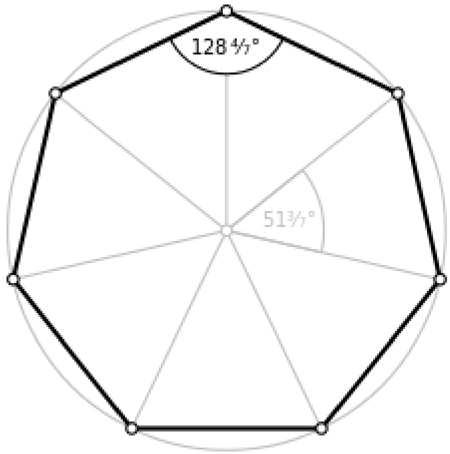
WIKIPEDIA

Field (mathematics)

In mathematics, a **field** is a set on which addition, subtraction, multiplication, and division are defined, and behave as when they are applied to rational and real numbers. A field is thus a fundamental algebraic structure, which is widely used in algebra, number theory and many other areas of mathematics.



The regular 7-gon cannot be constructed using compass and straightedge. This can be proven using the field of constructible numbers.

The best known fields are the field of rational numbers and the field of real numbers. The field of complex numbers is also widely used, not only in mathematics, but also in many areas of science and engineering. Many other fields, such as fields of rational functions, algebraic function fields, algebraic number fields, and *p*-adic fields are commonly used and studied in mathematics, particularly in number theory and algebraic geometry. Most cryptographic protocols rely on finite fields, i.e., fields with finitely many elements.

The relation of two fields is expressed by the notion of a field extension. Galois theory, initiated by Evariste Galois in the 1830s, is devoted to understanding the symmetries of field extensions. Among other results, this theory shows that angle trisection and squaring the circle can not be done with a compass and straightedge. Moreover, it shows that quintic equations are algebraically unsolvable.

Fields serve as foundational notions in several mathematical domains. This includes different branches of analysis, which are based on fields with additional structure. Basic theorems in analysis hinge on the structural properties of the field of real numbers. Most importantly for algebraic purposes, any field may be used as the scalars for a vector space, which is the standard general context for linear algebra. Number fields, the siblings of the field of rational numbers, are studied in depth in number theory. Function fields can help describe properties of geometric objects.

Contents

Definition

In a nutshell, a field is a set, along with two functions defined on that set: an addition function written as $a + b$, and a multiplication function written as $a \cdot b$, both of which behave similarly as they behave for rational numbers and real numbers, including the existence of an additive inverse $-a$ for all elements a, and of a multiplicative inverse b^{-1} for every nonzero element b. This allows us to consider also the so-called *inverse* operations of subtraction $a - b$, and division a / b, via defining:

$$a - b = a + (-b),$$
$$a / b = a \cdot b^{-1}.$$

Classic definition

Formally, a field is a set together with two operations called *addition* and *multiplication*.[1] An operation is a mapping that associates an element of the set to *every* pair of its elements. The result of the addition of a and b is called the *sum* of a and b and denoted $a + b$. Similarly, the result of the multiplication of a and b is called the *product* of a and b, and denoted ab or $a \cdot b$. These operations are required to satisfy the following properties, referred to as *field axioms*. In the following definitions, a, b and c are arbitrary elements of F.

- *Associativity* of addition and multiplication: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- *Commutativity* of addition and multiplication: $a + b = b + a$ and $a \cdot b = b \cdot a$.
- *Additive* and *multiplicative identity*: there exist two different elements 0 and 1 in F such that $a + 0 = a$ and $a \cdot 1 = a$.
- *Additive inverses*: for every a in F, there exists an element in F, denoted $-a$, called *additive inverse* of a, such that $a + (-a) = 0$.

- *Multiplicative inverses* for every $a \neq 0$ in F, there exists an element in F, denoted by a^{-1}, $1/a$, or $\frac{1}{a}$, called the *multiplicative inverse* of a, such that $a \cdot a^{-1} = 1$.
- *Distributivity* of multiplication over addition: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Alternative definitions

Fields can also be defined in different, but equivalent ways. One can alternatively define a field by four binary operations (add, subtract, multiply, divide), and their required properties. Division by zero is, by definition, excluded.[2] In order to avoid existential quantifiers, fields can be defined by two binary operations (addition and multiplication), two unary operations (yielding the additive and multiplicative inverses, respectively), and two nullary operations (the constants 0 and 1). These operations are then subject to the conditions above. This approach avoids existential quantifiers, which is important in constructive mathematics and computing.[3]

Examples

Rational numbers

Rational numbers have been widely used a long time before the elaboration of the concept of field. They are numbers which can be written as fractions a/b, where a and b are integers, and $b \neq 0$. The additive inverse of such a fraction is $-a/b$, and the multiplicative inverse (provided that $a \neq 0$) is b/a, which can be seen as follows:

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

The abstractly required field axioms reduce to standard properties of rational numbers. For example, the law of distributivity can be proven as follows:[4]

$$\begin{aligned}
& \frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) \\
&= \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{f}{f} + \frac{e}{f} \cdot \frac{d}{d}\right) \\
&= \frac{a}{b} \cdot \left(\frac{cf}{df} + \frac{ed}{fd}\right) = \frac{a}{b} \cdot \frac{cf + ed}{df} \\
&= \frac{a(cf + ed)}{bdf} = \frac{acf}{bdf} + \frac{aed}{bdf} = \frac{ac}{bd} + \frac{ae}{bf} \\
&= \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}.
\end{aligned}$$

Real and complex numbers

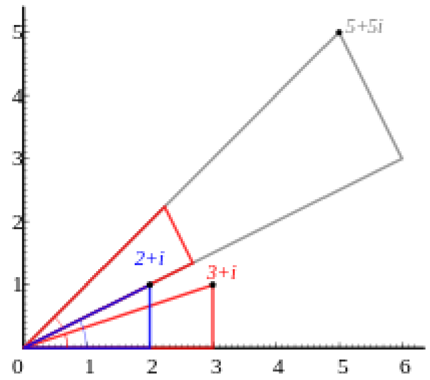
The real numbers $\mathbf{R}$, with the usual operations of addition and multiplication, also form a field. The complex numbers $\mathbf{C}$ consist of expressions

$$a + bi$$

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 $\mathbf{C}$. For example, the distributive law enforces

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

The complex numbers form a field. Complex numbers can be geometrically represented as points in the plane, and addition resp. multiplication of such numbers then corresponds to adding resp. rotating and scaling points. The fields of real and complex numbers are used throughout mathematics, physics, engineering, statistics, and many other scientific disciplines.

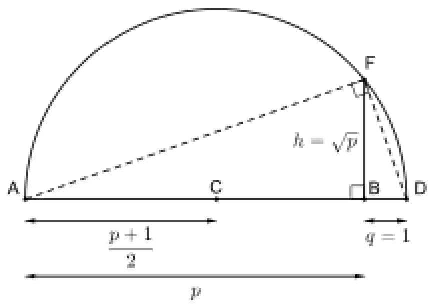


The multiplication of complex numbers can be visualized geometrically by rotations and scalings.

Constructible numbers

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. These problems can be settled using the field of constructible numbers.[5] Real constructible numbers are, by definition, lengths of line segments that can be constructed from the points 0 and 1 in finitely many steps using only compass and straightedge. These numbers, endowed with the field operations of real numbers, restricted to the constructible numbers, form a field, which properly includes the field $\mathbf{Q}$ of rational numbers. The illustration shows the construction of square roots of constructible numbers, not necessarily contained within $\mathbf{Q}$.

Not all real numbers are constructible, it can be shown that $\sqrt[3]{2}$ is not a constructible number, which implies that it is impossible to construct with compass and straightedge the length of the side of a cube with volume 2, another problem posed by the ancient Greeks.



The geometric mean theorem asserts that $h^2 = pq$. Choosing $q = 1$ allows to construct the square root of a given constructible number p. Construct the segments AB, BD, and a semicircle over AD (center at the midpoint C), which intersects the perpendicular line through B in a point F, exactly $h = \sqrt{p}$ apart from B.

A field with four elements

In addition to familiar number systems such as the rationals, there are other, less immediate examples of fields. The following example is a field consisting of four elements called O, I, A, and B. The notation is chosen such that O plays the role of the additive identity element (denoted 0 in the axioms above), and I is the multiplicative identity (denoted 1 in the axioms above). The field axioms can be verified by using some more field theory or by direct computation. For example

$$A \cdot (B + A) = A \cdot I = A, \text{ which equals } A \cdot B + A \cdot A = I + B = A, \text{ as required by the distributivity.}$$

Addition

+	O	I	A	B
O	O	I	A	B
I	I	O	B	A
A	A	B	O	I
B	B	A	I	O

Multiplication

·	O	I	A	B
O	O	O	O	O
I	O	I	A	B
A	O	A	B	I
B	O	B	I	A

This field is called a finite field with four elements, and is denoted $\mathbf{F}_4$ or $\mathrm{GF}(4)$.[6] The subset consisting of O and I (highlighted in red in the tables at the right) is also a field, known as the *binary field* $\mathbf{F}_2$ or $\mathrm{GF}(2)$. In the context of computer science and Boolean algebra, O and I are often denoted respectively by *false* and *true*, the addition is then denoted XOR (exclusive or), and the multiplication is denoted AND. In other words, the structure of the binary field is the basic structure that allows computing with bits.

Elementary notions

In this section, F denotes an arbitrary field and a and b are arbitrary elements of F.

Consequences of the definition

One has $a \cdot 0 = 0$ and $-a = (-1) \cdot a$.[7] In particular, one may deduce the additive inverse of every element as soon as one knows –1.

If $ab = 0$ then a or b must be 0. Indeed, if $a \neq 0$, then $0 = a^{-1} \cdot 0 = a^{-1}(ab) = (a^{-1}a)b = b$. This means that every field is an integral domain.

The additive and the multiplicative group of a field

The axioms concerning the addition operation in a field F are the very same axioms of an abelian group. This group is denoted by $(F, +)$ or often also simply as F and called the additive group of the field F. Similarly, the *nonzero* elements of F together with the multiplication operation form an abelian group, called the multiplicative group and denoted by $(F \setminus \{0\}, \cdot)$ or just $F \setminus \{0\}$ or $F^\times$. The structure of a field is thus the same as specifying such two group structures (on the sets of F and $F \setminus \{0\}$, respectively), obeying the distributivity of one over the other.[nb 1] Some elementary statements about fields can therefore be obtained by applying general facts of groups. For example, the additive and multiplicative inverses $-a$ and a^{-1} are uniquely determined by a.

The requirement $1 \neq 0$ is contained in the definition of a field for the following reason: if $1=0$, this implies that *any* element of F would be 0.[8] The resulting trivial ring (which consists only of a single element), is not considered to be a field, since the multiplicative group of this purported field would be empty, contradicting a standard convention in group theory.

Every finite subgroup of the multiplicative group of a field is cyclic.[9]

Characteristic

In addition to the multiplication of two elements of F, it is possible to define the product $n \cdot a$ of an arbitrary element a of F by a positive integer n to be the n-fold sum

$$a + a + \ldots + a \text{ (which is an element of } F.)$$

If there is no positive integer such that

$$n \cdot 1 = 0,$$

then F is said to have characteristic 0.[10] For example, $\mathbf{Q}$ has characteristic 0 since no positive integer n is zero. Otherwise, if there *is* a positive integer n satisfying this equation, the smallest such positive integer can be shown to be a prime number. It is usually denoted by p and the field is said to have characteristic p then. For example, the field $\mathbf{F}_4$ has characteristic 2 since (in the notation of the above addition table) $\mathrm{I} + \mathrm{I} = \mathrm{O}$.

If F has characteristic p, then $p \cdot a = 0$ for all a in F. This implies that

$$(a + b)^p = a^p + b^p,$$

since all other binomial coefficients appearing in the binomial formula are divisible by p. Here, $a^p := a \cdot a \cdot \ldots \cdot a$ (p factors) is the p-th power, i.e., the p-fold product of the element a. Therefore, the Frobenius map

$$\mathrm{Fr}: F \to F, x \longmapsto x^p$$

is compatible with the addition in F (and also with the multiplication), and is therefore a field homomorphism.[11] The existence of this homomorphism makes fields in characteristic p quite different from fields of characteristic 0.

Subfields and prime fields

Informally, a *subfield* E is a field contained in another field F. More precisely, E is a subset of F that contains 1, and is closed under addition, multiplication, additive inverse and multiplicative inverse of a nonzero element. This means that $1 \in E$, that, for all $a, b \in E$ both $a+b$ and $a \cdot b$ are in E. Moreover, for all $a \neq 0$ in E, one has $-a$ and $1/a$ are in E. It is straightforward to verify that a subfield is indeed a field.

Field homomorphisms are maps $f: E \to F$ between two fields such that $f(e_1 + e_2) = f(e_1) + f(e_2)$, $f(e_1 e_2) = f(e_1) f(e_2)$, and $f(1_E) = 1_F$, where e_1 and e_2 are arbitrary elements of E. All field homomorphisms are injective.[12] If f is also surjective, it is called an isomorphism (or the fields E and F are called isomorphic).

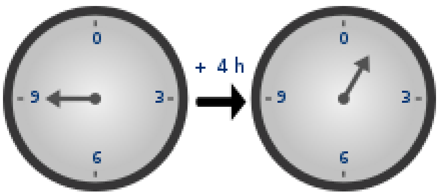
A field is called a prime field if it has no proper (i.e., strictly smaller) subfields. Any field F contains a prime field. If the characteristic of F is p (a prime number), the prime field is isomorphic to the finite field $\mathbf{F}_p$ introduced below. Otherwise the prime field is isomorphic to $\mathbf{Q}$.[13]

Finite fields

Finite fields (also called *Galois fields*) are fields with finitely many elements, whose number is also referred to as the order of the field. The above introductory example $\mathbf{F}_4$ is a field with four elements. Its subfield $\mathbf{F}_2$ is the smallest field, because by definition a field has at least two distinct elements $1 \neq 0$.

The simplest finite fields, with prime order, are most directly accessible using modular arithmetic. For a fixed positive integer n, arithmetic "modulo n" means to work with the numbers

$$\mathbf{Z}/n\mathbf{Z} = \{0, 1, \ldots, n-1\}.$$



In modular arithmetic modulo 12, 9 + 4 = 1 since 9 + 4 = 13 in $\mathbf{Z}$, which divided by 12 leaves remainder 1. Since 12 is not a prime, $\mathbf{Z}/12\mathbf{Z}$ is not a field, though.

The addition and multiplication on this set are done by performing the operation in question in the set $\mathbf{Z}$ of integers, dividing by n and taking the remainder as result. This construction yields a field precisely if n is a prime number. For example, taking the prime $n = 2$ results in the above-mentioned field $\mathbf{F}_2$. For $n = 4$ and more generally, for any composite number (i.e., any number n which can be expressed as a product $n = r \cdot s$ of two strictly smaller natural numbers), $\mathbf{Z}/n\mathbf{Z}$ is not a field: the product of two non-zero elements is zero since $r \cdot s = 0$ in $\mathbf{Z}/n\mathbf{Z}$, which, as was explained above, prevents $\mathbf{Z}/n\mathbf{Z}$ from being a field. The field $\mathbf{Z}/p\mathbf{Z}$ with p elements (p being prime) constructed in this way is usually denoted by $\mathbf{F}_p$.

Every finite field F has $q = p^n$ elements, where p is prime and $n \geq 1$. This statement holds since F may be viewed as a vector space over its prime field. The dimension of this vector space is necessarily finite, say n, which implies the asserted statement.[14]

A field with $q = p^n$ elements can be constructed as the splitting field of the polynomial

$$f(x) = x^q - x.$$

Such a splitting field is an extension of $\mathbf{F}_p$ in which the polynomial f has q zeros. This means f has as many zeros as possible since the degree of f is q. For $q = 2^2 = 4$, it can be checked case by case using the above multiplication table that all four elements of $\mathbf{F}_4$ satisfy the equation $x^4 = x$, so they are zeros of f. By contrast, in $\mathbf{F}_2$, f has only two zeros (namely 0 and 1), so f does not split into linear factors in this smaller field. Elaborating further on basic field-theoretic notions, it can be shown that two finite fields with the same order are isomorphic.[15] It is thus customary to speak of *the* finite field with q elements, denoted by $\mathbf{F}_q$ or $\mathrm{GF}(q)$.

History

Historically, three algebraic disciplines led to the concept of a field: the question of solving polynomial equations, algebraic number theory, and algebraic geometry.[16] A first step towards the notion of a field was made in 1770 by Lagrange, who observed that permuting the zeros x_1, x_2, x_3 of a cubic polynomial in the expression

$$(x_1 + \omega x_2 + \omega^2 x_3)^3$$

(with ω being a third root of unity) only yields two values. This way, Lagrange conceptually explained the classical solution method of del Ferro and Viète, which proceeds by reducing a cubic equation for an unknown x to an quadratic equation for x^3.[17] Together with a similar observation for equations of degree 4, Lagrange thus linked what eventually became the concept of fields and the concept of groups.[18] Vandermonde, also in 1770, and to a fuller extent, Gauss, in his *Disquisitiones Arithmeticae* (1801), studied the equation

$$x^p = 1$$

for a prime p and, again using modern language, the resulting cyclic Galois group. Gauss deduced that a regular p-gon can be constructed if $p = 2^{2^k} + 1$. Building on Lagrange's work, Paolo Ruffini claimed (1799) that quintic equations (polynomial equations of degree 5) can not be solved algebraically, however his arguments were flawed. These gaps were filled by Abel in 1824.[19] Évariste Galois, in 1832, devised necessary and sufficient criteria for a polynomial equation to be algebraically solvable, thus establishing in effect what is known as Galois theory today. Both Abel and Galois worked with what is today called an algebraic number field, but conceived neither an explicit notion of a field, nor of a group.

In 1871 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). The English term "field" was introduced by Moore (1893).[20]

> By a field we will mean every infinite system of real or complex numbers so closed in itself and perfect that addition, subtraction, multiplication, and division of any two of these numbers again yields a number of the system.
>
> — Richard Dedekind, 1871[21]

In 1881 Leopold Kronecker defined what he called a "domain of rationality", which is a field of rational fractions in modern terms. Kronecker's notion did not cover the field of all algebraic numbers (which is a field in Dedekind's sense), but on the other hand was more abstract than Dedekind's in that it made no specific assumption on the nature of the elements of a field. Kronecker interpreted a field such as $\mathbf{Q}(\pi)$ abstractly as the rational function field $\mathbf{Q}(X)$. Prior to this, examples of transcendental numbers were known since Liouville's work in 1844, until Hermite (1873) and Lindemann (1882) proved the transcendence of e and π, respectively.[22]

The first clear definition of an abstract field is due to Weber (1893).[23] In particular, Weber's notion included the field $\mathbf{F}_p$. Veronese (1891) studied the field of formal power series, which led Hensel (1904) to introduce the field of p-adic numbers. Steinitz (1910) synthesized the knowledge of abstract field theory accumulated so far. He axiomatically studied the properties of fields and defined many important field-theoretic concepts. The majority of the theorems mentioned in the sections Galois theory, Constructing fields and Elementary notions can be found in Steinitz's work. Artin & Schreier (1927) linked the notion of orderings in a field, and thus the area of analysis, to purely algebraic properties.[24] Emil Artin redeveloped Galois theory from 1928 through 1942, eliminating the dependency on the primitive element theorem

Constructing fields

Constructing fields from rings

A commutative ring is a set, equipped with an addition and multiplication operation, satisfying all the axioms of a field, except for the existence of multiplicative inverses a^{-1}.[25] For example, the integers $\mathbf{Z}$ form a commutative ring, but not a field: the reciprocal of an integer n is not itself an integer, unless $n = \pm 1$.

In the hierarchy of algebraic structures fields can be characterized as those commutative rings R in which every nonzero element is a unit (which means every element is invertible). Similarly, fields are those commutative rings which have precisely two distinct ideals, (0) and R. Fields are also precisely those commutative rings in which (0) is the only prime ideal.

Given a commutative ring R, there are two ways to construct a field related to R, i.e., two ways of modifying R such that all nonzero elements become invertible: forming the field of fractions, and forming residue fields. The field of fractions of $\mathbf{Z}$ is $\mathbf{Q}$, the rationals, while the residue fields of $\mathbf{Z}$ are the finite fields $\mathbf{F}_p$.

Field of fractions

Given an integral domain R, its field of fractions $Q(R)$ is built with the fractions of two elements of R exactly as $\mathbf{Q}$ is constructed from the integers. More precisely, the elements of $Q(R)$ are the fractions a/b where a and b are in R, and $b \neq 0$. Two fractions a/b and c/d are equal if and only if $ad = bc$. The operation on the fractions work exactly as for rational numbers. For example,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

It is straightforward to show that, if the ring is an integral domain, the set of the fractions form a field.[26]

The field $F(x)$ of the rational fractions over a field (or an integral domain) F is the field of fractions of the polynomial ring $F[x]$. The field $F((x))$ of Laurent series

$$\sum_{i=k}^{\infty} a_i x^i \ (k \in \mathbb{Z}, a_i \in F)$$

over a field F is the field of fractions of the ring $F[[x]]$ of formal power series (in which $k \geq 0$). Since any Laurent series is a fraction of a power series divided by a power of x (as opposed to an arbitrary power series), the representation of fractions is less important in this situation, though.

Residue fields

In addition the field of fractions, which embedds R injectively into a field, a field can be obtained from a commutative ring R by means of a surjective map onto a field F. Any field obtained in this way is a quotient $R\ /\ m$, where m is a maximal ideal of R. If R has only one maximal ideal m, this field is called the residue field of R.[27]

The ideal generated by a single polynomial f in the polynomial ring $R = E[X]$ (over a field E) is maximal if and only if f is irreducible in E, i.e., if f can not be expressed as the product of two polynomials in $E[X]$ of smaller degree. This yields a field

$$F = E[X]\ /\ (p(X)).$$

This field F contains an element x (namely the residue class of X) which satisfies the equation

$$f(x) = 0.$$

For example, $\mathbf{C}$ is obtained from $\mathbf{R}$ by adjoining the imaginary unit symbol i which satisfies $f(i) = 0$, where $f(X) = X^2 + 1$. Moreover, f is irreducible over $\mathbf{R}$, which implies that the map which sends a polynomial $f(X) \in \mathbf{R}[X]$ to $f(i)$ yields an isomorphism

$$\mathbf{R}[X]/(X^2+1) \xrightarrow{\cong} \mathbf{C}.$$

Constructing fields within a bigger field

Fields can be constructed inside a given bigger container field. Suppose given a field E, and a field F containing E as a subfield. For any element x of F, there is a smallest subfield of F containing E and x, called the subfield of F generated by x and denoted $E(x)$.[28] The passage from E to $E(x)$ is referred to by *adjoining an element* to E. More generally, for a subset $S \subset F$, there is a minimal subfield of F containing E and S, denoted by $E(S)$.

The compositum of two subfields E and E' of some field F is the smallest subfield of F containing both E and E'. The compositum can be used to construct the biggest subfield of F satisfying a certain property, for example the biggest subfield of F which is, in the language introduced below, algebraic over E.[nb 2]

Field extensions

The notion of a subfield $E \subset F$ can also be regarded from the opposite point of view, by referring to F being a *field extension* (or just extension) of E, denoted by

F / E (read "F over E).

A basic datum of a field extension is its degree $[F : E]$, i.e., the dimension of F as an E-vector space. It satisfies the formula[29]

$$[G : E] = [G : F]\,[F : E].$$

Extensions whose degree is finite are referred to as finite extensions. The extensions $\mathbf{C} / \mathbf{R}$ and $\mathbf{F}_4 / \mathbf{F}_2$ are of degree 2, whereas $\mathbf{R} / \mathbf{Q}$ is an infinite extension.

Algebraic extensions

A pivotal notion in the abstract study of field extensions F / E are algebraic elements $x \in F$. These are roots (or zeros) of polynomials, i.e., they satisfy a polynomial equation

$$e_n x^n + e_{n-1}x^{n-1} + \cdots + e_1 x + e_0 = 0,$$

for appropriate coefficients $e_n, \ldots, e_0 \in E$, $e_n \neq 0$. For example, $i \in \mathbf{C}$ is algebraic over $\mathbf{R}$ and even over $\mathbf{Q}$ since it satisfies the equation

$$i^2 + 1 = 0.$$

A field extension in which every element of F is algebraic over E is called an algebraic extension. Any finite extension is necessarily algebraic, as can be deduced from the above multiplicativity formula.[30]

The subfield $E(x)$ generated by an element x, as above, is an algebraic extension of E if and only if x is an algebraic element. That is to say, if x is algebraic, all other elements of $E(x)$ are necessarily algebraic as well. Moreover, the degree of the extension $E(x) / E$, i.e., the dimension of $E(x)$ as an E-vector space, equals the minimal degree n such that there is a polynomial equation involving x, as above. If this degree is n, then the elements of $E(x)$ have the form

$$\sum_{k=0}^{n-1} a_k x^k, \quad a_k \in E.$$

For example, the field $\mathbf{Q}(i)$ of Gaussian rationals is the subfield of $\mathbf{C}$ consisting of all numbers of the form $a + bi$ where both a and b are rational numbers: summands of the form i^2 (and similarly for higher exponents) don't have to be considered here, since $a + bi + ci^2$ can be simplified to $a - c + bi$.

Transcendence bases

The above-mentioned field of rational fractions $E(X)$, where X is an indeterminate, is not an algebraic extension of E since there is no polynomial equation with coefficients in E whose zero is X. Elements, such as X, which are not algebraic are called transcendental. Informally speaking, the indeterminate X and its powers do not interact with elements of E. A similar construction can be carried out with a set of indeterminates, instead of just one.

Once again, the field extension $E(x) / E$ discussed above is a key example: if x is not algebraic (i.e., x is not a root of a polynomial with coefficients in E), then $E(x)$ is isomorphic to $E(X)$. This isomorphism is obtained by substituting x to X in rational fractions.

A subset S of a field F is a transcendence basis if it is algebraically independent (don't satisfy any polynomial relations) over E and if F is an algebraic extension of $E(S)$. Any field extension F / E has a transcendence basis.[31] Thus, field extensions can be split into ones of the form $E(S) / E$ (purely transcendental extensions) and algebraic extensions.

Closure operations

A field is algebraically closed if it does not have any strictly bigger algebraic extensions or, equivalently, if any polynomial equation

$$f_n x^n + f_{n-1} x^{n-1} + \cdots + f_1 x + f_0 = 0, \text{ with coefficients } f_n, \ldots, f_0 \in F, n > 0,$$

has a solution $x \in F$.[32] By the fundamental theorem of algebra, $\mathbf{C}$ is algebraically closed, i.e., *any* polynomial equation with complex coefficients has a complex solution. The rational and the real numbers are *not* algebraically closed since the equation

$$x^2 + 1 = 0$$

does not have any rational or real solution. A field containing F is called an *algebraic closure* of F if it is algebraic over F (roughly speaking, not too big compared to F) and is algebraically closed (big enough to contain solutions of all polynomial equations).

By the above, $\mathbf{C}$ is an algebraic closure of $\mathbf{R}$. The situation that the algebraic closure is a finite extension of the field F is quite special: by the Artin-Schreier theorem, the degree of this extension is necessarily 2, and F is elementarily equivalent to $\mathbf{R}$. Such fields are also known as real closed fields.

Any field F has an algebraic closure, which is moreover unique up to (non-unique) isomorphism. It is commonly referred to as *the* algebraic closure and denoted $\overline{F}$. For example, the algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$ is called the field of algebraic numbers. The field $\overline{F}$ is usually rather implicit since its construction requires the ultrafilter lemma, a set-theoretic axiom which is weaker than the axiom of choice.[33] In this regard, the algebraic closure of $\mathbf{F}_q$, is exceptionally simple. It is the union of the finite fields containing $\mathbf{F}_q$ (the ones of order q^n). For any algebraically closed field F of characteristic 0, the algebraic closure of the field $F((t))$ of Laurent series is the field of Puiseux series, obtained by adjoining roots of t.[34]

Fields with additional structure

Since fields are ubiquitous in mathematics and beyond, there are several refinements of the concept which are adapted to the needs of a particular mathematical area.

Ordered fields

A field F is called an *ordered field* if any two elements can be compared, so that $x + y \geq 0$ and $xy \geq 0$ whenever $x \geq 0$ and $y \geq 0$. For example, the reals form an ordered field, with the usual ordering $\geq$. The Artin-Schreier theorem states that a field can be ordered if and only if it is a formally real field, which means that any quadratic equation

$$x_1^2 + x_2^2 + \cdots + x_n^2 = 0$$

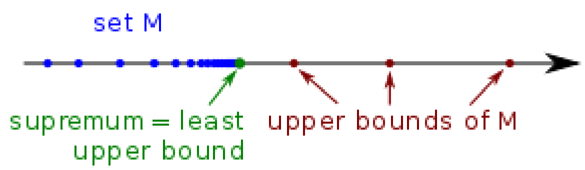
only has the solution $x_1 = x_2 = \ldots = x_n = 0$.[35] The set of all possible orders on a fixed field F is isomorphic to the set of ring homomorphisms from the Witt ring W(F) of quadratic forms over F, to $\mathbf{Z}$.[36]

An Archimedean field is an ordered field such that for each element there exists a finite expression

$$1 + 1 + \cdots + 1$$

whose value is greater than that element, that is, there are no infinite elements. Equivalently, the field contains no infinitesimals (elements which are smaller than all rational numbers); or, yet equivalent, the field is isomorphic to a subfield of $\mathbf{R}$.

An ordered field is Dedekind-complete if all upper bounds, lower bounds (see Dedekind cut) and limits, which should exist, do exist. More formally, each bounded subset of F is required to have a least upper bound. Any complete field is necessarily Archimedean,[37] since in any non-Archimedean field there is neither a greatest infinitesimal nor a least positive rational, whence the sequence $1/2, 1/3, 1/4, \ldots$, every element of which is greater than every infinitesimal, has no limit.



Each bounded real set has a least upper bound.

Since every proper subfield of the reals also contains such gaps, $\mathbf{R}$ is the unique complete ordered field, up to isomorphism.[38] Several foundational results in calculus follow directly from this characterization of the reals.

The hyperreals $\mathbf{R}^*$ form an ordered field which is not Archimedean. It is an extension of the reals obtained by including infinite and infinitesimal numbers. These are larger, respectively smaller than any real number. The hyperreals form the foundational basis of non-standard analysis.

Topological fields

Another refinement of the notion of a field is a topological field, in which the set F is a topological space, such that all operations of the field (addition, multiplication, the maps $a \mapsto -a$ and $a \mapsto a^{-1}$) are continuous maps with respect to the topology of the space.[39] The topology of all the fields discussed below is induced from a metric, i.e., a function

$$d : F \times F \to \mathbf{R},$$

which measures a *distance* between any two elements of F.

The completion of F is another field in which, informally speaking, the "gaps" in the original field F are filled, if there are any. For example, any irrational number x, such as $x = \sqrt{2}$, is a "gap" in the sense that it is a real number that can be approximated arbitrarily closely by rational numbers p/q, in the sense that distance of x and p/q given by the absolute value $|x - p/q|$ is as small as desired. The following table lists some examples of this construction. The fourth column shows an example of a zero sequence, i.e., a sequence whose limit (for $n \to \infty$) is zero.

Field	Metric	Completion	zero sequence
$\mathbf{Q}$	$\|x - y\|$ (usual absolute value)	R	$1/n$
$\mathbf{Q}$	obtained using the p-adic valuation, for a prime number p	$\mathbf{Q}_p$ p-adic numbers	p^n
$F(t)$ (F any field)	obtained using the t-adic valuation	$F((t))$	t^n

The field $\mathbf{Q}_p$ is used in number theory and p-adic analysis. The algebraic closure $\overline{\mathbf{Q}}_p$ carries a unique norm extending the one on $\mathbf{Q}_p$, but is not complete. The completion of this algebraic closure, however, is algebraically closed. Because of its rough analogy to the complex numbers, it is called the field of complex p-adic numbers and is denoted by $\mathbf{C}_p$.[40]

Local fields

The following topological fields are called *local fields*:[41][nb 3]

- finite extensions of $\mathbf{Q}_p$ (local fields of characteristic zero)
- finite extensions of $\mathbf{F}_p((t))$, the field of Laurent series over $\mathbf{F}_p$ (local fields of characteristic p).

These two types of local fields share some fundamental similarities. In this relation, the elements $p \in \mathbf{Q}_p$ and $t \in \mathbf{F}_p((t))$ (referred to as uniformizer) correspond to each other. The first manifestation of this is at an elementary level: the elements of both fields can be expressed as power series in the uniformizer, with coefficients in $\mathbf{F}_p$. (However, since the addition in $\mathbf{Q}_p$ is done using carrying, which is not the case in $\mathbf{F}_p((t))$, these fields are not isomorphic.) The following facts show that this superficial similarity goes much deeper:

- Any first order statement which is true for almost all $\mathbf{Q}_p$ is also true for almost all $\mathbf{F}_p((t))$. An application of this is the Ax-Kochen theorem describing zeros of homogeneous polynomials in $\mathbf{Q}_p$.
- Tamely ramified extensions of both fields are in bijection to one another.
- Adjoining arbitrary p-power roots of p (in $\mathbf{Q}_p$), respectively of t (in $\mathbf{F}_p((t))$), yields (infinite) extensions of these fields known as perfectoid fields. Strikingly, the Galois groups of these two fields are isomorphic, which is the first glimpse of a remarkable parallel between these two fields:[42]

$$\operatorname{Gal}(\mathbf{Q}_p(p^{1/p^\infty})) \cong \operatorname{Gal}(\mathbf{F}_p((t))(t^{1/p^\infty})).$$

Differential fields

Differential fields are fields equipped with a derivation, i.e., allow to take derivatives of elements in the field.[43] For example, the field $\mathbf{R}(X)$, together with the standard derivative of polynomials forms a differential field. These fields are central to differential Galois theory, a variant of Galois theory dealing with linear differential equations.

Galois theory

Galois theory studies algebraic extensions of a field by studying the symmetry in the arithmetic operations of addition and multiplication. An important notion in this area are finite Galois extensions F / E which are by definition those which are separable and normal. The primitive element theorem shows that finite separable extensions are necessarily simple, i.e., of the form

$$F = E[X] / f(X),$$

where f is an irreducible polynomial (as above).[44] For such an extension, being normal and separable means that all zeros of f are contained in F and that f has only simple zeros. The latter condition is always satisfied if E has characteristic 0.

For a finite Galois extension, the Galois group $\mathrm{Gal}(F/E)$ is the group of field automorphisms of F that are trivial on E (i.e., the bijections $\sigma : F \to F$ that preserve addition and multiplication and that send elements of E to themselves). The importance of this group stems from the fundamental theorem of Galois theory which constructs an explicit one-to-one correspondence between the set of subgroups of $\mathrm{Gal}(F/E)$ and the set of intermediate extensions of the extension F/E.[45] By means of this correspondence, group-theoretic properties translate into facts about fields. For example, if the Galois group of a Galois extension as above is not solvable (can not be built from abelian groups), then the zeros of f can *not* be expressed in terms of addition, multiplication, and radicals, i.e., expressions involving $\sqrt[n]{\ }$. For example, the symmetric groups S_n is not solvable for $n \geq 5$. Consequently, as can be shown, the zeros of the following polynomials are not expressible by sums, products, and radicals. For the latter polynomial, this fact is known as the Abel–Ruffini theorem:

> $f(X) = X^5 - 4X + 2$ (and $E = \mathbf{Q}$),[46]
> $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ (where f is regarded as a polynomial in $E(a_0, \ldots, a_{n-1})$, for some indeterminates a_i, E is any field, and $n \geq 5$).

The tensor product of fields is not usually a field. For example, a finite extension F / E of degree n is a Galois extension if and only if there is an isomorphism of F-algebras

$$F \otimes_E F \cong F^n.$$

This fact is the beginning of Grothendieck's Galois theory, a far-reaching extension of Galois theory applicable to algebro-geometric objects.[47]

Invariants of fields

Basic invariants of a field F include the characteristic and the transcendence degree of F over its prime field. The latter is defined as the maximal number of elements in F which are algebraically independent over the prime field. Two algebraically closed fields E and F are isomorphic precisely if these two data agree.[48] This implies that any two uncountable algebraically closed fields of the same cardinality and the same characteristic are isomorphic. For example, $\overline{\mathbf{Q}}_p$, $\mathbf{C}_p$ and $\mathbf{C}$ are isomorphic (but *not* isomorphic as topological fields).

Model theory of fields

In model theory, a branch of mathematical logic, two fields E and F are called elementarily equivalent if every mathematical statement which is true for E is also true for F and conversely. The mathematical statements in question are required to be first-order sentences (involving 0, 1, the addition and multiplication). A typical example is

> $\varphi(E)$ = "for any $n > 0$, any polynomial of degree n in E has a zero in E" (which amounts to saying that E is algebraically closed).

The Lefschetz principle states that $\mathbf{C}$ is elementarily equivalent to any algebraically closed field F of characteristic zero. Moreover, any fixed statement φ holds in $\mathbf{C}$ if and only if it holds in any algebraically closed field of sufficiently high characteristic.[49]

If U is an ultrafilter on a set I, and F_i is a field for every i in I, the ultraproduct of the F_i with respect to U is a field.[50] It is denoted by

$$\mathrm{ulim}_{i\to\infty} F_i,$$

since it behaves in several ways as a limit of the fields F_i: Łoś's theorem states that any first order statement which holds for all but finitely many F_i, also holds for the ultraproduct. Applied to the above sentence φ, this shows that there is an isomorphism[nb 4]

$$\mathrm{ulim}_{p\to\infty} \overline{\mathbf{F}}_p \cong \mathbf{C}.$$

The Ax–Kochen theorem mentioned above also follows from this and an isomorphism of the ultraproducts (in both cases over all primes p)

$$\mathrm{ulim}_p\, \mathbf{Q}_p \cong \mathrm{ulim}_p\, \mathbf{F}_p((t)).$$

In addition, model theory also studies the logical properties of various other types of fields, such as real closed fields or exponential fields (which are equipped with an exponential function $\exp : F \to F^\times$).[51]

The absolute Galois group

For fields which are not algebraically closed (or not separably closed), the absolute Galois group $\mathrm{Gal}(F)$ is fundamentally important: extending the case of finite Galois extensions outlined above, this group governs *all* finite separable extensions of F. By elementary means, the group $\mathrm{Gal}(\mathbf{F}_q)$ can be shown to be the Prüfer group, the profinite completion of $\mathbf{Z}$. This statement subsumes the fact that the only algebraic extensions of $\mathrm{Gal}(\mathbf{F}_q)$ are the fields $\mathrm{Gal}(\mathbf{F}_{q^n})$ for $n > 0$, and that the Galois groups of these finite extensions are given by

$$\mathrm{Gal}(\mathbf{F}_{q^n} / \mathbf{F}_q) = \mathbf{Z}/n\mathbf{Z}.$$

A description in terms of generators and relations is also known for the Galois groups of p-adic number fields (finite extensions of $\mathbf{Q}_p$).[52]

Representations of Galois groups and of related groups such as the Weil group are fundamental in many branches of arithmetic, such as the Langlands program. The cohomological study of such representations is done using Galois cohomology.[53] For example, the Brauer group which is classically defined to be the group of central simple F-algebras, can be reinterpreted as a Galois cohomology group, namely

$$\mathrm{Br}(F) = \mathrm{H}^2(F, \mathbf{G}_{\mathrm{m}}).$$

K-theory

Milnor K-theory is defined as

$$K_n^M(F) = F^\times \otimes \cdots \otimes F^\times / \langle x \otimes (1-x) \mid x \in F \smallsetminus \{0,1\} \rangle.$$

The norm residue isomorphism theorem, proved around 2000 by Vladimir Voevodsky, relates this to Galois cohomology by means of an isomorphism

$$K_n^M(F)/p = H^n(F, \mu_l^{\otimes n}).$$

Algebraic K-theory is related to the group of invertible matrices with coefficients the given field. For example, the process of taking the determinant of an invertible matrix leads to an isomorphism $\mathrm{K}_1(F) = F^\times$. Matsumoto's theorem shows that $\mathrm{K}_2(F)$ agrees with $\mathrm{K}_2{}^{\mathrm{M}}(F)$. In higher degrees, K-theory diverges from Milnor K-theory and remains hard to compute in general.

Applications

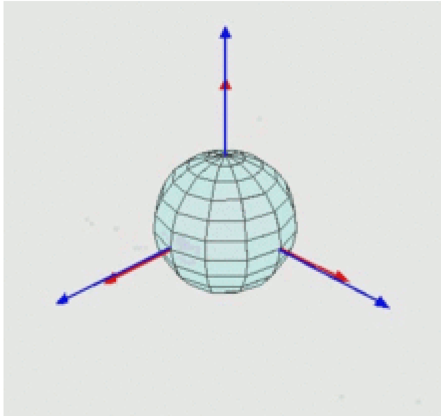
Linear algebra and commutative algebra

If $a \neq 0$, then the equation

$$ax = b$$

has a unique solution x in F, namely $x = b/a$. This observation, which is an immediate consequence of the definition of a field, is the essential ingredient used to show that any vector space has a basis.[54] Roughly speaking, this allows to choose a coordinate system in any vector space, which is of central importance in linear algebra both from a theoretical point of view and also for practical applications.

Modules (the analogue of vector spaces) over most rings, including the ring $\mathbf{Z}$ of integers, have a more complicated structure. A particular situation arises when a ring R is a vector space over a field F in its own right. Such rings are called F-algebras and are studied in depth in the area of commutative algebra. For example, Noether normalization asserts that any finitely generated F-algebra is closely related to (more precisely, finitely generated as a module over) a polynomial ring $F[x_1, ..., x_n]$.[55]



Euler angles express the relation of different coordinate systems, i.e., bases of $\mathbf{R}^3$. They are used in computer graphics.

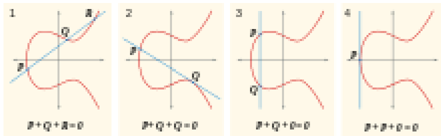
Finite fields: cryptography and coding theory

A widely applied cryptographic routine uses the fact that discrete exponentiation, i.e., computing

$$a^n = a \cdot a \cdot ... \cdot a \text{ (} n \text{ factors, for an integer } n \geq 1\text{)}$$

in a (large) finite field $\mathbf{F}_q$ can be performed much more efficiently than the discrete logarithm, which is the inverse operation, i.e., determining the solution n to an equation

$$a^n = b.$$



The sum of three points P, Q, and R on an elliptic curve E (red) is zero if there is a line (blue) passing through these points.

In elliptic curve cryptography, the multiplication in a finite field is replaced by the operation of adding points on an elliptic curve, i.e., the solutions of an equation of the form

$$y^2 = x^3 + ax + b.$$

Finite fields are also used in coding theory and combinatorics.

Geometry: field of functions

Functions on a topological space X can be added and multiplied pointwise, i.e.,

$$(f \cdot g)(x) = f(x) \cdot g(x).$$

In order to have multiplicative inverses requires considering ratios of functions, i.e., expressions of the form

$$\frac{f(x)}{g(x)}$$

where $g \neq 0$. Such ratios form a field, called the function field of X. This concept is of use when X is a complex manifold X. In this case, f and g are holomorphic functions, i.e., complex differentiable functions. Their ratios are referred to as meromorphic functions.

The function field of an algebraic variety X (a geometric object defined by polynomial equations) consists of ratios of regular functions, i.e., ratios of polynomial functions f and g. The function field of the n-dimensional space over a field k is $k(x_1, ..., x_n)$, i.e., the field consisting of ratios of polynomials f and g in n indeterminates. The function field of X is the same as the one of any open dense subvariety. In other words, the function field is insensitive to replacing X by a (slightly) smaller subvariety

The function field captures important geometric information about X such as its dimension, which equals the transcendence degree of $k(X)$.[56] For curves (i.e., the dimension is one), the function field $k(X)$ is very close to X: if X is smooth and proper (the analogue of being compact), X can be reconstructed, up to isomorphism, from $k(X)$.[nb 5] In higher dimension the function field remembers less, but still decisive information about X. The study of function fields and their geometric meaning in higher dimensions is referred to as birational geometry. The minimal model program attempts to identify the simplest (in a certain precise sense) algebraic varieties with a prescribed function field.

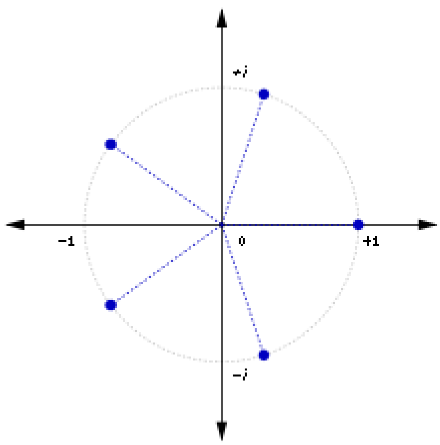
A compact Riemann surface of genus two (two handles). The genus can be read off the field of meromorphic functions on the surface.

Number theory: global fields

Global fields are in the limelight in algebraic number theory and arithmetic geometry. They are, by definition, number fields (finite extensions of $\mathbf{Q}$) or function fields over $\mathbf{F}_q$ (finite extensions of $\mathbf{F}_q(t)$). As for local fields, these two types of fields share several similar features, even though they are of characteristic 0 and positive characteristic, respectively. This function field analogy can help to shape mathematical expectations, often first by understanding questions about function fields, and later treating the number field case. The latter is often more difficult. For example, the Riemann hypothesis concerning the zeros of the Riemann zeta function (open as of 2017) can be regarded as being parallel to the Weil conjectures (proven in 1974 by Deligne).

Cyclotomic fields are among the most intensely studied number fields. They are of the form $\mathbf{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity, i.e., a complex number satisfying $\zeta^n = 1$ and $\zeta^m \neq 1$ for all $m < n$.[57] For n being a regular prime, Kummer used cyclotomic fields to prove Fermat's last theorem, which asserts the non-existence of rational nonzero solutions to the equation

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



The fifth roots of unity form a regular pentagon.

Local fields are completions of global fields. Ostrowski's theorem asserts that the only completions of $\mathbf{Q}$, a global field, are the local fields $\mathbf{Q}_p$ and $\mathbf{R}$. Studying arithmetic questions in global fields may sometimes be done by looking at the corresponding questions locally. This technique is called the local-global principle. For example, the Hasse–Minkowski theorem reduces the problem of finding rational solutions of quadratic equations to solving these equations in $\mathbf{R}$ and $\mathbf{Q}_p$, whose solutions can easily be described.[58]

Unlike for local fields, the Galois groups of global fields are not known. Inverse Galois theory studies the (unsolved) problem whether any finite group is the Galois group $\mathrm{Gal}(F/\mathbf{Q})$ for some number field F.[59] Class field theory describes the abelian extensions, i.e., ones with abelian Galois group, or equivalently the abelianized Galois groups of global fields. A classical statement, the Kronecker–Weber theorem, describes the maximal abelian $\mathbf{Q}^{\mathrm{ab}}$ extension of $\mathbf{Q}$: it is the field

$$\mathbf{Q}(\zeta_n, n \geq 2)$$

obtained by adjoining all primitive n-th roots of unity. Kronecker's Jugendtraum asks for a similarly explicit description of F^{ab} of general number fields F. For imaginary quadratic fields, $F = \mathbf{Q}(\sqrt{-d})$, $d > 0$, the theory of complex multiplication describes F^{ab} using elliptic curves. For general number fields, no such explicit description is known.

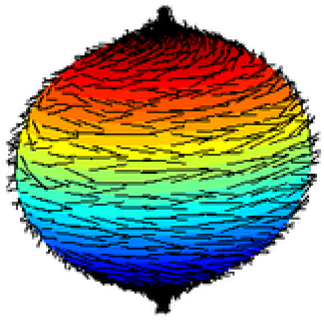
Related notions

In addition to the additional structure that fields may enjoy, fields admit various other related notions. Since $0 \neq 1$ in any field, any field has at least two elements. Nonetheless, there is a concept of field with one element which is suggested to be a limit of the finite fields $\mathbf{F}_p$, as p tends to 1.[60] In addition to division rings, there are various other weaker algebraic structures related to fields such as quasifields, near-fields and semifields.

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 nimbers, a concept from game theory form a Field.[61]

Division rings

Dropping one or several axioms in the definition of a field leads to other algebraic structures. As was mentioned above, commutative rings satisfy all axioms of fields, except for multiplicative inverses. Dropping instead the condition that multiplication is commutative leads to the concept of a *division ring* or *skew field*.[nb 6] The only division rings which are finite-dimensional $\mathbf{R}$-vector spaces are $\mathbf{R}$ itself, $\mathbf{C}$ (which is a field), the quaternions $\mathbf{H}$ (in which multiplication is non-commutative), and the octonions $\mathbf{O}$ (in which multiplication is neither commutative nor associative). This fact was proved using methods of algebraic topology in 1958 by Kervaire and Bott / Milnor.[62] The non-existence of an odd-dimensional division algebra is more classical. It can be deduced from the Hairy ball theorem illustrated at the right.



The hairy ball theorem states that a ball can not be combed. More formally, there is no tangent vector field on the sphere S^2, which is everywhere non-zero.

Notes

1. Equivalently, a field is 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;
   - $F \setminus \{0\}$ under ·, $^{-1}$, and 1, with $0 \neq 1$,

   with · distributing over +. Wallace (1998, Th. 2)
2. Further examples include the maximal unramified extension or the maximal abelian extension within F.
3. Some authors also consider the fields $\mathbf{R}$ and $\mathbf{C}$ to be local fields. On the other hand, these two fields, also called Archimedean local fields, share little similarity with the local fields considered here, to a point that Cassels (1986, p. vi) calls them "completely anomalous".
4. Both $\mathbf{C}$ and $\operatorname{ulim}_p \overline{\mathbf{F}}_p$ are algebraically closed by Łoś's theorem. For the same reason, they both have characteristic zero. Finally, they are both uncountable, so that they are isomorphic.
5. More precisely, there is an equivalence of categories between smooth proper algebraic curves over an algebraically closed field F and finite field extensions of $F(T)$.
6. Historically, division rings were sometimes referred to as fields, while fields were called *commutative fields*.

1. Beachy & Blair (2006, Definition 4.1.1, p. 181)
2. Clark (1984, Chapter 3)
3. Mines, Richman & Ruitenburg (1988, §II.2). See also Heyting field.
4. Beachy & Blair (2006, p. 120, Ch. 3)
5. Artin (1991, Chapter 13.4)
6. Lidl & Niederreiter (2008, Example 1.62)
7. Beachy & Blair (2006, p. 120, Ch. 3)
8. Sharpe (1987, Theorem 1.3.2)
9. See Root of unity § Cyclic groups
10. Adamson (2007, §I.2, p. 10)
11. Escofier (2012, 14.4.2)

12. Adamson (2007, section I.3)
13. Adamson (2007, p. 12)
14. Lidl & Niederreiter (2008, Lemma 2.1, Theorem 2.2)
15. Lidl & Niederreiter (2008, Theorem 1.2.5)
16. Kleiner (2007, p. 63)
17. Kiernan (1971, p. 50)
18. Bourbaki (1994, pp. 75–76)
19. Corry (2004, p.24)
20. *Earliest Known Uses of Some of the Words of Mathematics (F)* (http://jeff560.tripod.com/f.html)
21. Dirichlet (1871, p. 42), translation by Kleiner (2007, p. 66)
22. Bourbaki (1994, p. 81)
23. Corry (2004, p. 33). See also Fricke & Weber (1924).
24. Bourbaki (1994, p. 92)
25. Lang (2002, §II.1)
26. Artin (1991, Section 10.6)
27. Eisenbud (1995, p. 60)
28. Jacobson (2009, p. 213)
29. Artin (1991, Theorem 13.3.4)
30. Artin (1991, Corollary 13.3.6)
31. Bourbaki (1988, Chapter V, §14, No. 2, Theorem 1)
32. Artin (1991, Section 13.9)
33. Banaschewski (1992). Mathoverflow post (https://mathoverflow.net/questions/46566/is-the-statement-that-every-field-has-an-algebraic-closure-known-to-be-equivalent)
34. Ribenboim (1999, p. 186, §7.1)
35. Bourbaki (1988, Chapter VI, §2.3, Corollary 1)
36. Lorenz (2008, §22, Theorem 1)
37. Prestel (1984, Proposition 1.22)
38. Prestel (1984, Theorem 1.23)
39. Warner (1989, Chapter 14)
40. Gouvêa (1997, §5.7)
41. Serre (1979)
42. Scholze (2014)
43. van der Put & Singer (2003, §1)
44. Lang (2002, Theorem V.4.6)
45. Lang (2002, §VI.1)
46. Lang (2002, Example VI.2.6)
47. Borceux & Janelidze (2001). See also Étale fundamental group
48. Gouvêa (2012, Theorem 6.4.8)
49. Marker, Messmer & Pillay (2006, Corollary 1.2)
50. Schoutens (2002, §2)
51. Kuhlmann (2000)
52. Jannsen & Wingberg (1982)
53. Serre (2002)
54. Artin (1991, §3.3)
55. Eisenbud (1995, Theorem 13.3)
56. Eisenbud (1995, §13, Theorem A)
57. Washington (1997)

58. Serre (1978, Chapter IV)
59. Serre (1992)
60. Tits (1957)
61. Conway (1976)
62. Baez (2002)

References

- Adamson, I. T. (2007), *Introduction to Field Theory*, Dover Publications, ISBN 978-0-486-46266-0
- Allenby, R. B. J. T. (1991), *Rings, Fields and Groups*, Butterworth-Heinemann, ISBN 978-0-340-54440-2
- Artin, Michael (1991), *Algebra*, Prentice Hall, ISBN 978-0-13-004763-2, especially Chapter 13
- Artin, Emil; Schreier, Otto (1927), "Eine Kennzeichnung der reell abgeschlossenen Körper", *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* (in German), **5**: 225–231, doi:10.1007/BF02952522, ISSN 0025-5858, JFM 53.0144.01
- Ax, James (1968), "The elementary theory of finite fields", *Ann. of Math. (2)*, **88**: 239–271
- Baez, John C. (2002), "The octonions", *Bull. Amer. Math. Soc.*, **39**: 145–205, doi:10.1090/S0273-0979-01-00934-X
- Banaschewski, Bernhard (1992), "Algebraic closure without choice.", *Z. Math. Logik Grundlagen Math*, **38** (4): 383–385, Zbl 0739.03027
- Beachy, John. A; Blair, William D. (2006), *Abstract Algebra* (3 ed.), Waveland Press, ISBN 1-57766-443-4
- Blyth, T. S.; Robertson, E. F. (1985), *Groups, rings and fields: Algebra through practice*, Cambridge University Press. See especially Book 3 (ISBN 0-521-27288-2) and Book 6 (ISBN 0-521-27291-2).
- Borceux, Francis; Janelidze, George (2001), *Galois theories*, Cambridge University Press, ISBN 0-521-80309-8, Zbl 0978.12004
- Bourbaki, Nicolas (1994), *Elements of the history of mathematics*, Springer, doi:10.1007/978-3-642-61693-8, ISBN 3-540-19376-6, MR 1290116
- Bourbaki, Nicolas (1988), *Algebra II. Chapters 4–7*, Springer, ISBN 0-387-19375-8
- Cassels, J. W. S. (1986), *Local fields*, London Mathematical Society Student Texts, **3**, Cambridge University Press, doi:10.1017/CBO9781139171885, ISBN 0-521-30484-9, MR 0861410
- Clark, A. (1984), *Elements of Abstract Algebra*, Dover Books on Mathematics Series, Dover Publications, ISBN 978-0-486-64725-8
- Conway, John Horton (1976), *On Numbers and Games*, Academic Press Inc. (London) Ltd.
- Corry, Leo (2004), *Modern algebra and the rise of mathematical structures* (2nd ed.), Birkhäuser, ISBN 3-7643-7002-5, Zbl 1044.01008
- Dirichlet, Peter Gustav Lejeune (1871), Dedekind, Richard, ed., *Vorlesungen über Zahlentheorie (Lectures on Number Theory)* (in German), **1** (2nd ed.), Braunschweig, Germany: Friedrich Vieweg und Sohn
- Eisenbud, David (1995), *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, **150**, New York: Springer-Verlag, ISBN 0-387-94268-8, MR 1322960
- Escofier, J. P. (2012), *Galois Theory*, Springer, ISBN 978-1-4613-0191-2
- Fricke, Robert; Weber, Heinrich Martin (1924), *Lehrbuch der Algebra* (in German), Vieweg, JFM 50.0042.03
- Gouvêa, Fernando Q. (1997), *p-adic numbers*, Universitext (2nd ed.), Springer
- Gouvêa, Fernando Q. (2012), *A Guide to Groups, Rings, and Fields*, Mathematical Association of America, ISBN 978-0-88385-355-9
- Hazewinkel, Michiel, ed. (2001) [1994], "Field", *Encyclopedia of Mathematics*, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4
- Hensel, Kurt (1904), "Über eine neue Begründung der Theorie der algebraischen Zahlen", *Journal für die Reine und Angewandte Mathematik* (in German), **128**: 1–32, ISSN 0075-4102, JFM 35.0227.01
- Jacobson, Nathan (2009), *Basic algebra*, **1** (2nd ed.), Dover, ISBN 978-0-486-47189-1
- Jannsen, Uwe; Wingberg, Kay (1982), "Die Struktur der absoluten Galoisgruppe 𝔭-adischer Zahlkörper. [The structure of the absolute Galois group of 𝔭-adic number fields]", *Invent. Math.*, **70** (1): 71–98, MR 0679774

- Kleiner, Israel (2007), *A history of abstract algebra*, Birkhäuser, doi:10.1007/978-0-8176-4685-1, ISBN 978-0-8176-4684-4, MR 2347309
- Kiernan, B. Melvin (1971), "The development of Galois theory from Lagrange to Artin", *Archive for History of Exact Sciences*, **8** (1-2): 40–154, doi:10.1007/BF00327219, MR 1554154
- Kuhlmann, Salma (2000), *Ordered exponential fields*, Fields Institute Monographs, **12**, American Mathematical Society, ISBN 0-8218-0943-1, MR 1760173
- Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics, **211** (3rd ed.), Springer, doi:10.1007/978-1-4613-0041-0, ISBN 0-387-95385-X
- Lidl, Rudolf; Niederreiter, Harald (2008), *Finite fields* (2nd ed.), Cambridge University Press, ISBN 978-0-521-06567-2, Zbl 1139.11053
- Lorenz, Falko (2008), *Algebra, Volume II: Fields with Structures, Algebras and Advanced Topics*, Springer, ISBN 978-0-387-72487-4
- Marker, David; Messmer, Margit; Pillay, Anand (2006), *Model theory of fields*, Lecture Notes in Logic, **5** (2nd ed.), Association for Symbolic Logic, CiteSeerX 10.1.1.36.8448, ISBN 978-1-56881-282-3, MR 2215060
- Mines, Ray; Richman, Fred; Ruitenburg, Wim (1988), *A course in constructive algebra*, Universitext, Springer, ISBN 0-387-96640-4, MR 0919949
- Moore, E. Hastings (1893), "A doubly-infinite system of simple groups", *Bulletin of the American Mathematical Society*, **3** (3): 73–78, doi:10.1090/S0002-9904-1893-00178-X, MR 1557275
- Prestel, Alexander (1984), *Lectures on formally real fields*, Lecture Notes in Mathematics, **1093**, Springer, doi:10.1007/BFb0101548, ISBN 3-540-13885-4, MR 0769847
- Ribenboim, Paulo (1999), *The theory of classical valuations*, Springer Monographs in Mathematics, Springer, doi:10.1007/978-1-4612-0551-7, ISBN 0-387-98525-5, MR 1677964
- Scholze, Peter (2014), "Perfectoid spaces and their Applications" (PDF), *Proceedings of the International Congress of Mathematicians 2014*, ISBN 978-89-6105-804-9
- Schoutens, Hans (2002), *The Use of Ultraproducts in Commutative Algebra*, Lecture Notes in Mathematics, **1999**, Springer, ISBN 978-3-642-13367-1
- Serre, Jean-Pierre (1978), *A course in arithmetic. Translation of* Cours d'arithmetique, Graduate Text in Mathematics, **7** (2nd ed.), Springer, Zbl 0432.10001
- Serre, Jean-Pierre (1979), *Local fields*, Graduate Texts in Mathematics, **67**, Springer, ISBN 0-387-90424-7, MR 0554237
- Serre, Jean-Pierre (1992), *Topics in Galois theory*, Jones and Bartlett Publishers, ISBN 0-86720-210-6, Zbl 0746.12001
- Serre, Jean-Pierre (2002), *Galois cohomology*, Springer Monographs in Mathematics, Translated from the French by Patrick Ion, Berlin, New York: Springer-Verlag, ISBN 978-3-540-42192-4, MR 1867431, Zbl 1004.12003
- Sharpe, David (1987), *Rings and factorization*, Cambridge University Press, ISBN 0-521-33718-6, Zbl 0674.13008
- Steinitz, Ernst (1910), "Algebraische Theorie der Körper (English: Algebraic Theory of Fields)", *Journal für die reine und angewandte Mathematik*, **137**: 167–309, doi:10.1515/crll.1910.137.167, ISSN 0075-4102, JFM 41.0445.03
- Tits, Jacques (1957), "Sur les analogues algébriques des groupes semi-simples complexes", *Colloque d'algèbre supérieure, tenu à Bruxelles du 19 au 22 décembre 1956, Centre Belge de Recherches Mathématiques Établissements Ceuterick, Louvain*, Paris: Librairie Gauthier-Villars, pp. 261–289
- van der Put, M.; Singer, M. F. (2003), *Galois Theory of Linear Differential Equations*, Grundlehren der mathematischen Wissenschaften, **328**, Springer
- von Staudt, Karl Georg Christian (1857), *Beiträge zur Geometrie der Lage (Contributions to the Geometry of Position)*, **2**, Nürnberg (Germany): Bauer and Raspe
- Wallace, D. A. R. (1998), *Groups, Rings, and Fields*, SUMS, **151**, Springer
- Warner, Seth (1989), *Topological fields*, North-Holland, ISBN 0-444-87429-1, Zbl 0683.12014
- Washington, Lawrence C. (1997), *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, **83** (2 ed.), New York: Springer-Verlag, ISBN 0-387-94762-0, MR 1421575
- Weber, Heinrich (1893), "Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie", *Mathematische Annalen* (in German), **43**: 521–549, doi:10.1007/BF01446451, ISSN 0025-5831, JFM 25.0137.01
