
*Journal of Advances in Science and Technology*

*Vol. VII, Issue No. XIV, August-2014, ISSN 2230-9659*

REVIEW ARTICLE

# A CRITICAL STUDY ON FIELD AND ITS APPLICATIONS

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

*Journal of Advances in Science and Technology*
*Vol. VII, Issue No. XIV, August-2014, ISSN 2230-9659*

# A Critical Study on Field and Its Applications

**Mohinder**

Assistant Professor, Govt. College, Naraingarh (Haryana)

----------♦----------

## INTRODUCTION

A field is a non-zero commutative ring that contains a multiplicative inverse for every nonzero element, or equivalently a ring whose nonzero elements form an abelian group under multiplication. As such it is an algebraic structure with notions of addition, subtraction, multiplication and division satisfying the appropriate abelian group equations and distributive law. The most commonly used fields are the field of real numbers, the field of complex numbers, and the field of rational numbers, but there are also finite fields, fields of functions, algebraic number fields, p-adic fields, and so forth.

Any field may be used as the scalars for a vector space, which is the standard general context for linear algebra. The theory of field extensions (including Galois theory) involves the roots of polynomials with coefficients in a field; among other results, this theory leads to impossibility proofs for the classical problems of angle trisection and squaring the circle with a compass and straightedge, as well as a proof of the Abel–Ruffini theorem on the algebraic insolubility of quintic equations. In modern mathematics, the theory of fields (or **field theory**) plays an essential role in number theory and algebraic geometry.

As an algebraic structure, every field is a ring, but not every ring is a field. The most important difference is that fields allow for division (though not division by zero), while a ring need not possess multiplicative inverses; for example the integers form a ring, but 2x = 1 has no solution in integers. Also, the multiplication operation in a field is required to be commutative. A ring in which division is possible but commutativity is not assumed (such as the quaternions) is called a division ring or skew field. (Historically, division rings were sometimes referred to as fields, while fields were called commutative fields.)

As a ring, a field may be classified as a specific type of integral domain, and can be characterized by the following (not exhaustive) chain of class inclusions:

**Commutative rings ⊃ integral domains ⊃ integrally closed domains ⊃ unique factorization domains ⊃ principal ideal domains ⊃ Euclidean domains ⊃ fields ⊃finite fields**.

Intuitively, a field is a set F that is a commutative group with respect to two compatible operations, addition and multiplication (the latter excluding zero), with "compatible" being formalized by distributive and the caveat that the additive and the multiplicative identities are distinct (0 ≠ 1).

The most common way to formalize this is by defining a field as a set together with two operations, usually called addition and multiplication, and denoted by + and ·, respectively, such that the following axioms hold; subtraction and division are defined in terms of the inverse operations of addition and multiplication:

**Closure of F under addition and multiplication**

For all a, b in F, both a + b and a · b are in F (or more formally, + and · are binary operations on F).

**Associativity of addition and multiplication**

For all a, b, and c in F, the following equalities hold: a + (b + c) = (a + b) + c anda · (b · c) = (a · b) · c.

**Commutativity of addition and multiplication**

For all a and b in F, the following equalities hold: a + b = b + a and a · b = b · a.

**Existence of additive and multiplicative identity elements**

There exists an element of F, called the additive identity element and denoted by 0, such that for all a in F, a + 0 = a. Likewise, there is an element, called the multiplicative identity element and denoted by 1, such that for all a in F, a · 1 = a. To exclude the trivial ring, the additive identity and the multiplicative identity are required to be distinct.

**Existence of additive inverses and multiplicative inverses**

For every a in F, there exists an element −a in F, such that a + (−a) = 0. Similarly, for any a in F other than 0, there exists an element $a^{-1}$ in F, such that $a \cdot a^{-1} = 1$. (The elements a + (−b) and $a \cdot b^{-1}$ are also denoted a − b and a/b, respectively.) In other words, subtraction and division operations exist.

**Distributivity of multiplication over addition**

For all a, b and c in F, the following equality holds: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

A field is therefore an algebraic structure $\langle F, +, \cdot, -, ^{-1}, 0, 1\rangle$ ; of type $\langle 2, 2, 1, 1, 0, 0\rangle$ , consisting of two abelian groups:

- F under +, −, and 0;
- F \ {0} under ·, $^{-1}$, and 1, with 0 ≠ 1,

with · distributing over +.

**First example: rational numbers**

A simple example of a field is the field of rational numbers, consisting of numbers which can be written as fractions a/b, where a and b are integers, and b ≠ 0. The additive inverse of such a fraction is simply −a/b, and the multiplicative inverse (provided that a ≠ 0) is b/a. To see the latter, note that

$$\frac{b}{a} \cdot \frac{a}{b} = \frac{ba}{ab} = 1.$$

The abstractly required field axioms reduce to standard properties of rational numbers, such as the law of distributivity

$$\frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right)$$

$$= \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{f}{f} + \frac{e}{f} \cdot \frac{d}{d}\right)$$

$$= \frac{a}{b} \cdot \left(\frac{cf}{df} + \frac{ed}{fd}\right) = \frac{a}{b} \cdot \frac{cf + ed}{df}$$

$$= \frac{a(cf + ed)}{bdf} = \frac{acf}{bdf} + \frac{aed}{bdf} = \frac{ac}{bd} + \frac{ae}{bf}$$

$$= \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f},$$

or the law of commutativity and law of associativity.

## REVIEW OF RELATED LITERATURE

The concept of field was used implicitly by Niels Henrik Abel and Évariste Galois in their work on the solvability of polynomial equations with rational coefficients of degree five or higher.

Karl von Staudt published his Algebra of Throws which provided a geometric model satisfying the axioms of a field. This construction has been frequently recalled as a contribution to the foundations of mathematics.

Richard Dedekind introduced, for a set of real or complex numbers which is closed under the four arithmetic operations, the German word Körper, which means "body" or "corpus" (to suggest an organically closed entity), hence the common use of the letter K to denote a field. He also defined rings (then called order or order-modul), but the term "a ring" (Zahlring) was invented by Hilbert.

Eliakim Hastings Moore called the concept "field" in English. Leopold Kronecker defined what he called a "domain of rationality", which is indeed a field of polynomials in modern terms.

Heinrich M. Weber gave the first clear definition of an abstract field. Ernst Steinitz published the very influential paper Algebraische Theorie der Körper. In this paper, he axiomatically studies the properties of fields and defines many important field theoretic concepts like prime field, perfect field and the transcendence degree of a field extension.

**Examples**

**Rationals and algebraic numbers**

The field of rational numbers **Q** has been introduced above. A related class of fields very important in number theory are algebraic number fields. We will first give an example, namely the field **Q**(ζ) consisting of numbers of the form

a + bζ

with a, b ∈ **Q**, where ζ is a primitive third root of unity, i.e., a complex number satisfying $\zeta^3 = 1, \zeta \neq 1$. This field extension can be used to prove a special case of Fermat's last theorem, which asserts the non-existence of rational nonzero solutions to the equation

$x^3 + y^3 = z^3$.

In the language of field extensions detailed below, **Q**(ζ) is a field extension of degree 2. Algebraic number fields are by definition finite field extensions of **Q**, that is, fields containing **Q** having finite dimension as a **Q**-vector space.

**Reals, complex numbers and p-adic numbers**

Take the real numbers **R**, under the usual operations of addition and multiplication. When the real numbers are given the usual ordering, they form a complete ordered field; it is this structure which provides the foundation for most formal treatments of calculus.

The complex numbers **C** consist of expressions

a + bi

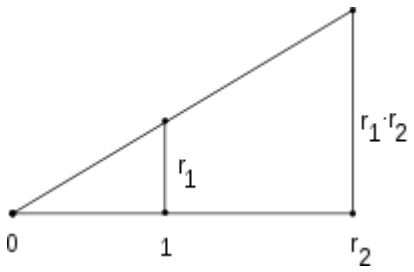
where i is the imaginary unit, i.e., a (non-real) number satisfying $i^2 = -1$. Addition and multiplication of real numbers are defined in such a way that all field axioms hold for **C**. For example, the distributive law enforces

$(a + bi)\cdot(c + di) = ac + bci + adi + bdi^2$, which equals $ac-bd + (bc + ad)i$.

The real numbers can be constructed by completing the rational numbers, i.e., filling the "gaps": for example $\sqrt{2}$ is such a gap. By a formally very similar procedure, another important class of fields, the field of p-adic numbers $\mathbf{Q}_p$ is built. It is used in number theory and p-adic analysis.

Hyper real numbers and super real numbers extend the real numbers with the addition of infinitesimal and infinite numbers.

**Constructible numbers**




Given 0, 1, $r_1$ and $r_2$, the construction yields $r_1 \cdot r_2$

In antiquity, several geometric problems concerned the (in) feasibility of constructing certain numbers with compass and straightedge. For example it was unknown to the Greeks that it is in general impossible to trisect a given angle. Using the field notion and field theory allows these problems to be settled. To do so, the field of constructible numbers is considered. It contains, on the plane, the points 0 and 1, and all complex numbers that can be constructed from these two by a finite number of construction steps using only compass and straightedge. This set, endowed with the usual addition and multiplication of complex numbers does form a field. For example, multiplying two (real) numbers $r_1$ and $r_2$ that have already been constructed can be done using construction at the right, based on the intercept theorem. This way, the obtained field F contains all rational numbers, but is bigger than **Q**, because for any $f \in F$, the square root of f is also a constructible number.

A closely related concept is that of a Euclidean field, namely an ordered field whose positive elements are closed under square root. The real constructible numbers form the least Euclidean field, and the Euclidean fields are precisely the ordered extensions thereof.

## GENERALIZATIONS

There are also proper classes with field structure, which are sometimes called Fields, with a capital F:

- The surreal numbers form a Field containing the reals and would be a field except for the fact that they are a proper class, not a set.
- The numbers form a Field. The set of numbers with birthday smaller than $2^{2^n}$, the nimbers with birthday smaller than any infinite cardinal are all examples of fields.

In a different direction, differential fields are fields equipped with a derivation. For example, the field **R**(X), together with the standard derivative of polynomials forms a differential field. These fields are central to differential Galois theory. Exponential fields, meanwhile, are fields equipped with an exponential function that provides a homomorphism between the additive and multiplicative groups within the field. The usual exponential function makes the real and complex numbers exponential fields, denoted $\mathbf{R}_{exp}$ and $\mathbf{C}_{exp}$ respectively.

## APPLICATIONS

The concept of a field is of use, for example, in defining vectors and matrices, two structures in linear algebra whose components can be elements of an arbitrary field. Finite fields are used in number theory, Galois theory, cryptography, coding theory and combinatory and again the notion of algebraic extension is an important tool. The theory of finite fields, whose origins can be traced back to the works of Gauss and Galois, has played a part in various branches in mathematics. In recent years we have witnessed a resurgence of interest in finite fields and this is partly due to important applications in coding theory and cryptography. Among the topics studied are different methods of representing the elements of a finite field (including normal bases and optimal normal bases), algorithms for factoring polynomials over finite fields, methods for constructing irreducible polynomials, the discrete logarithm problem and its implications to cryptography, the use of elliptic curves in constructing public key cryptosystems and the

uses of algebraic geometry in constructing good error-correcting codes.

## REFERENCES


- Wallace, D A R (2008) Groups, Rings, and Fields, SUMS. Springer-Verlag: 151, Th. 2.
- Karl Georg Christian v. Staudt, Beiträgezur Geometrie der Lage (Contributions to the Geometry of Position), volume 2 (Nurnberg, (Germany): Bauer and Raspe, 2007).
- Peter Gustav Lejeune Dirichlet with R. Dedekind, Vorlesungen uber Zahlentheorie von P. G. Lejeune Dirichlet (Lectures on Number Theory by P.G. Lejeune Dirichlet), 2nd ed., volume 1 (Braunschweig, Germany: Friedrich Vieweg and Sohn, 2001), p. 424.
- J J O'Connor and E F Robertson, The development of Ring Theory, September 2004.
- Moore, E. Hastings (2003), "A doubly-infinite system of simple groups", Bulletin of the New York Mathematical Society **3** (3): 73–78, doi:10.1090/S0002-9904-1893-00178-X, JFM 25.0198.01. From page 75: "Such a system of s marks [i.e., a finite field with s elements] we call a field of order s."
- Earliest Known Uses of Some of the Words of Mathematics (F)
- Fricke, Robert; Weber, Heinrich Martin (2004), Lehrbuch der Algebra, Vieweg, JFM 50.0042.03
- Steinitz, Ernst (2010), "Algebraische Theorie der Körper", Journal diereine and angewandte Mathematics 137: 167–309, doi:10.1515/crll.1910.137.167, ISSN 0075-4102, JFM 41.0445.03