



The Study of Properties of Group and Ring

Navita Department of Mathematics

Maharshi Dayanand University, Rohtak, Haryana (India)

Email: navitaphogat2711@gmail.com

Abstract-

Abstract algebra is the main branch of mathematics having many applications in different areas. It has number of advantage in mathematics and its role play an important part in mathematics. In this paper we discuss about fields, rings, groups, Galois group, primitive group. In this paper we discuss about the polynomial, cubic equation, quadratic equation. Here we discuss about mostly properties of groups, rings, and fields. These properties used in to differentiate between groups and ring. These properties also helps to find out which field (field of complex number, real number, rational number) make group and ring which is not. The theory of group gives discipline in mathematics which is free from calculation. It gives a technique for decrease and balancing the side of equation. It gives common geometric solution of cubic equation.

Keyword: Abstract algebra, Group, Ring, Field, Polynomial, Equation.

Introduction:

The underlying foundations of variable based math can be followed to the antiquated Babylonians, who fostered a high-level arithmetical framework with which they had the option to do estimations of algorithmic design. The formulas for calculation of problems of linear equations, quadratic equations, and indeterminate linear equations were developed by Babylonians. On the other hand, most Egyptians of this time, just as Greek and Chinese arithmetic in the first thousand years BC, normally addressed such equations by mathematical strategies, for example, those portrayed in the Eclud's element, 9 chapter of mathematical Art, and Rhind Mathematical Papyrus. The Greek in mathematical work , exemplified in the components, given the system to summing up formulae past the arrangement of specific issues into more broad frameworks of expressing and solving equations, in spite of the fact that mathematics created in middle age Islam until acknowledged would not be done.

At the time of Greek mathematics Plato had gone through an extraordinary difference. The mathematical algebra made by Greek where the terms are known by generating lines, sides of mathematical articles which had symbols related with these components. An Alexandrian Greek mathematician Diophantus write progression of books called Arithmetica. These notes help simplifying mathematical equation and number of theories which gives the advanced idea of Diophantine equation.

Prior customs talked about above affected the Persian Muḥammad ibn Mūsā alKhawārizmī (c. 780–850). He later composed The Compendious Book on Balancing, and calculation by completion, which set up algebra the discipline in mathematics that is free from calculation, arithmetic.

Hero of Alexandria and Diophantus are Hellenistic mathematicians, also Indian mathematicians for example, Brahmagupta proceeded with the customs of Egypt and Babylon,



however Diophantus' Arithmetica and Brahmagupta's Brāhmasphuṭasiddhānta are on more significant volume. For instance, first totally arithematic result (adverse answers and counting zero) for polynomial equations was depicted by Brahmagupta in his book Brahmasphutasiddhanta. Afterward, Arabic and Persian mathematicians created logarithmic techniques to a lot more significant level of complexity. Despite the fact that Diophantus and the Babylonians utilized generally uncommon impromptu strategies to tackle equations, AlKhwarizmi's commitment was essential. He tackled zero, negative numbers, quadratic equation, and linear equation along these lines needed to recognize a few kinds of equations.

In surroundings, the theory of equation is known as in terms of algebra, Diophantus (Greek mathematician) has been customarily known as the "father of algebra" however in later occasions there is more discussion about al-Khwarizmi, whose established discipline of al-jabr, merits that subject all things being equal. The individuals which support by Diophantus highlight way where Al-Jabr is found by algebra is somewhat many basic than that Arithmetica is timed where Arithmetica found in algebra while Al-Jabr is completely explanatory. The individuals who help Al-Khwarizmi highlight way that he presented techniques for "decrease" and "balancing" (interpretation of deducted components to other side of equation, for example, the undoing of same components on opposite sides of equation) which components Al-Jabr initially alluded to, and he gave a comprehensive clarification of settling quadratic equations, upheld by mathematical confirmations, while regarding algebra as autonomous discipline by him self doing. His variable based math was likewise as of now not worried "with a progression of issues to be settled, however a piece what begins with crude terms in which the mixes should give all potential models for equations, which henceforward expressly establish the genuine object of study". He likewise considered a equation for the wellbeing of its own and "in a nonexclusive way, to the extent that it doesn't just arise in the course of solving a problem, however is explicitly approached to characterize an endless class of issues".

Another Persian mathematician Omar Khayyam is set down with recognizing establishments of algebraic symmetry and tracked down common geometric solution of cubic equation. His book Treatise on Demonstrations of Problems of Algebra (1070), which set out the standards of algebra, which is part of collection of Persian mathematics that was at last communicated with Europe. One more Persian mathematician, Sharaf al-Dīn al-Tūsī, discovered algebraic and numeric solution for different instances of cubic equations. He additionally encourage idea of a function. The Indian mathematicians Mahavira what's more, Bhaskara II, the Persian mathematician Al-Karaji, and the Chinese mathematician Zhu Shijie, addressed different instances of quadratic, cubic, biquadratic and higher-order equations utilizing numerical methods. In thirteenth century, Fibonacci gives solution of cubic equation is illustrative of start of restoration in European algebra. The European world was rising while Islamic world was decreasing. Also, here additionally evolved of algebra.

Italian mathematician Girolamo Cardano describe in his 1545 book Ars magna that quadratic and cubic equation. At the end of sixteenth century Francois Viète's work on new algebra which a significant advance of modern algebra. In 1637, René Descartes distributed La Géométrie, creating modern algebraic symbols and analytic geometry. During 16th century



common arrangement of quadratic and cubic equation by further improvement in algebra on other critical. In 17th century Japanese mathematician Seki Kowa was determine all possibilities of determinant, followed autonomously by Gottfried Leibniz 10 years after the fact, to address frameworks of concurrent linear equations utilizing matrices. Gabriel Cramer additionally accomplished some work on determinants and matix in eighteenth century. Permutations were concentrated by Joseph-Louis Lagrange in his 1770 paper *Réflexions sur la résolution algébrique des équations* committed to solutions of arithmetical equations, in which he presented Lagrange resolvents. Paolo Ruffini was main individual to develop his archetypes and theory of permutation groups, additionally with regards to tackling algebraic equations. In 19th century algebra was created, getting from interest in tackling equations, at first concentrating on what is currently called Galois Theory, and on constructability issues. George Peacock was the author of aphoristic speculation in math and algebra. Augustus De Morgan found relation algebra in his *Syllabus of a Proposed System of Logic*. Josiah Willard Gibbs created algebra of vectors in three-D space, and Arthur Cayley created algebra of matrix (this is a noncommutative algebra).

Meaning:

In modern algebra, some random group and some random ring built a characteristic method in a ring and in group ring which is free module. In free module given ring have a ring of scalars components, and its premise is 1-1 with given group. According to ring, free module have expansion law and given group law has multiplication stretches out "by linearity" on premise. More informal, a given group is by postulation of a group ring, in a "weighting factor" from given ring which is joining to each component of group.

In this theory that a group ring having extra property from group, the given ring is commutative, it is sure for that a group over the given ring. In theory of group introduction the device of group ring is more helpful.

Definition:

Fields, groups and rings are three main parts in abstract algebra.

A group is known as: any number of components, with property performed on sets of these components with following activity that:

1. Closure Property:

This property contains that if we take any two element n and r from a group G then we apply a binary operation on these element then take a result n operation r which is also the member of that group. This property is also closure axiom

2. Associativity:

In this property take any three element of group such that n , r , and p which all belong that group and now apply operation such that $(n \text{ operation } r) \text{ operation } y$ consistently approaches n operation $(r \text{ operation } y)$. This property is associative.

3. Identity of a group:



Only one component of group is known as identity. Consequently in the event that if take any element r of group and apply the operation such that e operation $r = r$ operation $e = r$.

4. Inverse of a group:

Each component of a set have a unique inverse. On the off chance that any component of set n then there is other component r from the set n such that n operation $r = r$ operation $n =$ identity of group (e).

As result of 4th property of a group is that in a table of group there is any row or column does not contain any copy element. According to 2nd property, a finite group contain n element where 4th property of a group is applying to components of principal stage in other change.

Here a wide range of limited/ finite groups, some with especially complex structure. Mostly groups have a place with groups have infinite group. Here $U(10)$ is cyclic group and 3 is generator of $U(10)$ then inverse of 3 is 7 ; 7 is also generator of $U(10)$. $U(10)$ is a group of order 4. Be that as it may, there are 26 groups that don't have a place with these infinite group, called simple groups.

A group of component with having both properties addition and multiplication, called ring. In this we will known as add and multi. A ring have following axioms such that:

Let R be any no empty set. $(R, +, \cdot)$ its notation.

$(R, +)$ is a commutative group:

- (a) For all a and b belong to R implies that $a + b$ also belong to R .
- (b) $a + (b + c) = (a + b) + c$; for all a, b, c belong to R .
- (c) e belong R implies that $0 + a = a + 0$.
- (d) For each a belong R there exist b belong R implies that $a + b = b + a = e$.
- (e) $a + b = b + a$ for all a, b belongs to R .

(R, \cdot) is semi group :

- (f) For all a belongs to R , for all b belongs to R such that $a \cdot b$ also belong to R .
- (g) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b , and c belongs to R .

Left and Right distribution :

- (h) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all a, b, c belongs to R .
- (i) $(a + b) \cdot c = a \cdot c + b \cdot c$ for all a, b, c belongs to R .

A field is also a ring wherein components having same property, other than additive identity and multiplicative identity of component, additionally structure a group.

Here two types of finite field. One type of field is form of prime number under addition and multiplication modulo. The other kind of field is contain many component such that power of prime number. In prime addition exercise contain many kind of independent addition. The polynomial known by the element of the field which is prime that component are modulo number. All result will explained , the polynomial is called primitive polynomial which have polynomial are different type of polynomial has modulo while polynomial is multiplication polynomial with not any prime take coefficient modulo. The Galois field are those field which have each finite field especially those field have a subsequence type.

Let a ring R and a group G under multiplication. The notation $R(G)$ implies that group of G over R . $R(G)$ have taken order mapping such that $f: G \rightarrow R$ for some support. In this mapping



a vector which addressed as vector and α be any scalar product is αf . Let we take any two vector h and k vector in a group modulo. On the other hand we call the result of vector of f and g , A ring R into $R(G)$ be a group under group addition.

The axiom of ring are quickly verify and addition of f and g are real for a finite range. Organisation and expression are used in different kind of schemes mainly the mapping f such that $f: G \rightarrow R$ are present and after then apply in the classification of component in R have a element of group G is a set of linear combination.

Sub-parts of mathematics belonging to Algebra:

In the field theory, ring and group theory are the name in algebra have a sort term of arithmetic which under the sequence unique algebra. In this paper we use another name known modern algebra which also a short term of mathematics.

Groups:

Consolidating in group important framework in a arithmetic which is given by upper ideas. A mixture of binary operation and set S is known as group, characterized in any result you can take, yet with accompanying characteristics:

- An identity element e exists in a set S , such that $e a = a e = a$, for every a lies in S and identity is also lies in this set S .
- Each element of set S has a unique inverse: such that there exists the inverse of element a is a^{-1} where for every element of a belongs to S with result give that $(a a^{-1})$ and $(a^{-1} a)$ are both identical from the identity component.
- The activity is associativity: on the off chance that a , b and c are taken from S , such that $(a b) c$ is equal to $a (b c)$.

In this chapter group have additional property known as commutative such that we take any two element a and b of S , these product $a b$ is also belong to set S . If $a b = b a$ then this property resembles abelian group. For example, the set of whole numbers under property of addition is a group. Other example of natural number is not form a group under addition because the group identity 0 does not lie in set of natural numbers. In group of whole number, identity element is 0 and inverse of any element a is equal to $-a$. The associativity property is that we take any three element a , b , and c of group such that $a + (b + c) = (a + b) + c$, where every a , b , and c lies in this group.

Under multiplication non zero element form a group. Here, identity element is 1 , which $1 \times a$ and $a \times 1$ is equal to a ; on other hand inverse of a is $1/a$ where a is any rational number such that $a \times 1/a$ is equal to 1 .

Under the property of multiplication the element form a group may or may not be. This is on the grounds that, the multiplicative inverse of a whole number isn't a whole number. For example we take any an integer 4 and according to property of multiplicative inverse is $1/4$ where $1/4$ is not an integer which is a rational number.

Group hypothesis is focus on theory of group. An important result taken out from these hypothesis is grouping of finite simple group, for the most part distributed between around 1955 and 1983, which separate finite simple groups into about 30 fundamental sorts.



Semigroups, quasigroups, and monoids are structures like groups, however broader. They require a set and closed binary operation, however don't really fulfil different equations.

Semigroup: A group is called a semi group which have associative property however probably won't have identity element.

Monoid: A monoid is also a semigroup which has a identity yet probably won't have a inverse for each component.

Quasigroup: A quasigroup fulfill condition that any component can be transformed into other by either an extraordinary left-multiplication or right-multiplication; anyway the binary activity probably won't be associative.

Rings and Fields

Groups mainly one binary operation. To completely clarify conduct of different kinds of element, structures with two administrators should be examined. The most significant of these are rings and fields.

- A ring has two binary operation addition (+) and multiplication (\times), with property (\times) distributive over (+). Under principal administrator (+) it structures an abelian group. Under the subsequent administrator multiplication which is associative, so division is not possible because it does not have identity, or inverse. Additive element (+) identity component is composed as 0 and added element inverse of a is expressed as $-a$.
- In distributive law distributivity sum up for number. For any integer and \times is supposed to be distributive over +.
- The integers are an illustration of a ring. The integer has extra properties which make it an necessary space.

A ring is also a field which have an addition property is that every element taking 0 component form an abelian group under multiplication (\times). 1 is the multiplicative identity and multiplicative inverse of a is $1/a$. Complex numbers, real numbers, and the rational numbers are normally example of fields.

Conclusion

In this paper, we discovered that an investigation of sets and with assignment which characterized of sets in modern algebra. As fundamental, in starting we considered the investigation of groups. Group hypothesis is quite possibly most significant spaces of modern arithmetic, and with applications which going from coding to science and physical science also, cryptanalysis. Additionally one of exploration curiosity in this set. More investigation of groups can be attempted in suitable distinction's modules.

On the other hand, we discuss about rings and fields. We had seen some significant properties, which group have same property basically. More work on rings are likewise accessible at different level.

Today, groups, rings and fields, by the side of vector spaces, are observed as old style arithmetical order. There is likewise wide range of new constructions: semigroups, lattices, Boolean algebras, etc.

References



- [1] I. N. Herstein, Topics in Algebra, "An algebraic system can be described as a set of objects together with some operations for combining them." p. 1, Ginn and Company, 1964.
- [2] I. N. Herstein, Topics in Algebra, "...it also serves as the unifying thread which interlaces almost all of mathematics." p. 1, Ginn and Company, 1964
- [3] A. A. Bovdi (2001), "Group algebra", in Hazewinkel, Michiel, Encyclopedia of Mathematics, Springer,
- [4] Milies, César Polcino; Sehgal, Sudarshan K. An introduction to group rings. Algebras and applications, Volume 1. Springer, 2002.
- [5] Charles W. Curtis, Irving Reiner. Representation theory of finite groups and associative algebras, Interscience (1962)
- [6] D.S. Passman, The algebraic structure of group rings, Wiley (1977)
- [7] Berrick, A. J.; Keating, M. E. (2000). An Introduction to Rings and Modules with K-Theory in View. Cambridge University Press. Vijayashree S. Gaonkar International Journal of Scientific and Innovative Mathematical Research (IJSIMR) Page 29
- [8] Cohn, Paul Moritz (1995), Skew Fields: Theory of General Division Rings, Encyclopedia of Mathematics and its Applications, 57, Cambridge University Press,
- [9] Eisenbud, David (1995), Commutative algebra. With a view toward algebraic geometry., Graduate Texts in Mathematics, 150, Springer,
- [10] Gilmer, R.; Mott, J. (1973). "Associative Rings of Order". Proc. Japan Acad. 49: 795–799..
- [11] Kleiner, I., "The Genesis of the Abstract Ring Concept", Amer. Math. Monthly 103, 417–424, 1996. [12] Kleiner, I., "From numbers to rings: the early history of ring theory", Elem. Math. 53 (1998), 18–