*International Journal of Scientific and Innovative Mathematical Research (IJSIMR)*
*Volume 5, Issue 1, January 2017, PP 24-29*
*ISSN 2347-307X (Print) & ISSN 2347-3142 (Online)*
*DOI: http://dx.doi.org/10.20431/2347-3142.0501006*
*www.arcjournals.org*

# A Study on Algebra of Groups and Rings Structures in Mathematics

**Vijayashree S. Gaonkar**

Assistant Professor
Department of Mathematics
Govt. First Grade College, Ankola Taluka,
Uttar kannada Distict, Karnataka State, India

**Abstract:** ***Algebra*** *extends the familiar concepts found in elementary algebra and arithmetic of numbers to more general concepts. Algebra deals with the more general concept of* ***sets*** *is a collection of all objects (called elements) selected by property specific for the set. All collections of the familiar types of numbers are sets. Set theory is a branch of logic and not technically a branch of algebra.* ***Binary operation*** *is meaningless without the set on which the operation is defined. For two elements a and b in a set S, a ∗ b is another element in the set; this condition is called* ***closure****. Addition (+), subtraction (−), multiplication (×), and division (÷) can be binary operations when defined on different sets, as are addition and multiplication of matrices, vectors, and polynomials. Zero is the identity element for addition and one is the identity element for multiplication. For a general binary operator ∗ the identity element e must satisfy a ∗ e = a and e ∗ a = a, and is necessarily unique, if it exists. This holds for addition as a + 0 = a and 0 + a = a and multiplication a × 1 = a and 1 × a = a. Not all sets and operator combinations have an identity element. The* ***inverse*** *of a is written −a, and for multiplication the inverse is written* $a^{-1}$*. A general two-sided inverse element* $a^{-1}$ *satisfies the property that* $a * a^{-1} = e$ *and* $a^{-1} * a = e$*, where e is the identity element. Associativity is, the grouping of the numbers to be added does not affect the sum is (2 + 3) + 4 = 2 + (3 + 4).* ***Commutative*** *is, the order of the numbers does not affect the result is 2 + 3 = 3 + 2. Combining the concepts gives group and ring one of the most important structures in mathematics. A* ***group*** *is a combination of a set S and a single binary operation is an identity element e exists, such that for every member a of S, e ∗ a and a ∗ e are both identical to a. A group is also commutative—that is, for any two members a and b of S, a ∗ b is identical to b ∗ a—then the group is said to be abelian. A* ***ring*** *has two binary operations (+) and (×), with × distributive over +. Under the first operator (+) it forms an abelian group. Under the second operator (×) it is associative, but it does not need to have identity, or inverse, so division is not required. The additive (+) identity element is written as 0 and the additive inverse of a is written as −a.*

**Keyword:** *Groups, Rings and Fields are axiomatically and algebra*

## 1. INTRODUCTION

The roots of algebra can be traced to the ancient **Babylonians**, who developed an advanced arithmetical system with which they were able to do calculations in an algorithmic fashion. The Babylonians developed formulas to calculate solutions for problems typically solved today by using linear equations, quadratic equations, and indeterminate linear equations. By contrast, most Egyptians of this era, as well as Greek and Chinese mathematics in the 1st millennium BC, usually solved such equations by geometric methods, such as those described in the ***Rhind Mathematical Papyrus,*** **Euclid's** ***Elements***, and ***The Nine Chapters on the Mathematical Art***. The geometric work of the Greeks, typified in the ***Elements***, provided the framework for generalizing formulae beyond the solution of particular problems into more general systems of stating and solving equations, although this would not be realized until mathematics developed in medieval Islam.

By the time of **Plato**, Greek mathematics had undergone a drastic change. The Greeks created a geometric algebra where terms were represented by sides of geometric objects, usually lines, that had letters associated with them. Diophantus (3rd century AD) was an Alexandrian Greek mathematician

and the author of a series of books called ***Arithmetica***. These texts deal with solving algebraic equations, and have led, in number theory to the modern notion of Diophantine equation.

Earlier traditions discussed above had a direct influence on the **Persian Muḥammad ibn Mūsā al-Khwārizmī** (c. 780–850). He later wrote ***The Compendious Book on Calculation by Completion and Balancing***, which established algebra as a mathematical discipline that is independent of geometry and arithmetic.

The Hellenistic mathematicians Hero of Alexandria and Diophantus as well as Indian mathematicians such as **Brahmagupta** continued the traditions of Egypt and Babylon, though Diophantus' *Arithmetica* and Brahmagupta's *Brāhmasphuṭasiddhānta* are on a higher level. For example, the first complete arithmetic solution (including zero and negative solutions) to quadratic equations was described by Brahmagupta in his book *Brahmasphutasiddhanta*. Later, Persian and Arabic mathematicians developed algebraic methods to a much higher degree of sophistication. Although Diophantus and the Babylonians used mostly special *ad hoc* methods to solve equations, Al-Khwarizmi's contribution was fundamental. He solved linear and quadratic equations without algebraic symbolism, negative numbers or zero, thus he had to distinguish several types of equations.

In the context where algebra is identified with the theory of equations, the Greek mathematician **Diophantus** has traditionally been known as the "**father of algebra**" but in more recent times there is much debate over whether **al-Khwarizmi**, who founded the discipline of ***al-jabr***, deserves that title instead. Those who support Diophantus point to the fact that the algebra found in ***Al-Jabr*** is slightly more elementary than the algebra found in *Arithmetica* and that *Arithmetica* is syncopated while *Al-Jabr* is fully rhetorical. Those who support **Al-Khwarizmi** point to the fact that he introduced the methods of "reduction" and "balancing" (the transposition of subtracted terms to the other side of an equation, that is, the cancellation of like terms on opposite sides of the equation) which the term ***al-jabr*** originally referred to, and that he gave an exhaustive explanation of solving quadratic equations, supported by geometric proofs, while treating algebra as an independent discipline in its own right. His algebra was also no longer concerned "with a series of problems to be resolved, but an exposition which starts with primitive terms in which the combinations must give all possible prototypes for equations, which henceforward explicitly constitute the true object of study". He also studied an equation for its own sake and "in a generic manner, insofar as it does not simply emerge in the course of solving a problem, but is specifically called on to define an infinite class of problems".

Another Persian mathematician Omar Khayyam is credited with identifying the foundations of algebraic geometry and found the general geometric solution of the cubic equation. His book ***Treatise on Demonstrations of Problems of Algebra*** (1070), which laid down the principles of algebra, is part of the body of Persian mathematics that was eventually transmitted to Europe. Yet another Persian mathematician, Sharaf al-Dīn al-Tūsī, found algebraic and numerical solutions to various cases of cubic equations. He also developed the concept of a function. The Indian mathematicians Mahavira and Bhaskara II, the Persian mathematician Al-Karaji, and the Chinese mathematician Zhu Shijie, solved various cases of cubic, quartic, quintic and higher-order polynomial equations using numerical methods. In the 13th century, the solution of a cubic equation by Fibonacci is representative of the beginning of a revival in European algebra. As the Islamic world was declining, the European world was ascending. And it is here that algebra was further developed.

Italian mathematician **Girolamo Cardano** published the solutions to the cubic and quartic equations in his 1545 book ***Ars magna*.**

François Viète's work on new algebra at the close of the 16th century was an important step towards modern algebra. In 1637, René Descartes published ***La Géométrie***, inventing analytic geometry and introducing modern algebraic notation. Another key event in the further development of algebra was the general algebraic solution of the cubic and quartic equations, developed in the mid-16th century. The idea of a determinant was developed by Japanese mathematician **Seki Kōwa** in the 17th century, followed independently by **Gottfried Leibniz** ten years later, for the purpose of solving systems of simultaneous linear equations using matrices. Gabriel Cramer also did some work on matrices and determinants in the 18th century. Permutations were studied by **Joseph-Louis Lagrange** in his 1770 paper ***Réflexions sur la résolution algébrique des équations*** devoted to solutions of algebraic equations, in which he introduced Lagrange resolvents. **Paolo Ruffini** was the first person to develop

the theory of permutation groups, and like his predecessors, also in the context of solving algebraic equations.

Algebra was developed in the 19th century, deriving from the interest in solving equations, initially focusing on what is now called **Galois Theory**, and on constructability issues. **George Peacock** was the founder of axiomatic thinking in arithmetic and algebra. **Augustus De Morgan** discovered relation algebra in his ***Syllabus of a Proposed System of Logic*. Josiah Willard Gibbs** developed algebra of vectors in three-dimensional space, and **Arthur Cayley** developed algebra of matrices (this is a noncommutative algebra).

## 2. MEANING

In algebra, a **group ring** is a free module and at the same time a ring, constructed in a natural way from any given ring and any given group. As a free module, its ring of scalars is the given ring, and its basis is one-to-one with the given group. As a ring, its addition law is that of the free module and its multiplication extends "by linearity" the given group law on the basis. Less formally, a group ring is a generalization of a given group, by attaching to each element of the group a "**weighting factor**" from a given ring.

If the given ring is **commutative**, a group ring is also referred to as a group algebra, for it is indeed an algebra over the given ring. The apparatus of group rings is especially useful in the theory of group representations.

## 3. DEFINITION

Abstract algebra deals with three kinds of object: ***groups***, ***rings***, **and** ***fields***.

A **group** is defined as: a set of elements, together with an operation performed on pairs of these elements such that:

1. The operation, when given two elements of the set as arguments, always returns an element of the set as its result. It is thus fully defined and closed over the set.
2. One element of the set is an identity element. Thus, if we call our operation op, there is some element of the set e such that for any other element of the set x, e op x = x op e = x.
3. Every element of the set has an inverse element. If we take any element of the set p, there is another element q such that p op q = q op p = e.
4. The operation is associative. For any three elements of the set, (a op b) op c always equals a op (b op c).

A consequence of the third property is that there are no duplicate elements in any row or column of the operation table for a group. A consequence of the fourth property, together with the others, is that every finite group can be expressed as a set of permutations of n objects for some n, where the operation for the group is applying the second permutation to the elements of the first permutation.

There are many different kinds of finite groups, some with very complex structure. Most groups belong to families of groups with an infinite number of members. Thus, addition modulo 5 yields the cyclic group of order 5, and there are cyclic groups of every integer order starting with 2. However, there are 26 groups that don't belong to these infinite families, called sporadic simple groups.

A **ring** is a set of elements with two operations, one of which is like addition, the other of which is like multiplication, which we will call add and mul. It has the following properties:

1. The elements of the ring, together with the addition operation, form a group.
2. Addition is commutative. That is, for any two elements of the set p and q, p add q = q add p. (The word *Abelian* is also used for "commutative", in honor of the mathematician Niels Henrik Abel.)
3. The multiplication operation is associative.
4. Multiplication distributes over addition: that is, for any three elements of the group a, b, and c, a mul ( b add c ) = (a mul b) add (a mul c).

Addition and multiplication modulo 5 and modulo 6 both yield rings. Matrix multiplication also leads to rings as well.

A **field** is a ring in which the elements, other than the identity element for addition, and the multiplication operator, also form a group.

There are only two kinds of finite fields. One kind is the field formed by addition and multiplication modulo a prime number. The other kind of finite field has a number of elements that is a power of a prime number. The addition operator consists of multiple independent additions modulo that prime. The elements of the field can be thought of as polynomials whose coefficients are numbers modulo that prime. In that case, multiplication is polynomial multiplication, where not only are the coefficients modulo that prime, but the polynomials are modulo a special kind of polynomial, known as a *primitive* polynomial. All finite fields, but particularly those of this second kind, are known as *Galois fields*.

*G* be a **group**, written multiplicatively, and *R* be a **ring**. The group ring of *G* over *R*, which we will denote by *R*[*G*] (or simply *RG*), is the set of mappings $f : G \to R$ of finite support,where the module scalar product $\alpha f$ of a scalar $\alpha$ in *R* and a vector (or mapping) *f* is defined as the **vector** , and the module group sum of two vectors *f* and *g* is defined as the vector . To turn the additive group *R* [*G*] into a ring, we define the product of *f* and *g* to be the vector

The summation is legitimate because *f* and *g* are of finite support, and the ring axioms are readily verified. Some variations in the notation and terminology are in use. In particular, the mappings such as $f : G \to R$ are sometimes written as what are called "**formal linear combinations of elements of *G*, with coefficients in *R***"

## Study areas of mathematics with the word algebra in their name:

Some areas of mathematics that fall under the classification abstract algebra has the word algebra in their name are group theory, ring theory, and field theory. In this, article some areas of mathematics with the word "algebra" in the name.

### 4. GROUPS

Combining the above concepts gives one of the most important structures in mathematics is a **group**. A group is a combination of a set *S* and a single binary operation , defined in any way you choose, but with the following properties:

- An identity element *e* exists, such that for every member *a* of *S*, *e* *a* and *a* *e* are both identical to *a*.
- Every element has an inverse: for every member *a* of *S*, there exists a member $a^{-1}$ such that *a* $a^{-1}$ and $a^{-1}$ *a* are both identical to the identity element.
- The operation is associative: if *a*, *b* and *c* are members of *S*, then (*a* *b*) *c* is identical to *a* (*b* *c*).

If a group is also commutative—that is, for any two members *a* and *b* of *S*, *a* *b* is identical to *b* *a*—then the group is said to be abelian. For example, the set of integers under the operation of addition is a group. In this group, the identity element is 0 and the inverse of any element *a* is its negation, $-a$. The associativity requirement is met, because for any integers *a*, *b* and *c*, $(a + b) + c = a + (b + c)$

The nonzero rational numbers form a group under multiplication. Here, the identity element is 1, since $1 \times a = a \times 1 = a$ for any rational number *a*. The inverse of *a* is $1/a$, since $a \times 1/a = 1$.

The integers under the multiplication operation, however, do not form a group. This is because, in general, the multiplicative inverse of an integer is not an integer. For example, 4 is an integer, but its multiplicative inverse is ¼, which is not an integer.

The theory of groups is studied in group theory. A major result in this theory is the classification of finite simple groups, mostly published between about 1955 and 1983, which separates the finite simple groups into roughly 30 basic types.

**Semigroups, quasigroups, and monoids** are structures similar to groups, but more general. They comprise a set and a closed binary operation, but do not necessarily satisfy the other conditions.

A ***semigroup*** has an *associative* binary operation, but might not have an identity element.

A ***monoid*** is a semigroup which does have an identity but might not have an inverse for every element.

A ***quasigroup*** satisfies a requirement that any element can be turned into any other by either a unique left-multiplication or right-multiplication; however the binary operation might not be associative.

## 5. RINGS AND FIELDS

Groups just have one binary operation. To fully explain the behaviour of the different types of numbers, structures with two operators need to be studied. The most important of these are rings, and fields.

A **ring** has two binary operations (+) and (×), with × distributive over +. Under the first operator (+) it forms an ***abelian*** *group*. Under the second operator (×) it is associative, but it does not need to have identity, or inverse, so division is not required. The additive (+) identity element is written as 0 and the additive inverse of $a$ is written as $-a$.

**Distributivity** generalises the ***distributive law*** for numbers. For the integers $(a + b) \times c = a \times c + b \times c$ and $c \times (a + b) = c \times a + c \times b$, and × is said to be *distributive* over +.

The integers are an example of a ring. The integers have additional properties which make it an **integral domain**.

A **field** is a ***ring*** with the additional property that all the elements excluding 0 form an ***abelian group*** under ×. The multiplicative (×) identity is written as 1 and the multiplicative inverse of $a$ is written as $a^{-1}$.

The rational numbers, the real numbers and the complex numbers are all examples of fields.

## 6. CONCLUSION

In this article, we have learnt that modern algebra is a study of sets with operations defined on them. As the main, we have started a systematic study of groups. **Group** theory is one of the most important areas of contemporary mathematics, with applications ranging from physics and chemistry to coding and cryptography. It is also one of the research interests in this school. Further study of groups can be undertaken in the appropriate honours modules.

As our second, we have introduced **rings and fields**. We have seen that there are some important properties, which are very similar to groups. Further courses on rings are also available at the honours level.

Today, **groups, rings and fields**, along with vector spaces, are regarded as classical algebraic disciplines. There is also a wide variety of newer structures: 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.

[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), 18–35.