Field extension

In mathematics, and in particular, algebra, a field *E* is an **extension field** of a field *F* if *E* contains *F* and the operations of F are those of E restricted to F. Equivalently, *F* is a **subfield** of *E*.[1][2][3] For example, under the usual notions of addition and multiplication, the complex numbers are an extension field of the real numbers; the real numbers are a subfield of the complex numbers.

Field extensions are fundamental in algebraic number theory, and in the study of polynomial roots through Galois theory, and are widely used in algebraic geometry.

Contents

Subfield

Extension field

Caveats

Examples

Algebraic extension

Transcendental extension

Normal, separable and Galois extensions

Generalizations

Extension of scalars

See also

Notes

References

External links

Subfield

A **subfield** of a field *L* is a subset *K* of *L* that is a field with respect to the field operations inherited from *L*. Equivalently, a subfield is a subset that contains 1, and is closed under the operations of addition, subtraction, multiplication, and taking the inverse of a nonzero element of *L*.

As $1 - 1 = 0$, the latter definition implies *K* and *L* have the same zero element.

For example, the field of rational numbers is a subfield of the real numbers, which is itself a subfield of the complex numbers. More generally, the field of rational numbers is (or is isomorphic to) a subfield of any field of characteristic 0.

The characteristic of a subfield is the same as the characteristic of the larger field.

Extension field

If *K* is a subfield of *L*, then *L* is an **extension field** or simply **extension** of *K*, and this pair of fields is a **field extension**. Such a field extension is denoted *L* / *K* (read as "*L* over *K*").

If *L* is an extension of *F* which is in turn an extension of *K*, then *F* is said to be an **intermediate field** (or **intermediate extension** or **subextension**) of *L* / *K*.

Given a field extension L / K, the larger field L is a K-vector space. The dimension of this vector space is called the **degree of the extension** and is denoted by $[L : K]$.

The degree of an extension is 1 if and only if the two fields are equal. In this case, the extension is a **trivial extension**. Extensions of degree 2 and 3 are called **quadratic extensions** and **cubic extensions**, respectively. A **finite extension** is an extension that has a finite degree. The degree of a finite extension L / K is denoted $[L : K]$

Given two extensions L / K and M / L, the extension M / K is finite if and only if both L / K and M / L are finite. In this case, one has

$$[M : K] = [M : L] \cdot [L : K].$$

Given a field extension L / K and a subset S of L, there is a smallest subfield of L that contains K and S. It is the intersection of all subfields of L that contain K and S, and is denoted by $K(S)$. One says that $K(S)$ is the field *generated* by S over K, and that S is a generating set of $K(S)$ over K. When $S = \{x_1, \ldots, x_n\}$ is finite, one writes $K(x_1, \ldots, x_n)$ instead of $K(\{x_1, \ldots, x_n\}),$ and one says that $K(S)$ is finitely generated over K. If S consists of a single element s, the extension $K(s) / K$ is called a simple extension[4][5] and s is called a primitive element of the extension.[6]

An extension field of the form $K(S)$ is often said to result from the *adjunction* of S to K.[7][8]

In characteristic 0, every finite extension is a simple extension. This is the primitive element theorem, which does not hold true for fields of non-zero characteristic.

If a simple extension $K(s) / K$ is not finite, the field $K(s)$ is isomorphic to the field of rational fractions in s over K.

Caveats

The notation L / K is purely formal and does not imply the formation of a quotient ring or quotient group or any other kind of division. Instead the slash expresses the word "over". In some literature the notation $L:K$ is used.

It is often desirable to talk about field extensions in situations where the small field is not actually contained in the larger one, but is naturally embedded. For this purpose, one abstractly defines a field extension as an injective ring homomorphism between two fields. *Every* non-zero ring homomorphism between fields is injective because fields do not possess nontrivial proper ideals, so field extensions are precisely the morphisms in the category of fields.

Henceforth, we will suppress the injective homomorphism and assume that we are dealing with actual subfields.

Examples

The field of complex numbers $\mathbb{C}$ is an extension field of the field of real numbers $\mathbb{R}$, and $\mathbb{R}$ in turn is an extension field of the field of rational numbers $\mathbb{Q}$. Clearly then, $\mathbb{C}/\mathbb{Q}$ is also a field extension. We have $[\mathbb{C} : \mathbb{R}] = 2$ because $\{1, i\}$ is a basis, so the extension $\mathbb{C}/\mathbb{R}$ is finite. This is a simple extension because $\mathbb{C} = \mathbb{R}(i).$ $[\mathbb{R} : \mathbb{Q}] = \mathfrak{c}$ (the cardinality of the continuum), so this extension is infinite.

The field

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\},$$

is an extension field of $\mathbb{Q}$, also clearly a simple extension. The degree is 2 because $\{1, \sqrt{2}\}$ can serve as a basis.

The field

$$\begin{aligned} \mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}(\sqrt{2})\right\} \\ &= \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\right\}, \end{aligned}$$

is an extension field of both$\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}$, of degree 2 and 4 respectively It is also a simple extension, as one can show that

$$\begin{aligned}\mathbb{Q}(\sqrt{2},\sqrt{3}) &= \mathbb{Q}(\sqrt{2}+\sqrt{3}) \\ &= \left\{a+b(\sqrt{2}+\sqrt{3})+c(\sqrt{2}+\sqrt{3})^2+d(\sqrt{2}+\sqrt{3})^3 \mid a,b,c,d\in\mathbb{Q}\right\}.\end{aligned}$$

Finite extensions of $\mathbb{Q}$ are also called algebraic number fields and are important in number theory. Another extension field of the rationals, which is also important in number theory, although not a finite extension, is the field of p-adic numbers $\mathbb{Q}_p$ for a prime number p.

It is common to construct an extension field of a given field K as a quotient ring of the polynomial ring $K[X]$ in order to "create" a root for a given polynomial $f(X)$. Suppose for instance that K does not contain any element x with $x^2 = -1$. Then the polynomial X^2+1 is irreducible in $K[X]$, consequently the ideal generated by this polynomial is maximal, and $L = K[X]/(X^2+1)$ is an extension field of$K$ which *does* contain an element whose square is −1 (namely the residue class of$X$).

By iterating the above construction, one can construct a splitting field of any polynomial from $K[X]$. This is an extension field L of K in which the given polynomial splits into a product of linear factors.

If p is any prime number and n is a positive integer, we have a finite field GF(p^n) with p^n elements; this is an extension field of the finite field $\mathrm{GF}(p) = \mathbb{Z}/p\mathbb{Z}$ with p elements.

Given a field K, we can consider the field $K(X)$ of all rational functions in the variable X with coefficients in K; the elements of $K(X)$ are fractions of two polynomials over K, and indeed $K(X)$ is the field of fractions of the polynomial ring $K[X]$. This field of rational functions is an extension field of$K$. This extension is infinite.

Given a Riemann surface M, the set of all meromorphic functions defined on M is a field, denoted by $\mathbb{C}(M)$. It is a transcendental extension field of $\mathbb{C}$ if we identify every complex number with the corresponding constant function defined on M. More generally, given an algebraic variety V over some field K, then the function field of V, consisting of the rational functions defined on V and denoted by $K(V)$, is an extension field of$K$.

Algebraic extension

An element x of a field extension$L$ / K is algebraic over$K$ if it is a root of a nonzero polynomial with coefficients in K. For example, $\sqrt{2}$ is algebraic over the rational numbers, because it is a root of x^2-2. If an element x of L is algebraic over K, the monic polynomial of lowest degree that has x as a root is called the minimal polynomial of x. This minimal polynomial is irreducible over K.

An element s of L is algebraic over K if and only if the simple extension $K(s)$ /K is a finite extension. In this case the degree of the extension equals the degree of the minimal polynomial, and a basis of the$K$-vector space $K(s)$ consists of $1, s, s^2, \ldots, s^{d-1}$, where d is the degree of the minimal polynomial.

The set of the elements of$L$ that are algebraic over$K$ form a subextension, which is called thealgebraic closure of K in L. This results from the preceding characterization: if s and t are algebraic, the extensions $K(s)$ /K and $K(s)(t)$ /$K(s)$ are finite. Thus $K(s, t)$ /K is also finite, as well as the sub extensions$K(s \pm t)$ /K, $K(st)$ /K and $K(1/s)$ /K (if $s \neq 0$. It follows that$s \pm t$, st and $1/s$ are all algebraic.

An *algebraic extension*L / K is an extension such that every element of L is algebraic over K. Equivalently, an algebraic extension is an extension that is generated by algebraic elements. For example, $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is an algebraic extension of $\mathbb{Q}$, because $\sqrt{2}$ and $\sqrt{3}$ are algebraic over$\mathbb{Q}$.

A simple extension is algebraic if and only if it is finite. This implies that an extension is algebraic if and only if it is the union of its finite subextensions, and that every finite extension is algebraic.

Every field *K* has an algebraic closure, which is up to an isomorphism the largest extension field of *K* which is algebraic over *K*, and also the smallest extension field such that every polynomial with coefficients in *K* has a root in it. For example, $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$, but not an algebraic closure of $\mathbb{Q}$, as it is not algebraic over $\mathbb{Q}$ (for example π is not algebraic over $\mathbb{Q}$).

Transcendental extension

Given a field extension *L* / *K*, a subset *S* of *L* is called algebraically independent over *K* if no non-trivial polynomial relation with coefficients in *K* exists among the elements of *S*. The largest cardinality of an algebraically independent set is called the transcendence degree of *L*/*K*. It is always possible to find a set *S*, algebraically independent over *K*, such that *L*/*K*(*S*) is algebraic. Such a set *S* is called a transcendence basis of *L*/*K*. All transcendence bases have the same cardinality, equal to the transcendence degree of the extension. An extension *L*/*K* is said to be **purely transcendental** if and only if there exists a transcendence basis *S* of *L*/*K* such that *L* = *K*(*S*). Such an extension has the property that all elements of *L* except those of *K* are transcendental over *K*, but, however, there are extensions with this property which are not purely transcendental—a class of such extensions take the form *L*/*K* where both *L* and *K* are algebraically closed. In addition, if *L*/*K* is purely transcendental and *S* is a transcendence basis of the extension, it doesn't necessarily follow that *L* = *K*(*S*). For example, consider the extension $\mathbb{Q}(x, \sqrt{x})/\mathbb{Q}$, where *x* is transcendental over $\mathbb{Q}$. The set $\{x\}$ is algebraically independent since *x* is transcendental. Obviously, the extension $\mathbb{Q}(x, \sqrt{x})/\mathbb{Q}(x)$ is algebraic, hence $\{x\}$ is a transcendence basis. It doesn't generate the whole extension because there is no polynomial expression in x for $\sqrt{x}$. But it is easy to see that $\{\sqrt{x}\}$ is a transcendence basis that generates $\mathbb{Q}(x, \sqrt{x})$, so this extension is indeed purely transcendental.)

Normal, separable and Galois extensions

An algebraic extension *L*/*K* is called normal if every irreducible polynomial in *K*[*X*] that has a root in *L* completely factors into linear factors over *L*. Every algebraic extension *F*/*K* admits a normal closure *L*, which is an extension field of *F* such that *L*/*K* is normal and which is minimal with this property

An algebraic extension *L*/*K* is called separable if the minimal polynomial of every element of *L* over *K* is separable, i.e., has no repeated roots in an algebraic closure over *K*. A Galois extension is a field extension that is both normal and separable.

A consequence of the primitive element theorem states that every finite separable extension has a primitive element (i.e. is simple).

Given any field extension *L*/*K*, we can consider its **automorphism group** Aut(*L*/*K*), consisting of all field automorphisms *α*: *L* → *L* with *α*(*x*) = *x* for all *x* in *K*. When the extension is Galois this automorphism group is called the Galois group of the extension. Extensions whose Galois group is abelian are called abelian extensions.

For a given field extension *L*/*K*, one is often interested in the intermediate fields *F* (subfields of *L* that contain *K*). The significance of Galois extensions and Galois groups is that they allow a complete description of the intermediate fields: there is a bijection between the intermediate fields and the subgroups of the Galois group, described by the fundamental theorem of Galois theory.

Generalizations

Field extensions can be generalized to ring extensions which consist of a ring and one of its subrings. A closer non-commutative analog are central simple algebras (CSAs) – ring extensions over a field, which are simple algebra (no non-trivial 2-sided ideals, just as for a field) and where the center of the ring is exactly the field. For example, the only finite field extension of the real numbers is the complex numbers, while the quaternions are a central simple algebra over the reals, and all CSAs over the reals are Brauer equivalent to the reals or the quaternions. CSAs can be further generalized to Azumaya algebras, where the base field is replaced by a commutative local ring.

Extension of scalars

Given a field extension, one can "extend scalars" on associated algebraic objects. For example, given a real vector space, one can produce a complex vector space via complexification. In addition to vector spaces, one can perform extension of scalars for associative algebras defined over the field, such as polynomials or group algebras and the associated group representations. Extension of scalars of polynomials is often used implicitly, by just considering the coefficients as being elements of a larger field, but may also be considered more formally. Extension of scalars has numerous applications, as discussed in extension of scalars: applications.

See also

- Field theory
- Glossary of field theory
- Tower of fields
- Primary extension
- Regular extension

Notes

1. Fraleigh (1976, p. 293)
2. Herstein (1964, p. 167)
3. McCoy (1968, p. 116)
4. Fraleigh (1976, p. 298)
5. Herstein (1964, p. 193)
6. Fraleigh (1976, p. 363)
7. Fraleigh (1976, p. 319)
8. Herstein (1964, p. 169)

References

- Fraleigh, John B. (1976), *A First Course In Abstract Algebra* (2nd ed.), Reading: Addison-Wesley, ISBN 0-201-01984-1
- Herstein, I. N. (1964), *Topics In Algebra*, Waltham: Blaisdell Publishing Company, ISBN 978-1114541016
- Lang, Serge (2004), *Algebra*, Graduate Texts in Mathematics, **211** (Corrected fourth printing, revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4
- McCoy, Neal H. (1968), *Introduction To Modern Algebra, Revised Edition*, Boston: Allyn and Bacon, LCCN 68015225

External links

- Hazewinkel, Michiel, ed. (2001) [1994], "Extension of a field", *Encyclopedia of Mathematics*, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4