|l$ and $b|1$ (sol is a common multiple of a and b), and (b) if $a|m$ and $b|m$, then $I|m$ (so I is the least such multiple). For all integers, $dl = ab$.
The Division Algorithm states that if $a, b \in \mathbb{Z} - 0$, then there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$ where q is the quotient and r the remainder.
The **Eucledian Algorithm** produces the greatest common divisor of two integers a and b by iterating the Division Algorithm, from $a = q_0 + b$, $b = q_1 r_0 + r_1$, till the last non zero remainder is found, which is (a,b).
The gcd of a and b is a $\mathbb{Z}$-linear combination of a and b. That is $(a, b) = ax + by$, where $x, y \in \mathbb{Z}$, and are not unique.
An element p of $\mathbb{Z}^+$ is called a prime if $p > 1$ and the only positive divisors of p are 1 and p. An integer $n > 1$ which is not prime is called composite. If p is a prime and $p|ab$, for some $a, b \in \mathbb{Z}$, then either $p|a$ or $p|b$. The Fundamental Theorem of Arithmetic says: if $n \in \mathbb{Z}$, $n > 1$, the n can be factored uniquely into the product of primes. The GCD of 2 numbers is the min of each prime exponent in both expressions, and LCM as the maximum.
The Euler φ function is defined as follows: for $n \in \mathbb{Z}^+$ let $\varphi(n)$ be the number of positive integers $a < n$ with a relatively prime to n, i.e. $(a, n) = 1$. For primes we have $\varphi(p^a) = p^a - p^{a-1}$ and under multiplication as $\varphi(ab) = \varphi(a)\varphi(b)$ if $(a, b) = 1$. Together with the formula above this gives a general formula for the values of $\varphi(n) : n = \prod p_i^{\alpha_i}$ then $\varphi(n) = \prod p_i^{\alpha_i - 1}(p_i - 1)$.

§§1.3. $\mathbb{Z}/n\mathbb{Z}$

We define a relation on $\mathbb{Z}$ as $a \sim b$ iff $n|(b - a)$. We can see that this relation is an equivalence relation. For any $k \in \mathbb{Z}$ we shall denote the equivalence class of a by $\overline{a}$, also called the congruence class or residue class of $a \pmod{n}$, consisting of the integers which differ from a by an integral multiple of n, ie $\overline{a} = \{a + kn | k \in \mathbb{Z}\}$. For $a \pmod{n}$ this has n distinguishable classes. The set of equivalence classes under the equivalence relation is denoted by $\mathbb{Z}/n\mathbb{Z}$. We define addition and multiplication of this to follow the modular arithmetic as $\overline{a + b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a} \cdot \overline{b}$. These operations are well defined and hence do not depend on the choice of representatives taken. An important subset of $\mathbb{Z}/n\mathbb{Z}$ consists of the residue classes which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} | \text{ there exists } \overline{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \overline{a} \cdot \overline{c} = \overline{1}\} \tag{1.1}$$

It is also the collection of residue classes whose representatives are relatively prime to n. If a is an integer relatively prime to n then the Euclidean Algorithm produces integers x and y satisfying $ax + ny = 1$, hence $ax \equiv 1 \pmod{n}$, so that $\overline{x}$ is the multiplicative inverse of $\overline{a}$.

§2. Groups - The basics

§§2.1. Basic Axioms

Definition 2.1. A **binary operation** $\star$ on a set G is a function $\star : G \times G \mapsto G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$.

This is associative if for all $a, b, c \in G$ $a \star (b \star c) = (a \star b) \star c$ and commutative if $a \star b = b \star a$ for all $a, b \in G$. Suppose that $\star$ is a binary operation on a set G and H is a subset of G. If the restriction of $\star$ to H is a binary operation on H, i.e., for all $a, b \in H, a \star b \in H$, then H is said to be closed under $\star$.

Definition 2.2. A **group** is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:

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

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

For $n \in \mathbb{Z}^+$, $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the operation of addition of residue classes (with identity as $\overline{0}$ and inverse as $\overline{-a}$), and $n \in \mathbb{Z}^+$, $(\mathbb{Z}/n\mathbb{Z})^\times$ is an abelian group under multiplication of residue classes (with identity as $\overline{1}$, and inverse as defined above). If $(A, \star)$ and $(B, \diamond)$ are groups, we form $A \times B = \{(a, b) | a \in A, b \in B\}$ with component-wise operation as $(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2)$.

Theorem 2.3. If G is a group under $\star$, then -

- the identity of G is unique
- for each $a \in G, a^{-1}$ is unique
- $(a^{-1})^{-1} = a \quad \forall a \in G$
- $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$
- For any $a_1, a_2 \ldots a_n \in G$ the value of $a_1 \star a_2 \ldots \star a_n$ is independent of bracketing.

For ease of writing, we can ignore the operation $\star$ between two elements and simply write them as ab, with the group operation as $\cdot$, identity as 1, and a^{-1} as the inverse.
For a group G and $a, b \in G$, $ax = b$ and $ya = b$ have unique solutions as $a^{-1}b$ and ba^{-1} and similarly, the left and right cancellation laws hold.

Definition 2.4. For a group G and $x \in G$ define the order of x to be the smallest positive integer n such that $x^n = 1$, and denote this integer by $|x|$. If no positive power of x is the identity, the order of x is defined to be infinity. For a group however, order n implies that the cardinality of the group is n.

If $G = \{g_1, g_2, \ldots, g_n\}$ is a finite group with $g_1 = 1$, then multiplication/group table of G is the $n \times n$ matrix with g_{ij} as the i, j entry.

§§2.2. Dihedral Groups

For each $n \in \mathbb{Z}^+, n \geq 3$, let D_{2n} be the set of symmetries of a regular n-gon. Each symmetry s can be described uniquely by the corresponding permutation σ of $\{1, \ldots, n\}$ where if the symmetry s puts vertex i in the place where vertex j was originally, then σ is the permutation sending i to j. Now we see that we can make D_{2n} into a group by defining st for $s, t \in D_{2n}$ to be the symmetry obtained by first applying t then s to the n-gon. The binary operation on D_{2n} is associative since composition of functions is associative. The identity of D_{2n} is the identity symmetry, and the inverse of $s \in D_{2n}$ is the symmetry which reverses all motions of s.
We can show that $|D_{2n}| = 2n$, and is called the dihedral group of order $2n$ (Any adjacent pair of vertices can can end up in $n * 2$ positions, and once ordered pair determined, due to the rigidity of motion all other vertices are fixed). These are seen as the n rotations about the centre by $\frac{2\pi}{n}$ radians (labelled as r, with $|r| = n$), and n reflections about the lines of symmetry (labelled as s, with $|s| = 2$). The group can be shown to be represented as -

Definition 2.5. $D_{2n} = \{1, r, \ldots r^{n-1}, s, sr, \ldots, sr^{n-1}\}$, and having the property $r^i s = sr^{-i}$.

Definition 2.6. 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, writing it as $G = \langle S \rangle$.
Any equations in a general group G that the generators that is, from $S \cup \{1\}$ satisfy are called relations in G.

In general, if a group G is generated by a subset S and there is some collection of relations, say $R_1, R_2, \ldots, R_m$ such that any relation among the elements of S can be deduced from these, we call these generators and relations a presentation of G and write -

$$G = \langle s, R_1, R_2, \ldots, R_m \rangle$$

§§2.3. Symmetric groups

Theorem 2.7. For any non-empty Ω let S_Ω be the set of all bijections from Ω to itself, and is a group under function composition: $\circ$.

Proof. We can see this by noting that $\circ$ is a binary operation since if σ and τ are bijections, then so is the composition, associative is trivial, the identity is the identity map permutation, and the inverse satisfies $\sigma^{-1} \circ \sigma = 1$. This group is called the symmetric group on the set Ω. □

When Ω is the natural numbers till n, the symmetric group of degree n is called S_n. The order of S_n is $n!$.

We express the notation for writing elements of S_n with something known as cycle decomposition. The cycle $(a_1, a_2, \ldots, a_m)$ is the permutation which sends $a_i \mapsto a_{i+1}$ for $1 \leq i \leq m-1$ and sends $a_m \mapsto a_1$. We can generally group it into k cycles. For any $x \in \sigma$, find the immediate right neighbour, which is $\sigma(x)$, if there is no element to the right, cycle back to the start element. The product of all the cycles is called the cycle decomposition of σ. In general, we pick the smallest element to start a cycle which hasn't been picked yet, call it a. Read $\sigma(a)$, call it b, if it is a, it is the complete cycle. Similarly read off $\sigma(b)$. The length of a cycle is the number of integers which appear in it. Two cycles are called disjoint if they have no numbers in common.

We can also easily see that S_n is a non abelian group. Since disjoint cycles permute numbers which lie in disjoint sets it follows that disjoint cycles commute. The cycle decomposition of each permutation is the unique way of expressing a permutation as a product of disjoint cycles (up to rearranging its cycles and cyclically permuting the numbers within each cycle). We can also prove that the order of a permutation is the lcm of the lengths of the cycles in its cycle decomposition. The order of σ is n iff $\sigma^n(a_k) = a_k$ for all a_k in the cycle decomposition.

§§2.4. Matrix Groups

Definition 2.8. A field is a set F with binary operations $+$ and $\cdot$, on F such that $(F, +)$ is an abelian group (call its identity 0) and $(F - 0, \cdot)$ is also an abelian group, and the following distributive law holds: $a \cdot (b + c) = a \cdot b + a \cdot c$, for all $a, b, c \in F$.

Examples include $\mathbb{Q}, \mathbb{R}, \mathbb{Z}/p\mathbb{Z}$, with p prime.

For each $n \in \mathbb{Z}^+$, let $GL_n(F) = \{A |$ A is a $n \times n$ matrix with entries from F and $det(A) \neq 0\}$. Since matrix multiplication is associative, if $det(A) \neq 0$ and $det(B) \neq 0 \implies det(AB) \neq 0$, $det(A) \neq 0$ implies A^{-1} exists for each A such that $AA^{-1} = I$, the identity, making $GL_n(F)$ a group, called the general linear group of degree n .

§§2.5. Quarternion Group

$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, over $\cdot$ as 1 as the identity element, -1 reversing the sign of any element, $i \cdot i = j \cdot j = k \cdot k = -1$, and ij and other elements similar to the cross-product (hence, is also non-abelian).

§§2.6. Homomorphisms (no homo) and Isomorphisms

Definition 2.9. Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\varphi : G \mapsto H$ such that $\varphi(x \star y) = \varphi(x) \diamond \varphi(y)$ for all $x, y \in$ G is called a homomorphism.

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

Definition 2.10. A map $\varphi : G \mapsto H$ is called an isomorphism and G and H are said to be isomorphic ($G \cong H$) if -

- φ is a homomorphism
- φ is a bijection

Intuitively, G and H are the same group except that the elements and the operations may be written differently in G and H.

Theorem 2.11. If $\varphi : G \mapsto H$ is an isomorphism -

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

Let $\mathcal{G}$ be a nonempty collection of groups. Here, the relation $\cong$ is an 1equivalence relation on $\mathcal{G}$ and the equivalence classes are called isomorphism classes. Up to isomorphism there are precisely two groups of order 6: S_3 and $\mathbb{Z}/6\mathbb{Z}$. If G and H are 2 finite groups with the generators $S = \{s_1, \ldots, s_m\}$ and $R = \{r_1, \ldots, r_m\}$ be the generators with all all relations satisfied by r_i also be satisfied by s_i. Then there is a unique homomorphism $\varphi : G \to H$ mapping $s_i\ to\ r_i$, and if the order of G is same as H, then φ is an isomorphism.

§§2.7. Group Actions

Definition 2.12. A group action of a group G on a set A is a map from $G \times A$ to A, as $g \cdot a$ for all $g \in G$ and $a \in A$, satisfying -

- $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$. Note here that on LHS $g_2 \cdot a$ is a member of A, but on the RHS $g_1 g_2$ is a member of G.
- $1 \cdot a = a$ for all $a \in A$.

Theorem 2.13. Let G act on A. For each $g \in G$ define $\sigma_g : A \to A$ with the left action as $\sigma_g(a) = g \cdot a$. We now claim that ;

- for each fixed $g \in G$, σ_g is a permutation of A, since it is injective and maps A to A, hence being bijective and a permutation
- $\varphi : G \to S_A$ as $g \mapsto \sigma_g$ is a homomorphism by noting that $\varphi(g_1 g_2)(a) = \sigma_{g_1 g_2} = (g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = \sigma_{g_1}(\sigma_{g_1}(a)) = (\varphi(g_1) \circ \varphi(g_2))(a)$

The homomorphism φ is called the permutation representation associated to the given action. Thus actions of a group G on a set A and the homomorphisms from G into the symmetric group S_A are in bijective correspondence. If $ga = a\ \forall g \in G, a \in A$, it is called the trivial action, and the permutation representation is the trivial homomorphism which maps every element of G to the identity on S_A.

If G acts on A, and distinct elements of G induce district permutations of A, then the action is called faithful. A faithful action is therefore one in which the associated permutation representation is injective. The kernel of the action is $\{g \in G | gb = b \quad \forall b \in B\}$. For any group F and $A = G$, the left regular action of G on itself is defined as $g \cdot a = ga$. A group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.

§3. Subgroups

Definition 3.1. For a group G, a subset H of G is a subgroup of G if H is nonempty and H is closed under products and inverses, that is for all $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$. If H is a subgroup of G we shall write $H \leq G$. If $H \neq G$ then we write $H < G$.

Some examples include $\mathbb{Z} \leq \mathbb{Q}, \mathbb{Q} \leq \mathbb{R}$. $H = \{1\}$ is the trivial subgroup. The relation is a subgroup of is transitive: if H is a subgroup of a group G and K is a subgroup of H, then K is also a subgroup of G.

Proposition 3.2. A subset H of group G is a subgroup iff:

- $H \neq \emptyset$
- for all $x, y \in H$, $xy^{-1} \in H$

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Proof. We can prove this by seeing that the if condition is by definition, and the only if condition by ensuring that $1(x = y)$, for every z in $H(x = 1, y = z)$, z^{-1} is in H, and for all u and v in H, $x = u, y = v^{-1}$, uv is in H. Hence H is a subgroup. If H is finite and closed under multiplcation, then $x^{n-1} = x^{-1}$ is an element of H, and hence is closed under inverses. □

If H and K be subgroups of G. Then $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$. However, $H \cap K$ is a subgroup of G, and so is an arbitrary intersection of subgroups of G.

§§3.1. Centralizers, Normalizers, Stabilizers and kernels

Definition 3.3. $C_G(A) = \{g \in G | gag^{-1} = a \quad \forall a \in A\}$ called the centralizer of A in G. It is also the set of elements of G which commute with every element of A.

It is a subgroup of G since the identity belongs to it, and if $x \in C_G(A)$, then x^{-1} also commutes with all elements of G, and finally if x and y commute with all elements of A, then so does xy. Hence $C_G(A) \leq G$.

Definition 3.4. Define $Z(G) = \{g \in G | gx = xg \quad \forall x \in G\}$, is the set of elements commuting with all elements of G. It is called the centre of G and $Z(G) = C_G(G)$, hence $Z(G) \leq G$.

Definition 3.5. Let $gAg^{-1} = \{gag^{-1} | \ a \in A\}$. The normalizer of A in G is $N_G(A) = \{g \in G | \ gAg^{-1} = A\}$, and that $C_G(A) \leq N_G(A)$, and $N_G(A) \leq G$.
For an abelian group $C_G(A) = N_G(A)$ for any subset A of G, and $Z(G) = G$

Definition 3.6. If G is a group acting on a set S, fix some element s of S, then the stabilizer of s in G is $G_s = \{g \in G | g \cdot s = s\}$. We can see by the axioms of group action that $G_s \leq G$.

Definition 3.7. Define the kernel of an action of G on S as $\{g \in G | \ g \cdot s = s \forall s \in S\}$, and we can see that the kernel is a subgroup of G.

Theorem 3.8. Lagranges Theorem : if G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

§§3.2. Cyclic groups and subgroups

Definition 3.9. 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 $H = \{x^n | \ n \in \mathbb{Z}\}$. We say that H is generated by x, and write $H = \langle x \rangle$ (also implies $H = \langle x^{-1} \rangle$.

For example, if $G = D_{2n}$, H is the subgroup of all rotations, then $H = \langle r \rangle$. If $H = \mathbb{Z}$, then $H = \langle 1 \rangle$. We state a bunch of propositions here, the proofs of which are trivial.

Proposition 3.10. If $H = \langle x \rangle$, then $|H| = |x|$, where if one side of this equality is infinite, so is the other.

Proposition 3.11. Let G be an arbitrary group, and x is in G. Let $m, n \in \mathbb{Z}$. If $x^n = x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particular, if $x^m = 1$ for some integer m, then $|x|$ divides m .

The proof just follows the Euclid Division Algorithm.

Theorem 3.12.

- if $n \in \mathbb{Z}^+$, and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then $x^k \mapsto y^k$ is well defined and an isomorphism
- if $\langle x \rangle$ is a infinite cyclic group, then $k \mapsto x^k$ is well defined and an isomorphism

where well defined follows from the above proposition, and the law of exponents make sure that the map is a homomorphism, and since the 2 groups have the same order and the map is surjective, bijectivity and hence the 2 groups being isomorphic follows.

Proposition 3.13. For a group G, $z \in G$ and $a \in \mathbb{Z} - \{0\}$,

- If $|x| = \infty$, then $|x^a| = \infty$
- If $|x| = n$, then $|x^a| = \frac{n}{(n,a)}$

- in particular to above, if a divides n, then $|x^a| = \frac{n}{a}$

In a similar manner as above, we state

Proposition 3.14. If $H = \langle x \rangle$,

- Assume $|x| = \infty$, then $H = \langle x^a \rangle$ iff $a = \pm 1$
- Assume $|x| = n$, then $H = \langle x^a \rangle$ iff $(a, n) = 1$. Hence, the number of generators of H is $\varphi(n)$

Hence, $\bar{a}$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $(a, n) = 1$. Finally, putting it all together, we get -

Theorem 3.15. Let $H = \langle x \rangle$ be a cyclic group

- Every subgroup of H is cyclic, then either $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$, where $K \leq H$
- If $|H| = \infty$, then for any distinct nonnegative integers a and b, $\langle x^a \rangle \neq \langle x^b \rangle$ and $\langle x^m \rangle \neq \langle x^{|m|} \rangle$
- If $|H| = n$, then for each positive integer a dividing n there is a unique n subgroup of H of order a, which is the cyclic group $\langle x^d \rangle$, where $d = n/a$, and $\langle x^m \rangle \neq \langle x^{(n,m)} \rangle$

§§3.3. Subgroups generated by a subset of a group

Proposition 3.16. 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

Proof. Let $K = \cap_{H \in \mathcal{A}} H$, we see that since each H is a subgroup, 1 is in each H and hence in K, and if a, b are in K, then it is in each H, and hence so is ab^{-1} in each H and hence in K, and $K \leq G$. □

Definition 3.17. If A is any subset of G define $\langle A \rangle = \cap H$ such that $A \subseteq H, H \leq G$, called the subgroup of G generated by A.

We can see that A is the unique minimal element of $\mathcal{A}$. We define the closure of A as follows -

Definition 3.18. $\bar{A} = \{a_1^{\epsilon_1} \dots a_n^{\epsilon_n} | n \in \mathbb{Z},\ n \geq 0,\ a_i \in A,\ \epsilon_i = \pm 1\ \forall i\}$

and $\bar{A} = \{1\}$ if $A = \emptyset$.

Proposition 3.19. $\bar{A} = \langle A \rangle$

Proof. Since $\bar{A}$ is never empty, and we can see if a, b are in $\bar{A}$, ab^{-1} is again an element of $\bar{A}$, making it a subgroup. For each a in A, $a^1 = a$,and hence $A \subseteq \bar{A}$, and hence $\langle A \rangle \subseteq \bar{A}$. Since $\langle A \rangle$ is a subgroup, and hence closed under group operations and inverses, each element of $\bar{A}$ belongs in it. □

If G is abelian, we can collect all the powers together, and if each a_i has a finite order d_i, then note that $|\langle A \rangle| \leq d_1 \dots d_k$. Non abelian nature complicates matters, and even finite order generators can result in a subgroup of infinite order.
A subgroup M of a group G is called a maximal subgroup if $M \neq G$ and the only subgroups of G which contain M are M and G. If H is a proper subgroup of a finite group G, then there is such an H. We can also prove that if $G = \langle x \rangle$ of order n, then H is maximal iff $H = \langle x^p \rangle$ for some prime p dividing n.
The lattice of subgroups of a given finite group G is constructed as follows: plot all subgroups of G starting at the bottom with 1 , ending at the top with G and, with subgroups of larger order positioned higher on the page than those of smaller order. We draw paths upwards between subgroups using the rule that there will be a line upward from A to B if $A \leq B$ and there are no subgroups properly between A and B.
This may not be easily (or at all) carried out for infinite groups. Isomorphic groups have the same lattices (converse is not true).

§4. Quotient Groups and Homomorphisms

§§4.1. Definitions

Definition 4.1. If $\varphi : G \to H$ is a homomorphism the kernel of it is the set $\{g \in G | \varphi(g) = 1_H\}$, and denoted by $ker\varphi$.

Proposition 4.2. If $\varphi : G \to H$ is a homomorphism then

- $\varphi(1_G) = 1_H$
- $\varphi(g^{-1}) = (\varphi(g))^{-1}$
- $\varphi(g^n) = \varphi(g)^n$
- $ker\varphi$ is a subgroup of G
- the image of G under φ $(im\varphi)$, is a subgroup of H .

The proof follows a similar argument using the definition of a homomorphism as we have done multiple times.

Definition 4.3. Let $\varphi : G \to H$ be a homomorphism with kernel K . The quotient group or factor group, G/K is the group whose elements are the fibers of φ with group operation : if X is the fiber above a and Y is the fiber above b then the product of X with Y is defined to be the fiber above the product ab. This is associative under multiplication since it is associative in H, the identity is the fiber over the identity of H, and the inverse of the fiber over a is the fiber over a^{-1}, making the set of fibers into a group.

Proposition 4.4. Let $\varphi : G \to H$ be a homomorphism with kernel K. Let $X \in G/K$ be the fiber above a, $X = \varphi^{-1}(a)$.

- For any $u \in X$, $X = \{uk | k \in K\}$
- For any $u \in X$, $X = \{ku | k \in K\}$

Proof. (1) and (2) have the same proof. Let $uK = \{uk|k \in K\}$. For any k in K, $\varphi(uk) = \varphi(u)\varphi(k) = a$, hence uk is in X, thus $uK \subseteq X$. Let any g in X, and put $k = u^{-1}g$, then $\varphi(k) = 1$, thus k is in K, making $g = uk$, and hence $X \subseteq uK$. □

Definition 4.5. For any $N \leq G$, and any $g \in G$, $gN = \{gn|n \in N\}$ is the left coset and $Ng = \{ng|n \in N\}$ is the right coset of N in G. Any element of a coset is called a representative for the coset.

Theorem 4.6. 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, if u_1 and v_1 are the chosen representatives, then $uvK = u_1v_1K$. The same statement is true with right coset in place of left coset.

Proof. Let K is the kernel of some homomorphism $\varphi : G \to H$, and $X = \varphi^{-1}(a)$ and $Y = \varphi^{-1}(b)$. By definition of operation, if $Z = XY$ then $Z = \varphi^{-1}(ab)$. For any arbitrary representatives u, v of X and Y, we can see that uv is in Z. Hence Z is the left coset. We can show conversely every element z in Z is written as uv in the same way and well defined follows. The last statement follows from the definition. □

Example 4.7. For isomorphisms, $K = 1$ and G/K is isomorphic to G. If $H = 1$, then ker of homomorphism is G, and called the trivial homomorphism with G/G isomorphic to 1.

Proposition 4.8. If N is any subgroup of G, the set of left cosets form a partition of G. For all u, v in G, $uN = vN$ iff $v^{-1}u$ is in N, and $uN = vN$ iff u and v are representatives of the same coset.

Proof. Since N is a subgroup of G, 1 belongs to N, and $1 \cdot g = g$ belongs to gN, and any element of gN belongs to G by defintion, hence $G = \cup gN$ with g in G. If $uN \cap vN$ is not empty, and x is in the intersection, then $x = un = vm$, $u = vm_1$ for m, m_1, n in N. Hence any element ut of $uN = vm_1t$, which is in vN, and conversely we can prove the other inequality to show $vN = uN$. From this, if $u \cdot 1$ is in vN, this means that $v^{-1}u$ is in N, and equality of representatives follow. □

Proposition 4.9. Let G be a group and let N be a subgroup of G.

- 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.
- If well defied, the set of left cosets are a group, with identity 1N and inverse of gN is $g^{-1}N$

Proof. If well defined, then for any u, u_1 in uN and v, v_1 in vN using $u = 1, u_1 = n, v = v^{-1} = g^{-1}$, then $uvN = u_1v_1N$ implies $g^{-1}N = ng^{-1}N$, hence $ng^{-1} = g^{-1}n_1$, giving gng^{-1} in N. Conversely if gng^{-1} in N $u_1v_1 = unvm = uvv^{-1}nvm = uvn_1m = uvn_2$, hence uvN and u_1v_1N contain a common element and hence are equal. From above, verifying group axioms is easy. □

Definition 4.10. The set $gNg^{-1} = \{gng^{-1} | n \in N\}$ is the conjugate of N by g. g normalizes N if $gNg^{-1} = N$. A subgroup N of a group G is called normal if every element of G normalizes N. If N is a normal subgroup of G write $N \trianglelefteq G$.

Hence we conclude -

Theorem 4.11. If N is a subgroup of G, then the following are equivalent -

- $N \trianglelefteq G$
- $N_G(N) = G$
- $gN = Ng$ for all g in G
- the operation on left cosets makes it into a group
- $gNg^{-1} \subseteq N$ for all g in G

Proposition 4.12. A subgroup N of G is normal iff it is the kernel of some homomorphism.

Proof. If it is a kernel, we have already proved that it is normal. Let $N \trianglelefteq G$ let $H = G/N$ and define $\pi : G \to H$ as $\pi(g) = gN$, we can see from the above properties that it is a homomorphism. $ker\pi = \{g \in G | gN = 1N\}$, thus g is in N, and hence N is the kernel of π. □

Definition 4.13. Let $N \trianglelefteq G$, the homomorphism $\pi : G \to G/N$, as $\pi(g) = gN$ is the natural projection. If $\bar{H} \leq G/N$, then the complete preimage of $\bar{H}$ in G is the preimage of it under the natural projection homomorphism.

If G is an abelian group, any subgroup N of G is normal. We can prove that quotient groups of cyclic groups are cyclic, with $|G/N| = |G|/|N|$.

§§4.2. Lagranges Theorem

Theorem 4.14. 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 is $\frac{|G|}{|H|}$.

Proof. If $|H| = n$, and the number of left cosets be k. Consider the map $H \to gH$ as $h \mapsto gh$, is clearly a surjection and by cancellation law, an injection, hence $|gH| = |H|$. Since G is partitioned into k disjoint subsets each of which has cardinality n, $|G| = kn$, thus completing the proof. □

Definition 4.15. If G is a group and $H \leq G$, the number of left cosets of H in G is called the index of H in G and denoted by $|G : H|$.

We see here 2 corollaries. If G is a finite group and x in G, then the order of x divides the order of G (by Lagrange Theorem). In particular $X^{|G|} = 1$ for all x in G. If G is a group of prime order p , then G is cyclic, hence $G \cong Z_p$.

Definition 4.16. Groups G in which the only normal subgroups are the trivial ones: 1 and G are called simple groups.

The full converse to Lagrange's Theorem is not true: namely, if G is a finite group and n divides $|G|$, then G need not have a subgroup of order n. However the following partial converses are true -

Theorem 4.17. *Cauchy Theorem* : If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

Theorem 4.18. *Sylow* : If G is a finite group of order $p^\alpha m$ where p is a prime and p doesnt divide m, the G has a subgroup of order p^α.

We postpone the proofs.

Definition 4.19. Let H and K be subgroups of a group and define $HK = \{hk | h \in H, k \in K\}$. This need not be a group.

Proposition 4.20. H and K are finite subgroups of a group then $|HK| = \frac{|H||K|}{|H \cap K|}$.

Proof. HK is the union of left cosets of K, and each coset of K has $|K|$ elements, and 2 cosets are the same iff $h_1 h_2^{-1}$ is in K, thus $h_1(H \cap K) = h_2(H \cap K)$, and the number of distinct cosets is hence $\frac{|H|}{|H \cap K|}$ by Lagranges theorem, each of which has $|K|$ number of elements, hence the formula. □

Theorem 4.21. If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.

Proof. If $HK = KH$, then identity is in both, and let a, b be in HK, then let $a = h_1 k_1$ and $b = h_2 k_2$, then using $HK = KH$ we can see that ab^{-1} is in HK, and hence is a subgroup. Conversly, if it is a subgroup, $K \leq HK$ and $H \leq HK$, thus $KH \leq HK$, and by taking any element and its inverse in HK the reverse inclusion follows. □

A corollary follows that if H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. If $K \trianglelefteq G$, then $HK \leq G$ for any $H \leq G$. That is, HK is a subgroup if H normalizes K. In a finite group the number of left cosets of H in G equals the number of right cosets even though the left cosets are not right cosets in general (unless they are normal).

§§4.3. Isomorphism theorems

Theorem 4.22. The First Isomorphism Theorem: If $\varphi : G \to H$ is a homomorphism of groups, then $ker\varphi \trianglelefteq G$ and $G/ker\varphi \cong \varphi(G)$.

The corollary can be stated as - φ is injective iff $ker\varphi = 1$ and $|G : ker\varphi| = |\varphi(G)|$.

Theorem 4.23. The Second Isomorphism Theorem: If G is a group, A and B are subgroups, and let $A \leq N_G(B)$. Then AB is a subgroup, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.

Proof. By the above corollary, AB is a subgroup. Since $B \leq N_G(B)$, thus $AB \leq N_G(B)$, B is normal in AB and hence AB/B is defined. $\varphi : A \to AB/B$ as $\varphi(a) = aB$. We see that this is a homomorphism, identity is the coset B, hence $ker\varphi = A \cap B$. The result then follows from the first isomorphism theorem. □

Theorem 4.24. The Third Isomorphism Theorem: If G is a group and H and K are normal subgroups, with $H \leq K$, then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$.

Proof. The first part follows from the definition, and define $\varphi : G/H \to G/K$. We can see this is well defined since $gH \mapsto gK$, and that it is a surjective homomorphism. Noe that $ker\varphi = K/H$, and the result follows from the first isomorphism theorem. □

Theorem 4.25. The Fourth Isomorphism Theorem: If G is a group and N is 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 $A/N = \bar{A}$. Then -

- $A \leq B$ iff $\bar{A} \leq \bar{B}$
- if $A \leq B$ then $|B : A| = |\bar{B} : \bar{A}|$
- $\overline{\langle A, B \rangle} = \langle \bar{A}, \bar{B} \rangle$
- $\overline{A \cap B} = \bar{A} \cap \bar{B}$
- $A \trianglelefteq G$ iff $\bar{A} \trianglelefteq \bar{G}$

§5. Group Actions

§§5.1. Permutation representations

If G is the group acting on set A, then for each g in G, $\sigma_g : A \to A$ is defined as $\sigma_g : a \mapsto g \cdot a$. The homomorphism defined as $\varphi : G \to S_A$ as $\varphi(g) = \sigma(g)$ is the permutation representation to the given action. The Kernel of the action : $\{g \in G | g \cdot a = a\}$ for all a in A. The stabilizer of a in G is : $\{g \in G | g \cdot a = a\}$ denoted by G_a. An action is faithful if its kernel is the identity.

Proposition 5.1. For any group G and any nonempty set A there is a bijection between the actions of G on A and the homomorphisms of G into S_A .

This follows by noting that $g \cdot a = \varphi(g)(a)$. We shall say a given action of G on A affords or induces the associated permutation representation of G.

Proposition 5.2. If G acts on nonempty A, then the relation $a \sim b$ iff $a = g \cdot b$ is an equivalence relation. For each a in A, the number of elements in the equivalence class containing a is $|G : G_a|$

Proof. We can see that $a \sim a$ since it is connected by identity, it is symmetric since inverse of g connects b and a, and transitivity follows from the group action definition. Let $C_a = \{g \cdot a | g \in G\}$ is the equivalence class of a, define the map $g \cdot a \mapsto gG_a$. It is clearly a surjection, on g and $g \cdot a = h \cdot a$ iff $h^{-1}g$ is in G_a iff $gG_a = hG_a$ hence map is injective and thus a bijection. □

Definition 5.3. Let G be a group acting on the nonempty set A. The equivalence class $\{g \cdot a | g \in G\}$ is the orbit of G containing a. The action of G on A is called transitive if there is only one orbit, ie for any 2 elements a and b in A, $a = gb$ for some g in G.

Subgroups of symmetric groups are called permutation groups.

§§5.2. Groups acting on themselves by left multiplication

Here we consider $G = A$, ie $g \cdot a = ga$ for all g, a in G. For finite groups we label the elements as $g_1, \ldots, g_n$, with the permutation as $\sigma_g(i) = j$ iff $gg_i = g_j$. We can see that action of group on itself is transitive and faithful.

We consider a generalization of this action.

Definition 5.4. Let H be any subgroup of G and let A be the set of all left cosets of H in G. Define an action of G on A by $g \cdot aH = gaH$, for all g in G and aH in A. This clearly satisfies the axioms for group action. If H is the identity subgroup, then this specializes to the action described above, if it is of finite index m, then the permutation is described as $\sigma_g(i) = j$ iff $ga_iH = a_jH$.

Theorem 5.5. Let G be a group, let H be a subgroup of G and let G act by left multiplication on the set A of left cosets of H in G . Let π_H be the associated permutation representation afforded by this action. The G acts transitively on A, the stabilizer of H in A is H and the kernel of the action is $\cap_{x \in G} xHX^{-1}$ and it is the largest normal subgroup of G in H.

Proof. For any 2 cosets aH and bH, note that $g = ba^{-1}$ is the required element for transitivity. The stabilizer of H by definition is H itself ($\{g \in G | g \cdot 1H = 1H\}$. Note $ker\pi_H = \{g \in G | gxH = xH\}$ for all x in G, thus $x^{-1}gx \in H$ and hence the relation follows. Note that $ker\pi_h \trianglelefteq G$ and $ker\pi_h \trianglelefteq H$, if any N is normal in H then $N = xNx^{-1} \leq xHx^{-1}$ thus N is a subgroup of the intersection. □

The corollary is the Cayleys theorem which we prove using $H = 1$, obtaining a homomorphism and an isomorphism since kernel is the identity.

Theorem 5.6. Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n, then G is isomorphic to a subgroup of S_n.

The permutation representation afforded by left multiplication on the elements of G (cosets of $H = 1$) is called the left regular representation of G. Another corollary is as follows -

Theorem 5.7. If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.

Let $H \leq G$ and $|G : H| = p$ and π_H be the permutation representation and $K = ker\pi_H$, and let $|H : K| = k$ then $|G : K| = kp$ and G/K is isomorphic to a subgroup of S_p by the first isomorphism theorem, and by Lagranges theorem, pk divides $p!$ and hence k divides $(p-1)!$. By minimality of p, thus $k = 1$, and hence $H = K \trianglelefteq G$.

§§5.3. Groups acting on themselves by conjugation

Here we again consider $G = A$ but acting by conjugation : $g \cdot a = gag^{-1}$ for all g, a in G. We can see that it satisfies the asioms for group action.

Definition 5.8. Two elements a and b of G are said to be conjugate in G if there is some g in G such that $b = gag^{-1}$ (i.e., if and only if they are in the same orbit of G acting on itself by conjugation). The orbits of G acting on itself by conjugation are called the conjugacy classes of G.

For abelian groups the conjugacy classes are just $\{a\}$. If $|G| > 1$, then $\{1\}$ is a conjugacy class, and one element subset is a conjugacy class iff a is in the centre of G. We now generalize to any subset S of G and the action as $g \cdot S = gSg^{-1}$ for any g in G, and S in the set of all subsets of G.

Definition 5.9. Two subsets S and T of G are said to be conjugate in G if there is some g in G such that $T = gSg^{-1}$.

Proposition 5.10. The number of conjugates of S is the index $|G : N_G(S)|$, and in particular the number of conjugates of s is the index $|G : C_G(s)|$.

Proof. The number of conjugates of S is the index $|G : G_s|$ where $G_S = \{g \in G | gSG^{-1} = S\} = N_G(S)$, from an above proposition, hence the first part follows, the second follows by noting that $N_G(\{s\}) = C_G(s)$ □

Theorem 5.11. The Class equation: If G is a finite group and $g_1, \dots g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ then $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$.

Proof. This follows from the above proposition and noting that $\{x\}$ is a conjugacy class of size 1 iff x is in $Z(G)$. Since they contain just 1 element, hence the total number of elements of G follows as the sum of 1 centre order times and the number of conjugates for each representative for a conjugacy class. □

Theorem 5.12. If p is a prime and P is a group of order p^α for some $\alpha \geq 1$ then $Z(P) \neq 1$.

Proof. From definition we know that $C_P(g_i) \neq P$ hence p divides $|P : C_P(g_i)|$ hence by the class equation p divides $Z(P)$. □

A corollary follows that if $P = p^2$ for prime p then since $Z(P) \neq 1$ and hence $P/Z(P)$ is cyclic, making P abelian. If P has an element of order p^2 then it is cyclic and isomorphic to Z_{p^2} or $Z_p \times Z_p$.

Proposition 5.13. If σ, τ are elements of S_n and if σ has cycle decomposition $(a_1 a_2 ... a_{k1})(b_1 b_2 ... b_{k2})...$ then $\tau\sigma\tau^{-1}$ has cycle decomposition $(\tau(a_1)\tau(a_2)\dots\tau(a_{k1}))(\tau(b_1)\tau(b_2)\dots\tau(b_{k2}))\dots$.

Proof. This just follows from the fact that if $\sigma(i) = j$ then $(\tau\sigma\tau^{-1})\tau(i) = \tau(j)$. □

Definition 5.14. If $\sigma \in S_n$ is the product of disjoint cycles $n_1, \dots n_r$ with $n_1 \leq n_2 \dots \leq n_r$ then these r integers are called the cycle type of σ. A partition of n is a non decreasing sequence of integers whose sum is n.

Proposition 5.15. Two elements of S_n are conjugate iff they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.

Proof. Conjugates have the same cycle type from above, and conversely we first order the cycles in increasing length and define τ mapping the i position in σ_1 to the i position in σ_2, and we note from the above prop that $\tau\sigma_1\tau^{-1} = \sigma_2$. □

Using these we obtain that if σ is a m cycle, then $|C_{S_n}(\sigma)| = m(n-m)!$, explicitly written as $C_{S_n}(\sigma) = \{\sigma^i\tau | 0 \leq i \leq m-1, \tau \in S_{n-m}$, where S_{n-m} is the group fixing all integers in the m cycle.

Proposition 5.16. If $H \trianglelefteq G$ then for every conjugacy class $\mathcal{K}$ in G either $K \subseteq H$ or $K \cap H = \phi$.

Proof. This follows since if $x \in \mathcal{K} \cap H$, then $gxg^{-1} \in gHg^{-1}$ for all g. Since H is normal thus the relation follows. □

Definition 5.17. We now similarly define right group actions of G on A as a map from $A \times G$ to A that satisfies:

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

The conjugation action is written as $a^g = g^{-1}ag$ and we see this verifies the axioms for a group action. We see a left group action can be transformed to a right group action as $a \cdot g = g^{-1} \cdot a$, called corresponding group actions. Note that the relation conjugacy is the same for the left and right corresponding actions.

§6. Revised PoA

On track, so the PoA is the same as before -

- Till 25 June - The Fundamental Group
- Till 5 July - Seperation theorems in the plane
- TIll 15 July - The Seifert-van Kampen Theorem
- ENDTERM REPORT SUBMISSION

The main reference in the second half will be Topology (Second Edition) by James R Munkres.