A STUDY ON GROUP THOERY

Submitted to

University of Calicut

In partial fulfillment of the requirement for the award of the Degree of

Bachelor of Science (Mathematics)

Submitted by

Name

(Reg.no. 12345)

2017

DECLARATION

I do …(name)…….. hereby declare that this project report entitled as “A STUDY ON GROUP THEORY” is a bona-fide record of the project work carried by me during the academic year 2016-17 in partial fulfillment of the requirements for the award of the degree of B.Sc Mathematics of the University of Calicut. This work has not been undertaken or submitted elsewhere in connection with any academic course.

Place

date

CONTENTS

INTRODUCTION

Group theory has three main historical sources: number theory, the theory of algebraic equations, and geometry. The number-theoretic strand was begun by Leonhard Euler, and developed by Gauss's work on modular arithmetic and additive and multiplicative groups related to quadratic fields. Early results about permutation groups were obtained by Lagrange, Ruffini, and Abel in their quest for general solutions of polynomial equations of high degree. Évariste Galois coined the term "group" and established a connection, now known as Galois theory, between the nascent theory of groups and field theory. In geometry, groups first became important in projective geometry and, later, non-Euclidean geometry. Felix Klein's Erlangen program proclaimed group theory to be the organizing principle of geometry

Galois, in the 1830s, was the first to employ groups to determine the solvability of polynomial equations. Arthur Cayley and Augustin Louis Cauchy pushed these investigations further by creating the theory of permutation groups. The second historical source for groups stems from geometrical situations. In an attempt to come to grips with possible geometries (such as euclidean, hyperbolic or projective geometry) using group theory, Felix Klein initiated the Erlangen programme. Sophus Lie, in 1884, started using groups (now called Lie groups) attached to analytic problems.

The different scope of these early sources resulted in different notions of groups. The theory of groups was unified starting around 1880. Since then, the impact of group theory has been ever growing, giving rise to the birth of abstract algebra in the early 20th century, representation theory, and many more influential spin-off domains.

Objectives

1. To study about group theory
2. To get an idea about Rings and Integral Domains
3. To study about Fields
4. To study about Field of Quotients

METHODOLOGY

Secondary sources are used for collecting data.

RESULTS AND DISCUSSION

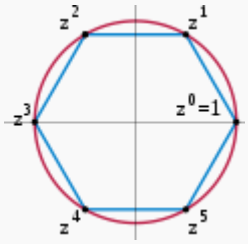
Group theory

For group theory in social sciences, see social group.

The popular puzzle Rubik's cube invented in 1974 by Ernő Rubik has been used as an illustration of permutation groups.

Algebraic structure → Group theory

Group theory



In mathematics and abstract algebra, **group theory** studies the algebraic structures known as groups. The concept of a group is central to abstract algebra: other well-known algebraic structures, such as rings, fields, and vector spaces, can all be seen as groups endowed with additional operations and axioms. Groups recur throughout mathematics, and the methods of group theory have influenced many parts of algebra. Linear algebraic groups and Lie groups

are two branches of group theory that have experienced advances and have become subject areas in their own right.

Various physical systems, such as crystals and the hydrogen atom, may be modelled by symmetry groups. Thus group theory and the closely related representation theory have many important applications in physics, chemistry, and materials science. Group theory is also central to public key cryptography.

One of the most important mathematical achievements of the 20th century[1] was the collaborative effort, taking up more than 10,000 journal pages and mostly published between 1960 and 1980, that culminated in a complete classification of finite simple groups.

Main classes of groups

The range of groups being considered has gradually expanded from finite permutation groups and special examples of matrix groups to abstract groups that may be specified through a presentation by generators and relations.

Permutation groups

The first class of groups to undergo a systematic study was permutation groups. Given any set X and a collection G of bijections of X into itself (known as *permutations*) that is closed under compositions and inverses, G is a group acting on X. If X consists of n elements and G consists of *all* permutations, G is the symmetric group S_n; in general, any permutation group G is a subgroup of the symmetric group of X. An early construction due to Cayley exhibited any group as a permutation group, acting on itself ($X = G$) by means of the left regular representation.

In many cases, the structure of a permutation group can be studied using the properties of its action on the corresponding set. For example, in this way one proves that for $n \geq 5$, the alternating group A_n is simple, i.e. does not admit any proper normal subgroups. This fact plays a key role in the impossibility of solving a general algebraic equation of degree $n \geq 5$ in radicals.

Matrix groups

The next important class of groups is given by *matrix groups*, or linear groups. Here G is a set consisting of invertible matrices of given order n over a field K that is closed under the products and inverses. Such a group acts on the n-dimensional vector space K^n by linear transformations. This action makes matrix groups conceptually similar to permutation groups, and the geometry of the action may be usefully exploited to establish properties of the group G.

Transformation groups

Permutation groups and matrix groups are special cases of transformation groups: groups that act on a certain space X preserving its inherent structure. In the case of permutation groups, X is a set; for matrix groups, X is a vector space. The concept of a transformation group is closely related with the concept of a symmetry group: transformation groups frequently consist of *all* transformations that preserve a certain structure.

The theory of transformation groups forms a bridge connecting group theory with differential geometry. A long line of research, originating with Lie and Klein, considers group actions on manifolds by homeomorphisms or diffeomorphisms. The groups themselves may be discrete or continuous.

Abstract groups

Most groups considered in the first stage of the development of group theory were "concrete", having been realized through numbers, permutations, or matrices. It was not until the late nineteenth century that the idea of an abstract group as a set with operations satisfying a certain system of axioms began to take hold. A typical way of specifying an abstract group is through a presentation by *generators and relations*,

A significant source of abstract groups is given by the construction of a *factor group*, or quotient group, G/H, of a group G by a normal subgroup H. Class groups of algebraic number fields were among the earliest examples of factor groups, of much interest in number theory.

If a group G is a permutation group on a set X, the factor group G/H is no longer acting on X; but the idea of an abstract group permits one not to worry about this discrepancy.

The change of perspective from concrete to abstract groups makes it natural to consider properties of groups that are independent of a particular realization, or in modern language, invariant under isomorphism, as well as the classes of group with a given such property: finite groups, periodic groups, simple groups, solvable groups, and so on. Rather than exploring properties of an individual group, one seeks to establish results that apply to a whole class of groups. The new paradigm was of paramount importance for the development of mathematics: it foreshadowed the creation of abstract algebra in the works of Hilbert, Emil Artin, Emmy Noether, and mathematicians of their school.

Topological and algebraic groups

An important elaboration of the concept of a group occurs if G is endowed with additional structure, notably, of a topological space, differentiable manifold, or algebraic variety. If the group operations m (multiplication) and i (inversion),

are compatible with this structure, i.e. are continuous, smooth or regular (in the sense of algebraic geometry) maps, then G becomes a topological group, a Lie group, or an algebraic group.[2]

The presence of extra structure relates these types of groups with other mathematical disciplines and means that more tools are available in their study. Topological groups form a natural domain for abstract harmonic analysis, whereas Lie groups (frequently realized as transformation groups) are the mainstays of differential geometry and unitary representation theory. Certain classification questions that cannot be solved in general can be approached and resolved for special subclasses of groups. Thus, compact connected Lie groups have been completely classified. There is a fruitful relation between infinite abstract groups and topological groups: whenever a group Γ can be realized as a lattice in a topological group G, the geometry and analysis pertaining to G yield important results about Γ. A comparatively recent trend in the theory of finite groups exploits their connections with compact topological groups (profinite groups): for example, a single p-adic analytic group G has a family of

quotients which are finite p-groups of various orders, and properties of G translate into the properties of its finite quotients.

Branches of group theory

Finite group theory

During the twentieth century, mathematicians investigated some aspects of the theory of finite groups in great depth, especially the local theory of finite groups and the theory of solvable and nilpotent groups. As a consequence, the complete classification of finite simple groups was achieved, meaning that all those simple groups from which all finite groups can be built are now known.

During the second half of the twentieth century, mathematicians such as Chevalley and Steinberg also increased our understanding of finite analogs of classical groups, and other related groups. One such family of groups is the family of general linear groups over finite fields. Finite groups often occur when considering symmetry of mathematical or physical objects, when those objects admit just a finite number of structure-preserving transformations. The theory of Lie groups, which may be viewed as dealing with "continuous symmetry", is strongly influenced by the associated Weyl groups. These are finite groups generated by reflections which act on a finite-dimensional Euclidean space. The properties of finite groups can thus play a role in subjects such as theoretical physics and chemistry.

Representation of groups

Saying that a group G *acts* on a set X means that every element of G defines a bijective map on the set X in a way compatible with the group structure. When X has more structure, it is useful to restrict this notion further: a representation of G on a vector space V is a group homomorphism:

$$\rho : G \to \mathrm{GL}(V),$$

where $\mathrm{GL}(V)$ consists of the invertible linear transformations of V. In other words, to every group element g is assigned an automorphism $\rho(g)$ such that $\rho(g) \circ \rho(h) = \rho(gh)$ for any h in G.

This definition can be understood in two directions, both of which give rise to whole new domains of mathematics.[3] On the one hand, it may yield new information about the group G: often, the group operation in G is abstractly given, but via ρ, it corresponds to the multiplication of matrices, which is very explicit.[4] On the other hand, given a well-understood group acting on a complicated object, this simplifies the study of the object in question. For example, if G is finite, it is known that V above decomposes into irreducible parts. These parts in turn are much more easily manageable than the whole V.

Given a group G, representation theory then asks what representations of G exist. There are several settings, and the employed methods and obtained results are rather different in every case: representation theory of finite groups and representations of Lie groups are two main subdomains of the theory. The totality of representations is governed by the group's characters. For example, Fourier polynomials can be interpreted as the characters of U(1), the group of complex numbers of absolute value *1*, acting on the L^2-space of periodic functions.

Lie theory

A Lie group is a group that is also a differentiable manifold, with the property that the group operations are compatible with the smooth structure. Lie groups are named after Sophus Lie, who laid the foundations of the theory of continuous transformation groups. Lie groups represent the best-developed theory of continuous symmetry of mathematical objects and structures, which makes them indispensable tools for many parts of contemporary mathematics, as well as for modern theoretical physics. They provide a natural framework for analysing the continuous symmetries of differential equations (differential Galois theory), in much the same way as permutation groups are used in Galois theory for analysing the discrete symmetries of algebraic equations. An extension of Galois theory to the case of continuous symmetry groups was one of Lie's principal motivations.

Combinatorial and geometric group theory

Groups can be described in different ways. Finite groups can be described by writing down the group table consisting of all possible multiplications $g \cdot h$. A more compact way of defining a group is by *generators and relations*, also called the *presentation* of a group. Given any set F of generators $\{g_i\}_{i \in I}$, the free group generated by F subjects onto the group G. The kernel of this map is called subgroup of relations, generated by some subset D. The

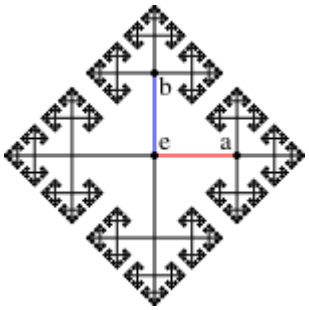
presentation is usually denoted by $\langle F \mid D \rangle$. For example, the group $\mathbf{Z} = \langle a \mid \rangle$ can be generated by one element a (equal to +1 or −1) and no relations, because $n \cdot 1$ never equals 0 unless n is zero. A string consisting of generator symbols and their inverses is called a *word*.

Combinatorial group theory studies groups from the perspective of generators and relations.[6] It is particularly useful where finiteness assumptions are satisfied, for example finitely generated groups, or finitely presented groups (i.e. in addition the relations are finite). The area makes use of the connection of graphs via their fundamental groups. For example, one can show that every subgroup of a free group is free.

There are several natural questions arising from giving a group by its presentation. The *word problem* asks whether two words are effectively the same group element. By relating the problem to Turing machines, one can show that there is in general no algorithm solving this task. Another, generally harder, algorithmically insoluble problem is the group isomorphism problem, which asks whether two groups given by different presentations are actually isomorphic. For example, the additive group $\mathbf{Z}$ of integers can also be presented by

$$\langle x, y \mid xyxyx = e \rangle \ ;$$

it may not be obvious that these groups are isomorphic.



The Cayley graph of ⟨ x, y | ⟩, the free group of rank 2.

Geometric group theory attacks these problems from a geometric viewpoint, either by viewing groups as geometric objects, or by finding suitable geometric objects a group acts on. The first idea is made precise by means of the Cayley graph, whose vertices correspond to group elements and edges correspond to right multiplication in the group. Given two elements, one constructs the word metric given by the length of the minimal path between the elements. A theorem of Milnor and Svarc then says that given a group G acting in a

reasonable manner on a metric space *X*, for example a compact manifold, then *G* is quasi-isometric (i.e. looks similar from a distance) to the space *X*.

Connection of groups and symmetry

Given a structured object *X* of any sort, a symmetry is a mapping of the object onto itself which preserves the structure. This occurs in many cases, for example

1. If *X* is a set with no additional structure, a symmetry is a bijective map from the set to itself, giving rise to permutation groups.
2. If the object *X* is a set of points in the plane with its metric structure or any other metric space, a symmetry is a bijection of the set to itself which preserves the distance between each pair of points (an isometry). The corresponding group is called isometry group of *X*.
3. If instead angles are preserved, one speaks of conformal maps. Conformal maps give rise to Kleinian groups, for example.
4. Symmetries are not restricted to geometrical objects, but include algebraic objects as well.

> The axioms of a group formalize the essential aspects of symmetry. Symmetries form a group: they are closed because if you take a symmetry of an object, and then apply another symmetry, the result will still be a symmetry. The identity keeping the object fixed is always a symmetry of an object. Existence of inverses is guaranteed by undoing the symmetry and the associativity comes from the fact that symmetries are functions on a space, and composition of functions are associative.

Frucht's theorem says that every group is the symmetry group of some graph. So every abstract group is actually the symmetries of some explicit object.

The saying of "preserving the structure" of an object can be made precise by working in a category. Maps preserving the structure are then the morphisms, and the symmetry group is the automorphism group of the object in question.

Applications of group theory

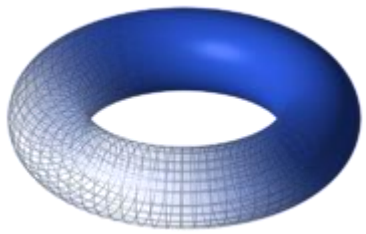
Applications of group theory abound. Almost all structures in abstract algebra are special cases of groups. Rings, for example, can be viewed as abelian groups (corresponding to addition) together with a second operation (corresponding to multiplication). Therefore, group theoretic arguments underlie large parts of the theory of those entities.

Galois theory

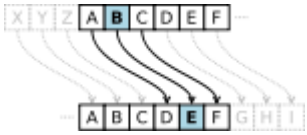
Galois theory uses groups to describe the symmetries of the roots of a polynomial (or more precisely the automorphisms of the algebras generated by these roots). The fundamental theorem of Galois theory provides a link between algebraic field extensions and group theory. It gives an effective criterion for the solvability of polynomial equations in terms of the solvability of the corresponding Galois group. For example, S_5, the symmetric group in 5 elements, is not solvable which implies that the general quintic equation cannot be solved by radicals in the way equations of lower degree can. The theory, being one of the historical roots of group theory, is still fruitfully applied to yield new results in areas such as class field theory.

Algebraic topology

Algebraic topology is another domain which prominently associates groups to the objects the theory is interested in. There, groups are used to describe certain invariants of topological spaces. They are called "invariants" because they are defined in such a way that they do not change if the space is subjected to some deformation. For example, the fundamental group "counts" how many paths in the space are essentially different. The Poincaré conjecture, proved in 2002/2003 by Grigori Perelman, is a prominent application of this idea. The influence is not unidirectional, though. For example, algebraic topology makes use of Eilenberg–MacLane spaces which are spaces with prescribed homotopy groups. Similarly algebraic K-theory relies in a way on classifying spaces of groups. Finally, the name of the torsion subgroup of an infinite group shows the legacy of topology in group theory.



A torus. Its abelian group structure is induced from the map $\mathbf{C} \to \mathbf{C}/\mathbf{Z} + \tau\mathbf{Z}$, where τ is a parameter living in the upper half plane.



The cyclic group $\mathbf{Z}_{26}$ underlies Caesar's cipher.

Algebraic geometry and cryptography

Main articles: Algebraic geometry and Cryptography

Algebraic geometry and cryptography likewise uses group theory in many ways. Abelian varieties have been introduced above. The presence of the group operation yields additional information which makes these varieties particularly accessible. They also often serve as a test for new conjectures.[9] The one-dimensional case, namely elliptic curves is studied in particular detail. They are both theoretically and practically intriguing.[10] Very large groups of prime order constructed in elliptic curve cryptography serve for public-key cryptography. Cryptographical methods of this kind benefit from the flexibility of the geometric objects, hence their group structures, together with the complicated structure of these groups, which make the discrete logarithm very hard to calculate. One of the earliest encryption protocols, Caesar's cipher, may also be interpreted as a (very easy) group operation. In another direction, toric varieties are algebraic varieties acted on by a torus. Toroidal embeddings have recently led to advances in algebraic geometry, in particular resolution of singularities.[11]

Algebraic number theory

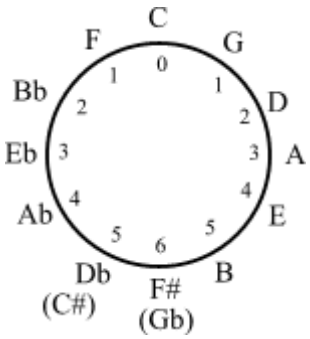
Algebraic number theory is a special case of group theory, thereby following the rules of the latter. For example, Euler's product formula captures the fact that any integer decomposes in a unique way into primes. The failure of this statement for more general rings gives rise to class groups and regular primes, which feature in Kummer's treatment of Fermat's Last Theorem.

Harmonic analysis

Analysis on Lie groups and certain other groups is called harmonic analysis. Haar measures, that is, integrals invariant under the translation in a Lie group, are used for pattern recognition and other image processing techniques.[12]

Combinatorics

In combinatorics, the notion of permutation group and the concept of group action are often used to simplify the counting of a set of objects; see in particular Burnside's lemma.



The circle of fifths may be endowed with a cyclic group structure

Music

The presence of the 12-periodicity in the circle of fifths yields applications of elementary group theory in musical set theory.

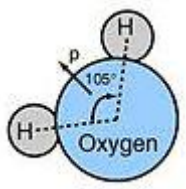
Physics

In physics, groups are important because they describe the symmetries which the laws of physics seem to obey. According to Noether's theorem, every continuous symmetry of a physical system corresponds to a conservation law of the system. Physicists are very interested in group representations, especially of Lie groups, since these representations often point the way to the "possible" physical theories. Examples of the use of groups in physics include the Standard Model, gauge theory, the Lorentz group, and the Poincaré group.

Chemistry and materials science

In chemistry and materials science, groups are used to classify crystal structures, regular polyhedra, and the symmetries of molecules. The assigned point groups can then be used to determine physical properties (such as polarity and chirality), spectroscopic properties (particularly useful for Raman spectroscopy, infrared spectroscopy, circular dichroism spectroscopy, magnetic circular dichroism spectroscopy, UV/Vis spectroscopy, and fluorescence spectroscopy), and to construct molecular orbitals.

Molecular symmetry is responsible for many physical and spectroscopic properties of compounds and provides relevant information about how chemical reactions occur. In order to assign a point group for any given molecule, it is necessary to find the set of symmetry operations present on it. The symmetry operation is an action, such as a rotation around an axis or a reflection through a mirror plane. In other words, it is an operation that moves the molecule such that it is indistinguishable from the original configuration. In group theory, the rotation axes and mirror planes are called "symmetry elements". These elements can be a point, line or plane with respect to which the symmetry operation is carried out. The symmetry operations of a molecule determine the specific point group for this molecule.



Water molecule with symmetry axis

In chemistry, there are five important symmetry operations. The identity operation (E) consists of leaving the molecule as it is. This is equivalent to any number of full rotations around any axis. This is a symmetry of all molecules, whereas the symmetry group of a chiral molecule consists of only the identity operation. Rotation around an axis (C_n) consists of rotating the molecule around a specific axis by a specific angle. For example, if a water molecule rotates 180° around the axis that passes through the oxygen atom and between the hydrogen atoms, it is in the same configuration as it started. In this case, $n = 2$, since applying it twice produces the identity operation. Other symmetry operations are: reflection, inversion and improper rotation (rotation followed by reflection).[13]

Statistical mechanics

Group theory can be used to resolve the incompleteness of the statistical interpretations of mechanics developed by Willard Gibbs, relating to the summing of an infinite number of probabilities to yield a meaningful solution.

1. **Rings**

A ring is a set *R* and two binary operations, called addition and multiplication, with the following properties:

- The ring is a commutative group under addition.
- Multiplication is associative:

  $a(bc) = (ab)c$

- Multiplication distributes over addition:

  $a(b+c)=ab+ac$
  $(a+b)c = ac + bc$

The properties of multiplication involving zero (the additive identity) and signed ring elements are the same as those derived for the integers (which are a ring), and the proofs are the same, but slightly more complicated because multiplication is not necessarily commutative:

- $0x = x0 = 0$
- $(-x)y = x(-y) = -(xy)$
- $(-x)(-y) = xy$

A ring isomorphism between the rings *R* and *S* is a one-to-one correspondence $f: R \longrightarrow S$ which preserves the ring operations:

- $f(x+y) = f(x) + f(y)$
- $f(xy) = f(x)\, f(y)$

There are minor variations in the definition of a ring; what we have presented is the minimal definition. Some authors require that a ring have a unit, which is an identity element for multiplication; i.e. a number *1* such that $1a = a1 = a$ for every element *a* of the ring. Also, it is often required that $0 \neq 1$, because a ring in which $0 = 1$ is a trivial ring with only one element.

A commutative ring is a ring with commutative multiplication.

The integers are a commutative ring with a unit. The even integers are a commutative ring without a unit. The set Z_M, previously defined as the integers $\{0, 1, ..., M-1\}$, where addition and multiplication are modulo *M*, is a commutative ring with a unit. We shall see some noncommutative rings later.

A left ideal of a ring is a nonempty subset closed under subtraction and left multiplication by any ring element; i.e. if *x* and *y* are in the ideal and *a* is any ring element, then *x-y* and *ax* are in the ideal. Similarly, a right ideal of a ring is a nonempty subset closed under subtraction and right multiplication by any ring element; i.e. if *x* and *y* are in the ideal and *a* is any ring element, then *x-y* and *xa* are in the ideal. An ideal is a set that is both a left ideal and a right ideal. Obviously, in a commutative ring there are no differences among the three kinds of ideals.

Although an ideal is required to be closed only under subtraction, it is easy to show that it is also closed under addition. If *x* and *y* are in the ideal, then *0* is in the ideal because it is equal to *x-x*, *-y* is in the ideal because it is equal to *0-y*, and *x+y* is in the ideal because it is equal to *x-(-y)*.

Ring theory is a well-developed branch of mathematics, but we need only these basic concepts. We will deal mainly with rings that have additional properties.

2. Integral Domains

An integral domain is a commutative ring with unit (and $0 \neq 1$) in which there are no zero divisors; i.e., $xy = 0$ implies that $x=0$ or $y=0$ (or both).

The integers are an integral domain; this is the reason for the name. The set Z_M, previously defined as the integers *{0, 1, ..., M-1}*, where addition and multiplication are modulo *M*, is an integral domain if *M* is prime.

Since an integral domain is a group under addition, the order of a nonzero element *a* is the smallest positive value of *n*, if any, such that $na = 0$ (where $na = a+a+a+...+a$ (*n* times)). Every nonzero element has the same order as *1* because $na = (n1)a = 0$ only when $n1 = 0$.

The order must be prime. If it could be factored as $n = ab$, then $1+1+...+1$ (*a* times) and $1+1+...+1$ (*b* times) would be two nonzero elements whose product would be zero.

The order of any nonzero element of an integral domain is often called the characteristic of the integral domain, especially when the integral domain is also a field.

3. Fields

An integral domain is a field if every nonzero element *x* has a reciprocal x^{-1} such that $xx^{-1} = x^{-1}x = 1$. Notice that the reciprocal is just the inverse under multiplication; therefore, the nonzero elements of a field are a commutative group under multiplication. The real numbers are one familiar field, and the ring Z_p is a field if *p* is prime. In fact, it is fairly easy to prove that any finite integral domain is a field.

Division in a field is defined in the usual way:

$x / y = x y^{-1}$,

where the denominator *y* must be nonzero.

From this definition and the properties of fields, we can derive the usual rules for operations on fractions:

- $a/b = c/d$ if, and only if, $ad = bc$
- $a/b + c/d = (ad + bc) / (bd)$
- $(a/b) (c/d) = (ac) / (bd)$
- $(a/b)^{-1} = b/a$
- $(-b)/a = b/(-a)a = -(a/b)$
- $0/a = 0$

- $a/1 = a$

A subfield of a field is a subset which is a field under the same addition and multiplication operations.

4. Fields of Quotients and the Rational Numbers

A rational number is a real number which can be expressed as the quotient of two integers. The integers are an integral domain, and the rational numbers are a field. This sort of relationship applies more generally. Every integral domain has a related field called its field of quotients, which is the smallest field that contains a subset isomorphic to the domain.

The relationship between the integers and the rational numbers shows how a field of quotients can be constructed.

Let D be an integral domain. We first define a relation on $D \times (D - \{0\})$ as follows:

$(a,b) \sim (c,d)$ if $ad = bc$

(Notice that this is $a/b = c/d$ cleared of fractions.) It is easy to show that this is an equivalence relationship.

We define addition and multiplication on $D \times (D - \{0\})$ as follows:

$(a,b)+(c,d)=(ad+bc,bd)$
$(a,b)(c,d) = (ac, bd)$

It can be shown that addition of equivalent pairs gives equivalent results. Hence the addition of two equivalence classes can be defined to be the class containing the sum of any elements in the two classes. Multiplication of equivalence classes can be defined in the same way.

It can be shown that the set of equivalence classes is a field under these definitions of addition and multiplication, and that the classes containing pairs of the form $(a,1)$ are isomorphic to D.

Moreover, this field is the smallest such field; any other field that contains a subset isomorphic to D also contains a subfield isomorphic to the field of quotients as constructed.

The isomorphism is a mapping that carries each quotient *a/b* of two elements of *D* to the equivalence class containing *(a,b)*.

The field of rational numbers derived from the integers is often written as *Q*.

5. Ordered Integral Domains

An ordered integral domain is an integral domain with a subset of positive elements with the following properties:

- The sum and product of two positive elements are positive.
- Zero is not positive.
- For every nonzero element *a*, either *a* or *-a*, but not both, is positive.

The element *a* of an ordered integral domain is said to be negative if *-a* is positive.

Since either *a* or *-a* is positive when *a* is nonzero, the product *aa*, which is equal to *(-a)(-a)*, is positive in either case. In particular, the unit is positive.

This is called an order because a linear order of the integral domain or field elements can be obtained by defining $a < b$ when $b-a$ is positive.

The field of quotients of an ordered integral domain is ordered by defining as positive the quotient of any two positive elements of the integral domain. In fact, this is the only way of ordering the field in a way that is consistent with the ordering of the integral domain.

An ordered field is archimedean if every number is less than some multiple of the unit. The field of rational numbers is archimedean; later we will see some non-archimedean fields.

6. The Field of Real Numbers

The field *Q* of rational numbers is insufficient for many purposes. It seems to be full of holes. For example, there is no rational number whose square is exactly *2*, which can be shown by assuming, for purpose of contradiction, that *m* and *n* are two integers such that $(m/n)^2 = 2$. This would imply that $m^2 = 2n^2$, which is impossible because the prime factor *2* would appear an even number of times in the left member and an odd number of times in the right

member. Hence every rational number is either less than the square root of *2* or greater than the square root of *2*, but never equal to the square root of *2*.

There are a number of ways to fill in the holes. One of them involves sequences and limits, which belong to the realm of analysis rather than algebra.

A sequence $\{x_1, x_2, x_3, ...\}$ of rational numbers is a Cauchy sequence if for every positive e there is an integer n such that $|x_i - x_j| < e$ whenever $i>n$ and $j>n$.

A Cauchy sequence of rational numbers does not always have a rational limit. For example, it is fairly easy to construct a Cauchy sequence of rational numbers that approaches the square root of *2*.

Two Cauchy sequences $\{x_1, x_2, x_3, ...\}$ and $\{y_1, y_2, y_3, ...\}$ are equivalent if their term-by-term difference $\{x_1 - y_1, x_2 - y_2, x_3 - y_3, ...\}$ approaches zero. It is easily shown that this is indeed an equivalence relation.

The equivalence classes are the real numbers.

We define addition and multiplication of Cauchy sequences with term-by-term addition and multiplication:

- $\{x_1, x_2, x_3, ...\} + \{y_1, y_2, y_3, ...\} = \{x_1 + y_1, x_2 + y_2, x_3 + y_3, ...\}$.
- $\{x_1, x_2, x_3, ...\} \{y_1, y_2, y_3, ...\} = \{x_1 y_1, x_2 y_2, x_3 y_3, ...\}$.

It is easy to prove that equivalent sequences have equivalent sums, and only slightly more difficult to prove that equivalent sequences have equivalent products. Hence addition and multiplication of equivalence classes is well-defined.

The result has all the required field properties, and sequences which have rational limits are isomorphic to *Q*.

The result is also an ordered field, where a positive number is an equivalence class containing a sequence $\{x_1, x_2, x_3, ...\}$ for which $x_i > e$ for all $i > n$ for some postive e and some integer n. It is easily seen to be archimedean.

The real numbers, thus defined, have another important property. The field is complete, which means that every Cauchy sequence of real numbers has a real limit.

Theorem 6.1 *The real numbers, as constructed from Cauchy sequences, is complete.*

Proof. Let $\{r_1, r_2, r_3, ...\}$ be a Cauchy sequence of real numbers. Then each term r_i is represented by an equivalence class of Cauchy sequences of rational numbers. Pick one, and find the first term in it such that difference in absolute values of subsequent terms in it will always be less than $1/i$. The equivalence class of the sequence of such first terms is the limit of the original sequence of real numbers.

The completeness property may be expressed in other ways. An upper bound for a set of numbers is just a number greater than, or equal to, every element of the set.

Theorem 6.2 *Every nonempty set of real numbers which has an upper bound has a least upper bound; i.e., an upper bound that is less than any other upper bound.*

Proof. The method of bisection is the simplest proof. We construct two Cauchy sequences $\{x_1, x_2, x_3, ...\}$ and $\{y_1, y_2, y_3, ...\}$ as follows.

Let x_1 be an element of the set, and let y_1 be an upper bound.

At the n-th step, x_n is not an upper bound, and y_n is an upper bound. Let $m = (x_n + y_n)/2$. Then if m is not an upper bound, let $x_{n+1} = m$ and $y_{n+1} = y_n$. If m is an upper bound, let $x_{n+1} = x_n$ and $y_{n+1} = m$.

These two Cauchy sequences have a common limit, which is the required least upper bound.

CONCLUSION

The main topic under this project is group theory. Main classes of groups such as permutation groups, matrix groups, Transformation groups and Abstract groups are discussed. From this project it is concluded that there are different branches of group theory including finite group theory, Lie theory and combinatorial and geometric theory. Several applications of group theory are studied in various fields such as music, chemistry etc. It is concluded that there is a connection between groups and symmetry. Moreover a brief idea about rings, integral domains, fields and fields of quotints is provided.

REFERENCES

- *Borel, Armand (1991), Linear algebraic groups, Graduate Texts in Mathematics,* ***126*** *(2nd ed.), Berlin, New York: Springer-Verlag, ISBN 978-0-387-97370-8, MR 1102012*
- *Carter, Nathan C. (2009), Visual group theory, Classroom Resource Materials Series, Mathematical Association of America, ISBN 978-0-88385-757-1, MR 2504193*
- *Cannon, John J. (1969), "Computers in group theory: A survey", Communications of the Association for Computing Machinery,* ***12****: 3–12, doi:10.1145/362835.362837, MR 0290613*
- *Frucht, R. (1939), "Herstellung von Graphen mit vorgegebener abstrakter Gruppe", Compositio Mathematica,* ***6****: 239–50, ISSN 0010-437X*
- *Golubitsky, Martin; Stewart, Ian (2006), "Nonlinear dynamics of networks: the groupoid formalism", Bull. Amer. Math. Soc. (N.S.),* ***43*** *(03): 305–364, doi:10.1090/S0273-0979-06-01108-6, MR 2223010* Shows the advantage of generalising from group to groupoid.

NB: This is only a model project. Sde students can choose any topic from their core or elective courses of the Programme.

This model is prepared by Praveena.V, Assistant Professor, Dept of mathematics, School of Disatnce Education, University of Calicut.

Fore more details : sdebscmaths@uoc.ac.in