WIKIPEDIA

Irreducible polynomial

In mathematics, an **irreducible polynomial** is, roughly speaking, a non-constant polynomial that cannot be factored into the product of two non-constant polynomials. The property of irreducibility depends on the nature of the coefficients that are accepted for the possible factors, that is, the field or ring to which the coefficients of the polynomial and its possible factors are supposed to belong. For example, the polynomial $x^2 - 2$ is a polynomial with integer coefficients, but, as every integer is also a real number, it is also a polynomial with real coefficients. It is irreducible if it is considered as a polynomial with integer coefficients, but it factors as $(x - \sqrt{2})(x + \sqrt{2})$ if it is considered as a polynomial with real coefficients. One says that the polynomial $x^2 - 2$ is irreducible over the integers but not over the reals.

A polynomial that is irreducible over any field containing the coefficients is absolutely irreducible. By the fundamental theorem of algebra, a univariate polynomial is absolutely irreducible if and only if its degree is one. On the other hand, with several indeterminates, there are absolutely irreducible polynomials of any degree, such as $x^2 + y^n - 1,$ for any positive integer n.

A polynomial that is not irreducible is sometimes said to be **reducible**.[1][2] However, this term must be used with care, as it may refer to other notions of reduction.

Irreducible polynomials appear naturally in the study of polynomial factorization and algebraic field extensions.

It is helpful to compare irreducible polynomials to prime numbers: prime numbers (together with the corresponding negative numbers of equal magnitude) are the irreducible integers. They exhibit many of the general properties of the concept of "irreducibility" that equally apply to irreducible polynomials, such as the essentially unique factorization into prime or irreducible factors.

Contents

Definition

If F is a field, a non-constant polynomial is **irreducible over F** if its coefficients belong to F and it cannot be factored into the product of two non-constant polynomials with coefficients in F.

A polynomial with integer coefficients, or, more generally, with coefficients in a unique factorization domain *R*, is sometimes said to be *irreducible* (or *irreducible over R*) if it is an irreducible element of the polynomial ring, that is, it is not invertible, not zero, and cannot be factored into the product of two non-invertible polynomials with coefficients in *R*. Another definition is frequently used, saying that a polynomial is *irreducible over R* if it is irreducible over the field of fractions of *R* (the field of rational numbers, if *R* is the integers). Both definitions generalize the definition given for the case of coefficients in a field, because, in this case, the non-constant polynomials are exactly the polynomials that are non-invertible and non-zero.

Nature of a factor

The absence of an explicit algebraic expression for a factor does not by itself imply that a polynomial is irreducible. When a polynomial is reducible into factors, these factors may be explicit algebraic expressions or implicit expressions. For example, x^2+2 can be factored explicitly over the complex numbers as $(x-\sqrt{2}i)(x+\sqrt{2}i)$; however, the Abel–Ruffini theorem states that there are polynomials of any degree greater than 4 for which complex factors exist that have no explicit algebraic expression. Such a factor can be written simply as, say, $(x-x_1)$, where x_1 is defined implicitly as a particular solution of the equation that sets the polynomial equal to 0. Further, factors of either type can also be expressed as numerical approximations obtainable by root-finding algorithms, for example as $(x-1.2837\ldots)$.

Simple examples

The following six polynomials demonstrate some elementary properties of reducible and irreducible polynomials:

$$\begin{aligned}
p_1(x) &= x^2+4x+4 \,=(x+2)(x+2)\,,\\
p_2(x) &= x^2-4 \,=(x-2)(x+2)\,,\\
p_3(x) &= 9x^2-3 \,=3(3x^2-1) \,=3(x\sqrt{3}-1)(x\sqrt{3}+1)\,,\\
p_4(x) &= x^2-\frac{4}{9} \,=\left(x-\frac{2}{3}\right)\left(x+\frac{2}{3}\right),\\
p_5(x) &= x^2-2 \,=(x-\sqrt{2})(x+\sqrt{2})\,,\\
p_6(x) &= x^2+1 \,=(x-i)(x+i)\,.
\end{aligned}$$

Over the integers, the first three polynomials are reducible (the third one is reducible because the factor 3 is not invertible in the integers); the last two are irreducible. (The fourth, of course, is not a polynomial over the integers.)

Over the rational numbers, the first two and the fourth polynomials are reducible, but the other three polynomials are irreducible (as a polynomial over the rationals, 3 is a unit, and, therefore, does not count as a factor).

Over the real numbers, the first five polynomials are reducible, but $p_6(x)$ is irreducible.

Over the complex numbers, all six polynomials are reducible.

Over the complex numbers

Over the complex field, and, more generally, over an algebraically closed field, a univariate polynomial is irreducible if and only if its degree is one. This fact is known as the fundamental theorem of algebra in the case of the complex numbers and, in general, as the condition of being algebraically closed.

It follows that every nonconstant univariate polynomial can be factored as

$$a(x-z_1)\cdots(x-z_n)$$

where n is the degree, a is the leading coefficient and $z_1,\ldots,z_n$ are the zeros of the polynomial (not necessarily distinct, and not necessarily having explicit algebraic expressions).

There are irreducible multivariate polynomials of every degree over the complex numbers. For example, the polynomial

$$x^n + y^n - 1,$$

which defines a Fermat curve, is irreducible for every positive n.

Over the reals

Over the field of reals, the degree of an irreducible univariate polynomial is either one or two. More precisely, the irreducible polynomials are the polynomials of degree one and the quadratic polynomials $ax^2 + bx + c$ that have a negative discriminant $b^2 - 4ac.$ It follows that every non-constant univariate polynomial can be factored as a product of polynomials of degree at most two. For example, $x^4 + 1$ factors over the real numbers as $(x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1),$ and it cannot be factored further, as both factors have a negative discriminant: $(\pm\sqrt{2})^2 - 4 = -2 < 0.$

Unique factorization property

Every polynomial over a field F may be factored into a product of a non-zero constant and a finite number of irreducible (over F) polynomials. This decomposition is unique up to the order of the factors and the multiplication of the factors by non-zero constants whose product is 1.

Over a unique factorization domain the same theorem is true, but is more accurately formulated by using the notion of primitive polynomial. A primitive polynomial is a polynomial over a unique factorization domain, such that 1 is a greatest common divisor of its coefficients.

Let F be a unique factorization domain. A non-constant irreducible polynomial over F is primitive. A primitive polynomial over F is irreducible over F if and only if it is irreducible over the field of fractions of F. Every polynomial over F may be decomposed into the product of a non-zero constant and a finite number of non-constant irreducible primitive polynomials. The non-zero constant may itself be decomposed into the product of a unit of F and a finite number of irreducible elements of F. Both factorizations are unique up to the order of the factors and the multiplication of the factors by a unit of F.

This is this theorem which motivates that the definition of *irreducible polynomial over a unique factorization domain* often supposes that the polynomial is non-constant.

All algorithms which are presently implemented for factoring polynomials over the integers and over the rational numbers use this result (see Factorization of polynomials).

Over the integers

The irreducibility of a polynomial over the integers $\mathbb{Z}$ is related to that over the field $\mathbb{F}_p$ of p elements (for a prime p). In particular, if a univariate polynomial f over $\mathbb{Z}$ is irreducible over $\mathbb{F}_p$ for some prime p that does not divide the leading coefficient of f (the coefficient of the higher power of the variable), then f is irreducible over $\mathbb{Z}$. Eisenstein's criterion is a variant of this property where irreducibility over p^2 is also involved.

The converse, however, is not true: there are polynomials of arbitrarily large degree that are irreducible over the integers and reducible over every finite field.[3] A simple example of such a polynomial is $x^4 + 1.$

The relationship between irreducibility over the integers and irreducibility modulo p is deeper than the previous result: to date, all implemented algorithms for factorization and irreducibility over the integers and over the rational numbers use the factorization over finite fields as a subroutine.

The number of irreducible monic polynomials over a field $\mathbb{F}_p$ for prime p is given by the necklace counting function. For p=2, such polynomials are commonly used to generate pseudorandom binary sequences

Algorithms

The unique factorization property of polynomials does not mean that the factorization of a given polynomial may always be computed. Even the irreducibility of a polynomial may not always be proved by a computation: there are fields over which no algorithm can exist for deciding the irreducibility of arbitrary polynomials.[4]

Algorithms for factoring polynomials and deciding irreducibility are known and implemented in computer algebra systems for polynomials over the integers, the rational numbers, finite fields and finitely generated field extension of these fields. All these algorithms use the algorithms for factorization of polynomials over finite fields

Field extension

The notions of irreducible polynomial and of algebraic field extension are strongly related, in the following way.

Let *x* be an element of an extension *L* of a field *K*. This element is said to be *algebraic* if it is a root of a polynomial with coefficients in *K*. Among the polynomials of which *x* is a root, there is exactly one which is monic and of minimal degree, called the minimal polynomial of *x*. The minimal polynomial of an algebraic element *x* of *L* is irreducible, and is the unique monic irreducible polynomial of which *x* is a root. The minimal polynomial of *x* divides every polynomial which has *x* as a root (this is Abel's irreducibility theorem).

Conversely, if $P(X) \in K[X]$ is a univariate polynomial over a field *K*, let $L = K[X]/P(X)$ be the quotient ring of the polynomial ring $K[X]$ by the ideal generated by P. Then L is a field if and only if P is irreducible over K. In this case, if x is the image of X in L, the minimal polynomial of x is the quotient of P by its leading coefficient.

An example of the above is the standard definition of the complex numbers as $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$.

If a polynomial P has an irreducible factor Q over K, which has a degree greater than one, one may apply to Q the preceding construction of an algebraic extension, to get an extension in which P has at least one more root than in K. Iterating this construction, one gets eventually a field over which P factors into linear factors. This field, unique up to a field isomorphism, is called the splitting field of P.

Over an integral domain

If *R* is an integral domain, an element *f* of *R* that is neither zero nor a unit is called irreducible if there are no non-units *g* and *h* with *f* = *gh*. One can show that every prime element is irreducible;[5] the converse is not true in general but holds in unique factorization domains. The polynomial ring *F*[*x*] over a field *F* (or any unique-factorization domain) is again a unique factorization domain. Inductively, this means that the polynomial ring in *n* indeterminants (over a ring *R*) is a unique factorization domain if the same is true for *R*.

See also

- Gauss's lemma (polynomial)
- Rational root theorem, a method of finding whether a polynomial has a linear factor with rational coefficients
- Eisenstein's criterion
- Perron method
- Hilbert's irreducibility theorem
- Cohn's irreducibility criterion
- Irreducible component of a topological space
- Factorization of polynomials over finite fields
- Quartic function § Reducible quartics
- Cubic function § Factorization
- Casus irreducibilis, the irreducible cubic with three real roots
- Quadratic equation § Quadratic factorization

Notes

1. Gallian 2012, p. 311.
2. Mac Lane and Birkhoff (1999) do not explicitly define "reducible", but they use it in several places. For example: "For the present, we note only that any reducible quadratic or cubic polynomial must have a linear factor." (p. 268).
3. David Dummit; Richard Foote (2004). "chapter 9, Proposition 12". *Abstract Algebra*. John Wiley & Sons, Inc. p. 309. ISBN 0-471-43334-9.
4. Fröhlich, A.; Shepherson, J. C. (1955), "On the factorisation of polynomials in a finite number of steps", *Mathematische Zeitschrift*, **62** (1), doi:10.1007/BF01180640 (https://doi.org/10.1007/BF01180640), ISSN 0025-5874 (https://www.worldcat.org/issn/0025-5874)
5. Consider p a prime that is reducible: $p = ab$. Then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. Say $p \mid a \Rightarrow a = pc$, then we have: $p = ab = pcb \Rightarrow p(1 - cb) = 0$. Because R is a domain, we have $cb = 1$. So b is a unit, and p is irreducible.

References

- Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics, **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR 1878556. This classical book covers most of the content of this article.
- Gallian, Joseph (2012), *Contemporary Abstract Algebra* (8th ed.), Cengage Learning
- Lidl, Rudolf; Niederreiter, Harald (1997), *Finite fields* (2nd ed.), Cambridge University Press, ISBN 978-0-521-39231-0, pp. 91.
- Mac Lane, Saunders; Birkhoff, Garrett (1999), *Algebra* (3rd ed.), American Mathematical Society
- Menezes, Alfred J.; Van Oorschot, Paul C.; Vanstone, Scott A. (1997), *Handbook of applied cryptography*, CRC Press, ISBN 978-0-8493-8523-0, pp. 154.

External links

- Weisstein, Eric W. "Irreducible Polynomial". *MathWorld*.
- Irreducible Polynomial at PlanetMath.org.
- Information on Primitive and Irreducible Polynomials, The (Combinatorial) Object Server.